RAPID7

# SIEM Deployment Checklist

## Insights from Rapid7's InsightIDR deployments and the Gartner® Report "How to Deploy a SIEM Solution Successfully"

No matter which SIEM you choose, deployment takes careful planning. Below are tried-and-true steps to follow and questions to ask yourself throughout the process:

### ☑ Create clear goals and use cases

- What problems do you intend the SIEM to address?
- Who are the intended users?
- What are their requirements?
- What data is required to support use cases, and where does it come from?

*Guidance: focus on data that will directly address required use cases. Gartner says "use an output-driven approach to deploy a SIEM solution..."*

### ☑ Align risk tolerance with use cases

- What are your business risks? (Define and rank order them)
- What are your technical risks? (Define, rank order)
- Align your risks with use cases and requirements
- Which log/data sources fit the use cases best?

*Guidance: build project advocacy and support by focusing on quick wins. Gartner says "the initial use case for SIEM should be valuable, but more importantly, achievable..."*

### ☑ Plan architecture around use cases and data sources

- Is a cloud log aggregator/collector required?
- How many on-prem collectors are required?
- What data is required to support use cases?
- Where does this supporting data come from?
- Where does the data need to be stored and for how long?

*Gartner says "Cloud SIEM solutions simplify the architecture and deployment of SIEM where the vendor is responsible for the back-end components and maintenance of the application…"*

☑ **Prepare for expansion at your own pace**

- What is the overall size and complexity of the environment?
- What compliance and administrative requirements will you need?
- Are there specific checks necessary to ensure optimal performance?

*Gartner says "Security and risk management leaders deploying a SIEM solution must follow a structured approach to ensure a successful implementation"*

Get the full Gartner® Report with our compliments. And if deployment speed matters to you, remember cloud-native InsightIDR leads the market. While the average SIEM deployment takes 6 months, InsightIDR is operational in weeks, often days.

*Gartner, How to Deploy a SIEM Solution Successfully, By Andrew Davies, Mitchell Schneider, Toby Bussa, Kelly Kavanagh, 7 July 2021*