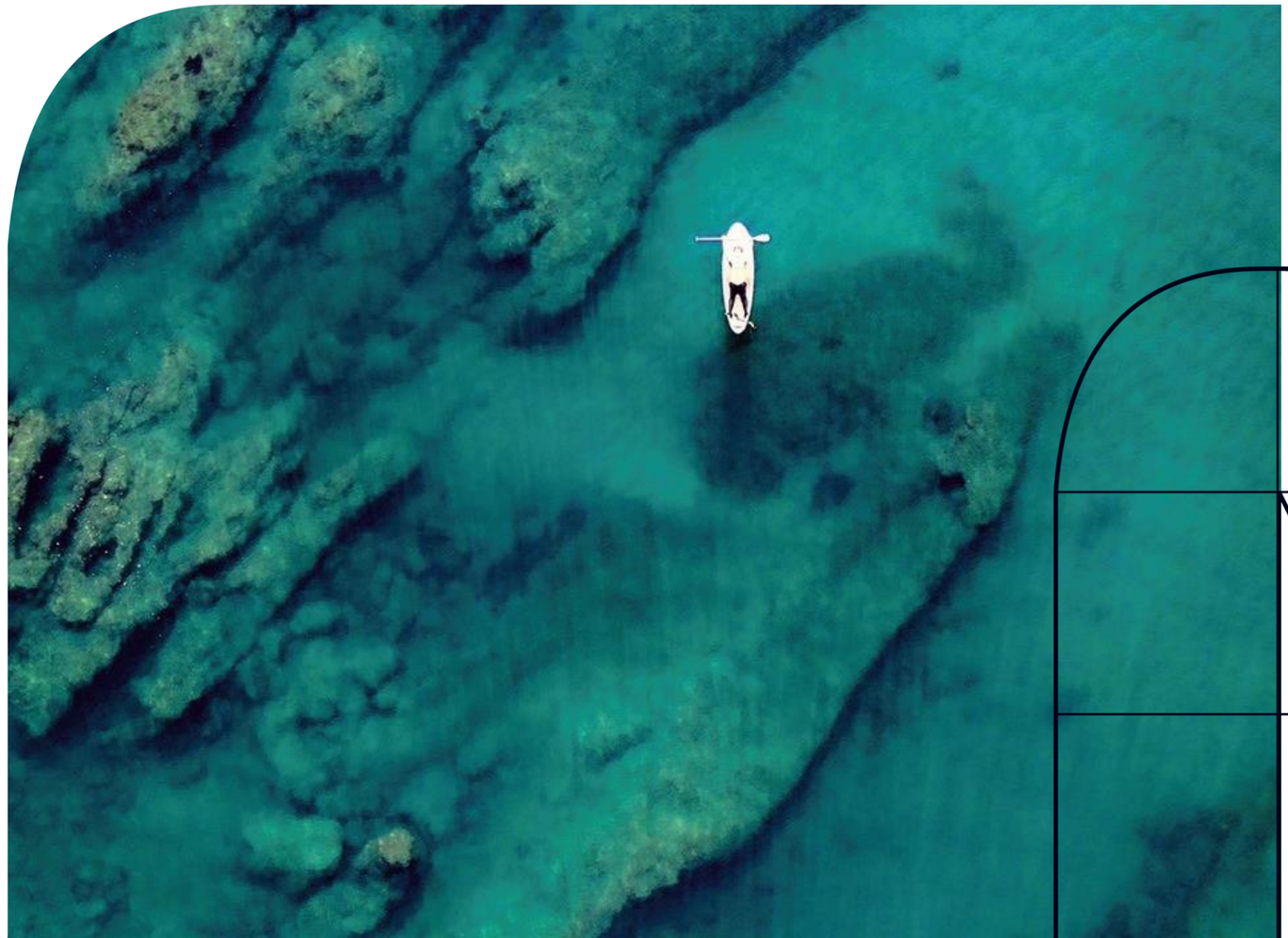
NTT DATA's
Global Cybersecurity Services



Cyber Security Department,
NTT DATA Group Corporation
E-mail: security-contact@kits.nttdata.co.jp

Index

1 Introduction

NTT DATA is developing next-generation managed security services to quickly detect and respond to cybersecurity threats. NTT DATA will make the most of the know-how it has accumulated over 30 years of experience in security operations and incident response to solve client security issues globally.
This article introduces the value that NTT DATA's Global Cybersecurity Services provide as a solution to cybersecurity threats that are advancing and becoming more sophisticated every day.

