PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND® PLATFORM INTEGRATION WITH CORTEX™ XSOAR BY PALO ALTO NETWORKS

Attivo Networks® has partnered with Cortex XSOAR by Palo Alto Networks to provide advanced security orchestration and incident management. With the joint solution, customers gain visibility into their environment and attack intelligence that the Attivo Networks ThreatDefend® platform collects and feeds to Cortex XSOAR. The Cortex XSOAR solution automates security orchestration and incident response and uses two-way communication to leverage the ThreatDefend platform's ability to use deception to provide an active defense. 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

THE CHALLENGE

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

Organizations need a new security approach to quickly detect and shut down these attacks, one that focuses on the threats that are inside the network and does not use typical measures such as looking for known signatures or matching attack patterns. This new attack detection method uses deception and concealment technology to trick attackers into revealing themselves. Defenders can engage with threats to capture valuable attack forensics that the organization can use to promptly identify the attacker's tactics, techniques, and procedures (TTPs) to delay them from continuing or completing their mission.

THE ATTIVO THREATDEFEND PLATFORM AND CORTEX XSOAR JOINT SOLUTION

The joint solution using the Attivo ThreatDefend Deception Platform and Cortex XSOAR is straightforward to set up. In minutes, organizations can have an integrated adaptive

security platform that provides effectual, 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 platform and Cortex XSOAR to deliver fast, accurate, and efficient incident response. The information security team can deal with real threats, without losing time investigating false positives, to minimize an attacker's ability to harm the environment or organization.

ATTIVO NETWORKS THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend® Platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It provides a comprehensive fabric that blankets the network with deceptive decoys, credentials, shares, bait, and other misdirections that derail adversaries early in the attack lifecycle. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response. The platform's components include the BOTsink deception server, the Endpoint Detection Net Suite, and ADSecure for Active Directory protection.

SUMMARY

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

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

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership.

www.attivonetworks.com

ABOUT CORTEX XSOAR

Cortex™ XSOAR by Palo Alto provides the industry's only extended security orchestration, automation, and response platform with native threat intelligence management. Cortex XSOAR is a single platform that orchestrates actions across your entire security product stack for faster and more scalable incident response. You can streamline processes, connect disparate tools and automate manual, repetitive tasks that don't require human intervention. SecOps teams have used Cortex XSOAR to automate up to 95% of all response actions, enabling their analysts to focus on the critical incidents that require their attention.

www.paloaltonetworks.com/cortex/xsoar