FRENOS

OT SECURITY ASSESSMENT REPORT

PROVIDED TO

FRENOS

REPORT ISSUED DATE:	GENERATED BY:
09/12/25	Default admin

EXECUTIVE SUMMARY

OT SECURITY POSTURE SCORE

D

(Letter grade of D reflects your current resilience against threat actors in your sector.)

Summary Scope

SITES
All Sites

NETWORKS
119

DEVICES
6,378

BUSINESS UNITS
0

Summary Opinion

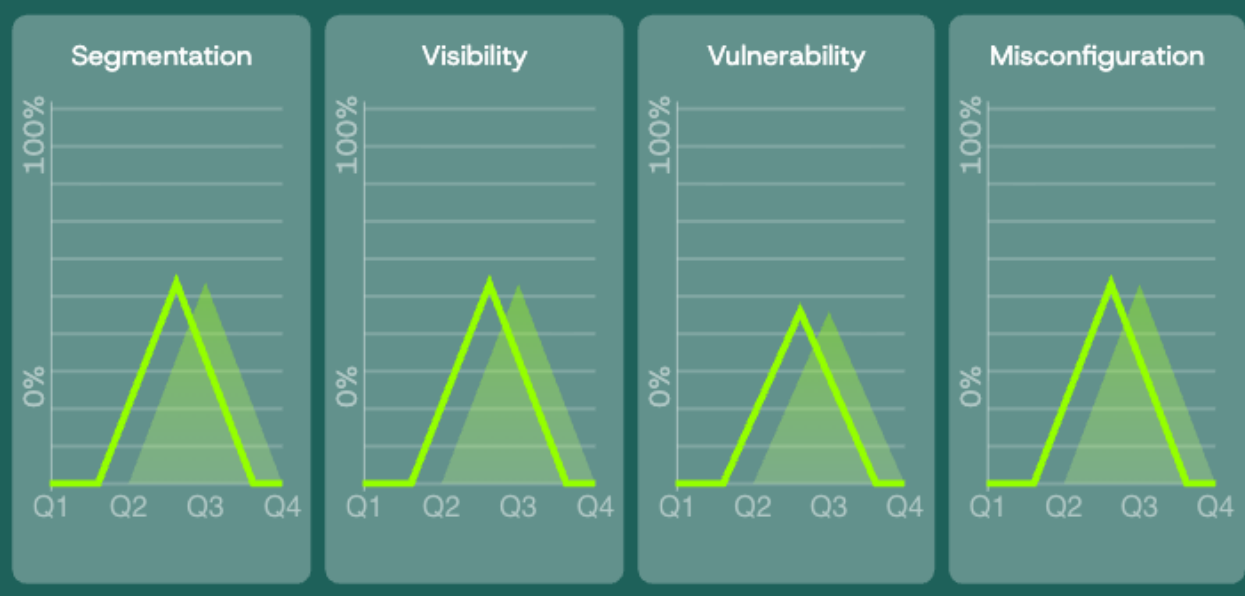
95 Vulnerabilities

141 Prioritized Threats

As a result of ongoing assessment activities, Frenos determined that Ninety Five vulnerabilities pose an immediate risk to Frenos and should be remediated as soon as reasonably possible.

While Frenos identified One Hundred Forty One additional vulnerabilities in enterprise networks with partial access to the ICS environment, these vulnerabilities do not pose an immediate, significant risk to the organization. These vulnerabilities could allow an attacker to obtain network and system configuration information or attack individual end-users on insecure networks.

Risk Trending



Count of Findings

FINDINGS IDENTIFIED:	FINDING CRITICALITY				
	Critical	High	Medium	Low	Total
	0	179	43	0	222

Critical Findings

FINDING	RECOMMENDATION	MPS
PAM lockout prevents brute force by limiting login attempts	Config PAM; lockout 5 tries	90%
Enables PAM; blocks unauthorized SSH	Enable PAM for SSH	90%
Disables .rhosts, blocks unauthorized SSH access	Set HostbasedAuthentication to no	90%
TFTP disable prevents ingresstooltransfer	Disable TFTP on Cooper Power Systems	90%
Disabling source routing blocks T1105 attacks	Disable source routing	90%

ASSESSMENT SCOPE

DEVICES	COUNTS	SOURCES
Firewall (PaloAlto)	9	PaloAlto
Devices (ForeScout)	6,378	ForeScout

The systems under consideration for this assessment were part of the All Sites and consisted of nine Firewall (PaloAlto) and six thousand three hundred seventy eight Devices (ForeScout) across PaloAlto and ForeScout

DIGITAL TWIN VS PRODUCTION

This document lists the attributes and differences of the digital twin in use as a simulated test environment for compliance and operational assessments.

Attributes of the Digital Twin

- Firewall and router configurations
- Asset visibility tools including Nozomi, Claroty, and Dragos
- Vulnerability data from OT visibility tools and Tenable, Rapid7, and other scanner vendors

> Represents modeled relationships of network devices, configurations, vulnerabilities, and assets and is periodically updated based on snapshots from upstream tools but does not operate in real time.

Differences from Production Environment

- The digital twin lacks live interactions, dynamic routing changes, and user activity
- Not all operational data is included, leading to potential blind spots in certain scenarios
- The model does not reflect changes not captured in source data inputs

> The digital twin is utilized for controlled testing and assessment, with limitations to guide result interpretation and mitigate production risks. To mitigate these differences, SAIRA (Simulated Adversarial Intelligence Reasoning Agent) accounts for these differences in the autonomous assessment and analysis of these results.

PRIORITIZED ROADMAP

QUICK WINS 01 02 03 04 05 06 07 08 LONG TERM

Quick Wins | NOW

These activities are prioritized based on risk reduction and time or effort required to accomplish them. These items require immediate action to remediate key identified vulnerabilities:

01 Configure PAM settings in /etc/pam.d/common-auth and password-auth to enable lockouts using pamtally2.so. Add auth required pamtally2.so onerr=fail audit silent deny=5 unlock_time=900, ensuring users are locked out after 5 failed attempts for 15 minutes. This setup~

02 Log in to the Recloser Control as an administrator and navigate to Settings > Security. In PAM settings, select "Enable PAM" under Authentication Method to secure SSH access against unauthorized entry. This action strengthens authentication protocols.

03 To disable SSH host-based authentication on Linux systems, edit /etc/ssh/sshd_config and set HostbasedAuthentication to 'no'. Restart the SSH service using # systemctl restart sshd. Ensure compliance by auditing configuration with # sshd -T | grep hostbasedauthenti~

04 Disable TFTP on Cooper Power Systems by configuring system settings to block unauthorized file transfers, enhancing security and preventing exploitation by malicious actors.

Next Steps | NEXT

The following tactical initiatives will help improve the overall security posture of critical networks:

05 CVE-2022-26809 should be remediated as soon as possible using guidance in the linked advisory. If patching isn't possible, block access using network segmentation/filtering, or disable the affected service if not business-critical and feasible.

06 CVE-2021-30853 should be remediated as soon as possible using guidance in the linked advisory. If patching isn't possible, block access using network segmentation/filtering, or disable the affected service if not business-critical and feasible.

07 CVE-2022-6101 should be remediated as soon as possible using guidance in the linked advisory. If patching isn't possible, block access using network segmentation/filtering, or disable the affected service if not business-critical and feasible.

08 CVE-2022-39135 should be remediated as soon as possible using guidance in the linked advisory. If patching isn't possible, block access using network segmentation/filtering, or disable the affected service if not business-critical and feasible.

Long Term | LATER

No strategic initiatives were identified for long-term cybersecurity planning at this time.