CHECK POINT sumo logic

YOU DESERVE THE BEST SECURITY

CHECK POINT + SUMO LOGIC

Easily orchestrate all your tools to empower SecOps

KEEP CYBER INCIDENTS UNDER CONTROL

Benefits

- All-in-one platform to improve your own processes (SOP)
- Easily orchestrate your tools leveraging Open Integration Framework
- Save time and focus on real Threats
- Automate mundane tasks
- Reduce false positives
- Respond to attacks in less time
- Centralize threat intelligence

Features

- Runbooks to efficiently improve SecOps processes
- Accurate & automated enrichment of alarms
- Progressive automation of time-consuming activities and mundane tasks
- Alarm Triage Management to empower reduction of false positives
- Immediate detailed Incident reports with related IOC's, timeline and corrective actions executed
- KPIs dashboards for analyst, SOC manager, CISO, audit manager
- Native Multi-Tenancy platform

CHALLENGE

Nowadays, cyber threats are becoming more difficult to trace and more unpredictable, which leaves analysts with the difficult task of investigating and containing each threat as it arrives in real-time. Security operations require the merging of intelligence, both from in-house staff and technology solutions to effectively respond to the following challenges.

- An increasing number of alerts
- False positives and false negatives
- Overwhelming workload for SecOps and SOCs
- Sophisticated attacks with no recognizable patterns

JOINT SOLUTION

With Sumo Logic SOAR and Check Point Next Generation Threat Prevention network, mobile, endpoint and cloud enforcement points, analysts will have the time to orchestrate, and efficiently implement a more effective security solution that keeps up with the fast pace of emerging threats. The integrated solution combines several approaches for responding to advanced threats. First, prevent the threat with static and dynamic CPU-level sandbox analysis. Second, endpoint forensics tracks activities of malware providing a path back to the initial infection. Third, infrastructure-wide event correlation hastens the time to identify and remediate infected devices. This enables security analysts to expedite incident response by automating the steps needed to block malicious sources and quarantine any compromised devices.

SOAR STARTS WHERE DETECTION STOPS

Sumo Logic SOAR (Security Orchestration, Automation, and Response) platform enables enterprises and MSSPs to improve security operations processes by identifying suspicious events that require deeper analysis.

First Sumo Logic SOAR leverages security events from Check Point to derive threat intelligence from tracked security observables.

Second Sumo Logic SOAR enriches alarms and blocks threats, enabling analysts to implement a more effective security solution, create detailed reports with related IOC’s, timeline, corrective actions and other information.

Third, using Check Point APIs Sumo Logic SOAR enriches and validates alarms and then manages the Check Point security policy to block threats.

© 2022 Check Point Software Technologies Ltd. All rights reserved. [Protected] | March, 2022

HOW AUTOMATION WORKS

Here are some Check Point actions that can be orchestrated and progressively automated with Sumo Logic SOAR.

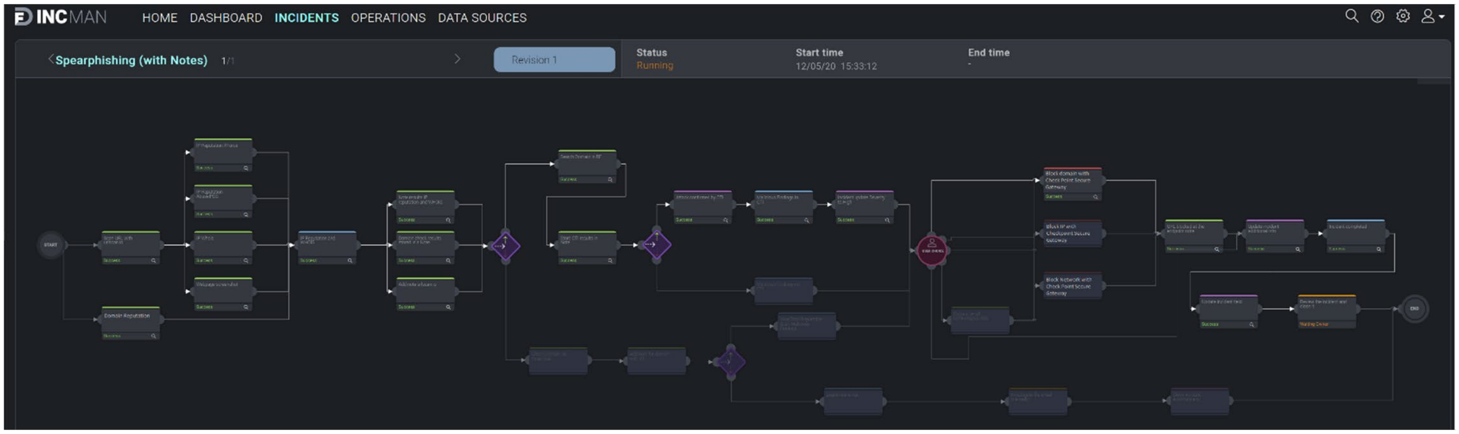
Enrichment leveraging Check Point actions:

