
NTT DATA
Trusted Global Innovator
素晴らしいガイド
Service Definition Document for G-Cloud 15 Services
Cybersecurity Services
NTT DATA UK LTD
Epworth House, 25 City Road, London, EC1Y 1AA
Tel.: +44 (0) 20 7220 9200
www.nttdata.com
Copyright NTT DATA UK Ltd 2026 All rights reserved
Proprietary and Confidential |
GUIDING GREATNESS

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

- **Cloud Security** - Cloud Security services protect workloads, data, and identities across public, private, and hybrid cloud environments. This includes CSPM, CWPP, configuration hardening, IAM governance, and compliance mapping.
- **Crisis Response** - Crisis Response provides rapid support during cybersecurity incidents such as ransomware or data breaches. Includes containment, forensics, recovery, communication, and post-incident reporting.
- **Data Privacy Management** - Privacy Management covers privacy governance, DPIAs, data subject rights workflows, consent management, and compliance with GDPR/CCPA/DPDP.
- **Data Security** - Data Security covers discovery, classification, encryption, tokenization, data loss prevention (DLP), insider risk mitigation, and access governance.
- **Emerging Technologies** - Security assessment and protection of AI/ML, IoT, blockchain, 5G, edge, and modern architectures including zero trust, threat modeling, and control validation.
- **EndPoint Security** - Endpoint Security ensures protection across laptops, servers, mobile, and edge devices through EPP, EDR, hardening, compliance, and threat hunting.
- **Infrastructure and Network Security** - This service protects enterprise networks, datacenters, and cloud infrastructures via segmentation, firewalls, WAF, IPS, NDR, and secure remote access.
- **Offensive Security** - Offensive Security includes penetration testing, red teaming, social engineering, breach simulation, and attack surface management.
- **OT-IOT Security** - OT/IoT Security protects industrial systems (ICS/SCADA) and connected devices with asset discovery, segmentation, protocol-aware monitoring, and firmware security.
- **Threat Management** - Threat Management delivers threat hunting, intelligence integration, malware analysis, and attack surface monitoring.
- **Unified Detect and Response** - UDR/XDR unifies telemetry from endpoint, cloud, identity, and network for correlated detections, automated response, and reduced dwell time.

See Section 2 for full-service descriptions.

2 Service Descriptions

2.1 Cloud Security

2.1.1 Overview

Cloud Security encompasses the technologies, policies, controls, and services designed to protect cloud data, applications, and infrastructure from threats. It provides a comprehensive security framework that addresses vulnerabilities across public, private, and hybrid cloud environments while enabling organizations to maintain compliance, protect sensitive information, and ensure business continuity. As organizations accelerate digital transformation initiatives, cloud security has become a strategic imperative rather than just an IT concern.

2.1.2 Service Specific Offerings

2.1.2.1 Managed CNAPP Security Services Portfolio

This portfolio outlines the comprehensive security services delivered through a Cloud-Native Application Protection Platform (CNAPP) framework, designed to provide a unified, automated, and expertly managed defence across the entire cloud application lifecycle, from code to cloud (development to runtime) approach. These services cover the technical operation and maintenance of the core CNAPP toolset (e.g., WIZ, Orca Security, Cortex Cloud, Microsoft Defender for Cloud), ensuring optimal performance and coverage across multi-cloud environments (AWS, Azure, GCP) & embedding security expertise directly into the development lifecycle in shift -left security ensuring proactive risk management and shift -right security through continuous threat monitoring and management by security operation centre(SOC). Our CNAPP Security Services portfolio encompasses the following key security capabilities

Advisory Services:

1. CNAPP Readiness & Maturity Assessment: Auditing the current cloud security state, identifying gaps in DevSecOps practices, multi-cloud coverage, and mapping current tools to CNAPP capabilities.
2. CNAPP Strategy & Roadmap Definition: Defining a roadmap for CNAPP adoption across AWS, Azure, and GCP and alignment of CNAPP capabilities with business objectives & developing a phased approach, including tool selection (Wiz, Palo Alto, Microsoft, etc.) and defining the Target Operating Model.
3. Architecture & Design Advisory: Designing a integrated framework comprising of CSPM, CWPP, CIEM and runtime protection and security baselines definition, compliance templates (CIS, NIST, PCI DSS, HIPAA, ISO) and development of the security guardrails for multi cloud deployments and integration with SIEM/SOAR, ITSM tools and DevSecops pipeline.
4. Cloud Security Posture (CSPM) Review: Evaluation of current cloud security posture and identification of misconfigurations, vulnerabilities and compliance gaps and risk prioritisation through business context mapping basis criticality and sensitive data exposure of workloads and providing executive level risk reporting.
5. Cloud Identity & Entitlement (CIEM) Audit: Analysis of human and non-human identities identification of over-privileged access, dormant roles, and toxic permission combinations to enforce the principle of least privilege.
6. Operational advisory: Implementation guidance for onboarding workloads into CNAPP, threat detection determination and response through attack path analysis and guided recommendations for remediations. continuous monitoring setup across multicloud, automation of remediation workflows and integration with ITSM tools. Posture Improvement through regular reviews and recommendations, cloud security maturity assessment and determining strategic roadmap towards advance CNAPP adoption.
7. Compliance & Governance advisory: Regulatory alignment by mapping CNAPP controls to frameworks like PCI-DSS, HIPAA, ISO 27001 etc, audit readiness through evidence collection, Reporting and development of compliance dashboards and defining Governance model.

Professional services:

1. CNAPP solution deployment & configuration: Platform deployment & setup: Architecting, deploying and configuring CNAPP for target cloud environments (AWS, Azure, GCP).
2. Shift-Left" Integration: Integration of CNAPP features (e.g., IaC scanning, secret scanning) directly into the CI/CD pipelines (e.g., Jenkins, GitLab, GitHub Actions). Configuring continuous scanning of container registries (e.g., ECR, ACR, Docker Hub) for vulnerabilities and malware and developing image admission policies for Kubernetes.
3. Runtime Protection (CWPP) Policy Definition: Defining and implementing runtime security policies for critical workloads (containers, VMs, serverless) to detect and prevent malicious behaviour.
4. Automated remediation workflow design: Building and testing automated security response workflows
5. CIEM policy enforcement & remediation: Analysis of cloud permissions through CIEM and integration with IAM tools for automating access requests and reviews.
6. Custom policy & guardrail development: Translation of organizational security policies into cloud-native security policies and compliance guardrails to be monitored and enforced by the CNAPP.
7. Cloud Detection and Response (CDR) Integration: Integrating CNAPP's alert and log data with existing SIEM/SOAR solution.

Managed CNAPP services:

1. [Optional service] 24x7 Threat monitoring and triage: 24/7 continuous monitoring of posture, misconfigurations, contextualised alerts, noise reduction, and initial investigation/triage of security incidents identified by the CNAPP platform.
2. Advanced Threat Hunting through proactive search for indicators of compromise across workloads and identities.
3. Compliance management: Continuous assessment and reporting against compliance frameworks (like PCI-DSS, HIPAA, and CIS Benchmarks) using CNAPP's built-in frameworks and developing baseline dashboards for CIS, NIST, ISO, PCI DSS.
4. Identity & access oversight: Monitoring of IAM drift and privilege escalations.
5. Runtime security
    a. Continuous behavioural monitoring and anomaly detection of running containerised workload against the established baselines and rapid threat containment.
    b. Forensics and post-Incident analysis: Collection and analysis of runtime logs and forensics data to determine compromised entry point.
    c. Custom runtime policy tuning through refinement of access -list for running processes, network activity to minimize attack surface.
    d. Vulnerability remediation prioritisation through patch management of critical risks over non-exploitable vulnerabilities to reduce alert-fatigue.
    e. Compliance enforcement ensuring workload configurations are aligned to regulatory standards.
6. SecOps process integration: Integrating CNAPP alerts and data feeds into existing SIEM/SOAR platforms (e.g., Splunk, Sentinel) to centralize incident management and threat intelligence.
7. Remediation and governance:
8. Guided remediation providing expert analysis and step by step guidance for fixing alerts. Managing and optimizing workflow automation to automatically remediate common misconfigurations.
9. Monthly reporting for risk posture summaries and recommended remediation. Quarterly service reviews across policy tuning, roadmap alignment, and optimisation sessions.
10. Platform Health & optimization: Ongoing maintenance, upgrades, and feature optimization of the CNAPP platform to ensure maximum coverage and security across the cloud environments.

2.1.2.2 Cloud Security Assurance

Cloud Security Assurance provides organizations with comprehensive validation, testing, and certification of cloud environments and applications to ensure they meet security requirements, compliance standards, and industry best practices. This service area helps organizations implement a continuous security validation approach throughout the cloud lifecycle, identifying vulnerabilities, validating controls, and providing evidence-based assurance that cloud deployments maintain appropriate security posture.

Core Components of Cloud Security Assurance

1. **Cloud Security Assessment**
   - Architecture Review: Evaluation of cloud design against security best practices
   - Configuration Analysis: Identification of misconfigurations and security gaps
   - Security Control Validation: Testing effectiveness of implemented controls
   - Risk Assessment: Identification and prioritization of cloud security risks
   - Threat Modeling: Structured analysis of potential threats and attack paths
   - Compliance Mapping: Assessment against relevant regulatory frameworks
2. **Cloud Penetration Testing**
   - Infrastructure Testing: Identifying vulnerabilities in cloud infrastructure components
   - Application Security Testing: Assessing security of cloud-hosted applications
   - API Security Testing: Validating security of cloud service interfaces
   - Container Security Testing: Assessing vulnerabilities in containerized environments
   - Serverless Security Testing: Evaluating security of Function-as-a-Service deployments
   - Red Team Exercises: Simulated attacks against cloud environments
3. **Compliance Validation**
   - Regulatory Compliance Assessment: Validation against industry regulations
   - Cloud Security Frameworks: Assessment against standards (CSA, NIST, ISO, etc.)
   - Certification Preparation: Readiness assessment for formal certifications
   - Evidence Collection: Gathering documentation for compliance audits
   - Control Mapping: Correlation of implemented controls to compliance requirements
   - Compliance Reporting: Documentation of compliance status and remediation plans
4. **Security Automation & Continuous Assurance**
   - Automated Security Scanning: Continuous identification of security issues
   - CI/CD Pipeline Integration: Security validation within development processes
   - Security as Code: Programmatic validation of cloud security controls
   - Continuous Compliance Monitoring: Ongoing validation of compliance requirements
   - Drift Detection: Identification of unauthorized configuration changes
   - Automated Remediation: Self-healing capabilities for security findings

2.1.2.3 Zero Trust for Application Security

At NTT Cloud Security Services, we help enterprises modernize their application security posture with a Zero-Trust framework built on Tetrate Service Bridge (TSB). Our approach ensures every service interaction is verified, encrypted, and monitored, delivering consistent protection across hybrid and multi-cloud environments.

Zero-Trust for Application Security goes beyond perimeter defense and it embeds security into the fabric of your applications, giving organizations visibility, control, and resilience across every microservice and API.

Zero-Trust for Application Security with Tetrate TSB transforms your application ecosystem into a self-defending, compliant, and resilient environment. It's not just about security, but it's about enabling trust, speed, and confidence across every service interaction.

