Service Definition Document for G-Cloud 13 Services

Security Services

NTT DATA UK LTD
2 Royal Exchange, London EC3V 3DG
Tel.: +44 (0) 20 7220 9200
www.nttdata.com/uk

Table of Contents

Confidential

1 Service Definition for Security Services

1.1 Introduction

This is the Service Definition Document for NTT DATA UK Ltd (NTT DATA) security services on the G-Cloud Framework. The information provided in this document is required by the G-Cloud framework and is designed to help clients determine how these services can meet their requirements.

1.2 Overview of services

The following services work with our cloud solutions to ensure that clients have appropriate security measures and procedures in place:

- Managed Security Service - following the deployment of cloud solutions, clients need to detect, mitigate and report on ever-changing security threats; simplify your information risk management and compliance efforts; benefit from security and risk management common procedures, integrated change management, and advanced reporting through the customer portal including real-time service level agreement conformance, alert summaries, graphical trend reports, and real-time availability statistics; gain immediate access to security expertise as needed; reduce your capital and operating expenses with our hosted solutions based on our state-of-the-art global managed security services platform and services.
- Security Consulting – NTT Security consulting services are divided into Strategic and Technical categories. Specific engagement activities are delivered as stand-alone services or as part of comprehensive programs and long-term strategies are integrated with our managed security services. These services will help our clients in planning and migration to cloud based services and hosting.
- Technical Security Service – our highly-experienced group of security specialists offers the flexibility of resource and breadth of expertise to ensure physical, virtual and cloud based security technology and technical security controls are effectively integrated, deployed and managed for cloud solutions. Our technical expertise can be leveraged to support the cloud journey and cloud migration as our clients transform their businesses.

Please see Section 2 for full service descriptions

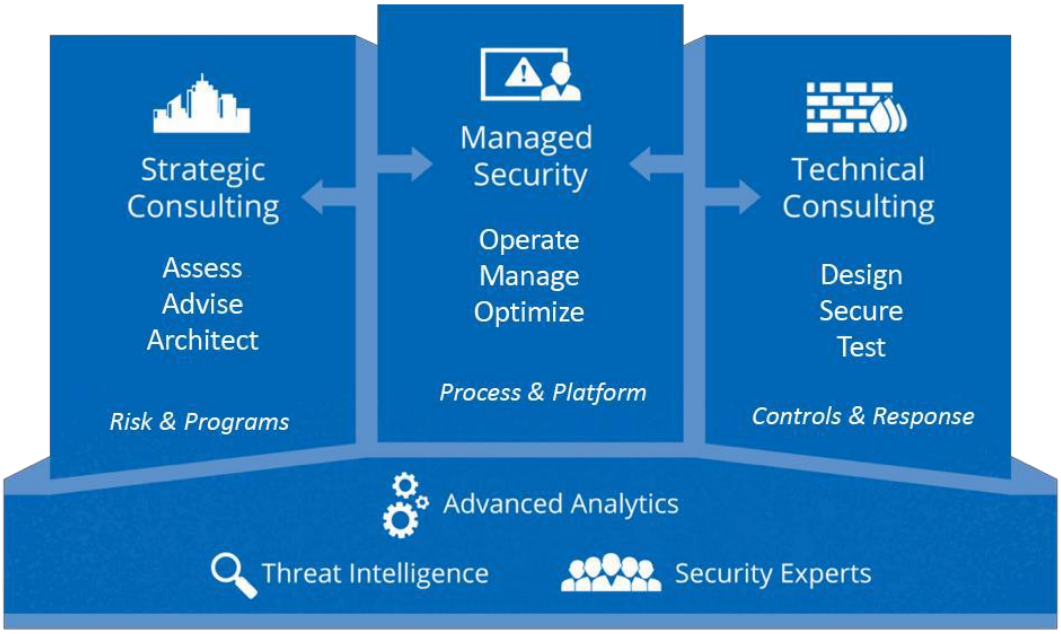
2 Service Descriptions

NTT Security services empower the global digital economy. Whether it is enabling a client's digital business transformation, or the continuing maturation of risk, security, and compliance programs, NTT Security provides the right combination of managed security, strategic consulting and technical consulting.

Through traditional on premise, cloud-based, or hybrid services, and via integration with the broad NTT Group company service portfolio, NTT Security protects infrastructure, platforms, applications, information, and users from today's advanced threats.

NTT Security services are delivered via three pillars: Managed Security, Strategic Consulting, and Technical Consulting.

Each pillar is supported by substantial R&D and operational investments in a purpose-built MSS platform that combines the power of **Advanced Analytics** (machine learning, big data, and complex event processing analysis), the breadth of **Threat Intelligence**, and certified, experienced **Security Experts** to provide the strongest possible protection.



Managed Security leverages investment in threat intelligence, advanced analytics, and security expertise to provide consistent, repeatable, and transparent services that identify and stop advanced threats, while providing insight and metrics into security posture and trends.

Trained and certified engineers carry out efficient, best practice, and compliant change management processes for networking and security devices and controls.

Experienced SOC threat and incident analysts use the NTT Security purpose-built, proprietary Global Managed Security Service Platform to collect, analyze, identify, and respond to Security Incidents.

Using extensive threat intelligence, analysts optimize the allocation of scarce resources by focusing on threats and vulnerabilities actively being exploited.

Operate – Execute accurate, timely, transparent, and documented operational processes in response to change or based on a recurring schedule.
Manage – Prevent, detect, and respond to new global techniques, tactics, and procedures, advanced targeted threats, and emerging vulnerabilities.

Optimize – Use global operations intelligence, client engagement, and security expertise to continually improve security processes, platform, and controls.

Strategic Consulting employs experienced, senior experts to define and communicate risk and security program strategy using real-world data, proven frameworks, and an understanding of industry and business.

CSO-level consultants understand the complexity of building a security program that allows business to achieve objectives while meeting risk tolerance.

NTT Security consultants work to define security defense architecture and make the necessary transformations in adapting to the digitalization of business.

Assess - Identify organizational risks, gaps in controls, and develop prioritized strategy.

Advise – CSOs advising CSOs: set strategy, shape culture, and communicate with executives and board.

Architect – Define a holistic security defense architecture and the supporting controls matched to the level of risk, risk-tolerance, and resources available.

Technical Consulting delivers technical expertise and security controls tailored to client infrastructure, information technology usage, and protected information assets.

Industry- and manufacturer-certified security experts understand how to apply best practices and meet compliance objectives using existing infrastructure and leveraging on-premise investments and cloud-based networking,
platforms, and controls.

Design – Plan, develop, design point solution or holistic technical solutions though a consultative and collaborative process

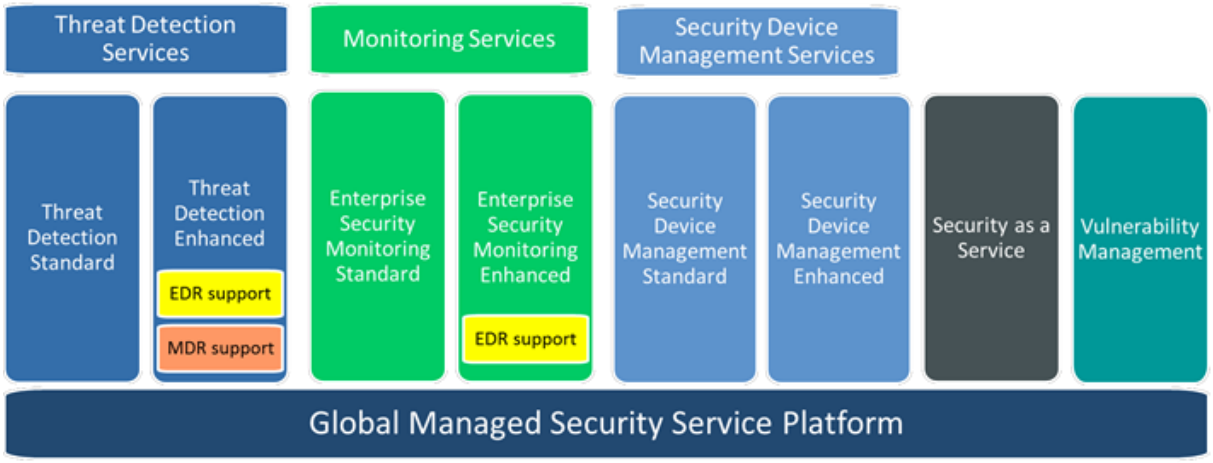
Secure – Implementation, tuning, continual insight into the security technology landscape and the ability to respond in the need of event or incident

Test – Validation of controls, programs, people, processes and technology.

