SWIMLANE

SIEM Alert Triage

How Swimlane's SOAR solution speeds up the SIEM alert triage process.

Security operations centers (SOC) are widely adopting SIEM to analyze a broad range of network, user and host behavior to identify patterns that indicate possible cyberattacks. These technologies accomplish this by collecting and correlating data from devices across the organization. Using predefined advanced analytics rules, SIEMs identify abnormalities and send alerts with relevant event context to the SOC team. Analysts then typically follow a manual triage process to determine whether an alert is a false positive and can be dismissed or if it's a real threat needing to be escalated. SOAR plaforms enables the automation of the SIEM alert trige process.

Challenges with SIEM tools

Alert Fatigue

Security teams are overwhelmed by the volume of daily alerts they receive from security information and event management (SIEM) tools. In a recent report by Enterprise Management Associates (EMA), many lament an excess of 10,000 alerts per day. Even more frustrating, analysts report a 50 percent or higher (up to 99 percent) false-positive rate, rendering their investigative efforts minimally effective. Attempting to decrease the number of false positives generates a futile, never-ending cycle of new rule creates and tuning of the SIEM. When analysts are only able to investigate a fraction of the real alerts that come in each day, threats go unnoticed, leaving the organization vulnerable.

Disjointed technology stack

When performing alert triage, analysts use various tools to enrich the alarm data with context to both validate and assess the potential impact of the threat. While there may be limited integration with the SIEM, analysts are typically forced to perform triage actions independent of the original alert, using multiple UIs and platforms. Some SIEM providers offer functionality that mitigates triage process inefficiencies to a degree, but analysts must often complete the majority of the triage and incident response process manually. The resulting inefficiencies increase mean time to resolution (MTTR) and organizational risk.

Automating SIEM alert triage with SOAR

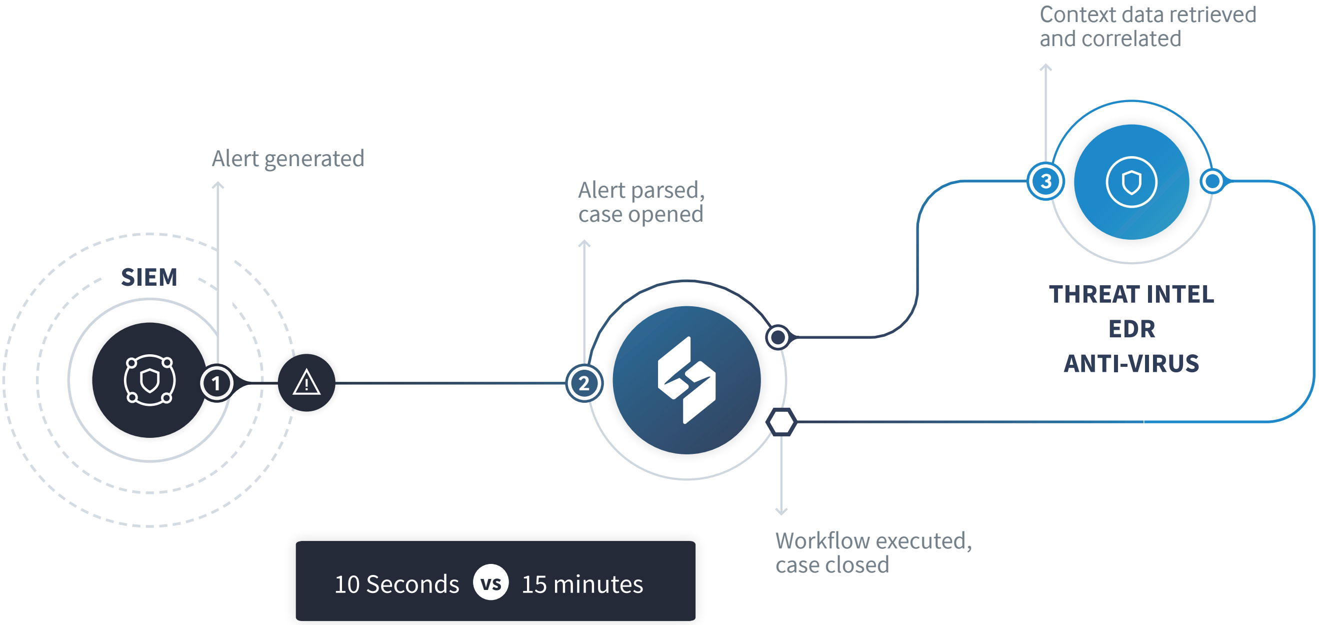
Security orchestration, automation and response (SOAR) platforms have extensive capabilities for automating and orchestrating the SIEM alert triage process by integrating previously disjointed tools and bringing all relevant data into a centralized case management interface. Security analysts can leverage existing out-of-the-box content or set up unique case views and configured workflows to automatically pull in necessary data and execute triage actions for different types of SIEM alerts. Swimlane can fully automate the incident response process to triage alerts, quickly identifying and eliminating false positives while escalating valid threats performing anything from initial analysis and validation to full remediation. When internal policies prevent or prohibit automated processes, Swimlane can queue up the incident for a one-click manual resolution directly within the case record. A drag-and-drop workflow builder and the flexibility to customize workspaces, dashboards and case views allow analysts to fine tune Swimlane for optimal SIEM alert triage.

False Positive Reduction

Problem: SIEM tools generate an overwhelming number of false positive alarms. The security team is often unable to triage and respond to such a high volume of alerts, which may allow real threats to go undetected.