Features:

- Unified Zero-Trust Architecture: We deliver a cohesive security model that unifies service-to-service authentication, policy enforcement, and observability across all environments. With TSB, enterprises gain consistent control and centralised governance over every workload, no matter where it runs.
- Identity-Driven Access & Policy Control: Our model enforces strong workload identities (SPIFFE/SPIRE) and mTLS encryption, establishing mutual trust between services. Through fine-grained RBAC/ABAC policies and least-privilege enforcement, we ensure that access is both precise and adaptive. Cultural and Process Readiness: Zero-Trust demands strong collaboration between development, security, and operations teams. Organisations transitioning from perimeter-based security models must evolve their governance and process maturity.
- Intelligent Observability & Threat Detection: We enable end-to-end visibility into east–west traffic by leveraging AI/ML-powered analytics to detect anomalies and threats in real time. Integrated telemetry, runtime integrity checks, and XDR/SOAR integrations provide proactive defence and rapid response. Operational and Cost Considerations: Implementing Zero-Trust with full telemetry, encryption, and observability introduces initial overhead. Cost optimisation and tuning become essential as automation and maturity increase over time.
- Operational Resilience through Automation: From self-healing mesh policies to automated failover and continuous compliance verification, we ensure your applications stay secure and resilient—even during change or disruption. Our computerized workflows drive faster recovery and policy consistency. Legacy and Third-Party Integrations: Connecting legacy applications or non-native services to the mesh can be challenging. Some older systems lack SPIFFE/mTLS support, requiring custom adapters or phased modernization.
- Cloud-Native Integration with DevSecOps: We align with modern DevOps pipelines, embedding security controls directly into CI/CD processes. This enables developers to move faster with security-as-code, ensuring every deployment meets Zero-Trust standards without slowing innovation. Governance and Policy Lifecycle: Frequent updates and dynamic workloads demand strong policy lifecycle management. Without automated governance and drift detection, maintaining compliance and performance can become complex.

2.2 Crisis Response

Crisis Response provides rapid support during cybersecurity incidents such as ransomware or data breaches. Includes containment, forensics, recovery, communication, and post-incident reporting.

2.2.1 Overview

The NTT Digital Forensic Incident Response (DFIR) Retainer services assist an organization in effectively preparing, responding, containing, and rapidly remediating from a wide array of cyber incidents.

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:

(a) Magnet Axiom - Digital Investigation, Forensics & Reporting
(b) MixMode Network Sensor – Network Packet Capture
(c) Forensic Toolsets (FTK, EnCase, X-Ways, Axiom Cyber)
(d) Intella – Email Investigation & eDiscovery
(e) Cellebrite – Mobile Device Forensics

NTT may exchange this software and require the Client to execute a new End User License Agreement in its sole discretion.

2.2.2 Service Features

Feature	Description
Retained Hours	The number of retained hours that can be utilized for DFIR-related activities per year before additional hours are required.
Remote Incident Response[1]	Remote incident response 24x7x365 within SLO to initiate phone contact with the client from a DFIR consultant.
Forensic Data Storage	Forensic data, by default, will be stored for up to 90 days
Tool Deployment	Deploy and manage NTT investigation / forensic tools on endpoints, servers, network technologies, and mobile devices (if required)
Quarterly Check-ups	Quarterly checkups to establish if there have been major incidents or new technologies which are important to know prior to a DFIR engagement
Hour Conversion	The ability to convert unused retainer hours for additional IR-related services

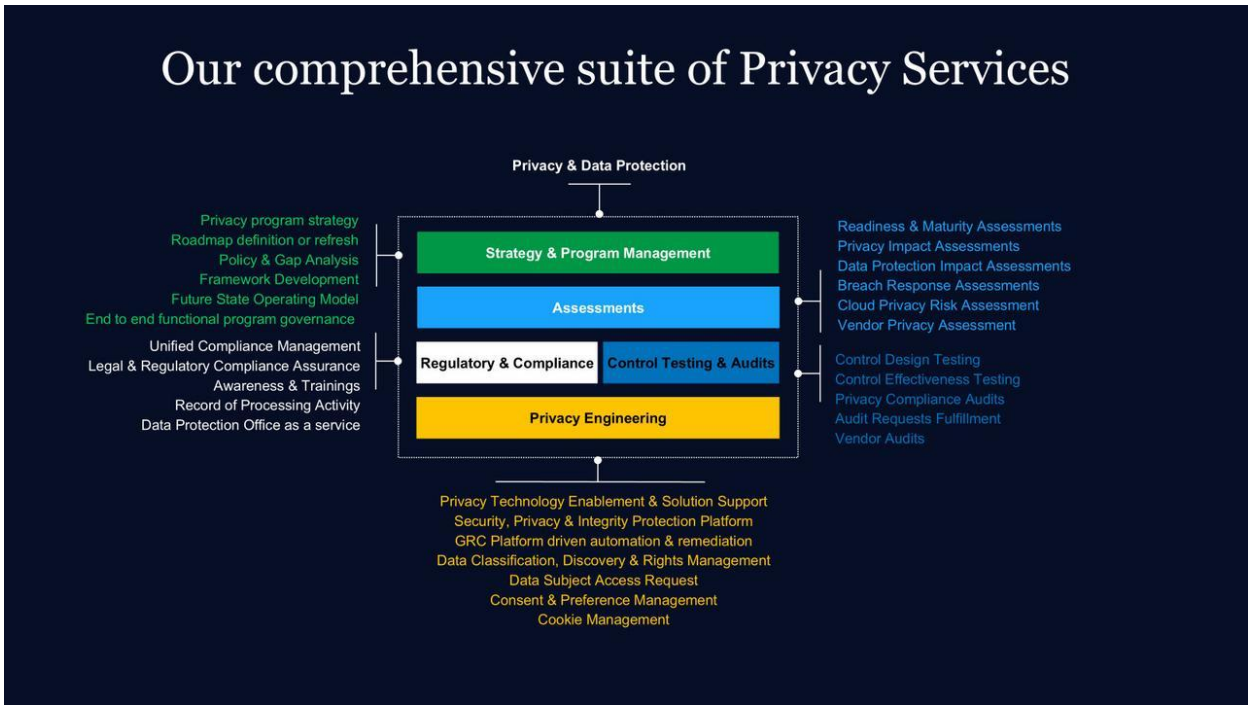
2.2.3 Supported Tasks

Task	Description
Incident Response Plan	Utilize NTT's standard incident response plan or if agreed upon by NTT, a client provided Security Incident Response plan for the duration of an incident
Onboarding & IR Plan Assessment	Remote onboarding session to understand the Client's network, estate and to agree on the IR processes & practices
Incident Response Identification	Collate log info on servers/endpoints or network technologies. Conduct rapid root cause analysis, and identify incident damage and residual risk. Maintain findings in line with client requirements.
Incident Containment	This may include the collection and analysis of volatile memory data, live acquisition, updating of managed endpoint protection systems, endpoint/server isolation, and tracking and enforcement of Indicators of Compromise.
Incident Eradication	Provide the client suggestions on how to handle and execute the eradication process.
Digital Forensics	Analysis to include forensic image (Windows / Linux), memory forensics, malware analysis, network forensics, or log file analysis as and when required.
Reporting	Provide final DFIR report including timeline and analysis findings and recommendations

2.3 Data Privacy Management

2.3.1 Overview

Through our extensive Privacy Services, NTT DATA partners with Clients to assess their privacy risks and regulatory landscape to help them develop an effective technology enabled privacy program that ensures compliance with evolving laws & regulations while managing user rights and mitigating risks across data life cycle. Our Privacy Services involve the practice of protecting personal, private, or sensitive information. It ensures that such information is collected with proper consent, kept secure, and used only for authorized purposes. We ensure that it includes control over personal data, applying security measures thereby meeting compliance with regulations and safeguarding consumer rights.



2.3.2 Service Specific Offerings

Privacy Strategy & Program Management

Our privacy strategy and program management services establish a strategic advisory partnership to help develop a robust framework for managing and protecting personal data, mitigating regulatory risks by aligning roadmap, policies, processes to business objectives and run the program. We define or refresh Client's strategic roadmap, design policies, perform gap analysis, develop future operating model. We provide a functional program governance service to client's data life cycle.

Privacy Assessments

Our services help assess the readiness and impact of client's current data privacy program. Through a meticulous assessment of client's current data landscape, we pinpoint opportunities for improvement and develop a roadmap for attaining a mature strategic data privacy program. Our comprehensive approach includes conduct privacy program readiness & maturity assessments, impact assessments, vendor assessments across all business dimensions aiding in establishing strategic roadmap for privacy maturity enhancement.

Privacy Regulatory & Compliance Management

Our regulatory & compliance management services provide for a unified compliance management tailored to client's risk appetite, to help a client respond to changing data protection laws & regulations, align to Industry standards and demonstrate strong commitment to privacy compliance.

Our DPO as a service offers cost effective and tailored data protection support, advice and expertise to client's business in ensuring regulatory compliance along with alignment to stakeholder and external authorities.

Privacy Control Testing & Audit Support

Our control testing and audit services provide for assessment of privacy policies and procedures and controls to determine correctness in design, effectiveness in implementation and intended operation. We provide reasonable assurance to ensure compliance and mitigate privacy and cyber risks.

Privacy Engineering

Through our privacy engineering services, we provide cutting-edge bespoke privacy technology solutions tailored to meet the unique needs of client's business. We embed security & privacy by design principles across the data life cycle, integrate platform driven solutions and harness privacy enhancing technologies for security, privacy and integrity protection for a client.

2.3.3 Engagement Model

Privacy services are delivered as consulting, advisory and managed services to our clients. The offerings, when delivered as advisory services enable the establishment of a strategic advisory partnership with our clients, while managed services help clients run, operate, and optimize their privacy programs and regulatory compliance posture on an ongoing basis.

Our integrated privacy engagement model brings to you our services, expertise, framework and platform. Our privacy service elements encompass full suite of Privacy Advisory & Consulting services, technical privacy solutions & managed privacy services delivered to clients.

2.4 Data Security

Data Security covers discovery, classification, encryption, tokenization, data loss prevention (DLP), insider risk mitigation, and access governance.

2.4.1 Overview

Data security is the practice of protecting digital information that are deemed as sensitive, critical, personal etc. from unauthorized access, corruption, or theft throughout its entire lifecycle. It encompasses a range of measures and strategies to ensure the confidentiality, integrity, and availability of data. Effective data security measures help organizations comply with legal and regulatory requirements, such as GDPR ,HIPAA, PCI-DSS etc. thereby avoiding hefty fines and legal repercussions. Additionally, robust data security safeguards against financial losses and reputational damage that can result from data breaches. In an era where cyber threats are constantly evolving, prioritizing data security is essential for the smooth and secure operation of any organization.

2.4.2 Service Specific Offerings

2.4.2.1 NTT Public Key Infrastructure

NTT's Public Key Infrastructure is a globally managed, cloud-delivered solution designed to simplify and strengthen digital trust for enterprises operating in hybrid, multicloud, and IoT environments. By combining NTT's global infrastructure and security expertise with the capabilities of a leading certificate authority, this service provides a comprehensive framework for secure identity management, encryption, and compliance without the complexity of traditional PKI deployments.

This Service offers fully managed root and subordinate certificate authorities, automated certificate lifecycle management, and centralized cryptographic key control backed by FIPS 140-2 Level 3 hardware security modules. It integrates seamlessly with enterprise systems, DevOps pipelines, and cloud-native workloads, supporting modern protocols such as ACME and EST for automated provisioning. The service includes robust governance and compliance features aligned with global standards like NIST and ISO, as well as regional mandates such as GDPR, HIPAA, and PCI DSS, ensuring audit readiness and regulatory adherence.

