Attivo Networks® ThreatMatrix™ Deception and Response Platform Integration with McAfee® ePolicy Orchestrator®

Highlights

- High-fidelity alerts
- Accelerated incident response
- Stronger security ecosystem
- Cross-platform information sharing

Attivo Networks® has partnered with McAfee® to detect real-time in-network attacks and to automate incident response by enabling the automated quarantine of infected endpoints. Leveraging the ePolicy Orchestrator integration, customers can review alerts and the accompanying attack forensics and assign endpoint policies to automatically block and isolate systems deemed compromised. Security operations teams can gain time and reduce the resources required for detecting threats, reporting and analysis of attacks, and managing incidents. This integration will improve visibility into in-network threats, enhance policy compliance, and provide additional controls for continuous threat management.

The Challenge

The increasing number of advanced threats and damages as a result of internal threat actors has led many organizations to change their overall security posture. The sophistication and high-impact nature of these attacks have compelled security professionals to take a new approach to security, one that provides a balance of prevention and detection security tools and platforms – each designed to play an important role in safeguarding their business.

As a result, companies are overwhelmed with information and logs that are not easily shared or leveraged between tools, creating silos of information and operational challenges. Manual efforts to collect data from each tool creates complexity and adds to the overall effort and cost of operations. Moving from one tool to another to correlate information for a comprehensive view and collective response to cyber threats can be time consuming and too often leaves threats unaddressed. Organizations need a new approach. One without false positive alarms but with high-fidelity alerts that allow efficient and timely responses to cyber threats.

The Joint Solution

The integration of the ThreatMatrix platform with the ePO Platform empowers organizations with the real-time detection of cyber-attacks and detailed forensics to proactively prioritize and address critical issues for prompt response and remediation. Offering a single unified console across multi-vendor network systems, ePO ensures a timely and accurate response to high-fidelity alerts raised for attacks detected by the ThreatMatrix solution.

The ThreatMatrix platform is comprised of BOTsink engagement servers, decoys, lures, and the ThreatStrike Endpoint Deception Suite. The ThreatStrike Suite effectively detects internal and external threats that start with reconnaissance or are moving laterally within the network. Adding in the ThreatPath solution will also provide visibility to misconfigurations and misused credentials in order to prevent attacks from occurring. Adding in the ThreatPath solution will also provide visibility to misconfigurations and misused credentials in order to prevent attacks from occurring.

Joint Solution Brief

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 McAfee

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

www.mcafee.com

Attivo NETWORKS®

intel Security

Joint Solution Brief

Attivo Networks ThreatStrike Endpoint Deception Suite deployment using ePolicy Orchestrator

The ThreatStrike Suite includes deceptive credentials, lures, and mapped drives for ransomware attacks that bait and route the attacker to the BOTsink engagement server. Once in the engagement server, the full Techniques, Tactics and Processes (TTP) of the attack are captured. Installation of the ThreatStrike Suite at endpoints can be completed within the BOTsink user interface or through ePO for simple, frictionless deployment. When an attacker attempts usage of these credentials, the BOTsink solution raises a high-fidelity alert, empowering the security operations team to take quick incident response actions.

Steps to automatically install ThreatStrike credentials on endpoints are simple and take only a few minutes.

1. ePO server detail is configured in the BOTsink.
2. Attivo ePSecClient package is deployed in the ePO server.
3. ePO Client Task is created to deploy Attivo ePSecClient in the endpoints.
4. Either the ePO ClientTask is added to ePO Deployment Policy or the ClientTask is executed on specific endpoints for deployment of the package.

Attivo Networks BOTsink and ePolicy Orchestrator Integration

A vital part of the ThreatMatrix platform, the BOTsink solution includes distributed decoy systems based on real operating systems and services for the highest levels of authenticity and attractiveness to an attacker. Dispersed across the network, the solution lures the attacker into engaging with it. Once engaged, the attack continues to play out safely in the BOTsink, which in turn identifies the infected endpoints, the attacker IP address, and generates attack signatures that are communicated to the ePO platform. Endpoint policies are then initiated enforcing the automated blocking and quarantining of the devices, thus preventing the attacker from completing their mission.

The integration can be completed in a minutes.

1. The ePO server detail is configured in BOTsink user interface.
2. The Attivo ePO extension is deployed in the ePO server using the BOTsink UI.
3. Auto-blocking is configured based on the severity of the attack and the corresponding attack policy in the BOTsink server.

Summary

The integrtation of the ThreatMatrix solution with the ePO platform allows customers to shorten time to response with detailed insight through to 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 cyber-attacks.