Application Security Deployment Package

Rapid7 Security Consulting & Education

Modern applications no longer consist of static web pages and simple delivery platforms. Abstraction and third party software packages introduce blindspots that could increase the risk of a breach. You need an application security solution as dynamic as your company; one that is quickly deployed and provides rapid time-to-value.

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

BASIC DEPLOYMENT PACKAGE

Days

- Up to two (2) days of deployment services

Overview

- Setup and Product Feature Overview

Primary Goals

- Onboard your security engineers, project managers and software engineers into InsightAppSec with Users and define Roles and Permissions for those users
- Identify applications that are not visible to our Insight Platform, and stand up local scan engines to accommodate intranet applications
- Ensure compliance requirements and maintenance periods are addressed with Schedule Scans and Blackouts
- Test coverage with a crawl scan, design an attack policy, and asses the web application
- Within InsightAppSec, sort and search through prioritized finding data or export reports for specific teams.

The Methodology

- Phase I — Architecture
  - Review objectives and success criteria
  - Evaluate system/server resources and validate prerequisites
    - Includes assistance with determining engine specifications
  - Install scan engine(s)
  - Gather any necessary information, such as web application users, URLs, and APIs
- Phase II — Configuration
  - Pair scan engine
  - Onboard web applications and APIs and associated scan configurations
  - Review scan settings and parameters
    - Modify settings to get the most accurate and fastest scan results
  - Enable authentication into application
  - Configure advanced crawling configurations
- Phase III — Scanning
  - Initiate crawl on customer web application/API to highlight and demonstrate coverage and test scan parameters
  - Tune attack policies and custom parameters by application
  - Using the attack policies, configure DAST scans using the crawl profile
  - Review guidelines for scanning web apps in depth
  - Review best practice guidelines for performing authenticated scans
  - Automate scanning process for enterprise environments to reduce administrative overhead
- Phase IV — Data Review
  - Review scan results and expansion methodologies
  - Show different attacks
    - Discuss application coverage and coverage expansion
    - Discuss plugin tool for Chrome or SeleniumIDE
    - Export results to CSV, PDF
    - Identify, generate, and review reports that will align with business security objectives
- Phase V — Knowledge Transfer
  - Cover detailed troubleshooting recommendations
  - Understand and review data points from scan results and reports and how to prioritize findings in depth
  - Understand API scanning and best practice usage
  - Receive guidance and best practices on how to best leverage tools for your AppSec needs
  - Perform high-level overview of AppSec and areas for potential program improvement
- Phase VI — Integration
  - Discuss, but not implement:
    - Ticketing with Jira & ServiceNow
    - CI/CD pipeline and build gating with scan data
    - Webhooks functionality

The Hard Deliverable

- Daily Status Updates

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 and Rapid7 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, Infrastructure, Cloud, or other Client personnel are accessible to provide guidance, access or the provision of services as necessary for the deployment.
- Provide Rapid7 with a list of relevant documentation necessary for Services, prior to the commencement of Services. This may include policies, procedures, network diagrams, system flow charts, and the like.
- Deployment
  - Items within the Deployment Handbook are complete prior to the start of the deployment
  - Rapid7 will, during remote engagements, provide Client with a Zoom (or similar) meeting link which will be used during the meeting to interact with the customer's InsightVM Console and engines.
  - Client has dedicated resource(s) available to work with Rapid7 consultant during working hours of the deployment
  - Client will have change control approvals in place to allow for the following during the deployment:
    - Security console installation and deployment;
    - Scan engine installation and deployment;
    - Discovery scans; and
    - Vulnerability scans

***All deployment packages can be delivered as an onsite service with the exception of Quick Start. Additional charges for travel and expenses will apply.**

****All mentions of Rapid7 InsightVM associated with deployment services also apply to Rapid7 Nexpose, except where noted. Some features unique to InsightVM are listed above that are not included as part of Nexpose.**

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.