The Most Comprehensive eBook on SOAR Use Cases.

Discover the 9 most common SOAR use cases to see how security orchestration, automation and response (SOAR) solutions can improve your security operations team’s efficiency by automating security operations workflows.
Contents

This document contains confidential and proprietary information for use only by DFLabs, SPA and its intended recipients and must not be disclosed to unauthorized individuals without prior, written consent.

Introduction 3
Phishing Attack 3
Insider Threat 4
Malicious File Download 6
Malicious Outbound Network Traffic 7
Compromised Internal Host in a Hybrid Environment 9
PII Breach Prevention 10
Industrial Security 13
Anti-fraud 15
Meltdown and Spectre Vulnerabilities 16
Final Thoughts 17
About Us 18
Introduction

A number of factors determine how using a Security Orchestration, Automation, and Response (SOAR) solution will affect use cases. Such factors include enterprise-specific internal environments, the vertical enterprises served, the industry, and even the legal and regulatory compliance that need to be met. This white paper will focus on 9 of the most common use cases for a SOAR solution. Specific attention will be placed on how utilizing this technology helps evade, detect, and prevent cyber threats and potential attacks without disrupting the workflow of the organization.

It's important to note that a use case is only limited by the organization’s creativity. Still, it’s natural to assume that a SOAR platform, such as IncMan SOAR from DFLabs, should be well-prepared and tackle every potential scenario and use case that is required.

1. Phishing Attack

This use case will demonstrate how to utilize IncMan’s integrations and R3 Rapid Response Runbooks to quickly alert the security team to a potential phishing attempt, triage any attachments, and take action to delete malicious attachments and reset the affected user’s password.

Goals

- Automatically receive potentially malicious email and extract attachments
- Evaluate the attachment and search for other instances of that attachment across the enterprise
- Gather user information for the affected user and system information for the affected host, including running processes
- Reset the victim’s password and send notification of the recent change to the account user

Integrations Used

- Exchange EWS
- Recorded Future
- Custom Scripts
- Email Notification
- Microsoft Active Directory

Implementation

The first step necessary to create an R3 Runbook is to outline how the organization will want to handle potential phishing emails. Before responding to any type of event an investigator must research aspects of the activity observed. This research is done through Enrichment tasks. These tasks will be based on the assumption that the incoming email contains the following information at a minimum:

- Recipient’s email address
- Email attachment
- Information Gathering & Enrichment

Before we can respond to a suspicious email we must first gather information regarding the email and its sender to determine how it should be handled. Our R3 Runbook will begin by searching the EWS instance for additional emails received from the sender and verify the existence of any attachments in the emails located.

Once we have queried for attachments our runbook will come to its first conditional argument. If there are attachments present, the R3 Runbook will check the attachment’s MD5 hash against two separate file reputation services. If either of those reputation services reports a risk score above a 50, our runbook will begin to take further containment and notification actions.

Containment & Notification

If the risk score has been confirmed to be above 50, the runbook will simultaneously delete the malicious attachments and query Active Directory for the affected user’s information. Armed with the affected user’s Active Directory information, our runbook will execute a custom script to generate a new random password for this user account. This newly created password will be set for our affected user account, we will force the user to reset their password upon next login, and a notification will be sent to the user containing these new login credentials.
Utilizing the R3 Rapid Response Runbook
Once the new R3 Runbook is created, IncMan must be told how and when to automate the use of this Runbook. This is achieved by creating an Incident Template, which will be used any time an incident is generated for a newly discovered vulnerability. Through this incident template, critical pieces of information such as Type, Summary, Category can be automatically applied to the newly created incident.

In addition to incident information, the Incident Template also allows R3 Runbooks to be automatically assigned and executed each time the incident template is used. Assigning the previous R3 Runbook to the Vulnerability Management Incident Template will cause the R3 Runbook to be automatically run for each matching incident. Finally, conditions must be set to indicate when IncMan should utilize the Exchange EWS Phishing Incident Template. In this use case, the Phishing Incident Template will be used to create an incident each time a potentially malicious email communication is forwarded from an organization’s user.

Solution in Action
When an email message is received from an organization’s user, IncMan will automatically generate a new incident based on the Exchange EWS Phishing Incident Template. Without requiring any action on the part of an analyst, the Exchange EWS Phishing Runbook is initiated, executing the Information Gathering and Enrichment, Containment, and finally the Notification sections automatically.

Summary
This use case frees up security teams from having to triage potentially malicious email communications submitted by their users and allows for their time to be better spent on tasks that require human intervention. The automated portions of this R3 Runbook can be executed in less than 60 seconds, orders of magnitude less than it would take an analyst to manually query all of these information sources. By automating responses to these malicious communications, it ensures our attackers would have less time to dwell in our environments and cuts them off at the pass preventing any lateral movement and further destruction or damage.

2. Insider Threat
This use case demonstrates how to use IncMan’s integrations and R3 Rapid Response Runbooks to quickly alert the security team to a potential insider threat, perform initial triage to determine the potential risk to the organization and create a helpdesk ticket to notify the team responsible for remediation.

Goals
• Automatically receive alerts regarding large data transfers from an organization’s Web server to an internal host.
• Perform initial triage of the destination host and associated user account to determine user’s risk score.
• Automatically elevate the priority of the suspected incident based on the user’s risk score and/or the observation of additional security alerts for the user account within a specific timeframe.
• Create a ticket to notify the teams responsible for vulnerability remediation.

Integrations Used
• Securonix
• Microsoft Active Directory
• Carbon Black Response
• IncMan SOAR
• Email Notification
• Implementation

Creating an R3 Rapid Response Runbook
The first step in creating an automated response to this type of event is to create an R3 Rapid Response Runbook which will perform Enrichment and Notification actions, as well as Containment actions if necessary. We will assume that the alert has provided the following information at a minimum:
• Source IP address
• Source name
• Destination IP address
• Destination name
• User account
• Information Gathering and Enrichment

This R3 Runbook begins by performing basic information gathering and enrichment of information provided by the original alert from Securonix. The source and destination IP address are parsed out and checked against Securonix asset lists. This information is then passed to the organization’s Active Directory service to gather data on the user’s attributes, associated groups, and to obtain the user’s risk score from Securonix.

