# (I) SentinelOne™

# SentinelOne for QRadar v3.5.x

Integration Guide

3 October 2019

#### Copyright © 2019 SentinelOne

This document contains SentinelOne proprietary information owned by Sentinel Labs, Inc. ("SentinelOne"), and is provided for use only in connection with SentinelOne's Endpoint Protection Platform. This document may also contain confidential information, and may not be reproduced or otherwise used without the express permission of SentinelOne. SentinelOne reserves the right to amend this document in its sole discretion. SentinelOne® and the SentinelOne logos are the registered and unregistered trademarks of Sentinel Labs, Inc. The SentinelOne Solutions are protected under various state and federal laws, including without limitation, US Patent Nos. 9,710,648 and 10,102,374. Please contact SentinelOne with questions.

# **Table of Contents**

| 1. QRadar and SentinelOne Integration                              | 1  |
|--|----|
| 1.1. QRadar and SentinelOne Integration Highlights                 | 1  |
| 2. Requirements  | 5  |
| 3. The SentinelOne DSM for QRadar                                  | 6  |
| 3.1. Installing the SentinelOne DSM in QRadar                      | 6  |
| 3.2. Adding SentinelOne as a Log Source for QRadar                 | 9  |
| 3.3. Integrating Your QRadar Syslog Server to SentinelOne          | 12 |
| 3.4. Seeing SentinelOne Events in QRadar                           | 15 |
| 4. The SentinelOne App for QRadar                                  | 21 |
| 4.1. Installing the SentinelOne App in QRadar                      | 21 |
| 4.2. Generate an API Token   | 27 |
| 4.3. Adding SentinelOne Management Consoles to the SentinelOne App | 28 |
| 4.4. Using the SentinelOne App                                     | 29 |
| 5. Upgrading From the Beta Version                                 | 34 |
| 6. Advanced Configuration  | 36 |
| 6.1. Configuring the Syslog Format                                 | 36 |
| 6.2. Finding SentinelOne Events                                    | 37 |
| 6.3. Regular Expressions for Mapping                               | 38 |
| 7. Troubleshooting   | 40 |
|  |    |

# **1. QRadar and SentinelOne Integration**

The integration of IBM® QRadar® Security Information and Event Management (SIEM) with SentinelOne® empowers organizations to combine the strengths of QRadar to consolidate, correlate, and aggregate log events and network flow data, with the visibility, detection, response, remediation and forensics capabilities of SentinelOne.

These are the components of this integration:

- SentinelOne Device Support Module (DSM) for QRadar: Collects the Syslog output from the SentinelOne Management as a log source for QRadar. Use the QRadar Console to see information in your environment, gathered from SentinelOne.
- SentinelOne App: An application running on the QRadar platform enabling you to see information about the endpoints in your environment, taken from SentinelOne, and take action. From the App, you can go to the SentinelOne Management Console.

# **1.1. QRadar and SentinelOne Integration Highlights**

After installing and running the SentinelOne DSM and App for QRadar, you can:

|            | 3M QRadar                    |                                   |                  |                  |            |                |                                 | ¢ 2                       |
|------------|------------------------------|-----------------------------------|------------------|------------------|------------|----------------|---------------------------------|---------------------------|
| Dashboard  | Offenses Log Activity Netwo  | ork Activity Assets Reports Admin | SentinelOne      |                  |            |                |                                 | System Time: 12:38 PM     |
| 🗰 Sentinek | Oner 🔄 🖪 Analyze 🛛 🖵 Network | III Settings                      | •                |                  |            |                |                                 | Scope purple   Site All - |
| Filter:    | Resolved                     |                                   | Migration Status |                  | Time       |                | Search                          | Apply                     |
|            | Select *                     |                                   | Select *         |                  | All time 👻 |                | Q. Search                       | 10 Results -              |
| Status     | File Name                    | Endpoint                          | Created          | Updated          | Site       | Classification | Action Done                     |                           |
|            | RwawWeY0.exe                 | desktop Enterprise-Desktop        | 05/05/2019 07:11 | 05/05/2019 08:02 | Demo TEST  | Malware        | quarantine, kill                |                           |
| 0          | <u>CV.exe</u>                | desktop Enterprise-Desktop        | 05/05/2019 07:11 | 05/05/2019 08:02 | Demo TEST  | Malware        | rollback, quarantine, kill, ren | nediate                   |
|            | <u>CV.exe</u>                | desktop Enterprise-Desktop        | 05/05/2019 07:11 | 05/05/2019 08:02 | Demo TEST  | Malware        | rollback, quarantine, kill, ren | nediate                   |
|            | <u>CV.exe</u>                | desktop Enterprise-Desktop        | 05/05/2019 07:11 | 05/05/2019 08:02 | Demo TEST  | Malware        | quarantine, kill                |                           |
|            | CV.exe                       | desktop Enterprise-Desktop        | 05/05/2019 07:11 | 05/05/2019 08:02 | Demo TEST  | Malware        | quarantine, kill                |                           |
|            | CV.exe                       | desktop Enterprise-Desktop        | 05/05/2019 07:08 | 05/05/2019 07:09 | Demo TEST  | Malware        | quarantine, kill                |                           |
|            | CV.exe                       | desktop Enterprise-Desktop        | 05/05/2019 07:08 | 05/05/2019 07:09 | Demo TEST  | Malware        | quarantine, kill                |                           |
|            | xwU6h1MX.exe                 | desktop Enterprise-Desktop        | 05/05/2019 06:45 | 05/05/2019 06:52 | Demo TEST  | Ransomware     | rollback, quarantine, kill, ren | nediate                   |
|            | RwawWeY0.exe                 | desktop Enterprise-Desktop        | 05/05/2019 06:45 | 05/05/2019 06:52 | Demo TEST  | Ransomware     | quarantine, kill                |                           |
|            | xwU6h1MX.exe                 | desktop Enterprise-Desktop        | 05/05/2019 06:45 | 05/05/2019 06:52 | Demo TEST  | Ransomware     | rollback, quarantine, kill, re  | nediate                   |
|            |                              |                                   | 1 2 3            | 4 5 6 7 8 9 10   |            |                |                                 |                           |

• View a list of threats from the SentinelOne App for QRadar Analyze page.

• View threat details and mitigate threats from the QRadar console. SentinelOne authorized users can also click a hyperlink to the SentinelOne Management Console Forensics page.



• Filter threat lists from the SentinelOne App for QRadar Network page.

|                            |   |  |   |   |  | ¢ 2   |
|----------------------------|---|--|---|---|--|---|
| rk Activity Assets Reports | Admin SentinelOne   |  |   |   |  | System Time: 12:42 PM   |
| ₩ Settings                 |   |  |   |   |  | Scope purple   Site All -   |
| Search                     |   | Active   |   |   | OS   | Apply   |
| nirg                       |   | All 👻  |   |   | All 👻  | 10 Results -  |
| Site                       | Group   | Domain   | Console Visible IP  | Agent Version   | Last Logged User   | Last Active   |
| AcmeHoldings               | Default Group   | local  |   | 2.6.5.2559  | nirg   | 23/04/2019 13:25  |
| AcmeHoldings               | Default Group   | local  |   | 2.6.5.1704  |  | 22/04/2019 18:38  |
| AcmeHoldings               | Default Group   | localdomain  |   | 2.6.5.1704  |  | 05/05/2019 09:42  |
| AcmeHoldings               | Default Group   | localdomain  |   | 2.6.4.1685  |  | 22/04/2019 17:32  |
| ABC-Corp                   | Default Group   | unknown  | 10.00   | 3.0.0.305   | unknown  | 03/05/2019 13:24  |
| ABC-Corp                   | Default Group   | unknown  |   | 3.0.0.1   |  | 02/05/2019 17:04  |
| ABC-Corp                   | Default Group   | local  |   | 3.0.1.391   |  | 02/05/2019 17:02  |
| ABC-Corp                   | Default Group   | sentinel.local   | 10.00   | 3.0.1.391   |  | 29/04/2019 18:59  |
| ABC-Corp                   | Default Group   | unknown  |   | 3.0.2.400   |  | 05/05/2019 09:42  |
|                            | Attack         Association         Association           INT Settings         Interpretation         Interpretation           Search         AcmetHoldings         Interpretation           AcmetHoldings         AcmetHoldings         Interpretation           AcmetHol | Atexte     Report     Atexte     Sectoration       It Setting:     Croup       State     Croup       Atexte Holdings     Capatul Group       Atexte Holdings     Capatul Group | Atech     Atech     Atech     Atech       11 Setting     Croup     Consin       Site     Croup     Consin       ArmeHoldings     Default Group     Coal       ARC-Corp     Default Group     Coal | Active     Active       Basting     Active       Size     Group     Domain       Concole Vaible P       Acmettokings     Default Group     local       Acmettokings     Default Group     local       Acmettokings     Default Group     localdomain       Accorp     Default Group     localdomain       ABC-Corp     Default Group     local       ABC-Corp     Default Group     local | Active     Active     Service     Active       It Setting:     Active     Active       Size     Group     Domain     Concole Vasible IP     Apent Version       AcmetHoldings     Default Group     Boal     Concole Vasible IP     Apent Version       AcmetHoldings     Default Group     Boal     Concole Vasible IP     Apent Version       AcmetHoldings     Default Group     Boal     Concole Vasible IP     Apent Version       AcmetHoldings     Default Group     Boal     Concole Vasible IP     Apent Version       AcmetHoldings     Default Group     Boaldomain     2.85.1764     2.85.1764       AcmetHoldings     Default Group     Iccaldomain     2.85.1764     2.85.1764       AcmetHoldings     Default Group     Iccaldomain     2.85.1764     2.85.1764       ABC-Corp     Default Group     Iccaldomain     2.85.1764     3.0.305       ABC-Corp     Default Group     Inknown     3.0.3.01     3.0.31       ABC-Corp     Default Group     Iccaldomain     3.0.1391       ABC-Corp     Default Group     Iccaldomain     3.0.1391       ABC-Corp     Default Group     Iccaldomain     3.0.1391       ABC-Corp     Default Group     Iccaldomain     3.0.1391 | Autor       Autor       Exercision         Search       Arive       Arive       OS<br>Arive       OS<br>Arive         Size       Group       Domin       Conolo Vable IP       Agent Varion       Lat Logged Uar         ArmeHoldings       Ofeduit Group       Ioal       Conolo Vable IP       Agent Varion       Lat Logged Uar         ArmeHoldings       Default Group       Ioal       Conolo Vable IP       Agent Varion       Lat Logged Uar         ArmeHoldings       Default Group       Ioal       Conolo Vable IP       Agent Varion       Lat Logged Uar         ArmeHoldings       Default Group       Ioal       Conolo Vable IP       Agent Varion       Lat Logged Uar         ArmeHoldings       Default Group       Ioaldomain       Eds.5754       Lat Logged Uar         ArmeHoldings       Default Group       Ioaldomain       Eds.1764       Lat Logged Uar         ArmeHoldings       Default Group       Ioaldomain       Eds.1764 |

• Disconnect an endpoint from the network and see endpoint associated information, such as the last logged in user and threat history.

|                         | Radar                              |                                  |                                    |                  |                                       |                   | ¢ º                                  |
|-------------------------|------------------------------------|----------------------------------|------------------------------------|------------------|---------------------------------------|-------------------|--------------------------------------|
| Dashboard Offer         | nses Log Activity Network Activity | Assets Reports Admin SentinelOne |                                    |                  |                                       |                   | System Time: 12:47 PM                |
| () SentinelOne          | _ Analyze                          | ngs                              |                                    |                  |                                       | S                 | cope purple   Site All -             |
| < Back                  | Lest Logged User: nirg             | Last Activ<br>Site: A            | e: 23/04/2019 13:25<br>cmeHoldings |                  | Group: Default Group<br>Domain: local |                   | Actions -<br>Full Scan<br>Abort Scan |
| Conorol                 |                                    |                                  |                                    | Net              | wark Adaptara                         |                   | Fetch Logs                           |
| General                 |                                    |                                  |                                    | Nam              | e IP                                  | Mac Address       | Uninstall                            |
| Agent Ver<br>Scan State | sion: 2.6.5.2559                   | Console connectivity: Fa         | alse                               |                  |                                       |                   | Shutdown                             |
| Memory:                 | 2048                               | Subscribed on: 11/11/2           | 018 10:36                          | utun             |                                       |                   | Disconnect                           |
| CPU: In                 | tel(R) Core(TM) i9-8950HK CPU @    | Console visible IP:              | 54.17.28                           | en0              | 100,100,00,00                         | 10.00             |                                      |
| Core Cour               | nt: 2                              | IP Address:                      |                                    |                  |                                       |                   |                                      |
| Disk Encr               | yption: False                      | UUID: 564D8B71-9E0               | A-5BFB-EE6B-7288F                  |                  |                                       |                   |                                      |
| Threats                 | File Name                          | Endpoint                         | Created                            | Updated          | Site                                  | Classification Ar | ction Done                           |
| ۲                       | vmware-tools-daemon                | desktop nirg-macos-vm1           | 23/04/2019 12:03                   | 23/04/2019 12:03 | AcmeHoldings                          | generic.heuristic |                                      |
| 8                       | vmware-tools-daemon                | desktop nirg-macos-vm1           | 23/04/2019 12:03                   | 23/04/2019 12:03 | AcmeHoldings                          | generic.heuristic |                                      |
| 8                       | uninstallTools                     | desktop nirg-macos-vm1           | 23/04/2019 11:59                   | 23/04/2019 11:59 | AcmeHoldings                          | generic.heuristic |                                      |
| 8                       | preinstall                         | desktop nirg-macos-vm1           | 23/04/2019 11:56                   | 23/04/2019 11:57 | AcmeHoldings                          | OSX.Malware       | ۲                                    |
| 8                       | <u>sh</u>                          | esktop nirg-macos-vm1            | 23/04/2019 11:46                   | 23/04/2019 11:53 | AcmeHoldings                          | generic.heuristic |                                      |
| 8                       | <u>sh</u>                          | desktop nirg-macos-vm1           | 23/04/2019 11:42                   | 23/04/2019 11:53 | AcmeHoldings                          | generic.heuristic |                                      |
| 0                       | vmware-tools-daemon                | desktop nirg-macos-vm1           | 23/04/2019 11:41                   | 23/04/2019 11:54 | AcmeHoldings                          | generic.heuristic |                                      |
| 0                       | invoices.docx                      | desktop nirg-macos-vm1           | 18/04/2019 15:11                   | 22/04/2019 15:30 | AcmeHoldings                          | Malware           |                                      |
| 0                       | nc                                 | esktop nirg-macos-vm1            | 01/04/2019 17:22                   | 01/04/2019 17:22 | AcmeHoldings                          | generic.heuristic |                                      |
| Ŕ                       | malware                            | desktop nirg-macos-vm1           | 01/04/2019 15:15                   | 01/04/2019 16:39 | AcmeHoldings                          | OSX.Malware       |                                      |

• Use the SentinelOne DSM to create saved searches and dashboards.

