

# Managed Detection & Response

with Microsoft Defender XDR

# Service Description & Key Capabilities

Neurosoft's MDR with Microsoft Defender XDR provides full lifecycle operation of your EDR-XDR environment, combining advanced detection engineering, enriched investigations, and coordinated response across your entire ecosystem.

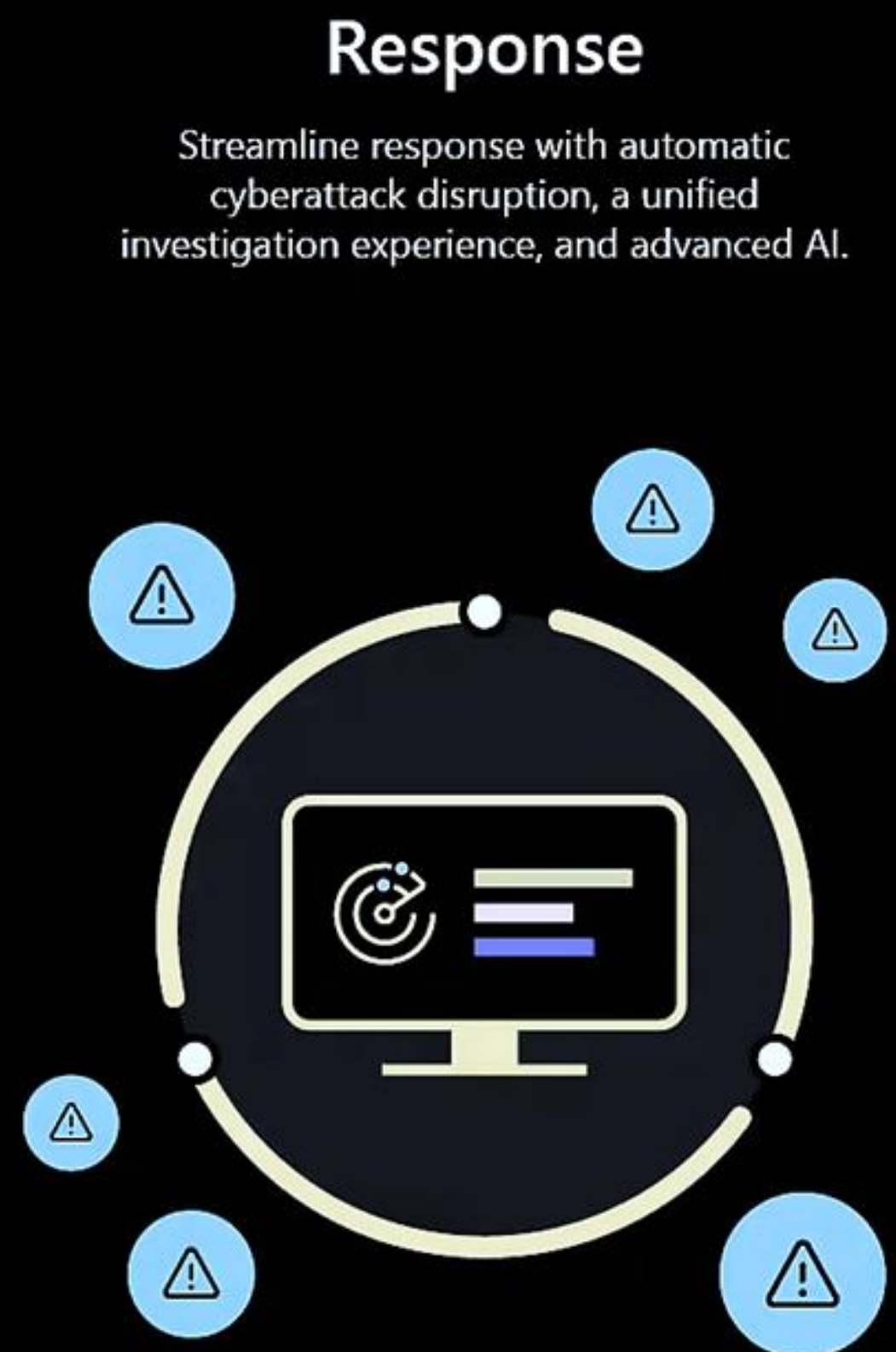
- End-to-end Microsoft Defender XDR management and tuning
- Custom detection rules aligned to attacker techniques & TTPs
- Continuous threat hunting across all Defender telemetry
- Intelligence-enriched investigations powered by Hackcraft Team insights
- SOAR-orchestrated response beyond EDR across identity, network, cloud & ITSM
- Easy expansion into a full Microsoft Sentinel-powered SOC





# Service Description & Key Capabilities

Achieve faster, more accurate threat detection and response through Microsoft XDR's expanded visibility and automated investigation capabilities, amplified by Neurosoft's MDR analysts who continuously hunt, validate, and contain attacks.



