RSA Archer GRC

RSA Archer Security Operations Management 1.3

Practitioner Guide

5.4 SP1 P1, 5.5, 5.5 SP1, 5.5 SP2, and 5.5 SP3

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:
http://www.emc.com/support/rsa/index.htm.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-party licenses

This product may include software developed by parties other than RSA.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

November 2015

Contents

Revision History

Revision	Date	Description
1	11/12/2015	Updated the following topics: • Supported and Generic SIEM • Integration with RSA Security Analytics

Preface

About This Guide

This guide contains information that helps RSA® Archer® GRC administrators and users understand the business use of the RSA Archer Security Operations Management™ solution.

This guide assumes the reader is knowledgeable about the GRC industry and RSA Archer GRC.

RSA Archer GRC Documentation

You can access the RSA Archer GRC documentation from the RSA Archer Exchange and RSA Archer Community.

Documentation	Location
Platform	On the RSA Archer Community at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**
Solutions, Applications, and Content	On Content tab on the RSA Archer Exchange at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**

RSA continues to assess and improve the documentation. Check the RSA Archer Community and RSA Archer Exchange for the latest documentation.

RSA Archer Security Operations Management *Data Dictionary*

The RSA Archer Security Operations Management *Data Dictionary* contains configuration information for the solution.

You can obtain the *Data Dictionary* for the solution by contacting your RSA Archer GRC Account Representative or calling 1-888-539-EGRC.

Support and Service

Customer Support Information	**www.emc.com/support/rsa/index.htm**
Customer Support E-mail	**archersupport@rsa.com**

Other Resources

RSA Archer Community enables collaboration among GRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide the RSA Archer GRC product roadmap.
https://community.emc.com/community/connect/grc_ecosystem/rsa_archer

RSA Archer Exchange is an online marketplace dedicated to supporting GRC initiatives that delivers on-demand applications with service, content, and integration providers to drive the success of RSA Archer GRC clients.
https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange

RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Secured by RSA Implementation Guides with instructions and other information about interoperation of RSA products with these third-party products.
https://gallery.emc.com/community/marketplace/

RSA SecurCare Online (SCOL) provides unlimited access to a wealth of resources on the Web, 24 hours a day. The secure system provides members access to a support knowledgebase, to download current platform patches and bug fixes, to sign up for notifications, to manage your support cases and more.
https://knowledge.rsasecurity.com/

Chapter 1: Security Operations Management

Security Operations Management

In the last few years, the information security industry has seen an upheaval in the understanding and definition of security incident response. Highly visible, high impact data breaches have clearly defined a turning point in the world of information security. Multiple studies and reports have been issued on the changing threat landscape. Hactivism, APTs, the digital underground, and many other trends have stressed to companies that incident response—while always a core part of information security for years—is not a stagnant science but a continually evolving art. The ability of an organization to identify active attacks to their assets and to respond quickly is essential to deal with the growing number, sophistication, and tenacity of today's security threats.

To protect a company against today's threats, an IT security organization must create a holistic strategy by implementing processes, tools, procedures, and enablers. The program should have a continuous cycle that flows from prevention to detection to response with a feedback loop to ensure that threats are proactively managed as much as possible. No organization can prevent every attack. The likelihood that a company will face a data breach has approached the absolute inevitable. The goal should be to identify and prevent as much as possible, effectively detect and respond to active threats, learn from events and incidents, and improve going forward. A key part of this strategy is security operations management.

The objectives of security operations management are to:

- Effectively and efficiently identify active attacks within an organization
- Escalate the attack to a team that has the skills and resources to analyze, respond to, and contain the threat
- Remediate the issue as fast as possible

- Approach incident response in an operational way – not as a loose, ad-hoc process

Note: Incident response centers are known by several names. The most common ones are Security Operations Center (SOC), Critical Incident Response Center (CIRC), Computer Security Incident Response Team (CSIRT), and Critical Incident Response Team (CIRT). In this document, the term Security Operations Center (SOC) team will refer to the overall team of individuals charged with identifying and resolving security issues.

Challenges in Security Operations Management

Several key challenges make implementing a consolidated, organized security operations management process difficult. The result of these challenges is that, many times, a security attack can escalate into a major data breach before the security team has a chance to contain the issue.

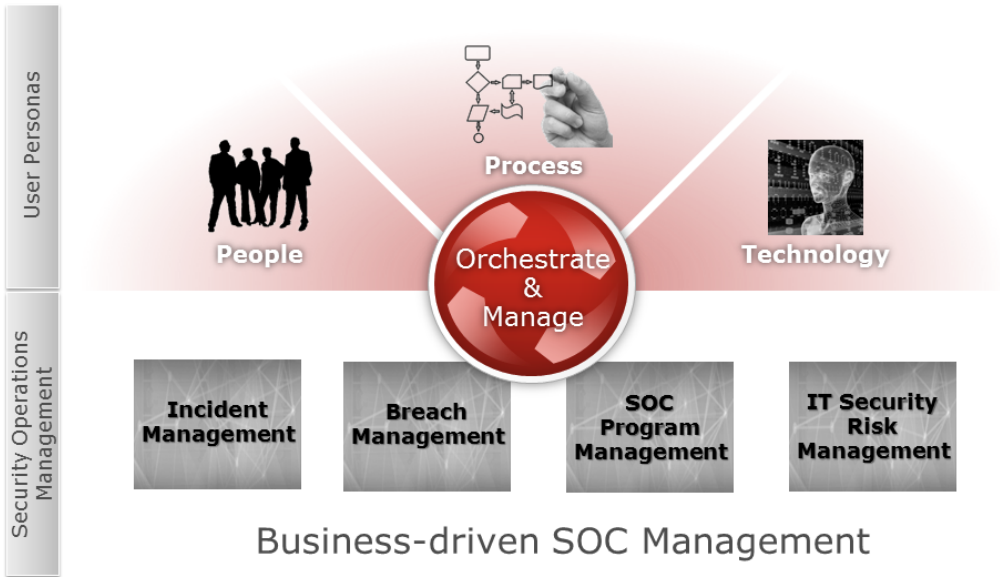
1. The SOC team needs a centralized incident management solution for managing all alerts from security monitoring tools that require review and triage by SOC analysts. A typical SOC has multiple security alerts sources and call centers that enable employee crowdsourcing of security intelligence. Without a centralized tool to aggregate and manage the security alerts and their review process, SOCs cannot scale their incident response process.
2. Context (such as asset, data, identity, and business impact metrics) and cyber threat intel (such as known attack vectors and C2 domains) are crucial for efficient and effective incident triage. Current tools lack integrated context and threat intel, requiring manual data collection for reviewing cases and inefficient prioritization of incidents.
3. SOCs are struggling to gather, organize and share threat intelligence between security teams. If the SOC is manned 24x7, or incident handling is outsourced at times to a third party, the hand-off between shifts and resources is very manual and things slip through the cracks.
4. SOC teams are struggling with disconnected processes and systems to manage the end-to-end security incident lifecycle. Most incident reviews require cross-functional engagement and business process workflows to enable collaboration.
5. Organizations lack a defined approach to develop incident response procedures and industry best practices for incident and breach management. Incident handlers may lack in-depth security incident analysis experience and need incident response guidelines to help them quickly analyze the security incidents and either classify them as false positives or escalate them to more experienced analysts for further investigation. Team members also need to be aware of organizational and regulatory policy requirements when handling a data breach.
6. SOC Managers need a tool to optimize SOC investments. SOC teams are

always under pressure to demonstrate return on investment and make the most of the budget they are allocated. SOC Managers need a tool that helps perform analytics on security alert and incident response data to identify SOC performance metrics and control effectiveness.

RSA Archer Security Operations Management

The RSA Archer Security Operations Management solution provides four primary capabilities:

- Incident Management. The RSA Archer Security Operations Management solution integrates with systems that collect security alerts, such as RSA Security Analytics. RSA Archer Security Operations Management then provides a workflow-driven incident response process. Context and intelligence are critical for effective security incident management process and RSA Archer Security Operations Management makes the context (asset attributes and business context from the Enterprise Management solution) available to an analyst when reviewing/triaging an incident. Incidents can be then escalated to the various analysts during the investigation and response process.
- Breach Management. Data breaches have dramatic impact on organizations: they may result in large fines (regulatory, PCI), loss of competitive advantage, business disruption, brand damage, lack of trust, and more. As a result, organizations care about data breaches and need to quickly manage and remediate a breach once identified. The RSA Archer Security Operations Management solution helps organizations manage breach remediation tasks and procedures by running a cross functional program that provides visibility to senior executives.
- SOC Program Management. RSA Archer Security Operations Management enables SOC Managers to effectively monitor SOC KPIs, measure control efficacy, and manage SOC team personnel.
- IT Security Risk Management. RSA Archer Security Operations Management integrates with other RSA Archer GRC solutions, such as Business Continuity Management and Enterprise Risk Management, to maximize returns on RSA Archer GRC solutions and deliver quick time to value.



RSA Archer Security Operations Management Components

RSA Archer Security Operations Management is composed of the following:

- RSA Archer Security Operations Management solution:
  - Incident Response subsolution
    - Security Incidents application
    - Security Alerts application
    - Security Events application
    - Incident Investigations application
    - Forensic Analysis application
    - Incident Response Procedures application
      (Levels: Incident Response Procedures > Incident Response Tasks)
    - Incident Journal application
  - Data Breach Response subsolution
    - Data Breaches application
    - Breach Tasks application
    - Breach Risk Assessment questionnaire
    - Notifications and Call Trees application
    - Notification History application

    - SOC Program Management subsolution
        - Shift Handover application
        - Breach Response Procedure Library application
        - Incident Response Procedure Library application
          (Levels: Incident Response Procedures > Incident Response Tasks)
        - Security Controls application
        - SOC Policies application
        - Contacts application
        - Teams application
          (Levels: Teams > Team Members)
        - Question Library application
        - Degrees and Certifications application
        - Training application
    - Issue Management subsolution
        - Findings application
        - Remediation Plans application
        - Exception Requests application
        - Policy Change Requests application

- Integrations with a Security Information and Event Management (SIEM) tool:
    - RSA Security Analytics. For more information, see **Integrations with RSA Security Analytics**.
    - Other supported third-party SIEM tools. For more information, see the **RSA Archer Exchange**.
- RSA Unified Collector Framework (UCF):
    - Security Analytics Incident Management (SA IM) Integration Service
    - Enterprise Management Plug-in
    - Syslog Server
    - RSA SecOps Watchdog Service

Important: The RSA Archer Enterprise Management solution is required for RSA Archer Security Operations Management to be fully functional.

Solution Sources, Standards, and Frameworks

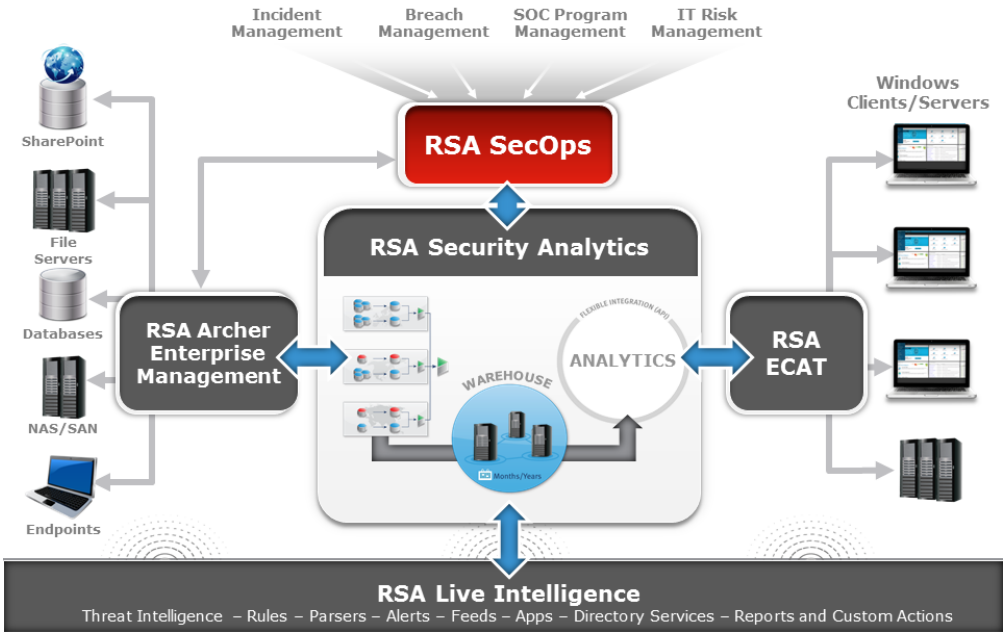
The RSA Archer Security Operations Management solution leverages several different sources and frameworks for solution workflows and capabilities. Because security operations management can be a complex discipline, you may want to refer to these sources for further information about responding to and investigating security incidents.

Standard	Description
NIST SP800-61	This publication provides guidelines and best practices for incident management. A key part of this document is the phases of incident management, especially post-incident analysis. The RSA Archer Security Operations Management solution uses several of these concepts within the solution design. **http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf**
US-CERT	In the RSA Archer Security Operations Management solution, you can extend the Threat Category enumeration to include the seven incident categories (CAT0 – CAT6) that US-CERT uses. You can also create response procedures for each of these categories in the Incident Response Procedure Library application, and then automatically generate incident response tasks for incident handlers. **https://www.us-cert.gov/government-users/reporting-requirements**
SANS 20 Critical Security Controls	The RSA Archer Security Operations Management solution provides the capability to track all of the security controls deployed in your organization, such as the SANS top 20, and monitor their effectiveness at detecting, preventing, or investigating security incidents. **http://www.sans.org/critical-security-controls/**
VERIS Framework	The RSA Archer Security Operations Management solution uses the VERIS framework for taxonomy and enumerations, enabling standard incident reporting and consistent information sharing with others. **http://www.veriscommunity.net/doku.php**

Architecture Overview

RSA SOC Reference Architecture

The RSA Archer Security Operations Management solution is part of a broader architecture to respond to current security attacks. A security operations management program depends on multiple technologies to identify and respond to an active attack. As shown in the following diagram, RSA Archer Security Operations Management (denoted as RSA SecOps) provides the overlay of program enablement to the incident response process.



Additional components of this broader architecture include the following:

- RSA Archer Enterprise Management is a required component of the overall solution and provides the asset and business context information to support all solution processes. The RSA Archer Enterprise Management solution gives you an aggregate view of critical infrastructure technologies and their relationships to your organizational hierarchy and business offerings and enables you to relate assets to the business processes that they support. This information provides immediate business context to incident handlers, giving them insight into the possible business impact of a security event and allowing them to appropriately prioritize incidents.
- RSA Security Analytics provides the deep network packet and event forensics necessary to identify security attacks. The Incident Management module consumes alerts from various sources, such as Malware Analytics, RSA ECAT, and the Security Analytics Reporting Engine and Event Steam Analysis appliance, and aggregates them into incidents. For companies that do not utilize

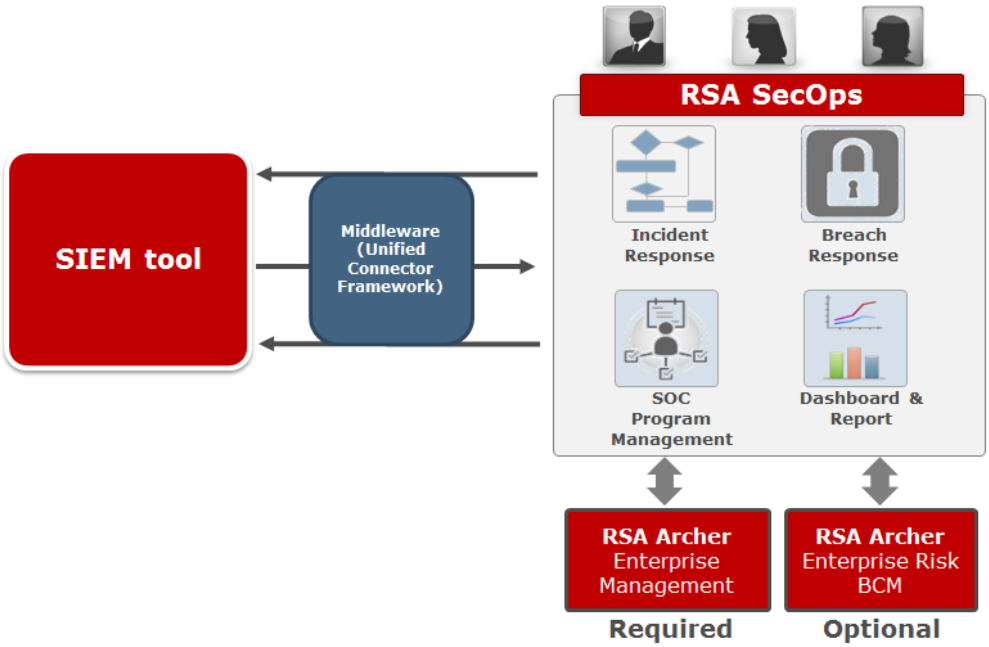
RSA Security Analytics, this function may be performed by other technologies such as SIEM and log management tools.

Regardless of the technology, security operations management requires insight into the actual system and security events occurring on the network and hosts. The business criticality of a given asset (as defined by RSA Archer Enterprise Management) should also drive forensic and monitoring priorities in RSA Security Analytics. The integration between RSA Archer GRC and RSA Security Analytics streamlines this process.

- RSA ECAT represents the host level forensics capabilities to deal with today's malware attacks. Many security threats today utilize malware as launching points to larger security breaches. Security operations need this type of capability to analyze and identify malicious software at the host level.
- RSA Live Intelligence. With today's constant change in security threats, security operations need a constant flow of security intelligence to adapt and focus on emerging threats. RSA Live represents the need for an up-to-date feed of security information to adjust security operation priorities based on the latest security intel such as indicators of compromise (IOCs), threat attach vectors, known bad hosts, or malicious threat actors.

RSA Archer Security Operation Management Architecture

The RSA Archer Security Operations Management solution is architected to streamline the escalation of security alerts from monitoring systems to an incident response process, enabling security incidents to be analyzed, investigated and resolved. The following diagram shows the high-level architecture of the RSA Archer Security Operations Management solution.



The solution is comprised of three main elements:

- The RSA Archer Security Operations Management solution provides the process workflow, reporting, and program management capabilities necessary to manage a security operations center.
- A SIEM tool serves as the source of security alerts.

  Note: For more information about using the solution with Security Analytics, see **Integrating with RSA Security Analytics Incident Management**.

- RSA Archer Enterprise Management is a required component of the overall solution and provides the asset and business context information to support the entire process.

Additional RSA Archer GRC solutions (such as RSA Archer Business Continuity Management) can also be integrated to extend the organization's capabilities and blend security operations management into the bigger IT and business risk management program. This is also out of the scope of this document.

RSA Archer Enterprise Management Key Considerations

This document does not go into detail of Enterprise Management, however, the following are some key points to consider:

- For organizations that do not have a significant IT asset catalog or an existing RSA Archer Enterprise Management implementation, a discussion of how this catalog will be built should be part of the overall security operations strategy. This may be as simple as starting with cataloging known business critical devices such as key production, application, database and file servers or networking devices and infrastructure. From this starting point, more assets can be added. If the organization does have an IT asset catalog but limited insight into the business context (such as usage, related business process, and the business ownership/contact), the process may focus on building tactical relationships between business processes, IT applications and devices and executing business impact analysis. These functions are included in the RSA Archer Enterprise Management solution.
- The more business context (through relationships to business assets) the security operations team has on IT assets, the better the prioritization process for security events will be. This will require an analysis of the existing and planned attributes of IT assets within the RSA Archer Enterprise Management solution to ensure a security operations has contextual information for security response processes.
- Additional attributes on IT assets (such as compliance states, risk assessments, vulnerability scan results or other information that gives the security responders insight into the risk profile of an asset) can also play a big role in proper containment of a security incident. Therefore, as part of the overall implementation strategy, the continuous growth of the asset understanding should be included.

Integrating with RSA Security Analytics Incident Management

RSA Archer Security Operations Management integrates with the RSA Security Analytics Incident Management module, which consumes alerts from various sources (such as Malware Analytics, RSA ECAT, and the Security Analytics Reporting Engine and Event Steam Analysis appliance) and aggregates them into incidents.

