PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH TANIUM®

Attivo Networks® has partnered with Tanium® to provide advanced, real-time, in-network threat detection, attack analysis, and improved automated incident response to block and quarantine infected endpoints. With the joint solution, customers can review alerts and the accompanying attack forensics and assign endpoint policies to automatically block and isolate systems deemed compromised. Security operations teams can gain time and reduce the resources required for detecting threats, reporting and analysis of attacks, and managing incidents. Tanium along with the Attivo ThreatDefend™ Platform provides enhanced visibility and control into in-network threats, enhances policy compliance, and provides additional controls for continuous threat management.

HIGHLIGHTS

- Actionable High-fidelity Alerts
- Accelerated Incident Response
- Stronger Security Ecosystem
- Cross-platform Information Sharing

THE CHALLENGE

The increasing number of advanced threats and damages as a result of internal threat actors has led many organizations to change their overall security posture. The sophistication and high-impact nature of these attacks have compelled security professionals to take a new approach to security, one that provides a balance of prevention and detection security tools and platforms—each designed to play an important role in safeguarding their business.

As a result, companies are overwhelmed with information and logs that are not easily shared or leveraged between tools, creating silos of information and operational challenges. Manual efforts to collect data from each tool creates complexity and adds to the overall effort and cost of operations. Moving from one tool to another to correlate information for a comprehensive view and collective response to cyber threats can be time consuming and too often leaves threats unaddressed. Organizations need a new approach, one without false positives but with high-fidelity alerts that allow efficient and timely responses to cyber threats.

THE ATTIVO THREATDEFEND AND TANIUM JOINT SOLUTION

The ThreatDefend platform is comprised of the Attivo Networks BOTsink® deception servers, ThreatStrike® endpoint deception suite, ThreatPath® for attack path visibility, ThreatOps™ for repeatable response playbooks, DecoyDocs for data loss tracking, ThreatDirect for deployment flexibility in micro-segmented, remote, or branch environments, and the Attivo Central Manager (ACM) for enterprise deception and threat intelligence management. Together, these solutions create a comprehensive early detection and continuous threat management defense against information security threats. The Attivo BOTsink solution and the ThreatStrike® suite are the main integrations with Tanium.

The ThreatStrike® Suite includes deceptive credentials, lures, and mapped drives for ransomware attacks that bait and lead the attacker to the BOTsink solution engagement server. The engagement server captures the Indicators of Compromise (IOC) and full Techniques, Tactics, and Procedures (TTP) of the attack. Security teams can install the ThreatStrike® Suite at endpoints within the BOTsink solution user interface or through integration with Tanium for easy, frictionless deployment. When an attacker attempts usage of these credentials, the BOTsink solution raises a high-fidelity alert, empowering the security operations team to take quick incident response actions.

A vital part of the ThreatDefend platform, the BOTsink solution includes distributed decoy systems based on real operating systems and services for the highest levels of authenticity and attractiveness to an attacker. The solution is dispersed across the network to lure the attacker into engaging with it. Once engaged, the attack continues to play out safely in the BOTsink solution, which in turn identifies the infected endpoints, the attacker IP address, and generates attack signatures it communicates to the Tanium platform. The BOTsink solution or the ThreatOps™ solution will then initiate endpoint policies through Tanium enforcing the automated blocking and quarantining of the devices, thus preventing the attacker from completing their mission.

The integration of the ThreatDefend platform with Tanium allows customers to shorten response time with detailed insight provided by actionable dashboards with advanced queries and reports. Organizations receive an efficient solution for early detection of active attacks and prompt incident response handling of cyberattacks.

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.

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 ThreatDefend Platform plays a critical role in empowering an active defense with in-network threat detection and native integrations to dramatically accelerate incident response. Together, Attivo Networks and Tanium allow customers to shorten response time with detailed insight provided by actionable dashboards with advanced queries and reports. Combined, organizations receive an efficient solution for early detection of active attacks and for prompt incident responses handling of cyberattacks. By automating the deception deployment and providing full-VPC visibility of attacker reconnaissance, lateral movement, and cloud credential theft, organizations benefit from an early detection for active attacks and accelerated incident responses.

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 TANIUM

Tanium provides organizations with a single point of visibility and control to secure and manage endpoints at massive scale enterprise-wide. The Tanium platform enables Business Resilience to ensure the technology powering businesses today can adapt to disruption. Many of the world's largest and most sophisticated enterprises including half of the Fortune 100, most of the top retailers and financial institutions, and four of the five United States Armed Forces branches rely on Tanium for Business Resilience.

www.tanium.com