KNIGHTGUARD

CONTINUOUS THREAT EXPOSURE MANAGEMENT PLAYBOOK

How to successfully build your CTEM program and a robust threat-informed defense

Gambit Cyber B.V. is a Netherlands-headquartered cybersecurity company pioneering AI-driven, risk-centric Continuous Threat Exposure Management (CTEM). Through its AI-native and risk-centric Preemptive threat exposure management platform, **KnightGuard**, Gambit Cyber helps enterprises move from reactive, alert-driven security to continuous, validated, and threat-informed defence that reduces real-world cyber risk.

The company's core leadership team brings over 100 years of combined experience in cybersecurity across global technology organizations, having built and scaled large-scale security programs in complex, regulated environments. Gambit Cyber was recently recognized as one of **Europe's Top Cybersecurity Startups** by the **European Cyber Security Organization (ECSO)**.

Gambit Cyber is backed by a strong investor base including **Expeditions, Bitdefender Voyager Ventures**, and seasoned angel investors. Their confidence in our vision not only fuels our growth but also brings invaluable expertise and strategic support to accelerate our journey.

Our Investors

KnightGuard is a vendor-agnostic, preemptive threat exposure management platform with in-built agentic AI workflows. It is designed to empower executive decision-makers and leadership teams in building a resilient, threat-informed security posture by delivering a continuous, real-time view of an organisation's true cyber exposure.

As a unified platform, KnightGuard brings together critical threat intelligence (CTI), exposure validation, and risk prioritisation capabilities, helping organisations reduce mean time to detect (MTTD) and mean time to respond (MTTR) while improving coordination across ITOps, SecOps, and GRC teams. By validating which exposures are actually exploitable and aligning remediation with business impact, KnightGuard enables a structured, step-by-step CTEM program focused on measurable risk reduction rather than alert volume.

HOW EXPOSED ARE WE?

In today's rapidly evolving threat landscape, effective exposure management demands a continuous, business-aligned approach that scopes and prioritises the most relevant threats and assets. This enables organisations to dynamically reassess and reprioritise remediation efforts as environments, technologies, and threat vectors change. Moving beyond traditional isolated vulnerability scans and periodic penetration tests, this approach gives CISOs a unified, single-pane-of-glass view of exposure - one that reflects the interconnected nature of modern threats and organizational controls, enhancing overall cybersecurity resilience.

Many organisations are realising that existing security initiatives—such as vulnerability management, threat intelligence, and penetration testing often operate in silos rather than as part of an integrated, risk-led program. When these activities are not aligned to business priorities or the protection of mission-critical assets, organisations struggle to answer a fundamental question: "**How exposed are we?**" The result is fragmented remediation that consumes resources but fails to meaningfully reduce business risk.

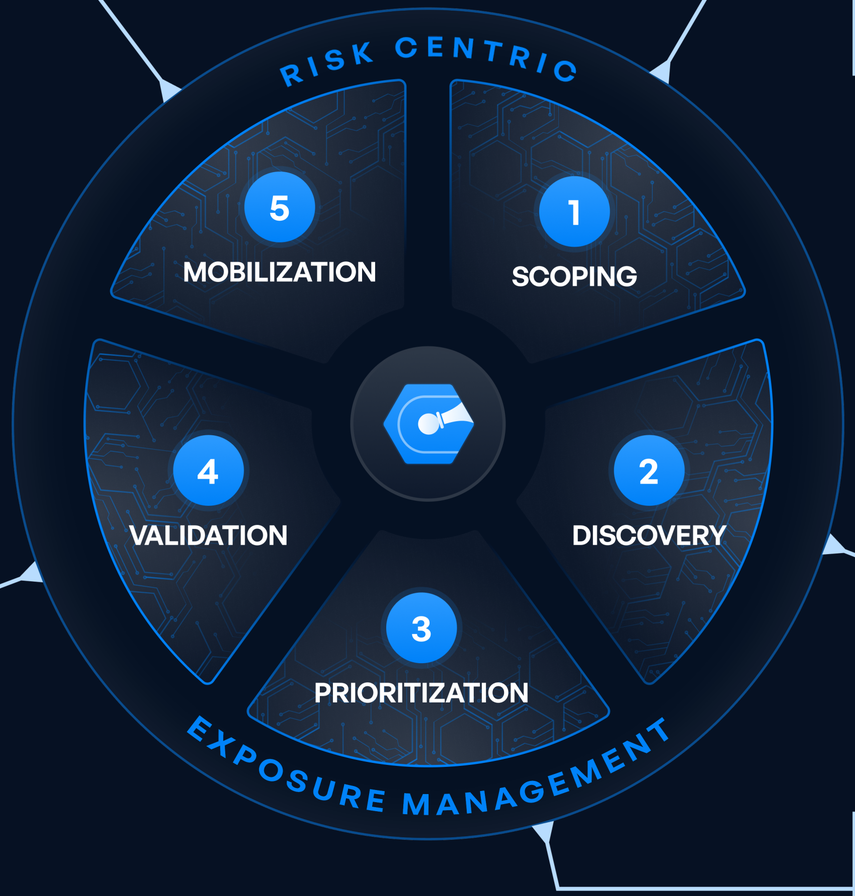
Contrary to common perception, the majority of security breaches do not stem from zero-day vulnerabilities, but from gaps in **threat-informed defence**. While zero-days are inherently unpredictable, attackers typically rely on known tactics, techniques, and procedures (TTPs) that leave detectable patterns across environments. Focusing on identifying and disrupting these behaviours enables organisations to move from reactive detection to a more resilient, proactive security posture.

