IBM Security

Systems Guide

IBM SECURITY SOAR CLEARING SYSTEM

Technical View and Use-Cases

Version 1.5.1-141, 12-01-2021: Draft

NOTICES

This information was developed for products and services offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

TRADEMARKS

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.
Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.
ITIL is a Registered Trade Mark of AXELOS Limited.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.
© Copyright International Business Machines Corporation 2020.
This document may not be reproduced in whole or in part without the prior written permission of IBM.
US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© Copyright IBM Corp. 2020. All rights reserved

Table of Contents

1. Description 3
2. Introduction 4
    2.1. Purpose of this document 4
    2.2. Target audience of this document 4
3. Architectures 5
    3.1. Clearing-Application-Architecture 5
    3.2. Clearing-Server-Architecture 5
4. Use-Cases 7
    4.1. View shared incidents 7
    4.2. Distribute incident to other brands 8
    4.3. Distribute SOAR configuration across clearing network 8
5. Clearing Release & Development Cycle 10
6. Resources 12

© Copyright IBM Corp. 2020. All rights reserved

1. Description

IBM Security SOAR Clearing System is an extension for a secure interconnection of multi server and multi brand Resilient/SOAR platform in international corporate environments. It is designed to help the various security teams of a company to collaborate with consistency across borders, no matter if these borders are regional or systemic.

© Copyright IBM Corp. 2020. All rights reserved

2. Introduction

2.1. Purpose of this document

This document describes the necessary infrastructure for secure data transmission between different IBM Security SOAR Systems in international customer environments and shows their intention on selected use cases.

2.2. Target audience of this document

This document serves as a reference work for the employees responsible for the system and enables external IT specialists to understand the essential functions of the system described in the event that no qualified employees are available.

© Copyright IBM Corp. 2020. All rights reserved

3. Architectures

3.1. Clearing-Application-Architecture

Figure 1. Overview of Clearing internal application architecture

The clearing server has been developed in Python3.

The Flask framework with the Jinja2 rendering engine has been used as the technology for answering web queries.

An MySQL database has been used as the database for the configurations.

SOAR provides the required information via the REST API, i.e. HTTPS traffic on port 443 and the resilient circuits, i.e. the STOMP protocol.

No data is stored on the clearing server.

The only information that is saved is the clearing program log.