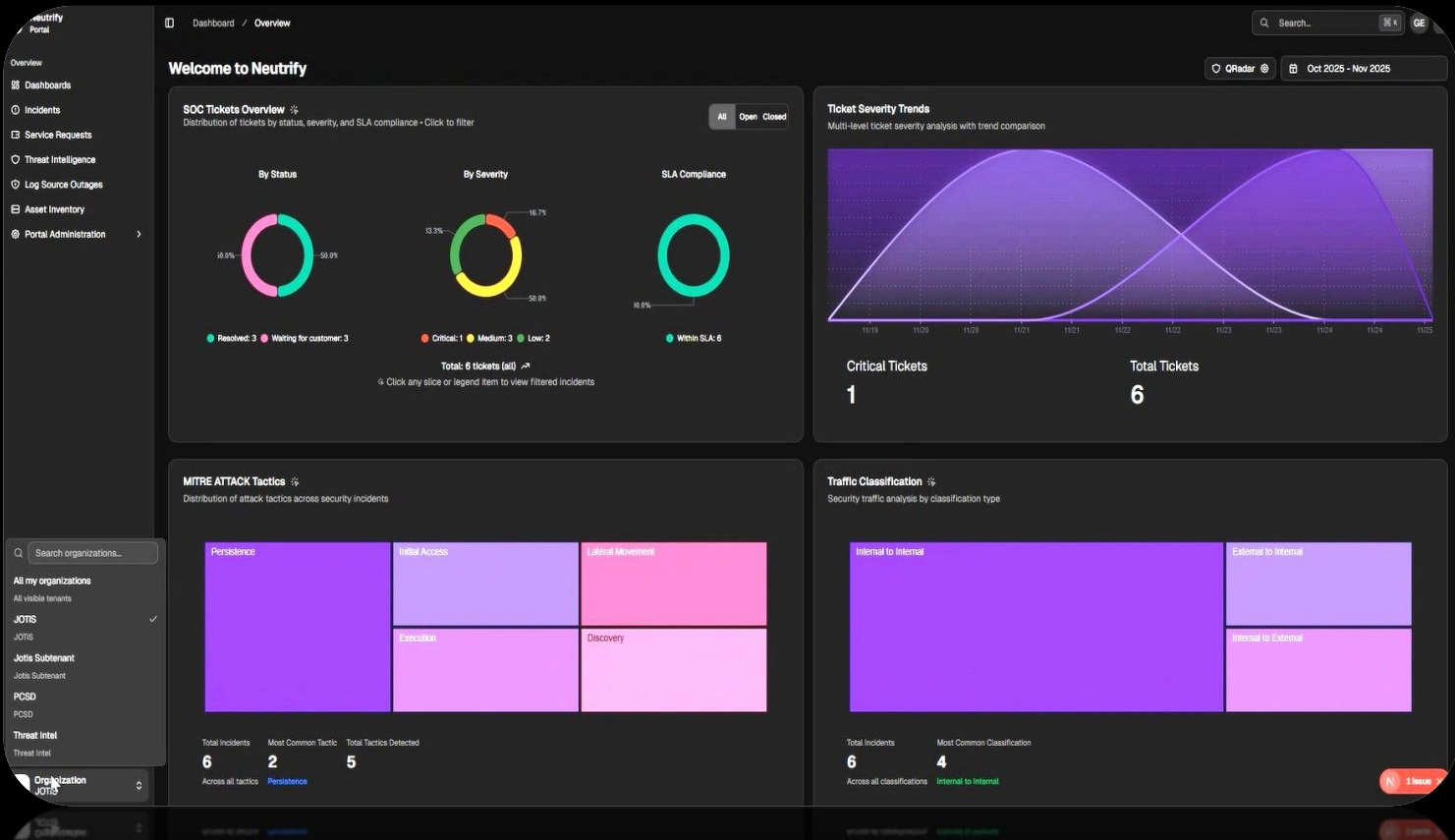
