Check Point + Splunk

Accelerate Cyber Threat Prevention

Accelerate Threat Prevention

Benefits

- **Focused Security Analysis and Reporting:** Correlates logs from all enforcement points, network cloud, endpoint and mobile to identify suspicious activity, track trends and investigate and mitigate incidents.
- **Reduce Incident Analysis Time:** Correlation of millions of logs from Check Point and security devices across your organization identifies significant events easily, reducing your overall investigation response time.
- **Automate Incident Response:** Rapidly investigate incidents and seamlessly trigger mitigation policies on Next-Gen Threat Prevention devices.
- **Customizable Views and Reports:** Security events automatically alert on critical events.

Challenge

Targeted advanced persistent threats place high demands on security staff charged with remediating the effects of those threats. Unfortunately, traditional Next-Gen Firewall products that only detect and not prevent threats create more work for security and helpdesk staff. Security staff are left to sift through a lot of logs and alerts to find the path back to the initial infection and may miss critical events. The advantage goes to the threat actors, who have ample time to achieve their goal.

Solution

Check Point Software® and Splunk® address this problem with an integrated solution that delivers highly effective threat reporting, incident forensics investigation, and automated response to block advanced cyber threats. With the Check Point App for Splunk, security teams have a powerful platform for security visualization, monitoring and analysis that enables them to fully leverage the extensive threat data visible to Check Point Next Generation Threat Prevention network, mobile, endpoint and cloud enforcement points.

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 administrators to expedite incident response by automating the steps needed to block malicious sources and quarantine any compromised devices.

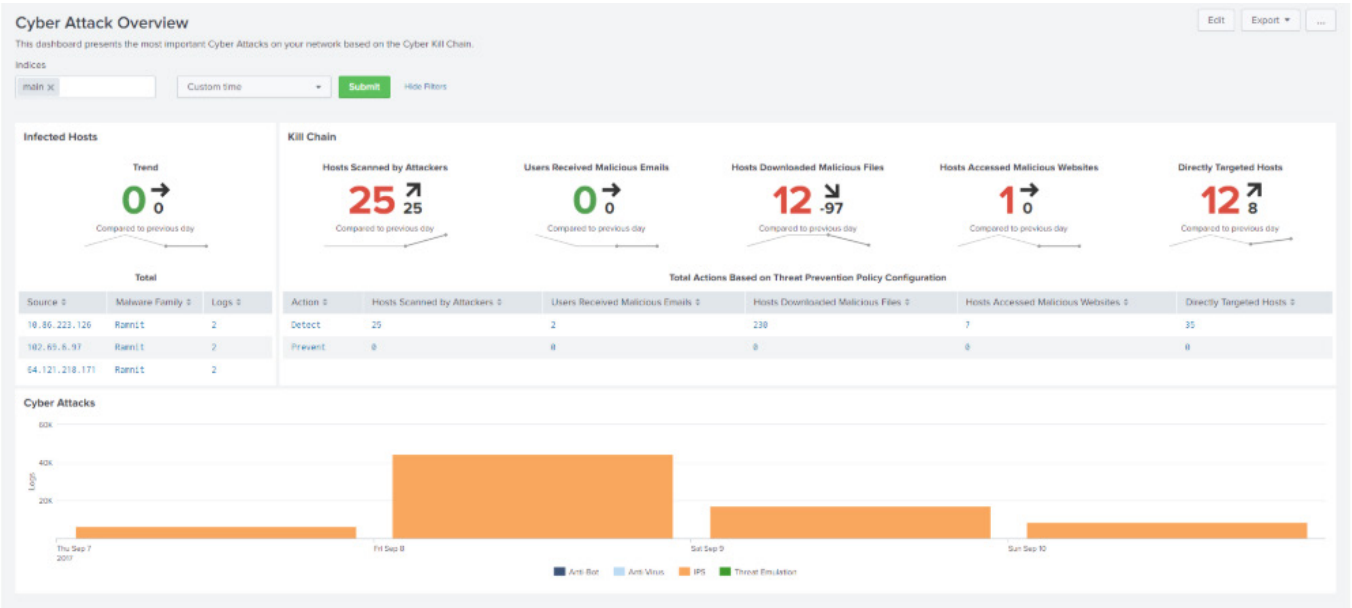
Integrated Threat Prevention Ecosystem

Check Point offers a fully consolidated cyber security architecture to protect your business and IT infrastructure against sophisticated cyber-attacks across networks, endpoint, cloud and mobile. Our prevention technologies stop both known and unknown zero-day attacks across all areas of the IT infrastructure, including cloud, endpoint and mobile. And if an attacker does penetrate the perimeter, we terminate command and control channels and break the cyber-attack kill chain before they can extract data.