3.2. Clearing-Server-Architecture

© Copyright IBM Corp. 2020. All rights reserved

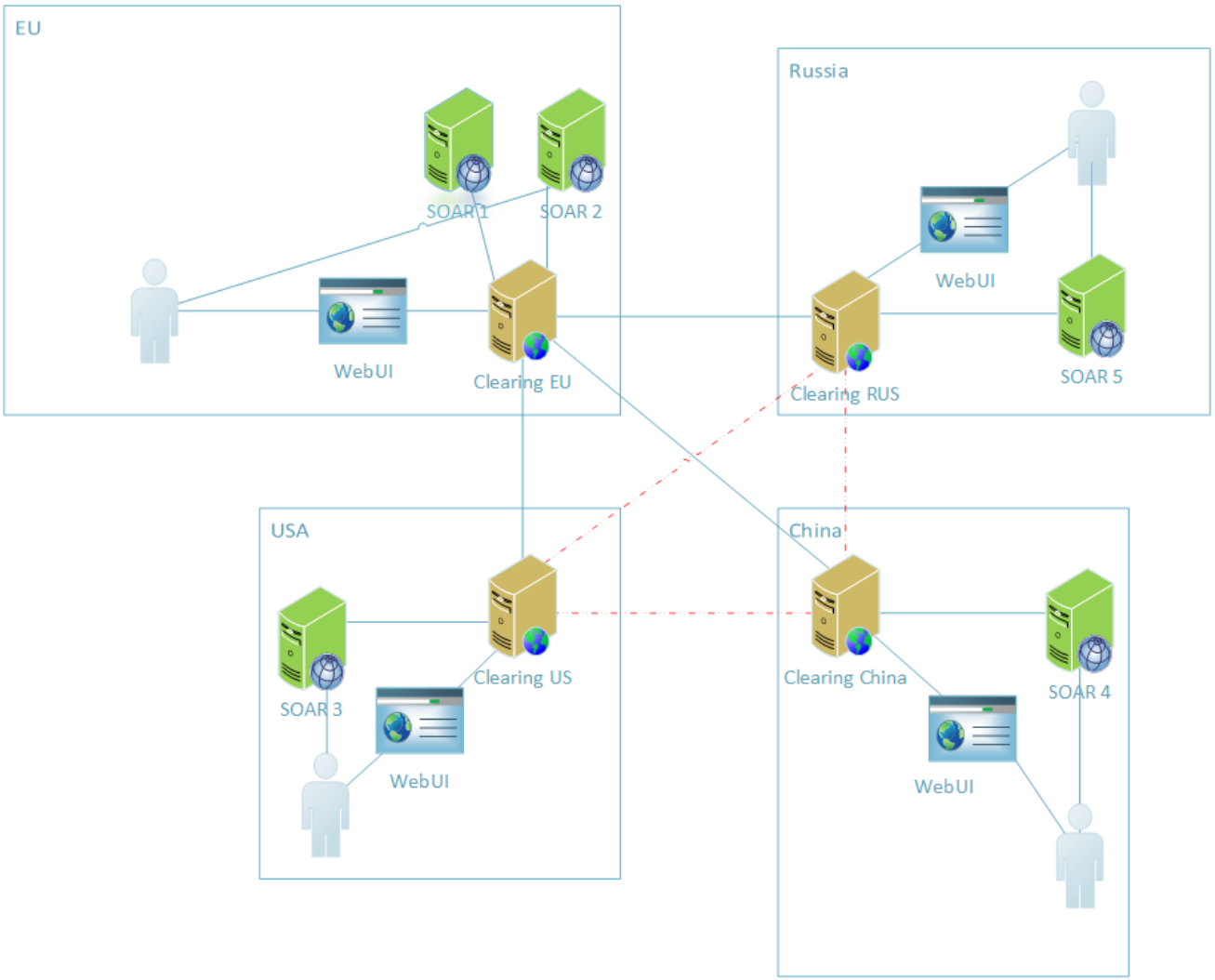

Figure 2. Overview of Clearing server architecture between Regions

SOAR is built up in a distributed, independent environment. Each region and each subsidiary has its own SOAR instance. There is no direct connection between different SOAR servers. Likewise, there is no direct connection between the clearing servers in one region and SOAR servers in another region. Any communication between the regions takes place exclusively via the respective clearing servers of the regions concerned.

The clearing servers communicate with each other via REST-API over HTTPS and port 443.

© Copyright IBM Corp. 2020. All rights reserved

4. Use-Cases

This section describes the different use-cases which can be achieved with the documented clearing system.

With the Clearing system, newly created incidents will get a new task "Involve Group Coordination" added. This task can be used for two use-cases. Firstly, the task controls with a distribution table whether other brands get access to read an incident through their clearing system WebUI. Secondly, a brand can decide to distribute this incident to another brand, which means to create a copy of this incident on the other SOAR system.

4.1. View shared incidents

The sharing of incidents through the clearing system is controlled with a `READ-Only` flag within a distribution table for each SOAR system (named `brand`).

