NEUROsoft

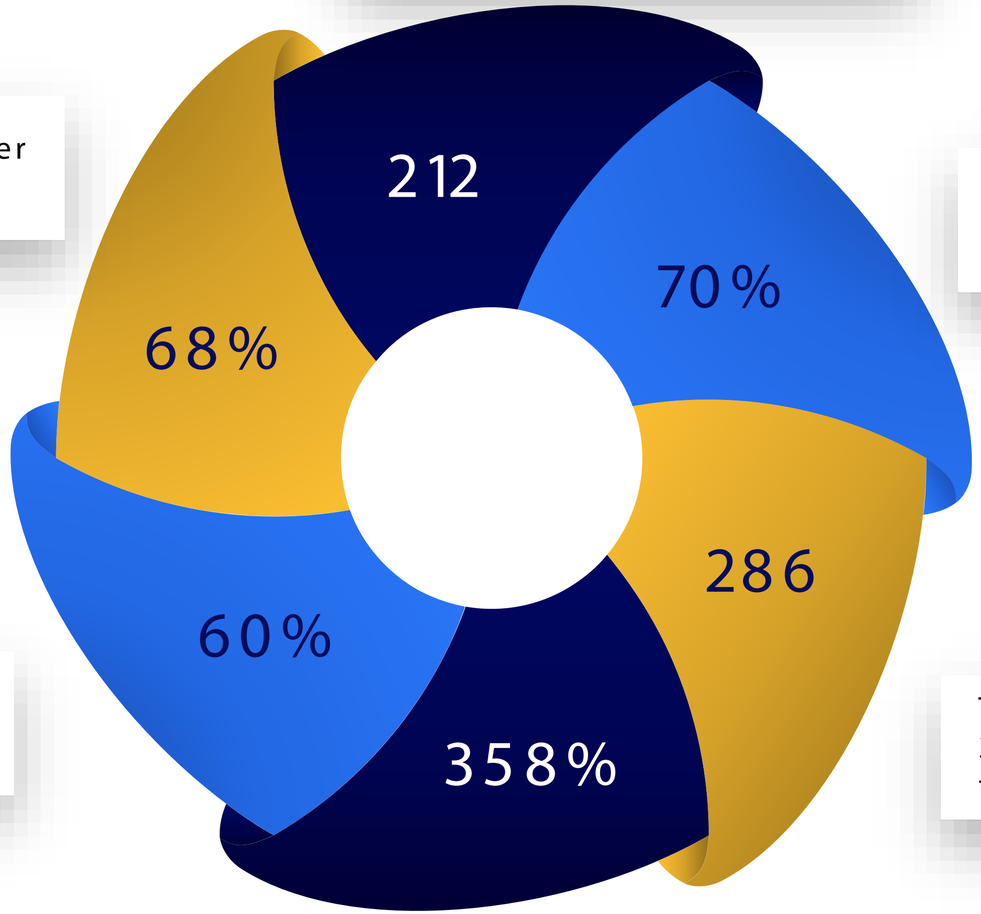
SOC Visibility Triad & the Challenges of a modern SOC.

Name: Giannis Malafekas
Position: Technical Account Manager

Do numbers tell the truth?

The average time to identify a breach in 2021was **212** days.

68% of business leaders feel the cyber security risks are increasing



Lack of visibility. **70%** of the attack surface is opaque and not covered by agents or logging

Due to the pandemic, nearly **60%** of internet users have reported an elevated risk of a data breach.

The average lifecycle of a breach in 2021was **286** days from identification to containment.

Malware increased by **358%** in 2021

From Monitoring to Effective Response.

