SecPoint® Penetrator Vulnerability Scanner V 68

Firmware Release

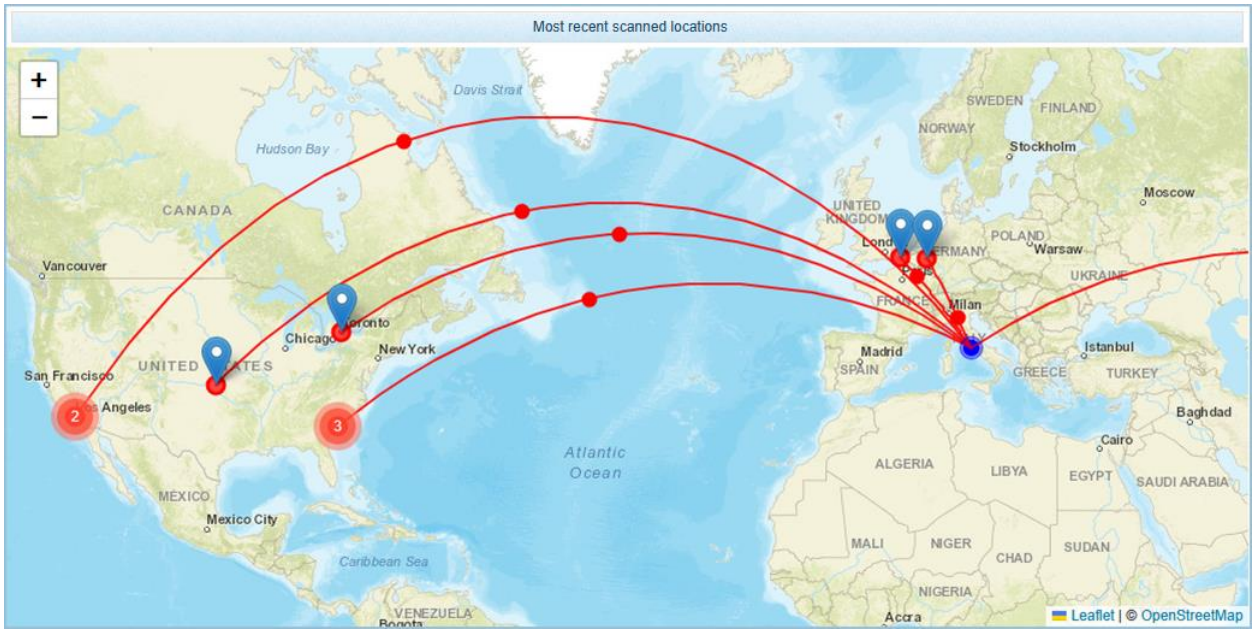
https://www.SecPoint.com/penetrator.html

Penetrator 68 – June 2026

- **Scan Map Improvement**

An important enhancement has been introduced to the Scan Map, significantly improving the real-time visualization and interpretation of vulnerability scans conducted by the Penetrator.

The map now provides a more intuitive representation of scanning activity by clearly distinguishing between ongoing and completed scans.



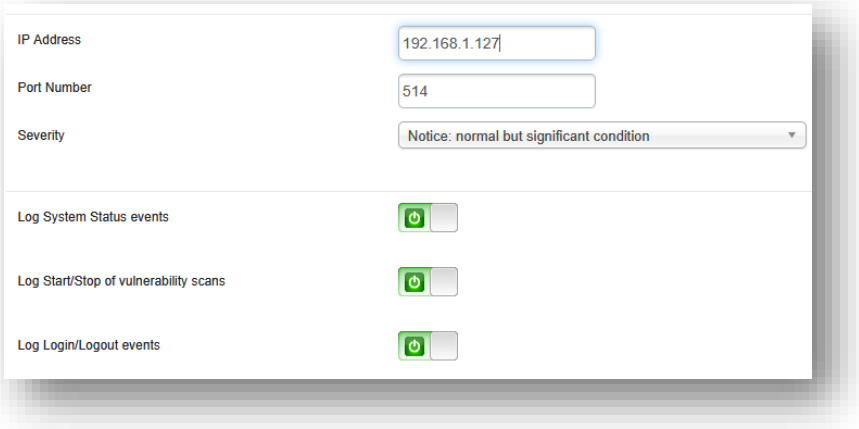
The map displays a single source point from which animated geodesic lines extend to each target being scanned. For ongoing scans, animated geodesic lines with moving red dots travel from the Penetrator's location to each active target. Completed scans are represented by static markers at the target locations with a color that indicates the state of the scan: Completed, Canceled, Target Offline, etc.

To further improve situational awareness, the Penetrator's location is highlighted with an animated visual indicator, while each target under active scanning is emphasized through pulsating markers. The moving red dots that travel along the scan paths move at the same perceived speed, resulting in a realistic visualization regardless of the number of targets being scanned simultaneously.

The logic used to display scan paths is optimized to present a clear view: each scan with multiple targets at the same location is displayed with a single marker.

- **Remote Syslog Improvement**

The remote syslog capability is available under menu System > System Logs, clicking the *Activate Syslog* button. This feature allows administrators to forward system logs to a remote syslog server for centralized log management and long-term retention.



