PARTNER BRIEF

ATTIVO NETWORKS THREATDEFEND® PLATFORM INTEGRATION WITH IBM SECURITY RESILIENT

Attivo Networks® has partnered with IBM® to provide advanced security orchestration and incident management through the Resilient SOAR platform. The solution enables organizations to respond rapidly to detected threats by reducing false-positive alerts and excessive manual intervention. The Attivo Networks ThreatDefend® platform integration for Resilient configures quickly to give organizations the ability to combine early and accurate detection with automated security orchestration. The integration reduces an organization's time and resources required to detect, identify, and respond to threats, thereby reducing the risk of a successful attack.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Forensics and Threat Analysis
- Expedited Incident Response
- Visibility and Awareness

THE CHALLENGE

Attackers have repeatedly proven their ability to bypass defenses and infiltrate networks to breach critical data and infrastructure. Whether through stolen credentials, a zero-day exploit, a ransomware attack, or starting as an insider, they will establish a foothold and move laterally throughout the environment until they can complete their mission. Once attackers bypass the existing prevention mechanisms, they have the freedom to move around and can remain undetected for extended periods.

Organizations looking for a novel way to identify and contain such attacks should focus on solutions that excel at finding in-network threats without relying on known signatures or attack patterns. Deception technology achieves this detection, tricking attackers into revealing themselves by deceiving them into engaging with decoy assets and credentials. The decoy environment records attack activities and captures forensic evidence that the organization can use to develop company-centric threat intelligence. The organization can leverage this intelligence to improve defenses and make it difficult for attackers to complete their mission.

THE ATTIVO THREATDEFEND PLATFORM AND IBM SECURITY RESILIENT JOINT SOLUTION

The Attivo ThreatDefend Platform and IBM Resilient integration configures quickly to give organizations an adaptive security platform that combines early and accurate detection with automated security orchestration. The Attivo BOTsink solution is available to the security community through IBM Security App Exchange, a marketplace where developers across the industry can share applications based on IBM Security technologies. As threats are evolving faster than ever, collaborative development amongst the security industry helps organizations adapt quickly and speed innovation in the fight against cybercrime.

The BOTsink server integrates with Resilient, which accelerates incident response with its orchestration and automation capabilities, to investigate and mitigate threats. Leveraging Resilient's open application programming interfaces (APIs), the BOTSink server integration for Resilient allows Attivo Networks and Resilient customers to automate security orchestration, reduce triage times and accelerate incident response. Organizations gain accurate detection early in the attack cycle, which can trigger incident response playbooks, that can leverage automation, for faster response. It also provides forensic evidence collection and attack activity recordings that organizations can leverage for threat intelligence development. Resilient can dynamically deploy decoys from the BOTsink server as part of an orchestration playbook to add on-demand deception coverage in response to detected activity.

With the speed at which threats can move, from initial compromise to data exfiltration, the combined solution's accuracy, coupled with its accelerated response, gives organizations the ability to deal with threats quickly to minimize the time attackers have to remain undetected within the network.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Considered the industry's most comprehensive deception platform, the Attivo Networks solution provides network, endpoint, application, and data deception across the entire network of an organization. The system has proven highly effective in detecting attack activity that other security solutions overlook, including network reconnaissance, credential theft/reuse, man-in-the-middle attacks, Active Directory reconnaissance/compromise, ransomware, and insider threats.The ThreatDefend Deception Platform is a modular solution comprised of the Attivo BOTsink engagement servers that forms the foundation of the deception environment, the ThreatDirect® endpoint deception solution for deception in remote sites, the ThreatStrike® endpoint deception suite, the ThreatPath® solution for attack path visibility, the ThreatOps® solution that provides repeatable incident response playbooks, and the Attivo Central Manager (ACM) for enterprise-wide management of the deception environment. Together, these components create a comprehensive deception platform to detect and respond to in-network attackers.

SUMMARY

The Attivo ThreatDefend Platform plays a critical role in giving organizations early and accurate detection while denying in-network threats the ability to move laterally or remain undetected.

Incident response teams gain fast detection, automated response, and security orchestration to mitigate the risk of in-network attackers substantially. By quickly and efficiently detecting attackers as they try to conduct reconnaissance or move laterally through an organization's environment with coordinated responses through an advanced orchestration platform, the organziaiton can derail an attack before it can cause significant damage to systems, services, customers, or reputation.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement detection, delivers a defense for revealing and preventing unauthorized insider and external threats. The customer-proven, scalable solution derails attackers and reduces the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The ThreatDefend® Platform 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 3rd party native integrations streamline incident response.

www.attivonetworks.com

ABOUT IBM

IBM Security Resilient, the company's security orchestration, automation and response (SOAR) platform is the leading platform for quickly and easily integrates with an organization's existing security and IT investments. It makes security alerts instantly actionable, provides valuable intelligence and incident context, and enables adaptive response to complex cyber threats.

www.IBM.com