Once this information is gathered the R3 Rapid Response Runbook comes to its first conditional statement. This conditional statement is evaluating the user’s risk score. If the risk score is either medium...
or high, the runbook will move into the escalation phase by escalating the incident’s priority to high. If the user’s risk score is low, the runbook will then query Securionx for additional alerts and events where the user or their workstation were involved. If additional alerts or events have been observed, the R3 Rapid Response Runbook will move into the escalation phase by escalating the incident’s priority to high.

**Escalation**
Prior to the escalation phase the R3 Rapid Response Runbook evaluates the user’s risk score to determine if the incident should be upgraded in priority or if more information needs to be gathered to make the determination. If the user’s risk score is either medium or high, the priority is adjusted, and a query is issued to Securionx to gather historical events and alert data regarding the user and their workstation. If additional security alerts have been observed, the incident is upgraded to critical priority before moving to the containment phase of the suspicious user activity workflow.

If the user’s risk score is considered low, the same query is issued to Securionx to determine if the user’s account or their workstation had been observed in any security events or alerts over the last 30 days. If the account has been observed in additional security incidents, the incident’s priority is upgraded and automatically moves into the containment phase of the runbook. If there are no additional alerts for the user or their workstation a user choice selection is issued. This user choice entry temporarily pauses the runbook to allow an analyst to review the initial alert, the user involved, and the actions the user had taken to determine whether they would like to proceed in containing the user or to exit the runbook without taking further action.

**Containment**
Once the R3 Rapid Response Runbook enters the containment phase of the workflow an additional conditional statement is evaluated to determine if containment actions are required. If it is found that containment actions are required, the runbook’s workflow follows four separate paths to determine what containment actions are appropriate.

The first path is executed if the initial user’s risk score was medium or high and additional security alerts were observed. After escalating the priority to critical, the host machine is quarantined by Carbon Black Protect, the user’s account is disabled in Microsoft Active Directory, and an email notification is sent out to the security team to follow up with the suspected user.

The second path is executed if the user account associated with the medium to high-risk score has not been observed in any additional security alerts the R3 Rapid Response Runbook disables the user’s account in Active Directory and an email notification is sent out for the security team to investigate.

The third path is executed if the user’s risk score is low and they have been observed in additional security alerts over the last 30 days. After the priority of the incident is elevated to high, the user account is disabled in Active Directory and an email notification is sent out to the security team for further remediation efforts. The final path is followed if the user’s account has a low-risk score and has not been involved with any additional security alerts in the last 30 days.

If this path is taken the R3 Rapid Response Runbook issues a user choice selection before a containment action is taken. The user choice selection temporarily pauses the runbook and allows an analyst to review all the evidence that has been collected for the potential incident. Depending on the findings the analyst will choose whether or not containment activities are warranted. If the analyst decides to take containment actions against the observed activity, the runbook will disable the user’s account and allow the security team to follow up with remediation activities. If the analyst decides that containment actions are not needed the runbook will be unpaused and exit.

**Utilizing the R3 Rapid Response Runbook**
Once the new R3 Runbook is created, IncMan must be told how and when to automate the use of this Runbook. This is achieved by creating an Incident Template, which will be used any time an incident is generated for a newly discovered vulnerability. Through this incident template, critical pieces of information such as Type, Summary, Category can be automatically applied to the newly created incident.

In addition to incident information, the Incident Template also allows R3 Runbooks to be automatically assigned and executed each time the incident template is used. Assigning the previous R3 Runbook to the Suspicious User Activity Incident Template will cause the R3 Runbook to be automatically run for each matching incident.

Finally, conditions must be set to indicate when IncMan should utilize the Suspicious User Activity Incident Template. In this use case, the Suspicious User Activity Incident Template will be used to create an incident each time an event is received from the organization’s endpoint detection system.
Summary
This use case allows the security team to be automatically notified each time an event is observed where a large data transfer has taken place. By automating this type of alert, they will help to reduce the time between detection and response for this type of activity, helping to prevent a potentially serious data breach.

The automated portions of this R3 Runbook can be executed in less than 60 seconds, orders of magnitude less than it would take an analyst to manually query all of these information sources. In addition, this R3 Runbook allows security managers to codify what criteria is indicative of a large data transfer event and what criteria may be grounds for immediate isolation until a mitigation can be completed. This allows for an effective, efficient, and consistent security response to any new attempt to transfer data both internally and externally to the company.

3. Malicious File Download

The purpose of this use case is to demonstrate how to utilize IncMan SOAR’s integrations and R3 Rapid Response Runbooks to quickly detect and respond to threats targeting an organization’s endpoints. This use case will combine advanced endpoint detection capabilities with automated workflows to gather additional evidence and take containment actions across the network.

Goals
• Automatically gather incident evidence from endpoint and network-based tools
• Evaluate incident evidence to make automated response decisions
• Adjust incident priority based on incident findings
• Take containment actions against potential attackers
• Create tickets for responsible parties to take manual action where necessary
• Integrations Used
  • Cisco AMP for Endpoints
  • DomainTools
  • Splunk
  • Cisco Umbrella
  • Jira
• Implementation

Creating an R3 Rapid Response Runbook
When creating an R3 Rapid Response Runbook within the IncMan SOAR platform, the first task is usually to perform enrichment actions that are built into the automation process. For the “Malicious File Download Use Case,” we will assume the alert contains the following information:
• Source Address
• Destination Address
• SHA-256 File Hash
• Domain Name

This R3 Runbook can be broken down into three main sections: information gathering and enrichment, escalation, and containment.

Information Gathering and Enrichment
Upon receipt of a malicious download event, IncMan will kick-off the Malicious File Download Runbook. The Runbook begins by pulling information from Cisco AMP for Endpoints regarding the current activity observed from the victim machine, as well as any other host activity that may have interacted with the malicious file or domain in question.

Next, the R3 Runbook will query DomainTools to gather domain reputation information on the potentially malicious domain. Once this information is gathered, the R3 Rapid Response Runbook will split off into two separate conditional statements which will determine how the automated workflow will continue.