Delivered through NTT's resilient global network with 24/7 monitoring and high availability, PKIaaS provides advanced capabilities such as code signing, IoT device identity management, and future-ready support for post-quantum cryptography, enabling organizations to secure their digital ecosystems at scale. With its API-first architecture and automation-driven approach, NTT PKIaaS empowers businesses to reduce operational overhead, accelerate deployment, and maintain strong security posture across diverse environments—all while leveraging the trust and reliability of a globally recognized PKI framework.

Features:

- **Simplified Deployment**
  - Eliminates the complexity of setting up on-prem PKI infrastructure.
  - Rapid onboarding without specialized hardware or deep PKI expertise.
- **Global Scalability**
  - Supports large-scale certificate issuance for hybrid, multicloud, and IoT environments.
  - High availability through globally distributed infrastructure.
- **Automation & Integration**
  - Automated certificate lifecycle management (issuance, renewal, revocation).
  - Integrates with enterprise systems, DevOps pipelines, and cloud-native workloads.
- **Compliance & Governance**
  - Built-in adherence to global standards (NIST, ISO) and regional regulations (GDPR, HIPAA, PCI DSS).
  - Audit-ready reporting and centralized policy enforcement.

- **Advanced Security**
  - FIPS 140-2 Level 3 HSM-backed key management.
  - Support for modern protocols (ACME, EST) and future-ready post-quantum cryptography.
- **Cost Efficiency**
  - Reduces capital expenditure on hardware and PKI expertise.
  - Predictable subscription-based pricing model

2.4.2.2 Cryptographic Services

In today's hyper-connected world, data is everywhere—and so are the threats. Our Cryptographic Service is a next-generation solution that empowers organizations to secure, control, and manage their most sensitive data across any environment: on-premises, cloud, or hybrid.

Why This Service Stands Out

This isn't just key management—it's a comprehensive data security platform that delivers:

- **Confidential Computing**: Protect data even while it's being processed, using secure enclaves and runtime encryption.
- **Unified Key and Secrets Management**: Centrally manage encryption keys, secrets, and certificates across clouds and applications.
- **Cloud-Native Architecture**: Deploy anywhere—on-prem, in public cloud, or as-a-service—without compromising performance or control.
- **Zero Trust Security Model**: Enforce strict access controls, policy-based governance, and full auditability.
- **Developer-First APIs**: Seamlessly integrate with DevOps pipelines, CI/CD tools, and modern application stacks.

Features:

- **Unified Key Discovery and Mapping**
  - Automatically discovers encryption keys and maps them to data services across on-premises, cloud, and hybrid environments.
  - Provides a centralized view of cryptographic assets, enabling better visibility and control.
- **Cryptographic Security Posture Assessment**
  - Assesses the strength, usage, and compliance of cryptographic keys.
  - Identifies vulnerabilities and policy violations, helping organizations prioritize remediation
- **Quantum-Resistant Cryptography**
  - Supports CNSA 2.0 algorithms including CRYSTALS-Kyber and CRYSTALS-Dilithium, preparing clients for post-quantum threats
  - Enables crypto agility for seamless transition to quantum-safe algorithms.
- **Policy Compliance and Governance**
  - Enforces key management policies including key rotation, algorithm strength, and lifecycle management
  - Helps meet regulatory requirements like PCI DSS 4.0 and NSM-10 for cryptographic standards
- **Confidential Computing Integration**
  - Leverages Fortanix's Confidential Computing capabilities to protect data even during processing.
  - Ensures data remains encrypted and secure in memory, reducing exposure to insider threats.
- **Scalable Multi-Cloud Support**
  - Seamlessly integrates with Azure, AWS, GCP, and other platforms.
  - Ensures consistent cryptographic controls across diverse infrastructures
- **Crypto Agility and Automation**
  - Enables automated discovery, assessment, and remediation of cryptographic risks.
  - Supports rapid deployment of new cryptographic standards and protocols

2.4.2.3 Cyber resilience

With the NTT DATA's Cyber Resilience-as-a-Service Organizations will be equipped to defend their data and detect anomalies, monitor and respond to incidents and recover quickly when an incident such as Ransomware occurs.

Our Cyber Resilience-as-a-Service provides you with a single unified Zero Trust Data Security platform delivering the ability to have Data Resilience, Data Observability and Data Recovery with 24/7/365 monitoring and management wherever the data resides. This service is a Hybrid Data Security service and is available across Public and Private Clouds, as well as On-Premises and Data Centre environments.

NTT's Cyber Resilience solution features immutable backups to protect against ransomware, automated data protection for simplified management, and instant recovery to minimize downtime. It is highly scalable, handling large data volumes across hybrid and multi-cloud environments. Additionally, it supports regulatory compliance with secure, auditable data management, ensuring operational resilience and quick recovery from cyber threats

Features:

- Fully immutable backups from the original copy.
- Logical Air Gapping – No Open Protocols
- Encryption Everywhere
- Zero Trust by Design (MFA)
- Retention Locks and Two-Person Integrity
- Flexible Managed and Self-Managed backup service options supportive of hybrid IT environments, including cloud and colocation infrastructure
- Cost-effective cloud-based offering with no upfront costs and flexible billing options
- Secure environment compliant with strict industry regulatory requirements
- Scalable backup solution that protects ever-growing data sets of all types and applications
- Fast data recovery begins instantly, regardless of location
- Future-proofed IT infrastructure is continuously updated to provide a long-term backup solution
- Efficient cloud-based solutions eliminate the need for in-house IT staff to manage and maintain data storage using tapes or hard disks

2.4.2.4 Data loss Prevention

Data Loss Prevention (DLP) is a security strategy and technology designed to detect, monitor, and prevent the unauthorized movement or exposure of sensitive data. It ensures that confidential information—such as intellectual property, financial records, or personally identifiable information (PII)—remains secure and compliant, whether in use, in motion, or at rest.

DLP solutions leverage content inspection, contextual analysis, and policy enforcement to stop data breaches before they occur, giving organizations visibility and control over their most critical assets.

Features:

- **Comprehensive Data Protection** - Prevents unauthorized access, sharing, or exfiltration of sensitive data across endpoints, networks, and cloud environments.
- **Regulatory Compliance** - Helps organizations meet compliance requirements like GDPR, HIPAA, PCI DSS by enforcing data handling policies.
- **Visibility & Control** - Provides granular visibility into data flows and user behavior, enabling proactive risk management.
- **Policy Enforcement** - Automates enforcement of security policies to reduce human error and insider threats.
- **Real-Time Monitoring** - Detects and blocks suspicious activities instantly, reducing the risk of data breaches.
- **Integration with Security Ecosystem** - Works with SIEM, CASB, and other security tools for a unified defense strategy.

2.4.2.5 Data Security Posture Management

DSPM is an emerging category in data security that focuses on **discovering, monitoring, and** managing **the security posture of data across hybrid and multi-cloud environments**. It helps organizations understand where sensitive data resides, how it is accessed, and whether it is adequately protected.

Key Objectives of DSPM

- **Data Discovery & Classification**
  - Automatically identify sensitive data (PII, PHI, financial, intellectual property) across structured and unstructured sources.
  - Classify data based on sensitivity and compliance requirements.
- **Risk Assessment**
  - Detect misconfigurations, excessive permissions, and policy violations.
  - Identify shadow data stores and orphaned data that increase risk.
- **Continuous Monitoring**
  - Track changes in data posture over time.
  - Monitor access patterns and detect anomalies.
- **Compliance & Governance**
  - Map data to regulatory frameworks (GDPR, HIPAA, PCI-DSS).
  - Generate audit-ready reports for compliance teams.
- **Remediation & Response**
  - Provide actionable insights to fix misconfigurations.
  - Integrate with security orchestration tools for automated remediation

Features:

- **Comprehensive Data Visibility**
  - DSPM discovers **all data assets**, including shadow data and orphaned data, across **cloud, SaaS, and on-prem environments**.
  - Unlike traditional DLP or CSPM, DSPM focuses on **data itself**, not just endpoints or configurations.
- **Contextual Risk Analysis**
  - It combines **data sensitivity** (e.g., PII, PHI, financial data) with **exposure level** (permissions, sharing, encryption status).
  - Provides **risk prioritization** based on business impact, not just technical severity.
- **Continuous Monitoring**
  - Tracks changes in **data posture** over time.
  - Detects **anomalous access patterns** and policy violations in real-time.
- **Compliance Alignment**
  - Maps discovered data to **regulatory frameworks** like GDPR, HIPAA, PCI-DSS.
  - Generates **audit-ready reports**, reducing compliance overhead.
- **Agentless & Scalable**
  - Uses **API-based scanning** for cloud-native environments, avoiding heavy agent deployments.
  - Scales across **multi-cloud and hybrid architectures**.
- **Integration with Security Ecosystem**
  - Works alongside **CSPM, SIEM, DLP, and IAM** tools for a holistic security posture.
  - Enables **automated remediation** through orchestration platforms.
- **Proactive Risk Reduction**
  - Identifies **misconfigurations, excessive permissions, and unencrypted sensitive data** before they lead to breaches.
  - Supports **crypto-agility** and advanced encryption strategies (including PQC in future-ready architectures).

2.5 Emerging Technologies

Emerging technology focus is on securing AI-driven systems, including GenAI and Agentic AI, while embedding AI into cybersecurity operations to enhance enterprise resilience.

2.5.1 Overview

Emerging technology focus is on securing AI-driven systems, including GenAI and Agentic AI, while embedding AI into cybersecurity operations to enhance enterprise resilience. This includes building AI-powered, platform-based services to identify, mitigate, and manage AI-specific risks across the enterprise. The approach enables detection and response to both AI-focused and AI-powered threats, such as model abuse, data poisoning, and deepfakes. It also ensures alignment with evolving regulatory, governance, and responsible-AI compliance requirements.

2.5.2 Service Specific Offerings

2.5.2.1 Security for AI

NTT Data, a leader in AI cybersecurity, offers comprehensive end-to-end services to ensure AI regulatory compliance, mitigate risks, and safeguard AI workloads and data. Their solutions provide AI risk and compliance coverage, protecting AI systems and enabling clients to innovate without associated risks. NTT Data's services help identify AI risks, implement necessary guardrails, and continuously validate AI security posture.

- **AI Risk and Compliance Service**: Perform AI Risk and Impact assessment, ensuring regulatory compliance and mitigate risks in AI systems throughout their lifecycle.
- **AI Protection Service**: Safeguard AI workloads and data with advanced security measures and threat detection.
- **AI Assurance Service**: Guarantee the reliability and integrity of AI solutions through rigorous security validation and monitoring.

Value Differentiators

- **Secure AI Lab - CoE**: A turnkey Gen AI Security experimental playground designed to rapidly learn, experiment and define security strategy for Gen AI use cases.
- **Continuous AI Red Teaming**: Continuous Generative AI/LLM focused Red Teaming and Continuous AI Vulnerability assessment

Features:

- End-to-End Solutions: Governance, security, and assurance tailored to your AI maturity.
- Regulatory Mastery: Deep experience with EU AI Act, NIST, and ISO standards.
- Actionable Demos: See threats and solutions in real-time
- NCAP - AI Risk Assessment
- Secure AI Lab Service
- AI TRiSM Workshop for quick decision making.
- AI Red Teaming Service

2.6 Endpoint Security

Endpoint Security ensures protection across laptops, servers, mobile, and edge devices through EPP, EDR, hardening, compliance, and threat hunting.

