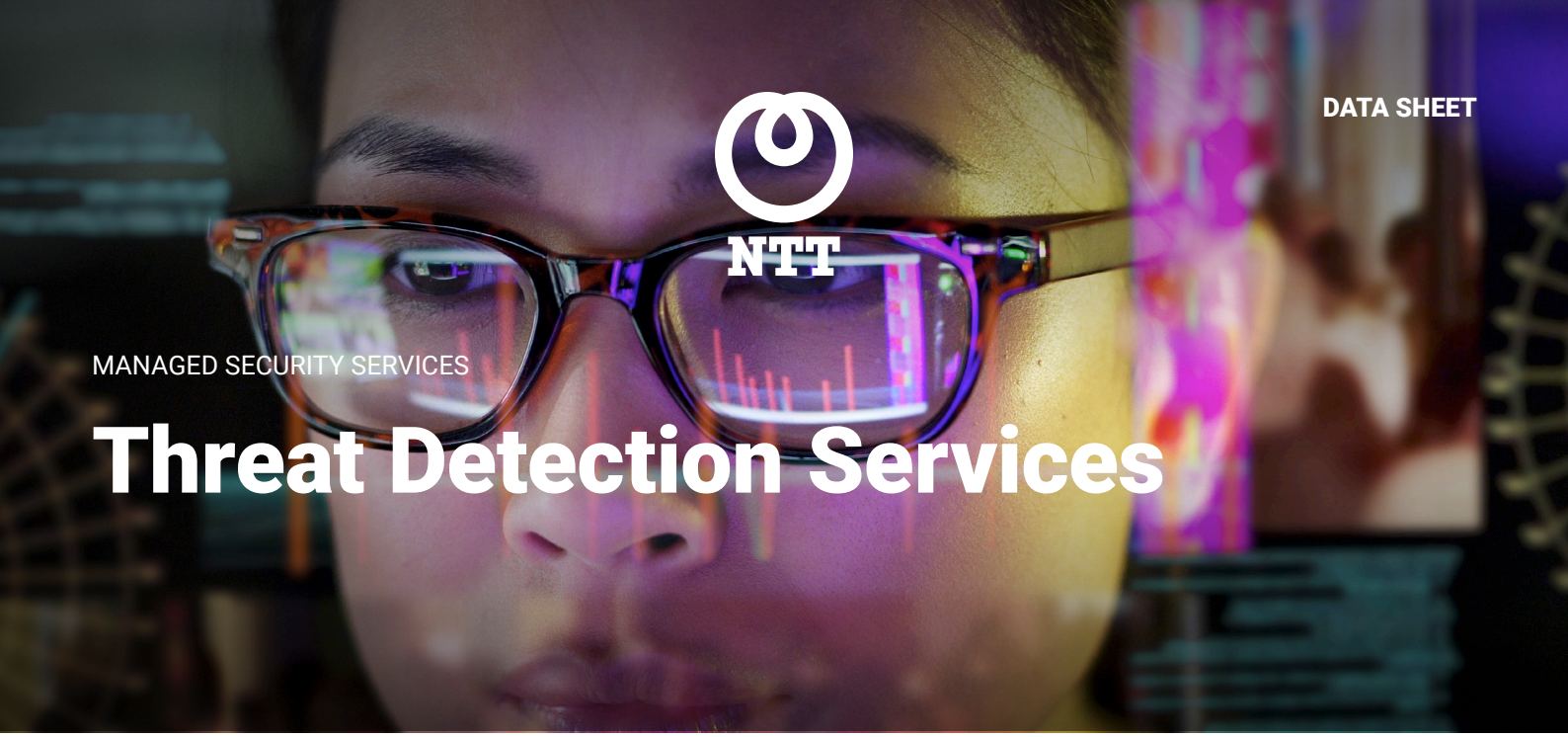

DATA SHEET

MANAGED SECURITY SERVICES

Threat Detection Services

Businesses today are under attack from persistent and sophisticated cyber criminals who are able to bypass traditional security measures.

The attacks bring a level of sophistication that results in a longer time-to-detection and response, giving attackers more time to carry out their objectives in breached environments. The longer a breach goes unnoticed, the greater the commercial impact on the organization, damaging trust, brand value and share price, and increasing the likelihood of financial penalties and lawsuits.

There's no single solution or detection technique that offers complete detection of sophisticated attacks. With this in mind, our threat detection services deliver security insights and advanced protection by harnessing a number of sources: commercially available monitored sources, combined with our proprietary advanced analytics, threat hunting, threat detection, and response capabilities.

