# SOAR

## Introduction

Security events and attacks are becoming more complex, with adversaries showcasing sophisticated capabilities and tools. This has raised challenges for the security defence teams and brought about justifications for performing security differently.

In this room, we shall look at one of the different ways of organising security defences through orchestration, automation and response, commonly referred to as SOAR.

**Learning Objectives**

- Expand the users' knowledge of security operations through orchestration, automation and response.
- Familiarise yourself with common SOAR workflows.
- Assemble a malware investigation workflow.

**Learning Prerequisites**

A look at the following rooms would be helpful before embarking on this room:

- Security Operations
- Junior Security Analyst Intro
- Intro to Detection Engineering

## Security Operations Centers

### Evolution of Security Operation Centres (SOCs)

Security operations centres have become visualised as large action-packed rooms with threat alerts firing from numerous monitors, with analysts rushing about and trying to contain the threat. However, no two SOCs are the same and are set up differently. At the basics, SOCs are meant to provide a location to centralise crisis communication for organisations and provide monitoring capabilities for physical, logical and network security. All this is to protect assets. For a quick introduction to SOCs and their operations, check out the Security Operations room.

SOCs have evolved over time, with every generation adding new technology. A quick rundown of the SOC generations is as follows:

- First-Generation: Initial SOC functions were handled by the IT operations teams; thus, tasks were more blended. The main functions included device monitoring, managing antivirus security and log collection, which was limited and often referred to in the event an incident was reported.

- Second-Generation: SIEM tools emerged here and were meant to add to the previous SOC functions. The added operational aspects included events correlation, network and Syslog log collection and case management. This meant that security threat management was the main focus and aimed at correlating events to establish links and provide analysts with visuals that would assist them in investigating incidents.
- Third-Generation: Expanded the use of SIEMs by adding vulnerability management and incident response capabilities.
- Fourth-Generation: Advanced security capabilities are introduced here, including big data security and data enrichment. With this generation, SOCs can analyse large amounts of data to uncover threats in real-time. As an example, threat intelligence feeds have become valuable to SOC teams, expanding the horizons of security investigations.

You can read more on the SOC generations in the book: “Security Operations Center: Building, Operating and Maintaining your SOC.”

**SOC Capabilities**

The main advantage of an organisation having a SOC is to enhance their security incident handling through continuous monitoring and analysis. This is achievable through having the right amount and implementation of people, processes and technologies that would support the capabilities of the SOC and business goals.

On the matter of SOC capabilities, the key ones to have include the following:

- Monitoring and Detection: This focuses on continuously scanning and flagging suspicious activities within a network environment. It leads to awareness of emerging threats and how to prevent them in their early stages.
- Incident Response: SOC teams operate as first responders when cyber threats are identified. They perform operations such as isolating or shutting down infected endpoints, removing malware and stopping malicious processes.
- Threat Intelligence: Monitoring environments continuously requires a constant flow of intel. This ensures that SOC teams are always updated on the latest developments and have the best available resources to address emerging threats.
- Log Management: A SOC gathers, maintains and reviews logs of all network connections and activities within an organisation. With all this information, baselines for regular activities can be established and provide evidence for forensic investigations.
- Recovery and Remediation: Organisations rely on their SOC to provide a hub for recovery and remediation when incidents occur. Additionally, the SOC provides

effective communication with affected parties to ensure that the incidents are addressed.

- Security Process Improvement: Adversaries are continuously refining their tactics and tools. This means that the SOC must always carry out improvements by performing post-mortem investigations and identifying areas to work on.

**SOC Challenges**

- Alert fatigue: As a result of using numerous security tools, a huge number of alerts will be triggered within a SOC. Many of these alerts are false positives or insufficient for an investigation, leaving analysts overwhelmed and unable to address any serious security events.
- Disparate tools: Security tools are often deployed without integration within an organisation. Security teams are tasked with navigating through firewall logs and rules which are handled independently from endpoint security logs. This also leads to an overload of tools.
- Manual Processes: SOC investigation procedures are often not documented, leading to a lack of efficient means of addressing threats. Most rely on established tribal knowledge that was built by experienced analysts, and the processes are never documented.
- Talent Shortage: SOC teams find recruiting and expanding their talent pool difficult to address the growing security landscape and sophisticated threats. Combining this with the alert overload teams face, security analysts become more overwhelmed with the number of responsibilities they have to undertake, resulting in less efficient work and extended incident response times that allow adversaries to reign havoc within an organisation.

