Microsoft MDR (Managed Detection & Response) Services

Do you have a Microsoft Security Ecosystem but unsure how to effectively utilize it for your cyber resilience journey?

BENEFITS

- No additional tools need to be deployed, use what you have. Flexible OpEx model
- Review & configure policies based on offensive security tactics & principles
- Identity-centric architecture that allows an identity to be isolated instead of isolating an entire infrastructure in the event of a breach
- Tactical incident response & dedicated threat hunters that continually evaluate alerts and hunt for questionable activity in your environment
- Eliminate vendor sprawling & consolidate technology abilities

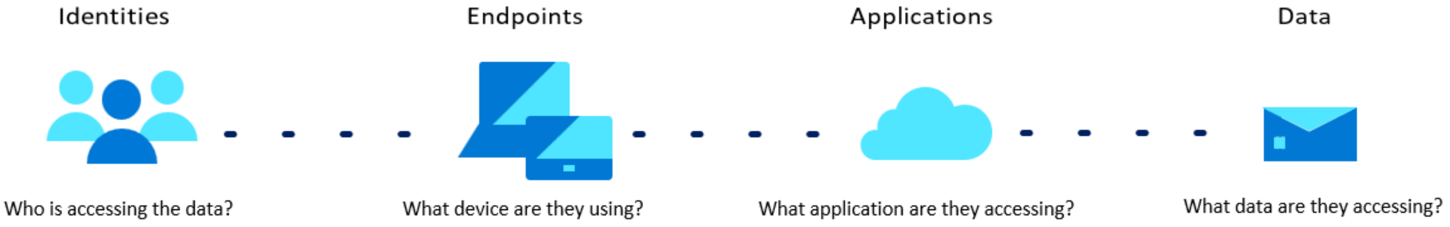
The Attack Surface

The attack surface has shifted from a perimeter-centric architecture to an everywhere-centric architecture. The attack surface moves with your employees and assets. Today's sophisticated cyber-attacks are no longer exclusive to endpoints. They are multifaceted and target identities, email, infrastructure, cloud platforms, servers, databases, and more. Endpoint-centric detection and response solutions alone do not provide the visibility and response capabilities required to identify and neutralize broader cyber-attacks.

"*Identity is the new perimeter*", a methodology that lives in our DNA. Think about your passport when you travel, and your ID or license wherever you go, identity has always been centric around our ability to access something. We use our identity-centric methodology to help customers use Microsoft technologies to reduce the attack surface to a containable environment that is centric on identity to ensure that we control the architecture where data resides and what the conditions are to access the data.

Service Overview

NEC XON offers clients an end-to-end portfolio of consulting, implementation, and managed security services, all powered by Microsoft's security technologies and designed to expand on your existing Microsoft security tools investment to increase business profitability and cyber resilience by countering the emerging cyber threat landscape with tools you already have at your disposal.


Identities
Endpoints
Applications
Data
Who is accessing the data?
What device are they using?
What application are they accessing?
What data are they accessing?

