Scope of Service

Managed Application Security Service

Rapid7's Managed Application Security (MAS) Service leverages our application security expertise to deliver the high-fidelity results our customers need to effectively manage and reduce their vulnerable application-based exposures.

This document will outline the scope of Rapid7's MAS offering and how we plan to reach our stated mission, including:

- Technology Overview
- Service Overview
- Rapid7 Responsibilities and Requirements
- Customer Responsibilities and Requirements

Any responsibilities and/or actions not explicitly defined in this Scope of Service are not part of the MAS offering.

Managed AppSec Team

The Managed AppSec (MAS) team provides actionable web application security findings and expertise to our customer base. The team is English-speaking and comprised of AppSec Analysts who work closely together to deliver the service. The MAS team performs tasks such as onboarding customer applications into Rapid7's DAST solution (InsightAppSec), monitoring scans for issues/failures, and validating the vulnerabilities that are produced from the DAST scans. The MAS team works together to deliver findings to customers in a manner that is digestible, driving remediation and program success. During the term of the MAS offering, a named advisor will communicate with the customer's designated point of contact to provide updates on service delivery and ensure Rapid7 is addressing the customer's security goals. For purposes of clarity, Customers with a total spend of less than $40,000 will not be provided access to a named advisor, but will have direct access to the Managed AppSec analyst team for support and service delivery.

Technology Overview

The Rapid7 insight platform is utilized for all log management, data processing, enrichment, and storage of customer data. Each customer instance on the insight

platform is isolated from other instances.

The MAS offering leverages Rapid7's InsightAppSec solution for Dynamic Application Security Testing (DAST) of web applications and APIs. This includes authenticated scans, coverage of complex applications via traffic files and macros, support for APIs using specification documents, and other features.

Scans will be configured monthly for the number of applications under management by Rapid7. If intrusion detection/prevention systems (IPS/IDS), web application firewalls (WAF), or any other security solution that might hinder Rapid7's ability to scan the contracted applications are in use, it is recommended that the customer make exceptions to accept the originating IP address of the scanning tool/engine to ensure scans are comprehensive and accurate. If this is not possible, then the scan should originate from a network location that prevents IDS/IPS/WAF interference. Verification of the existence of or level of controls in place for IDS/IPS/WAF applications is outside the scope of the MAS offering.

Externally-accessible applications will be scanned using the Rapid7 InsightAppSec cloud engines. The MAS team supports the scanning of internal applications with an InsightAppSec scan engine deployed on premises and network access to the in-scope applications granted to the MAS team via Rapid7's Pro Tunnel Kit (PTK). The MAS team will not use customer-provided hardware, complete training, or perform any additional requirements such as background checks, fingerprinting, drug testing, etc. that may be requested by the customer for the provision of internal network access.

The MAS team requires the customer to disable Multi-factor Authentication (MFA) and recaptcha for the testing account that Rapid7 will use to scan. If MFA cannot be disabled, the customer must provide a static token/value as the second factor so that the scans can still be automated.

Service Overview

Rapid7 will provide knowledgeable security experts to perform application security testing using InsightAppSec. The MAS team will validate test results, deliver reports to the customer, and provide remediation recommendations based on industry best practices.

The Rapid7 MAS offering includes:

- Onboarding of contracted applications into the InsightAppSec tool.
- Scan configuration, scheduling, and routine tuning of contracted applications.

- Monthly DAST scans of contracted applications[1].
- Vulnerability validation by Rapid7's MAS team to remove false positive findings and suppress duplicate findings, leaving only actionable findings.
- Monthly vulnerability report of verified findings.
- Remediation prioritization and guidance.
- Meetings with AppSec analyst on request
- Customer "read-only" access to the InsightAppSec service management console, allowing visibility to service activity and reporting[2].

Managed AppSec Deployment

Kickoff Call: Rapid7 will schedule a kickoff call to introduce the Rapid7 team to the customer's authorized contacts. An overview of the MAS process and review of in-scope applications will be conducted to ensure overall alignment. Communication channels will be discussed and a primary and a secondary point of contact will be designated by the customer to work with Rapid7.

Scan Engine Deployment: If internal applications are under contract for management, the Managed AppSec Team will work with the primary and/or secondary customer points of contact to coordinate deployment of internal scan engines on the customer premise. This includes the customer granting Rapid7 access to the customer's network to facilitate this action and Rapid7 shall not have any liability in relation therewith.

Application Onboarding: The customer must provide the Managed AppSec Team with details on in-scope applications including (but not limited to) URL(s), testing credentials, properly formatted API documentation, and any other relevant information. The initial testing cannot begin until these details have been provided.

