The Cyber Resilience Guide

The 7 most common security mistakes

– and how to prevent them

CYLOQ

Threats are moving faster. Is your security keeping up?

Cyber threats are evolving faster than ever. AI-driven attacks, zero-days exploited within hours, and supply chain intrusions are no longer things that might happen, they happen all the time.

According to the IBM Cost of a Data Breach Report 2025, the median cost of a data breach was 4.44 million USD. A large portion of these incidents originated from vulnerabilities that could have been prevented if the right protective measures had been in place. Among the most common entry points were phishing, attacks via suppliers and third parties, and compromised login credentials. At the same time, automation and AI accelerate both the speed and reach of attacks, resulting in more infections as more targets are hit in less time.

At Cyloq, we review hundreds of environments every year. In this guide, we summarize the seven most common security mistakes we see in the real world. Not only in code and configuration, but also in workflows, decision-making, and security culture.

Established frameworks like the OWASP lists are important reference points, especially within web application security, but they only capture part of the picture. In this guide, we combine these frameworks with insights from real-world attacks, tests, and operations. We highlight both technical and organizational weaknesses that appear again and again, and provide actionable advice and recommendations on how to prevent them.

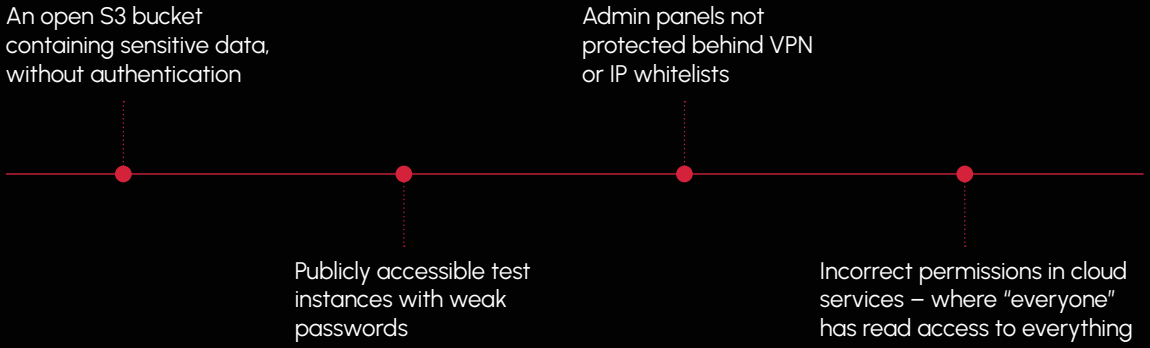
1

Misconfigured systems and services

Misconfigurations are among the most underestimated risks to IT security. They appear in everything from applications and cloud services to network infrastructure and authentication solutions.

In the OWASP Top 10 2025 for web applications, this is listed as A02: Security Misconfiguration, but the problem extends far beyond the web. Incorrect settings, leftover functions, and open access points show up across all types of systems and environments. All it takes is a single incorrect setting, an unnecessarily open port, or a leftover debug function to open the door for an intrusion.

Common mistakes we see:



The root cause is often small mistakes often caused by stress, unclear responsibilities, or complex environments where no one has full oversight. Many systems are gradually built by different people, often with inconsistent documentation, which makes it difficult to maintain full visibility. This lack of consistency can easily result in oversights that leave the entire environment exposed.

What you can do:

Continuously scan for vulnerabilities

Use automated vulnerability scanning tools, both on code level and exposed infrastructure. Do this continuously, not just at release. Make sure to include test and staging environments in your scans.

Define standard configurations

Define what a secure system configuration looks like in your organization. This makes deviations easier to detect and ensures security settings are actually followed in practice.

Establish clear deployment and change management routines

All changes must be followed by testing. Automated CI/CD pipelines with integrated security controls reduce the risk that misconfigurations reach production.

Review, audit, document

Secure configuration is not a one-time task. It requires ongoing work, clear ownership, and updated routines. Make sure to document not only what you do - but why you do it.

2

Insufficient network segmentation

Network segmentation is one of the most fundamental defense mechanisms in modern IT environments.

A flat network structure is like leaving all the doors of a building unlocked. If an attacker gains access through a single vulnerable point, for example, a user's device or a minimally protected server, they can often move freely through the rest of the infrastructure. This is called lateral movement, and it is common in targeted attacks.

An attacker may gain initial access through an outdated external web interface and, within hours, obtain full access to internal HR systems, financial data, and customer information. All because segmentation was missing.

What you can do:

- Separate sensitive environments from user networks
- Restrict communication between segments with firewalls and policies
- Allow only "need-to-know" access between systems
- Combine segmentation with Zero Trust principles

Segmentation doesn't solve everything. But it can be the difference between a local incident and a full-scale breach. By restricting access, segmentation compensates for other weaknesses and buys you time to react.