*****************************************************************************************************

**Answer the questions below:**

**Under which SOC generation did SIEM tools emerge?**
Answer: second

**How would you describe the experience of having an overload of security events being triggered within a SOC?**
Answer: Alert fatigue

## Security Orchestration, Automation and Response

As we have covered in the previous task, security operations face numerous challenges and analysts are left overwhelmed. Security teams would love to handle all their alerts and triage processes from a single platform or interface, making integrating all their existing tools possible.

Security Orchestration, Automation, and Response (SOAR) platforms come into play and allow organisations to analyse threat intelligence efficiently, automate response workflows and triage incidents using human and machine power. SOARs operate using the following capabilities:

**Security Orchestration**

Just like organising a musical orchestra, security orchestration is an act of connecting and integrating security tools and systems into seamless workflows. This develops streamlined processes and information flow, effectively helping organisations handle security events. Orchestration works in tandem with automation, which we shall define shortly.

What is vital to remember is that orchestration chains together individual security tools, tasks and processes to work together towards the same tune.

**Security Automation**

As workflows are developed with orchestration, repeatable patterns will emerge. Automation comes into play at this point and becomes a “must-have” element in dealing with complex tools and information flows. Automation goes beyond just laying out the necessary action steps to handle a security event and offer preventive measures. It is meant to provide additional insights into threat response and allow security teams to adopt and customize the response workflows to reduce handling time.

**Security Response**

Once security incidents are detected and analysed, a triage plan must be set in motion to avert damages from any adversary. This requires analysts to identify the appropriate steps to contain and remediate the threat. With the help of automation, incident response processes can be executed seamlessly.

**SOAR vs SIEM**

SOARs are commonly compared with SIEMs and are deployed alongside each other. Let us analyse some key differences between these technologies:

| **SOAR** | **SIEM** |
|---|---|
| Fetches threat feeds from SIEM, threat intelligence, endpoint security. | Centrally collected log and event data from security, network, server and |

| | |
|---|---|
| | application sources. |
| Collects security alerts and intel using a centralized platform. | Generates alerts to be assessed by analysts. |
| Orchestration and automation ensure less human intervention when addressing threats. | More human intervention is required to manage rules, use cases and alerts. |
| Employs workflows and playbooks to ensure end-to-end response automation. | Limited response workflows result in longer response times. |

**SOAR Playbooks & Runbooks**
The SOAR capabilities run efficiently through playbooks. A security playbook is a structured checklist of actions used to detect, respond and handle threat incidents. Another common terminology for them is a standard operating procedure (SOP). Playbooks assist SOC teams in having an end-to-end process of handling routine incidents and establishing repeatability and metrics for the response. We shall look at some SOAR playbook uses in the next task.

On the other hand, we have runbooks which are predefined procedures to achieve a specific outcome and have a high degree of automation. Runbooks can include human decision elements depending on the level of automation applied.

**Workflow of a SOAR**
Putting together the SOAR capabilities, a typical workflow would look as follows:

- Detection: A security event may be triggered and detected by an integrated security system such as a network intrusion detection system (NIDS) or a SIEM.
- Enrichment: Threat intelligence would be gathered from feeds, reports and other sources to provide additional context about the event, such as the tactics, techniques and procedures (TTPs). SOC analysts can use the orchestrated data to conduct deeper investigations.
- Triage: The SOAR would analyse the event, determining its severity and potential impact on the organisation. This reduces the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to security incidents.
- Response: Automated actions are set in motion to contain the threat and mitigate any potential damage. For example, implemented playbooks could trigger the isolation of compromised systems or block identified malicious IP addresses. A new level of enhanced incident response.
- Remediation: Root cause analysis of the event is done through the coordinating efforts of security analysts and incident responders. Additionally, patch management operations and vulnerability upgrades are automated efficiently.

- Reporting: Communication and reports about the incident and remediation are standardised to ensure a reliable and repeatable flow of information involving both internal and external stakeholders. Actionable metrics may also be extracted.

**SOAR Tool Factors**

With the understanding that all aspects of a security incident should be managed from a single platform, some notable factors to look out for when sourcing a SOAR solution include the following:

- Open integration with existing security and IT tools out-of-the-box. Future integrations with new or custom technologies should also be considered.
- They provide a streamlined collaboration, smooth handoffs and escalations to support day-to-day SOC operations.
- Operations dashboards that provide analysts with capabilities to build, customise and test playbooks to improve the incident response processes.
- Role-based KPI dashboards and reporting libraries are available to support measuring and improving SOC performance.
- Automatically correlate and combine related alerts from multiple tools to minimise false positives and eliminate alert fatigue on analysts.

