

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH SPLUNK PHANTOM®

Attivo Networks® has partnered with Splunk® to provide advanced security orchestration and incident management through the Splunk Phantom platform. With the joint solution, customers gain visibility into their environment and attack intelligence that the Attivo Networks ThreatDefend™ decoy systems collect and feed to Splunk Phantom. The Phantom platform then automates security orchestration and incident response, including leveraging the ThreatDefend platform's ability to provide an active defense through deception. With this integration customers can reduce the time and resources required to detect and identify threats and respond to them, ultimately reducing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Malware Hunting
- Expedited Incident Response

measures such as looking for known signatures or attack pattern matching. This new method to detect attacks uses deception technology to mislead attackers into revealing themselves and, once engaged, can capture valuable attack forensics that can be used to promptly identify the attacker's tools to delay them from continuing or completing their mission.

THE CHALLENGE

Cyberattackers have repeatedly proven that they can and will infiltrate the networks of even the most security-savvy organizations. Whether the attacker finds their way in using stolen credentials, a zero-day exploit, a ransomware attack, or simply starts off as an insider, they will establish a foothold and move laterally throughout the environment until they can complete their mission. Once attackers bypass the existing prevention mechanisms, they can easily move around the network undetected by the remaining security solutions.

A new approach to security is needed to quickly detect and shut down these attacks, one that focuses on the threats that are inside the network and does not use typical

THE ATTIVO THREATDEFEND PLATFORM AND THE SPLUNK PHANTOM SOLUTION

The joint solution using the Attivo ThreatDefend Deception Platform and the Splunk Phantom platform is easily configured. In minutes, organizations can have an integrated adaptive security platform that provides effective, real-time, detection of cyberattacks with automated threat intelligence sharing, analysis, and security orchestration.

Automating response and remediation is becoming critically important as threats move more rapidly through the environment. This combined solution uses real-time, two-

way communication between the ThreatDefend and Phantom platforms to deliver fast, accurate, and efficient incident response. The information security team can deal with substantiated threats, without losing time investigating false positives, to minimize an attacker's ability to harm the environment or organization.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the solution provides network, endpoint, and data deceptions and is highly effective in detecting threats from all vectors such as reconnaissance, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, and insider threats. The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink engagement servers, decoys, lures, and breadcrumbs, the ThreatStrike® endpoint deception suite, ThreatPath® for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) which together create a comprehensive early detection and active defense against cyber threats.

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

SUMMARY

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

High severity attacks may not afford the incident response team much time to react, but the time an organization saves with fast detection, automated response, and security orchestration, can mitigate the risk substantially. By quickly and efficiently detecting attackers as they try and do reconnaissance or move laterally through an organization's environment, then coordinating their defenses through an advanced orchestration platform, they can derail an attack before it can do major damage to their systems, services, customers, or reputation.

ABOUT SPLUNK PHANTOM

Splunk Inc. is the market leading platform that powers Operational Intelligence. Splunk pioneers 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/phantom