CISCO SECUREX THREAT RESPONSE CASE STUDY

Large Enterprise Retail Company

Introduction

This case study of a large enterprise retail company is based on a May 2020 survey of Cisco SecureX threat response customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

> “Email and web security. These products have extended our ability to search for iocs through the message header and body, a very complex thing to do without it.”
>
> “It allows me to easily search and remediate systems "

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Cisco SecureX threat response:

- Needed to solve the following security challenges when they started using SecureX threat response with their Cisco Security products:
  - Needed their security technologies to work together
  - Needed a better way to visualize whether a threat has impacted their environment
  - Wanted to identify and remediate threats faster
  - Wanted to centralize and triage high priority alerts
  - Wanted to maximize the time of their skilled resources due to being understaffed

Use Case

The key features and functionalities of Cisco SecureX threat response that the surveyed company uses:

- Uses SecureX threat response daily.
- Improved collaboration across the following teams after using Casebook in SecureX threat responsee:
  - Improved collaboration across NetOps and/or IT
- agrees that SecureX threat response’s ability to connect with 3rd party security tools for comprehensive investigations is important to them.

Results

The surveyed company achieved the following results with Cisco SecureX threat response:

- Greatest value they get from the Chrome or Firefox browser plug-in for SecureX threat response:
  - Ability to kick off an investigation
- Eliminated the following tasks after using SecureX threat response:
  - Planning tasks
- Weekly time savings their Security Operations team achieved by using SecureX threat response for the following use cases:
  - incident management: at least 4-6 hours/week
  - threat intelligence and investigations: at least 4-6 hours/week
  - remediation / first strike response actions: at least 1-3 hours/week

Company Profile

The company featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Company Size:
Large Enterprise

Industry:
Retail

About Cisco SecureX threat response

Don’t clone your security team—get Cisco Threat Response instead. Threat Response automates integrations across select Cisco Security products and accelerates key security operations functions: detection, investigation, and remediation. It is a key pillar of our integrated security architecture.

Learn More:

Cisco

Cisco SecureX threat response

Source: TechValidate survey of a Large Enterprise Retail Company

✓ Validated Published: Jul. 16, 2020 TVID: 119-932-577

Research by TechValidate by SurveyMonkey