Rapid7 InsightIDR Case Study: CU4SD

Introduction

This case study of CU4SD is based on an October 2021 survey of InsightIDR customers by TechValidate, a 3rd-party research service.

> "It's vastly improved the visibility of our network, endpoints, and weak spots. We, now, have the ability to respond to threats we didn't see before we had InsightDR."

Challenges

The business challenges that led the profiled company to evaluate and ultimately select InsightIDR:

- Difficulty identify cyber security threats on endpoints
- Lacking SOC efficiency around detection and response
- Dealing with many blind spots across our environment

Use Case

The key features and functionalities of InsightIDR that the surveyed organization uses:

- User Behavior Analytics (UBA)
- Curated Threat Intelligence and Detections
    - Network Traffic Analysis (NTA)
- Cloud Monitoring and Detections
- Centralized Log Management
- Investigations and Incident Response
- Deception Technology
- File Integrity Monitoring (FIM)
- Automation

This organization leverages InsightIDR as both their SIEM and XDR.

They have deployed the Rapid7 Insight Agent across 76% – 99% of the assets in their environment. Outcomes realized by leveraging the Insight Agent with InsightIDR:

- Improved endpoint visibility
- Accelerated detection of targeted or compromised assets
- Accelerated time to contain threats on the endpoint

Results

The surveyed company achieved the following results with InsightIDR:

- Confirmed that InsightIDR provided superior time to value, compared to similar tools used in the past.
- Since they started using InsightIDR, they said that Threat detection and response is greatly improved.

The surveyed company agreed that InsightIDR helped them to:

- Level up and advance security program
- Spend more time on training and advancing security skills
- Spend more time on innovative work / special projects
- Greatly improve team efficiency
- Reduce team burnout
- Improve work-life balance
- Improve employee retention

Since adopting InsightDR, they stated that they were able to reduce:

- Team time to address an incident by 50% or more
- Mean time to respond (MTTR) by 25-50%
- Mean time to resolution or containment (MTTC) by 25-50%
- Employee downtime as a result of incidents by 50% or more
- Occurrence of false positives by 25-50%

Organization Profile

Organization:
CU4SD

Industry:
Educational Institution

About Rapid7 InsightIDR

Rapid7 is advancing security to accelerate innovation. Learn how our Insight Platform delivers shared visibility, analytics, and automation at www.rapid7.com.

Learn More:

↗ Rapid7