nexion IT SOLUTIONS

Heimdal®

Revolutionary. Unified. AI Cybersecurity.

Our Mission

Simple, next-level cybersecurity protection. Immediately effective. Unified.

Panos Tsadaris
General Manager

Panos.Tsadaris@nexion.gr
www.heimdalsecurity.com

Heimdal®

One Platform | One Agent | Complete Protection

To Infinity & Beyond

Revolutionary | Unified | AI Cybersecurity | FY23

nexion IT SOLUTIONS

Heimdal®

What are the most common cybersecurity risks that organizations face within the market?

The most common cybersecurity risks recognized by organizations are:

- ✓ Phishing and Social Engineering Attacks
- ✓ Ransomware
- ✓ Insider Threats
- ✓ Unpatched Software
- ✓ Remote Work (Enterprise Anywhere)

Heimdal®

One Platform | One Agent | Complete Protection

The Security Maturity landscape

Building a resilient security posture

nexion IT SOLUTIONS

Heimdal®

Simplify your Operations

Heimdal® combines threat prevention, vulnerability management, access management, and antivirus and e-mail security into a single platform that simplifies IT operations and helps companies stop any cyberattack, keeping critical assets, information and intellectual property safe.

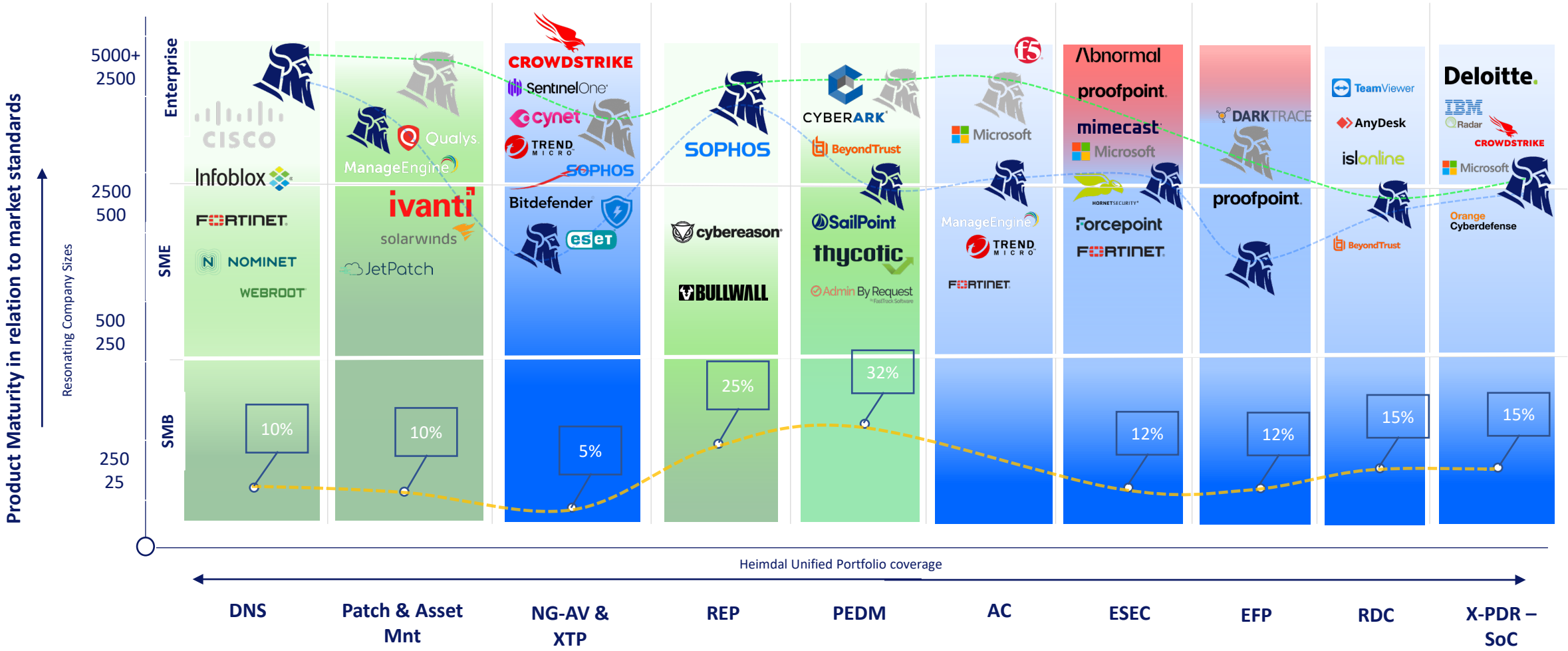
Advance your Defences

Innovative components, unified in a complete Endpoint Prevention, Detection and Response platform, intelligently work together as one through AI to empower organizations to predict and stop tomorrow's threats, today. With total confidence and complete visibility over any environment.

