KNIGHTGUARD

KnightGuard for Threat Hunting and Detection

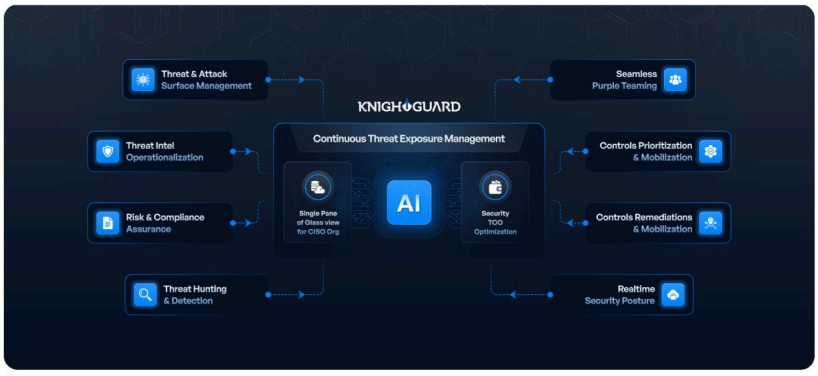
Expose Hidden Adversaries | Maximize ROI | Operationalize intelligence

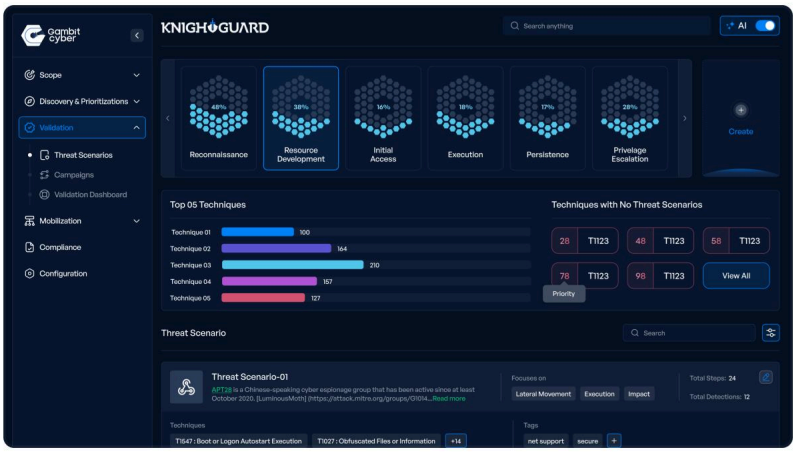
KnightGuard is an **AI-native & Risk Centric Preemptive Threat Exposure Management** Platform which provides centralised visibility into organisations' most relevant threats. Each threat in the platform is tagged with Industry standard **General Intel Requirements (GIR) Framework** helping organisations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

KnightGuard helps organizations turn noise into actionable insights and threats into prevention. Maximizing security ROI.

Even the most advanced detection-based defenses can be evaded by determined threat actors and once inside, their actions still follow recognizable adversary patterns.

Adversary behaviors offer one of the most reliable ways to identify threats. Unlike traditional indicators of compromise (IOCs), which are often short lived and specific to known attacks, behaviors tend to persist over time and reflect consistent tactics used by threat actors. These patterns often become ingrained in their operational playbooks, making them less likely to change. Detecting even one behavioral clue in an attack sequence can serve as a gateway to uncovering additional techniques linked to the same threat actor, enabling broader and more effective threat detection.





KnightGuard helps Threat Hunters quickly identify the most relevant threats. From there the team can quickly pivot to the most common behaviours depicted by adversaries across various Threat Campaigns. Understating these Choke Points help the team identify where to focus their hunting efforts & significantly increase their chances of detecting threats.

At the same time KnightGuard provides detection engineers with ready to deploy high fidelity and SIEM agnostic Detection Analytics that can be quickly operationalised in any SIEM of choice. This significantly helps security teams reduce their false positives and increase detection of threats.

Why It Matters

Threat detection and hunting is a critical function in any security program because it enables organizations to proactively identify and respond to threats that have bypassed traditional defenses. While automated tools catch known attacks, threat hunting focuses on uncovering stealthy, novel, or advanced threats through human-led investigation and behavioral analysis. This capability reduces dwell time, strengthens incident response readiness, and improves overall visibility into the environment. By continuously validating and tuning detection logic, it also ensures that defenses evolve alongside adversary tactics making the organization more resilient against both current and emerging threats.

✦ Key Benefits :

Early Threat Identification
Detects threats that bypass traditional security tools, including zero-day exploits, insider threats, and advanced persistent threats (APTs), allowing earlier intervention.

Reduced Dwell Time
Actively hunting for threats shortens the time attackers can remain undetected, minimizing potential damage and data loss.

Improved Detection Logic
Findings from threat hunts feed back into detection engineering, helping teams continuously refine rules, reduce false positives, and close detection gaps.

Threat Intelligence Validation
Hunting validates threat intelligence against real-world data, confirming whether known attacker tactics or indicators are present in the environment.

Strengthened Incident Response
Threat hunters often uncover attacker behavior patterns that improve the effectiveness and speed of incident response during live attacks.

Continuous Security Posture Improvement
Ongoing detection and hunting efforts help organizations move from reactive to proactive defense, improving resilience over time.

Better ROI on Security Investments
Maximizes the value of existing telemetry, security tools, and threat intelligence by turning raw data into actionable insights.

