

stig-ai-pipeline

An open-source, AI-enabled toolkit consisting of AI skills and scripts, so that a generalist administrator can apply Department of Defense hardening checklists without a compliance specialist.

THE PROBLEM

The US Department of Defense publishes free cybersecurity checklists called STIGs (Security Technical Implementation Guides) for almost every common system: Windows, Linux, macOS, SQL Server and hundreds more. Each lists a few hundred settings that make the system secure against cyberattacks. Anyone can download them.

Applying one takes a specialist. Every rule has to be read, understood, ranked by risk, and translated into a change on a real machine. Scanners can say which rules a system fails; they cannot say what a rule means, whether the fix is safe here, or what to do first. Most organisations do not have that person, so they do not use the checklists at all.

WHAT THE TOOLKIT DOES

1 Read the guide — stig-prep

Turns any STIG, exactly as DISA publishes it, into a tracker: one row per rule, severity ranked, with the full check and fix text. Excel, CSV, JSON or Markdown.

2 Explain every rule — stig-explain

For each rule: what it actually makes you do and why, a rating (quick win / needs a policy pushed out / needs a human decision / can break things), whether it can be scripted, and what could go wrong. Written by the AI assistant you already have; no account, no key. The results are published in the repository, so anyone gets them with no AI at all.

3 Check a machine — stig-scan

Turns each rule into a runnable check and reports pass, fail, or error for the machine in front of you. Every check is unreviewed until a named person reads it and approves it; approval freezes a fingerprint of the exact command; a safety gate refuses anything that could change the system. The report says first how many rules were actually evaluated.

BY THE NUMBERS

7

DISA STIGs rules parsed and validated explained

1,440

3

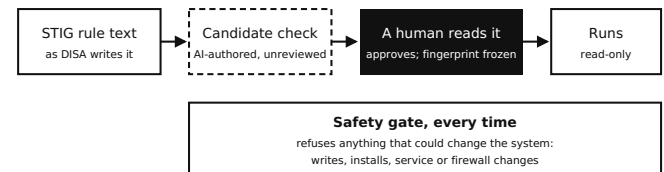
platforms: macOS, Linux, Windows*

77

automated tests

Windows 11, Windows Server 2019, RHEL 9, Ubuntu 24.04, macOS 26, SQL Server 2022 Instance and Database. *Windows: parse and explain; scanning planned. MIT licence.

HOW IT STAYS SAFE



AI may help write a check. It never runs one.

Edit an approved check and the approval is void.

TRY IT IN THREE COMMANDS

```
git clone https://github.com/himanshusaxenagithub/stig-ai-pipeline
cd stig-ai-pipeline
python3 -m stigprep parse U_MS_Windows_11_V2R9_STIG.zip --explain
```

Python 3.9+, no dependencies. Download the STIG zip from public.cyber.mil. The Windows 11 explanations are already in the repository.

HOW THIS HELPS YOU

A week of specialist work in one command. You start from a ranked, explained plan, not 300 pages of XML.

You know what to do first, and what could go wrong.

Every rule is rated quick win / policy / decision / risky, with the caution a specialist would have given you.

Nothing runs without your approval, and nothing changes your systems. Safe to hand to a junior admin.

Evidence you can show an auditor, a customer or an insurer. Every scan records what ran, what came back, and what was not checked.

A recognised baseline. Rules map to NIST 800-53 controls through DISA's own identifiers, carried in the tracker.

Free, and asks for nothing. MIT licence, no account, no key, no vendor. Built for the IT generalist at a school district, a clinic, a small bank or a municipal agency.

What it looks like in practice

One rule, followed from the DISA guide to a plain-English explanation to a scan result. Everything below is real output from the toolkit.

STEP 1 — WHAT DISA GIVES YOU (ONE OF 257 RULES IN THE WINDOWS 11 GUIDE)

WN11-00-000030 · Severity: high (CAT I)

Windows 11 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.

Discussion: If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove nonvolatile memory and read it directly...

Check: For AVD implementations with no data at rest, this is NA. Verify all Windows 11 information systems (including SIPRNet) employ BitLocker for full disk encryption. If full disk encryption using BitLocker is not implemented, this is a finding...

Fix: Enable full disk encryption on all information systems (including SIPRNet) using BitLocker...

Multiply by 257 rules for this guide, 445 for Red Hat Linux. This is the wall a generalist hits.

STEP 2 — WHAT THE TOOLKIT TURNS IT INTO: ONE ROW IN A TRACKER

```
$ python3 -m stigprep parse U_MS_Windows_11_V2R9_STIG.zip --explain
Parsed: Microsoft Windows 11 Security Technical Implementation Guide
257 rules — 27 CAT I, 214 CAT II, 16 CAT III
explanations: all 257 rules annotated from filed sets
```

Rule ID	CAT	What it means	Triage	Scriptable	Caution
WN11-00-000030	I	Turn on full-disk encryption (BitLocker) for the Windows drive and every fixed data drive, so a lost or stolen machine cannot be read by pulling the disk out.	config-profile	manual	Back up the BitLocker recovery key somewhere safe before enabling it; without the key a locked drive is unrecoverable.
WN11-00-000040	I	Keep Windows 11 on a version Microsoft still supports (22H2 build 22621.380 or newer), because older versions stop receiving security fixes.	quick-win	automatable	A feature update takes time and a reboot; schedule it, and check any line-of-business software supports the newer version first.
WN11-00-000070	I	Only the accounts that actually administer the machine may be in the local Administrators group. Ordinary user accounts must be removed.	needs-judgment	manual	Removing the wrong account can lock out the person who supports the machine; confirm who needs admin rights first.

The Excel tracker has all 257 rows, sorted CAT I first, with a status dropdown, owner and target-date columns for the team, and a Details sheet with the full check and fix text. The triage rating tells a generalist what to do first: 143 of these 257 rules are quick wins.

STEP 3 — CHECKING A REAL MACHINE (A MACBOOK AGAINST THE MACOS 26 GUIDE, 7 SEPTEMBER 2026)

```
$ python3 -m stigscan approve checkpacks/macos-26-v1r3.json --by "Himanshu Saxena" --id APPL-26-005001 ...
Approved 10 check(s) as 'Himanshu Saxena'; content digests frozen.

$ python3 -m stigscan scan checkpacks/macos-26-v1r3.json -o out/ --record evidence/2026-09-07/
Scanned macos-26-v1r3 on MacBookPro.lan
pass 3 fail 7 error 0 manual 0 skipped 150
CAT I failures: 7
APPL-26-005020 The macOS system must enforce FileVault.
...
```

The report leads with the sentence that matters: **"10 of 160 rules (6.2%) were actually evaluated on this host. The remaining 150 produced no compliance evidence and must not be counted as either compliant or non-compliant."** Only the ten checks a named person approved were run; the safety gate refused nothing because nothing approved could change the system; and every failure is shown with its plain-English explanation from Step 2, so the administrator knows what it means and how risky the fix is.

What stays with you: which checks to approve, which changes to make, in what order, and what to accept as a risk. The tool drafts, explains and checks. It never changes a system.

Himanshu Saxena · Repository: github.com/himanshusaxenagithub/stig-ai-pipeline · Write-up: hackernoon.com/building-a-reusable-ai-skill-for-stig-to-excel-conversion