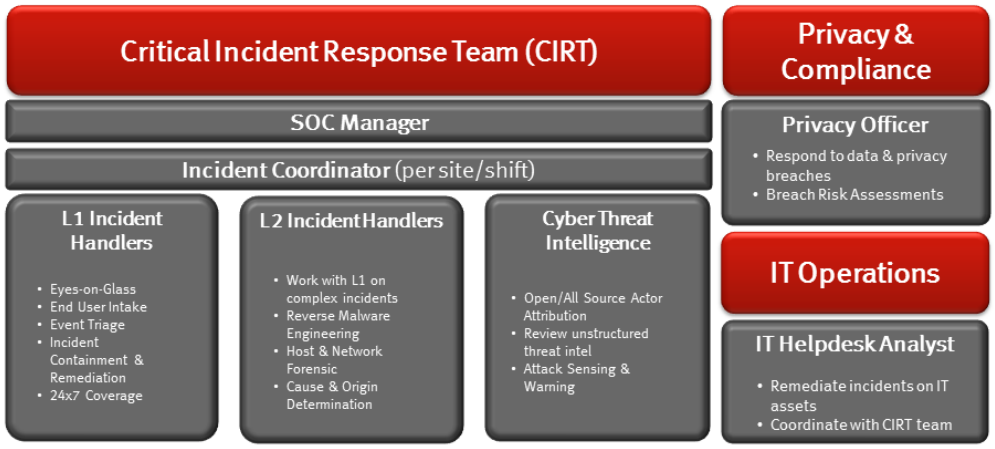
The following table describes the different integration options and what data is transported for each option.

Integration option	Data transported into RSA Archer GRC
Manage incidents in the RSA Archer Security Operations Management solution	Incidents. **Note:** Once incidents are transported into RSA Archer Security Operations Management, incidents and remediation tasks are no longer visible in RSA Security Analytics.
Manage incidents in the RSA Security Analytics Incident Management module	Data breaches Remediation tasks (as Findings), which can be assigned to either the GRC or Operations queues for remediation. **Note:** When updates are made in RSA Archer Security Operations Management, the remediation status is automatically synchronized across the two systems. Incidents (records are read only)

For more information about setting up the integration, see the *RSA Archer Security Operations Management 1.3 Installation and Configuration Guide*.

Key Personas in Security Operations Management

A SOC team, in most cases, has three to four sub-teams as summarized in the following diagram. In a typical setup, over 50% of analysts are Level 1 (L1) Incident Handlers, followed by Level 2 (L2) Incident Handlers and Cyber Threat Intelligence Analysts.



The management of a SOC team is a complex process. These personas may be shared between different individuals or multiple personas may be assigned to one individual. These personas are reflected in various workflows and processes within the RSA Archer Security Operations Management solution and the solution helps each role with their key challenges.

SOC Manager

Job Description

The SOC Manager runs the SOC and owns the SOC budget which eventually rolls up to CISO/CSO. The SOC Manager is responsible for the following (but not limited to) tasks:

- Preventing successful cyber-attacks and leakage of sensitive information from the organization as much as possible by deploying various types of security controls.
- Effectively responding to security incidents to minimize impacts to the business.
- Providing visibility to CISO/CSO & Business Managers on ongoing incidents and possible cyber threats that affect the organization through a combination of periodic reports and real time dashboards.
- Tracking SOC KPI/KRIs and managing the SOC resources and budget in the most effective way to meet objectives above.

Key Challenges

Most SOC teams rely on a collection of manual processes, home grown tools and scripts and an IT Helpdesk system for managing security incidents and cyber threat intelligence. The SOC Manager faces the following challenges:

- Needs business, asset, identity, and threat intelligence context for an effective response to security incidents, but this information is difficult to organize.

- Incident management processes are too manual, which leads to a lot of inefficiencies including the lack of centralized tool for incident collection and aggregation, inconsistent priorities across alerts, manual response procedures, and remediation tracking.
- Wants the team to stay ahead of the adversaries by collecting cyber threat intelligence data from different sources, reviewing them and taking a proactive remediation action based on its impact to the organization.
- Wants to monitor SOC KPIs and KRIs in a dashboard by summary metrics in a score card. However, this is challenging because the current tools and processes lack consistent attributes and enumerations.

Primary Tasks

- **Managing SOC Readiness**
- **Responding to Incidents**
- **Responding to Data Breaches**

Incident Coordinator

Job Description

The Incident Coordinator manages the Level 1 and Level 2 teams at an operational site. In a large organization, there are typically one or more Incident Coordinators (sometimes considered Shift Managers) to help drive 24x7 coverage for the SOC. The Incident Coordinator is responsible for ensuring that incident response SLAs (service-level agreements) are met and high priority incidents are contained and remediated immediately. The Incident Coordinator achieves this by completing the following tasks:

- Defining and managing the incident response process.
- Ensuring response procedures are in place.
- Monitoring incident queues to ensure the SOC meets its SLAs such as MTTR (mean time to resolution) for security incidents.
- Coordinating shift hand-offs by creating a daily shift handover report which is used by his counterparts running shifts at different sites.

Key Challenges

- The incident response process is many times managed manually through separate documents or through some ticket system which is not security oriented.
- Required to manage and respond to security alerts from multiple tools:
  - Collection of security alerts from these tools and aggregation (grouping) of similar alerts into a single incident is not automated.
  - Varying alert priorities from different sources are not normalized to incident

priorities based on business, asset, and identity context as well as cyber threat intelligence data.

- While triaging security incidents, incident handlers may spend 40 to 60% of their time gathering contextual and threat intelligence data for internal and external systems and identities involved in the incident. This consumes a significant amount of the handlers' time and needs to be minimized by connecting incident management tools with enterprise asset and user repositories.
- Needs defined incident response procedures for various categories of security incidents to enforce consistent triage and review processes for responding to incidents.
- Spends a lot of time summarizing the work done on high priority incidents during the shift so that the next incident coordinator can pick them up from where the previous incident handlers leyft them.
- Needs a real-time dashboard to monitor incident metrics such as status and SLAs that are currently in L1 and L2 incident queues as well as pending remediation from IT Operations.

Primary Tasks

- **Managing SOC Readiness**
- **Managing Shift Handovers**
- **Assign an Incident to a Handler**
- **Ensuring Timely Response to Incidents**
- **Responding to Incidents**

L1 Incident Handler

Job Description

The L1 Incident Handler is a member of the Level 1 Incident Handler team and reports to the Incident Coordinator. The L1 Incident Handler is typically an intermediate level security expert responsible for the following tasks:

- Reviewing incidents in their incident queue first thing in the morning and working through them in the prioritized order.
- If done with current issues and the Incident Coordinator has not yet added anything to their queue, checking on the overall L1 incident queue for the shift, adding appropriate incidents to their queue and working through them.
- During an incident review and triage process, spending the majority of his or her review time gathering context and intel.

- Performing quick analysis of incidents to decide one of the following actions:
  - Is the incident a false positive? Remove noise and document why the incident is a false positive.
  - Is this something that requires further investigation by an L2 Incident Handler? If so, escalate.
  - Is this a standard security incident with well-defined incident response procedures? If so, follow the steps in the response procedure and recommend remediation to IT Operations by opening a ticket in an IT Helpdesk system.
- Tracking open IT Helpdesk tickets for remediation before closing the incident.

Key Challenges

- Could benefit from economy of scale by grouping multiple similar alerts together into an incident, instead of working on an individual security alert as an incident.
- Spends 40 to 60% of his or her time gathering context and threat intelligence for systems, applications, and users involved in an incident.
- Could significantly benefit from incident response checklists for each category of incident, so that all required procedures are executed for a given incident before escalating or closing them.
- It is time consuming to manually create IT Helpdesk tickets and track the status for all open security incidents.
- During the incident review process, the L1 Handler needs to take notes on actions performed during incident response for reporting and historical audit reasons. However, it is tedious to take notes in a paper notebook and then type them into the incident management tool.
- Needs an L1 Incident Handler dashboard to track assigned queue, status of all the incidents and their SLAs, as well as any open tasks.

Primary Tasks

- **Responding to Incidents**
- **Remediating Issues**

L2 Incident Handler

Job Description

The L2 Incident Handler is a member of the Level 2 Incident Handler team, reports to the Incident Coordinator, and is typically a more senior security expert with advanced skills in network and host forensics and malware reverse engineering. A typical day at work includes the following tasks:

- Reviewing incidents in their incident queue first thing in the morning and working through them in the prioritized order.

- If done with current issues and the Incident Coordinator has not yet added anything to the queue, checking on the overall L2 incident queue for the shift, adding incidents appropriate incidents to the queue, and working through them.
- During an investigation, using multiple network forensic tools such as RSA Security Analytics and host forensic tools such as RSA ECAT to perform in-depth analysis. After completing the analysis, records the observations of the forensic investigation into the incident management tool and justifies whether the system is compromised or not. If needed, can take steps to contain the intrusion/infection immediately to minimize the impact of the attack.
- Creating tickets in an IT Helpdesk system for remediating a given incident and tracking their completion before closing the incident.

Key Challenges

Many of the L2 incident handler's issues are similar to those of the L1, although the following issues are more important:

- Collect and visualize context (asset, data, user and file) and cyber threat intelligence within the incident review tool so that he can significantly enhance his productivity.
- During forensic analysis, needs to work with one or more security tools and has to log into those tools and manually create filters to locate the alerts under investigation.
- While performing forensic analysis, needs to take multiple notes and screenshots that must be captured and organized for documentation of the investigation.

Primary Tasks

- **L2 Incident Handler**
- **Responding to Incidents**
- **Performing Forensic Analysis**
- **Recommending Issues for Remediation**
- **Remediating Issues**

CSO/CISO

Job Description

(For purposes of this document, only the responsibilities related to Security Operations are included.) The CSO/CISO is accountable for providing effective IT security to the enterprise and responsible for the security tools and staff. The CSO/CISO needs to receive consistent security incident summaries but is also part of the escalation of any high impact security incident. If an incident results in a data breach or loss, the CSO/CISO may take the lead role for driving the breach management program.

Key Challenges

- Needs a consistent, real-time summary of security incidents and cyber threats to the organization. Would prefer to have a dashboard that summarizes the metrics instead of a weekly report from the SOC Manager and regular meetings to discuss the details.
- Wants to be able to track SOC investments in security tools closely and measure the efficacy of these controls, instead of asking the board or CFO for more money.

Primary Tasks

- **Managing SOC Readiness**
- **Monitoring Incident Metrics and Status**
- **Responding to Data Breaches**

IT Helpdesk Analyst

Job Description

The IT Helpdesk Analyst is responsible for working through the queue of tickets created by L1/L2 Incident Handlers for remediating security incidents. The analyst assigns remediation tasks to system administrators in IT Operations.

Primary Tasks

- **Remediating Issues**

Cyber Threat Intel Analyst

Job Description

The Cyber Threat Intel Analyst is the lead for the Cyber Threat Intelligence team. Typically this role is a security expert with advanced skills in cyber threat intelligence gathering and tracking new attack patterns from adversaries by using feeds from partnering SOCs, industry (such as FS-ISAC, REN-ISAC, and ENISA) and government (such as DOD DC3, DSIE, and DIB) government sources. A typical day at work includes the following tasks:

- Reviewing unstructured and relevant cyber threat intelligence feeds from one or more sources.
- Identifying feeds that are relevant to the organization, creating new IOCs (indictors of compromise) and attack patterns and feeding them to SIEM/SEM tools such as RSA Security Analytics (via Live) to:
  - Check if a similar pattern has occurred within his organization, but went unnoticed

  - Automatically detect events that match the IOC going forward by updating the correlation rules.
- Sharing new threat intel with the industry and partners, based on the organization's policies and NDAs.

Key Challenges

- Manually reviews the threat intelligence data from various portals (such as DoD and DHS portals) blogs, emails, and information sharing groups. This is just too much information to review in a timely fashion. There is concern that important intelligence data is missing because there is time to review only 10-20% of the data available via these sources.
- Knows that threat intelligence sharing is a two-way road to effectively combat advanced threats. Sharing new threat intelligence data with internal and outside parties is minimal and done manually via emails or over phone, which is very time consuming.
- The current process for reviewing and managing threat intel data is ad hoc.

Primary Tasks

- **Investigating New Threat Intel**

Note: There is no out of the box access role built for the Cyber Threat Intel Analyst, however it is a role that you should consider as you develop your full SOC management process.

Business Unit Manager

Job Description

The Business Unit (BU) Manager persona is a generic term for the individuals outside of IT that are responsible for a line of business or department and may be involved in identifying the business impact (if any) from security incidents and recovering from them. A BU Manager may be involved in assisting with issue remediation, depending on the nature of the incident.

Primary Tasks

Monitoring and ensuring remediation of issues:

- **Reviewing a Finding**
- **Reviewing an Exception Request**
- **Reviewing a Remediation Plan**

Corporate Compliance/Privacy Officer

Job Description

Depending on the size or structure of an organization, the title of this persona may differ, but the role is responsible for ensuring that the policies and control procedures required to meet regulatory requirements and follow industry best practices have been implemented in the organization. For RSA Archer Security Operations Management, this role is mostly concerned with the root cause of security incidents and how they map to control procedures and regulatory frameworks. This persona will most likely be engaged if there is a security incident that results in data compromise or disclosure of regulatory related or personal information and may take the lead role for driving the breach management program.

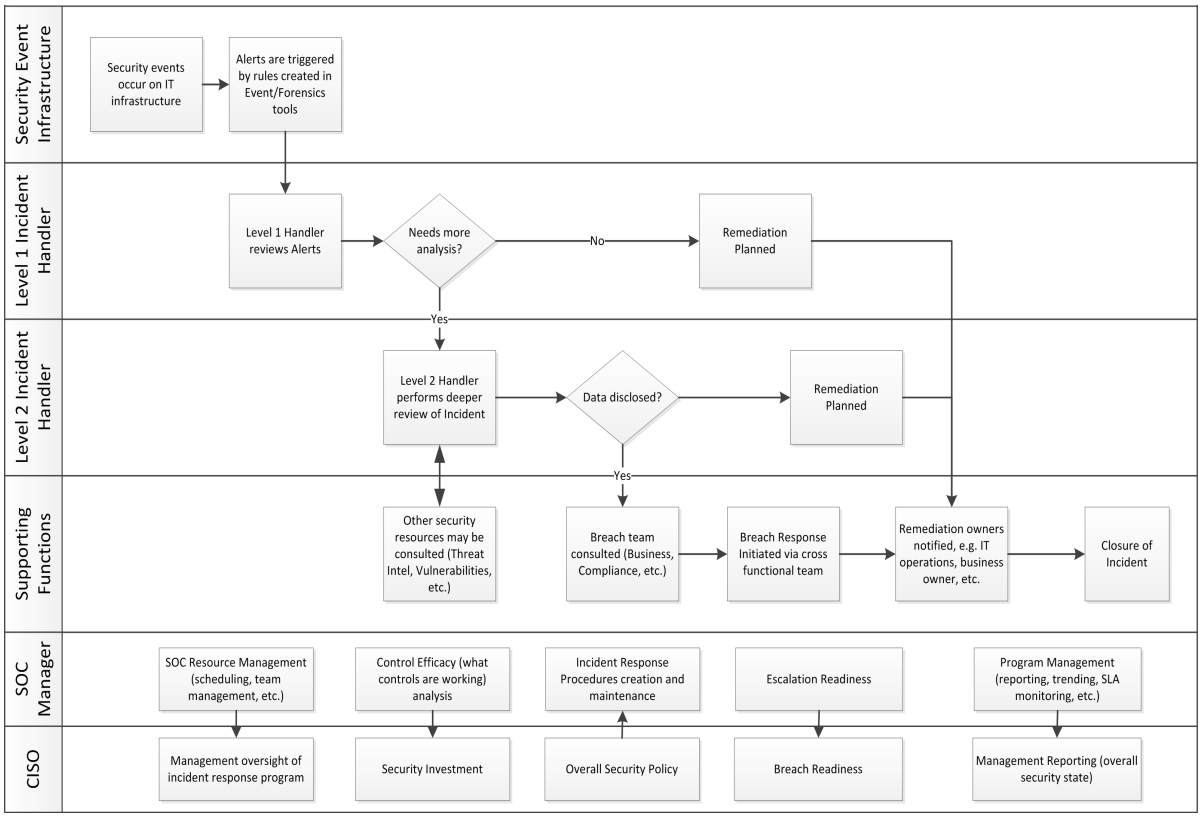
Primary Tasks

- **Responding to Data Breaches**

RSA Archer Security Operations Management Workflow Overview

How a security team investigates and resolves possible security attacks depends greatly on the nature of the attack, the data and systems involved, the skills and resources of the organization, and many other factors. The following diagram shows the high-level workflow included in the RSA Archer Security Operations Management solution. The purpose of this diagram is to provide an overview of the SOC Management processes, how the work flows from one role to another, and how the program is managed. More information on the individual stages of an incident can be found in the respective chapters of this document.

Note: If you have integrated with RSA Security Analytics, you can also manage the first three rows of this workflow in the Incident Management module. For more information about managing incidents in the Incident Management module, see the Security Analytics documentation.



The major personas are included from the initial identification of a possible security event through the various escalations until closure. This workflow highlights the importance of defining the hand-offs and communication methods between personas. The RSA Archer Security Operations Management solution provides the mechanism to manage these various workflows while engaging the different personas.

The following points about the high-level workflow are important to consider:

- The escalation of events and alerts from the security event infrastructure may be automated or manual. This will depend on the nature of the infrastructure. The critical point is to define how an event is identified and how the SOC team is notified of a possible security incident. The quicker this process happens, the more likely the organization will be able to respond and contain security incidents and prevent serious data disclosures, disruptions or negative impacts.
- The Level 1 and Level 2 analyst roles acknowledge that most organizations have a mix of security resources with differing skills and experiences. In companies with limited security resources, these roles may actually be assigned to one singular team or resource. However, as a SOC matures, there will be the need to expand resources into varying levels – leveraging the skills of experienced security practitioners as Level 2 analysts while building the experience of Level 1 analysts.

- The supporting functions of the SOC team are varied. Security, IT, and Business resources outside the SOC play an important role in understanding and properly remediating a security incident. This communication is important to build a support function that can input into the process when needed.
- The CISO and SOC manager have multiple responsibilities, but the following are the main responsibilities:
  - The security response program management need is growing in importance for organizations. Incident Response can no longer be an ad-hoc process and leveraging the skills and resources of the SOC is extremely critical. The SOC Manager provides the frontline management while the CISO provides the executive oversight for the entire program.
  - Control Efficacy is also a growing need. Security organizations must invest in high impact technologies and processes, and the security incident process can give strong visibility into how well the controls are operating. The SOC Manager can provide the CISO with frontline information on which controls are working and which technologies are providing the most impact. The CISO can then leverage this insight to guide security investments.
  - Operational Procedures within the SOC are necessary to streamline response and triage of incidents and leverage experience and skills across the security team. These procedures should also be connected to the overall security policy to ensure proper practices are implemented.
  - The SOC Manager must ensure the Escalation Readiness is in place to move an incident “up the chain” when warranted, especially in terms of data breaches and disclosures. The CISO must also ensure that organization is properly prepared for a data disclosure event with the right connections to the business and compliance teams. Compliance and reputational risks can be substantial when related to a data breach and the organization needs to have proper processes in place to be prepared for a data breach.
  - Reporting upwards from the SOC to the CISO to the business and executive management will be very important. The SOC Manager should provide the right level of empirical data (metrics) and anecdotal information (such as lessons learned and threat trends) so the CISO can put this information in the context of the overall health of the security of the company.

