PENETRATION TESTING SERVICES BY LRQA

Penetration Testing Services

Contents

Our accreditations

As a leading penetration testing company, LRQA holds the most coveted accreditations across the world.

- We are the only organisation in the world with a full suite of CREST accreditations;
- We are a proud member of the UK Government's NCSC CHECK scheme. Our team of testers includes CHECK team leaders within infrastructure and web applications, as well as CHECK team members;
- We are an ISO 9001, ISO 14001, and ISO 27001 certified organisation, and as such, we guarantee to provide our clients with top-quality services from within a rigorously controlled environment;
- LRQA are certified by a variety of governing bodies for the work that we regularly perform within a range of highly regulated industries, including the financial and payment card sectors;
- We are an accredited supplier of CREST and an approved provider of STAR testing services. We also deliver services for both TIBER and iCAST in heavily regulated financial services environments;
- Our security consultants hold a variety of different certifications across a multitude of different areas of information security. Consultants possess penetration testing-specific certifications such as the Offensive Security Certified Professional (OSCP) and Offensive Security Certified Expert (OSCE) certifications. In addition, all of our penetration testers have been fully background-checked;
- The LRQA security testing team includes not only those accredited with the OSCP and OSCE certifications, but also CREST Certified Infrastructure Testers (CCT Inf), CREST Certified Web Application Testers (CCT App), and CREST Registered Testers (CRT);
- In addition, our team is comprised of industry-recognized consultants and published authors who have been recognised by the media and the cybersecurity community.

The types of penetration testing we offer

Active Directory Testing

Most enterprise networks are managed by Windows Active Directory and store sensitive data such as PII, PCI DSS and R&D. An attack that successfully compromised Active Directory would likely have significant ramifications for any organisation. LRQA's team of CREST-certified internal penetration testers are able to review the configuration of Active Directory in order to identify any insecure practices or attack vectors that could be exploited by a malicious agent.

ASV Services

As an Approved Scanning Vendor (ASV), LRQA conducts quarterly external and web application vulnerability scans in line with PCI DSS external scanning requirements. Experienced ASV professionals are able to walk you through the process and provide remediation guidance should a failed scan occur.

CBEST Testing

Created by the Bank of England and supported by CREST, CBEST assessments reflect some of the most sophisticated types of assessments that exist within the financial services sector today. LRQA is one of only a handful of service providers to be accredited by both CREST and the Bank of England as CREST Penetration Testing providers and CBEST Threat Intelligence providers. This unique capability allows us to provide our clients with end-to-end CBEST services.

Cloud Service Testing

Cloud Penetration Testing is an authorised simulated cyber attack against a system that is hosted on a Cloud provider, such as Amazon's AWS or Microsoft's Azure.

The main goal of a cloud penetration test is to assess the security posture of the environment, find common security misconfigurations and assess publicly accessible services that could prove to be an attractive target for bad actors.

Code Review Services

Traditional penetration tests often focus on addressing threat actors with limited or no prior information about the target system. In some cases, this is appropriate, but for maximum levels of assurance, a code review is often a sensible approach. LRQA has a team of application security experts who are able to review source code to identify vulnerabilities and dangerous coding practices. This would not be possible with traditional dynamic testing.

Firewall Security Testing

As firewalls continue to advance in sophistication and functionality, a simple misconfiguration could render it incapable of meeting an organisations security requirements. LRQA's expert, highly experienced firewall testers will assess the security of firewalls deployed within your organisation from the perspective of a remote third-party threat actor.Comprehensive reviews of the rules implemented by the target firewalls will be conducted, as well as their overall configuration to identify any vulnerabilities and weaknesses.

Hybrid Testing

A hybrid environment is the term used when Microsoft Azure AD is incorporated into existing on-premises Active Directory. A compromise of on-premises Active Directory could lead to the compromise of Azure AD and vice-versa. LRQA consultants will look to assess the configuration of both the Azure AD and Active Directory looking for misconfigurations that could be exploited by an attacker. Particular focus is placed on attack paths that could lead to the compromise of Azure AD Connect, a high-value target with high privileges both on-premises and within the cloud.

Intelligence-Led Testing (STAR)

Simulated Target Attack Response (STAR) is an approach to security assessment that was created by CREST. LRQA is a CREST STAR-approved Threat Intelligence (TI) and Testing Provider, delivering in-depth assessments for clients across the globe. STAR engagements commence with a comprehensive STAR Threat Intelligence assessment of the likely threats that are relevant to an organisation.

The types of penetration testing we offer

IoT Testing

LRQA routinely works closely with the creators of smart devices in order to provide assurance about the security posture of their products. Internet of Things (IoT) testing services provide a valuable way to assess the security levels associated with a given connected device or any potential risk a third-party device could bring if utilised within your environment. LRQA has extensive experience in IoT testing and assuring smart devices for domestic usage, industrial usage, smart metering, connections for utilities, and smart devices aimed at the automotive and transport sectors.

Managed Vulnerability Scanning

LRQA provides a comprehensive Managed Vulnerability Scanning (MVS) solution, using leading technology deployed by security professionals to scan and report your assets for known vulnerabilities. Using our team of security professionals, who understand the current threat landscape, offensive techniques of attackers, and how to achieve a strong security posture, LRQA's MVS service will give you confidence and power to stay on top of emerging vulnerabilities and the changing vulnerability landscape.

