Enhanced Visibility and Defense with HPE Security and Attivo Networks®

Highlights

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

Joint Solution Brief

Attivo Networks® ThreatMatrix™ Detection and Response platform complements HPE ArcSight's Enterprise Security Management System (SIEM) providing intelligent data management and correlation, with real-time in-network threat detection and detailed attack forensics for improved incident response.

The Challenge

Cyber-attacks and their vectors are continuously growing in number and sophistication making security a challenging task for IT professionals. In fact, a recent Mandiant M-Trends research found APTs to persist for over 205 days before being detected in company networks that were unaware of getting hacked. Today, organizations need a security solution that can help them detect and defend against threats that are bypassing traditional prevention systems to enter seemingly security-savvy enterprises. Early detection, real-time attack analysis, monitoring of logging activities and prioritization of critical incidents have become crucial for effective defense against cyber-threats, and companies that fail to do so may give criminals more time to do damage.

The ThreatMatrix™ Deception and Response Platform

The ThreatMatrix Platform is an innovative solution that detects real-time in-network threats using planted decoys and lures throughout the network. The attackers are deceived into engaging with them and are lured away from valuable production assets and to the BOTsink server before revealing themselves. The BOTsink lets the attacks play out, allowing the platform to capture detailed attack forensics and create high-fidelity alerts for automated incident response.

The ThreatMatrix solution includes the BOTsink® engagement servers and decoys that appear as production assets and obfuscates the attack surface turning the entire network into a trap. It also includes the ThreatStrike™ deception suite that installs deceptive credentials and mapped drives at end-points, to lure attackers to the BOTsink once they engage with them, and the ThreatPath™ solution that highlights misconfiguration gaps and exposed credentials to reveal possible paths an attacker can use. Full Tactics, Techniques, and Practices (TTP) captured by the BOTsink, as well as identification of the infected system and the attacker's IP address, promotes accelerated incident response.

The Joint Solution

Attivo Networks® ThreatMatrix solution has integrated with HPE ArcSight to provide advanced adaptive security with real-time inside-the-network threat detection, attack analysis, event correlation and improved incident response for cyber-attacks. With this joint solution, customers gain enhanced visibility that helps them prioritize critical incidents, in turn enabling faster remediation actions that improve efficiencies in security management, reduces an organization's risk of breaches and data loss, and provide more control over threat management.

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 HPE Security

HPE is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products fromHPE Security ArcSight, HPE SecurityFortify, and HPE Security—Data Security,the HPE Security Intelligence Platformuniquely delivers the advance correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

www.hpe.com/software

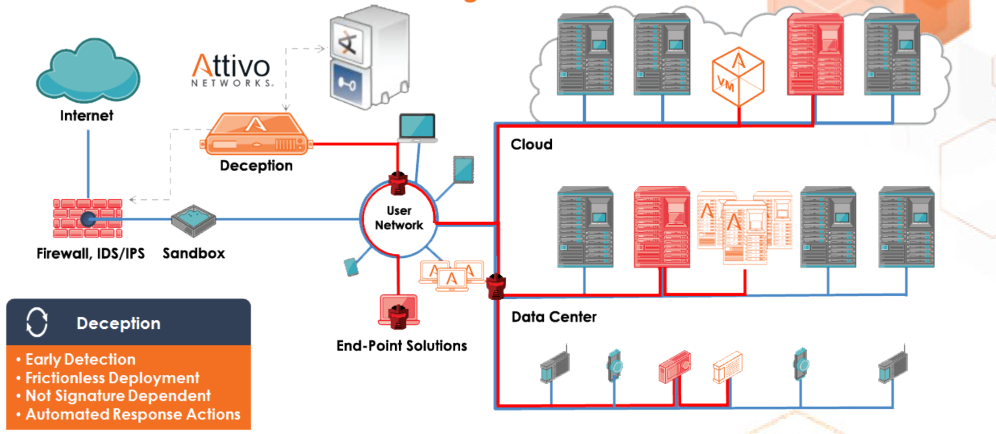
Attivo NETWORKS®

Hewlett Packard Enterprise

Joint Solution Brief

Real-time In-Network Visibility & Threat Detection

ThreatMatrix for Continuous Threat Management



Deception

- Early Detection
- Frictionless Deployment
- Not Signature Dependent
- Automated Response Actions

Key Benefits:

- Real-Time alert into ArcSight with the identification of the infected end-point, time-stamp, and full attack TTP — for prompt blocking and quarantining of an attack.
- Automatic querying from ArcSight SIEM for deceptive credential usage – to detect stolen credential attacks.
- Prioritization of critical threats and incidents among billions of daily received data points.
- Proactive analysis of existing risks due to device misconfiguration and credential vulnerabilities.

Use Cases

Use Case 1: Advanced Threat Detection

A technology company has the ArcSight SIEM installed, which effectively detects signatures of attackers. But the company wanted to add to its security infrastructure for a more granular detection of advanced threats. The Attivo ThreatMatrix solution was added to detect zero-day, polymorphic, stolen credential, and other forms of advanced threats.

Through the ThreatMatrix and ArcSight integration, the company set up automated information sharing to update the SIEM on new signatures detected from the attacks. With this integration, the company achieved a stronger defense system and is now able to save time on incident response through automations.

Use Case 2: Stolen Credential Detection

An attacker steals deception credentials from a financial company end-point. When he tries to use the credentials, it creates failed logins. The BOTsink queries the ArcSight SIEM and finds logs of the failed login attempts. It automatically generates an alert to notify the security teams of the infection.

With this integration, the financial company receives alerts with substantiated and actionable attack information that they can use to immediately address critical incidents. Previously, these alerts were often buried under logs of data until sometimes, it would get a little too late to address them.

Summary

The combination of early detection, attack analysis, and comprehensive analytics provides a highly efficient platform for detection of advanced threats and continuous threat management. The ArcSight Enterprise SIEM can leverage Attivo Networks ThreatMatrix Platform's detection, reporting and querying capabilities to monitor the threats, and enable faster incident investigations and an adaptive response, resulting in effective threat containment.