****************************************************************************************************

**Answer the questions below:**

**The act of connecting and integrating security tools and systems into seamless workflows is known as?**

Answer: Security Orchestration

**What do we call a predefined list of actions to handle an incident?**

Answer: Playbook

## SOAR Workflows

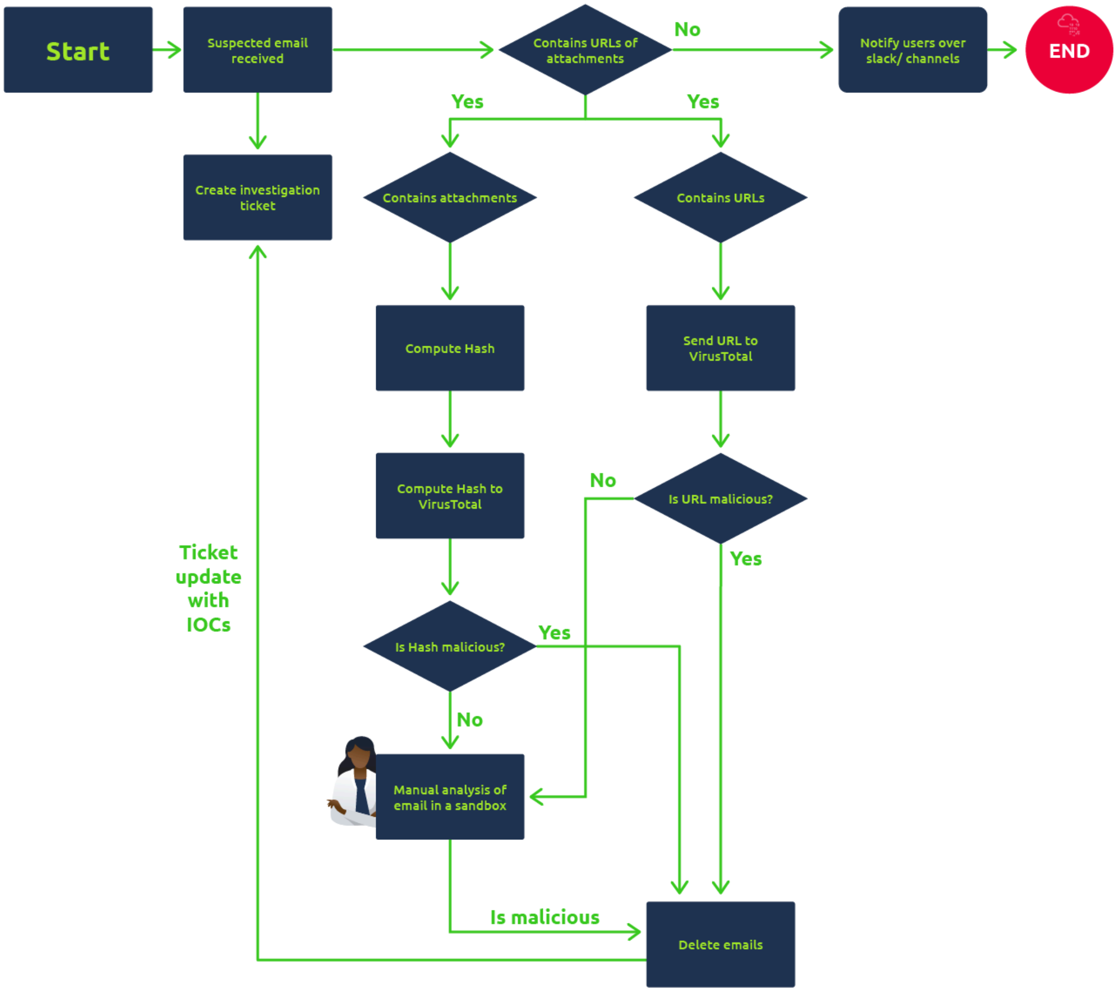
### Phishing Workflow

Scenario: THM Corp employees have recently received numerous suspicious emails and have reported them to the SOC team for investigation. As the lead analyst, you wish to develop an automated workflow to analyse email files and perform case management using various security tools.

Phishing attacks remain the most common attack vector used in breaches. Unfortunately for security analysts, investigating phishing emails becomes time-consuming and involves manual exercises such as analysing attachments and URLs. SOAR solutions can execute these tasks in the background while other investigations are ongoing. Additionally, remediation can be performed when a positive phishing email is identified.