Mobile Testing

Mobile application testing reveals vulnerabilities in the cybersecurity posture of a mobile application. Most commonly, it is the safety and security of iOS and Android applications that requires assessment. LRQA is a top provider of mobile application penetration tests, accredited by CREST against their OWASP Verification Standard (OVS).

This is a framework which provides a scalable and consistent approach to web and mobile application security standards.

Purple Teaming

Purple teaming is a cybersecurity testing exercise that incorporates components of both red teaming and blue teaming to provide insight and effectiveness with regard to attack detection and response. Experts from the LRQA red team will work alongside the blue team of your organisation to coordinate and carry out attacks, identify which attacks succeeded, which attacks failed, and determine the reason for each outcome. Purple teaming provides much greater visibility to your organisation regarding weaknesses and how to effectively resolve them.

Red Teaming

Red teaming provides your organisation with real-world scenarios to help your organisation identify and understand where your gaps are and advise how you can patch them up. LRQA provides advanced network protection through state-of-the-art red team testing techniques.

SCADA & ICS Testing

Industrial Control Systems (ICS) can be tested with many of the same techniques as other types of systems, but there are some important differences. SCADA/ICS tests require more planning and a more tailored approach than other types of security testing. LRQA performs testing of SCADA/ICS systems across multiple industry sectors including Utilities (electricity, gas, and water), Manufacturing, and Waste Disposal against a range of industry standards.

Social Engineering

The objective of a social engineering attack typically includes manipulating people into divulging confidential information or performing an activity that benefits the attacker, preferably without those people realising it. At LRQA, we have a dedicated team of social engineers who always practice and constantly refine their craft. LRQA can assess your physical security, travelling to a specified location and attempting to infiltrate the building to achieve pre determined objectives such as network access. We can also perform remote social engineering, such as phishing, to validates the effectiveness of user security awareness training, and spam and malware filters.

Web Application Testing

Due to their complexity and ubiquity, web applications represent a unique challenge to the security posture of any organisation. LRQA has a large team of CREST-certified penetration testers who specialise in web application penetration testing. The LRQA penetration testing team is diverse and contains a wealth of knowledge and experience in both security and software development.

Wireless Infrastructure Testing

Wireless assessments can be delivered through attacks that target the existing wireless infrastructure that runs and operates within your organisation. An engagement will look to target any client interacting with the wireless infrastructure and ensure that correct network segmentation is in place. LRQA delivers wireless device testing as a common component of many internal on-site penetration tests.

Penetration testing strategies

Let LRQA guide you through the differences between black, grey, and white box penetration testing services.

Black box testing

In a black box test, the client does not provide LRQA with information about their infrastructure other than a URL or IP, or in some cases, just the company name;

LRQA is tasked with assessing the environment as if they were an external attacker with no information about the infrastructure or application logic that they are testing. Black box penetration tests provide a simulation of how an attacker without any information, such as an internet hacker or a nation-state-sponsored attacker, could exploit the environment.

Grey box testing

A grey box test is a blend of black box and white box testing techniques;

In grey box testing, clients provide LRQA with snippets of information to help with the testing procedures. This results in added breadth and depth, along with wider testing coverage than black box testing. Grey box penetration tests provide an ideal approach for clients who want to have a cost-effective assessment of their security posture.

White box testing

White box penetration testing is almost the opposite of blind/black box penetration testing. Penetration testers are given access to the source code and relevant design documentation which applies to the application being tested. Penetration testers are able to perform static testing using source code analyzers to identify vulnerabilities. They are then able to then compile the application and run it within a sandboxed environment, making use of dynamic testing using debuggers and common application testing tools. As a result, white box testing offers one of the highest levels of technical assurance.

Our approach, reports, and deliverables

Our approach to penetration testing

LRQA has a robust testing methodology that extends across infrastructure and application testing engagements. Although every penetration test is tailored to our client's individual needs, we follow the same proven methodology so as to maintain a consistent set of results.

- Phase 1: Scoping
- Phase 2: Reconnaissance and Enumeration
- Phase 3: Mapping and Service Identification
- Phase 4: Vulnerability Analysis
- Phase 5: Service Exploitation
- Phase 6: Pivoting and general post-exploitation
- Phase 7: Reporting and Debrief

Testing report and documentation

You will receive a high-level management report and an in-depth technical review document for each engagement. Where appropriate, LRQA consultants will include an Attack Indicator Report (AIR) which includes recorded time-stamped attacks that serve as crucial indicators of attack. They serve as red flags that signal possible malicious activities, allowing for proactive threat hunting and early response that will allow you to compare the attacks performed against your logging and monitoring solutions.

- These documents will highlight security vulnerabilities and identify areas for exploitation;
- In addition, they will provide guidance on remediation, with a focus on preventative countermeasures.

Test debrief

LRQA ensures that all tests have a full debrief at the end of the engagement.

If required, LRQA can deliver this debrief in a face-to-face manner. During this process, we will provide a presentation of critical and high-level vulnerabilities, along with guidance on remediation and countermeasures.

When a face-to-face debrief is not required, LRQA conducts debriefs via a video conference. Through this approach, we are still able to have a comprehensive presentation of vulnerabilities and areas identified as being high risk.

About LRQA:

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

Get in touch

Visit **www.lrqa.com** for more information or email **cybersolutions@lrqa.com**

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