RSA Professional Services

Model Number:
PS-BAS-CON-ACDUCD
Effort Estimate: Up to 10 days
Travel Included: 1 Trip

RSA® ADVANCED CYBER DEFENSE USE CASE DEVELOPMENT FOR RSA NETWITNESS®

Project Overview

This RSA[1] Service Brief outlines the RSA *Advanced Cyber Defense Use Case Development for RSA NetWitness* service. This service provides customers with strategic consulting services to identify and develop use cases for implementation in the RSA NetWitness suite of products. This service is delivered by RSA's Advanced Cyber Defense (ACD) team of practitioners which specializes in the development of solutions for advanced threat detection and response.

Project Scope

An RSA Advanced Cyber Defense consultant, or authorized agent, will work closely with Customer staff to perform the various tasks within the time available, which may include the following:

- Perform the Services as indicated in this Service Brief and subject to the Effort Estimate.
- Manage the overall engagement and conduct pre-engagement teleconference to plan and schedule the engagement's tasks and ensure that the environmental and operational requirements (for example, preparation of documentation and meeting rooms) are met by the Customer.
- Gather requirements for use case development, which may require:
  - Conduct of workshops for information gathering
  - Observation and review of existing operational state
  - Documentation review, which may relate to organization structure, workflows, policies, procedures, guidelines and standards
  - Systems architecture and technology review, including logs, packets and endpoints
- Review requirements for monitoring use cases in association with RSA's Use Case Framework, which may include:
  - Definition of use case objectives (e.g. a goal to monitor and alert on C2 malicious hosts)
  - Identification of threat elements (e.g. a compromised host succumbing to attacker takeover)
  - Identification of stakeholders (e.g. Level 1 SOC Analyst, Level 2 SOC Analyst and SOC Manager)
  - Identification of data requirements (e.g. detection sources such as logs and packets)
  - Definition of logic requirements (e.g. the rules or filters which need to be configured to detect the threat)
  - Testing requirements (e.g. to validate the logic)
  - Priority definition (e.g. to categorize the threat level based on impact and urgency)
  - Response Procedure Development (e.g. the procedure to be followed when the threat is detected in order to manage the incident lifecycle)
- Develop up to ten (10) use cases based on the use case requirements

[1] For all purposes hereunder, "RSA" means the RSA or Dell EMC entity that has executed this Service Brief.

- Conduct knowledge transfer

  Notes: "*Knowledge Transfer*" relates to the RSA Advanced Cyber Defense Use Case Development for RSA NetWitness service as implemented in the Customer's environment, and is not a substitute for formal RSA Education Services product course offerings. RSA strongly encourages attendance at these courses to gain further insight into the product features, installation, configuration and administration.

  Travel & Expense for one (1) trip is included and should be reviewed with the ACD team prior to booking of the engagement to determine whether additional T&E may be required.

  Configuration and implementation of the use case in RSA NetWitness is out of scope and available as a separate service from RSA NetWitness Professional Services. Please contact your RSA representative for further information.

Deliverables

The following deliverables are provided in connection with this Service:

- *Engagement Summary*, identifying the engagement deliverable as mutually agreed with RSA in the "Project Scope" section above.

RSA Staffing

- RSA provides appropriate personnel to perform the Services specified in the "Project Scope" section, subject to the Effort Estimate. RSA also provides project management and oversight by an ACD Practice Manager, which is provided in addition to the Effort Estimate.

Customer Responsibilities

- Provide at least one (1) contact with incident response responsibilities and appropriate system/information access privileges.
- Reviewing and agreeing on engagement objectives.
- Ensure that all environment and operational requirements are met prior to commencement of the Services.
- Provide access to the Customer's systems and networks as necessary to perform the Services during RSA's normal business hours, or at mutually-agreed times.
- Provide support from technical support teams for all vendors and third parties as necessary.
- Assume all responsibility for network connectivity, performance, and configuration issues.

Service Schedule

- The Services described in this *Service Brief* are delivered during RSA's normal business hours (M–F, excluding RSA/local holidays).
- Unless otherwise specified or agreed by RSA, the Services are performed on consecutive days.
- The anticipated Service start date is within thirty (30) days, or a mutually agreed upon start date, after receipt and approval by RSA of the Customer's purchase order for this Service.
- Subject to Customer satisfying the "Customer Responsibilities" specified above, RSA estimates that it will complete the Services within a corresponding number of consecutive days (during RSA's normal business hours) for the noted level of effort, subject to any intervening time allowed to facilitate reasonable and timely Customer review of any draft deliverables.
- Once the Deliverables have been met, RSA Project Manager will notify by e-mail the proof-of-delivery (POD) and the project will be considered complete. Implementation support beyond the Deliverables will be subject to additional fees.

Project Scope Exclusions/Changes

Any additions or changes to the Project Scope must be mutually agreed upon by RSA and the Customer in a separate RSA *Statement of Work* detailing the proposed changes, the impact of the proposed change on pricing and schedule, and other relevant terms. Such changes include, but are not limited to:

- Any additional activities not listed in this *Service Brief.*
- Prolonged service duration.
- Any actions associated with remediation of any identified compromise.
- Product deployment or configuration.
- Modification of application software.
- Configuration and implementation of use case logic.
- Host forensics and analysis.

Fixed Bid Service Fee and Invoicing Schedule

- Invoices are issued upon RSA's receipt and approval of the Customer's purchase order. Customers shall have twelve (12) months from the date of each RSA invoice to use the Services described herein ("Service Period"). If customer fails to use this service within the Service Period, the services shall expire. Under no circumstances shall Customer be entitled to a credit or refund of any unused portion of this invoice.
- For purchases of multiple service units which includes services for delivery consecutive to the initial 12-month Service Period, invoices shall be issued yearly, and the Service Period shall expire with each unique expiration occurring at the 12-month mark from each of the yearly invoices. The customer intention to utilize multiple quantities of services concurrently or consecutively must be clearly annotated on the quote to the customer.
- Customer will provide a new or amended purchase order and shall pay additional amounts related to (i) performance of services outside RSA's normal business hours or consecutive days, and (ii) reimbursement of any travel-related expenses beyond the one (1) trip included in the service.

This Service Brief is subject to RSA's standard terms and conditions (https://www.rsa.com/content/dam/rsa/PDF/professional-services-terms-and-conditions.pdf) for professional services in effect as of the date of approval by RSA of the Customer's purchase order for this engagement. Notwithstanding any rights in standard terms or negotiated agreement, no Termination for Convenience will apply to this offering.