Digital Forensics Incident Response – Breach Attack Simulation (BAS)

1 Overview of the Service

Breach Attack Simulation (BAS) is one of the ways to evaluate a Client's security, demonstrate possible methods of attacks, identify existing security problems, and validate the effectiveness of Cyber Security Controls across People, Processes and Technology.

1.1 Technologies for the BAS Service

(a) The tools stated within this list may be used with NTT's sole discretion at no additional cost to the Client, the Client agrees to abide by any required End User License Agreement:

(i) Cymulate – SaaS-based Extended Security Posture Management PlatformNTT may exchange this software and require the Client to execute a new End User License Agreement in its sole discretion.

2 Client Responsibilities

(a) **Point of contact:** The Client will appoint a primary point of contact for NTT personnel to liaise with throughout the engagement to gather specific information (e.g. existing incident response plans and other IR-related material), schedule and attend workshops, and support the successful completion of IR Plan Design. The primary form of communication will be written (Email).

(b) **Control Domain Agreement:** The Client will agree to the control domain(s) that will be tested prior to the engagement kick-off. The specific attack type(s) that reside within the control domain are to be agreed upon and documented in the statement of work. The control domains that may be tested are as follows:

(i) Immediate Threats Intelligence

(ii) Email Gateway

(iii) Phishing

(iv) Web Gateway

(v) Web Application Firewall (up to 5 domains included)

(vi) End Point

(vii) Lateral Movement

(viii) Data Exfiltration

(ix) Full APT Kill-Chain

(c) **Cymulate Agent Deployment Agreement** (Non-NTT Hosted Clients): Agree and deploy the Cymulate agent. NTT will provide guidance and the pre-requisites for the agent to be installed and configured. The deployment of the agent is only applicable to the following control domains:

(i) Web Gateway

(ii) Web Application Firewall

(iii) Email Gateway

(iv) Endpoint Security

(v) Lateral Movement

(d) **Removal of Cymulate Agent** (Non-NTT Hosted Clients)**:** The Client will remove the Cymulate agent as per the guidance provided by NTT if applicable.

(e) **Control Domain-Specific Requirements:**

(i) **Email Gateway Only Requirements:** Create a dedicated mailbox with MFA disabled. Exclude IP address from anti-spam / anti-phishing protection and add a given email address as a permitted sender (details to be provided by NTT).

(ii) **Web Application Firewall Only Requirements:** Exclude IP address from anti-bot / anti-DdoS protection (details to be provided by NTT).

(iii) **Phishing:** Exclude IP address from anti-spam / anti-phishing protection (details to be provided by NTT).

(f) **Control Verification:** Verify that for all equipment, servers or other items delivered to NTT, Clint has appropriate access and proper rights to perform the In Scope items.

3 Service Specific Operations

The following Control Domain must be selected as In Scope in the SOW, otherwise it is out of scope.

Control Domain	Description
Control Domain Agreement	The agreement and selection of a specific control group(s) as listed below.