2.1 Managed Security Service

With over 15 years of industry experience using a proprietary Global Managed Security Services Platform (GMSSP), managing a global Security Operations Center (SOC) infrastructure, and maintaining a dedicated team of certified Security Analysts, NTT Security offers clients a broad range of Managed Security Services.

The following diagram presents Managed Security Services delivered via the NTT Security GMSSP:



Key NTT Security GMSSP services include:

Threat Detection Services – Threat Detection Services include Standard and Enhanced services for advanced detection, investigation, and reporting of Security Incidents. The Threat Detection – Enhanced service includes support for Endpoint Detection and Response technologies, as well as Managed Detection and Response capabilities.

Monitoring Services – Monitoring services include Standard and Enhanced services for security detection and compliance reporting. The Enterprise Security Monitoring – Enhanced service includes support for Endpoint Detection and response technologies. Enterprise Security Program Services (ESPS), which add consulting services for strategic planning, architecture, implementation, reporting, and overall security program guidance can be added to Enhanced monitoring services.

Security Device Management Services – Security Device Management Services include Standard and Enhanced services for management of a broad range of security technologies.

Security as a Service – Security as a Service includes management and monitoring of cloud-based security solutions.

Vulnerability Management – Vulnerability Management services deliver customized vulnerability management with a variety of compliance and reporting options.

2.1.1 Threat Detection Services

Overview

Businesses today are under attack from commercially driven attackers that are highly motivated in targeting specific victims with predetermined objectives.
Using a variety of attack vectors, sophisticated attack techniques and previously unseen vulnerabilities makes these attackers more effective and evasive, able to bypass the traditional security measures used to protect and monitor businesses.
The level of sophistication and evasiveness allows attackers to not only to bypass these measures, but also benefit from a longer mean-time to detection and response, which gives attackers significantly more time to act on their objectives in breached environments.
Having threats go unnoticed for a long period of time can result in significant commercial impact, including damage to company trust, brand value, loss of intellectual property, and financial penalties and lawsuits.

Understanding that there is no single solution or detection technique that offers complete detection of sophisticated attacks, NTT Security GMSSP Threat Detection services leverage the combined insights and capabilities of monitored sources with that of NTT Security's proprietary Advanced Analytics, threat hunting and threat validation capabilities, delivering insights from the network perimeter to the endpoint.

As threats are identified and separated from large amounts of false-positives typically generated by security technologies, relevant contextual information is gathered and presented to a Security Analyst in the global operational teams or sent to the client directly as a Security Incident report.
In the Threat Detection – Standard service, *threats with high confidence* are sent directly to clients in the form of a detailed Security Incident report that describes the full extent of the identified Security Incident with general recommendations that enable client's Incident Response team to act on the identified activity, reducing the mean time to respond to mitigate the associated risk.

In the Threat Detection – Enhanced service *suspicious activities* and all relevant contextual information are presented to a skilled Security Analyst, who engages in threat hunting and threat validation activities to verify the threat, its impact and identify additional information associated with the potential breach. Once verified, the Security Analyst creates a detailed Security Incident report and initiates Security Incident notifications in accordance with documented client procedures, providing a detailed description of the Security Incident combined with scenario specific actionable response recommendations, which significantly assist businesses in reducing the time to take informed responsive measures, lowering associated risks.

With supported Endpoint Detection and Response (EDR) technologies, clients can add optional Managed Detection and Response (MDR) services. MDR services enable NTT Security Analysts to take responsive actions (such as remote isolation of compromised hosts) to reduce risk of the compromise spreading further in the environment.

Additional details about the Threat Detection service levels are presented in the following sections

Threat Detection – Standard

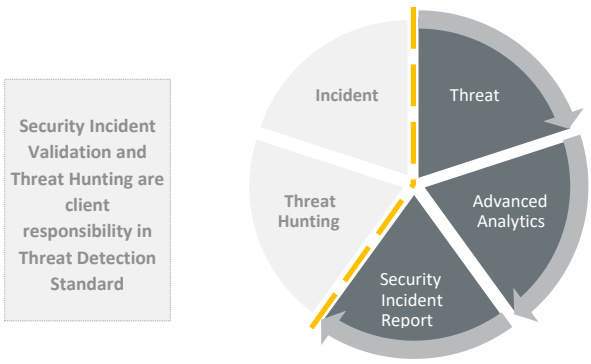
NTT Security Threat Detection – Standard is an automated service offering for organizations looking for entry-level threat detection while seeking to leverage the sophisticated threat detection abilities of the NTT Security GMSSP, its threat intelligence delivered by NTT Security's Global Threat Intelligence Center, and 24/7 monitoring capabilities.

Using the same analytics platform as Threat Detection – Enhanced, the Threat Detection – Standard offering leverages a combination of traditional threat detection techniques (e.g. correlation, pattern matching, reputation feeds) with Advanced Analytics (e.g. Machine Learning, statistical modelling, Kill-chain modelling) and Threat Intelligence which enable detection of sophisticated threats.

Detection and reporting capabilities are continuously improved based on threat data acquired from the from Threat Detection – Enhanced service delivery and Threat Intelligence efforts.

As Security Incidents are identified by the Security Analysts in the Threat Detection – Enhanced service delivery, NTT Security's machine learning classifiers build confidence in identification of patterns, signatures, and behaviours associated with these suspicious activities.

Once the threat confidence level and the true-positive rate are within established boundaries, suspicious behavi*o*r is categorized as threats and made available for the Threat Detection – Standard service delivery and established as detection and Security Incident reporting capabilities. This enables Threat Detection – Standard clients to leverage the experience and continuous efforts of the Security Analysts as part of Threat Detection – Enhanced, with a delay in detecting the latest threats.



NTT Security Threat Detection - Standard, threats identified with a certain level of confidence are sent to clients as Security Incident reports containing detailed description and generic recommendations for identified threats, significantly reducing the lead-time for businesses Incident Response team to act in identifying and mitigating threats.

Threat Detection – Enhanced

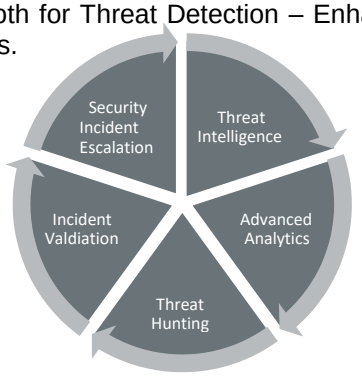
NTT Security Threat Detection – Enhanced, offers advanced detection of today's advanced and evasive Threat Actors, and guidance on response.

Combining the capabilities of the supported technologies with the NTT Security's proprietary GMSSP, its Threat Intelligence and Advanced Analytics with threat hunting and threat validation capabilities, the Threat Detection – Enhanced service enables early detection of sophisticated threats, reducing the risk of having such threats go undetected for a long period of time.

As suspicious activities are identified, the team of skilled Security Analysts receives events with contextual information of the activity and then engages in threat validation and threat hunting activities across the client environment, enabling validation of the malicious nature of a threat and assessment of the threat's potential impact.

An accurate, relevant and actionable Security Incident report is issued for validated Security Incidents, helping clients to significantly reduce the lead-time to take informed measures in threat response.

Findings are automatically propagated back to the GMSSP in the form of Threat Intelligence resulting in increased coverage globally both for Threat Detection – Enhanced, as well as Standard, enabling future detection of similar activities.



