Top five use cases for Logpoint SOAR

Security operation centers (SOCs) are constantly overwhelmed. They have too many alerts and threats to investigate and resolve. Analysts are drowning in alerts and relying on repetitive and time-consuming manual steps to respond to incidents to make things worse.

Logpoint SOAR helps security teams respond to the increasing number of security alerts more efficiently by collecting security threats data and alerts from multiple sources. SOAR can automatically prioritize and respond to security threats and incidents, reducing the manual operations in the security team.

This e-book presents five common SOAR use cases that every organization should implement to reduce alert overload and increase SOC productivity.

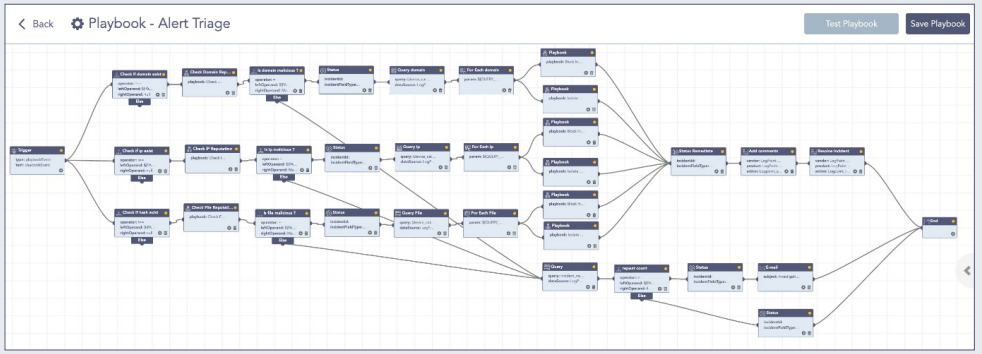
For more information, contact Logpoint:
https://www.logpoint.com/en/contact/

LOGPOINT

Automated alert triage and enrichment

Most SOCs are drowning in security alerts, receiving thousands of alerts daily. Manually reviewing and investigating all security alerts that lack additional context is challenging. Security analysts must search manually for indicators of compromise (IOCs) such as URL, IP address, or domain to determine the severity of the threat.

Logpoint SOAR can automatically perform alert triage and enriches the alerts with additional information from multiple sources so that analysts can focus on incidents requiring human intervention. Using APIs, Logpoint SOAR integrates with many solutions, such as HR or travel systems. This capability enriches the alerts with additional relevant information for easier triage, such as logins from unusual locations or devices. By automating the process of data collection and alert enrichment, security analysts will have important details of the threat as soon as it arises. Automated alert triage reduces alarm fatigue, lowers response times, and improves operational efficiency.



Alert triage playbook

Reduce the noise with Logpoint SOAR

The actions in this playbook include:

- Alert rule triggering the SOAR playbook
- Extraction of parameters from the incident (file hash, IP, domain, sender, receiver, subject)
- Parameter reputation check with Threat Intelligence

If found malicious

- Changing the incident status to malicious
- Querying SIEM to identify other affected endpoints with malicious indicators
- Running a playbook to isolate affected endpoints
- Running a playbook to block malicious IoCs
- Setting the status of the case to Mitigated
- Resolving the incident in SIEM with detailed comments

Else

- Querying SIEM and UEBA solutions for more information (the number of times the alert was triggered in the last 24 hours, users and entity risk score)

If any anomalous observations are found

- Changing the incident status to malicious
- Notifying system admin to check alert details and prompt for the action to run corresponding investigation and remediation playbooks
- Setting the status of the case to Mitigated
- Resolving the incident in SIEM with detailed comments

Else

- Setting the status of the case to Mitigated
- Resolving the incident in SIEM with comments as false positive

LOGPOINT

Endpoint malware mitigation

Organizations typically have hundreds or thousands of endpoints that are the targets of malware attacks. Attacks on endpoints are the most popular ones, with smartphones and laptops being the most vulnerable targets. As a research by Ponemon Institute points out, the frequency of malware attacks against endpoints is drastically increasing.

These endpoints possess even more risk due to the increasing popularity of remote working, moving corporate endpoints outside the organization's network, making them more vulnerable to attacks. These endpoints generate tons of malware alerts every day. Many of them are either low severity or false positive. Manually investigating and responding to these alerts result in a long response time and greater risk.