Unify your Security

Effectiveness, convenience and very competitive pricing combined into a unique security offering that simplifies your IT infrastructure, minimizes risk and boosts productivity, enabling you to replace up to 7 vendors with just 1. Empower your employees, whether on-site or remote.

Product maturity Landscape



OUR COMPETITIVE ADVANTAGE

Competitive Positioning vs Other Market Players

- **UNRIVALLED PLATFORM FOR MID-MARKET**
- **GLOBAL MULTI-CHANNEL GO-TO-MARKET**
- **STRONG INDUSTRY RECOGNITION**
- **HIGH CUSTOMER INTIMACY/ADVOCACY**

nexion IT SOLUTIONS

CYBERSECURITY maxvalor Heimdal™ Security Alliance Partner

Heimdal®

What is the most expensive part of a SOC and why?

The most expensive part of a SOC (Security Operations Center) is usually the staff.

Security staff are highly trained and *experienced professionals* who are *responsible* for identifying and responding to security incidents, conducting threat analysis, and implementing security policies.

They require a significant investment in terms of salaries, training, and technology to ensure they can perform their duties effectively and keep up with the latest security trends and threats.

OUR UNIFIED THREAT DASHBOARD

Revolutionary SIEM/SOAR Platform Fully Integrated with the Heimdal Suite

THREAT-HUNTING AND ACTION CENTER (TAC)

*New **Threat-Hunting & Action Center** product provides **granular telemetry** to enable **swift decision, unifying data visualisation, threat hunting, remediation and mitigation***

