



Managed Security Services

Threat Detection Services

Accurately detect sophisticated security threats and speed up issue resolution

Our threat intelligence, advanced analytics and certified security analysts accurately detect known and unknown threats and provide fast mitigation.

Business outcomes

- Detection of known and unknown threats that may evade standard forms of detection
- Faster detection and response to security incidents
- Increased productivity of in-house security and incident response teams
- Existing security infrastructure investments enhanced with the power of analytics

Challenges

Businesses today are under attack from persistent and sophisticated cyber criminals who can bypass traditional security measures. These attacks bring a level of sophistication that results in a longer time to detection and response, allowing attackers more time to carry out their objectives in breached environments. The longer a breach goes undetected, the greater the commercial impact on the organization; damaged trust, brand value, share price and increased likelihood of financial penalties and fines.

No single technique or product offers complete detection from sophisticated attacks. That's why our Threat Detection Services deliver security insights and advanced protection by harnessing a number of sources, combined with our proprietary threat detection capabilities using advanced analytics, threat intelligence, threat hunting and sophisticated threat validation.

Solution

Our Threat Detection Services provides sophisticated threat detection capabilities, 24/7 threat monitoring and comprehensive threat intelligence delivered by the NTT Security Global Threat Intelligence Center. Threats are identified by analysing vast amounts of raw log data from your networks, end-points, cloud and secure access service edge (SASE). The large number of false positives typically generated gets separated from the true positives and suspicious activity is identified. By using threat intelligence, machine learning, advanced correlation and threat behavior modelling, we can accurately detect both known and unknown threats that evade standard detection techniques.

Our Threat Detection Services deliver the strong, resilient security posture needed to protect your valuable information assets against dynamic security threats.

Service packages

We offer two service plans for Threat Detection: Standard and Enhanced.

Threat Detection: Standard provides an automated service for organizations, and is underpinned by the threat detection investments and capabilities of NTT.

Threats with high confidence are sent directly to you in a report that clearly describes the security incident and makes recommendations for your incident response team.

Threat Detection Standard clients also benefit from the ongoing threat intelligence gathered. Once security incidents are thoroughly analyzed and categorized as threats, this intelligence is made available as part of the service to all clients.

Threat Detection: Enhanced service plan offers advanced detection of today's sophisticated attack types, detailed security incident investigation, guidance on incident response and more.

73% of all validated security incidents last year were detected with tools and methods developed by NTT Ltd.

As part of the enhanced services, suspicious activities and all relevant contextual information are passed to a skilled security analyst who verifies the threat and its impact. You then receive a detailed security incident report, with a comprehensive description of the incident and specific, actionable response recommendations. This enables you to significantly reduce the time required to take informed response measures.

Our security analyst will provide updates on the incident report and support your remediation activities until the incident can be closed. Furthermore, to reduce security incident response time and to prevent the spread of an infection, they can optionally take responsive actions to isolate compromised hosts.

Vendor integration and evidence collection

The Enhanced service plan provides vendor integration including evidence collection. A deep integration with multiple supported vendors and technologies enables the collection of evidence data and contextual information beyond standard device outputs.

Event-driven threat hunting

Security analysts perform event-driven threat hunting for a range of vendor technologies as part of the Enhanced service. Utilizing sophisticated proprietary toolsets, skilled security analysts gain full insight into client-monitored sources combined with machine learning, visualization, contextual information and evidence data. This approach allows the analyst to proactively uncover threats or malicious behaviors before they cause significant issues.

Services element	Service package	
Threat Detection Service	Standard	Enhanced
24/7 Security operations center	✓	✓
Services enhanced by NTT Ltd.'s Global Threat Intelligence Center	✓	✓
Continuous threat intelligence updates driven by production investigations	✓	✓
Advanced analytics with proprietary machine learning/behavioral modelling	✓	✓
Vendor integration and evidence collection for key security technologies ¹		✓
Detailed security incident investigation by security analysts		✓
Event-driven threat hunting		✓
Automated security incident reports	✓	
Security incident reports based on detailed investigation and threat hunting	✓	✓
Remote isolation of endpoints		✓
Client access to incident data and 90 days of event data	✓	✓
Client enriched and aggregated log search option		✓
Proactive response with network containment		✓
Cyber Threat Sensor		✓
Vulnerability correlation		✓
Service management		
Service delivery manager	✓	✓
Client services manager		✓

¹ Gathers and analyses additional vendor evidence data including packet capture data (PCAP), malware execution reports and host recordings.

² Endpoint containment requires the EDR solution managed by NTT Ltd.

Organizations which keep a close watch on the current threat environment **will have a significant advantage in addressing threats**. Leveraging intelligent cybersecurity to guide decisions, support business agility and maintain an acceptable risk level for the organization **is essential to success**. If your organization isn't leveraging organic threat intelligence capabilities, or actively collaborating in threat intelligence communities, **it will be at a disadvantage** while attempting to manage risk.

Summary of the NTT Global Threat Intelligence Report 2020

End-to-end managed services to meet your unique needs

We offer a holistic approach with our Cybersecurity Advisory, to help you develop a roadmap to strengthen your security posture and architect a secure hybrid IT environment.

With our full suite of integrated Managed Security Services, you can combine our Security Device Management, Enterprise Security Monitoring, and Vulnerability Management with Threat Detection to meet your unique security and compliance requirements.

Our complementary, platform-enabled Managed Network Services and Managed Collaboration Services enable you to optimize your end-to-end IT environment using leading management tools and operational automation combined with ITIL-aligned service features.

With our extensive portfolio of on-premise and cloud services, ranging from monitoring and operations to threat hunting, we can protect your intellectual property and secure your IT infrastructure.

Advisory Services

Our Cybersecurity Advisory covers the entire lifecycle of security from developing a strategy and plan aligned to your business needs, optimizing existing environments, to designing your next-generation enterprise security architecture.

Support Services

Our Uptime Support service plans improve infrastructure availability across networking, security, collaboration and communication assets. We make it easier for you to balance the cost of supporting your infrastructure against the risk of downtime.

Technical Services

We offer assessment, design, compliance and implementation services worldwide to support your existing and future applications and infrastructure.

We're a leader in the IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment.



Leader IDC MarketScape: Worldwide Managed Security Services (MSS) 2020 Vendor Assessment



Leader IDC MarketScape: Asia Pacific Managed Security Services (MSS) 2020 Vendor Assessment



2020 Asia Pacific Managed Security Services Provider of the Year



Certified for Cyber Security Incident Response and Penetration Testing, Audited for SOC Certification

The NTT Ltd. advantage



Market leading threat detection

We connect threat monitoring fuelled by rich threat intelligence, our own IP and leading tools and processes with advanced analytics and threat hunting, to accelerate threat detection and response.



Holistic and integrated Managed Security Services

We combine and integrate our security operations center and threat intelligence capabilities with our device management to deliver a better, more sustainable security posture.



End to end security capabilities at scale

We combine Managed Security Services with our Advisory, Support and Technical Services to deliver better business outcomes at scale globally.



Experience and expertise across technology domains

We have the skills and expertise to secure and manage a hybrid IT environment. We have management and operations expertise across security, networking, endpoints and applications.