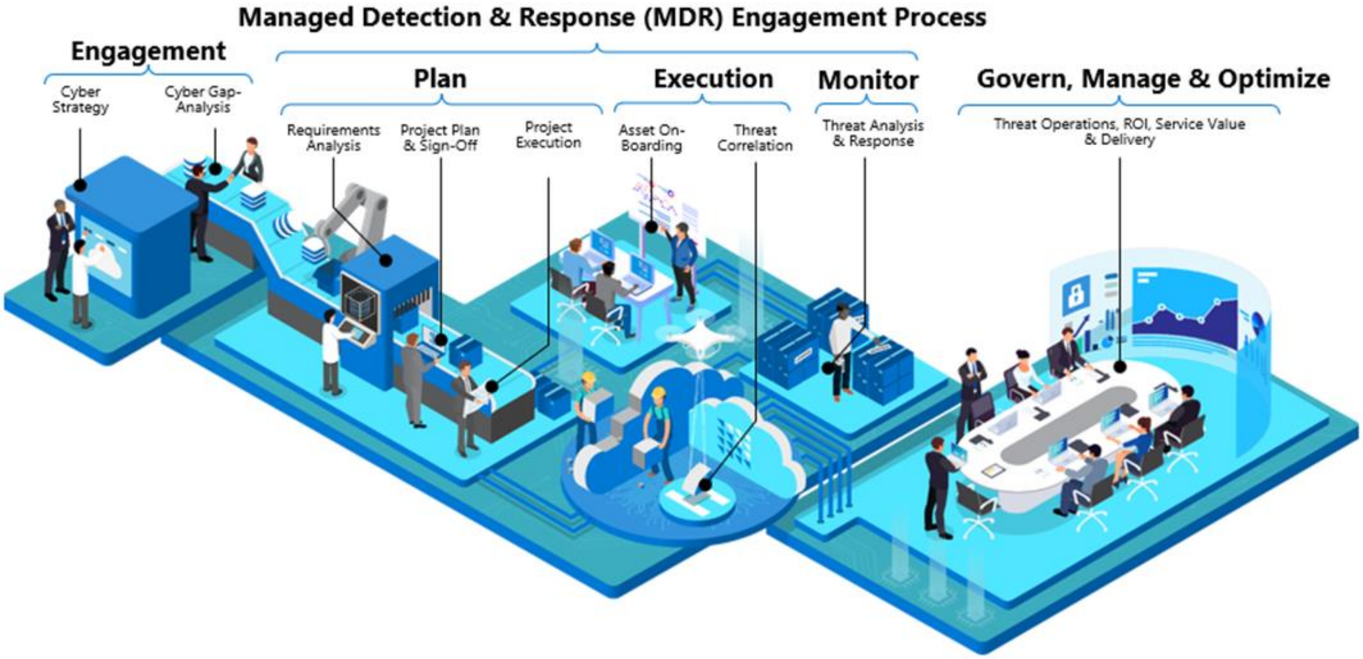
Explore the NEC XON MDR Program

Flexible to meet your cyber needs. Cost-effective to meet your budget.

1
Select a package

2
Start the Engagement Process

3
Modernize and maximize your ROI with cyber resilience



Why us?

- The NEC XON Managed Detection and Response service keeps organizations and their sensitive data safe from advanced attacks that traditional perimeter-centric, signature and log-based security tools alone have not prevented. The MDR service is built on a foundational adversarial-based mindset to ensure that our threat analysis is based on realistic attack strategies & methodologies. Our Threat Analysis Team is staffed by a team of highly trained & threat-mindset security analysts and incident responders who proactively hunt for threats, fully investigate and respond to detected threats, and stop attacks before they cause any business disruption.