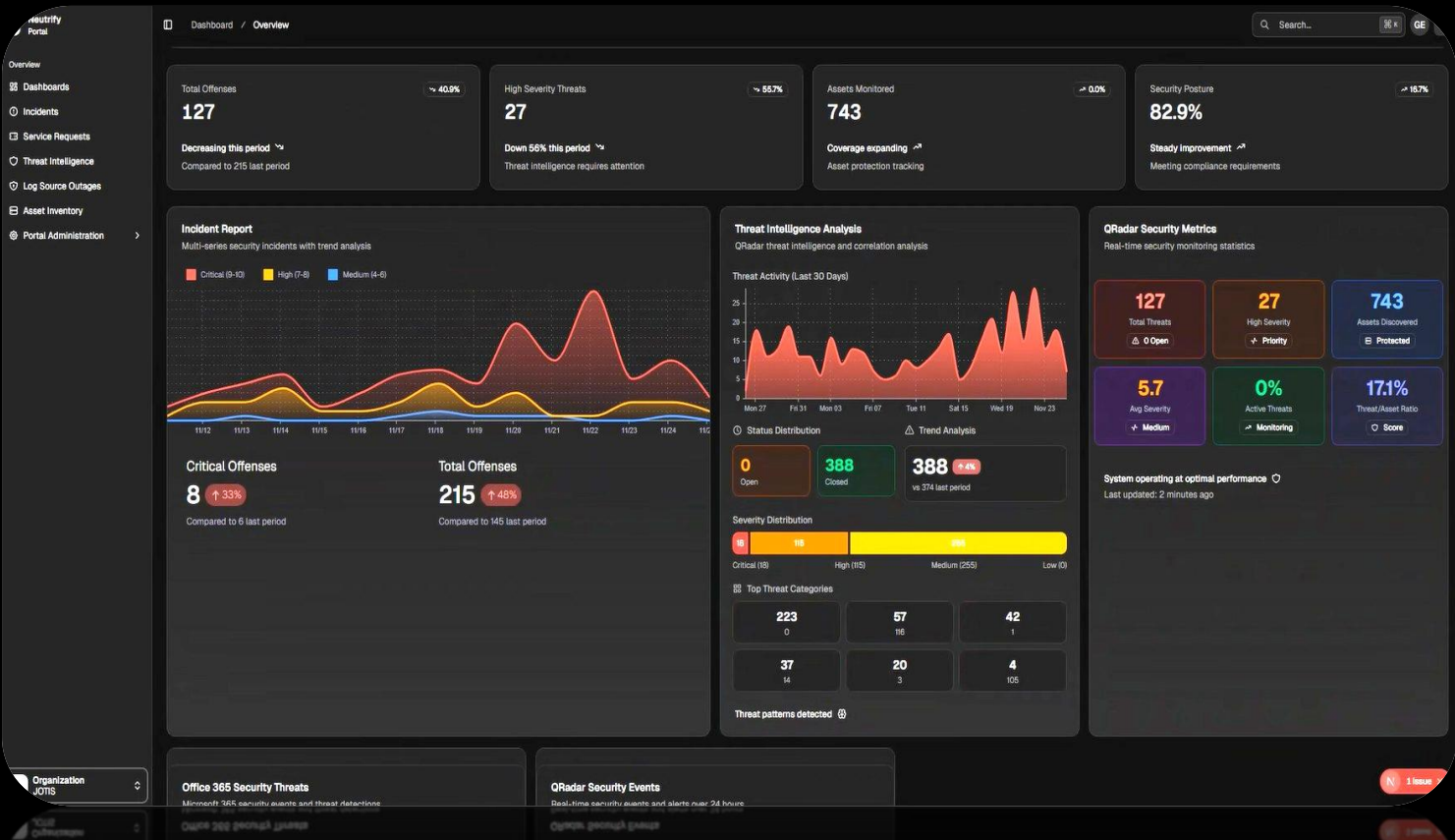


