SWIMLANE

8 Real-World Use Cases for Security Orchestration, Automation and Response (SOAR)

Introduction

Security operations present an escalating series of management challenges. As the frequency and variety of attacks accelerate, even the best teams can get overwhelmed.

Security orchestration, automation and response (SOAR) offers a solution. Eighty to ninety percent of most security operations' tasks can be automated to some extent, and the data that disparate tools create can be distilled into a single pane of information. The resulting efficiency gains allow security teams to handle vastly **more** tasks while significantly **decreasing** mean times to resolution (MTTR).

Sounds good in theory, but how does security operations teams use SOAR in the real-world?

- Phishing Attacks
- SIEM Triage
- Threat Hunting
- Insider Threat Detection
- Threat Intelligence
- Identify Verification/Enforcement
- Endpoint Protection
- Forensic Investigation

Read on to learn how SOAR can help *your* team stay ahead of the bad guys.

SWIMLANE

Phishing Attacks

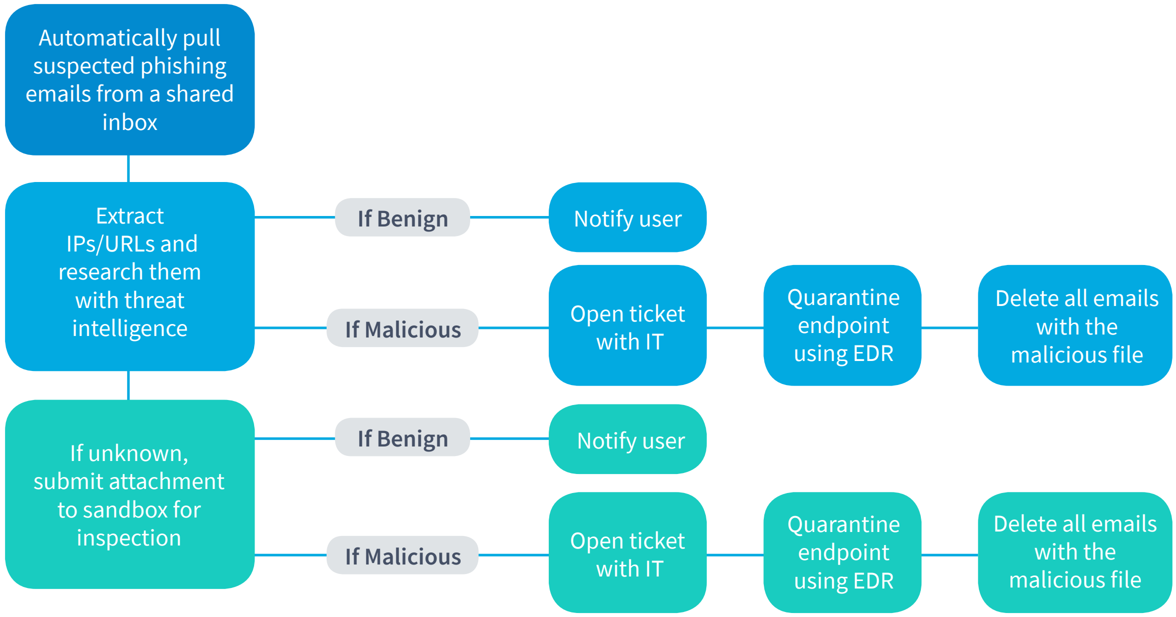
With millions of phishing emails sent out daily, it should be no surprise that there are new and increasingly-damaging attacks making headlines on a regular basis.

Problem

1. Too many potential phishing emails every day to investigate.
2. Investigations typically require the use of multiple security platforms.
3. Manual processes can take between 10-45 minutes per threat.
4. Most organizations lack the necessary personnel to investigate the high volume of daily phishing attempts.
5. Slow MTTRs increase risk and potential damages.

Solution

Automate the investigation and quarantine of suspected emails.



