ThreatPath™ Attack Path Vulnerability Assessment

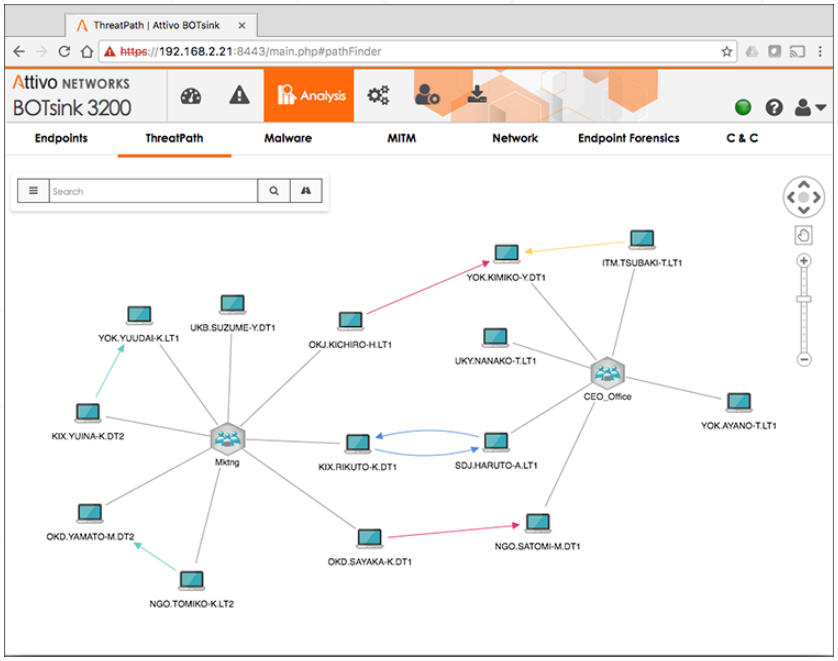
The Attivo ThreatPath™ solution, part of the modular ThreatDefend™ Platform, provides continuous attack path vulnerability assessment of likely lateral movement avenues that an attacker would take to compromise a network. The solution exposes and provides visual graphs to the paths an attacker would traverse through the internal network based on misconfigured systems and misused or orphaned credentials. Integrations with workflow and incident management systems like Service Now and JIRA can be activated inside the dashboard and used for automating remediation notifications and processes.

Attack Path Visibility

A topographical illustration provides a straightforward visual map of how an attacker can move laterally once they have engaged with their first end-point system and to the locations of systems susceptible to compromise. Clickable drill downs provide easy, detailed views of the weaknesses and IP addresses for systems needing to be isolated and/or fixed. Organizations can then use this information to remediate exposures and for insight into prime locations for deceptive credentials to be deployed.

Attack Path Vulnerability Reporting

The ThreatPath solution provides easy to understand views and reporting on attack path vulnerabilities that are within the network. The UI will show network maps demonstrating the possible attacker lateral movement paths and will provide actionable insights that can be used to strengthen policies and prevent attacker lateral movement.



Attack Path Alerting

The ThreatPath solution provides continuous assessment of the network and is designed to alert when new paths open to critical assets.

Attack Path Vulnerability Remediation

Incident workflow management and trouble ticket creation are dramatically simplified with the solution's in-depth data on the compromised asset and double click integrations to automated trouble ticket creation. Customers will benefit from visibility into these workflows, closed loop remediation, and reporting for recording the handling of compromised systems.

Deception Asset Management

The ThreatPath solution can also be used to view and download all ThreatStrike deception lures, simplifying deception asset management.

Conclusion

It is critical to understand and have visibility into attack path risks before they present an attacker with the opportunity to penetrate a network. The ThreatPath solution provides crucial continuous visibility into possible attack path vulnerabilities and provides simplified views of asset relationships and avenues that create the greatest risks. The ThreatPath solution adds pre-attack visibility, vulnerability assessment, and works seamlessly with the Attivo ThreatDefend Platform to strengthen an organization's overall security defense. The ThreatDefend Platform provides comprehensive network, endpoint, data, and application deceptions that efficiently and accurately reveal in-network attacker presence, analyze the attack, and simplify incident response.

About Attivo Networks

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. www.attivonetworks.com