KNIGHTGUARD

Gambit cyber

Continuous Threat Exposure Management

OVERVIEW

In today's hyper-connected landscape, organizations face a "perfect storm" of expanding attack surfaces, fragmented tools, and relentless generic alerts. Most are stuck in a reactive **Scan-and-Patch cycle**, patching without business context, managing silos instead of risk.

> *"Threats without exposure is noise. Exposure without risk context is aimless."*

Modern adversaries do not exploit isolated vulnerabilities they execute **Multi-Stage Attack Paths**, leveraging real-world Tactics, Techniques, and Procedures (TTPs) across an organization's infrastructure, often using legitimate tools (Living Off The Land). This creates three fundamental gaps that drive the need for CTEM:

Gap 1 — The Context Gap
Gap 2 — The Detection Blind Spot
Gap 3 — The Execution Gap

A Seismic Industry Shift

The industry is moving from reactive to preemptive, business-aligned security. KnightGuard delivers precisely where it matters most, measurable risk reduction, faster response, and board-ready outcomes.

THE SHIFT KNIGHTGUARD ENABLES

Reactive →	Preemptive
Siloed Alerts →	Unified Risk View
CVSS Scores →	Business impact
Patch Counts →	Measurable Resilience
Assumed Security →	Validated defence

Measurable Risk Reduction	Business-Aligned
Faster MTTD & MTTR	AI-Accelerated
Tools consolidation	Lower TCO
Improved team efficiency	More from Existing Tools

THE 5-STEP CTEM JOURNEY

AI NATIVE & RISK CENTRIC

MOBILIZATION

Drive remediation, mitigation, or compensating controls across stakeholders.

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

SCOPING

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

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

VALIDATION

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

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

DISCOVERY

Identify assets, vulnerabilities, misconfigurations, and exposures.

- Unified Vulnerability Management
- AI Threat Surface Management
- AI Security Controls Management
- Dark Web Monitoring
- Cloud Misconfiguration

PRIORITIZATION

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

- AI Threat Prioritization
- Controls Prioritization
- Vulnerability Prioritization

Continuous Threat Exposure Management

STEP 1 - SCOPING

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

Attack Surface Management

Map your complete digital footprint: domains, subdomains, IPs, web technologies, SSL certificates, shadow IT assets, identity, cloud assets, etc.

Unified Risk Context

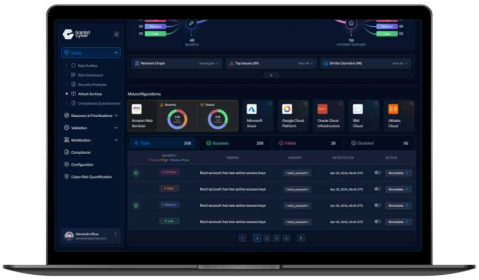
Seamlessly integrate asset, threat, and vulnerability data to visualize the "big picture" of exposure gaps.

Risk Quantification

Focus budgets on exposures with the highest potential financial impact. Correlate with business risk profiles.

STEP 2 - DISCOVERY

Identify assets, vulnerabilities, misconfigurations, and exposures.



Comprehensive Cloud Visibility

Identify misconfigurations across AWS, GCP, Azure, GitHub, Kubernetes, and other environments.

Security Controls Effectiveness

Map current controls to MITRE ATT&CK and NIST to identify gaps in defenses before attackers do.

Dark Web Monitoring

Proactively surface leaked credentials, brand mentions, and hacker chatter before attackers exploit them.

Threat-Informed Operations

Align detection rules and incident response with real-world adversary TTPs for improved accuracy and response speed.

STEP 3 - PRIORITIZATION

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

Contextual Prioritization

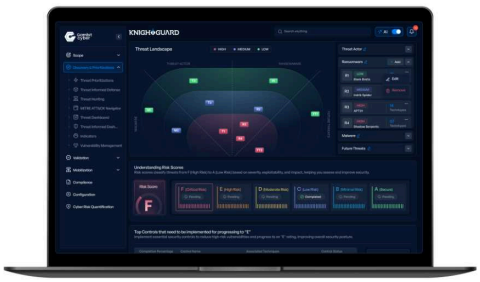
Prioritize not just vulnerability but also external threats in a unifies manner, rank by actual exploitability, not just CVSS score.

