AI-AUTOMATED THREAT HUNTING AND INCIDENT RESPONSE
FOR A MODERNIZED CYBER SECOPS

In today's ever-evolving cyber threat landscape, one of the most pressing challenges hindering effective Threat Hunting is the time-intensive and fragmented process of monitoring thousands of alert logs to detect and prioritize breaches which puts businesses at a huge risk.

By integrating AI-automated threat hunting with SOAR capabilities SOC teams can unlock the power of threat hunting and tackle the most critical threats with smarter tactical decisions, at a much faster pace.

Cortex™ XSOAR by Palo Alto Networks is an industry-leading comprehensive SOAR platform with built-in native threat intelligence management that allows to unify case management, automate, collaborate in real-time, and manage threat intel to serve security teams across the incident lifecycle.

LinkShadow the next-generation cybersecurity analytics, is a dynamic technology platform, designed for organizations looking to improve their defenses against advanced cyberattacks. With its multiple features that caters to Behavioral Analytics, CXO Visibility, Security Synopsis and Threat Hunting, LinkShadow empowers security teams to gain maximum insights that helps enhance productivity of existing security tools as well as support with a host of complementary functions for a holistic single-pane-of-glass view of the critical challenges faced by organizations.

LET US LOOK AT THE CORE CHALLENGES COMMONLY FACED BY SECURITY TEAMS:

» The dynamic nature of the network activities and users and entities behavior.

» Limited network visibility and anomaly detection.

» The complexity of day-to-day collaboration across disparate teams and siloed tools.

» The difficulty of tracking and optimizing the full lifecycle of an incident.
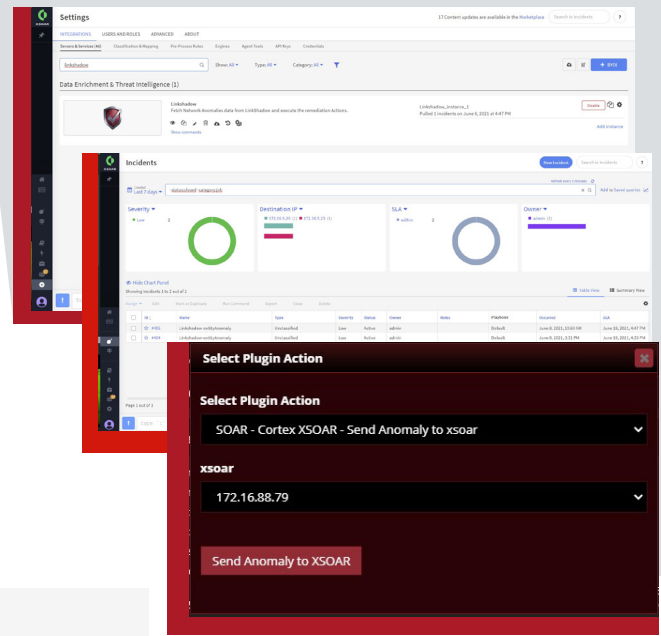
INTEGRATION STORY:

LinkShadow integrates with **Cortex™ XSOAR** by Palo Alto Networks, to automate and optimize complex workflows across the full stack of information systems and security tools. Using the Cortex™ XSOAR and LinkShadow content pack, security teams can automate the incident response and can seamlessly integrate LinkShadow with existing security tools and workflows. Thus minimizing investigation time and maximising detection and threat hunting efficacy.
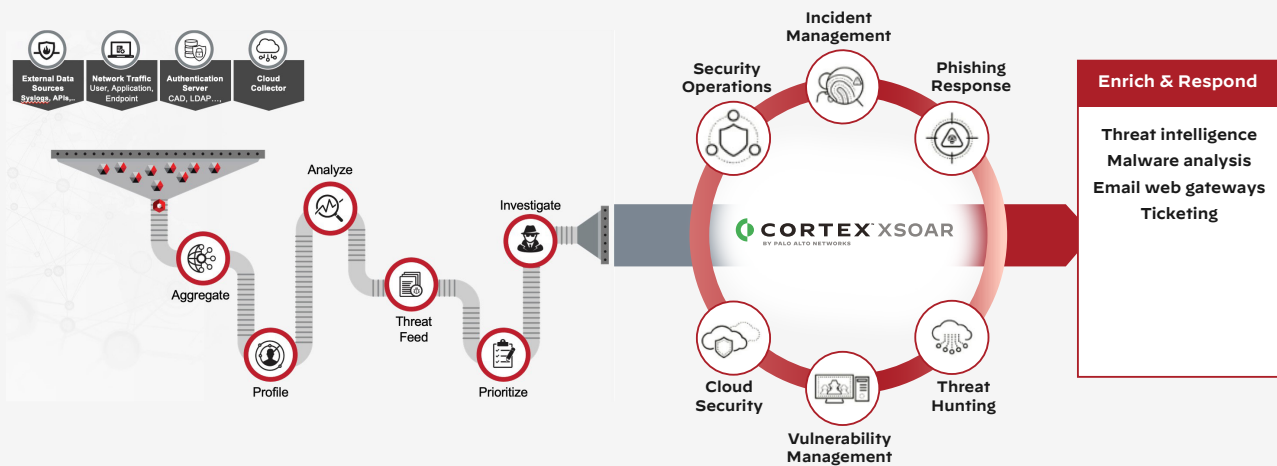
KEY HIGHLIGHTS:

This robust technology alliance equips security teams to:

» Leverage insights by taking information from LinkShadow to coordinate security responses from 550+ Cortex XSOAR third-party product integrations.

» Extend LinkShadow and XSOAR functionality to get a Modernized Cyber SecOps driven by AI-based Advanced Machine Learning Algorithms.

» Increase ROI on the security investments with informed and actionable insights.

» Use LinkShadow Analytics to enrich the Incident Intelligence to fully Automate Threat Hunting, and Incident Investigation, Orchestration and Response.

» Improve team's effectiveness and efficiency by minimizing the work overhead and automating the repetitive actions with Cortex SOAR.

🖥 www.paloaltonetworks.com/cortex/xsoar