Active directory

The attacker’s perspective

Contents

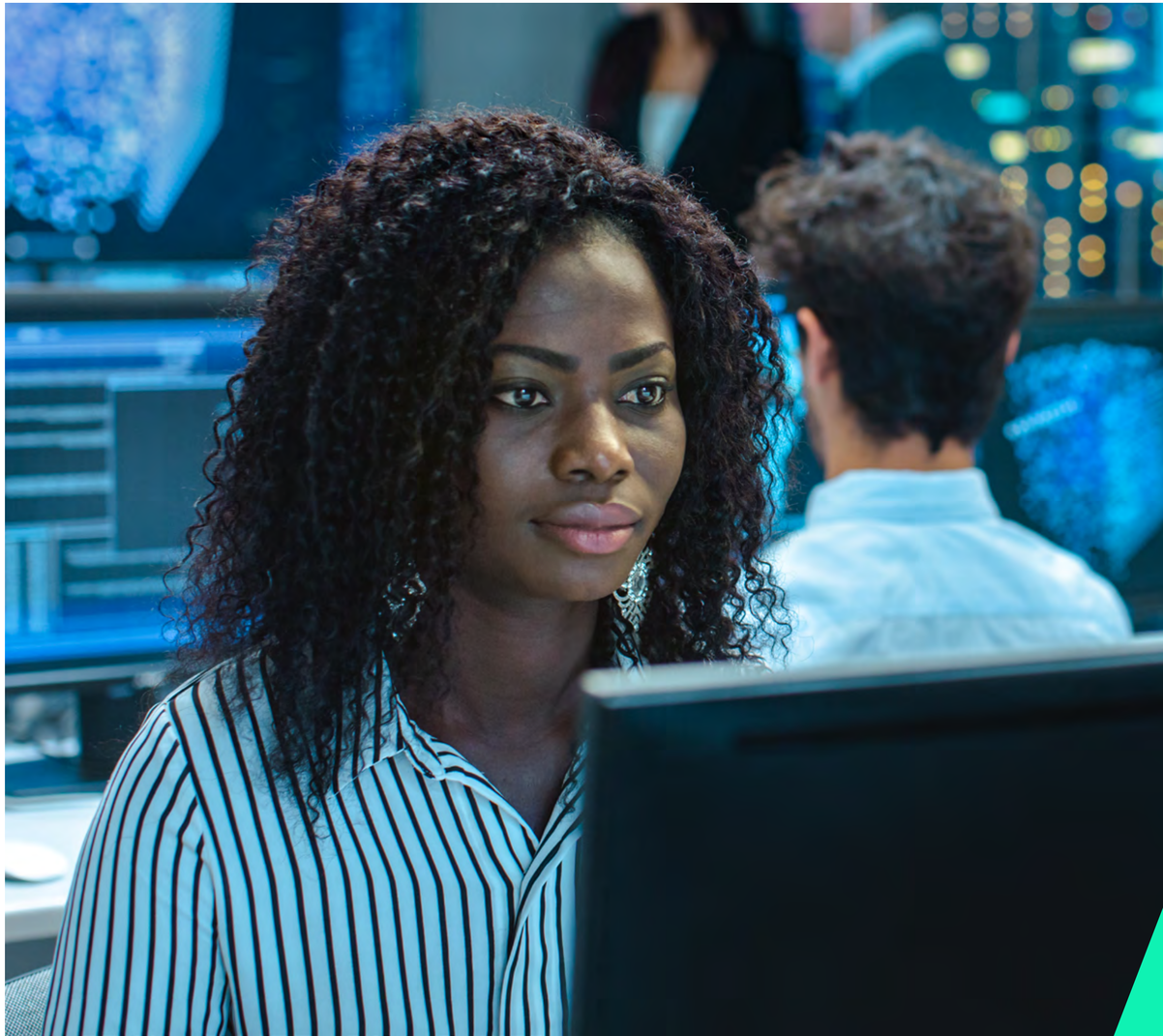
Introduction

Active directory (AD) is the centre of many organisations' identity and access management (IAM). As such, it plays a key part in safeguarding business interests.

