SOCROOT

Synthetic Security Assessment Sample

A portfolio demonstration of scope, evidence, findings, and verification - not a customer report.

SYNTHETIC / PUBLIC

Fictional organization	Northstar Labs
Example target	example.org - reserved example domain
Report ID	SAMPLE-2026-001
Purpose	Portfolio demonstration only
Data classification	Public synthetic content

No scan was run against a real client.

Names, assets, findings, severity, and evidence are fictional and demonstrate reporting structure only.

1. Executive summary

This sample shows how SOCRoot intends to present an authorized external assessment: with an explicit scope, evidence provenance, uncertainty, prioritized remediation, and retest criteria. It is deliberately conservative and does not imply a production service, customer engagement, SLA, certification, or autonomous remediation capability.

Assessment type	Synthetic external exposure assessment walkthrough
Authorization	Fictional written authorization assumed for example.org
Included	Passive discovery, safe configuration checks, evidence review
Excluded	Exploitation, credential use, social engineering, denial of service
Default response	Dry-run proposals with human approval
Overall conclusion	No real-world security conclusion - demonstration data only

Methodology

- Confirm asset ownership, testing window, exclusions, and data-handling rules.
- Collect passive and low-impact signals only from approved sources.
- Validate scanner output manually before calling it a finding.
- Record the evidence, confidence, uncertainty, and remediation owner.
- Retest approved changes and document the outcome and rollback path.

Limitations

- This document uses fictional observations and screenshots are intentionally omitted.
- A real assessment may miss vulnerabilities and does not prove the absence of compromise.
- Control mapping can support readiness but is not certification or legal advice.
- Response times and service availability require a separate written agreement and operating evidence.

2. Illustrative findings

SYN-01	MEDIUM

HTTP Strict Transport Security not demonstrated

Illustrative observation: The fictional evidence set does not demonstrate an HSTS response header on the example web service. Without HSTS, a browser may not be instructed to require HTTPS for future requests.

Recommended validation: Capture response headers from the authorized service, verify redirect behavior, deploy an appropriate HSTS policy after compatibility review, then retest.

Evidence expected: Response headers, redirect chain, browser compatibility decision, post-change retest.

SYN-02	MEDIUM

DMARC enforcement not demonstrated

Illustrative observation: The fictional DNS evidence shows an example DMARC policy in monitoring mode. Monitoring can provide visibility, but it does not instruct receivers to quarantine or reject unauthenticated mail.

Recommended validation: Review legitimate mail sources, analyze aggregate reports, stage SPF/DKIM corrections, and move toward enforcement only after owner approval.

Evidence expected: DNS record, authorized sender inventory, aggregate-report review, staged enforcement plan.

SYN-03	LOW

Administrative access boundary not evidenced

Illustrative observation: The fictional scope includes an administrative service, but the provided evidence does not show an approved source allowlist, VPN boundary, or bastion-host policy.

Recommended validation: Confirm whether the service is required, restrict sources, require strong authentication, enable logging, and document emergency access and rollback.

Evidence expected: Firewall policy, identity controls, access logs, exception owner, retest result.

3. Priorities and verification

Priority	Illustrative action	Completion evidence
1	Confirm authorization and asset ownership	Signed scope, asset owner, exclusions, test window
2	Validate transport and email-control observations	Timestamped headers/DNS output plus analyst notes
3	Approve bounded remediation	Owner approval, change plan, rollback steps
4	Retest and close	Before/after evidence, residual risk, closure decision

Evidence chain

Source	Name the approved source and collection method.
Timestamp	Use an unambiguous UTC timestamp.
Integrity	Retain original output or a documented hash where appropriate.
Interpretation	Separate observed facts from analyst inference.
Decision	Record who approved, rejected, or deferred the action and why.
Outcome	Retest, capture residual risk, and document rollback status.

Safety rules used in SOCRoot design

- Sensitive remediation stays human-controlled.
- SOAR dry-run is the default.
- CDN and RFC1918 ranges are not automatically blocked.
- DNS events remain notification-only.
- Raw client data is not sent to external AI providers.
- Production claims require tests, monitoring, rollback paths, and operational evidence.

4. Interpretation and next steps

A professional security report should make it easy to distinguish what was authorized, what was observed, what was inferred, what changed, and what still requires a decision. The purpose of this sample is to demonstrate that reporting discipline without inventing customer outcomes.

What this sample demonstrates	What this sample does not prove
- Scope and authorization structure - Conservative finding language - Evidence expectations - Human-controlled remediation - Retest and rollback records	- A real customer engagement - A production deployment or SLA - Continuous monitoring coverage - Regulatory compliance or certification - Autonomous exploitation or remediation

Public engineering sources

Architecture	github.com/Muath-Yousef/project-synapse
Control plane	github.com/Muath-Yousef/ide-agentic-engine
SOC runtime	github.com/Muath-Yousef/Project-Synapse-SOC-Factory
Portfolio	github.com/Muath-Yousef/portfolio-site

SYNTHETIC PORTFOLIO SAMPLE No customer data. No real assessment. No compliance or SLA claim.