Security Scan Attestation

SCAN-20260115-200116

DATE: January 15, 2026

HOST: `edd14482955a0437dace904a4cda00ae9c86a9cd7feba5df0690bf8cfa94165c`

PATH: `/Users/brucedombrowski/Security` (Security)

SUBJECT: Automated Security Scan Attestation

1. Purpose

This document attests that automated security scans were executed against **Security** using the Security Verification Toolkit. The scans verify alignment with NIST SP 800-53 security controls.

2. Scan Environment

- **Scan Timestamp:** 2026-01-15T20:00:59Z
- **Toolkit Version:** v0.0.0-test.20260115T195412Z-2-g978a1d3 (978a1d3)
- **Toolkit Repository:** https://github.com/brucedombrowski/Security

3. Host Inventory Reference

A host inventory snapshot was collected at scan time to establish a verifiable system thumbprint. This enables integrity verification while keeping sensitive machine data (MAC addresses, serial numbers) separate from shareable scan results.

Inventory File	`host-inventory-2026-01-15-T200059Z.txt`
SHA256 Checksum	`edd14482955a0437...`
NIST Control	CM-8 (System Component Inventory)

Note: The host inventory contains sensitive information. All scan outputs reference this checksum rather than embedding the actual data, allowing scan results to be shared without exposing machine-specific details.

4. NIST Control Mapping

The following NIST SP 800-53 Rev 5 controls were verified:

Control	Family	Verification Method
CM-6	Configuration Management	Host security posture
CM-8	Configuration Management	Host inventory collection
SA-11	System & Services Acquisition	Secrets and credential scanning
SC-8	System & Comms Protection	MAC address detection
SI-3	System & Info Integrity	ClamAV malware scanning
SI-12	System & Info Integrity	PII pattern detection

5. Scan Results

Scan	NIST Control	Result	Findings
PII Scan	SI-12	**PASS w/ exceptions**	13 reviewed exceptions
Malware Scan	SI-3	**PASS**	No malware detected
Secrets Scan	SA-11	**PASS w/ exceptions**	3 reviewed exceptions
MAC Address Scan	SC-8	**PASS**	No MAC addresses detected
Host Security	CM-6	**PASS**	All checks passed

Summary: 5 passed, 0 failed

Overall Result: PASS

PASS w/ exceptions = reviewed exceptions documented in Section 6

6. Reviewed Exceptions

Items flagged by automated scans but reviewed and accepted as non-issues are documented in allowlist files. Each exception includes a SHA256 hash for integrity verification and reviewer justification.

6.1 PII Scan Exceptions

Allowlist File	`.pii-allowlist`
SHA256 (first 16)	`f906fbb6db7bc3a8`
Total Exceptions	13

#	Justification
1	Documenting localhost quick-accept feature
2	X.509 OID example, not an IP address
3	Version string example, not an IP address
4	Shell command syntax, not PII data
5	X.509 OID documentation note
6	X.509 OID for Email Protection (1.3.6.1.5.5.7.3.4)
7	X.509 OID for Document Signing (1.3.6.1.4.1.311.10.3.12)
8	Historical command log, not active PII
9	Placeholder pattern (build-time substitution)
10	LaTeX template placeholder (replaced at runtime)
11	Example/placeholder data (not real PII)
12	Example/placeholder data (not real PII)
13	Placeholder pattern (build-time substitution)

6.2 Secrets Scan Exceptions

Allowlist File	`.secrets-allowlist`
SHA256 (first 16)	`67537c26531da807`
Total Exceptions	3

#	Justification
1	Internal controlled variable assignment (safe eval)
2	Internal controlled variable assignment (safe eval)
3	Internal controlled variable assignment (safe eval)

Note: Full details including file paths and SHA256 hashes are in the respective allowlist files.

7. Scan Output Checksums

The following SHA256 checksums were generated for scan output files:

Scan Output File	SHA256 (first 16)
host-inventory	`edd14482955a0437...`
pii-scan	`bc1450d6f914f39a`
malware-scan	`21086a59a14d448a`
secrets-scan	`c10be2b702638828`
mac-address-scan	`dc33c153493567da`
host-security-scan	`c3c8d86b669d1cd8`
security-scan-report	`b23679ab38316d7e`

checksums.md SHA256 (full):

`12dda6b0acb8380a130777202fbb55fd0e54b17d6671055537e44bd4e2309eec`

Full file names: `*-2026-01-15-T200059Z.txt`. The `checksums.md` file contains full SHA256 hashes for all scan outputs.

8. Verification Chain

This document establishes a chain of trust for verifying scan integrity:

Chain of Trust:

1. **Digital Signature** → This PDF is digitally signed, establishing authenticity
2. **checksums.md Hash** → This PDF includes the SHA256 hash of `checksums.md` (Section 7)
3. **Scan File Hashes** → `checksums.md` contains full SHA256 hashes of all scan output files
4. **File Verification** → Any scan file can be verified against `checksums.md`

Verification Commands:

```
# 1. Verify PDF signature (platform-dependent)
# 2. Extract checksums.md hash from PDF Section 7
# 3. Verify checksums.md integrity:
shasum -a 256 .scans/checksums.md

# 4. Verify all scan files against checksums.md:
cd .scans && shasum -a 256 -c checksums.md
```

9. Attestation

This document certifies that:

(a) Automated security scans were executed against the target repository

(b) Scan results are accurately represented in this document

(c) The Security Verification Toolkit version and commit hash are recorded for traceability

(d) Detailed scan logs are available in the `.scans/` directory

(e) The verification chain above enables independent validation of all scan outputs