

Rapid7 InsightIDR Case Study: Critical Software

Introduction

This case study of Criticalsoftware is based on a March 2022 survey of Rapid7 InsightIDR customers by TechValidate, a 3rd-party research service.

Challenges

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

- Too many false positive alerts from current detection tools; too much noise
- Lacking SOC efficiency around detection and response

Use Case

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

- Endpoint Detection and Response (EDR)
- Centralized Log Management
- Compliance Reporting
- Investigations and Incident Response

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

Results

The surveyed company achieved the following results with Rapid7 InsightIDR:

- Since they started using InsightIDR, they said that Threat detection and response has 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
- Greatly improve team efficiency
- Reduce team burnout
- Improve work-life balance

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

- Mean time to respond (MTTR) by 25-50%
- Mean time to resolution or containment (MTTC) by 25-50%

Company Profile

Company:
Criticalsoftware

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](#)