safous Security Assessment

AT-A-GLANCE

Internal Vulnerability Assessment

Visualize internal risk. Strengthen control. Prevent impact.

Gain visibility into hidden internal risks across your environment — and reduce both security exposure and operational risk.

Internal risks are not visible — and not controlled

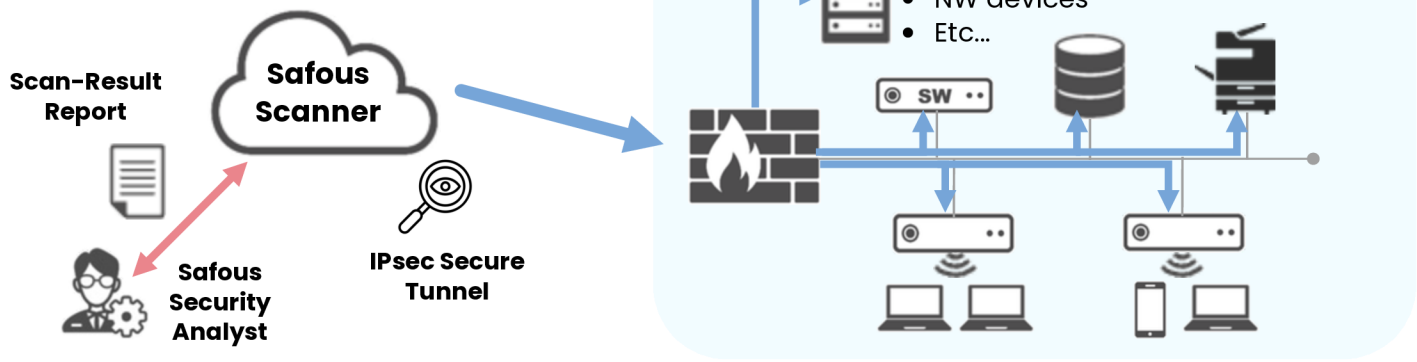
Hidden internal risks
Not visible from the outside

Limited branch visibility
Difficult to assess from HQ

Security resource gaps
Risks are identified but not addressed

Paths for lateral movement
Weak sites enable spread

How the Internal Vulnerability Assessment works



How Safous works

Asset Discovery
Find internal assets

Vulnerability Detection
Identify vulnerabilities

Risk Prioritization
Prioritize critical risks

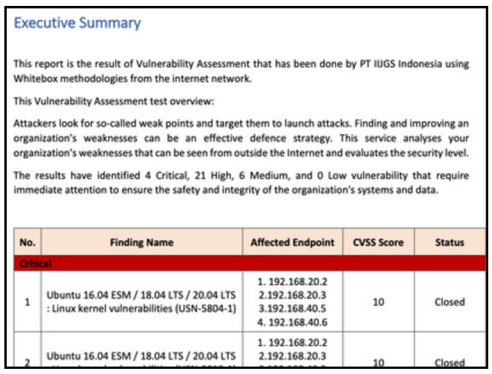
Reports & Guidance
Guide next actions

Centralized visibility and control of internal risk

See how our Vulnerability Assessment Report deliveres the insights you need.

SAMPLE REPORT

1 Executive Summary



Executive Summary

This report is the result of Vulnerability Assessment that has been done by PT IUGS Indonesia using Whitebox methodologies from the internet network.

This Vulnerability Assessment test overview:

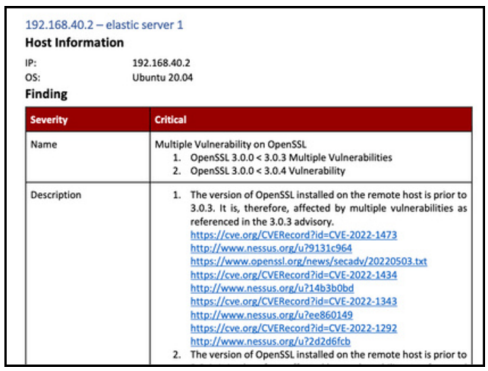
Attackers look for so-called weak points and target them to launch attacks. Finding and improving an organization's weaknesses can be an effective defence strategy. This service analyses your organization's weaknesses that can be seen from outside the Internet and evaluates the security level.

The results have identified 4 Critical, 21 High, 6 Medium, and 0 Low vulnerability that require immediate attention to ensure the safety and integrity of the organization's systems and data.

No.	Finding Name	Affected Endpoint	CVSS Score	Status
Critical				
1	Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6	10	Closed
2	Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS	1. 192.168.20.2 2.192.168.20.3	10	Closed

High-level overview of risk posture and key findings.

2 Detailed Findings



192.168.40.2 – elastic server 1

Host Information

IP: 192.168.40.2
OS: Ubuntu 20.04

Finding

Severity	Critical
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.3 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.4 Vulnerability
Description	1. The version of OpenSSL installed on the remote host is prior to 3.0.3. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.3 advisory. https://cve.org/CVERecord?id=CVE-2022-1473 http://www.nessus.org/u?9131c964 https://www.openssl.org/news/secadv/20220503.txt https://cve.org/CVERecord?id=CVE-2022-1434 http://www.nessus.org/u?14b3b0bd https://cve.org/CVERecord?id=CVE-2022-1343 http://www.nessus.org/u?ee860149 https://cve.org/CVERecord?id=CVE-2022-1292 http://www.nessus.org/u?2d2d6fcb 2. The version of OpenSSL installed on the remote host is prior to

In-depth findings with affected assets, severity, and remedtiation guidance.

Comprehensive assessment across multiple systems, configurations, and security vulnerabilities.

Use Cases: Are these challenges familiar?

Regional Offices / Subsidiaries
Limited visibility

Distributed Environments
No unified risk view

Limited Security Resources
Risks remain unresolved

Governance Initiatives
No standardized control

Continuously identify, prioritize, and reduce internal risk across your organization.

Safous enables continuous visibility and control of internal risk, helping organizations manage security across distributed environments.

Safous is a global cybersecurity team within the Internet Initiative Japan Inc. (IIJ) Group. With Safous, you can keep your corporate resources secure while giving your remote teams safe and easy network access through our zero trust security platform.

Contact us today to get started.

- RPAM
- Industrial Cybersecurity

- Zero Trust Platform
- PAM
- OT Security

info@safous.com

safous IIJ

www.safous.com