The following table provides a service feature comparison of the Threat Detection – Standard and Threat Detection Enhanced services:

Capability	Threat Detection Services	
	Threat Detection – Standard	Threat Detection – Enhanced
24/7 Security Operations Center coverage	✓	✓
Services enhanced by NTT Security Global Threat Intelligence Center	✓	✓
Continuous Threat Intelligence updates driven by production investigations	✓	✓
Advanced Analytics with proprietary machine learning / behavioral modeling	✓	✓
Vendor integration and evidence collection for key security technologies[4]		✓
Detailed Security Incident investigation by Security Analysts		✓
Event-driven threat hunting		
Automated Security Incident reports	✓	
Security Incident reports based on detailed investigation and threat hunting		
Customizable web portal	✓	
Client access to 90 days of Event and Incident data	✓	
[Option] Client raw log search		
[Option] Secure long-term log storage and management		
[Option] On-premise POD[5]		
[Option] Immediate response to isolate compromised endpoints (Remote IR)[6] and/or network blocking of confirmed malicious URL/IPs [7]		

4 Gathers and analyses additional vendor evidence data including packet capture data (PCAP), malware execution reports, and host recordings.

5 On-premise POD is installed on premise for clients that require or prefer that logs remain on-site.

6 Endpoint containment requires an Endpoint solution managed by NTT Security.

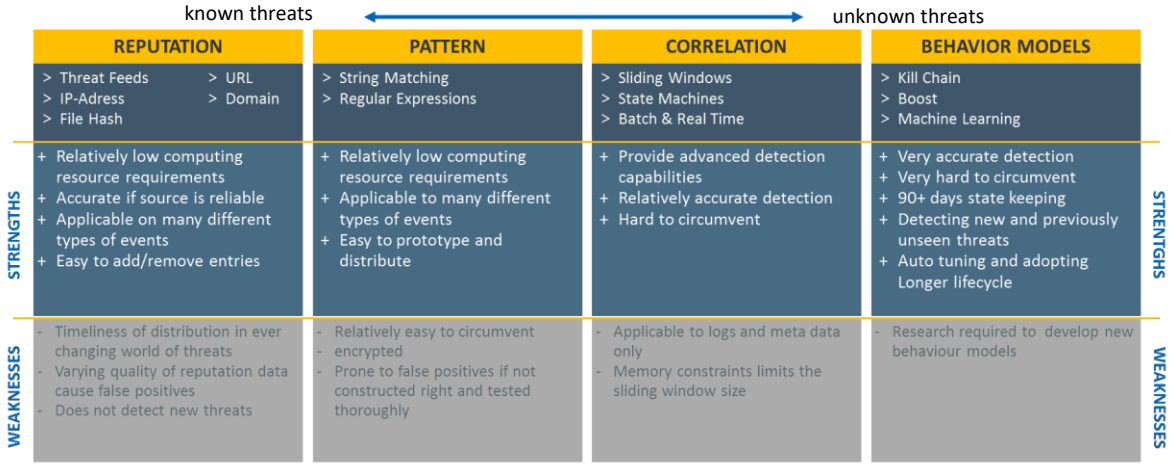
7 Network IP/URL containment requires a network solution managed by NTT Security.

Feature Details

Advanced Analytics with proprietary machine learning & behavioural modelling

Modern threats utilize techniques with rapidly changing indicators (e.g. source IP address, landing page URLs, file names, file hashes) utilized for detection using traditional pattern- and reputation-based techniques.

As a result, modern Threat Detection services cannot rely solely on traditional detection techniques but must also utilize Advanced Analytics (including machine learning, advanced correlation, threat behaviour modelling, and threat intelligence) techniques to identify suspicious activities. These techniques enable Threat Detection services to detect known and unknown threats. An overview of detection capabilities utilized in NTT Security Threat Detection services is presented in the following diagram:



This combination of detection techniques enables broad threat coverage from usage of static Indicators of Compromises and robust coverage for evasive and unknown threats using behaviour models and various forms of anomaly detection, ensuring swift and accurate threat detection overage over time.

Vendor integration and evidence collection

Threat Detection – Enhanced has established deep integration with multiple supported vendors and technologies to enable collection of evidence data and contextual information beyond standard syslog outputs.

This additional evidence (e.g. PCAP's, malware execution reports, host recordings, files, and signature information) not only provides event describing that something suspicious have happened, but also significant additional insights into the identified threats.

This additional evidence greatly enhances the Security Analyst's ability to validate the threat, support threat hunting activities, and gain a better understanding of the threat's potential impact.

This evidence data can be anything from a TCP packet as part of a PCAP trace, to a detailed listing of IOC's and behavioural information in a sandbox executional report, to gigabytes of data in an endpoint recording. Evidence data is made available to the Security Analyst in a proprietary Analyst Workbench, enabling the Security Analyst with the ability to perform Security Incident Validation and Threat Hunting.

Example, Syslog (SIEM) vs. Threat Detection – Enhanced

Syslog event (typical output stored in a SIEM)	Same event, combined with PCAP data
2017-12-08T21:35:09;83.123.221.23; 80; 192.168.10.10; 23491; virus; 191338785; Trojan/Win32.docdl.ltl; allowed	2017-12-08T21:35:09;83.123.XXX.XX; 80; 192.168.10.10; 23491; virus; 191338785; Trojan/Win32.docdl.ltl; allowed GET /***M2z/ HTTP/1.1 Host: ****.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Thu, 07 Dec 2017 06:06:50 GMT Server: Apache X-Powered-By: PHP/7.0.26 Pragma: no-cache Content-Disposition: attachment; filename="0926.exe" Content-Transfer-Encoding: binary Transfer-Encoding: chunked Content-Type: application/octet-stream 11ff8 MZ.....@.....!..L.!This program cannot be run in DOS mode.

Continuous threat intelligence propagation from production

Threat Intelligence is continuously curated and propagated into the Threat Detection services from multiple technical and operational sources in an integrated manner that enables efficient and accurate threat detection.

Threat Intelligence propagation are built into the foundation of Threat Detection services and are ever changing. Additions are made as technical capabilities and operational capabilities are established, and partnerships and collaborations are initiated, examples:

Product threat data are gathered from the global network of Analysis Engines monitoring client businesses and NTT Group Networks, as these continuously identifies known and unknown threats in specific locations the threat data gathered and used to improve the detection logic globally through, improving Machin-Learning capabilities, creation of rules and additions to various blacklists.

As Security Analysts identify and escalate verified threats as Security Incidents within the Threat Detection – Enhanced Service, delivery data are automatically gathered and used for the same purposes.

In addition, dedicated Threat Intelligence Analysts in the NTT Global Threat Intelligence Centre monitor the global threat landscape for new threats, trends and advisories. Upon identifying such scenarios, the team engages in threat research activities to identify additions and modifications to NTT Security threat detection capabilities, including:

- Blacklist additions
- Pattern signature modification, or creation
- Correlation signature modification, or creation
- Collaboration with data scientists improve machine learning capabilities

Event-driven threat hunting

Security Analysts perform event-driven threat hunting activities as part of Security Incident validation in the Threat Detection – Enhanced service. Empowered with the NTT Security's proprietary Analyst Workbench toolset, Security Analysts gain full insights of the client monitored sources, as well as contextual information and evidence data in one single-pane of glass.

Enabling not only the ability to follow a Threat throughout its life-cycle but also hunt for additional activities and lateral movement possibly not detected by any of the monitoring capabilities in place, this is critical in understanding the extent of identified threats and the potential impact.

Threat Detection enabling device list

Useful and enabling devices for Threat Detection services are identified in one of three categories. These categories are presented below:

Highly Recommended - Important log sources for highly effective Threat Detection – Enhanced.

Recommended - Useful log sources for Threat Detection – Enhanced.

Yes - Supporting log and event sources utilized for Security Incident Investigation and Threat Hunting and that shorten time to validation but are not necessary sources to enable the service.