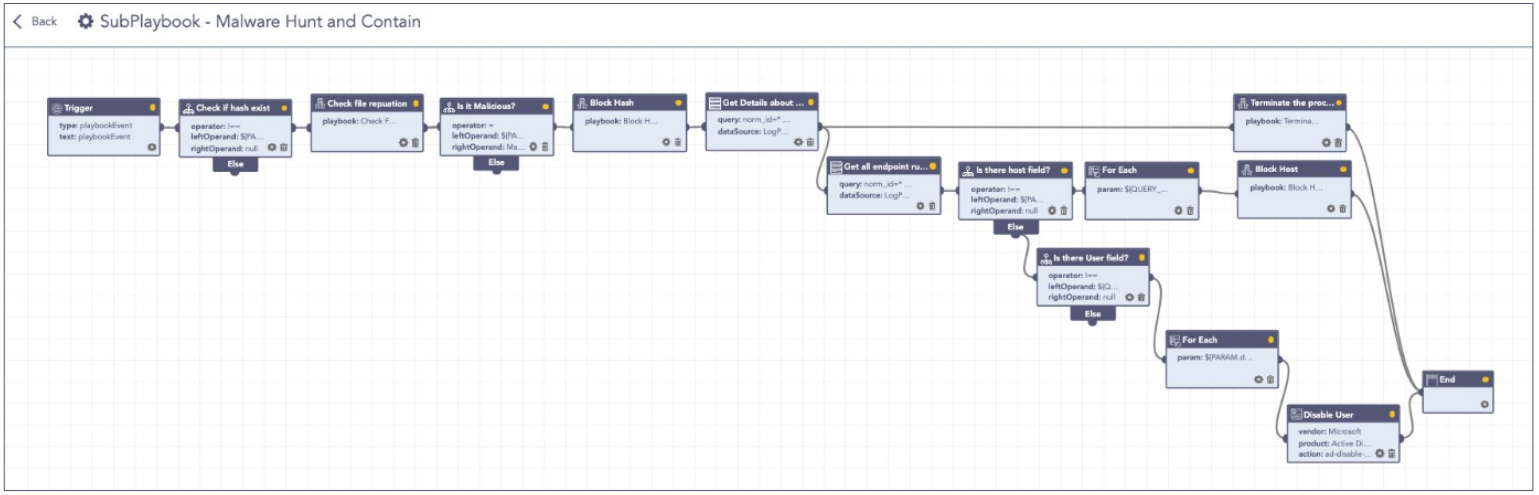
Speed up resolving malware alerts from hours to seconds

Fortunately, Logpoint SOAR can orchestrate and automate actions to investigate and respond to the high volume of alerts in a matter of seconds. Logpoint SOAR can also determine the severity of the alerts and respond accordingly, ensuring that the security team prioritizes the most critical malware attacks, drastically minimizing risk.

Protect endpoints from malware with Logpoint's pre-built malware playbook

The actions in this playbook include:

- Alerting on suspicious file download triggering the SOAR Malware playbook
- Extraction of actionable parameters from the incidents (file hash)
- File reputation check with Threat Intelligence
- Detonating suspicious files in a sandbox environment
- Adding the hash to the blocklist
- Querying SIEM to get the details of the file and process
- Terminating the process
- Querying SIEM to get all hosts with a malicious file
- Isolating infected machine(s)
- Running automated investigation playbooks looking for other malicious activities



Malware hunt playbook

Automated Phishing Investigation and Response

Phishing attacks are on the rise, and it does not seem that they will be gone soon. According to the 2021 Data Breach Investigation Report by Verizon, 36% of data breaches involved phishing, which is an 11% increase compared to 2020.

