SERVICE
Portfolio

Provider
45 Cyber Labs
Finland

Revised
February 2025

CYBER LABS

TABLE *of Content*

From **over 200 available solutions**, we highlight the most impactful to your attention. We believe that each of our partners has unique requirements, and we deliver customized services. Talk to our Subject Matter Experts — your cybersecurity objectives deserve top-tier expertise.

CYBER LABS

PENETRATION *Testing*

Penetration Testing is a methodical and controlled simulation of cyber attacks on web and mobile apps, IoT devices, SaaS solutions, and both traditional and cloud infrastructure. It aims to identify and exploit weaknesses and vulnerabilities, and provide an understanding of risks to your business.

What we deliver?

The resulting report bridges the gap between strategy and execution by providing an executive summary for leadership as well as in-depth technical details for engineering teams. Each finding is contextualized and clearly describes the impact and remedial action needed to strengthen your security posture.

Web Application Penetration Testing involves simulating real-world attacks on your web application to identify and exploit vulnerabilities, such as authentication flaws, injection attacks, or misconfigurations, ensuring your application is secure against potential threats.

Azure / AWS Configuration Review assesses and validates the security settings and configurations of cloud Infrastructure as a Service (IaaS) resources and subscriptions to ensure they follow best practice, compliance requirements, and mitigate potential vulnerabilities.

Kubernetes Review evaluates the security configurations of your Kubernetes clusters to identify vulnerabilities, misconfigurations, and potential risks that could expose the system to attacks or breaches.

Windows / Linux / Network Device Review evaluates the configuration to identify vulnerabilities, misconfigurations, or security weaknesses that could be exploited by attackers. It involves a review of settings, account and access controls, local security policies, logging and network and firewall rules to ensure proper security measures are in place.

Segregation Testing evaluates the effectiveness of your security controls that isolate different network segments or systems, ensuring that sensitive data and resources are properly separated and protected from unauthorised access.

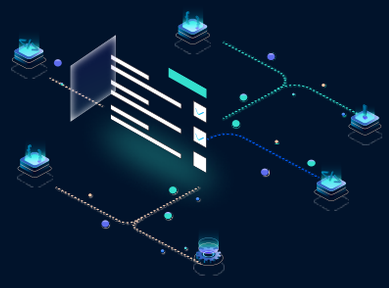
Infrastructure Penetration Testing is a systematic security evaluation that assesses vulnerabilities and defenses of your network, focusing on internet-facing services and internal systems to identify and exploit weaknesses upon agreement. Our goal is to simulate real-world attack scenarios, helping your organisation to protect sensitive information and enhance overall network resilience.

Mobile Application Testing simulates attacks on your mobile apps to identify vulnerabilities, such as insecure data storage, weak authentication, or code flaws, which could be exploited by attackers. This involves assessing both the app itself and its communication with RR backend servers to protect sensitive data and ensure proper security measures.

Client Application / Thick Client Testing assesses the security of your standalone software applications that run on client machines, such as desktops, laptops, or mobile devices, to identify and exploit vulnerabilities, assess security controls, data handling, communication with servers and evaluate overall system resilience against potential threats.

Breakout Testing simulates attacks on your escape-restricted environments, such as VMs, containers, or kiosks, identifying vulnerabilities and assessing security controls. The aim is to determine if an attacker can break free from the isolated environment and gain unauthorised access to your host system or network.

CYBER LABS



STRATEGY *& Compliance*

Ensure your organization meets legal and regulatory requirements and industry standards with our cybersecurity Strategy & Compliance services. We help businesses adopt compliance frameworks through maturity assessments, gap analyses, and provide advice to set out a cyber defence strategy. Our expert guidance supports leadership teams in making informed decisions to strengthen security and achieve compliance. Partner with us to safeguard your operations and build trust with stakeholders.

What we deliver?

The agreed outcome may be a report, provision of policies and procedures, or a complete suite of insights, strategies and tools designed to align your operations with the requirements of the regulation or standard in scope.

DORA (Digital Operational Resilience Act) is a regulatory framework to address cyber threats and operational risks in financial institutions and their critical suppliers, ensuring institutions can manage and recover from disruptions. It applies to banks, insurers, fintechs, and ICT providers, harmonising resilience standards across the EU.

NIS 2 (Network and Information Security Directive 2) provides a solid framework that tackles cyber risks in critical sectors by enhancing security and incident handling. It covers key industries such as energy, healthcare, transport, and digital infrastructure, and its implementation slightly varies across member states.

CRA (Cyber Resilience Act) provides a regulatory framework for cybersecurity requirements in digital products such as smart devices, when they enter the EU market. We provide guidance to manufacturers, importers and distributors and assessments of their products to ensure they are in a state of compliance.

ISO 27001 is an international standard for managing information security through a structured Information Security Management System (ISMS). It provides a framework of policies and enhances security, builds trust, and supports regulatory compliance through promoting best practice.

