KNIGHTGUARD

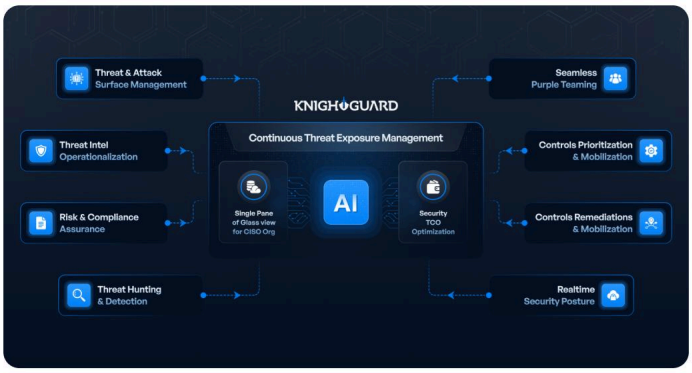
KnightGuard for Threat Informed Defense

Turn intelligence into action | Aligning security with real-world adversaries | Maximize ROI

KnightGuard is an **AI-native & Risk Centric Preemptive Threat Exposure Management** Platform which provides centralised visibility into organisations most relevant threats. Each threat in the platform is tagged with Industry standard **General Intel Requirements (GIR) Framework** helping organisations easily prioritize threats that matter most. All threats in KnightGuard platform are aligned and mapped to MITRE ATT&CK.

Once threats have been prioritized, KnightGuard platform automatically through its inbuilt AI functionality finds the Top ATT&CK Choke points and assigns priorities, so the team knows where to focus.

KnightGuard then provides the security teams, ready to deploy, SIEM agnostic, Detection Analytics. It also gives flexibility and functionality to the security teams to define scenarios and easily generate Detection Analytics using KnightGuard's **Fine Tuned Detection AI Agent**. The platform provides easy visualization of the status of detections against each technique on a detailed MITRE ATT&CK Dashboard.



KnightGuards' Fine-Tuned AI-enabled Data Ingestion pipeline helps organisations bring in unstructured Threat Intel (PDF's / Doc's / Weblinks etc) into the platform and quickly turn it into actionable Threat Intel. Security Operations Team can then swiftly generate, test and deploy their own SIEM specific Detection Analytics within the knightguard platform using our In-build Detection AI Agents. This helps organisations remain SIEM agnostic and drastically reduce MTTD and MTTR.

KnightGuard provides a centralised and customisable Threat Informed Risk Dashboard helping map organisation specific Threats on Impact Matrix.

The Dashboard adapts automatically and provides clear insights and guidance into how good the security posture is against the relevant threats. Our proprietary risk calculation algorithm takes all of the below factors, assign appropriate weights to each and then calculates the risk score:

- Top techniques associated with the threats and how well these threats are mitigated (deployed, tested and validated)
- Top controls associated with the threats that have been implemented and the ones pending actions
- Attack emulations conducted by the security teams against relevant threats and their outcomes.

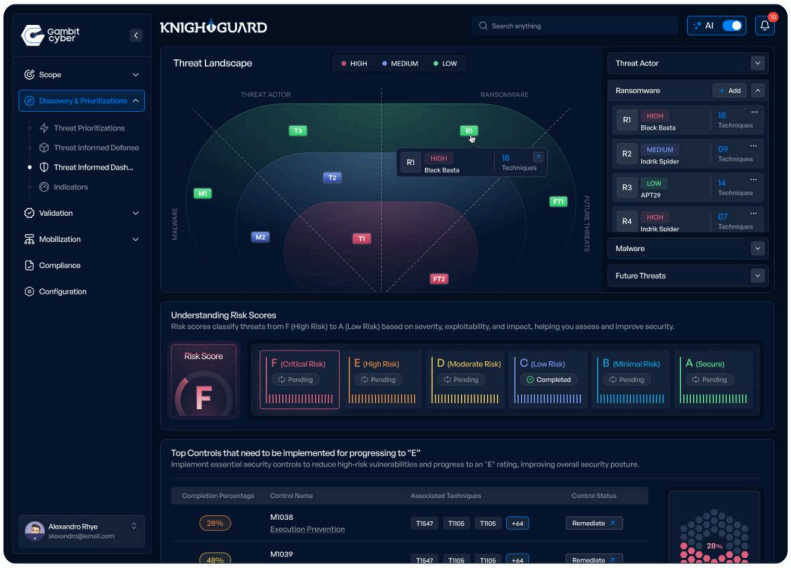
> *"With KnightGuard, organisations can not only gain insight into their existing Threat Informed Risks, but also visualise step-by-step actions to improve their risk score through our **Dynamic** Dashboard"*

✦ Key Capabilities :

Gain Central Visibility Into All Relevant Threats

KnightGuard platform provides central Visibility into all critical threats mapped to their impact – offering relevant, intuitive and customisable dashboards displaying information on current security posture against tracked threats, including

- Top Controls to implement
- Top Techniques to Detect
- Top Emulation Campaigns mapped to Top Threats



Prioritize Controls And Measure Control Effectiveness

KnightGuard Platform automatically maps MITRE ATT&CK to various mitigation and controls framework including **NIST 800-53, MITRE DEFEND, MITRE Mitigation** and many more.