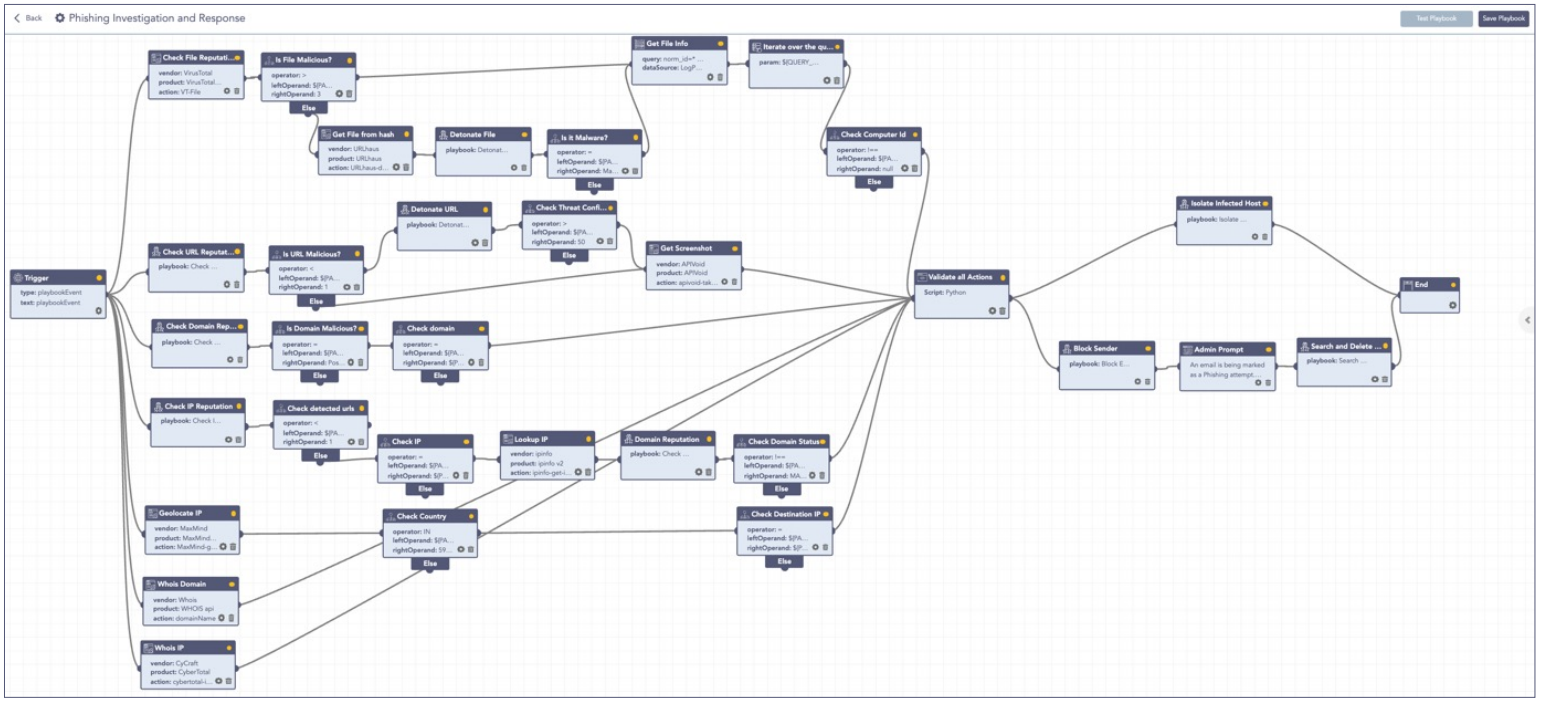
Consequently, security teams have many potential phishing emails every day to investigate. Manually investigating a phishing alert can take hours or even days for the analysts and require multiple security tools. If the SOC wants to bring in threat intelligence, correlations, or logs from other sources to investigate the threat properly, it takes even more time. These slow response times result in increased risk leading to potential damages to your organization.

Logpoint SOAR accelerates the phishing investigation and response time from hours to minutes with out-of-the-box playbooks. We created these playbooks to eliminate phishing attacks before they can cause irreversible damage to the organization. These automated response processes are ready to implement to reduce the manual and time-consuming tasks from day one. The solution integrates disparate security tools to simplify the incident response cycle and increase SOC productivity.