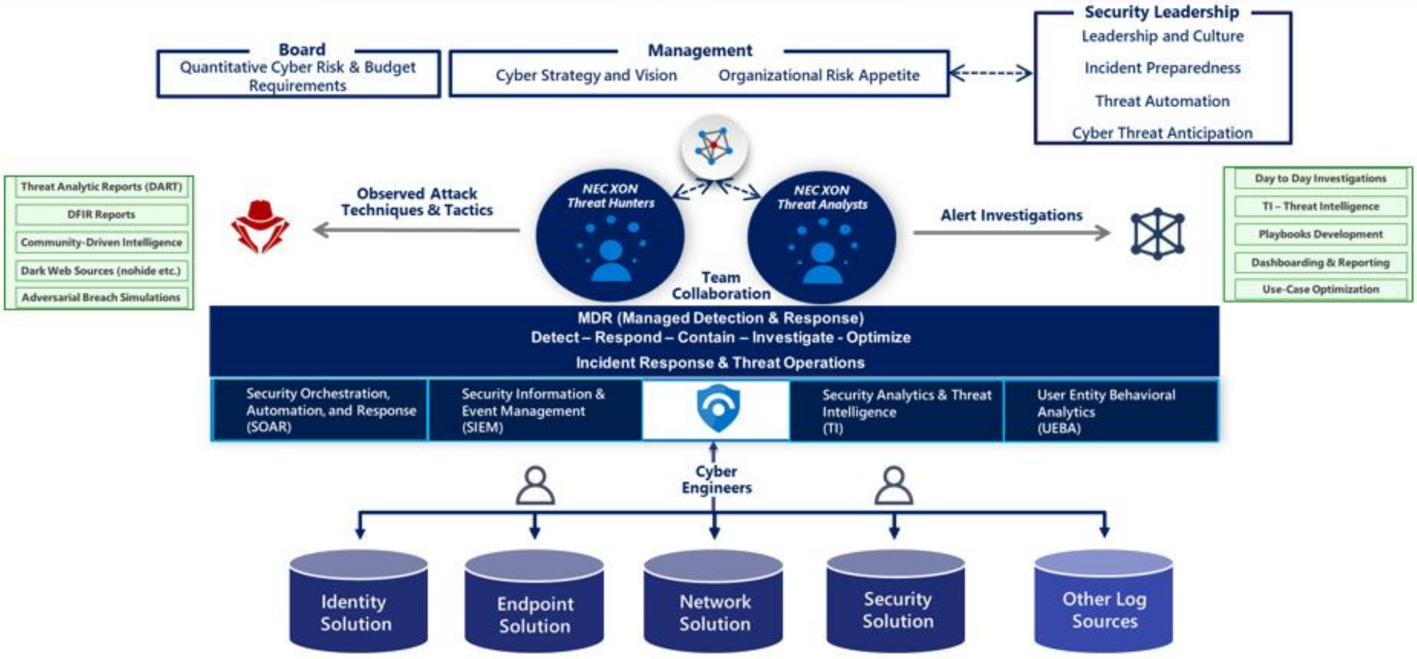
We have you covered!

- Our MDR service delivers enterprise-grade security detection & response capabilities to organizations of all sizes. Augment your existing cyber solutions with proactive threat hunting or have us act as your trusted security team running the NEC XON MDR service. With NEC XON MDR, you gain a competitive edge with the benefits of an unmatched security approach and a unified security operations platform that has been designed to protect the most complex environments based on realistic adversarial attack tactics, methodologies & strategies.

Increase Cyber Resilience

- See across all ports and protocols, endpoint activities, lateral movement, and data theft
- Get deeper insights into what is happening in your network
- Automate response by jumpstarting playbooks, preventing malware, terminating attacks from multiple angles, and stopping data theft — within seconds or minutes, not days or hours
- Detect threats in real-time and retroactively by analyzing network and endpoint metadata based on observed attack techniques
- Lure attackers and malicious insiders away from critical assets and data to decoys and breadcrumbs that look and feel real
- Continuous incident response with root cause analysis to improve and continually optimize

Tactical Service Overview


Board
Quantitative Cyber Risk & Budget Requirements
Management
Cyber Strategy and Vision
Organizational Risk Appetite
Security Leadership
Leadership and Culture
Incident Preparedness
Threat Automation
Cyber Threat Anticipation
Threat Analytic Reports (DART)
DFIR Reports
Community-Driven Intelligence
Dark Web Sources (nohide etc.)
Adversarial Breach Simulations
Observed Attack Techniques & Tactics
NEC XON Threat Hunters
NEC XON Threat Analysts
Team Collaboration
Alert Investigations
Day to Day Investigations
TI – Threat Intelligence
Playbooks Development
Dashboarding & Reporting
Use-Case Optimization
MDR (Managed Detection & Response)
Detect – Respond – Contain – Investigate - Optimize
Incident Response & Threat Operations
Security Orchestration, Automation, and Response (SOAR)
Security Information & Event Management (SIEM)
Security Analytics & Threat Intelligence (TI)
User Entity Behavioral Analytics (UEBA)
Cyber Engineers
Identity Solution
Endpoint Solution
Network Solution
Security Solution
Other Log Sources

*Other refers to another log source such as firewalls, network detection solutions etc.