2.6.1 Overview

Endpoint Security evolves safeguarding & fortification of the various types of IT endpoints (from Laptop, desktop, servers, tablets, MacOS, Mobile devices) with controls such as antimalware, white/blacklisting & encryption.

2.6.2 Service Specific Offerings

2.6.2.1 Managed Endpoint Detection Response

NTT DATA's Managed Endpoint Detection and Response (MEDR) service is designed to provide robust, end-to-end security for your organization's endpoints. Leveraging advanced technologies and expert support, our Managed EDR service ensures continuous protection against evolving cyber threats.

MEDR service integrates real-time monitoring, advanced threat detection, and rapid incident response to safeguard your endpoints. By combining machine learning, behavioral analysis, and proactive threat hunting, we identify and mitigate both known and unknown threats, including malware, ransomware, and zero-day attacks.

MEDR Platform and service

A modernised approach to detect, respond and investigate threats.

End-to-end platform and service delivery:

- Scalable, cloud-native platform for detection and response.
- Driven by security analytics services that integrate threat intelligence with data from sources across the enterprise.
- Integrates with our key strategic technology partner ecosystem.

Vendor-Agnostic Service:

The MEDR Design and Implementation Service assists you in architecting and deploying a comprehensive, ***vendor-agnostic*** Endpoint Detection and Response (EDR) solution tailored to your organization's security requirements. This service focuses on constructing a resilient infrastructure that enables robust threat detection and response capabilities across all endpoints, ensuring strong defense against cyber threats.

Vendor-Agnostic Platform:

- **Vendor-Agnostic Technology Stack***:* Utilize a Bring Your Own License approach to integrate various technologies seamlessly.
- **Enhanced Security***:* Ensure strong defense against cyber threats across all endpoints.
- **Native Sensors Deployment***:* Deploy sensors both on-premises and within the cloud to ensure comprehensive coverage.

2.6.3 Service Features

- **Comprehensive Security Coverage**: NTT's Managed EDR service offers 24x7 security monitoring and detection, leveraging advanced analytics to reduce the mean time to detect (MTTD) threats.
- **Advanced Threat Hunting**: The service includes security analyst-driven threat hunting capabilities, which help in the proactive investigation and disruption of attacks.
- **Automated Response**: Utilizing Security Orchestration Automation and Response (SOAR), NTT's service reduces the mean time to respond (MTTR) to incidents.
- **Endpoint Protection**: The service provides fully managed EDR, alert detection, and remote isolation capabilities, which can be rapidly deployed.
- **Threat Intelligence**: NTT integrates global threat intelligence to detect and disrupt sophisticated attacks, enhancing the overall security posture.

2.7 Infrastructure and Network Security

This service protects enterprise networks, data centers, and cloud infrastructures by implementing layered defences—segmentation and micro-segmentation, firewalls, WAF, IPS, NDR, and secure remote access—to prevent and contain cyber threats, secure application and data flows, and maintain availability. Guided by Zero Trust Network principles, it enforces least-privilege access and continuous verification for every connection, limiting lateral movement and ensuring only authenticated, authorized, and policy-compliant users, devices, and workloads can communicate with critical resources.

2.7.1 Overview

Infrastructure security focuses on protecting hardware, software, and underlying systems from unauthorized access and cyberattacks. Key strategies include:

- **Access Control & Authentication**: Using multi-factor authentication (MFA) and role-based permissions ensures that only authorized users access critical systems.
- **Network Segmentation & Micro-Segmentation (Zero Trust):** Dividing the network into controlled zones limits lateral movement and ensures users/workloads can access only the specific resources they're authorized to use.
- **Secure Remote Access:** Enforcing encrypted access (VPN/ZTNA), device posture checks, and least-privilege connectivity allows remote users and third parties to connect safely without exposing internal networks.
- **Threat Prevention & Traffic Inspection:** Next-generation firewalls, and WAF inspect and enforce policies on inbound/outbound traffic to block malicious activity, exploit attempts, and application-layer attacks.

Network security protects data in transit and prevents unauthorized access to networks. Leading services include:

Service Offerings	Services Description
Zero Trust Network Access (ZTNA) Management	• Provides secure, unified access for modern businesses. • Enables any user to access any application from any location. • Replaces traditional VPN technology by securing access to private business applications. Facilitates secure third-party, vendor, and partner access without extending network access or requiring an agent install.
Secure Web Gateway (SWG) Services	• Protects against malicious online threats. • Provides URL filtering and web reputation filtering. • Includes SSL/TLS inspection at scale for complete data security. • Offers malware scanning and AI-based sandboxing for unknown threats.
Micro-Segmentation	• Flexible Implementation Methodologies • Creates isolated network segments for granular traffic monitoring and control, significantly enhancing security.
Next-Gen Firewall	• Provides deep inspection and control of traffic. • Includes Intrusion Prevention System (IPS) capabilities. • Offers policy enforcement based on application ID, user ID, and device ID. • Facilitates network segmentation and micro-segmentation.
Web Application Firewall (WAF)	• Provides configuration and management of a web application firewall (WAF) • Creation and troubleshoot WAF rules, change/tune and deletion of rules on a per domain/URL policy basis

DDoS Protection	• Comprehensive Mitigation Services • Monitor alerts, traffic pattern recognition • Investigate potential DDoS attacks, rate-limiting • Build mitigation strategies, post-mortem analysis of attacks
Firewall Assurance	• Compliance checks, Reporting, policy management, rule set management • Design and implementation of assurance mechanisms
Email Security Service	• Defend against email borne threats • Automated inbound email scanning • Continuous protection against phishing attacks

2.7.2 Service Specific Offerings

2.7.2.1 Zero Trust Network Access

Zero Trust Network Access is a security framework designed to protect networks by implementing the principle of "never trust, always verify." It shifts away from traditional perimeter-based models, ensuring access to organizational resources is granted only after robust verification of identities, devices, and contexts.

Features:

- **Enhanced Security:**
  - The "never trust, always verify" principle significantly reduces the likelihood of breaches caused by insider threats or compromised accounts.
  - Micro-segmentation limits the scope of damage in case of an attack, as unauthorized lateral movement is blocked.
- **Scalability for Modern Workforces:**
  - ZTNA supports remote and hybrid work environments effectively by ensuring secure access regardless of user location.
  - Works well with cloud-based applications, facilitating modern operational models.
- **Granular Control:**
  - Enforces least privilege access, ensuring users and devices can access only what is necessary.
  - Focuses on application-level access instead of broad network access, reducing exposure.
- **Continuous Monitoring:**
  - Real-time analysis and anomaly detection help proactively identify and mitigate threats.
- **Flexibility with Third-Party Access:**
  - Provides secure access for vendors or contractors without compromising the overall network.

2.7.2.2 Managed SASE

NTT DATA's Managed SASE services are designed to protect our clients' business from cyber threats with a cloud-native and truly unified approach. Our Managed SASE Services consolidate multiple security services - such as secure web gateways, cloud access security brokers, and zero trust network access— into a single cloud-delivered solution and cover the entire lifecycle, from initial consultation and design to ongoing operation and optimization. Unlike traditional approaches that rely on a patchwork of separate tools, NTT DATA's Managed SASE services ensure cohesive security management and performance optimization from start to finish. Our Managed SASE Services simplify and accelerate SASE adoption, reduce cost and complexity, and increase organizational agility.

Key features**:**

- **Cloud-Native Security**: Our SASE solutions leverage cloud-native technologies to provide scalable and resilient security measures, ensuring your business is protected against evolving cyber threats.
- **Unified Approach**: By integrating network and security functions into a single service, we offer a seamless and cohesive security framework that enhances visibility and control.
- **End-to-End Services**: From initial consultation and design to implementation and ongoing optimization, our end-to-end services ensure a smooth transition and continuous improvement of your SASE environment.

2.8 Offensive Security

Offensive Security includes penetration testing, red teaming, social engineering, breach simulation, and attack surface management.

2.8.1 Overview

NTT Assurance Services empower clients by providing valuable security recommendations that safeguards their digital assets. Through meticulous vulnerability assessments and penetration testing for web, mobile, and API platforms, we identify and address potential threats before they can be exploited. Our source code analysis, including SAST and SCA, ensures that applications are secure from the ground up. With desktop application penetration testing, and infrastructure assessments, we offer a comprehensive approach to security, giving clients peace of mind and confidence in their digital operations. Our services help clients maintain a secure environment, protect sensitive data, and comply with industry regulations, ultimately enhancing their overall security posture

2.8.2 Service Specific Offerings

Task	Description
Vulnerability Assessment	Identify and evaluate security weaknesses in web, mobile, and API platforms.
Web Penetration Testing	Simulate attacks on web applications to uncover vulnerabilities and assess security posture.
Mobile Penetration Testing	Test mobile applications for security flaws and potential exploits.
Desktop Application Penetration Testing	Test desktop applications for security weaknesses and potential attack vectors.
Infrastructure Penetration Testing	Evaluate the security of network infrastructure, servers, and other critical systems.
Compliance Audits	Conduct audits to ensure adherence to industry regulations and standards.
Remote Security Assessments	Perform security assessments remotely using advanced digital tools and methodologies.
Remediation Support	Provide guidance and support for addressing identified vulnerabilities and implementing fixes within 90 days of final report delivery.

2.8.2.1 AI Red Teaming

AI Red Teaming is a specialized security assessment method that tests the strength, safety, and trustworthiness of AI systems, especially **Large Language Models (LLMs)** and agentic AI implementations, by mimicking real-world adversarial attacks. Unlike conventional testing, it emphasizes how AI reacts under manipulation, investigating vulnerabilities like prompt injection, hallucinations, logic bypasses, context poisoning, and data leaks. This process involves creating malicious or deceptive inputs to reveal unintended behaviors, policy violations, or security issues that could lead to financial fraud, impersonation, or denial of service. AI Red Teaming assists organizations in identifying emerging threats, strengthening defenses, and developing more resilient AI systems. It also incorporates tools, threat models (such as MITRE ATLAS, OWASP LLM Top 10), and red teaming techniques adapted from traditional cybersecurity practices, providing an essential perspective on the real-world risks associated with AI deployments.

Features:

- We deliver CREST-accredited offensive security, incident response, SOC optimization, and security architecture services across regions, ensuring globally recognized assurance and technical excellence.
- Our Global Red Team blends deep hands-on offensive security expertise with advanced AI threat research to conduct realistic, APT-style adversarial simulations targeting LLMs and agentic AI systems.
- Backed by $3.6 billion in annual global R&D spend, we have established advanced AI Security Testing Labs focused on cutting-edge research, tool development, and simulation of emerging AI threat scenarios.
- Our methodology is grounded in industry-leading frameworks such as MITRE ATLAS, OWASP LLM Top 10, and NIST AI RMF, enabling precise risk mapping and actionable mitigation through secure design and policy enhancements.
- Our Services are empaneled with key regulatory bodies, and we are authorized to deliver certifications and attestations including PCI SSC (QSA, ASV) and CERT-In, enhancing trust and compliance in regulated environments.
- Our AI red teaming services integrate directly into enterprise DevSecOps pipelines, enabling continuous testing, secure model deployment, and proactive risk mitigation without disrupting business workflows.
- With over 50 coordinated CVE disclosures, we have demonstrated a strong commitment to proactive security research, helping to shape global defenses through responsible vulnerability reporting and remediation insights.
- 5-phase adversarial assessment methodology tailored for AI security engagements.
- Continuous model monitoring and post-assessment support for regression testing and incident triage.
- Security-by-design advisory integrated into AI lifecycle, from model selection to production rollout.

