# Automated Internet Security Intelligence Enrichment, Detection & Prevention

CORTEX XSOAR BY PALO ALTO NETWORKS | RISKIQ

Cybercriminals are ever-increasing the scale and sophistication of their attacks, making it harder to detect and block their activity. Now more than ever, it is important that your security solutions and programs have access to up-to-date, internet-scale intelligence to counteract this trend. Having direct, high-volume access to internet intelligence and data allows security teams to build programmatic enrichment and defense mechanisms to better protect their enterprises, customers, and data.

RiskIQ Security Intelligence Services Cortex XSOAR enables security teams to rapidly scale and automate their threat detection and response programs. RiskIQ's Internet Intelligence Graph provides crucial external context to all internal IOC's and incidents. This context helps security teams understand how internal assets interact with external infrastructure to better detect and prevent attacks. With these insights, security teams can also proactively detect and block the new threat infrastructure that's part of attacks against their organization that they wouldn't otherwise know existed.

## Integration Features

- Extend the power of XSOAR native threat intel management by consuming millions of indicators of compromise every hour.
- Proactively enrich, investigate or block newly observed infrastructure that may leverage current events or your organization brand to exploit user trust.
- Curated feeds with lists of known bad URLs, Domains, and IP addresses associated with malware, phishing, and scam activity globally
- Leverage hundreds of Cortex XSOAR third-party product integrations to coordinate response across security functions based on insights from RiskIQ Security Intelligence Services.

## Benefits

- Improve SecOps efficiency with automated enrichment of internal indicators with petabytes internet security intelligence
- Generate new high-fidelity security incidents based on newly observed infrastructure, known malicious domains, phish, and scam content
- Proactively detect and block the latest malicious attacks and infrastructure before they are used against your organization.
- Automate and accelerate response efforts and threat investigations.

## Compatibility

**Products:** Cortex XSOAR, RiskIQ Security Intelligence Services

paloalto NETWORKS

CORTEX XSOAR
BY PALO ALTO NETWORKS

# Use Case #1
# Proactively Defend Your Organization with Latest Global Threat Intelligence

**Challenge:** Transformation initiatives, which have been accelerated by COVID-19, are producing an ever-expanding and dynamic digital presence for all companies. Threat Actors are taking advantage with increasingly sophisticated and agile attacks and campaigns. Your security solutions need internet-scaled, real-time threat intelligence updates to detect and prevent these attacks.

**Solution:** The RiskIQ Security Intelligence Services pack provides customers with filtered lists of known bad hosts, domains, IPs, and URLs that have been associated with malware, phishing, and scam events. These curated lists of malicious observations are powered by RiskIQ's Internet Intelligence Graph and updated continuously. Cortex XSOAR with native threat intel management automates the aggregation of intel feeds, monitoring and blocking actions across your security infrastructure.

**RiskIQ Security Intelligence Services - Attack Analytics Packs:**

- **Newly Observed Domains** - Domain names resolving to an IP address for the very first time in our Passive DNS repository since registration.
- **Newly Observed Hosts** - Hostnames observed resolving to an IP address for the very first time in our Passive DNS repository since registration.
- **Malware List** - Domains, IPs, and URLs associated with malware.
- **Phishing List** - Domains, IP addresses, and URLs associated with Phishing campaigns
- **Scam List** - Domains, IP addresses, and URLs associated with internet scams, including fake software, tech support, banking, and scareware
- **Content Filtering** - Domains and URLs categorized according to content that organizations may wish to block such as gambling, adult, liquor, weapons, etc.

**Benefit:** RiskIQ's Security Intelligence Services Attack Analytics pack for Cortex XSOAR enables security teams to detect, investigate, and prevent attacks faster and more effectively than ever before based on global intent security intelligence. Select the intelligence list that is most appropriate for threats that you face.

## About RiskIQ

RiskIQ is the leader in digital attack surface management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 75 percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social and mobile exposures. Trusted by thousands of security analysts, security teams, and CISO's, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect the business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures.

Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/. To learn more about RiskIQ, visit www.riskiq.com.

## About Cortex XSOAR

Cortex XSOAR, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit https://www.paloaltonetworks.com/cortex/xsoar.

paloalto NETWORKS