Escalation and Containment
This R3 Runbook examines the previously enriched information for one of the following conditions:
• Are there additional hosts that interacted with the malicious file in the past 30 days?
• Does the domain visited have a negative reputation score?
• If the visited domain has a negative reputation score, have any additional hosts visited this domain in the last 30 days?

If any of these conditions exist, the incident priority will automatically be updated to a high priority incident and any additional hosts will be added to the incident as an incident artifact. This will be followed by creating a new helpdesk ticket through the organization’s ticketing system to alert the responsible teams that an incident has occurred.

Finally, the organization’s SIEM will be queried for any alerts that have been generated by the vulnerable host in the recent past. If none of these conditions exist, this R3 Runbook will conclude, without alerting the security team to the false positive event. If any of the criteria in the Escalation section were met, this R3 Runbook will issue a containment action.
associated with the condition being evaluated. If the file which was downloaded is found to be malicious, it is automatically added to the block list created in Cisco AMP.

Finally, if the domain where the file was downloaded from is also found to be malicious or have a negative reputation score, IncMan will automatically block the domain using Cisco Umbrella. Once these containment and escalation actions have been executed the R3 Runbook will conclude.

**Utilizing the R3 Rapid Response Runbook**

When the new R3 Runbook is created, IncMan must be told how and when to automate the use of this Runbook. This is achieved by creating an Incident Template, which will be used any time an incident is generated for a potentially malicious download. Through this Incident Template, critical pieces of information such as Type, Summary, and Category can be automatically applied to the newly created incident.

In addition to incident information, the Incident Template also allows R3 Runbooks to be automatically assigned and executed each time the incident template is used. Assigning the previous R3 Runbook to the Malicious File Download Incident Template will cause the R3 Runbook to be automatically run for each matching incident.

Finally, conditions must be set to indicate when IncMan should utilize the Malicious File Download Incident Template. In this use case, this Incident Template will be used to create an incident each time a syslog message is received from the organization’s endpoint detection system.

**Summary**

This use case allows the security team to be automatically notified once a potential incident has been confirmed as valid, preventing valuable time from being wasted by analysts triaging an event. The automated portions of this R3 Runbook are executed in less than 60 seconds, which is exponentially faster than the time an analyst would need to spend querying and evaluating incident evidence to determine validity. This R3 Runbook also will allow security teams to identify poorly executed rulesets which will provide insight on what aspects of these rulesets must be adjusted to eliminate false-positive alerting.

**4. Malicious Outbound Network Traffic**

This use case demonstrates how to use IncMan’s integrations and R3 Rapid Response Runbooks to quickly respond to an alert indicating potentially malicious network traffic originating from an internal host, destined for an unknown host on the Internet.

**Goals**

Automatically receive alerts for potentially malicious outbound network traffic from a device such as a web gateway or IDS/IPS, create an Incident and perform automated Notification, Enrichment and Containment tasks assess and mitigate any potential risk to the organization.

**Integrations Used:**

- Cisco Threat Grid
- Hacker Target
- McAfee Web Gateway
- PostgreSQL
- VirusTotal

**Creating an R3 Rapid Response Runbook**

The first step in creating an automated response to this type of incident is to create an R3 Rapid Response Runbook which will perform Enrichment, and if necessary, Containment actions as part of the response. We will assume that the alert has provided a minimum of a source IP address and a destination IP address, although the alert will likely contain much more detailed information. The specific integrations used in this use case could easily be replaced with other similar technologies already deployed in the organization.

The Runbook begins by performing several basic information gathering Enrichment actions; IP Geolocation, a WHOIS query and a reverse DNS query. In this case, this information is not used as part of the automated decision-making process (although it easily could be). Instead, this information will be automatically saved as part of the Incident and will be available to the security analyst to review at any time. Following these basic information gathering
Enrichment actions, additional Enrichment actions are utilized to query two different threat reputation services. In this case, we have chosen to use both VirusTotal and Cisco Threatgrid, although IncMan also has integrations with several other threat reputation and intelligence services, such as Recorded Future and ThreatConnect.

Following each of these two queries, an automated decision point is reached. These automated decision points will examine the information returned by each threat reputation service and determine if the results meet a certain user-defined threshold. This user-defined threshold could be based on any of the information returned by each service, such as the overall threat score or the number of records returned.

If neither threat reputation service returns information that meets or exceeds the user-defined thresholds, no further automated actions will be taken and the information will be saved as part of the Incident and will be available to the security analyst to review at any time.

If either threat reputation service returns information which meets or exceeds the user-defined thresholds, the Runbook will continue by performing a query of the IT asset inventory using a PostgreSQL Enrichment action. Like the previous basic information gathering Enrichment actions, this information will not be used directly for automated decision making; however, it will also be available to the security analyst to review as part of the Incident record.

The final Enrichment action utilizes the same PostgreSQL integration, this time to query a database of known-good, or whitelisted hosts to see if the external destination IP address matches a known-good host. This assumes that the organization has pre-populated the table with the IP addresses, hostnames and other information regarding hosts which are known to be non-malicious or should not be blocked for one reason or another.

Following this final Enrichment action, another automated decision point is reached. This decision point will determine if the query of the known-good host database yielded any results. If the external destination IP address matches a known-good host, the runbook will conclude without further actions. If no matches were found, a special type of decision point will be reached; a User Choice decision. A User Choice decision will temporarily halt the automatic execution of the Runbook and will prompt the security analyst to make a manual decision. In this case, the security analyst is prompted with the question “Would you like to block the destination IP address?” While the Runbook is temporarily paused, the security analyst has the opportunity to examine the results of all the previous Enrichment actions as part of the manual decision-making process. This step is entirely optional, however, adds an additional layer of assurance that the blocking the destination IP address will not result in adverse consequences. Once the security analyst makes a decision and selects the appropriate option, the automated execution of the Runbook will continue.

