Develop an Incident Investigation and Response Plan

Develop an Incident Investigation and Response Plan

Reducing the mean time to detect (MTTD) and mean time to respond (MTTR) are the end goals of any security operations team. How long does it take to detect an issue, and then how quickly can we respond?

Security information and event management (SIEM) is a well-tested take on log-and-event management solutions. At its core, SIEM is about gathering as much log information as possible from all over an organization. Many SIEM solutions can take log data from IoT security tools, firewall event logs, and everything in between. This kind of solution starts to break down the silo walls, integrating with multiple solutions and centralizing important security information. What SIEM doesn't do is give security engineers a boost in threat response time and efficacy. Seeing the security landscape of your organization is great for many things but responding to threats is just as important.

Security orchestration, automation and response (SOAR) takes a lot of what makes SIEM great and adds extra layers to account for some of the limitations. Like SIEM, SOAR solutions take data from different parts of the security infrastructure and put it in one place. SOAR solutions offer options to automate various auditing, log, and scanning tasks. Automation can't take care of everything, however, and sometimes requires human intervention. The "response" part of SOAR is about organizing and managing the response to a security threat. This feature set utilizes orchestration and automation information to help security staff make decisions and respond to threats. SOAR automation doesn't automate responses to security breaches. It automates simple analysis tasks to reduce security personnel workloads.

While SIEM and SOAR emphasize logs and analysis, Extended Detection and Response (XDR) solutions focus on the endpoints themselves. This is where the action is. This is what the outside parties are attacking.

Cisco SecureX

SecureX is a cloud-native, built-in platform experience within the Cisco Secure portfolio and connected to your infrastructure, which is integrated and open for simplicity, combines multiple otherwise disparate sensor and detection technologies into one unified location for visibility, and provides automation and orchestration capabilities to maximize operational efficiency, all to secure your network, users and endpoints, cloud edge, and applications. With SecureX, security teams can:

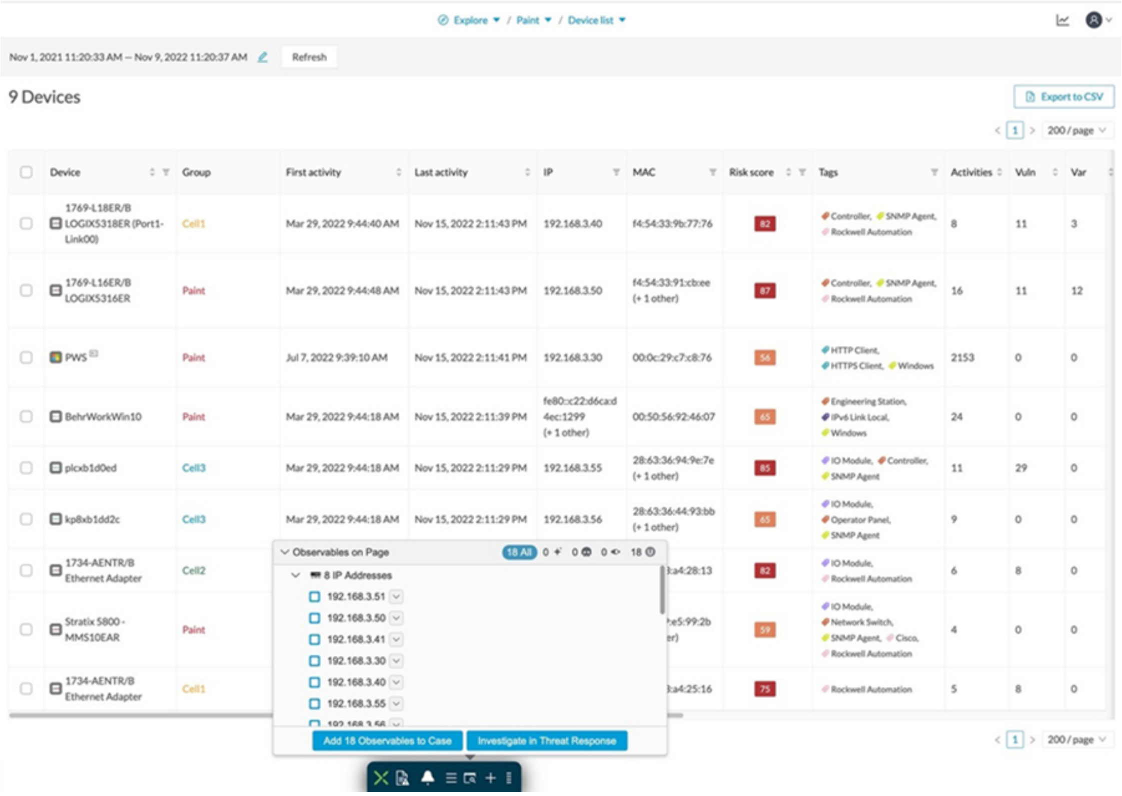
- **Radically reduce the dwell time and human-powered tasks** involved with detecting, investigating, and remediating threats to counter attacks or securing access and managing policy to stay compliant – make faster decisions with less overhead and better precision with less error.
- **Enable time savings and better collaboration** involved with orchestrating and automating security across SecOps, ITOps, and NetOps teams, which helps advance your security maturity level using your existing resources and realizes more desired outcomes with measured, meaningful metrics.

