Managed Detection and Response in the face of Evolving Challenges

Introducing NTT's Managed Detection and Response

NTT DATA

#55 in Fortune Global 500

#35 Global Brand in Brand Finance

#5 Global IT Service Provider

#2 Data Centre in Tele Geography

NTT Group

Real Estate and Energy

Real estate business, energy business and others. NTT aims to revitalize industry and shape a more sustainable society.

NTT Urban Solutions   NTT Anode Energy

Regional Communication Business

Domestic intra-prefectural communications services and related ancillary services.

NTT WEST   NTT EAST

Global Solutions Business

System integration services, network system services, cloud & security services, global data center services, and related services

NTT   NTT DATA

NTT DATA

Integrated ICT Business

Mobile services, domestic inter-prefectural communications services, international communications services, solutions services, and system development services and related services.

NTT docomo   NTT Communications   NTT COMWARE

Why NTT?

NTT DATA

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

Security Advanced Specialization
Threat Protection,
Information Protection &
Governance

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

Microsoft Partner Award
Microsoft Partner Awards 2021
Most Skilling Partner

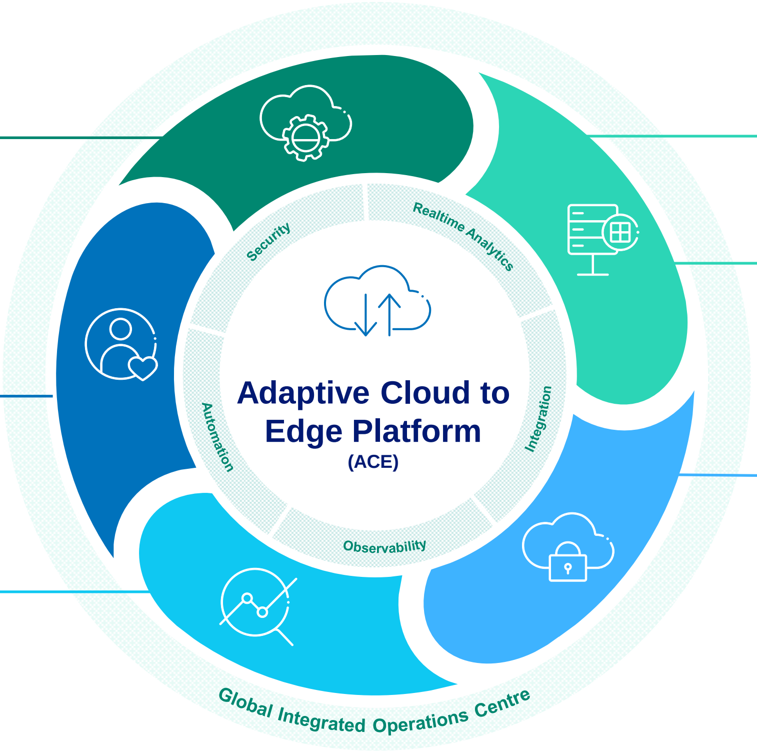
Microsoft Partner Awards 2023
Outstanding Partner for Infrastructure

Microsoft Capabilities
Azure Expert MSP
18 Gold competencies
12 Advanced Specializations

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

MCIS Portfolio

Full Stack Managed Services


Adaptive Cloud to Edge Platform
(ACE)
Security
Realtime Analytics
Integration
Observability
Automation
Global Integrated Operations Centre

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

NTT MDR

NTT and Microsoft

A cloud-native, analytics-driven MDR service, built on Microsoft's leading next-gen SIEM – powered by AI, automation, and threat intelligence.

Improves overall security posture by providing faster and more informed detection and response times for joint clients.

- **Microsoft's GOLD solution provider for Security, with Information Protection and Governance specialization**
- **Microsoft's Azure expert Managed Services Provider**
- **Member of the Microsoft Intelligent Security Association (MISA)**

#1

Leverage Microsoft's leading next-gen security information and event management (SIEM) platform. Sentinel enables organizations to collect data at scale across all users, devices, apps, and infrastructure, both on-prem and in multicloud environments.