|  | Radar  |                        |  |  |  |  |  |  |               |   |  | Ċ.   |
|--|--|------------------------|--|--|--|--|--|--|---------------|---|--|--|
| lashboard Offe   | enses Log Activity   | Network Activity A     | lssets Reports A   | Admin SentinelOne  |  |  |  |  |               |   |  | System Time: 12:50   |
| in and a Codeb (   | and a state from a   | Louis Columba - D. Com | num O curre à c  | alaa Daalibuu Dadaa 🕷 A  | <b>-</b>   |  |  |  |               |   |  |  |
| earch • Guick e  | searches • ¶ Add Piller  | Save Criteria 📳 Save   | resons 0, carcar 7 ra  | aserosave Notes • A  | coons +  |  |  |  |               |   |  |  |
| Advanced Searc   | ch * select *  | from events where      | LOGSOURCETYPENAME(   | (devicetype) = 'Se   | ntinelOne'   |  |  |  |               |   | •  | 3 Search   |
|  |  |                        | Start Time   | 5/5/2019 ~   | 6:50 AM - End T  | ime 5/5/2019   | * 12:50 PM   | * Update   |               |   |  | . • .  |
|  |  |                        | View:  | Select An Option:  | - Display: Default (   | Normalized) +  | Results Limit  | *  |               |   |  |  |
|  |  |                        |  |  | Using Search: Sen  | tinelOne Raw   |  |  |               |   |  | Completed  |
| Current Statis<br>Total Results  | 77 (107KB Total)   | Compressed Data File   | as Searched 0 (0B Tot  | tal) Duration 1  | Zms  |  |  |  |               |   |  |  |
| Data Files Searche   | d 60 (6.5MB Total)   | Index File Count       | 56 (2.7M   | B Total) More Details  | k  |  |  |  |               |   |  |  |
| Records Matche   | d Over Time  |                        |  |  |  |  |  |  |               |   |  |  |
| Reset Zoom   |  |                        |  |  |  |  |  |  |               |   | 5/5/19, 6:50 AM  | M - 5/5/19, 12:50 PM ¢   |
| 15   |  |                        |  |  |  |  |  |  |               |   |  |  |
|  |  |                        |  |  |  | ٨  |  |  |               |   |  |  |
| 10   |  |                        |  |  |  | Λ  |  |  |               |   |  |  |
| 5  |  |                        |  |  |  |  |  |  |               |   |  |  |
|  |  |                        |  |  |  |  |  |  | -             | $\ldots $   |  |  |
| 0  |  |                        |  |  |  |  |  |  |               | $\sim \sim \sim$  |  | $\land$  |
| 7:00 AI  | M 7.30 AP  | A 8:00                 | AM 8:30 /  | AM 9:00  | AM 9:30 A  | M 10:0   | 0 AM 10:   | 30 AM 11   | 00 AM 1       | L:30 AM 1   | 2:00 PM  | 12:30 PM   |
| 7:00 A   | M 7.30 A/  | A 8:00                 | AM 8:30 /  | AM 9:00  | ) AM 9:30 A  | M 10:0   | 0 AM 10:   | 30 AM 11   | 00 AM 1:      | L:30 AM 1   | 2:00 PM  | 12:30 PM   |
| ° 7:00 A   | m 7.50 An  | 4 8:00                 | AM 8:30 /  | AM 9:00  | ) AM 9:30 A  | M 10:0<br>Update Details<br>(Hide Charts)  | 0 AM 10:   | 30 AM 11:  | 00 AM 1:      | 1:30 AM 1   | 2:00 PM  | 12:30 PM   |
| starttime  | protocolid   | sourceip               | AM 8:30 /  | AM 9:00  | AM 9:30 A<br>sourceport  | M 10:0<br>Update Details<br>(Hide Charts)<br>eventcount  | io AM 10:<br>magnitude   | identityip   | destinationip | destinationport   | category   | 12:30 PM<br>username   |
| 7:00 Al  | protocolid<br>255<br>255   | sourceip               | AM 8:30 /  | qid<br>1002250034  | AM         9:30 A           sourceport         0   | M 10:0<br>Update Details<br>(Hide Charts)<br>eventcount<br>4<br>2  | M 10:<br>magnitude   | identityip 0.0.0.0   | destinationip | destinationport   | category<br>6001   | 12:30 PM   |
| 57040490122<br>557040738948<br>557040738948  | protocolid<br>255<br>255   | sourceip               | AM 8:30 /<br>logsourceid<br>118<br>118<br>118  | AM 9:00<br>qid<br>1002250034<br>1002250038<br>1002250145   | AM 9:30 A<br>sourceport<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0   | M 10:0<br>Update Details<br>(Hide Charts)<br>eventcount<br>4<br>2<br>3   | 0 AM 10:<br>magnitude<br>4<br>3  | identityip<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0  | destinationip | 1:30 AM 1      destinationport     0     0     0  | category<br>6001<br>8008<br>8053   | 12:30 PM username admin admin admin  |
| starttime<br>s57040490122<br>557040738948<br>557040738948<br>557040738948  | protocolid<br>255<br>255<br>255<br>255   | sourceip               | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118                                  | AM 9:00<br>qid<br>1002250034<br>100225008<br>1002250145<br>1002250212  | AM 9:30 A<br>sourceport<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0   | M 10::<br>Update Details<br>(Hide Charts)<br>eventcount<br>4<br>2<br>3<br>1  | M 10:<br>magnitude<br>4<br>3<br>3  | identityip<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0  | destinationip | :30 AM         1           destinationport         0           0         0           0         0           0         0  | category<br>6001<br>8008<br>8053<br>8037   | 12:30 PM username admin admin admin momtauto   |
| starttime<br>557040490122<br>557040738948<br>557041294243<br>557041294243<br>557041299105  | protocolid<br>255<br>255<br>255<br>255<br>255  | 4 8:00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118                    | AM 9:00<br>qid<br>1002250034<br>1002250145<br>1002250145<br>100225013  | AM 9:30 A     Sourceport     0     0     0     0     0     0   | M 10::<br>Update Details<br>(Hee Charls)<br>eventcount<br>4<br>2<br>3<br>1<br>1  | magnitude<br>4<br>3<br>3<br>3<br>3   | identityip<br>0.0.0.0<br>0.0.0<br>0.0.0<br>0.0.0<br>0.0.0<br>0.0.0<br>0.0.0  | destinationip | 1:30 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0   | category<br>6001<br>8008<br>8053<br>8037<br>8006   | 12:30 PM<br>admin<br>admin<br>admin<br>mgmtauto<br>N/A   |
| starttime<br>557040490122<br>557040738948<br>557041294243<br>557041299105<br>55704718930   | m 7.30 A9  | A 8:00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>118             | AM 9:00<br>qid<br>1002250034<br>100225008<br>1002250145<br>1002250145<br>1002250212<br>1002250213<br>1002250008  | AM 9:30 A     Sourceport     0     0     0     0     0     0     0     0     0     0     0   | M 10::<br>Update Details<br>(Hide Charts)<br>eventcount<br>4<br>2<br>3<br>1<br>1<br>1<br>1   | magnitude<br>4<br>3<br>3<br>3<br>3<br>3<br>3   | identityip<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0   | destinationip | 130 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0  | Category<br>6001<br>8008<br>8053<br>8037<br>8006<br>8008   | 12:30 PM<br>admin<br>admin<br>admin<br>mgmtauto<br>N/A<br>admin  |
| starttime<br>i57040490122<br>i57040738948<br>i57040738948<br>i57040738948<br>i57040738948<br>i57041299105<br>i57040718930<br>i57040723948  | m 7.30 A9<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8:00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9:00<br>qid<br>1002250034<br>100225008<br>100225045<br>1002250212<br>1002250212<br>1002250212<br>1002250010   | AM 9:30 A  | M 10:(<br>Update Details)<br>(Hde Charts)<br>eventcount<br>4<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>1   | magnitude         4         3         3         3         3         3         3         3         3         3         3         4         4         3         3         3         3         3         3         3         3         3         4         4         3         3         3         4         4         3         3         3         4         4         3         3         3         4         4         3         3         4         4         3         3         4         3         3         4         4         3         3         4         3         3         4         4         3         3         4         3         3         4         3         3         3         4         3         3         3         4         3         3         3         4         3         3         3         4         3  | identityip 0.0.0 0   | destinationip | 130 AM 1<br>destinationport<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0  | category<br>6001<br>8008<br>8053<br>8037<br>8006<br>8008<br>8008<br>8008   | 12:30 PM<br>admin<br>admin<br>admin<br>mgmtauto<br>N/A<br>admin<br>admin<br>admin  |
| starttime<br>i57040490122<br>i57040738948<br>i57040738948<br>i57041292105<br>i5704129105<br>i57040718930<br>i57040723948<br>i57040723948   | m 7.30 rs9 protocolid 255 255 255 255 255 255 255 255 255 25   | A 8:00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9:00<br>qid<br>1002250034<br>100225008<br>1002250145<br>1002250213<br>1002250213<br>1002250010<br>1002250145  | AM 9:30 A     Sourceport     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0   | M 10:<br>Update Details<br>(Hde Charts)<br>eventcount<br>4<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>1   | io AM 10:<br>magnitude<br>4<br>3<br>3<br>3<br>3<br>3<br>4<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3  | identityip 0.0.0 0   | destinationip | 130 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0  | Category<br>6001<br>8008<br>8053<br>8037<br>8036<br>8006<br>8008<br>6019<br>8053   | 12:30 PM<br>admin<br>admin<br>admin<br>admin<br>mgmtauto<br>N/A<br>admin<br>admin<br>admin<br>admin  |
| 557040490122<br>557040490122<br>557040738948<br>557040738948<br>557041299105<br>557041299105<br>55704728948<br>557040728948<br>557040728948  | m 7.30 A9<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | 4 8:00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9:00<br>qid<br>1002250034<br>1002250034<br>100225015<br>1002250212<br>1002250213<br>1002250218<br>1002250010<br>1002250010  | AM 9:30 A  sourceport  0  0  0  0  0  0  0  0  0  0  0  0  0   | M 10:(<br>Update Details<br>(45e Charts)<br>eventcount<br>4<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | magnitude<br>4<br>3<br>3<br>3<br>3<br>3<br>4<br>4<br>4   | identityip 0.0.0.0 0.0.0 0.0 0.0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0   | destinationip | 130 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0  | category<br>6001<br>8008<br>8053<br>8037<br>8006<br>8037<br>8006<br>8038<br>6019<br>8053<br>6019   | 12:30 PM  username admin admin admin mgmtauto N/A admin admin admin admin admin admin admin  |
| starttime<br>557040490122<br>557040738948<br>557041294243<br>557041294243<br>557041294243<br>55704723948<br>557040723948<br>557040723948<br>557040723948   | m 7.30 rs9 protocolid 255 255 255 255 255 255 255 255 255 25   | A 8.00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9:00<br>qid<br>1002250034<br>100225008<br>1002250145<br>1002250145<br>1002250010<br>1002250010<br>1002250010<br>1002250145  | AM 9:30 A  | M 10:(<br>Update Details)<br>(#496 Charts)<br>eventcount<br>4<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>1<br>3<br>3  | magnitude 4 3 3 3 4 4 4 3 3 3 4 4 3 4 3 4 4 3 3 4 4 4 3 3 4 4 4 3 3 4 4 4 3 4 4 4 3 4 4 4 4 4 4 4 4 5 4 4 4 5 4 4 4 5 5 4 4 5  | Identityip 0.0.0 0.0 0.0 0.0 0   | destinationip | .30 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0  | category<br>6001<br>8008<br>8008<br>8003<br>8006<br>8006<br>8006<br>8006<br>8006   | 12:30 PM username admin admin admin mgmauto N/A admin admin admin admin admin admin admin admin  |
| 5570407490122<br>557040738948<br>557040738948<br>557040738948<br>557041294243<br>557041294105<br>557040728948<br>557040723948<br>557040723948<br>557040723948  | m 7.30 A9<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9-00<br>gld<br>1002250034<br>1002250034<br>1002250145<br>1002250145<br>1002250145<br>1002250145   | AM 9:30 A  sourceport  0  0  0  0  0  0  0  0  0  0  0  0  0   | M 10:1<br>Update Details<br>(#464 Charts)<br>eventcount<br>4<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>3<br>2  | 10:<br>magnitude<br>4<br>3<br>3<br>3<br>3<br>4<br>4<br>3<br>3<br>4<br>3<br>3<br>4<br>3<br>3<br>3<br>4<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3<br>3   | i0 AM         11           identifyip         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0  | destinationip | Image: 30 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0  | category<br>6001<br>8008<br>8053<br>8005<br>8008<br>8008<br>6019<br>8008<br>6019<br>8008<br>6019<br>8063<br>8008<br>8063   | 12:30 PM<br>sdmin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin   |
| 7:00 AJ  | m 7.30 A9<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9-00  gld  1002250034  1002250034  1002250145  1002250145  1002250145  100225010  100225010  100225010  100225010  100225010  100225010  100225010  100225010  100225010  100225000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  10025000  1002500  10025000  1002500  1002500  1002500  1002500  1002500  1002500  1002500  1002500  1002500  1002500  1002500  100250  100250  1002500  100  1  | AM         9:30 A           sourceport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0 | M 10:<br>Update Details<br>(Update Details)<br>(Update | magnitude 4<br>4<br>3<br>3<br>3<br>3<br>4<br>4<br>3<br>3<br>3<br>3<br>4<br>3<br>3<br>3<br>4<br>4<br>3<br>3<br>4<br>4   | identityip<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0. | destinationip | 30 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0   | Category<br>6001<br>8008<br>8053<br>8057<br>8006<br>8006<br>8006<br>8008<br>8008<br>8008<br>8053<br>8053<br>8053<br>8063<br>8066<br>8060<br>8060<br>8060<br>8060<br>8060<br>806  | 12:30 PM   |
| starttime<br>557040490122<br>557040738948<br>557040738948<br>557041299105<br>557041299105<br>557040723948<br>557040723948<br>557040723948<br>557040723948<br>557040723948<br>557040723948  | m 7.30 Ab<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | M 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11 | AM 9:00  | AM 9:30 A<br>sourceport<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0   | M 10:0<br>Update Details<br>(H496 Charts)<br>(H496 Charts)<br>4<br>2<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>3<br>2<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1  | 0 AM         10:           magnitude         4           4         3           3         3           4         3           3         4           4         3           3         4           4         5   | identityip         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0   | destinationip | 1 destinationport 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0  | category           6001           8008           8033           8008           8033           8033           8033           8033           8033           8033           8033           8033           8033           8034           8035           8036           8037  | 12:30 PM<br>schrin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin   |
| 2:00 AU<br>starttime<br>557040490122<br>557040738948<br>557041292105<br>557041292105<br>557041292105<br>557040723948<br>557040723948<br>557040723948<br>557040723947<br>5570404723947<br>557040414087  | m 2.30 Ad<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | M 8:30 /<br>logsourceld<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11 | AM 9:00  gld 1002250034 1002250036 1002250036 1002250036 1002250016 1002250016 1002250016 1002250016 1002250016 1002250016 10022500145 1002250008 1002250145 1002250034 1002250034 1002250034 1002250145 1002250034 1002250145 1002250034 1002250145 1002250034 1002250145 1002250145 1002250034 1002250145 1002250034 1002250145 1002250034 1002250145 1002250034 1002250145 1002250145 1002250034 1002250145 1002250145 1002250145 1002250145 1002250145 1002250145 1002250145 1002250145 1002250034 1002250145 1002250145 1002250145 1002250145 1002250145 1002250034 1002250145 1002250145 100225003 1002250145 100225003 1002250145 100225003 1002250145 100225003 1002250145 100225003 1002250145 100225003 100225014 100225003 100225014 100225003 100225014 100225003 100225014 100225003 100225014 10025014 1002501 1002501 1002501 1002501 1002501 100250 100 100 100 100 100 100 100 100 100 1  | AM 9:30 A<br>sourceport<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0   | M 10:<br>Update Details<br>Q456 Charlsy<br>eventceunt<br>4<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>2<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | magnitude         4           4         3           3         3           3         3           4         4           3         3           4         5  | identifyip         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0  | destinationip | destinationport         1           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0   | category<br>6001<br>8008<br>8033<br>8037<br>8006<br>8006<br>8006<br>8008<br>6019<br>8053<br>8008<br>6019<br>8053<br>8008<br>8008<br>8008<br>8008<br>8008<br>8009<br>8009<br>800  | 12:30 PM   |
| 7:00 Al<br>starttime<br>67040490122<br>57040738948<br>5704129426<br>5704129428<br>5704129428<br>5704129428<br>57040728948<br>57040728948<br>57040728948<br>57040728948<br>57040728948<br>57040728948<br>57040728948  | m 7.30 Ab<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | AM 8:30 /<br>10gsourceld<br>110<br>110<br>110<br>110<br>110<br>110<br>110<br>11              | AM 9:00  | AM 9:30 A  sourceport  0  0  0  0  0  0  0  0  0  0  0  0  0   | M 10:<br>Update Details<br>0456 Charsis<br>eventcount<br>4<br>2<br>3<br>1<br>1<br>1<br>1<br>3<br>2<br>1<br>1<br>1<br>1<br>3<br>4<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | 0 AM         10:           magnitude         4           4         3           3         4           4         3           4         5           5         5           5         5   | identifyip         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0  | destinationip | 1 destinationport 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0<br>0 0  | 2:00 PM category 6001 8008 8037 8006 8037 8006 8053 805 805 805 805 805 805 805 805 805 805  | 12:30 PM   |