Simplified Threat Hunting (KQL – Kusto Query Language)

External Hunting

- ✓ Perform continuous external attack surface assessments to find external intrusion points
- ✓ Review & monitor for any credential leaks with active account mitigation to prevent them from being abused
- ✓ Threat Research, Digital Forensics and Incident Response (DFIR) to learn & counter the latest observed adversarial TTPs (Tactics, Techniques & Procedures)

Internal Hunting

- ✓ Investigate detected alerts to find the source "*Root Cause*" activity that led to the initial alert
- ✓ Monitor all user/service account activity for any suspicious authentication requests & overall behavior
- ✓ Hunt & analyze of any lateral movement opportunities to determine the probable attack paths and action for mitigation as a proactive control approach

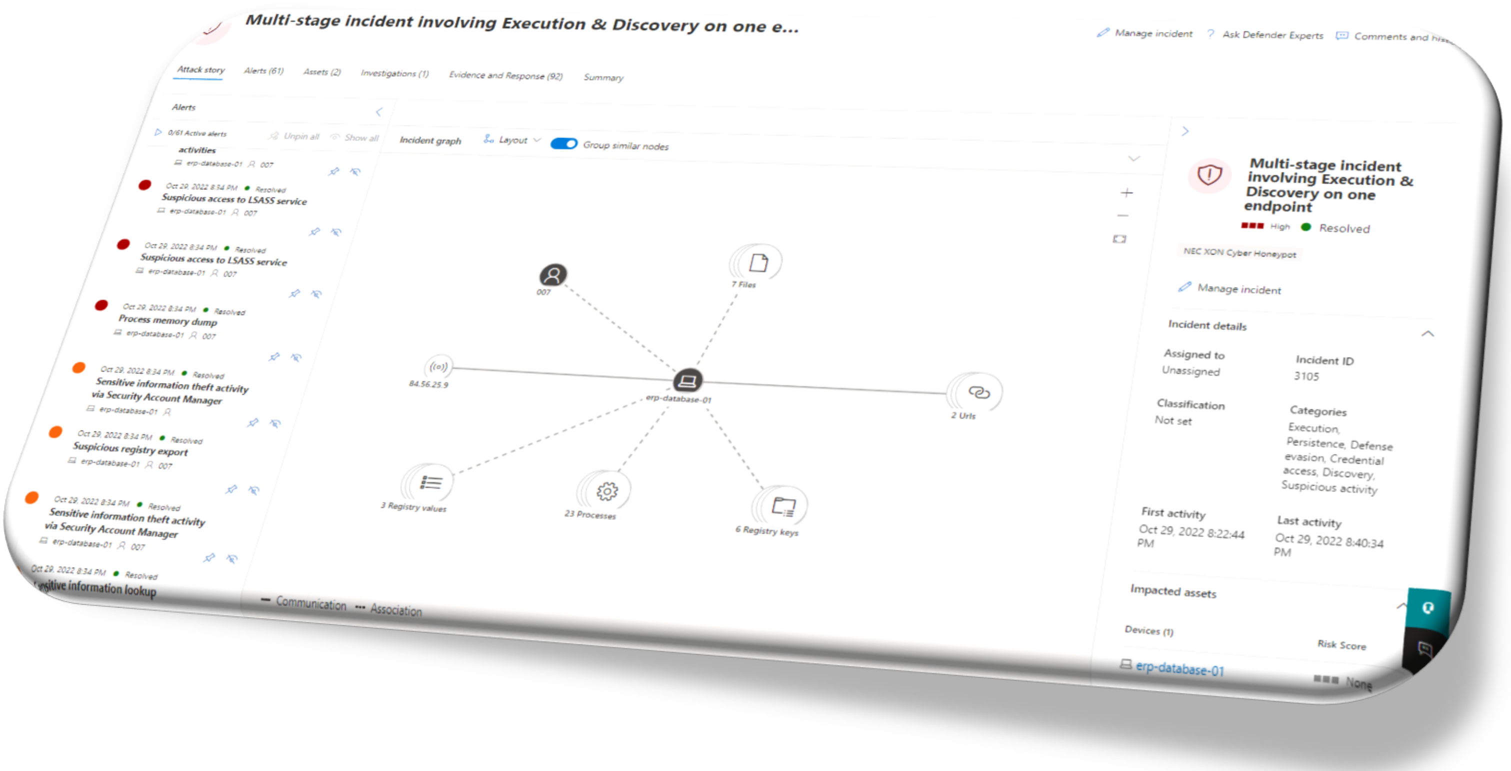
Enriched Hunting Sources

- ✓ Research the latest vulnerabilities and methods to determine how they are abused to achieve desired illicit objectives
- ✓ Compare alerts to other customers to determine the customers breach probability & susceptibility to being targeted
- ✓ Plan & Execute BAS (Breach & Attack Simulations) to test the overall detection capabilities and verify the current protection safeguards