Automatically pull suspected phishing emails from a shared inbox

Extract IPs/URLs and research them with threat intelligence

- If Benign → Notify user
- If Malicious → Open ticket with IT → Quarantine endpoint using EDR → Delete all emails with the malicious file

If unknown, submit attachment to sandbox for inspection

- If Benign → Notify user
- If Malicious → Open ticket with IT → Quarantine endpoint using EDR → Delete all emails with the malicious file

Benefit

Security analysts can research and resolve the high volume of phishing attacks with minimal effort. Analysts can **automate 80-90 percent of the repetitive tasks** immediately. **MTTR is reduced** with responses initiated immediately upon an alert. Containment is performed at machine speeds.

Incident response processes are **clearly defined and consistently executed.** All suspicious emails are investigated properly, while human error is minimized at every step. Workflows can be easily adapted to incorporate new anti-phishing processes and technologies.

Technologies being used

- Email
- Threat Intelligence
- Sandboxing
- EDR
- Trouble Ticketing

SWIMLANE

SIEM Triage

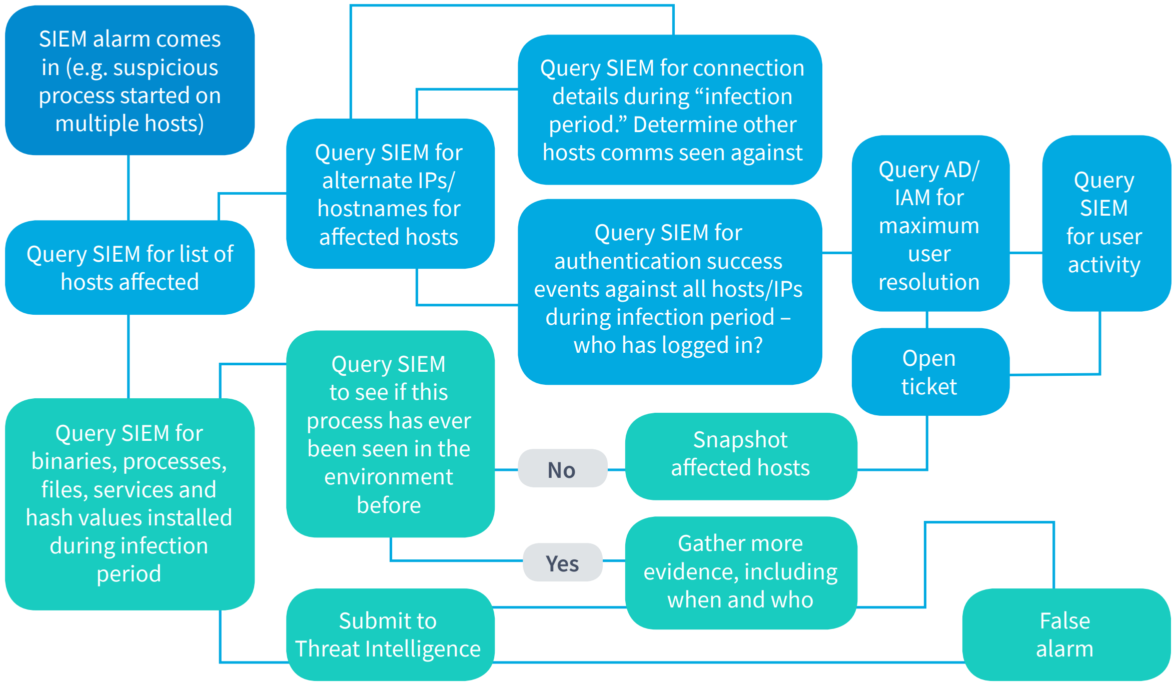
Less than 1 percent of severe/critical security alarms are ever investigated—and in many organizations, the majority are being generated by their SIEM. Security teams need to triage all alarms and potential threats—not just the highest rated.

Problem

1. Manually reviewing and investigating all SIEM alarms is logistically impossible.
2. SIEM alarms often lack necessary event context, requiring additional, time-consuming research.
3. SecOps are only able to investigate a small percentage of alarms, increasing the likelihood of missed attacks.

Solution

Automate as much of the process as possible while providing context to investigations.



SIEM alarm comes in (e.g. suspicious process started on multiple hosts)

Query SIEM for list of hosts affected

Query SIEM for alternate IPs/ hostnames for affected hosts

Query SIEM for connection details during "infection period." Determine other hosts comms seen against

Query SIEM for authentication success events against all hosts/IPs during infection period – who has logged in?

