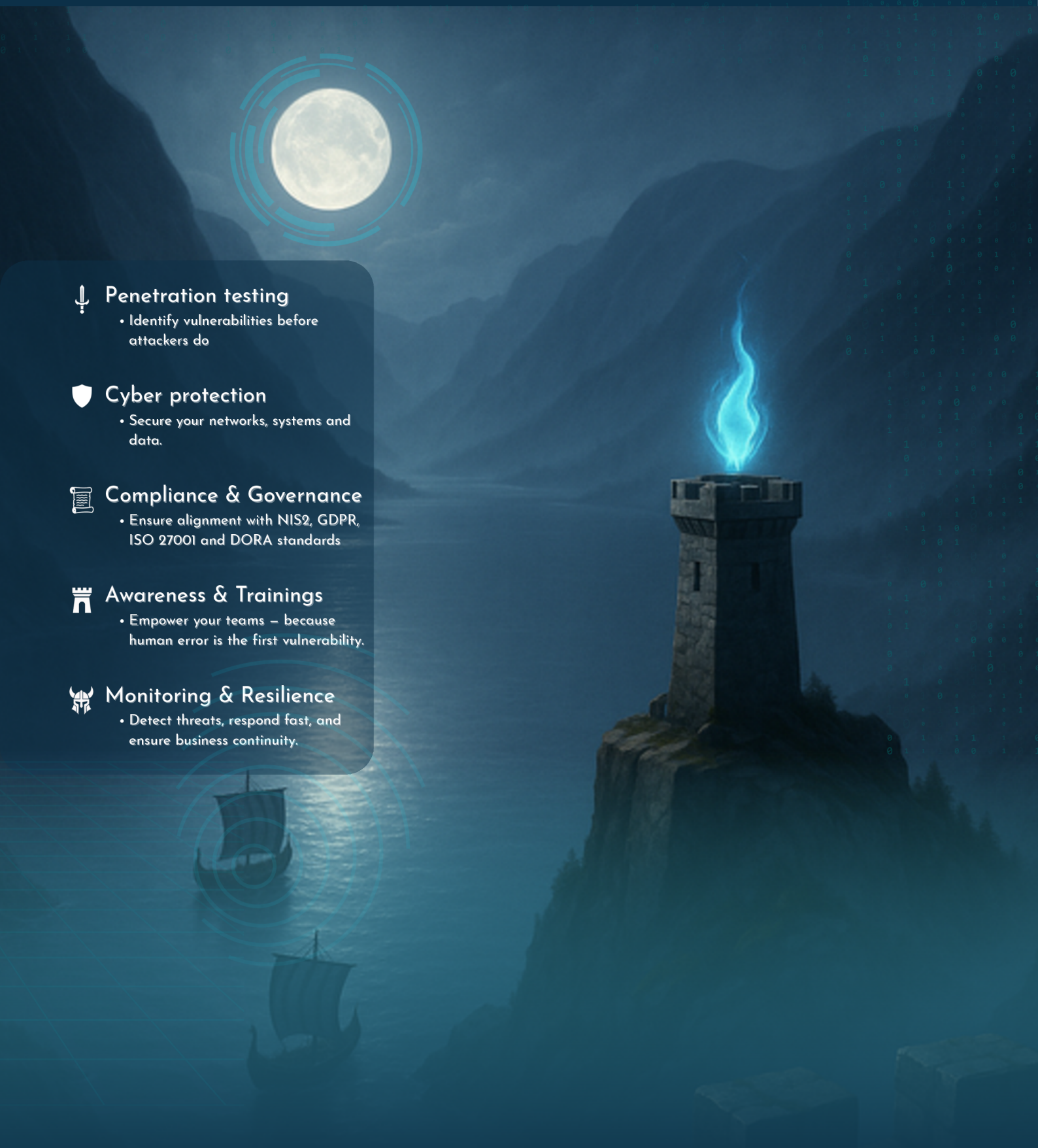
VARDEN security

MODERN GUARDIANS, ANCIENT SPIRIT



Penetration testing

- Identify vulnerabilities before attackers do

Cyber protection

- Secure your networks, systems and data.

Compliance & Governance

- Ensure alignment with NIS2, GDPR, ISO 27001 and DORA standards

Awareness & Trainings

- Empower your teams – because human error is the first vulnerability.

Monitoring & Resilience

- Detect threats, respond fast, and ensure business continuity.

Penetration testing

Identify vulnerabilities before attackers do.

We deliberately **simulate attacks** on your infrastructure—applications, networks, systems, APIs—to reveal hidden weaknesses that real adversaries could exploit. A penetration test is more than a vulnerability scan: it's an intentional, adversarial approach that tests not just what's wrong, but how far an attacker could go.

During a pentest, we exploit **chains of vulnerabilities** (e.g. weak credentials + misconfiguration + outdated software) to expose the impact (data exfiltration, lateral movement, privilege escalation). Then, we deliver a prioritized roadmap so you can remediate the most critical issues first.

