CHECK POINT + STELLAR CYBER

ACCELERATE CYBER THREAT PREVENTION

ELIMINATE ALERTS, FOCUS ON ACTIONABLE SECURITY EVENTS AND AUTOMATE RESPONSE

Benefits

- **Prevent Zero-day threats:** deploy security that detects and also prevents threats first
- **Gain context to alerts:** Firewall logs are fused with contextual information such as geolocation, IP/URL reputation, user, endpoint and domain registrar information
- **Eliminate alert fatigue:** Focus on actionable security events that matter vs. the millions of logs 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 policy rules
- **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

Security Operations and IT staff struggle with false positives and alert fatigue. Unfortunately, protection signatures for known malicious network behavior will never be 100% accurate. Combine this with the volumes of logs that firewalls generate every day and you end up with alert fatigue and missed threat indicators.

A new approach is needed. Check Point threat prevention technology combined with Stellar Cyber's Interflow and Machine Learning technology solves these problems.

JOINT SOLUTION

Check Point Software® and Stellar Cyber® address these problems with an integrated solution that delivers reduced and actionable firewall and IPS (Intrusion Prevention System) events. Check Point firewall and IPS logs are sent to Stellar Cyber's integrated detection and response platform. Stellar Cyber then normalizes this data, fuses it with rich contextual information and turns alerts into actionable events.

Check Point events are converted into Stellar Cyber Interflow™ records which are fused with other contextual information. This newly formatted log record then runs through a patent-pending machine learning process, specifically designed for firewall and IPS data. The end result reduces up to 8,000 IPS alerts into one actionable event that needs to be investigated or 20,000 firewall deny logs from a single persistent hack attempt down to 5,000. In addition, firewall policy rules that are not regularly triggered are identified, so that firewall administrators can optimize the firewall policy.

INTEGRATED THREAT PREVENTION ECOSYSTEM

The solution starts with a Check Point prevent-first, fully consolidated cyber security architecture to protect your business and IT infrastructure against sophisticated cyber-attacks. 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 that 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.

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.

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's Open XDR platform delivers Everything Detection and Response by ingesting data from all tools, automatically correlating alerts into incidents across the entire attack surface, delivering fewer and higher-fidelity incidents, and responding to threats automatically through AI and machine learning. Our XDR Kill Chain™, fully compatible with the MITRE ATT&CK framework, is designed to characterize every aspect of modern attacks while remaining intuitive to understand. This reduces enterprise risk through early and precise identification and remediation of all attack activities while slashing costs, retaining investments in existing tools and accelerating analyst productivity. Typically, our platform delivers an 8X improvement in MTTD and a 20X improvement in MTTR.