Query AD/ IAM for maximum user resolution

Query SIEM for user activity

Open ticket

Query SIEM for binaries, processes, files, services and hash values installed during infection period

Query SIEM to see if this process has ever been seen in the environment before

No

Snapshot affected hosts

Yes

Gather more evidence, including when and who

Submit to Threat Intelligence

False alarm

Benefit

The overwhelming number of SIEM alerts means **many alerts aren't investigated promptly, if at all.** By automating as much as 80-90 percent of the incident response process, SOAR enables security teams to address the high volume of alerts faster, without requiring more resources. The remaining tasks that need human intervention benefit from enhanced context and improved consistency.

SOAR radically improves security operations efficiency, while reducing risk and increasing threat protection. Quickly respond to *all* of your SIEM alerts.

Technologies being used

Active Directory/ IAM

SIEM

Threat Intelligence

EDR

Threat Hunting

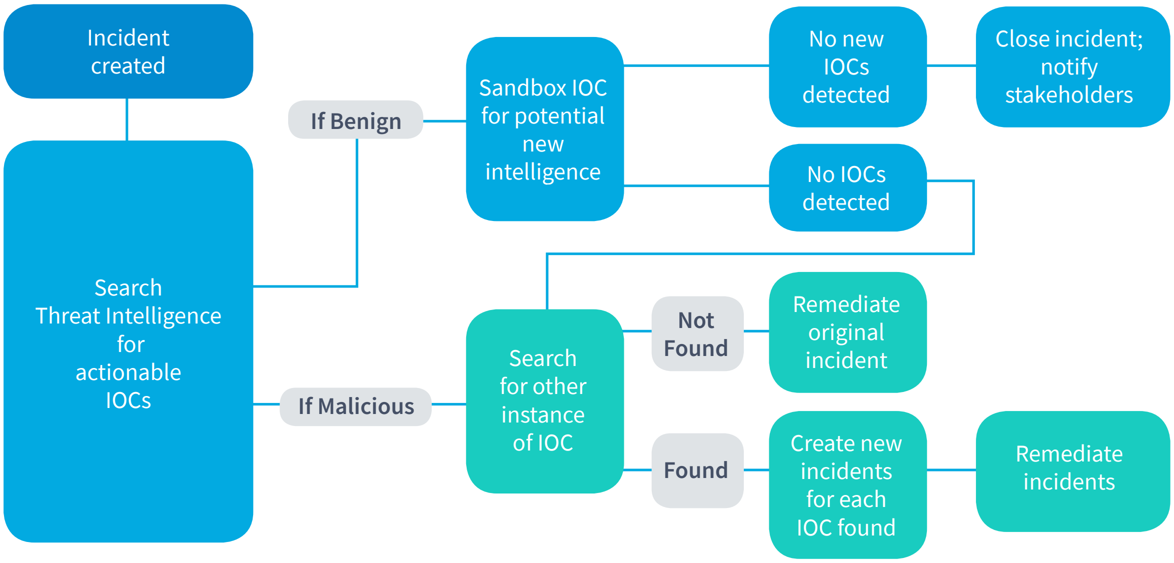
In today's threat environment, it's no longer enough to be passively vigilant. True protection requires proactively identifying and hunting for threats.

Problem

1. Slow, manual processes limit hunting frequency.
2. Collecting evidence requires manually drilling down into logs or packet captures.
3. Threat research validation requires accessing multiple 3rd party systems.

Solution

Automatically search indications of compromise (IOC) against threat intelligence.



Incident created

Search Threat Intelligence for actionable IOCs

If Benign

Sandbox IOC for potential new intelligence

No new IOCs detected

Close incident; notify stakeholders

No IOCs detected

If Malicious

Search for other instance of IOC

Not Found

Remediate original incident

Found

Create new incidents for each IOC found

Remediate incidents

Benefit

Integrating security technologies and taking advantage of a comprehensive and centralized view into all relevant threat data means that **analysts now have a clear picture of the complete landscape of an alert or incident without having to manually hunt** for this information. By automating time-consuming and repetitive tasks, analysts can spend more time hunting new threats and getting ahead of advisories.