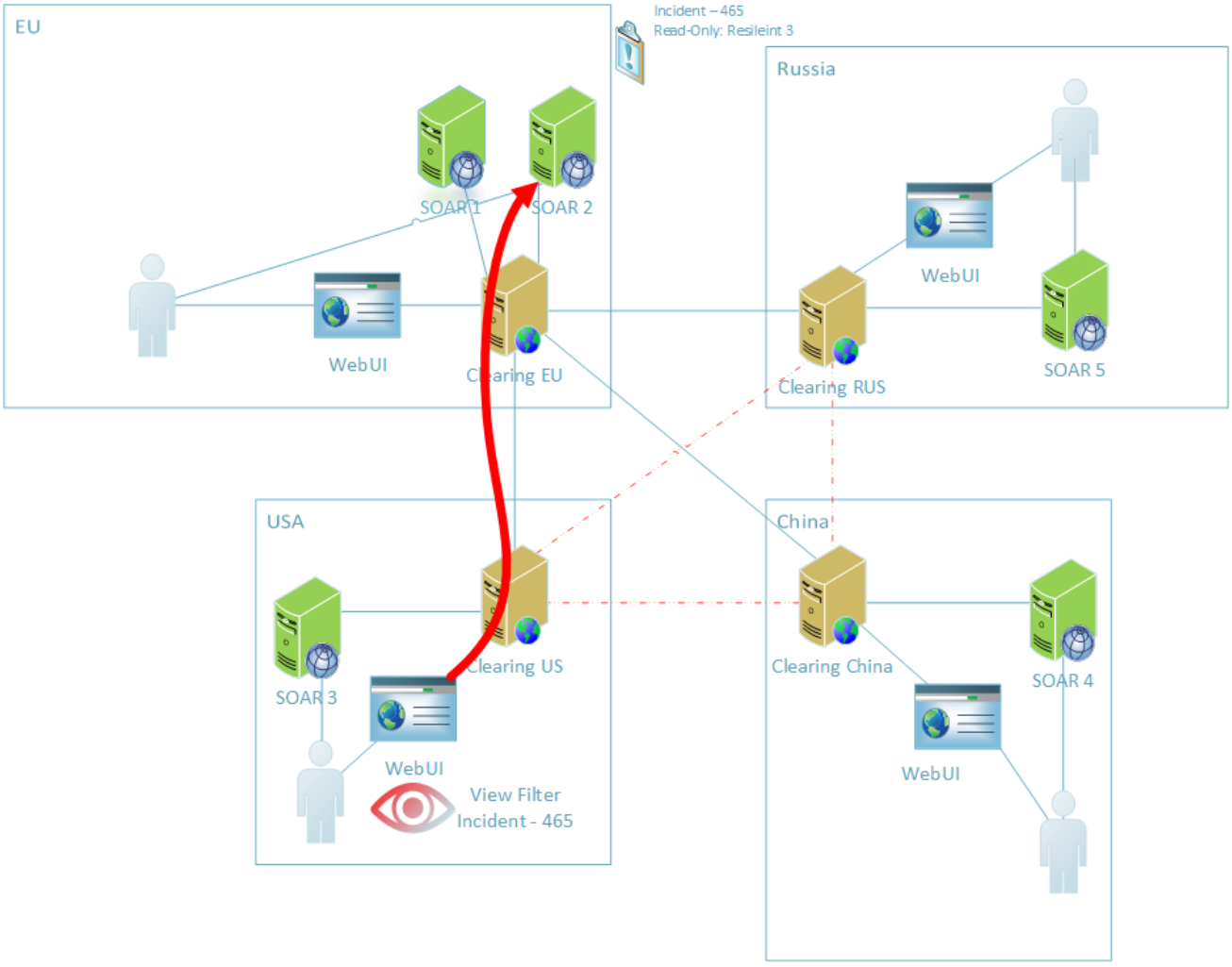

Figure 3. Clearing view shared incident from Europe on clearing USA

As shown in the example above `SOAR 2` allows `SOAR 3` to view the shared incident `incident-465`, which gets filtered according to a whitelist before a user from `SOAR 3` can

© Copyright IBM Corp. 2020. All rights reserved

view that incident on their clearing system US WebUI.

4.2. Distribute incident to other brands

During the evaluation of an incident `incident-465` it's concluded that another SOAR system needs a copy of this incident for their own incident response. The `Distribute` flag within the distribution table can be leveraged to create a new copy incident `incident-123` from the originating incident `incident-465`. This copied incident gets filtered according to the same whitelist used for viewing shared incidents.

