PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH SPLUNK

Attivo Networks® has partnered with Splunk to provide advanced, real-time, in-network threat detection and improved automated incident response. With the joint solution, customers receive improved threat intelligence with high fidelity alerts based on suspicious activity. Organizations can reduce time and resources required to detect threats, analyze attacks, isolate attackers, and to remediate infected endpoints, ultimately decreasing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- End-point Deception Credentials Distribution

THE CHALLENGE

Cyberattackers have proven repeatedly that they can, and will, infiltrate the networks of even the most security-savvy organizations. Whether the attacker gets in using stolen credentials, a zero-day exploit, an email-based attack, or simply starts off with insider access, they will establish a foothold and move laterally through the network until they reach their intended target. Attackers have also proven that they can evade the remaining security solutions and traverse the network undetected once inside.

Organizations have responded to these threats by reinforcing their defenses, including an investment in SIEMs, to improve their security monitoring in the hopes of detecting advanced attacks. However, even with this investment, less than half of the breaches are detected internally[1]. Adding to the challenge, security analysts are bombarded with undifferentiated alerts, putting them at risk of missing real threats while chasing false positives.

THE ATTIVO THREAT DEFEND PLATFORM AND SPLUNK SIEM JOINT SOLUTION

Attivo Networks® has integrated the ThreatDefend™ solution with Splunk to provide advanced adaptive security with real-time, in-network threat detection, attack analysis, event correlation, and improved incident response for cyberattacks. The ThreatDefend platform outputs attack information using the Common Information Model (CIM) format, so the data gets properly indexed and stored into Splunk. The high-fidelity alerts and detailed attack information from the Attivo ThreatDefend Platform further augments the data available to incident responders through Splunk.

[1] https://enterprise.verizon.com/resources/reports/dbir/

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the Attivo Networks solution provides network, endpoint, and data deception across an organization. The system has proven highly effective in detecting threats from all vectors, including reconnaissance, stolen credentials, Man-in-the-Middle attacks, Active Directory compromise, ransomware, and insider threats.

The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink engagement servers delivering decoys, lures, and breadcrumbs to an attacker, ThreatDirect™ to extend deception into remote locations, the ThreatStrike® endpoint deception suite, ThreatPath® for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) to coordinate the entire deception suite. Together, these components create a comprehensive early detection and active defense platform against advanced cyber threats.

SUMMARY

The Attivo Networks ThreatDefend Platform plays a critical role in enabling an active defense with in-network threat detection and native integrations to dramatically accelerate incident response.

The combination of early detection, attack analysis, and comprehensive forensic information provides a highly efficient platform for detection of advanced threats and continuous threat management. The Splunk SIEM can leverage the Attivo Networks ThreatDefend Platform's detection, reporting and integrations to monitor for threats, enabling faster incident investigations and adaptive responses, resulting in effective threat containment.

ABOUT ATTIVO NETWORKS®

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, ICS-SCADA, POS and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT SPLUNK

Splunk Inc. is the market-leading platform that powers Operational Intelligence. Splunk pioneered innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government, and education more efficient, secure and profitable.

www.splunk.com