3

Incident response that only exists on paper

Most organizations have some form of incident response plan. It sits in a folder on the intranet, was last updated a few years ago, and includes roles and processes that are no longer relevant. And it has never been tested in practice. Only when a real incident occurs do the weaknesses become clear, such as:

- Roles are unclear or unstaffed
- Logging doesn't capture what is actually happening
- Communication paths are unclear
- Decisions are made too late - or not at all

The impact is that the attack is not stopped in time, and the consequences become enormous. Imagine a ransomware attack starting late on a Friday. The IT department scrambles to contain it, but with limited visibility, they don't realize how severe it is. The security manager isn't looped in until Monday morning. By then, the damage is already done. The attack has spread, backups are encrypted, and multiple business-critical systems are offline.

To strengthen your incident response capabilities:

Simulate real scenarios

Run tabletop or red teaming exercises with real-time decisions.

Test your tech stack

Do your logs capture what you actually need?

Clarify responsibilities

who makes decisions, communicates, and handles recovery?

Train the entire organization

Not everyone needs to know everything, but everyone should know their role.

4

Overconfidence in internal competence

Another common mistake is relying too heavily on the internal security team. Even highly skilled teams risk becoming blind to their own environments. When you review the same codebase, the same configurations, and the same systems daily, it's easy to miss subtle issues. And that's often where the real threats are hiding.

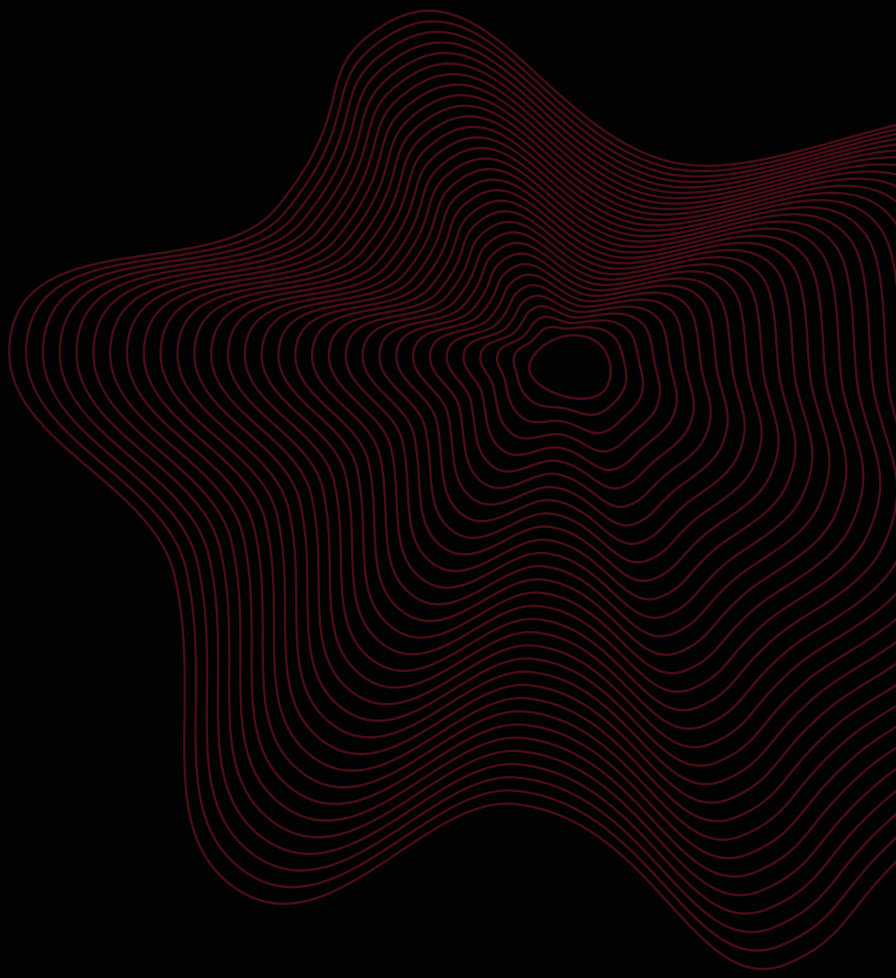
Many organizations also overestimate their security posture. Internal code reviews, automated tools, or checklist-based audits may create a sense of safety, but it is not always reality. We often hear: "We did our own review recently – it looked good."
Yet during the first external test, we've uncovered critical vulnerabilities such as RCE (Remote Code Execution) or exposed sensitive data.

We recommend supplementing the internal team with an external security expert who is not part of the organization's processes and sees the environment with fresh eyes. This is often when the real risks are uncovered. And to maintain perspective over time, rotate between external testers, as they too can become blind to an environment.