2 Recent Cybersecurity Challenges

2.1 Changes in Cybersecurity Threats

The number of IT assets, and attack surfaces that can be targeted by cyberattacks is increasing globally as companies expand overseas, diversify their supply chains, and promote remote work. The attack methods are becoming more sophisticated and advanced every day, and as security damage is spreading worldwide, governments are strengthening cybersecurity regulations (Figure 1).

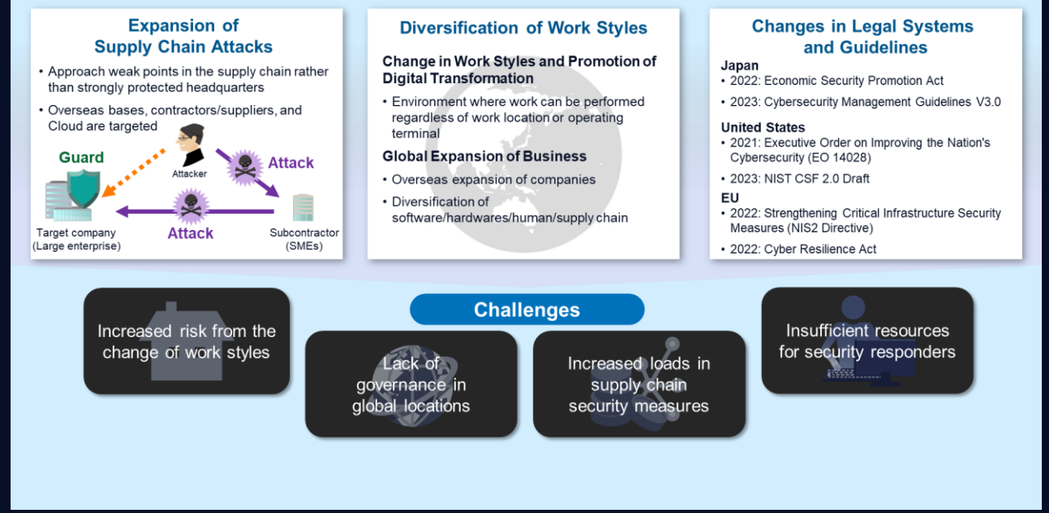
1. **Supply Chain Attacks Targeting Subsidiary Companies and Overseas Sites**
   Today's software and IT systems typically involve many stakeholders in their procurement process. In many cases, software components developed by subsidiaries or overseas offices that lack adequate security measures include component vulnerabilities or inadequacies in access management. These security risks in the software supply chain can be a prime target for attackers.

2. **Diversifying Work Styles**
   Against the backdrop of work style reforms and the spread of COVID-19, the improvement of the remote work environment has accelerated rapidly. A lot of companies have moved their business infrastructure to online services and applications in the cloud in order to work from home. On the other hand, some businesses are still forced to allow external access to their existing on-premises IT assets. Dealing with the risk of information leakage through the use of services that are not authorized by the enterprise, as well as unauthorized access to internal networks by attackers, is a major challenge.

3. **Changes in National Cybersecurity Guidelines**
   As threats and IT assets around cybersecurity change, national cybersecurity guidelines are also changing. In Japan, the Ministry of Economy, Trade and Industry revised its Cybersecurity Management Guidelines (1) to Version 3.0 in March 2023. This includes the development of an incident response system for the entire supply chain. Looking overseas, a draft version (2) of the Cybersecurity Framework (CSF) issued by NIST in the United States has also been released, with a revision to Ver. 2.0 scheduled for 2024. Similarly, the CSF focuses on ensuring security in the supply chain.