If the security analyst determines that the destination IP address should not be blocked, the Runbook will conclude without further action. If the security analyst determines that the destination IP address should be blocked, a Containment action will utilize IncMan’s integration with McAfee Web Gateway to block the address. Following this Containment action, the Runbook will conclude.

Utilizing the R3 Rapid Response Runbook

Once the new Runbook is created, IncMan must be told how and when to automate the use of this Runbook. This is achieved by creating an Incident Template, which will be used any time an incident is generated for potentially malicious outbound network traffic. Through this incident template, critical pieces of information such as Type, Summary, Category can be automatically applied to the newly created incident.

From the Runbook tab of the Incident Template wizard, the previously created Malicious Outbound Traffic Runbook is selected and set to autorun. Each time this template is used to generate an incident, the appropriate information such as the source and destination IP addresses will be used as inputs to the Runbook and the Runbook will be automatically executed.

In this use case, an alert received from a simulated web gateway is used to initiate automatic incident creation within IncMan. However, a SIEM integration or email could also be utilized to achieve the same outcome. A new syslog Incoming Event Automation rule is added and the defined action is to generate a new incident from the previously created Malicious Outbound Traffic Incident Template.

Summary

When a syslog message matching the criteria pre-defined for the detection of malicious outbound network traffic, IncMan SOAR will automatically generate a new incident based on the Malicious Outbound Traffic Incident Template.

Without requiring any action on the part of an analyst, the Malicious Outbound Traffic Runbook is automatically initiated, performing the Enrichment actions and pausing at the User Choice decision point. At this point, the security analyst has the opportunity to review all of the information gathered from the previous
This use case will demonstrate how to use IncMan SOAR’s integrations and R3 Rapid Response Runbooks to quickly gather incident data from across diverse hybrid-cloud environments to provide incident responders with the evidence necessary to rapidly prioritize and respond to a potential incident.

Goals

- Automatically gather incident data from both on-prem and cloud environments
- Perform initial triage of the host to determine the potential risk to the organization
- Isolate a compromised user account
- Create a ticket to notify the teams responsible for response efforts

Integrations Used

- Carbon Black Response
- AWS Security Hub
- Splunk
- Microsoft Active Directory
- BMC Remedy

Creating an R3 Rapid Response Runbook

The first step in creating an automated response to this type of event is to create an R3 Rapid Response Runbook within the IncMan SOAR platform which will perform Enrichment actions, as well as Containment actions if necessary. We will assume that the alert has provided the following information at a minimum:

- Source IP Address (internal)
- Source Name
- Destination IP Address
- Information Gathering and Enrichment

This R3 Runbook begins by simultaneously gathering enrichment data from across the AWS cloud environment, the internal environment via the SIEM architecture, and from the internal endpoint solution. IncMan first queries AWS for all findings where the destination IP address has been observed within the last month. At the same time, the SIEM and endpoint solution is queried for internal activity towards the victim IP. Additional security events involving the user account, and the system settings which include running processes are also gathered for investigation.

After enriching the initial information, this R3 Runbook comes to a series of conditional statements which will dictate how the Runbook will finish its sequence. The first set of conditional statements looks for additional security alerts involving either the source of the incident, or the victim machine housed in the AWS cloud.

The second conditional statement looks for additional security alerts involving the potentially compromised user account. Upon evaluation of these statements IncMan will begin to initiate additional actions based on their findings.

5. Compromised Internal Host in a Hybrid Environment

Enrichment actions, including the information returned from VirusTotal.

In this case, VirusTotal has returned dozens of results matching the destination IP address. Based on this information, the security analyst has determined that blocking the destination IP address is the appropriate action and approves the User Choice decision. At this point, the automation continues and the McAfee Web Gateway Containment action is executed before the Runbook execution concludes.

This entire process, from receipt to containment, has taken place in a matter of minutes, likely before a security analyst would have been able to even manually acknowledge the alert under normal circumstances. IncMan’s automation and orchestration functions automated the initial response and provided the security analyst with all the information necessary to make an informed decision and contain the threat immediately.

Escalation and Containment

If the first conditional statement finds that additional alerts involving the source are found, IncMan will gather details on the system’s settings and its running processes. After this information is gathered, the R3 Runbook is paused and issues a User Choice action. A User Choice action is used when information is gathered that cannot be automatically verified and requires an analyst to review before continuing its execution.

Once the incident data is reviewed, the analysts will have to decide whether the data gathered presents enough evidence to determine whether an incident has occurred. If the evidence proves that further response efforts are necessary, the analysts will select to proceed and the R3 Runbook will upgrade the incident priority to high, quarantine the potentially infected internal host, and send an email notification to the response teams to let them know that a potential incident has occurred.

Simultaneously the second conditional statement is evaluated, and if there are additional security events
revolving around the user’s account, the R3 Runbook executes an additional Runbook to disable the account and reset its password. This nested Runbook will gather user account details from Active Directory, execute a custom script to generate a random password, reset the user’s password, and send an email notification to the security team to inform them of the potentially compromised credentials.

**Utilizing the R3 Rapid Response Runbook**

Once the new R3 Runbook is created, IncMan must be told how and when to automate the use of this Runbook. This is achieved by creating an Incident Template, which will be used any time an incident is generated that matches the incident condition. Through this incident template, critical pieces of information such as Type, Summary, Category can be automatically applied to the newly created incident.

In addition to incident information, the Incident Template also allows R3 Runbooks to be automatically assigned and executed each time the Incident Template is used. Assigning the previous R3 Runbook to the Compromised Host Incident Template will cause the R3 Runbook to be automatically run for each matching incident.

Finally, conditions must be set to indicate when IncMan should utilize the Compromised Host Incident Template. In this use case, the Compromised Host Incident Template will be used to create an incident each time a syslog message is received from the organization’s endpoint detection system.

**Summary**

This use case allows the security team to be automatically notified each time an alert is triggered indicating a potentially compromised host. The automated portions of this R3 Runbook can be executed in less than 60 seconds, which is far less time than it would take an analyst to manually query all of these information sources. In addition, this R3 Runbook allows security managers to codify what criteria is indicative of a potential high priority incident which must be addressed immediately, and what criteria may be grounds for false positive notification and can be discarded. This allows for an effective, efficient and consistent security response to each newly identified security incident.