  Reduce MTTD / MTTR and reduce costs with real benefits in 15 minutes – even if you start small with a single product and grow as your needs dictate over time to consolidate security vendors without compromising security efficacy.

SecureX Ribbon

Part of the SecureX design philosophy is that you should not have to navigate to multiple different consoles to get all the functions you need for one business task. The SecureX ribbon brings this philosophy to reality across the portfolio. Via the ribbon, a persistent bar in the lower portion of the UI of all ribbon-capable products, you have access to all the functions lent to SecureX by all your deployed SecureX-capable technologies. The ribbon is collapsible and expandable to open ribbon apps, launch integrated applications, and view your account profile. From the ribbon, you can pivot between SecureX or the console of any integrated product, into any other integrated product, and search the current web page for malicious file hashes, suspicious domains and other cyber observables. You can then also add observables to a case or investigate observables in the threat response application.

Figure 1: SecureX Ribbon in Cyber Vision



Nov 1, 2021 11:20:33 AM – Nov 9, 2022 11:20:37 AM

9 Devices

□	Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags	Activities	Vuln	Var
□	1769-L18ER/B LOGIX5318ER (Port1-Link00)	Cell1	Mar 29, 2022 9:44:40 AM	Nov 15, 2022 2:11:43 PM	192.168.3.40	f4:54:33:9b:77:76	82	Controller, SNMP Agent, Rockwell Automation	8	11	3
□	1769-L16ER/B LOGIX5316ER	Paint	Mar 29, 2022 9:44:48 AM	Nov 15, 2022 2:11:43 PM	192.168.3.50	f4:54:33:91:cb:ee (+ 1 other)	87	Controller, SNMP Agent, Rockwell Automation	16	11	12
□	PWS	Paint	Jul 7, 2022 9:39:10 AM	Nov 15, 2022 2:11:41 PM	192.168.3.30	00:0c:29:c7:c8:76	56	HTTP Client, HTTPS Client, Windows	2153	0	0
□	BehrWorkWin10	Paint	Mar 29, 2022 9:44:18 AM	Nov 15, 2022 2:11:39 PM	fe80::c22:d6ca:d4ec:1299 (+ 1 other)	00:50:56:92:46:07	65	Engineering Station, IPv6 Link Local, Windows	24	0	0
□	plcxb1d0ed	Cell3	Mar 29, 2022 9:44:18 AM	Nov 15, 2022 2:11:29 PM	192.168.3.55	28:63:36:94:9e:7e (+ 1 other)	85	IO Module, Controller, SNMP Agent	11	29	0
□	kp8xb1dd2c	Cell3	Mar 29, 2022 9:44:18 AM	Nov 15, 2022 2:11:29 PM	192.168.3.56	28:63:36:44:93:bb (+ 1 other)	65	IO Module, Operator Panel, SNMP Agent	9	0	0
□	1734-AENTR/B Ethernet Adapter	Cell2				:a4:28:13	82	IO Module, Rockwell Automation	6	8	0
□	Stratix 5800 - MMS10EAR	Paint				:e5:99:2b er)	59	IO Module, Network Switch, SNMP Agent, Cisco, Rockwell Automation	4	0	0
□	1734-AENTR/B Ethernet Adapter	Cell1				:a4:25:16	75	Rockwell Automation	5	8	0

The SecureX ribbon is a feature of Cyber Vision and appears on the bottom of the Cisco Cyber Vision Center user interface.