Companies urgently need to implement advanced security operations not only for their local headquarters but also for the assets and facilities of their globally distributed bases and overseas subsidiaries. The way to do this is not only to confirm the safety of IT systems through security tests at the IT system development stage but also to ensure security monitoring in normal times after the start of operations, as well as a response and recovery system in the event of an incident.

Figure 1 - Changes in Cybersecurity Threats



2.2 Lack of Highly Skilled Cybersecurity Talent

Unfortunately, the number of professionals dedicated to protecting the security of a diversified IT environment is not sufficient worldwide. According to an international security organization, there is a global shortage of 3.4 million cybersecurity personnel (3). In particular, responding to security incidents and post-convergence recovery requires a high level of expertise and skills developed through practical experience. We are required to make a comprehensive decision on the internal development of human resources responsible for these issues and the use of outsourcing to external security services, and ultimately develop an organizational structure.

3 Cybersecurity Capabilities of NTT DATA

In response to the aforementioned changes in security threats, NTT DATA has been strengthening its internal global security governance and providing advanced managed security services externally.

3.1 49 SOC locations worldwide and 7,500 cybersecurity professionals

NTT DATA has been providing cybersecurity services for more than 30 years. With 49 security operations centers (SOCs) locations worldwide and approximately 7,500 cybersecurity specialists, NTT DATA provides SOC services 24 hours a day, 365 days a year. Generally, SOC services include those that monitor the client's private environments for security information and event management (SIEM*1) and endpoint detection and response (EDR*2) and those that allow security service providers to collect and monitor client endpoints and network logs with their own log analysis environment. NTT DATA can flexibly customize and provide both types of services to meet the needs of various clients (Figure 2).

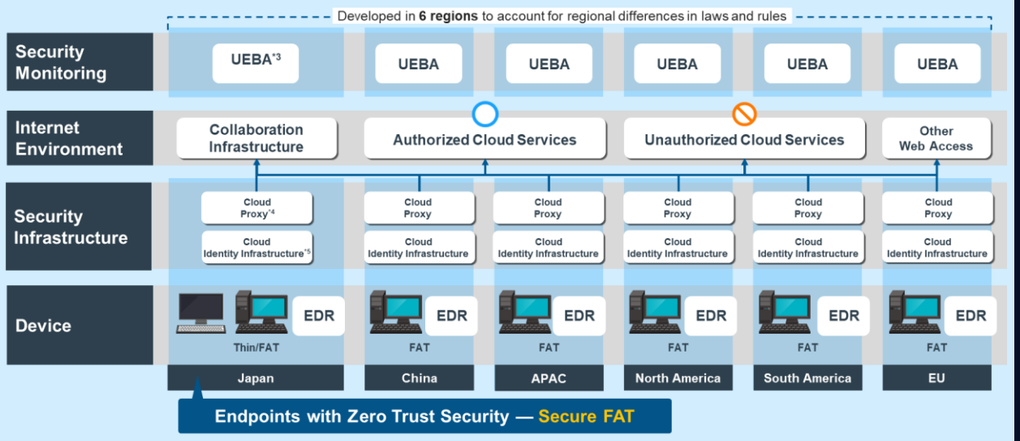
Figure 2 - NTT DATA's Global Cybersecurity Services

*1: SIEM is products and services that perform security information analysis and collection, as well as event management.
*2: EDR is a solution that constantly monitors endpoint devices such as PCs and servers to detect threats immediately if suspicious activity occurs.

3.2 Utilizing the Company's Knowledge of Strengthening Global Security Governance

As NTT DATA has expanded its overseas business over the past 10 years, it has been acquiring overseas companies with different security levels. Naturally, NTT DATA faced security governance issues at the global level, but this was resolved by realizing a Zero Trust security infrastructure that can be utilized by approximately 190,000 employees worldwide. System logs of all global sites are collected and analyzed to realize real-time monitoring operations 24 hours a day, 365 days a year. By returning the know-how we have accumulated through strengthening our own security governance to service operations, we are able to propose practical security services to our clients (Figure 3).

