KNIGHTGUARD

KnightGuard for Seamless Purple Teaming

Turn Attack Simulation to Actionable Defense | Maximize ROI | Zero Blind Spots

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 the KnightGuard platform are aligned and mapped to MITRE ATT&CK metrics.

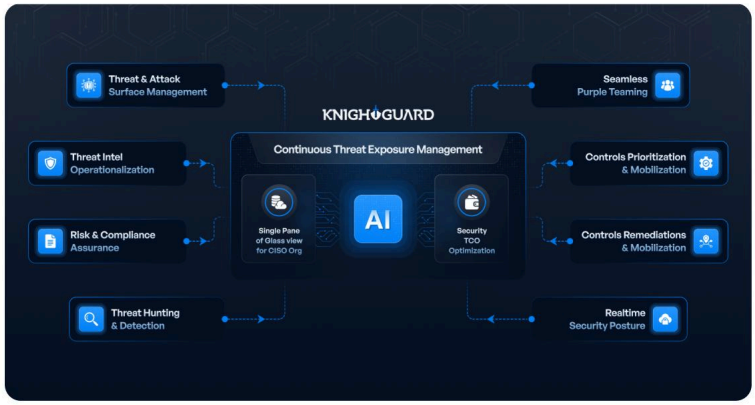
Once threats have been prioritized, KnightGuard automatically finds the Top ATT&CK choke points and assigns priorities to these Top ATT&CK choke points so the team knows where to focus. This helps purple teams to quickly identify most relevant techniques to emulate and detect.

KnightGuard then provides the RED team, ready to emulate threat scenarios, significantly improving the time to emulate threats. Our AI enabled RED team agent quickly enables the team to write emulation scripts for any scenario. KnightGuard also provides ready to deploy, SIEM agnostic, detection analytics for the BLUE team. If the security team doesn't find a detection for their scenario, they can easily generate detection analytics using KnightGuard's Fine tuned detection AI agent.

The security team can easily visualise the status of emulation and detection against each technique on a detailed MITRE ATT&CK dashboard.

The security operations teams can quickly generate, test and deploy their own SIEM specific detection analytics within the KnightGuard platform using detection AI agents. This helps organisations remain SIEM agnostic.

KnightGuard provides a centralised and customisable threat Informed risk dashboard that helps organisations map organisation specific threats on an impact matrix.



Once the threats have been mapped, the dashboard adapts automatically and provides clear insights and guidance into how good the security posture is against the relevant threats. This risk score takes multiple parameters into account like:

- What are the top techniques associated with the threats and how well these threats are mitigated by the team, including deployed, tested, validated detection analytics.
- What top controls associated with the threats have been implemented and which ones are left.
- What simulations have been conducted by the security teams against the relevant threats and what the outcome of those emulations were.

Why It Matters

Organizations should adopt purple teaming because it bridges the traditional gap between offensive (red team) and defensive (blue team) security operations enabling continuous collaboration, faster detection improvements, and measurable risk reduction. Instead of isolated exercises, purple teaming creates a feedback loop where simulated attacks are immediately translated into detection tuning, response playbook validation, and control hardening. This leads to more resilient defenses, reduced dwell time, and better return on existing security investments. In an era where threats evolve rapidly, purple teaming ensures security teams move just as fast together.

✦ Key Benefits :

Continuous Improvement of Detection & Response
Purple teaming enables real-time collaboration between offensive and defensive teams, allowing organizations to rapidly identify and close detection and response gaps.

Threat-Informed Defense
It aligns security efforts with real-world attacker behaviours (e.g., MITRE ATT&CK), ensuring that defenses are tailored to the threats most relevant to the organization.

Measurable Security Outcomes
By simulating attacks and observing defensive performance, organizations can measure improvements in detection reliability, response time, and control effectiveness.

Enhanced Team Collaboration
Purple teaming breaks down silos between red and blue teams, fostering a shared understanding of how attacks unfold and how to stop them, boosting cross-functional expertise.

Validation of Security Controls
It tests the effectiveness of SIEM rules, EDR capabilities, SOAR playbooks, and other controls, ensuring they perform as intended under real-world attack conditions.

Maximized ROI on Security Investments
By continuously testing and refining existing tools and processes, purple teaming helps organizations get the most value out of their current security stack.

Accelerated Incident Readiness
Frequent purple team exercises help prepare the organization to respond more quickly and effectively to actual incidents, reducing dwell time and potential impact.