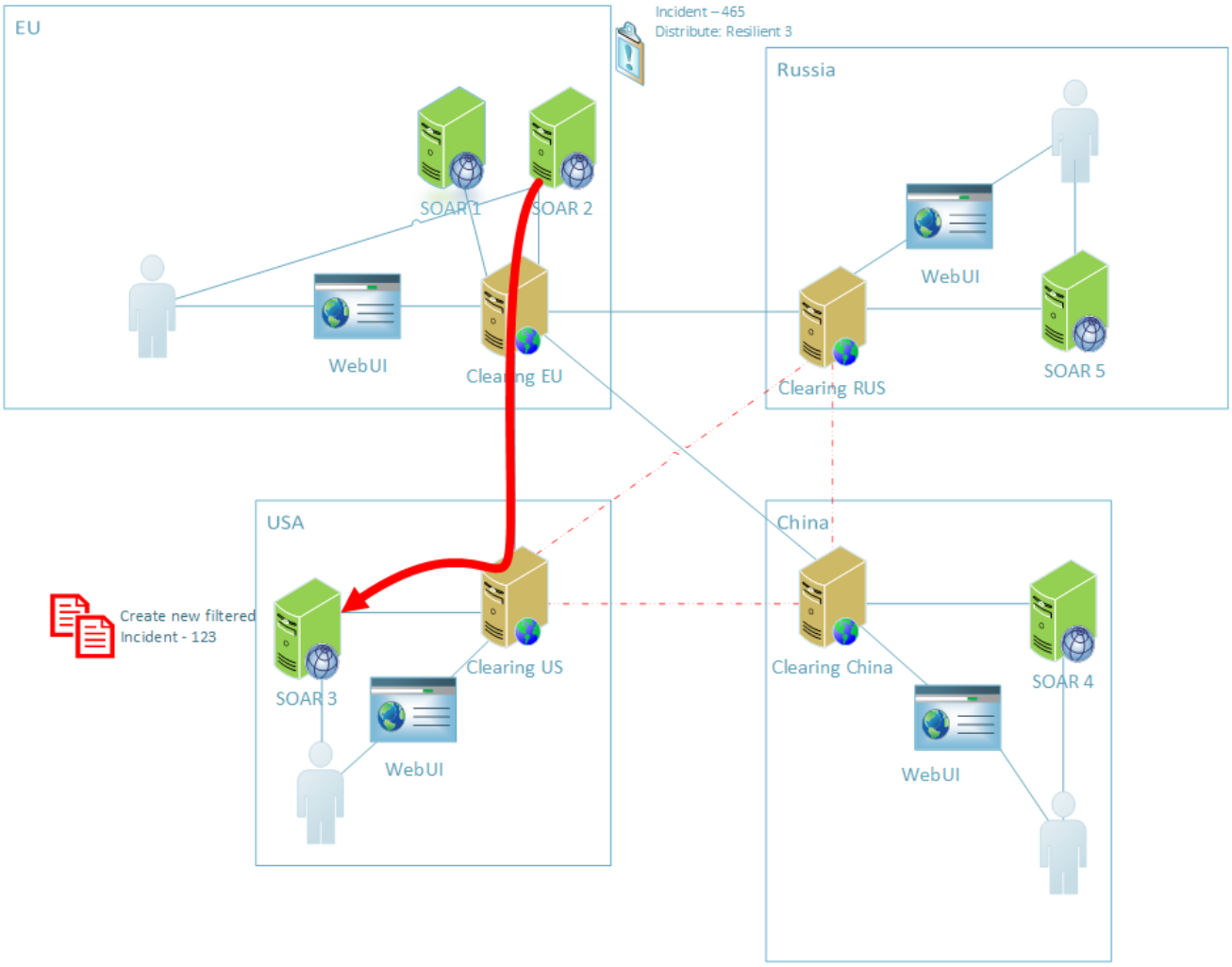

Figure 4. Distribute incident from Europe to USA

As shown in the example above, SOAR 2 enabled the distribution of incident `incident-123`. This triggered the clearing system EU to send a pre-filtered copy of this incident through clearing system US to SOAR 3.