AI-Enabled BYO Intel

Normalize and correlate multi-source threat feeds automatically. Support OSINT and commercial/non-commercial intelligence (BYO-Intel).

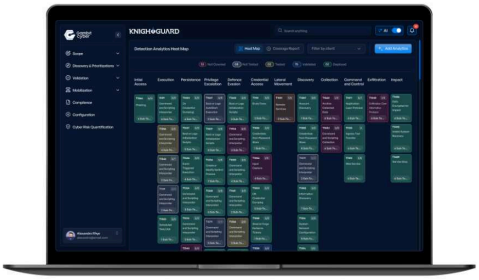
Controls Prioritization

Organisation specific MITRE ATT&CK heatmap identifies top techniques to address. Maps controls to NIST 800-53, MITRE Mitigation, and MITRE D3FEND.



STEP 4 - VALIDATION

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



AI-Powered Attack Emulation

Generate and run breach-attack emulation scripts against 1,500+ ready-to-deploy campaigns. Test whether your SIEM triggers an alert against the latest MITRE ATT&CK techniques.

Seamless Purple Teaming

Conduct and track Red/Blue team collaborative exercises in a single unified view. Faster detection and response readiness with built-in threat scenarios.

AI-Powered Detection Engineering

SIEM-agnostic, high-fidelity detection analytics ready to deploy. Validate detection logic against threat intel to ensure defenses align with adversary TTPs.

Agentic Threat Hunting

AI agents generate hunt queries in KQL, SPL, or AQL to proactively search for signs of compromise across your environment.

STEP 5 - MOBILIZATION

Drive remediation, mitigation, or compensating controls across stakeholders.

Ticketing & ITSM Integration

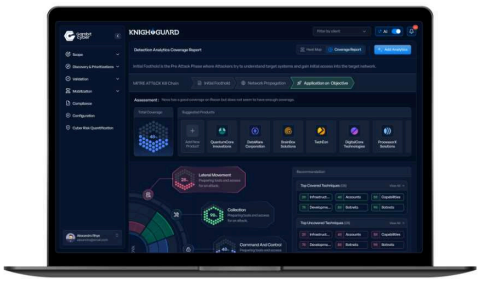
Bi-directional sync with Jira, ServiceNow, Slack, etc. Every prioritized risk gets a ticket with remediation playbook and tracked outcome.

Remediation Playbooks

AI-generated, step-by-step remediation guidance mapped to specific security controls. Move from "Reporting" to "Remediating."