Consider:

- **Complement internal reviews with external validation**
  Internal insights are valuable, but outside perspective reveals what teams often miss.
- **Schedule regular external penetration tests**
  Frequent, real-world testing uncovers vulnerabilities before attackers do.
- **Choose a skilled partner**
  Not all auditors deliver the same value. Find experts who understand your risks.

External validation also builds trust among customers, investors, and the board by showing that your security has been practically tested and verified.



5

Weak authentication and access controls

Authentication is the first barrier an attacker must bypass. But if that barrier is weak or inconsistent, the strength of the rest of the infrastructure doesn't matter. We still see shared accounts, plaintext passwords, MFA enabled but not required, or even default passwords on exposed services. But authentication (who can log in) is only half the story. Authorization (what they can do once logged in) is equally crucial.

OWASP classifies these under:

- A07: Authentication Failures
- A01: Broken Access Control (one of the most critical and common vulnerabilities we find)

Common mistakes we see:

- MFA configured but not enforced for all endpoints (A07)
- Missing protections against repeated login attempts, enabling credential stuffing and hybrid password spraying (A07)
- Improper session token handling logged in plaintext (A07)
- Users modifying API calls or URL parameters to access others' data (A01)
- Poorly defined roles that allow regular users to gain admin access (A01)

These issues create an attack surface that can be exploited for long periods before being detected.

What you can do:

- Implement centralized, standardized authentication (SAML, OIDC)
- Manually review permissions and access logic
- Require MFA everywhere
- Apply least privilege for users and integrations
- Enforce protections against brute-force attempts
- Ensure proper session management
- Monitor authentication flows in real time

6

Supply chain vulnerabilities

You may have full control over your own systems, but that doesn't help if your suppliers don't uphold the same standard. Modern systems rely heavily on third-party components: libraries, APIs, plugins, cloud services, SaaS platforms. Each integration is a potential entry point.

Supply chain attacks have skyrocketed. According to the 2025 DBIR, breaches involving a third party have doubled: from 15% in 2024 to 30% in 2025. Attackers often look for side doors. Third-party integrations frequently receive less scrutiny, despite holding access to critical systems or data.

Common mistakes we see:

- External components without update or ownership checks
- Weak security clauses in contracts
- Lack of security requirements in procurement
- No follow-up on supplier security stance

OWASP defines this category as A03: Software Supply Chain Failures.

What you can do:

Demand strict requirements from vendors and third-party services

Define clear minimum requirements for security levels, patching policies, incident reporting, and role-based access.

Maintain separate environments and access controls for different vendors

Isolate integrations so they cannot affect core systems in case of a compromise.

Implement Software Composition Analysis (SCA)

Use automated tools that flag vulnerable dependencies and license risks within the codebase.

Regularly review software dependencies

Keep track of which components you use, and how they evolve over time.

Follow up with recurring reviews and security dialogues

Setting requirements during onboarding is not enough; continuous follow-up is mandatory.

7

Weak security culture

Cybersecurity starts with people, not firewalls. That is why the human factor is one of the most vulnerable points in most organizations. According to Verizon DBIR 2025, 60% of all breaches involved human error. A clicked phishing link, an unlocked workstation, or mishandled USB stick can trigger a chain reaction. Even the best technical defenses can be bypassed if users aren't aware of how attacks work, or how their actions might open the door.

Security culture does not happen on its own. It requires long-term work. A single annual e-learning module is simply not enough.

