BLACK CELL
Protecting critical infrastructures

WHITEPAPER

ACTIVE DIRECTORY SECURITY IN PRACTICE

Why Evidence-Based Configuration Audits Matter for Resilient Enterprise Environments

Created by

Donát Kovács | Offensive Security

June 2026

TABLE OF CONTENTS

01

ABOUT BLACK CELL

Black Cell is a European cybersecurity company focused on protecting critical infrastructures and the organizations that support them. Our business units cover SOC, Integration, Offensive Security, Cloud Security, Compliance, and ESM (Enterprise Security Monitoring). We take a customer first approach that starts with listening, then shaping solutions to fit the way our clients operate.

Our teams are adaptable and draw on deep knowledge across industries and technologies, from IT and Cloud to ICS/OT. We engage for the long term, providing continual support, service improvement, and measurable outcomes over the lifecycle of the relationship. Clients rely on us to connect regulatory requirements with technology choices and to guide organizational transformation that sticks.

We combine architecture, implementation, and managed operations to close gaps quickly and build sustainable capability. Local presence in Central Europe matters to us, with teams in Budapest and Frankfurt am Main that understand the regional context. This proximity helps us respond faster, coordinate with partners, and keep stakeholders aligned. Above all, we aim to be a trusted partner who strengthens resilience today and prepares you for what comes next.

DISCLAIMER

The information provided in this document is for general guidance only and is used at your own risk. No contractual or advisory relationship is created between Black Cell and any person accessing or using this document or any part of it. Black Cell accepts no liability for any actions, decisions, or consequences arising from the use of this material.

References to third-party sources are included where appropriate. Black Cell is not responsible for the content, accuracy, or availability of external sources, including websites mentioned in this publication.

CONTACT

Donát Kovács
Offensive Security Director
donat.kovacs@blackcell.io

COPYRIGHT NOTICE

02

OVERVIEW

2.1. EXECUTIVE OVERVIEW

Active Directory remains one of the most critical trust anchors in enterprise environments. Even organizations with mature endpoint, identity, and cloud security programs often still carry legacy Active Directory configurations, privilege design issues, and hardening gaps that materially increase the risk of credential theft, privilege escalation, and unauthorized access.

The central challenge is not simply finding misconfigurations. It is determining which findings represent real, exploitable, operationally relevant risk and which are merely theoretical or low-priority deviations. Many organizations therefore end up with either noisy, automated reports full of unactionable findings or with high-level recommendations that are too generic to support safe remediation.

This whitepaper argues that effective Active Directory security assessments should be based on four principles:

1. evidence-based review
2. manual validation
3. exploitability-driven prioritization, and
4. remediation guidance that can be operationalized without disrupting core services.

evidence-based review

manual validation

exploitability-driven prioritization

remediation guidance

The same approach also creates value for defenders by linking findings to adversary behaviors and supporting detection engineering.

03

ACTIVE DIRECTORY RISK

3.1. WHY ACTIVE DIRECTORY STILL MATTERS

Despite the industry shift toward cloud-first security architectures and modern identity platforms, Active Directory still underpins authentication, authorization, delegation, and privileged access in many enterprise environments. As a result, weaknesses in Active Directory are rarely isolated weaknesses. They frequently translate into broader systemic trust issues across servers, workstations, service accounts, PKI components, and integrated Microsoft infrastructure.

Active Directory risk persists not because organizations ignore it, but because it is deeply embedded in the system. Domain Controllers, Group Policy, legacy authentication settings, administrative group design, certificate services, and operational exceptions often accumulate over years. These design choices may be individually understandable, yet collectively they create exploitable conditions that are difficult to see without a structured review.

3.2. THE CORE PROBLEM: TOO MUCH DATA, TOO LITTLE PRIORITIZATION

Modern security teams can collect significant amounts of directory and configuration data. The most complex part of the problem is converting that vast amount of data into practical risk-driven decisions. In Active Directory, the key question is rarely whether a deviation exists; the real question is whether the deviation creates a realistic path to privilege misuse, lateral movement, persistence, credential exposure, or unauthorized administrative control.

This distinction is critical. Long lists of automated findings can overwhelm infrastructure and security teams, while under-explained results would slow down remediation because teams cannot safely evaluate the impact of the proposed change. A high-value assessment must therefore do more than enumerate settings. It must validate findings, explain their security relevance, and help teams act on them in a controlled way.

04

ASSESSMENT PRINCIPLES

4.1. WHAT A MODERN AD SECURITY REVIEW SHOULD EXAMINE

A modern Active Directory review should focus on the trust boundaries and configuration areas that most directly influence exploitability, resilience, and recovery confidence.

