NTT Security Capability Sharing

Managed Detection and Response Services

Why NTT?

Security Solution Partner
Technical capabilities, experience, and ability to deliver successful customer outcomes.

Security Advanced Specialization
Threat Protection,
Identity and Access Management,
Information Protection & Gov,
Cloud Security (not reflected yet)

End-to-end Microsoft Security Journey
NTT can help client journey from consulting, assessment, workshop, POC (Pre-sales) and all the way to delivery & implementation (Post-sales)

Security expertise and experience
Design, integration and security management supporting millions of users globally

Massive Scale
300+ security-certified professionals locally
More than 5,000 professionals worldwide that Microsoft and client can tap

Multi-tower services
Cross domain services deliver transformation and enable a smart world (slide 4)

Microsoft Partner Award
Microsoft Partner Awards 2021
Most Skilling Partner

Microsoft Capabilities
Azure Expert MSP
18 Gold competencies
10 Advanced Specializations

Licensing Solution Partner (LSP)
Cloud Solution Provider (CSP)

Accelerated through NTT 's end-to-end services

consulting • technical • support • managed

Intelligent Digital Transformation
- Application Modernization
- Data & AI
- Azure Kubernetes Services
- Azure Containers
- Smart Cities/Industries

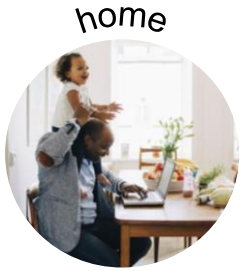
Intelligent Networking
- Interconnect (ExpressRoute)
- SD-WAN / WAN solutions

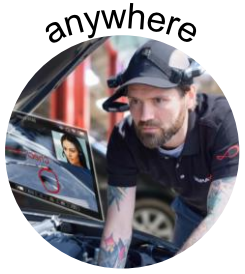
Intelligent Datacenter and Hybrid Cloud
- Public
- Hosted
- Hybrid
- Private
- On-premise

Secure by Design

Intelligent Cybersecurity
- Azure Sentinel (SIEM)
- Microsoft 365 Defender (XDR)
- Microsoft Entra
- Microsoft Intune

Intelligent Workplace
Intelligent Customer Experience
- Microsoft Teams + Calling + Meeting
- Windows Virtual Desktop
- Microsoft 365
- Windows 365
- Firstline Worker Solutions
- Smart Workplaces