As AI-enabled attacks grow in sophistication, defensive strategies must also evolve. Effective solutions must leverage organisation-specific data to apply AI defensively—improving risk prioritisation, strengthening decision-making, and enabling meaningful measurement of security outcomes. This results in a cohesive, business-aligned Threat Exposure Management approach that replaces fragmented, reactive processes with **continuous, prioritised, and actionable risk reduction**, empowering organisations to anticipate threats and protect their most critical assets.

Why it matters?

- Focus on "How exposed are we?" and its business alignment.
- Lack of managing end-to-end awareness processes. Need for a step-by-step action plan and remediation playbooks to bridge the gap between the current and targeted risk profile.
- Building a strong threat-informed defence.
- Lack of threat intelligence operationalization from multiple sources and capitalizing on existing threat intelligence services & subscriptions.
- Growth in sophisticated AI-driven attacks, and the need to use organization-specific data to adopt AI to defend, optimize, manage, and measure security operations.

Catalyst for a Robust AI Native & Risk Centric CTEM Program



Mobilization

Drive remediation, mitigation, or compensating controls across stakeholders.

- IT Service Management (AI)
- Remediation Playbook (AI)
- CISO Dashboards & Reporting

Validation

Test whether prioritized exposures can be exploited in real-world scenarios.

- Detection Engineering (AI)
- Attack Emulation (AI)
- Seamless Purple Teaming
- Threat Hunting (AI)
- Inbuilt Threat Scenarios (AI)

Scoping

Define which assets, environments, and attack surfaces to assess.

- External Attack Surface
- Risk Profiles (Current VS Target)
- Risk Quantification

Discovery

Identify assets, vulnerabilities, misconfigurations, and exposures.

- Vulnerability Identification
- Threat Surface Management (AI)
- Security Controls Management (AI)
- Dark Web Monitoring
- Cloud Misconfiguration

Prioritization

Rank threats based on exploitability, impact, and business context.

- Threat Prioritization (AI)
- Controls Prioritization
- Vulnerability Prioritization

BUILDING THE CTEM PROGRAM STEP BY STEP WITH KNIGHTGUARD

1 SCOPING

"Define which assets, environments, and attack surfaces to assess."

