PALO ALTO NETWORKS AND SECBI

Network Traffic Analysis for Automated Threat Investigation

HIGHLIGHTS

The SecBI app automates your ability to detect and investigate incidents with:

- **Full Scope Incident Detection:** Compiling multiple users, domains and assets into a single incident storyline enables analysts to respond immediately for effective and comprehensive remediation.
- **Automated Detection and Investigation:** SecBI analyzes massive amounts of log data from network security gateways for the purposes of detection and investigation, and to produce better responses with fewer false positives.

Use Case: Incident Response

SecBI enables analysts to more efficiently prioritize and investigate incidents in their environments, reducing the time spent on threat investigations by up to 90 percent, which lets security teams focus on complete remediation.

Use Case: Threat Hunting

SecBI's Autonomous Investigation technology helps analysts more efficiently hunt for threats and gain insight into what is happening in their environments to triage incidents quickly. SecBI's analytics provides context for efficient threat-hunting operations over extended periods.

The Challenge

Analysts in a security operations center are tasked with securing their organization's crown jewels, yet they are overwhelmed by billions of security events. To find advanced threats, they hunt for suspicious incidents by piecing together disparate alerts and sporadic anomalies. Making the situation more daunting, most of these alerts turn out to be false positives. Unfortunately, both security analysts and hunters have inadequate tools to achieve full-scope incident detection, accurate investigation and effective threat remediation of today's increasingly stealthy attacks. Too often, analysts miss parts of an incident's end-to-end attack lifecycle – or miss the incident entirely. Consequently, assets and brands are often damaged due to partial breach remediation or a long history of malicious activity.

SecBI's Autonomous Investigation

SecBI's Autonomous Investigation™ technology uses unsupervised and supervised machine learning to perform network traffic analysis, automating the detection and investigation of complex, stealthy threats and malicious communications. Using metadata from existing Palo Alto Networks infrastructure, SecBI presents analysts with all incidents involved in malicious communications, whether internal, such as from users and their devices; or external, such as from web domains, IPs, command-and-control servers, or drop points. SecBI creates a comprehensive view of cyber incidents by combining disparate alerts, events and logs into a comprehensive picture of attacks. This eliminates noise and focuses on the valuable information needed for cyber investigations. Identifying a malicious incident, as opposed to a single discrete anomaly or sporadic alert, ensures fast and comprehensive detection while significantly reducing the rate of false positives.

The results are dramatically shortened response times for cybersecurity teams, thanks to information they can act on immediately to, for instance, block malicious hosts or sanitize endpoints.

Palo Alto Networks Security Operating Platform

The Palo Alto Networks Security Operating Platform prevents successful cyberattacks through intelligent automation. The platform combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle. Because the platform was built from the ground up with breach prevention in mind – with important threat information shared across security functions system-wide – and architected to operate in modern networks with new technology initiatives like cloud and mobility, customers benefit from better security than legacy or point security products provide and realize better total cost of ownership.

Palo Alto Networks and SecBI

The Palo Alto Networks and SecBI integration enables log data from Panorama™ network security management to be collected for update and analysis by SecBI's Autonomous Investigation technology. Groups of events are clustered together according to significant, correlated behaviors. Detection at this cluster level provides Panorama customers with greater accuracy and deeper insight into full-scope incidents at machine speed. Use of unsupervised and supervised machine learning increases the likelihood of detection and results in fewer false positives as well as shorter remediation times.

About SecBI

SecBI has developed a revolutionary approach to network traffic analysis to deliver automated threat detection and investigation for security operations centers (SOCs) and managed security service providers (MSSPs). Without the need to deploy special appliances or agents, the solution can be deployed on premise or in the cloud, and is currently used by financial institutions, telecoms, retailers, and manufacturing enterprises worldwide.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices.

Find out more at www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com