

GSM 35

Datenblatt

Der **Greenbone Security Manager (GSM)** ist eine Schwachstellen-Management-Lösung, die sich nahtlos und transparent in Ihre Sicherheits- und GRC-Strategie integriert und Funktionen zur Schwachstellenanalyse, zur Schwachstellenintelligenz und zum Bedrohungsmanagement bietet. Auch das Aufdecken von Verstößen gegen die Sicherheitsrichtlinien und -vorschriften des Unternehmens wird abgedeckt. Mit einem starken Fokus auf 3rd-Party-Integration und offene Standards ist der GSM eine Best-of-Breed-Sicherheitslösung, die Ihre Sicherheitslage verbessert und ergänzt und einen proaktiven Ansatz für ein automatisiertes Schwachstellen-Lebenszyklus-Management ermöglicht.

Der **GSM 35** arbeitet als Scan-Sensor für GSM ab GSM 400 und deckt bis zu 300 IP-Adressen ab. Die Einsatzfelder sind kleinere Zweigstellen von Unternehmen.



Vorteile

- Schlüsselfertige Lösung: Inbetriebnahme innerhalb von 10 Minuten
- Leistungsstarkes Appliance-Betriebssystem Greenbone OS mit speziell angepasster, konsolenbasierter Administration und aufbauend auf einer umfangreichen Sicherheitskonzeption
- Integrierter Greenbone Security Feed mit über 85.000 Schwachstellen-Tests mit täglicher, automatisierter Aktualisierung
- Integriertes GOS-Upgrade
- Keine Begrenzung bezüglich Anzahl der Zielsysteme bzw. IP-Adressen (erreichbare Anzahl hängt vom Scan-Muster und von den Scan-Zielen ab)
- Flatrate-Subskription umfasst das Platin-Support-Paket, den Greenbone Security Feed und Feature-Updates



Spezifikationen

Maße

430/480 mm (exkl./inkl. Rackmount) x 200 mm x 45 mm

Zertifizierung

- CE
- FCC

Umgebung

- Betriebstemperatur: 0 °C bis 45 °C (32 °F bis 113 °F)
- Lagertemperatur: -20 °C bis 80 °C (-4 °F bis 176 °F)
- Luftfeuchtigkeit: 10 % bis 90 % (nicht kondensierend)

Anschlüsse

- 4 Port GbE 10/100/1000 Base-TX (Kupfer)
- 1 Port für serielle Konsole RS-232
- 2 USB-Ports
- 1 HDMI-Anschluss

Konstruktion

- Kompaktbauweise, stabiles Stahl-Gehäuse
- Rackmount-Kit
- Integriertes Netzteil



Unterstützte Standards

- Netzwerkintegration: SMTP (E-Mail), SNMP, SysLog, LDAP, NTP, DHCP, IPv4/IPv6
- Schwachstellendetektion: CVE, CPE, CVSS, OVAL
- Netzwerkscans: WMI, LDAP, HTTP, SMB, SSH, TCP, UDP usw.
- Richtlinien: IT-Grundschutz, PCI-DSS, TLS-Map usw.



Management über webbasierte Schnittstelle (HTTPS) des Masters

- Management von Scan-Aufgaben mit Notizen und Falsch-Positiv-Meldungen
- Unterstützung des Mehrbenutzer-Betriebs
- Clustering und verteiltes Scanning über Sensor-Betrieb
- Berichtsdurchsicht mit Filterung, Sortierung, Notizen und Risikoeinstufung
- Plugin-Framework für Berichte: XML, PDF usw.
- Performance-Übersicht der Appliance



Integration/API

- Greenbone Management Protocol (GMP), verschlüsselt
- Alle Anwenderfunktionen der Web-Schnittstelle in der API verfügbar
- Leichte Integration mit anderen Applikationen via API
- Einfache Automatisierungen via Kommandozeilen-Tools (CLI)

Administration über Konsolen-Schnittstelle

- Konfiguration der Netzwerkintegration
- Backup, Restore, Snapshot, Factory-Reset, Upgrade

Scan-Applikationen

- Scan-Maschine und -Framework: Greenbone Vulnerability Manager (GVM) mit integriertem Greenbone Security Feed



Ihr Greenbone Security Solutions Partner:

Greenbone Networks GmbH

Neumarkt 12
49074 Osnabrück
Germany

Office: +49-541-760278-0
Fax: +49-541-760278-90
E-Mail: sales@greenbone.net
Web: www.greenbone.net