2.8.2.2 Offensive Security as a Services

NTT DATA's **Offensive Security as a Service** provides a comprehensive approach to security testing, unifying all security testing activities on one platform. This service includes:

- **Cloud Configuration Review**: Detecting insecure cloud configurations that could lead to infrastructural compromise.
- **Infrastructure Assessments**: Simulating real-world attacks to identify and analyze security vulnerabilities within your infrastructure.

The platform automates routine tasks, enhancing the productivity of penetration testers and allowing them to focus on complex business logic vulnerabilities. It also incorporates an AI-enabled back-end engine for efficient automated scanning and recommends potential entry points or test cases based on application features and industry verticals.

The service offers several benefits, including:

- **Central Visibility & Control**: Real-time tracking of vulnerabilities, test progress, and remediation status.
- **Standardization & Consistency**: Facilitates repeatable and scalable testing processes.
- **Improved Efficiency & Automation**: Automates scheduling, execution, and reporting of tests, saving 30-40% in costs.
- **Advanced Analytics & Reporting**: Custom dashboards and detailed analytics to track KPIs and measure security posture over time

NTT Data has partner Astra Security to leverage their Penetration Testing as a Service platform, customized for our specific requirement.

The platform automates many activities in traditional pentesting lifecycle, and hence improves efficiency of our resources by eliminating repeatable task, allowing more time to discover complex vulnerabilities.

2.8.2.3 Vulnerability Management as a Service

NTT's Vulnerability Management as a Service (VMaaS) is a service that utilizes NTT's' Vulnerability Scanning platform for detecting vulnerabilities in a range of systems in an effort to assist the Client with effective remediation.

NTT's Vulnerability Scanning platform may require one or more of the following Technology configurations:

- Internal scanner
- External scanner
- Agent software
- Gateway server software

Service Tasks Included

Task	Description	Phase
Perform monthly **Internal** scan	Perform monthly credentialed internal vulnerability scan on internal IPs for assets listed in SOW for vulnerability scanning service.	**Discover**
Perform monthly **External** scan	Perform monthly external network-based vulnerability scan on Internet accessible IPs for assets listed in SOW for vulnerability scanning service.	
Vulnerability scanning reports	Generate monthly Vulnerability scan report.	**Assess**
Client Notification	Notify Client of vulnerabilities associated with unsupported or end of life systems.	
Portal	Generated reports available in the NTT Services Portal	
Vulnerability management and remediation reports	Generate monthly standardized Vulnerability management and remediation report.	**Prioritize**
Information Security Manager (ISM)	Client receives support from an Information Security Manager who works to improve the overall security posture of the Client. See *Information Security Manager* section below in this description.	
Monthly review	ISM reviews findings and recommendations with Client in a scheduled monthly meeting. All calls are held remotely and are scheduled during the normal business work hours of the ISM.	
Awareness and classification of Client systems	Understand the Client's business critical applications, tag them, and categorize assets into relevant groups.	
Prioritize vulnerabilities and remediation efforts	Help the Client to prioritize vulnerabilities and focus efforts on remediation based on organizational risk	
Maintain audit trail of non-remediated vulnerabilities	Maintain an audit trail of Client decisions regarding non-remediated vulnerabilities.	**Remediate**
Communications to asset owners	Provide communications to application and asset owner and/or operational risk manager to coordinate vulnerability risk mitigation and remediation.	
Remediation guidance	Provide remediation assistance for "Critical" and "High" rated operating system or managed application vulnerabilities for	

	NTT hosted or managed systems. "Critical" and "High" are defined per the Common Vulnerabilities and Exposures ("CVE") standard. • For systems managed by the Client or other 3rd parties NTT will provide the scanning vendors published remediation advice to the asset owners. • For systems managed by NTT on behalf of the Client, the relevant NTT team will perform remediation actions in accordance with the scanning vendors published remediation advice. The ISM will log tickets and work with the teams responsible for remediation through to completion.	
Validation of successful remediation actions	Perform a post remediation scan to confirm that remediation actions have been successful, and the vulnerability closed.	**Validate**
Remediation execution reporting	Information in the Vulnerability management and remediation report confirming validity of remediation actions. Confirmation will be provided in the standard monthly reporting cycle.	

2.9 OT-IOT Security

OT/IoT Security protects industrial systems (ICS/SCADA) and connected devices with asset discovery, segmentation, protocol-aware monitoring, and firmware security.

2.9.1 Overview

OT/IIoT security services provide specialised solutions & services, designed to safeguard Operation Technology (OT) & Industrial Internet of Things (IIoT) assets & networks. Ensuring the secure & uninterrupted operation of critical industrial systems & infrastructure.

2.9.2 Service Specific Offerings

2.9.2.1 OT secure Remote Access

OT Secure Remote Access Services provide industrial organizations with a controlled, hardened, and monitored mechanism for enabling remote connectivity to Operational Technology (OT) environments. These services ensure that engineers, technicians, and third-party vendors can access critical industrial assets safely—without exposing operational networks to cyber threats. Modern secure remote access solutions incorporate strong authentication, network segmentation, protocol isolation, and continuous monitoring to maintain operational integrity while supporting real-time industrial workflows.

Features:

- **Seamless User Access**: Delivering Unmatched Zero-Trust Secure User Access Without Disruptions Our Secure Remote Access (SRA) infrastructure is purpose-built to provide frictionless and compliant user access to OT environment and operational technology (OT) assets. SRA enables simple and secure remote operations to OT assets while protecting them from cyber threats posed by a distributed workforce including third parties. SRA allows users to quickly connect and manage critical infrastructure assets and systems from anywhere at any time.
- **Enabling Secure Remote Operations**: Our SRA service will reduce the dependency on less secure, complex, and outdated legacy technologies such as IPSEC VPNs and Jump Servers. Our SRA service is trusted by leaders in the chemical, energy, food & beverage, government, industrial machinery, manufacturing, oil & gas and transportation industries.
- **Scalable Secure User Access**: Our SRA platform has integrated a zero-trust framework comprised of multi-factor authentication, user-to- asset access controls, protocol isolation, user session analytics, and automatic video recording.
- **Zero Trust with Security by Design Approach**: Address shadow IT issues, insecure workarounds like risky password sharing. Delivers session moderation & auditing, Zero Trust by design, mature integrations & APIs, secure boot, dramatically reduces the network attacks surface, and breaks the cyber kill chain for malware and ransomware attacks

2.9.2.2 IT- OT convergence

- **Seamless System Integration:** IT-OT convergence represents the strategic alignment of Information Technology (IT) and Operational Technology (OT) systems. IT focuses on data processing, software applications, and network infrastructure, while OT governs industrial control systems (ICS), supervisory control and data acquisition (SCADA), and programmable logic controllers (PLCs). This integration facilitates bidirectional data flow, enabling unified management of digital and physical operations across enterprise ecosystems.
- **Optimized Operational Performance:** The convergence empowers organizations to harness OT-generated data—such as sensor readings and machine telemetry, within IT frameworks for advanced analytics, real-time monitoring, and process optimization. This results director leverages IT-OT integration to enable predictive maintenance, reduce unplanned downtime, and enhance overall equipment effectiveness (OEE), delivering measurable improvements in industries like manufacturing, energy, utilities, and transportation.
- **Scalable Digital Transformation Enablement:** IT-OT convergence forms the backbone of Industry 4.0 initiatives by supporting the deployment of transformative technologies such as the Industrial Internet of Things (IIoT), artificial intelligence (AI), and machine learning (ML). By providing a

cohesive platform for data aggregation and analysis, it enables scalable digital transformation, fostering innovation in areas like smart manufacturing, energy management, and intelligent logistics.

- **Robust Security and Compliance Framework:** The integration of IT and OT environments introduces complex security challenges, necessitating a unified cybersecurity strategy. A converged IT-OT framework implements zero-trust architecture, multi-factor authentication (MFA), and anomaly detection to mitigate risks such as ransomware and advanced persistent threats (APTs). Additionally, it ensures compliance with standards like IEC 62443 and NIST 800-82, safeguarding critical infrastructure and maintaining operational resilience

Features:

- **Enhanced Operational Efficiency**: Streamlines processes by integrating IT and OT systems, reducing manual interventions and improving productivity.
- **Real-Time Data Visibility**: Provides unified insights into operations, enabling better decision-making and predictive maintenance.
- **Cost Savings**: Reduces redundancy in systems and infrastructure, lowering operational and maintenance costs.
- **Improved Security Posture**: Combines IT cybersecurity practices with OT requirements, creating a more robust defense against threats.
- **Scalability**: Supports future growth by enabling flexible and adaptive infrastructure.

2.10 Threat Management

Threat Management delivers threat hunting, intelligence integration, malware analysis, and attack surface monitoring.

2.10.1 Overview

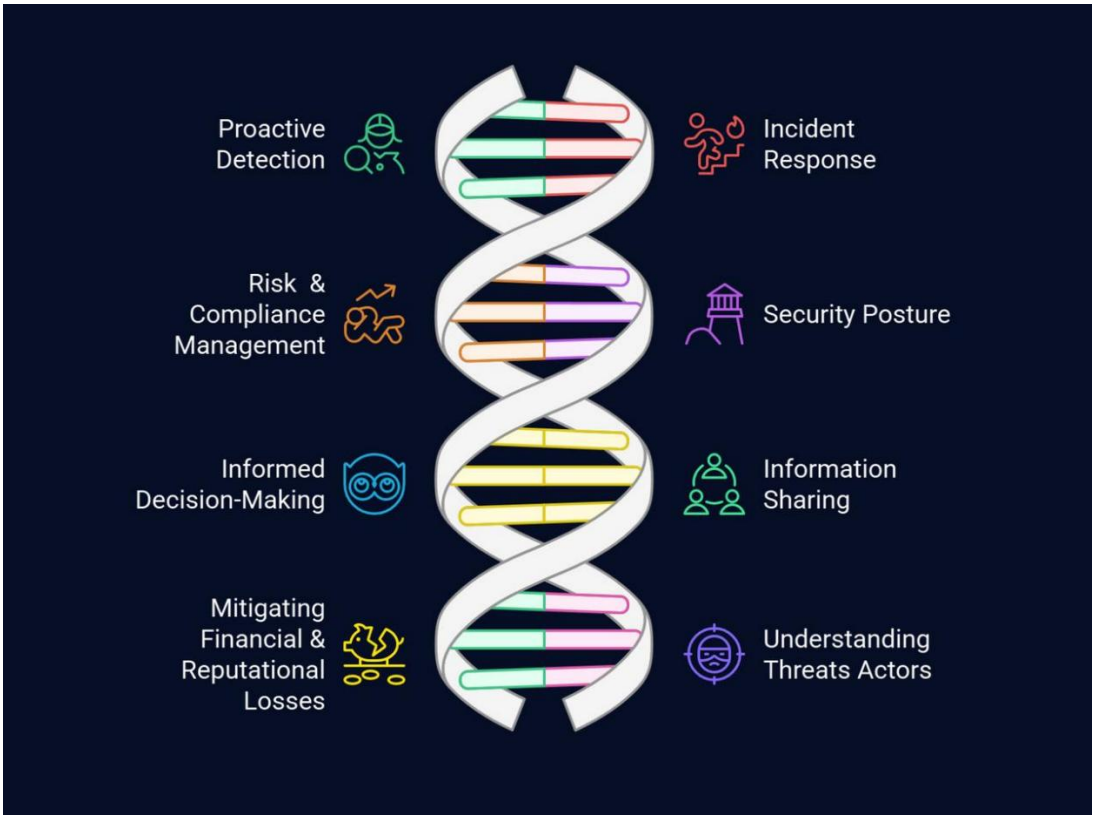
Are you ready to transform your security posture and stay ahead of evolving threats? Our comprehensive threat management solutions are designed to proactively mitigate risks, enhance your security, and ensure compliance with industry standards.