# Neurosoft SOC/MDR Service Portal

The Neurosoft SOC/MDR Service Portal provides a unified view of all security operations, offering full transparency and streamlined collaboration with our SOC Team.

## Key Features

- Visibility into all open tickets and incident status
- Direct collaboration and communication with SOC analysts
- Full access to SLA performance and service metrics
- Clear oversight of your MDR service, enabling real-time awareness and efficient interaction with the SOC.



The **All Incidents** section provides a detailed view of security incidents, including a table with columns for Ticket ID, Organization, Summary, Status, Severity, Traffic Classification, MITRE Tactics, Created, and Last Updated.

Ticket ID	Organization	Summary	Status	Severity	Traffic Classification	MITRE Tactics	Created	Last Updated
J0710-425	J0710	Successful VPN connection from two distinct...	Waiting For Customer	Low	External To Internal	Initial Access	25 Nov 2025	25 Nov 2025
J0710-426	J0710	Suspicious File Detected by Cortex XDR	Waiting For Customer	Low	Internal To External	Execution	24 Nov 2025	24 Nov 2025
J0710-427	J0710	Members were added to security-enabled gr...	Waiting For Customer	Medium	Internal To Internal	Persistence	24 Nov 2025	25 Nov 2025
J0710-428	J0710	Excessive Amount of SMB Traffic	Resolved	Medium	Internal To Internal	Lateral Movement	21 Nov 2025	24 Nov 2025
J0710-429	J0710	A member was added to a security-enabled s...	Resolved	Critical	Internal To Internal	Persistence	21 Nov 2025	21 Nov 2025
J0710-430	J0710	Group Membership Modification - Member Ad...	Resolved	Medium	Internal To Internal	Discovery	19 Nov 2025	20 Nov 2025
J0710-431	J0710	Multiple Failed Remote Authentication Atte...	Closed	Low	Internal To Internal	Credential Access	19 Nov 2025	24 Nov 2025
J0710-432	J0710	Users created and added to security-enabled...	Closed	Medium	Internal To Internal	Persistence	13 Nov 2025	21 Nov 2025
J0710-433	J0710	Users created and added to security-enabled...	Closed	Medium	Internal To Internal	Persistence	12 Nov 2025	21 Nov 2025
J0710-434	J0710	Successful VPN connection	Closed	Low	External To Internal	Initial Access	11 Nov 2025	19 Nov 2025
J0710-435	J0710	Internal Port Scanning Activity detected	Closed	Low	Internal To Internal	Discovery	10 Nov 2025	19 Nov 2025
J0710-436	J0710	User created and added to security-enabled...	Closed	Medium	Internal To Internal	Persistence	10 Nov 2025	19 Nov 2025
J0710-437	J0710	Suspicious DNS Request	Closed	Medium	Internal To External	Initial Access	10 Nov 2025	19 Nov 2025
J0710-438	J0710	Users created and added to security-enabled...	Closed	Medium	Internal To Internal	Persistence	07 Nov 2025	17 Nov 2025
J0710-439	J0710	Sharpshound Tool Detected	Closed	Medium	Internal To Internal	Discovery	07 Nov 2025	17 Nov 2025
J0710-440	J0710	Users created and added to security-enabled...	Closed	Medium	Internal To Internal	Persistence	07 Nov 2025	17 Nov 2025
J0710-441	J0710	Users created and added to security-enabled...	Closed	Medium	Internal To Internal	Persistence	07 Nov 2025	17 Nov 2025
J0710-442	J0710	Users created and added to security-enabled...	Closed	Medium	Internal To Internal	Persistence	07 Nov 2025	17 Nov 2025
J0710-443	J0710	CVE-2013-3882 vulnerability detected in adv...	Closed	Medium	Internal To Internal	Impact	03 Nov 2025	17 Nov 2025
J0710-444	J0710	Users created and added to security-enabled...	Closed	Medium	Internal To Internal	Persistence	01 Nov 2025	08 Nov 2025
J0710-445	J0710	A member was added to a security-enabled...	Closed	Medium	Internal To Internal	Discovery	30 Oct 2025	07 Nov 2025

# MDR Team Expertise

Neurosoft, a leading MSP in Cybersecurity, Technology Solutions and Field Services, is a Microsoft Security Solutions Specialized Partner, holding Microsoft Security Specializations in Threat Protection and Cloud Security. This recognition highlights our proven expertise in delivering Microsoft's advanced security technologies and protecting organizations from evolving cyber threats.

## Team Certifications:

- SC-100, SC-200, SC-300, SC-400, SC-900
- MS-102, MS-900
- AZ-104, AZ-140, AZ-305, AZ-500, AZ-700, AZ-800, AZ-801
- GCFR, GCIH, GCFE, GCFA, GREM
- CISSP, CCSP, CISM
- ISA/IEC 62443 Expert

Our MDR and SOC operations are delivered by an EU-based team (Greece – Cyprus) of more than 40 analysts, engineers, automation specialists, threat intelligence researchers, and forensics experts. Supporting over 50 clients across all industries—including critical infrastructure, financial services, enterprise, and public sector—Neurosoft provides a mature, scalable, and field-proven Microsoft-powered detection and response capability.





# NEUROSOFT

## Athens

466 Irakliou Ave. & Kiprou  
141 22 Iraklio, Athens  
Greece  
Email: [info@neurosoft.gr](mailto:info@neurosoft.gr)

## Thessaloniki

6th km Thessaloniki –  
Oraiokastro  
564 30, Efkarpia  
Greece

## Nicosia

2 Sophouli Street  
The Chanteclair House,  
1096, Nicosia  
Cyprus