Given AD's innate ties to IAM, it commonly forms part of any cyber incident. By being proactive in defence, organisations can slow attackers down, reduce lateral movement opportunities, increase the chance of detection, and reduce chances for credential theft.

This review is not focused on active directory best practice, it is focused on hardening your primary IAM provider against motivated and skilled attackers.

This testing focuses exclusively on breaking attack paths, hardening the environment through built-in Windows features, and increasing the detective opportunities to catch malicious threat actors.



Why conduct an active directory security review?

Active directory is an extremely large and nuanced product, with a significant attack surface. Due to its extensive use, it is under constant scrutiny by threat actors and vulnerability researchers looking to gain an advantage. Even today many AD environments suffer from domain user to domain admin privilege escalation opportunities that circumvent tiered accounts and privileged access management products.

The increased focus in security community research and the inclusion of AD attacks in threat actor playbooks show that it is critical to conduct hardening of insecure defaults and maintain point-in-time visibility of the attack surface. By partnering with LRQA to support this challenge, you gain experienced red team knowledge of attacker tactics, techniques, and procedures (TTPs) and what works in modern enterprise environments.

Security reviews can complement and reinforce existing assurance activities such as penetration testing. However, whereas broad-scoped penetration testing aims to locate a breadth of vulnerabilities across an entire infrastructure, a focused AD security review provides nuanced, pragmatic guidance that will make a meaningful difference in stopping attackers who have gained a foothold in the environment.

Why Conduct an Active Directory Security Review?

Methodology

Active directory security reviews are only conducted by our red team consultants, who have years of experience operating covertly in large intercontinental networks.

The assessment begins with speaking to administrative staff and aiming to understand the network, critical servers/assets, and any areas of particular concern. This then informs later testing which centres around Kerberos misconfigurations, unsafe access control lists, insecure defaults, attack path mapping, and understanding where key service accounts are logging on.

This data collection uses a variety of open-source and privately-written tools that can be run from a Windows host in the environment, collecting a large amount of data for later parsing by the consultants. Using this data, LRQA's red team bring their years of real-world experience to map out likely routes to compromise, before making sensible, realistic, and pragmatic recommendations to break those attack paths, while providing the context as to why these changes matter.

Some recommendations will reduce the overall attack surface, whilst other recommendations will be centred around hardening existing AD defaults to prevent the weaponisation of new research and attack methods. Throughout the process, LRQA works with your IT staff to understand critical systems, map out overly permissive groups and users, and seek to implement good practice in as many areas as possible.

At the end of the process, you will have a consolidated list of improvements that will make meaningful changes to your security posture. As well as qualitative and quantitative data to support those change programmes. Depending on your organisation's maturity, once the first assessment has been completed, a second shorter period of work can be undertaken. This will verify and assure those improvements and suggest more advanced hardening steps in line with your new posture. This allows LRQA to continually increase the maturity of the AD environment while working at your pace, focusing on high-risk items first.

Time frame

The scope of this bespoke package of work is commonly found to be two working weeks for a large enterprise environment. This includes testing, data gathering, and a detailed discussion with your technical teams.

The engagement will then move into the reporting phase to produce the technical deliverables. Certain nuances around heavily segregated or very large environments may increase this time, but LRQA can discuss and assist through the scoping phase.

Why conduct an active directory security review?

Deliverable

LRQA will produce a full technical report that details each area for improvement and the underlying supporting information.

The report will focus on protective and detective controls, with an alignment where appropriate to MITRE TTPs and the NIST cybersecurity famework.

A technical summary for IT leadership will also detail any thematic observation, each technical finding comes with detailed recommendations to increase the protective and detective posture of the network. Where complex topics and concepts are conveyed, LRQA provides additional reading and supporting scripts and tools to understand the scope of the issue within the network, as well as proof of concept snippets (if required).