ISO 9001 is an international standard for quality management systems (QMS) that ensures organizations consistently meet customer and regulatory requirements. It focuses on improving processes and customer satisfaction. By fostering a culture of continuous improvement, it boosts efficiency, credibility, and competitiveness.

RED (Radio Equipment Directive) sets essential requirements for wireless devices such as smartphones, Wi-Fi routers, and IoT devices, ensuring compliance with cybersecurity provisions, such as protections against fraud, data breaches, and unauthorized access.

IEC 62443 provides a standard for securing industrial automation and control systems (IACS) against cyber threats. It applies to industries like energy, manufacturing, and critical infrastructure. By defining clear security measures, it enhances system resilience, reduces vulnerabilities, and promotes global interoperability.

SOC 2 (Systems and Organization Controls 2) is a framework for managing data securely to protect the privacy and interests of an organization's clients. It applies to technology and service providers handling sensitive customer data. By ensuring compliance with trust principles, it enhances data protection, builds customer confidence, and supports regulatory alignment.

CYBER *SkillUp*

Cybersecurity training equips organizations with the knowledge to identify, prevent, and respond to cyber threats, reducing the risk of breaches. A culture of security awareness among employees helps to reduce human error, which is a leading cause of breaches. By recognizing malicious patterns early, teams can act proactively to mitigate threats before they cause significant harm.

What we deliver?

Training sessions include real-world scenarios and interactive labs (where applicable), allowing participants to fully immerse themselves in the experience. Each session comes with detailed reference materials, guidelines, checklists, and remediation strategies, and can be delivered in-person or online.

Cyber Awareness for Decision-Makers focuses on understanding key cybersecurity risks, the potential business impacts of breaches, and the importance of proactive security strategies. We emphasise aligning cybersecurity with business objectives and legal compliance while promoting a culture of accountability. You gain practical insights into responding to incidents to support organizational resilience.

Cyber Awareness for Employees empowers cyber preparedness by recognizing common threats like phishing, ransomware, and social engineering, along with safe online practices. We emphasize the importance of following company policies, using strong passwords, and reporting suspicious activity. Practical examples and hands-on tabletop exercises help to reinforce your employees' role in protecting the organization’s security

Secure Engineering Training focuses on secure coding practices, identifying and mitigating common vulnerabilities like SQL injection, XSS, and insecure authentication. We include threat modelling, secure development lifecycle processes, and understanding of technical cybersecurity frameworks such as OWASP and MITRE ATT&CK. Practical exercises in code review, penetration testing, and integrating security into DevOps pipelines are essential for real-world applications.

Professional Exam Preparation includes a thorough review of the selected exam's core domains, key concepts, and frameworks, such as those in CISSP, CEH, or CISM, as well as a range of hands-on practical exams. We arm candidates with advice, scenario-based exercises, and tips for tackling complex questions. Our focused study plans and guidance from certified experts help candidates build confidence and achieve success.

DEVOPS *Validation*

The service integrates cybersecurity into your sprints, transforming your DevOps into a powerhouse that delivers faster, higher-quality results with robust security. It equips product managers with tools like on-demand defect validation and real-world cyber-attack insights to balance speed, quality, and budget effectively. With built-in security and a trusted partner, your product remains secure without slowing down development momentum.

What we deliver?

Our project manager provides structured project plans, milestone tracking, and risk management strategies, ensuring smooth execution from kickoff to completion. Clear progress reports and updates are provided to inform stakeholders and align teams.

Cybersecurity On-Demand provides on-demand access to a dedicated team of cybersecurity experts, available to support your projects and augment your team's capabilities. They help clear backlogs of cybersecurity defects, so your team can focus on core tasks while maintaining strong, integrated cybersecurity throughout the development process.

The Cybersecurity Engineer-in-Residence service ensures security is seamlessly integrated into your development process, helping you accelerate sprint delivery. you gain access to tailored expertise, whether it's quick guidance for specific issues or support for complex, large-scale cybersecurity tasks. This service adapts to your team's workflow, providing the flexibility to address your unique security needs efficiently.

Secure Development Practices embed security into every line of code, ensuring your product is safeguarded from the very beginning. This proactive approach minimizes vulnerabilities and promotes a culture of security within your team. By making secure development a mindset, it transforms security from a task into a core principle of the engineering process.

Cybersecurity Automation Made Easy enhances your security tooling with custom test cases to uncover more vulnerabilities. It empowers your scrum teams by sharing knowledge, enabling them to maximize the effectiveness of their efforts and existing SAST and DAST tools. This service streamlines and strengthens your security automation process, making it more efficient and impactful.

light up your cyber defense **STRATEGY**

We are **45 CYBER LABS**, a Finnish cybersecurity company driven by innovation, integrity, and the relentless pursuit of digital safety. What started as a casual chat between friends has grown into a dedicated team committed to protecting your business in an ever-changing digital landscape.

INFO@45CYBER.COM

45CYBER.COM