4.3. Distribute SOAR configuration across clearing network

The clearing system can distribute the SOAR configuration from a primary node across the same clearing network to all non-primary nodes.

© Copyright IBM Corp. 2020. All rights reserved

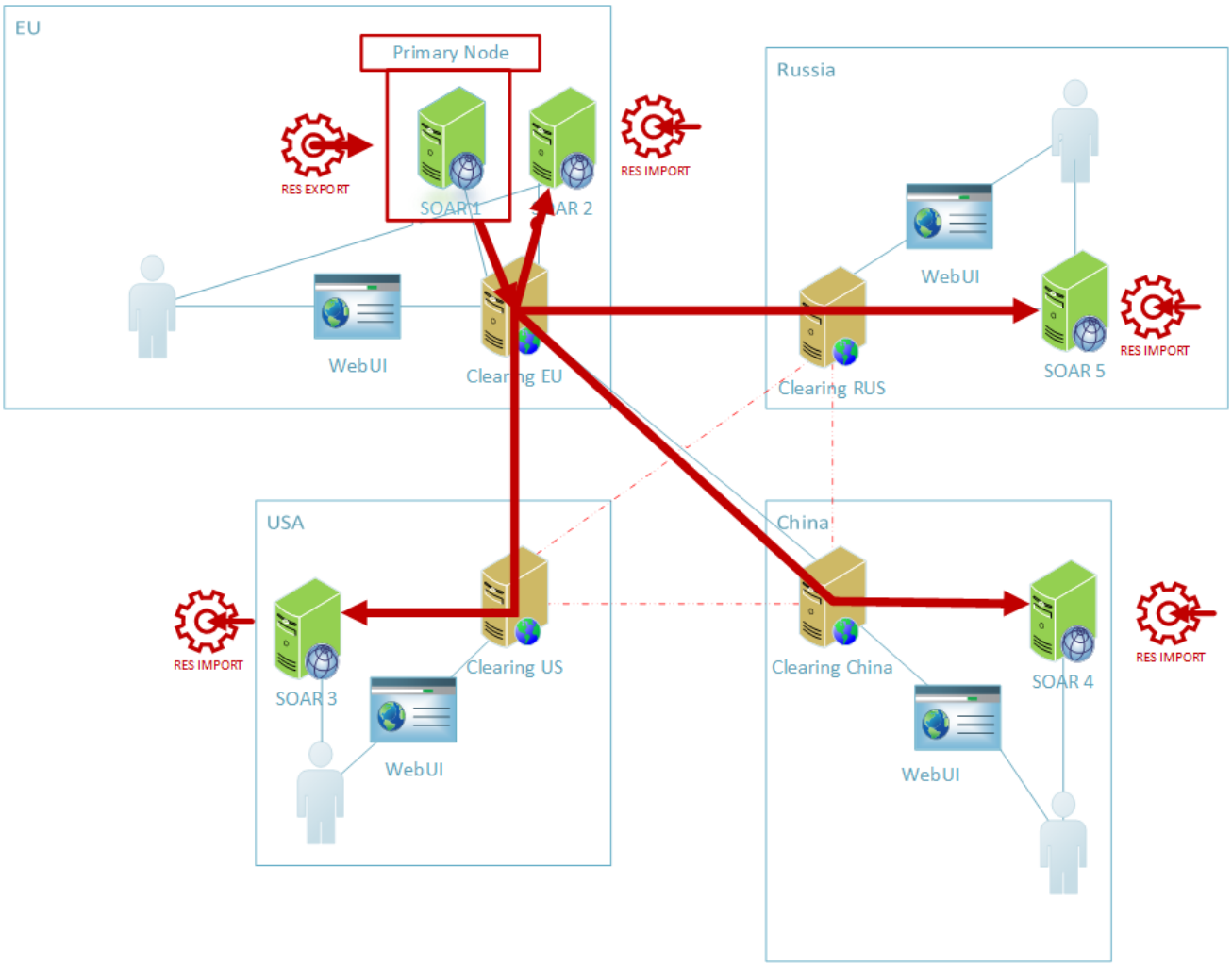

Figure 5. Clearing Configuration distrubtion among clearing network

© Copyright IBM Corp. 2020. All rights reserved

5. Clearing Release & Development Cycle

The current release and development cycle of the clearing system is as follows:

