Incident Detection & Response Health Check 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. Our Health Check Services for InsightIDR help you verify system health and configuration, and ensure that you continue to 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.

Depending on the size and complexity of your environment, this engagement will take between 1 to 3 days.

Overview

- Verify InsightIDR system health and configuration.
- Engagement deliverable: InsightIDR Health Check Report*.

Primary Goals

- Assess your current configuration and usage of InsightIDR
- Align the capabilities of InsightIDR with your business requirements
- Engagements of one or more days will benefit from an actionable report with alignment against Rapid7 best practices, to get the most of your InsightIDR product investment

The Methodology

- Phase 1 — Architecture
  - Review health check objectives, and any customer pain points
  - Evaluate system resources of Collector(s), Honeypot(s), and Network sensor(s) as applicable

* Engagements of up to one (1) day will provide an actionable list of recommendations in email format, with alignment against Rapid7 best practices

- Phase II — Configuration
  - Review location, sizing and health of collector(s)
  - Review event source configuration and health
  - Review data collection methods for user endpoints and servers
  - Review product configuration settings
- Phase III — Advanced Configuration Options
  - Review deployed deception technology health
  - Review threat, threat community and threat configuration
  - Review configuration of ABA and UBA detection rules
  - Review custom alerts
- Phase IV — Knowledge Transfer
  - Demonstrate log search capabilities using simple, advanced and Visual Mode
  - Demonstrate the configuration of complex regular expression log searches
  - Review dashboards and reports
  - Demonstrate the creation & modification of dashboard cards
  - Demonstrate incident Investigation functionality
  - Overview and walkthrough of InsightIDR user interface
- The Hard Deliverable
  - Action plan for Rapid7's recommended changes

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.