Vendor	Product Name	Threat Detection – Standard Support	Threat Detection – Enhanced Support
Apache	Web Server - Access Logs	No	Yes
Apache	Web Server - Error Logs	No	Yes
Blue Coat	ProxyAV	No	Yes
Blue Coat	Web Proxy (Proxy SG)	Yes	Highly recommended
Carbon Black	Enterprise Protection	No	Yes
Carbon Black	Enterprise Response	No	Yes
Check Point	All-in-one UTM Appliances	Yes	Highly recommended
Check Point	Firewall-1	Yes	Yes
Cisco	ASA Firewall	Yes	Yes
Cisco	FirePOWER Threat Defense Firewall	Yes	Highly recommended
Cisco	Firewall Services Module	Yes	Yes
Cisco	Meraki	No	Yes
CounterTack	Endpoint Detection and Response	No	Yes
F5 Networks	ASM	Yes	Yes
F5 Networks	LTM	Yes	Yes
FireEye	Email Malware Protection System (EX)	Yes	Recommended
FireEye	Web Malware Protection System (NX)	Yes	Recommended
FireEye	HX	No	Yes
Fortinet	All-in-one UTM Appliances	Yes	Yes
Fortinet	Web Application Firewall	Yes	Yes
Imperva	SecureSphere Web Application Firewall	Yes	Yes
McAfee	Network Security Platform	Yes	Highly recommended
Microsoft	Internet Information Server (IIS)	Yes	Yes
Microsoft	SQL Server	No	Yes
Microsoft	Windows - OS/Domain Controller	No	Yes
Oracle	Database Monitoring	No	Yes
Palo Alto Networks	Next-Generation Firewall	Yes	Highly recommended
Palo Alto Networks	Wildfire	Limited	Recommended
Snort	IDS	No	Recommended
Squid	Squid Proxy	Yes	Highly recommended
UNIX/Linux	Syslogd or Syslog-ng, rsyslog	Yes	Yes
Websense	Web Security Gateway	Yes	Yes
Zscaler	Web Security	No	Yes

2.1.2 Managed Detection and Response Capabilities

With supported Endpoint Detection and Response technologies, clients can add optional Managed Detection and Response (MDR) services.

MDR services enable NTT Security Analysts to take responsive actions to reduce risk of the compromise spreading further in the client environment. Responsive actions include:

- Immediate response to isolate compromised endpoints (Endpoint containments requires an EDR solution managed by NTT Security)
- Network blocking of confirmed malicious URLs/IP addresses (Network containment requires a network solution managed by NTT Security).

These containment capabilities on managed Endpoint Detection and Response, combined with the sophisticated threat detection abilities of NTT Security Threat Detection Enhanced enables clients to experience the benefit of a fully Managed Detection and Response (MDR) service offering.

2.1.3 Enterprise Security Monitoring

Comprehensive log monitoring is a critical component of your security program and a requirement for regulations such as PCI DSS, GLBA, HIPAA, SOX, and others. Logs require extended analysis 24 hours a day, seven days a week.

Strengthen your security program with advanced threat detection and reduce costs by shifting the burden from your staff to ours. Benefit from our Global Services Platform (GSP), global SOC infrastructure, and trained and certified SOC Analysts.

Using our proprietary, cloud-based SIEM platform, we can provide:

- 24/7 log collection and active monitoring
- Security event escalation and context-aware alerting
- Customizable advanced analytics
- Multiple Security Operations Centres (SOCs)
- Analysis and validation by certified security experts
- Cross-device and cross-client correlation
- 100% retention of collected logs
- Flexible service tiers
- Dedicated service delivery manager

There are two main levels of service within our Enterprise Security Monitoring Service.

- Enterprise Security Monitoring – Standard (ESM-S)
- Enterprise Security Monitoring – Enhanced (ESM-E)

Enterprise Security Monitoring Standard (ESM-S)

NTT Security's Enterprise Security Monitoring – Standard service utilizes the Global Managed Security Services Platform to provide enterprise security detection and compliance monitoring to protect against threats and keep clients in compliance.

Enterprise Security – Standard services have been designed for organizations with standardized security detection and compliance requirements across a core set of security technologies.

Enterprise Security Monitoring – Standard services include 24/7/365 monitoring using a standardized set of detection rules for core security technologies.

Enterprise Security Monitoring – Standard services include access to a customized portal that efficiently communicates event information, a dashboard view of services, and executive and technical compliance reporting.

Enterprise Security Monitoring Enhanced (ESM-E)

NTT Security's Enterprise Security Monitoring – Enhanced Service utilizes the Global Managed Security Services Platform to provide enterprise security detection and compliance monitoring to protect against threats and keep clients in compliance.

Enterprise Security Monitoring – Enhanced services have been designed for organizations with have been designed for organizations with custom security detection and compliance requirements across a wide set of security technologies (Enterprise Security Monitoring – Enhanced includes support for almost 200 different technologies).

Enterprise Security Monitoring – Enhanced services include 24/7/365 monitoring by NTT Security's Global Security Operations Centers. Identified Events are escalated to experienced, certified, and shared level 1 and level 2 Security Analysts for review and validation – events validated by Security Analysts are escalated to clients as Security Incident reports for additional investigation by the client.

Enterprise Security Monitoring – Enhanced services are enhanced by NTT Security Global Threat Intelligence, and include access to a customizable portal that efficiently communicates Event and Security Incident information, a dashboard view of services, and executive and technical compliance reporting.

Service Level Feature Comparison

Capability	Enterprise Security Monitoring - Standard	Enterprise Security Monitoring - Enhanced
24/7 Security Operations Center coverage	✓	✓
Services enhanced by NTT Security Global Threat Intelligence Center		✓
Standardized security detection and compliance profile	✓	
Customized security detection and compliance profile for large range of devices		✓
Analyst reviewed Security Incident reports[8]	✓	✓
Customizable web portal	✓	✓
Customizable monitoring and compliance reporting	✓	✓
Client access to 90 days of Event and Security Incident data	✓	✓
[Option] Client raw log search		✓
[Option] Secure long-term log storage and management	✓	✓

Monitoring Supported Device List

Key technologies supported by the GMSSP monitoring services are presented in the following table. A complete list of log sources available via ESM Enhanced (~200 individual log sources) is available in the NTT Security GMSSP Supported Device List.

Vendor	Product Name	ESM Standard	ESM Enhanced
Amazon Web Services	CloudTrail		✓
Apache	Tomcat Web Server		✓
Apache	Web Server - Access Logs	✓	✓
Apache	Web Server - Error Logs	✓	✓
Blue Coat	ProxyAV	✓	✓
Blue Coat	Web Proxy (Proxy SG)	✓	✓
Carbon Black	Enterprise Protection		✓
Carbon Black	Enterprise Response		✓
Check Point	All-in-one UTM Appliances	✓	✓
Check Point	Firewall-1	✓	✓
Cisco	ASA Firewall	✓	✓
Cisco	ASA VPN		✓
Cisco	FireAMP		✓
Cisco	FirePOWER Threat Defense Firewall	✓	✓
Cisco	Firewall Services Module	✓	✓
Cisco	Meraki	✓	✓
Cisco	Routers and Switches		✓
Cylance	PROTECT		✓
F5 Networks	ASM	✓	✓
F5 Networks	LTM	✓	✓
FireEye	Email Malware Protection System (EX)	✓	✓
FireEye	Web Malware Protection System (NX)	✓	✓
FireEye	HX	✓	✓
Fortinet	All-in-one UTM Appliances	✓	✓
Fortinet	Web Application Firewall		✓
IBM	WebSphere		✓
Imperva	SecureSphere	✓	✓
Juniper Networks	IDP		✓
Juniper Networks	Pulse Secure User Access Control		✓
McAfee	Host Intrusion Prevention (ePolicy Orchestrator)		✓
McAfee	Network Security Platform	✓	✓
Microsoft	Internet Information Server (IIS)	✓	✓
Microsoft	SQL Server	✓	✓
Microsoft	Windows - OS/Domain Controller	✓	✓
Oracle	Database Monitoring	✓	✓
Palo Alto Networks	Next-Generation Firewall	✓	✓
Palo Alto Networks	Wildfire	✓	✓
Snort	IDS	✓	✓
Symantec	End Point Protection (SEP)		✓
UNIX/Linux	Syslogd or Syslog-ng, rsyslog	✓	✓
VMWare	ESXi		✓
Websense	Web Security Gateway	✓	✓
Zscaler	Web Security		✓

Monitored Device comparison of Threat Detection and Monitoring services

The following table presents a supported and useful device list comparison of the four GMSSP Threat Detection and Monitoring services.