Solution Dashboards

The RSA Archer Security Operations Management solution has six dashboards that provide detailed summary information for each of the primary users within the solution :

- SOC Manager
- Incident Coordinator

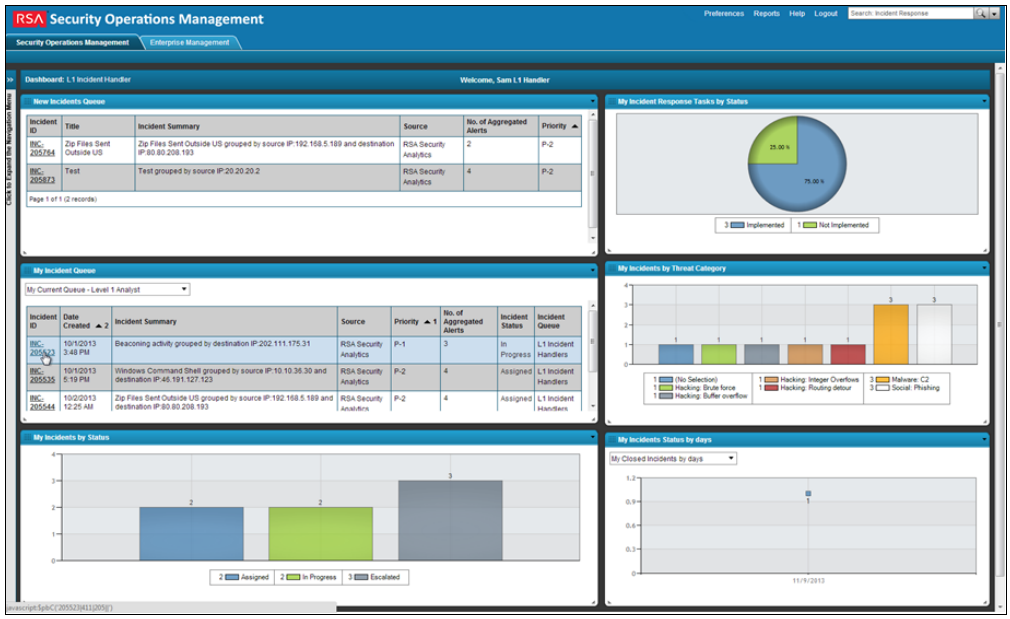
- L1 Incident Handler
- L2 Incident Handler
- Compliance/Privacy Officer (Breach Response Lead)
- IT Helpdesk Analyst

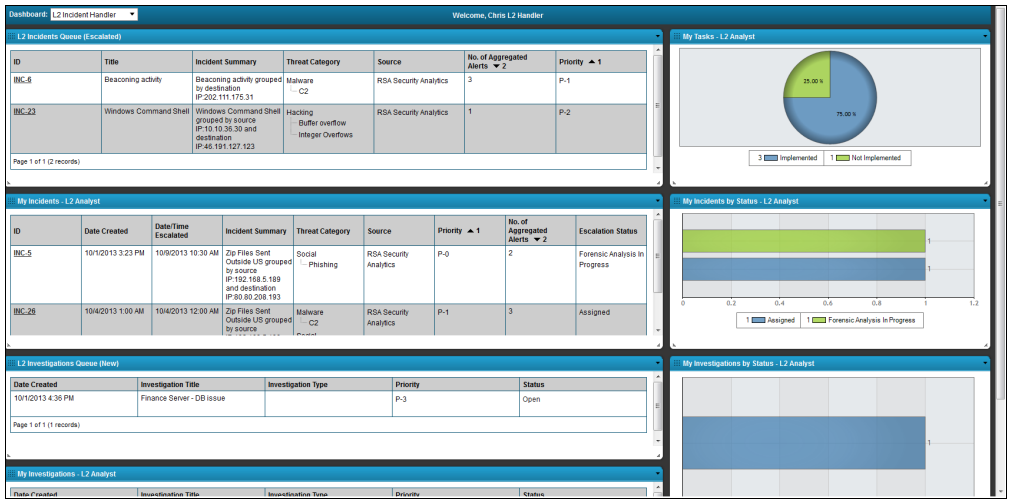
Each dashboard serves as the primary point of entry to the solution for that user, and the majority of all tasks that each user needs to perform begin from their dashboard. When each user logs on, they see their particular dashboard in the center of the screen, the solution applications on the left, and the Security Operations Management and Enterprise Management workspace tabs at the top.

L1/L2 Incident Handler Dashboards

The L1 Incident and L2 Incident Handler dashboards display information about security incidents and (for L2 Handlers) incident investigations. The charts and tables in each dashboard allow that user to see the items they are currently assigned, items in the queue that they can begin working on, open tasks, and other metrics.

Only users assigned to the L1 Incident Handler role can view the L1 Incident Handler dashboard and only users assigned to the L2 Incident Handler role can view the L2 Incident Handler dashboard.



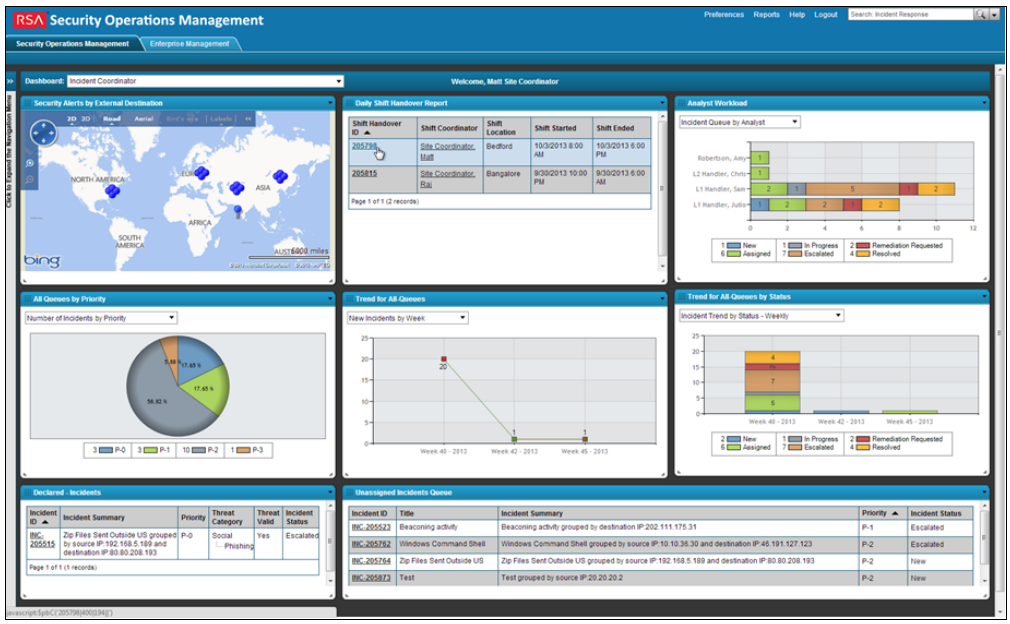


Note: All of the screenshots in this guide show a UI configured with the SecOps theme. For instructions on creating this theme and using it in your own environment, see **Configure the SecOps Theme**.

Incident Coordinator Dashboard

The Incident Coordinator dashboard provides summary information about all open incidents and investigations, shows the current workload for each Incident Handler, shows all unassigned incidents that the Incident Coordinator needs to assign, and displays recent shift handover reports for the incident coordinator to review at the beginning of a shift.

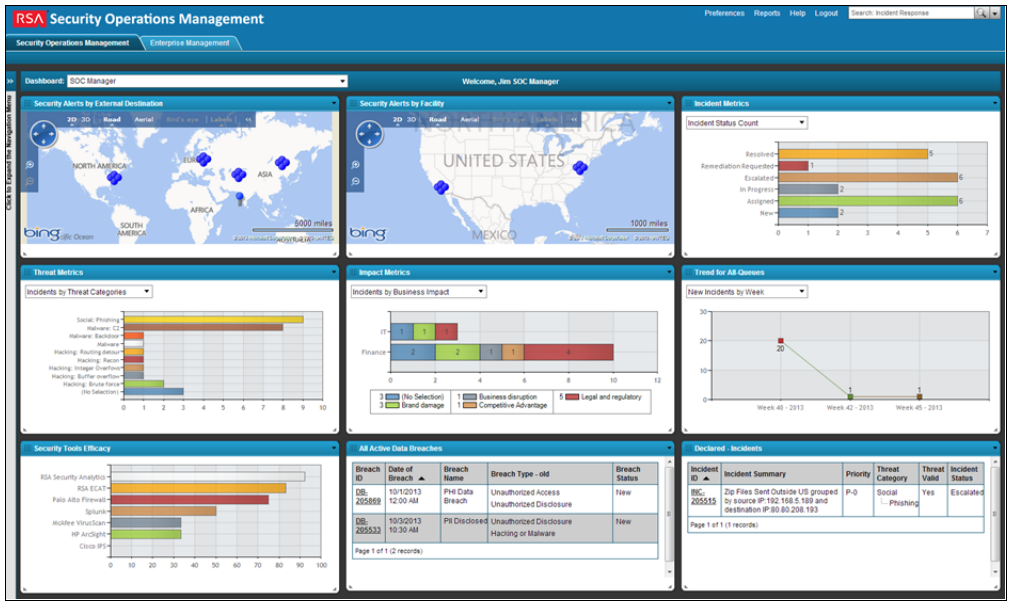
Only users assigned to the Incident Coordinator role can view the Incident Coordinator dashboard.



SOC Manager Dashboard

The SOC Manager dashboard provides summary information about all active incidents and data breaches, displays maps of recent security alerts by external destination and facility, shows metrics about the threat categories and business impacts of incidents, and displays the most effective security controls in the SOC.

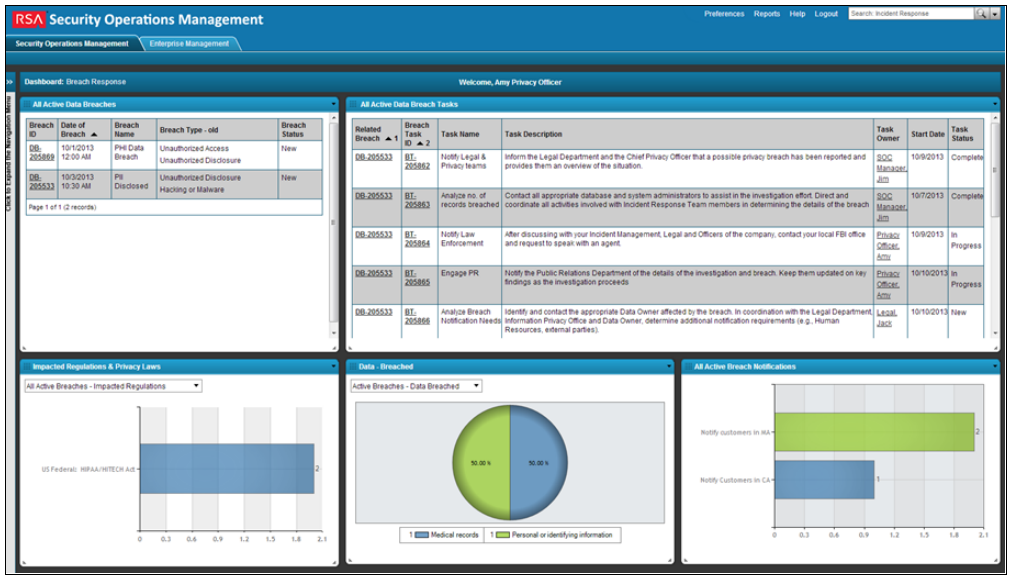
Only users assigned to the SOC Manager role can view the SOC Manager dashboard.



Breach Response Dashboard

The Breach Response dashboard provides a high-level view of your entire breach response program. You can view all active data breaches, any open tasks that need to be completed as part of a breach response, which regulations have been most impacted by data breaches, and what type of data has been disclosed.

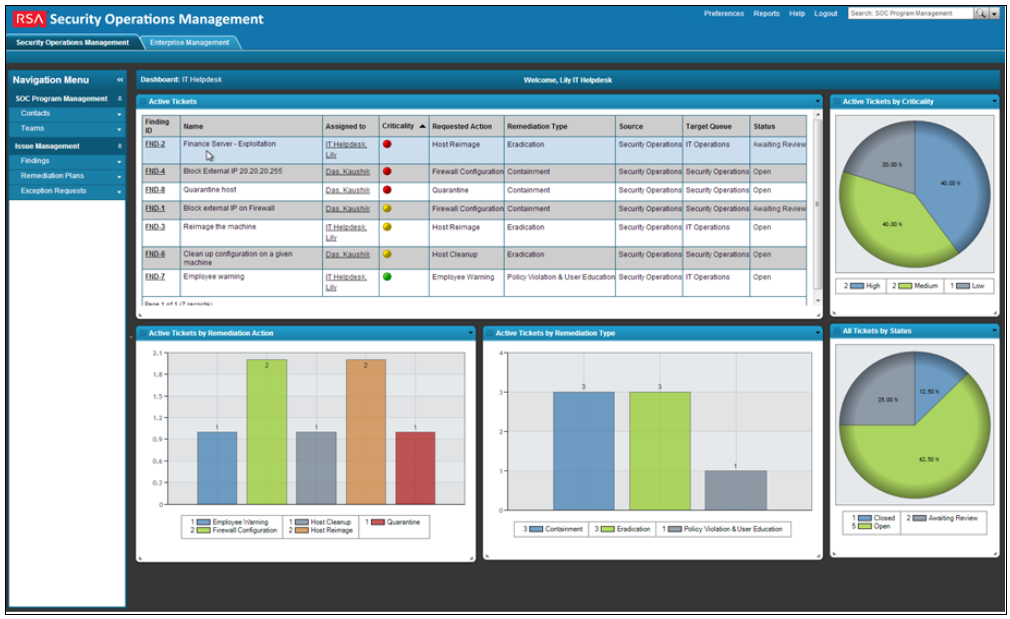
Only users assigned to the Compliance/Privacy Officer, SOC Manager, or CISO/CSO roles can view the Breach Response Dashboard.



IT Helpdesk Dashboard

The IT Helpdesk dashboard provides a summary view of all tickets (findings) that need to be remediated for either an incident or a breach. You can view all open tickets, all tickets that match a particular remediation type or action, and the most critical open tickets.

Only users assigned to the IT Helpdesk role can view the IT Helpdesk dashboard.



Solution Implementation

There are many items to consider when implementing the RSA Archer Security Operations Management solution. The chapters of this Practitioner Guide outline the details of the different phases, but the following sections highlight some important initial considerations.

Managing SOC Readiness

This phase is the responsibility of the SOC Manager, who outlines the different steps necessary to lay out the approach for the overall SOC team. Most often, existing SOC teams will have assigned roles that may or may not align with the personas in the solution. When planning for the implementation, it is important to map the roles/personas described in this document to your own team members. If there are gaps, or roles that are not accounted for, then the team should determine how current personnel are mapped to the roles in the solution. The solution also includes the ability to catalog the skills of the team so the SOC Manager can understand skill gaps and plan accordingly.

The SOC Manager should document the different security controls within the infrastructure. Security controls could be both technology (such as tools, platforms, and systems) as well as manual controls (such as a manual log review process). The inventory of security controls enables the SOC manager to track the effectiveness of the controls as they pertain to security incidents. The SOC Manager should itemize security controls in the early phases – to set a baseline set of controls – but also maintain this catalog over time as new technologies or processes are implemented based on lessons learned from monitoring control efficacy.

Policies and procedures for incident management will solidify the overall SOC team strategy. Policies and procedures are important pieces of maintaining a methodical approach to triaging and responding to security events. The solution allows the SOC team to document specific procedures for different types of security incidents. These procedures will enable the team to maintain a common set of steps based on the profile of incidents and assist not only in the immediate response but also build a common knowledgebase for information sharing between security team members. This should be an active part of the overall SOC program management.

Call trees are necessary to itemize personnel relevant to different types of security incidents. Building a call tree upfront (or as different types of incidents and events are investigated and resolved) streamlines the communications necessary to handle security events.

Responding to Incidents

The next phase of the implementation will focus on building the workflow and mechanics of identifying a possible security event and escalating through the different layers of the SOC team for investigation and resolution.

Some actions to consider for this phase:

- If the RSA Archer Security Operations Management solution is integrated with RSA Security Analytics, this phase will include ensuring the integrations are working properly. Planning should be instituted to run through various testing cycles to ensure the data is properly flowing and the team understands how security alerts are correlated into security incidents.
- The team should be trained extensively on the mechanics of the process including how to create an incident, assign an incident and move an incident through the workflow. This will require some training sessions that should be part of the initial implementation. Ongoing training (for new team members) should be considered as standard processes as the SOC team progresses.

Responding to Data Breaches

Data breaches are security incidents that result in some type of data disclosure or compromise. Most data breaches will have some regulatory impact. For example, a compromise of personally identifiable information (PII) such as credit card data may require certain regulatory reporting processes to be initiated. Data breaches do not have to be regulatory related. A data breach could be designated based on internal types of information – for example, very sensitive intellectual property being accessed by an unauthorized person.

Some actions to consider for this phase:

- The workflow for data breaches will engage other parts of the organization – for example, designees from Public Relations, Compliance, Legal, or Privacy functions. These individuals may not be daily users of RSA Archer GRC and most likely will not have deep security backgrounds. Therefore, the individuals that are designated to be participants in this workflow should be briefed and a periodic review of the process should be instituted.
- Since data breach response may require input and actions from parties outside the SOC team, a periodic review of contact information and roles should be instituted.
- Data breaches can happen very quickly and are usually unique to the circumstances. Once the data breach extended team is designated and organized, it is recommended to have periodic testing or reviews of the process. Table top exercises such as what if scenarios are a good way to ensure the team understands the process of managing a data breach, comprehends the different roles, and the process is fine-tuned as much as possible. Many organizations unfortunately learn about data breach management during a breach and are unprepared for the different scenarios. This type of testing can also be coordinated with other business continuity, disaster recovery, or crisis management programs.

Remediating Issues

Many times a security event will require non-security team involvement. For example, a virus infection on an end-user device could spawn a security alert. The remediation of that alert could be the re-imaging of the infected device by the IT desktop management function. Just like data breach management, these users may not be daily RSA Archer GRC users and may require special training.

Some actions to consider for this phase:

- Personnel that are designated or planned to be part of the remediation cycle should be briefed and trained on the process. This will require both an initial rollout training program and an ongoing periodic training offering to ensure new resources are trained.
- The concept of "champions" or extended team members may be necessary to help train and provide point-of-contact with the various remediation areas. For example, a Point of Contact may be designated in the Server, Desktop, Application and Network areas (or however the IT organization is structured) to assist in these processes.
- Reporting to those Points of Contacts or the management level of the different operational units on key metrics, such as time to close, time to respond, etc. should be reviewed with the management team members to ensure proper reporting is in place to the various operational teams.

Chapter 2: RSA Archer Security Operations Management Solution Components

Incident Response Subsolution

The RSA Archer Incident Response subsolution allows you to manage the complete incident handling process, from incident and alert creation through the investigation process and to incident resolution.

Security Incidents Application

The Security Incidents application provides a central location managing incidents, both those created from aggregated security alerts and those that are manually reported. In the Security Incident application, you can do you the following:

- Capture information about the incident, including the factors that contributed to it, the assets and information targeted, and the efficacy of your security controls
- Manage the complete incident handling workflow, from assigning an L1 incident handler to review and assess the incident, escalating an incident to an L2 incident handler for further investigation and analysis, and creating and assigning response and remediation tasks
- Capture forensic and impact analysis

Security Alerts Application

The Security Alerts application stores the individual alerts reported by a SIEM tool that make up an incident. In the Security Alerts application, you can do the following:

- View the details about the security alert, such as source and destination IP addresses and the severity level
- Open Bing maps to view the Source city or country and the Destination city or country in the security alert
- Launch Security Analytics to view the security alert in context

Security Events Application

The Security Events application stores the individual events that make up an alert. In the Security Events application, you can view the details about the security event, such as source and destination IP addresses and source and destination MAC addresses.

Incident Investigations Application

The Incident Investigations application allows you to tie multiple related incidents together for faster handling and resolution. You can document the impact analysis, response and remediation tasks required, and results of your investigation just as you can for an incident.

You can also create an investigation record to look into suspicious activity, threat intelligence, or other information reported outside of RSA Archer Security Operations Management.

Forensic Analysis Application

The Forensic Analysis application allows an Incident Handler to capture details about any relevant host or network forensic analysis that they perform in the course of investigating an incident.

Incident Response Procedures Application

Incident Response Procedures is a leveled application that allows you to document, manage, and track all of the specific tasks that must be completed for an incident or an investigation. The first level, Incident Response Procedures, describes the overall procedure, including the threat and response categories to which it applies. The second level, Incident Response Tasks, describes the individual tasks that an incident handler should complete.

Procedures and tasks can be manually created by anyone assigned to work on incident or investigation, such as an incident handler. Procedures and tasks can also be created automatically based on the templates stored in the Incident Response Procedure Library application.

Incident Journal Application

The Incident Journal application allows an Incident Handler to record notes about each action they take while working on an incident, investigation, or breach.

Data Breach Response Subsolution

In the event of a breach related to privacy data, credit card data, intellectual property, or trade secrets, members of an organization business, legal, compliance, and HR departments must assess the situation and identify the corrective course of action. The Data Breach Response subsolution allows you to do the following:

- Identify incidents that have resulted in a breach
- Manage and remediate the breach
- Track the activities required of these cross-functional teams when a breach occurs

Data Breaches Application

The Data Breaches application allows you to manage the process of handling a breach related to privacy data, credit card data, intellectual property, or trade secrets. In the Data Breaches application, you can do the following:

- Capture information about the assets and data involved in a breach
- View the investigation or incidents that led to the discovery of the breach
- Track the activities required of cross-functional teams and have cross-functional team members provide impact assessments for the breach

Breach Tasks Application

The Breach Tasks application allows you to document, manage, and track all of the specific tasks that must be completed in the event of a breach. Tasks can be manually created by anyone assigned to work on breach, such as an incident handler or compliance officer, while other tasks can be created automatically based on the templates stored in the Breach Response Procedure Library application.

