PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH CARBON BLACK

Attivo Networks has partnered with Carbon Black to provide advanced real-time in-network threat detection and improve automated incident response to block and quarantine infected endpoints. With the joint solution, customers can review alerts and have the choice to make manual updates or alternatively to create policies to automatically block endpoints based on suspicious activity. Customers can reduce time and resources required to detect threats, analyze attacks, and to remediate infected endpoints, ultimately reducing 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

THE CHALLENGE

Cyberattackers have repeatedly proven that they can and will get inside the networks of even the most security-savvy organizations. Whether the attacker finds their way in through the use of stolen credentials, zero-day exploitation, a ransomware attack or simply start as an insider, they will establish a foothold and will move laterally throughout the network until they can complete their mission.

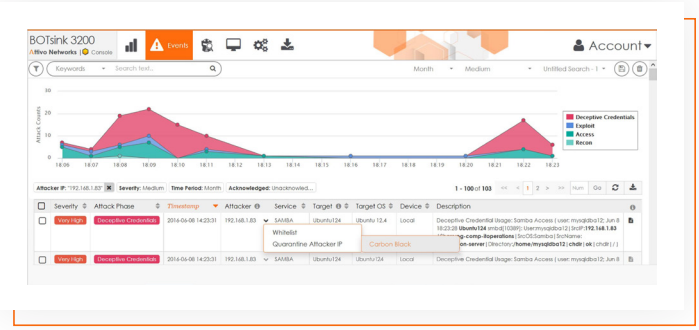
Once attackers bypass the existing security prevention mechanisms they can easily move around the network undetected by current security solutions. To quickly detect and shut down these attacks, a new approach to security is needed. This approach focuses on the threats that are inside the networks and 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 can be used to promptly block the attacker from continuing or completing their mission.

THE ATTIVO THREATDEFEND PLATFORM AND CARBON BLACK JOINT SOLUTION

The integration of the Attivo ThreatDefend Platform with Carbon Black empowers organizations with an integrated, active defense platform that provides effective endpoint control through policy and threat prevention, real-time detection of cyber attackers, and the ability to mitigate risks by instantly quarantining the infected endpoints.

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 credential, 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, and deceptions, 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 and Carbon Black Cb Response empower organizations with an active defense management platform that provide seamless visibility, effective threat containment, and the ability to instantly mitigate risks by auto-blocking infected endpoints through set policy enforcements with Carbon Black.

Together, Attivo ThreatDefend platform and Carbon Black Cb Response allow customers to shorten response time with detailed insight provided by actionable dashboards with advanced queries and reports. Combined, organizations receive an efficient solution for early detection of active attacks and for prompt incident responses handling of cyberattacks.

The need for this type of joint solution 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 these solutions that detect in-network threats early and have the ability to automatically block and quarantine those threats, organizations can 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 CARBON BLACK

Carbon Black Cb Response is the most precise IR and threat hunting solution, allowing you to get the answers you need faster than any other tool. Only Cb Response continuously records and captures all threat activity so you can hunt threats in real time, visualize the complete attack kill chain, and then respond and remediate attacks, quickly.

www.carbonblack.com