6. PII Breach Prevention

This particular use case will pertain to privacy breaches. Over the past couple of years we have experienced some of the greatest PII breaches in modern history. Aside from the financial loss, the victims have had their personal information and privacy exposed to the world for monetary reasons. Such information includes social security numbers, home addresses, emails, credit card numbers, login information, and access to bank accounts.

This type of information is referred to as Personally Identifiable Information (PII). Additionally, when a hospital or healthcare system has been breached all of the information blended with that is termed Protected Health Information (PHI). Both PII and PHI are often sold on the black market and can be very lucrative. Thus, one of the many reasons as to why PII breaches are so prevalent within the theme of cybersecurity attacks.

**Use Case: PII Breach - Hypothetical Scenario**

We will break down and explain different phases of the attack, numerous tools that are used within those phases, and why Advanced Persistent Threats (APTs) of this nature go unnoticed for so long.

There are a significant number of other methods that can be used to gain access into a computer system in order to own the infrastructure. This spans way beyond the scope of this use case but just to name a couple for informational purposes, these might include:

- Unpatched Assets with Multiple Vulnerabilities for Exploitation
- Insider Threats (Intentional & Non-Intentional)
- Social Engineering Tactics & Phishing Campaigns
- Poorly Written Programs/Applications Containing Vulnerabilities

**Malware Embedded Pop-Ups & Adware**

Henceforth, we will render a few basic security measures that if implemented would prevent 99% of the large-scale breaches and cybersecurity attacks that we witness every day. Additionally, we will illustrate how specially crafted runbooks are developed to address these types of attacks in DFLabs’ IncMan SOAR solution. Moreover, we will indicate how IncMan SOAR supports defensive and offensive security measures in an autonomous manner, eliminating the need for continuous human intervention and oversight, which in turn eliminates a lot of remedial tasks and frees your security teams and resources to focus on other important tasks.
Use Case: PII Breach Objectives

- Confirm that an actual PII Breach has occurred and if so determine the scope, severity and amount of information disclosed.
- Document and log all events and actions for the Post-Incident After Action Report (AOR).
- Verify the TTPs' that were used by the threat actor to identify the vulnerabilities in the network.
- Illustrate how IncMan SOAR's Runbooks play a vital role in minimizing the impact of the breach.
- Contain and isolate all recognized infected systems assets.
- Eradicate and remediate all malicious content from compromised assets.
- Prepare public/employee statements and work with the legal and public relations departments for further actions.
- Conduct post-incident processes such as modifications of the company's PII Breach policies, debriefings, and lessons learned.

Security Tool Integrations Used for PII Incident Response Breach

The tools listed below that will be used in this hypothetical scenario are for training purposes only. There exists no partiality among these tools aside from the fact that IncMan SOAR's integration capabilities are directly partnered with these products and services. Seemingly, the tools chosen for this scenario remain very popular within the cybersecurity industry.

These are the specific security tools that are used by the breached organization within their Information Security Department and Security Operations Center. IncMan SOAR guarantees that these devices are fully integrated and are being employed to their greatest potential to provide optimal security measures.

- ServiceNow
- Cisco Threat Grid
- IBM X-Force
- Tenable
- Splunk
- Carbon Black Defense
- FireEye
- McAfee Web Gateway
- Carbon Black Response

PII Breach Runbook

The Runbook defines what specific tools, actions, logical decisions, and automation capabilities will occur during an incident. Below you'll find the entire PII Breach Runbook from start to finish with all of the included stages needed to remediate a compromise.

Notification

Communication and Notification of an incident are incredibly important. We will be using ServiceNow to create an initial ticket to permit those that have access to that ticket to provide continuous updates on the current incident. Additionally, an email will be drafted and sent to various stakeholders, key individuals, and distribution groups like incident response teams. Microsoft Outlook will be the application used for email creation distribution.

Enrichment

During the Enrichment portion, we will be validating the compromise assuring that it is not a false positive. Reputation checks of potentially malicious IPs, URLs, and Domain Names will be conducted by IBM X-Force and Cisco Threat Grid. This will be able to provide us with intelligence about any type of malicious command and control servers that might be being used as a means to store the data that has been excavated outside of the company's network. It will also be essential to initiate a scan on the network assets to determine any abnormalities on the host or other systems assets such as suspicious open ports, unauthorized executables and applications, and rogue user or administrative accounts.

If there is a particular asset in question that may support indications of already being compromised, a special scan of system processes will be conducted through the use Carbon Black Defense. Moreover, Splunk, which is the company's primary Security Information and Event Management (SIEM) tool will generate a report of the last six months to identify any abnormalities and behaviors, especially those associated with data exfiltration.

Once all of the scanning has been completed the reports are available for review and the information will be provided to the appropriate personnel. Analysis of the reports will support the decision on whether or not to follow through with the incident response lifecycle. Additionally, if it turns out to be a false positive it will not warrant any further action.

If it is not a false positive and it is an actual breach, then we will continue with the rest of the incident response process. In this case all of the indicators of compromise have validated that it is in fact a breach and the rest of the incident response portion will continue.
Containment
If the reports generated by the scans and the other intelligence gathered on the incident during the enrichment phase validate that the incident is in fact a true compromise, the containment portion is now enacted. There will be a host of tools and actions to follow that will be necessary to promote a successful triage process. If a company has pre-develop policies and procedures this aspect should run rather smoothly. Additionally, relying on the Runbooks and the documentation associated with each step will be incredibly valuable in eliminating the need for any second-guessing on what procedures to follow. Now that the incident response team has identified the infected host, it will be mandatory to quarantine it among the rest of the network assets. Once segregation has occurred, all running processes on the host will be terminated and a snapshot of the current state of the asset must be obtained. Generating a snapshot of the infected host for forensics purposes is essential to understanding the TTPs utilized by the threat actors.