Breach Risk Assessment Questionnaire

The Breach Risk Assessment questionnaire allows you to calculate the risks to your organization caused by a breach based on the type of data disclosed, the risk of harm to individuals, and whether the disclosure was intentional or inadvertent.

Notifications and Call Trees Application

The Notifications and Call Trees application serves as a central repository for call trees (for both external and internal notifications) that should be executed as part of breach tasks. You can capture the call initiator and call recipient (references the Contacts application) and create custom messages to send to recipients.

Notification History Application

The Notification History application provides a history of when call trees were executed as part of a breach task. The application captures the number of people contacted, the number of people reached, and the duration of the activity.

SOC Program Management Subsolution

The SOC Program Management subsolution allows you to document, manage, and track your SOC program infrastructure, such as team personnel, standard incident or breach response procedures, and security policies and controls.

Shift Handover Application

The Shift Handover application allows the Incident Coordinator to capture all the information that the Incident Coordinator of the next shift requires to take over incident response duties. The Incident Coordinator of the current shift can capture items that have been closed, items that required follow-up, and summaries of what each incident handler did during their shift. The Incident Coordinator of the next shift can then review all of this information at the beginning of their shift.

Breach Response Procedure Library

The Breach Response Procedure Library application provides a repository for templates of response tasks that must be completed for a breach.

Incident Response Procedure Library

Incident Response Procedure Library is a leveled application that provides a repository for templates of response tasks that must be completed for a incident. The first level, Incident Response Procedures, allows you to document the overall procedure, including the threat and response categories to which it applies. The second level, Incident Response Tasks, allows you to document the individual tasks that an incident handler should complete.

Security Controls Application

The Security Controls application allows you to document information about the security controls of your organization, including names and descriptions, the security tool that provides the control, the costs associated with the control, and the control owner.

SOC Policies Application

The SOC Policies application allows you to document your organization security policies, including names and descriptions, policy owners, and stakeholders.

Contacts Application

The Contacts application serves as a central repository for contact information, allowing you to document information about CIRC staff, such as their skills and roles, as well as information about other internal and external contacts who need to be involved in the incident management or breach management process.

The Contacts application is utilized across multiple areas of the RSA Archer GRC Suite and contains information that is often leveraged by other solutions. Updates to the profile record of an individual within this application will automatically be propagated in any records where that contact information is displayed.

Teams Application

The Teams application allows you to capture information about your teams of incident handlers, such as the team name, manager, and a description of the team responsibilities, as well as information about the individual team members, such as their names and roles.

Question Library

The Question Library application documents assessment questions linked to authoritative sources, control standards, and risks. You can use these questions as needed when creating a breach risk assessment.

Degrees and Certifications Application

The Degrees and Certifications application allows you to capture information about team members' education, such as their certifications and degrees, in order to help assign incident handlers with the appropriate background to specific incidents.

Training Application

The Training application allows you to capture team members' training history and the Continuing Professional Education (CPE) credits they have obtained toward renewing professional certifications, in order to help assign incident handlers with the appropriate background to specific incidents.

RSA Archer Issue Management Subsolution

The RSA Archer Issue Management subsolution allows you to manage the remediation of any issues that are found in the course of investigating a security incident or responding to a data breach.

Findings Application

The Findings application allows you to document and track all of the individual issues that must be resolved in order to close an incident or breach. You can resolve a finding through either a remediation plan or exception request.

Exception Requests Application

The Exception Requests application allows you to manage the process of granting denying, and expiring exceptions to the remediation required in a Finding. Through the built-in workflow, the application enables you to ensure that all exceptions are properly reviewed. You can also report on exceptions across the enterprise, monitoring them by control, department, or severity, to visualize the impact of exceptions on the business and its compliance posture.

Remediation Plans Application

The Remediation Plans application allows you to centrally manage multiple findings and track actual and estimated remediation costs and timeframes. Relating multiple findings in the context of remediation plans allows you to identify larger issues and support informed decision making.

Policy Change Requests Application

The Policy Change Requests application is included as part of the Issue Management subsolution but is not part of the RSA Archer Security Operations Management workflow.

RSA Archer Enterprise Management Solution

The RSA Archer Security Operations Management solution references the RSA Archer Enterprise Management solution, allowing you to do the following.

- Document locations affected by a security incident
- Document business processes and applications affected by a breach

The RSA Archer Enterprise Management solution is packaged separately. For compatible versions, see the *RSA Archer Security Operations Management 1.3 Installation Guide*. To read an overview of RSA Archer Enterprise Management components and features, see the *RSA Archer Enterprise Management 4 Overview Guide*.

Supported and Generic SIEM

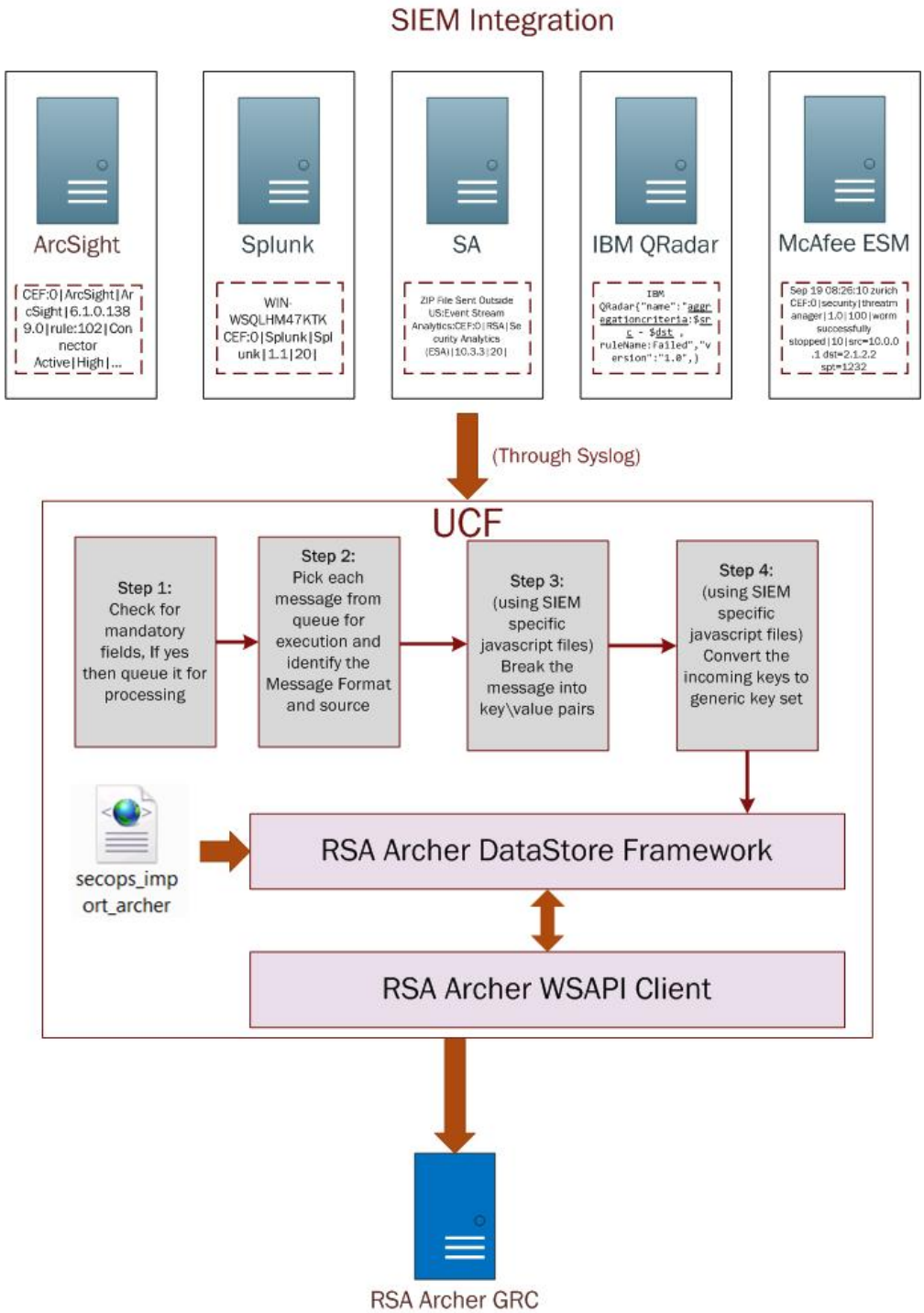
The UCF uses a generic SIEM implementation to integrate with various SIEM tools and provide event forwarding through Syslog. Out of the box, RSA Archer Security Operations Management 1.3 supports integration with the following tools:

- RSA Security Analytics Reporting Engine (SA RE)
- RSA Security Analytics Event Stream Analysis (SA ESA)
- HP ArcSight
- Splunk
- McAfee Enterprise Security Manager (ESM)
- IBM QRadar

SIEM tools that are not supported out of the box can also be configured to work with RSA Archer Security Operations Management.

Note: If you integrate with the RSA Security Analytics Incident Management module, integrating with SA RE and SA ESA can result in duplicate events and incidents created in RSA Archer GRC.

The UCF supports multiple SIEM tools at the same time, such as supporting SA RE, ArcSight, and SA IM. Different instances of the same SIEM tool are not supported, such as running two SA servers connected to the same UCF.



Integration with RSA Security Analytics

RSA Archer Security Operations Management integrates with RSA Security Analytics using the RSA Unified Collector Framework.

RSA Unified Collector Framework

The RSA Unified Collector Framework (UCF) integrates with all supported SIEM tools and the RSA Archer Security Operations Management solution. When integrating with the RSA Security Analytics Incident Management module, you can choose one of the following integration options:

- Manage the full incident workflow in RSA Archer Security Operations Management. If you select this option, the Unified Collector Framework transports incidents from the Security Analytics Incident Management module into the solution.
- Manage the incident workflow in the Security Analytics Incident Management module and allow analysts the option to escalate remediation tasks and open data breaches for management and remediation in the RSA Archer Security Operations Management solution. If you select this option, the Unified Collector Framework transports remediation tasks (created as Findings), data breaches, or both.

  Important: You must configure the same option in both RSA Security Analytics and the Unified Collector Framework.

Chapter 3: Managing SOC Readiness

Managing SOC Staff and Contacts

As the SOC Manager, you can use RSA Archer Security Operations Management as a central repository for any information you require about SOC staff members and cross-functional team members. You can document your teams of incident handlers, capture the education and training history of each team member in order to help assign the right handlers to incidents, and store contact information for anyone who needs to be notified about a breach.

Document Solution Users

User: SOC Manager, Incident Coordinator

For each user who needs to access the RSA Archer Security Operations Management solution, you need to create both a record in the Contacts application, (to capture basic contact info, job title, team membership, and educational background) and an RSA Archer GRC user account (to use to log on and to assign access rights and group membership).

Procedure

1. Create a user account for the user:

   Note: You may require your Solution Admin to create the RSA Archer GRC user accounts, depending on what administrative access you have been granted.

   b. Click Administration > Access Control > Manage Users > Add New.

   c. Fill out the General Information and Contact Information sections.

   d. Click the Groups tab, and click Lookup.

   e. Expand the Groups list, and select the group to which the user belongs.

   When you assign a user to a group, the user also inherits the access roles associated with the group. Each SOC user group is associated with the related SOC access role.

   f. Save the user account.

2. Create a contacts record for the user:

   Note: User can also log on and create their own contacts records.

   a. In the Security Operations Management solution, in the Navigation menu, click Contacts > Add New.

   b. Complete the required fields in the General Information section, and fill out any other information as needed.

      Note: If you are creating a Contacts record for someone other than yourself and want that user to have the ability to edit or update the record, assign them as a Record Owner.

   c. Save the contacts record.

Document SOC Staff Skill Sets

User: Any SOC Staff Member

Documenting the skills, education, and training history of each incident handler allows the Incident Coordinator to assign security incidents to handlers with the appropriate skills and background.

Procedure

1. In the Contacts application, open the user record.
2. Click the Education tab.
3. In the Skills and Capabilities field, select the user skills.
4. In the Degrees and Certifications section, click Add New.
5. Fill out and save the record. If you also want to document training courses that support the degree or certification, click Add New in the Training Courses section, and fill out the record.
6. Repeat steps 3 – 5 for each degree or certification the team member holds.
7. (Optional) Document other training courses.
   a. In the Training Courses section. click add Add New
   b. Fill out and save the record.
   c. Repeat steps a – b for all the training courses of the user.

Document SOC Teams and Team Members

User: SOC Manager or Incident Coordinator

Procedure

1. Create a team record:
   a. From the Navigation menu, click Teams > Add New.
   b. Enter a team name and description, and select the team manager.
   c. Click Apply to save the Teams record.
2. Add team members to the team:
   a. In the Members section, click Add New.
   b. Select the name of the team member and their role.

      Note: The Member Name field is a cross-reference to the Contacts application. After you save the member record, the user team membership information is also displayed in their contact record.

   c. Click Save.
   d. Repeat steps a – c for each member of the team.
3. Save the team record.

Managing SOC Policies and Procedures

As the SOC Manager, you can use RSA Archer Security Operations Management to track all the security policies you are required to follow, all the security controls that you have invested money in, and how effective those controls are at detecting, preventing, and investigating incidents. You can also use RSA Archer Security Operations Management to document standard processes and procedures for team members to follow when handling an incident or a breach.

SOC Policies

SOC policies define the processes, terms, and standards that your SOC team is bound to follow. For example, your SOC might be required to respond to an incident within a set amount of time depending on the incident priority level. RSA Archer Security Operations Management allows you to document all of your SOC policies and to manage the process of reviewing and approving them with all required stakeholders.

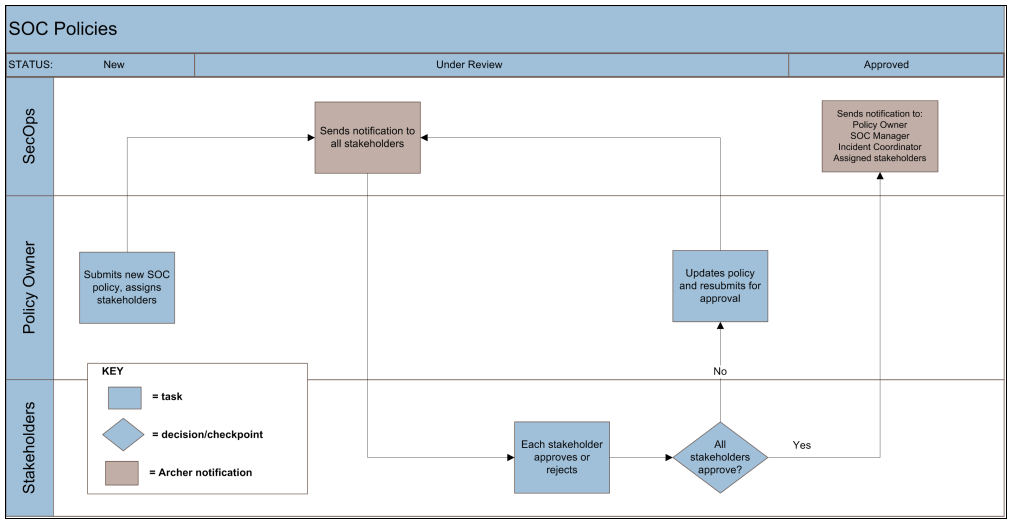
Establishing SOC policies around the following list of subjects up front will also help you manage subsequent SOC processes for handling incidents and responding to breaches in the RSA Archer Security Operations Management solution.

Policy	What it should define
Incident Priority Classification	What does each priority level mean to your organization? How should they be assigned to incidents?

Policy	What it should define
Incident Handling SLA Requirements	How quickly must incidents be looked at, investigated, resolved? How does this vary based on incident priority?
Declared Incidents	What does a declared incident means to your organization? When an incident should be declared?
Confidential Incidents	What incidents should be marked confidential? Who should have access to confidential incidents?
IT Operations Remediation SLA Requirements	How quickly must a ticket be resolved? How does this vary based on criticality?
Breach Handling	Who should be responsible for managing the entire breach response process?

SOC Policy Review Process

The following figure shows the process of creating and reviewing a SOC policy.



When you create and save a new SOC policy record, notifications are sent to each assigned stakeholder to tell them that a new policy requires their review. Each stakeholder must review the policy and either approve or reject the policy.

When all stakeholders have reviewed and approved the policy, the status becomes Approved. If all stakeholders have not yet reviewed the policy or some have rejected it, the status remains as Under Review.

Document SOC Policies

User: SOC Manager or Incident Coordinator

Procedure

1. In the Security Operations Management solution, in the Navigation menu, click Security Policies > Add New.
2. Enter a policy name, description, owner, and stakeholders.

   Note: The Stakeholder 1 role is automatically populated with the SOC Manager.

3. Click Save.
4. Repeat steps 1 – 3 for each security policy that you want to document in RSA Archer Security Operations Management.

Response Procedure Libraries

Response procedures define the tasks that incident handlers should complete or the guidelines or checklists they should follow when responding to an incident or breach. RSA Archer Security Operations Management allows you to maintain a library of all of your standard response procedures.

By defining response procedures, you can provide incident handlers with guidance and consistent processes for reviewing incidents and handling breaches. When an incident handler categorizes an incident, any response procedures that match that category are automatically copied from the Incident Response Procedure Library into the Incident Response Procedures application and linked to the incident record. When a breach response team member selects impacted regulations, any response procedures that match those regulations are automatically copied from the Breach Response Procedure Library into the Breach Tasks application and linked to the breach record.

Document Incident Response Procedures

User: SOC Manager, Incident Coordinator, or L2 Incident Handler

Procedure

1. In the Security Operations Management solution, in the Navigation menu, click Incident Response Procedure Library > Add New.
2. Ensure that Incident Response Procedures is selected, and click Continue.
3. Enter a name and description for the procedure.
4. Select the source of the procedure.
5. Select whether the procedure is active or inactive.

   When an incident handler selects an incident category, only active procedures are included in the data feed and copied into the Incident Response Procedures application.

6. In the Threat Category field, select the category of incident to which this procedure should apply.

7. Select the response phases that the procedures applies to.
8. In the Incident Response Tasks section, click Add New, and do the following:
   a. Enter a name and description for the task.
   b. Select the response phase to which this task belongs.
   c. If the task is one of many in a procedure, assign a step number to the task.
   d. In the Target field, assign a default user group who should complete the task.
   e. Select whether the task is required or optional.
   f. (Optional) Add attachments or screenshots.
   g. Save the task record.
9. Repeat step 8 for each response task that you want to associate with this response procedure.
10. Save the procedure record.

Document Breach Response Procedures

User: SOC Manager, Incident Coordinator, or L2 Incident Handler

Procedure

1. In the Security Operations Management solution, in the Navigation menu, click Breach Response Procedure Library > Add New.
2. Enter a name and description for the procedure.
3. Select the priority level of the breach to which this response procedure should apply.
4. Select whether the procedure is required or optional.
5. Select whether the procedure is active or inactive.
   When a breach response team member selects impacted regulations, only active procedures are included in the data feed and copied into the Breach Tasks application.
6. In the Target field, assign a default user group who should implement the procedure.
7. For a breach procedure, select any applicable regulations to which this procedure should apply.
8. Save the record.

Call Trees

A call tree is a list of persons, roles, and/or organizations that you may need to notify in a particular sequence in the event of a breach. You may have call trees for internal contacts, such as a list of senior management who need to stay informed about the response to a breach, or external contacts, such as a list of government bodies that you are required to notify in the case of a breach.

Set Up Call Trees

User: SOC Manager, Incident Coordinator, L1 or L2 Incident Handler

Procedure

1. In the Security Operations Management solution, in the Navigation menu, click Call Trees > Add New.
2. Complete the General Information Section.
3. In the Call Initiator section, select the user who is responsible for contacting others in the event of a breach.
4. In the Call Recipients section, add or lookup the user or users who need to be contacted.
5. In the Message section, enter the message that the Call Initator is required to deliver.
6. Click Save.

Security Controls

Security controls are all of the tools or technologies that your SOC uses to detect, prevent, and investigate security incidents. RSA Archer Security Operations Management allows you to document all of your security controls, including each control owner, deployment status, control category, and fixed and annual operational costs.

