Attivo Networks® ThreatMatrix™ Platform Integration with Aruba ClearPass Policy Manager

Highlights

- Real-time Threat Detection
- Attack TTP Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- Centralized Threat Intelligence

a Hewlett Packard Enterprise company

Joint Solution Brief

Attivo Networks® has partnered with Aruba, a Hewlett-Packard Enterprise company, to provide advanced real-time inside-the-network threat detection, attack analysis, and improved automated incident response to block and quarantine infected end-points. Leveraging the Aruba ClearPass integration, customers can detect and defend against advanced threats by automating a quarantine from the Attivo® ThreatMatrix™ solution based on suspicious activity and the severity of the attacks. ClearPass Extensions repository along with the Attivo® ThreatMatrix™ Deception and Response Platform provides enhanced visibility and control, resulting in higher productivity and efficiencies in security management, ultimately reducing the organization's risk of breaches and data loss.

The Challenge

The attack vectors are constantly evolving and can range from tailor-made APTs to mass-produced malware to methods based on social engineering or spear phishing. Reliably defending the perimeter against such a wide variety of attacks has proven unachievable and has resulted in 9 out of 10 company's admitting that they have been breached.

Additionally, the ubiquity of mobile and IoT devices connected to enterprise networks and applications requiring external admin controls pose a major challenge to IT professionals in maintaining network security, as points of entry can open for attackers into some of the most security-savvy organizations.

Once attackers bypass the existing security prevention mechanisms, they can establish a foothold and move laterally throughout the network until they can complete their mission. To quickly detect and defend against these attacks, the Attivo solution brings a new approach of dynamic deception that deceives attackers into revealing themselves. Once engaged, the solution captures valuable attack forensics, which can be communicated to Aruba ClearPass to promptly block the attacker from continuing or completing their mission.

The Joint Solution

The integration of the ThreatMatrix Platform with Aruba ClearPass empowers organizations with an integrated, coordinated defense platform that provides effective end-point control through policy and threat prevention, real-time detection of cyber attackers, and the ability to mitigate risks by instantly quarantining the infected end-points.

Attivo Networks ThreatMatrix Platform

The Attivo Networks ThreatMatrix Platform can detect internal and external threat actors conducting reconnaissance of the network to identify potential targets or looking to escalate privileges to move laterally and attack critical servers.

All types of attacks can be detected, from zero-day & polymorphic attacks, to stolen credential ones. This is all achieved with zero false positive accuracy since the solution is not inline and does not rely on data base look up.

About Attivo Networks®

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatMatrix 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 Aruba

Aruba, a HPE company is a leading provider of next-generation network access solutions for the mobile enterprise. To create a mobility experience that #GenMobile and IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

www.arubanetworks.com

Attivo NETWORKS®

aruba
a Hewlett Packard Enterprise company

Joint Solution Brief

The Attivo Deception Platform is comprised of three core products.

1. The BOTsink® Engagement Server is designed to replicate the production environment and engage with the attacker to collect detailed forensics. The BOTsink solution runs real operating systems and services that can be completely customized to match the environment - from typical corporate networked devices to SCADA/IoT devices. Lured to the server by using decoys present throughout the network, the full Techniques, Tactics and Procedures (TTP) with associated forensics (IOC, STIX, CSV & PCAP) are captured and the relevant information is passed on to the Aruba ClearPass to automate the incident response.

2. The Attivo ThreatStrike™ End-Point Deception Solution includes deceptive credentials, mapped drives for ransomware attacks, and other deceptive bait to drive attackers into engaging with and revealing their presence the BOTsink Solution.

3. The Attivo ThreatPath™ solution checks for any misconfiguration gaps and exposed credentials to reveal possible attack paths a threat actor is likely to use. Possible attack paths and vulnerable IP addresses get highlighted early for remediation to help protect organizations against possible infection or breach.

ThreatMatrix and ClearPass Manager Integration

Installation takes only a few minutes.

1. The BOTSink Engagement Server is configured to treat ClearPass system as a Syslog server.
2. Critical events are set to be automatically sent over to the ClearPass Manager.
3. Next, the Attivo Plugin is installed in the ClearPass Manager enabling the automatic or manual quarantine of infected systems.

Summary

Together, the ThreatMatrix Platform and Aruba ClearPass Policy Manager empower organizations with a continuous threat management platform that provide seamless visibility, effective threat containment, and the ability to instantly mitigate risks by auto-blocking infected end-points through set policy enforcements with ClearPass.

The time saved in blocking malicious traffic on the network is crucial to preventing lateral movement and data exfiltration. Automating blocking and quarantining gives the security team additional time that can be critical to containing the attack before mass damage can be done.