After the asset image has been obtained, the forensics tools will be determined if it is necessary to reimaging the entire assets. While this process is taking place the company’s security operation center will also blacklist all malicious Domain Names and IP addresses via McAfee’s Web Gateway. Additionally, all users of the network that have Active Directory and email accounts will be required to perform a password reset. Because of the nature of the attack type, threat actors will often create administrative accounts to elevate their privileges to gain access to restricted material. This is why it will be necessary to temporarily disable administrative accounts to perform an audit on all users with administrative rights. After the forensic images have been captured and the host have been reimaged and all malicious content and artifacts have been removed, it will now be time to transition into the final phase of Recovery.

Recovery
At this point, the containment phase has been completed and all compromised assets have been remediated. Any host needing reimaging has been completed and all users requiring password resets have been done. As part of the triage process, the scanning of network assets will begin again to validate that infected hosts are in fact remediated fully. Once the scanning reports validate full remediation the assets can now be reintroduced into the network. This also includes reopening necessary ports for business and reinitializing services. Additionally, the original incident ticket created in ServiceNow will be updated and remain open to allow for post-incident information inclusion.

PII Breach Runbook
A properly developed Runbook is considered one of the most important aspects to successful remediation. In linear fashion, it explicitly details each step in a systematic manner for each phase of the incident response lifecycle. Below you will find the runbook developed specifically for a PII Breach. Some of the steps within the categories are universal and can be applied to many runbooks. There are also multiple steps specific to this compromise. We will not be going into depth on every single step for each stage of the incident response Runbook but will summarize and highlight the key points that should be taken into consideration.

Preparation
It is during the preparation phase of the incident response process that identifies each and every aspect of the steps necessary to achieve a successful end-to-end recovery. Preparation is the first stage of the program and it is by far the single most important aspect of the incident response lifecycle. It is during this stage that policies, documentation, and procedures are drafted, reviewed and practiced. Specifically concerning the current PII Breach, it will be quintessential in thoroughly reviewing the specific policy on PII Breaches pertaining to the company. It will also be an essential time for all necessary stakeholders, executive staff, incident response teams, and any other individuals that are relevant to the situation. The primary means of communication will be through email chains and via ticketing systems such as the one used in this scenario ServiceNow.

Detection
Moving from the preparation to the detection phase there will be multiple actions that will occur. This is where enrichment actions pertaining to the portions of the Runbook can be validated and cross-referenced with other types of threat intelligence reputation feeds. Being able to successfully validate IP addresses, Domain Names, Geolocations, and infected assets provide the needed information to guarantee that the artifacts and indicators of compromise are in fact malicious.

Analysis
During the analysis phase we can take all of the information that has been gathered from the logs, along with all of the intelligence data obtained on the artifacts for incident review. This is a very important aspect of the incident response lifecycle because if the information provided turns out to be a false positive the entire compromise will be finalized and no further actions will be taken. If it turns out to be an actual incident then processes associated with prioritization and criticality will take hold and various
types of matrices shall be created.

**Containment**

After the analysis phase is complete, the containment of the compromise is to follow. During this stage a multitude of actions will take place, such as isolating the compromised host, requiring users to reset their passwords. The purpose behind this is to ensure that the threat actor that has invaded the system will no longer have their user credentials to traverse through the system. Additionally, it will be necessary to block certain IPs and Domain Names that are associated with the incident.

**Eradication**

The eradication portion will conduct certain actions to facilitate in eliminating all malicious artifacts associated with the compromise. This will include reimaging the compromised asset if necessary and performing forensics operations on any other network assets that may have been subject to the attack. It will also be necessary to run another network scan to validate that all remediation on the compromised assets are in fact clear of any residual malicious content.

**Recovery**

The actions of the recovery phase are very similar to that of the eradication phase in the sense that certain remediation actions go hand-in-hand. For instance, once the compromised assets have been reimaged they will have their network and port configurations reset and introduced back into the environment. Moreover, an important aspect about the recovery phase is that all of the status reports of all the phases will be accumulated and prepared for the next phase which is the lessons learned phase.

**Lessons Learned**

The lessons learned phase could be considered one of the most important aspects of the incident response lifecycle. It is here that all of the documentation and information is stored, reviewed, and used for lessons to be learned. Oftentimes the outcome of the lessons learned phase will result in certain company policies being modified or network systems that may need to be reconfigured, to prevent the possibility of a future compromise such as the one experienced.

---

**7. Industrial Security**

The goal of this use case is to demonstrate how IncMan’s integrations and R3 Rapid Response Runbooks quickly alert the security team about potential cyber threats. In this process, SOC operators are enabled to make a fast and well-informed decision regarding a possible threat via automation, or they can choose to manually handle the evaluation of the security alert and related courses of action.

**Goal**

- Receive alerts regarding suspicious activities or exceeding threshold over industrial systems.
- Automatically download specific activity logs related to specific industrial machines and store them as evidence.
- Automatically analyze those logs and extract the host originator of the latest commands sent to the machines.
- Retrieve information and reputation of the extracted hosts.
- Inform SOC operators of the threat and allow them to be able to decide what course of action needs to be taken.
- Contain the incident isolating the host from the network.
- Recover the state of industrial machines.

**Integrations Used**

- Cisco Cyber Vision
- Cisco Cyber ISE
- SIEM
- Alleantia
- MSSQL Server
- Email notification
Creating an R3 Rapid Response Runbook

The first step is receiving an alert related to the industrial machine status via multiple alerts (email, syslog, or others). In case of a threshold exceeding event or deviation from normal working, a baseline is converted into an alert and sent to IncMan.

Then, IncMan starts with a series of enrichment actions. For instance, it can start by retrieving the latest events related to the industrial machine under analysis from Alleantia. Afterward, those logs are stored inside the incident container created in IncMan. For each log, a subset of information is extracted, and the analysis process starts in order to determine whether some host systems, voluntarily or not, sent commands to the industrial machine. The analysis output contains the host list that interacted with the industrial machine.

The host list is used to query Cisco Cyber Vision in order to extract more information about host like, for example:

- Whether the host is well-known or new
- Whether it is present into the network perimeter recently or not
- Whether the details about Operative System are available or not
- Whether the host/s have in general have a good or bad reputation

Once this data is automatically collected by IncMan, which would only take a few minutes, the SOC operator responds. Then, IncMan generates a series of User Choices for a specific user, or group of users, asking what the next steps should be.

