Automating Investigation and Defense with ThreatX and Cortex™ XSOAR by Palo Alto Networks

CORTEX XSOAR
BY PALO ALTO NETWORKS

AppSec teams must defend an ever-growing set of web applications and APIs from a wide variety of evolving threats. To keep pace, teams must make sure their efforts are efficient and impactful. The integration of ThreatX and Cortex XSOAR delivers on this goal by pairing next-generation application security with industry-leading security automation and orchestration.

ThreatX provides a unique and comprehensive approach to application security that is both cloud and API native. The platform brings together traditional WAF protection, application and attacker behavioral analysis, anti-bot functionality, deception, and DDoS protection into a single context. Entities and evolving threats are tracked and scored over time in terms of their risk, and behavioral analysis and active interrogation is used to identify known and unknown threats even without a signature.

VALUE	Single Solution	Reliable Prevention	Save Time and Effort	Expertise on Demand
ARCHITECTURE & DELIVERY	**Cloud Native** *Support any app, microservice, etc.*	**API Native** *Protect APIs same as the front end*	**AppSec-as-a-Service (ASaaS)** *Staffed by AppSec experts, 24x7, monitoring, management, hunting, response*	
APPSEC CAPABILITIES	**WAF** *OWASP Top 10, injection, XSS...*	**Behavorial** *Signatureless, unknown threats*	**Anti-Bot** *Credential stuffing, ATO automation*	**DDoS** *Volumetric, Layer 7 attacks*
ANALYSIS TECHNIQUES	**Global Intelligence and Rules**	**Application Behavior Profiling**	**Attacker Behavior Profiling**	**Fingerprinting and Lifecycle Context** / **Active Interrogation and Deception**

The solution can be run can be delivered as a service, providing 24/7 monitoring, management, threat hunting, and response staffed by AppSec experts. The result provides organizations with a simple single solution to address all AppSec threats, highly reliable detection and enforcement, and the ability to save time and offload work from the internal security team.

Integration with XSOAR ensures that analysts can seamlessly access ThreatX's rich context for their investigations and trigger mitigation actions quickly. Analysts can easily pull context for any entity in an investigation including a variety of entity traits, IP information, notes, and risk scores. In addition to ThreatX's built-in enforcement options such as blocking or tarpitting, teams can use XSOAR to block or unblock an IP or whitelist or blacklist an IP as needed. These integrations allow for highly efficient analyst investigations as well as fully automated response and enforcement actions.

KEY BENEFITS

» **Faster Investigations** - Automatically pull important context such as host or risk traits for any entity in an investigation without the need for swivel-chair analysis. Analysts can both retrieve and add notes for an entity on demand.

» **Add Risk-Based Context to Investigations** - Easily integrate ThreatX Risk Scores into analysis and workflows. Threat Risk Scores automatically correlate across multiple detection strategies and phases of attack to provide a single highly-enriched score for the entity that accounts for the full scope and impact of an attacker's actions.

» **Stop Threats with Automated or Manual Enforcement** - Easily trigger enforcement actions based on investigations or policies including block/unblock IPs or whitelist/blacklist IPs.

FEATURES AND USE CASES

The integration between ThreatX and XSOAR enables security teams to automate many of the most common and time-consuming investigative and response tasks. This includes common malware investigation, containment of command-and-control traffic, as well as the ability to trigger enforcement based on detections from other security tools. The table below provides a list of the actions included in the integrations and playbooks that can use those actions.

Key Supported Actions

» **Block ip** - Block an IP

» **Unblock ip** - Unblock an IP

» **Blacklist ip** - Add an IP to the Blacklist

» **Whitelist ip** - Add an IP to the Whitelist

» **Get entities** - Get high-level Entity information

» **Get entity ips** - Get all Entity IP addresses

» **Get entity risk** - Get the latest Entity risk score

» **Get entity notes** - Get the Entity notes

» **New entity note** - Add a new note for the Entity

THREATX

SRC CYBER SOLUTIONS LLP

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

ABOUT CORTEX XSOAR by Palo Alto Networks

Cortex XSOAR by Palo Alto Networks is an extended security orchestration, automation and response (SOAR) platform that unifies case management, automation, real-time collaboration and threat intel management to transform every stage of the incident lifecycle. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intel and automate response for any security use case - resulting in significantly faster responses that require less manual review.