Now, what would this workflow look like? Let's build a flow of events using our scenario as a security analyst assigned to the incident.

1. The suspected emails have been received and isolated in a sandbox environment prepared for such events.
2. A trigger is executed to create a ticket on the case management solution (such as TheHive). This will allow for better documentation and follow-up on the incident.
3. Parse the email for URLs, attachments and other possible IOCs. If any IOCs are present, they will be extracted.
4. File hashes will be generated for extracted attachments.
5. A VirusTotal trigger is executed to analyse extracted URLs and file hashes.
6. In the event there are no results from VirusTotal, a manual email analysis has to be done to ensure whether it is malicious.
7. Malicious outcomes from automated or manual analysis trigger a deletion of the malicious email and a communication notification to the organisation.
8. The incident ticket is updated with IOCs' results and reports generated.
9. End of workflow.



## CVE Patching

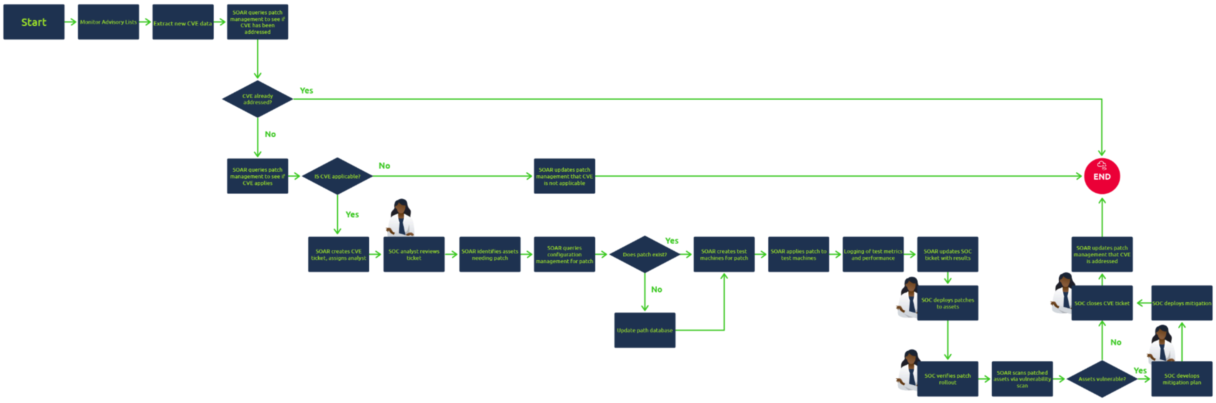
Scenario: A new CVE report has been received. As the lead SOC analyst, you need to establish a workflow that will analyse the CVE details, assess its risk threshold, create a patching ticket and test the patch before being pushed to the production environment.

The Common Vulnerabilities and Exposures (CVE) is a classification list for publicly disclosed vulnerabilities based on a scoring system that evaluates the threat level of the vulnerability. If you need a refresher on vulnerabilities, check out the room Vulnerabilities 101.

As a security analyst, you must always be on the lookout for publications on new CVEs and remediation plans. The process can become overwhelming, resulting in a mounting backlog and patches not being applied, leaving the environment more vulnerable.

SOARs can be used to orchestrate and automate vulnerability management processes, addressing critical issues based on released security advisories in a timely and efficient manner. The workflow for this scenario can be detailed as follows:

1. The SOAR monitors advisory lists and pulls details, extracting any new CVE data.
2. The SOAR queries the internal patch management system if the received CVE has been seen before and patched.
3. If CVE has been addressed, end workflow. If not, the CVE will be assessed to see if it applies to any assets.
4. If CVE is applicable, a tracking ticket is created and assigned to an analyst. If not, the patch management system is updated with the information, and the workflow ends.
5. For a created CVE Ticket, the SOAR will compile a list of assets needing patching against the CVE.
6. The patch management system is queried for the presence of the patch. The database is updated with the latest patch information if the patch is not present.
7. The SOAR creates virtual test environments to test the patch. The patch is applied, and test metrics are logged.
8. The SOAR updates the CVE ticket with test outcomes and notes success and failure rates.
9. The patch is deployed to production assets. The analyst verifies the rollout of the patch.
10. The SOAR conducts a vulnerability scan against the patched assets for the CVE. The analyst develops and deploys a mitigation plan if assets are still vulnerable.
11. The CVE ticket is closed, vulnerabilities cleared, and patch management is updated with the CVE addressed.
12. End workflow.