| 7:00 Al<br>starttime<br>57040490 122<br>5704078848<br>57041294243<br>57041294243<br>57041294243<br>57041294243<br>57041294243<br>5704729848<br>57040729348<br>57040729348<br>57040729348<br>5704072948   | * 7.30 A   | A 8.00                 | M 8:30 /<br>logsourceld<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11 | AM 9:00  gld 1002250034 1002250036 1002250036 1002250036 100225003 100225030 10022503 10022503 10022503 10022503 10022503 10022503 10022503 10022503 10022503 1002250 1002250 1002250 1002250 1002 1002  | AM 9:30 A<br>sourceport<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0   | M 10:0<br>Update Details<br>0(456 Charl)<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>3<br>2<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | magnitude         4           4         3           3         3           3         3           4         4           5         3           3         4  | identifyip         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0  | destinationip | 30 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0   | category           6001           8008           8037           8006           8033           8006           601           8053           8068           601           8008           601  | 12:30 PM<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin  |
| 27-00 AI<br>starttime<br>57040480122<br>5704078848<br>57041284243<br>57041284243<br>570412915<br>5704129105<br>57040723948<br>57040723948<br>57040723948<br>57040723947<br>57040723947<br>57040723947<br>5704074895<br>57040748925   | m 7.30 Ab<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | AM 8:30 /<br>10gscurceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>gid<br>100225004<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250010<br>1002250145<br>1002250010<br>1002250010<br>1002250018<br>1002250034<br>1002250038<br>1002250038   | AM 9:30 A  sourceport  0  0  0  0  0  0  0  0  0  0  0  0  0   | M 10:<br>Update Details<br>0456 Charsis<br>eventcount<br>4<br>2<br>3<br>1<br>1<br>1<br>1<br>2<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1  | 0 AM         10:           magnitude         4           4         3           3         3           4         3           3         4           3         3           4         3           5         3           4         5           3         3           4         4           5         3           4         4   | i0 AM         11           Identityip         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0  | destinationip | 30 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0   | 2:00 PM category 6001 8008 8009 8009 8009 8009 8009 8009 8   | 12:30 PM   |
| 7:00 Al<br>startline<br>5704/0401 (22<br>5704/073804)<br>5704/0738048<br>5704/0738048<br>5704/073804<br>5704/073804<br>5704/073804<br>5704/073804<br>5704/073804<br>5704073804<br>5704073804<br>5704073804<br>5704073804<br>5704073804<br>5704073804<br>5704073804<br>5704073804<br>5704073804<br>5704023801<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>5704032810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>570403810<br>5   | m 7.30 Ab<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | AM 8:30 /<br>logsourceld<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>qid<br>1002250004<br>1002250004<br>10022500145<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>10025005<br>1005005<br>1005005<br>1005005<br>1005005<br>1005005<br>1005005<br>1005005<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>100505<br>1005   | AM 9:30 A  | M 10:0<br>Update Details<br>0/650 Charl<br>2<br>3<br>1<br>1<br>1<br>1<br>2<br>3<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1  | 0 AM 10:<br>magnitude 3 3 3 3 3 3 4 4 5 5 5 5 5 4 4 4 4 5 5 3 4 4 5 5 3 3 4 4 5 5 3 3 4 4 5 5 3 3 4 4 5 5 5 5  | 0 AM         11           Identifyp         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0   | destinationip | 1   | category           6001           8008           8037           8006           8038           8006           601           8008           8053           8006           6019           8053           8068           6019           8053           8068           6001           8006           6001           6001           6001           6001           6001           6001           6001           6002  | 12:30 PM<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>ado |
| 2:00 Al<br>startline<br>i57040480122<br>i5704078848<br>i5704078848<br>i57041284243<br>i57041284243<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i5704072848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i570407848<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i5704078<br>i57040<br>i5704078<br>i5704078<br>i57040<br>i57040<br>i570400   | **************************************   | A 8.00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>gid<br>100225004<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250010<br>1002250010<br>1002250010<br>1002250018<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>1002250038<br>100250038<br>100250038<br>100250038<br>100250038<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>10025008<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>1002508<br>100508<br>100508<br>100508<br>100508<br>100508<br>100508<br>100508<br>100508<br>1   | AM 9:30 A<br>sourceport<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0   | M 10:0<br>Update Details<br>(#66 Chans)<br>eventcount<br>4<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>1<br>2<br>2<br>1<br>1<br>1<br>1<br>2<br>1<br>1<br>1<br>1<br>1   | 0 AM         10:           magnitude         4           4         3           3         3           4         3           3         4           3         4           3         3           4         3           5         3           4         4           5         3           4         4           3         4           4         3   | identityip         11           Identityip         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0           0.0.0.0         0.0.0.0   | destinationip | 30 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0   | category<br>6001<br>8008<br>8008<br>8007<br>8006<br>8006<br>8006<br>8006<br>8008<br>8008   | 12:30 PM   |
| 27-00 Al<br>starttime<br>57/04/0401/22<br>57/04/78846<br>57/04/78846<br>57/04/78846<br>57/04/78846<br>57/04/73846<br>57/04/73846<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/73848<br>57/04/7388<br>57/04/7388<br>57/04/7388<br>57/04/7388<br>57/04/7388<br>57/04/7388<br>57/04/7388<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/7888<br>57/04/   | m 7.30 Ab<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | AM 8:30 /<br>logsourceld<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.00<br>9.0 | AM 9:30 A sourceport 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0   | M 10:0<br>Update Details<br>0/660 Coatta)<br>eventcount<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1  | 0 AM 10:<br>magnitude<br>3<br>3<br>3<br>3<br>3<br>3<br>4<br>4<br>5<br>5<br>4<br>4<br>5<br>5<br>4<br>4<br>5<br>5<br>4<br>4<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5   | 0 AM         11           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0  | destinationip | Image: Section 2         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0  | 2.00 PM<br>category<br>6001<br>8005<br>8005<br>8006<br>8006<br>8006<br>8008<br>6019<br>8053<br>6019<br>8053<br>6019<br>8053<br>6019<br>8053<br>6019<br>8056<br>8006<br>8006<br>8006<br>8006<br>8006<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>8005<br>805<br>8  | 12:30 PM   |
| 27:00 Al<br>starttime<br>5770478491 22<br>57704738448<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>5770478888<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>57704728848<br>577047888<br>577047888<br>577047888<br>577047888<br>577047888<br>577047888<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048<br>577048  | <ul> <li>Protocolid</li> <li>255</li> <li>255</li></ul> | A 8.00                 | AM 8:30 /<br>logsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>qid<br>100225004<br>100225004<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>1002250145<br>100225004<br>1002250145<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250014<br>1002250145<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>1002250015<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225015<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225005<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100255015<br>100555015<br>100555015<br>100555015<br>100555015<br>100555015   | AM 9:30 A  | M 10:0<br>Update Details<br>946 Okea<br>4<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>3<br>2<br>2<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1  | 0 AM 10:<br>magnitude<br>4<br>3<br>3<br>4<br>3<br>4<br>5<br>5<br>4<br>5<br>5<br>4<br>5<br>5<br>4<br>5<br>5<br>4<br>5<br>5<br>4<br>5<br>5<br>4<br>5<br>5<br>6<br>4<br>5<br>5<br>6<br>6<br>7<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>8<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>8<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>7<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8 | 00 AM         11           Identityp         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0  | destinationip | 30 AM         1           destinationport         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0   | category     content     category     cont   | 12:30 PM<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>adm |
| 27:00 Al<br>startline<br>55704490122<br>55704738848<br>55704738848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5570472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472884<br>5770472885<br>577047788<br>577047888<br>577047788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788<br>57704788  | m 7.30 Ab<br>protocolid<br>255<br>255<br>255<br>255<br>255<br>255<br>255<br>25   | A 8.00                 | AM 8:30 /<br>10gsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>gld 9.00<br>100225004<br>100225004<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>1002250145<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>10025004<br>1002500   | AM 9:30 A  sourceport 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0  | M 10:0<br>Update Details<br>(Prise Cava)<br>eventcount<br>2<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>3<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | 0 AM 10:<br>magnitude<br>3<br>3<br>3<br>3<br>3<br>4<br>4<br>3<br>3<br>4<br>4<br>5<br>5<br>4<br>4<br>5<br>5<br>4<br>4<br>5<br>5<br>6<br>4<br>4<br>5<br>5<br>6<br>6<br>7<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8  | 0 AM         11           10 a00 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)           0.000 (0)         0.000 (0)   | destinationip | Image: State  | category           colo  | 12:30 PM addini addini addini addini addini mgmulao NNA addini ad   |
| 27:00 Al<br>starttime<br>5770478490 122<br>57704738448<br>57704728448<br>57704728448<br>57704728448<br>57704728448<br>57704728448<br>57704728448<br>57704728448<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>5770472849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849<br>577047849  | <ul> <li>Protocolid</li> <li>255</li> <li>255</li></ul> | A 8.00                 | AM 8:30 /<br>logsourceld<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>qld<br>100225004<br>100225004<br>100225004<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100   | AM 9:30 A<br>sourceport<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0   | M 10:0<br>Update Details<br>Vedorbue<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>1<br>2<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | AM         10:           magnitude         4           3         3           3         3           4         3           5         3           6         3           7         4           8         3           9         3           10:         10:   | 10 AM         11           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0   | destinationip | Image: Section 2000 (Section 2000) (Section | category     category     control     contro     contro     control     control     control     control     c  | 12:30 PM  definition  definiti   |
| 2:00 Al<br>starttime<br>55704490122<br>55704738848<br>55704738848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704728848<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>55704028810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>5570408810<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>557040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>577040<br>5770000<br>577040<br>5770000<br>57700000<br>5770000000000 | <ul> <li>Protecolid</li> <li>Protecolid</li> <li>255</li> <li>255</li></ul>       | A 8.00                 | AM 8:30 /<br>10gsourceid<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>gld 9.00<br>100225004<br>100225004<br>100225004<br>100225004<br>1002250145<br>1002250145<br>1002250015<br>1002250015<br>1002250016<br>1002250016<br>1002250016<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>100250145<br>1002500   | AM 9:30 A  sourceport 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0  | M 10:0<br>Update Details<br>eventcount<br>2<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>3<br>3<br>2<br>2<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | 0 AM 10:<br>magnitude<br>4<br>3<br>3<br>3<br>4<br>4<br>3<br>4<br>4<br>3<br>4<br>4<br>5<br>5<br>4<br>4<br>3<br>4<br>4<br>3<br>4<br>4<br>3<br>4<br>4<br>3<br>4<br>4<br>3<br>5<br>5<br>5<br>6<br>6<br>7<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8  | 10 AM         11           Identityp         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0           0.00.0         0.00.0  | destinationip | Image: State  | colo PM           colo pM <td< td=""><td>12:30 PM admin admin admin admin mgmabo NA admin admin</td></td<> | 12:30 PM admin admin admin admin mgmabo NA admin   |
| 2:00 Al<br>startline<br>5570409122<br>557040912846<br>557040738446<br>557040738464<br>557040728464<br>557040728464<br>557040728464<br>557040728446<br>557040728446<br>557040728446<br>557040728446<br>557040728446<br>557040728446<br>557040728446<br>557040278464<br>55704032810<br>55704032810<br>55704032810<br>55704032810<br>55704032810  | protecolid           255      255      25  | A 8.00                 | AM 8:30 /<br>logsourceld 118 118 118 118 118 118 118 118 118 11                              | AM 9.00<br>qld<br>100225004<br>100225004<br>100225004<br>100225004<br>1002250145<br>1002250015<br>1002250015<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>100225004<br>100225004<br>100225004<br>100225004<br>100225004<br>1002250145<br>100225004<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>1002250145<br>100225004<br>100225015<br>1002250145<br>1002250145<br>100225015<br>100225004<br>100225015<br>100225015<br>100225005<br>100225015<br>100225015<br>100225005<br>100225015<br>100225015<br>100225005<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>100225015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025015<br>10025005<br>100505<br>100505<br>100505<br>1005   | AM 9:30 A  | M 10:0<br>Update Details<br>Prés Details<br>Prés Details<br>2<br>2<br>3<br>1<br>1<br>1<br>1<br>2<br>2<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1  | 0 AM 10:<br>magnitude<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9   | 0 AM         11           0.0010         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000           0.000         0.000   | destinationip | Image: Section 2000 (Section 2000) (Section | category           601           8008           8008           8009           8008           8009           8008           8009  | 12:30 PM<br>admin<br>admin<br>admin<br>admin<br>mymtabo<br>NA<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin<br>admin   |
| Control 102     Control 1  | Protecolid           255      255      25  | A 8.00                 | AM 8:30 /<br>logscurold<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11               | AM 9.00<br>qld 100225004 100225004 100225004 100225004 100225004 1002250145 1002250145 1002250145 1002250145 1002250145 1002250145 1002250145 1002250145 100225004 100225004 100225004 100225004 100225004 100225004 100225004 1002250145 100225004 1002250145 100225004 1002250145 100225004 1002250145 1002250145 100225014 1002250145 100225014 10025014 1002501 1002501 1002501 1002501 1002501 1002501 1002501 1002501 1002501 1002501 100250 100 100 100 100 100 100 100 100 100 1   | AM 9:30 A  | M 10:00<br>Ubdate Details<br>VedarDate<br>2<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>1<br>2<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | 0 AM 10:<br>magnitude<br>4<br>3<br>3<br>3<br>4<br>4<br>3<br>3<br>4<br>5<br>5<br>4<br>5<br>5<br>4<br>5<br>5<br>4<br>5<br>5<br>4<br>5<br>5<br>6<br>4<br>5<br>5<br>6<br>6<br>7<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8<br>8   | 11           Identityp           0.00.0  | destinationip | 30 AM         1           destinationport         0           0         0   | celegory   | 12:30 PM  sadmin admin a   |
| Continue     STANDARD     Continue     STANDARD   | protecolid           255      255      25  | A 8.00                 | AM 8:30 /<br>logsourceld<br>118<br>118<br>118<br>118<br>118<br>118<br>118<br>11              | AM 9.00<br>qld<br>1002250004<br>1002250004<br>1002250004<br>10022500145<br>10022500145<br>10022500145<br>10022500145<br>10022500145<br>10022500145<br>10022500145<br>10022500145<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250005<br>1002250065<br>1002250065<br>1002250065<br>1002250065<br>1002250065<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>10022500165<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>1002250016<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>100225006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>10025006<br>100250000<br>10   | AM 9:30 A  | M 10:0<br>Update Details<br>yete Own<br>2<br>3<br>3<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1   | 0 AM 10:<br>magnitude<br>3<br>3<br>3<br>3<br>3<br>3<br>4<br>5<br>5<br>5<br>5<br>4<br>4<br>5<br>4<br>4  | 0 AM         11           Identifyp         0.00.0           0.00.0         0.00.0   | destinationip | Image: Section 2000 (Section 2000) (Section | category           cont  | 12:30 PM  Username sdrini admin beno-test admin  |