Figure 3 - Strengthening NTT DATA's Global Security Governance

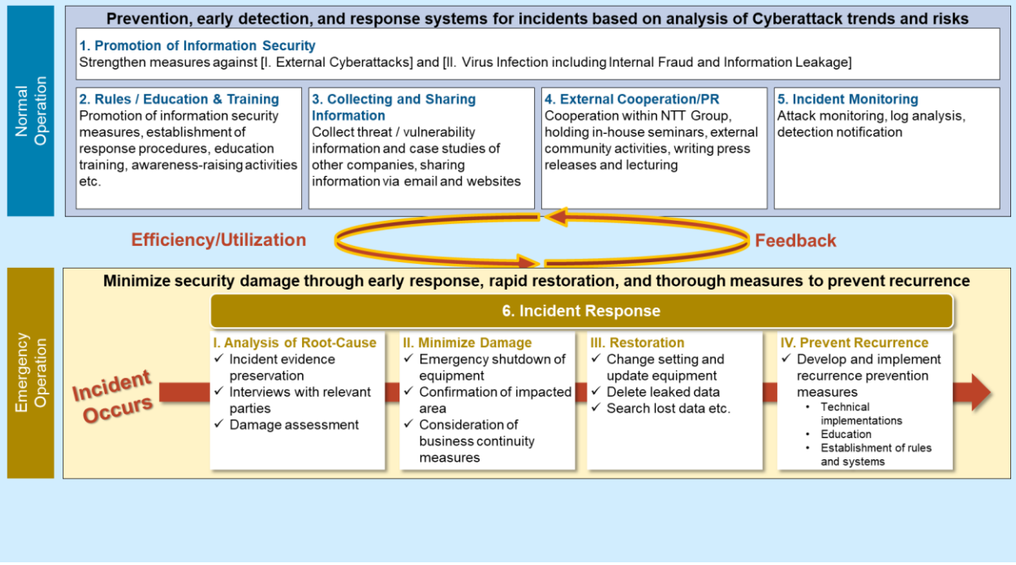


*3: UEBA (User and Entity Behavior Analytics) is a solution that aggregates logs from multiple security products, network devices, and so on to analyze the behavior of each user.
*4: Cloud Proxy is a security web proxy that runs in the cloud. It aggregates an organization's web access communications and enforces policies to provide secure Internet access regardless of location or device.
*5: Cloud identity infrastructure is a service that manages employee identity information such as IDs and passwords in the cloud.

3.3 30 years of Experience in Security Incident Response

NTT DATA has specialized international incident response organizations, including NTTDATA-CERT. In everyday activities, NTT DATA monitors cyberattacks against NTT DATA and analyzes security logs to prevent incidents from occurring. In addition, when an incident occurs, we minimize security damage through early action and take thorough measures to respond quickly and prevent recurrence. We provide our clients with the know-how we have accumulated over these 30 years of security operations and incident response experience within NTT DATA's Global Cybersecurity Services (Figure 4).

Figure 4 - Security Incident Response at NTT DATA



4 Value Provided by NTT DATA's Global Cybersecurity Services

NTT DATA has launched a globally unified cybersecurity strategy to provide one-stop support for organizations tackling cybersecurity challenges globally. NTT DATA has consolidated and standardized its long-accumulated cybersecurity expertise and evolved to consistently provide high value in end-to-end services on a global scale, from strategy to implementation of security measures, managed services, and crisis response.

NTT DATA's Global Cybersecurity Services contain 15 globally unified technology domains and provide multilingual, 24-hour, 365-day monitoring and incident response services (Figure 5). As a global One Team, NTT DATA's experienced security professionals in each country develop the technology assets necessary to provide services, sharing the know-how they have cultivated in their respective countries. NTT DATA is striving to adopt emerging technologies to stay ahead of cyber threats and is also strengthening partner collaborations and talent development globally so that multinational corporations can rely on consistent cybersecurity experience anywhere in the world. The global strategy will assist clients in overcoming the differences and challenges of each location in terms of the business environment, resources, language, culture, and laws and regulations. (Table 1).

