KROLL™

Red Teaming

Simulate real-world cyberattacks to uncover hidden weaknesses and strengthen your organization's resilience.

KROLL

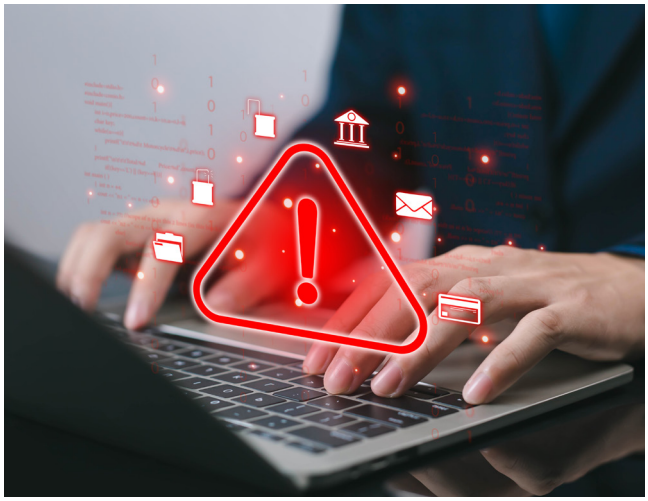
Are you confident your organization can withstand a real-world attack?

The modern threat landscape is dominated by highly organized, well-resourced attackers. Their campaigns are designed to disrupt operations, compromise sensitive data, and erode trust, often before security teams realize an incident is underway.

Attackers exploit:

- Identity weaknesses to hijack privileged accounts and impersonate trusted users
- Cloud misconfigurations to access sensitive data stored in hybrid environments
- Unmonitored endpoints and shadow IT to establish stealthy footholds
- Lateral movement tactics to silently escalate privileges and target high-value systems

These threats are especially dangerous as they may be completely undetected. In many cases, attackers can dwell inside networks for weeks, sometimes months, before security teams notice suspicious activity.



Simulate Real World Threats, Strengthen Organizational Resilience

Kroll's Red Teaming Assessment takes an enterprise-wide, business-aligned approach to identify and exploit potential weaknesses in your critical systems, applications, and processes. By simulating adversary TTPs, we provide actionable insights into your organization's true readiness, ensuring you're prepared for modern, complex attacks.

Uncover Hidden Weaknesses

Simulate real-world attack scenarios to identify vulnerabilities across your environment, including gaps in security controls, detection capabilities, and response processes, before adversaries exploit them.

Intelligence-Led Attack Scenarios

Leverage Kroll's global threat intelligence to emulate the latest adversary tactics, techniques, and procedures (TTPs), ensuring each scenario is realistic, relevant, and tailored to your industry.

Validate Security Controls

Benchmark your organization's overall readiness by evaluating how people, processes, and technologies perform against sophisticated threats, providing a clear view of true security maturity.

Strengthen Detection and Response

Measure your blue team's effectiveness during simulated attacks and gain insights to enhance threat detection, streamline escalation workflows, and optimize incident response capabilities.

KROLL

Kroll's Intelligence-Led Approach To Red Teaming

Kroll's Red Teaming exercise is designed to go beyond traditional penetration testing by simulating realistic, high-impact attack scenarios tailored to your organization. **Unlike standard tests, our approach integrates business objectives, operational realities, and Kroll's proprietary threat intelligence to deliver actionable insights that improve resilience across your entire environment.**

We follow a proven, four-phase methodology that blends advanced adversary simulation with collaborative engagement, ensuring scenarios are controlled, safe, and outcome-driven:

SCOPING

- Agree on goals, scenarios and assisted footholds.
- Define timeline
- Set up communication channels
- Validate project plan

PREPARATION

- Perform active and passive reconnaissance
- Set up attack infrastructure
- Prepare payloads

EXECUTION

- Infiltrate network
- Identify path(s) to goals
- Execute and log relevant TTPS
- Observe defence mechanisms and blue team reactions

ANALYSIS

- Evaluate observed defence mechanisms and reactions
- Identify gaps and possible root causes
- Provide report
- Support blue team in remediating gaps
- Retest findings (if required)

Each engagement follows a threat-driven, scenario-based framework that mirrors the tactics, techniques, and procedures (TTPs) used by real-world adversaries. Leveraging advanced capabilities such as payload engineering, EDR bypassing, lateral movement, and cloud exploitation, we deliver simulations that accurately reflect modern attacker behaviors.

Why Kroll as your Red Teaming partner?

Intelligence-Driven Engagements

Powered by Kroll's global threat intelligence and insights from thousands of incident response cases annually, ensuring scenarios mirror real-world adversary tactics.

Elite Global Expertise

Our Red Team consultants maintain dedicated R&D functions to build custom payloads, validate techniques against the latest EDR, and deploy flexible C2 infrastructure — ensuring engagements emulate today's most advanced adversaries.

Business-Aligned Testing

Each assessment is tailored to your environment, focusing on your most critical systems, data, and operational functions to deliver findings that are actionable and prioritized.

KROLL™

Case Study – Network Analytics for Financial Crime Risk Detection

The Challenge

The cryptocurrency sector has been heavily targeted by advanced threat actors, including the North Korea–linked Lazarus Group (KTA071), leading to **billions in losses globally.**

This institution sought to test its ability to detect and respond to sophisticated adversary tactics.

The Solution

Kroll's intelligence-led Red Team designed an engagement that emulated Lazarus TTPs through a series of targeted initial access campaigns using custom-developed malware, including:

- Malicious GitHub repositories
- Weaponized SumatraPDF payload
- Trojanized VPN client
- Malicious NPM package

The team also deployed a custom browser injection tool and delivered tailored threat intelligence and detection guidance.

Key Results/Outcomes

- Expanded detection coverage across high-risk attack vectors
- Strengthened incident response capabilities
- Validation of existing defensive controls
- Improved overall security maturity and readiness

Trusted Leader in Cyber and Data Resilience

World's largest IR provider with **thousands of** IR cases a year

Preferred vendor for **85+** insurance carriers

Experience from **Govt. & Law Enforcement, Industry & Consulting** backgrounds

EUROPOL

700+ experts across 19 countries

100+ certifications

CISM CREST ISO 27001

Expertise in **AI, Crypto, Cloud, Data Analytics, Web 3.0 security and data** risk

700k+ actively monitored endpoints

Rated as **industry leaders**

FORRESTER Gartner

computing Security Excellence Awards 2023 WINNER

SC 2022 awards WINNER

Computing Security Awards 2021 WINNER

WANT TO LEARN MORE ABOUT HOW IT WORKS OR PRICING? CONTACT THE FOLLOWING:

Benjamin Mahar
Associate Managing Director
+1 416 643 3531
benjamin.mahar@kroll.com

Blair Mcintyre
Senior Associate
+1 647 801 8102
blair.mcintyre@kroll.com

Additional hotlines at:
kroll.com/hotlines

Or via email:
CyberResponse@kroll.com