Respond to phishing attacks in minutes with the out of the box playbook within Logpoint SOAR

The actions in this playbook include:

- Phishing alert triggering the SOAR playbook
- Extraction of parameters from the incident (file hash, IP, domain, sender, receiver, subject)
- Parameter reputation check with Threat Intelligence
- Detonating suspicious files in a sandbox environment
- Blocking malicious email sender
- Searching for and deleting all infected emails
- Isolating infected machines



Phishing investigation and response playbook

Automated Threat Intelligence management

Threat Intelligence (TI) sources constantly expand to accommodate new and updated IOCs. This information is usually checked manually to ensure the validation of the alerts, which is a time-consuming and inefficient process.

Logpoint SOAR automatically collects and centralizes threat data from various threat intelligence sources, ensuring that analysts leverage the most current threat intelligence data. This data can be used to discover malicious indicators or to understand how different alerts are connected, enabling faster response to real threats, drastically minimizing risk.

Threat Intelligence capabilities of Logpoint SOAR include:

- Centralized collection of TI
- Lower risk rating on a TI feed, based on actual false positives found
- Fusion and deduplication of TI feeds
- Search and graph analysis of indicators
- Storage of machine-readable and nonstructured TI
- Distribution of TI to external tools, such as SIEM, EDR, and firewalls

Get the latest threat intelligence automatically at all times

The actions in this playbook include

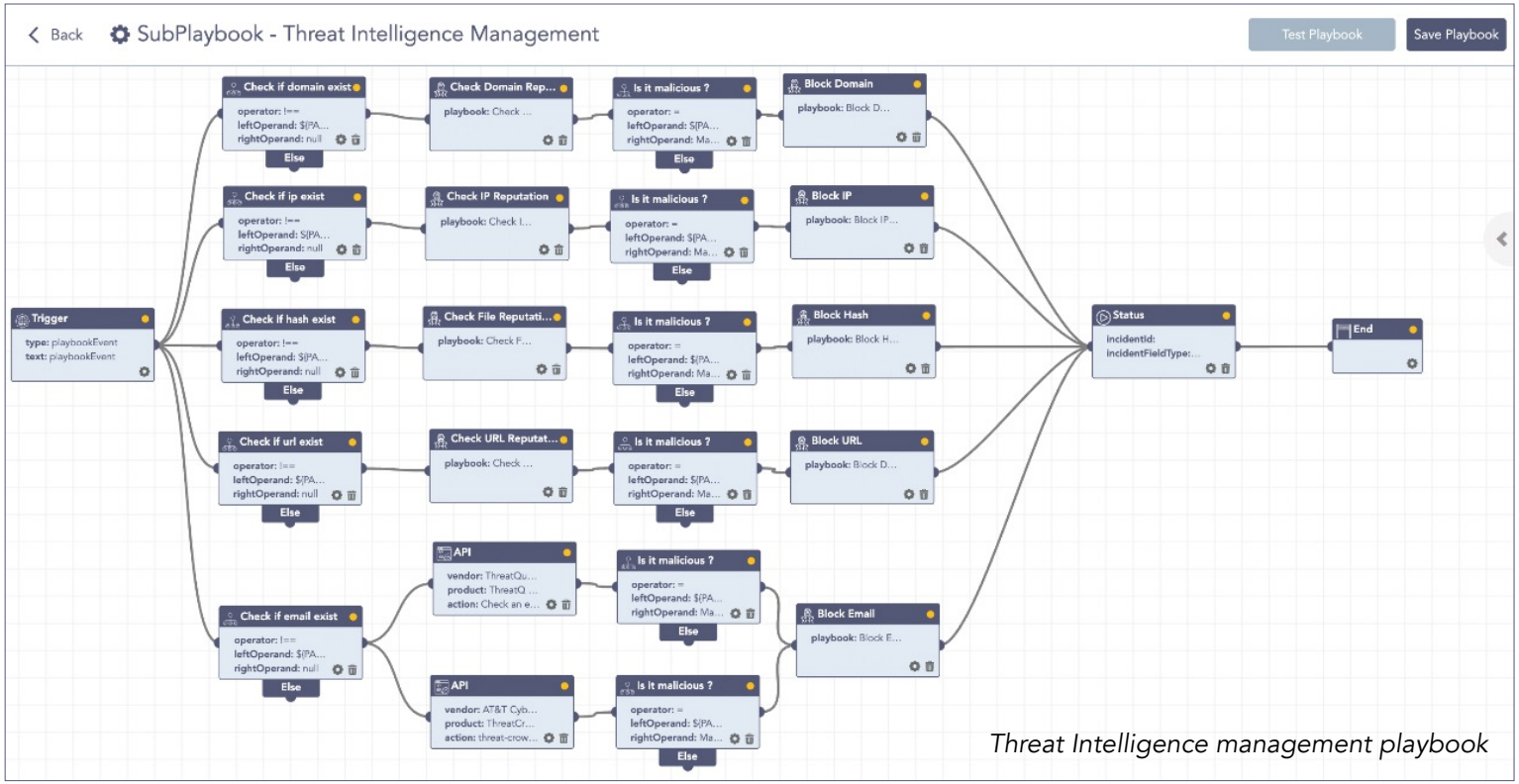
- Alert rule triggering the SOAR playbook
- Extraction of parameters from the incident (file hash, IP, domain, sender, receiver, subject)
- Parameter reputation check with Threat Intelligence