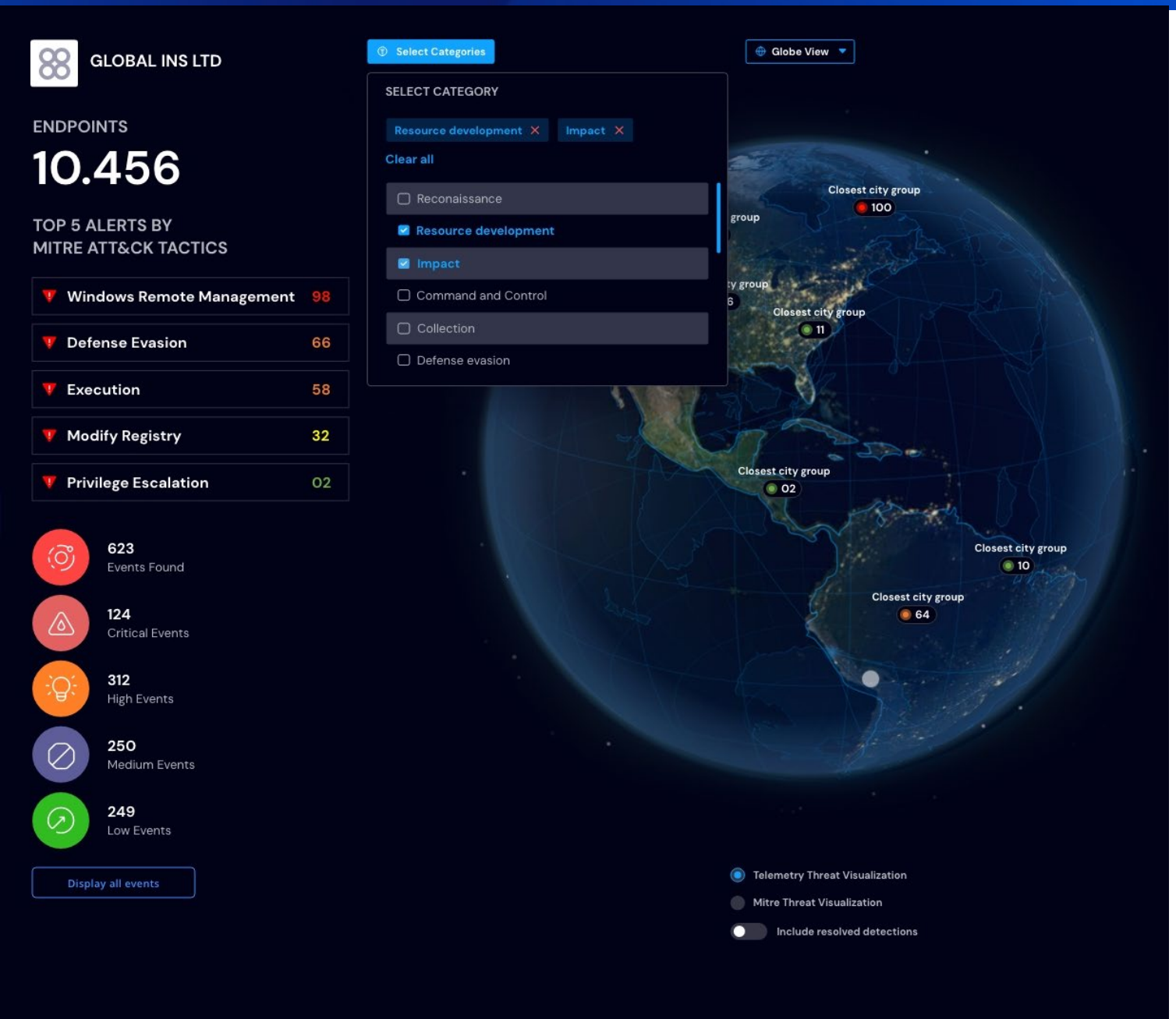
Dashboard Features

- **Unparalleled actionability of risk**
- **Real-time aggregated data**
- **Risk scoring providing tactical command of SecOps**
- **Threat visualisation**
- **AI-enabled deep analysis of risk**

> *This is **absolutely game-changing** for the market*
>
> *CTO, MSP Partner*

SIEM = Security Information and Event Management, SOAR = Security Orchestration, Automation and Response.

TAC



Strategic Benefits:

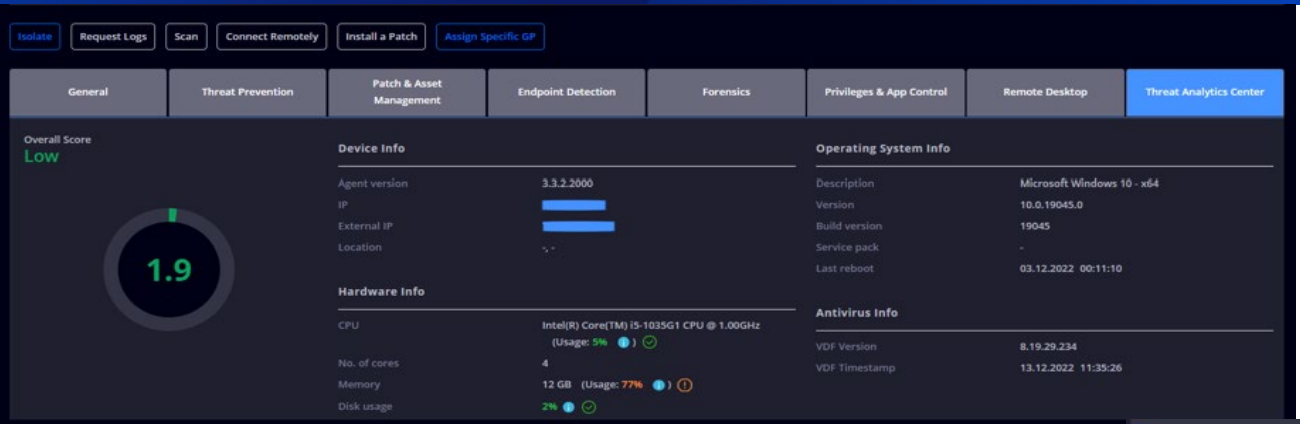
- ✓ Unparalleled risk actionability
- ✓ Risk's Unified, Aggregated and Analysed for your team
- ✓ Single pane of glass risk & compliance overview
- ✓ SOC TCO is reduced by 90% and time to action improved, as analysis is removed
- ✓ SOC is made available for everyone
- ✓ 0-time to implement