• Use the SentinelOne DSM to classify and parse SentinelOne content rich Syslogs.

| ≡ IBM QRadar   |  |  |  |   |  | ¢ s                  | 2   |
|--|--|--|--|---|--|----------------------|-----|
| Dashboard Offenses   | Log Activity Network Activity Assets Reports Admin SentinelOne   |  |  |   |  | System Time: 12:51 P | м   |
| Return to Event List   | nnes 🔗 Map Event 🤸 False Positive 🄀 Extract Property 🛛 🔞 Previous 🧐 Next 🖉 Print 🔒 Obluscation 🔻   |  |  |   |  |                      |     |
| Event Information  |  |  |  |   |  |                      |     |
| Event Name   | NEW_THREAT_NOT_MITIGATED   |  |  |   |  |                      | 1   |
| Low Level Category   | Unknown Malware  |  |  |   |  |                      |     |
| Event Description  |  |  |  |   |  |                      | _   |
| Magnitude  | (4) Relevance 3  |  |  | Severity  | 4 Credibility  | 5                    | -   |
| Start Time   | admin May 5, 2019, 10:14:50 AM Storage Time Ma   | av 5. 2019. 10:15:50 AM  |  | Log Source Time   | May 5, 2019, 10:14:59 AM   |                      | -   |
| AccountDomain  | WORKGROUP  | ., .,,   |  |   |  |                      | 1   |
| Action (custom)  | active   |  |  |   |  |                      | -   |
| Agentid (custom)   | 3d68b0d067d67c5e2be853c538d5b9edcea23b81   |  |  |   |  |                      | 1   |
| Category Description<br>(custom)   | New active threat - machine Enterprise-Desktop   |  |  |   |  |                      | 1   |
| Event Summary<br>(custom)  | New active threat - machine Enterprise-Desktop   |  |  |   |  |                      |     |
| File Hash (custom)   | 0da2192d5b9aaef3a4b02c00c38f6f8879496841   |  |  |   |  |                      | -   |
| File Path (custom)   | \Device\HarddiskVolume2\Users\admin\Desktop\CV.exe   |  |  |   |  |                      |     |
| Filename (custom)  | CV.exe   |  |  |   |  |                      |     |
| Hostname (custom)  | Enterprise-Desktop   |  |  |   |  |                      | _   |
| Service (custom)   | 34.35.16.19  |  |  |   |  |                      | ١.  |
| (custom)   | Enterprise-Desktop   |  |  |   |  |                      | 1   |
| (custom)   | Malware  |  |  |   |  |                      | _   |
| Threat Count (custom)  | 3  |  |  |   |  |                      | -   |
| UNIX path name   | N/A  |  |  |   |  |                      | -   |
| (custom)<br>deviceHostName   | unant sumle continuine not   |  |  |   |  |                      | -   |
| (custom)   | usear-purple-semimetories.net  |  |  |   |  |                      | -   |
| siteName (custom)  | Demo TEST  |  |  |   |  |                      | 1   |
| sourceDnsDomain  | WORKGROUP  |  |  |   |  |                      |     |
| (custom)<br>Domain   | Default Domain   |  |  |   |  |                      |     |
|  |  |  |  |   |  |                      | 1   |
| Source and Destination   | n Information  |  |  |   |  |                      |     |
| Source IP  |  | Destination IP   | 172.31.  | 2.68  |  |                      | -1  |
| Source Port  | 0  | Destination Port   | 0  |   |  |                      |     |
| Pre NAT Source IP  |  | Pre NAT Destination IP   | -  |   |  |                      | 1   |
| Pre NAT Source Port  | 0  | Pre NAT Destination Port   | 0  |   |  |                      | 1   |
| Post NAT Source IP   |  | Post NAT Destination IP  |  |   |  |                      | 1   |
| Post NAT Source Port   | 0  | Post NAT Destination Por   | t 0  |   |  |                      | - 1 |
| Source IPv6  | 0:0:0:0:0:0:0:0  | Destination IPv6   | 0:0:0:0  | 0:0:0:0   |  |                      | -   |
| Dauland Information  | 0.00.00.00.00  | Destination MAC  | 00.00.0  | 0.00.00.00  |  |                      | 1   |
| Payload Information  |  |  |  |   |  |                      |     |
| Wrap Text  | 4  |  |  |   |  |                      |     |
| <pre>Ci420.7=030 077 purple.sentinolog thtp://www.sentinolog thtp://www.sentinolog thtp://www.sentinolog thtp://www.sentinolog ising/ising</pre> | .nel  orificationScoperSTIT iio204931060344204931 iio204930 iiio204930 iio204930 iio20 | de Liemour quin-unear - puipter s<br>lone (originatorikame Binterpri<br>admin Noesktop/CV-exe [filedam<br>castHitigationStatusIP-] [http:<br>-2d63bDd67d67c5s2bed53c538d5<br>Name-Enterprise-Desktop] sour | se-Desktop c<br>e=CV.exe thr<br>atCommandLir<br>b9edcea23b81<br>ceUserName=a | W:  uerustandinamin,l.l.12 eventID=19 ev<br>eactlassification=0.1.1.12 eventID=19 ev<br>eactlassification=Maluwre threatClassif<br>excyuments= heatID=519757571244114<br> sourcefrgdm=HOKKEROUP.Enterprise<br>dmin sourceUperId=5-1-5-21-4097623257-2 | rentDesc=New active<br>ficationSource=Stati<br>i sourceAgentLastAct<br>3326715497- |                      |     |
| Additional Information   |  |  |  |   |  |                      |     |
| Protocol   | 255  | QID  |  | 1002250034  |  |                      | 1   |
| Log Source   | Sen_   | Event Co   | unt  | 4   |  |                      |     |
| Custom Rules   | Destination Asset Weight is Low<br>Source Asset Weight is Low<br>Context is Remote to Local  |  |  |   |  |                      |     |
| Custom Rules Partially<br>Matched  |  |  |  |   |  |                      |     |
| Annotations  | Relevance has been decreased by 2 because the destination network weight is low.   |  |  |   |  |                      | 1   |
|  | Relevance has been decreased by 2 because the source network weight is low.  |  |  |   |  |                      |     |
| Log Only (Exclude  | Pelevance has been increased by 2 because the context is memore to Local.  |  |  |   |  |                      | -   |
| -unaryucoj   | I  |  |  |   |  |                      | 4   |
| Identity Information   |  |  |  |   |  |                      |     |
| Identity Username  | N/A  | Identity Host Name   | N/A  |   |  |                      | -   |
| Identity IP  | N/A  | Identity MAC   | N/A  |   |  |                      | -   |
| Identity Extended Field  | N/A  | activity droup name  |  |   |  |                      |     |
| Has Identity (Flag)  | False  |  |  |   |  |                      | 1   |
|  |  |  |  |   |  |                      | 1   |
|  |  |  |  |   |  |                      |     |

# 2. Requirements

- QRadar 7.2.8 patch 7 or higher.
- One of these SentinelOne Management versions: Eiffel, Fuji, and above. Versions Central Park and Denali are expected to work although they are End Of Service (EOS).
- SentinelOne App for QRadar.

**Note:** The SentinelOne App is not supported on Internet Explorer.

- DSM Syslog Parsing and Classification for SentinelOne
- In QRadar, allow Syslog TLS, Syslog, or the forwarding of incoming data.
- In SentinelOne, configure Syslog integration.

# 3. The SentinelOne DSM for QRadar

To see SentinelOne logged events in the QRadar Console:

- 1. Make sure the QRadar Console is installed and running.
- 2. Install the SentinelOne DSM in QRadar.
- 3. Add SentinelOne as a log source for QRadar.
- 4. Integrate your QRadar Syslog Server to SentinelOne.
- 5. See that SentinelOne events appear on the QRadar Console.

# 3.1. Installing the SentinelOne DSM in QRadar

The SentinelOne DSM enables you to send SentinelOne log events and endpoint data to the QRadar Console.

**Important:** If you have an earlier version of the SentinelOne DSM, you must remove it before you install the new DSM. Go to Upgrading From the Beta Version [34] and follow the instructions.

#### To install the SentinelOne DSM:

- 1. Download the SentinelOne DSM ZIP file available on IBM App Exchange.
- 2. Log in to the QRadar Console as Admin.
- 3. From the Main menu, click Admin.

| ≡ в       | M QRadar |              |                  |        |         |       |  |
|-----------|----------|--------------|------------------|--------|---------|-------|--|
| Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin |  |

4. Click Extensions Management.

| ≡ IBM QRadar                                  |                              |                                 |                                 |                   |                               |                         |                                  | Ļ             | <u> </u> |
|---|------------------------------|---------------------------------|---------------------------------|-------------------|-------------------------------|-------------------------|----------------------------------|---------------|----------|
| Dashboard Offenses Lo                         | ng Activity Network Activity | Assets Reports                  | Admin                           |                   |                               |                         |                                  | System Time:  | 11:58 AM |
| Admin   | Opploy Changes Advan         | ced 🔻                           |                                 |                   |                               |                         |                                  |               | 0        |
| <ul> <li>System Configuration</li> </ul>      | ()) There are no changes     | s to deploy.                    |                                 |                   |                               |                         |                                  |               |          |
| ▶ Data Sources                                | System Configuration         |                                 |                                 |                   |                               |                         |                                  |               |          |
| Remote Networks and<br>Services Configuration |                              |                                 | 4                               | 14 C              | Gei                           | e <sup>tt</sup> o       | <b>M</b>                         | <u>w</u>      |          |
| Try it out                                    | Auto Update                  | Backup and Recovery             | Global System<br>Notifications  | Index Management  | Aggregated Data<br>Management | Network Hierarchy       | System and License<br>Management | System Health |          |
| ► Apps  | <b>1</b>                     | 見中                              | ui).                            | 2                 |                               | <u> </u>                |                                  | 5             | . 1      |
|   | System Settings              | Asset Profiler<br>Configuration | Custom Offense Close<br>Reasons | Store and Forward | Reference Set<br>Management   | Centralized Credentials | Forwarding Destinations          | Routing Rules |          |
|   | Domain Management            | 🗱<br>Extensions Management      | Resource Restrictions           |                   |                               |                         |                                  |               |          |

5. In the window that opens, click **Add**.

| Extensions Management                      | Search by extension name | Q         |             | IBM Security App Exchange 🛛 💡 |
|--|--------------------------|-----------|-------------|-------------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED          |                          |           |             | Add                           |
| Name                                       |                          | Status    | Author      | Added On 👻                    |
| SentinelOne App for QRadar - v.3.5.0(Beta) |                          | Installed | SentinelOne | March 12, 2019                |
| QRadar Log Source Management               |                          | Installed | IBM QRadar  | March 7, 2019                 |
| App Authorization Manager                  |                          | Installed | IBM QRadar  | March 7, 2019                 |
| QRadar Assistant App                       |                          | Installed | IBM QRadar  | March 7, 2019                 |

6. In the window that opens, click **Browse**. Browse to the location of the downloaded SentinelOne DSM file.

| Extensions Management | Search by extension name | Q      |        | IBM Security App Exchange |
|-----------------------|--------------------------|--------|--------|---------------------------|
| ALL ITEMS INSTALLED   | NOT INSTALLED            |        |        | Add                       |
| Name                  |                          | Status | Author | Added On 👻                |
|                       | No items to dis          | play   |        |                           |
|                       |                          |        |        |                           |
|                       | Luis No. Exercise        |        |        |                           |
|                       | Add a New Extension      |        | _      |                           |
|                       | From local storage:      | Browse |        |                           |
|                       | Install immediately      |        |        |                           |
|                       | Add                      | Cancel |        |                           |
|                       | Add                      |        |        |                           |

- 7. To immediately install the app, select **Install immediately** and click **Add**.
- 8. Click Install.

| Extensions Management  | Search by extension name   | Q   |                                     | IBM Security App Exchange 💡 |
|--|--|---|-------------------------------------|-----------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED  |  |   |                                     | Add                         |
| Name   |  | Status  | Author                              | Added On 👻                  |
| SentinelOne Labs App for QRadar - Beta                                   | for OPadar Beta API undate   | -   |                                     | March 12, 2019              |
| SentinelOne App for QRadar - v.3.5.0(Bet                                 | ems which are already on the system and n<br>extension that you are about to install, or you | arked with REPLACE. You c<br>ou can preserve existing items | an replace these<br>s as-is and add | March 12, 2019              |
| QRadar Log Source Management Orrest Control only new terms. How would yo | u like to proceed?   |   |                                     | March 7, 2019               |
| App Authorization Manager  | wing changes will occur in the system:   |   | A                                   | March 7, 2019               |
| QRadar Assistant App SentinelOneCustom_ext                               |  | ADD   |                                     | March 7, 2019               |
| Log Source Types (1)   |  |   |                                     |                             |
| SentinelOne  |  | ADD   |                                     |                             |
| QID Records (141)  |  |   |                                     |                             |
| Activity marked as Threat  |  | ADD   |                                     |                             |
| Machine Decommissioned   |  | ADD   |                                     |                             |
| Full Disk scan aborted   |  | ADD   |                                     |                             |
| Full disk Scan start   |  | ADD   |                                     |                             |
| New Blocked Threat   |  | ADD   | -                                   |                             |
|  |  | Install   | Cancel                              |                             |

9. In the window that opens, click **OK**.

| 1e                                     |  |                           | Status      | Author   | Added On       |
|--|--|---------------------------|-------------|----------|----------------|
| SentinelOne Labs App for QRadar - Bet  |  |                           |             |          | March 12, 2019 |
| SentinelOne App for QRadar - v.3.5.0(B | SentinelOne Labs App for<br>By: Sentinel Labs<br>The extension has been installed su | or QRadar - Beta API upda | te<br>nary: |          | March 12, 2019 |
| QRadar Log Source Management           | DSM Event Mappings (134)   |                           |             | <b>^</b> | March 7, 2019  |
| App Authorization Manager              | 4001:3005:unknown<br>4001:5020:unknown   |                           | ADD         |          | March 7, 2019  |
|  | 4001:74:unknown  |                           | ADD         |          |                |
| QRadar Assistant App                   | 4001:5009:unknown  |                           | ADD         |          | March 7, 2019  |
|  | 4001:5008:unknown  |                           | ADD         |          |                |
|  | 4001:5007:unknown  |                           | ADD         |          |                |
|  | 4001:5008:unknown  |                           | ADD         |          |                |
|  | 4001:5005:unknown  |                           | ADD         |          |                |
|  | 4001:5004:unknown  |                           | ADD         |          |                |
|  | 4001:5003:unknown  |                           | ADD         |          |                |
|  | 4001:33:unknown  |                           | ADD         |          |                |
|  | 4001:27:unknown  |                           | ADD         | -        |                |

The SentinelOne DSM is installed and appears in the list of Extensions.

| Extensions Management                      | Search by extension name | Q             |                | IBM Security App Exchange 💡 |
|--|--------------------------|---------------|----------------|-----------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED          |                          |               |                | Add                         |
| Name                                       | Status                   | Author        | Added On 👻     |                             |
| SentinelOne DSM for QRadar - v.3.5.0(Beta) | A Installed              | Sentinel Labs | March 12, 2019 |                             |
| SentinelOne App for QRadar - v.3.5.0(Beta) |                          | ▲ Installed   | SentinelOne    | March 12, 2019              |
| QRadar Log Source Management               |                          | Installed     | IBM QRadar     | March 7, 2019               |
| App Authorization Manager                  | Installed                | IBM QRadar    | March 7, 2019  |                             |
| QRadar Assistant App                       | Installed                | IBM QRadar    | March 7, 2019  |                             |

10. Exit the Extensions Management window.

# 3.2. Adding SentinelOne as a Log Source for QRadar

Add each SentinelOne Console as a log source to define how QRadar gets Syslog messages from SentinelOne.

#### To add SentinelOne as a log source for QRadar using the TLS syslog protocol:

Use the TLS Syslog protocol for QRadar to receive encrypted syslog events from SentinelOne.

- 1. Log in to the QRadar Console as Admin.
- 2. From the Main menu, click Admin.

| ≡ IB      | M QRadar |              |                  |        |         |       |  |
|-----------|----------|--------------|------------------|--------|---------|-------|--|
| Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin |  |

3. Click Log Sources.

| Data Sources |            |             |                       |                   |                                |                         |                 |                                |
|--------------|------------|-------------|-----------------------|-------------------|--------------------------------|-------------------------|-----------------|--------------------------------|
| Events       |            |             |                       |                   |                                |                         |                 |                                |
| DSM Editor   | WinCollect | Log Sources | Log Source Extensions | Log Source Groups | Log Source Parsing<br>Ordering | Custom Event Properties | Event Retention | Data Obfuscation<br>Management |

4. Click Add.

| Search For: Grou | Search For: 🐨 🖉 All Log Source Groups 🔹 Go 🌇 Search For: 🐨 Entertie Disable 🕲 Delete Bulk Actions 🗸 🛔 Extensions 🗻 Parsing Order 🔅 Assign 🕴 |        |          |       |                    |         |                          |                       |             |             |                    |                  |                      |                                 |
|------------------|---|--------|----------|-------|--------------------|---------|--------------------------|-----------------------|-------------|-------------|--------------------|------------------|----------------------|---------------------------------|
| Name             | Desc  | Status | Protocol | Group | Log Source<br>Type | Enabled | Log Source<br>Identifier | Target<br>Destination | Credibility | Autodiscove | Last Event<br>Time | Creation<br>Date | Modification<br>Date | Average<br>EPS (Last<br>Minute) |
|                  | No results were returned.   |        |          |       |                    |         |                          |                       |             |             |                    |                  |                      |                                 |

- 5. In the form that opens:
  - Log Source Name: Enter a unique name of the log source.
  - Log Source Type: Select SentinelOne.

- Protocol Configuration: Select TLS Syslog. See TLS syslog protocol configuration options.
- Log Source Identifier: Enter sentinel.net.
- TLS Listen Port: Make sure it is set to 6514.
- Log Source Extension: Make sure SentinelOneCustom\_ext is selected.

For the other fields, use the default settings or other values according to your environment.

| Add a log source                        |                                      |
|---|--------------------------------------|
| Log Source Name                         | SentinelOne                          |
| Log Source Description                  |                                      |
| Log Source Type                         | SentinelOne +                        |
| Protocol Configuration                  | TLS Syslog 🔻                         |
| Log Source Identifier                   | sentinel.net                         |
| TLS Listen Port 😨                       | 8514                                 |
| Authentication Mode 🚱                   | TLS T                                |
| Certificate Type 💡                      | Generate Certificate 🔻               |
| Maximum Connections 📀                   | 50                                   |
| TLS Protocols 😨                         | TLS 1.2 and above ▼                  |
| Enabled                                 | ×                                    |
| Credibility                             | 5 🔻                                  |
| Target Event Collector                  | eventcollector0 :: int-qrd-es-dev3 🔻 |
| Coalescing Events                       | ×                                    |
| Store Event Payload                     |                                      |
| Log Source Language                     | V                                    |
| Log Source Extension                    | SentinelOneCustom_ext 🔻              |
| Please select any groups you would like | this log source to be a member of:   |
|   |                                      |
|   |                                      |
|   |                                      |
|   | Save Cancel                          |
|   |                                      |

- 6. Click Save.
- 7. Close the **Log Sources** window.

