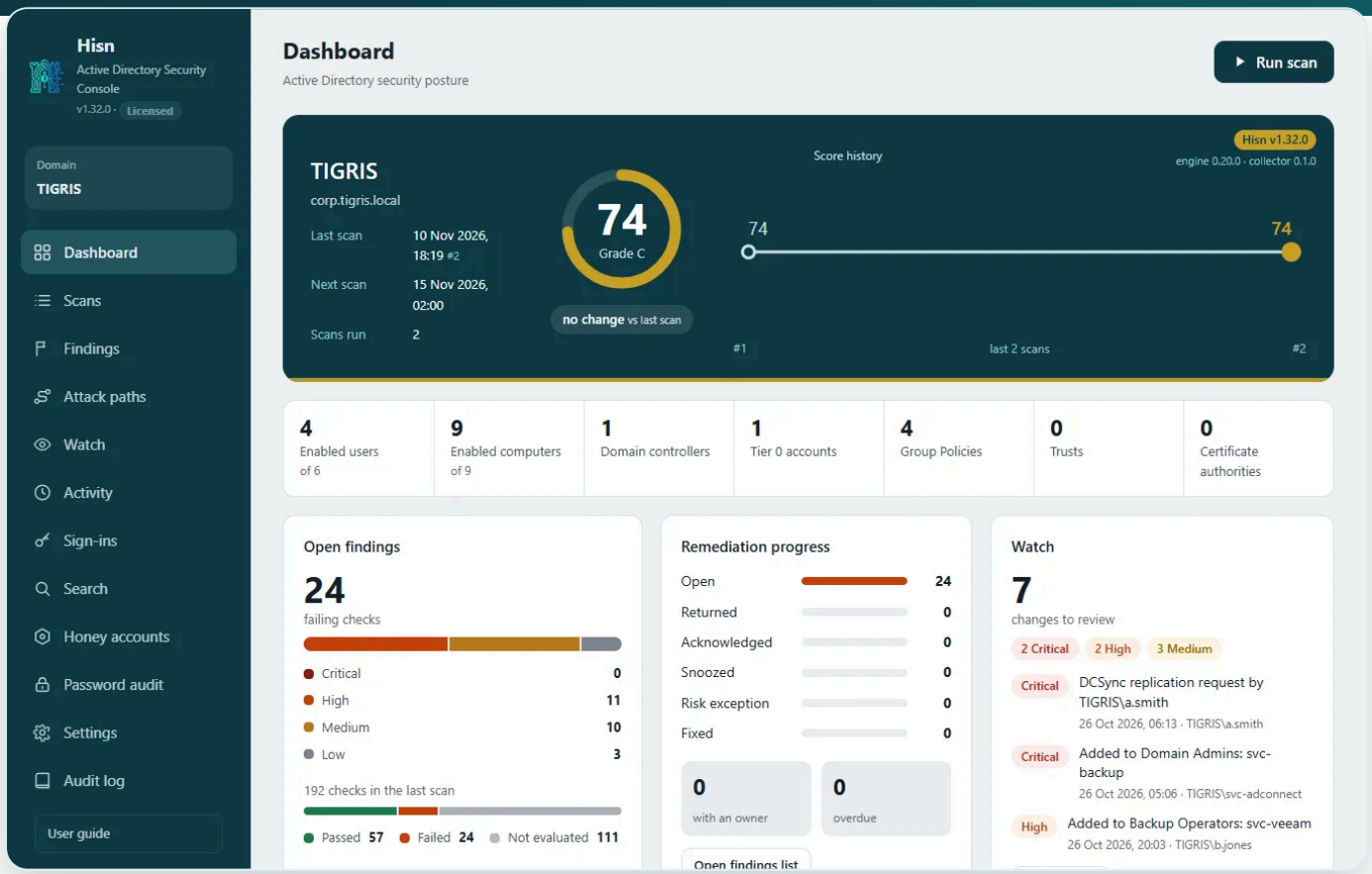
HISN
Active Directory security console

Offline | Read-only | Arabic and English | One Windows service

See every weakness in your Active Directory. Before an attacker does.

Hisn scans your domain for the 192 things attackers look for, draws every path from an ordinary account to control of the domain, and watches your domain controllers live. It never writes a change to Active Directory and needs no internet connection.



192

Assess

Security checks in 11 areas, from accounts and Kerberos to AD CS (ESC1–ESC16), Group Policy and member servers. A score and grade, and for every finding a fix script and a rollback script your administrators review and run.