Figure 5 - NTT DATA's Global Cybersecurity Services Portfolio

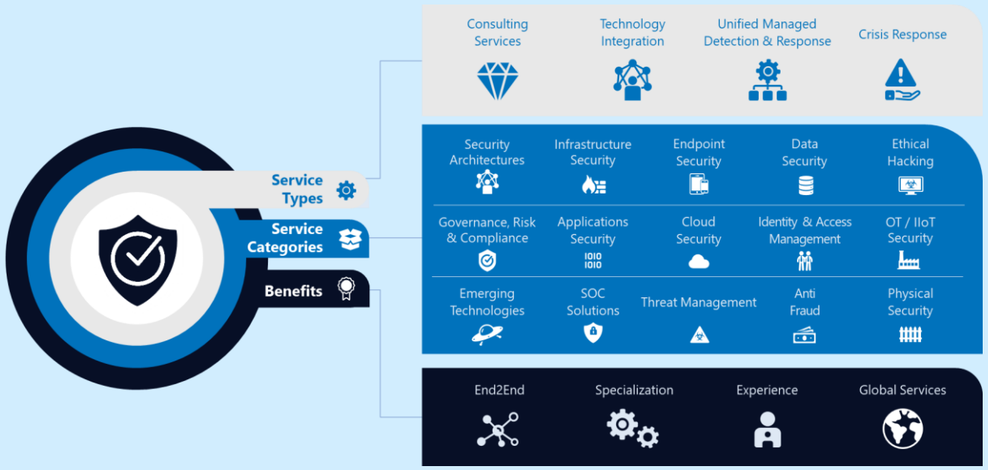


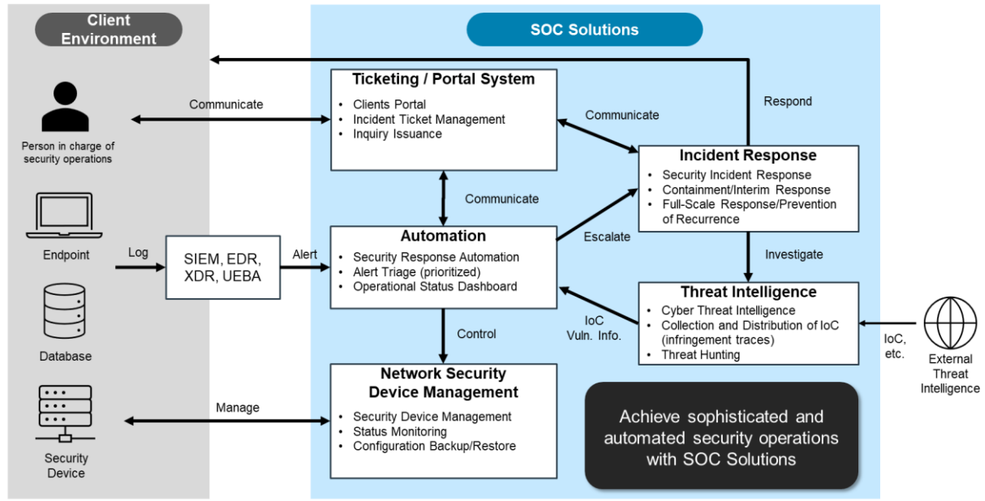
Table 1 Technology Domains Contained in NTT DATA's Global Cybersecurity Services (Excerpt)

Technology Domain	Overview
Security Architectures	The meticulous design, implementation, and assessment of a comprehensive suite of services to make your system secure and ready for Zero Trust.
Infrastructure Security	Support the identification, protection, detection, response, and recovery of an organization's network infrastructure from various cyber threats and potential risks.
Endpoint Security	Revolve around the specialized safeguarding and fortification of various endpoints with antimalware protection.
SOC Solutions	Offer a comprehensive suite of capabilities, including SIEM integration, SOAR optimization, and real-time continuous monitoring.
Governance, Risk & Compliance	Help the organization maintain compliance with regulatory requirements, mitigate risk, and uphold responsible governance practices.
Applications Security	Offer specialized measures for assessing, enhancing, and safeguarding software applications during the development and operation phase
Cloud Security	Protect data, applications, and infrastructure hosted in cloud environments.
Identity Access Management	Provide meticulous administration and precise control over user identities and access privileges to ensure secure and authorized access with an End-to-End approach.
OT / IIoT Security	Ensure the secure and uninterrupted operation of critical industrial systems and infrastructure.