Start
Monitor Advisory Lists
Extract new CVE data
SOAR queries patch management to see if CVE has been addressed
CVE already addressed?
Yes
No
SOAR queries patch management to see if CVE applies
IS CVE applicable?
No
SOAR updates patch management that CVE is not applicable
END
Yes
SOAR creates CVE ticket, assigns analyst
SOC analyst reviews ticket
SOAR identifies assets needing patch
SOAR queries configuration management for patch
Does patch exist?
Yes
No
Update path database
SOAR creates test machines for patch
SOAR applies patch to test machines
Logging of test metrics and performance
SOAR updates SOC ticket with results
SOC deploys patches to assets
SOC verifies patch rollout
SOAR scans patched assets via vulnerability scan
Assets vulnerable?
Yes
SOC develops mitigation plan
SOC deploys mitigation
No
SOC closes CVE ticket
SOAR updates patch management that CVE is addressed

**********************************************************************************************************************

**Answer the questions below:**

**Are manual analyses vital within a SOAR workflow? yay or nay?**

Answer: yay

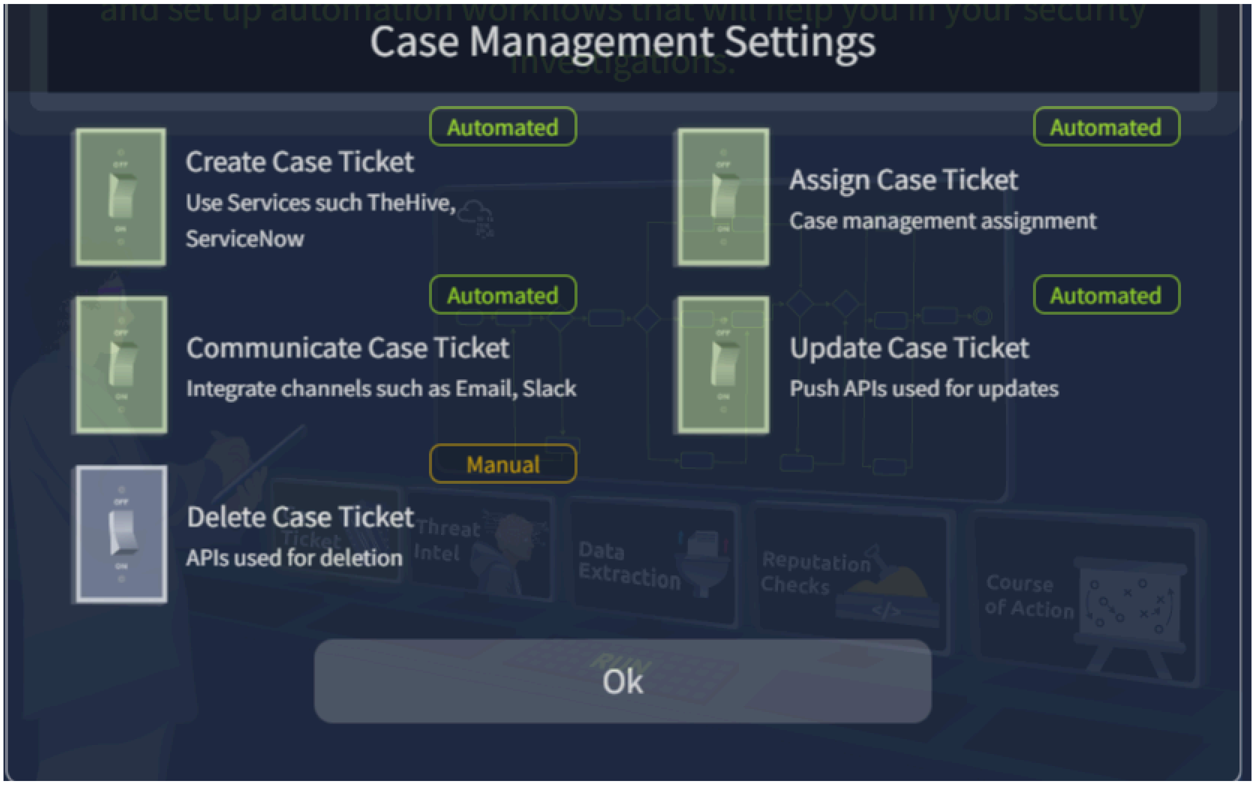
## Threat Intel Workflow Practical

You are a SOC Lead who has recently faced a large breach investigation that took ages to complete due to a lack of automation. Your friend, McSkidy, recently advised you to adopt a SOAR and set up automation workflows to help your security investigations. McSkidy sent you a checklist for a Threat Intelligence integration workflow, and your task is to figure out how it works. Click the View site button at the top of the task to launch the site in split view. To automate the process, use the different screens to activate the elements required for the SOAR workflow. Run and test the workflow until you obtain a smooth transition on the flowchart to complete the task.