Continuous hunting using automated workflows to leverage a fully integrated security infrastructure empowers proactive protection by helping SecOps stay on top of threats and understanding all **integrated threat information.**

Technologies being used

SIEM

Threat Intelligence

Packet Capture

Sandboxing

EDR

SWIMLANE

Insider Threat Detection

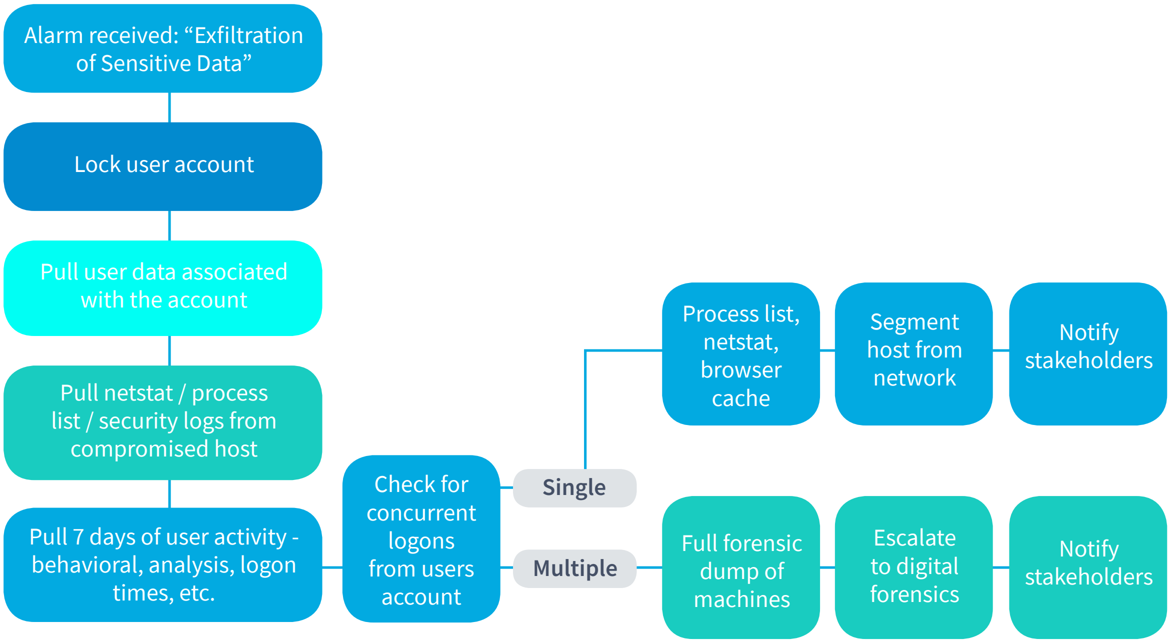
Malicious and negligent acts from insiders and attacks using stolen credentials are a major source of successful breach attempts. But quickly identifying insider threats is a challenge for security operations teams.

Problem

1. Researching and validating potential insider threats require extensive manual effort.
2. A disparate set of security tools is necessary to verify potential insider threats, requiring analysts to investigate in each tool to get a complete picture of the incident.
3. Insider threat activity frequently emulates normal behavior and is spread out over multiple systems, making it hard to detect and understand the scope of an attack.
4. Reducing MTTD and MTTR is critical for minimizing the damage tied to insider threats.

Solution

Integrate multiple tools for rapid insider threat detection and response.



Alarm received: “Exfiltration of Sensitive Data”

Lock user account

Pull user data associated with the account

Pull netstat / process list / security logs from compromised host

Pull 7 days of user activity - behavioral, analysis, logon times, etc.

Check for concurrent logons from users account

Single

Process list, netstat, browser cache

Segment host from network

Notify stakeholders

Multiple

Full forensic dump of machines

Escalate to digital forensics

Notify stakeholders

Benefit

By using SOAR platforms, you can easily reduce MTTR and further protect your organization by making it possible to identify and stop insider **threats before they cause major damage.**

Integrating your security toolset and orchestrating threat detection gives your security team a **complete understanding of all insider threat detection alerts.** Automating significant components of the detection and response process makes your entire security infrastructure more effective without adding overhead.

