Managed Extended Detection and Response

One platform to improve business resilience through cyber resilience

How quickly can you respond to a cyberattack?

- Too many security tools
- Too many false alerts
- Outdated threat prevention tools
- Lack of true AI-driven threat intelligence

If any of the above challenges are familiar to you, your ability to quickly respond to a cyberattack is greatly inhibited.

4 million*

2023 global cybersecurity workforce gap. Up 13% from 2022

The power of NTT DATA's Managed Extended Detection and Response (MXDR) and Palo Alto Networks Cortex XSIAM is that it converges SOC capabilities, such as XDR, SOAR, ASM and SIEM, into a single platform that eliminates console switching and streamlines security operations. It combines orchestration, automation and AI-driven threat intelligence leading to improved operational, financial and staff resilience to augment your security teams.

*ISC2 Cybersecurity workforce study 2023, Nov 2023

Eliminate console switching. Streamline security operations with one platform.

MXDR with Cortex XSIAM provides a robust defense against complexity while improving security posture.

One security console

Resilience: End-to-end integrated and automated services that secure digital transactions, protects information and data and deters downtime to ensure workforce productivity.

270x faster MTTR (Mean-Time-To-Resolution) *

Improved speed and efficiency: Through orchestration, automation and AI-driven threat intelligence and digital forensics.

*Services Company case study, Cortex XSIAM

10x improvement in incident closure rates *

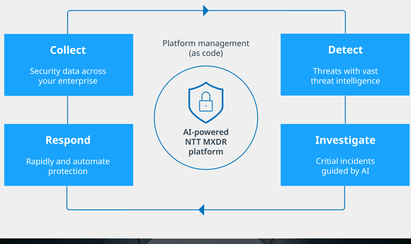
Less complexity: Provides a unified view of security across the organization.

*Watch Cortex XSIAM video testimonial here

Reduce false positives by 99%

By combining AI and intelligence from our SOC analysts and experts, we can reduce the false positive rate by up to 99%.

AI-powered NTT DATA MXDR platform



MXDR capabilities include:

- 24x7 security monitoring and detection
- Threat hunting
- Automated response
- Endpoint protection
- Playbook as a service
- Digital forensics and incident response
- Threat intelligence

Immediate value received from MXDR

Block known and unknown attacks

Block malware, exploits and fileless attacks with intergrated AI-driven antivirus and threat intelligence using endpoint protection.

Gain visibility across all data and detect sophisticated attacks 24/7

- Collect and correlate data from any source to detect, triage, investigate, hunt and respond to threats.
- Use out-of-the-box analytics and custom rules to detect advanced persistent threats and other covert attacks.

Avoid alert fatigue

Simplify investigations with automated root cause analysis and a unified incident engine, reducing the number of alerts the SOC team needs to review and lowering the skill required for triage.

Shut down advanced threats restore hosts after a compromise

Quickly recover from an attack by removing malicious files and registry keys, as well as restoring damaged files and registry keys using remediation suggestions.

Extend detection and response to third-party data sources

Enable behavioral analytics on logs collected from third-party firewalls while integrating third-party alerts into a unified incident view and root cause analysis for faster investigations.

To learn more about NTT DATA and Palo Alto Networks MXDR services, speak to your client manager or contact us online.

Join the conversation