****************************************************************************************************

**Answer the questions below:**

**What is the flag received?**



Case Management Settings

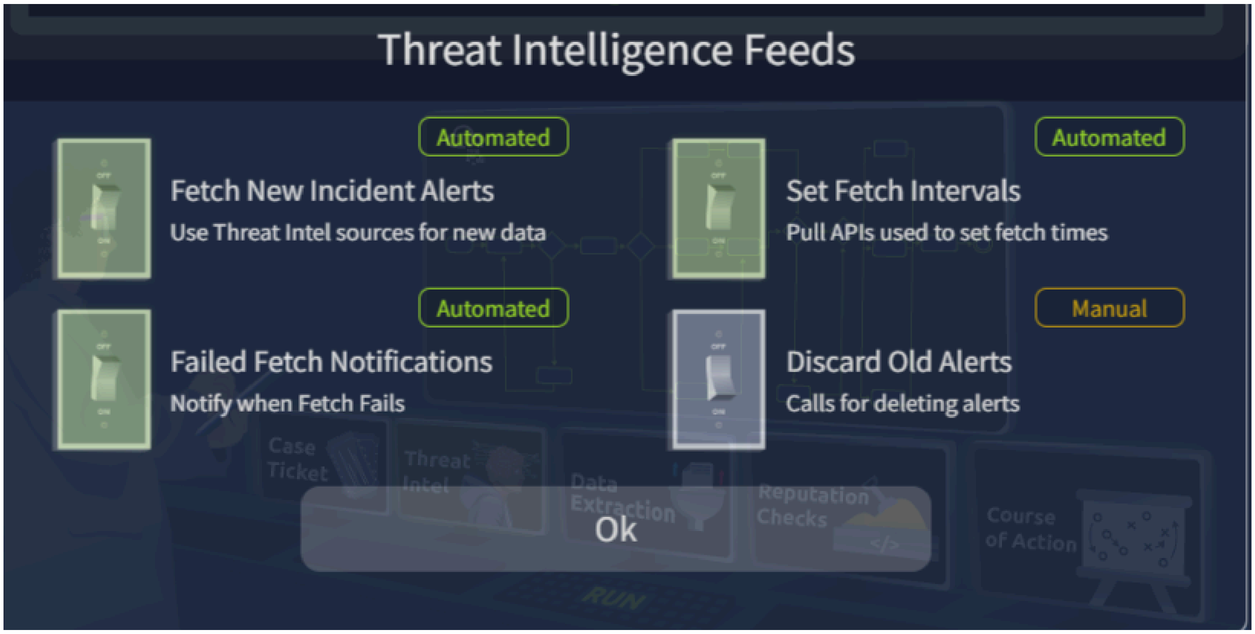
Automated — Create Case Ticket — Use Services such TheHive, ServiceNow