Tactical Benefits:

- ✓ Unparalleled Threat visualization
- ✓ Automated Risk Scoring for tactical command of SecOPS
- ✓ MITRE and Heimdal risk scoring included
- ✓ XTP Engine is included for a new dimension of threat hunting
- ✓ Full action storyboard

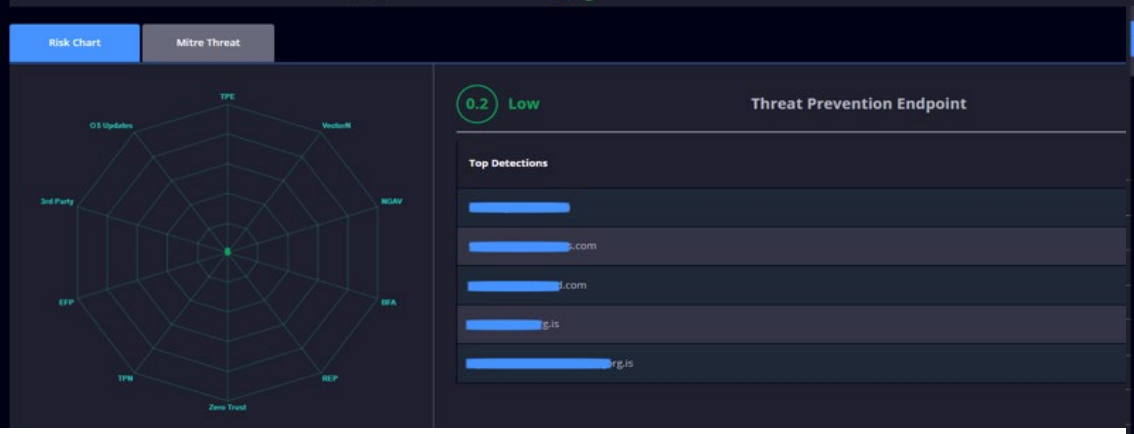
TAC

Heimdal®



Operational Benefits:

- ✓ Full action storyboard
- ✓ One portal for operational excellence
- ✓ Instant deployment, no operational time wasted on setup
- ✓ Simplified focus on what's important
- ✓ Incident response is much faster and easier

