Advisory & Consulting Services

Cyber Risk Assurance

Equip your business with the strategic means to identify cyber risks, be prepared and improve your risk resilience with a holistic and integrated risk mitigation approach.

Red Team Exercises

Be prepared for a real security incident, without the risks. The Liquid C2 team simulates a multi-layered cyber-attack that targets an agreed upon set of objectives. The exercise and assessment let you experience a real-world attack and gives you a better view of your team's readiness to detect and respond to it without any risk. Red Team exercises are conducted without the blue team awareness of them to depict an accurate picture of how your organization would react to an advanced persistent threat.

Penetration Testing

Find and fix your vulnerabilities before an attacker exploits them. Our security experts simulate multiple attack vectors to discover vulnerabilities across your systems components and applications that external and internal malicious actors could exploit. Get a clearer picture of your organization's overall security posture through:

Application Penetration Testing
Determine whether your web, mobile, API, or desktop applications have exploitable vulnerabilities with our test methodology based on the OWASP application testing guidelines.

External Penetration Testing
Meet your compliance requirements and test the effectiveness of your perimeter security controls in preventing and detecting attacks against your internet-facing assets by an external attacker.

Internal Penetration Testing
Meet your compliance requirements and test the effectiveness of your internal controls in preventing an adversary from laterally moving across your internal network and compromising your organization's crown jewels.

Wireless Penetration Testing
Determine if an adversary can exploit your internal systems through your wireless services and validate the configuration and encryption of your access points to identify vulnerabilities and provide remediation advice.

Container Penetration Testing
Determine externally whether the clusters' internet-facing assets are misconfigured or vulnerable to attacks and identify how far an attacker can go if a container is compromised or if the clusters' API services and CI/CD tools are misconfigured.

Purple Team Exercises

Attack, defend, and remediate in this exercise where our Red Team plays the role of the attacker, and your Blue Team is the defender. The Liquid C2 Red Team will test the effectiveness of your security program and the ability of your internal security team (the Blue Team) to detect and respond to these simulated attacks.

Infrastructure Assessment

Identify vulnerabilities in the configuration and setup of your network and IT infrastructure components. Whether you're looking to review your on-prem, cloud, virtual, or hybrid infrastructure, or evaluate your network architecture, our assessments provide you with a better understanding of the security of your infrastructure environment, as well as actionable recommendations to mitigate any identified risks.

On-Prem Infrastructure
Maintain your on-prem infrastructure security by identifying vulnerabilities, understanding the risk level involved, and pinpointing how best to fill security gaps.

Cloud Infrastructure
Assess and analyze your organization's cloud infrastructure whether it is based in AWS, Azure, GCP, or exists across multiple cloud providers, through our vendor-agnostic assessment that offers you better visibility over potential threats affecting your cloud infrastructure.

Virtual Infrastructure
Analyse the configuration of your virtual infrastructure components against renowned frameworks and industry standards to get a comprehensive view of your security and available mitigation options to improve protection and reduce risk.

Vulnerability Assessment
Define, identify, and classify your systems' weaknesses and possible exploits covering the latest attack vectors and zero-day vulnerabilities using automated tools to provide you with the necessary knowledge to react to threats in your environment.

Network Architecture Review
Expand or review your network design and relevant artifacts. Liquid C2 assesses the current setup of your architecture, the security controls in place, and the processes surrounding network usage, monitoring, and review to identify relevant threats and how to best address them.

Advisory & Consulting Services

Cyber Risk Assurance

Discover vulnerabilities in your systems and applications with a wide range of in-depth assessments of your IT environment to identify and fix vulnerabilities to enhance your organisation's overall security posture

Application Assessments

Identify, assess, and map out the application's attack surface to find the weak links and pain points in your security processes and build your security roadmap to prevent the exposure of security defects and vulnerabilities.

Secure Code Review
Get an in-depth review of all components of the application code for a comprehensive view of any architectural issues or logic errors, to eliminate vulnerabilities before application release.

Threat Modeling
Gain more insight into the threats affecting your applications and systems to determine previously unknown or overlooked risks. Our experts will coordinate with your team to develop a threat model framework assessing current security control practices and where security vulnerabilities have been introduced, and present recommendations to reduce potential risks and improve your application design.

Security Controls Assessment

Evaluate system components' configuration across your environment to identify misconfigured security controls and outline mitigation options to ensure your system components are not left vulnerable.