Data sheet

Security Services

Managed Detection and Response

Our **Managed Detection and Response** (MDR) service combines human and machine expertise, leading EDR technologies, global threat intelligence to detect and disrupt hard-to-find attacks

The threat landscape continues to become more dynamic and dangerous while the attack surface expands and becomes more complex to secure.

Lean security teams lacking the right skills results in disjointed incident management and undetected attacks, especially sophisticated attacks from Advanced Persistent Threat (APT) actors. Adding more security layers increases complexity and generates even more logs and alerts that go untreated.

'Shifting our approach to MDR reduced the impact of security incidents.'
- CISO, regional bank

Organizations turn to more tools like SIEM and SOAR in the hopes that the next generation of technology will improve the situation. Organizations need to realize SIEMs are not a panacea and must shift their attention to a focused approach of detection and response.

Managed Detection and Response (MDR)

MDR is the ideal foundation for organizations that need to discover hard-to-find threats, disrupt complex and sophisticated cyberattacks, and improve cyber-resilience. MDR is expertly-driven from modern Security Operations Centers (SOC) as a turnkey project with a simplified technology stack for easy deployment. With decades of security expertise, organizations can trust NTT as their security partner of choice.

Make a good thing better

MDR is fully integrated, via APIs and automation, with several market-leading endpoint detection and response (EDR) technologies. MDR augments endpoint visibility with our Cyber Threat Sensor (CTS), a purpose-built, fully managed network traffic analysis (NTA) technology with full packet capture (PCAP) recording. The combination of event and evidence data from our curated endpoint and network technology stack gives us the deep visibility we need to detect sophisticated attacks.

Global threat intelligence

Our scale of operations as a tier 1 backbone ISP and our global client base generates truly big data and unmatched security telemetry. With human and machine learning analysis, we monitor threat actors, infected host communications and command and control infrastructure. Deep experience and exclusive research produce unrivalled insights into malicious actor tools and capabilities, often before it is leveraged. This helps our clients and the community when we participate in major disruption and takedown efforts with industry partners and law enforcement.[1]

Key benefits:

- Minimize business impact by disrupting threats early
- Gain cyber resilience quickly with a turnkey solution
- Reduce risk by detecting threats that bypass existing controls
- Fast response with isolation of endpoints
- Integrated digital forensic and incident response retainer
- Improve security maturity with the full weight of NTT's capabilities

[1] Thomas, M., 2020. https://hello.global.ntt/en-us/insights/blog/international-efforts-in-the-fight-against-global-cybercrime

MDR process flow

Our curated technology stack provides native protection capabilities while monitoring data for suspicious activity. Advanced analytics using AI/ML detects events that merit closer examination. Humans investigate the incident and disrupt legitimate threats with endpoint containment.

'PCAP data helps us detect four times more incidents than without.'
- Security analyst

MDR provides:

- Immediate network and endpoint visibility with market-leading EDR technologies and our Cyber Threat Sensor
- Our advanced analytics with machine learning and threat intelligence applied across network and endpoint data
- 24/7 Analyst-driven investigation and disruption of attacks using NTT'S threat hunting platform
- Comprehensive incident reports
- Orchestrated remote isolation of compromised hosts
- Flexible delivery with ability for clients to approve/deny remote isolation of endpoints as recommended by the SOC
- CREST certified incident response team ready to act 24/7 with integration to SOC team
- Portal for centralized information and reports
- EDR policy management is available with Security Device Management service
- Collaborative workflow with Technical Account Manager to increase cyber resilience

Achieve your cyber-resilience goals with MDR

Advanced Analytics finds more threats

The Advanced Analytics engine leverages our big data threat intelligence and an extensive machine learning (ML) framework. Our algorithms continuously harvest vast amounts of data from exclusive sources that are applied to multiple supervised and unsupervised ML stages. We train existing ML models; extract features for new ML models; create behavior and pattern signatures; and generate IOCs. NTT is uniquely positioned to build robust detection algorithms that quickly and accurately identify suspicious and malicious activity. This is why more security incidents are initially detected by NTT methods rather than by the native detection capabilities of any single technology.

Threat hunting with evidence data

Evidence data is like having all the clues from a crime scene, enabling the detective to develop plausible theories. Security analysts use digital evidence from EDR tools and PCAP data from the Cyber Threat Sensor. The analysts hunt for threats as they pivot from one piece of evidence to another until they find an attack path that leads to a security incident.

Rapid response with remote isolation and DFIR

After detecting signs of initial compromise, it is imperative to respond as fast as possible to reduce potential impact. MDR includes response capabilities in the form of remote isolation of compromised hosts that can be actioned by NTT or client. For incident management and coordination of major incidents, the service includes CREST certified Digital Forensic and Incident Response retainer that can be activated 24/7.

Expert guidance and oversight

The Technical Account Manager (TAM) team have a wealth of security experience aligned to our 24/7 Security Operations Center (SOC). On a regular basis, the TAM provides operational support aligned to your business priorities and technology strategy. This expert technical guidance and risk-based oversight helps you stay focused on making the right decisions for your business.

Finding business efficiencies

Organizations are challenged with hiring, training and retaining expert security staff, especially if they want 24/7 security operations. The most experienced security analysts rarely work night shifts long-term. And even with unlimited budgets, some organizations realize that in-house capabilities are not the most efficient use of corporate resources. MDR delivers the security outcomes without the operational challenges so clients can confidently focus on their core business.

Get in touch

If you'd like to find out more about our MDR, or are interested in other services, speak to your client manager or contact us here: hello.global.ntt/en-us/contact-us

Why NTT?

Extensive track record
We mitigate 2 billion security threats every year.

Full lifecycle
Turn goals into outcomes through a lifecycle of services.

Next-generation analytics capabilities
Advanced analytics based on decades of ML algorithm development and threat intelligence.

Global scale
We deliver services in over 200 countries across five regions.