Vendor	Product Name	Threat Detection - Standard	Threat Detection - Enhanced	ESM Standard	ESM Enhanced
Amazon Web Services	CloudTrail				✓
Apache	Tomcat Web Server				✓
Apache	Web Server - Access Logs		✓	✓	✓
Apache	Web Server - Error Logs		✓	✓	✓
Blue Coat	ProxyAV		✓	✓	✓
Blue Coat	Web Proxy (Proxy SG)	✓	✓	✓	✓
Carbon Black	Enterprise Protection		✓		✓
Carbon Black	Enterprise Response		✓		✓
Check Point	All-in-one UTM Appliances	✓	✓	✓	✓
Check Point	Firewall-1	✓	✓	✓	✓
Cisco	ASA Firewall	✓	✓	✓	✓
Cisco	ASA VPN				✓
Cisco	FireAMP				✓
Cisco	FirePOWER Threat Defense Firewall	✓	✓	✓	✓
Cisco	Firewall Services Module	✓	✓	✓	✓
Cisco	Meraki		✓	✓	✓
Cisco	Routers and Switches				✓
CounterTack	End Point Protection and Response		✓		
Cylance	CylancePROTECT				✓
F5 Networks	ASM	✓	✓	✓	✓
F5 Networks	LTM	✓	✓	✓	✓
FireEye	Email Malware Protection System (EX)	✓	✓	✓	✓
FireEye	Web Malware Protection System (NX)	✓	✓	✓	✓
FireEye	HX		✓	✓	✓
Fortinet	All-in-one UTM Appliances	✓	✓	✓	✓
Fortinet	Web Application Firewall	✓	✓		✓
IBM	WebSphere				✓
Imperva	SecureSphere	✓	✓	✓	✓
Juniper Networks	IDP				✓
Juniper Networks	Pulse Secure User Access Control				✓
McAfee	Host Intrusion Prevention (ePolicy Orchestrator)				✓
McAfee	Network Security Platform	✓	✓	✓	✓
Microsoft	Internet Information Server (IIS)	✓	✓	✓	✓
Microsoft	SQL Server		✓	✓	✓
Microsoft	Windows - OS/Domain Controller		✓	✓	✓
Oracle	Database Monitoring		✓	✓	✓
Palo Alto Networks	Next-Generation Firewall	✓	✓	✓	✓
Palo Alto Networks	Wildfire	✓	✓	✓	✓
Snort	IDS		✓	✓	✓
Symantec	End Point Protection (SEP)				✓
UNIX/Linux	Syslogd or Syslog-ng, rsyslog	✓	✓	✓	✓
VMWare	ESXI				✓
Websense	Web Security Gateway	✓	✓	✓	✓
Zscaler	Web Security		✓		✓

✓ use/support devices

✓ Important and useful monitoring devices or devices that enable remote Incident Response

Monitoring Add-on - Enterprise Security Program Services

NTT Security Enterprise Security Program Services (ESPS) are designed for Enterprise Security Monitoring - Enhanced clients with business-specific security objectives requiring customized Managed Security Services (MSS).

Beyond traditional MSS, ESPS services enable clients to mature their security program by including a dedicated team of security professionals responsible for strategic planning, architecture, implementation, advanced analytics, reporting, and overall security program guidance.

Clients realize strategic security goals through a custom MSS implementation, including a roadmap aimed at aligning the security program with evolving business needs to improve risk posture. The ESPS team also analyses and advises on use-case development, event tuning, topology, and asset inclusion from a risk-based perspective.

A customized implementation approach and methodology reduces implementation risk, and established project management methodologies are employed to identify, manage, and mitigate project obstacles that can arise from resource, investment, or technology limitations.

As the process advances to optimization, executive communication provides continuous feedback to the client executive team on the implementation's success using metrics and a go-forward plan.

A developed operations process ensures the client team is prepared and capable of managing continued operations once the project concludes. Process development includes defining Security Incident notification and response procedures, along with lessons learned — techniques aimed at maturing processes after a Security Incident occurs.

Key features of the ESPS service include:

- **Onsite Planning and Design:** Capture strategic objectives, key information assets, and establish a program roadmap.
- **Security Architecture Assessment:** Evaluate network topology and build log collection architecture and define the requirements-driven cases to meet business objectives.
- **Implementation & Service Delivery:** Execute and deliver technical components, along with developing service operation processes. A dedicated project manager is assigned for planning, reporting, and communications.
- **Security Control Enhancements:** Recurring review and gap analysis of MSS operations tune performance and drive value throughout the life of the contract.
- **Security Program Guidance:** Define the program target state and lay out concrete steps to reach maturity. Five key areas—Program Planning, Infrastructure, Operations, Response, and Reporting—are considered in the final analysis.
- **Executive Briefings & Account Reviews:** Conduct on-site quarterly account project reviews and semi-annual executive briefings during engagement and for a period following conclusion of implementation.

2.1.4 Security Device Management

Getting the basics right from the beginning is a fundamental aspect to good Cyber Security practices. Secure configuration, management and maintenance of security devices is essential to protect assets and meet numerous compliance regulations. Managing security devices, however, requires a specific and specialized skill set that requires constant attention, training and upkeep.

Keeping solutions updated and patched while monitoring them 24/7 is a challenge for all organizations big and small. NTT Security reduces that burden for NTT clients with Security Device Management Services that follow industry best practices to provide appropriate service fulfilment and change management processes, event, incident and problem management ensuring security devices are available, and that organizations maintain compliance with applicable regulatory requirements.

- NTT Security Device Management Services provide:
- On-Demand device configuration and tuning
- Timely updates and release management (patch & security hotfix)
- Continuous device health and availability monitoring
- 24/7 Coverage via ISO/IEC 27001 certified Security Operation Centres
- Highly experienced industry and vendor certified engineers
- Proven operational processes aligned with industry best practice and guidelines
- Device incident/event/problem/capacity management and escalation through to resolution
- Service Level Agreement and Objectives commitments and targets to our clients
- Flexibility through available operational levels and options

The Security Device Management Service provides organizations with full maintenance, updates, change management, tuning and 24/7 device monitoring by NTT Security experts.

Clients can leverage their current technology investment, using leading security vendors. Security devices and applications such as Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), Content Filters, Web Application Firewalls (WAF), Identity and Access Management systems (IAM) and Endpoint security solutions must be properly provisioned, configured, updated and patched to protect against internal and external threats.

Policies, signatures and rules need to be updated and maintained to ensure accessibility, provide security and to comply with regulations. Security best practices and many regulations also require continuous monitoring to detect and respond to threats.

NTT Security provide flexible bespoke and standard services, therefore can offer standalone Security Device Management Services or integrated with Monitoring and Threat Detection offerings.

Through various operational levels NTT Security can help organizations reduce capital expenditure and resourcing costs whilst maintaining quality and control. Using NTT Security's highly qualified and experienced security analysts to monitor and manage your security devices 24/7, enables your organization to focus in-house resources on adding value to core business activities.

Service Level Feature Comparison

NTT Security Device Management Services provide operational levels with various options to meet an organizations business requirement. The following table outlines each operational level with the applicable service modules, elements and options available:

Service Module	Service Elements	Enhanced	Standard
Availability / Event / Incident / Problem	Health and Availability Monitoring Event/Incident/Problem Management	✓	✓
Asset Management	Release Management (Patch & Security Hotfix)	✓	✓
	Backup for device configuration and OS	✓	✓
	Restore + Out of Band (Availability SLA/OLA for Recovery Time Objective)	✓	
Service Request Fulfilment	Support change request align with predefined client's Move, Add, Change, Delete (MACD)	✓	
	Additional MACD's	Option	

Standard services provide a client further asset-based services through release management elements (patch and security hotfix) as well as health and availability monitoring and event, incident and problem management to minimize disruption to business with options to ensure availability is maximized.