This proactive approach helps you:

🚨 Prevent data breaches before they happen
📊 Allocate your security budget where it matters most
✅ Demonstrate control and maturity to stakeholders and regulators

According to industry benchmarks:

- In 2023, external penetration tests uncovered 34 % of vulnerabilities as **critical or high risk**.
- 72 % of organizations said pentesting had prevented a breach at their company
- In **85 % of organizations**, pentesters detected password policy flaws; in 60 %, they found high-risk vulnerabilities linked to outdated software.
- 50 % of critical network pentest findings stemmed from **misconfigurations**; 30 % from **unpatched systems**.

These figures show that even well-equipped systems often hide serious risks, risks that can **only be revealed by a skilled, adversarial test**.

Cyber protection

Secure your networks, systems and data.

In today's digital world, vulnerabilities are **no longer a matter of if, but when**. Our Cyber Protection services build resilient defenses across your entire ecosystem, from networks to endpoints, from the cloud to your most sensitive data.
We apply a **defense-in-depth strategy,** combining strong network security, intelligent endpoint protection, strict access control, and continuous encryption of information in motion or at rest. Every layer reinforces the next, ensuring that **even if one fails, the others contain the threat.**
This holistic approach transforms cybersecurity from a technical shield into a source of confidence and continuity protecting not only your systems, but your organization's reputation and trust.

The Microsoft / SMB Cybersecurity Report indicates that the average cost of a cyberattack for small and medium-sized businesses is **USD 254,445**.

The website ZeroThreat reports that in 2025, an average of **133 new vulnerabilities are identified each day**.

According to Cybersecurity Ventures, the annual cost of cybercrime is expected to reach USD 10.5 trillion by 2025.

NIS2 — A European directive that strengthens cybersecurity obligations for companies and public bodies to protect essential services and digital infrastructure.

GDPR — The EU regulation that protects personal data and ensures individuals' privacy rights.

ISO 27001 — An international standard that defines how to manage information security through a structured risk-based system.

DORA — A European regulation ensuring that financial institutions can resist and recover from digital disruptions and cyberattacks.

Compliance & Governance

Ensure alignment with NIS2, GDPR, ISO 27001 and DORA standards

In an increasingly regulated digital environment, **compliance** is no longer just a legal obligation, it **is a cornerstone of trust and responsability**.

Our Compliance & Governance services help organizations navigate the **complex landscape of European and international cybersecurity standards**, including NIS2, GDPR, ISO 27001 and DORA.

We translate regulatory requirements into concrete, operational measures that strengthen both your security posture and your reputation. Through structured **risk assessments and policy frameworks**, we ensure that your organization not only meets compliance criteria but also integrates them into daily operations.

A spear-phishing test is a controlled, ethical simulation of a targeted phishing attack. It uses publicly available information (Open-Source Intelligence, or OSINT) to craft realistic and personalized messages that assess an organization's resilience to social-engineering threats.
The goal is to measure vulnerability, improve awareness, and strengthen defenses before a real attacker strikes.

In 2024, **95% of data breaches were linked to human errors**, such as insider mistakes, mishandling of information, or poor credential management according to a report by Mimecast and Infosecurity Magazine.

According to SentinelOne, **approximately 90% of cyber incidents result from human behavior or mistakes**, such as weak passwords or clicking on malicious links.

Varden Academy: awareness & trainings

Empower your teams – because human error is the first vulnerability.

Technology alone cannot secure an organization. **People are at the heart of cybersecurity.** Our Awareness & Trainings programs are designed to transform your teams from potential targets into active defenders. Through interactive workshops, real-life simulations and tailored e-learning modules, **we raise awareness about the most common risks** such as phishing, social engineering, password misuse and data leaks.

Beyond simple information, we foster a **culture of vigilance** and responsibility. Employees learn to recognize suspicious behavior, respond appropriately, and adopt best practices in their daily work. By empowering people with the right reflexes, organizations dramatically reduce their exposure to incidents.

At Varden Security, we believe that awareness is the first and most powerful firewall, the one built in every individual's mind.

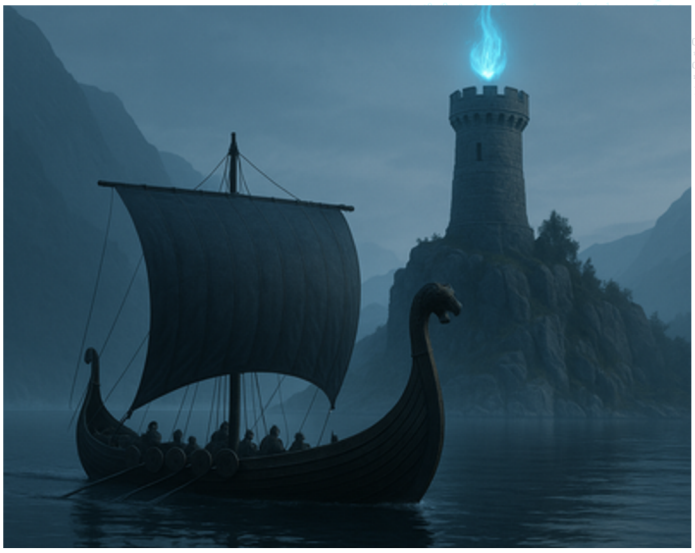
Monitoring & Resilience

Detect threats, respond fast, and ensure business continuity.

