CSIS

REST ASSURED.

Active Directory Health Check

Don't let Active Directory become your Achilles heel.

The leader in actionable and intelligence-driven
detection and response services

www.csis.com

Nowadays IT criminals put significant effort towards attacking Active Directory (AD).

We firmly believe that companies need to switch to an "Assume Breach Paradigm" to adapt to this new attack landscape.

Active Directory is the lifeblood of modern networks, and without it, the whole organization can grind to a halt. Attackers target the system to access and obtain new credentials to help them move laterally in the network. It is a significant reason to secure Active Directory and follow best practices.

10 minutes

Average time
for a local attacker
to gain access to your organization's AD installations

95%

of AD installations
can be compromised during a cyberattack

50%

organizations
do not have AD cyber disaster recovery plan

Source: Semperis

"The progressive nature of Active Directory and the complex security framework gives an unfair advantage to attackers. We must be more diligent and improve our security posture on such critical infrastructure."

Ian Qvist
Director of Chronos Services, CSIS

The purpose of the AD Health Check
is to mitigate the risk associated with targeted attacks against your network.

If an attacker gains access to your AD, they control your organisation.

The AD Health Check comes in 2 different offerings, so you can choose the depth that suits you and the security level that matches your organization.

The Essential package

Gives you a general AD security health check. We check 25 essential controls to see if the Active Directory follows the most widely accepted best practices and ensures that attackers cannot obtain access with the most commonly used attack tools. Here are some examples of controls:

- Credential stealing and account takeover
- Misconfiguration of privileged users
- Kerberoasting of privileged users
- Hardening of Enterprise, Domain and Local Administrators
- Access Control List misconfigurations
- Strong password policies
- Best practice audit logging
- Domain & forest functional levels

The Advanced package

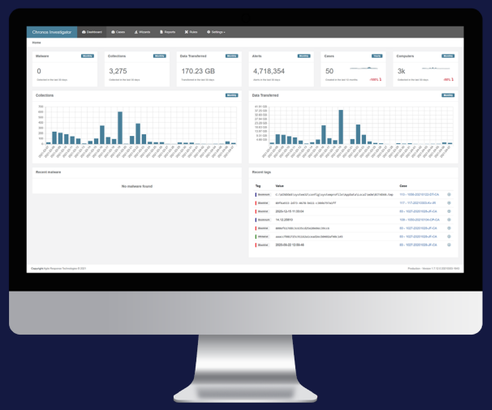
Covers the same 25 controls as the essential package, but with an additional 75 security controls. The package gives you a more in-depth analysis and better coverage of your security posture. The result leaves you with a healthy level of security that can withstand even skilled attackers. The additional controls include:

- Protections against advanced credential-stealing attacks
- Unconstrained delegation analysis
- Protections against Golden and Silver Ticket attacks
- Legacy protocols and broken cryptography primitives
- Implanted malicious accounts and Shadow Administrator activity
- Analyzing group policies for credential leaks
- Best practices in architecture such as Administrative Tier Model and Enhanced Security Administrative Environment (ESAE)
- Control path analysis

With an AD Health Check Essential package we detect every common vulnerability that attackers use in the wild. It makes it much more difficult to attack the network, but some advanced attack techniques might still be present. That's why we have AD Health Check Advanced package, which meticulously goes through the AD in depth and finds those more advanced vulnerabilities.

Our methodology is extensive & fast

We leverage our proprietary, purpose-built platform called Chronos to ensure a fast, accurate and effective service delivery process.



- Scales automates and improves every aspect of the investigative process, from data collection, to analysis and reporting
- It takes only 5 minutes to run our application and it can be run from anywhere
- Powerful intelligence and analytics tools ensure depth and breadth of analysis

Benefits

- Get an overview of your organization health issues, vulnerabilities and misconfigurations
- Improve your security posture in limited amount of time
- Mitigate the risk associated with targeted attacks against your network
- Our specialists provide you with recommendations and detailed mitigations in English to match a broad audience

References & testimonials

"AD Health Check became an amazing solution for our business, where we managed to get a full report covering all our security issues and misconfigurations. The unparalleled expertise that we gained from CSIS specialists has helped us significantly to strengthen our organization's security posture and improve resilience against targeted attacks."

Brian Lolk,
Team leader - IT and Project, Amgros

AMGROS

REST ASSURED.

CSIS IN BRIEF

- Founded in 2003
- Leading pure-play cybersecurity services player
- Delivering actionable and intelligence-driven detection and response services
- Preferred partner to leading organizations across multiple sectors
- Trusted advisor to law enforcement agencies, government and news media
- Credited by Gartner

OUR OFFERING

- Managed Detection & Response (MDR)
- Cyber Threat Intelligence (CTI)
- Brand Protection
- Incident Response
- Security Consulting
- Security Software

CSIS Security Group A/S

Head office
Vestergade 2B, 4th floor
1456 Copenhagen
Denmark

UK office
95 Aldwych
London, WC2B 4JF
UK

+45 88 13 60 30

The leader in actionable and intelligence-driven **detection and response services**

www.csis.com