- Show access rule base
- Show threat rule base
- User attributes
- Domain Info
- IP Info

Containments leveraging Check Point actions:

- Add/delete threat rule
- Block/unblock Domain
- Block/unblock IP
- Unlock user
- Delete rule
- Block/unblock Port

Runbooks improve SecOps processes and allow analysts to follow Standard Operating Procedures (SOP).
A Sumo Logic runbook is a graphical definition of a workflow to resolve an incident or complete an investigation. In runbooks, Check Point actions can be easily called up via API connectors to the Check Point security management server.



An Example Sumo Logic SOAR Spear Phishing Runbook: Ban a Domain with Check Point NGFWs

The role of automation in SOAR is to ease the burden of cyber security organizations by automating repetitive behavior and recurring tasks. The degree of automation can be adjusted, and security teams can determine whether they want some tasks to include human interaction (extremely fundamental in some processes) or if they want all of their tasks to be fully automated.

Via automation, security teams can deal with potential alerts in a faster, more effective manner, and also have total control of the tasks where they wish to include human interaction. The degree of automation is completely adjustable, and security teams can choose to fully automate time-consuming and repetitive tasks and also include human interaction in tasks that require expert attention.

EASE OF INTEGRATION

Sumo Logic SOAR allows clients and partners to create an integration with various tools in 3 days average time, with no advanced coding experience required beforehand. Thanks to orchestration, you can connect all the technologies SecOps need through API connectors. This permits replication and improvement of SOC processes, and security analysts have all the information they need on one unique SOAR platform. This way you can benefit from the full power of Check Point Next-Gen Firewalls by calling up their actions within runbooks to respond quickly to threats.

© 2022 Check Point Software Technologies Ltd. All rights reserved. [Protected] | March, 2022

SUMMARY

With Check Point and Sumo Logic, security teams have a solution to improve Standard Operating Procedures to keep up with the fast pace of cyber attacks and scale their infrastructure. This combined approach offers a number of benefits, including:

Improve SecOps process
With Sumo Logic and Check Point, users have a single, consistent method to add observables to configured block lists, distribute them to all Check Point security gateways and create standardized workflows based on these insights.

Optimizing security response
SOAR allows security teams to automate repetitive, mundane, and time-consuming tasks by effectively tackling alerts from detection to resolution in a fast and concise manner. Sumo Logic SOAR's triage capability allows reducing the number of false positives and other red flags raised by an elevated number of suspicious events that have to be inspected and can be achieved with different techniques of pre-processing based on automation, machine learning, correlation, and aggregation of events.

Faster and more efficient incident reporting
Sumo Logic SOAR allows analysts to be more effective as it creates extremely fast incidents reports that only take a couple of minutes. SOAR provides an immediate and detailed incident report of the corrective actions executed.

Centralizing threat intelligence
Sumo Logic's dashboard and reporting capabilities for collecting security incident data from distributed Check Point NGFWs allows analyst teams to have centralized visibility into their security environment.

Probatory role and Chain of custody
Sumo Logic's case management also handles forensics, the evidentiary chain of custody of the incident response processes, including but not limited to, reports, evidence preservation, integration with forensic technology, incident artifact, IoCs, etc. Via case management, clients can stay on top of all of the relevant information of a cyber incident, including the elements which have been found, the type of attack that was intended, and who made the attack. Sumo Logic' evidentiary and probatory role provides in-depth information in over a hundred customizable case management fields.

Multi-Tenancy and clustering
IncMan SOAR applies a sophisticated multi-tenant engine, which is specifically designed to support both MSSPs and also adjust to complex corporate environments.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT SUMO LOGIC

Sumo Logic Inc. (www.sumologic.com) is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy.