ATTIVO NETWORKS® THREATDEFEND® PLATFORM INTEGRATION WITH MICRO FOCUS ARCSIGHT® ESM

Attivo Networks® has partnered with Micro Focus 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 suspicious activity. Organizations can reduce the time and resources required to detect threats, analyze attacks, isolate attackers, and remediate infected endpoints, ultimately decreasing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- End-point Deception Credentials

THE CHALLENGE

Cyberattackers have repeatedly proven 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 starts 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.

Organizations have responded to these threats by reinforcing their defenses, including investment in SIEMs, to improve their security monitoring in the hopes of detecting advanced attacks. However, even with this investment, less than half of the breaches are detected internally. Security analysts are bombarded with undifferentiated alerts, adding to the challenge, and increasing the risk of missing real threats while chasing false positives.

THE ATTIVO THREATDEFEND PLATFORM AND MICRO FOCUS ARCSIGHT JOINT SOLUTION

Attivo Networks® has integrated the ThreatDefend® platform with the ArcSight Enterprise Security Manager to provide advanced adaptive security with real-time in-network threat detection, attack analysis, event correlation, and improved incident response for cyber-attacks. BOTsink, the core of the ThreatDefend platform, sends detailed events from the deception environment to the ESM, where the high-fidelity alerts and detailed attack information augments the data available to incident responders from ArcSight. Additionally, BOTsink regularly queries ESM to identify any attempt to use its deceptive credentials anywhere in the production environment.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Organizations are shifting to an identity-first posture for cybersecurity with today's distributed workforce and migration to the cloud. The Attivo Networks ThreatDefend platform provides a customer-proven solution to prevent identity-based privilege escalation and detect attacker lateral movement. The platform's visibility programs deliver insight into credential and attack path vulnerabilities and Active Directory domain, user, and device-level exposures for organizations seeking increased security based on least privilege access. The ThreatDefend platform's concealment technology derails attackers as they can no longer find or access the data, files, AD objects, and credentials they seek.

Additionally, the solution's decoys obfuscate the attack surface, collect forensic data, automatically analyze attack data, and automate incident response through its 30 native integrations. The platform provides the most comprehensive in-network detection solution, providing a detection fabric that scales to on-premises, cloud, remote worksites, and specialty environments such as IoT, SCADA, POS, SWIFT, and network infrastructure.

The ThreatDefend Platform modular components include the ADAssessor solution, which identifies AD exposures and alerts on attacks targeting it. The Endpoint Detection Net (EDN) suite consists of the ThreatStrike® credential lures endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement. The Attivo BOTsink® deception server provides decoys, gathers attacker threat intelligence, and automates incident response with its orchestration playbooks. Joining the EDN, ADSecure, and ADAssessor solutions as part of Attivo's identity security offerings, the IDEntitleX solution reduces the attack surface by providing visibility to cloud identity entitlement exposure. The ThreatDirect deception forwarders support remote and segmented networks. Attivo Central Managers are available as management consoles.

SUMMARY

The Attivo Networks ThreatDefend Platform plays a critical role in enabling an active defense with in-network threat detection and native integrations to accelerate incident response dramatically. The combination of early detection, attack analysis, and comprehensive forensic information provides a highly efficient platform for advanced threat detection and continuous threat management. The ArcSight ESM can leverage the Attivo Networks ThreatDefend platform's detection, reporting, and integrations to monitor threats, enabling faster incident investigations and adaptive responses, resulting in effective threat containment.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. The ThreatDefend® Platform provides unprecedented visibility to risks, attack surface reduction, and attack detection across critical points of attack, including endpoints, in Active Directory, and cloud environments.

www.attivonetworks.com.

ABOUT MICRO FOCUS

Micro Focus is one of the world's largest enterprise software providers. They deliver trusted and proven mission-critical software that keeps the digital world running. Their pragmatic, disciplined, customer-centric approach allows customers to succeed in today's rapidly evolving marketplace.

www.microfocus.com