PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH IBM QRADAR®

Attivo Networks has partnered with IBM QRadar to provide advanced real-time, in-network threat detection and improve automated incident response to hunt for other threats or infected endpoints. With the joint solution, customers can review alerts and have the choice to hunt for compromised systems based on suspicious activity. Customers can reduce time and resources required to detect threats, analyze attacks, and to remediate infected endpoints, ultimately decreasing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Threat 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. Regardless of how the attacker enters the network, 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 organizations can use to promptly delay the attacker from continuing or completing their mission.

THE ATTIVO THREATDEFEND PLATFORM AND IBM QRADAR JOINT SOLUTION

The integration of the Attivo ThreatDefend™ Deception Platform with IBM QRadar is very simple to set up. In minutes, organizations can have an integrated adaptive security platform that provides effective, real-time detection of cyberattackers and automatic threat hunting of infected systems to effectively stop data exfiltration and contain the attack. With native QRadar LEEF support, 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 exfiltrate valuable company assets and information. Automating remediation is becoming critically important as malware-based lateral movement speeds increase. The combination of the Attivo BOTSink® Engagement Server and IBM QRadar provides real-time threathunting 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 native integrations to dramatically accelerate incident response.

By identifying the source of breach attempts, the Attivo ThreatDefend Platform can be configured to send compromised endpoint alerts directly to IBM QRadar. Policies configured in QRadar can then automatically hunt for additional compromised systems to reduce the attacker's ability to spread undetected. The time saved in automated threat hunting on the network is critical to preventing lateral movement and data exfiltration. A strategy that depends upon manual intervention may work for low-severity alerts. Highseverity attacks may not afford security teams the benefit of time to react to these alerts. Automation of threat hunting 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 threats, 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, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT IBM

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 60 billion security events per day in more than 130 countries, and has been granted more than 8,000 security patents worldwide.

www.ibm.com/security