Immediate Threats Intelligence	• The threat assessment operates in several vectors depending on the specific threat being tested and uses the exact Indicators of Compromise (IOCs) and TTPs of that threat. • These new attacks, orchestrated by known and unknown hostile entities, come in different forms such as email attachments or downloadable links appearing on legitimate or compromised websites. • Assessments are divided into four vectors: ○ Email Gateway - Send malicious files containing the selected threat to the dedicated target mailbox. Each file will be sent within different file formats to challenge the filtering and detection controls. ○ Web Gateway - Trying to access IP addresses and URLs associated with the malicious activity and downloading malicious payload samples through HTTPS. ○ Endpoint Security – Deploying real malware samples onto the disk to validate detection and deletion by Endpoint Security. ○ Network Traffic - Simulating the network traffic issued by the immediate threat (only relevant for user-created threat simulations).
Email Gateway	• Cymulate attack servers send out payloads to a dedicated target email address, which will then perform the assessment in a controlled manner without actually running the payloads. • The payloads are not able to spread internally within the organisation. • Furthermore, each email sent by Cymulate is automatically deleted, so none of the payloads will remain on the email servers.
Phishing Awareness	• Phishing emails are sent from Cymulate's cloud to a list of emails chosen by the Client; • None of the emails contain real malicious content (ransomware, URLs, worms, etc.); • Events are tracked and tracked by Cymulate throughout the campaign; and • The NTT consultant has full control of email templates, attachments, and login pages, and can create their own templates aligned with the Client expectations.
Web Gateway	• Test using one dedicated machine which does not affect users or servers in the organisation's network (pre-requisite setup). • All stages of the test are done automatically, including website access, file downloads, and clean-up on completion • The tests are updated daily with malicious URLs for continuous validation of the web security controls • Both inbound and outbound traffic are tested. Outbound tests include accessing suspicious and malicious sites that are involved with activities such as phishing, ransomware, etc. Inbound tests include downloading malicious files and exploits • All tests are done in a secure and controlled manner, and mitigation recommendations are offered for each gap that was found, depending on the tested component and risk level
Web Application Firewall	• Cymulate's library of web attack types is utilised to test the Client's WAF security efficacy against an array of payloads mapped to OWASP TOP 10; • All stages of the test are automatic, including the initial crawling of the target websites and the response comparison; and • The testing does not affect the websites since no exploitation is performed.
Endpoint Security	• Test using one dedicated machine which does not affect users or servers in the organisation's network (pre-requisite setup) • Leverage Cymulate's library of commands mapped to the MITRE ATT&CK Framework • Allows organisations to deploy and run real ransomware, Trojans, worms, and viruses on a dedicated endpoint in a controlled and safe environment • Execute simulated attack from a collection of pre-compiled behavior-based malware simulations, executed using different methods:

	○ Behavior-based-collection of pre-compiled behavior-based simulations ○ Signature-based-Daily list of identified malware samples dropped on disk, without execution
Lateral Movement	• Progresses with only minimal CPU usage with zero user interaction; • No destructive actions such as exploitation, deletion, encryption, DDOS, etc.; • Abuses OS apps for privilege escalation capabilities; and • Uses a single agent to perform a full lateral movement assessment within a network.
Data Exfiltration	• A broad library of synthetic regulatory and company confidential data types in addition to custom data sets are available for Data Loss Prevention (DLP) testing; • Assessments use multiple exfiltration methods and file types. • Uses a single agent to test the Client's organization's security controls; and • Testing is non-disruptive and can be performed on the production network.
Full Kill-Chain APT	• Full Kill-Chain APT utilizes an array of different vectors that are launched sequentially, starting from a simulated attack delivered through email or web browsing, followed by the execution of code and evasion techniques that test endpoint security mechanisms. • Depending on the template chosen, the module may then challenge network configuration and policies by attempting to move laterally. • It then attempts to exfiltrate predefined sets of data, for example, mock PII, health records, card details, etc., to test DLP controls.

3.1 DFIR Retainer Hours

(a) *This section is out of scope for Clients acquiring this service as a standalone offering.*

(b) NTT enables Clients that have selected Gold and Platinum DFIR retainer packages to utilise unused retainer hours towards the deployment of this service. These Clients can utilise this service anytime within their contracted term (up to the last 60 days) and are strongly encouraged to do so.

(c) Gold Clients can use **no more than 50%** of their unused retainer hours towards additional IR-related services. The balance of unused hours must meet or exceed the minimum hourly requirement per control domain as stated below.

(d) Platinum Clients **can use 100%** of their unused retainer hours towards this service. The balance of unused hours must meet or exceed the minimum hourly requirement per control domain as stated below.

3.2 Hourly Requirements Per Assessment

(a) Immediate Threats Intelligence: 30 Hours

(b) Email Gateway: 30 Hours

(c) Phishing: 30 Hours

(d) Web Gateway: 30 Hours

(e) Web Application Firewall: 30 Hours

(f) End Point: 30 Hours

(g) Lateral Movement: 30 Hours

(h) Data Exfiltration: 30 Hours

(i) Full APT Kill-Chain: 60 Hours

4 NTT DFIR Deliverables

The main deliverables for this service include:

Deliverable Summary	Deliverable
Executive Report	A single executive report that details a high-level overview of the assessment(s), documenting findings and recommendations.
Technical Report	A technical report that provides detailed insights into the assessment(s), e.g. the attack payloads used, descriptions, and specific mitigation details. A .csv file can be provided with all outcomes provided in the technical report for ease of reference.

