Discovery, Monitor and Defend Your Attack Surface

CORTEX XSOAR BY PALO ALTO NETWORKS | RISKIQ

The first step in every security program is knowing what you own, you leverage and what is connected to your organization. You can't protect what you don't know about. RiskIQ Digital Footprint pack for Cortex XSOAR provides you a deep, accurate, risk-based insight into your digital footprint. This integration enables proactive attack surface management and defense and allows security teams to create and enrich incidents with RiskIQ asset information.

Integration Features

Automate actions against new assets discovered like websites, domains, ip addresses and more in your attack surface in order to stay ahead of the adversary.

Accelerate triage efforts by querying your asset inventory in order to understand if the asset is owned and if so, by who within the organization.

Gain immediate insight into vulnerable assets that may be impacted by new or resurging exploits being abused by malicious actors.

Confidently approve or deny inbound or outbound network connections with automation.

Leverage hundreds of Cortex XSOAR third-party product integrations to coordinate response across security functions based on insights from Digital Footprint.

Benefits

Gain visibility into your digital attack surface from the outside in

Quickly pinpoint and remediate vulnerable assets

Automate response efforts to your ever-changing attack surface

Enrich security incidents with related asset information

Compatibility

Products: Cortex XSOAR, RiskIQ Digital Footprint

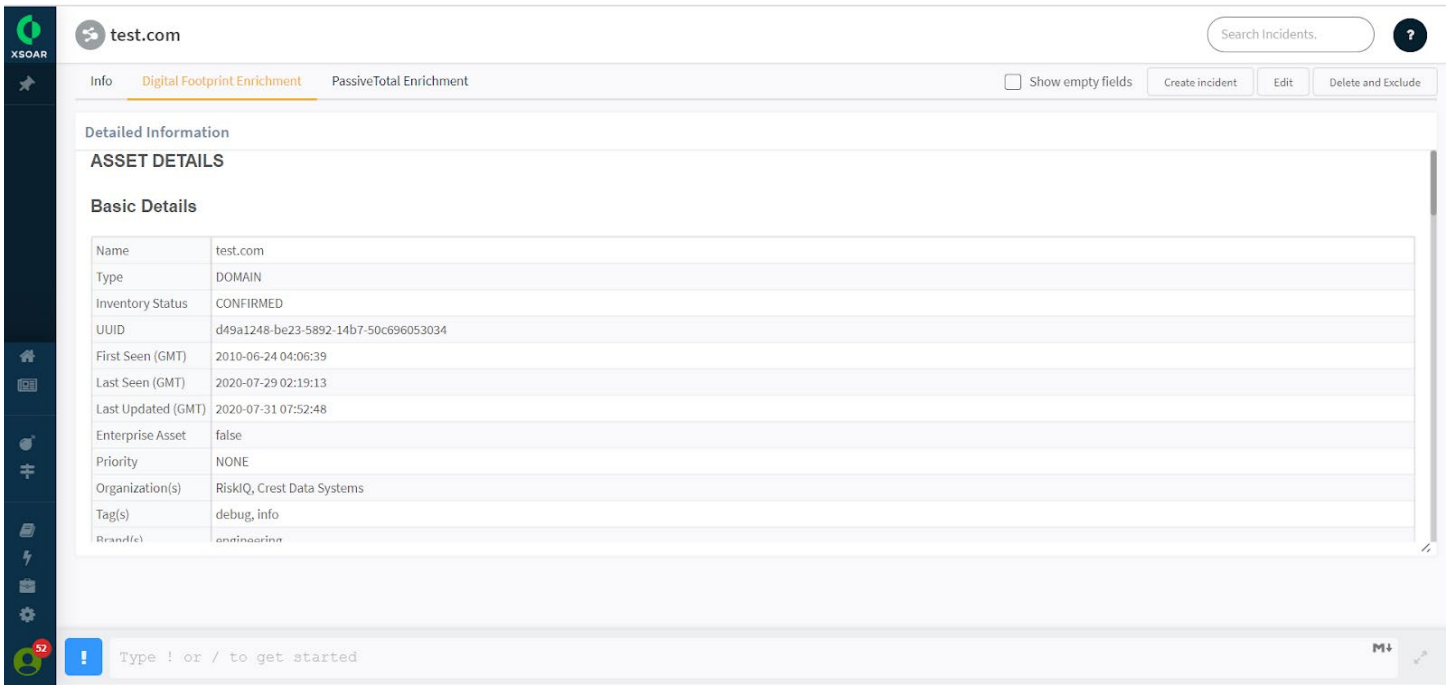
paloalto NETWORKS

Use Case #1
Continuously Discover and Secure Your Digital Assets

Challenge: Transformation initiatives are producing an ever-expanding and dynamic digital presence for all companies regardless of size. Department heads and business units are adopting new packlications and deploying new infrastructure at a rapid, unforeseen pace––often outside the control of IT or Security. This combined with the rise of sophisticated, global adversaries leaves companies vulnerable and security teams struggling or blind to the threats that are trying to exploit their company, brand, customers, partners, networks, and data. In order to protect your organization, you need an accurate, dynamic inventory of how you look to an attacker.