Enhanced services build upon Standard services by inherently providing service level agreements and objectives also including device configuration and tuning with a predefined bundle of MACD's.

Device management supported device list

NTT Security provides global/multi-region Security Device Management services for key security technologies, these are presented in the following table. A complete listing of supported devices can be found in the NTT Security GMSS Supported Device List.

Vendor	Product Name	Device Management Services
Blue Coat	ProxyAV	✓
Blue Coat	Web Proxy (Proxy SG)	✓
Carbon Black	Enterprise Protection	✓
Check Point	All-in-one UTM Appliances	✓
Check Point	Firewall-1	✓
Check Point	Provider-1	✓
Cisco	ASA Firewall	✓
Cisco	ASA VPN	✓
Cisco	FirePOWER + FireSIGHT	✓
Cisco	Firewall Services Module	✓
Claroty	Continuous Threat Detection	✓
F5 Networks	ASM	✓
F5 Networks	LTM	✓
FireEye	Web Malware Protection System (NX)	✓
FireEye	E-mail Malware Protection System (EX)	✓
Fortinet	All-in-one UTM Appliances	✓
Gemalto	Secure Authenticate V2 (SAV2)	✓
IBM	ISS	✓
IBM	Proventia	✓
Imperva	SecureSphere	✓
Juniper Networks	IDP	✓
McAfee	Network Security Manager	✓
Palo Alto Networks	Next-Generation Firewall	✓
Palo Alto Networks	Wildfire	✓
Pulse Secure	SA	✓
Snort	IDS	✓
Symantec	End Point Protection (SEP)	✓

2.1.5 Vulnerability Management Service

Traditional **Vulnerability Management** processes are time-consuming, inefficient, resource intensive, and can focus on the wrong criteria, resulting in organization security and compliance programs gaps.

To see measurable improvements in vulnerability reduction, NTT Security Vulnerability Management services, combined with threat intelligence and exploit tracking, focus vulnerability management efforts on the highest impact vulnerabilities in an environment.

The NTT Security cloud-based Vulnerability Management platform provides:

- Asset Documentation
- Scanning Setup and configuration
- Scanning Execution Validation
- Flexible Service Tiers
- NTT Security-managed Ad-Hoc Scanning
- Unlimited Self-Service re-scanning

2.1.6 Service Management

NTT Security provides the following services as service management to accelerate client's experience throughout the IT lifecycle by implementing services from introduction to operation, periodic performance review, and technical support for client's infrastructure management as a one-stop window.

Client Service Management (CSM) - Standard

CSM Standard is the baseline and mandatory service offering to all clients and targeted towards small to medium sized customers, where they are managed by a pool of CSMs and not a designated CSM.

From Service Activation the Client is welcomed to and shown the 'self-help' Service Request portal for Changes or Incidents and to get their monthly reporting online. The client also is engaged for quarterly service reviews ensuring the service is being delivered correctly and for any enhancements.

Client Service Management (CSM) - Enhanced

CSM Enhanced is aimed at larger and more complex clients where the function provides additional Service Management activities in addition to CSM Standard, where clients are provided a designated CSM, receive weekly updates and monthly meetings to review reporting, recommendations and advisory.

A CSM Enhanced FTE (Full-time equivalent) will be measured by number of services subscribed to and size of account (revenue) and will provide financial recovery for CSM functions across mid-tier to large clients.

Technical Account Manager (TAM)

TAM is a designated resource for larger and more complex client estates providing additional technical support coverage, security governance and cyber security insights for MSS services, offering advisory, recommendations, technical reviews, and the ability to be available for technical guidance or questions. A TAM can assist with Technical Audits.

Charged separately and assigned by FTE (Full-time equivalent) value, offering clients and account teams a senior technical resource to complement their organization. TAM is backed by a pool of Cyber Security specialists within NTT Security and has access to all the resources required.

2.1.7 Managed SIEM Services

Successful implementation and operation of third party Security Information and Event Management (SIEM) technologies, other than NTT Security core GMSSP SIEM, can require significant investment in staff, configuration, and operational processes. These investments can be capital and resource prohibitive for many organizations.

Managed and Co-Managed SIEM services improve SIEM effectiveness by ensuring that SIEM implementations are properly configured, tuned, and accepting feeds from relevant systems, that SIEM events are monitored 24x7, critical events are immediately escalated to key personnel, and that overall SIEM health is continuously monitored, with updates applied in a timely manner.

NTT Security provides global Managed SIEM services to help clients ensure effective operations and monitoring of SIEM technologies.

These services also include multi-layered monitoring of a client's in house SIEM as well as the NTT Security GMSSP platform and enable both client security engineers and NTT Security analysts to monitor and detect threat across both platforms to avoid false negative Security Incidents. Key features of these services include:

- SIEM Configuration and tuning
- Updates and patch management
- Continuous Monitoring of SIEM health and configuration
- 24/7 Coverage via ten Security Operation Centers
- Proven Operational Processes refined over 15 years of delivering managed services

NTT Security provides global/multi-region managed SIEM services for key SIEM technologies, including:

- LogRhythm
- Qradar
- RSA Security Analytics
- Splunk

2.2 Technical Security Services

The threat landscape is evolving, with increasing demands that require varying technologies, each with unique contacts, processes, and escalation paths.

Technical Security Services SecureCall provides a single point of contact across multiple security technologies to efficiently resolve complex technical issues and maximize a client's return on investment. NTT Security assumes responsibility for technical security support issues, meaning that we manage all vendor correspondence, and provide arbitration on a client's behalf.

With SecureCall, NTT Security provides a simplified vendor solution with certified, multilingual experts that act as an extension of the client's technical support team, reducing overhead, and helping organizations stay ahead of threats. Nearly 80% of service requests are resolved without engaging outside vendors.

Comprehensive support is offered at two levels: Classic (Monday - Friday, regular business hours) or Premium (24x7x365). Clients may purchase additional services to extend SecureCall's coverage, including:

- A Technical Account Manager (TAM) that works closely with clients to understand their infrastructure and business, and conducts regular review calls as the dedicated escalation point
- SecureHands provides remote technical assistance for minor software updates, configuration changes, and training

- A Technical Baseline Assessment provides a comprehensive health check of Firewalls, Web Proxies, Remote Access Devices, and Application Delivery Controller (ADC)
- Security Technology Training (STT) provides remote training for vendor specific issues such as troubleshooting, configuration, upgrades and admin tasks. Training on non-vendor specific issues is also provided.
- A Security Assessment Scan (SAS) provides a technical and executive report of potential vulnerabilities on your external facing assets using Qualys vulnerability assessment tools

This service is designed to provide a single point of contact for multiple security technology vendors, the service if often much more competitive than vendor direct pricing for the same service level.

2.3 Security Consulting Services

NTT Security provides a full suite of consulting services that are shaped by the understanding of information security risk, security challenges in specific industry verticals and missions, and the intent to consult and advise though all phases of the information security management lifecycle.

NTT Security consulting services are divided into Strategic and Technical categories. Specific engagement activities are delivered as stand-alone services or as part of comprehensive programs and long-term strategies are integrated with our managed security services.

Strategic Consulting	Technical Consulting
• Risk Assessment & Risk Analysis • Compliance & Framework Lifecycle Services • Strategic Planning & Road Map Development • Policy & Program Services • Executive Security & Risk Advisory	• Penetration Testing, Social Engineering & Vulnerability Assessments • Red & Purple Team • Application Security • Security Technology Solutions • SIEM & Log Management • Network, Cloud and Infrastructure • Incident Response & Forensics • Reputation Threat Services • Operational Technology Security

2.3.1 Strategic Consulting

2.3.1.1 Risk Assessments & Risk Analysis

Risk Assessments are the starting point for security strategy and are required periodically to align current business direction with the current threat landscape

.

