Attivo NETWORKS®

# Advanced Threat Detection and Continuous Security Monitoring with Attivo Networks and Splunk Integration

**Highlights**

- Real-time Threat Detection
- Attack TTP Analysis and Forensics
- Integrations for Quarantine and Blocking
- Accelerated Incident Response
- Centralized Threat Intelligence

Attivo NETWORKS®

splunk>

Joint Solution Brief

Attivo Networks® ThreatDefend™ Deception and Response Platform and Splunk® SIEM are integrated to provide customers with a simplified solution that combines continuous in-network threat detection and attack analysis with intelligent data management and correlation capabilities for improved incidence response and threat containment. Customers gain early visibility to in-network threats, and prioritization of critical incidents for immediate, automated remediation. Users can also take advantage of the Splunk App by Attivo Networks for a comprehensive visualization of the Attivo dashboard.

## Challenges

Cyber-attackers are becoming increasingly sophisticated in finding ways to evade traditional perimeter and endpoint defense solutions. In response, organizations continue to invest in SIEMs to improve their security monitoring in the hopes of detecting advanced attacks, yet less than 20% of breaches are detected internally. Furthermore, security analysts are bombarded with undifferentiated alerts, putting them at risk of missing real threats while chasing false positives.

## The ThreatDefend Deception and Response Platform

The ThreatDefend Platform is an innovative solution that detects real-time advanced threats inside the network. It includes the BOTsink® decoys, and the ThreatStrike™ endpoint deception suite that, together make the entire network a trap through a distributed system of highly interactive decoys. The deceptive credentials lure the attackers to the Attivo ThreatDefend BOTsink engagement servers that work in collaboration with the Attivo Multi-Correlation Detection Engine to analyze attacker IP addresses, methods, and activities by allowing the attack to play out in a safe environment, and generate an engagement-based alert. Security teams can take advantage of third-party integrations to block and quarantine compromised systems automatically. The ThreatDefend Platform provides threat visibility through its ThreatPath™ feature for awareness into exposed credentials, misconfigurations, and other network vulnerabilities to identify possible attack paths.

## The Joint Solution

Attivo Networks ThreatDefend solution has integrated with Splunk to provide advanced adaptive security with real-time in-network threat detection, attack analysis, event correlation and improved incident response for cyber-attacks. The ThreatDefend platform outputs the attack information using the Common Information Model (CIM) format, so that the data gets properly indexed and stored into Splunk. The high-fidelity alerts and detailed attack information from the Attivo ThreatDefend Platform further augments the data available to incident responders through Splunk.

## 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, IoT, and POS environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

## About Splunk

Splunk Inc. is the market-leading platform that powers Operational Intelligence. We pioneer innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government, and education more efficient, secure and profitable.

www.splunk.com

Attivo NETWORKS

splunk>

Joint Solution Brief

### Key Benefits:

- Real-Time alert into Splunk with identification on the infected end-point, time-stamp, and full attack TTP for prompt incident and response to an attack.
- Prioritization of critical threats and incidents from billions of data points received daily.
- Proactive analysis through ThreatPath of existing risks from device misconfiguration of existing risks and exposed credentials.

### Use Case: Threat Hunting

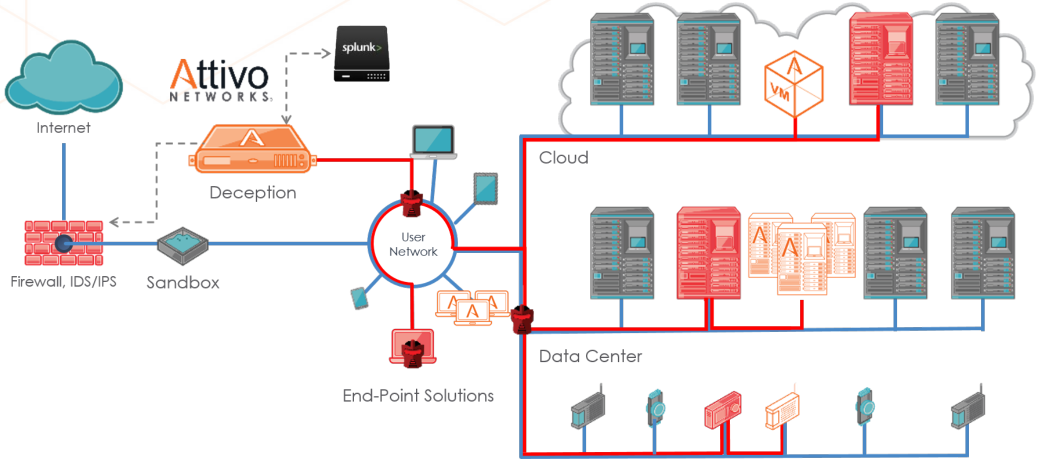
A company has Splunk installed, which indexes all available syslog data. The BOTsink solution identifies an attacker by IP, and identifies indicators of compromise (IOC) relevant to the attack. The security team then uses Splunk to search for the IOCs across the enterprise, identifying other potentially compromised systems. With this integration, the company can hunt for compromised systems from a verified attacker with IOCs developed by the BOTsink solution. Previously, IOC development would have been a manual process.

### Use Case: Stolen Credential Detection

An attacker steals deception credentials from a company end-point. When he tries to use the credentials, it creates a failed login. The BOTsink solution queries the Splunk search head and finds the failed login attempts, automatically generating an alert to notify the security teams of the incident. With this integration, the user receives alerts with substantiated and actionable attack information that they can use to immediately address critical incidents. Previously, these alerts were often buried beneath hundreds or thousands of other alerts, and analysts failed to identify them in a timely manner.

## Summary

The combination of early detection, attack analysis, and comprehensive forensic information provides a highly efficient platform for detection of advanced threats and continuous threat management. The Splunk SIEM can leverage the Attivo Networks ThreatDefend Platform's detection, reporting and integrations to monitor for threats, enabling faster incident investigations and adaptive responses, resulting in effective threat containment.


Internet
Attivo NETWORKS
splunk>
Deception
Firewall, IDS/IPS
Sandbox
User Network
End-Point Solutions
Cloud
VM
Data Center