Our threat management services provide a strategic and systematic approach to identifying, assessing, and mitigating potential cybersecurity threats. We address the entire chain of attack, including Indicators of Compromise (IoCs), adversaries, vulnerabilities, Brand & Digitial risk protection, dark web insights, and AI-driven threat hunts.

2.10.2 Service Specific Offerings

2.10.2.1 Threat Intelligence

NTT DATA's Threat Intelligence offers proactive security, actionable insights, and enhanced collaboration, ensuring your organization stays ahead of potential threats. By investing in our CTI solution, you're not just enhancing your security posture; you're gaining a competitive edge and peace of mind. With cyber threats evolving rapidly, there's no better time than now to strengthen your defences



2.10.2.2 Brand & Domain Monitoring Plus Takedown

NTT offers two service levels for Brand & Domain Monitoring Plus Takedown service. The service level must be selected as In Scope in the SOW, otherwise all are out of scope.

Tasks legend:

- Tasks marked as ✓ are included in the service for the specified level.
- Tasks marked as ✗ are not included in the service for the specified level.

Task	Description	Gold	Platinum
Data gathering and project Kick-off	Gather information related to the customer requirements, assets and scoping the solution aligned to customer requirements one time	✓	✓
Phishing Protection	The detection and alerting of domains involved in phishing email campaigns, client look-alike domains and subdomains that can be used deceive online users.	✓	✓
Domain Monitoring	Monitors, analyses and alerts the client to registered domains that impersonate a client that could be used in a malicious attack against the client, its customers or supply chain	✓	✓
Domain Takedown	Manual or automated take down of malicious domains that have been identified as malicious.	✗	✓
Social Media Monitoring	Continuously monitor major social media sites like Facebook and Instagram for brand infringement and provide alerting capabilities.	✗	✓
Malicious Social Media Takedown	Utilize takedown processes to remove malicious social media content that infringes on the clients brand. (pre agreed legitimate social media sites to be provided by the client)	✗	✓
Brand Impersonation Detection	Search and neutralize unauthorized brand affiliations, and rogue applications registered in App Stores globally. Search engine scanning to identify brand affiliations and malicious adverts used to mislead potential clients	✗	✓

2.10.2.3 Digital Risk Protection Service (DRPS)

NTT offers two service level for the DRPS offering. The service level must be selected as In Scope in the SOW, otherwise all are out of scope.

Tasks legend:

- Tasks marked as ✅ are included in the service for the specified level.
- Tasks marked as ❌ are not included in the service for the specified level.

Task	Description	Gold	Platinum
Leaked Data Detections (Gold)	Identify leaked data across the surface, deep and dark web (Monitor up to 100 domains and 5 brand names)	✅	❌
Credential Monitoring	Identify clients leaked credentials (passwords and / or usernames), provide alerting capabilities to enable Client credential resets.	✅	✅
Social Media Data Leakage	Monitor the client's social media presence for malicious use or brand infringement and inform the client.	✅	✅
Code Repository Leakage	Monitor all official code repositories for detected leaks and provide alerting capabilities to the client.	✅	✅
Deep / Dark Web Monitoring	Provide monitoring capabilities across the surface, deep and dark web. Monitoring capabilities cover; social media, typo-squatting, messaging platforms, dump & paste sites, search engine adverts, data breaches and news & blog channels.	✅	✅
3rd Party Breach Notification (Gold)	Monitor and provide alerting for a clients critical suppliers (**up to 20**) that have been breached.	✅	❌
Bespoke Alerting, Scoring & Recommendations	Generate bespoke, prioritized reports that detail the specific risks attributed to a client's organization over the month. Findings are prioritized, and specific recommendations are provided to enable the mitigation / reduce the threat severity.	✅	✅
Leaked Data Detections (Platinum)	Identify leaked data across the surface, deep and dark web (Platinum 250 domains, 10 brand names)	❌	✅
3rd Party Breach Notification (Platinum)	Monitor and provide alerting for a clients critical suppliers (**up to 50**) that have been breached	❌	✅

2.10.2.4 Tailored Threat Intelligence (TTI)

NTT offers two service level for the TTI service. The service level must be selected as In Scope in the SOW, otherwise all are out of scope.

Tasks legend:

- Tasks marked as ✅ are included in the service for the specified level.
- Tasks marked as ❌ are not included in the service for the specified level.

Task	Description	Gold	Platinum
Sector Aligned Threat Alerts	Filtered alerts that are ranked by severity for each client. Each alert contains an overview, severity rating, Traffic Light Protocol (TLP), source, intelligence analysis, assessment and recommendations. Where appropriate Indicators of Compromise (IOCs), associated alerts/profiles and comments are also provided.	✅	✅
Threat Actor Operations	A view of an overall operation by specific threat actors against either an entity, sector or nation.	✅	✅
Threat Actor, Tactics, Techniques & Procedures (TTPs) Updates	Provide an in-depth analysis of threat actors (nation state, organized crime groups, hackers, hacker groups, hacktivists), including their usual tactics, techniques and procedures (TTPs), related tools and malware, incidents and associated profiles.	✅	✅
Cyber Significant activities (SIGACTS)	Provide a view of a malicious event against a specific organization(s), government agency or military department, this includes the: who, what, when, where, and why (5Ws) of attacks related to a cyber incident.	✅	✅
RFI Support	8 hours of direct support monthly through 'Requests for Information' where the Client can request information from CTI consultants and analysts about the provided intelligence under this Statement of Work	❌	✅
Consolidated Threat Reports	Provide a monthly bespoke threat intel report. This report may contain: • Bespoke, organizational specific alerts (brand, leaked creds etc) and documents, • The client's monthly incidents, • The wider threat landscape specific to the client. • What are the threat levels for the client's region and sector. • Provides an overview of the client's threat landscape.	❌	✅
Annual Threat Assessment of Clients threat landscape	An analysis and threat assessment developed via the fusing of threat intelligence and red team techniques. This service develops threat scenarios that can be used to test a Client's organizations defense posture against a real-world attack, linked to specific threat actors targeting a Client's industry vertical within a given geo-location. Red team testing is out of scope for this service.	❌	✅

2.10.3 Reporting

2.10.3.1 Brand and Domain Monitoring Plus Takedown Reports

Reports Summary	Reports
Alerting Information: *Phishing Protection, Domain Monitoring, Social Media Monitoring*	Alert information generated upon detection and published on the NTT portal or PAN XSIAM Threat Intelligence Platform[1]. Phishing Protection & Domain Monitoring alerts will contain; automated alerts of newly registered domain variants, certificate variants, domains containing client's brands. automated updated alerts if/as the threat changes Alerts for malicious social media sites will contain daily automated alerts of imposter domains infringing the client's brand. Alerts for malicious brand impersonation will contain daily automated alerts of imposter apps and adverts infringing the client brand.
Takedown Service	The domain takedown service and brand impersonation will provide daily automated alert updates confirming take down requested and alert updates until the domain or fake application take down is successful.

2.10.3.2 Digital Risk Protection Service Reports

Reports Summary	Reports

Alerting Information: *Leaked Data Detection, Credential Monitoring, Social Media Data Leakage, Code Repository Leakage, Deep Dark Web Monitoring, 3rd Party Breach Notification*	• Alert information generated upon detection and published on the NTT portal or PAN XSIAM Threat Intelligence Platform[1].
	• Automated alerts upon detection. Each alert is to contain a severity score assessment and remediation recommendations.
	  ○ Credential Monitoring: Alerts of client Credentials breached and leaked by malware, infostealers, client or 3rd party breaches
	  ○ Social Media Leakage: Alerts of client of brand abuse on Social Media.
	○ Code Repository Leakage: Alerts of client leakage via repositories shared via scoping exercise.
	• Leaked data detection provides daily automated alerts of client data (when associated to brand of domain) included in data breaches or for sale.
	• Third party breach notification provides daily automated alerts of client mentions in 3rd party breaches or breaches of 3rd parties on the scoping document.

[1] *Automated Alerts are sent as new threats are detected. This may be multiple times per day or every few days, depending upon cadence of breaches.*

2.10.3.3 Tailored Threat Intelligence Reports

Reports Summary	Reports
Sector Aligned Threat Alerts	• Automated Alerts of Threat aligned to or relevant to the sectors the client operates in.
Threat Actor Operations	• Automated Operation Updates of Threat Actor or Malware Operations that are relevant to the customer or globally significant events
Threat Actor, Tactics, Techniques & Procedures (TTPs) Updates	• Monthly Alerts to updates in Actor TTPs. • *Continuous Access to Threat Actor Profiles for those who have ThreatMatch Access**
Cyber Significant activities (SIGACTS)	• Automated Alerts and updates to Significant Events in Region, Sector or Globally Important
RFI Support	• Ah-Hoc short form reports as requested by the client, specific to their Intelligence Requirements.
Consolidated Threat Reports	• Monthly Intelligence Report specific to the clients Threat landscape and alerting.
Annual Threat Assessment	• Threat Assessment of the entities threat landscape • Client specific threat scenarios to be generated utilizing threat intelligence and client specific risk appetite data.

**Client must acquire all three threat intelligence services Brand and Domain Monitoring, DPRS and Tailored Threat Intelligence to gain direct access to the Threat Match portal*

2.11 Unified Detect and Response

UDR/XDR unifies telemetry from endpoint, cloud, identity, and network for correlated detections, automated response, and reduced dwell time.

2.11.1 Overview

Application Security services help organizations design, develop, and operate applications that are secure by default. This includes secure SDLC implementation, code reviews, threat modelling, penetration testing, DevSecOps integration, and continuous assurance.

2.11.2 Managed Detection and Response

2.11.2.1 Overview

NTT's Managed Detection and Response (MDR) is a turnkey service focused on quickly detecting and effectively responding to cybersecurity threats, using advanced analytics, threat intelligence, expert-driven threat hunting and validation capabilities.

NTT will deploy Required Operational Technologies and Optional Operational Technologies as required and necessary used exclusively for the delivery of the MDR Service in the Client's Azure environment within the specific limits as specified in the SOW Service Offering table, except as required in the Client Responsibilities section.

2.11.2.2 Operations Offerings

NTT offers three Service Tiers for MDR.

The service Tier must be selected as In Scope in the SOW, otherwise all are out of scope.

Tasks legend:

- Tasks marked as ✅ are included in the service for the specified Service Tier.
- Tasks marked as ❌ are not included in the service for the specified Service Tier.

