NTT Security

NTT Security Targeted Threat Intelligence

Enhance Security and Improve Situational Awareness

Targeted Threats Require Targeted Intelligence

Malicious actors are increasingly targeting specific industries, organizations and even individuals. Attacks and threats can be specifically crafted for individual environments to achieve the attacker's goals. To protect themselves, organizations need proactive intelligence about the threats and malicious actors targeting them. Most organizations don't have the internal resources and expertise required to perform this research and analysis themselves.

With NTT Security Targeted Threat Intelligence, clients have access to NTT Security Threat Advisors who work on the client's behalf and threat intelligence that is relevant to the individual client. NTT Security Targeted Threat Intelligence provides clients with proactive, relevant threat intelligence they can use to increase situational awareness, identify targeted threats and potentially avoid attacks altogether.

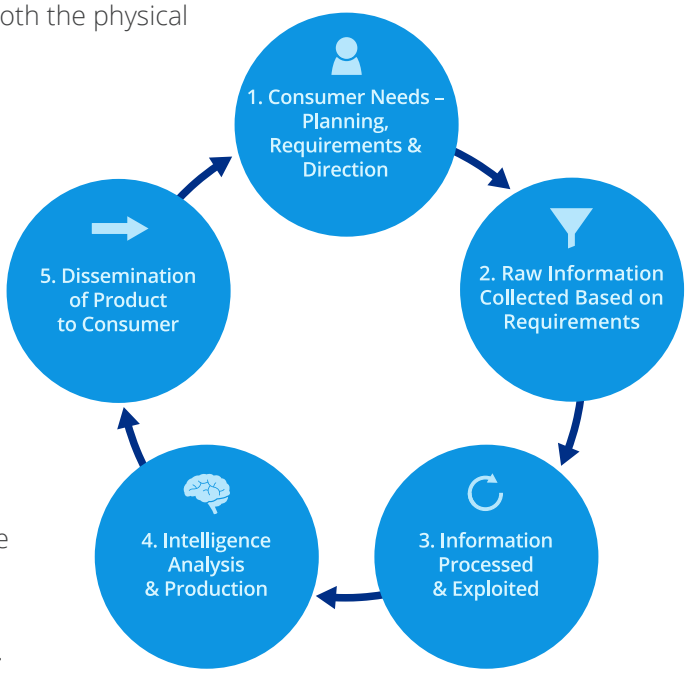
SERT Threat Advisors consume information from over 600,000 unique sources including:

- Open source intelligence
- Dark Web
- Threat intelligence feeds
- Information Sharing and Analysis Centers (ISACs)
- Niche intelligence groups
- Proprietary sources
- Attack data gleaned from the ActiveGuard® Security Analytics platform

NTT Security Targeted Threat Intelligence

NTT Security Targeted Threat Intelligence is delivered by the our Security Engineering Research Team (SERT). SERT consists of expert security researchers and threat analysts who continually collect and analyze threat information and convert it into actionable threat intelligence to protect clients. With the global nature of security threats, SERT has multilingual analysts and pulls from information sources in over seven languages. Information from both the physical and cyber realms is considered for analysis.

Unlike traditional threat intelligence feeds and automated tools, NTT Security Threat Advisors analyze and exploit information, converting it into enriched, actionable threat intelligence for each client. The service is geared toward individual client and NTT Security Priority Intelligence Requirements (PIR). This focus helps to make sure each client is getting valuable intelligence that is aligned with their priorities.



Threat Advisors also look for signs that sensitive client data, exposed credentials or intellectual property has been disclosed on the internet. These are signs a breach may have occurred and mitigation actions are needed. By proactively seeking this type of information, NTT Security is able to help clients react quickly and limit the impact of a targeted attack.

Achieve Greater Situational Awareness

NTT Security Targeted Threat Intelligence allows clients to achieve greater situational awareness of the threat environment, helping them stay abreast of potential threats and threat actors. NTT Security Threat Advisors continually monitor the threat landscape, looking for signs that attackers may target an organization.

Malicious actors may also target specific industry verticals. If NTT Security observes organizations in the same industry vertical being targeted by a threat actor or group, advance notice allows the client to take proactive steps to mitigate the impact.

