PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH FIREEYE MALWARE ANALYSIS®

Attivo Networks® has partnered with FireEye to provide advanced, real-time, in-network threat detection and improved automated incident response. With the joint solution, customers receive improved threat intelligence to isolate compromised systems based on suspicious activity. Organizations 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 Quarantine and Blocking
- Expedited Incident Response
- End-point Deception Credentials Distribution

THE CHALLENGE

Cyberattackers have proven that they can infiltrate the networks cyber infrastructure 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 starts 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 organizations can use to promptly delay the attacker from continuing or completing their mission.

THE ATTIVO THREATDEFEND PLATFORM AND FIREEYE MALWARE ANALYSIS JOINT SOLUTION

The integration of the Attivo ThreatDefend™ Deception Platform with FireEye Malware Analysis is very simple to set up. In minutes, organizations can have an integrated adaptive security platform that provides effective prevention, real-time detection of cyber-attackers, and automatic blocking and isolation of infected systems to effectively contain the attack and stop data exfiltration. 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 threat identification is becoming critically important as malware lateral movement

speeds increase. The combination of the Attivo BOTSink® Engagement Server and FireEye Malware Analysis provides real-time detection and identification 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.

The Attivo ThreatDefend Platform can identify suspect files on decoy systems and pass them to the FireEye Malware Analysis system for rapid analysis and identification. Hostile files can be quickly and automatically identified across the environment, isolating compromised systems and reducing 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. High-severity attacks may not afford security teams the benefit of time to react to these alerts. Automated threat hunting gives the advantage back to the security team and helps contain attacks before they can inflect mass damage or exfiltrate data.

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, 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 FIREEYE

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber-attacks.

www.fireeye.com