Incident Detection & Response Deployment Package

Rapid7 Security Consulting & Education

Rapid7 products are easy to install and use, and our team can provide expert guidance to take your usage of the product much further. The Quick Start Services for InsightIDR help you through deployment and ensure that you get the most value out of your investment.

Rapid7's Security Consulting & Education team is composed of field experts with years of security experience, helping you extract the maximum value of our incident detection & response solutions. Our deployment services are tailored to operationalize your IR program, augmenting your deployment with product configurations, process automation, and reporting workflows. Working directly with your team and your current tools—onsite if you choose, we help you align InsightIDR with industry best practices. Our deployment services make the best use of valuable budget dollars and position you to maximize the success of your program.

2 DAY QUICK START DEPLOYMENT PACKAGE

Days

- Up to two (2) days of deployment services
- Up to 10,000 Assets

Overview

Rapid7 products are easy to install and use, and our team can provide expert guidance to take your usage of the product much further. One of our Consultants will work with you, or your team, to deploy and configure the product to the latest recommended practices. Significant focus will be placed on Cybersecurity knowledge transfer and demonstrating how you, or your team, can quickly get the most value out of your investment.This package is suitable for deployments of up to 10,000 Assets.

Rapid7's Security Consulting & Education team is composed of field experts with years of security experience, helping you extract the maximum value of our incident detection & response solutions. Our deployment services are tailored to operationalize your IR program, augmenting your deployment with product configurations, process automation, and reporting workflows.

The topics we will cover include:

- InsightIDR configuration and knowledge transfer, based on Rapid7 best practices
- Overview of the InsightIDR Platform and User interface
- Demonstration of the deployment of core system components
- Configuration Core Event Sources & optional High Value Event Sources;
- Best practice alignment for
  - Log Ingestion;
  - Log Searches;
  - Alerting;
  - Investigations, Incident Detection & Threat Hunting;
  - Early Detection & Deception Technology;
  - Monitoring of User & Account Activity
- Walkthrough of
  - Dashboards and Reporting;
  - Customisation of Dashboards
  - Custom Alerts
  - Forensic Jobs
  - Scheduled Threat Hunts
  - Effective use of Deception Technologies
- Review, Discussion and as time permits, optional implementation of Advanced Features;
  - Collecting custom logs
  - Automation workflows
  - Network traffic analysis

Primary Goals

- Set up InsightIDR using Rapid7's best practices
- Configure Collectors, core and high value event log sources
- Review and configure InsightIDR product settings and the Insight agent deployment
- Demonstrate the incident detection and investigation workflow
- Workshop log search, dashboards, custom parsing, custom alerts and advanced product features

The Methodology

- Phase I - Architecture
  - Mapping out the placement, resource requirements and connectivity for the InsightIDR Collectors and Insight Agents
- Phase II – Configuration
  - Collector deployment and activation
  - Best practice setup of core event sources, Insight agents, and deception technologies
  - Review and configure additional event sources

- Review and configure product settings

- Phase III – Knowledge Transfer
  - Demonstrate Log Search capabilities and workshop LEQL queries
  - Workshop Dashboards and reporting
  - Discuss, detection rules, alerts and the incident investigation workflow
  - Overview of custom alerting capabilities. Create custom alerts (as time permits)
  - Discuss and demonstrate private and public community threat feeds
- Phase IV – Review and Discuss Advanced Features
  - Configure the collection of custom logs (if applicable), and demonstrate the use of the custom data parser
  - Review the use of built in InsightIDR automation workflows
  - Review network traffic analysis requirements, system requirements for the network sensor, and suggested placement

Requirements

Rapid7 Requirements

The following includes responsibilities of Rapid7:

- Provide consultant(s) with adequate training and certifications to conduct the Services.
- Provide the appropriate hardware and software to perform the Services.
- Work with the Client appointed project manager to schedule the work.
- Complete all deliverables and documents.

Customer Requirements

The following includes the responsibilities of Client to be performed prior to the engagement:

- Designate a Project Manager to work with Rapid7. Where onsite services are necessary, the Project Manager will arrange for access to the business site during normal business hours.
- Ensure all key network, security, or other Client personnel are accessible for interviews or meetings as necessary for services.
- Provide Rapid7 with a list of relevant documentation (i.e., policies, procedures, diagrams, flow charts, etc.) necessary for Services, prior to the commencement of Services.
- Deployment
  - Pre-Engagement checklist (will be provided during Intro call) is complete by start of deployment
  - Client to provide Rapid7 consultant with appropriate access to any on-premise/ infrastructure required for the engagement
  - Client has a dedicated resource(s) available to work with Rapid7 consultant during working hours of deployment
  - Client will have appropriate change control approvals in place prior to the engagement

Terms and Conditions

Services are performed between standard business hours, 9:00 AM to 5:00 PM local time, Monday through Friday, excluding nationally observed holidays, and in contiguous business days once commenced unless otherwise agreed upon in advance. Rapid7 will provide final deliverables no later than ten (10) business days from completion of work. Rapid7 requires written confirmation ten (10) business days prior to scheduled Services for cancellation or postponement of Services. If fewer than the ten (10) business days' notice is given, only the portion of the Services falling after the ten (10) day notice period may be available for rescheduling. Client understands that Rapid7 must allocate resources in advance and that if Client cancels the Services within 10 business days of the Services' scheduled start date, Rapid7 would suffer damages and costs. Accordingly, in the event Client cancels the start date of the Services in each case within ten(10) business days of the Services' scheduled start date, Client shall remain responsible for, as an early termination fee and not as a penalty, the portion of the Services that were canceled without the required ten (10) day notice. Pricing is for all tasks defined by this Service, will be itemized in a Rapid7 quotation, based on the established terms and conditions between client and Rapid7. Service fees are non-refundable and good for a period of twelve (12) months from the effective date of the aforementioned quotation.