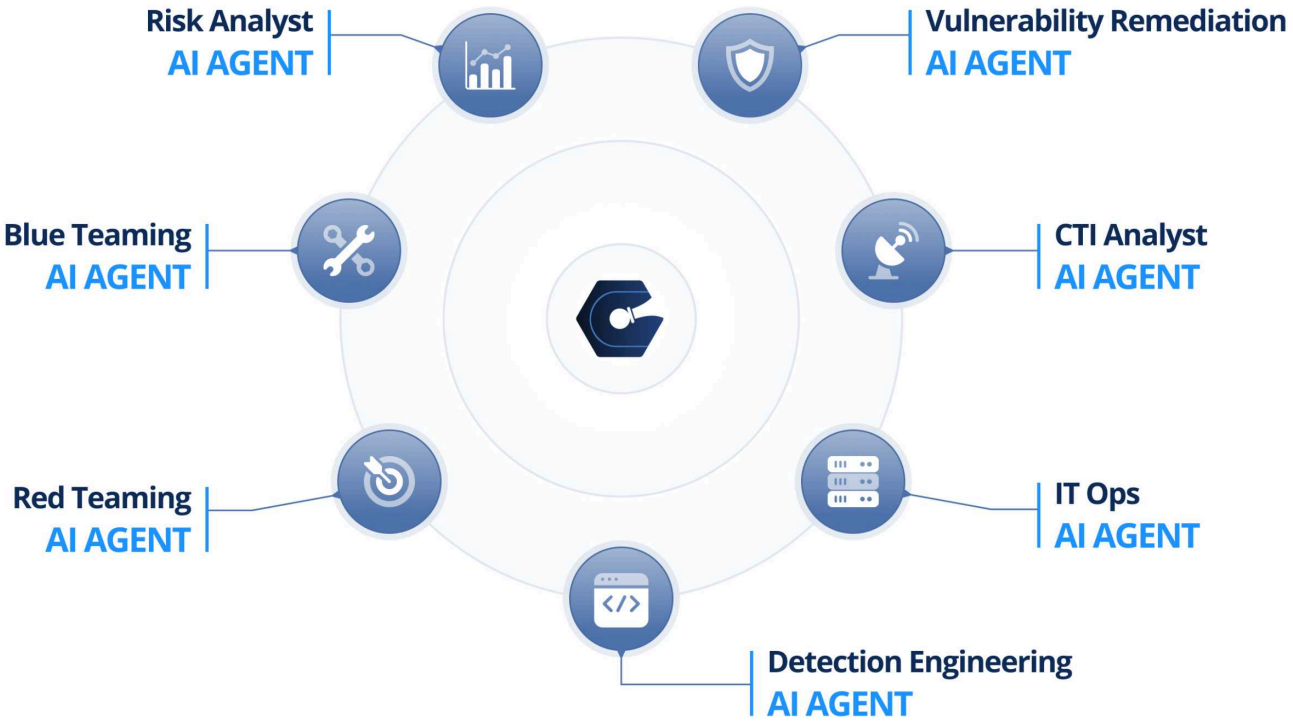
Executive Dashboards

CISO-ready, customizable views. Automatic reports showing how actions reduce the Threat Exposure Score.



AGENTIC AI

A MESH OF AI AGENTS - ALWAYS WORKING



Reduced TCO

Consolidate fragmented tools into one vendor-agnostic platform.

Faster Identification

Discover hidden gaps across cloud, on-prem, and the dark web.

Lower MTTR & MTTD

Autonomous agents accelerate both finding and fixing.

Swift Prioritization

Use AI to rank exposures based on actual exploitability.

Outcome-Based Remediation

Focus on the 5% of gaps that represent 90% of your risk.

KNIGHTGUARD

Gambit cyber

Continuous Threat Exposure Management

SUBSCRIPTION MODULES

KnightGuard Unified Vulnerability Management

- Attack Surface Management
- Unified Asset Intelligence & Prioritization
- Unified Asset Exposure Scoring
- Cloud Misconfigurations NEW
- Dark Web Monitoring
- Unified Vulnerability Prioritization (based on Threat Intelligence, Dark Web, Exploit Availability, Ease of Exploitation, Risk score from security tools, etc.)
- Vulnerability Attack Paths NEW
- Asset Exploitability Attack Paths NEW
- Unified Vulnerability Management Metrics (Team Velocity, Critical Trends, Open/in-progress/fixed Trends, Resurfaced Vulnerabilities, etc.)
- Native Integrations
  - VM Scanners (Tenable, Qualys, OpenVAS, etc.)
  - Cloud Providers & Repositories (AWS, Azure, GCP, GitHub, M365 etc.)
  - Firewalls (Fortinet, Cloudflare, Palo Alto, Cisco, etc.)
  - Identity Solutions (Microsoft EntraID, Okta, etc.)
  - ITSM (ServiceNow, Jira, Slack, Teams, etc)
  - EDR (CrowdStrike, SentinelOne, Defender, etc.)
- Named Customer Success Manager

Vulnerability Remediation AI AGENT

KnightGuard Threat Informed Defense

- MITRE Aligned Threat Intelligence + OSINT
- GIR (General Intelligence Requirements) based Threat Intelligence Prioritization
- Threat Intelligence Operationalization (BYO Threat Intelligence)
- SIEM agnostic Detection Analytics
- Threat Monitoring
- ATT&CK-mapped Adversary Playbooks NEW
- Threat-Based Risk Scoring NEW
- Threat-aligned Logs Prioritisation
- Campaign Intelligence (TTP evolution, tooling, timelines, etc.)
- Top Techniques & Controls Identification
- Controls Mapping & Prioritization (NIST 800-53, MITRE Mitigation, MITRE Defend) NEW
- NIST & MITRE-Based Remediation Guidance
- MITRE Aligned Detection Analytics
- Multi-SIEM Detections NEW
- NIST CSF 2.0 Controls Remediation Mapping
- Threat Coverage & GAP Analysis NEW
- Board Reporting NEW
- Named Customer Success Manager

CTI Analyst AI AGENT

IT Ops AI AGENT

KnightGuard Unified Exposure Validation

- MITRE Aligned Detection Engineering
- Threat Hunting
- Breach Attack Emulation
- 1500+ Ready-to-deploy Emulation Campaigns
- Seamless Purple Teaming
- Detection As Code NEW
- Multi-SIEM Detection Management NEW
- Multi-SIEM Unification NEW
- Native Integrations with SIEM (Sentinel, Splunk, Elastic, etc.)