If the host can be considered as “trusted,” IncMan makes an assessment and analyzes if any escalation is needed or if it is possible to close the incident as a false positive. In addition, the SOC operators are asked if the industrial machine needs to be restarted or if any commands should be sent in order to reactivate the normal operations.

If the host is considered as “not trusted,” an extra enrichment step can be executed, asking the SIEM relevant questions regarding the enrichment phase, such as:

- Whether the host/s under analysis communicated with other systems
- If yes, when did the communication take place
- Whether they have access to the Internet

After those enrichment actions, the user can decide to: isolate the host from the network using a Cisco technology like Cisco ISE or leave this task as a manual intervention to be performed by an authorized operator.

In case the host is recently added to the network, IncMan SOAR can update the SOC operators with the new information collected from the moment the host was added to the network.

Summary

Depending on the information received in the alert, SOC operators can determine whether the alert can pass as a false positive or whether it can pose an actual threat to the system. If so, the SOC operators can decide whether they want to manually pursue the remediation phase and choose the course of actions themselves, or whether they want to apply automation to the task in hand.

Either way, IncMan SOAR’s enrichment phase utilizes the extracted information from the Runbook’s actions to create a valid assessment of the alert and provide the SOC operators with the opportunity to single-handedly carry out the rest of the remediation phase by providing them with valuable information regarding the alert, and if the SOC operators deem that the alert doesn’t require human interaction, they apply automation to finalize the remainder of the remediation phase.

Thanks to IncMan’s prompt and thorough enrichment phase, SOC operators can make an accurate decision regarding an alert and carry out the remediation processes in the most effective manner.
8. Anti-fraud

Financial institutions are a constant target of intrusion attempts, which underlines the need for additional cyber security technologies that are capable of nullifying the risk of potential cyber attacks. However, the fact that financial institutions don’t have a way to better integrate their security tools with their SecOps teams means that their resources are being poorly distributed. Analysts are spending more time on false positives, while the real threats are left unattended. This decreases the optimal efficacy of the entire organization and reduces the ability of the SOC and CSIRT to properly respond to cyber attacks. 

In this regard, by acting as connective tissue amongst security tools via orchestration and automation, IncMan SOAR allows SOCs to drastically reduce their response time to cyber threats and increases their chances of intercepting cyber fraud alerts even before they evolve into full-blown incidents.

How IncMan SOAR Helps Fight Anti-Fraud

In the battle against cyber fraud, IncMan SOAR has proven time and time again that it can be an indispensable asset. And to show its value in practice, we will take the example of one of the largest banks in Europe.

The bank utilizes IncMan SOAR’s monitoring software to detect any potentially fraudulent transactions that may arise from the external systems. Such transactions include:

- National Wire Transfers
- Prepaid Phone Card
- Prepaid Credit Cards
- International Wire Transfers
- Credit Cards

In the event of a fraudulent transaction, the anti-fraud analysts will first create a pre-validation in order to verify the legitimacy of the transaction and determine whether or not the alert is a false positive.

Furthermore, in order to confirm whether an alert is a real threat or possible false positive, IncMan receives valuable data regarding these transactions from the RAKE API and stores them into its TRIAGE function. After IncMan SOAR receives the data regarding the nature of the transaction, it uses its TRIAGE capability to store and utilize that data. The data is then sent to IncMan automatically from the Fraud Management System’s API. IncMan then analyzes the data and uses it to perform enrichment of the potentially fraudulent transaction via its R3 Rapid Response Runbooks.

Analysts then read this information, and upon analyzing all of the data they decide whether a transaction is fraudulent and should be converted into an incident. This is done with the goal of preventing these transactions to be converted into incidents if there is no actual need of converting them into incidents.

After reviewing all the evidence gathered, the transaction can be closed as a false positive or converted into an incident, according to the bank’s policies. If needed, a closed transaction can be reopened for additional processing. When a transaction is converted into an incident, all the enrichment actions that have already been performed will be visible inside the incident along with their results, and the team members will then process the new incident in accordance with the bank’s policies. All actions performed to a suspected transaction and an incident, and any user activity is automatically captured and stored into IncMan’s audit trail. Finally, specific reporting capabilities are created within IncMan which are related to the processing of these transactions to analyze the results.

Furthermore, IncMan SOAR allows the bank to conduct this process continuously, as during working hours IncMan is operated by internal users, and in non-working hours IncMan is operated by external contractors.

Using IncMan’s SOAR unique features for preventing cyber fraud IncMan SOAR allows users to customize their workflow and adjust it in different ways in order to enhance their user experience. In this case, the bank used different colors to map out the processes in a more visually accessible manner. This allowed the bank to create a visual representation which helped the team coordinate better:

- White: still to be processed
- Purple: assigned to a user
- Green: assigned to a group

This creates a visual cue that leads to fewer errors amongst the team. Any owner of a transaction can re-route it to a different user or team if necessary. When a user takes ownership of a transaction, an IncMan Rapid Response Runbook is executed. And, depending on the type of transaction in hand, the Runbook contains the appropriate enrichment actions.

Different Runbooks are defined for the varying transaction types. The information resulting from all the enrichment actions executed by the Runbooks are stored within the transaction and are available to the analysts. The actions typically involve accessing the information on the Mainframe and other external systems.
Summary

In this use case, we elaborated on the benefits of IncMan SOAR depicted properly in a real-life example. We explained how the bank utilizes IncMan SOAR as an effective technology toward discovering potentially fraudulent transactions and to improve its cyber security posture overall. We showed how IncMan's flexibility plays a major part in improving the communication between team members, thus allowing the entire process to go smoothly.

In regard to tackling fraudulent transactions, IncMan SOAR offers two very unique capabilities that can greatly enhance the chances of preventing such cyber threats:

- **Open Integration Framework:** With the Open Integration Framework (OIF) we want all vendors to integrate bi-directionally with us and everyone to be independent in creating integrations. DFLabs even integrate Mainframes for this particular type of use case.

