PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND® PLATFORM INTEGRATION WITH SERVICENOW

Attivo Networks® has partnered with ServiceNow 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 confirmed suspicious activity, that lets them initiate service tickets automatically. Organizations can reduce the time and resources required to detect and respond to threats, analyze attacks, isolate attackers, and remediate infected endpoints, all while increasing efficiency and ultimately decreasing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Validated Security Alerts
- Automated Service Ticketing
- Expedited Incident Response

THE CHALLENGE

Cyber-attackers 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.

Contributing to the challenge, security analysts are often bombarded with a large volume of undifferentiated alerts that increase the risk of missing real threats while chasing false positives. In response to these evolving threats, organizations have reinforced their defenses across the board with improved detection and the addition of automated response capabilities.

THE ATTIVO THREAT DEFEND PLATFORM AND SERVICENOW JOINT SOLUTION

The Attivo Networks® has integrated the ThreatDefend® solution with ServiceNow to provide advanced adaptive security with real-time, in-network threat detection, attack analysis, event correlation, and improved incident response to advanced cyber-attacks. The Attivo BOTsink appliance, the core of the ThreatDefend platform, uses deception to accurately identify attackers. When it detects suspicious activity, it sends detailed events to ServiceNow which generates service tickets that are automatically routed to the correct resources.

The combination of high-fidelity alerts and automated service ticketing can dramatically improve the information security team's efficiency and effectiveness, without increasing overhead.

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 and remediation.

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. To build strength upon strength, ServiceNow leverages the Attivo Networks ThreatDefend Platform's detection, reporting, and integrations to monitor for threats so the organization can automatically dispatch resources in reaction to a security event. This is an effective combination that leads to adaptive responses, faster incident investigations, and more 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, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT SERVICENOW

ServiceNow (NYSE: NOW) makes work, work better for people. ServiceNow's cloud-based platform and solutions deliver digital experiences that help people do their best work.

www.servicenow.com