CISCO THREAT RESPONSE CASE STUDY

Oznet

Introduction

This case study of Oznet is based on a May 2020 survey of Cisco Threat Response customers by TechValidate, a 3rd-party research service.

> "All these solutions we handle in the Threat Response Stealthwatch Enterprise, Firepower, Umbrella."
>
> "It is a very good tool to perform event analysis in a centralized console, for me it is the best."
>
> "Cisco allows me to visualize quickly and to correct in time."

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Cisco Threat Response:

- Needed to solve the following security challenges when they started using 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 Threat Response that the surveyed company uses:

- Uses Threat Response daily.
- Agrees that 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 Threat Response:

- Greatest value they get from the Chrome or Firefox browser plug-in for Threat Response:
  - Ability to kick off an investigation
  - Ability to consume threat intelligence blogs
  - Immediate access to context from Cisco Security products
  - Immediate access to context their 3rd party web-based product (SIEMs or other security consoles)
- Eliminated the following tasks after using Threat Response:
  - Planning tasks
  - Detection & Analysis tasks
  - Post-Incident Activity tasks
- Weekly time savings their Security Operations team achieved by using Threat Response for the following use cases:
  - Incident management: at least 12-18 hours/week
  - Threat intelligence and investigations: at least 7-12 hours/week
  - Remediation / first strike response actions: at least 7-12 hours/week

Company Profile

Company:
Oznet

Company Size:
Small Business

Industry:
Security Products & Services

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: Dennis Morales, Security Officer, Oznet

Research by TechValidate by SurveyMonkey

Validated Published: Jun. 19, 2020 TVID: E6A-0F1-341