4.1 Advanced Security Operations with Unique Threat Intelligence and Response Automation

SOC Solutions in NTT DATA's Global Cybersecurity Services consist of five features that solve the challenges that many companies face in achieving security operations. (Figure 6) The two most important features, Automation and Threat Intelligence, are described below.

Figure 6 - Five Features of the SOC Solutions



4.1.1 Automation

This component is a core feature of security operations. The challenge in security operations these days is to accelerate the workload required to respond to alerts and automated triage. It is very common for security analysts to be late in responding to critical alerts that indicate malware infections because they are buried in other low-severity alerts. In such a situation, analysts become exhausted by daily alert responses and are unable to promote the automation of alert analysis and response tasks through standardization, which should be the original intention.

Therefore, NTT DATA's Global Cybersecurity Services have adopted an automation platform that automates the reception of security alerts, the triage of alerts based on predefined severity and rules, the analysis tasks that link threat intelligence, and the execution of the primary response according to the playbook.

4.1.2 Threat Intelligence

As mentioned above, NTT DATA has an experienced SOC/CSIRT*6 organization in each country. These organizations have been working closely together on a regular basis, but a notable activity is that they routinely share threat intelligence (IoC) and use it in security governance and managed services in each country. They have developed their own threat information database with millions of records that they use to analyze alerts and investigate breaches in incident response in NTT DATA's Global Cybersecurity Services. Threat information discovered in a country's security operations is designed to be immediately linked to SOC operations in other locations through a threat information linkage mechanism called MISP. (4)

The value of real-time threat information linkage is that even if a trace of an attack is found in the security monitoring of a client in a specific country, it can be identified whether a similar attack is occurring in the monitoring service in another country's location, thereby contributing to the same level of security for the client globally.

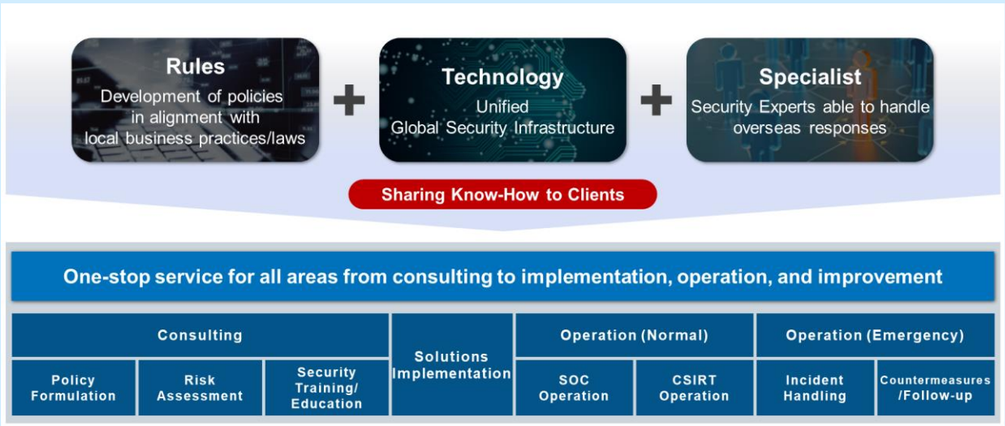
*6: Computer Security Incident Response Team. A team that responds when a security incident occurs.