Cybersecurity is not a one-time effort. It's a continuous process of vigilance. Our Monitoring & Resilience services ensure that every alert is detected, analyzed, and addressed before it becomes a crisis. By combining advanced detection tools with human expertise, **we provide 24/7 visibility** over your digital environment, enabling rapid response to emerging threats.

Effective monitoring is about more than technology; it's about anticipation. Through constant surveillance of systems, networks, and endpoints, **we identify anomalies in real time** and activate the right countermeasures. When incidents occur, our resilience protocols, from containment to recovery, guarantee operational continuity and minimal downtime.

At Varden Security, **we believe resilience is the true measure of cybersecurity maturity.** Detecting threats is essential, but being able to adapt, recover, and keep moving forward is what truly defines a secure and trusted organization.



In 2023, the a**verage period an attacker remains in a system before being detected was 10 days**, down from 16 days in 2022, according to the Mandiant M-Trends Report.

During an outage or security incident, **direct financial losses can range from USD 10,000 to over USD 1 million**, depending on the severity, according to The State of Resilience 2025 report.

Ethical & Legal Framework

- Written authorization is mandatory before any test (management, HR, legal).
- Rules of engagement (ROE) must clearly define scope, targets, exclusions, and technical boundaries.
- No real credential harvesting, simulated login pages must not store real passwords.
- Full anonymity in reporting: no individual naming or shaming.
- Immediate educational feedback for employees who interact with the simulated attack.
- Incident response plan in place: if the test triggers an actual alert, treat it as a real event and stop immediately.

VARDEN security

When the Vikings' flames turned digital...

A long time ago, in the misty lands of the North, Viking villages entrusted their safety to an elite group. These men and women, **known as the Varden**, were neither kings nor ordinary warriors. They did not fight for glory, but for vigilance, prevention, and silent protection.

While others set sail to conquer new territories, **the Varden remained at the edge of the fjord, watching for signs in the fog**, listening to the wind, and observing the sky. Their strength lay in their intuition — in their ability to **analyze danger and anticipate attacks** before they occurred.

Their emblem was a stone tower, symbolizing a watch post, topped with an eternal blue flame, a reminder of their unwavering vigilance. This flame was neither destructive nor warlike; it represented **the light of knowledge, the one that illuminates dark paths**, unmasks deception, and reveals invisible threats.

Today, in a digital world where attacks strike without a sound, **Varden Security carries the torch of those ancient sentinels**.

The warriors have changed their weapons. Swords have become algorithms. Shields have become firewalls. Yet **the spirit of the Varden endures**.

In the cyber realm, Varden Security is the sentinel on the tower, the one who sees before others, and acts before it's too late.

Our expertise:

1. Penetration Testing — Identify vulnerabilities before attackers do
Our pentesting services follow a progressive framework to meet every security maturity level:
- One-time Pentest — a focused security audit to detect vulnerabilities.
- Pentest + Fix & Validation — we correct the vulnerabilities and verify remediation.
- Pentest + Verification — independent validation of in-house fixes.
- Pentest + Guidance & Verification — full support from detection to confirmed closure.
- Custom Pentest (on request) — tailored scenarios, including advanced red-team testing.

2. Cyber Protection — Secure your networks, systems and data
Our system protection services strengthen your digital infrastructure through:
- EDR (Endpoint Detection & Response) — advanced endpoint defense.
- XDR (Extended Detection & Response) — unified threat detection across all layers.
- SIEM (Security Information & Event Management) — centralized monitoring and correlation.
- Secure storage per workstation — data encryption and controlled access.

3. Compliance & Governance — Ensure alignment with NIS2, GDPR, ISO 27001 and DORA standards
We help your organization meet European and international cybersecurity requirements through:
- Risk assessments and gap analysis for NIS2, GDPR, ISO 27001, and DORA (financial sector).
- Tailored compliance roadmaps and continuous improvement frameworks.
- Policy development and risk governance models aligned with your business processes.

4. Varden Academy, awareness & Trainings — Empower your teams against human error
Our awareness programs combine OSINT-based spear-phishing and custom training campaigns:
- Controlled phishing campaigns using Varden's secure delivery systems.
- Targeted OSINT data collection to craft realistic test scenarios.

5. Monitoring & Resilience — Detect threats, respond fast, and ensure business continuity
We ensure continuity through proactive monitoring and recovery strategies:
- Continuous threat monitoring and anomaly detection.
- PRA (Disaster Recovery Plan) — structured business continuity and recovery procedures.
- Incident response playbooks and resilience audits.

www.varden-security.eu
contact@varden.io
Axel: +32470478806
Stéphane: +32495267506
Mathieu: +32477357176

Editeur responsable Mathieu Michel, rue Saint Urbain, 5 - 1370 Jodoigne