Document Security Controls

User: SOC Manager or Incident Coordinator

Procedure

1. In the Security Operations Management solution, in the Navigation menu, click Security Controls > Add New.

2. Complete the General Information section.

General Information			
Tracking ID:	SC-205809	**Control Number:**	
Control Name:	RSA ECAT	**SOC Policy:**	
Control Description:	Malware detection		
Control Owner:	SOC Manager, Jim	**Control Category:**	Detective Investigative
Security Tool:		**Deployment Status:**	Deployed
Annual Operational Cost:	$ 100,000.00	**Fixed Cost:**	$ 200,000.00

3. In the Site Location section, add a cross-reference to the facility to which the control applies.
4. Click Save.

View Security Control Efficacy

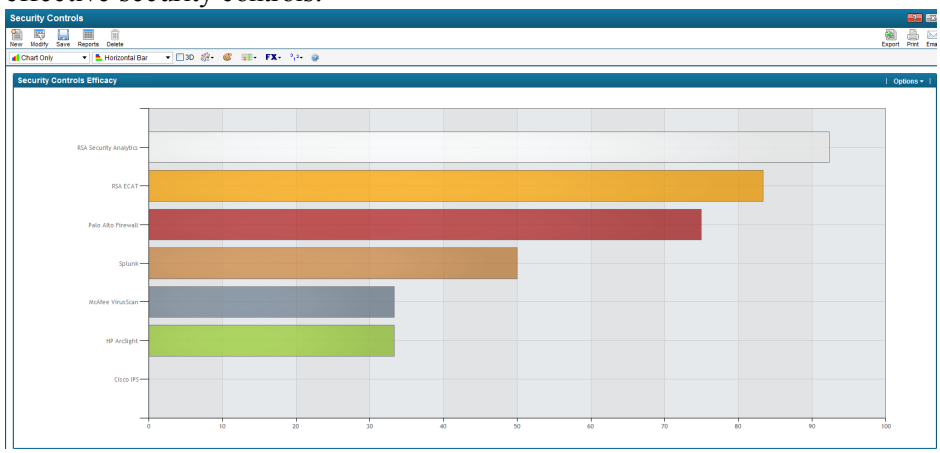
User: SOC Manager

As incident handlers resolve incidents and note which security controls they found effective and ineffective, you can get a picture of your overall security control efficacy.

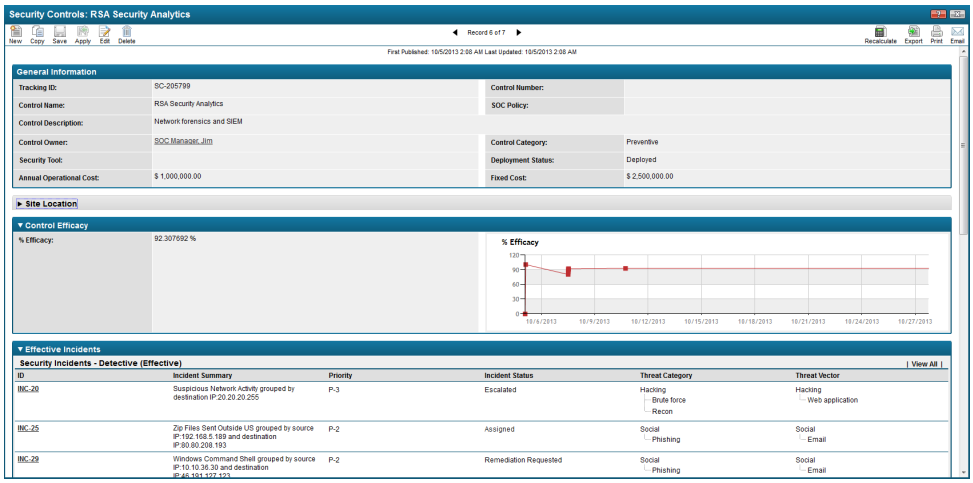
Procedure

- To view your overall security controls efficacy:
  - In the Security Operations Management workspace, select the SOC Manager dashboard.
  - In the Navigation menu, click Security Controls > Reports > Security Controls Efficacy.

    The Security Tools Efficacy report shows a summary of the top 10 most effective security controls.



- To view the efficacy of a particular security control, open the security control record.



The Control Efficacy section shows the overall efficacy of the control and its efficacy over the last 3 years. The Effective Controls section displays the incidents that the control was effective in detecting, in preventing, or at investigating an incident. The Ineffective Controls section displays the incidents in which the control was not effective.

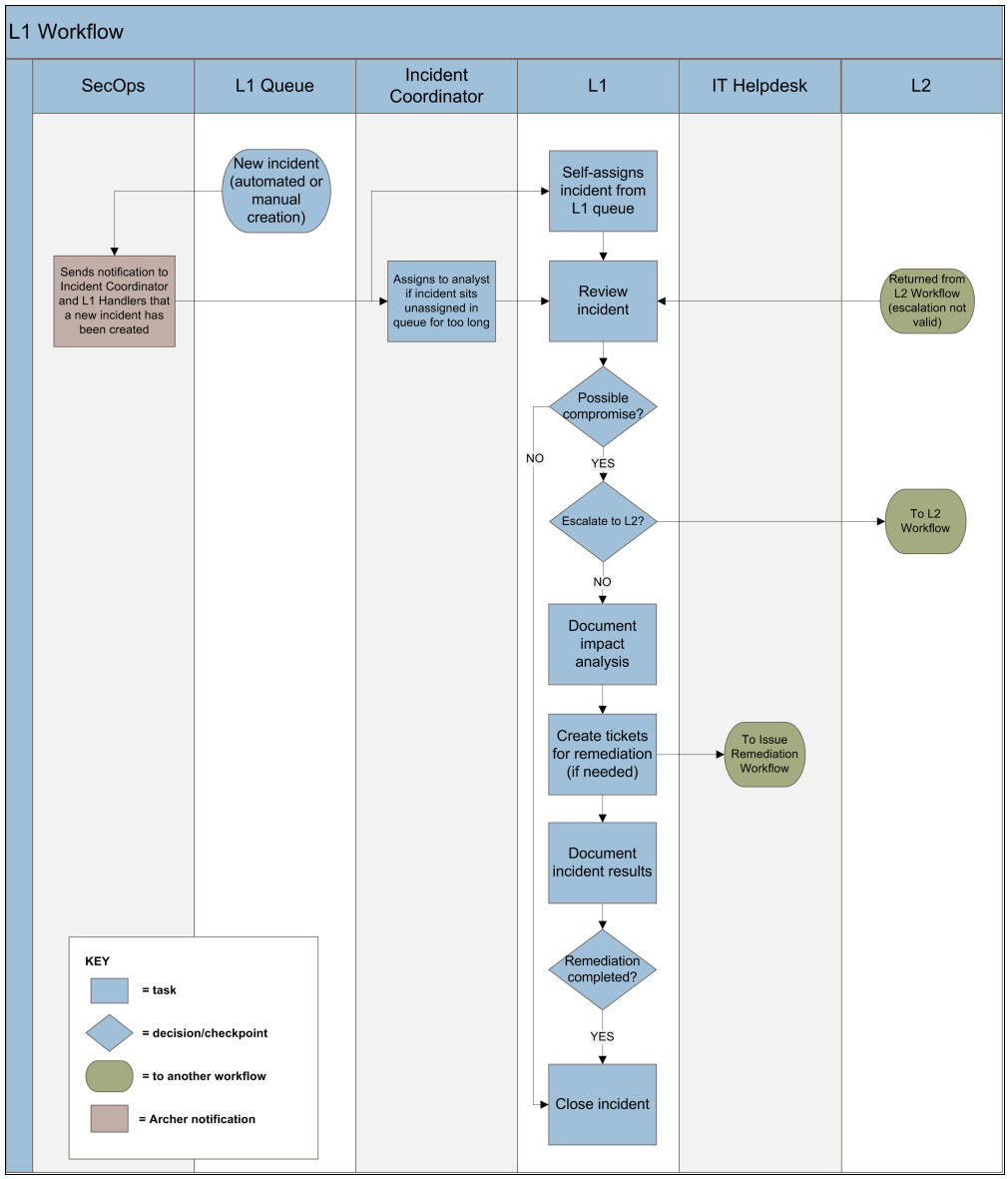
- To view the efficacy of security tools for a particular incident or investigation:

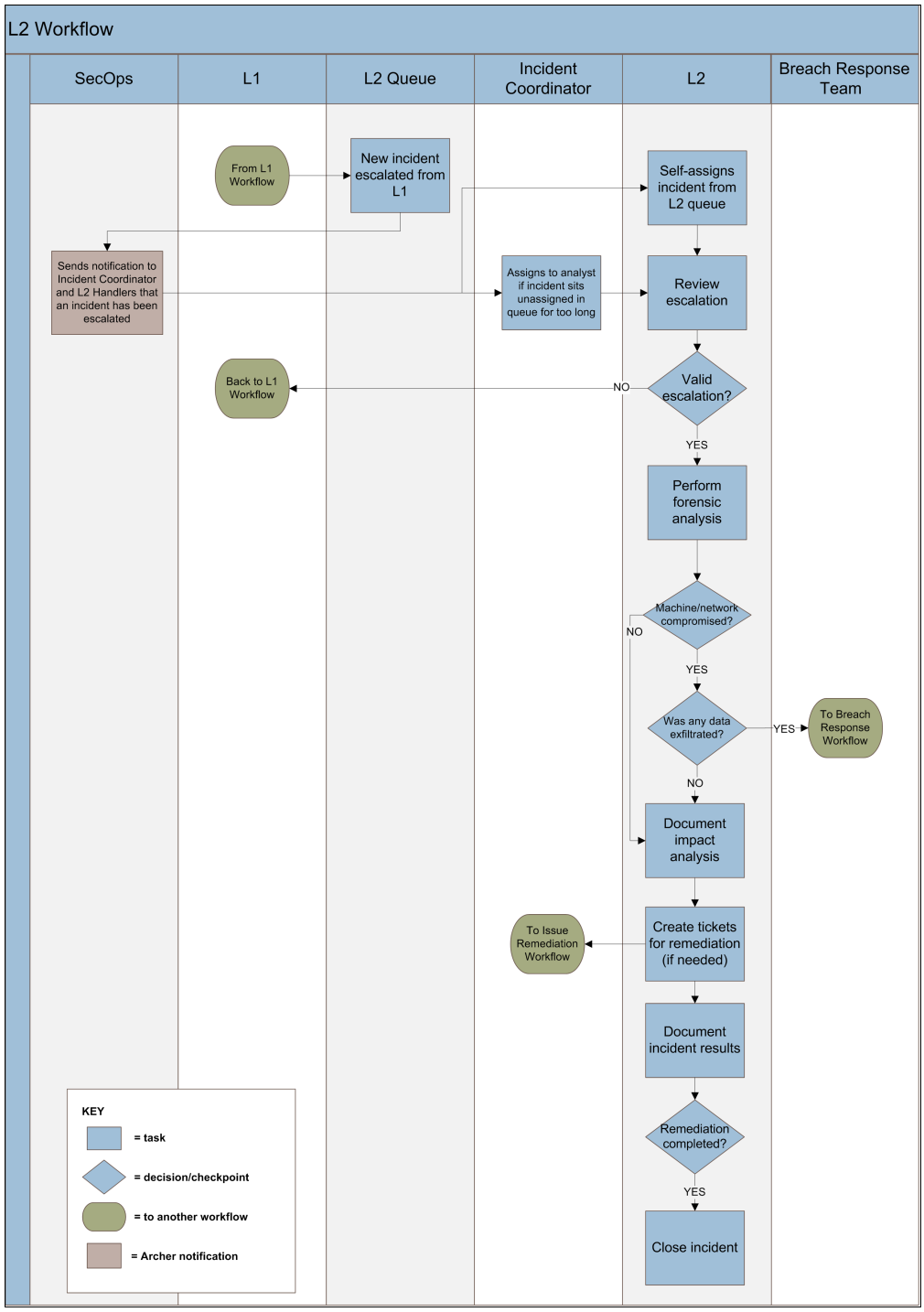
  1. Open the incident or investigation record.
  2. Click the Results tab.
  3. In the Controls Efficacy section, view the detective, preventive, and investigative controls that the incident handlers deemed effective and ineffective.

Chapter 4: Responding to Incidents

Incident Response Workflow

The RSA Archer Security Operations Management solution is built to enable the following incident response workflows.


L1 Workflow
SecOps
L1 Queue
Incident Coordinator
L1
IT Helpdesk
L2
New incident (automated or manual creation)
Sends notification to Incident Coordinator and L1 Handlers that a new incident has been created
Assigns to analyst if incident sits unassigned in queue for too long
Self-assigns incident from L1 queue
Review incident
Returned from L2 Workflow (escalation not valid)
Possible compromise?
NO
YES
Escalate to L2?
To L2 Workflow
NO
Document impact analysis
Create tickets for remediation (if needed)
To Issue Remediation Workflow
Document incident results
Remediation completed?
YES
Close incident
KEY
= task
= decision/checkpoint
= to another workflow
= Archer notification



Note: Only notifications that are a key part of the workflows are included in the diagrams. For a complete list of notifications, see the *Data Dictionary*.

Alerts vs Incidents

Security Alert	Security Incident
A correlated event with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data, or a combination of one or more of these events.	A distinct group of security alerts involving specific attackers, attacks, objectives, sites, and timing that results in a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

RSA Archer Security Operations Management can collect alerts from SIEM tools and aggregate alerts into incidents, can collect incidents from Security Analytics, or allows you to create an incident manually. Alert data is stored in the Security Alerts application, and the aggregated incidents are created in the Security Incidents application.

One security incident can be made up of multiple security alerts, however a security alert can only be tied to one security incident. All alerts must be tied to an incident.

Aggregating Multiple Alerts into a Single Incident

The Security Analytics Incident Management module collects alerts from multiple sources and allows you to configure rules to aggregate alerts into incidents, so that the incident handlers can investigate and remediate multiple alerts in the context of a single incident.

If you are using a third-party SIEM tool as an alert source, the UCF middleware allow you to define the aggregation criteria by which alerts are grouped into incidents.

In both cases, alerts continue to be added to an incident according to the aggregation criteria until the incident is assigned.

Incident Status

The status of the incident record reflects where in the overall workflow you currently are.

Incident Status	What it Means
New	Default status when a record is created.

Incident Status	What it Means
Assigned	Incident has been assigned to an L1 Incident Handler, but the Handler has not yet started working on the incident.
In Progress	The L1 Incident Handler has started working on the incident.
Escalated	The L1 Incident Handler has escalated the incident to an L2 Incident Handler.
Returned to Level 1	The L2 Incident Handler has reviewed the incident found that the escalation is not valid. For example, the L1 Incident Handler may have missed checks before they escalated the incident.
Remediation Requested	The L2 Incident Handler has completed their analysis and found items that require remediation.
Remediation Completed	The required remediation has been completed.
Resolved	All tasks have been resolved and the incident is not tied to any open investigations or breaches.
Invalid	After review, the information in the incident does not reflect a security compromise or malicious activity.

Declared Incidents

Your organization may have hundreds of incidents to investigate, but not every incident necessarily reflects an attack or breach. For example, an incident handler may investigate and discover than an incident was a false positive. RSA Archer Security Operations Management allows you to flag an incident as a Declared Incident for those incidents which you want to provide management visibility into or those that are confirmed issues that require remediation.

When a handler flags an incident as Declared, the SOC Manager and Incident Coordinator groups are notified and the incident appears in the Declared Incidents report on the SOC Manager and Incident Coordinator dashboards.

RSA recommends that you establish a SOC policy about what a declared incident means to your organization and which incidents should be declared.

Confidential Incidents

Some incidents may be highly sensitive and require that you restrict who has access to the record. For example, an investigation might be occurring about a SOC staff member, in which case you do not want them to have access to the incident record. When you flag an incident as Confidential, only members of the SOC Manager and Incident Coordinators groups are granted access.

RSA recommends that you establish a SOC policy about what a confidential incident means to your organization, which incidents should be marked confidential, and who should maintain access to these records.

Creating an Incident

In RSA Archer Security Operations Management, there are two ways that incidents can be created:

- Automatically, using the UCF to aggregate alerts from a SIEM tool into incidents
- Manually, in the RSA Archer Security Incidents application.

Create an Incident Manually in the Security Incidents Application

User: SOC Manager, Incident Coordinator, L1/L2 Incident Handler

Procedure

1. In the Security Operation Management solution, in the Navigation menu, click Security Incidents > Add New.
2. In the Overview tab, enter a title, summary, and any other initial information that you have.
3. Save the record.

   If you assign an incident owner, the incident will appear in that user queue. If you do not assign an owner, the incident will appear in the L1 Incident Handler queue for any member of the team to begin work on the incident.

Assigning Incidents

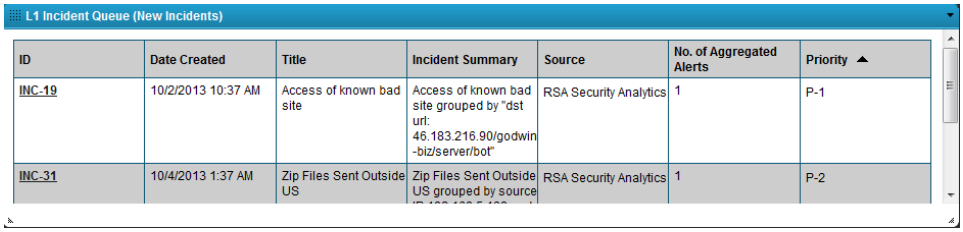
Once an incident is assigned, no additional alerts can be tied to the incident by the Unified Collector Framework. You can manually associate new alerts to an assigned incident.

Assign Yourself an Incident from the Queue

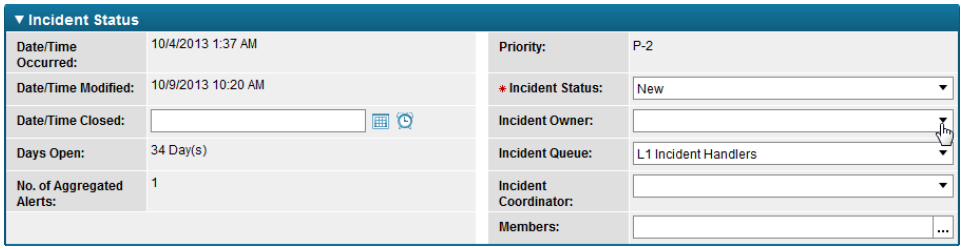
User: L1 or L2 Incident Handler

Procedure

1. From the Security Operations Management workspace, and select the L1 or L2 Incident Handler dashboard.
2. From the L1 or L2 Incident Queue iView, click the ID of the incident that you want to work on.



3. In the incident record, in the Incident Owner field, select yourself.



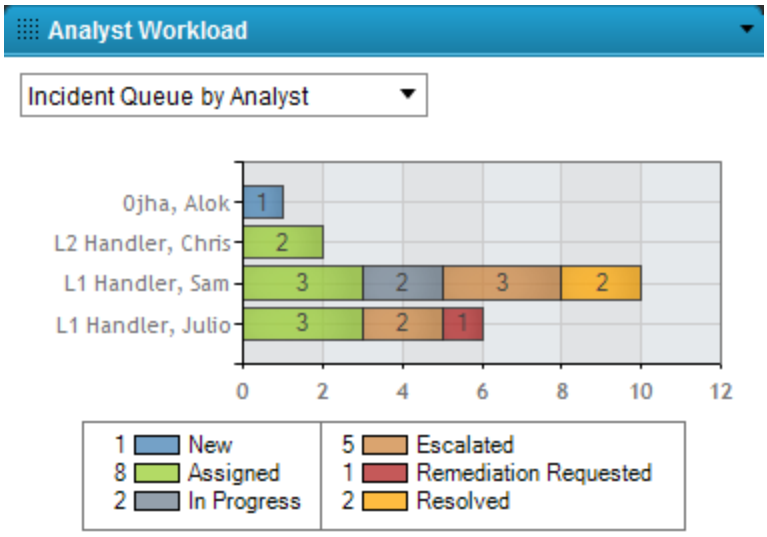
4. Save the incident record.

