NANO DEFENSE

SECURITY INTELLIGENCE / EVIDENCE / ACTION

CLIENT DELIVERABLE PREVIEW

Sample Security Assessment

An illustrative example of how Nano Defense turns observable security exposure into prioritized findings, supporting evidence, intelligence context, and practical remediation decisions.

OVERALL RISK	PRIORITY FINDINGS	ASSESSMENT
HIGH	3	EXTERNAL EXPOSURE

ILLUSTRATIVE SAMPLE - NOT A REAL CLIENT ASSESSMENT
All organizations, systems, IP addresses, evidence, and findings are fictional or use documentation-reserved values. This report demonstrates the intended reporting approach only.

Prepared for: **Example Organization**
Assessment date: August 2026
Prepared by: Nano Defense

Executive Security Summary

This illustrative external assessment identified three priority conditions that increase observable attack surface. The highest-priority issue is an externally reachable remote-access service. Additional findings demonstrate outdated web software and unnecessary information exposure. These findings indicate exposure requiring remediation; they do not establish that compromise occurred.

HIGH	3	2	1
OVERALL RISK	PRIORITY FINDINGS	EXPOSED SERVICES	HIGH-SEVERITY ISSUE

Assessment Scope & Methodology

PERSPECTIVE	External / unauthenticated	EXAMPLE TARGET	203.0.113.25
SCOPE	Approved external exposure review	SERVICES OBSERVED	SSH, HTTP/HTTPS
APPROACH	Discover -> validate -> correlate -> prioritize	LIMITATION	Point-in-time sample; no exploitation performed

What matters most

01 **Reduce remote-access exposure first.**
Restrict unnecessary reachability and strengthen authentication before lower-priority hardening work.

02 **Bring web software to an approved supported baseline.**
Patch or upgrade outdated components, then validate the resulting exposure.

03 **Reduce avoidable information disclosure.**
Disable unnecessary directory indexing and remove exposed artifacts that aid reconnaissance.

EXECUTIVE TAKEAWAY
Nano Defense separates what is observed from what is inferred. The objective is to reduce exposure based on evidence, prioritize what matters, and give the customer a defensible next action.

Priority Findings & Evidence

Each finding is presented with observable evidence, why the condition matters, and a practical defensive action. This sample intentionally avoids invented exploit results or unsupported attribution.

HIGH

Externally Reachable SSH Service

203.0.113.25:22 / TCP

OBSERVABLE EVIDENCE
An SSH service is reachable from the external assessment perspective.

WHY IT MATTERS
Internet-facing remote access increases opportunity for password attacks, credential abuse, and automated reconnaissance.

RECOMMENDED ACTION
Restrict access to approved source networks; prefer key-based authentication and strong MFA where supported; review authentication logs and disable unnecessary password access.

HIGH

Outdated Web Software Version

203.0.113.25:443 / TCP

OBSERVABLE EVIDENCE
The observed web service identifies a software version outside the illustrative approved baseline.

WHY IT MATTERS
Unsupported or outdated components can contain known weaknesses and can be targeted by automated exploit tooling.

RECOMMENDED ACTION
Validate the installed version, patch or upgrade to a supported release, remove unused modules, and retest after remediation.

MEDIUM

Web Directory Indexing Enabled

203.0.113.25:80 / TCP

OBSERVABLE EVIDENCE
Directory listing is enabled on a public web path in this illustrative scenario.

WHY IT MATTERS
Directory indexing can expose filenames, backups, scripts, or other information that increases reconnaissance value.

RECOMMENDED ACTION
Disable indexing unless explicitly required, review exposed directories for sensitive artifacts, and validate server configuration after the change.

Risk Prioritization & Remediation Roadmap

The goal is not simply to enumerate findings. Nano Defense organizes remediation around observable exposure, urgency, and the defensive value of the next action.

2	1	0
HIGH	MEDIUM	LOW

PRIORITY	DEFENSIVE ACTION	RATIONALE	TARGET
1	**Restrict and harden SSH exposure**	Reduces direct remote-access attack surface.	0-7 days
2	**Upgrade web software**	Reduces exposure to known weaknesses and unsupported components.	7-30 days
3	**Disable unnecessary indexing**	Reduces information disclosure and reconnaissance value.	7-30 days
4	**Retest and validate**	Confirms that corrective action changed observable exposure.	After changes

Remediation sequence

REDUCE EXPOSURE → PATCH / HARDEN → VALIDATE → MONITOR

Validation standard

Closure should be evidence-based. After remediation, rerun the approved scope, confirm that exposed services and versions changed as expected, review remaining findings, and document accepted exceptions or compensating controls.

Nano Defense Intelligence Analysis

This section demonstrates how Nano Defense can preserve context across observations rather than treating every finding as an isolated alert. The analysis remains conservative: unsupported conclusions stay indeterminate.

CORRELATE	REMEMBER	PROFILE	REASON	PREDICT	DECIDE

CORRELATION	The SSH exposure, outdated web component, and directory indexing collectively increase the observable attack surface. No compromise is inferred from these findings alone.
CAMPAIGN MEMORY	No prior assessment history is included in this illustrative sample. In a real deployment, repeated observations can be compared over time.
ADVERSARY PROFILE	**Indeterminate.** The sample contains insufficient evidence to infer a named actor, skill level, stealth, or persistence.
INCIDENT REASONING	The evidence supports exposure reduction and hardening. It does not establish that an incident occurred.
PREDICTION	If remote access remains exposed, automated reconnaissance and authentication attempts are plausible future observations. This is a defensive planning estimate, not a claim of observed activity.
REMEDIATION DECISION	Prioritize externally reachable remote access, then patching and information-exposure reduction, followed by validation and monitoring.

EVIDENCE OVER ASSUMPTIONS.
Where evidence is absent or conflicting, Nano Defense should say so. A defensible 'indeterminate' is more useful than an impressive unsupported conclusion.

What a real client assessment can include

Validated scope and methodology; observable findings and supporting evidence; severity and business context; prioritized remediation; assessment limitations; and a client-ready executive summary for technical and business stakeholders.

REQUEST A NANO DEFENSE SECURITY ASSESSMENT

Illustrative sample only. This document is not a penetration-test report, compliance attestation, certification, or statement that any real organization is vulnerable.