RAPID7 INSIGHTIDR CASE STUDY

Rapid7 InsightIDR Case Study: ODEK Technologies

Introduction

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

> "InsightIDR gives us visibility into the activities on our servers and network. Before we were blind."

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

Use Case

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

- What they leverage InsightIDR for:
  - User Behavior Analytics (UBA)
  - Curated Threat Intelligence and Detections
  - Network Traffic Analysis (NTA)
- InsightIDR is their Security Incident and Event Management (SIEM) product. "As our SIEM we leverage InsightIDR for our data lake, log ingestion, data retention and compliance tool, and to monitor for policy violations."
- They have deployed 51% – 75% of their assets in the Insight Agent.
- Outcomes realized by leveraging the Insight Agent with InsightIDR:
  - 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 about the same 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.
- 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 by how much were you able to reduce the following:
  - The team time to address an incident: 50% or more
  - The mean time to respond (MTTR): 50% or more
  - The mean time to resolution or containment (MTTC): 25-50%
  - Employee downtime as a result of incidents: 50% or more
  - Occurrence of false positives: 50% or more

Company Profile

Company:
ODEK Technologies

Company Size:
Medium Enterprise

Industry:
Financial 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

✓ Validated   Published: Nov. 11, 2021   TVID: 3A4-B4C-4BA

Research by **TechValidate** by SurveyMonkey