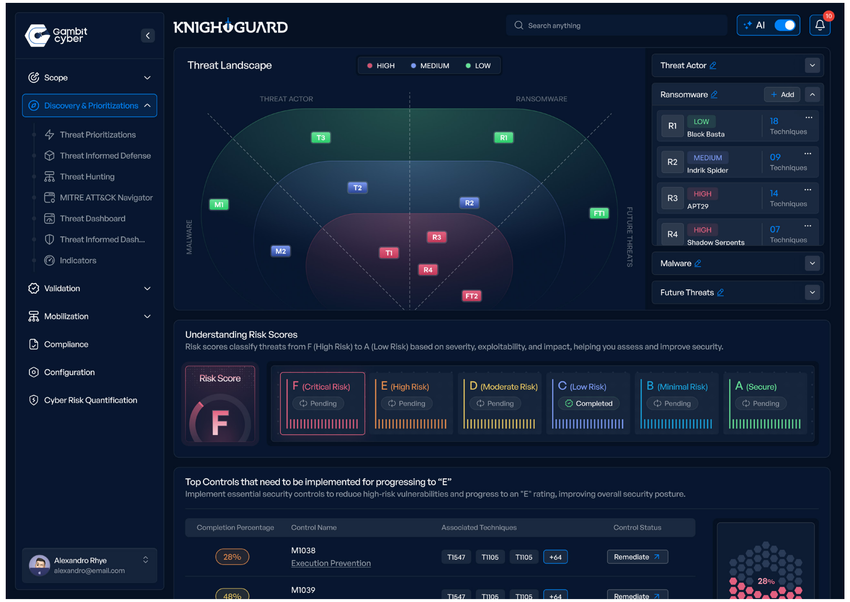
External Attack Surface | **Risk Profile** (Current VS Target) | **Risk Quantification**

- **Attack Surface Management:** Identifying assets, exposures, and vulnerabilities. Domains, Subdomains, IPs, Web technologies, SSL certificates.
- **Unified Risk Context:** Seamlessly integrate asset, threat, and vulnerability data to identify critical exposure gaps.
- **Business Aligned Scoping:** Correlate and contextualize insights (from asset scan and vulnerability intelligence) with threat intel profiles and business risks to define what truly matters for protection.
- **Risk Quantification:** Focus on scoping most critical business risks based on potential financial impact and allocate budgets toward reducing exposures that poses higher potential business losses.

Attack surface management dashboard

“Identify assets, vulnerabilities, misconfigurations, and exposures.”

DISCOVERY **2**



Threat informed defense dashboard

Vulnerability Management

Threat Surface Management

Security Controls Validation

Dark Web Monitoring

Cloud Misconfiguration

- **Comprehensive Visibility:** Centralized visibility into all critical threats, mapped to their potential business impact, enabling better threat modeling.
- **Controls Effectiveness Tracking:** Measure security controls effectiveness by mapping MITRE ATT&CK techniques to multiple frameworks (NIST 800-53, MITRE DEFEND, CIS, etc.).

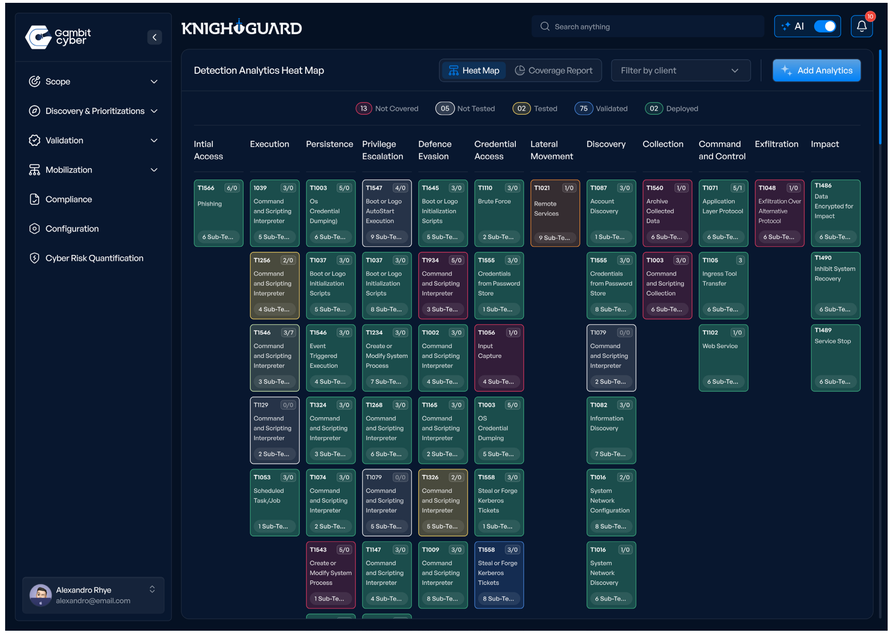
- **Dark Web Monitoring:** Brand monitoring, leaked credentials, and chatters.
- **Cloud Misconfigurations:** Identify misconfigurations across multiple cloud infrastructure and code resources. (AWS, GCP, Azure, GitHub, Kubernetes, etc.).
- **Actionable Controls Breakdown:** Convert high-level security controls into actionable, granular statements and sub-statements for step-by-step implementation.
- **Threat-Informed Operations:** Align detection rules and incident response with real-world adversary tactics and techniques for improved detection accuracy and response time.

