RAPID7 INSIGHTIDR CASE STUDY

Rapid7 InsightIDR Case Study: Medium Enterprise Computer Software Company

Introduction

This case study of a medium enterprise computer software company is based on a March 2022 survey of Rapid7 InsightIDR customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

> "Rapid7 InsightIDR is a great tool that has helped us gather all of our resources into one place for analysis."

Challenges

The business challenges experienced before evaluating and ultimately selecting Rapid7 InsightIDR:

- Too many false positive alerts from current detection tools; too much noise
- Difficulty identifying cyber security threats on endpoints
- Lacking SOC efficiency around detection and response
- Lots of jumping between different tools; leveraging multiple tools to look at different security telemetry
- Challenged to satisfy compliance and regulatory requirements around log retention and monitoring

Use Case

The key features and functionalities of Rapid7 InsightIDR that the surveyed company uses:

- User Behavior Analytics (UBA)
- Endpoint Detection and Response (EDR)
- Network Traffic Analysis (NTA)
- Centralized Log Management
- Compliance Reporting
- Threat Hunting
- Deception Technology

This organization leverages InsightIDR as both their SIEM and XDR.

They have deployed the Rapid7 Insight Agent across 51% – 75% of the assets in their environment. Outcomes realized by leveraging the Insight Agent with InsightIDR:

- Improved endpoint visibility
- Accelerated time to contain threats on the endpoint

Results

The surveyed company achieved the following results with Rapid7 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 Rapid7 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 Rapid7 InsightIDR, 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 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:
Computer Software

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 Medium Enterprise Computer Software Company

Research by TechValidate by SurveyMonkey

Validated Published: Apr. 8, 2022 TVID: 565-E6F-62E