KNIGHTGUARD

Gambit cyber

Unified Exposure Validation (UEV)

Knowing where you're exposed is not enough. The critical question every security team must answer is: **"Can a real adversary, using known attack techniques, successfully execute an attack in our environment and will we detect it?"** KnightGuard's Unified Exposure Validation (UEV) module answers this definitively by combining 1,500+ real-world emulation campaigns with AI-driven Detection Engineering creating a high-speed feedback loop that transforms offensive validation from a simple "test" into an automated "upgrade" for your defensive stack.

UEV continuously validates that your SIEM, EDR, and firewall controls work as intended, closing the silent failure gap that leaves 40% of security controls ineffective due to misconfiguration or drift.

KEY UEV CAPABILITIES

Agentic Purple Teaming

The Red agent helps generate exploits for specific scenarios while the Blue agent simultaneously generates detection analytics to validate control effectiveness replacing weeks of manual work with minutes of automated precision.

AI-enabled Detection as a Code (DaaC) NEW

Treat your security logic like software. Manage detections life cycle within the platform. Write the rule once; automatically translate it for Splunk, Sentinel, QRadar, or Elastic simultaneously.

1,500+ Ready-to-Deploy Campaigns

Extensive library of adversary playbooks mapped to the latest threat intelligence, updated weekly. Covers lateral movement, data exfiltration, credential theft, and LOTL scenarios without disrupting production environments.

Multi-SIEM Unification NEW

Eliminate the "language barrier." Normalize detection logic across Splunk, Sentinel, QRadar, and Elastic deploying a single rule across all SIEMs simultaneously.

THE PURPLE TEAM FEEDBACK LOOP

CONSUME	VALIDATE	ENGINEER	ORCHESTRATE
Ingest Threat Data	**Red Team Tests**	**Detection as Code**	**Push & Patch**
High-risk ATT&CK and techniques from the TID module	AI Agents generate exploits for each stage	AI Agents generate context specific detections	Rule to SIEM, ticket to ITSM for patching

THE SHIFT UEV ENABLES

Assumed Security	→ Validated Defence
Manual Red Teaming	→ Agentic Purple Teaming
Static Detection Rules	→ AI-enabled Detection as Code
Siloed BAS Tools	→ Integrated Exposure Loop
Reactive Threat Hunting	→ Intelligence-Led Hunting
IOC-Based Response	→ ATT&CK Aligned Detection

UEV BUSINESS BENEFITS

↓ MTTR

AI workflows automate step-by-step remediation playbooks

↑ ROI

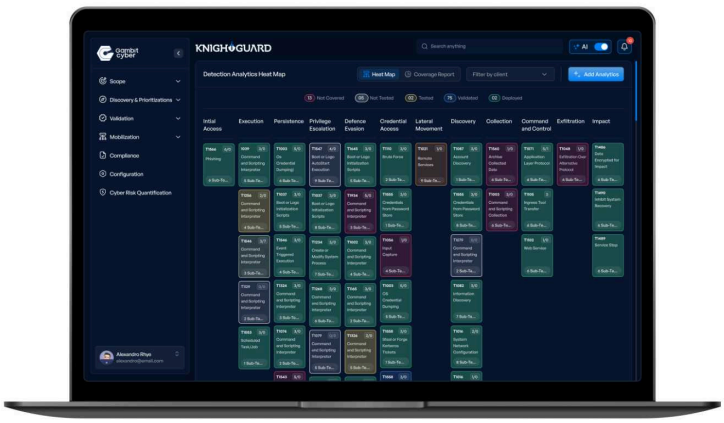
Identify which controls work and which are redundant

1,500+

Ready-to-Deploy Emulation Campaigns

40%

of Controls Fail Silently UEV helps validate them



ADVANCED AGENTIC THREAT HUNTING NEW

KnightGuard's pre-built hunting queries leverage the same intelligence used in emulation campaigns, generating hunt logic in KQL, AQL, SPL, or any query format automatically enabling proactive search for silent threats that have already evaded perimeter controls.

KNIGHTGUARD

Gambit cyber

Unified Exposure Validation (UEV)

UEV VS. TRADITIONAL BAS: THE DIFFERENTIATORS

CAPABILITY	STANDARD BAS	KNIGHTGUARD UEV
Validation Method	Static path analysis (mathematical)	Active emulation: 1,500+ real-world campaigns
SIEM Support	Usually proprietary or single-connector	Multi-SIEM unification: one rule, many platforms
Logic Management	Manual rule creation in console	Detection as Code: scalable, versioned, automated
AI Integration	Chatbots for "summarization"	Agentic AI: autonomous Red/Blue agents that execute tasks
Threat Hunting	Reactive, IOC-based	Proactive: intelligence-led, and TTP-based

UEV AGENTIC AI - USE CASES

1 Ransomware Readiness Test

When a new ransomware strain is identified, the Red Agent parses the threat report, maps relevant ATT&CK techniques, and runs emulation campaigns - confirming whether your SIEM and EDR would catch the attack in minutes, not days.

2 Detection Gap Remediation

Emulation confirms SIEM failed to alert on a lateral movement technique. The Blue Agent immediately generates the specific KOL/SPL detection logic, which is validated, deployed, and tracked without any manual engineering effort.

3 Controls Validation

Re-test controls after system updates, patches, or configuration changes. Every validated fix is recorded with evidence creating a defensible audit trail for compliance and board reporting.

4 ATT&CK Aligned Threat Hunting

Intelligence from emulation campaigns automatically seeds hunt queries targeting TTPs known to evade your specific control stack proactively surfacing threats that bypassed detection before they escalate.

WHY KNIGHTGUARD WINS

Evidence-Based Defence

Replace "we think we're secure" with "we have validated our controls work against these specific threat scenarios" - backed by continuous, automated evidence.

Faster Detection & Response

AI-driven Detection as Code reduces mean time to detect (MTTD) and mean time to respond (MTTR) through automated detection generation and deployment.

Maximise Security ROI

Identify which controls work and which are redundant. Eliminate tool overlap and reallocate budget toward validated, effective security investments.

Continuous Improvement Loop

Every emulation feeds back into detection improvements, which feed back into hunt queries, which feed back into future campaigns - a self-reinforcing cycle.

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

Unified Exposure Validation (UEV)

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

Unified Exposure Validation (UEV)

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