If found malicious

- Running a playbook to isolate affected endpoints and block malicious IoCs
- Setting the status of the case to Mitigated

Else

- Playbook end

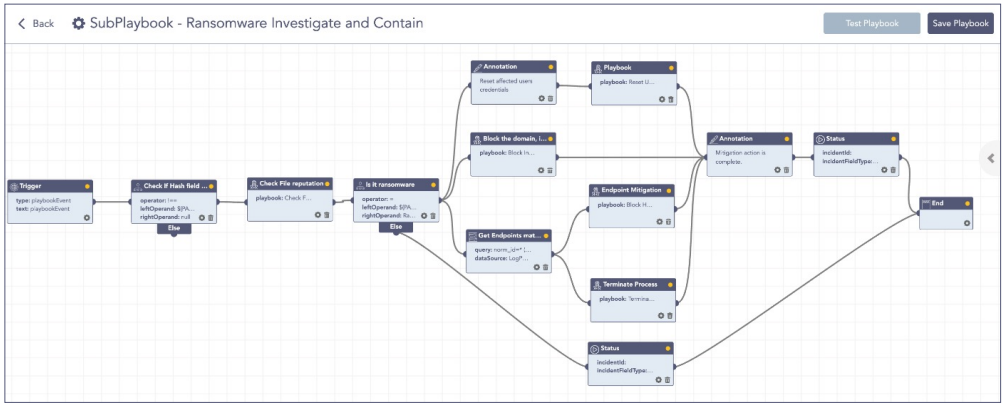


Threat Intelligence management playbook

Ransomware mitigation

Ransomware attacks are on the rise, while at the same time, variants are constantly evolving. According to the Cyber Threat Report by CyberEdge Group, 62% of organizations were victimized by ransomware last year. Ransomware attacks are fueled by the increasing number of companies willing to pay the ransom for recovering their data. As some advanced techniques are also coming into play, such as fileless malware, manually responding to these threats became a more challenging task. Therefore, rather than constantly improving existing endpoint protection platforms, companies should use a solution that can successfully detect and respond to the attacks.

When dealing with ransomware, the most critical factor is how much time it takes to detect and respond to it. The longer ransomware is active in the infrastructure, the costlier it is to recover from the attack. Logpoint has tied detection, classification, investigation, and response together for the analysts to accelerate the incident investigation process. Logpoint SOAR acts quickly and automatically based on the classification of the alerts mapped to the MITRE ATT&CK framework. Therefore, it is possible to detect and mitigate even the most advanced and sophisticated ransomware attacks in a matter of minutes without the long and complex manual processes that would tie up the analysts for hours.



Ransomware Investigation playbook

Protect your data from ransomware with Logpoint SOAR

The actions in this playbook include

- Possible ransomware attack rule triggering the SOAR playbook
- Extraction of parameters from the incident (file hash, IP, domain, sender, receiver, subject)
- Parameter reputation check with Threat Intelligence

If found malicious

- Changing the incident status to malicious
- Querying SIEM to identify affected endpoints that communicate with malicious IoCs
- Running a playbook to isolate affected endpoints and block malicious IoCs
- Terminating associated processes and services
- Resetting the credentials of affected users
- Setting the status of the case to Mitigated

Else

- Setting the status of the case to Benign

LOGPOINT