Task	Description	Silver	Gold	Platinum
Ingest Data from Log and Event Sources*	Support the ingestion of data from a range of technologies and services as log and event sources as provided by NTT from time to time. Monitor log feed for log ingestion failure.	✅	✅	✅
Data Retention	Retain Analytics Logs for in scope devices for ninety (90) days from the date of transmission to NTT. Retain Alert and Incident data for 18 months from the date of creation.	✅	✅	✅
MDR Incident Detection	Provide 24 x 7 MDR incident detection. Alerts created by the MDR platform, based on the severity of the alert a ticket will be logged in NTT ITSM with a notification to Client, upon NTT's determination in its sole and absolute discretion that an alert requires a ticket.	✅	✅	✅
MDR Incident Report	Provide Client with a MDR Incident Report that includes a detailed description of the threat, identified activity combined with a recommendation of suitable incident response steps to take. Further updates to the MDR Incident are updated on the Services Portal.	✅	✅	✅

Information Security Manager (ISM)	Provide a subject matter expert in cyber security, with a strong operational focus ensuring value realization of the MDR service. The ISM supports Client as part of a long-term relationship which enables the ISM to develop a deep understanding of the Client's environment and business. ISM support includes: • MDR incident escalation point • Major incident support between NTT and the Client • Optimization recommendations	✓	✓	✓
Monthly Service Report	Provide Client with a monthly service report which include extracts from Sentinel Workbooks, Services Portal Widgets, and ITSM incident summary.	✓	✓	✓
Monitoring	NTT shall monitor the health of deployed system components using native and 3rd party tooling, which shall include at a minimum heartbeat functionality of the agent installed on syslog forwarders in order to ensure at regular intervals of at least every 30 minutes the system is alive (unless otherwise agreed with the Client). In the event that NTT becomes aware of downtime or other technical issue which adversely affects NTT's ability to deliver the In Scope services within Client's Azure subscription or on other Client managed infrastructure NTT shall make commercially reasonable efforts to notify the Client Contract Executive.	✓	✓	✓
Response Action	A Response Action will be performed if the following are met: • The technology that requires the Response Action has the capability of NTT performing the action; • NTT has been granted the appropriate access by the Client; • Client has completed the required consent and documentation; and • NTT has detected an MDR Incident in its' sole and absolute discretion that requires a Response Action. Otherwise, all Response Actions are out of scope. A Response Action for a Client under this Service Description shall be limited to restriction on the flow of traffic through a device which manages traffic through the environment.	✓	✓	✓
Digital Forensics and Incident Response	Provide up to twenty-five hours of DFIR support per contract year, which includes the following: • 24 x 7 on-call service • 4-hour Contact Response • Provide remote support and coordination with security and/or IT staff and management to accomplish incident response activities • Provide expert guidance on eradication and recovery • Correlation analysis across various supported and unsupported log sources • Evidentiary compliant handling with chain of custody • Forensic data storage up to 30 days, which shall be in one of the following: Australia, America or the United Kingdom.	✓	✓	✓

	• Expert digital forensic imaging and analysis on most platforms including mobile, at NTT's sole and absolute discretion • Memory forensics • Review and analysis of various Attack Sensing and Warning (ASW) technologies and related log and network data applicable to the active threat in the environment • Malware reverse engineering • Provide final DFIR report including timeline and analysis findings and recommendations • NTT may provide endpoint detection response tools temporarily to support DFIR investigative activities upon agreement of any required End User License Agreements.			
Use Case Tuning	Tune existing Use Cases for supported sources, to reduce false positives, based on emerging threats, updates to the watchlist and results from threat hunting.	✓	✓	✓
Quarterly Service Review Meeting	Client meetings with ISM to review monthly reports and discuss overall service performance and discuss additional features and roadmap for client.	✗	✓	✓
MDR Incident Management	24 x 7 security analysts validate and investigate threats, suspected threats and notify Client through the Services Portal. NTT may contact Client by telephone for Severity 1 or Severity 2 MDR Incidents. Where applicable, the security analyst will initiate a Response Action.	✗	✓	✓
Check Event Distribution	Compare data source event distribution against historical trends. Associate specific changes linked to seasonal events. Identify risk impact on the Client and provide the ISM with a breakdown of the events.	✗	✓	✓
Threat Hunting	Security analyst proactively and iteratively search through logs to detect and isolate advanced threats that evade existing use cases and existing security solutions using threat intelligence data.	✗	✓	✓
Custom Use Case Tuning	Create Client custom detection rules (up to 10 per year) for specific cases based on Client requirements as deemed reasonable by NTT in its sole discretion.	✗	✗	✓
Targeted Threat Hunting	Investigate and identify patterns on data collected for a specific industry or region (up to 24 per year and no more than 2 per month). Security Analysts review and analyze logs in the LAW and conduct comparisons against new threats and industry specific threats, hunting for any anomalies in a client's environment.	✗	✗	✓
Update Special Handling Notes	Quarterly update special handling notes for Client Security Incident Notification and Management.	✗	✗	✓

2.11.2.3 NTT Service Portal

The MDR system integrates with the provided NTT Services Portal and allows the Client to view interrogate and leverage MDR dashboards and MDR incident reporting. Select dashboards, information and alerts may be linked to or provided within the Client Azure Tenant. NTT reserves the right to update the NTT Services Portal and provide additional functionality in the future using either the Client Azure Tenant or a Third Party Provided Application which shall provide at least substantially similar or enhanced functionality.

2.11.2.4 Optional Extended Log Management Services

Client must expressly select Extended Log Management Services in the SOW as in-scope otherwise they are expressly out of scope.

- Log Analytics Workspace Data Retention up to two years.
- Log Analytics Workspace Data Archive up to seven years.

2.11.2.5 Information Security Management

Information Security Management is a component of NTT's Managed Detection and Response (MDR) Service delivered by a designated individual. The key functions of Information Security Management include:

- Interpret MDR security information potentially to identify trends and make recommendations.
- Support appropriate business, security, and technical reviews as part of the regular Service Management cadence as detailed below in Coverage.
- Support for Severity 1 and Severity 2 MDR Incidents and provide recommendations on response options up to the provided limits Coverage section.

The primary responsibilities of the Information Security Manager (ISM) include:

- Advise on service optimizations through additional log sources, feeds and intelligence as required to maintain Client service quality.
- Communicate any changes in Client environment/network that will impact the MDR service.
- Perform reviews of the MDR service against Client security objectives annually.
- Function as final escalation point for technical service-related issues and MDR Incidents requiring additional support after the standard ticket process has been followed.
- Engage with other NTT security teams as required (e.g., MDR Incident Response, Digital Forensics and Incident Response, Cyber Threat Intelligence and Threat Vulnerability Management).
    - Review alerts and advisories from NTT and other Threat Intelligence sources to determine the applicability of the vulnerability to Client's environment and provide advice on actions.
    - Provide potential security insights and recommendations based on evolving threats.
    - Form part of escalation team for technical escalations during Business Hours.

2.11.3 Managed Extended Detection and Response

NTT’s Managed XDR is a holistic offering securing the enterprise and providing rapid detection and effectively responding to cybersecurity threats, using advanced analytics, threat intelligence, expert-driven threat hunting, automation, and validation capabilities.

Required Operational Technologies for the Managed XDR Service provided by Client:

- Palo Alto Networks XSIAM Base
- Either Palo Alto Networks XSIAM Enterprise or XSIAM Enterprise & Cloud

2.11.3.1 Service Specific Offerings

NTT offers three service levels for Managed XDR. The service level must be selected as In Scope in the SOW, otherwise all are out of scope.

Tasks legend:

- Tasks marked as ✅ are included in the service for the specified level.
- Tasks marked as ❌ are not included in the service for the specified level.

Task	Description	Silver	Gold	Platinum
Data gathering and project Kick off	Gather information related to the Client requirements, assets and scoping the solution aligned to Client requirements which may only be performed once	✅	✅	✅
Platform Deployment Management	Deploy and Configure the XSIAM management platform and components which may only be performed once	✅	✅	✅
Agent and log forwarder Deployment Management	Support in the deployment of the XDR & EDR agents, log forwarders and perform testing to ensure data is correctly being received into the MXDR platform. Provide the client with the EDR agent (license provided by Client) and liaise with the client to enable the agent to be uploaded to the Client's software distribution tool (Intune / SCCM (Microsoft Endpoint Configuration Manager (MECM)) as example) for the client to deploy.	✅	✅	✅
Ingest Data from Log and Event Sources*	Support the ingestion of data from a range of supported technologies and services which maybe updated from time to time. Monitor log feed for log ingestion failure.	✅	✅	✅
Data Retention	Retain ingested raw data for 30 days within the XSIAM platform, alert and incident data for 180 days and forensic data for 90 days. Data storage is only applicable for devices that are in scope. Incident and alert data are retained according to the last Update Date and Creation Date, respectively.	✅	✅	✅
System Monitoring	NTT shall monitor the health of deployed NTT system components using native and 3rd party tooling, which shall include at a minimum, heartbeat functionality of the agent installed on syslog forwarders in order to ensure at regular intervals of at least every 30 minutes the system is alive (unless otherwise agreed with the Client). In the event that NTT becomes aware of downtime or other technical issue which adversely affects NTT's ability to deliver the In Scope services within Client's Palo Alto XSIAM subscription or on other Client managed infrastructure NTT shall make commercially reasonable efforts to notify the Client	✅	✅	✅
Incident Detection	Provide 24 x 7 incident detection and endpoint detection generated by the XDR agent on the device. Alerts created by the Managed XDR platform based on the severity of the alert, a ticket will be logged in NTT ITSM with a notification to Client, upon NTT's determination in its sole and absolute discretion that an alert requires a ticket.	✅	✅	✅

Endpoint Detection & Response Policy Management	Utilize the pre-defined EDR policies that are included within the XDR platform to control the behavior of the agent on each device providing a more tailored EDR experience aligned to the Client requirements. Maintain and configure EDR policies and exclusion policies for specific assets and applications upon reasonable Client request up to NTT's reasonably determined limits. Work with the Client to provide ongoing optimization and policy changes to reduce the number of false positives.	✓	✓	✓
Response Action	A Response Action will be performed if the following are met: • The technology that requires the Response Action has the capability of NTT performing the action; • NTT has been granted the appropriate access by the Client; • Client has completed the required consent and documentation; and • NTT has detected an MXDR Security Incident in its' sole and absolute discretion that requires a Response Action. Otherwise, all Response Actions are out of scope. A Response Action for a Client under this Service Description shall be limited to restriction on the flow of traffic through a device which manages traffic through the environment. Response Action means an action taken by NTT in response to an analysist confirmed MXDR Security Incident that impacts a Client system.	✓	✓	✓
Endpoint Remote Isolation	Perform remote actions for isolation of compromised / malicious hosts following security analyst validation only for Endpoints with the Cortex XDR agent installed and managed and in accordance with the acceptable task list provided by Client	✓	✓	✓
Digital Forensics and Incident Response	Provide up to twenty-five hours of DFIR support per contract year, which includes the following: • 24 x 7 on-call service • 4-hour Contact Response • Provide remote support and coordination with security and/or IT staff and management to accomplish incident response activities • Provide expert guidance on eradication and recovery • Correlation analysis across various supported and unsupported log sources • Evidentiary compliant handling with chain of custody • Forensic data storage up to 30 days. • Digital forensic imaging and analysis on most platforms including mobile, at NTT's sole and absolute discretion • Memory forensics • Review and analysis of various Attack Sensing and Warning (ASW) technologies and related log and network data applicable to the active threat in the environment • Malware reverse engineering	✓	✓	✓

