Check Point SOFTWARE TECHNOLOGIES LTD. Siemplify

WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT + SIEMPLIFY

THE ORCHESTRATION, AUTOMATION AND RESPONSE STACK

SOAR TO A HIGHER SOC LIFESTYLE

Benefits

- Automate contextual grouping of alerts to clean up your queue and streamline cross-product triage
- Run playbooks that automate away false positives and consistently reduce response times
- Manage and measure the success of your SOC from a single view with ticketing and dashboards
- Collaborate on cases with internal and external teams directly from the platform
- Kick off with Check Point use cases created by Siemplify power users and the Siemplify Community

Integration Capabilities

- Fusing data coming from Check Point products onto one canvas with over 200 additional products
- Grouping Check Point detections with other sources to create a single contextual case
- Automating malware analysis processes with Check Point SandBlast
- Blocking IP/URL addresses in Check Point NGFW
- Automating firewall rule management in Check Point NGFW

CHALLENGE

The most pressing challenges in security operations are well known: 1) the overload of alerts flooding the SOC, which forces teams to skip countless alerts just to keep up, 2) the growing stack of tools used to respond to these alerts, 3) the reliance on manual and inconsistent processes which simply cannot compete with the evolving technologies used by the bad guys and 4) the shortage of talent, which makes virtually all security operations teams feel understaffed and overworked.

SOC teams need a scalable solution that can bridge the talent gap and provide the much-needed working power for a more effective SOC and a better SOC lifestyle. This brief explains how this can be achieved by combining Check Point products with security orchestration, automation and response (SOAR) through the Siemplify Security Operations Platform.

THE SOLUTION

The Siemplify SOAR platform connects to your entire technology stack and provides a single workbench for security analysts to solve threats and work side by side with automated flows that accelerate the incident response processes.

This is demonstrated with the following use cases:

1 - AUTOMATE ALERT HANDLING AND CASE MANAGEMENT

Challenge

Thanks to an increasing and often overwhelming number of threats, security stacks are generating a massive volume of alerts and, in turn, a steady procession of incident response (IR) processes. However, many organizations are still relying on manual tasks to work through their alerts, meaning securing your organization is getting more challenging by the day.

Solution

To handle the growing backlog of investigations, from phishing to malware to rogue insider, a security analyst needs to go far beyond validating and blocking a specific threat. In fact, before initiating any playbook, the Siemplify Security Operations Platform first, and continuously, analyzes each alert as it comes into the system, looking for contextual relationships. If a relationship is identified, the alert gets automatically grouped with the related alerts into a case. Then, the Siemplify platform is integrated with the Check Point Next Generation Firewall (NGFW) to automatically block an attack on the firewall and/or disable a compromised user in the enterprise.

Value

Siemplify connects the security operations center with Check Point products to streamline every step of detection and response, replacing manual processes with automated workflows that ensure optimized triage, investigation and containment.

2 - STREAMLINE FIREWALL POLICY MANAGEMENT

Challenge

With endpoints proliferating across businesses, firewalls help control traffic based on actions configured within their policies. Poorly implemented firewall rules can lead to major business risks. Standardizing these firewall policy actions across disparate networks, processes and platforms poses a significant impediment for businesses with a large user population.

Solution

Playbooks running inside the Siemplify Security Operations Platform that are integrated with Check Point NGFW can be scheduled to run at set intervals for firewall policy management. Operators can automate auditing and remediation, such as activating a firewall rule, and workflows can tie into ticketing systems to notify administrators and track efforts.

Value

Optimizing firewall auditing and remediation to identify rules violations and analyze access policies can considerably reduce firewall management, freeing up SOC analysts to concentrate on higher-order tasks

3 - ADVANCED MALWARE ANALYSIS AND PROACTIVE FIREWALL UPDATES

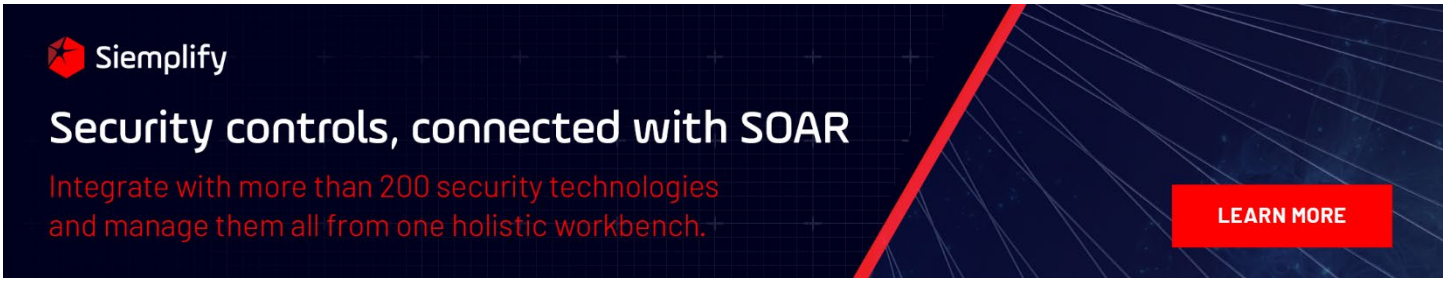
Firewall block lists need to be tight and precise to reduce false positives and security headaches. In Siemplify, a common way to increase accuracy surrounding indicators of compromise (IOCs) is to leverage multiple sources of threat intelligence to increase diversity of opinion and classification accuracy. But what when threat intelligence does not have an answer?

Solution

The most abundant type of IOC is the file hash. Using advanced sandboxing technology, such as Check Point's Sandblast, the security team can take advantage of threat intelligence and sandboxing automatically in a single pane of glass through Siemplify. The playbook queries SandBlast initially to see if the file already has classification, and then if not, it detonates the file using the same integration, then finally pulls the result and pushes it into their NGFW if it returns negative and has the option to triple check with additional sources of threat intelligence.

Value

Through Siemplify, the security team gets the full power of Check Point SandBlast's API to refine intelligence surrounding files of questionable reputation, as well as the customizability of adding further checks to 3rd party intelligence. They can automatically then maintain and update the IOC values of their Check Point NGFW's block lists. Additionally they can continue to automate their security processes in Siemplify and proceed to automated remediation or other steps depending on the relevant security alert.



ABOUT SIEMPLIFY

Siemplify is the leading vendor-agnostic security operations platform globally, and is consistently chosen by world's best security teams, from Fortune 500 firms to global MSSPs, as their security platform of choice. Siemplify provides much more than playbooks and automation. Based on years of expertise running and training military and civilian SOCs across the globe, Siemplify has built a complete security operations platform that addresses the broadest set of SecOps needs. With built-in case management, investigation, crisis management, collaboration, KPI tracking and a rich library of built-in knowledge – Siemplify is a true workbench for analysts and engineers, and the SOC manager's secret weapon to driving continuous improvement.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyber attacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.