Technologies being used

EDR

SIEM

DLP

User Behavior Analytics

Threat Intelligence

SWIMLANE

Threat Intelligence

Effectively leveraging comprehensive IOC data throughout your security infrastructure is inefficient and time-consuming without orchestration and automation.

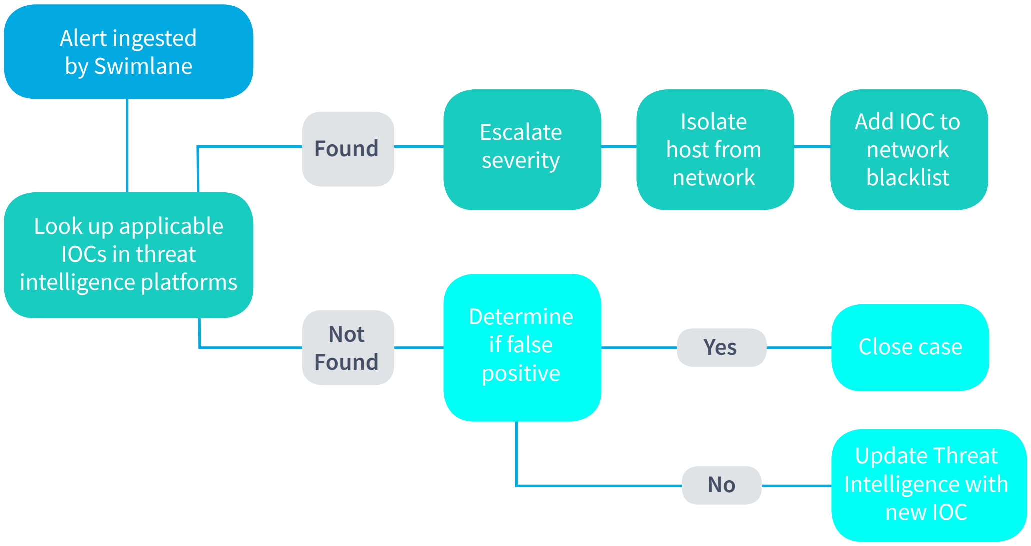
Problem

1. Threat intelligence feeds are constantly evolving to accommodate new and updated indicators of compromise (IOCs). Ensuring accurate validation of security alarms requires continuously checking them against up-to-date IOCs to ensure that they are real—a time consuming and inefficient manual process.

2. In the amount of time it takes for an analyst to get the alert, check threat intelligence feeds, make a decision, and submit network change requests, the malicious actor will have plenty of time to gather information and perform any tasks necessary.

Solution

Automate the lookup of IOCs in all threat tntelligence platforms.



Alert ingested by Swimlane

Look up applicable IOCs in threat intelligence platforms

Found

Escalate severity

Isolate host from network

Add IOC to network blacklist

Not Found

Determine if false positive

Yes

Close case

No

Update Threat Intelligence with new IOC

Benefit

SOAR solutions provide security teams with an efficient and nearly instantaneous way of ensuring their security infrastructure is **leveraging the most current threat intelligence data at all times.** By operating with an accurate and up-to-date understanding of IOCs, **analysts are able to respond faster to real threats,** drastically reducing MTTR and minimizing risk.