3 PRIORITIZATION

“Rank threats based on exploitability, impact, and business context.”

Threat Prioritization | **Controls Prioritization** | **Vulnerability Prioritization**

- **Intelligence Flexibility:** Support OSINT and integrates any commercial /non-commercial threat intelligence feed (BYO threat intelligence), ensuring flexibility and cost optimization.
- **AI-Enabled Integration:** Centralize multi-source threat intelligence with an AI-powered ingestion pipeline that normalizes, enriches, and correlates feeds automatically.
- **Contextual Prioritization:** Combine threat mapping, modelling, and vulnerability prioritization to focus on exposures most likely to be exploited.



MITRE dashboard

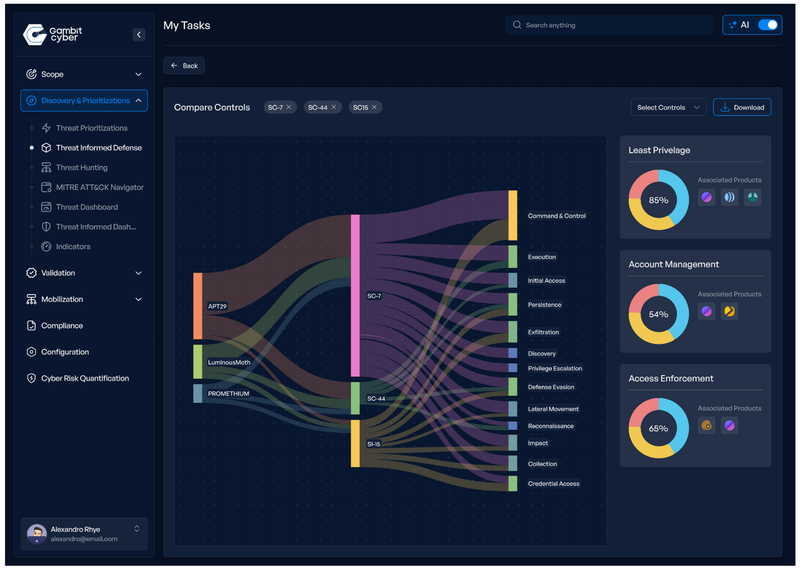
> “ ***Threats*** *without exposure is* ***noise****,*
> ***exposure*** *without* ***risk*** *context is aimless* ”

“Test whether prioritized exposures can be exploited in real-world scenarios”

VALIDATION **4**

Detection Engineering | **Attack Emulation** | **Seamless Purple Teaming** | **Threat Hunting** | **Inbuilt Threat Scenarios**

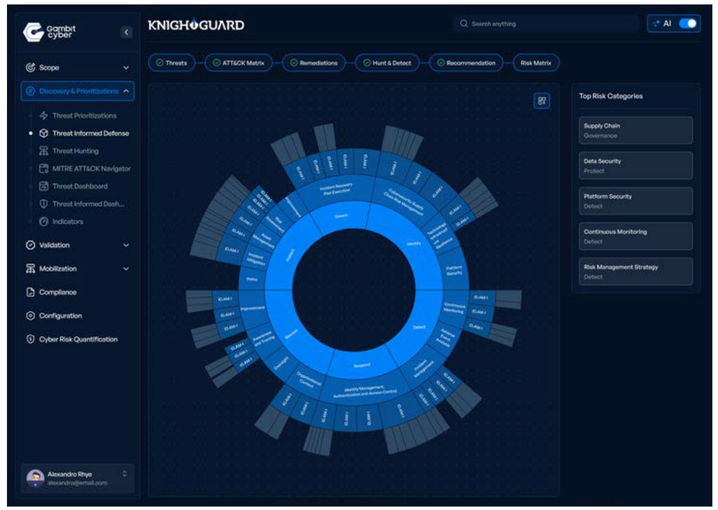
- **Faster Threat Validation:** Rapidly identify active threats and pivot to common adversary behaviors to uncover choke points across campaigns.
- **Faster Red Teaming:** Provide ready-to-emulate threat scenarios to speed up red team operations.
- **AI-powered Emulation:** AI enabled and generated emulation scripts and SIEM agnostic detection analytics for blue teams.
- **Unified Purple Teaming:** Conduct and track purple team exercises in one view for faster detection and response readiness.
- **Operationalized Detections:** Provide ready-to-deploy, SIEM-agnostic, high fidelity detection analytics to cut false positives and accelerate detections.



