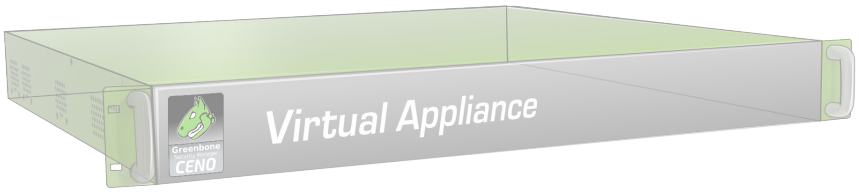
GSM CENO

Datenblatt

Greenbone
Sustainable Resilience

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, Schwachstellenintelligenz und 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 CENO** deckt bis zu 500 IP-Adressen ab. Die Einsatzfelder sind kleinere bis mittlere Unternehmens-IT oder mittlere Zweigstellen.



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 69.900 Schwachstellen-Tests mit täglicher, automatisierter Aktualisierung
- Integriertes GOS-Upgrade
- Integrierter Greenbone Security Assistant als zentrale Web-Schnittstelle
- 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 Platinum-Support-Paket, den Greenbone Security Feed und Feature-Updates

Spezifikationen

Virtual Appliance Format
Die OVA kann in die folgende virtuelle Umgebung importiert werden:
- VMware ESXi

Appliance-Details
- 64 bit Linux OS
- 2 vCPUs
- 8 GB RAM
- 32 GB HDD Storage

Anschlüsse
- 4 vir. Ethernet-Ports

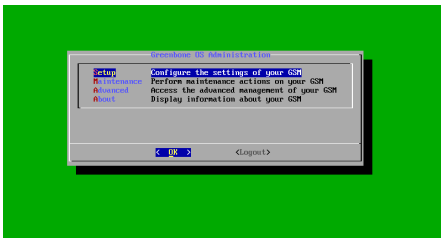
Lösungsumfang
- Virtuelle Appliance
- 1, 3 oder 5 Jahre Anspruch auf den Greenbone Platinum Support

GSM CENO

Datenblatt

Unterstützte Standards
- Netzwerkintegration: SMTPS (Email), LDAP, RADIUS, DHCP, IPv4/IPv6
- Schwachstellenerkennung: CVE, CPE, CVSS, OVAL
- Netzwerkscans: WMI, LDAP, HTTP, SMB, SSH, TCP, UDP usw.
- Richtlinien: IT-Grundschutz, PCI-DSS, ISO 27001

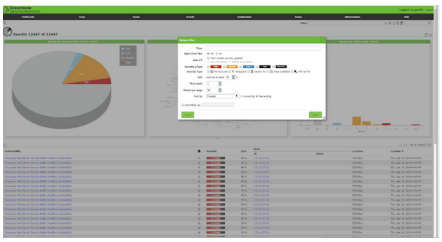
Webbasierte Schnittstelle (HTTPS)
- Scan-Aufgabenverwaltung mit Notizen und false-positive Markierung
- Mehrbenutzer-Unterstützung
- Gebündeltes und verteiltes Scanning über den Sensormodus
- Berichtdurchsicht durch Filterung, Sortierung, Notizen und Risikoeinstufung
- Plugin-Framework für Berichte: XML, PDF usw.
- Performance-Übersicht der Appliance



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

Administration über Konsolen-Schnittstelle
- Netzwerkintegration und -konfiguration
- Upgrade

Scan-Applikationen
- Scan Engine und Framework: Greenbone Vulnerability Manager (GVM) mit integriertem Greenbone Security Feed (GSF)



Ihre Greenbone Security Solutions Partner:

Communication Systems GmbH
Frankfurter Str. 233 | Triforum Eingang C1
63263 Neu-Isenburg
T: +49 6102 7840 0

Am Gierath 20A
40885 Ratingen
T: +49 2102 5789 800

www.com-sys.de | info@com-sys.de

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück
Germany

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

20190701