Gambit cyber

www.gambitcyber.org

KNIGHGUARD

KnightGuard for Operationalizing Threat Intelligence

Capitalize Threat Intel Services

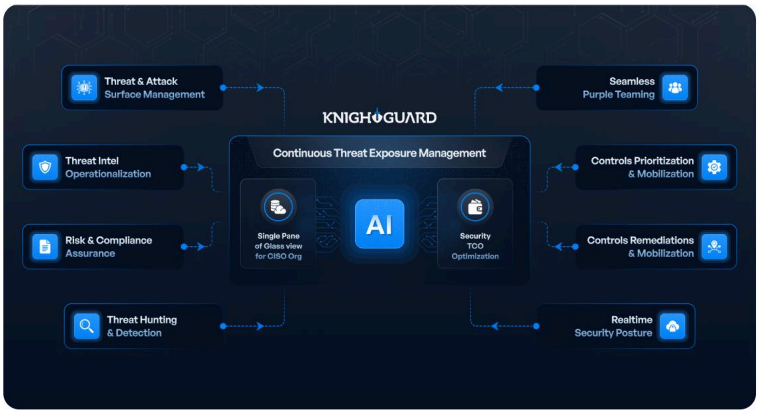
Reduce MTTD & MTTR

Bring your Own Threat Intel

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.

Operationalizing threat intelligence is the process of transforming raw or strategic threat intelligence into actionable insights that can improve efficiency across detection engineering, security controls, incident response, and threat modelling. It helps in capitalizing on threat intelligence services to reduce TCO and bridges the gap between intelligence production and security operations. Organizations without operational threat intelligence rely heavily on generic IOCs and automated feeds, leading to alert fatigue, poor prioritization, and reactive defense.

Threat-Informed Defense (TID), pioneered by the MITRE Engenuity Center for Threat Informed Defense, is a key methodology that uses adversary behavior (e.g., from MITRE ATT&CK) to shape defenses proactively which helps security operations teams move from reactive to proactive security.


KNIGHGUARD
Continuous Threat Exposure Management
AI
Single Pane of Glass view for CISO Org
Security TCO Optimization
Threat & Attack Surface Management
Threat Intel Operationalization
Risk & Compliance Assurance
Threat Hunting & Detection
Seamless Purple Teaming
Controls Prioritization & Mobilization
Controls Remediations & Mobilization
Realtime Security Posture

KnightGuard helps CTI and SecOps teams find answers to the following key questions:

- What threats are relevant to my organisation (Threat Discovery)
- Where should the team focus to have maximum impact (Threat Prioritization)
- Do I have the right set of controls in place to stop the threat from materialising (Threat Mitigation)
- What controls should I prioritize to fix and how can I track the progress (Resource Mobilization)
- How can I detect and hunt for the threats (Threat Detection and Hunting)
- How does performing all of the above lead to a positive impact on my organisation's risk profile.

KnightGuard is a threat intel agnostic platform, which means that organisations can bring threat intel from various sources and track them centrally in the platform and aligns to various industry standard frameworks for Threat Intel Prioritization. In addition, KnightGuard provides a proprietary mechanism to curate a pre-defined list of prioritized techniques aligned to organisation's current security landscape. This helps organisation's understand where the security team should focus their efforts in order to have maximum impact on Risk Mitigation.

KnightGuard's Fine Tuned AI-enabled Data Ingestion pipeline helps organisations bring in unstructured Threat Intel into the platform and quickly turn it into actionable Threat Intel.

Once Threats are prioritized, The KnightGuard platform automatically finds the Top ATT&CK Choke points and assigns priorities to these Top ATT&CK Choke points so the team knows what needs to be mitigated first.

To build a robust preemptive cyber defense, simply prioritizing threats and attack techniques is not enough. The key is to enable security operations and IT Operations team to action the prioritizations and effectively mitigate the threats. KnightGuard, provides security operations teams, including detection engineering and hunt teams, ready to deploy, SIEM agnostic, detection analytics.

> *KnightGuard not only provides insights into the existing Threat Informed Risk, but also visual, step-by-step guidance to improve the risk score through its centralised and customisable Risk Dashboard*

KnightGuard's RED and BLUE Team AI Agent helps security operations team quickly generate detection analytics in any SIEM format (KQL,AQL, SIGMA, SPLUNK, Elastic). This helps security and detection engineering teams significantly reduce MTTD and MTTR.

The security teams can easily visualise the status of detection against each technique on a detailed prioritized MITRE ATT&CK Dashboard.

Knightguard also provides IT Operations teams with a prioritized list of security controls that should be in place in order to mitigate the threat. KnightGuard's IT Ops AI Agent automatically generates a security tool specific playbook to quickly implement the security control.

Why It Matters

Most organizations collect threat intelligence but struggle to apply it effectively. Without operationalisation, intel remains siloed and underutilized. Threat Intel Operationalisation coupled with a Threat Informed Defense approach provides a structured framework to translate threat insights into defensive actions, closing detection gaps and improving resilience.

✦ Key Benefits :

- **Capitalizing Threat Intelligence Services to reduce TCO.**
- **Bridge the gap between Intelligence Production and Security Operations.**
- **Improve Cyber Resiliency by conducting proactive RED and BLUE teaming exercises using relevant threat actor emulations.**
- **Enhanced detection logic based on real-world adversary TTPs.**
- **Improved prioritization of vulnerabilities.**
- **Stronger collaboration between CTI, SOC, and Engineering teams.**

✦ Key Capabilities :

Bring all your Threat Intel from different sources into a Centralised Platform using AI Enabled Data Ingestion Pipeline

KnightGuard is a Threat Intel agnostic platform.