#### 8. Click Deploy Changes.

| ≡ IBM QRadar                                  |                              |                                   |                                |                       |                               |                       |
|---|------------------------------|-----------------------------------|--------------------------------|-----------------------|-------------------------------|-----------------------|
| Dashboard Offenses L                          | og Activity Network Activity | Assets Reports                    | SentinelOne                    |                       |                               |                       |
| Admin  System Configuration                   | Deploy Changes Advanced      | l ▼<br>hanges. Click 'Deploy Chan | ges' to deploy them. View D    | etails                |                               |                       |
| ► Data Sources                                | System Configuration         |                                   |                                |                       |                               |                       |
| Remote Networks and<br>Services Configuration |                              |                                   | 4                              | <u>ж</u> .            | <b>G</b>                      | <i>с</i> в.           |
| Try it out                                    | Auto Update                  | Backup and Recovery               | Global System<br>Notifications | Index Management      | Aggregated Data<br>Management | Network Hierarchy     |
| ► Apps  | <b></b>                      | <b>5</b>                          |                                | *                     | *                             | 6                     |
|   | Forwarding Destinations      | Routing Rules                     | Domain Management              | Extensions Management | Node Management               | Resource Restrictions |
|   | User Management              |                                   |                                |                       |                               |                       |
|   |                              | 11 C                              | 9                              | w8,                   |                               |                       |
|   | Users                        | User Roles                        | Security Profiles              | Authentication        | Authorized Services           | Tenant Management     |

9. Configure a second log source, using either the **Syslog** or **Forwarded** protocol. For instructions, see To add SentinelOne as a log source for QRadar using the Syslog or Forwarded protocol [11].

# To add SentinelOne as a log source for QRadar using the Syslog or Forwarded protocol:

Use the Syslog or Forwarded protocol for QRadar to receive unencrypted syslog events from SentinelOne.

- 1. Log in to the QRadar Console as Admin.
- 2. From the Main menu, click **Admin**.

| ≡ IB      | M QRadar |              |                  |        |         |       |
|-----------|----------|--------------|------------------|--------|---------|-------|
| Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin |

3. Click Log Sources.

| Data Sources |            |             |                       |                   |                                |                         |                 |                                |
|--------------|------------|-------------|-----------------------|-------------------|--------------------------------|-------------------------|-----------------|--------------------------------|
| Events       |            |             |                       |                   |                                |                         |                 |                                |
| DSM Editor   | WinCollect | Log Sources | Log Source Extensions | Log Source Groups | Log Source Parsing<br>Ordering | Custom Event Properties | Event Retention | Data Obfuscation<br>Management |

4. Click Add.

| Search For: Grou | Saarch For: @roup 🔻 All Log Source Groups 👘 Go 🎦 Add 🔐 Edit 🔣 EnableDisable 🕲 Delete Bulk Actions 🔻 🛸 Extensions 🛦 Parsing Order 🖗 Assign 🔮 |        |          |       |                    |         |                          |                       |             |             |                    |                  |                      |                                 |
|------------------|---|--------|----------|-------|--------------------|---------|--------------------------|-----------------------|-------------|-------------|--------------------|------------------|----------------------|---------------------------------|
| Name             | Desc  | Status | Protocol | Group | Log Source<br>Type | Enabled | Log Source<br>Identifier | Target<br>Destination | Credibility | Autodiscove | Last Event<br>Time | Creation<br>Date | Modification<br>Date | Average<br>EPS (Last<br>Minute) |
|                  | No results were returned.   |        |          |       |                    |         |                          |                       |             |             |                    |                  |                      |                                 |

5. In the form that opens:

- Log Source Name: Enter a unique name of the log source.
- Log Source Type: Select SentinelOne.
- Protocol Configuration: Select Syslog or Forwarded.
- Log Source Identifier: Enter the IP address of the SentinelOne Management Console.
- Log Source Extension: Make sure SentinelOneCustom\_ext is selected.

For the other fields, use the default settings or other values according to your environment.

- 6. Click Save.
- 7. Close the Log Sources window.
- 8. Click Deploy Changes.

| ≡ IBM QRadar                                  |                              |                            |                                |                       |                               |                       |
|---|------------------------------|----------------------------|--------------------------------|-----------------------|-------------------------------|-----------------------|
| Dashboard Offenses L                          | og Activity Network Activity | Assets Reports             | SentinelOne                    |                       |                               |                       |
| Admin   | Oppioy Changes Advanced      | ¥ €                        |                                |                       |                               |                       |
| <ul> <li>System Configuration</li> </ul>      | 1 There are undeployed c     | hanges. Click 'Deploy Char | iges' to deploy them. View D   | etails                |                               |                       |
| Data Sources                                  | System Configuration         |                            |                                |                       |                               |                       |
| Remote Networks and<br>Services Configuration |                              |                            | <u> </u>                       | <u>1</u>              | <b>D</b>                      | ÷.                    |
| Try it out                                    | Auto Update                  | Backup and Recovery        | Global System<br>Notifications | Index Management      | Aggregated Data<br>Management | Network Hierarchy     |
| ► Apps  | 5                            | <b>E</b>                   |                                | *                     | *                             | 6                     |
|   | Forwarding Destinations      | Routing Rules              | Domain Management              | Extensions Management | Node Management               | Resource Restrictions |
|   | User Management              |                            |                                |                       |                               |                       |
|   |                              | ÷2                         | 9                              | wil.                  | ш.                            |                       |
|   | Users                        | User Roles                 | Security Profiles              | Authentication        | Authorized Services           | Tenant Management     |

# 3.3. Integrating Your QRadar Syslog Server to SentinelOne

Integrate your QRadar Syslog server to collect SentinelOne logs.

#### To integrate your Syslog server:

1. Open a supported browser on a computer with an active connection to the Internet (or to the On-Prem Management).

For a list of supported browsers, see System Requirements.

- 2. In the browser address bar, enter the management console URL provided by the SentinelOne support team (for example, *https://yourcompany.sentinelone.net/*).
- 3. Enter your username and password, and click Login.

If you want to create a new user for QRadar integration, follow the steps in Creating New Management Console Users and then log in to the new user.

**Note:** A user with a role of **Site Admin** can mitigate threats from the QRadar Console. A user with a role of **Site Viewer** can view threats but cannot take action.

4. In the SentinelOne Management Console, click **Settings**.



- 5. If you are a Site or Account Admin, you must select one Site to open Settings.
- 6.
- 7. Click SYSLOG.

| SETTINGS > CONFI | GURATION NOTIFICATIONS USERS INTEGRATIONS POLICY OVERRIDE SITES |
|------------------|---|
| Types            | Syslog  |
| SMTP             |   |
| SYSLOG           | Disable STSLOG  |
| 550              | Host Your syslog host IP or host name : 0                       |
|                  |   |
|                  | SSL Use SSL secure connection                                   |
|                  | Formatting Information format CEF -                             |
|                  |   |
|                  |   |
|                  | Save DISCARD CHANGES  |

- 8. Click Enable SYSLOG.
- 9. In Host, enter the QRadar FQDN or IP address, and its listening port (514 or 6514).
- 10. To use SSL or TLS channel authentication and privacy, click Use SSL secure connection.

If you do not select this, UDP is used.

11. In Certificate, you can upload server and client certificates to verify client/server authorization between the SentinelOne Management (client) and the syslog server (server). These options only show if Use SSL secure connection is selected. Passphrase certificates are not supported. Make sure you know how the Syslog server is configured, and that you have the correct certificates from that configuration.

| SSL         | Use SSL secure conne                                     | on  |  |
|-------------|--|---|--|
| Certificate | Certificates sent from/to t<br>Choose one out of three v | syslog server.<br>fication options: server of | nly, client only or server & client verification |
|             | Server certificate                                       | Ipload (?)                                    |  |
|             | Client certificate                                       | pload (?)                                     |  |
|             | Client key   | pload   |  |

- · Server certificate Select and upload a certificate to verify the syslog server identity.
- **Client certificate** Select and upload a certificate to verify the SentinelOne Management as a client of the syslog server. Use a certificate file with a client key. A Client certificate is necessary if the server requires client authentication.
- Client key Select and upload the client key of a client/server key pair. A Client key is necessary, along with a Client certificate, if the server requires client authentication.

To find the QRadar certificate and key files:

- 1. Using an SSH session, login to the QRadar Console as root user.
- 2. Run:cd /opt/gradar/conf/trusted\_certificates/
- 3. Extract: syslog-tls.cert and syslog-tls.key.
- 12. In Formatting, select **CEF2**. This format is required to enable integration with the SentinelOne DSM.
- 13. To verify connectivity with your QRadar server, click **TEST** to send a test trap.
- 14. If the test passed, click SAVE.

# 3.4. Seeing SentinelOne Events in QRadar

After the SentinelOne DSM is installed, SentinelOne is added as a log source in QRadar, and your Syslog is integrated, you will see SentinelOne events in the QRadar Console.

#### To see all SentinelOne logged events:

- 1. In the QRadar Console, click Log Activity.
- 2. Click Search and select New Search.

| = "                                 | BM QRadar   |              |                  |              |          |                  |         |                  |
|-------------------------------------|---|--------------|------------------|--------------|----------|------------------|---------|------------------|
| Dashboard                           | Offenses  | Log Activity | Network Activity | Assets       | Reports  | SentinelOne      |         |                  |
| Search V<br>New S<br>Edit S<br>Mana | Quick Searches ▼<br>Search<br>search<br>ge Search Resul | Add Filter   | Save Criteria 🜘  | Save Results | R Cancel | 🛧 False Positive | Rules ¥ | Actions <b>V</b> |

3. In Search Parameters > Parameter , select Log Source Type [Indexed].

Make sure **Operator** is set to **Equals**.

Select SentinelOne as the Value.

| Search Parameters         |                      |   |            |
|---------------------------|----------------------|---|------------|
| Parameter:                | Operator: Value:     |   |            |
| Log Source Type [Indexed] | Equals 👻 SentinelOne | • | Add Filter |

4. Click Add Filter. The new filter is in the Current Filters list.

| earch Parameters              |           |                           |   |           |
|-------------------------------|-----------|---------------------------|---|-----------|
| arameter:                     | Operator: | Value:                    |   |           |
| Log Source Type [Indexed]     |           | * 3Com 8800 Series Switch | • | Add Filte |
|                               |           |                           |   |           |
| Current Filters               |           |                           |   |           |
|                               |           |                           |   |           |
| Log Source Type is SentinelOr | le        |                           |   |           |
| Log Source Type is SentinelOr | le        |                           |   |           |

5. Click Search. The QRadar Log Activity shows all log activity sent from SentinelOne to QRadar.



6. Double-click an event row for more details.

| ≡ IBM QRadar                  |  |   |                                |  |  |  |  |  |
|-------------------------------|--|---|--------------------------------|--|--|--|--|--|
| Dashboard Offenses Log        | Activity Netw                            | ork Activity Assets Reports SentineOne  |                                |  |  |  |  |  |
| The Besture in France Lint    | Otton Erent A                            | Talas Davidina - The Extend Demonstry - A Davidina - Diata - A Distance -             |                                |  |  |  |  |  |
| []] Return to Event List      | Swap Event 🤸                             | alse Postive 🚺 Extract Property 🔮 Previous 🚭 Next 🔤 Print 🔞 Obluscation 🕈             |                                |  |  |  |  |  |
| Event Information             |  |   |                                |  |  |  |  |  |
| Event Name                    | NEW_TH                                   | REAT_SUSPICIOUS   |                                |  |  |  |  |  |
| Low Level Category            | Suspiciou                                | s Activity  |                                |  |  |  |  |  |
| Event Description             |  |   |                                |  |  |  |  |  |
| Magnitude                     |  | (4) Relevance 1   | Severity                       |  |  |  |  |  |
| Username                      | admin                                    |   |                                |  |  |  |  |  |
| Start Time                    | Mar 5, 20                                | 2019. 4:12:58 PM Storage Time Mar 5, 2019, 4:12:58 PM Log Sc                          |                                |  |  |  |  |  |
| AccountDomain (custom)        | WORKG                                    | GROUP   |                                |  |  |  |  |  |
| Action (custom)               | active                                   | e   |                                |  |  |  |  |  |
| Agentid (custom)              | b994add3ftbc14245092821be0efe09a21273bea |   |                                |  |  |  |  |  |
| Category Description (custon  | i) New Sus                               | New Suspicious threat detected - machine mo-win10-po1                                 |                                |  |  |  |  |  |
| File Hash (custom)            | 80249804                                 | 802498041b393ad1e92a27cfbdfb8882025234dc  |                                |  |  |  |  |  |
| File Path (custom)            | \Device\H                                | DeviceHarddiskVolume2UsersIadminIDesktopINL_Test_SamplesICryptoLocker_Symptomatic.exe |                                |  |  |  |  |  |
| Filename (custom)             | CryptoLo                                 | CryptoLocker_Symptomatic.exe  |                                |  |  |  |  |  |
| Hostname (custom)             | mo-win10                                 | pc1   |                                |  |  |  |  |  |
| Service (custom)              |  |   |                                |  |  |  |  |  |
| Threat Classification (custom | ) Malware                                |   |                                |  |  |  |  |  |
| Threat Count (custom)         | 32                                       |   |                                |  |  |  |  |  |
| Threat id (custom)            | 57448638                                 | 7315488038  |                                |  |  |  |  |  |
| UNIX path name (custom)       | N/A                                      |   |                                |  |  |  |  |  |
| Domain                        | Default D                                | smain   |                                |  |  |  |  |  |
| Source and Destination Info   | ormation                                 |   |                                |  |  |  |  |  |
| Source IP                     |  |   | Destination IP                 |  |  |  |  |  |
| Source Asset Name             |  | NA  | Destination Asset Name         |  |  |  |  |  |
| Source Port                   |  | 0   | Destination Port               |  |  |  |  |  |
| Pre NAT Source IP             |  |   | Pre NAT Destination IP         |  |  |  |  |  |
| Pre NAT Source Port           |  | 0   | Pre NAT Destination Port       |  |  |  |  |  |
| Post NAT Source IP            |  |   | Post NAT Destination IP        |  |  |  |  |  |
| Post NAT Source Port          |  | 0   | Post NAT Destination Port      |  |  |  |  |  |
| Source IPv6                   |  | 0:0:0:0:0:0:0   | Destination IPv6               |  |  |  |  |  |
| Source MAC                    |  | 00:00:00:00:00  | 00:00:00:00:00 Destination MAC |  |  |  |  |  |

# To use predefined SentinelOne filters:

The SentinelOne DSM comes with SentinelOne predefined saved filters.

- 1. In the QRadar Console, click Log Activity.
- 2. Click Search and select New Search.

| = "       | 3M QRadar        |              |                  |              |         |                  |                |                  |
|-----------|------------------|--------------|------------------|--------------|---------|------------------|----------------|------------------|
| Dashboard | Offenses         | Log Activity | Network Activity | y Assets     | Reports | SentinelOne      |                |                  |
| Search V  | Quick Searches V | Y Add Filter | Save Criteria    | Save Results | Cancel  | K False Positive | Rules <b>V</b> | Actions <b>V</b> |
| New S     | earch            |              |                  |              |         |                  |                |                  |
| 🔍 Manag   | ge Search Result | ts           |                  |              |         |                  |                |                  |

3. In Type Saved Search or Select from List, enter SentinelOne.

| ≡ IB                       | 3M QRadar                                       |   |                  |        |         |               |
|----------------------------|---|---|------------------|--------|---------|---------------|
| Dashboard                  | Offenses  | Log Activity  | Network Activity | Assets | Reports | Admin         |
| K Manage Se                | earch Results 👔                                 | Manage Custom   | Properties       |        |         |               |
| Save                       | ed Search                                       | )es Group:  | Select a group   |        | *       | Manage Groups |
| sent                       | tinel   | or select from L  | .151             |        |         |               |
| Availab                    | ole Saved Sear                                  | ches  |                  |        |         |               |
| Sentin                     | elOne - Syste                                   | m Activity logs a   | audit            |        |         |               |
| Sentin                     | elOne - Event                                   | s Filename  |                  |        |         |               |
| Sentin<br>Sentin<br>Sentin | elOne - Malwa<br>elOne - Malwa<br>elOne - Malwa | are by source ip<br>are Events by us<br>are Events file p | sername<br>ath   |        |         |               |
| Lo                         | bad D   | elete S   | how AQL          |        |         |               |

- 4. Select one of the predefined saved filters.
- 5. Click Load.