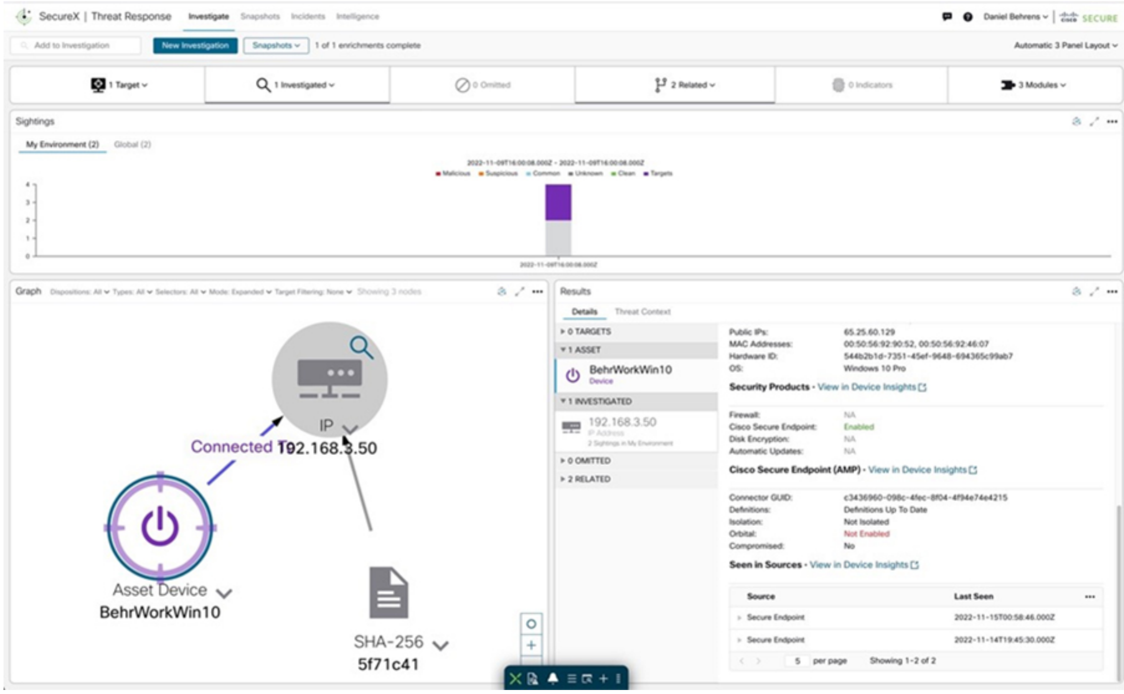
SecureX Threat Response

SecureX threat response is a security investigation and incident response application. It simplifies threat hunting and incident response by accelerating detection, investigation, and remediation of threats. The threat response application provides your security investigations with context and enrichment by connecting your Cisco security solutions (across endpoint, network, and cloud) and integrating with third-party tools, all in a single console.

To understand whether a threat has been seen in your environment as well as its impact, SecureX threat response aggregates contextual awareness from Cisco security product data sources along with global threat intelligence from Talos® and third-party sources via APIs. Threat response identifies whether observables such as file hashes, IP addresses, domains, and email addresses are suspicious or malicious, and whether you have been affected by them. It also provides the ability to remediate directly from the interface and block suspicious files, domains, isolate hosts, and more without pivoting to another product first. Key features and benefits include:

- **Relations Graph**: visualize all the observables found during the investigation and determine the relationships between them
- **Casebook**: save, share, and enrich threat analysis to enable documentation of all analysis in a cloud casebook so seamlessly work a case across multiple tools, Cisco or otherwise and better collaborate among staff
- **Response Actions**: enforce protective controls without pivoting to other product consoles

Figure 2: SecureX Threat Response Example



Public IPs: 65.25.60.129
MAC Addresses: 00:50:56:92:90:52, 00:50:56:92:46:07
Hardware ID: 544b2b1d-7351-45ef-9648-694365c99ab7
OS: Windows 10 Pro

Security Products · View in Device Insights

Firewall: NA
Cisco Secure Endpoint: Enabled
Disk Encryption: NA
Automatic Updates: NA

Cisco Secure Endpoint (AMP) · View in Device Insights

Connector GUID: c3436960-098c-4fec-8f04-4f94e74e4215
Definitions: Definitions Up To Date
Isolation: Not Isolated
Orbital: Not Enabled
Compromised: No