KnightGuard systematically divide the security control into actionable statements and sub-statements that can be assigned to organisation's Ticketing System or within KnightGuard's in-built Ticketing System.

For each actionable statement, KnightGuard provides AI-Enabled playbooks for quickly and efficiently implementing the prioritized mitigation. Significantly reducing the Mean Time To Remediate a Threat.

SOC Optimisation Using Centralised AI Enabled Threat Detection and Hunting

KnightGuard Platform provides a centralised capability for the security operations team to quickly identify the most relevant detections against prioritized MITRE ATT&CK Techniques and quickly operationalise it in their SIEM of choice with a single click.

KnightGuard also provides AI-Enabled Detection and Hunt Analytics generation based on context. This helps Security Teams significantly speed up their Detection Analytics capabilities and enhance efficiencies.

✦ Key Benefits :

Prioritized Security Efforts

Focus resources on the most relevant and impactful threats.

Improved Detection & Response

Align detection rules and incident response with known adversary tactics and techniques.

Continuous Improvement

Refine security posture based on evolving threat landscape.

Measurable Security Outcomes

Use threat-informed assessments to benchmark and improve.

✦ Core Capabilities :

Adversary Emulation

Simulate real-world attacks based on threat intelligence (e.g., MITRE ATT&CK).

Gap Analysis

Identify gaps in detection and mitigation coverage.

Threat Mapping

Map existing controls to adversary behaviors.

Threat Modeling & Prioritization

Determine which threats matter most to the organization.

Security Control Validation

Test effectiveness of defenses against known TTPs.

Build a Robust CTEM Program with KnightGuard

Mobilization

AI-Enhanced Step-by-Step Remediation Guidance

Actions Prioritization

Leverage our Ticketing System

Dynamic Integrations with (JIRA, ServiceNow, Slack)

Validation

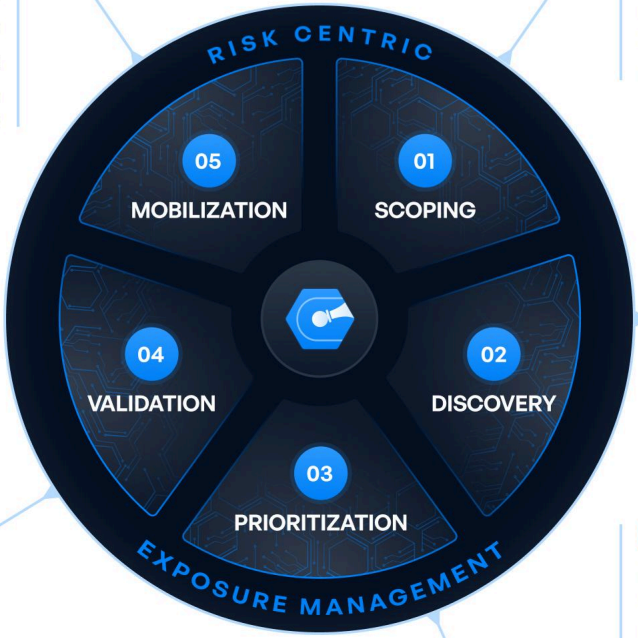
Threat Hunting & Detection (SIEM Agnostic)

Emulate Real-world Attacks

Seamless AI-Enabled Purple Teaming / Breach Attack Emulation

Identify Control Coverage, Gaps and Overlaps

Utilize Organization specific Agentic AI workflows



Scoping

Complete Threat & Attack Surface Visibility

Define Business Specific Risk Functions/ Categories

Controls Categorization & Centralization

Discovery

Visibility of "Current" & "Target" Risk Profile

Vulnerability Scanning

Dynamic Risk & Compliance Assurance (MITRE, NIST, DORA, SEBI CSCRF etc.)

Understand Attack Scenarios & Model Relevant Threats

Threat Intelligence Operationalization through specific AI-Agents (BYO Threat Intel)