- Privileged groups, delegated administration, and administrative tiering design.
- Group Policy hardening, inheritance issues, and control consistency across the environment.
- Legacy authentication settings, compatibility-driven exceptions, and weak operational defaults.
- Active Directory Certificate Services (AD CS), including Certification Authority and Certificate Template configuration.
- AD-integrated Microsoft infrastructure components that can introduce additional trust relationships or exploitable paths.

The goal is not to review every object with equal weight. The goal is to identify the settings and relationships that increase the likelihood of credential theft, privilege escalation, unauthorized access, or weakened trust boundaries.

4.2. THE VALUE OF EVIDENCE-BASED FINDINGS

The most useful security findings are those that can be independently verified and clearly understood by both security and infrastructure teams. Evidence-backed reporting improves trust in the results, reduces internal friction, and accelerates decision-making. When findings include reproducible proof (such as executed queries, command output, configuration extracts, or screenshots) teams can validate the issue and plan remediation with confidence.

This approach also reduces the hidden cost of false positives. In many organizations, the largest operational burden is not the existence of security issues, but the time spent disproving irrelevant ones. Assessments that emphasize manual validation and evidence-first reporting allow teams to focus scarce capacity on confirmed, meaningful risks.

4.3 PRIORITIZATION MUST REFLECT EXPLOITABILITY

Not every misconfiguration deserves the same urgency. Effective prioritization must consider not only severity, but also exploitability, preconditions, likely attacker value, and operational impact of remediation. A technically valid finding may not justify immediate change if exploitation requires unrealistic assumptions. By contrast, a seemingly routine configuration weakness may warrant urgent remediation if it creates a practical path toward privileged access or persistence.

Exploitability-based prioritization helps organizations avoid two common failures: overreacting to low-value deviations and underreacting to genuinely dangerous but less obvious weaknesses. It also improves remediation planning by aligning effort with realistic risk reduction.

4.4. REMEDIATION GUIDANCE MUST RESPECT OPERATIONAL INTEGRITY

Security recommendations only create value when they can be implemented safely. In Active Directory, even well-intentioned changes can affect authentication flows, service dependencies, compatibility, and production stability. As a result, high-quality assessments should include step-by-step remediation guidance that helps teams understand not only what to change, but how to test, phase, and validate that change.

Practical guidance may include GPO paths, relevant registry keys, AD attribute changes, sequencing considerations, and notes on potential side effects. This level of detail is especially important for resource-constrained teams that do not have the time to translate abstract recommendations into implementation plans from scratch.

05

BEST PRACTICES

5.1. DETECTION ENGINEERING SHOULD BE BUILT IN

Configuration audits should not only identify what to fix; they should also improve what the blue team can see. When findings are linked to adversary tactics and techniques, defenders gain practical input for detection engineering, alert tuning, hunting, and control validation.

Mapping findings to frameworks such as MITRE ATT&CK is particularly useful when it is done in a way that supports operational workflows rather than simple labeling. A finding tied to known adversarial tradecraft allows defenders to ask better questions: What would this misuse look like in telemetry? Do our detections cover it? Which log sources are required? Where are our current blind spots?

5.2. COMMON CHARACTERISTICS OF HIGH-VALUE AD ASSESSMENTS

- They combine broad coverage with manual validation.
- They emphasize evidence-backed reporting rather than volume of findings.
- They prioritize issues according to both severity and exploitability.
- They include remediation guidance that can be executed safely in production-oriented environments.
- They help defenders improve detections, not just close gaps.

In practice, the difference between a formal review and a useful review is execution quality. One produces a long document. The other drives measurable risk reduction.

5.3. STRATEGIC RECOMMENDATIONS FOR ORGANIZATIONS

- Treat Active Directory as a Tier-0 trust system rather than a routine infrastructure component.
- Favor assessments that provide reproducible evidence and minimize false positives.
- Require prioritization that reflects exploitability and realistic attacker tradecraft.
- Expect remediation guidance detailed enough to support controlled operational rollout.
- Use findings as inputs for detection engineering, not only for hardening backlogs.
- Include related components such as AD CS and other AD-integrated infrastructure in the review model where relevant.

06

CONLUSION

Active Directory security is not merely a hardening exercise. It is a resilience challenge that directly affects how well an organization can prevent privilege abuse, contain compromise, and recover trust. Organizations that rely only on automated enumerations or context-free scoring often struggle to distinguish noise from real risk.

An effective Active Directory assessment, such as the one conducted by Black Cell's offensive security experts, is one that identifies meaningful weaknesses, validates them with evidence, prioritizes them according to exploitability, and supports safe remediation while also improving defender visibility. That is the difference between a report that gets archived and an assessment that drives measurable security improvement.