Automated — Assign Case Ticket — Case management assignment

Automated — Communicate Case Ticket — Integrate channels such as Email, Slack

Automated — Update Case Ticket — Push APIs used for updates

Manual — Delete Case Ticket — APIs used for deletion



## Threat Intelligence Feeds

Automated

**Fetch New Incident Alerts**
Use Threat Intel sources for new data

Automated

**Set Fetch Intervals**
Pull APIs used to set fetch times

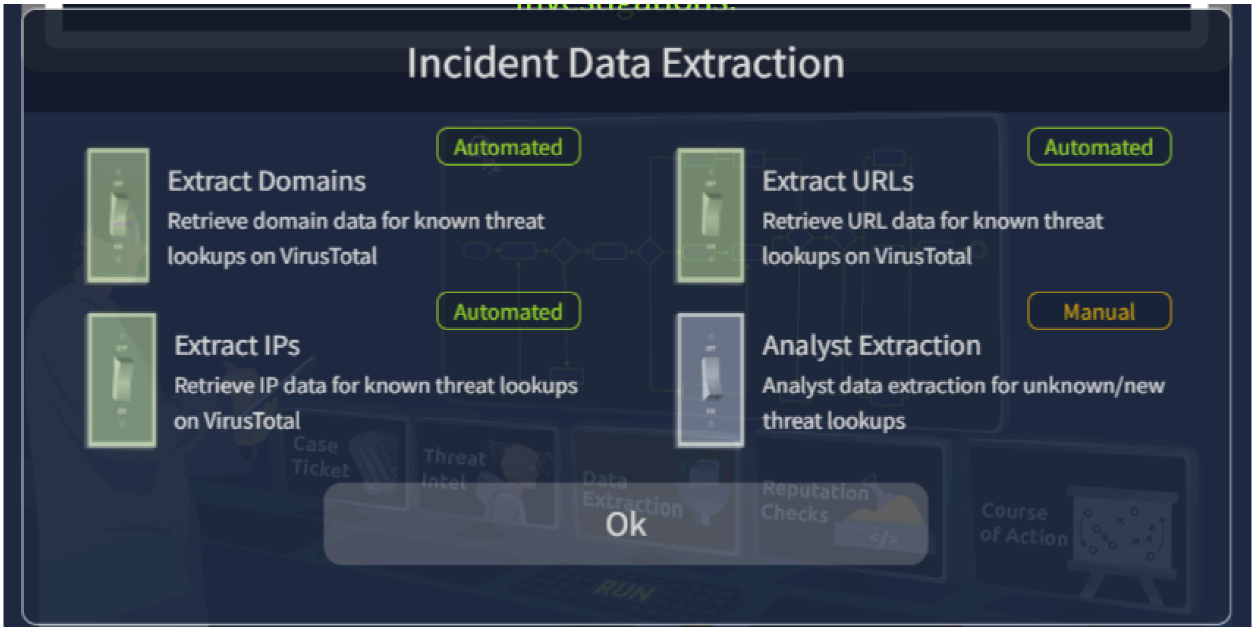
Automated

**Failed Fetch Notifications**
Notify when Fetch Fails

Manual

**Discard Old Alerts**
Calls for deleting alerts

investigations.



## Incident Data Extraction

Automated

**Extract Domains**
Retrieve domain data for known threat lookups on VirusTotal

Automated

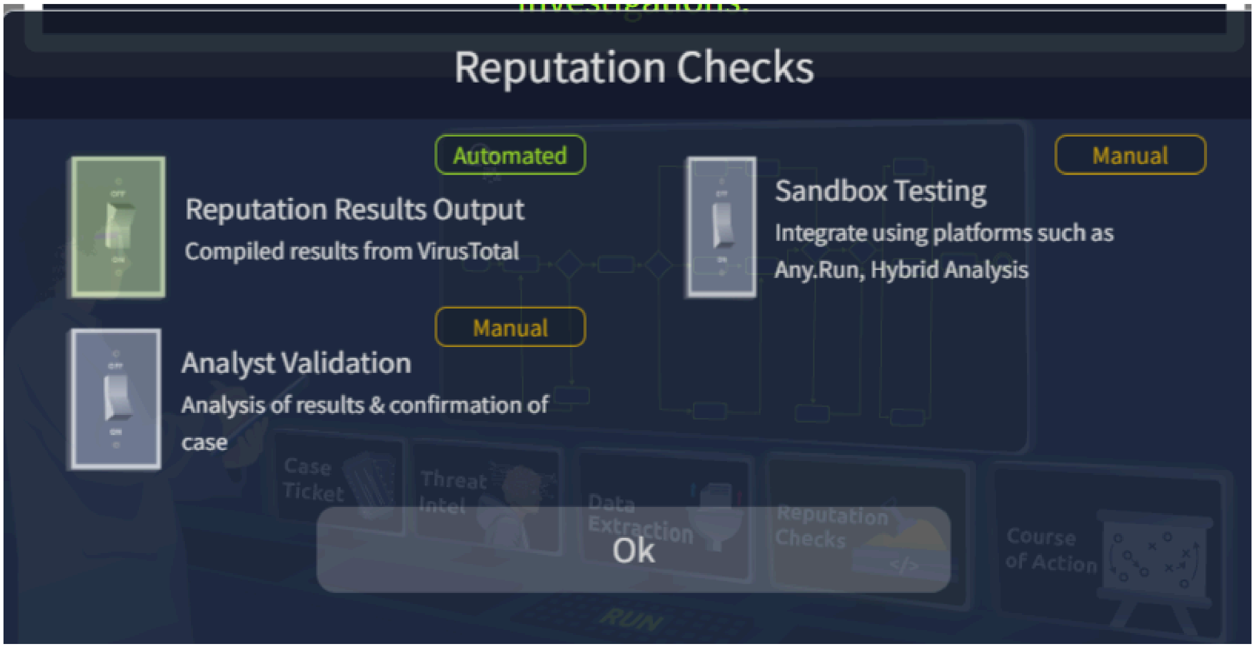
**Extract URLs**
Retrieve URL data for known threat lookups on VirusTotal