Assign an Incident to a Handler

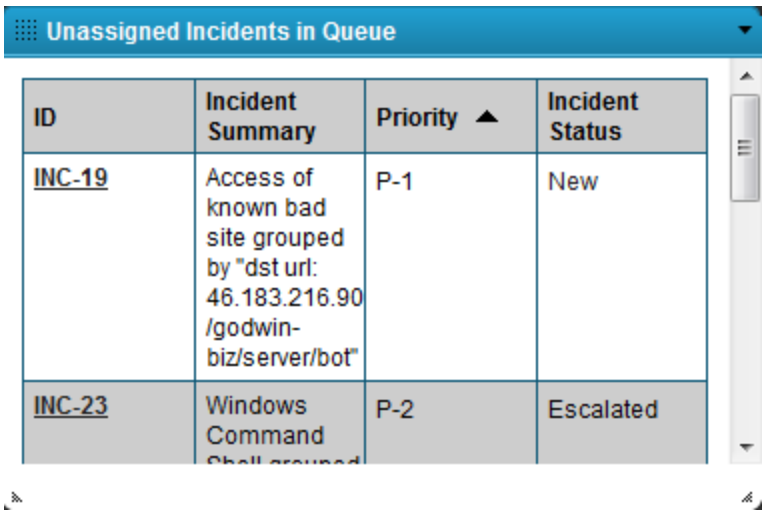
User: Incident Coordinator

Procedure

1. From the Security Operations Management workspace, and select the Incident Coordinator dashboard.
2. (Optional) Review the Analyst Workload iView. These reports show you the total number of incidents assigned to each L1 and L2 Incident Handler.



3. From the Unassigned Incidents Queue iView, click the ID of the incident that you want to assign.



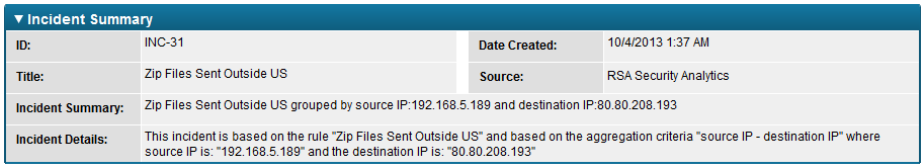
4. Review the incident record, then in the Incident Owner field, select the incident handler who you want to assign to the incident.
5. Save the incident record.

Review an Incident

User: L1 Incident Handler

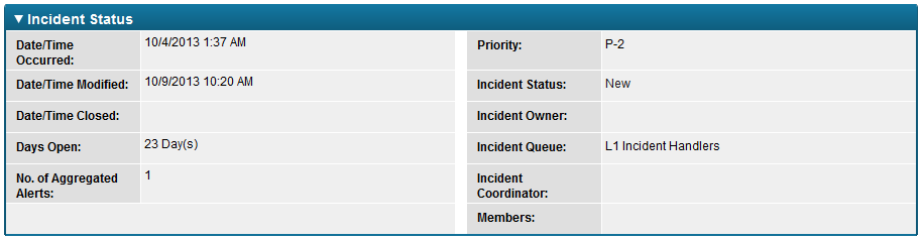
Procedure

1. Review all the existing information:
   - The Incident Summary section provides basic information, such as the title, summary, basic details, and the source of the incident.



     If you are using Security Analytics Incident Management, the Incident Source field shows which source the alert originally came from.

   - The Incident Status section provides the current status, date created, incident owner, and the priority of the incident.

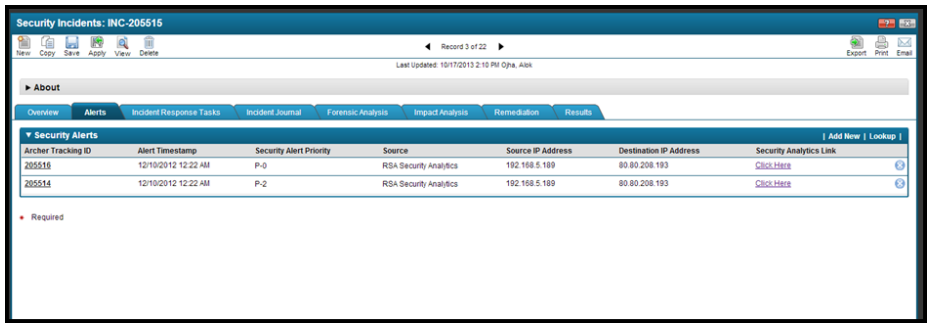


     The Priority field is initially populated as follows:

     - If you are using Security Analytics, the priority is the incident priority from the Incident Management module.
     - If you are using a third-party SIEM tool, the incident priority is based on the highest priority level of all the associated alerts. The alert priority level is based on the alert severity level from the SIEM tool, as follows:

Alert severity level	Alert priority level
1-2	P3
3-5	P2
6-8	P1
9-10	P0

- The Alerts tab shows all of the individual alerts that comprise the incident.



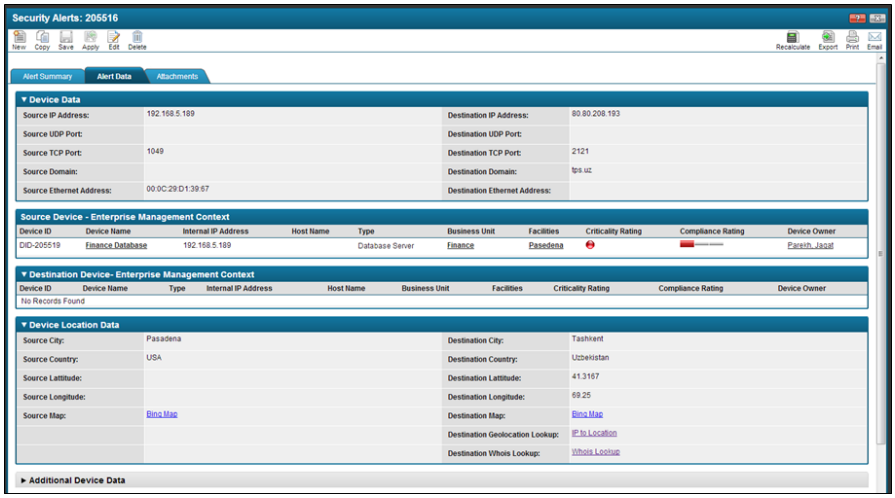
You can click the Security Analytics Incident Management link to launch the Security Analytics UI in-context of the given alert for additional investigation. The default time range is 1 hour before and 1 hour after the alert, but you can customize this by drilling into the alert, entering a value in the Custom Time Range field, and applying the changes.

Note: If your Solution Admin has configured the Enterprise Management plug-in, the Security Analytics UI also displays criticality information and other business context about your RSA Archer GRC assets.

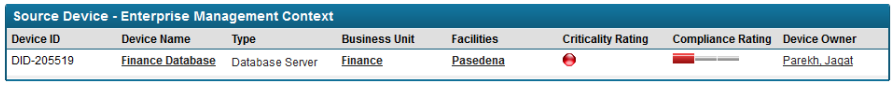
You can drill down into each alert to view more details in the alert record.

Note: If your alerts are coming from the Security Analytics ESA module, much of the data described below is actually displayed at the event level. You can drill into the Security Event record from the Security Alert record.

- The Alert Summary tab displays alert metadata, such as the source of the alert, its category and severity, as well as the raw alert message.
- The Alert Data tab display information parsed from the raw alert, such as source and destination IP addresses, user data, and location information.



If a device is internal, business context from the Enterprise Management solution is automatically displayed.



You can also use the pre-generated links to look up WHOIS and Geolocation information.

2. Classify the incident. In the Initial Threat Classification section, do the following:
   - Select a threat category.

     Based on the regulations you select, any response procedures and tasks in the Incident Response Procedure Library that match the selected category will be copied into the Incident Response Procedures application and will appear on the Incident Response Tasks tab in the breach record.

     Note: If you later change the threat category, any tasks that are no longer required are moved to the Not Applicable section on the Incident Response Tasks tab.
   - Select whether the threat actor is internal or external.
   - Select the threat vector
   - Select the asset type that was targeted
   - Select whether the threat is valid.
3. In the Incident Reporting section, select whether the incident is confidential or declared (if yet known; the L2 analyst may determine this during their analysis).
4. Save the incident record.

Using Investigations

An investigation record allows you to tie together multiple related incidents for faster handing and resolution. You can also create an investigation in order to look into suspicious activity, threat intelligence, or other information reported outside of RSA Archer Security Operations Management. For example, a Cyber Threat Intel Analyst might create an investigation and assign it to a L1 or L2 Incident Handler in order to have the handler find and document any traffic associated with specific new threat intelligence.

Create an Investigation

User: L1 or L2 Incident Handler, Cyber Threat Intel Analyst

Procedure

1. Do either of the following:
   - In the Security Operation Management solution, in the Navigation menu, click Incident Investigations > Add New.
   - From an existing incident or investigation record, click the Overview tab, and in the Related Mappings section, click Add New.
2. In the Overview tab, enter a title, summary, and any other initial information that you have.
3. In the Related Mappings section, click Lookup, and add any related incidents or investigations.
4. Save the record.

Close an Investigation

User: L1 or L2 Incident Handler

Procedure

1. Open the investigation record, and in the Related Mappings section, verify that that all related security incidents have been closed.
2. Change the investigation status to Closed.
3. Save the investigation record.

Manually Add Incident Response Procedures and Tasks

User: SOC Manager, Incident Coordinator, L1/L2 Incident Handler

Procedure

1. In the Security Operations Management solution, select the incident to which you want to add a task.
2. Select the Incident Response Tasks tab.
3. Do one of the following:
   - To attach new incident response procedures and tasks, click Add New.
     a. Select Incident Response Procedures, and click Continue.
     b. Complete the General Information section.
     c. In the Incident Response Tasks section, click Add New.
     d. Fill out the task record, and click Save.

e. Repeat steps c – d for any other tasks you want to add.

f. Click Save.

- To attach existing incident response procedures and tasks, click Lookup.

  a. Select the Incident Response Procedure and any tasks associated with that procedure that you want to add to the incident.

  b. Click OK.

  Important: You must select the procedure and the associated tasks to create a direct link from the Security Incidents application to both the Incident Response Procedures and Incident Response Tasks. This ensures that the correct hierarchy displays within the record.

4. Click Save.

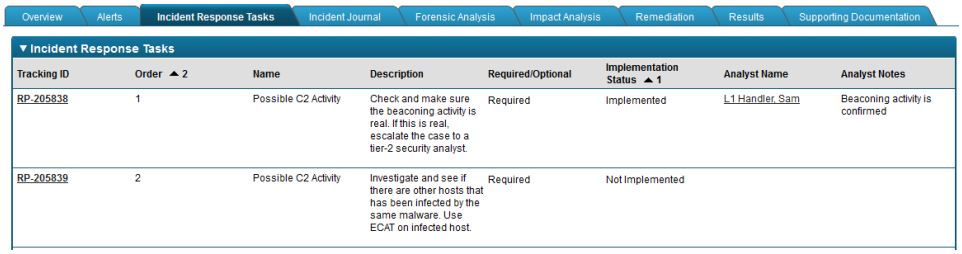
Complete Incident Response Tasks

User: Incident Owner (L1 or L2 Incident Handler)

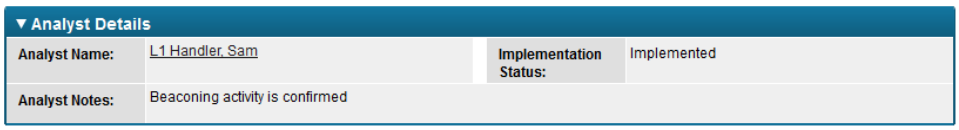
Note: You can also complete response tasks for an Incident Investigation record.

Procedure

1. In the Security Incident record, click the Incident Response Tasks tab. You can see which tasks are required and which are optional, and you can see which tasks that have not been completed (status = Not Implemented).



2. Open the task you want to complete.
3. Complete the task, then in the Analyst Details section, select yourself as the analyst, enter any notes about the task, and change the status to Implemented.



4. Save the record.
5. Repeat steps 2 – 4 for any other incident response tasks.
6. Save the record.

Add Shift Notes to an Incident

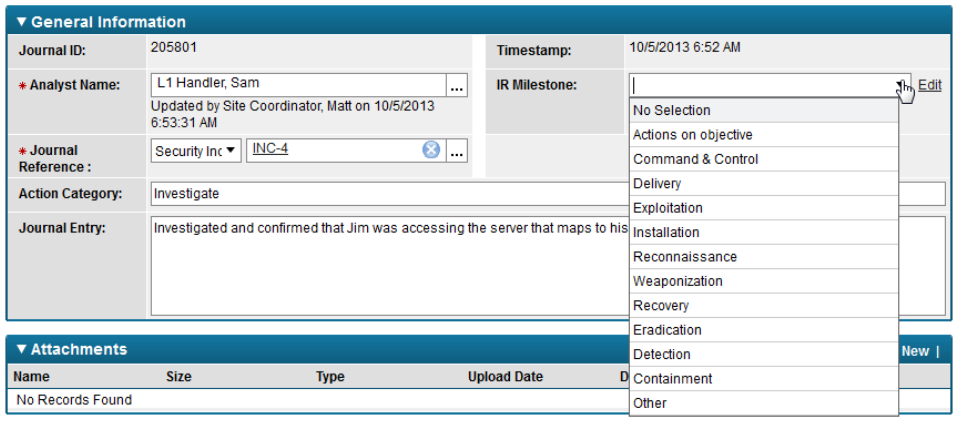
User: L1 or L2 Incident Handler

An incident may take more than your shift to resolve, in which case you should leave shift notes to inform the next handler about the current status.

Note: You can also add shift notes to an Incident Investigation record.

Procedure

1. In the Security Incident record, click the Incident Journal tab.
2. Click Add New.
3. In the Journal Entry field, enter any information that you want to provide the next incident handler.
4. In the IR Milestone field, select either a stage in the attack process or a stage in the incident response process, depending on what notes you are adding.



5. Save the Incident Journal record.

Escalate an Incident

User: L1 Incident Handler

Procedure

1. Open the incident record.
2. Change the Incident Status to Escalated.
3. Save the incident record.

   The incident is automatically moved to the L2 Incident Handlers queue, so that an L2 incident handler can begin work on it.

Review an Escalated Incident

User: L2 Incident Handler

Procedure

1. From the Security Operations Management workspace, and select the L2 Incident Handler dashboard.
2. From the Level 2 Incident Queue iView, open an incident to review.
3. Change the Escalation Status to Assigned, and select yourself as the Escalation Owner.
4. Review the incident details and work done to date and determine whether the escalation is valid.
5. Do one of the following:
   - If the escalation is not valid, change the Escalation Status to Returned. You can also use the Incident Journal tab to note anything that the L1 Handler missed. Save the record.

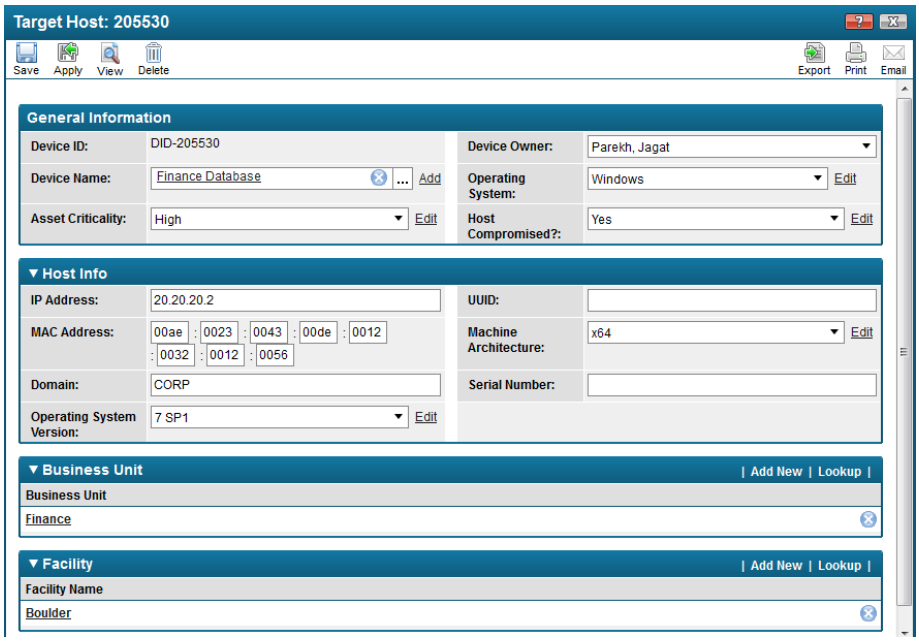
     The incident status changes to Returned to Level 1 and the queue changes to L1.
   - If the escalation is valid, **perform forensic analysis** and document your results.

Perform and Document Forensic Analysis

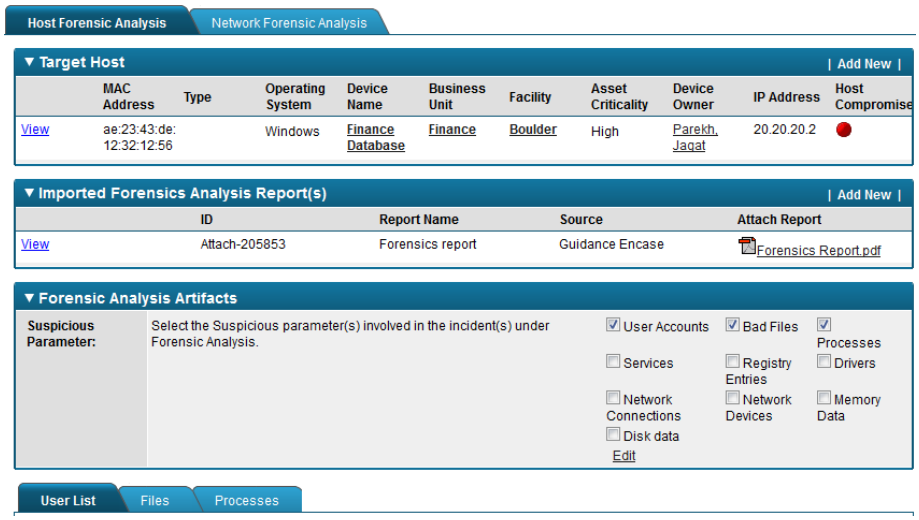
User: L2 Incident Handler

Procedure

1. In the Security Incident record, change the Escalation Status to Forensic Analysis In Progress.
2. Click the Forensic Analysis tab.
3. Document host forensic analysis:
   a. In the Host Forensic Analysis section, click Add New.
   b. Document information about the host that was targeted. Save the Target Host record.



c. Import and attach any external forensic analysis reports.



d. Document any suspicious parameters. In the Forensic Analysis Artifacts section, when you select each suspicious parameter that you want to document, a corresponding tab appears below. From each tab you can add and fill out a new sub-form to capture the details of the suspicious parameter.

e. Save and close the forensic analysis record.

4. Document network forensic analysis:

   a. In the Network Forensic Analysis section, click Add New.

   b. Fill out the General Information section.

c. Click the Network Forensic Analysis tab.

d. Fill out the Summary section.

e. In the Suspicious Traffic section, add and fill out a new sub-form to capture any details about suspicious network traffic.

f. Save and close the forensic analysis record.

5. Click the Overview tab, and change the escalation status to Forensic Analysis Completed.

6. Save the incident record.

   When you save the record, the overall Incident Status changes to Remediation Requested.

Document Impact Analysis

User: Incident Owner (L1 or L2 Incident Handler)

Once you have confirmed a security compromise, you must document the impact of the incident. You can document the business, corporate policy, confidentiality, integrity, and availability impact of the incident.

Note: You can also document impact analysis for an Incident Investigation record.

Procedure

1. In the Security Incident record, click the Impact Analysis tab.
2. Document the business impact of the incident. If you have licensed the RSA Archer Risk Management solution, you can tie the incident to an existing risk register record.
3. Document the confidentiality impact. If you find that data has been disclosed, create a data breach record for the breach response team to track and resolve. For more information, see **Create a Breach Record**.
4. Document the integrity impact.
5. Document the availability impact. If you have licensed the RSA Archer Business Continuity Management solution, you can create a crisis event record for your crisis event team to track and resolve.
6. Document the corporate policy impact.
7. Save the incident record.

Log Issues for Remediation

User: Incident Owner (L1 or L2 Incident Handler)

Note: You can also log issues for remediation from an Incident Investigation record.

Procedure

1. In the Security Incident record, click the Remediation tab.
2. In the Remediation Required field, select Yes.
3. In the Specify Remediation Action field, select the types of remediation action required.

   For each action type you select, a new section appears in the Remediation tab.
4. In each section, click Add New.
5. In the Findings record, enter the following:
   a. Enter a name and description of the action that needs to be completed.
   b. Select a criticality for the finding.
   c. In the Source Override field, select Security Operations.
   d. In the Security Operations Response section, select a target queue and remediation task type.
6. Save and close the Findings record.
7. Repeat steps 4 – 6 for each issue that needs remediation.
8. Save the incident record.

Document Overall Incident Analysis Results

User: Incident Owner (L1 or L2 Incident Handler)

Note: You can also document the overall results for an Incident Investigation record.