These engagements calculate risk for a business based on relevant business information, industry vertical, current landscape and threat intelligence. These engagements are designed to align budget allocation allocated with areas where the impact will be highest. The output from this is not only comprehensive and calculated data analysis, gaps and recommendations, but actionable and prioritized road map items that can be executed to drive the business forward. Assessment and Analysis of security risks is differentiated from compliance or “security assessments,” as assessments do not typically include elements such as threat modeling, threat intelligence, and risk calculations. Risk analysis considers business impacts, organizational context, and specific assets to be protected, which may be specific to an application, infrastructure, network, facility, or even vendor relationship(s). Many compliance programs require regular risk assessments which are in addition to other security, compliance & gap assessment which are also completed.

2.3.1.2 Compliance & Framework Lifecycle Services

Compliance & Framework Lifecycle Services address global, regional, regulatory and industry standards as well as client-specific developed programs. NTTS uses a full lifecycle of services to strategically and tactically guide organizations from non-compliance to a state of managed compliance and managed risk. Services can include implementation of compliant security controls, design of workflows, building security checks into existing procedures, and similar support services. Regulatory standards supported include but are not limited to HIPAA, PCI-DSS, NIST 800-53, NIST Cyber Security Framework (CSF), ISO27001/2, and the EU General Data Protection Regulation (GDPR).

2.3.1.3 Strategic Planning and Roadmap Development

Road Maps & Strategic Planning assessments typically result in road map to be developed, this is a customized set of activities an organization needs to execute to achieve the desired state. Though the use of multiple factors a road map is developed in collaboration with the business with properly prioritized tasks to meet business needs. When possible additional information such as likely project costs, duration, technology needs, and other specifics are included. Other strategic planning services are available, including development of plans for security and risk management, presentations on the needs of the organization or information on the existing landscape and potential business impact. Collaborative consulting with boards, executives, or specific business units can be a component of these projects as well.

2.3.1.4 Policy & Program Services

Policy & Program Services provides evaluation of an organizations existing processes and effectiveness, as well as services to help organizations develop and implement larger programs. Whether organizations need a complete information security & risk management program, technology lifecycle program, or information awareness program it can be delivered. NTT Security supports all stages of developing an Information Security Management System (ISMS) from understanding the assets being protected and the risks against them to management of implemented security controls, continually improvement, and measurement metrics. Program development and implementation of GRC tools (such as Archer) are engaged here; addressing the policy, process, and continual management for an organization's GRC programs. There are also options for a managed program or long term, periodic consulting to support client run programs.

2.3.1.5 Executive Security & Risk Advisory

Executive Security & Risk Advisory services allow businesses to leverage the depth and breadth of NTT Security expertise to drive client-side executive decision making and direction. These services are designed to educate executives, so they can make well informed, educated business decisions focused on Security.
The offering provides both virtual and interim CISOs offerings, as well as Executive Business Consultants, Executive Security Advisor, and Executive Security Architects. There are also options for a Lifeline Advisor, who can be called on only as needed. Offerings are designed help to support board level conversations and can be leveraged for managerial and executive level of training, presentation, and strategic planning.

2.3.2 Technical Consulting

2.3.2.1 Red & Purple Teaming

A Red Team assessment is designed to simulate an Advanced Persistent Threat (APT). It includes covert exploitation of various attack vectors over an extended period. This is recommended for organizations with mature security programs. This assessment is ideally suited to validate existing programs and controls, while identifying less obvious risks.

A Purple Team assessment is designed to bring the attackers (Red Team) and defenders (Blue Team) together to mature security programs and controls. The Red Team will launch select attacks and collaborate with the Blue Team to validate or develop controls. This assessment is ideally suited to quickly mature specific areas within a security program.

2.3.2.2 Penetration Testing, Social Engineering & Vulnerability Assessment

Penetration testing addresses areas related to hacking and vulnerability assessment. A comprehensive suite of services is available to conduct single attacks on an environment or application, as well as complete program development or execution integrated with business needs. Tests are conducted in the scope of Network (internal, external, wireless), Application, Social Engineering and Physical engagements, with many options around the level of prior knowledge with customization of attack vectors and scenarios.

Social engineering assessment evaluates risks associated with human interactions. It can include Phishing, Vishing, or onsite testing. The social engineering assessment is designed to validate employee security awareness and supplement security awareness training.

Vulnerability assessment programs are developed and executed based on the needs of the business and create a solid program for organizations to execute regular testing of technology, processes and staff. These programs integrate with our managed services and vulnerability scanning services to provide comprehensive solutions for businesses.

2.3.2.3 Application Security

Application Security addresses the need for code to be developed in a secure manner and continually tested to maintain security. These services help in the assessment and development of a Secure Systems Development Lifecycle (SDLC) and help to verify an application's ability to withstand malicious penetration, privilege escalation, and data exfiltration. The development team will gain actionable intelligence on how their code can be exploited; and thereby learn how to improve their code to prevent such attacks.

2.3.2.4 Security Technology Solutions

Security Technology Solutions includes the assessment, selection, planning, deployment, integration, tuning, migration, refresh, and decommission of security technology and related programs. These services address the technical controls and the processes around which they are used by the staff supporting them. These services can be integrated into our Managed Security Services offering to provide more effective use of technology and services through the products lifecycle. As the vendor landscape around security controls moves, these services are continually growing to adopt new solutions.

2.3.2.5 SIEM & Log Management

SIEM & Log Management addresses the intricate needs of SIEM and Log management with a dedicated team delivering services on selection, implementation, tuning and management of these complex systems. Services around the handling processes and integration into managed services, Security Incident handling, and execution of "mean time to respond" table top engagements are also

conducted. Services to help client solutions vary from periodic health checks, to SIEM assessments, process review or development of programs. Technology supported varies by region and is generally consistent with regional and global market leading products.

2.3.2.6 Network, Cloud & Infrastructure

Network, Cloud & Infrastructure Consulting is delivered by employing highly skilled security consultants and integrating our capabilities with managed services and cloud providers (NTT/non-NTT, public/private.) We can deliver security in depth to client network infrastructures and cloud solutions. This includes working in the cloud with security solutions as well as development of cloud security programs. Aligned closely with our technology services, comprehensive assessments, deployments, and programs can be delivered to deploy or improve any combination of network models: dedicated cloud, hybrid, on-premise, datacenter and more…

2.3.2.7 Incident Response & Forensics

Incident Response & Forensics addresses the policy and process aspects of Incident Response as well as delivering the skills to respond in case of a Security Incident. These services assist clients in fully addressing all aspects of proactive and reactive Incident Response. These services are complemented by our threat intelligence, SIEM, MDR, & MSS teams; these services in combination provide end-to-end security management by having a plan to isolate the issue and begin restoration in the event of a Security Incident. Services include Incident Response Plan testing and development, table top exercises and multiple options for retainer services for breach response.

2.3.2.8 Reputation Threat Services

Reputation Threat Services is an extension of NTT Security's Global Threat Intelligence Center (GTIC) which employees Security Analysts and Intelligence Analysts to conduct in depth research on the threats specific to an organization or industry vertical. This includes executive profiles, current state of reputation, potential to remediate existing issues, and how to prevent new ones. The service provides a standard baseline which is highly customizable for long term reputation management; integrated with managed services, and threat intelligence provides great capability in early awareness and allows organizations to manage business specific threats.

2.3.2.9 Operational Technology (OT) Security

Operational Technology (OT) Security leverages a specialized set of skills and technologies required to evaluate, secure and manage OT systems security. This is achieved though the creation of an OT Security Center of Excellence providing global collaboration and skills. OT services utilize a methodology of: asset discovery, risk & program assessment/improvements, securing of defense & detection, and incident response & management. There is support for multiple technologies today with a continual program of evaluation of technology. Consulting services are available for asset discovery, technology selection, planning and deployment, as well as threat modeling, vulnerability assessments, and risk & security assessments. OT engagements can be one-time, more often engaging in the full lifecycle provides higher value to program development and improvement. Options for managed services are also available for these specific OT environment.

