RAPID7 INSIGHTIDR CASE STUDY

Rapid7 InsightIDR Case Study: Medium Enterprise Professional Services Company

Introduction

This case study of a medium enterprise professional services company is based on an October 2021 survey of InsightIDR customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

Challenges

The business challenges experienced before evaluating and ultimately selecting InsightIDR:

- Lots of jumping between different tools; leveraging multiple tools to look at different security telemetry
- Dealing with many blind spots across our environment

Use Case

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

- User Behavior Analytics (UBA)
- Curated Threat Intelligence and Detections
- Endpoint Detection and Response (EDR)
- Investigations and Incident Response
- File Integrity Monitoring (FIM)

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

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 50% or more
- Mean time to resolution or containment (MTTC) by 50% or more
- Employee downtime as a result of incidents by 50% or more
- Occurrence of false positives by 50% or more

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:
Medium Enterprise

Industry:
Professional Services

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