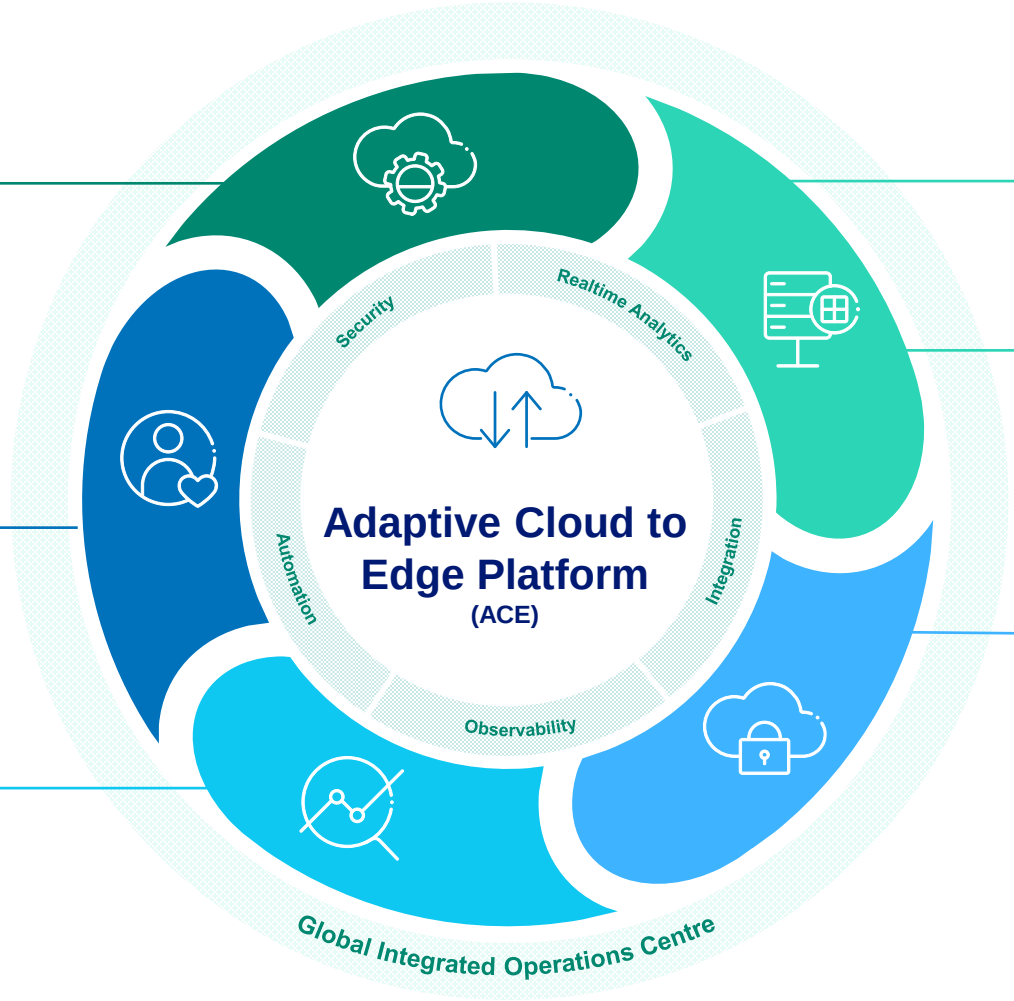




MDR
a Modern SOC Function

MCIS Portfolio

Full Stack Managed Services



Cloud Services
- Cloud Advisory
- Cloud Migration
- Managed Public Cloud
- Managed Private Cloud
- Managed Edge Compute
- Managed DC Infrastructure

End User Services
- Managed Desktop as a Service
- Managed Endpoint & Mobile Device
- End User Service Desk

Observability Services
- Observability Advisory
- Managed Observability
- Observability as a Service

Business Application Services
- Business Application Advisory
- Managed SAP
- Managed Oracle

Application Infrastructure Services
- Managed Web Applications
- Managed Database
- Managed Containers
- Managed Cloud Native Architecture

Cloud Security Services
- Security Advisory
- Integrated Security Operations
- **Managed Detection & Response**
- Managed SAP Security Services
- ControlPanel^{GRC} for SAP

Full Stack Security Services

Advise & Assess

- **Security Strategy & Architecture**
- **Data Security / Privacy Assessment**
- **Zero Trust Security**
- **OT/IOT Security**
- **PCI DSS Consulting**
- **Vulnerability Assessment & Penetration Testing**
- **Digital Forensic & Incident Response (DFIR)**

Implement & Integrate

- **Design & Architect**
- **Implement**
- **Integrate**
- **Uptime Maintenance and Support Services**

Monitor & Manage

- fully managed SOC operations with **Managed Detection & Response (MDR)**

MDR
Service Overview

What is Managed Threat Detection & Response (MDR)?

MDR is a detection and response SERVICE and not a TECHNOLOGY

The MDR Definition

Gartner Defines MDR as :

Delivered with Modern SOC Functions

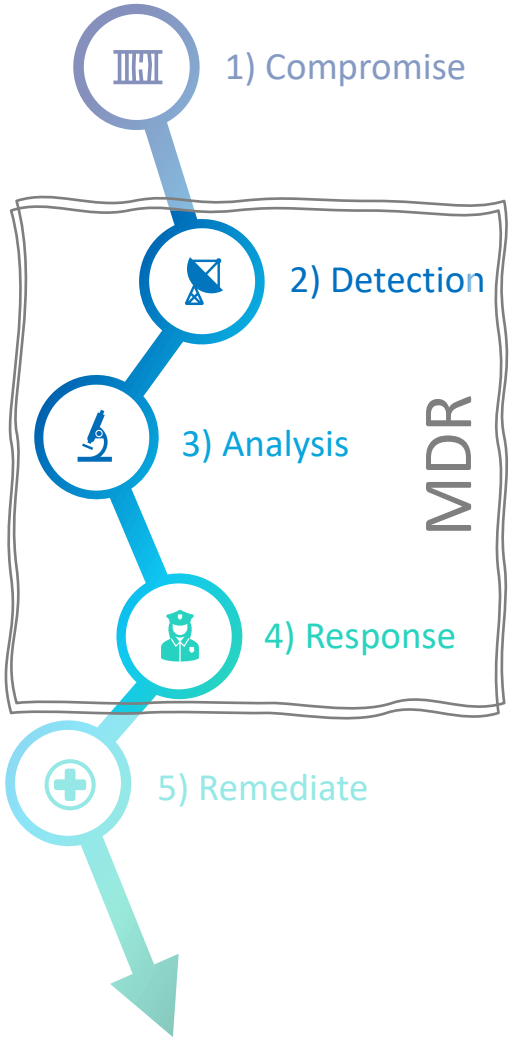
- MDR services provide customers with remotely delivered modern security operations centre functions.

Being a Turnkey Experience

- MDR service providers offer a turnkey experience, using a predefined technology stack.

Providing Actionable Outcomes

- Telemetry is analysed within the provider's platform using a range of techniques.



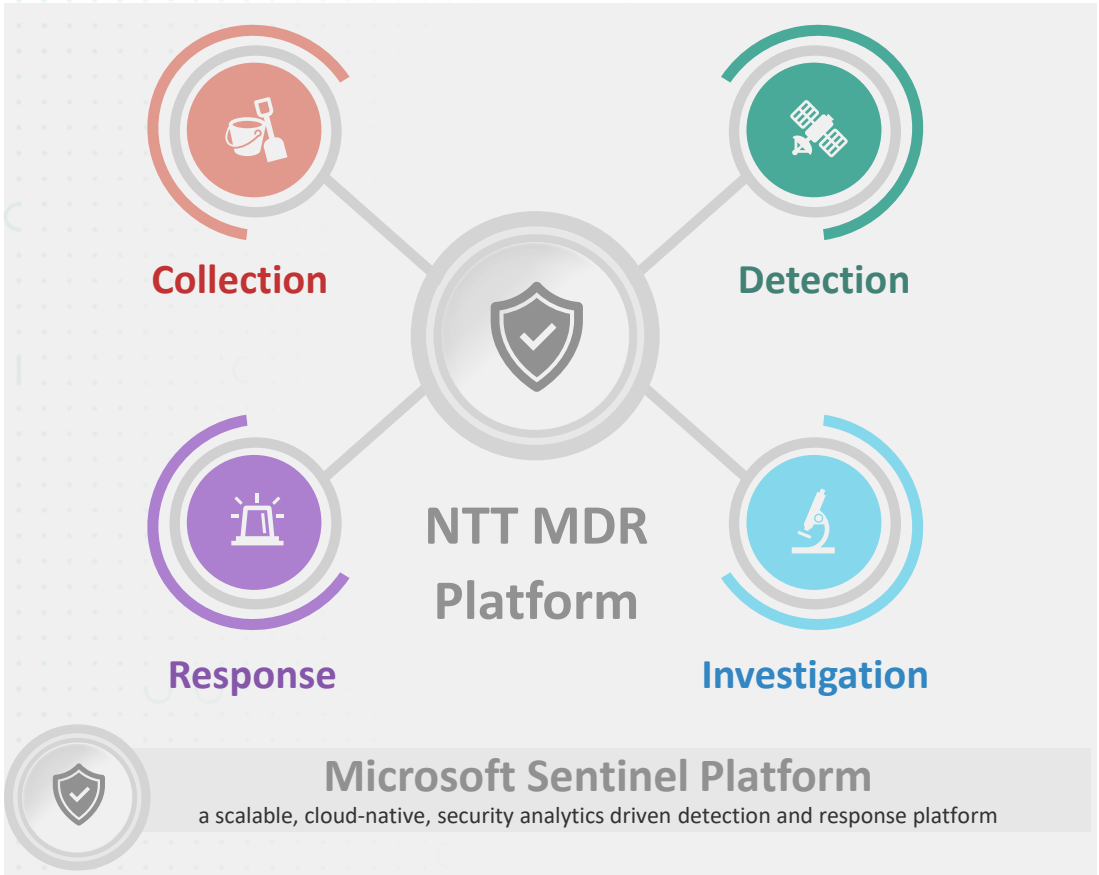
What are the Core Attributes of an MDR Service?

- 24/7 Service
- Threat Hunting
- Expert Analysts
- Remote Response Mitigation
- Protection Across the Digital Estate
- Real-time Detection & Response

The NTT MDR Platform

a service that delivers security insights and advanced protection via a variety of telemetry sources including cloud, network, computers and mobile devices - provide faster, more accurate detections and – reduced risk for your business

The NTT MDR Platform



CROWDSTRIKE · Microsoft · paloalto NETWORKS · cisco · Carbon Black. · FORTINET · zscaler · CHECK POINT

SOC Analysts | Threat Hunters | DFIR

- Security Monitoring and detection of threats: 24 x 7 security monitoring with advanced analytics reducing the Mean Time to Detect (MTTD) threats
- Threat Hunting: Security Analyst-driven investigation and disruption of attacks using NTT's threat hunting capabilities
- Response: Threat response using Security Orchestration Automation and Response (SOAR) reducing Mean time to respond (MTTR)
- Expertise and experience: NTT's expertise, experience, advanced analytics, and external threat intelligence
- Portal: Comprehensive, MITRE ATT&CK framework aligned, incident reports to enable a rapid response
- Digital Forensics & Incident Response (DFIR): Digital Forensics and Incident Response (DFIR) for the provision of incident response support in the event of critical incidents

Information Security Manager (ISM)

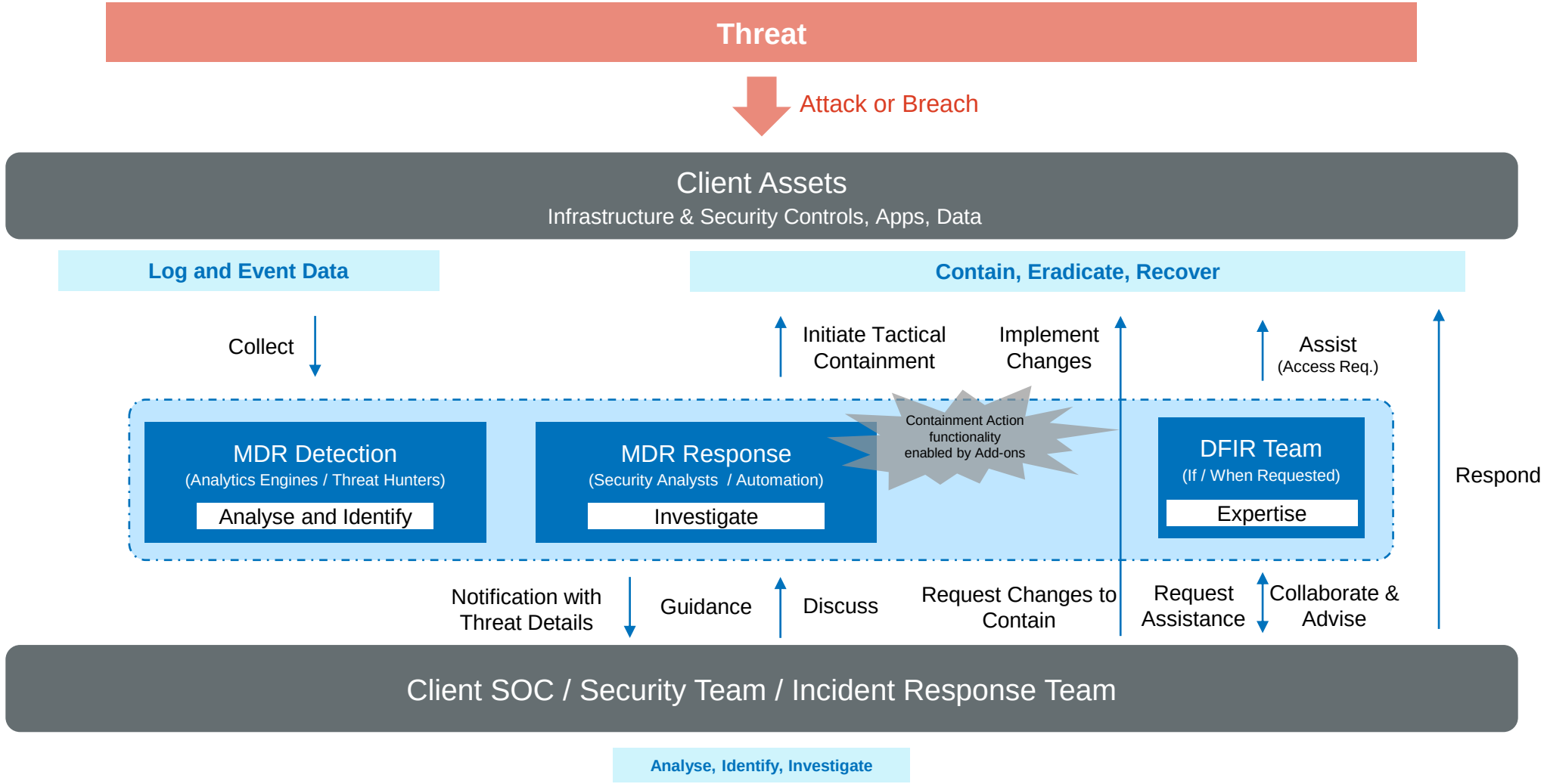
Service Delivery Manager (SDM)

Monthly Service Report

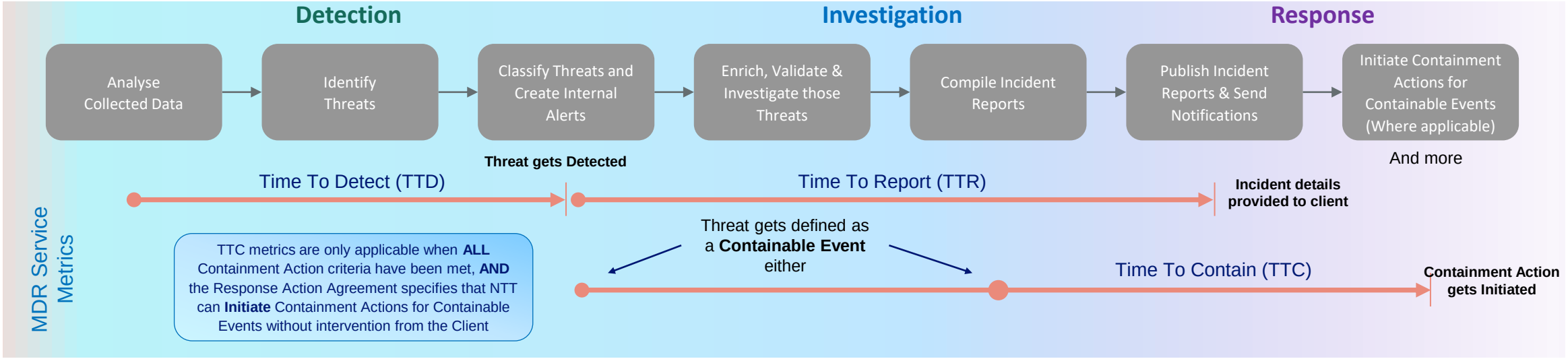
Quartey Service Review Meeting

Detecting and Responding to Threats

With MDR



MDR Service Level Agreements (SLA)



The NTT MDR service has three SLAs

Mean Time To Detect (MTTD) < 15 min

Average time taken for processing logs up until the creation of an internal alert (Threats classified as P1 or P2 only)

Mean Time To Report (MTTR) < 30 min

Average time taken from the creation of an P1 or P2 internal alert to the time when an incident report is created and made available on the portal

Mean Time To Contain (MTTC) < 15 min

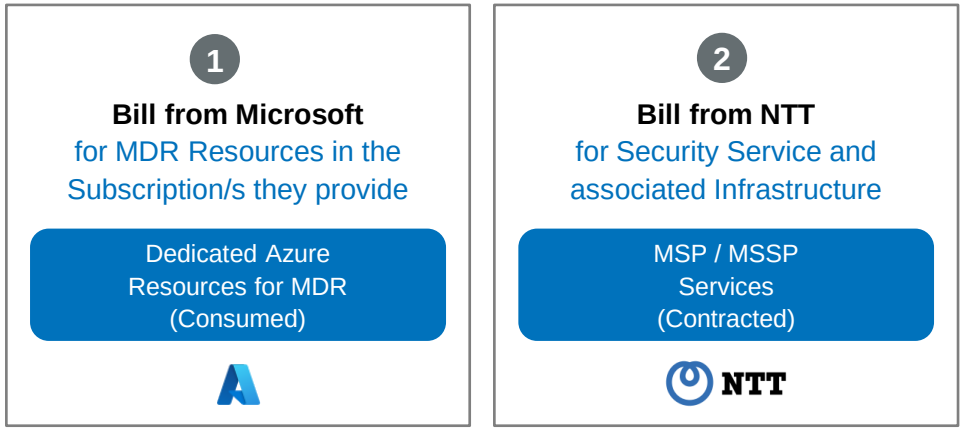
Average time taken to **Initiate** Containment Actions for a P1 or P2 Containable Event without intervention from the Client

MDR Service Offers

MDR

Resembles ‘Managed Service’ model

Client-provided Subscription/s (‘BYO’)
for Client resources

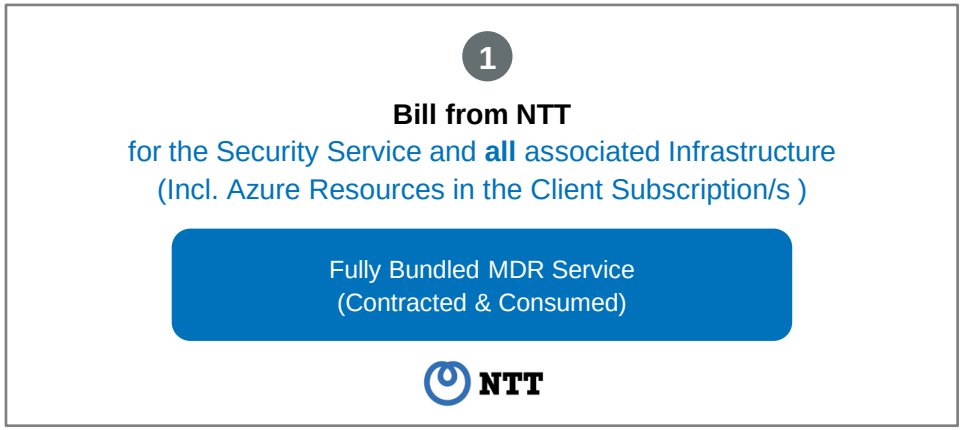


- NTT deploys and manages the resources in the Client Azure Subscription.
- Applicable for clients who are heavily embedded into Microsoft Cloud ecosystem.

MDRaaS

As-a-Service model

NTT provides consumable MDR Service



- NTT provides clients a log destination but manages all infrastructure transparently to the client.

Note: Future slides which show detail of the platform would present to a client as a “Black Box”.

MDR Service Components - MDR

NTT MDR consists of a number of one off, recurring and consumptive cost components

One off Services

- Preparation
- Build & Deploy
- Onboarding
- Transition & Close

Managed Services (recurring)

Client Ownership

MDR Azure components (Per Client consumption cost)

Azure Subscription(s)

- Azure Sentinel
- Log Analytics Workspace
- Analytics Logs (90 days)
- Syslog CEF Forwarder(s)
- Load Balancer
- Logic Apps (SOAR)
- VPN Gateway
- Log Storage & Retention Options

MDR Service

MDR Packages

- *24x7 Monitoring*
- *Threat Detection & Response*
- *Incident Management*
- *Use Case Tuning*
- *Trend Analysis & Reporting*

- Information Security Manager (ISM)
- Service Delivery Manager
- DFIR
- Committed Consumption

MDR Platform

The NTT MSSP MDR Platform and the associated components

- *Azure infrastructure and services*
- *Threat intelligence*
- *Client reporting infrastructure and services*

- Connectivity Methods

MDR Add-ons

- MDR for Endpoint
- SecDM for MDR

MCIS Service Operations

- IOC, Tools & Licences, Azure Management (platform, ops)

MDR Service Components - MDRaaS

NTT MDR consists of a number of one off, recurring and consumptive cost components

One off Services

- Preparation
- Build & Deploy
- Onboarding
- Transition & Close

Managed Services (recurring)

Part of the aaS model

Design and cost provided by MCIS SD

MDR Service

MDR Packages

- *24x7 Monitoring*
- *Threat Detection & Response*
- *Incident Management*
- *Use Case Tuning*
- *Trend Analysis & Reporting*

- Information Security Manager (ISM)
- Service Delivery Manager
- DFIR
- MDRaaS Locations
- Log Storage & Retention Options
- Committed Consumption

MDR Platform

The NTT MSSP MDR Platform and the associated components

- *Azure infrastructure and services*
- *Threat intelligence*
- *Client reporting infrastructure and services*

- Connectivity Methods

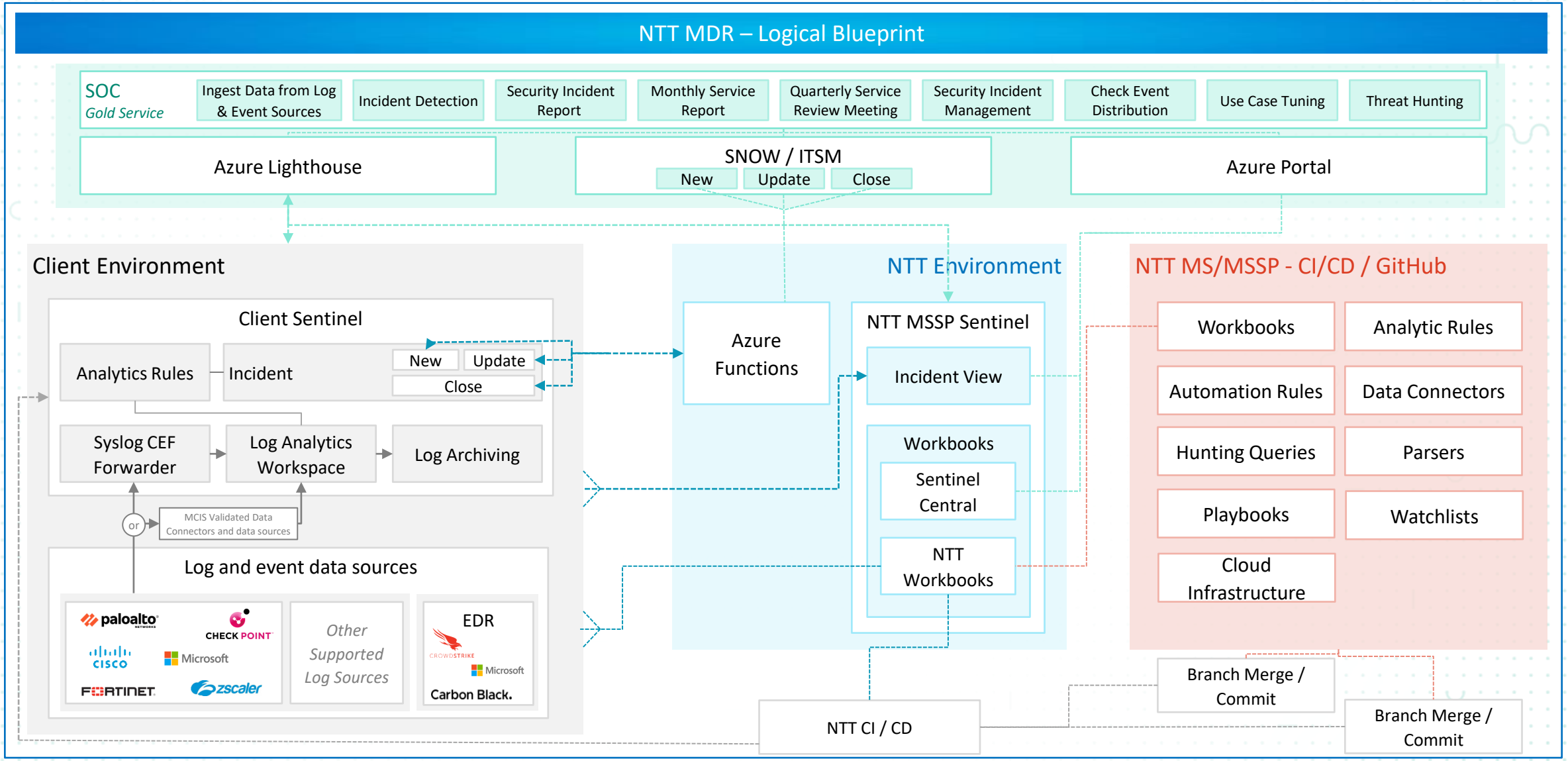
MDR Add-ons

- MDR for Endpoint
- SecDM for MDR

MCIS Service Operations

- IOC, Tool & Licences, Azure Management (platform, ops)

NTT MDR– Logical Blueprint



MDR Service Delivery Elements

- The SOC team using an MSSP Sentinel, monitor a clients Sentinel instance. This is made possible using Azure Lighthouse which provides access to a client's subscription.
- Using an MSSP model, log and event data from a client's environment is never copied to NTT.
- Instead, the data remains in client's Sentinel and Log Analytics Workspace instance, where it is analysed and queried.
- Whether MDRaaS or Managed MDR, the Azure subscription, represents the boundaries of a client's environment.
- There are no shared Sentinel or Log Analytics Workspaces.
- Each client is logically and technically separated from others providing increased security on a per client level by using an Azure subscription for each client.
- Log and event data sources vary by type and method of sending logs to the Log Analytics Workspace (LAW) / Sentinel Workspace.
- Direct API ingestion goes direct into the Log Analytics Workspace.
- Syslog data sources send logs to a Syslog CEF Forwarder which in turn sends it to Log Analytics Workspace.
- Agents send logs direct to LAW.
- Log sources need to be validated by NTT for ingest and usefulness before being an officially supported technology.

- CI/CD Continuous integration / continuous deployment pipeline:
- In our MDR solution, Cloud Infrastructure is maintained as Infrastructure as Code, and Sentinel components such as workbooks, analytic rules, playbooks etc., are maintained as code.
- CI/CD bridges the gaps between development and operation activities and teams by enforcing automation in building, testing and deployment of Azure Cloud Infrastructure as well as Sentinel Specific content.

  CI/CD services compile the incremental code changes made by developers, then link and package them into software deliverables. Automated tests verify the software functionality, and automated deployment services deliver them to required subscription / Sentinel instance.

Service Matrix

The MDR service is available in three service offer options

Domain	Silver	Gold	Platinum
Professional Services, Azure Platform Costs, MDR Platform Costs, MCIS Service Costs, DFIR	✓	✓	✓
Information Security Manager - ISM (Per Month)	8 Hr (Max)	24 Hr (Max)	48 Hr (Max)
Service Delivery Manager - SDM (Per Month)	8 Hr (Max)	24 Hr (Max)	32 Hr (Max)
DFIR (Per Year)	25 hrs	25 hrs	25 hrs
MDR Managed Service Elements			
Ingest Data from Log and Event Sources	✓	✓	✓
Data Retention	✓	✓	✓
Incident Detection	✓	✓	✓
Security Incident Report	✓	✓	✓
Monthly Service Report	✓	✓	✓
Use Case Tuning	✓	✓	✓
Quarterly Service Review Meeting		✓	✓
Security Incident Management		✓	✓
Check Event Distribution		✓	✓
Threat Hunting		✓	✓
Custom Use Case Tuning			✓
Targeted Threat Hunting			✓
Update Special Handling Notes			✓

Summary Definitions for Components within the Packages (1 of 2)

Domain	Overview
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: Security incident escalation point, Risk management support for NTT and the Client improvement recommendations.
Service Delivery Manager (SDM)	The Service Delivery Manager (SDM) provides an NTT interface that can manage the service delivery relationship between NTT and the Client. Conducts operational reviews and business performance reviews following a defined management cadence and provides a key point of escalation for the Client (e.g., through Major Incident escalations).
DFIR (25 Hours per Year)	Twenty-Five (25) hours of DFIR support per contract year, which includes the following: 24 x 7 on-call service, Incident Management and Coordination, On-demand Threat-Hunting on supported and unsupported log sources, Evidentiary compliant handling with chain of custody, Expert digital forensic analysis, Deploy endpoint detection response tools to support DFIR activities as necessary and Malware reverse engineering.
Silver Package	
Ingest Data from Log and Event Sources	Support the ingestion of data from a range of technologies and services as log and event sources.
Data Retention	Retain Analytics Logs for in scope devices for ninety (90) days. (See Optional Extended Log Management Services)
Incident Detection	Provide 24 x 7 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.
Security Incident Report	Provide Client with a Security Incident Report that includes a detailed description of the threat, identified activity and impact combined with a recommendation of suitable incident response steps to take. Further updates to the Security Incident are updated on the Services Portal.
Monthly Service Report	Provide Client with a monthly service report which includes extracts from Sentinel Workbooks, Sentinel Widgets, and ITSM incident summary.
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.

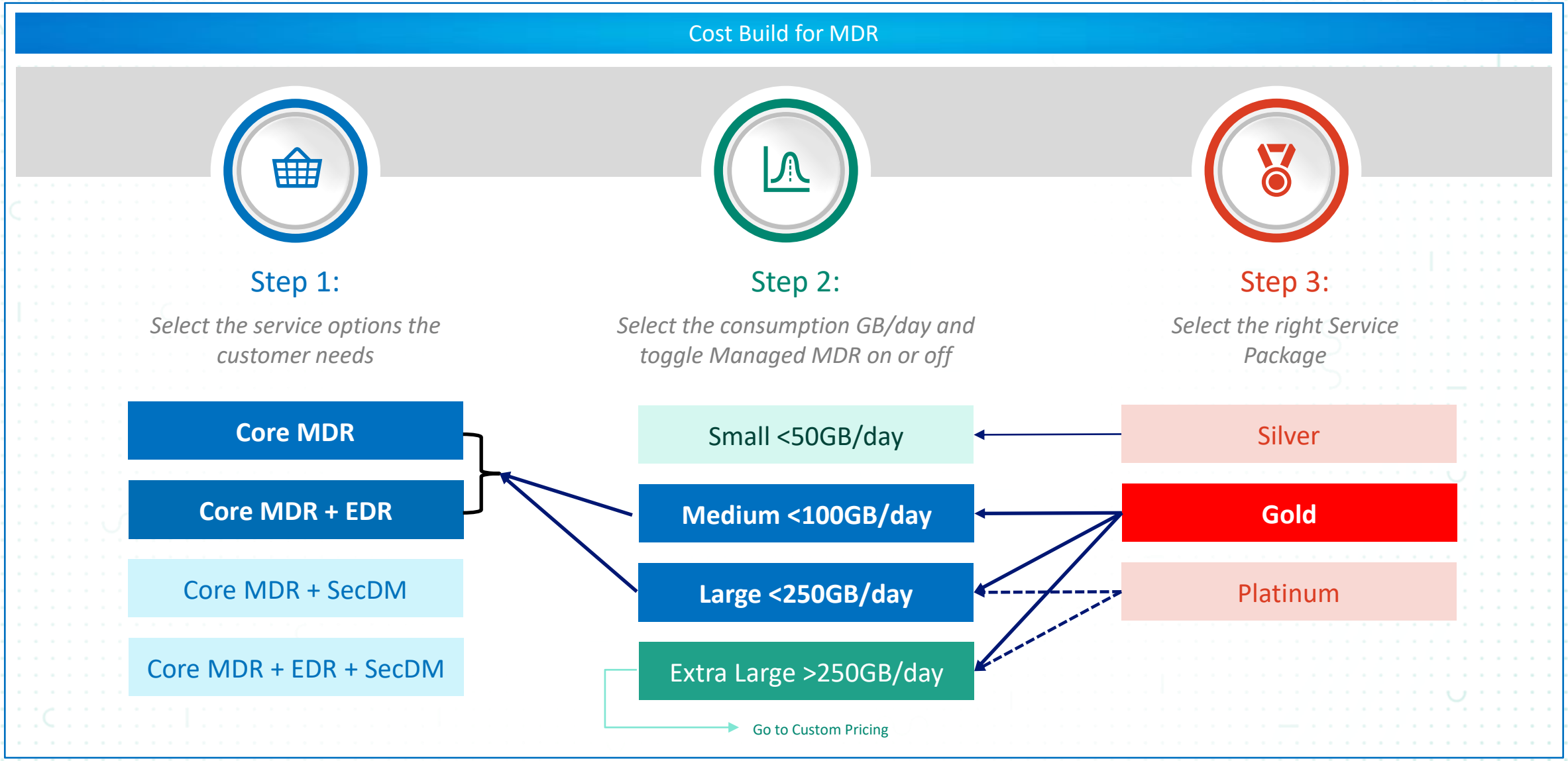
Summary Definitions for Components within the Packages (2 of 2)

Domain	Overview
Gold Package	Includes All Items in Silver and the Following:
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.
Security 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 high severity security 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.
Platinum Package	Includes All Items in Silver and Gold and the Following:
Custom Use Case Tuning	Create Client custom detection rules (up to 10 per year) for specific cases based on Client requirements.
Targeted Threat Hunting	Investigate and identify patterns on data collected for a specific industry or region. 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.

MDR
Pricing

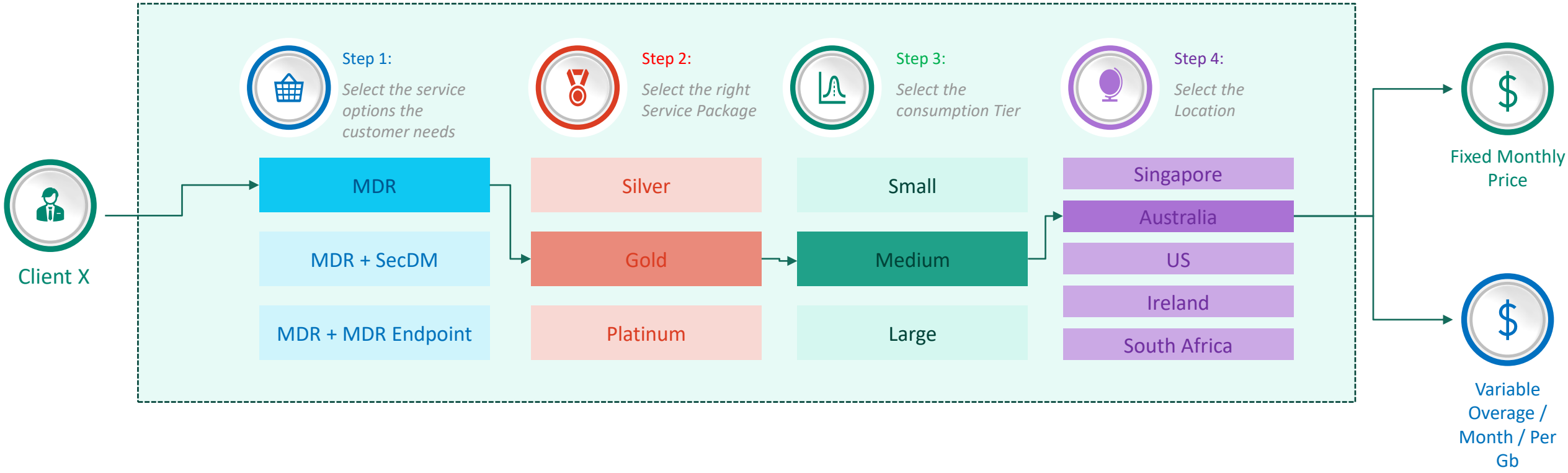
How the MDR costs are built up

A three step process to determine the charges



Pricing Options for MDR as Service

any overage is costed using an fixed overage cost, fair use policy applies to the managed services



Fair usage policy: breach of monthly ingest for 3 consecutive months will result in the consumption model automatically increasing to the next tier at NTTs discretion.