Procedure

1. In the Security Incident record, click the Results tab.
2. Capture the results of the incident. Confirm the incident and your confidence rating, and the attack category and method of discovery.
3. Capture the actors, tactics, and techniques that contributed to the incident.
4. Capture details about the target of the incident.
5. Look up and add the security controls that were effective in discovering the incident and those that were not effective.
6. Save the incident record.

Close an Incident

User: Incident Owner (L1 or L2 Incident Handler)

An incident cannot be closed if it has:

- An open investigation or breach tied to it
- Open tasks that are marked as Required, if the incident has a priority of P0 or P1. You can close P2 or P3 incidents even if they have required tasks that remain open.
- Open findings

Procedure

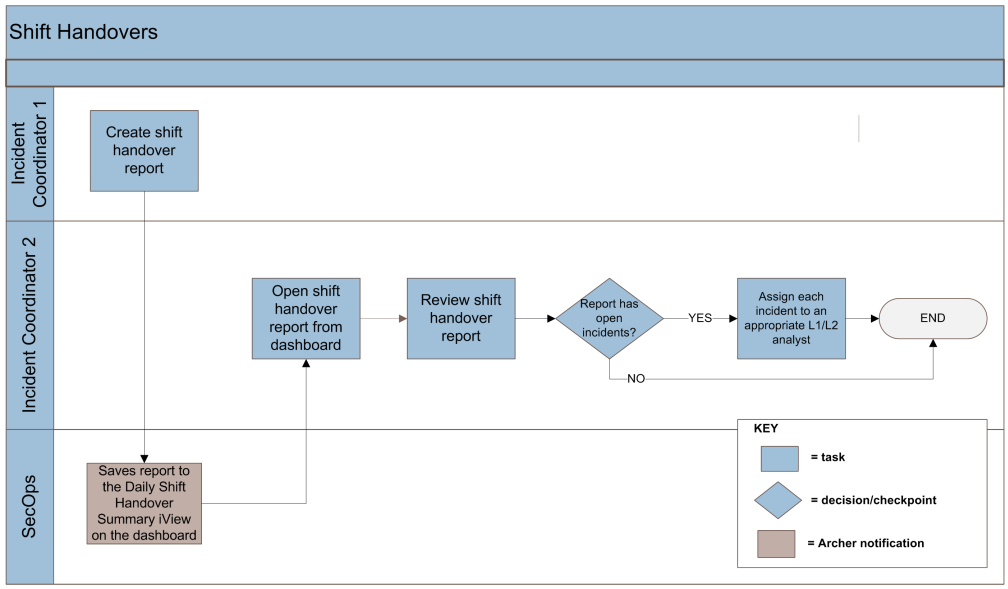
1. Open the incident record.
2. Change the Incident Status to Resolved.
3. Save the incident record.

Shift Handovers

If your SOC is manned 24x7 or has teams in multiple locations, the Incident Coordinator of each shift should create a daily shift handover report for the Incident Coordinator of the next shift. The shift handover report provides a summary of incidents closed, incidents that still require follow-up, and any other information that the next Incident Coordinator needs to take over incident handling coverage.

Shift Handover Workflow

The following diagram shows the process for creating and reviewing shift handover reports.



Create a Shift Handover Report

User: Incident Coordinator

Procedure

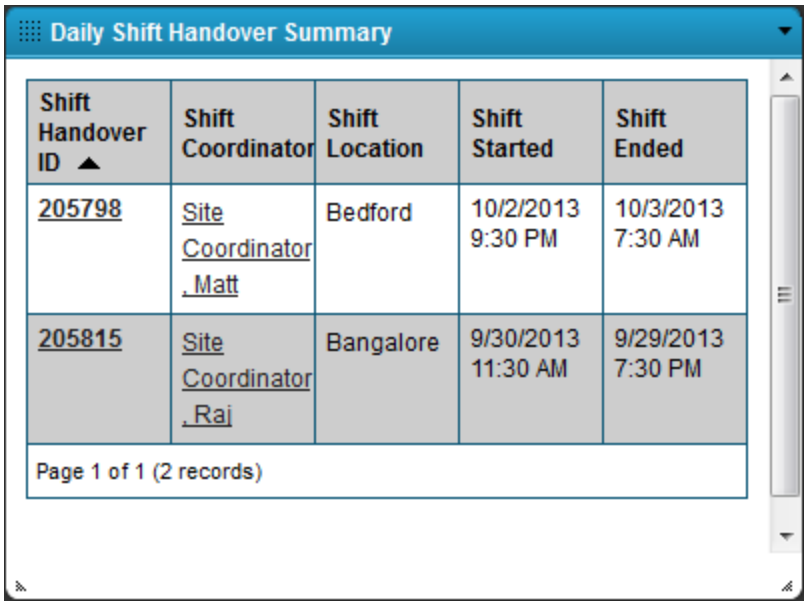
1. In the Security Operation Management solution, in the Navigation menu, click Shift Handover > Add New.
2. In the Shift Overview tab, fill out the shift location, coordinator, start and end times, and a summary of the shift.
3. In the Items Closed tab, add cross-references to any incidents or investigations that were closed during the shift.
4. In the Items for Follow Up tab, add cross-references to any incidents or investigations that remain open and should be picked up by the next shift.
5. In the Analyst Blogs tab, add any summary information about the shift, such as overall trends or information not specific to a particular incident.
6. Save the record.

Review a Shift Handover Report

User: Incident Coordinator

Procedure

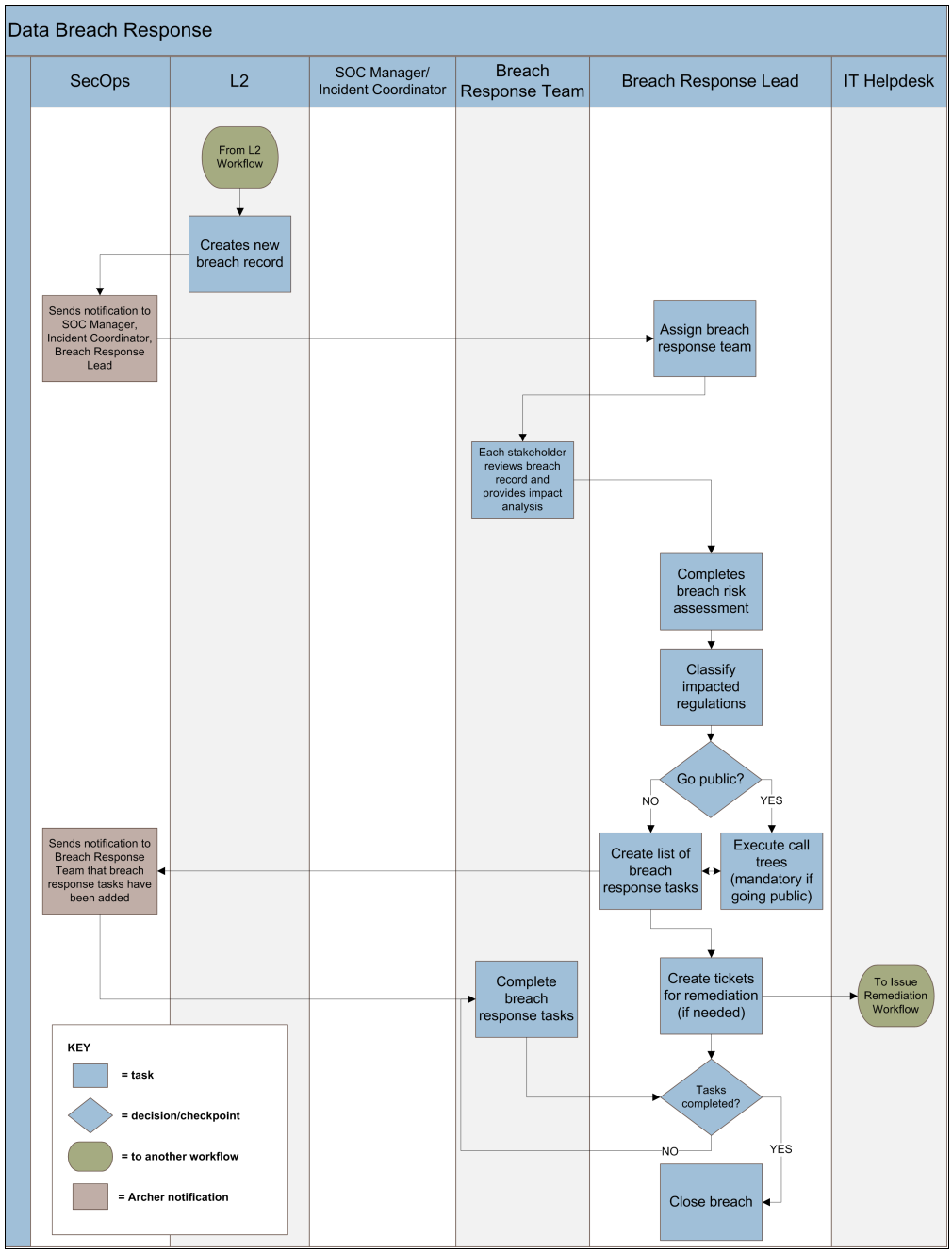
1. From the Security Operations Management workspace, and select the Incident Coordinator dashboard.
2. In the Daily Shift Handover iView, open the shift handover report that you want to review.



Chapter 5: Responding to Data Breaches

Data Breach Response Workflow Overview

The RSA Archer Security Operations Management solution is built to enable the following incident response workflow.



Note: Only notifications that are a key part of the workflow are included in the diagram. For a complete list of notifications, see the *Data Dictionary*.

Breach Response Lead

When an Incident Handler creates a breach record, they should assign a Breach Response Lead. The Breach Response Lead is the person who will be responsible for coordinating and managing the entire breach response process. Depending on the organization, the Breach Response Lead may be a Privacy/Compliance Officer, the CISO/CSO, a Legal Officer, or another user.

RSA recommends that you document your SOC policies about breach response, but especially who should be designated as the Breach Response Lead, so that the breach record creator knows who to assign in the event of a breach.

Breach Response Team

When a breach record is created. the Breach Response Lead should assign other members to the Breach Response Team, the cross-functional group whose impact analysis is required and who may help respond to the breach.

By default, only the SOC Manager, Incident Coordinator, CISO/CSO, the Incident Handler who identified the breach, and the assigned Breach Response Lead have access to the breach record. Any users who are assigned to the Breach Response Team (the Business Manager, Legal Analyst, Customer Support, Public Relations, Compliance/Privacy Officer, IT Manager, and Other Members fields) are also then granted access to the record.

Create a Breach Record

User: L1 or L2 Incident Handler, Incident Coordinator, SOC Manager

Procedure

1. Create a new record from any of the following locations:
   - In an incident or investigation record, click the Impact Analysis tab, and in the Confidentiality Impact Assessment section, click Add New.
   - In the Navigation Menu, click Data Breach Response > Data Breaches > Add New.
2. In the breach record, document the following in the Overview tab:
   - A name and description of the breach
   - The breach type
   - When the breach occurred
   - How and when the breach was discovered
   - Who reported the breach
3. Assign a Breach Response Lead.

4. Save the breach record.

   When you save the record, notifications are sent to the SOC Manager, all Incident Coordinators, and the Breach Response Lead to inform them that a new breach record has been created.

Document Data Disclosed and Assign the Breach Response Team

When a breach record is created, the Breach Response Lead should first document where the data was disclosed and assign members to the Breach Response Team.

User: Breach Response Lead

Procedure

1. In the data breach record, in the Data Disclosure tab, document the data disclosed and the disclosures by region:
   a. In the Data Disclosed section, click Add New and document the following:
      - The data type and format
      - The data loss vector
      - The total number of records disclosed
      - Whether the data was encrypted

      Note: You can only have one Data Disclosed record per data breach. If you need to document more than one type of data that was disclosed, you must create a separate breach record.

   b. Save the sub-form.
   c. In the Disclosures by Region section, click Add New and document each region in which data was disclosed and the number of records disclosed in each region.

      The location where the data was disclosed affects which regulations or privacy laws may have been impacted and what response you will need to take to remediate the breach.

   d. Save the sub-form.
2. In the Overview tab, assign users to the following roles:
   - Business Manager
   - Legal Analyst
   - Customer Support
   - Public Relations
   - Compliance/Privacy Officer

- IT Manager
- Other Members

3. Save the record.

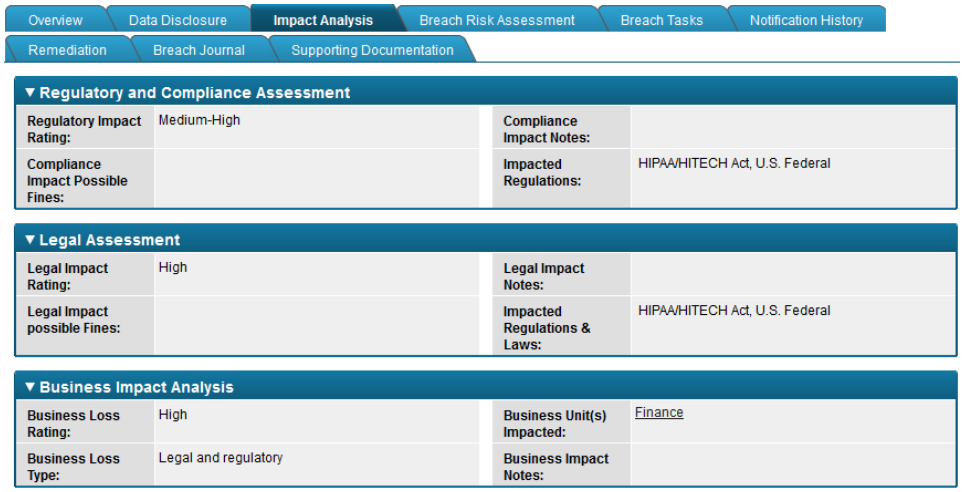
Provide Breach Impact Analysis

User: BU Manager, Compliance/Privacy Officer, Legal Counsel

When a breach record is created and saved, notifications are automatically sent to each member of the breach response team to inform them that they must review the breach record and provide an impact assessment.

Procedure

1. Open the breach record, and click the Impact Analysis tab.
2. Depending on your role, enter your analysis about the impact rating, possible fines, and your notes in the appropriate section.



3. Save the breach record.

   When all the required breach impact analysis is completed, all members of the breach response team are notified.

Complete a Breach Risk Assessment

Once all required reviewers have provided their impact assessments, you should perform a breach risk assessment.

User: Breach Response Lead

Procedure

1. In the breach record, click the Breach Risk Assessment tab.
2. In the Breach Risk Assessment section, click Add New.

3. Complete and submit the assessment.

   When you submit the completed assessment, the assigned Reviewer is notified that the assessment is ready for review. You are then notified when the Reviewer either approves or rejects the assessment.

   Based on the assessment results, the values in the Assessment Results section are then automatically populated.

Decide Whether to Declare a Breach

User: Breach Response Lead

Once all the impact analysis has been gathered and the breach risk assessments have been completed, you must decide whether to declare a breach.

Procedure

1. In the breach record, click the Breach Risk Assessment tab.
2. In the Assessment Results section, fill out the following:
   - Impacted Regulations. Select any regulations that have been impacted by the breach.

     Based on the regulations you select, any response procedures in the Breach Response Procedure Library that match that selected regulations will be copied into the Breach Tasks application and will appear in the Breach Tasks tab in the breach record.

     Note: If you later change the Impacted Regulations, any tasks that are no longer required are moved to the Not Applicable section on the Breach Tasks tab.

   - Declared Breach. Select Yes or No.
   - Notification Decision. Select whether to send a notifications to affected parties. If you decide to send notifications, you must execute and document those notifications in the Notifications tab.

Creating and Assigning Breach Tasks

User: Any Breach Response Team member

Anyone who is assigned to work on a breach can create and assign tasks that must be completed. Breach tasks can be created manually or they can be created automatically using the Breach Tasks data feed. If your Solution Administrator set up the data feed, when you select regulations impacted by the breach, any response procedures in the Breach Response Procedure Library that match those regulations are copied into the Breach Tasks application and are associated with the breach record.

Manually Create and Assign Breach Tasks

User: Any Breach Response Team member

Procedure

1. In the breach record, click the Breach Tasks tab.
2. In the Breach Tasks section, click Add New.
3. Assign an owner.
   The Task Owner will be notified that they have a new task to complete.
4. Save the breach task record.
5. Repeat steps 2 - 4 for all the tasks that need to be completed to close the breach.

Complete Breach Tasks

User: Any Breach Response Team member

Procedure

1. In the breach record, click the Breach Tasks tab.
2. Open any task that is assigned to you or which has your role assigned as the Target Analyst.
3. Complete and save the task record.

Executing a Call Tree

A breach task may require that you notify specific individuals or groups through email or phone. For example, if a breach needs to be made public, the Breach Program Lead may create a task to notify key stakeholders.

Execute a Call Tree

User: Any Breach Response Team member

Procedure

1. Open the breach record, and click the Notifications tab.
2. In the Notification Details section, click Add New.
3. Fill out the Notification Record.
4. If the notification is part of a documented call tree, you can associate the call tree record. In the Notification/Call Tree section, click Lookup and select the call tree. You can associate the notification with more than one call tree.

Log Issues for Remediation

User: Breach Record Creator, SOC Manager, Incident Coordinator

Procedure

1. In the Data Breaches record, click the Remediation tab.
2. In the Remediation Required field, select Yes.
3. In the Findings section, click Add New.
4. In the Findings record, do the following:
   a. Enter a name and description of the action that needs to be completed.
   b. Select a criticality for the finding.
   c. In the Source Override field, select Security Operations.
   d. In the Security Operations Response section, select a target queue and remediation task type.
   e. Save and close the Findings record.
5. Repeat steps 3 – 4 for each issue that needs remediation.
6. Save the breach record.

Close a Breach Record

User: Breach Response Lead

Once all the tasks associated with a breach have been completed, you can close the breach record.

Procedure

1. Open the data breach record, click the Breach Tasks tab, and verify that all associated required tasks have been completed.
2. Click the Overview tab, and change the breach status to Closed.
3. Save the breach record.

Chapter 6: Remediating Issues

Issue Remediation

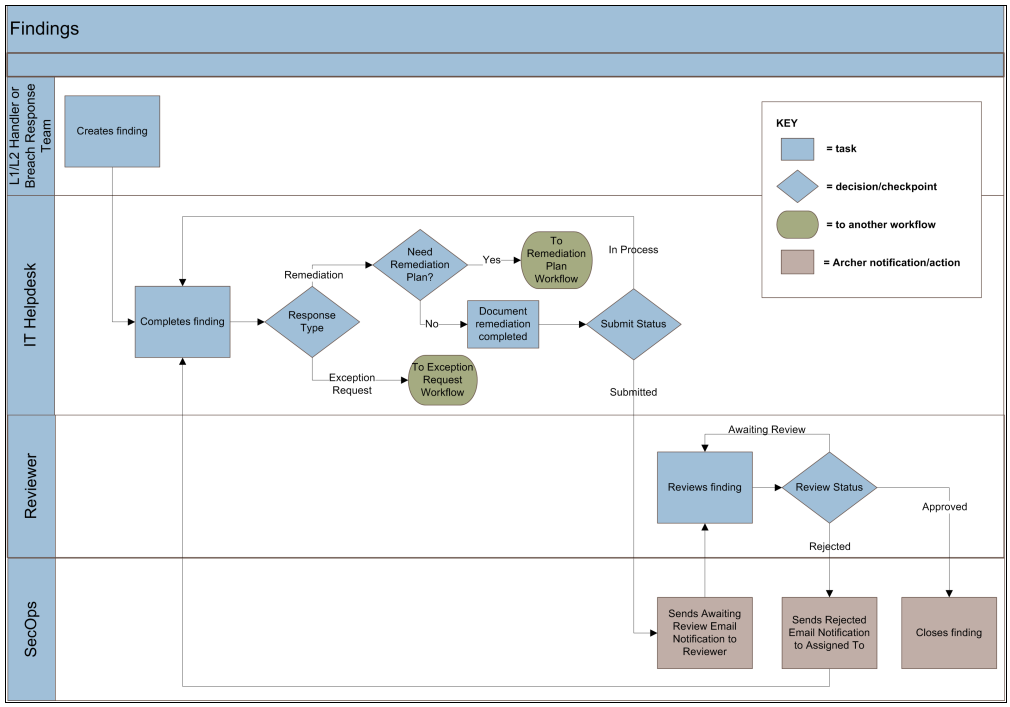
The Issue Management subsolution allows the IT Helpdesk Analyst to manage the remediation process for any tickets that are logged for remediation in the course of investigating a security incident or responding to a data breach. Tickets are logged as records in the Findings application, in which the analyst can document the remediation performed and track the ticket to closure.

