SecureX Threat Response

https://cs.co/1page

SecureX Threat Response is an investigation and remediation application that dramatically simplifies security by cutting the time and manual effort required for threat hunting and incident response. Included with SecureX at no additional cost with Cisco security products.

Use Cases:

- **Incident Response:** Leverage multiple security technologies in a single console to address and manage the aftermath of an attack by aggregating multiple security technologies for a holistic investigation and remediating in a single console.
- **Threat Hunting:** Proactively search for active threats in your environment with a holistic, integrated approach by aggregating multiple security technologies in a single console.

Key Features:

Casebook: A built-in tool to assign a case a name, description, organize, and share sets of observables of interest primarily during an investigation and threat analysis.

Incident Manager: Automated triage and prioritization of alerts from Cisco Secure Firewall and Cisco Secure Network Analytics. Allows for investigating and enriching events with context from integrations across security products as well as responding to high-urgency incidents.

Response: Respond to threats immediately through the convenient interface of one console (e.g., isolate hosts, block files, block domains).

Browser Plug-in: Browser extension (e.g., Chrome & Firefox) that allows for pulling IP addresses or domains from anywhere an observable is seen, for an investigation.

Relations Graph: Part of the Threat Response interface that shows all the observables found during the investigation and indicates relationships between them. Intuitive color and shape coding helps determine the nature of the events and the relationships.

Open-source Integrations: Custom integrations of any security operations tools and workflows available through open and well-documented APIs.

What can I search for?

- **IP Addresses (v4 and v6)**
- **Domains**
- **File Hashes (SHA-256, SHA1, MD5)**
- **MAC addresses**
- **URLs**
- **Syslog Messages**
- **Security Alerts (any format)**
- **Observables using the format:**
  <type>:"<value>" where the type could be (file_path, mac_address, device, hostname, url, user, ipv6, email, sha256, sha1, md5, ip, domain, email_subject, imei, amp_computer_guid, cisco_mid, pki_serial, imsi, amp-device, file_name, swc_device_id)

Value of Cisco Integrations:

Umbrella: The integration provides complete visibility into Internet activity across all locations and users and allows you to take action with a two-click response to quickly block domains.

Secure Email: Understand email as a threat vector by visualizing message, sender, and target relationships in the context of a threat. You can search for multiple email addresses, subject lines, and attachments at once to understand how a threat has spread.

Secure Firewall: Provides the capability to investigate, identify, and enrich intrusion events with context from integrations across security products. It also offers an automated triage and prioritization of intrusion events through the built-in Incident Manager.

Secure Endpoint: Investigate and identify files with context from integrations across security products. Get detailed information on affected endpoints and devices, including IP addresses, OS. Additionally, block files at endpoints and immediately quarantine affected endpoints with the Host Isolation response feature.

Malware Analytics: Get detailed intelligence about malware, associated paths, and more.

Secure Network Analytics: Visibility and security capabilities will enrich threat detection and response in the Threat Response console with agentless behavioral and anomaly detection capabilities.

Secure Web Appliance: Leverage multiple technologies to protect your network against the most common threat vector and provides Threat Response users with visibility into connections with unsafe or suspicious websites.

Resources:

SalesConnect
Data Sheet
3rd Party Integrations
Console access
Developer
YouTube Channel
HOWTO Series
Public link