Seen in Sources · View in Device Insights

Source	Last Seen
Secure Endpoint	2022-11-15T00:58:46.000Z
Secure Endpoint	2022-11-14T19:45:30.000Z

5 per page Showing 1-2 of 2

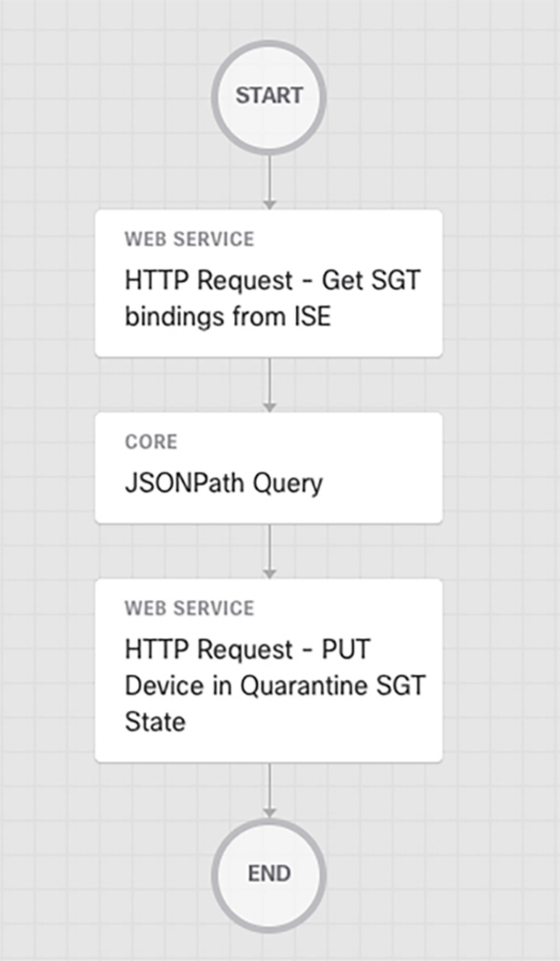
It is possible to launch a SecureX investigation from Cisco Cyber Vision Center. The Cyber Vision baseline feature can help highlight unexpected and potentially malicious activity in the network by monitoring a known good state for any changes. Often, an infected device starts by scanning the network to identify vulnerable components to attack. This traffic anomaly can be easily identified using Cisco Cyber Vision Monitor Mode.

To cross launch an investigation in SecureX Threat Response, click on the *Investigate in Cisco Threat Response* button after clicking on the suspicious component.

SecureX Orchestration

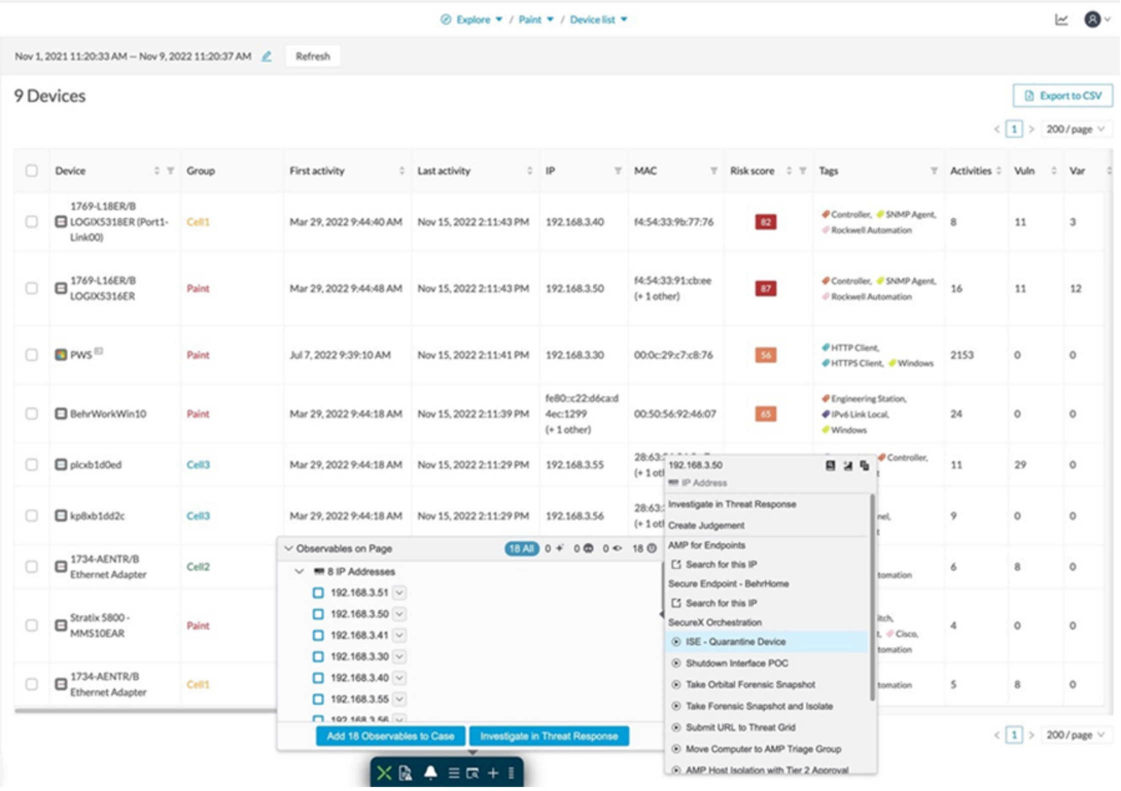
SecureX orchestration automates repetitive and critical security tasks such as threat investigation, hunting, and remediation use cases. SecureX orchestration provides pre-built workflows and response capabilities, or you can build your own with a no/low-code, drag-drop canvas to strengthen operational efficiency and precision, and lower operational costs.