For tickets that require more extensive remediation, you can create a Remediation Plan from the Finding. You can also tie multiple Findings to in a single Remediation Plan in order to track the remediation in a single location.

For tickets that cannot be remediated, you can create an Exception Request from the Finding to track and manage the risk of not performing the remediation.

Findings Process

The following figure shows the process of remediating a finding.



Resolve a Finding

User: IT Helpdesk Analyst

Procedure

1. In the IT Helpdesk dashboard, from the All Open Tickets iView, open a Finding to begin work on.
2. In the Assigned to field, assign yourself to the Finding.
3. Complete the work required in the Finding.
4. Click the Response tab.
5. In the Response field, select either Accept Risk or Remediate Risk.
   - If you select Accept Risk, **create a new Exception Request**.
   - If you select Remediate Risk, complete the Remediation section. If the necessary remediation is extensive, **create a new Remediation Plan**.

     Note: If you find that the Finding is not applicable or has already been remediated, select Remediate Risk and add an explanation in the Remediation Overview field.
6. Once all associated Exception Requests and Remediation Plans are closed, click the Workflow tab.
7. In the Reviewer field, assign a user to review the Finding.

You may want to assign the incident handler who created the ticket as the reviewer, but this may depend on the procedures of your organization and is not required.

8. Change the Submission Status to Submitted.
   The Review Status changes to Awaiting Review.
9. Save the record.
   A notification is sent to the assigned Reviewer to inform them that the Finding requires review.

Review a Finding

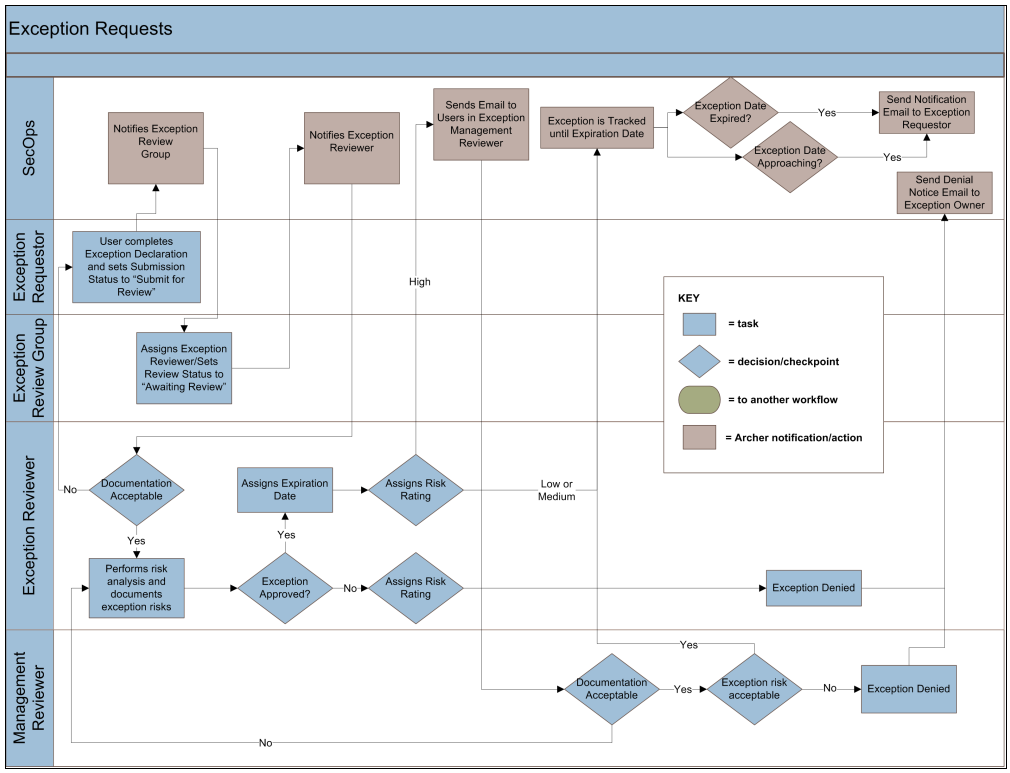
User: Finding Reviewer

Procedure

1. In the Finding record, review the work that was completed.
2. In the Review Status field, select either Rejected or Approved.
   - If you select Rejected, a notification is sent to the Finding owner to continue work on the Finding and resubmit it.
   - If you select Approved, the Finding is automatically closed.
3. Save the record.

Exception Request Process

The following figure shows the process of creating and reviewing an Exception Request.



Create a New Exception Request

User: Finding Owner

Procedure

1. In the Exception Request record, enter a description and business justification for the exception.
2. Change the Submission Status to Submit for Review.
3. Save the record.

   A notification sent to the Exceptions Review Group that there is a new exception request to review.

Assign an Exception Request for Review

User: Exception Review Group

Procedure

1. In the Exception Request record, click the Review and Approvals tab.
2. In the Reviewer field, assign a user to review the exception request.
3. Save the record.

Review an Exception Request

User: Exception Request Reviewer

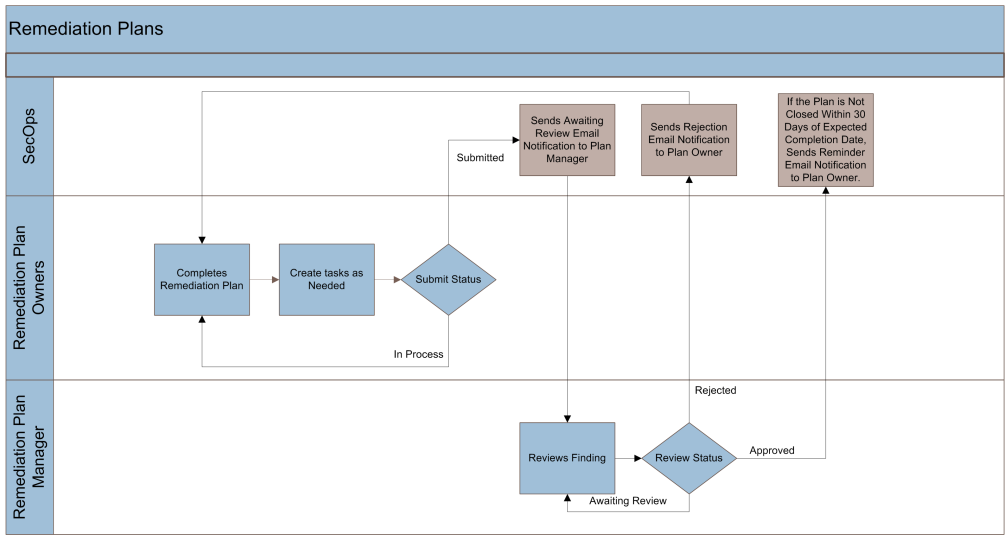
Procedure

1. In the Exception Request record, review the request and determine whether the documentation is acceptable.
   - If the documentation is not acceptable:
     a. Assign a risk rating.
     b. Change the Review Status to Denied.
   - If the documentation is acceptable:
     a. Perform risk analysis and document any risks the exception poses.
     b. Change the Review Status to Approved.
     c. Assign an initial expiration date.
     d. Assign a risk rating.
2. Save the record.
   If you assigned a risk rating of Low or Medium, the exception request is tracked until the expiration date.

   If you assigned a risk rating of High, a notification is sent to the management reviewer to determine whether the documentation and exception risks are acceptable.

Remediation Plans Process

The following figure shows the process of creating and reviewing a Remediation Plan.



Create a New Remediation Plan

User: Finding Owner

Procedure

1. In the Remediation Plan record, enter a name and description, and select a remediation type.
2. Assign either yourself or another user as the Remediation Plan Owner.
3. Assign a user as the Remediation Plan Manager.
4. Create and assign remediation tasks as necessary.
5. Enter an estimated cost, start date, and completion date for the remediation work.
6. Change the Submission Status to Submitted.
7. Save the record.

   A notification is sent to the Remediation Plan Manager to review the remediation plan.

   Important: Even though you have submitted the remediation plan, you must still complete the remediation work and update the record when it is complete.

Review a Remediation Plan

User: Remediation Plan Manager

Procedure

1. In the Remediation Plan record, review the plan, and in the Review Status field, select either Approved or Rejected.
2. Save the record.

   If you selected Approved, the remediation plan is automatically closed. A reminder notification is sent to the Remediation Plan Owner if the plan is not closed within 30 days of the expected completion date.

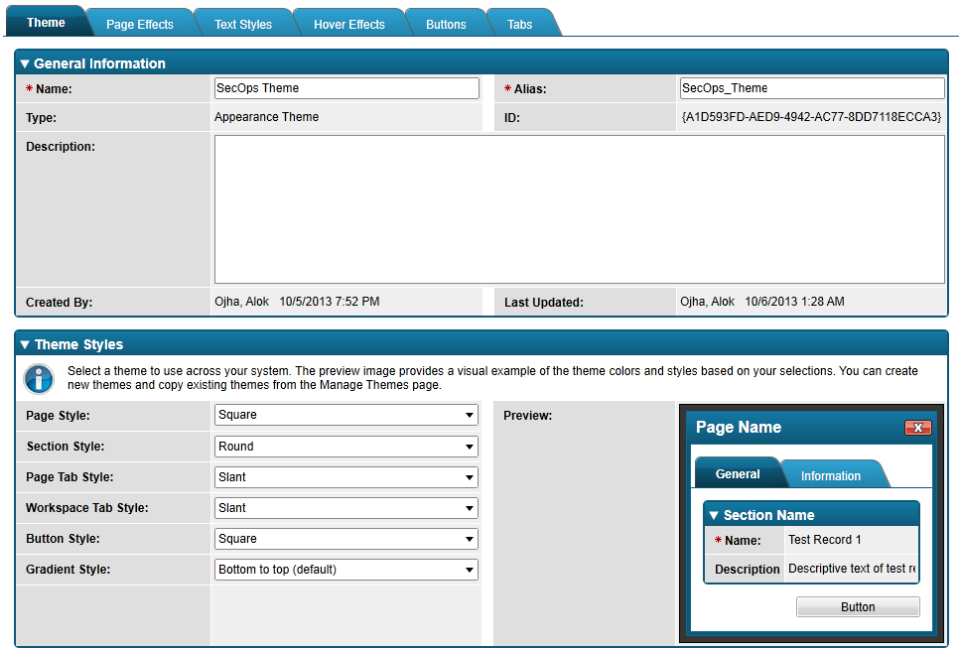
   If you selected Rejected, the Remediation Plan Owner is notified.

Appendix A: Configure the SecOps Theme

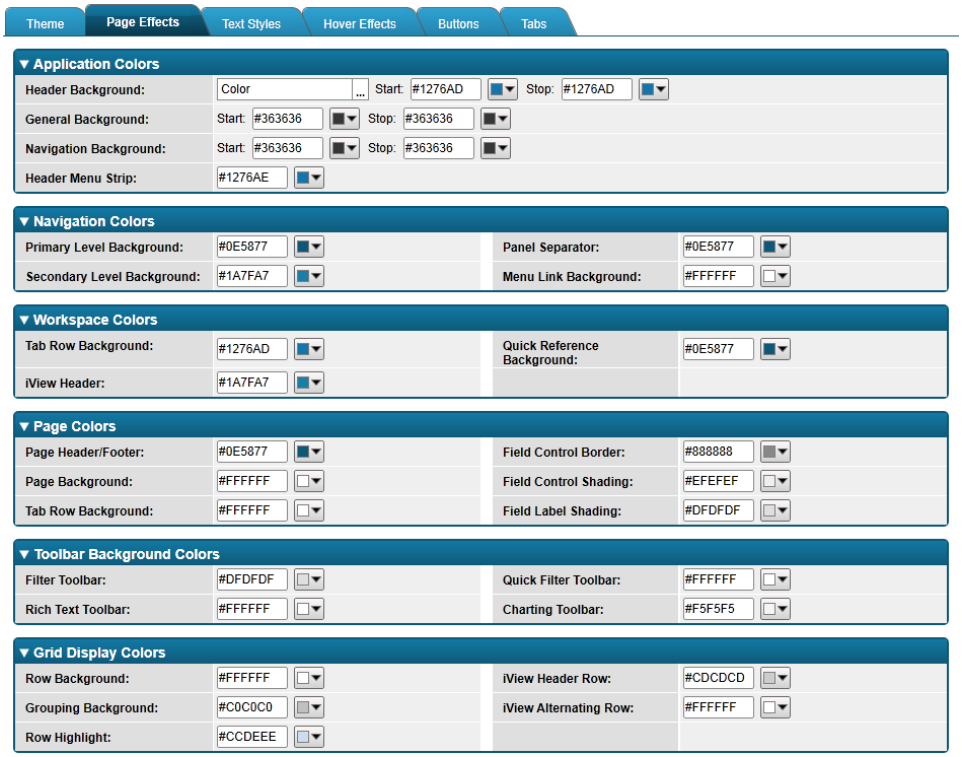
The screenshots in this guide show a UI configured with the SecOps theme. You can configure this in your own environment, if desired.

Procedure

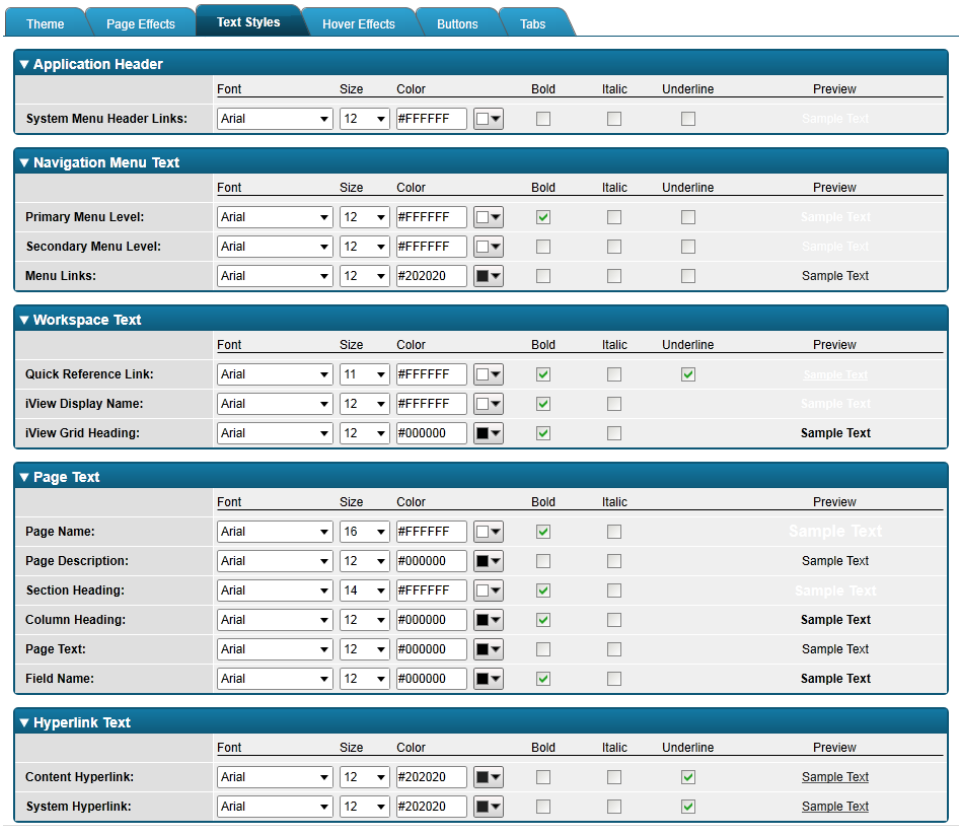
1. Click Administration > Appearance > Manage Themes.
2. Click Add New.
3. Ensure that Create a new theme from scratch is selected, and click OK.
4. On the Theme tab, select the following:



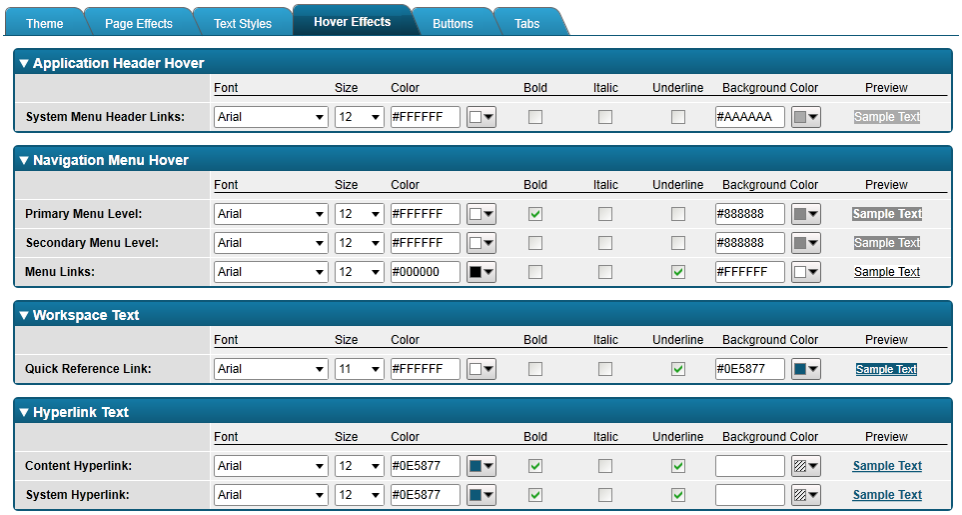
5. On the Page Effects tab, select the following:



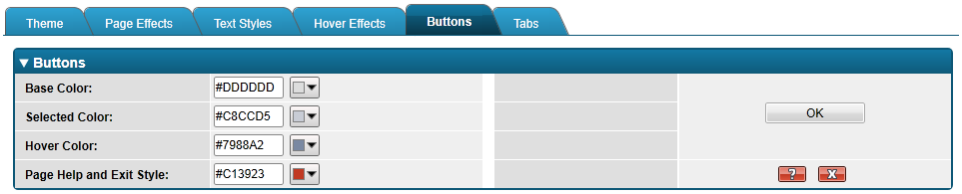
6. On the Text Styles tab, select the following:



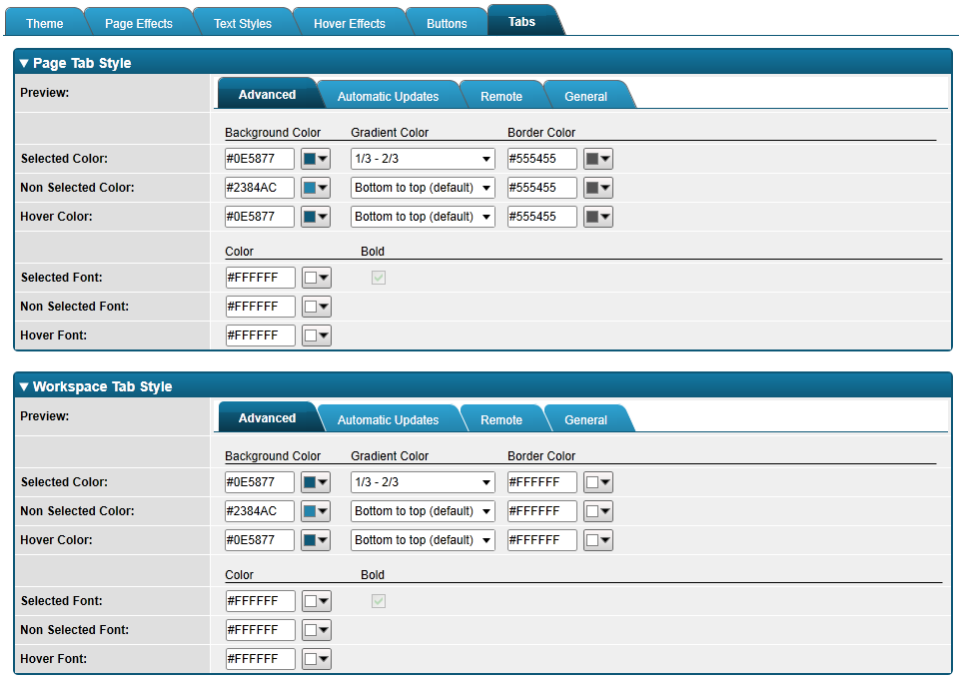
7. On the Hover Effects tab, select the following:



8. On the Buttons tab, select the following:



9. On the Tabs tab, select the following:



10. Click Save.
11. To select the new theme in your system:
    a. Click Administration > Appearance > Manage Appearance.
    b. In the Theme field, click ....
    c. Scroll to the SecOps theme, and click OK.
    d. Click Save.