Tier 0

Attack paths

Every chain of permissions, memberships and sessions from an ordinary account to control of the domain, with the single change that breaks each one, and the one change that closes the most.

~1 min

Live Watch

Reads the domain controllers' Security logs every minute by default and alerts on Tier 0 changes, DCSync, Kerberoasting, password spraying, decoy-account use and more, between scans.

Pictures show an invented demo domain.

hisnsecure.com

What Hisn gives your team

Findings you can act on

Each finding explains the risk, lists the affected objects, its MITRE ATT&CK techniques and framework controls, and tracks its state from open to fixed across scans, with owners, due dates and risk exceptions.

Tier 0 sign-in exposure

Shows where privileged accounts sign in, and alerts when one is used on a workstation or server outside Tier 0, where its credentials could be stolen.

Lockouts explained

Every account lockout with the machine that caused it and the likely reason: an old stored password, a service, a device, a mistyped password, or an attack.

Who changed what

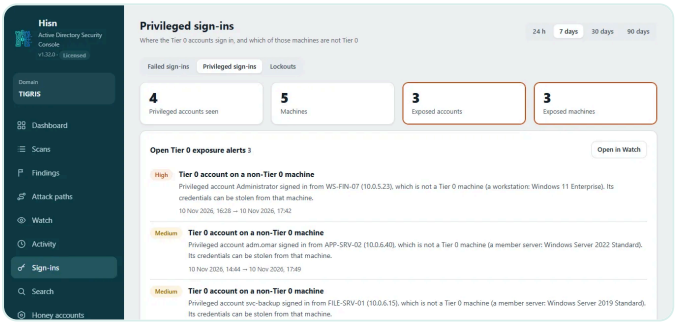
User, group, computer and GPO changes with the actor, including which Group Policy setting changed, old and new value. One search over changes, sign-ins and alerts, exportable to CSV.

Seven reports

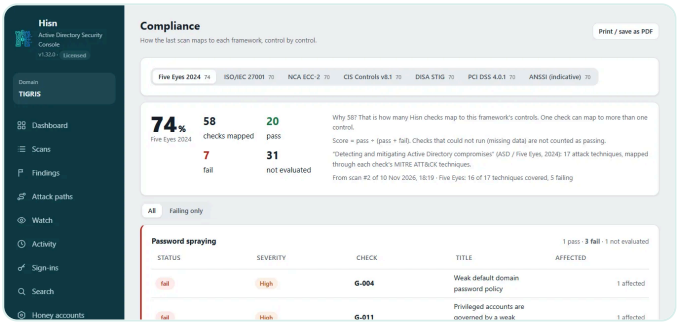
Executive, technical, framework mapping, remediation plan, changes, attack paths and custom. Arabic or English, A4, with a report ID and SHA-256 fingerprint.

Compliance mapping

Checks mapped to Five Eyes 2024, ISO/IEC 27001, NCA ECC-2, CIS Controls v8.1, DISA STIG, PCI DSS 4.0.1 and ANSSI (indicative). Hisn maps to frameworks; it does not certify compliance.



Privileged sign-ins: Tier 0 accounts used outside Tier 0.



Compliance: each framework, control by control.

Built for sensitive networks

- **Inside your network.** No internet connection to run or to activate; updates arrive as signed files you carry in.
- **Read-only.** Hisn never writes to Active Directory, Group Policy or servers. Fixes are scripts your administrators review and run.
- **Agentless.** One Windows service on one server reads the domain over standard protocols.
- **No password hashes.** Never read or stored by the console; stored secrets are protected with Windows DPAPI.
- **Arabic and English** throughout the console, reports and user guide.

Requirements

- Windows Server 2016 or later, domain-joined
- PowerShell 5.1
- Edge, Chrome or Firefox for the console
- About 1 GB free memory per 20,000 accounts while scanning

Licensing

- Priced per Active Directory domain
- A signed licence file, imported offline
- Built-in demo: one full scan, every report
- 14-day trial, subscription, or perpetual with maintenance

Try it on your own domain.

Download the installer, run the built-in demo scan, then ask for a trial licence.

hisnsecure.com

sales@hisnsecure.com

Hisn (حصن) 1.32 · Active Directory and Windows are trademarks of Microsoft. Framework names belong to their owners; Hisn maps its checks to them and does not certify compliance.