Increased Visibility

- Network visibility at packet level
- Endpoint visibility at runtime memory
- Business-Centric Setup

Advanced Threats Identification

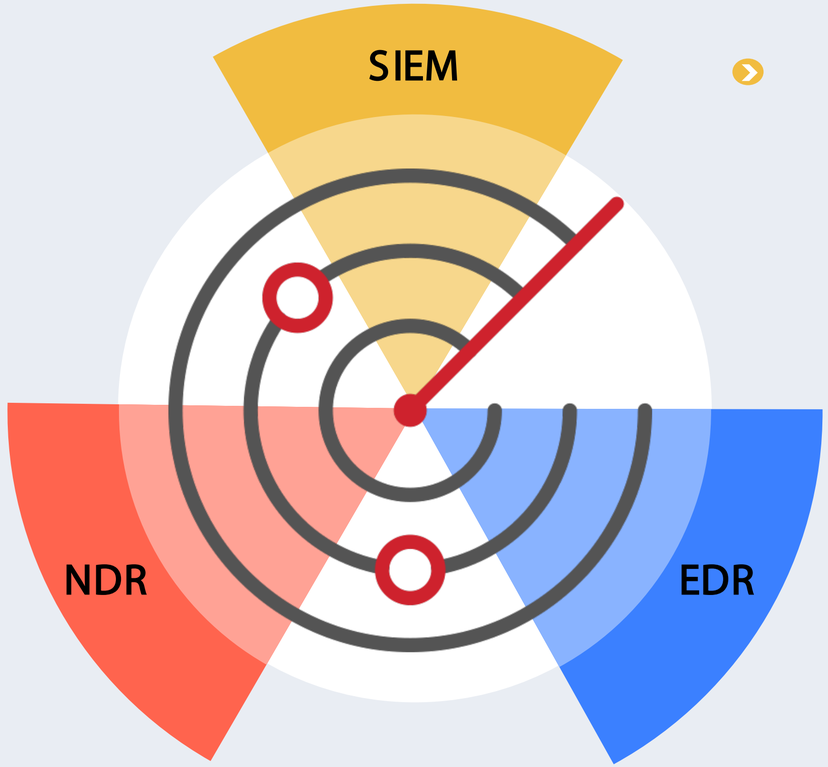
- Behavioural Analytics
- Configuration Analysis
- See beyond encryption
- 3rd Party Intelligence Sources
- Management of valid activity that may be used by attackers
- Use-Case Setup

Effective Incident Response

- Network Isolation
- Endpoint Isolation
- Threat Hunting Tools available during isolation
- Playbooks for automated response
- Technical Expertise

SOC Visibility Triad.

To build a complete and fully operational cybersecurity solution that can deal with the growing stack of cyberthreats, **Neutrify unites SIEM, EDR and NDR under one, vendor-agnostic solution.**



Collects data from various sources.
Normalizes and aggregate the collected data.
Analyzes the data to discover threats.
Identifies security breaches
Assists in alerts investigation.

Analyzes network traffic
Real-time network communications inspection.

Complements SIEM solution
Collects data directly on endpoint
Detects malicious activities on endpoints.
Blocks malicious activities on endpoints.
Enhances threat hunting capabilities

Three Beats One.

Enabling automated or rapid responses to security incidents for remediation and containment.

SOC Visibility Triad offers automation which is a prime way to address talent shortages and more complex threat landscapes

Combining these three technologies and methods increases overall visibility

Reduce the time to detection and resolution

Malicious actors have fewer places to ‘hide’

Extended Monitoring Capabilities.

SIEM

- ✓ Collection and analysis of Logs
- ✓ User Behavioral Analytics
- ✓ Event Correlation / Threat Monitoring / Incident Response
- ✓ Advanced Rules based on Business Needs

EDR

- ✓ Automated Remediation
- ✓ Record system activities and events taking place on endpoint side
- ✓ Behavioral Analytics

NDR

- ✓ Analyze network traffic in depth
- ✓ Enables rapid response in network suspicious activity
- ✓ Real-time detection of threats and performance anomalies

Extended Visibility as an Incident Response enabler.