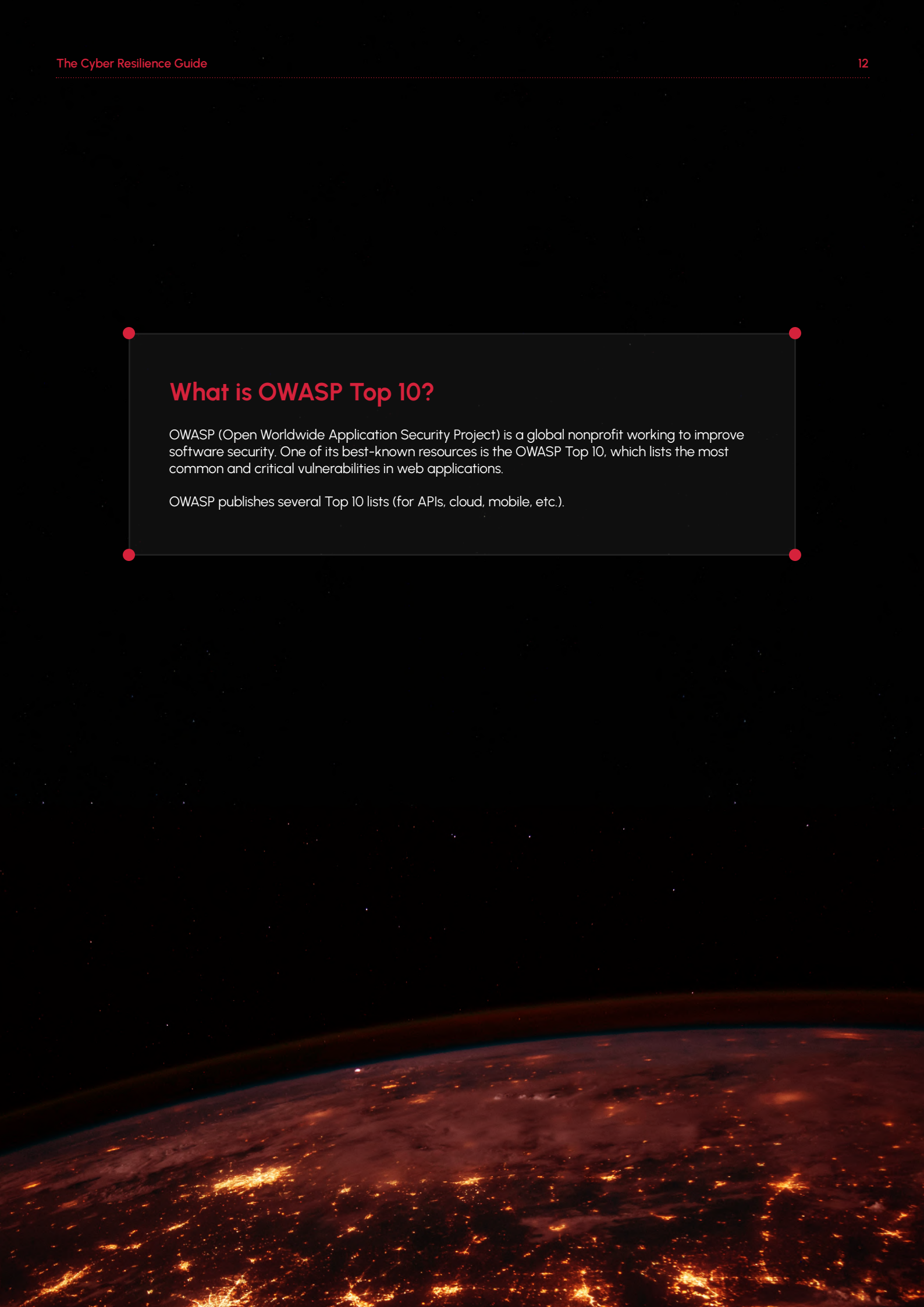
What you can do:

- Configure spam filters to stop phishing before it reaches inboxes
- Train continuously, not occasionally
- Run realistic simulations
- Put security on the internal agenda
- Build an environment where people report issues quickly
- Track behaviors and improve continuously

What is OWASP Top 10?

OWASP (Open Worldwide Application Security Project) is a global nonprofit working to improve software security. One of its best-known resources is the OWASP Top 10, which lists the most common and critical vulnerabilities in web applications.

OWASP publishes several Top 10 lists (for APIs, cloud, mobile, etc.).



About Cyloq

We have worked with everything from tech companies and government agencies to international enterprises and critical infrastructure. With more than 15 years of experience, we've developed a sixth sense for how attacks happen, how weaknesses arise, and where real risks hide.

We're a partner you can trust, with the expertise to understand your reality and adapt our work to your industry's specific requirements.

Ready to see if your systems are as secure as you think?

Now you know the mistakes that can undermine even the most experienced security teams. Knowledge goes a long way, but you also need to test your systems for real.

A penetration test is the most concrete way to identify vulnerabilities before someone else does. It shows exactly where the weaknesses are – and where to strengthen.

Cyloq performs advanced, manual tests from an attacker's perspective. We map your attack surface, identify vulnerabilities, and show how far an attacker could get – and what you can do to stop it.

Our goal is not to confirm that everything looks fine. Our goal is to find what could bring you down, before someone else does. And if we can't find anything – you can be confident no one else will either.

"We want them to find things, but of course we had strong confidence. We didn't think they'd be able to do it in such a short time."

- Tim, VX Fiber

"We were pleasantly surprised. They found several issues that hadn't been discovered in previous penetration tests or our bug bounty program. We were very happy with the results!"

- Marcus, Stravito

Prevent weaknesses. Test for real.

This is how a penetration test with Cyloq works:

Scoping meeting

We define scope and goals together

Attack phase

We test your environment thoroughly

Ongoing reporting

Critical issues are reported immediately

Delivery

You receive a clear, actionable report

Andreas Gjelset

Cybersecurity Consultant
Tel: +46766777766
Mail: andreas@cyloq.se

Cyloq AB
Pyramidvägen 7, 169 56 Solna
+46 (0) 10 333 10 33
hello@cyloq.se