Simplified Adversarial Containment

- ✓ Disable/Change Account Password
- ✓ Isolate Source (Identity/Endpoint)
- ✓ Re-Route Network Pathways
- ✓ Disrupt the adversaries attack blueprint
- ✓ Block IOC (Indicators of Compromise) across all sources

Platform Overview



activities
erp-database-01 007

Oct 29, 2022 8:34 PM ● Resolved
Suspicious access to LSASS service
erp-database-01 007

Oct 29, 2022 8:34 PM ● Resolved
Suspicious access to LSASS service
erp-database-01 007

Oct 29, 2022 8:34 PM ● Resolved
Process memory dump
erp-database-01 007

Oct 29, 2022 8:34 PM ● Resolved
Sensitive information theft activity via Security Account Manager
erp-database-01

Oct 29, 2022 8:34 PM ● Resolved
Suspicious registry export
erp-database-01 007

Oct 29, 2022 8:34 PM ● Resolved
Sensitive information theft activity via Security Account Manager
erp-database-01 007

Oct 29, 2022 8:34 PM ● Resolved
sitive information lookup

Multi-stage incident involving Execution & Discovery on one endpoint
■■■ High ● Resolved
NEC XON Cyber Honeypot
Manage incident

Incident details

Assigned to
Unassigned

Incident ID
3105

Classification
Not set

Categories
Execution, Persistence, Defense evasion, Credential access, Discovery, Suspicious activity