RAPID ISOLATION CAPABILITIES

AVOID DOWNTIME

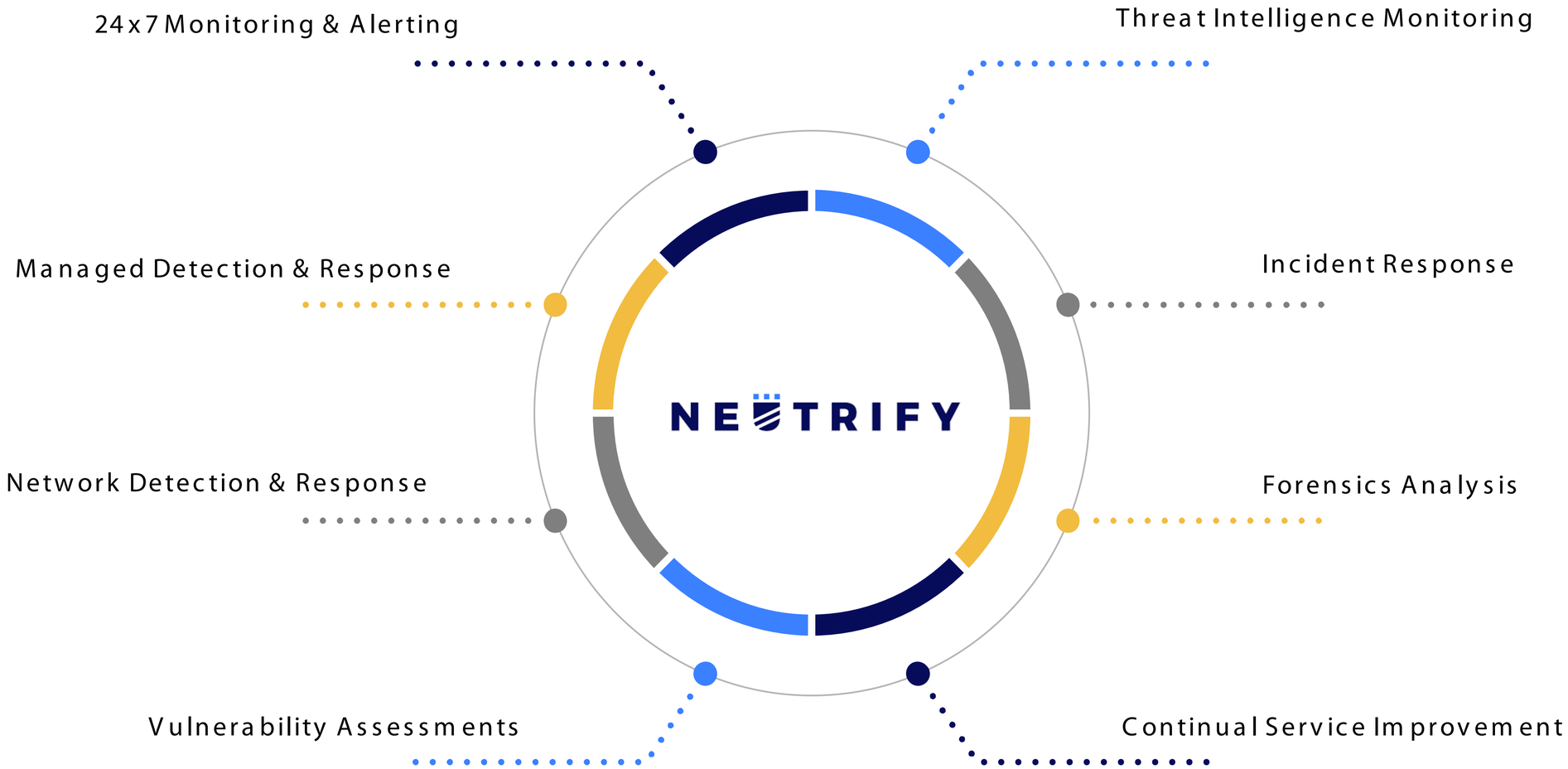
DEEP NETWORK TRACING

ADVANCED THREAT HUNTING

FORENSICS ANALYSIS

RISK MITIGATION

Neutrify Components.



What we achieve.

- Increased overall visibility
- Fast and well-coordinated responses
- Reduced Mean Time To Detect
- Strengthen each other by reduction of false positives

NEUROsoft

WE IMPROVISE. WE ADAPT. WE DELIVER.

Find us

Greece
Athens
Thessaloniki
Patras

Cyprus
Nicosia

Contact Details

info@neurosoft.gr
sales@neurosoft.gr

+30 210 68 55 061