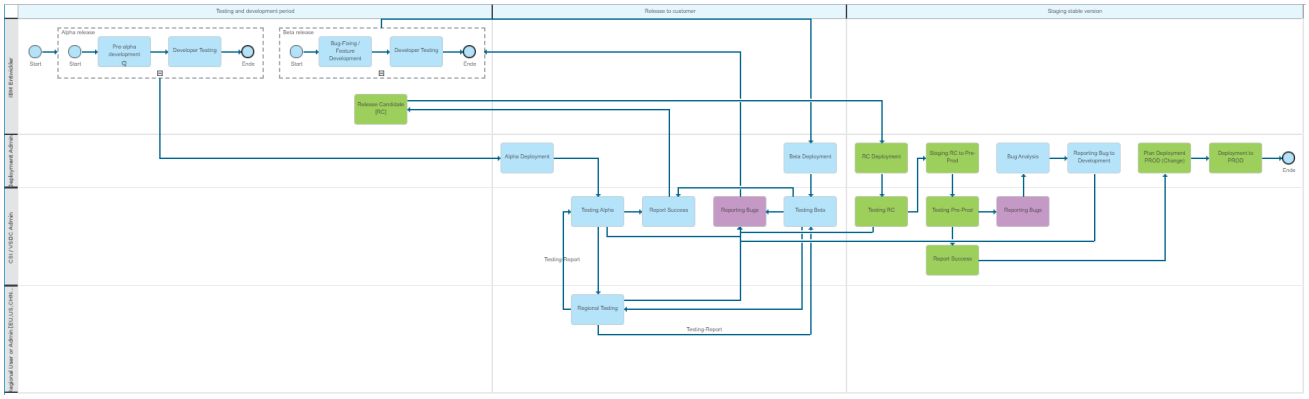

Figure 6. Clearing Release and Development Cycle

A more detailed representation of the release and development cycles are as follows:

