Data sheet

Managed Detection and Response

A next-generation approach to cybersecurity

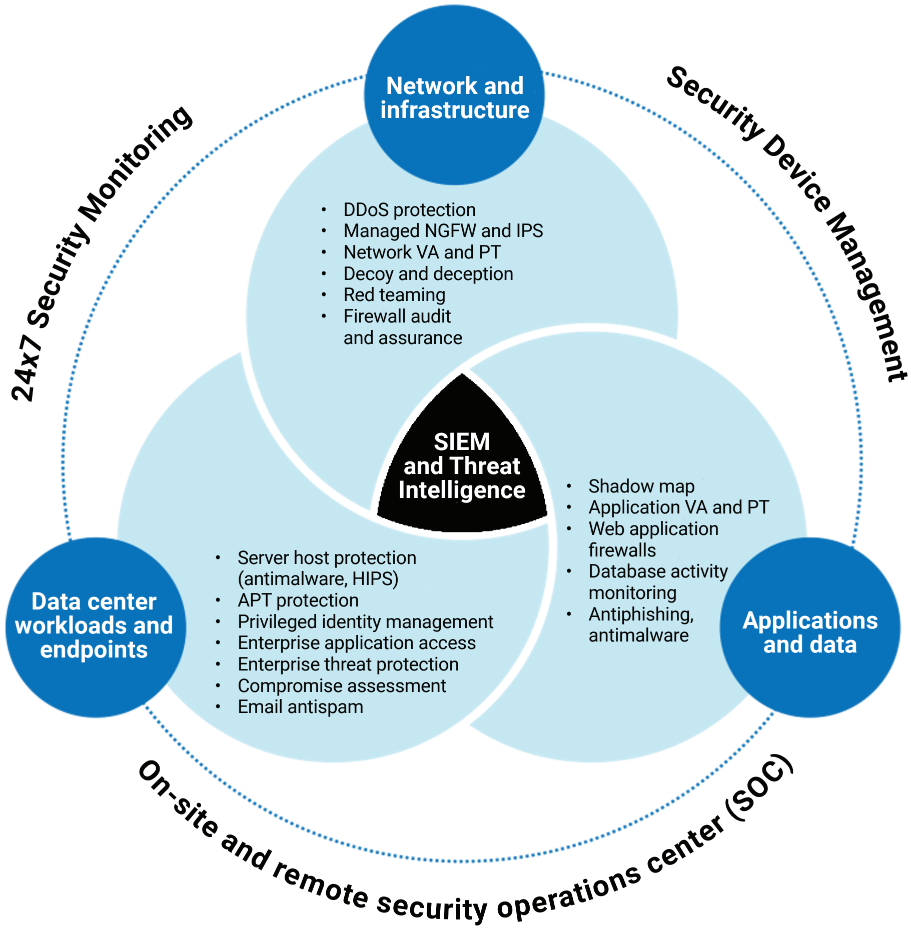
Optimize your **organization's security posture** with our **superior threat intelligence and analytics capabilities.**

Service overview

We leverage advanced technologies and service expertise to improve your ability to identify, measure, manage and mitigate information security risks. This involves enhanced focus on 24x7 monitoring and threat detection using advanced analytics, contextual threat intelligence and responsive strategic intervention. We provide rapid incident response and actionable remediation guidance.

We bring years of experience in security information and event management, security orchestration, automation and response, threat intelligence and endpoint protection to our Managed Detection and Response service. Our future-focused approach enhances traditional security monitoring, proactively keeping your organization safe from undetected security breaches.

How we deliver



Network and infrastructure

- DDoS protection
- Managed NGFW and IPS
- Network VA and PT
- Decoy and deception
- Red teaming
- Firewall audit and assurance

SIEM and Threat Intelligence

Data center workloads and endpoints

- Server host protection (antimalware, HIPS)
- APT protection
- Privileged identity management
- Enterprise application access
- Enterprise threat protection
- Compromise assessment
- Email antispam

Applications and data

- Shadow map
- Application VA and PT
- Web application firewalls
- Database activity monitoring
- Antiphishing, antimalware

24x7 Security Monitoring
Security Device Management
On-site and remote security operations center (SOC)

Security information and event management (SIEM)

Real-time threat detection and response.

Our next-generation, managed SIEM helps you manage security use cases from basic compliance and advanced correlation rules to more complex end-to-end automated responses. We support various OEMs and offer delivery options that are cloud-based, on-premises or hybrid.

With our cloud-based solution, you don't need to invest in hardware or software. You can use our SIEM infrastructure and can contract services based on events per second or log volume.

We bundle our service with commercial threat intelligence, orchestration and automation and threat hunting. Our SOC monitors alerts 24x7, analyzes them and recommends remedial methods.

