Check Point SOFTWARE TECHNOLOGIES LTD.

WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT + STELLAR CYBER

ACCELERATE CYBER THREAT PREVENTION

ELIMINATE ALERTS, FOCUS ON ACTIONABLE SECURITY EVENTS AND TAKE AUTOMATED RESPONSE

Benefits

- **Gain context to alerts:** FW/IDS data is fused with contextual information such as geolocation, IP/URL reputation, user, endpoint and domain registrar information and more to gain better context for alerts generated by the Firewall.
- **Eliminate alert fatigue:** Focus on actionable security events that matter vs. the millions of alerts generated by firewalls. Advanced machine learning algorithms determine what events are normal noise vs. high-fidelity anomalies.
- **Audit firewall policies:** Clean up firewall policies and eliminate unused and unneeded policies by machine learning identifying commonly used vs. unused policies that are configured on your firewalls.
- **Identify sequences of events:** Leverage automatic correlation to identify events seen on the firewall that lead to other events seen on endpoint and cloud applications to get a better understanding of a breach timeline.
- **Take automated action:** Leverage integrated security orchestration and response (SOAR) to take automated action such as automatically blocking a malicious actor on the firewall or disabling an infected user within the enterprise.

CHALLENGE

The cyber security industry has traditionally struggled with false positives and alert fatigue. The reason for this is because signatures that detect known malicious network behavior can never be close to 100% accurate. Sometimes legitimate traffic will trigger a match on a signature. It's like sending an email that says, "be on the lookout for this virus" and a signature looking for the keyword "virus' in the packet stream blocks the email. Obviously blocking the email would present a problem.

Another challenge is that firewalls by nature are designed to block traffic and logging firewall deny events can create a mound of logs that can lead to alert investigation fatigue. A new approach to both of these problems is needed, and with Checkpoint FW/IDS technology combined with Stellar Cyber's Interflow & Machine Learning technology, both of these problems can be solved.

JOINT SOLUTION

Check Point Software® and Stellar Cyber® address these problems with an integrated solution that delivers reduced and actionable Firewall and IDS events. The joint solution works by sending Checkpoint FW/IDS logs to Stellar Cyber's Open-XDR Platform called Starlight. XDR means anywhere detection and response. Once these alerts are received by Starlight, the data is normalized, fused with contextual information and Starlight begins the process of turning alerts into actionable events. The joint solution leverages a rich data set around alerts seen from the Checkpoint FW/IDS and converts that dataset to a Stellar Cyber Interflow™ record, which is fused with other contextual pieces of information to form the perfect data record. This newly formatted record (log) then runs through a patent-pending machine learning process that is specifically designed for FW/IDS data. The result could be 8,000 IDS alerts that are turned into one actionable event that a security analyst needs to investigate, or 20,000 FW deny logs that expose a single persistent hacker that generated 5,000 of them. Lastly, the joint solution can identify firewall policies that are not regularly triggered, so that firewall administrators can clean up and remove unneeded firewall policies. A response action on Starlight can be triggered by calling Check Point's Firewall API to disable an attacker's IP address.

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, endpoints, 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. If an attacker penetrates the organization via an insider, we can terminate command and control communications and break the cyberattack kill chain before the attacker can extract data.

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

[1] 2018 Verizon Data Breach Investigations Report: https://enterprise.verizon.com/resources/reports/dbir/

CHECK POINT INTEGRATION FOR STELLAR CYBER

Check Point brings you an advanced and real-time threat analysis, reporting and threat hunting tool for Stellar Cyber. With the *Check Point app for Stellar Cyber,* 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 Stellar Cyber's Interflow format, allowing you to respond to security risks immediately and gain true insights into threats targeting your organization.

Dashboards	Kill Chain View
Kill Chain Overview	Reconnaissance
Affected Hosts	Delivery
Actionable Security Events	Exploitation
Events Timeline	Installation
Malware Detection	C&C
	Actions & Exfiltration

Fast and Secure Deployment

The Check Point App for Stellar Cyber comes built into the Stellar Cyber platform and the Stellar Cyber platform is fast and easy to deploy. The solution can be deployed as a turnkey hardware appliance or can be installed as software in a public or private cloud.

SUMMARY

Benefits of the joint solution include:

- **Entire Kill Chain Detection**: Detect actionable security events across the entire kill chain from within a single product.
- **Automate Response Actions**: Automatically, with or without human intervention, take actions to thwart attacks.
- **Reduced Incident Analysis Time**: Detect critical security events within minutes, negating the need for human triage.
- **Reporting**: Generate compliance reports such as PCI, HIPPA, NIST controls and GDPR.

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 STELLAR CYBER

Stellar Cyber makes Starlight, the only comprehensive security platform providing maximum protection of applications and data wherever they reside and automatically responding to attacks wherever they occur. Starlight tightly integrates dozens of security applications from an App Store and presents results in an intuitive dashboard to supercharge analyst productivity by slashing attack response times to seconds or minutes. Starlight deploys easily on premises, in public clouds or with service providers. Stellar Cyber is based in Silicon Valley and is backed by Valley Capital Partners, Northern Light Venture Capital, Digital Hearts, SIG and other investors. For more information, contact https://stellarcyber.ai.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2117 | Fax: 650-628-2117 | www.checkpoint.com