RAPID7 | insightIDR

RAPID7 INSIGHTIDR CASE STUDY

Rapid7 InsightIDR Case Study: Educational Institution

Introduction

This case study of a educational institution is based on an October 2021 survey of Rapid7 InsightIDR customers by TechValidate, a 3rd-party research service. The profiled organization asked to have their name blinded to protect their confidentiality.

> “Rapid7 InsightIDR improved our detection and response times”

Challenges

The business challenges that led the profiled organization to evaluate and ultimately select Rapid7 InsightIDR:

- Difficulty identifying 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 Rapid7 InsightIDR that the surveyed organization uses:

- User Behavior Analytics (UBA)
- Curated Threat Intelligence and Detections
- Endpoint Detection and Response (EDR)
- Centralized Log Management
- Investigations and Incident Response
- Automation

This organization leverages InsightIDR as both their SIEM and XDR.

They have deployed the Rapid7 Insight Agent across 100% 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 organization achieved the following results with Rapid7 InsightIDR:

- Confirmed that they have not used a similar tool 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
- Improve work-life balance

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

- Team time to address an incident by 25-50%
- Mean time to respond (MTTR) by 50% or more
- Mean time to resolution or containment (MTTC) by 50% or more
- Employee downtime as a result of incidents by 10-25%
- Occurrence of false positives by 25-50%

Organization Profile

The organization 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.

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

Source: TechValidate survey of a Educational Institution

Validated Published: Feb. 8, 2022 TVID: 48D-1F8-936

Research by TechValidate by SurveyMonkey