5 Billing

Standalone: Charges shall be based on a fixed fee based on the control group(s) selected for the work to be carried out.

(a) Any work beyond the specified In Scope hour maximum listed in the SOW, shall be out of scope and subject to additional charges at NTT's current list rate.

6 Limitations

(a) The BAS service will be carried out via remote means only and no onsite delivery will occur.

(b) Upon engagement kick-off, all activity must occur before the end of the following calendar month. Any work that is required beyond this period will be charged as appropriate.

(c) A maximum of two assessments will be carried out per attack vector during the engagement, any additional assessments will be charged as appropriate.

(d) Operating System dependence: An assessment is specific to a given operating system and version. Assessments required across multiple operating systems or versions may incur additional charges.

(e) The scope of work will be determined by the control domain selected which can be assessed concurrently should more than one assessment be selected. As for the Lateral Movement, Data Exfiltration and a Full APT Kill-Chain assessments, these will be triggered on their own to ensure the correct attack surfaces are measured.

7 Service Transition

Pre-service activation remote workshop:	
Kick-off to introduce the service and confirm details	X1 two-hour remote workshop (Video Teleconference (VTC), e.g., Microsoft Teams)). Provide an overview of the service, including the features that are available, timelines, points of contact etc.
Control Domain Identification	Identify the control domain(s) that are in scope and discuss the pre-requisites dependencies and expectations.

8 Service Transition Out of Scope

Any actions not specified within the service transition scope.

9 Out of Scope

(a) Any activity not specified as in scope.

(b) Any breach attack simulation work occurring 3 months after the engagement kick-off.

(c) More than two assessments without explicit mention in the statement of work

(d) Any remediation activities to detect or respond to identified gaps within the Client's security infrastructure.

(e) The creation or amendments to a Client's incident response plan.

10 Service Specific Terms and Conditions

The following terms and conditions apply to this Service Description and any dependent thereon, and specifically supersede any conflicting terms and conditions in any other agreement between the parties.

- Client warrants that it has obtained all consents necessary for the data to be collected and used on its behalf for compromise assessment and that it has a legal basis for requesting such information (excluding consents from NTT employees and agents) and shall indemnify, defend and hold harmless NTT for the use of this information for this Service.
- Client expressly agrees to enable the deployment of NTT DFIR tooling within the clients environment if required
- All data related to the investigation will be deleted 90 days after the conclusion of the investigation, unless expressly requested otherwise. All costs associated with storing data beyond this time will be billed to the client.
- NTT shall own all rights, title and interest to any Work Product, Intellectual Property, code or otherwise, developed as part of this Service. In the event Client provides any ideas, suggestions, improvement, Work Product, Intellectual Property, code or otherwise as a suggestion, improvement or otherwise required to enable this Service, Client hereby assigns all rights, title and interest to NTT. Client expressly agrees to the use of Third Party and Open Sources components and services in this Service and agrees to abide by all required terms and conditions of any third-party product.
- No Control Rule compliance will be included in this Service. This Service Description and Service may be cancelled at any time, in NTT sole and absolute discretion. NTT reserves the right to replace, change, alter, or not provide any third-party software required to perform the Services and any Service that depends on those items may be terminated by NTT.
- An investigation will be conducted, which may include deployment of analytical tools or transfer of forensic images to regional forensic processing servers (in line with local data processing regulations/compliance requirements).
- NTT will use a blend of on-shore and off-shore resources to securely deliver the service unless directly requested or legally complied not to. Any additional costs associated with 100% on-shore or a change in the delivery will be charged to the client accordingly
- Client shall indemnify, defend and hold harmless NTT from any and all claims for directing NTT to perform a service herein that the Client does not have permission or legal rights to have it performed on.