Identify and Avoid Targeted Threats
Proactive identification of a threat, or the advance notice of a malicious actor, allows clients time to take action and possibly avoid the threat altogether. With increased situational awareness and advance notice, NTT Security Threat Advisors can make recommendations to defend against potential attacks before the attack is manifested. When the Targeted Threat Intelligence service is combined with our Security Log Monitoring, NTT Security engineers are able to develop custom signatures to detect targeted attacks.

Multiple Service Tiers

NTT Security Targeted Threat Intelligence is available in two service tiers tailored for each individual client.

Basic Targeted Threat Intelligence: provides threat intelligence alerts and reports. SERT Threat Advisors work with clients to understand their environment, their industry and their specific needs to establish a baseline. Using this information, SERT analysts monitor for targeted threats, exposed credentials, sensitive information disclosure and IP reputation for the client address space. Clients receive client-specific Emerging Threat Advisories, vertical market landscape analysis and reporting.

Managed Targeted Threat Intelligence: provides a Dedicated Threat Advisor who partners with the client's internal team, acting as an extension of that team. Clients are able to interact directly with their Dedicated Threat Advisor on a regular basis. This service level provides a much more comprehensive approach with manual threat research and a deeper understanding of the client environment. Clients receive quarterly executive threat briefings, advance access to SERT research, executive monitoring, threat actor dossiers and vendor monitoring. NTT Security can also provide Structured Threat Information Expression (STIX™) packages to clients for specific threats.

Brand Protection
Successful attacks can have a significant impact on an organization's brand and corporate image. This can have direct negative financial and regulatory impact. Identifying and mitigating threats early can help limit the impact of targeted threats, thereby reducing or eliminating any impact to the client's brand.

Integration with Security Log Monitoring
Gain enhanced awareness and detection of targeted threats with this proactive intelligence. Quickly identify targeted threats and design effective countermeasures. As threats are discovered, SERT Threat Advisors work with other NTT Security teams to design client and industry-specific signatures for ActiveGuard to detect. Advisors are also able to use information gleaned from ActiveGuard to validate threats and to determine if similar activities are being seen with other clients.

Additional Services

Clients are also able to add other services such as: Enterprise Credential Monitoring, Phishing Site Takedown service and Executive Monitoring. Enterprise Credential Monitoring provides additional monitoring for leaked credentials in the wild. The Phishing Site Takedown service helps to protect company brand by removing malicious sites using the client's brand in phishing campaigns. The Executive Monitoring service allows clients to monitor any threats or online sentiment directly targeting the organization's executives.

Services	Basic Targeted Threat Intelligence	Managed Targeted Threat Intelligence
Emerging Threat Advisories (ETA)	•	•
Microsoft MAPP Advisories	•	•
Monthly Security Threat Report	•	•
Quarterly SERT Research Reports	•	•
Annual Global Threat Intelligence Report	•	•
Global ActiveGuard Rules	•	•
NTT Security Minds Award Winning Blog	•	•
Client Cyber Profiling and Discovery	•	•
Client-specific IP Space Reputation Analysis	•	•
Enterprise Leaked Credential Monitoring	•	•
Enterprise Sensitive Data Leak Monitoring	•	•
ActiveGuard Threat Indicator Integration	•	•
Client-specific Emerging Threat Advisories	•	•
Vertical Market Threat Landscape Analysis	•	•
STIX Threat Indicator Packages		•
Client-specific Threat Summary Reports		•
Dedicated Threat Advisor (DTA)		•
Manual Analyst Threat Research		•
Quarterly Executive Threat Briefings		•
Advance Access to SERT Research Reports		•
Executive Monitoring		•
Threat Actor/Group Dossiers		•
Vendor Risk Management Monitoring		•

Threat Intelligence Service Features Include:

- Comprehensive client-specific view of threats
- View of existing target profile and exposed data
- Actionable intelligence specific to individual organizations
- IP reputation monitoring
- Integration with ActiveGuard detection
- Access to experienced NTT Security Threat Advisors

Managed Targeted Threat Intelligence Only:

- Dedicated Threat Advisor
- STIX threat indicator packages
- Executive Monitoring (for one executive)

Add On Features:

- Enterprise Credential Monitoring
- Phishing Site Takedown
- Executive Monitoring

Get Started Today

See how NTT Security can help optimize security, improve efficiency and ease compliance. Contact NTT Security (US) directly.

Ph: 866-333-2133
Email: us-info@nttsecurity.com

NTT Security seamlessly delivers cyber resilience by enabling organizations to build high-performing and effective security, and risk management programs with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com.**

1265DS 9/16