Validation dashboard

- **AI-assisted Hunting:** AI agents to generate hunt queries in any language (KQL, AQL, SPL, etc.) Improved efficiencies and lower costs.
- **MITRE ATT&CK Tracking:** Continuously track detection and response coverage against the MITRE ATT&CK matrix to visualize progress and gaps.
- **Threat Informed Gap Analysis:** Validate detection logic and test against threat intel, ensuring defenses align with adversary TTPs.

5 MOBILIZATION "Drive remediation, mitigation, or compensating controls across stakeholders."



Risk framework dashboard

IT Service Management | **Remediation Playbook** | **CISO Dashboards & Reporting**

- **Tools-to-Controls Mapping:** Associate security tools with compliance and controls for stronger governance.
- **Ticketing and ITSM:** Connect, track, and sync with any ITSM / Ticketing system (Slack, Jira, ServiceNow, Teams, etc.)
- **Framework Mapping:** Map business risks and outcomes to frameworks like NIST, MITRE, DORA, SEBI-CSCRF.
- **Executive Dashboards:** CISO-ready-to-use, customizable, and business-aligned dashboards.

> *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*

Mesh Of AI Agents for Preemptive Cyber Defense

CTI Analyst AI Agent

Our **Customer Specific CTI Analyst AI Agent** helps turn unstructured security advisories, security blogs as well as proprietary intel reports into Structured Actionable Intel in minutes.

SOC Analyst AI Agent

Our **Security Operations Analyst AI Agent** takes this structured intel and instantly generates detection analytics in any language and query format (Sigma, FQL, KQL, Splunk, etc.) to be deployed in a single click across any SIEM.

Red & Blue Team AI Agents

Our **RED Team AI Agent** helps security teams seamlessly emulate threat campaigns & attack paths to validate detections analytics. Our **BLUE Team AI Agent** adapts the detection analytics for seamless purple teaming.

ITOps AI Agent

Our **ITOps AI Agent** looks at the step-by-step remediation guidance and generates playbooks specific to a security control for enhancing Security Posture.

CUSTOMIZABLE DASHBOARDS

In an increasingly complex and adversary-driven threat landscape, building a Continuous Threat Exposure Management (CTEM) program anchored in a Threat-Informed Defense is no longer optional but foundational to cyber resilience. By continuously identifying, prioritising, and validating exposures in the context of real-world threats and business impact, organisations can focus remediation efforts where they matter most.

A mature CTEM approach unifies security, IT, and risk teams, operationalises threat intelligence, and adapts to change—shifting security from reactive activity to continuous, measurable risk reduction.

Gambit Cyber partners with CISOs, SOC leaders, and MSSPs to design, operationalise, and scale CTEM programs using a structured, step-by-step approach powered by the KnightGuard platform. If you are looking to move beyond fragmented security efforts and build a threat-informed, business- aligned exposure management program, we'd welcome the opportunity to support your CTEM journey.

sales@gambitcyber.org **www.gambitcyber.org**

Confidentiality, Trademark & Copyright Notices
This document is intended to provide you with a statement of the products and services currently available from Gambit Cyber as well as the direction of our product marketing and development efforts. Gambit Cyber cannot guarantee that this position will not change in the future, and this document is not intended to bind Gambit Cyber to any particular course of product marketing or development. The final terms of the negotiated agreement will solely govern Gambit Cyber's provision of the products and services described herein; any additional terms or commitments, whether contained in your RFI or our response, will become part of the agreement only upon mutual written agreement.

Confidentiality
This document contains confidential material that is proprietary to Gambit Cyber B.V. The material, ideas, and concepts contained herein are to be used exclusively to evaluate the capabilities of Gambit Cyber B.V. to provide assistance to your organization. The information and ideas herein may not be disclosed to anyone outside your organization or be used for purposes other than the evaluation of Gambit Cyber capabilities.

Copyright

Copyright © 2026 Gambit Cyber B.V. or its affiliates. All rights reserved.

No part of this document may be reproduced or distributed in any form or by any means without the prior written permission of Gambit Cyber.