MODERNIZE YOUR SOC WITH EXTENDED THREAT HUNTING AND RESPONSE

Detect Cyber and Insider Threats

www.linkshadow.com
LINKSHADOW, NEXT-GENERATION CYBERSECURITY ANALYTICS.

Designed to manage threats in real-time with attacker behavioral analysis, LinkShadow is meant for organizations that are looking to enhance their defenses against advanced cyberattacks, zero-day malware and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments.
AI-Powered Engine

AI-Powered Engine is an end-to-end mechanism that enriches data for Advanced Machine Learning (AML) Anomalies Detection capabilities. It will empower the Enterprise to manage the whole process from data collection to detection and visualization, seamlessly. Simply, an Enterprise can collect data, create a Machine Learning model, build a data list, or upload a ready-to-use one, train a Machine Learning model, monitor its details, quality, and accuracy, and get detections visualised.

Remote Access Visibility

With the recent turn of events, work from home trend has increased the exposure of compromise along with network abuse by insider threats. LinkShadow provides visibility of the Remote Access patterns to your organization and finds the ‘who’, ‘when’, ‘where’ of their activities.

MITRE ATT&CK & Cyber Kill Chain Frameworks

Uncover the attackers TTPs with LinkShadow threat detections mapped to MITRE Framework. Identify which techniques are more prominently used in your environment with suggestions to mitigate. Help environment to thwart the attackers and strengthen Security Posture.

www.linkshadow.com