✦ Core Capabilities :

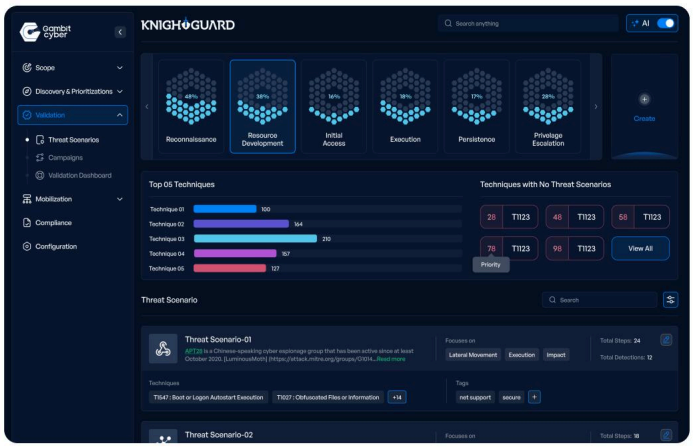
Adversary Emulation
Simulate real-world attacks based on threat intelligence (e.g., MITRE ATT&CK).

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 :

Ready to Deploy Hunt and Detection Packages
The KnightGuard Platform provides Threat Hunting and Detection Engineering teams, ready to deploy Detection Analytics. Its AI Agents help Threat Hunters quickly generate Hunt queries in any language format significantly reducing the time to hunt. Teams can track their progress against MITRE ATT&CK Matrix thereby gaining full visibility into their progress in hunting and detecting threats.

SIEM Cost Reduction
The KnightGuard platform has a built in capability where teams can gain insights into which logs should be enabled across which platform for a specific ATT&CK Technique. This helps security teams bring only relevant logs into the platform thereby helping reduce SIEM costs over a period of time.

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

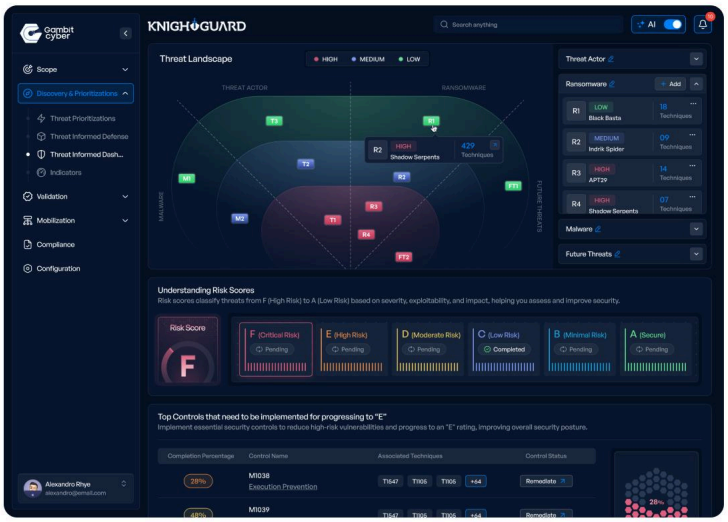
Prioritization

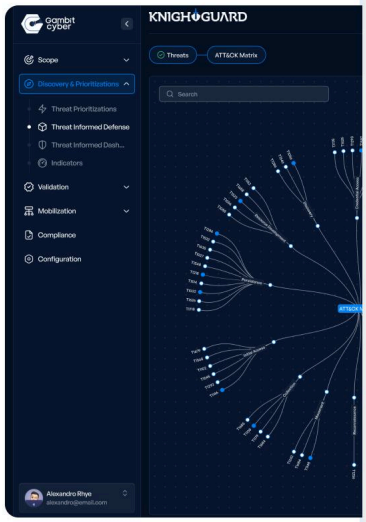
Categorize Assets & Prioritize Controls based on Effectiveness

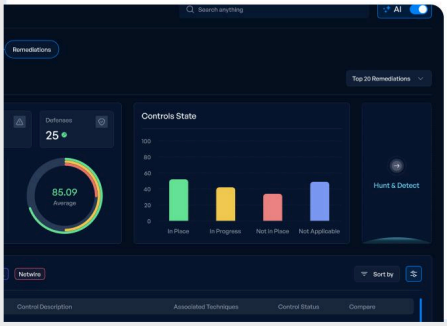
Prioritize Threats Most Relevant to the Industry / Region

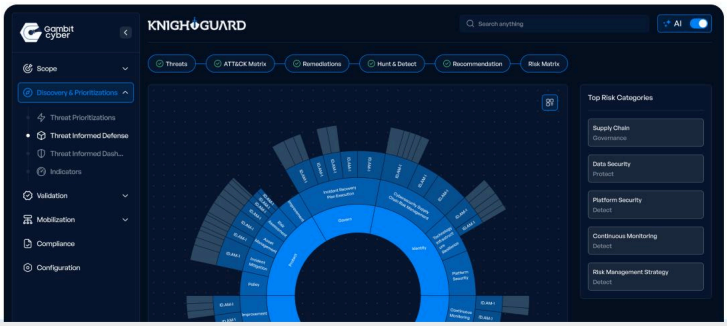
Prioritize Key Attack Paths

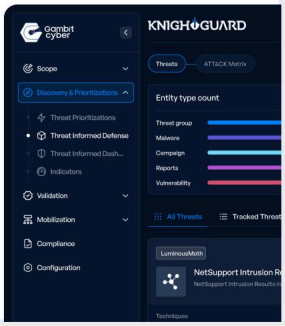
Realtime Security Posture











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