Activating your Managed AppSec Service

Rapid7 can begin the Managed AppSec service as soon as the Kickoff Call and Application Onboarding steps mentioned above are completed.

Managed AppSec Process

Scan configuration: After onboarding in-scope applications, the Managed AppSec Team will make best effort attempts to configure scans to achieve optimal coverage. This can include recording authentication macros, generating traffic files, attaching

[1] Each contracted application will be scanned in a single environment. The MAS team will support configuration of unique user roles required to gain full coverage of the application as mutually agreed upon by the customer and the MAS team.
[2] The severity and status of findings should only be modified in the InsightAppSec console by the MAS team to maintain data integrity.

API documentation, and other configuration changes as deemed necessary by the Managed AppSec Team. Scans can be configured in such a way as to minimize any interruption to the normal operation of the customer environment.

Initial scanning: Once scan configuration is complete, the Managed AppSec Team will run a crawl-only scan to evaluate application coverage. The customer will be given the opportunity to confirm the scope and coverage of the application. Additional changes to the configuration will be made as needed by the Managed AppSec Team prior to running an attack scan. The attack scan will be run using the Managed AppSec Team's custom attack template.

Vulnerability validation: After scans have been completed, the Managed AppSec Team will attempt to validate any "High," "Medium," or "Low" severity findings (as defined by Rapid7 in the default attack policy). This will be accomplished by analyzing the scan data using various tools to eliminate findings that are false positives or contextually have no impact to the business. The customer can open a support inquiry with any questions around validated findings.

Steady state: Once apps are fully onboarded and initial scanning/validation is complete, cadence scans will be scheduled by the Managed AppSec Team. The MAS Team will use best efforts to accommodate requests from the customer regarding preferred scanning windows. Vulnerability validation of newly discovered findings will occur within five business days after the completion of scans. The customer can reach out to the MAS Team via the Rapid7 support portal to ask questions or request ad hoc calls, if needed. Reports will be generated every month and delivered via the Rapid7 services portal. Report format, content, and layout are subject to change as the InsightAppsec technology and/or the MAS offering evolve. Changes will be implemented at the discretion of the Managed AppSec Team.

Rapid7 Responsibilities & Requirements

- Provide a named advisor[3] as the point-of-contact for the duration of the MAS subscription term to ensure program success.
- Assist with initial service deployment and implementation.
- Work with the customer-designated point of contact to schedule scans and other jointly coordinated service deliverables.
- Complete and provide all in-scope service deliverables referenced herein.
- Delivery of all reports via the Rapid7 services portal in accordance with this Scope of Service.

[3] Customers with a total spend of less than $40,000 will not be provided access to a named advisor, but will have direct access to the Managed AppSec analyst team for support and service delivery

- Notify you of service delivery changes in relation with the MAS offering.

Customer Responsibilities & Requirements

- Designate a Project Manager/point of contact to work with Rapid7.
- Ensure all key network, security, or other customer personnel are accessible for interviews or meetings as necessary for the provision of the MAS offering.
- Provide Rapid7 with a list of in-scope application information and relevant documentation (i.e., application workflows, architecture diagrams, API documentation, etc.) necessary for the provision of the MAS offering.
- Install virtual machines and/or software in the customer environment as requested by Rapid7 to enable delivery of the MAS offering.
- Authorize platform admin access to the InsightAppSec console for all required MAS team members
- Provide Rapid7 with necessary access to the customer systems and applications in scope. This includes allowing scans to run without interference from web application firewalls or filters designed to block specific scanning activity.
- Customer is responsible for providing testing credentials with a suitable access level and ensuring they remain valid and the access level does not change. The customer must complete any initial setup required for the testing account. The email address mas_testing@rapid7.com should be utilized, if possible. Provisioning individual user accounts for testing purposes is not recommended.
- Access the InsightAppSec service management console in a “read only” manner unless explicitly reviewed and approved by the Rapid7 Managed AppSec Team.

Additional Terms

This Scope of Service is governed by Rapid7’s standard Master Services Agreement, and any other terms and conditions, as applicable, available at https://www.rapid7.com/legal/terms/ unless the parties have a fully executed Master Services Agreement which supersedes such standard terms. Any responsibilities and/or actions not explicitly defined in this Scope of Service are not considered part of the Rapid7 Managed Application Security service. Rapid7 may modify this Scope of Service at any time by posting a revised version on our managed services doc pages which modifications will become effective as of the first day of the calendar month following the month in which they were first posted.