Automated

**Extract IPs**
Retrieve IP data for known threat lookups on VirusTotal

Manual

**Analyst Extraction**
Analyst data extraction for unknown/new threat lookups

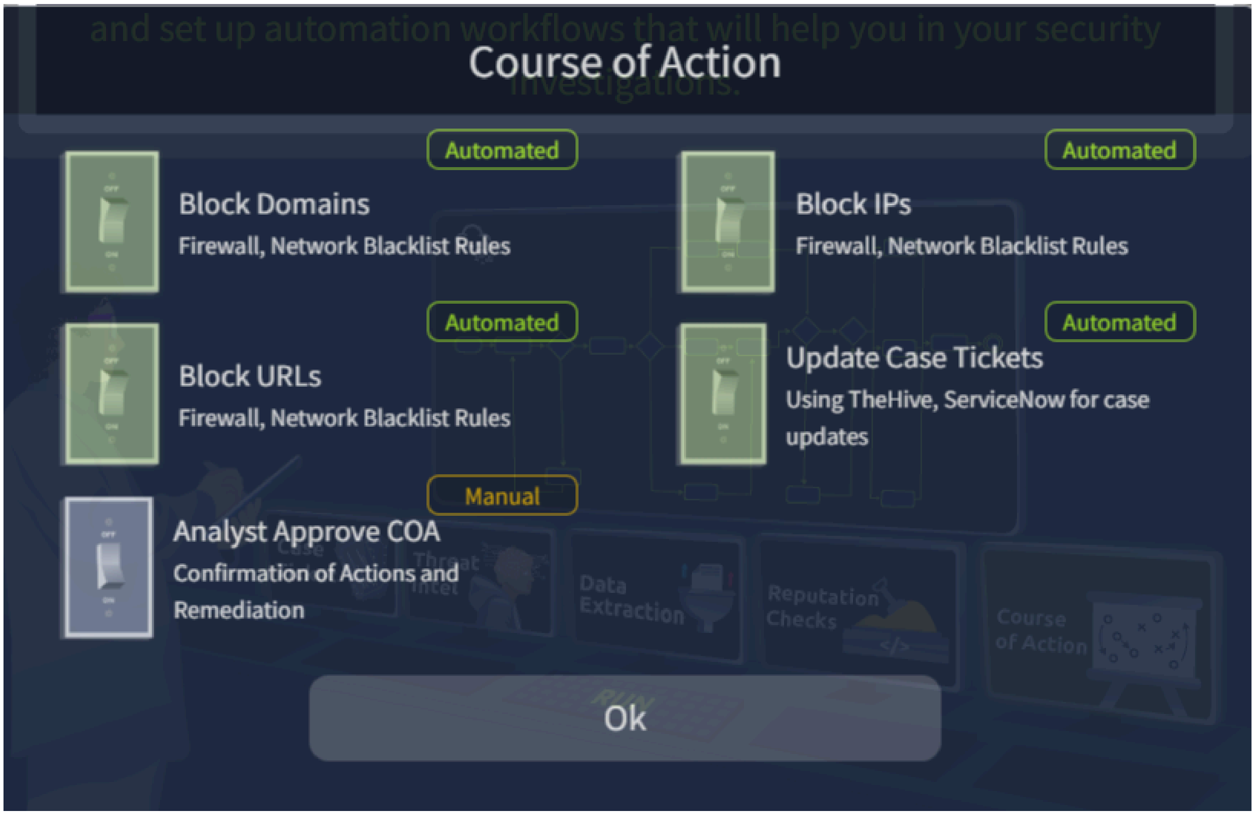


## Reputation Checks

Automated — Reputation Results Output: Compiled results from VirusTotal

Manual — Sandbox Testing: Integrate using platforms such as Any.Run, Hybrid Analysis

Manual — Analyst Validation: Analysis of results & confirmation of case



## Course of Action

Automated — Block Domains: Firewall, Network Blacklist Rules

Automated — Block IPs: Firewall, Network Blacklist Rules

Automated — Block URLs: Firewall, Network Blacklist Rules

Automated — Update Case Tickets: Using TheHive, ServiceNow for case updates

Manual — Analyst Approve COA: Confirmation of Actions and Remediation

and set up automation workflows that will help you in your security investigations.
Case
Threat Intel
Data Extraction
Reputation Checks
Course of Action
Ok

Answer: THM{AUT0M@T1N6_S3CUR1T¥}