Key features.

Best of both worlds

Own platform-based security services and on-premises solutions

Flexible options

SaaS-based pricing and easy deployment of an SLA-driven service

End-to-end capabilities

A fully managed, customizable SIEM solution with 24x7 support

Fully automated alerts

Centralization, correlation, analysis and retention of event data to generate automated alerts

Stronger compliance

Meet regulatory and compliance requirements and audit support

Comprehensive outlook

Get a bird's-eye view of the security landscape through log data and audit trails

Optimized and value-added total cost of ownership

Delivered through effortless deployment and efficient SOC support

24x7 threat hunting

Real-time monitoring with proactive hunts to reduce risk and uncover malware, threats and incidents

Security orchestration, automation and response (SOAR)

We assist organizations looking for a mature SOC with SOAR capabilities that augment SIEM.

Our SOAR services are a combination of three services: security orchestration and automation, our security incident response platform, and our threat intelligence platform. They typically involve:

- Automated processing of security information, event management or SIEM alerting, and threat intelligence.
- Orchestration of workflow elements (data collections, approvals and audit-based markers).
- Added implementation or support of a response procedure or action.

Key Features

Faster incident response

Through the automation of repetitive manual tasks and custom, intuitive playbooks with express countermeasures

Lower false positives

Our automated SOC workflows with optimized playbooks improve analyst participation and failover or cross-correlation capabilities

Enhanced visibility

On-time threat intelligence, vulnerability and malware management, and MITRE ATT&CK framework mapping create an optimized security landscape

> We bundle our service with **commercial threat intelligence, orchestration and automation and threat hunting.**

Threat intelligence

We offer threat intelligence as a service and offer expertise on enhancing preventive capabilities in your existing security products.

Targeted attacks are becoming more sophisticated. Organization-specific threat intelligence is required to ensure near-zero false positives, avoid critical information being compromised, and enhance your security posture.

Key features

Advanced analytics

- Predictive analytics deployed early in the kill chain
- Trend analysis over time

Actionable intelligence

- Identify your real weaknesses and reduce false positives
- Augment threat hunting and incident response

Deception technology

- Client-specific threat intelligence
- Early intelligence with decoys and deception

Endpoint detection and response (EDR) and endpoint protection platform (EPP)v

Our response to the challenges posed by the lack of next-generation antivirus tools in the market is the powerful Secure-Host solution.

This software-as-a-service-based solution offers advanced endpoint protection with automated detection and response capabilities – a unique combination that gives you the confidence to detect and prevent advanced targeted attacks.

Next-generation antivirus (NGAV) analyzes behavior and threats on a single endpoint. EDR services consolidate data across all endpoints to provide a complete picture of potential advanced threats and improve your SOC detection and response capabilities.

Advanced decoy and deception are a core component of our defense strategy. They lure, detect and defend against potential attacks in real time using powerful emerging technologies.

Key features

Combination of NGAV and EDR

AI solution to detect zero day exploits; understand complex alerts with MITRE ATT&CK-based detectio

Patented kernel-based protection

Protects from malicious executables written to disk, and fileless attacks

Automated response actions and forensics

Response by containment or remediation; forensics through investigation or root cause analysis

Pre- and postinfection protection

Defuse threats in real time

Security Operations Center (SOC)

Built on the three fundamental pillars of people, process and technology, our SOC services bolster your security posture by uncovering all major network susceptibilities and remediating them.

Our state-of-the-art SOC is ISO 27001 certified and CERT-In empaneled. A powerful combination of advanced technology innovations and a highly skilled team allows us to offer round-the-clock SOC services to monitor, prevent, detect, analyze and respond to cybersecurity incidents.

We provide real-time threat monitoring and response, 24x7 security, device management and professional services such as audits, red teaming and breach assessments.

Our SOC services are available as a remote shared model, an on-site dedicated team, or as a hybrid approach combining a dedicated team with the additional scalability and expertise of the remote SOC.

Key features

Complete managed SOC services

Pay-as-you-use approach to security

Round-the-clock

24x7 log collection, active monitoring and incident response

Real-time services

Real-time threat intelligence and correlation aligned to current business risks

Advanced capabilities

Security orchestration and response, advisory reports and collaboration

Specialized skills

Event-based threat hunting, honeynet intelligence and more

Why NTT

Extensive global track record
Our security specialists mitigate billions of security threats every year.

Superior client experience
Our clients benefit from comprehensive analytics, service delivery and ongoing process development.

Financial stability
We're a leading global technology services company.

Deep investment
We invest in innovative solutions and groundbreaking service development.

Get in touch

If you'd like to find out more about our Managed Detection & Response service, speak to your Client Manager or visit our website