Solution: Swimlane can fully automate the process of triaging SIEM alarms to identify and dismiss false positives quickly, which can enable security analysts to clear their queue and ultimately save time. While the manual SIEM alert triage process can take several minutes or longer per alert, automating the process takes only seconds—rapidly decreasing MTTR with the ability to respond at machine speeds.

Benefit: Swimlane eliminates alert fatigue and empowers analysts to analyze and respond to all incoming SIEM alerts, thus reducing security risk. This enables analysts to spend their limited time on the remediation of real threats, free from the alert noise generated by a SIEM.

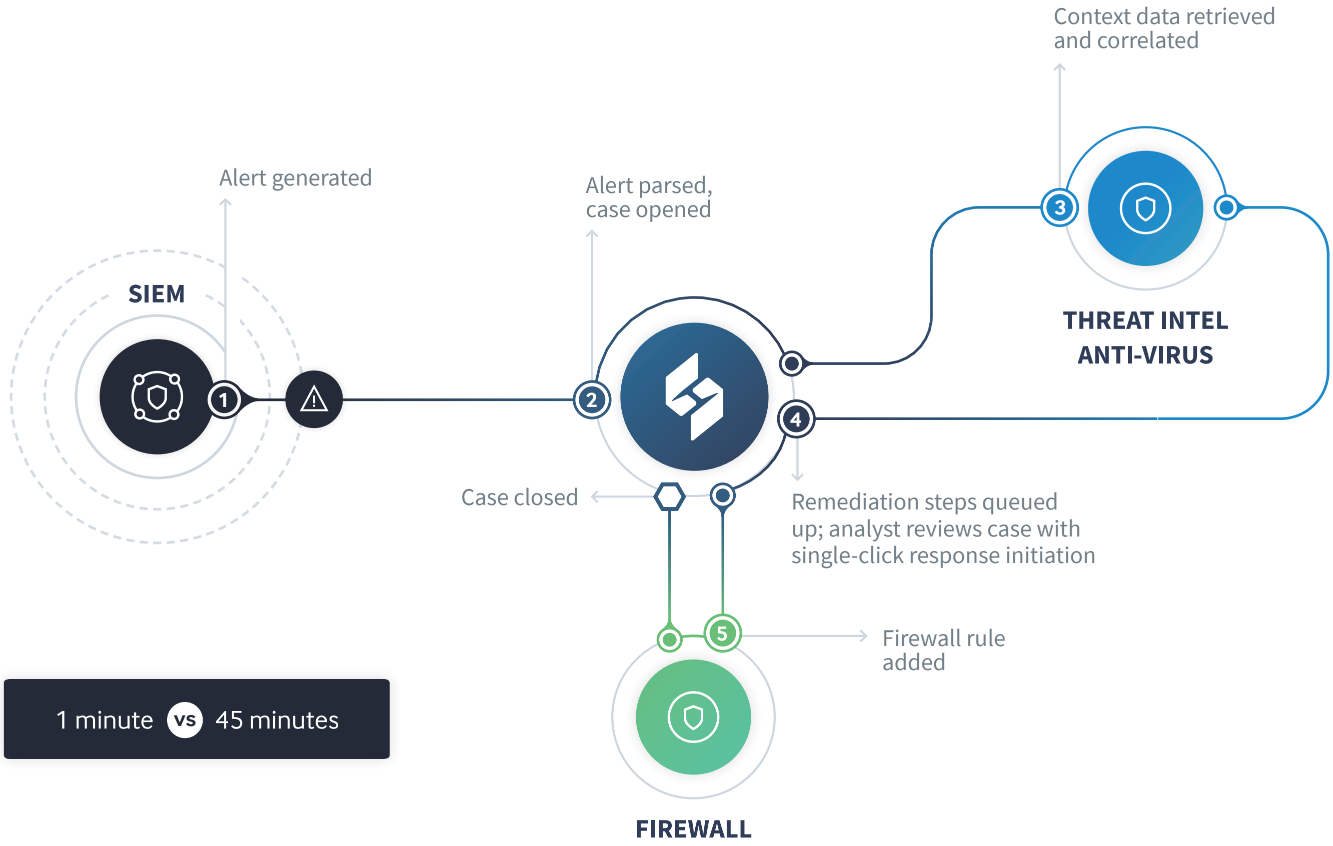

Context data retrieved and correlated
Alert generated
Alert parsed, case opened
SIEM
1
2
3
THREAT INTEL
EDR
ANTI-VIRUS
Workflow executed, case closed
10 Seconds VS 15 minutes

Process Optimization

Problem: When triaging SIEM alerts, analysts typically spend most of their time performing each step manually, while switching between multiple tools. Such manual and disjointed environments result in increased MTTR and inconsistent response processes.

Solution: Swimlane automates the manual, repetitive steps of the SIEM alert triage process and consolidates necessary event data for the analyst. Customized case management views allow organizations to tailor their processes based on their unique needs to enforce consistent incident response and streamline execution.

Benefit: Swimlane delivers a centralized case management environment embodied in an optimized platform that acts as a control hub for all incident response processes. SOCs gain back control over their SIEM alert triage process, resulting in an enhanced security posture for the whole organization.


Context data retrieved
and correlated
Alert generated
Alert parsed,
case opened
SIEM
1
2
3
4
5
THREAT INTEL
ANTI-VIRUS
Case closed
Remediation steps queued
up; analyst reviews case with
single-click response initiation
Firewall rule
added
1 minute vs 45 minutes
FIREWALL