Vulnerability Remediation AI AGENT

Red Teaming AI AGENT

Blue Teaming AI AGENT

KnightGuard Unified Risk Management/Quantification

- Cyber Risk Prioritization (MITRE, NIST, etc.)
- Ready to Quantify Risk Scenarios (BEC, Ransomware, Dataloss, etc.) NEW
- Cyber Risk Quantification (based on NIST RMF, NIST 800-30, NIST 800-39, NIST 800-53)
- Risk Gap Analysis NEW
- Risk Reduction Guidance Mapped to Organizational Controls
- Organization Context-Based Quantification NEW
- Organization Specific Risk Profiles
- Use case specific Risk Profiles (for DORA, OT, Ransomware, etc.)
- Automated Compliance Coverage (for AWS, GCP, AZURE, etc.)
- CISO Dashboards

Risk Analyst AI AGENT

Notes:

KnightGuard Unified Exposure Validation

KnightGuard Unified Exposure Validation is an add-on module to KnightGuard Threat Informed Defense or KnightGuard Unified Vulnerability Management.

KnightGuard Unified Risk Management & Quantification

KnightGuard Unified Risk Management & Quantification is an add-on module to KnightGuard Threat Informed Defense + KnightGuard Unified Vulnerability Management + KnightGuard Unified Exposure Management.

KNIGHTGUARD

Gambit cyber

Continuous Threat Exposure Management

ABOUT GAMBIT CYBER

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

Expeditions | Bitdefender VOYAGER VENTURES | TRIDENT HORIZON

START WITH ONE MODULE. GROW AT YOUR PACE.

Complete flexibility to begin modestly and expand your CTEM program step by step - no big-bang deployment required.

1. START HERE - PHASE 1 — Unified Vulnerability Management
2. PHASE 2 — Threat Informed Defense
3. PHASE 3 — Unified Exposure Validation
4. PHASE 4 — Unified Risk Management & Quantification

COMPREHENSIVE FRAMEWORK ALIGNMENT

FRAMEWORK CATEGORY	SUPPORTED FRAMEWORKS	KNIGHTGUARD APPLICATION
Security Governance	NIST 800-53 & NIST-CSF 2.0	Automatically maps identified exposures to NIST control families, prioritizing fixes that satisfy regulatory audits.
Intelligence Planning	GIR (General Intelligence Requirements)	Uses GIR framework to categorize threat intelligence.
Adversary Behavior	MITRE ATT&CK®	Operationalize, defences aligned to adversary behaviours across ITOps and SecOps
Defensive Mapping	MITRE D3FEND™ MITRE MITIGATION	Suggests specific technical countermeasures (File Analysis, Decoy Environment) to neutralize identified threats.
Risk Quantification	NIST RMF, NIST 800-30, NIST 800-39	Prebuilt quantification modules for 9+ risk scenarios like BEC, Ransomware, Data Loss, and Insider Threat scenarios.

WHY KNIGHTGUARD WINS

Vendor-Agnostic "Agentic Layer"

Sits on top of existing tools - no rip-and-replace. Operationalizes intelligence in real-time to answer: "Are we actually protected against this specific threat right now?"

Evidence-Based Defense

Replaces "we think we are secure" with "we have validated that our controls work against these specific threat scenarios."

Rapid Time-to-Value

Zero-infrastructure SaaS deployment. Agentic onboarding go from Zero to Visibility in under 60 minutes.

Operational Harmony

Aligns SecOps, ITOps, and GRC under a single source of truth - eliminating silo fatigue permanently.

GET IN TOUCH

Visit Our Website
www.gambitcyber.org

Chat to Sales
sales@gambitcyber.org

Chat to support
support@gambitcyber.org

Our Locations
The Netherlands | India