4.2 End-to-End Support from Strategy to Implementation of Security Measures, Managed Services, and Crisis Response

In a typical managed security service, it is often the responsibility of the provider to operate the SOC operation, that is, to receive alerts from the security device and report the incident to the client. In such a service, it is the client's task not only to analyze the security alert but also to respond to the incident and consider how to prevent it from happening again after it has been resolved, which can increase the burden on the security department. In addition, before implementing the security operation, a global enterprise will be required to develop a security policy and assess the risk in accordance with the national legal system.

NTT DATA's Global Cybersecurity Services provide a one-stop support from consulting services that can respond to foreign-specific legal systems and guidelines, to building a security architecture and improving existing security operations. We elevate client's security to a higher level which ensures a better alignment with client organization's business objectives by creating the right structure and solution for clients' requirements (Figure 7).

Figure 7 - End-to-End Abilities of NTT DATA's Global Cybersecurity Services

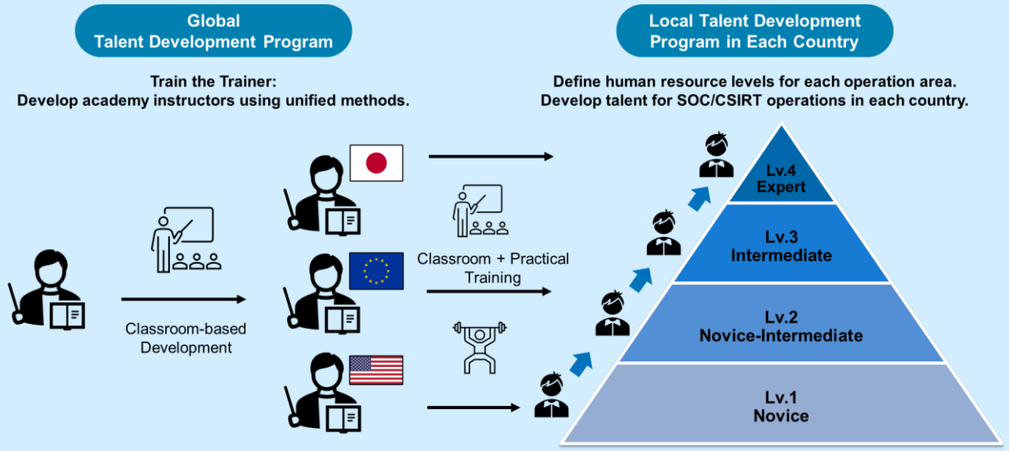


4.3 Cybersecurity Talent Development Program

NTT DATA has established the Cybersecurity Talent Development Program as an in-house project to develop advanced security personnel at the global level. The program is divided into two types: global and local. The former provides training to train instructors globally, while the latter provides training to train operators who support MDR (Managed Detection and Response) services in each country.

As specialists in MDR services, we offer hands-on programs that teach the knowledge and skills necessary for SOC operations, CSIRT operations, and malware forensic analysis. These training programs are currently designed for NTT DATA's employees, but we plan to offer them as training services for external users in the future (Figure 8).

Figure 8 - Talent Development Programs at NTT DATA



5 Conclusions

In this article, the features and values of NTT DATA's Global Cybersecurity Services were explained. The attack routes and attack methods of cyberattacks are becoming more complex and sophisticated as companies expand globally. As a leading company, NTT DATA enhances the cyber resilience of our global client companies, supports their business transformation, and contributes to the realization of a safe and secure society.

References

(1) Ministry of Economy, Trade and Industry, Cybersecurity Management Guidelines Ver. 3.0, March 24, 2023, CSM_Guideline_v3.0_en.pdf (meti.go.jp)

(2) NIST (National Institute of Standards and Technology), Cybersecurity Framework 2.0 Draft, August 8, 2023, NIST Releases Cybersecurity Framework 2.0 Draft & Implementation Examples | CSRC

(3) (ISC) ², Cybersecurity Workforce Study 2022, October 26, 2022, ISC2-cybersecurity-workforce-study–2020.pdf

(4) NTT DATA Group Corporation, MISP improves response to cyber attacks!, January 24, 2022, MISPでサイバー攻撃対応力アップ！ | NTTデータ | DATA INSIGHT | NTTデータ – NTT DATA