6. Click an event for more details.

For example, if you selected the **Events Filename** filter, double-click a filename for more details.

| Current Statisti | C9         | Start Time View | 2/26/2019<br>Select An Opt | <ul> <li>▼ 4:54 PM</li> <li>iion: ▼ Disp</li> </ul> | End Time Iay: Default (N | e 3/5/2019<br>ormalized) = |           | M v Update  | •             |                 |                    |            |
|------------------|------------|-----------------|----------------------------|---|--------------------------|----------------------------|-----------|-------------|---------------|-----------------|--------------------|------------|
| Current Statisti | CS         |                 |                            |   |                          |                            |           |             |               |                 | -                  |            |
|                  |            |                 |                            |   |                          |                            |           |             |               |                 | c                  | mpieted    |
| cords Matched    | Over Time  |                 |                            |   |                          |                            |           |             |               |                 |                    |            |
| set Zoom         |            |                 |                            |   |                          |                            |           |             |               | 2/26/19         | 9, 4:54 PM - 3/5/1 | 9, 4:54 PM |
|                  |            |                 |                            |   |                          |                            |           |             |               |                 |                    |            |
|                  |            |                 |                            |   |                          |                            |           |             |               |                 |                    |            |
|                  |            |                 |                            |   |                          |                            |           |             |               |                 |                    |            |
|                  |            |                 |                            |   |                          |                            |           |             |               |                 |                    |            |
| Feb 2            | 7 2.00     | PM Fab 2        | 8 2:00 PM                  | Mar 1   | 2-00 PM                  | Mar 2                      | 2:00 PM   | Mar 3 2:00  | PM Mar        | 4 2:00 PM       | d Mar 5            | 2:00       |
| 1002             | 2.00       | 10020           | 2.0011                     | inter 1   | 2.0011                   | Update Details             | 2.00 11   | 1111 0 2.00 |               | 2.0011          | in mar 5           | 2.00       |
|                  |            |                 |                            |   |                          | (Hide Charts)              |           |             |               |                 |                    |            |
| tarttime         | protocolid | sourceip        | logsourceid                | qid   | sourceport               | eventcount                 | magnitude | identityip  | destinationip | destinationport | category           | userna     |
| 1795146391 25    | 5          |                 | 73                         | 1002250045  | 0                        | 1                          | 2         | 0.0.0.0     |               | 0               | 19001              | Win10Vict  |

7. Double-click an event row for specific details about that event.

| Event Informatio                     | n  |  |            |                              |                   |                 |        |                  |   |
|--------------------------------------|--|--|------------|------------------------------|-------------------|-----------------|--------|------------------|---|
| Event Name                           | THREAT_STATUS_CHANGED                                  |  |            |                              |                   |                 |        |                  | _ |
| Low Level<br>Category                | General Audit Event                                    |  |            |                              |                   |                 |        |                  |   |
| Event<br>Description                 |  |  |            |                              |                   |                 |        |                  |   |
| Magnitude                            | (2)  | Relevance  | 1          |                              |                   | Severity        | 1      | Credibility      | 5 |
| Username                             | Win10Victim  |  |            |                              |                   |                 |        |                  |   |
| Start Time                           | Mar 5, 2019, 4:12:28 PM                                | Storage Time   | Mar 5, 201 | 19, 4:12:26 PM               |                   | Log Source Time | Mar 5, | 2019, 4:12:26 PM |   |
| AccountDomain<br>(custom)            | WORKGROUP  |  |            |                              |                   |                 |        |                  |   |
| Action (custom)                      | active   |  |            |                              |                   |                 |        |                  |   |
| AgentId (custom)                     | E9FF25635C14411BBA799DB4F7531CD400000000               |  |            |                              |                   |                 |        |                  |   |
| Category<br>Description<br>(custom)  | Threat status changed                                  |  |            |                              |                   |                 |        |                  |   |
| File Hash<br>(custom)                | de18926ec32da081036932d8d9d5b906b3149b23               |  |            |                              |                   |                 |        |                  |   |
| File Path<br>(custom)                | \Device\HarddiskVolume3\Users\Win10Victim\AppData\Loca | Device/HarddiskVolume3/Users/Win10/ictim/AppData/Loca/Wicrosoft/Windows/INetCache/Content.Outlook/J00094X3/Thunderbird Vulnerable (003).docm |            |                              |                   |                 |        |                  |   |
| Filename<br>(custom)                 | Thunderbird Vulnerable (003).docm                      | Thunderbird Vulnerable (003).doom  |            |                              |                   |                 |        |                  |   |
| Hostname<br>(custom)                 | DESKTOP-37TJ1RM  |  |            |                              |                   |                 |        |                  |   |
| Service (custom)                     |  |  |            |                              |                   |                 |        |                  |   |
| Threat<br>Classification<br>(custom) | Malware  |  |            |                              |                   |                 |        |                  |   |
| Threat Count<br>(custom)             | 1  |  |            |                              |                   |                 |        |                  |   |
| Threat id<br>(custom)                | 574616618466591986                                     |  |            |                              |                   |                 |        |                  |   |
| UNIX path name                       | N/A  |  |            |                              |                   |                 |        |                  |   |
| Domain                               | Default Domain   |  |            |                              |                   |                 |        |                  |   |
| Source and Dest                      | tination Information                                   |  |            |                              |                   |                 |        |                  |   |
| Source IP                            |  |  |            | Destination IP               |                   |                 |        |                  | _ |
| Source Asset Nan                     | ne N/A   |  |            | Destination Asset<br>Name    | N/A               |                 |        |                  |   |
| Source Port                          | 0  |  |            | Destination Port             | 0                 |                 |        |                  |   |
| Pre NAT Source IF                    |  |  |            | Pre NAT Destination IP       |                   |                 |        |                  |   |
| Pre NAT Source P                     | vort 0   |  |            | Pre NAT Destination<br>Port  | 0                 |                 |        |                  |   |
| Post NAT Source                      | IP   |  |            | Post NAT Destination         |                   |                 |        |                  |   |
| Post NAT Source                      | Port 0   |  |            | Post NAT Destination<br>Port | 0                 |                 |        |                  |   |
| Source IPv6                          | 0:0:0:0:0:0:0  |  |            | Destination IPv6             | 0:0:0:0:0:0:0:0   |                 |        |                  |   |
| Source MAC                           | 00:00:00:00:00   |  |            | Destination MAC              | 00:00:00:00:00:00 |                 |        |                  |   |
| ayload Informa                       | tion   |  |            |                              |                   |                 |        |                  |   |
| utf hex                              | base64   |  |            |                              |                   |                 |        |                  | _ |
| Wrap Text                            |  |  |            |                              |                   |                 |        |                  |   |

# 4. The SentinelOne App for QRadar

To mitigate SentinelOne logged events in the QRadar Console:

- 1. Make sure the QRadar Console is installed and running.
- 2. Add SentinelOne as a log source for QRadar [9].
- 3. Install the SentinelOne App in QRadar [21].
- 4. Generate an API Token [27].
- 5. Add your SentinelOne Management Console to the SentinelOne App [28].
- 6. View and mitigate SentinelOne events that appear in the App [29].

# 4.1. Installing the SentinelOne App in QRadar

The SentinelOne App enables you to mitigate threats from the QRadar Console instead of performing them from the SentinelOne Management Console.

Note: The SentinelOne App is not supported on Internet Explorer.

**Important:** If you have an earlier version of the SentinelOne App for QRadar, you must remove it before you install the new app. Go to Upgrading From the Beta Version [34] and follow the instructions.

#### To install the SentinelOne App:

- 1. Download the SentinelOne App ZIP file available on IBM App Exchange.
- 2. Log in to the QRadar Console as an Admin.
- 3. From the Main menu, click Admin.



4. Click Extensions Management.



5. In the window that opens, click **Add**.

| Extensions Ma | anagement |               | Search by extension | n name Q       |        | IBM Security App Exchange | je 🌘 |
|---------------|-----------|---------------|---------------------|----------------|--------|---------------------------|------|
| ALL ITEMS     | INSTALLED | NOT INSTALLED |                     |                |        | Add                       |      |
| Name          |           |               |                     | Status         | Author | Added On                  | •    |
|               |           |               | No ite              | ems to display |        |                           |      |
|               |           |               |                     |                |        |                           |      |
|               |           |               |                     |                |        |                           |      |
|               |           |               |                     |                |        |                           |      |

6. In the window that opens, click **Browse**. Browse to the location of the downloaded SentinelOne App file.

If you do not see this option, make sure you have the required Admin permissions.

| Extensions Management             | Search by extension name Q |        | IBM Security App Exchange 👩 |
|-----------------------------------|----------------------------|--------|-----------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED |                            |        | bbA                         |
| Name                              | Status                     | Author | Added On 👻                  |
| Add<br>Fror                       | No items to display        |        |                             |

7. If you want to immediately install the app, skip to Step 10.

If you want to add the SentinelOne App to the Extensions Management list but install it later, do not select **Install immediately**. Click **Add**.

| Extensions Management                        | Search by extension name  | Q         |            | IBM Security App Exchange 💡 |
|--|---|-----------|------------|-----------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED            |   |           |            | Add                         |
| Name   |   | Status    | Author     | Added On 👻                  |
| QRadar Log Source Management                 |   | Installed | IBM QRadar | March 7, 2019               |
| App Authorization Manager                    |   | Installed | IBM QRadar | March 7, 2019               |
| QRadar Assistant App                         |   | Installed | IBM QRadar | March 7, 2019               |
| Add a N<br>From loca<br>SentineOn<br>Install | lew Extension<br>Istorage:<br>e App-20190307190059.zip Bro<br>immediately | Cancel    |            |                             |

| Extensions Management                      | Search by extension name | Q               |             | IBM Security App Exchange |
|--|--------------------------|-----------------|-------------|---------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED          |                          |                 |             | Add                       |
| Name                                       |                          | Status          | Author      | Added On 👻                |
| SentinelOne App for QRadar - v.3.5.0(Beta) |                          | A Not Installed | SentinelOne | March 10, 2019            |
| QRadar Log Source Management               |                          | Installed       | IBM QRadar  | March 7, 2019             |
| App Authorization Manager                  |                          | Installed       | IBM QRadar  | March 7, 2019             |
| QRadar Assistant App                       |                          | Installed       | IBM QRadar  | March 7, 2019             |

# 8. Select SentinelOne App for QRadar.

| Extensions Management                      | Q               |             | IBM Security App Exchange 👩 |               |  |  |  |  |
|--|-----------------|-------------|-----------------------------|---------------|--|--|--|--|
| ALL ITEMS INSTALLED NOT INSTALLED Add      |                 |             |                             |               |  |  |  |  |
| Name                                       |                 | Status      | Author                      | Added On 👻    |  |  |  |  |
| SentinelOne App for QRadar - v.3.5.0(Beta) | A Not Installed | SentinelOne | March 10, 2019              |               |  |  |  |  |
| QRadar Log Source Management               |                 | Installed   | IBM QRadar                  | March 7, 2019 |  |  |  |  |
| App Authorization Manager                  | Installed       | IBM QRadar  | March 7, 2019               |               |  |  |  |  |
| QRadar Assistant App                       | Installed       | IBM QRadar  | March 7, 2019               |               |  |  |  |  |

9. In the box that opens, click **Install**.

| Extensions Management   | Search by extension name   | Q             |             | IBM Security App Exchange 💡 |
|---|--|---------------|-------------|-----------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED   |  |               |             | Add                         |
| Name  | Sta  | latus         | Author      | Added On 👻                  |
| SentinelOne App for QRadar - v.3.5.0(Beta)<br>SentinelOne is a next-generation endpoint security product used to protect against<br>unknown malware and other bad programs out of endpoints. SentinelOne combine<br>with advanced state prevention in the form of deep file inspection to block threads to<br>your endpoints.Detect and Content Threads On December 10, block threads to<br>your endpoints.Detect and Content Threads On December 10, block threads to<br>your endpoints.Detect and Content Threads On December 10, block<br>detection of a new thread, SentinelOne stops its programs by disconnecting the infer-<br>net thread threads and the sentime of | A all threat vectors. Keep known and<br>e dynamic whitelisting and blacklisting<br>effort hery have a chance to impact<br>rs all activity and apples machine<br>s, and schlisticated malware. Upon<br>ted device from the<br>d to incidents. After stopping attacks,<br>wo of endpoints and threats from<br>(More Details) | Not Installed | SentinelOne | March 10, 2019              |
| QRadar Log Source Management  | Ins  | stalled       | IBM QRadar  | March 7, 2019               |
| App Authorization Manager   | ins  | stalled       | IBM QRadar  | March 7, 2019               |
| QRadar Assistant App  | Ins  | stalled       | IBM QRadar  | March 7, 2019               |

You can click **More Details** to see more information and the installation files.

| Extensions Management  | Search by extension name | Q           |                | IBM Security App Exchange 💡 |
|--|--------------------------|-------------|----------------|-----------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED  |                          |             |                | Add                         |
| Name   |                          | Status      | Author         | Added On 🗸                  |
| SentinelOne App for ORadar - v.3.5.0(Beta)<br>SentinelOne is a next-generation endpoint security product used to protect against<br>why and points Detect and Cortain Thread to Oraginary and the sentinelOne on the<br>point of a new thread. SentinelOne above is programs by disconnecting the info<br>detection of a new thread. SentinelOne above is programs by disconnecting the info<br>detection of a new thread. SentinelOne above is programs by disconnecting the info<br>detection of a new thread. SentinelOne above is programs by disconnecting the info<br>detection of a new thread. SentinelOne above is programs by disconnecting the info<br>detection of a new thread. SentinelOne above is programs by disconnecting the info<br>detection of a new thread.<br>Instal Detection<br>Oraginary Constants (SentinelOne above information)<br>(SentinelOne above information powers forensics and policy enforcement.<br>(Instal Detection)<br>Oraginary Constants (SentinelOne above information (SentinelOne above)<br>(SentinelOne above information (SentinelOne above information (SentinelOne above)<br>(SentinelOne above information (SentinelOne above informati | A Not installed          | SentineiOne | March 10, 2019 |                             |
| QRadar Log Source Management   |                          | Installed   | IBM QRadar     | March 7, 2019               |
| App Authorization Manager  |                          | Installed   | IBM QRadar     | March 7, 2019               |
| QRadar Assistant App   |                          | Installed   | IBM QRadar     | March 7, 2019               |

10. To immediately install the app, select  $\ensuremath{\text{Install immediately}}$  and click  $\ensuremath{\text{Add}}.$ 

| Extensions Management             | Search by extension name  | Q          |               | IBM Security App Exchange 🛛 😨 |
|-----------------------------------|---|------------|---------------|-------------------------------|
| ALL ITEMS INSTALLED NOT INSTALLED |   |            |               | Add                           |
| Name                              | Status  | Author     | Added On 👻    |                               |
| QRadar Log Source Management      | Installed   | IBM QRadar | March 7, 2019 |                               |
| App Authorization Manager         | Installed   | IBM QRadar | March 7, 2019 |                               |
| QRadar Assistant App              | Installed   | IBM QRadar | March 7, 2019 |                               |
| Add<br>From<br>Sent<br>W          | a New Extension n local storage: inelOne App-20100307160059.sip install immediately Add | Browse     |               |                               |

11. In the window that opens, click Install.

| Extensions Management                    |   | Search by extension name | Q      |         |       | IBM Security App Exchange |
|--|---|--------------------------|--------|---------|-------|---------------------------|
| ALL ITEMS INSTALLED NOT                  | INSTALLED   |                          |        |         |       | Add                       |
| Name                                     |   |                          | Status | Autho   | pr    | Added On 👻                |
| SentinelOne App for QRadar - v.3.5.0(Bet |   |                          |        |         |       | March 10, 2019            |
| QRadar Log Source Management             | SentinelOne App for QR<br>By: SentinelOne<br>By installing this extension, the follow | adar - v.3.5.0(Beta)     |        |         |       | March 7, 2019             |
| App Authorization Manager                | Custom Applications (1)   |                          |        | 400     |       | March 7, 2019             |
| QRadar Assistant App                     |   |                          |        |         |       | March 7, 2019             |
|  |   |                          |        |         |       |                           |
|  |   |                          |        |         |       |                           |
|  |   |                          |        |         |       |                           |
|  |   |                          |        |         |       |                           |
|  |   |                          |        |         |       |                           |
|  |   |                          |        |         |       |                           |
|  |   |                          |        | Install | ancel |                           |

The installation might take a couple of minutes.

