PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH CROWDSTRIKE FALCON

Attivo Networks has partnered with CrowdStrike to give organizations early and accurate in-network threat detection, better protection at the endpoint, and automated incident response to block and quarantine attackers before they spread. The joint solution improves security through the rapid detection of and response to an attacker's attempts to move laterally across the network. The partnership provides company-centric threat intelligence to improve defenses and elevate the organization's security posture, reducing the time and resources required to detect threats, analyze attacks, and remediate infected endpoints.

HIGHLIGHTS

- Early and Accurate Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Faster Incident Response

THE CHALLENGE

Attackers have demonstrated their ability to bypass perimeter defenses and infiltrate networks through many tactics, such as reusing stolen credentials, exploiting zero-day vulnerabilities, using ransomware, or starting as an insider. Once attackers have established a beachhead, they will move laterally throughout the network, expanding their footprint until they can find the data they are looking for and complete their mission.

Detecting threats that are already inside the network is challenging. Identifying these attackers once they have broken in requires a different approach that does not rely on recognizing known signatures or analyzing patterns of behavior. This method of detection uses deception to trick attackers into revealing themselves and engaging with decoy assets that can forensically capture valuable attack information while alerting on their activity. This early and accurate detection allows organizations to respond to incidents quickly to deny attackers the ability to move laterally and develop company-specific threat intelligence to increase their security posture and improve defenses.

THE ATTIVO THREATDEFEND PLATFORM AND CROWDSTRIKE JOINT SOLUTION

The partnership between Attivo Networks and CrowdStrike gives organizations an integrated defensive strategy that takes advantage of both the ThreatDefend platform and the Falcon endpoint protection solution. The joint solution provides early and accurate threat detection coupled with the ability to quarantine a compromised endpoint instantly. Whether it is an automated attack or a human attacker, the joint solution can reduce the risk of a breach through rapid detection, triage, and response. The Attivo solution feeds the endpoint IP address that is interacting with Attivo decoys to allow customers to leverage CrowdStrike's advanced forensic capabilities to further understand the TTP of the attack.

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 that covers network and endpoint detection. The Attivo BOTsink engagement servers, decoys, lures, and breadcrumbs provide detection for the network, while the Endpoint Detection Net portfolio consists of the ThreatStrike® endpoint lures, ThreatPath® for attack path visibility, and the ADSecure module protect at the endpoint. Together, these create a comprehensive early detection and active defense against cyber threats.

SUMMARY

The Attivo ThreatDefend Platform and CrowdStrike Falcon empower organizations with a robust defensive strategy that combines quick and accurate detection with rapid threat containment. Together, the joint solution allows organizations to shorten triage time with actionable alerts, reduce response delays with automated quarantines, and improves defenses with company-centric threat intelligence.

By implementing these solutions jointly, organizations can confidentially detect in-network threats early and automatically block and quarantine those threats to mitigate the risk of large-scale breaches.

ABOUT ATTIVO NETWORKS®

Attivo Networks® provides 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 CROWDSTRIKE

CrowdStrike is a cybersecurity technology company that provides endpoint security, threat intelligence, and cyberattack response services. CrowdStrike Falcon is a unifed platform that provides next-generation antivirus (NGAV), endpoint detection and response (EDR), cyber threat intelligence, managed threat hunting capabilities, and security hygiene.

www.crowdstrike.com