NETWITNESS

Model Number:

PS-BAS-NW-RETP

Effort Estimate: Up to 242 hours

Delivered remotely

NETWITNESS® RETAINER FOR INCIDENT RESPONSE – PLATINUM

Project Overview

This NetWitness Service Brief details the NetWitness *Retainer for Incident Response – Platinum* service offering. This service provides customers with a proactive incident discovery review of traffic entering, leaving and within the network, and on host systems and a process for engaging NetWitness on retainer, facilitating rapid access to incident response resources and expertise, should an incident occur.

The service is delivered by NetWitness' team of experts in incident forensics and data analysis. Through a combination of NetWitness® NetWork, Endpoint and open-source analysis and research, NetWitness conducts incident discovery to identify potential anomalies in the IT systems environment.

All services, contracts, and activities in connection with this Service Brief shall be conducted in English.

Project Scope

A NetWitness Professional Services consultant, or authorized agent, will work closely with Customer staff to perform the various NetWitness Retainer for Incident Response – Platinum tasks, which may include some or all of the following:

- Perform the services within the Customer's environment as defined in this Service Brief.
- Conduct the engagement within prescribed terms of the "Fixed Bid Service Fee and Invoicing Schedule" (below).
- Proactively define engagement process in anticipation of incident scenario ("*Initial Review*"):
  - Identify the locations relating to any Initial Response services which may be provided.
  - Review organizational mission, asset criticality and the nature of potentially targeted data.
  - Identify points of contact, roles and responsibilities and related contact information.
  - Review the incident handling and escalation process and breach disclosure requirements.
  - Identify Customer technologies which may assist in any potential incident response activities.
  - Review geographic footprint and locations for any potential follow-on incident response activities.
  - Review engagement "Welcome Pack," consisting of the instructions and guidelines for engaging NetWitness' Incident Response team in the event of an incident.
  - Review customer provided Incident Response Plan if applicable, to align potential use of NetWitness' Incident Response team with customer processes, procedures, and workflows for incident response.
- Subject to being contacted by Customer in an actual incident scenario ("*Initial Response*"):
  - Develop and share NetWitness Endpoint agent and begin endpoint analysis for mutually agreed upon number of endpoint systems
  - Conduct initial triage:
    - Review current situation, participant roles and responsibilities (including finance, legal, law enforcement, etc.), activities and data gathered to date, the nature of targeted data and its criticality.
    - Identify additional data gathering requirements (e.g., log files, network packet capture, host forensic images, memory dumps and malware)
  - Conduct preliminary analysis:
  - Draft and review *Preliminary Analysis Report* outlining general findings and suggested next steps.

        - Review data gathered to date, which may include using a combination of open-source intelligence gathering and research, host-based forensic analysis, network-based forensic analysis and malware analysis.
    - Provide direction and guidance for additional activities, including the deployment of enterprise-class NetWitness tools and technologies as appropriate, for incident response and remediation activities to be fulfilled in a separate Statement of Work.
    - Draft and review *Preliminary Retainer Analysis Report* outlining general findings and suggested next steps.
- In conjunction with the *Incident Discovery*:
    - Fulfill the initial installation and deployment of a NetWitness NetWork appliance-based solution at a single location to enable network security monitoring and/or network forensics for the purposes of this engagement.
    - Activate a NetWitness Endpoint client-server solution on one customer provided server and a mutually agreed upon number of endpoint systems.
    - Analyze network and host data for indications of attacker activity, active malware, beaconing activity, lateral movement to other systems, “Command and Control” efforts and information exposure or exfiltration.
    - Conduct analysis on any identified malware and attempt to determine its capabilities and functionality and derive indicators of compromise (IOCs) to further the investigation.
    - Create forensic images according to industry standards and best practices of either live or dead media as appropriate.
    - If requested by the customer, provide samples of any malware discovered and reconstructed.
    - If requested by the customer, remove all collected data from the NetWitness NetWork appliances and NetWitness Endpoint systems using industry-standard software wipe processes. If the Customer requires physical data destruction, NetWitness will provide a quote for Customer to purchase all non-volatile storage devices within the deployed NetWitness appliances.
    - Subject to the limitation of the Estimate of Effort, and in conjunction with any related investigative workstreams, provide guidance and direction relating to strategies for incident remediation and recovery. Assistance may include security control recommendations, implementation of recommendations associated with the NetWitness toolset, project management support, and interaction with executive leadership/legal counsel to provide clarity with respect to the nature of the threat environment, associated challenges, and recommended best practices for long term success.
    - Provide updates on the status of the incident response along with an *Incident Discovery Findings Report* summarizing relevant findings and details of the incident.

** Travel is not included. Please work with your NetWitness representative regarding any requirements for on-site consulting*

Deliverables

The following deliverables are provided in connection with this Service:

- *Preliminary Analysis Report*, if applicable
- In connection with Incident Discovery, provide *Incident Discovery Findings Report*.

NetWitness Staffing

- NetWitness provides appropriate personnel to perform the Services specified in the "Project Scope" section. Some or all services may be delivered remotely.

Customer Responsibilities

- Provide at least one (1) technical contact with system administration 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 NetWitness' 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.
- Verify that the equipment location (work site) is prepared to perform the engagement services.
- Respond in a timely fashion to questions posed by NetWitness regarding the project.
- Complete all planning and scheduling activities required by customer.

Service Schedule

- The Services described in this *Service Brief* are delivered during NetWitness' normal business hours (M–F, excluding NetWitness/local holidays).
- Unless otherwise specified or agreed by NetWitness, 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 NetWitness of the Customer's purchase order for this Service.

After having completed the Initial Review:

- The service level for initial triage is within three (3) hours of being contacted by Customer in an actual incident scenario.
- The service level for remote preliminary analysis is within twelve (12) hours of being contacted by Customer in an actual incident scenario.
- The service level for any on-site preliminary analysis is to be en route within twenty-four (24) hours of being contacted by Customer in an actual incident scenario, subject to any visa or travel requirements which may be outside of NetWitness' control.

Project Scope Exclusions/Changes

Any additions or changes to the Project Scope must be mutually agreed upon by NetWitness and the Customer in a separate NetWitness *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.*
- Development of incident response processes and procedures.
- Incident remediation activities.
- Modification of any Customer hardware or software.
- Multiple, basic engagement services requiring Project Management services.

Fixed Bid Service Fee and Invoicing Schedule

- Customer shall have twelve (12) months from the date NetWitness books the Services described herein ("Service Period"). This Service shall automatically expire on the last day of the Service Period. Under no circumstances shall Customer be entitled to a credit or refund of any unused portion of this Service if Customer fails to use this Service within the Service Period.
- Invoices are issued upon NetWitness' receipt and approval of the Customer's purchase order.
  - For multi-unit purchases (multiple years of retainer service) invoices shall be issued yearly, at the beginning of each year's Service Period. Effort hours must be consumed within each associated Service Period. Each unit will expire 12 months after initiation. The customer's 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 NetWitness' normal business hours or consecutive days, and (ii) reimbursement of any travel-related expenses.

This Service Brief is subject to NetWitness' Terms and Conditions for professional services in effect as of the date of approval by NetWitness of the Customer's purchase order for this engagement. If necessary, in order to furnish the Services, NetWitness agrees to lend the Customer certain NetWitness products, which shall be governed by the NetWitness standard Evaluation Terms in effect as of the Effective Date. Notwithstanding any rights in standard terms or negotiated agreement, no Termination for Convenience will apply to this offering.