KnightGuards' Fine Tuned AI-enabled Data Ingestion pipeline helps organisations bring unstructured Threat Intel from various sources into the platform and quickly turn it into actionable Threat Intel.

Seamless Purple Teaming

The KnightGuard Platform provides ready to test and deploy threat scenario templates for various relevant use cases. Teams can simply filter and choose the threat scenarios most relevant to them and then convert them into organisation specific campaigns with a single click of a button.

KnightGuard automatically generates relevant detection analytics in organisation's preferred SIEM format. This can be quickly tested directly from within the platform without ever logging into the SIEM.

RED and BLUE Teams can emulate and detect threat scenarios simultaneously which significantly speeds up the overall time to proactively defend against relevant threats.

KnightGuard also provides AI-Enabled detection and hunt analytics generation based on context. This helps security teams significantly speed up their detection analytics capabilities with a small team.

Prioritize Controls And Measure Control Effectiveness

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

KnightGuard systematically divides the security control into actionable statements and sub-statements that can be assigned to the 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 MTTD and MTTR.

✦ 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

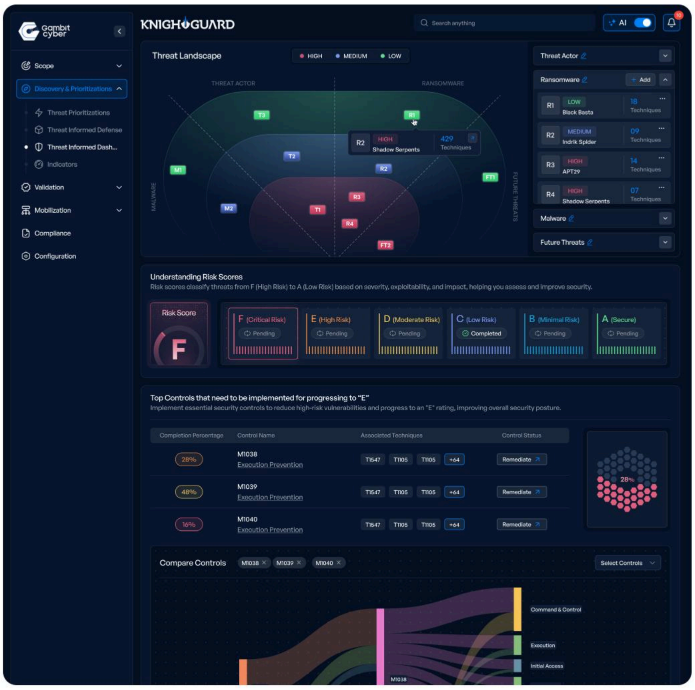
Map existing controls to adversary behaviours.

Threat Modeling & Prioritization

Determine which threats matter most to the organization.

Security Control Validation

Test effectiveness of defenses against known TTPs.



Threat Actor

Ransomware + Add

R1	LOW Black Basta	18 Techniques
R2	MEDIUM Indrik Spider	09 Techniques
R3	HIGH APT29	14 Techniques
R4	HIGH Shadow Serpents	07 Techniques

R2 HIGH Shadow Serpents 429 Techniques

Malware

Future Threats

Understanding Risk Scores

Risk scores classify threats from F (High Risk) to A (Low Risk) based on severity, exploitability, and impact, helping you assess and improve security.

F (Critical Risk)	Pending
E (High Risk)	Pending
D (Moderate Risk)	Pending
C (Low Risk)	Completed
B (Minimal Risk)	Pending
A (Secure)	Pending

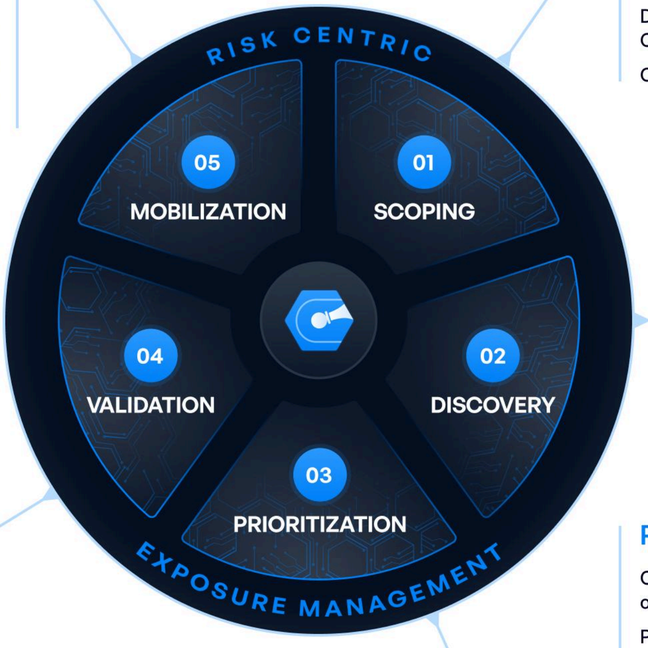
Top Controls that need to be implemented for progressing to "E"

Implement essential security controls to reduce high-risk vulnerabilities and progress to an "E" rating, improving overall security posture.

Completion Percentage	Control Name	Associated Techniques	Control Status
28%	M1038 Execution Prevention	T1547 T1105 T1105 +64	Remediate
48%	M1039 Execution Prevention	T1547 T1105 T1105 +64	Remediate
16%	M1040 Execution Prevention	T1547 T1105 T1105 +64	Remediate

Compare Controls M1038 × M1039 × M1040 × Select Controls

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