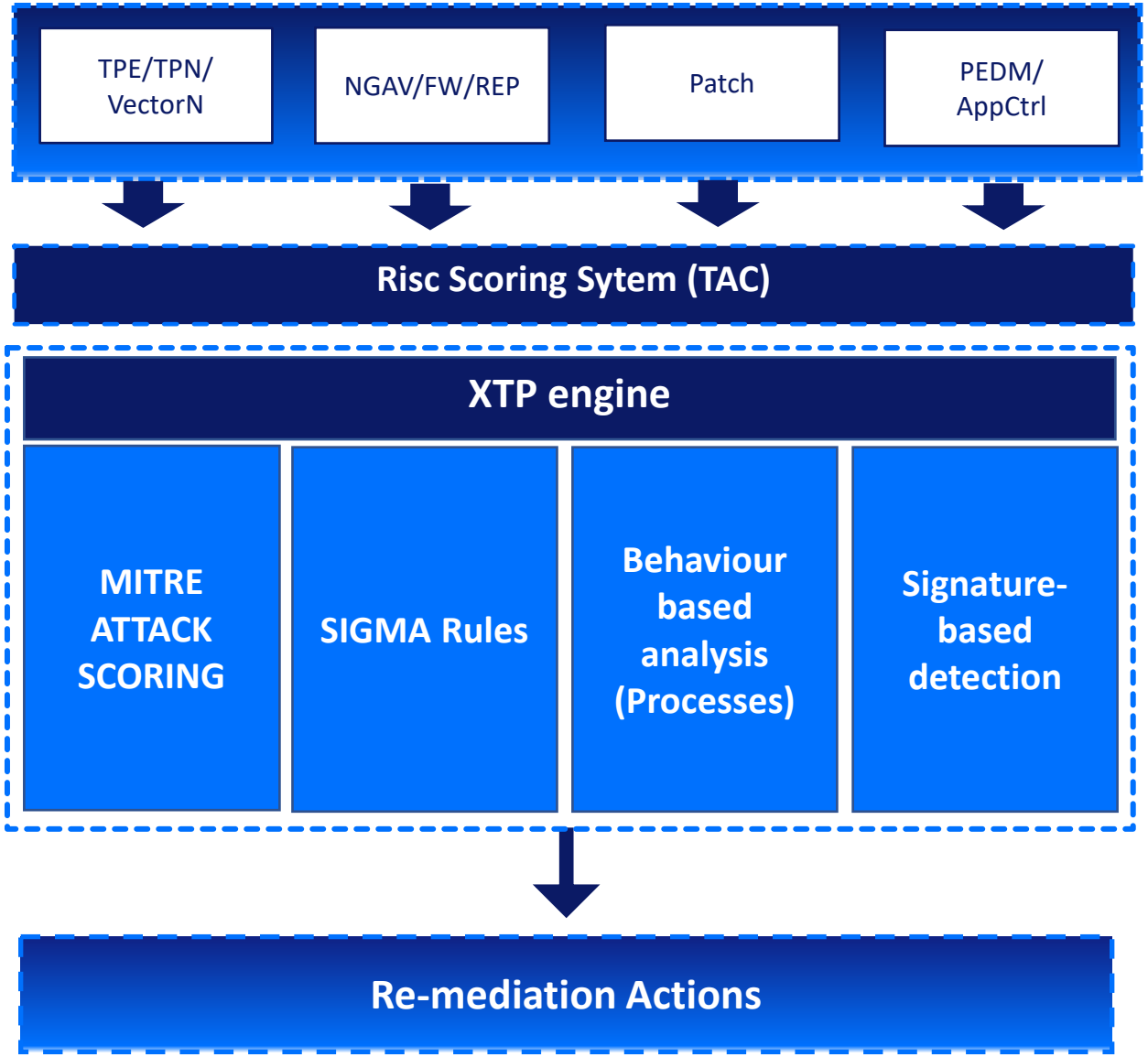


- ✓ Extremely easy Click-to-remediate risks
- ✓ Deep Analysis of risks, when needed
- ✓ Threat classification is built-in
- ✓ Full Process tree view for any attack
- ✓ Based on the most comprehensive security suite in the market for maximum data visibility
- ✓ Multiple view angles on what's happening

Heimdal XTP-Engine:

- **Detection for Highly Sophisticated attack types**
- **MITRE scoring included**
- Classification of events for easy prioritization
- Detection for all types of attacks, such as Lateral Movement, Defense Evasion, Credential Harvesting, Credential access, Persistence, Exfiltration, PowerShell, Scripting to name a few
- Easy & Actionable management and overview

TAC



The engine uses a combination of behavioral analysis and signature-based detection to identify malware and other malicious activity.

It also includes features such as web-filtering, application control, and exploit protection to provide comprehensive security for a user's device or network.

The XTP engine uses MITRE's knowledge base to map the different stages of an attack, from initial delivery to the final stage of execution. By identifying the different stages of an attack, the engine can detect malicious activity at different points in the attack chain.

The engine also uses the MITRE framework to classify and identify known and unknown cyber threats based on their tactics, techniques, and procedures (TTPs). The classification of the threat into a TTP helps the security team to understand and respond to the threat quickly and effectively.

The integration with the MITRE ATT&CK framework maps the different stages of an attack, classify and identify known and unknown cyber threats and their TTPs.

Heimdal®

Threat Hunting & Action Center

Who is the Heimdal® Threat-hunting & Action Center for?

Revolutionary | Unified | AI Cybersecurity

Security Leaders

- ✓ Enterprise-level risk reporting an prioritization
- ✓ Brings security posture into the boardroom
- ✓ Complete threat-centric view of the company's digital risk appetite
- ✓ Helps balance budget & skill gaps within the security department

Strategic

Security Practitioners

- ✓ Boosted hunting capabilities
- ✓ Reduced time and resource consumption on SecOps
- ✓ Adds supercharged detection and action capabilities to the standard suite
- ✓ Reduces alert fatigue through unification

Tactical

MS(S)Ps

- ✓ Fully adaptable multi-tenant architecture
- ✓ Visibility into the customer environment by risk and alerts to action
- ✓ Game changer for versatile and global customer environment management
- ✓ Efficient for all enterprise clients, regardless of seat size

Operational

Panos Tsadaris
General Manager
panos.Tsadaris@nexion.gr