- **Triage:** Triage is a major differentiator that distinguishes DFLabs from the rest. This feature allows users to properly deal with potentially harmful alerts that require a more thorough analysis. Through triage, analysts can also decrease the number of false positives by relying on contemporary technology and software, mostly based on automation, machine learning, correlation, and aggregation of events.

The inevitable reality is that financial institutions are, and will continue to be, lucrative targets for cyber attackers. In this regard, financial institutions must think one step ahead and implement proper technologies, like IncMan SOAR, that will strive not to recover, but to intercept and prevent fraudulent transactions from ever happening.

9. Meltdown and Spectre Vulnerabilities

This use case demonstrates how to use IncMan's integrations and R3 Rapid Response Runbooks to quickly respond to hosts exposed to the Meltdown and Spectre vulnerabilities, reducing the risks posed by these potentially critical issues.

Goal

Automatically receive alerts for hosts which have been identified as being vulnerable to Meltdown or Spectre, create an Incident and perform automated Notification, Enrichment and Containment tasks to reduce the risk these vulnerabilities present to the organization.

Integrations Used:

- Jira
- McAfee ePO
- McAfee Web Gateway
- MSSQL Server
- QRadar

The first step in reducing the risk from the Meltdown and Spectre vulnerabilities is to create a runbook to handle alerts for newly detected vulnerable hosts. In this use case, we will use integrations with Jira, McAfee ePO, McAfee Web Gateway, MSSQL Server and QRadar to perform Notification, Enrichment and Containment actions; however, this can easily be adapted to include any other technology integrations as well.

Using a Jira Notification action, a new Jira issue is created. This Notification action should notify the IT or Infrastructure teams and initiate the organizations' normal vulnerability management process.

Next, an MSSQL Server Enrichment action is used to query an IT asset inventory for the host name of the vulnerable host, which is passed to the runbook automatically when the incident is created. This asset information is then available to the analyst for further review.

Once the IT asset information is retrieved, a decision point is reached. If the IT asset information indicates that the host is a server, one path (the top path) is taken. If the IT asset information indicates that the host is not a server, another path (the bottom path) is taken.

If the asset is determined to be a server the Jira Enrichment action is used to update the Jira issue, informing the appropriate parties that the host has been determined to be a server and should be treated as a higher priority. Next, two McAfee ePO Enrichment actions are performed. The first Enrichment action queries McAfee ePO for the system information of the given hostname, providing the analyst with additional information. The second Enrichment action uses McAfee ePO to tag the host with the appropriate tag. Finally, a Task is added to IncMan reminding the analyst to follow up with the appropriate teams to ensure that the vulnerability has been appropriately mitigated.
If the asset is determined not to be a server, the two previously mentioned McAfee ePO Enrichment actions are immediately run (System Info and TAG). Following these two Enrichment actions, a McAfee Web Gateway Containment action is used to block the host from communicating outside of the network. This Containment step is completely optional but is performed here on non-servers only to minimize the Containment action’s potential impact on critical systems.

**Utilizing the R3 Rapid Response Runbook**

Once the new runbook is created, IncMan must be told how and when to automate the use of this runbook. This is achieved by creating an Incident Template, which will be used any time an incident is generated for a Meltdown or Spectre vulnerability. Through this incident template, critical pieces of information such as Type, Summary, Category can be automatically applied to the newly created incident.

From the Runbook tab of the Incident Template wizard, the previously created Meltdown and Spectre runbook is selected and set to autorun. Each time this template is used to generate an incident, the appropriate information such as the hostname and host IP address will be used as inputs to the runbook and the runbook will be automatically executed. In this use case, alerts from QRadar are utilized to initiate automatic incident creation within IncMan.

However, another SIEM integration, syslog or email could also be utilized to achieve the same outcome. A new QRadar Incoming Event Automation rule is added and the defined action is to generate a new incident from the previously created Meltdown and Spectre Incident Template.

### Summary

When a QRadar Alert is generated matching the criteria defined for a Meltdown or Spectre vulnerability detection, IncMan will automatically generate a new incident based on the Meltdown and Spectre Incident Template. Without requiring any action on the part of an analyst, the Meltdown and Spectre runbook is automatically initiated, performing the defined Notification, Enrichment and Containment actions (in the example shown here, the ‘server’ path is taken).

This entire process has taken place in a matter of minutes, likely before anyone has even had time to acknowledge the alert. As an analyst begins to manually examine the alert, many of the mundane tasks have already been completed, allowing the analyst to focus on the tasks which require human intervention and reducing the time required to remediate this issue, ultimately reducing risk to the organization.

---

**Final Thoughts**

These 9 use cases can assist you in building your own implementation within your organization in your own organization without interrupting the workflow. It is vital to note that the potential of SOAR goes beyond these 9 use cases, but the very core of SOAR as a cyber security solution is to learn repetitive behavior through AI and machine learning, save valuable time by automating repetitive tasks, and distinguish false positive and false negative. Ultimately, SOAR provides you with the ability to centralize your security operations from one single place by easily integrating SOAR with other security tools, reduce the amount of time needed to assess potential threats, eliminate the necessity of manually assessing each alert, and successfully detect and prevent real cyber attacks. And all of these processes were perfectly encapsulated in the 9 use cases we explained throughout this white paper, where you can see the potential of SOAR manifested in practice through real examples.
About Us.

DFLabs is an award-winning and recognized global leader in Security Orchestration, Automation and Response (SOAR) technology.

Its pioneering purpose-built platform, IncMan SOAR, is designed to manage, measure and orchestrate security operations tasks, including security incident qualification, triage and escalation, threat hunting & investigation and threat containment. IncMan SOAR harnesses machine learning and automation capabilities to augment human analysts to maximize the effectiveness and efficiency of security operations teams, reducing the time from breach discovery to resolution and increasing the return on investment for existing security technologies.

As its flagship product, IncMan SOAR has been adopted by Fortune 500 and Global 2000 organizations worldwide. The company’s management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121.

DFLabs has operations in Europe, North America and EMEA.

For more information visit www.dflabs.com or connect with us on Twitter @DFLabs.