Technologies being used

SIEM

Threat Intelligence

Next Gen Firewalls

Identity Verification/ Enforcement

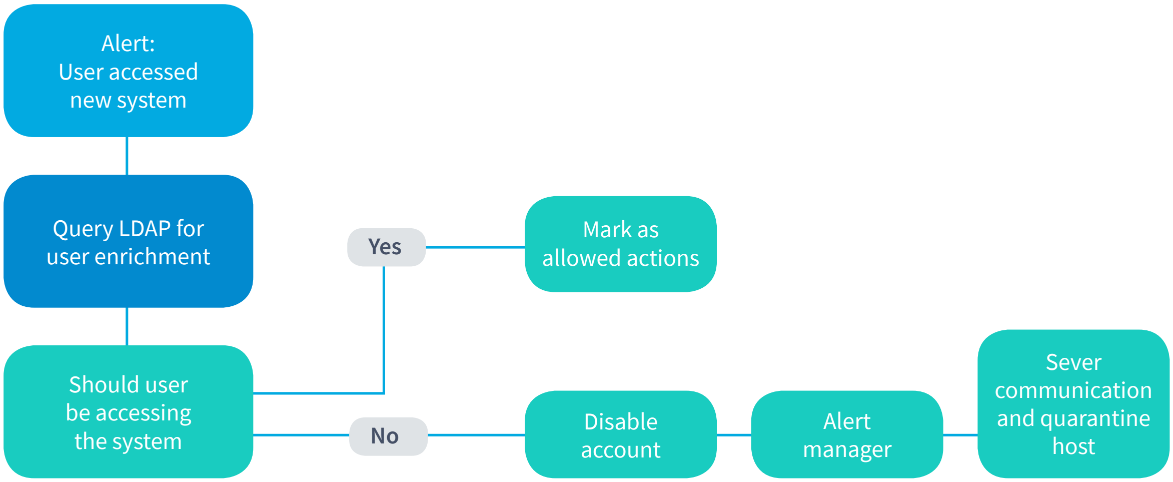
The smooth and rapid verification of privileged credentials is critical to maintaining good security hygiene. Security operations is challenged to ensure easy access by legitimate users while also protecting against stolen or improper use of credentials.

Problem

1. Large organizations can't feasibly validate all user activity at all times.
2. Security teams need to quickly determine if new user behavior is legitimate or malicious.
3. Manually checking user permissions to identify aberrant behavior is slow and time consuming.

Solution

Automatically validate user permissions for specific resources.



Benefit

It is important that enterprises can verify and control the access of confidential information to protect against data breaches. If verification shows a high likelihood of unauthorized behavior, **automatic actions** can disable the user account and quarantine the host from the network to avoid further malicious activity.

Security analysts can also automate other protective actions like running AV scans and disabling AD accounts, so the **effects of the malicious activity can be mitigated as quickly as possible.**

Technologies being used

Active Directory/LDAP

EDR

UEBA

SWIMLANE

Endpoint Protection

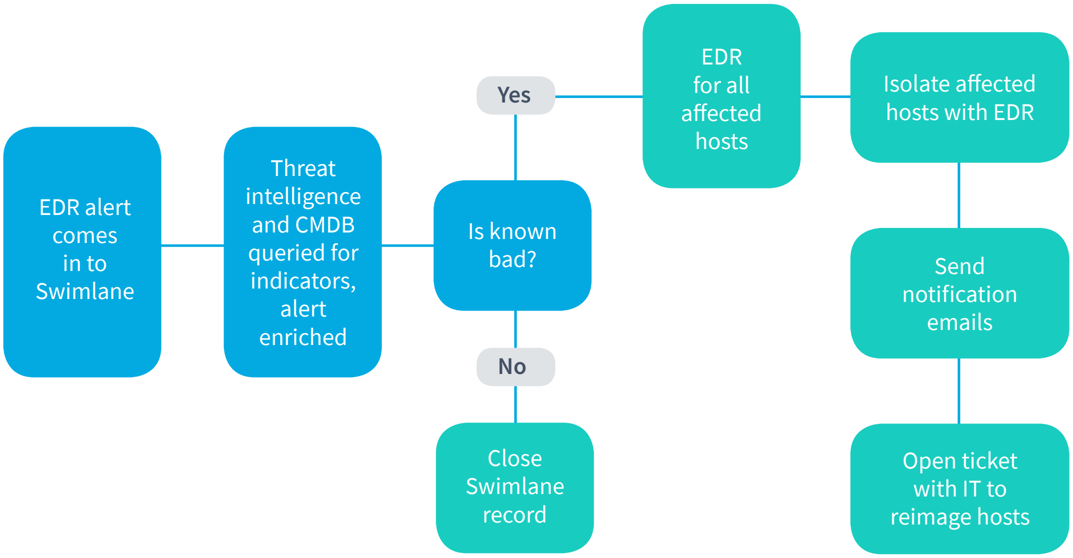
Endpoint related alerts can quickly overwhelm a security operations team and prevent an effective alert response.

