RAPID THREAT CONTAINMENT

THE CENTERPIECE IN ZERO-TRUST SECURITY FOR THE WORKPLACE

A critical component of any zero-trust strategy is securing the workplace that connects everyone and everything. Cisco Identity Services Engine (ISE) enables a dynamic and automated approach to policy enforcement that simplifies the delivery of highly secure network access control. ISE empowers software-defined access and automates network segmentation within IT and OT environments.

With ISE, security teams no longer need to pivot from detection to remediation. It helps break the silo between visibility and control and empowers the teams to stop the spread of highly impactful malware by automating their responses.

INTEGRATION STORY:

Cisco ISE when integrated with LinkShadow Cybersecurity Analytics Platform automates threat containment, removes complexity and protects organizational resources whilst preventing security incidents from turning into breaches.

With an open and standard-based pxGrid and pxCloud ecosystem, ISE gains visibility and context from multiple Cybersecurity Analytics, Security and Intelligence Solutions as well as third-party vendors, be it on-premises or in the cloud. This unification of visibility and control results in automating threat containment that limits or removes access, based on organizational risk tolerance. Suspected endpoints no longer remain in the network or move laterally, infecting other endpoints and causing havoc.

CHALLENGES:

LinkShadow, an agentless solution with zero impact on the network performance, builds a Machine Learning Model for every User and Asset in environment, to hunt and detect anomalies using AI-Based Advanced Machine Learning Algorithms, that might otherwise go unnoticed.

LinkShadow leverages from the integration with ISE for Automated Incident Response. It detects an anomaly and immediately forwards the actionable insight to Cisco ISE for Rapid Threat Containment and apply a policy to the offending device, preventing it from causing any further damage. This provides a high-end protection against most sophisticated threats, zero-day attacks and even unknown anomalies.

KEY BENEFITS:

» LinkShadow Analytics and Cisco ISE minimizes the investigation complexity, time, and resources required with maximum automation and intelligence.

» LinkShadow platform assists in providing feed visibility and context to Cisco ISE and helps in reducing attack surface.

» Cisco ISE accelerates LinkShadow incident response with automated detection and containment.

» Increases ROI with minimal cost on the defense system with the Rapid Threat Containment.

www.cisco.com