© Copyright IBM Corp. 2020. All rights reserved

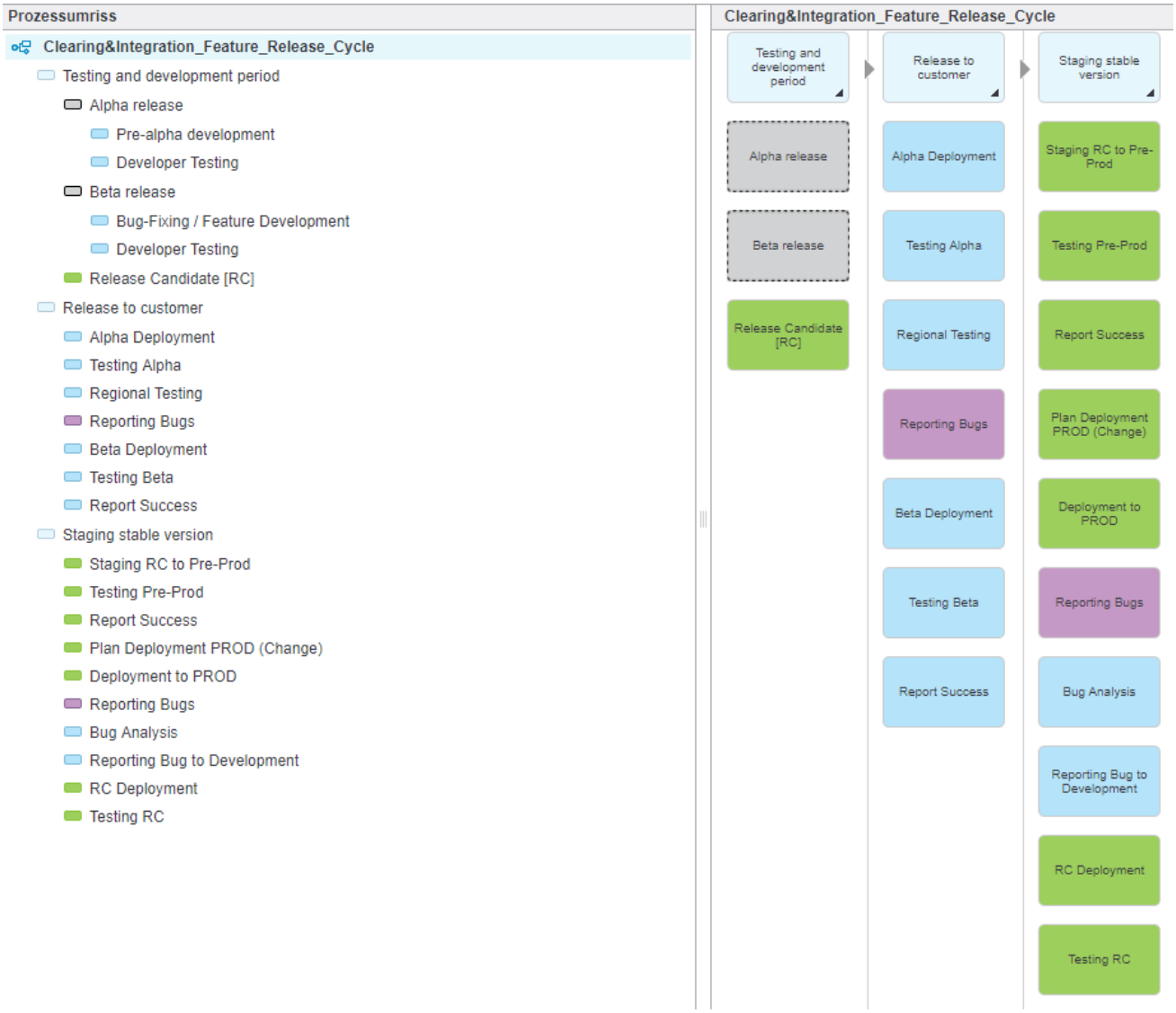

Figure 7. Clearing Release and Development Cycle Steps

© Copyright IBM Corp. 2020. All rights reserved

6. Resources

No resources provided

Change Log

Revision	Date	Responsible	Description
Initial	01-06-2020	IBM Security Knowledge Exchange	Initial package template
Theming & Split	01-21-2020	IBM SECURITY RESILIENT CLEARING SYSTEM [RCS]	Initial System Guide Content v0.1.0
Release	01-04-2021	IBM SECURITY RESILIENT CLEARING SYSTEM [RCS]	Updated System Guide Content for v1.3.3
Release	01-12-2021	IBM SECURITY SOAR CLEARING SYSTEM	Updated System Guide Content for v1.5.0

© Copyright IBM Corp. 2020. All rights reserved

Document Source

Package Author: Sebastian Vetter sebastian.vetter@de.ibm.com
Package Owner: Technical View and Use-Cases skesel@be.ibm.com

If you wish to suggest a change to this document, please do so. You have the following options:

- Email the owning author above or reach out on Slack at IBM Security #ske, or https://ibm.biz/ske-slack
- Raise an issue on the package's github repository at: https://github.ibm.com/skelib/1685-resilient-clearing-system/issues
- Leave feedback comments where you have obtained access to this material. For example, SLA course feedback.

© Copyright IBM Corp. 2020. All rights reserved

© Copyright IBM Corporation 2021

IBM Security
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
February 2018
All Rights Reserved

IBM, the IBM logo, ibm.com, and IBM X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ® or ™, these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: ibm.com/legal/copytrade.shtml

Other product, company or service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.