12. When you see the message that the extension installed successfully, click **OK**.

| Extensions Management                  |   | Search by extension name  | Q                                |                    |                 | IBM Security App Exchange |
|--|---|---|----------------------------------|--------------------|-----------------|---------------------------|
| ALL ITEMS INSTALLED NOT                | - INSTALLED   |   |                                  |                    |                 | Add                       |
| Name                                   |   |   | Status                           |                    | Author          | Added On 👻                |
| SentinelOne App for QRadar - v.3.5.0(B |   |   |                                  |                    |                 | March 10, 2019            |
| QRadar Log Source Management           | SentinelOne App for QRa<br>By: SentinelOne<br>The extension has been installed succ | dar - v.3.5.0(Beta)<br>essfully. Please review the install summa                        | iry:                             |                    |                 | March 7, 2019             |
| App Authorization Manager              | This extension contains one or more a<br>is necessary to refresh your browser. It   | pplications. In order for all new user inte<br>t may also be necessary to clear your br | face elements to<br>owser cache. | appear and functio | n correctly, it | March 7, 2019             |
| QRadar Assistant App                   | Custom Applications (1)<br>SentinelOne  |   |                                  | INSTALL            |                 | March 7, 2019             |
|  |   |   |                                  |                    | ОК              |                           |

The SentinelOne App is installed and appears in the list of Extensions.

| Extensions Management                      | Search by extension name | ٩           |                | IBM Security App Exchange 💡 |  |  |  |  |  |
|--|--------------------------|-------------|----------------|-----------------------------|--|--|--|--|--|
| ALLITEMS INSTALLED NOT INSTALLED Add       |                          |             |                |                             |  |  |  |  |  |
| Name                                       |                          | Status      | Author         | Added On 👻                  |  |  |  |  |  |
| SentinelOne App for QRadar - v.3.5.0(Beta) | A Installed              | SentinelOne | March 12, 2019 |                             |  |  |  |  |  |
| QRadar Log Source Management               |                          | Installed   | IBM QRadar     | March 7, 2019               |  |  |  |  |  |
| App Authorization Manager                  | Installed                | IBM QRadar  | March 7, 2019  |                             |  |  |  |  |  |
| QRadar Assistant App                       | Installed                | IBM QRadar  | March 7, 2019  |                             |  |  |  |  |  |

- 13. Exit the Extensions Management window.
- 14. Click **Deploy Changes** or refresh the QRadar Console screen.

| <b>≡</b> " | BM QRadar  |              |                  |                |            |                                |                    |                                 |  |
|------------|--|--------------|------------------|----------------|------------|--------------------------------|--------------------|---------------------------------|--|
| Dashboard  | Offenses   | Log Activity | Network Activity | Assets Rep     | orts Risks | Vulnerabilities                | Admin              |                                 |  |
| Admin      | Admin Monoced V  |              |                  |                |            |                                |                    |                                 |  |
| System     | System Configuration     A There are undeployed changes. Click 'Deploy Changes' to deploy them. View Details |              |                  |                |            |                                |                    |                                 |  |
| ► Data So  | ources   | System Co    | onfiguration     |                |            |                                |                    |                                 |  |
| Remote     | e Networks and<br>s Configuration  | (            |                  |                |            | 4                              | <u>.</u>           | Gei                             |  |
| Try it o   | ut   | Auto         | Update           | Backup and Rec | overy      | Global System<br>Notifications | Index Managemen    | t Aggregated Data<br>Management |  |
| ► Apps     |  |              |                  |                |            |                                | *                  |                                 |  |
|            |  | Forwarding   | Destinations     | Routing Rule   | s Do       | main Management                | Extensions Manager | ent Resource Restrictions       |  |

You should see the SentinelOne tab in QRadar.

| <b>≡</b> 1 | BM QRadar |              |                  |        |         |       |             |
|------------|-----------|--------------|------------------|--------|---------|-------|-------------|
| Dashboard  | Offenses  | Log Activity | Network Activity | Assets | Reports | Admin | SentinelOne |

# 4.2. Generate an API Token

To use the SentinelOne App, you must generate an API token from the SentinelOne Management Console.

**Important:** If you have multiple SentinelOne Management Consoles, you must generate an API Token for each one.

The API token you generate is time limited. To regenerate a new token (and invalidate the old one), log in with the dedicated SentinelOne account. You do not need to create a new account.

#### To generate an API Token:

1. In your Management Console, click **Settings** > **USERS**.



2. Find your user and click its edit button.

If you want to create a new user for QRadar integration, follow the steps in Creating New Management Console Users and then log in to the new user.

**Note:** A user with a role of **Site Admin** can mitigate threats from the QRadar Console. A user with a role of **Site Viewer** can view threats but cannot take action.

Note: You can generate a token only for your own user.

| SET | TINGS |          | CONFIGURATION | NOTIFICATIONS          | USERS I           | NTEGRATIONS | POLICY OVERRIDE | SITES |  |                          |   |
|-----|-------|----------|---------------|------------------------|-------------------|-------------|-----------------|-------|--|--------------------------|---|
|     |       | New User | Delete Select | tion No Items Selected | 1                 |             |                 |       |  |                          |   |
|     | 0     | Email 🔺  | .com          | Full Name<br>Eyal Test | Role<br>Site admi | Sites       | Se<br>Se        | ource | Last Connected<br>Feb 20th 2019 13:42:29 | Remote Shell<br>Disabled | Q |

The Edit User window opens.

3. In the API Token section, click Generate.



If you see **Revoke** and **Regenerate**, you already have a token. If you revoke or regenerate it, scripts that use that token will not work. There is no confirmation. **Revoke** removes the token authorization. **Regenerate** revokes the token and generates a new token.

If you click Generate or Regenerate, a message shows: This is the last time you can see this token. It shows the token string and the date that the token expires.

| API T | ōken   | × |  |  |  |  |  |  |
|-------|--|---|--|--|--|--|--|--|
|       |  |   |  |  |  |  |  |  |
|       | This is the last time you can see this token.  |   |  |  |  |  |  |  |
|       | 2814957599651442944XFL7RYcMn2xTAbZVAfpq74dJRNItkzznJiJOpGs   |   |  |  |  |  |  |  |
|       | This API token will expire on 7/26/18  |   |  |  |  |  |  |  |
|       | Download Copy  |   |  |  |  |  |  |  |
| By    | y electing to click "Download" you agree that if you use this token to integrate your SentinelOne instance with another service provider, Section 2.4 of SentinelOne's Terms of Service shall apply to such integration. |   |  |  |  |  |  |  |
|       | K Back   |   |  |  |  |  |  |  |

4. Copy the token or click **Download** to save it.

# 4.3. Adding SentinelOne Management Consoles to the SentinelOne App

To use the SentinelOne App, you must add each SentinelOne Management Console as input for the SentinelOne App.

#### To add a SentinelOne Management Console in the SentinelOne App:

**Note:** If you have more than one SentinelOne Management Console, repeat this procedure for each one.

1. Click the **SentinelOne** tab of the QRadar Console.

| ≡ IB      | M QRadar |              |                  |        |         |       |             |
|-----------|----------|--------------|------------------|--------|---------|-------|-------------|
| Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin | SentinelOne |

If you are adding a second SentinelOne Management Console, click the SentinelOne tab of the QRadar Console, and click **Settings**.

| ≡ в           | M QRadar   |              |                  |        |         |       |             |
|---------------|------------|--------------|------------------|--------|---------|-------|-------------|
| Dashboard     | Offenses   | Log Activity | Network Activity | Assets | Reports | Admin | SentinelOne |
| (II) Sentinel | Dhe 🏻 📲 An | alyze 🖵 N    | letwork          | ngs    |         |       |             |

2. Click Create New Input.

| =         | BM QRadar |              |                  |        |           |          |               |       |             |                    |       | ¢ 2                  |
|-----------|-----------|--------------|------------------|--------|-----------|----------|---------------|-------|-------------|--------------------|-------|----------------------|
| Dashboard | otlenses  | Log Activity | Network Activity | Assets | Reports I | nisks vu | inerabilities | Admin | sertinelone |                    |       | System Time: 5:00 PM |
|           |           |              |                  |        |           |          |               |       |             | + Create New Input |       |                      |
| Name      |           |              |                  |        |           |          | URL           |       | 551.        |                    | Adve? | Actions              |
| NO DA     | ТА        |              |                  |        |           |          |               |       |             |                    | False |                      |

- 3. In the window that opens, enter:
  - **Name** The name of the SentinelOne Management Console as it will show in the QRadar Console.
  - URL The URL of the SentinelOne Management Console. For example: https://xyz.sentinelone.net.
  - API Token The SentinelOne API token generated in the SentinelOne Console.
  - **SSL Verification** The default is selected. We strongly recommend you keep this selected to use server certificate verification.
- 4. Click Add.

# 4.4. Using the SentinelOne App

The SentinelOne App shows threats collected from your different SentinelOne Sites. The data is from real-time API requests.

### To see and filter threats:

By default, all threats from all sites are shown.

- 1. Click **SentinelOne > Analyze**.
- 2. To view threats from a specific site, select the site from the **Site** menu.



3. To find specific threats, use the Filter and Search options, and click Apply.

| ≡ івм с       | Radar  |                                       |                  |                  |            |                   |                                       | 다 으                      |
|---------------|--|---------------------------------------|------------------|------------------|------------|-------------------|---------------------------------------|--------------------------|
| Cashboard O   | flerses Log Activity Network Activity Assets Reports Adr | nin sentinelOne                       |                  |                  |            |                   |                                       | System Time: 2:10 PM     |
| 🗰 SentinelOng | Analyze 🗸 Network 🖷 Settings                             |                                       |                  |                  |            |                   |                                       | Scope purple  Site All - |
| Filter:       | Resolved   |                                       | Migration Status | 7                | ne         |                   | Search                                | Apply                    |
|               | Select *   |                                       | Select *         | A                | time *     |                   | Q. Search                             | 10 Results *             |
| Status        | File Name  | Endpoint                              | Created          | Updated          | Site       | Classification    | Action Done                           |                          |
| •             | Unknown file   | a mana i are                          | 07/05/2019 10:28 | 07/05/2019 10:30 | wee        | Hacktool          | quarantine, kill, remediate           |                          |
| 0             | AsankaBorus.doo  | A 1997                                | 07/05/2019 10:05 | 07/05/2019 10:12 | wee        | PUA               | quarantine, kill, remediate           |                          |
| 0             | yearweith.aua  | · · · · · · · · · · · · · · · · · · · | 07/05/2019 09:22 | 07/05/2019 09:33 | Andre      | Malware           |                                       |                          |
| 0             | Ransomware sco   | E many 111 (201)                      | 07/05/2019 09:22 | 07/05/2019 09:33 | Andre      | Malware           | rollback, quarantine, kill, remediate |                          |
| 0             | Ransomware exe   | 4 mana 211 million                    | 07/05/2019 09:20 | 07/05/2019 09:33 | Andre      | Malware           |                                       |                          |
| 0             | EpicGamesLaunche: exe                                    | <b>H</b>                              | 07/05/2019 08:32 | 07/05/2019 08:32 | Demo MacOS | generic heuristic |                                       |                          |
| 0             | 19.033.0218.0011   |                                       | 07/05/2019 00:39 | 07/05/2019 00:39 | merrick    | Malware           |                                       |                          |
| 0             | ami84  | E many (10000 0000)                   | 07/05/2019 00:39 | 07/05/2019 00:39 | merrick    | Malware           |                                       |                          |
| 0             | EpicGamesLauncher.exe                                    | 4 mms 101-101-00.770                  | 07/05/2019 00:15 | 07/05/2019 00:15 | JKim_Home  | Malware           |                                       |                          |
| 0             | Thunderbirder Vulnerable[15].doom                        | · · · · · · · · · · · · · · · · · · · | 05/05/2019 21:29 | 05/05/2019 21:55 | ScottR     | Malware           | rolback, quarantine, kill, remediate  |                          |
|               |  |                                       | 1 2 3 4 5 6      | 7 8 9 10         |            |                   |                                       |                          |

4. Click a threat name to view more details about that threat.

#### To mitigate a threat:

- 1. Click **SentinelOne > Analyze**.
- 2. Click an item link (for example, a file name) to see its details.
- 3. Optional: Click **Google** or **Virus Total** to see if the hash is known.
- 4. Click Actions.

| = IBM QRadar   |  | ¢ 2   |
|--|--|---|
| Dazhboard Offenses Log.Adviety Network.Adviety Assets Reports Admin Seministone                    |  | Spilen Time 2:37 PM   |
| 🗰 Sentenel Oner 🔄 🗄 Analyze 🖉 Network 🛛 🗃 Settings   |  | Scope purple   Site All -   |
| K Back U streadth can<br>active  | Action Dune  | W SenterAuthon Consults Actions -   |
| File Info  | Summary  | Indicators Mark as Threat   |
| File Name: incomedition and Gates<br>Prete: "Device/Handdish Volume 102 ens/Andr                   | Status:         active         0           Status:         553:651         424-64278048655665682556  | Nil<br>Abnormalities Ourrantine<br>This binary uses non-standard DOS stubs Un-quarantine<br>Hiding/Seeabhiness Remediate<br>Remediate |
| Drvice WNR-AMH-GEMO  | Solato Assol (K. Solato | This biary may contain encrysted/compressed into as measured by high Resolves General This binary creates a System Service            |
| Deename: WNR7-AMR-DEMIONAble Noordam<br>Agent water: 3.1.3.3<br>Bec: Andre<br>Group: Default Group | Canadicator: Malanzo<br>Bigen Monthy: NAA<br>Grows: Collad Corop<br>Management: Antico   |   |
| Time<br>Crushel: 07/05/2019 09:22<br>Upsmil: 07/05/2019 09:33                                      |  |   |

5. Select a mitigation option.

#### **Mitigation Options:**

- Mark as benign For false positives. Adds the item to the whitelist, marks the threat as resolved, and removes it from the **Dashboard** view.
- Mark as threat Defines the item as a threat in the Dashboard.
- Kill Stops processes. Active content in documents, executables, and sub-processes are stopped. The Agent enables Kill for processes that act against normal endpoint behavior or do not fit the actions of the application the process is hiding in.

• Quarantine - Stops processes, encrypts the executable, and moves it to a confined path.

If a threat is known, the Agent automatically kills the threat before it can execute. The only mitigation action for you is **Quarantine**.

- Un-quarantine Removes a file from quarantine.
- **Remediate** (Windows and macOS) Stops processes, quarantines binaries, removes linked libraries, deletes seed files, and restores configuration of the OS, application, and user settings to the state before the attack began.
- Rollback (Windows only) Restores the endpoint to a saved point.

This option is best for ransomware mitigation and disaster recovery. It can remove legitimate work done since the last VSS snapshot.

• **Resolve** - Removes the threat from the Dashboard.

#### To see and filter endpoints:

- 1. Click **SentinelOne > Network**.
- 2. Use the **Filter** and **Search** options to find specific endpoints, for example, of a specific OS.

| E IBM QRadar  |                           |               |           |                    |               |                  |                  | 4 <u>°</u>               |
|---|---------------------------|---------------|-----------|--------------------|---------------|------------------|------------------|--------------------------|
| Dashboard Offenses Log Activity Network Activity Assets | Reports Admin SentinelOne |               |           |                    |               |                  |                  | System Time: 2.41PM      |
| 🗰 Sentimel Chitr 🔄 Analyze 📿 Network 🔠 Settings         |                           |               |           |                    |               |                  |                  | Scope purple  Site All - |
| Filter:   | Search                    |               | Active    |                    |               | 08               |                  | Apply                    |
|   | Search                    |               | At *      |                    |               | AT *             |                  | 10 Results *             |
| Endpoint Name   | Site                      | Group         | Domain    | Console Visible IP | Agent Version | Last Logged User | Last Active      |                          |
| GRANTM-Win8-v3  | Moerschel                 | detect-detect | WORKGROUP | 10.0203            | 2.8.2.6745    | user             | 06/05/2019 22:08 |                          |
| KCMD19-WIN7   | merrick                   | Wo-Server     | WORKGROUP |                    | 3.0.2.35      | PlexPass         | 07/05/2019 12:40 |                          |

- 3. Click Apply.
- 4. Click an endpoint name to view the endpoint details, and threats associated with the endpoint.