Pre-requisites

Normal user

LRQA can conduct this review with conventional domain privileges, with no special access or privileges required. The consultants will require access to a domain-joined Windows host with internet access and an antivirus exclusion folder for scripts and tools to be kept in.

Elevated user

For more detailed collection and analysis around session collection and logged-on users, LRQA can conduct this service from an elevated context. This can take the form of domain admin, server admin, workstation admin.

The advantage of the elevated collection method is that LRQA can collect session information from the workstations and servers, allowing an understanding of where privileged accounts are used across the environment. This can assist with developing restrictions and detections around privileged accounts, and locating machines where privileged accounts are potentially being used in unauthorised hosts.

Additional testing

This package of work can be undertaken on a standalone basis, or as part of a wider enterprise infrastructure security assessment.

This can be complemented with password-strength audits (as well as checking for password reuse between networks) and can be complemented with an investigation into the configuration of the System Centre Configuration Manager (SCCM), and Active Directory Certificate Services (ADCS).

Please contact us for details on assurance around other business-critical systems.

Why LRQA?

World leading red team

LRQA has been conducting on-premise penetration testing for decades and were part of the original group of companies selected by the Bank of England to conduct financial services Red Teaming under the CBEST scheme.

We are trusted to conduct penetration testing against government systems and critical national infrastructure. LRQA are also counted upon to conduct months-long simulated attacks against central banks around the world.

Research-led

We ensure we stay at the forefront of enterprise security through dedicated research time and exposure to networks across the globe.

Research and innovation are core to that process. Vulnerability research and offensive security software development is part of who we are. We share our work through conferences, our website, and beyond.

Trust

Our clients trust us to deliver accurate, realistic, and workable solutions to their security challenges, as well as provide top-tier training workshops to other red teamers, technical staff, and executive leadership.

All our consultants understand the challenges that enterprise-scale can bring, and assist with developing a plan of incremental improvements to continually mature your cybersecurity posture.

Service

- Access to a highly-skilled team of security-cleared cybersecurity professionals.
- The same risk management controls we have developed over 20 years of offensive security engagements.
- Dedicated consultants throughout the engagement – they will be working exclusively for you throughout the process.
- Access to our advisory consulting team, able to brief at all levels of your organisation, and assist with prioritisation of fixes and retesting.

Unrivalled quality deliverables

- We provide an impact statement, a walkthrough of exploitation, screenshots, reproduction instructions, and remediation guidance for each finding.
- Links to best practices, remediation guidelines, and underlying attack theory is provided for all findings, allowing your IT staff to upskill at the same time.
- Each finding is given a severity rating – calculated through ease of exploitation, the impact of exploitation, and the impact it would have on your organisation. Each finding and recommended remediation is tailored to your environment, with no unrealistic recommendations.

Frequently asked questions

How will we distinguish testing activity from real attacks?

Attribution is important. All our red team consultants will use dedicated testing accounts and hosts which will be provided by you, or dedicated LRQA virtual machines. By doing this, you can be confident that our testing activity is us and not a real threat actor.

We have production systems in scope. How do you manage the risk of service impact?

We follow a non-disruptive methodology. All testing is done by team members who are experienced in testing high-importance and production systems safely. While no testing activity is entirely risk-free, we are very experienced at avoiding disruption and operate using an extensive risk management strategy.

Most of the analysis is conducted offline from your environment, so outside of the initial data collection period, there should be no change to the normal network traffic. The data collection approach is light touch and non-invasive.

What if I have follow-up questions about a finding or misconfiguration?

Each vulnerability that we discover is written up clearly and concisely. We strive to demonstrate impact, ensure reproducibility, and provide detailed remediation guidance. If you need to discuss a finding, you can do that throughout the engagement, or during remediation.

LRQA endeavours to leave you prepared with all the information and understanding that you need.

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