PARTNER BRIEF

ThreatConnect

Attivo NETWORKS®

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH THREATCONNECT®

Attivo Networks has partnered with ThreatConnect to provide advanced threat intelligence sharing and analysis capabilities. With the joint solution, customers gain visibility on attack information and threat intelligence that the ThreatDefend™ decoy systems collect and feed to ThreatConnect®. With this integration customers can reduce time and resources required to detect and identify threats and disseminate the information, 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

THE CHALLENGE

Cyberattackers have repeatedly proven that they can and will get inside the networks of even the most security-savvy organizations. Whether the attacker finds their way in using stolen credentials, zero-day exploitation, a ransomware attack or simply start as an insider, they will establish a foothold and move laterally throughout the network 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. To quickly detect and shut down these attacks, a new approach to security is needed. This approach focuses on the threats that are inside the networks and does not use typical measures such as looking for known signatures or attack pattern matching. This new method to detect attacks uses deception to deceive 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 ATTIVO THREATDEFEND PLATFORM AND THREATCONNECT JOINT SOLUTION

The integration of the Attivo ThreatDefend Deception Platform with ThreatConnect is very simple to set up. In minutes, organizations can have an integrated adaptive security platform that provides effective, real-time detection of cyberattackers with automated threat intelligence sharing and analysis. With native support for file submissions and lookups, the integrated solution provides a real-time, non-disruptive way of detecting and blocking BOTs and APTs inside the network, closing the opportunity for an attacker to leverage unknown malware to exfiltrate valuable company assets and information. Automating remediation is becoming critically important as malware lateral movement speeds increase. The combination of the Attivo BOTSink® Engagement Server and ThreatConnect provides real-time threat hunting capabilities that outperform systems that depend upon manual intervention.

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.

SUMMARY

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

By identifying the source of breach attempts, the Attivo ThreatDefend Platform can be configured to send malicious file hashes and samples directly to ThreatConnect for lookup and analysis. The time saved in automated malware hunting on the network is critical to preventing malware-based lateral movement and data exfiltration. A strategy that depends upon manual intervention may work for low-severity alerts. High-severity attacks may not afford security teams the benefit of time to react to these alerts. Automation of malware hunting and file reputation lookups give the advantage back to the security team and will help contain the attack before mass damage or exfiltration can be done. The need for this integration is urgent. In a single year, over one billion sensitive records have been stolen with detrimental impact to individuals and enterprises. The resulting damage to the companies' reputations and balance sheets has reached into the billions of dollars. By implementing solutions that detect in-network threats early and having the ability to automatically hunt for additional malware infections, organizations can mitigate the risk of large-scale breaches.

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 THREATCONNECT

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions.

www.threatconnect.com