#### To run an action on an endpoint:

- 1. Click **SentinelOne > Network**.
- 2. Use the **Filter** and **Search** options (and click **Apply**) to find specific endpoints on which you will run the action.
- 3. From the SentinelOne API **Network** tab, click an endpoint. You see the details of that endpoint and its network status.
- 4. Click Actions.

| SentinelOng | Analyze C Network III Setting     | P                          |                          |                  |                                   | 12                | Scope purple   Site ABC-Corp * |
|-------------|-----------------------------------|----------------------------|--------------------------|------------------|-----------------------------------|-------------------|--------------------------------|
| K Back      | Last Logged User: ning            | Last Active:<br>Site: ABC  | 22/05/2019 09:28<br>Corp | Gre              | aup: Default Group<br>main: local |                   | Actions -                      |
| General     |                                   |                            |                          | Network          | Adapters                          |                   |                                |
| Agent Ver   | rsion: 2.6.5.2559                 | Console connectivity: True |                          | Name             | P                                 | Mac Ad            | dress                          |
| Scan Stat   | itus: none                        | Network status: connecte   | d                        | enD              |                                   | 00.0c.25          | k8tx3:61                       |
| Memory:     | 2048                              | Subscribed on: 11/11/201   | a 10: <b>1</b> 6         |                  |                                   |                   |                                |
| CPU: In     | ntel(R) Core(TM) i9-8950HK CPU @. | Console visible IP:        |                          | (BUNO            |                                   | 00.00.0           | 202:02:00                      |
| Core Cou    | unt: 2                            | IP Address:                | 5050 5560 70005          |                  |                                   |                   |                                |
| Threats     | File Name                         | Endpoint                   | Created                  | Updated          | Site                              | Classification    | Action Done                    |
| 0           | invoices.docx                     | esktop nirg-macos-vm1      | 20/05/2019 07:21         | 20/05/2019 07:25 | ABC-Corp                          | Malware           |                                |
| 0           | sudo                              | esktop nirg-macos-vm1      | 12/05/2019 15:51         | 12/05/2019 15:52 | ABC-Corp                          | Benign            |                                |
| ٢           | exthen                            | esktop nirg-macos-vm1      | 12/05/2019 12:50         | 12/05/2019 13:02 | ABC-Corp                          | Benign            |                                |
| 0           | invoices.docs                     | desktop nirg-macos-vm1     | 12/05/2019 12:50         | 12/05/2019 13:02 | ABC-Corp                          | Malware           |                                |
| 0           | matware                           | desktop nirg-macos-vm1     | 12/05/2019 12:50         | 12/05/2019 13:02 | ABC-Corp                          | OSX.Malware       |                                |
| 8           | vmware-scole-daemon               | desktop nirg-macos-vm1     | 23/04/2019 12:03         | 12/05/2019 13:03 | ABC-Corp                          | generic.heuristic |                                |
| 1.00        |                                   |                            |                          | 00.0010010.00.00 | 100.0                             |                   |                                |

5. Select an action.

Actions:

- Full Scan Scans the SentinelOne Agent installed on this endpoint. Finds dormant suspicious activity, threats, and compliance violations, that are then mitigated according to the policy.
- Abort Scan Stops scanning the SentinelOne Agent installed on this endpoint.
- · Fetch Logs Generates logs of SentinelOne Agent activity on this endpoint.
- **Disconnect** Disconnects the endpoint from the network. The endpoint can communicate only with the SentinelOne Management Console but not with other components on the network.

#### To manage SentinelOne Consoles integrated with QRadar:

- 1. Click **SentinelOne > Settings** to see a list of SentinelOne Management Consoles integrated with QRadar.
- 2. If you have more than one SentinelOne Management Console, to integrate a new one with QRadar, click **Create New Input**.
- 3. To remove the integration of a SentinelOne Management Console, click **delete**.

| ≡ IBM QRadar                                     |                                  |                    |         |         |
|--|----------------------------------|--------------------|---------|---------|
| Dashboard Offenses Log Activity Network Activity | Assets Reports Admin SeminelOne  |                    |         |         |
| 🗰 SentinelOng   🧟 Analyze 📿 Network 🛛 H. Se      | tings                            |                    |         |         |
|  |                                  | + Create New Input |         |         |
| Name   | URL                              | SSL                | Active? | Actions |
| purple   | Nan Load activities with the set | True               | True    | delete  |

# To view threats in the SentinelOne Management Console:

Open the SentinelOne Management Console for more features. For example: Perform more actions on endpoints, view threat attack story lines, and run administrative actions. For a video tour of the Management Console, click here.

- 1. Click SentinelOne> Analyze.
- 2. Click an item you want to view from the SentinelOne Management Console.
- 3. Click the **SentinelOne Console** button.

(I) SentintelOne Console

# 5. Upgrading From the Beta Version

**Important:** If you are upgrading from the Beta version, you must first follow this procedure BEFORE installing the latest SentinelOne DSM and App.

- 1. Uninstall the existing SentinelOne DSM.
  - 1. Select Admin from the Main menu, and click Extensions Management.
  - 2. Select the SentinelOne DSM from the list, and click Uninstall.
- 2. Uninstall the existing SentinelOne App.
  - 1. Select Admin from the Main menu, and click Extensions Management.
  - 2. Select the SentinelOne App from the list, and click Uninstall.
- 3. Delete the existing SentinelOne Dashboard.
  - 1. Click Dashboard and select SentinelOne Dashboard.
  - 2. Click Delete Dashboard.

|   | ≡         | IBM    | QRadar       |               |                  |        |          |           |                 |                    |            |
|---|-----------|--------|--------------|---------------|------------------|--------|----------|-----------|-----------------|--------------------|------------|
| ſ | Dashboard |        | Offenses     | Log Activity  | Network Activity | Assets | Reports  | Admin     | SentinelOne     |                    |            |
|   | Show Da   | shboai | rd: Sentinel | One Dashboard |                  | ¢      | New Dash | board 📑 R | ename Dashboard | 😫 Delete Dashboard | Add Item V |

- 4. Delete all SentinelOne saved searches.
  - 1. Click Log Activity > Search > New Search.



- 2. Filter the list of Available Saved Searches for SentinelOne.
- 3. Delete all SentinelOne saved searches.

| ≡   | E IE     | 3M QRadar     |                   |                  |        |         |               |
|-----|----------|---------------|-------------------|------------------|--------|---------|---------------|
| Das | shboard  | Offenses      | Log Activity      | Network Activity | Assets | Reports | Admin         |
| ¢   | Manage S | earch Results | Manage Custom     | Properties       |        |         |               |
| •   | Save     | ed Searcl     | 16S Group         | Select a group   |        | ·       | Manage Groups |
|     | Type S   | Saved Search  | or Select from L  | .ist             |        |         |               |
|     | sent     | tinelone      |                   |                  |        |         |               |
|     | Availat  | ble Saved Sea | rches             |                  |        |         |               |
|     | Sentin   | elOne - Syste | m Activity logs   | audit            |        |         |               |
|     | Sentin   | elOne - Event | s Filename        |                  |        |         |               |
|     | Sentin   | elOne - Malw  | are by source ip  | )                |        |         |               |
|     | Sentin   | elOne - Malw  | are Events by us  | sername          |        |         |               |
|     | Sentin   | elOne - Malw  | are Events file p | ath              |        |         |               |
|     | Lo       | oad D         | eleteS            | how AQL          |        |         |               |

- 5. Install the SentinelOne DSM for QRadar. Go to Installing the SentinelOne DSM in QRadar [6] and follow the instructions.
- 6. Install the SentinelOne App for QRadar. Go to Installing the SentinelOne App in QRadar [21] and follow the instructions.

# 6. Advanced Configuration

# 6.1. Configuring the Syslog Format

The Syslog output generated by SentinelOne must be properly parsed to create meaningful and valid log entries in QRadar. The DSM integration maps SentinelOne IDs to QRadar fields. The IDs are from SentinelOne API, version 2.0.



# NOTE

The Syslog format uses a pipe ( | ) as a delimiter. In this article, it is not a code symbol for "or". Enter the pipe as a shown.

#### Syntax:

CEF:2|SentinelOne|Mgmt|OS|eventID|eventName|eventSeverity|Details

## Valid Values

| Field                      | Description   | Valid Values             | Mapped QRadar<br>Field |
|----------------------------|---|--------------------------|------------------------|
| Format type<br>and version | Use CEF, version 2, for integration with SentinelOne.   | CEF:2                    | Event Category         |
| SentinelOne                | The Company field is hard-<br>coded to SentinelOne.   | SentinelOne              | SentinelOne            |
| Mgmt                       | SentinelOne component and version.  | Mgmt                     | Slenvironment          |
| OS                         | Short name of the operating system of the endpoint.   | Windows<br>Linux<br>OS X | SlosName               |
| eventID                    | Unique ID Of the event. This is matched to the QRadar Event IDs.                                      | integer                  | Event ID               |
| eventName                  | Readable text to complement the ID and to headline the event in text.                                 | string                   | EventDesc              |
| eventSeverity              | Threat level, according<br>to SentinelOne intelligence,<br>mapped to the RFC 3164<br>severity values. | string                   |                        |
| Details                    | Available on certain alerts, in standard and custom QRadar variables, for correlation when possible.  | See next table           |                        |

# **6.2. Finding SentinelOne Events**

To add SentinelOne events to the QRadar logs, you need a list of the SentinelOne event names and ID numbers.

## To see a complete list of SentinelOne events:

- 1. Open the SentinelOne Management Console.
- 2. Click the **Help menu > API Doc**.



3. Click API REFERENCE.



4. Click Activities > Get activities types.

| OVERVIEW<br>MANAGEMENT SDK<br>API REFERENCE | Get activities types                   |
|---|--|
| Accounts                                    | Get a list of activities types.        |
| Activities                                  |  |
| Get activities types                        | <ul> <li>Test this endpoint</li> </ul> |
| Get activities                              |  |
| Agent Actions                               | KON ON CONSOLE                         |

5. Click RUN ON CONSOLE.

The list of activities opens. For example, ID 48 is the event Agent Recommissioned.



# 6.3. Regular Expressions for Mapping

## **Regular Expressions for QRadar Mapping**

| Field          | Regular Expression                     |
|----------------|--|
| Event Category | (CEF):2                                |
| S1environment  | CEF:2\ SentinelOne\ (\w+)\ .+\ .+\ .+\ |

| Field            | Regular Expression   |
|------------------|--|
| S1osName         | CEF:2\ SentinelOne\ .+\ (.+)\ .+\ .+\ .                        |
| Event ID         | CEF:2\ SentinelOne\ .+\ .+\ (\w+)\ .+\ .+\                     |
| EventDesc        | CEF:2\ SentinelOne\ .+\ .+\ .+\ (.+)\ .+\                      |
| Log Source Time  | $\t((\S+)\s(\d+)\s(\d+)\s(\d+1,2)\:(\d\{1,2\})\:(\d\{1,2\})\)$ |
| Source IP        | \ssrc\=(\d{1,3}\.\d{1,3}\.\d{1,3})                             |
| Source Port      | \sspt\=(\d{1,5})   |
| Source MAC       | \ssmac\=((?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2})                |
| Destination IP   | \sdst\=(\d{1,3}\.\d{1,3}\.\d{1,3})                             |
| Destination Port | \sdpt\=(\d{1,5})   |
| Destination MAC  | \sdmac\=((?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2})                |
| Username         | \sduid\=(\d{1,10})   |
| S1sourceHost     | \sshost\=(\S+)   |
| S1deviceHost     | \sdvchost\=(\S+)   |
| S1deviceIP       | \sdvc\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})                    |
| Protocol         | \sproto\=(TCP UDP ICMP GRE)                                    |
| S1destService    | \sdestinationServiceName\=(\S+)                                |
| S1eventCat       | \scat\=(\S+)   |

# 7. Troubleshooting

#### Basic SentinelOne App troubleshooting before I open a Support ticket

Here are some solutions to troubleshoot this issue. Do them in the order listed until the problem is solved.

- 1. See if the Deploy Changes button appears in the QRadar dashboard. If it does, click it.
- 2. Earlier versions of the SentinelOne app should be removed before you install a newer version. Check whether there are two versions of the SentinelOne app installed. (In the QRadar Console, click the **Admin** menu and click **Extensions Management** to see a list of installed extensions.) If there is more than one SentinelOne app installed, uninstall both of them and reinstall one.
- 3. Uninstall and reinstall the app.

#### Why do I not see any SentinelOne events?

Here are some solutions to troubleshoot this issue. Do them in the order listed until the problem is solved.

- 1. See if the **Deploy Changes** button appears in the QRadar dashboard. If it does, click it.
- 2. Check the Log Source configuration settings. In the QRadar Console, click the **Admin** menu and click Log Sources. Make sure **Log Source Extension** is set to the SentinelOne extension.
- 3. Check the Syslog settings. In the SentinelOne Management Console, click **Settings** > **Integrations** > **Syslog**. Make sure that **Formatting** is set to **CEP2**.
- 4. Contact SentinelOne Support.

#### Why do I see an Unknown event?

An Unknown event is collected and parsed, but is not mapped or categorized to a specific log source.

If you see a SentinelOne log event marked as **Unknown**, you can manually add it to the QRadar system using the correct SentinelOne activity type and ID. For a list of SentinelOne activity types, see Finding SentinelOne Events [37].

#### What information should I submit to SentinelOne Support when opening a ticket?

- 1. URL of your SentinelOne Management Console.
- 2. QRadar version and build number. This information is available from the QRadar Console. From the Dashboard tab, select **Help >About**.
- 3. The SentinelOne DSM version, and SentinelOne App version, installed on the QRadar Console.
  - a. Log in to the QRadar Console as Admin.
  - b. From the Admin tab, in the System Configuration group, click Extensions Management.
  - c. Search for the SentinelOne extensions, and write their version numbers.

- 4. A detailed description of what occurred, and how to reproduce it.
- 5. What you expected compared to what you saw.
- 6. A screen capture showing the issue or on-screen error message.
- 7. A screen capture of the log source configuration.
  - a. Log in to the QRadar Console as Admin.
  - b. From the Admin tab, in the Events group, click **Log Sources**.
  - c. Double-click the log source to open the edit screen and take a screen capture.
- 8. A screen capture of the incorrect event. Double-click an event in the **Log Activity** tab to view the Event Summary, and submit a screen capture.
- 9. Steps taken by the user or administrator to try and resolve the issue.
- 10. The QRadar support package tar.gz file.
  - a. Using SSH, log in to the QRadar Console as the root user.
  - b. Run:sudo /opt/qradar/support/get\_logs.sh -a
  - c. Attach the generated /store/LOGS/XXXX.tar.gz file to the support ticket.

For example: logs\_qrd-dev-test3\_20190505\_3620c115.tar.gz

- 11. An export of the log files.
  - a. Log in to the QRadar Console as Admin.
  - b. From the Admin tab, click System and License Management.
  - c. Select the QRadar appliances that you want to collect logs from in the user interface. If you do not select any appliance, the default action is to collect logs from the QRadar Console.
  - d. Select Actions > Collect Log Files.
  - e. Click **Collect Log Files**. The log collection process starts and the status bar will update when log collection is complete.
  - f. Click **Download** and save the file.
  - g. Attach the log to your support ticket.
- 12. A Full XML export from the **Log Activity** tab on the QRadar Console. Explain the events that appear to be parsing incorrectly in the description of your service request.
  - a. From the QRadar Console, click the Log Activity tab.
  - b. Click the **View** drop-down and select a time interval.
  - c. Review the filtered events to ensure that it contains your issue or concern.
  - d. From the navigation menu, select Actions > Export to XML > Full Export (All Columns).
  - e. Attach the XML event export.

Checklist before sending email to SentinelOne Support: The email to SentinelOne Support includes: [] URL of the SentinelOne Management Console [] QRadar version and build number [] SentinelOne DSM version number [] SentinelOne App version number [] A detailed description of what occurred, and how to reproduce it [] What you expected compared to what you saw [] A screen capture showing the issue or on-screen error message [] A screen capture of the log source configuration. [] A screen capture of the incorrect event [] Steps taken to try and resolve the issue [] Attachment of the QRadar support package tar.gz file [] Attachment of the exported log files [] Attachment of the XML exported Log Activity tab

#### How do I contact SentinelOne Support?

Phone: +1-855-868-3733 select Option 2

Web: support.sentinelone.com

Email: Support@sentinelone.com