Sophos XDR Use Cases

Available with Intercept X Advanced with XDR and Intercept X Advanced for Server with XDR

Answer business critical IT operations and threat hunting questions then take action where needed. Both IT admins and cybersecurity analysts can take advantage of the powerful functionality.

Perform IT security operations and threat hunting tasks

- Choose from fully customizable, pre-written template use cases
- Quickly take action when you have the information you need
- Covers endpoints, servers, firewalls, email, cloud hosts, mobiles and 0365

IT Operations Use Cases

IT Operations Use Cases keep your IT operations hygiene in peak condition. Here are a few example use cases:

Device health checks

Identify devices that are having performance issues then remotely access them and take needed action.

- Find devices with low disk space, high memory/CPU usage or that are pending reboot
- Remotely access devices to free up disk space, investigate causes of high usage and reboot as needed

Vulnerabilities

Detect devices that have issues or vulnerabilities that can be exploited by malware or attackers.

- Locate devices with software vulnerabilities, unknown services running or unauthorized browser extensions and detect shared or stolen account credentials
- Remotely access devices to install patches, investigate and terminate unknown services, uninstall browser extensions and update cloud account credentials

Unwanted software

Track down software that could cause compliance or productivity issues.

- Find unwanted programs such as Spotify, Steam and Bittorrent
- Remotely access devices and uninstall the software

Configuration oversights

Find devices and cloud workloads that have configuration issues that can pose security risks.

- Identify servers with RDP and SSH enabled, cloud security groups with network ports left open, monitor and inventory public cloud hosts, containers and more
- Remotely access the servers, disable RDP/SSH and check for servers listening on the open ports

Compliance

Identify and address compliance issues on-premises and in the cloud.

- Find sensitive files, assess configurations for AWS, Azure and GCP environments
- Remotely access devices to delete sensitive files, ensure secure cloud configurations against CIS benchmarks

Project rollouts

Check whether IT projects have been rolled out across all devices.

- See if software has been deployed on devices to measure progress throughout rollout
- Remotely access devices to ensure successful deployment and reboot if required to make any necessary changed

SOPHOS

Office network issues (requires Sophos Firewall)

See and rectify network issues across your office sites.

- Understand why an office is having network issues that are slowing performance
- Identify which application is causing the problem

Device management (requires Sophos Firewall)

Identify and understand the devices in your organization's IT environment.

- See unmanaged and unprotected devices such as laptops, mobiles and IoT devices
- Get additional oversight on legacy or unmanageable devices such as specialized medical equipment

Expect the unexpected

With 30 days of cloud storage don't get caught out by unexpected events.

- Look back 30 days for unusual activity on a missing device
- See what happened to a device even if it has been wiped or destroyed

Threat Hunting Use Cases

Track down evasive, subtle threats and quickly clean them up. Here are just a few example use cases:

Network attacks

Identify process making unusual network access attempts.

- Detect processes attempting to connect on non-standard ports or unusual outbound traffic from a cloud workload
- Analyze cloud security groups to identify resources exposed to the public internet
- Remotely access the device/workload, terminate the process and check for lateral movement

Modified files

Find items that haven been modified in an unexpected manner.

- Identify processes that have recently modified files or registry keys
- Remotely access the device, examine the changes and take action

Obfuscated scripts

File-less, memory-based attacks are a common attack vector.

- Dig into the details of unexpected PowerShell executions
- Remotely access the device, run additional forensic tools and terminate suspect processes

Disguised processes

Some malicious processes disguise themselves to avoid detection.

- Detect processes that have disguised themselves
- Remotely access the device, terminate suspicious processes and run forensic tools

MITRE ATT&CK framework

The MITRE ATT&CK framework is a commonly used template for identifying attack techniques.

- Use your own or Sophos queries to identify attack tactics and techniques used by adversaries
- Based on the identified technique hone your investigation to look at potential follow up attacks or areas to double check

Incident scope

Understand the impact of an incident and which devices and users were impacted.

- Identify devices that clicked on a link from a phishing email
- See which devices downloaded files from the phishing site, remotely access them and perform cleanup

Extend investigation periods

Use 30 days of cloud data in addition to 90 days on device and real-time state.

- Investigate 30 days of data without needing to bring a device back online
- See what happened to devices incapacitated in an attack

Use rich network data (requires Sophos Firewall)

Incorporate network data into your threat hunting and investigation.

- Cross reference blocked malicious traffic with other IoCs to understand a wider attack
- Use ATP and IPS detections from the firewall to investigate suspect hosts and devices

Use rich email data (requires Sophos Email)

Integrate email information to get additional insight into your environment.

- Compare email header information with other IoCs to better understand an incident
- Identify suspicious files and quickly delete them from devices and O365 mailboxes

Enhanced cloud workload protection (requires Cloud Optix Advanced)

Detect and respond to public cloud incidents from the same console.

- Investigate AWS cloud environment API, CLI, and management console activities with seamless integration to AWS CloudTrail
- Use a range of queries associated with attacker tactics: Initial Access, Persistence, Privilege Escalation and Exfiltration

To learn more about Sophos XDR head over to Sophos.com/XDR.

22-01-04 UC-NA (NP)

SOPHOS