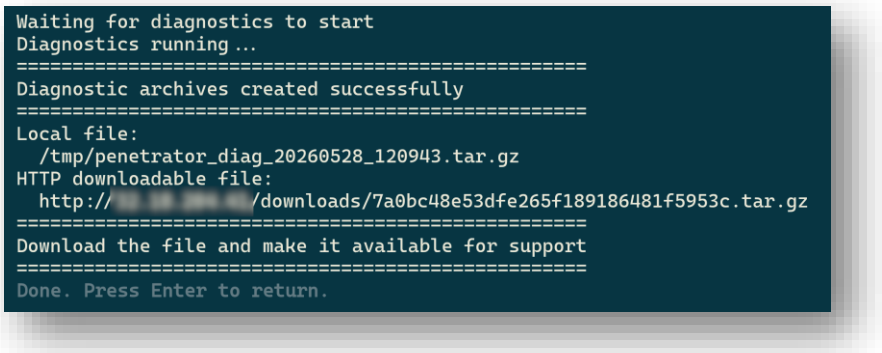
Once activated, administrators can now tune what gets forwarded, by selecting the categories of events to send:

- System events – general system health and operational messages
- Scan events – start and stop of vulnerability scans
- User login/logout events – authentication and session activity

Additionally, a severity threshold can be set so that only events at or above the selected level are forwarded. This helps reduce noise and ensures that only relevant, actionable events are sent to the remote syslog server.

- **Diagnostics Log File**

A new diagnostic tool is now available in the system console under option 26. This option automatically collects the most critical system logs along with key information about the

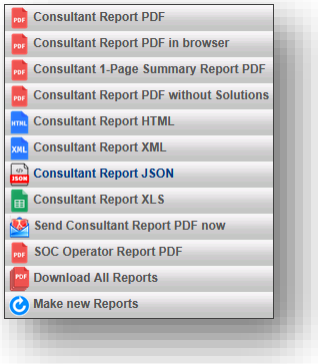


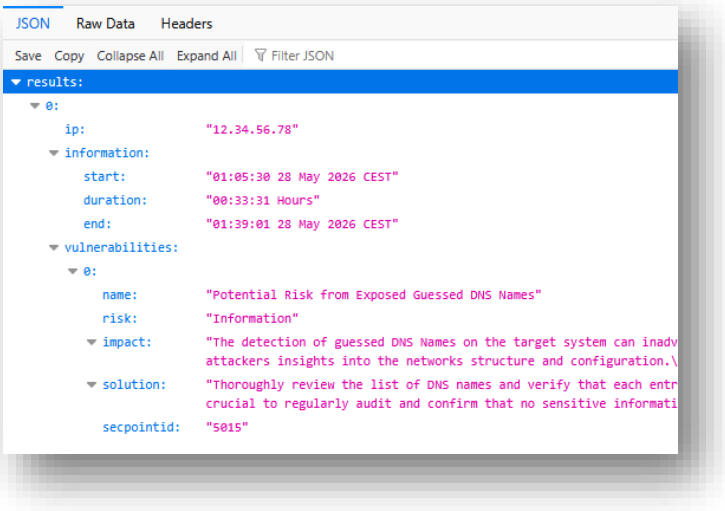
current unit's status and configuration, packages everything into a single compressed file, and generates a local file and a download URL.

This diagnostic bundle is designed to streamline the support process. When contacting technical support, providing this file gives engineers immediate access to all the information needed to diagnose and troubleshoot any potential malfunctions, significantly reducing customer's interaction and resolution time.

- **Report: new JSON format**

Reporting functionality has been extended to provide greater flexibility and audit transparency. A new JSON report format is now available, enabling users to easily integrate findings into internal reporting or compliance workflows.
The new format is available in the floating menu next to the other available report functions.





- **And…**

  - Dark Web Search can be enabled/disabled at user-level
  - Maximum number of Dark Web searches reduced to 2 per day
  - New option to disable the left-side map that shows the Penetrator location

- System status charts are hidden to non-admin users
- Report Notification Sender: email address replaced by description
- Option to choose appliance image and upload a custom image
- Automatic update of vulnerability count on all scans when a vulnerability is added/removed to false positives or downgraded/upgraded.
- Firmware Update: new download always restarts from the beginning, to avoid file corruption
- New option "7 days" added to remote support auto-switch off
- OWASP profile updated to the 2025 version
- Review of profile descriptions, to clearly separate human actions from automated actions
- SPID renamed to "SecPoint ID"
- Better logic for displaying information on the Insights page, to avoid showing occasionally wrong information
- In Insights page, fixed empty space when OS icon is missing
- Review of scan end time and duration displayed on reports when time zone is not the default one
- Some old links to www.secpoint.com have been updated
- Fixed occasional empty vulnerability page for super administrator
- Fixed minor bug in the analysis of completed scans
- Fixed display of right panel on mobile phones
- On vulnerability detail page and on reports, when URLS are on port 80, the protocol is now HTTP instead of HTTPS
- Minor PHP error fix

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