#2

Improved speed and efficiency of threat detection, prevention, and response through advanced analytics, continuous monitoring, and security orchestration

#3

24x7x365 security analyst investigations and threat hunting capabilities from certified, accredited and specialized security delivery locations

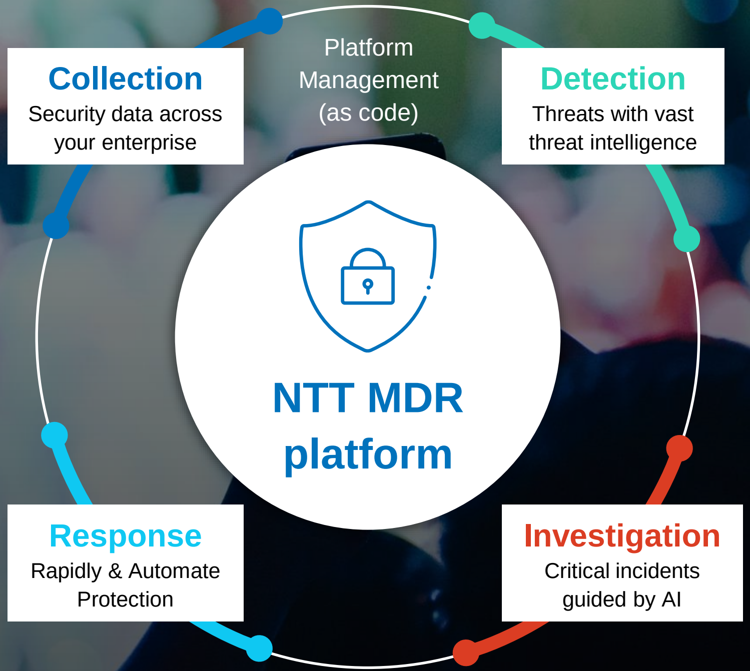
#4

Digital Forensics and Incident Response (DFIR) for the provision of incident response support in the event of critical incidents

NTT MDR

A modernized approach to detect, respond and investigate threats

- Data ingestion
- Workspaces to store data for analysis
- Commitment tiers
- Data retention and archiving



Platform Management (as code)

Collection
Security data across your enterprise

Detection
Threats with vast threat intelligence

NTT MDR platform

Response
Rapidly & Automate Protection

Investigation
Critical incidents guided by AI

- Analytics engines
- Analytics rules, custom queries and automation rules
- Threat hunters (structured hunting, situational hypothesis)
- Threat intelligence

- Channels of communication with client IR teams
- Incident detail on the NTT services portal
- Reporting functions
- Base Response in the core service
- Response actions enabled by add-ons
- Playbooks for response tasks

- Security analysts (specialists)
- Threat hunting (unstructured)
- Workbooks
- Understand and gather evidence
- Playbooks for investigation

Security analysts

DFIR experts

Information Security Manager (ISM)

Service Delivery Manager (SDM)

CSD Security Service Delivery Model Overview

Security Operating Model

NTT

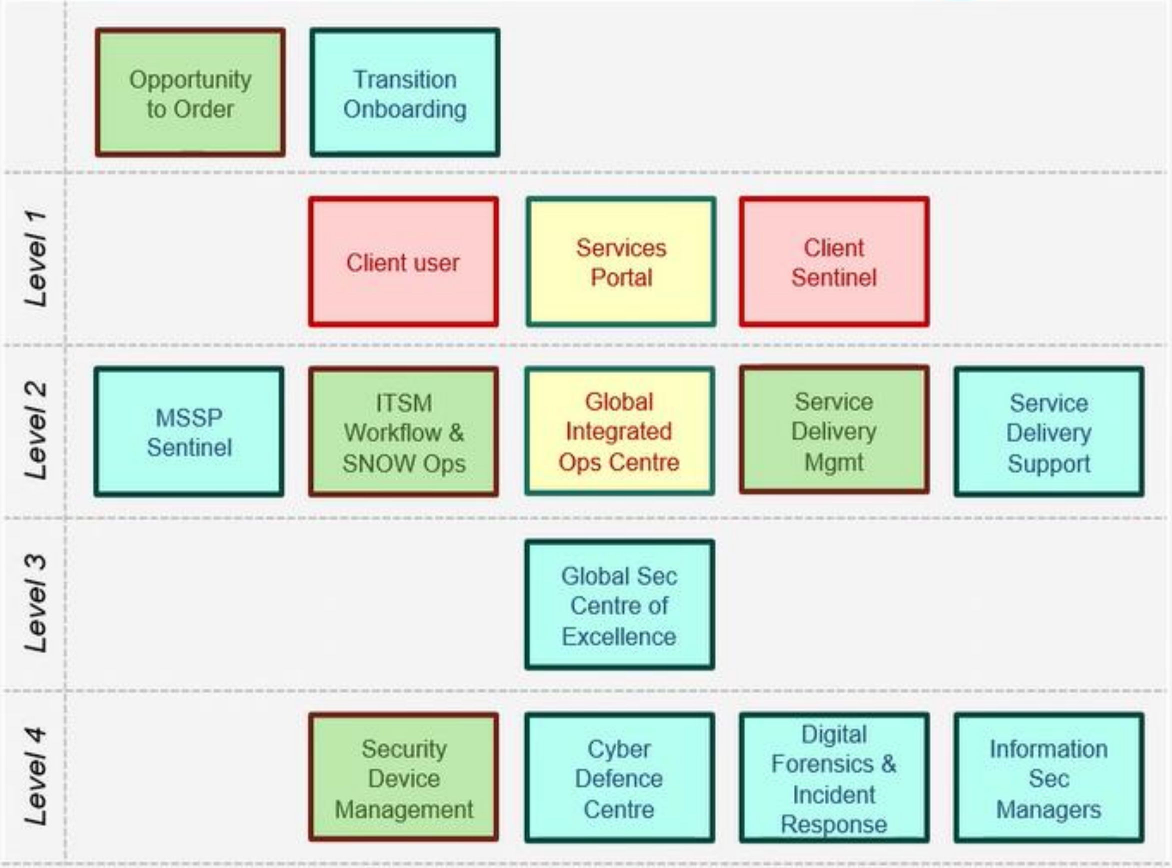
Following the standard CSD “Opportunity to Order” process, the client onboards onto the MDR via the specialist Security Transition Team

Level 1 – The client interfaces with their service via the Services Portal & through the CSD Services Management function. Service status, performance management & SLA compliance are available via Portal dashboards & monthly reporting.

Level 2 – Client generated Security incidents are triaged by Global IOC, with basic client request resolution. Ticket handling for 2nd & 3rd tier resolver group Support allocation. Support provided by the Service Delivery Support team.

Level 3 – Security incident management is delivered through Global Centres of Excellence.

Level 4 – Specialist support is offered via the Security Analysts within the CDC and the DFIR teams. Information Security Managers offer technical expertise to the client and health, availability & policy device management for devices included within the service.

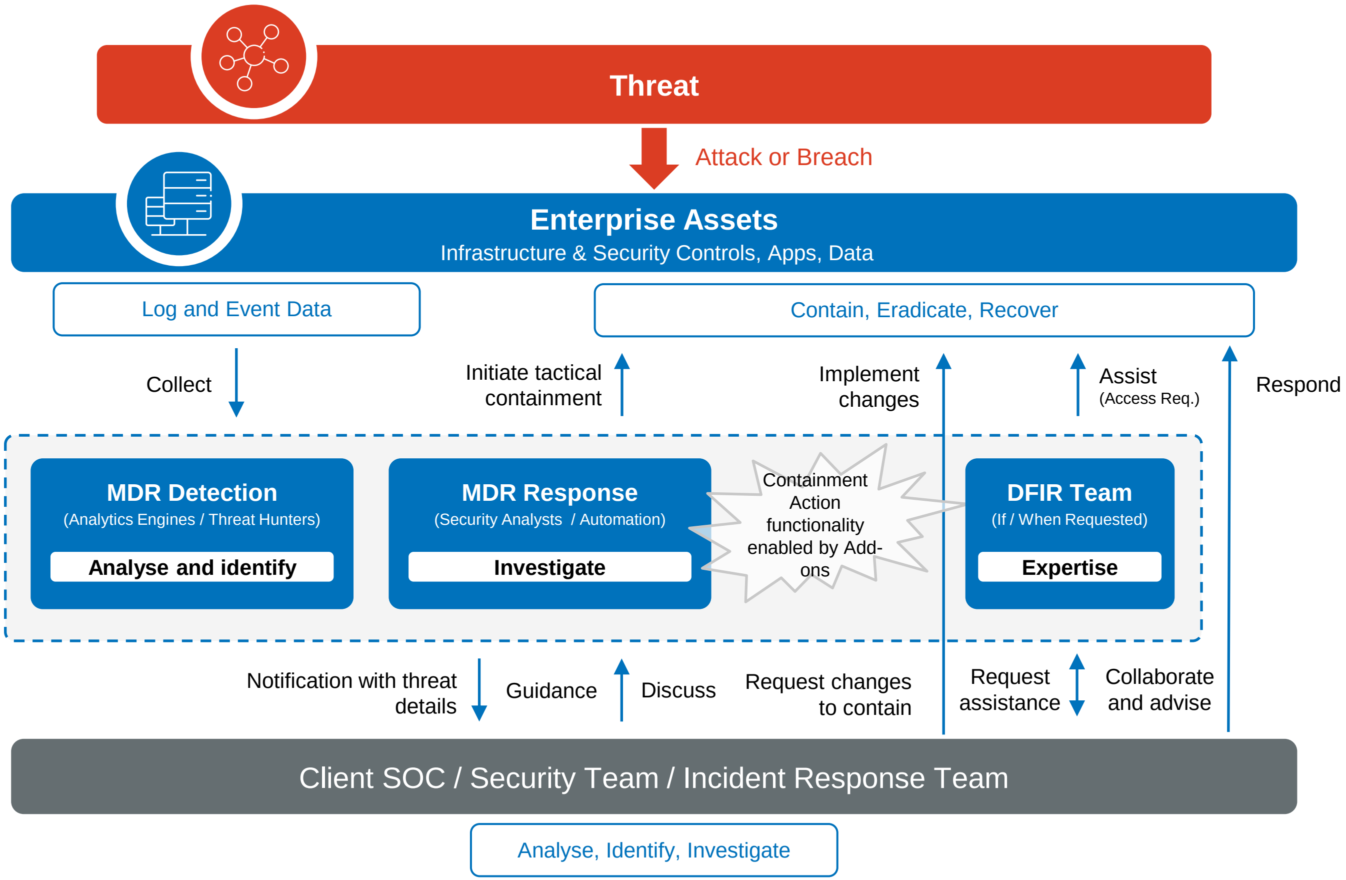


	Opportunity to Order	Transition Onboarding			
Level 1		Client user	Services Portal	Client Sentinel	
Level 2	MSSP Sentinel	ITSM Workflow & SNOW Ops	Global Integrated Ops Centre	Service Delivery Mgmt	Service Delivery Support
Level 3			Global Sec Centre of Excellence		
Level 4		Security Device Management	Cyber Defence Centre	Digital Forensics & Incident Response	Information Sec Managers

Legend: CSD Service | NTTL Service | CSD Security | Client

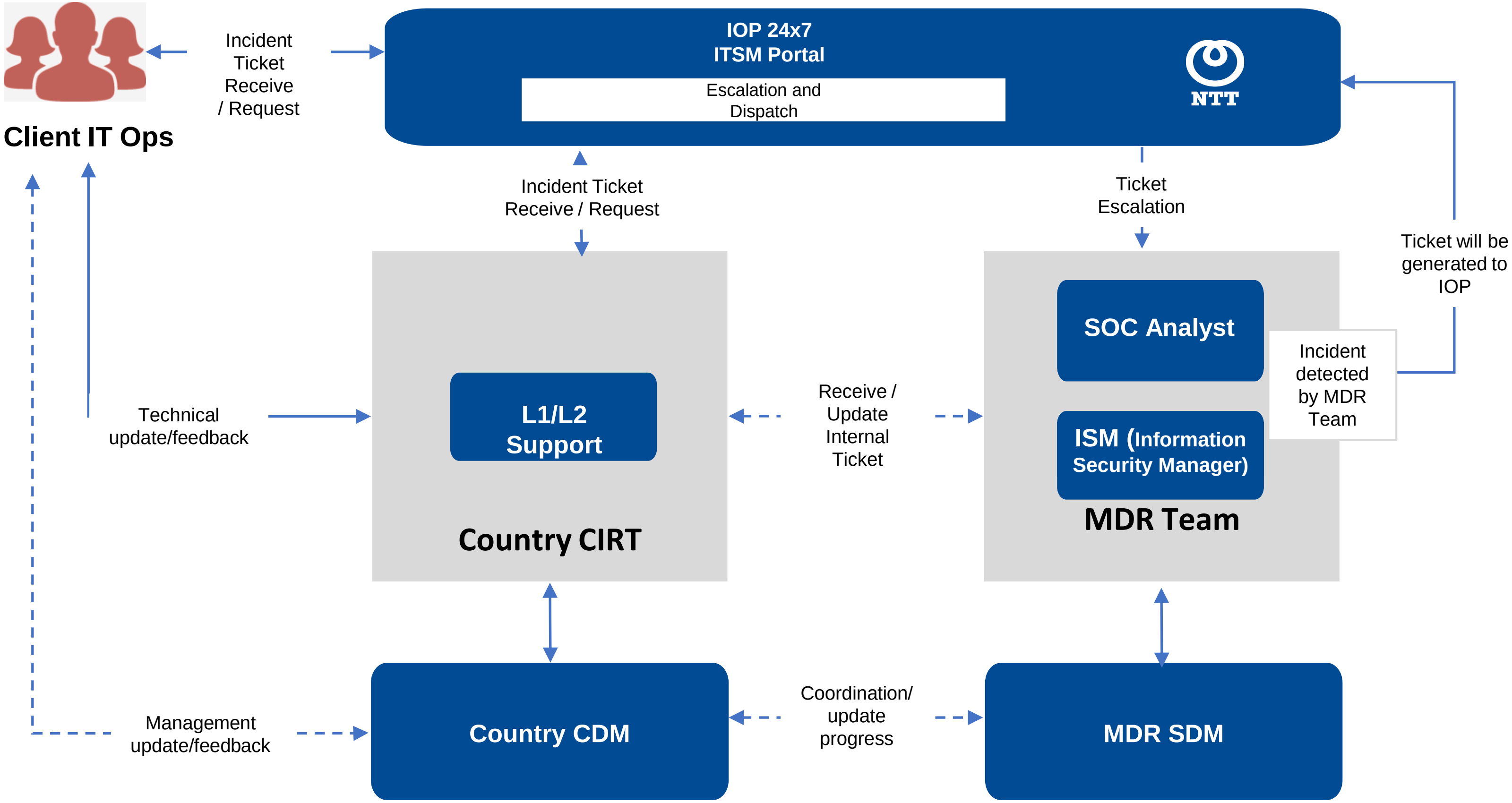
Security Incident Response

with MDR

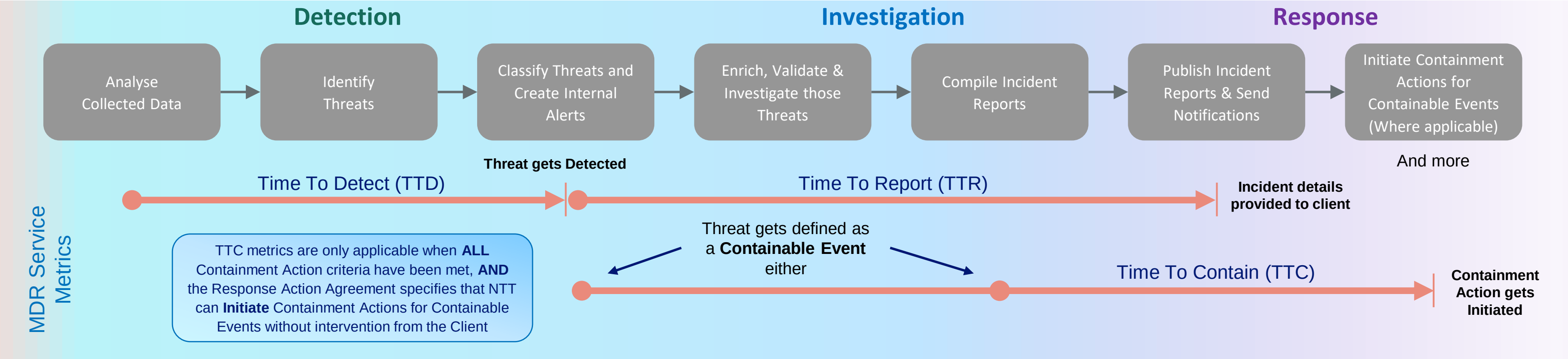


Threat
Attack or Breach
Enterprise Assets
Infrastructure & Security Controls, Apps, Data
Log and Event Data
Contain, Eradicate, Recover
Collect
Initiate tactical containment
Implement changes
Assist
(Access Req.)
Respond
MDR Detection
(Analytics Engines / Threat Hunters)
Analyse and identify
MDR Response
(Security Analysts / Automation)
Investigate
Containment Action functionality enabled by Add-ons
DFIR Team
(If / When Requested)
Expertise
Notification with threat details
Guidance
Discuss
Request changes to contain
Request assistance
Collaborate and advise
Client SOC / Security Team / Incident Response Team
Analyse, Identify, Investigate

Operational Flow


Client IT Ops
Incident Ticket Receive / Request
IOP 24x7
ITSM Portal
Escalation and Dispatch
NTT
Incident Ticket Receive / Request
Ticket Escalation
Ticket will be generated to IOP
SOC Analyst
Incident detected by MDR Team
ISM (Information Security Manager)
MDR Team
L1/L2 Support
Country CIRT
Technical update/feedback
Receive / Update Internal Ticket
Management update/feedback
Country CDM
Coordination/ update progress
MDR SDM

MDR Service Level Agreements (SLA)



Detection

Investigation

Response

Analyse Collected Data → Identify Threats → Classify Threats and Create Internal Alerts → Enrich, Validate & Investigate those Threats → Compile Incident Reports → Publish Incident Reports & Send Notifications → Initiate Containment Actions for Containable Events (Where applicable)

And more

MDR Service Metrics

Threat gets Detected

Time To Detect (TTD)

Time To Report (TTR)

Incident details provided to client

Threat gets defined as a **Containable Event** either

Time To Contain (TTC)

Containment Action gets Initiated

TTC metrics are only applicable when **ALL** Containment Action criteria have been met, **AND** the Response Action Agreement specifies that NTT can **Initiate** Containment Actions for Containable Events without intervention from the Client

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)

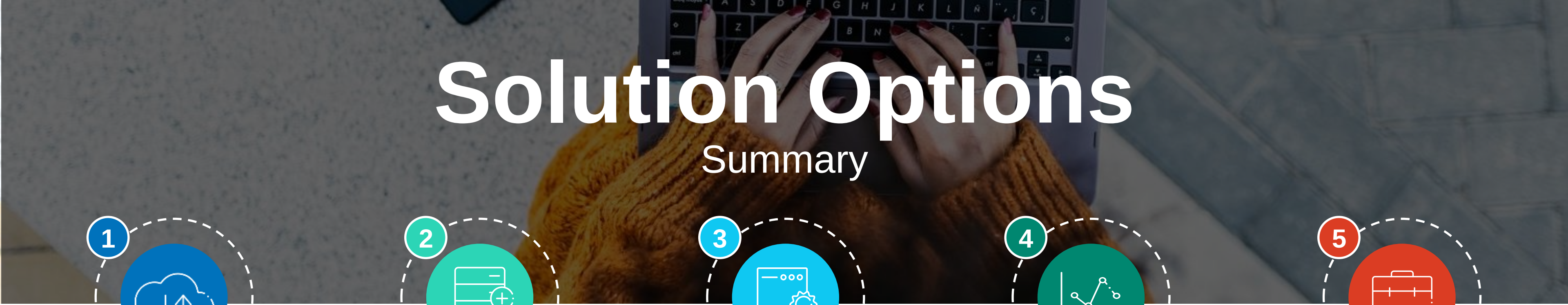
Mean Time To Report (MTTR)
< 30 min

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 Solutions Offers



Solution Options

Summary

1 Service offer

Managed MDR

MDRaaS

2 Service add-ons

○ **MDR for Endpoint**

SecDM for MDR

○ Managed Advanced Firewall **without** Firewall Policy Management

○ Managed Advanced Firewall **with** Firewall Policy Management

□ Management of other Security technologies

3 Service package

○ Silver

○ Gold

○ Platinum

4 Commitment Tier/s

MDR

○ Small <50GB/day

○ Medium <100GB/day

○ Large <250GB/day

○ 2TB < Extra Large>250GB/day

MDRaaS

Starting at 10GB/day

10GB/day ⌄

5 Data retention periods

Interactive Retention

2 years ⌄

Total Retention

7 years ⌄

Why MDR?

Value Proposition

Cyber resilience and our Managed Detection and Response (MDR) service

Operational resilience

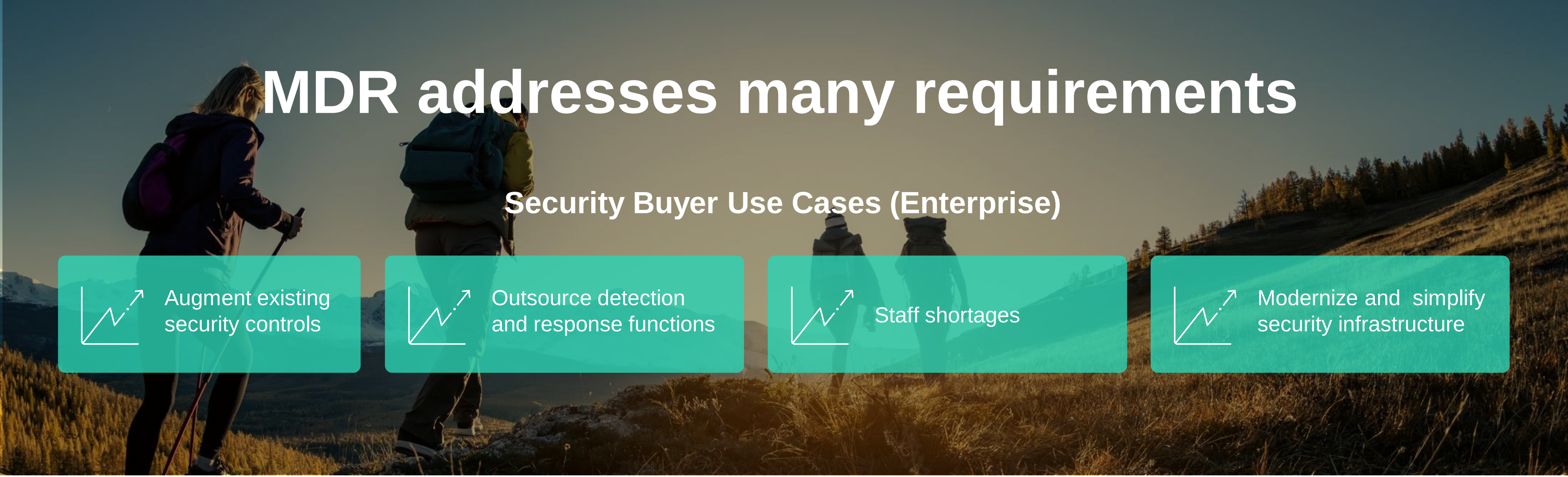
Positive impact on IT and security resources though advanced skill and subject matter expertise augmentation.

Financial resilience

Strong and proven digital backbone to secure customer and employee engagements across all surfaces, around the globe.

Skill and staffing

Drives speed, efficiency and response-time improvements through orchestration, automation and AI-driven threat intelligence and digital forensics.



MDR addresses many requirements

Security Buyer Use Cases (Enterprise)

- Augment existing security controls
- Outsource detection and response functions
- Staff shortages
- Modernize and simplify security infrastructure

Business needs

Detection Capabilities

To improve detection capabilities (discover hard-to-find threats)

Visibility

To consolidate Alerts and centralise threat notifications (security monitoring)

Skills

To provide deeper analysis, investigation and mitigation capabilities

Availability

For access to skilled security specialists when most needed

Management

To address operational (24/7) or technology constraints and complexity

Response capabilities

To disrupt complex and sophisticated cyberattacks

Speed

For faster reaction to threats (24/7) response)

Experience

For threat hunting capabilities

Partnering with NTT

We will be right there **helping to transform your business** at the **pace you aspire** to, **delivering the outcomes you want** with **the services you need.**

Thank you