

krome

PENETRATION TESTING

Find the weaknesses before the attackers do

Do you know what your external attack surface really looks like?

Have you tried seeing your organisations through the eyes of a hacker?

Real world attacks. Real insights. Stronger security.

We simulate real-world cyber attacks to identify and exploit vulnerabilities before threat actors do.
Our penetration testing services give you a clear view of your security posture, practical recommendations and the confidence and insights to move forward.

External infrastructure testing

We test public IP addresses, internet facing services, VPNs, remote-access platforms, cloud-hosted infrastructure, and exposed management interfaces. We determine what attacker can interact with and how, whether those weaknesses are exploitable, and (where authorised) how far they could move from an external starting point.

Internal network and identity testing

Krome simulates an attacker who has already gained a foothold to see how far they could move through your environment.

This includes testing for privilege escalation, compromised identities, access to critical systems, lateral movement, and the ability to reach sensitive data.

Web application and API testing

We test web applications, portals, APIs, and authenticated user journeys for flaws in authentication, authorisation, session handling, data exposure, input validation, and business logic. Where applicable, we analyse how weaknesses across different services could be combined to create a more serious route to compromise.

Wireless & physical attack simulation

Krome can conduct controlled wireless and physical attacks. This includes testing wireless-network security with specialised devices, testing building entry controls, visitor procedures, exposed network ports, and device security. All tests are conducted according to your specific objectives and agreed safety rules by testers who have extensive experience.

More than just a test: A stronger, safer business

Reduce Risk

Identify and fix vulnerabilities before they can be exploited

Prove Resilience

Demonstrate strong security to customers, partners and regulators

Meet Compliance

Support regulatory requirements such as ISO 27001, PCI DSS, NIS 2

Gain Expert Insights

Work with experienced ethical hackers who think like real attackers

Start with a free external exposure review.

Krome offers a free external exposure review as a first step in understanding what your organisation exposes to the internet. This includes a review and high-level assessment of public-facing IP addresses and services. As captured by commercial crawlers and spiders. We identify what is easily and readily visible to the world and determine if it creates an obvious path into your network.

How our penetration testing works

PLAN
Agree scope, objectives, rules of engagement and testing approach

TEST
Simulate real-world attacks using expert attacks

ANALYSE
Identify and validate vulnerabilities and access potential impact

REPORT
Receive clear findings with practical recommendations

REMEDIATE
We can support you with prioritising and fixing any issues

Controlled, professional pen testing.

Before your pen test assessment, we agree on targets, depth operating windows, exclusions, escalation contacts, and stop conditions.

All testing is conducted responsibly, within clear boundaries to protect your systems, user and data.

Test as deeply as the risk requires.

Every assessment is shaped by scope, time and access.

A focused external exposure review gives a clear starting point, but doesn't provide the same assurance as testing a full attack path. When risks or business needs justify it, we can expand the engagement under an agreed statement of work and a strict set of rules of engagement.

This allows us to move from identifying exposed services to validating weaknesses and seeing what an attacker could achieve after gaining a foothold.

Clear findings and practical next steps.

Following the assessment, you will receive a report on what was found, how it could be exploited, the potential business impact and exactly what next steps to take, in order of priority.

A Krome Senior Cyber Analyst and/or our CISO will review the findings to provide practical remediation guidance.

We filter out the noise so your technical team can focus their time and resources on the actions that make the most significant difference. Should you need our assistance, we can also help you implement the required remediations.



> "Krome gave us an independent view of our security posture and more importantly, a clear route forward.
>
> The combination of technical depth, practical advice and open discussion throughout the whole engagement gave us confidence in both the findings and the actions we needed to take."
>
> IT Manager | Transportation Logistics

Talk to Krome about seeing your organisation through the eyes of an attacker.

+44 (0)1932 232345 | sales@krome.co.uk

Krome Technologies Ltd
Head Office: Krome House Pound Road Chertsey Surrey KT16 8ER Tel:01932 232345
Manchester Office: Quays Reach Salford Manchester M50 2ZY Tel: 0161 868 1360
www.krome.co.uk | sales@krome.co.uk