SECBI and ZSCALER

Automated Threat Investigation using SecBI's XDR Platform

Challenge of Hidden Threats

Today's advanced attacks penetrating the IT environment are stealthy. These attacks hide as benign communication, avoiding signature-based security controls, leaving customers completely unaware that they are victims of a breach.

Organizations seek to gain a unified view of log data across an increasingly complex and heterogeneous environment to effectively detect and respond to indicators of compromise (IOCs) in their web traffic and identify anomalies and security vulnerabilities.

SecBI's XDR Platform for Automated Detection & Response

SecBI's cross product XDR platform groups collection of events into clusters using machine learning and behavioral analysis. A suspicious behavior uses forensic evidence to help analysts see the potentially bad behavior quickly. These clusters are categorized into incident narratives which contain a history of blocked and allowed traffic. Traffic patterns are clustered to create risk associations. When a threat is detected, endpoints exhibiting similar "stories" can be identified as risky.

SecBI's XDR cross product platform is based on unsupervised machine learning to identify malicious behavior and cluster it with related forensic evidence to build a full narrative and incident report. Analysts are assured of faster and more accurate detection, with substantially reduced number of false positives. The capability of combining an entire incident together into one cluster, containing the entire life cycle of the incident with all the data and possible alerts, allows for a centralized triage and validation of true/false positive to threat hunting followed by manual or automated remediation.

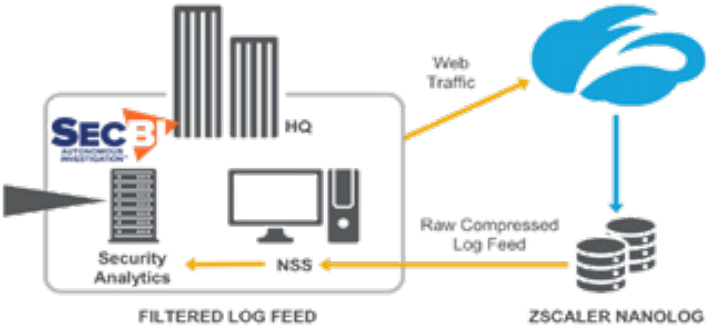
INTEGRATION BENEFITS

- Detect incidents using SecBI XDR platform to correlate Zscaler data and alerts
- Increase efficiency and consistency of security operations
- Automate remediation of incidents using playbook-based mitigation and policy

Solution Overview

The Zscaler™ and SecBI® joint solution offers customers the best-of-breed protection from Zscaler, combined with SecBI's cross product automated detection and response system, based on unsupervised machine learning and analytics. This joint solution enables the detection of stealthy threats and full scope automated mitigation.

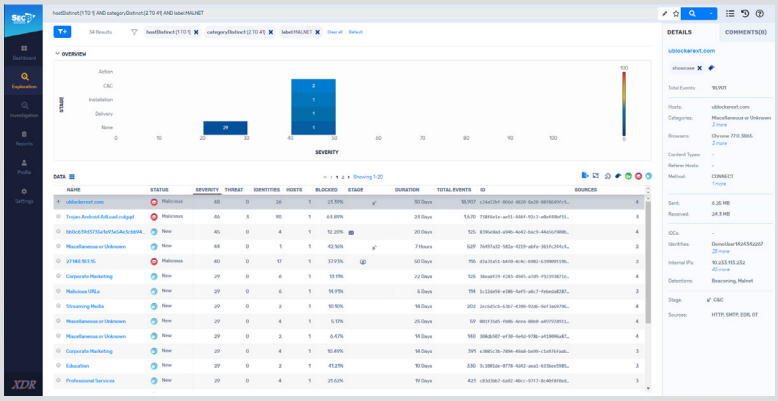
Zscaler Cloud Security Platform delivers world-class threat protection and policy control over all of your web traffic. Zscaler sits in the cloud, between your company and the Internet, protecting your enterprise from cyberthreats, stopping intellectual property leaks, and ensuring compliance with corporate content and access policies. It monitors your network and user activity, secures roaming users and mobile devices, and manages all of this globally from a single management console. Zscaler's security capabilities provide defense-in-depth, protecting you from a broad range of threats including malicious URL requests, viruses, Advanced Persistent Threats (APTs), zero-day malware, adware, spyware, botnets, cross-site scripting, and much more.



Zscaler Nanolog Streaming service (NSS) streams real-time and comprehensive log data to SecBI. SecBI provides full visibility into data captured, applying machine learning to detect and classify user behaviors within the organization. Every such behavior including all related users, devices and locations over time. These behaviors are then turned into a full scope of suspicious incidents and enables comprehensive automated response using Zscaler policy updates or through other security controls.

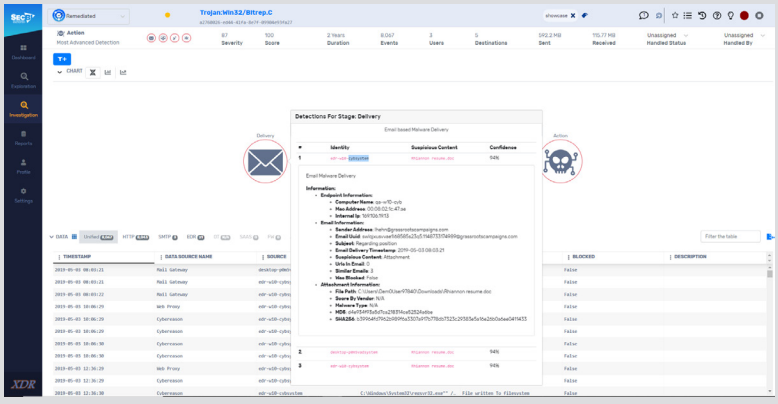
Use Case: Threat Hunting

- Zscaler's sandbox can detect and block malicious content in downloaded files
- SecBI will look for behaviors contained in this alert and automatically remediate all cases where the file has been downloaded in the past, prior to the new classification



Use Case: Machine Learning Blocklists

- Zscaler Threat Research team maintains and updates blacklists of malicious servers with over 120K+ updates daily
- SecBI leverages this information to search through behaviors and find the malicious destinations which are related to the known ones, enabling immediate policy updates and the prevention of the next possible incident



About SecBI

SecBI is a disruptive player in automated cyber threat detection and response. The company's XDR Platform uses unsupervised machine learning to uncover and remediate the full scope of cyberattacks, including all affected entities and malicious activities. SecBI detects advanced threats that other systems miss, creates a comprehensive incident storyline, and automates rapid and accurate mitigation. SecBI's technology is currently used by financial institutions, telecoms, retailers, and manufacturing enterprises worldwide.

Learn more at www.secbi.com or write info@secbi.com

About Zscaler

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100 percent cloud-delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant distributed cloud security platform, protecting thousands of customers from cyberattacks and data loss.

Learn more at zscaler.com or follow us on Twitter @zscaler