First activity
Oct 29, 2022 8:22:44 PM

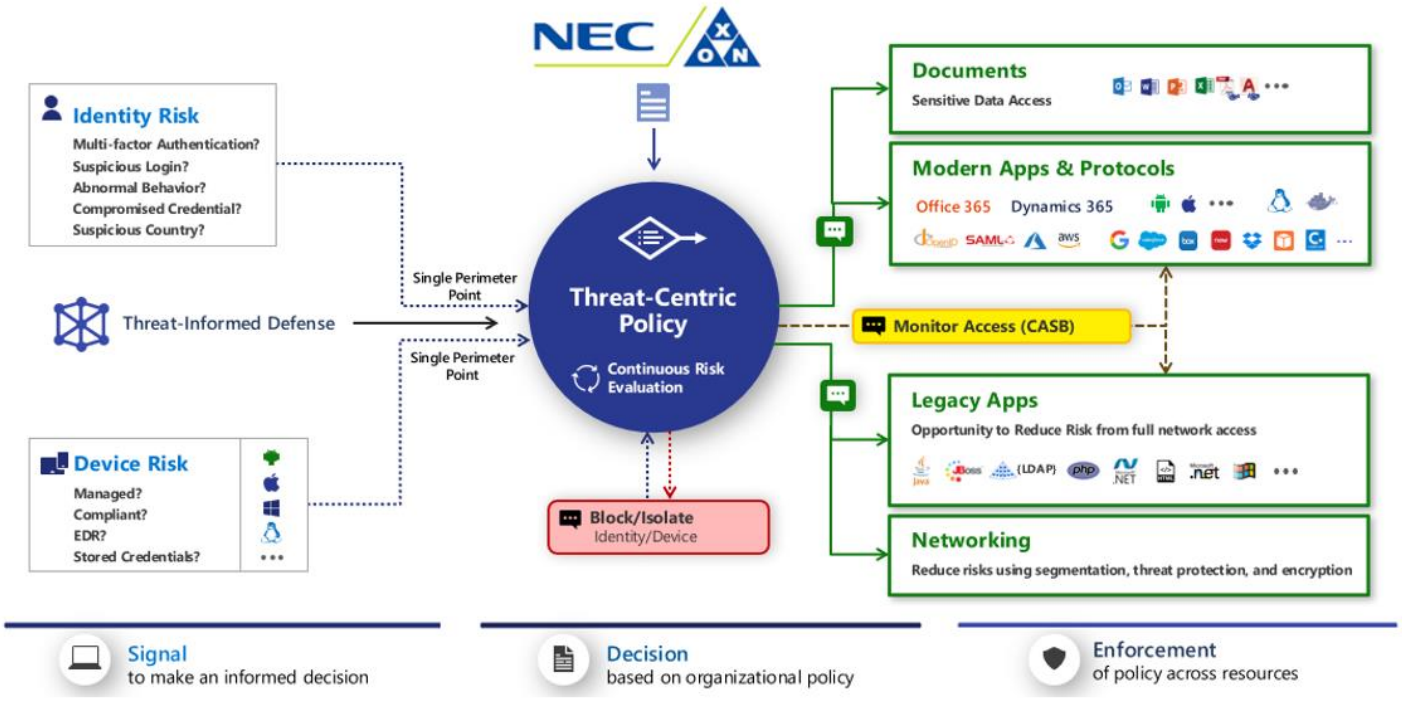
Last activity
Oct 29, 2022 8:40:34 PM

Impacted assets

Devices (1)
Risk Score
erp-database-01 ■■■ None

Figure 1: Hands-on-keyboard breach detected by custom NEC XON rules

Our Zero-Trust Model



Solution Features

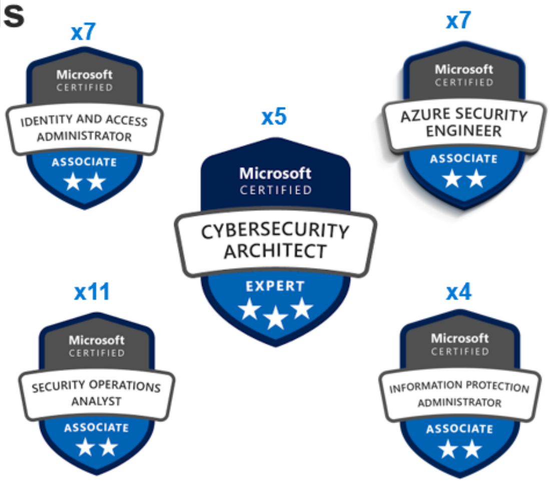
Microsoft Sentinel / Microsoft 365 Defender (XDR)

- Threat Detection & Response
- Proactive Threat Hunting & Incident Response
- Microsoft 365 Defender (XDR) Management
- Identity-Centric Architecture Development (MFA – Identity Protection - Conditional Access – SAML – RBAC - PIM)
- Threat Alert Tuning
- Breach & Attack Simulations (BAS) with Cyber Attack Strategies
- Attack Intelligence, Disruption & Neutralization
- Technology Optimization & Threat Capability Improvements
- Microsoft Sentinel (Optional) Setup + Log Ingestion

Our Partnership Status

Microsoft
Solutions Partner
Security

Our Skills



Interested? Visit the below link and complete the form with your selected package
Contact form: https://www.nec.xon.co.za/contact-us/

NEC XON (Pty) Ltd
1 Mints Street, Old Mint Park
Louwlardia 1683, South Africa

About NEC XON
We deliver advanced solutions to government, telecommunications providers, mobile network operators, network service providers and enterprise. The comprehensive and tightly integrated offering across infrastructure, safety, communications and digital provides carrier-grade solutions with enterprise-class services, maintenance and support.