Solution: RiskIQ fingerprints billions of web pages and IPs every day, collecting telemetric data to produce an Internet Intelligence Graph. RiskIQ Digital Footprint leverages the Internet Intelligence Graph to uncover and inventory all the digital assets that are related to your organization, including third parties that you leverage or depend on and assets that may be impersonating you. Once you have this digital asset inventory, Digital Footprint enables security and IT teams to easily identify which assets are known/managed, unknown/shadow IT, vulnerable, or rogue.

Benefit: RiskIQ Digital Footprint pack for Cortex XSOAR enables you to discover, visualize, and defend your digital assets. See and manage your attack surface from a threat actor's point of view. Quickly pinpoint vulnerable assets leverage XSOAR playbooks to drive automated remediation activities.



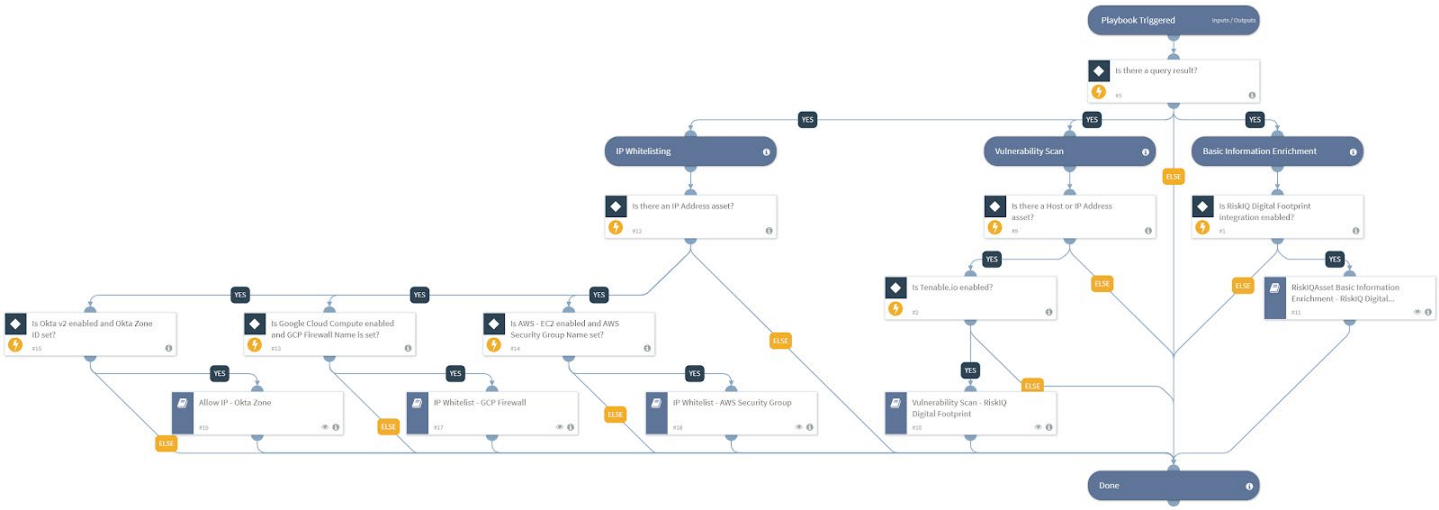
Use Case #2

Automate Attack Surface Risk Reduction & Reporting

Challenge: Because certificates expire, software requires patching, and assets associated with partner infrastructure can be compromised, that blind spot can leave your organization at serious risk. Digital threats outside the firewall include unknown and unmanaged assets, website defacement, compromised or vulnerable web components, broken links, and assets that have been blacklisted, currently or historically, as hosting phish or malware.

Solution: Digital Footprint pack for XSOAR consolidates all of your internet-exposed assets into an easy to manage inventory. These assets include websites, domains, hosts, web page content, ASNs, IPs, and active services on over 110 ports, nameservers, social media profiles, and mobile applications. Our dynamic inventory system provides full visibility into the state of all the assets and actively monitors them for unsanctioned changes or compromise.

Benefit: The RiskIQ Digital Footprint pack for XSOAR will automatically ingest your external asset inventory including asset metadata. We correlate and enrich this external asset inventory with XSOAR incidents and data to build reports, dashboards, trigger alerts, or aid in the identification of vulnerabilities or exposures against your assets.



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.