Problem

1. Large organizations have hundreds or thousands of endpoints generating alarms tied to potential threats every day.
2. Manually executing high volume endpoint actions in an enterprise environment is time consuming and ineffective.
3. Slow MTTR leads to broader threat proliferation and greater risk.

Solution

Automatically triage endpoint-related alerts and take appropriate remediation action.



EDR alert comes in to Swimlane

Threat intelligence and CMDB queried for indicators, alert enriched

Is known bad?

Yes

EDR for all affected hosts

Isolate affected hosts with EDR

Send notification emails

Open ticket with IT to reimage hosts

No

Close Swimlane record

Benefit

Swimlane can **automatically triage** endpoint-related alerts by enriching the data with external Threat Intelligence sources, internal sources like a CMDB, or querying an EDR tool for additional context, find other affected endpoints by querying the EDR tool, and **take appropriate remediation actions** like isolating an endpoint, killing processes, etc.

Using security automation and orchestration ensures that **all endpoint-related alerts are addressed.** Response and remediation actions can be taken in real-time, helping **prevent incidents from escalating into full-fledged security breaches.**

Technologies being used

SIEM

EDR

Forensic Investigation

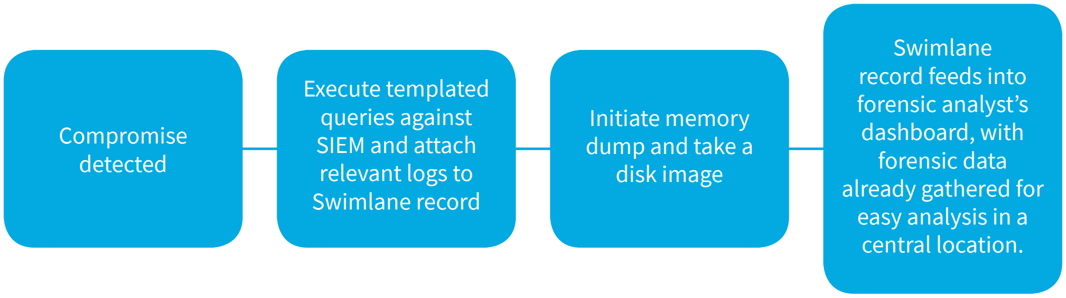
SOAR platforms streamline investigations by automating forensic data collection from disparate tools and providing a centralized repository for all collected evidence. Integrated case management provides immediate, intuitive access to all forensic detail necessary to rapidly conduct an investigation.

Problem

1. Gathering forensic detail post-incident is a cumbersome manual task.
2. Investigators are typically required to access evidence from multiple 3rd party systems.
3. Evidence is often stored in multiple locations.

Solution

Automatically centralize relevant forensic data.



Compromise detected

Execute templated queries against SIEM and attach relevant logs to Swimlane record

Initiate memory dump and take a disk image

Swimlane record feeds into forensic analyst's dashboard, with forensic data already gathered for easy analysis in a central location.

Benefit

Swimlane can automatically query a SIEM tool to gather relevant forensic log data and automatically initiate actions in forensic software to gather endpoint data, such as memory dumps and disk images. All of this data can be automatically centralized within Swimlane until the forensic investigator performs more detailed analysis.

Analysts don't have to waste time gathering information from a variety of sources; security orchestration centralizes this information. A forensics investigator **doesn't have to manually leverage different tools** to gather the forensic detail required for an in-depth investigation, allowing them to spend more time **analyzing and less time performing administrative functions.**

Technologies being used

SIEM

Forensic Software

About Swimlane

Swimlane is at the forefront of the growing market of security automation, orchestration and response (SOAR) solutions and was founded to deliver scalable and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages.

Swimlane's solution helps organizations address all security operations (SecOps) needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats—improving performance across the entire organization.

To arrange a demo of Swimlane or to speak with one of our security architects to see if security orchestration, automation and response would be helpful to your organization, please contact us at 1.844.SWIMLANE or www.swimlane.com