Two service levels share common features

We provide two services for threat detection, **Threat Detection Standard** and **Threat Detection Enhanced**. Both services offer sophisticated threat detection capabilities, 24/7 threat monitoring, hunting, and comprehensive threat intelligence delivered by the NTT Global Threat Intelligence Center.

In both services, threats are identified and separated from the large number of false positives typically generated by security technologies and a security incident report is sent directly to you.

Our security analysts and automated systems engage in threat hunting and validation to verify the threat, its impact, and any additional information associated with the potential breach. You then receive a detailed summary and actionable response recommendations, enabling you to significantly reduce the time required to take informed response measures.

Advanced analytics

Today's threats utilize techniques with rapidly-changing indicators and as a result, most threat detection services cannot rely on traditional detection techniques alone. Our threat detection services utilize advanced analytics techniques to identify suspicious behavior. Using machine learning, advanced correlation, threat behavior modeling, and threat intelligence, we can accurately detect both known and unknown threats.

Threat Detection Standard

This option provides a sophisticated, automated service for organizations looking for entry-level threat detection, underpinned by our threat detection capabilities.

Security incident reports are sent directly to you, clearly describing the security breach and making recommendations for your incident response team. You can tailor the confidence level for incidents so you receive the appropriate reports.

Benefits of our Threat Detection Services

- Advanced analytics capabilities, including machine learning and threat behavior modeling, enable detection of potential security threats that may evade standard forms of detection.
- SOC security analysts with tailored analyst workbench†.
- Deeper incident investigation and validation through expert analysis with all the information at their fingertips†.
- Event-based threat hunting†.
- Actionable incident notification with recommendations.
- Incident support until resolution is achieved†.
- Proactive response with network threat containment.

†These services are only available to Threat Detection Enhanced clients

Threat Detection clients also benefit from the ongoing threat intelligence gathered by us. Once security incidents are identified and categorized as threats, this intelligence is made available as part of the service.

Threat Detection Enhanced

The enhanced service provides advanced detection of today's sophisticated attack types, through the use of advanced analytics, threat intelligence and threat hunting.

As part of the enhanced service, 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.

Our security analyst will provide updates on the incident report and support your remediation activities until the incident can be closed.

Figure 1: Service feature comparison of Security Threat Detection Standard and Threat Detection Enhanced services.

Capability	Threat Detection Services	
	Threat Detection – Standard	Threat Detection – Enhanced
24/7 Security Operations Center coverage	✔	✔
Services enhanced by NTT Global Threat Intelligence Center	✔	✔
Continuous Threat Intelligence updates driven by production investigations	✔	✔
Advanced Analytics with proprietary machine learning or behavioral modeling	✔	✔
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		✔
Customizable web portal	✔	✔
Client access to 90 days of event and incident data	✔	✔
[Option] Client raw log search		✔
[Option] Secure long-term log storage and management		✔
[Option] On-premise POD[2]		✔
[Option] NTT response to isolate compromised endpoints (Remote IR)[3] and/or network blocking of confirmed malicious URLs/IPs[4]		✔
[Option] Vulnerability Correlation with output from NTT Vulnerability Management service		✔

Threat Detection Enhanced features

Vendor integration and evidence collection

Vendor integration is offered as part of the enhanced service. A deep integration with multiple supported vendors and technologies enables the collection of evidence data such as captured traffic information, endpoint recordings, malware executional traces, and contextual information beyond standard syslog outputs.

Vulnerability correlation

Threats that target vulnerable assets increase the severity of an incident. Clients with NTT Vulnerability Management benefit from a further improved Threat Detection Enhanced service.

Event-driven threat hunting

Security analysts perform event-driven threat hunting for a range of vendor technologies as part of the enhanced service. Utilizing our proprietary toolset, Analyst Workbench, security analysts gain full insight into client-monitored sources as well as contextual information and evidence data.

Response Services

NTT analysts take responsive actions to ensure that any compromise will not spread further into the client environment. These actions include remote incident response to isolate compromised endpoints, and network blocking of confirmed malicious URLs and IP addresses.

Combining these containment capabilities with our sophisticated threat detection abilities enables clients to experience the benefits of a full Managed Detection and Response (MDR) service offering.

1. Gathers and analyses additional vendor evidence data including packet capture data (PCAP), malware execution reports, and host recordings. 2. On-premise POD is installed for clients that require or prefer that logs remain on-site. 3. Endpoint containment requires an endpoint solution managed by NTT. 4. Network IP/URL containment requires a network solution managed by NTT.

About us

NTT Ltd. is a global technology services company bringing together the expertise of leaders in the field, including NTT Communications, Dimension Data, and NTT Security. We partner with organizations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital, and secure. As a global ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace, and deliver services in over 200 countries and regions. Together we enable the connected future.

Visit us at our new website **hello.global.ntt**