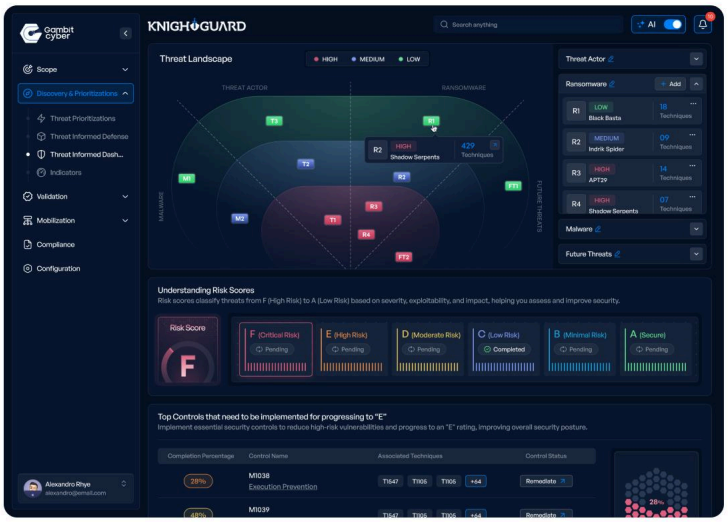
Prioritization

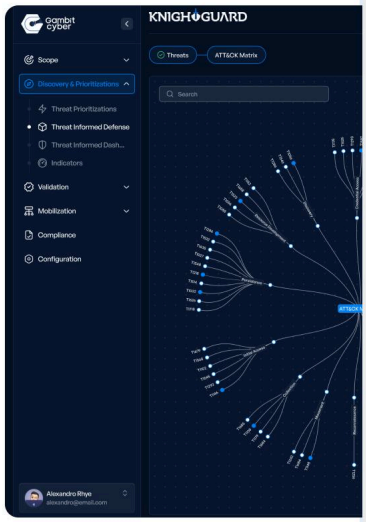
Categorize Assets & Prioritize Controls based on Effectiveness

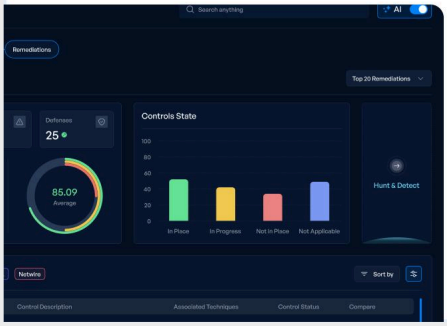
Prioritize Threats Most Relevant to the Industry / Region

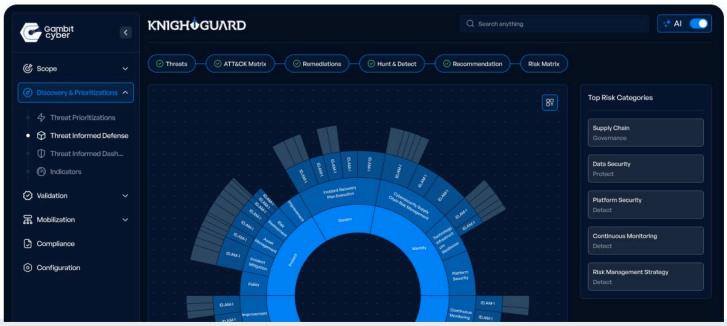
Prioritize Key Attack Paths

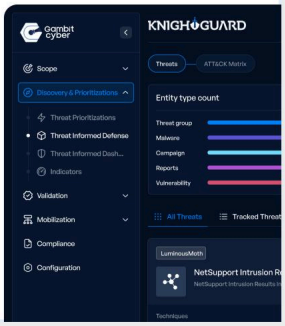
Realtime Security Posture











KnightGuard Subscription Plans

Standard Subscription

- Attack Surface Management
- Threat Surface Management
- Threat Intelligence Operationalization with OSINT – BYO Threat Intel
- AI Enabled Threat Intelligence Creation
- Threat Informed Defense (MITRE ATT&CK Based Threat Prioritization, Mitigation and Remediation)
- Cyber Defence Prioritization based on Industry Standard Frameworks like MITRE, NIST, DORA, SEBI-CSCRF etc
- AI Enabled step-by-step Remediation Playbooks
- Realtime Security Posture
- Customizable Dashboards to Measure & Manage Security Risks to Threat Intel Program

Enterprise Subscription

Includes everything in Standard Subscription and

- AI Enabled Threat Hunting & Detection
- Prioritise SIEM Collection sources (Focused Detections & Hunting)
- AI Enabled Breach Attack Emulation
- AI Enabled Seamless Purple Teaming
- Ready to Emulate Threat Scenarios
- AI Enabled Threat Scenario Generator
- Access to Enterprise Threat Detection & Hunt Queries
- Risk Profile Management
- CISO Dashboards

Book A Demo

AI-Native & Risk Centric
Preemptive Threat Exposure Management

Gambit Cyber B.V. is an emerging force in cybersecurity, dedicated to empowering businesses to build robust defensive security operations through its AI-Native & Risk Centric Preemptive Threat Exposure Management Platform, KnightGuard. Headquartered in The Netherlands, Gambit Cyber is committed to helping businesses strengthen their cyber defence.

Our trusted network of MSSP's and Channel Partners are helping private and public sector organizations of all sizes build a robust and vigilant cyber defence with Gambit Cyber's KnightGuard Platform.

Visit Our Website
www.gambitcyber.org

Chat to sales
sales@gambitcyber.org

Chat to support
support@gambitcyber.org