Figure 3: SecureX Orchestration Workflow - Quarantine Device using SGT


START
WEB SERVICE
HTTP Request - Get SGT bindings from ISE
CORE
JSONPath Query
WEB SERVICE
HTTP Request - PUT Device in Quarantine SGT State
END

SecureX orchestration enables you to define workflows that reflect your typical security processes; the automation steps (activities), the logic or flow between these steps, and how to flow data from one step to the next. With SecureX, you can leverage Cisco Secure and thirdparty multi-domain systems, applications, databases, and network devices in your environment to create these workflows. An example workflow would be to take an IP address, or hostname and assign that endpoint an SGT in ISE that would ultimately block communication from occurring on the network.

Figure 4: Invoking SecureX Orchestration Workflow from the Ribbon in Cyber Vision



Nov 1, 2021 11:20:33 AM – Nov 9, 2022 11:20:37 AM

9 Devices

☐	Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags	Activities	Vuln	Var
☐	1769-L18ER/B LOGIX5318ER (Port1-Link00)	Cell1	Mar 29, 2022 9:44:40 AM	Nov 15, 2022 2:11:43 PM	192.168.3.40	f4:54:33:9b:77:76	82	Controller, SNMP Agent, Rockwell Automation	8	11	3
☐	1769-L16ER/B LOGIX5316ER	Paint	Mar 29, 2022 9:44:48 AM	Nov 15, 2022 2:11:43 PM	192.168.3.50	f4:54:33:91:cb:ee (+ 1 other)	87	Controller, SNMP Agent, Rockwell Automation	16	11	12
☐	PWS	Paint	Jul 7, 2022 9:39:10 AM	Nov 15, 2022 2:11:41 PM	192.168.3.30	00:0c:29:c7:c8:76	56	HTTP Client, HTTPS Client, Windows	2153	0	0
☐	BehrWorkWin10	Paint	Mar 29, 2022 9:44:18 AM	Nov 15, 2022 2:11:39 PM	fe80::c22:d6ca:d 4ec:1299 (+ 1 other)	00:50:56:92:46:07	65	Engineering Station, IPv6 Link Local, Windows	24	0	0
☐	plcxb1d0ed	Cell3	Mar 29, 2022 9:44:18 AM	Nov 15, 2022 2:11:29 PM	192.168.3.55	28:63: (+ 1 ot		Controller,	11	29	0
☐	kp8xb1dd2c	Cell3	Mar 29, 2022 9:44:18 AM	Nov 15, 2022 2:11:29 PM	192.168.3.56	28:63: (+ 1 ot		nel, t	9	0	0
☐	1734-AENTR/B Ethernet Adapter	Cell2						tomation	6	8	0
☐	Stratix 5800 - MMS10EAR	Paint						itch, t, Cisco, tomation	4	0	0
☐	1734-AENTR/B Ethernet Adapter	Cell1						tomation	5	8	0

Note: The current version of the Industrial Security Design guide does not provide in-depth design guidance for Incident Investigation and Response. This part of the security will be added in a future release.