Furthermore, we understand that any security infrastructure likely requires additional products and data sources. Check Point network, endpoint, cloud and mobile device events enrich the data that Splunk then analyzes for threats. Splunk collects and analyzes terabytes of data per day in real time, offering Check Point users a scalable real-time IT data engine.

Check Point App for Splunk

Check Point brings you an advanced and real-time threat analysis and reporting tool for Splunk. With the Check Point App for Splunk you can collect and analyze millions of logs from all Check Point technologies and platforms across networks, cloud, endpoints and mobile. This includes key forensics indicators formatted to the Splunk Common Information Model (CIM), allowing you to respond to security risks immediately and gain true insights into threats targeting your organization.



Dashboards	Cyber Attack View
General Overview	Reconnaissance Actions against the Network
Top Attacks	Delivery Methods
Detected and Prevented Events	Malicious Emails
Events Timeline	Malicious File Download
Security Statistics	Server Exploit
	Infected Hosts

Fast, Secure Deployment

The Check Point App for Splunk Enterprise Security receives logs from Check Point log servers via a secure TLS syslog connection to Log Exporter, a multi-threaded daemon capable of serving multiple SIEM applications. Check Point gateways, endpoints and mobile devices send logs to central log servers, where Log Exporter transforms the logs from a Check Point format into the desired format and mapping of SIEM applications. To learn more, read the Check Point App for Splunk User Guide.

Indicator-Rich Data Sets

Check Point fuels Splunk with a rich set of indicators from Check Point advanced threat prevention technologies, such as SandBlast Network, SandBlast Agent on endpoints and SandBlast Mobile on mobile devices. For example, SandBlast Agent's combination of advanced algorithms and deep analysis of raw forensic data builds a comprehensive incident summary, which is then sent to Splunk.

The forensics analysis process automatically starts when a malware event occurs on a protected endpoint. Key actionable attack information includes:

- Malicious events – What evidence of suspicious behavior was detected throughout the attack lifecycle?
- Entry point – How did the attack enter the network?
- What were the main elements used in the attack? How was the attack initiated?
- Damage scope – What did the malware do once activated that may impact the business?
- What data was compromised and/or copied externally?
- Infected hosts – Who else or what else is affected?

Automate Incident Response

The Check Point and Splunk solution goes a step beyond event correlation and analysis. Incidents from Check Point and other devices fed into Splunk can generate new threat indicators for malware, threat behavior and network addresses associated with each identified attack. These indicators are then distributed from Splunk to Check Point Next Generation Firewalls to protect the organization with real-time blocking.

The Splunk Adaptive Response framework provides a mechanism for running preconfigured actions that can be automatically triggered by correlation search results or manually run on an ad hoc basis from the Splunk Enterprise Security Incident Review dashboard. Supported Indicators of Compromise (IoC) include Domain, Mail from, Mail-cc, Mail-reply-to, Mail-to, Mail-subject, URL, MD5, IP (IPv4 only) and IP Range. Splunk connects securely to Check Point gateways and adds the IoCs, which are then enforced by Antivirus and Anti-Bot protections on the Check Point security gateways. To learn more, visit the Check Point Adaptive Response Add-on for Splunk page on Splunkbase.

Summary

Benefits of the joint solution include:

• **Focused Security Analysis and Reporting:** Correlates logs from all enforcement points, network cloud, endpoint and mobile to identify suspicious activity, track trends and investigate and mitigate incidents.

• **Customizable Views and Reports:** Security events automatically alert on critical events.

• **Reduced Incident Analysis Time:** Correlation of millions of logs from Check Point and security devices across your organization identifies significant events easily, reducing your overall investigation response time.

• **Automated Incident Response:** Rapidly investigate incidents and seamlessly trigger mitigation policies on Check Point Next Generation Threat Prevention security gateways.

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 Splunk

Splunk Inc. (NASDAQ: SPLK) helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data. Join millions of passionate users and try Splunk for free today.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com