TENABLE Network Security®

Product Features and Technical Specifications

SecurityCenter

Tenable's SecurityCenter enables real-time scanning, log analysis, compliance auditing and security monitoring.

SecurityCenter Features

Alerting Actions
- Create ticket
- Email one or more users
- In-system event notification
- Launch existing Nessus scan
- Send syslog

Alerting Logic
- Greater than, less than, equal and not equal for any query
- Independent policy alerting schedules
- Event IP count queries
- Event Count queries
- Event Port count queries
- Vulnerability IP count queries
- Vulnerability Count queries
- Vulnerability Port count queries

Asset Discovery and Filtering
- IP address watch lists
- Nessus scan results
- PVS discovered nodes
- LCE IP address queries
- Manual IP list upload
- API IP list upload
- Regular Expressions
- Classification by OS
- Classification by App
- Classification by Domain
- DNS and Name patterns

SecurityCenter
Supported Installation Platforms
- RedHat 4 and 5
- CentOS 4 and 5
- 64 bit support for RedHat and CentOS 5
- Tenable Virtual Appliance
- Tenable Hardware Appliance

Configuration Audit Policy Management
- Upload new .audit polices
- Associate .audit policies with scan policies
- Share audit polices with organization

Console Login Authentication
- TNS local authentication (username/passwords)
- LDAP authentication
- Enforce custom login banners

Credential Management for Scanning
- Role based access to stored credentials
- Kerberose
- SNMP
- SSH
- SU/SUDO
- Telnet
- Windows Domain
- Web Authentication

Dashboard Data Sources
- Vulnerabilities
- Missing Patches
- Configuration Information
- Any Log Events
- User Activity
- Network Activity

Dashboard Graph Types
- Tabbed interface of multiple dashboards
- Bar charts
- Pie Charts
- Single and multiple trend lines
- Tables

Data Analysis Output
- Export results as CSV
- Save matching IP addresses as Asset List
- Open ticket for matching IP addresses
- Save filter as query for re-use

Data Filtering Options
- IP addresses
- Ports
- Protocols
- Event type and name
- Asset
- User
- Date or time range
- Inbound, outbound, external events
- Plugin family
- Scan Policy
- Plugin ID
- Severity
- Active, Passive or Compliance plugins
- Matching text searches
- Days since vulnerability was observed
- Days since vulnerability was found
- Reoccurring vulnerabilities
- Re-casted severity adjustments
- Risk Accepted vulnerabilities
- Specific SecurityCenter repository

Data Management
- Scan results stored in separate repositories
- Repository sharing with multiple Security Centers
- Manual Nessus scan result uploads
- SC4 API for automatic data queries
- CSV data exports
- Full saved log search results text download
- Individual scan results saved for retention and download

Detailed Event and Vulnerability Analysis Tools
- Asset summary
- Event and Type Summary
- Plugin family summary
- Protocol Summary
- List each unique OS

(continued)

TENABLE Network Security®

SecurityCenter Product Features And Technical Specifications

Detailed Event and Vulnerability Analysis Tools (continued)

- List Each event
- Summarize Events by Date
- Summarize Events by Sensor
- Summarize Events by User
- Severity Summary
- Summary by Class C Addresses
- Summary by Class B Addresses
- Summary by Class A Addresses
- Summary By IP Address
- Summary by Port
- Vulnerability Summary
- Detailed Syslog display
- Detailed vulnerability details
- Trend matching events

Distributed Scanner Support

- Push latest plugins to remote scanners
- Support for up to 512 Nessus scanners
- External and internal Nessus deployment
- Grouping of Nessus scanners into zones
- Load balanced scans across multiple scanners
- Multiple Passive Vulnerability Scanners

Log Search

- Boolean logic to search logs
- Search limited to specific dates
- Saved searches can be re-launched
- Distributed searches with multiple LCEs

Licensing

- Licensed by active nodes with vulnerability
- No need to tell Tenable your IP addresses
- Unlimited discovery scans
- Upgrades for increased IP counts easily procured and added to production systems
- Includes up to 512 Nessus scanners
- PVS and LCE purchased separately

Report Chapter Types

- Custom paragraph
- Tables
- Pie chart
- Bar chart
- Single and multiple trend lines

Report Filter Options

- Vulnerability Discovery Date
- Last seen vulnerability date
- Asset based report filtering
- Nessus plugin family
- Port, protocol and IP address
- Events by user
- Normalized and true IDS event names
- Vulnerability correlated IDS events

Report Template Types

- CIS
- FISMA
- FDCC
- Common IT Audits
- Common Network Monitoring Reports
- OWASP 2010
- SANS CAG
- PCI
- Missing Patches
- Nessus Plugin Families

Report Output Formats

- PDF
- Password protected PDF
- Watermark for PDF reports
- RTF
- CSV
- 3D Visualization
- Log search text results
- Footer, Header & Table of Contents management
- Multiple landscape and letter layouts

Scan Policy Management and Schedules

- Daily, weekly, monthly & yearly
- Support for any Nessus scan preference
- Separate scan scheduled per asset
- Independent credentials used for scans
- Dozens of default scan polices
- Email notification of scan results
- Scan schedule copying
- Launch, pause and stop buttons for scans

Scan Types

- Nessus network vulnerability scans
- Nessus credentialed patch audits
- Nessus credentialed configuration audits
- Nessus web application audits

Scheduled Actions

- Automatic compliance alerts
- Nessus vulnerability, patch and config scans
- Automatic Dashboard updates
- Report creation with optional email delivery
- Nessus and PVS plugin update and distribution
- Dynamic asset list creation

Ticketing

- Automatic creation based on policy alerting
- Manual creation based on vulnerability analysis
- Manual creation based on log/event analysis
- Association of security data with ticket

User Access Control

- Organizational resource sharing
- Role-based user creation
- Custom role profile creation
- Scan policy sharing
- Access limited to authorized assets
- User grouped into organizations
- Logging of user actions

Part# SCTJ11-001