SECPOINT®
www.secpoint.com

SecPoint® Penetrator Vulnerability Scanner V 69 Firmware Release

https://www.SecPoint.com/penetrator.html

Penetrator 69 – July 2026

- **Dark Mode for Scan Map**

The Scan Map has received some usability enhancements to provide a clearer and more informative dashboard experience.
When no active scans are in progress, the map now displays an informational message that clearly indicates that the absence of paths is due to no scans currently being launched by the Penetrator.

A new Light/Dark slider switch has been added directly to the map title bar, allowing administrators to instantly switch between the two display modes without leaving the page. The selected mode is applied immediately, making it easy to adapt the interface to different lighting conditions and personal preferences.

The preferred map style can also be configured under menu *System > Home Page Map Style*.

• New One-Page Certificate

A new one-page Certificate has been introduced to provide a concise and professional summary of the results of a Vulnerability Assessment and Penetration Testing technical-readiness scan.

SecPoint Cyber Security
VAPT Scan Service

Issued on: 2026-05-30 14:39:36

Technical Readiness Scan Certificate

This is to certify that a Vulnerability Assessment and Penetration Testing (VAPT) technical-readiness scan of the target system(s) listed below was performed by **SecPoint Cyber Security** on 2026-05-30 14:39:36. The scan was executed with the profile indicated below and the audited targets were checked against the platform's vulnerability database. The detailed findings, if any, are recorded in the full report that accompanies this certificate.

Certificate ID	[redacted]
Auditor	[redacted]
Issued by	SecPoint Cyber Security
Scan Name	[redacted]
Scan Profile	NIS2
Audit Period	2026-05-30 14:39:36 — 2026-05-30 15:11:16
Audited Target(s)	[redacted]

Overall Result

No potential vulnerabilities were identified. The technical-readiness scan is satisfactory.

CONFIDENTIAL

Conclusion

At the time of testing, the audited target system(s) are in a satisfactory state of technical readiness. Recommendations: 1.Maintain a scanning cadence of at least quarterly, and after every significant change to the target system(s). 2.Keep the platform's signature database and firmware up to date, and apply accepted hardening baselines to the audited systems. 3.Maintain continuous monitoring so that anomalies outside the scope of a periodic scan are detected promptly.
This certificate remains valid until the first of the following events occurs: a change to the target system(s); the disclosure of a vulnerability not yet present in the platform's signature database; or one year from the date of audit completion.

Signature
SecPoint Cyber Security

Date of Issue
2026-05-30 15:11:16

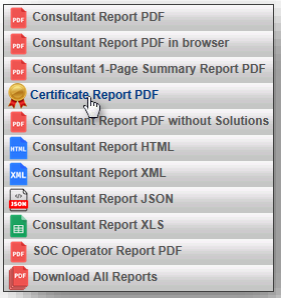
Authorized Seal

This certificate is a snapshot of the technical-readiness scan results and is valid only in conjunction with the full scan report.

A new one-page Certificate has been introduced to provide a concise and professional summary of the results of a Vulnerability Assessment and Penetration Testing technical-readiness scan.

The certificate confirms that the audited target systems were assessed against the Penetrator's vulnerability database and provides the overall result, the technical readiness conclusion, the date and time of the assessment, the scanned targets, and the scan profile used.

It also states the level of technical readiness achieved against the selected scan profile or international standard, together with best-practice recommendations for maintaining or improving security, and a validity statement that defines the conditions under which the certificate remains valid.



The one-page format is ideal for customer documentation, audit evidence, and demonstrating that a technical-readiness assessment has been successfully completed.

This certificate is available through the Report menu next to each target in the list of targets of a scan.

- **Reporting Improvements**

A few improvements have been made to reporting to provide greater accuracy and consistency.

- When Informational findings are disabled in the scan configuration, they are no longer included in the count of potential vulnerabilities shown in reports, ensuring that vulnerability statistics accurately reflect the selected scan policy.

- Following a factory reset, newly generated reports now include "CONFIDENTIAL" as the default watermark, providing immediate classification of generated documentation. The watermark can still be customized as required.

- The wording "Compliance" previously used in scan profile descriptions has been replaced with "Technical Readiness" to better reflect the purpose and scope of the available scanning profiles.

- **And…**

  - Improved handling of Let's Encrypt responses to prevent successful operations from being incorrectly reported as errors.
  - The Unit ID has been removed from Dark Web Search requests to further enhance privacy.
  - Fixed minor issues affecting the factory reset procedure.
  - Corrected an ambiguity in CST time zone interpretation that could cause a mismatch between recorded scan start and stop times.

HAFS
Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY V vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision