Cyber **security**

THREAT INTELLIGENCE & PENETRATION TESTING SERVICES

CBEST, GBEST, GCASE, STAR, STAR-FS, TIBER





THREAT READY

LRQA

Your Risk Management Advantage

REGULATORY SERVICES

LRQA provides independent Threat Intelligence and Penetration Testing services for UK public sector organisations, government departments, regulated financial institutions, and critical infrastructure providers. Our expertise spans CBEST, GBEST, GCASE, STAR / STAR-FS, and TIBER frameworks, helping organisations assess cyber resilience, demonstrate regulatory compliance, identify gaps, strengthen controls, and reduce operational and cyber risk.



CBEST

LRQA is one of a few CBEST-approved providers accredited by CREST and the Bank of England for both Penetration Testing and Threat Intelligence. CBEST assessments use threat intelligence and Red Team exercises to evaluate financial institutions' cyber resilience.

GBEST

GBEST focuses on UK government departments and agencies, leveraging simulated real-world attacks and threat intelligence to test critical systems and strengthen security controls.

GCASE

The Government Cyber Attack Simulation Exercise is a rapid penetration testing service for UK government bodies designed to improve cyber resilience. GCASE provides a faster, less in-depth simulation than the complementary GBEST service and forms part of the Government's broader assurance program.

STAR

STAR (Simulated Targeted Attack and Response) enables critical infrastructure providers outside financial services to identify vulnerabilities and improve resilience through controlled, threat-led testing aligned with NCSC guidance.

STAR-FS

LRQA is CREST-accredited to deliver STAR-FS, which applies Red Teaming and threat intelligence to financial institutions similarly to CBEST but with lighter or optional regulator involvement.

TIBER

TIBER-EU (Threat Intelligence-Based Ethical Red Teaming) is the European Central Bank's framework. LRQA simulates advanced persistent threats using threat intelligence and Red Team techniques, helping banks and financial institutions test detection, response, and mitigation capabilities in a controlled, regulator-compliant environment.

THREAT INTELLIGENCE CAPABILITY

Our threat intelligence (TI) services are a core strength of our delivery capability. LRQA has built a dedicated TI practice with certified experts and methodologies aligned to regulatory expectations, ensuring we can provide the high-quality, targeted intelligence that underpins effective threat-led testing.

CERTIFIED EXPERTISE

Our team includes CREST Certified Threat Intelligence Managers (CCTIM), as well as specialists with deep experience in cyber threat research, adversary tracking, and financial services sector intelligence. The presence of CCTIM-certified practitioners demonstrates our ability to lead and quality-assure TI engagements, ensuring adherence to CREST standards. This certification also evidences our ability to manage the entire TI process - from collection and analysis to scenario development and stakeholder reporting.



STRUCTURED INTELLIGENCE METHODOLOGY

Our TI approach is built on internationally recognised frameworks, including the Diamond Model of Intrusion Analysis and the MITRE ATT&CK framework. By applying these, we ensure intelligence outputs are structured, repeatable, and directly translatable into attack scenarios for Red Team exercises. This structured methodology also ensures traceability from intelligence collection through to Red Team execution, a critical requirement for regulatory engagements.

INTEGRATION WITH RED TEAM ACTIVITIES

We have extensive experience in collaborating with Red Teams, whether this is our own internal Red Team or alternative providers, to translate intelligence findings into realistic, regulator-aligned attack scenarios. Our TI reports explicitly map adversary TTPs to client environments, enabling the Red Team to replicate authentic threat actor behaviour in a controlled manner. This ensures the subsequent Penetration Testing phase is realistic, relevant, and regulator compliant.

PENETRATION TESTING / RED TEAM CAPABILITY

Our Red Team capability is a central pillar of LRQA's service portfolio. It is built on the expertise of our accredited consultants, the proprietary tooling we have developed to support safe and repeatable testing, and a methodology that ensures regulator-ready outcomes. Together, these elements enable us to deliver simulations that accurately reflect the behaviour of sophisticated threat actors while maintaining strict governance and operational control.

ACCREDITED EXPERTISE

Our Red Team practitioners hold CREST Certified Red Team Specialist (CCRTS) and CREST Certified Red Team Manager (CCRTM) qualifications. These certifications provide formal recognition of both technical competence and programme governance, demonstrating our ability to deliver complex simulated attacks to regulatory standards. The dual accreditation ensures that our team can not only execute advanced attack scenarios but also design and manage engagements in line with regulatory and client requirements.



STRUCTURED METHODOLOGY

Our methodology follows recognised frameworks such as MITRE ATT&CK and CREST best practice, but it is tailored to the specific demands of each framework. Scenarios are derived directly from threat intelligence outputs and translated into controlled campaigns that may include social engineering, targeted exploitation, lateral movement, and privilege escalation. Every stage is carefully documented and evidenced, creating a transparent chain of activity that links intelligence to execution and outcomes. This structured approach ensures realism while meeting regulator expectations for safety and accountability.

PENETRATION TESTING / RED TEAM CAPABILITY

PROPRIETARY TOOLING AND ORCHESTRATION

LRQA has developed a suite of proprietary, state-of-the-art tools purpose-built to emulate the tactics, techniques and procedures of sophisticated threat actors targeting high-value sectors. This bespoke capability goes well beyond commodity tooling and enables simulations that are tightly tailored to the exact threat profile of each engagement; our custom implants and droppers have been engineered to operate on Windows, macOS and Linux and are designed to mirror the stealth, functionality and persistence of real-world malware so that exercises are highly realistic and intelligence-representative.

POSHC2

C2 framework for post-exploitation and lateral movement emulation; Windows/ macOS/Linux; enhanced droppers, proxy-aware communications and EDR/AV resilience, with evidence logging and blast-radius controls.

RAIJIN

Next-generation modular native Windows implant/C2 for rapid prototyping and in-engagement customisation; emulates advanced actor TTPs with controlled feature toggles and full audit trails.

RACCOON

Discreet desktop collection module for fine-grained capture of high-value artefacts (including minimised window images); low-impact collection governed by strict data-handling RoE.

ALADDIN

Initial access/application-control bypass technique for testing WDAC/AppLocker resilience on Windows; used only under explicit RoE and legal approval to surface hardening gaps safely.

SHARPCONFLUX

Targeted Confluence discovery module for cloud and on-prem instances; supports multiple auth methods for low-noise identification of credentials and sensitive content, operated under controlled escalation and retention policies.

TOOLBOX & DEVOPS PIPELINES

Automated payload/module build and obfuscation pipeline integrated with our C2s; produces unique, project-specific artefacts with centralized OPSEC controls and artefact tracking.

INTEGRATION WITH THREAT INTELLIGENCE

Our Red Team works in close collaboration with LRQA's CCTIM-certified Threat Intelligence Analysts and has a wealth of experience in working alongside alternative TI providers. This integration ensures that scenarios reflect authentic adversary behaviour relevant to the client's operating environment. The result is a testing exercise that provides meaningful insights into how an organisation would withstand actual threat actor activity, rather than a generic penetration test. The strong link between intelligence and execution is a cornerstone of our delivery model.

REPORTING AND OUTCOMES

The outputs of our Red Team engagements are designed to satisfy both regulator submission requirements and client decision-making needs. We provide detailed technical reporting with evidence trails, attack timelines, and indicators of compromise, as well as executive-level summaries that translate findings into business risk.



ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit **LRQA.com** for more information or email **enquiries.uk@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management Advantage