	• Provide final DFIR report including timeline and analysis findings and recommendations			
Standardized Playbooks	Activation and deployment of playbooks that are provided within the XSIAM technology stack enabling incident detection, response and remediation automation.	✓	✓	✓
MXDR Incident Management	24 x 7 security analysts validate and investigate threats, suspected threats and notify Client through the Services Portal. NTT may notify a Client by telephone or Microsoft Teams for Severity 1 or Severity 2 MXDR Incidents only. Where applicable, the security analyst will initiate a Response Action.	✓	✓	✓
MXDR Incident Report	Provide Client with an Incident Report that includes a description of the threat, identified activity combined with a recommendation of further incident response steps to take. Further updates to the Incident are updated on the Services Portal.	✓	✓	✓
Information Security Manager (ISM)	Provide a subject matter expert in cyber security, with a strong operational focus ensuring value realization of the Managed XDR service. The ISM supports Client as part of a long-term relationship which enables the ISM to develop an understanding of the Client's environment and business. ISM support includes: • Managed XDR incident escalation and communication point • Major incident support during ISM's business hours between NTT and the Client	✓	✓	✓
Monthly Service Report	Provide Client with a monthly service report which may include: • Overview of service status, SLA compliance, high risk observations and trends within the client environment. • EDR compliance reports and remediation recommendations Additional security services recommendations aligned with the client's threat profile.	✓	✓	✓
Portal Access	Client access to a unified portal that will act as a single interface point enabling for example security incident reports, ticket management, document sharing etc.	✓	✓	✓
Threat Hunting	NTT Threat Hunters will search through the ingested logs to detect and isolate advanced threats. This threat hunting is triggered by a security incident, threat intelligence or a new security advisory.	✓	✓	✓
Quarterly Service Review Meeting	Client meetings with ISM to review monthly reports and discuss overall service performance and discuss additional features and roadmap for client.	✗	✓	✓
XSIAM Addon Modules	Provide additional managed service capabilities for XSIAM addons which include; Threat Intelligence Management and Digital Forensics and Incident Response at an additional cost and all licenses must be provided by the Client.	✗	✓	✓

Notification & Detection Playbooks (Gold)	Create and deploy up to 10 customized playbooks per year for supported sources, detection alerts, reduce false positives, based on emerging threats, updates to the watchlist and results from Threat Hunting as deemed reasonable by NTT in its sole discretion.	✗	✓	✗
Targeted Threat Hunting (Gold)	Upon client request, investigate and identify patterns on data collected for a specific industry or region (up to 10 per year and no more than 2 per month). Security analysts review and analyze log data and conduct comparisons against new threats and industry specific threats, hunting for any anomalies in a client's environment upon client request.	✗	✓	✗
Notification, Detection and Response Playbooks (Platinum)	Create and deploy 20 customized playbooks per year for supported sources, detection alerts, reduce false positives, incident response based on emerging threats, updates to the watchlist, results from threat hunting and threat intelligence.	✗	✗	✓
Targeted Threat Hunting (Platinum)	Upon client request, investigate and identify patterns on data collected for a specific industry or region (up to 24 per year and no more than 2 per month). Security analysts review and analyze log data and conduct comparisons against new threats and industry specific threats, hunting for any anomalies in a client's environment upon client request.	✗	✗	✓
Phishing Protection	Provide detection and alerting of domains involved in phishing email campaigns, client look-alike domains and subdomains that can be used deceive online users and notify the client.	✗	✗	✓
Domain Monitoring	Monitor, analyze and alert the client to registered domains that impersonate a client that could be used in a malicious attack against the Client	✗	✗	✓
Threat Intelligence – Sector Reporting	Generate threat report by pulling Threat alerts, Threat Actor updates & TTPs, and significant events that may impact the Client	✗	✗	✓
Attack Surface Management	Monthly threat exposure reporting that contains prioritized threat scores of risky client assets, automated resolutions (via playbooks) and benchmark against other organizations*. ISM meeting to run through and contextualize the threat report in conjunction with the client risk appetite and security posture prioritization.	✗	✗	✓

***Playbook Defined**: a series of tasks, conditions, automations, conditions, commands, and loops that run in a predefined flow to save time and improve the efficiency and results of the investigation and response process.

Attack Surface Management (ASM) (Platinum Clients Only)

The management of Palo Alto Network's Attack surface management solution is included at no extra cost for Platinum clients. The client is responsible for acquiring the license from Palo Alto before any management services can be deployed.

Task	Description	Silver	Gold	Platinum
Digital Asset Library	Provide accurate inventory of clients digital assets and provide a report including what is connected to the network, where it is located, and its current state.	✗	✗	✓
Un-associated Responsive IPs	Provide a list of IP addresses that may pose a security risk but are not yet linked to specific assets.	✗	✗	✓
Asset Certifications	Identify certificates attributed to the Clients organization and whether the certificate advertised recently, misconfigures or up for renewal.	✗	✗	✓
Organizational Domains	Provide a list view of all domains that attributed to the Client's organization and whether each domain has a recent resolution.	✗	✗	✓
External Services	Provide an inventory of all of the public internet-facing services attributed to the Client's organization. An external service can be any internet-facing device or software that communicates on domain:port or IP:port pair.	✗	✗	✓
External IP Address Ranges	Provide external IP address ranges enabling the Client to understand threats originating from outside the organization	✗	✗	✓
Managed & Unmanaged Asset Identification	Discover externally exposed cloud services running on the known IP space of various cloud providers. Ability to discover a service NTT is confident belongs to the client but was unable to find any assets present in Prisma Cloud to correlate with this service. This means that there is an asset/service exposed to the public internet that is seemingly unmanaged.	✗	✗	✓
Shadow Cloud Detection – Domains	Closely observe domains linked to a client's organization that resolve to IP addresses associated with cloud-based services. This insight allows NTT to recognize the presence of cloud services used by a Clients organization.	✗	✗	✓
Shadow Cloud Detection – Certificates	Discover certificates that are attributed to the client and are observed on services discovered on cloud IPs. NTT notes these certificates when they are observed on services hosted on cloud IPs, further expanding its understanding of the cloud infrastructure's impact on security.	✗	✗	✓
Monthly Reporting	Aggregate and summarize monthly trending insights into a single report, enabling the Client to: • Maintain a continuously up-to-date inventory of all internet-connected assets. • Identify Cloud and On-Premises assets that do not comply with company policy. • Prioritizing exposures for remediation based on risk. • Track digital assets like IP addresses, certificates, domains, and their registrations. The NTT ISM will conduct monthly sessions with the client to: • Review the Client's overall security posture, with a high-level summary of the providers and region with the highest risk	✗	✗	✓

	• Analyse the Client's security posture trend over the last 90 days • Discuss the Client's security posture score broken down by business unit, geo-IP location, and hosting provider. • Provide a list of the Client's highest risk incidents, enabling the Client to focus their remediation efforts where they will have the most significant impact.			
Peer Benchmark	Provide a benchmark using the ASM tooling to inform the Client of their security posture vs similar peer organizations and provide prioritized recommendations in improving their score.	✗	✗	✓
Attack Surface Testing	Determines the status of an application vulnerability, benign exploitation of the vulnerability is often required. Attack Surface Testing fills this need by running unintrusive, benign exploits to confirm the exploitability of vulnerabilities on the organization's owned services. Up to 10 tests can be conducted per month.	✗	✗	✓
Alert Tuning	Work with the Client to tune the alerting functionality to the Client's requirement and change the priority scoring of the alerts to the Client risk profile.	✗	✗	✓

2.11.3.2 NTT Service Portal

The MXDR system integrates with the provided NTT Services Portal and allows the Client to view, interrogate and leverage MXDR dashboards and MXDR incident reporting. Select dashboards, information and alerts may be linked to or provided within the Palo Alto Networks console. NTT reserves the right to update the NTT Services Portal in its sole discretion.

2.11.3.3 Information Security Management

Information Security Management is a component of NTT's Managed Extended Detection and Response (MXDR) Service delivered by a designated individual. The key functions of Information Security Management include:

- Interpret MXDR security information potentially to identify trends and make technology, service and/or configuration recommendations.
- Support appropriate business, security, and technical reviews as part of the regular Service Management cadence as detailed below in Coverage.
- Support for Severity 1 and Severity 2 MXDR Incidents and provide recommendations on response options up to the provided limits Coverage section.
- The primary responsibilities of the Information Security Manager (ISM) include:
- Advise on service optimizations through additional log sources, feeds and intelligence as required to maintain Client service quality.
- Communicate any changes in Client environment/network that will impact the MXDR service.
- Perform reviews of the MXDR service against Client security objectives annually.
- Function as final escalation point for technical service-related issues and MXDR Incidents requiring additional support after the standard ticket process has been followed.
- Engage with other NTT security teams as required if the team is in scope (e.g., MXDR Incident Response, Digital Forensics and Incident Response, Cyber Threat Intelligence and Threat Vulnerability Management).
    - Review alerts and advisories from NTT and other Threat Intelligence sources to determine the applicability of the vulnerability to Client's environment and provide advice on actions.
    - Provide potential security insights and recommendations based on evolving threats.
    - Form part of escalation team for technical escalations during Business Hours.

3 Commercial Arrangements

3.1 Parent Company Guarantee (PCG)

Please note that NTT DATA is not able to provide a Parent Company Guarantee (PCG).

3.2 Use of subcontractors and partners

These services are delivered by NTT DATA with support from selected, specialist partners only where required, and with approval from the client in advance.

3.3 Pricing

Please see the Digital Marketplace for the NTT DATA Pricing associated with these services.

3.4 Ordering and invoicing process

Clients will be expected to follow the G-Cloud 15 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 based on milestones, with Managed Services Charges invoiced quarterly in advance

3.5 Client 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 and MCA 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
- ISO 22301 Business Continuity
- ISO 45001 Health and Safety Management Systems
- Cyber Essentials
- Cyber Essentials+

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 a top tier global IT Services provider (reference: Gartner). It employs more than 190,000 people across 70 countries.

For more than 50 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 Europe, the Americas, the Middle East, Africa, and Asia Pacific regions.

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 City of London and Birmingham. NTT DATA in the UK is a £400m+ per annum turnover organisation that focuses on supporting clients in:

- Public Services
- Automotive
- Banking and Financial Services
- Education and Research
- Energy and Utilities
- Healthcare
- Insurance
- Life Sciences and Pharma
- Manufacturing and Consumer Packaged Goods
- Retail
- Telco, Media and Technology
- Travel, Transportation and Logistics

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.

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 trade body and our activities are supported by technical and vendor accreditations:

- Snowflake Global Elite Partner
- Informatica Enterprise Premier Partner
- Google Cloud Platform Premier Partner
- Microsoft Solution Partner Designation: Business Application, Data & AI, Digital & App Innovation, Infrastructure, Security, Modern Work.
- AWS Premier Partner | AWS Partner Programs; Premier Tier Services, AWS Managed Service Provider, Authorized Commercial Reseller, AWS Public Sector Partner, AWS Solution Provider Program, AWS Public Sector Solution Provider, Authority to Operate on AWS
- AWS Competencies | Machine Learning Consulting, Telecom Services, DevOps Consulting, Government Consulting, Migration Consulting
- Salesforce Platinum Partner
- Genesys Global Gold partner
- Service Now Elite partner
- Red Hat Premier Business Partner
- Palo Alto Networks Diamond Innovator (Global)
- Check Point 5 Star Partner
- Fortinet Global Partner
- F5 Platinum Partner
- Zscaler GSI
- Cisco Gold Partner
- SAP Global Platinum Partner
- Dell Titanium 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 https://uk.nttdata.com for further information, or contact us at nttdatauk.requirements@nttdata.com