✦ Core Capabilities :

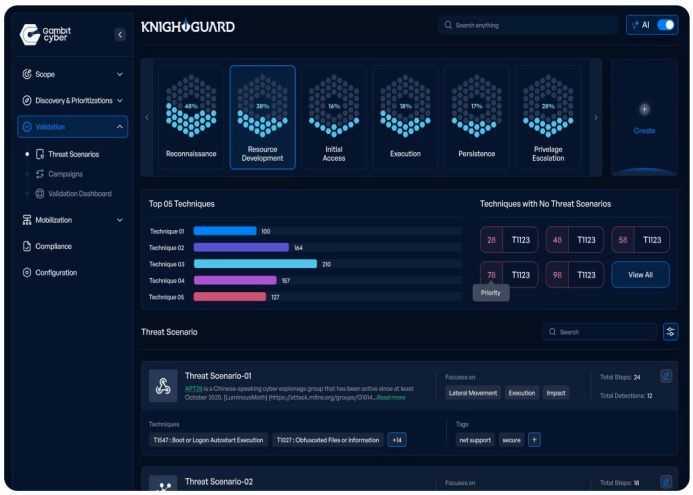
Adversary Emulation
Simulate real-world attacks based on threat intelligence (e.g., MITRE ATT&CK).

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.



✦ Key Capabilities :

Conduct and Track Purple Teaming Exercises using a Unified View

KnightGuard Platform provides a unified view to conduct and track purple teaming exercises. It starts with the RED team defining a scenario by either choosing from one of the hundreds pre-curated threat scenarios or generating them using our RED team AI agent or manually curating them. The team can also upload attack flow files to directly convert it into a purple teaming exercise.

Once the RED team has curated a threat acenario, it can then initiate a campaign that will emulate the threat.

BLUE teams can monitor, detect and respond to these threats in real time. During or after the emulation, the two teams can collaborate on deploying the best detection analytics right in the platform. All these things can be easily tracked from within the platform.

This significantly helps teams to collaborate efficiently and increase productivity.

Gain Central Visibility Into All Relevant Threats

The 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

Unless the RED teaming has insights into the most relevant threats, its difficult for them to prioritize threat scenarios for emulation

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)

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)

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

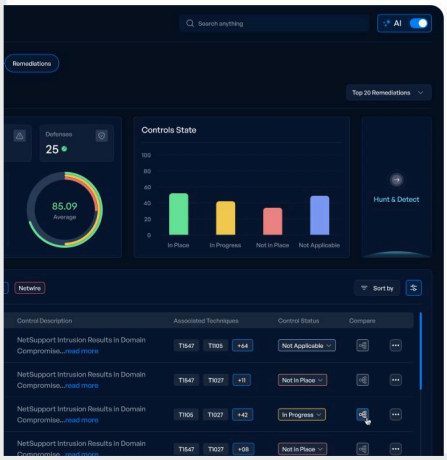
Prioritization

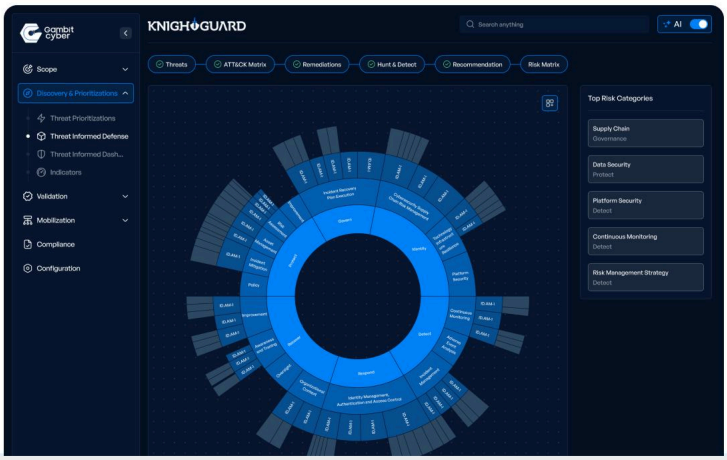
Categorize Assets & Prioritize Controls based on Effectiveness

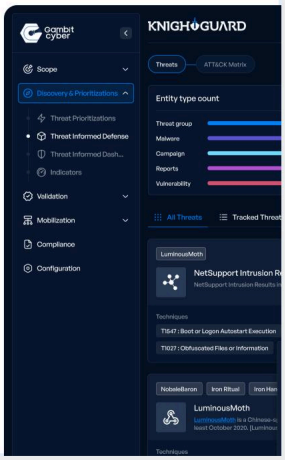
Prioritize Threats Most Relevant to the Industry / Region

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