3 Commercial Arrangements

3.1 Parent Company Guarantee (PCG)

Please note the following details in relation to any direct award or competition under the G-Cloud framework agreement.

NTT DATA is not able to provide a Parent Company Guarantee (PCG). If your call-off order or competition requires a PCG, then NTT DATA will be forced to decline the call-off order or withdraw from the competition.

3.2 Use of subcontractors and partners

These services are delivered by NTT DATA with support from partners such as ITelligence, Charteris, Triad, Dimension Data, Bluemetrix, Qualitest and Certeco.

3.3 Pricing

Please see the Cloud Store for the NTT DATA Pricing Document and SFIA Rate Table associated with these services.

3.4 Ordering and invoicing process

Clients will be expected to follow the G-Cloud 13 ordering process as outlined in the Framework's Terms and Conditions. This will ensure that the scope, timeline and technical requirements are understood, agreed and can be delivered.

Each assignment will then require a formal work order to be raised, which would define:

- The name and contact details of the consumer's representative.
- The objective(s) of the work and the Key Performance Indicators.
- The amount and type of resource required (number of roles and duration).
- Start and end dates for the project.
- The scope and requirements for the project.
- The specific technical or business knowledge required by NTT DATA.
- Advise whether the project is expected to be carried out on the consumer's premises (in which case location is required), or at NTT DATA's premises.
- Expected deliverables, quality levels and acceptance criteria for sign-off.

Upon receipt of a work order, NTT DATA will evaluate the requirement and confirm a start date. Once NTT DATA accepts a work order, we will commence work upon receipt of a purchase order.

NTT DATA will operate the following invoicing process:

- For time and material projects and assignments - monthly invoices will be issued in arrears for payment within 30 days.
- For fixed price projects and assignments - invoices will be based upon agreed staged payments associated with formal client sign-off of interim or final deliverables. Invoices are issued in arrears for payment within 30 days.
- For managed services - Transition Charges and Managed Services Charges will be invoiced quarterly in the middle of each quarter.

3.5 Consumer responsibilities

The client will provide a Project Manager responsible for the following activities:

- Ensure the organisation is aware that external support is being provided by NTT DATA and that staff and teams are clear about the project, its scope and their roles and responsibilities in it.
- Manage the client personnel and responsibilities for this project.
- Serve as the interface between NTT DATA and all the client's departments participating in the project.
- Administer the Change Control Procedure with the NTT DATA Project Manager.
- Participate in project status meetings.
- Obtain and provide information, data, and decisions within three working days of NTT DATA's request unless a different response time is agreed in writing.
- Review and approve the Milestone achievements.
- Help resolve any project issues and the client deviations from the estimated schedule, and escalate issues within the client organisation, as necessary.
- Provide staff as required to undertake the User Acceptance Testing.
- Ensure client staff are made available for any meetings, interviews, document review and presentations within the proposed timescale.
- Provide client staff able to deliver authoritative answers to questions and clarification requests in a timely manner.
- Provide NTT DATA personnel with suitable office space, other accommodation and facilities that personnel may reasonably require to perform the services required during the project.

3.6 Accreditations

For these services, NTT DATA has corporate membership of the ITSMF, SDI, MCA and techUK (formerly Intellect) trade bodies and holds a number of relevant accreditations including:

- ISO 9001 Quality Assurance
- ISO 14001 Environmental Management
- ISO 27001 Information Security Management
- PRINCE2 Practitioner Project Managers
- ISO 20000-1 IT Service Management
- Cyber Essentials

NTT DATA's IT services and systems integration activities are supported by a wide range of technical and vendor accreditations including:

BMC Premier/Elite	Interactive Itelligence Elite Partner
CDC (Pivotal)	ITyX Partner
Click Dimensions Partner	Microsoft Gold certified Dynamics CRM, Cloud Accelerate Partner
Cisco	Oracle Platinum, Gold and OPN Partner
Cordys Gold Partner	Salesforce Platinum Partner
Genesys Strategic VAR/ Premier Partner	SAP Expertise Partner, Partner Edge Service
HP VAR, Business Partner, Systems Integrator	Scribe Insight
IBM Business Partner Premier (Value Package), Systems Integrator	Tibco Consulting /Platinum Partner
Adobe accredited partner	Mulesoft UK accredited partner

4 About NTT DATA

4.1 Globally

NTT DATA Corporation is a global IT innovator delivering technology-enabled services and solutions to clients around the world and is the world's 6th largest global IT Services provider (reference: Gartner). It employs more than 110,000 people across 40 countries and has annual revenues of more than $16bn.

For more than 45 years, the NTT DATA Corporation has been successfully providing IT services to a wide range of clients in the automotive, electronics and high technology, energy and utilities, financial services, healthcare and life sciences, insurance, manufacturing, media and entertainment, professional services, public, retail, telecommunications and transportation and logistics sectors.

NTT DATA has significant global coverage across the Americas, Europe/Middle East and Africa (EMEA) and Asia Pacific regions. In EMEA, NTT DATA has operations in 39 cities across the region.

4.2 In the UK

NTT DATA UK Ltd (NTT DATA) is a subsidiary of the NTT DATA Corporation and is a systems integrator headquartered in the Royal Exchange in the heart of the City of London and Birmingham.

NTT DATA in the UK is a £140m per annum turnover organisation that focuses on supporting clients in Public Services, Telecommunications and Media, Insurance and Manufacturing sectors. Its operations are underpinned by ISO registrations (ISO9001, ISO27001 and ISO14001), Cyber Essentials and membership of UK professional bodies.

NTT DATA has partnerships with a number of leading software vendors and works closely with NTT group companies to provide a wide range of solutions to UK clients, companies include NTT Europe, NTT Security, Itelligence, Everis and Dimension Data.

4.3 How we help our clients?

NTT DATA provides a portfolio of services to support every aspect of its clients' business technology life cycle, including:

- Strategy to create competitive advantage.
- Implementation with speed, confidence, efficiency, and surety.
- On-going management to optimise your assets with the best resource mix and cost.
- Evolution to create new opportunities and future-proof your enterprise.

NTT DATA helps its clients by building value through the visualisation and realisation of innovation. This involves working in close partnership with clients to:

- Design innovation - create robust IT strategies geared towards optimising business processes and the use of IT and networking concepts along the customer's entire value chain. We help our clients use IT to differentiate themselves from their competitors.
- Develop solutions - use our advanced systems structuring and application capabilities to develop and provide solutions that make business innovation a reality.
- Drive performance and efficiency - provide constant support for our clients helping them exploit the full potential of their IT solutions and take advantage of the latest IT innovation thinking.

4.4 Trade body membership and accreditations

NTT DATA has corporate membership of the MCA and techUK trade bodies and our activities are supported by technical and vendor accreditations including: BMC Premier/Elite; CDC (Pivotal); ITyX Partner; Click Dimensions Partner; Microsoft Gold certified Dynamics CRM, Cloud Accelerate Partner; Oracle Platinum, Gold and OPN Partner; Cordys Gold Partner; Salesforce Platinum Partner; SAP Expertise Partner, Partner Edge Service; HP VAR, Business Partner, Systems Integrator; Scribe Insight; IBM Business Partner Premier (Value Package), Systems Integrator; Tibco Consulting /Platinum Partner.

4.5 Services

We support UK clients through the following digital focus areas:

- Customer Experience - engaging with customer to maximise user understanding, engagement and support
- Data & Intelligence - excel in new data model creation using gathered intelligence that can produce actionable results for organisation success
- Intelligence Automation - automate repetitive business processes for success in a digitally-dynamic environment
- Internet of Things - connecting and communicating with an ever-expanding base of devices connected to the internet
- IT Optimisation - revolutionising IT environments by delivering the agility necessary to remain effective in a rapidly changing landscape
- Cyber security - protecting against data breaches and unauthorized use of confidential information in today's connected digital world

4.6 Further information

See http://emea.nttdata.com/uk/home/index.html for further information or contact Tom Watson, nttdatauk.requirements@nttdata.com, 02072209200