tenable
network security

Audits de sécurité, supervision en continu

Renaud Deraison

Bio (en deux phrases)

Auteur du logiciel “Nessus” (1998 -)

Co-fondateur de Tenable Network Security, Inc. (Maryland, 2002 -)

tenable
network security

Tenable

La société

- Fondée en 2002
- 280 employés
- Etats-Unis, UK, Asie

Les produits

Gestion de vulnérabilités et conformité

Nessus: standard

Mobile, Cloud, VMs

Monitoring des réseaux les plus complexes

La communauté

- Un million d'utilisateurs de Nessus
- 18,000 clients

tenable network security

Notre vision

- Monitoring en continu
  - Savoir ce qui est sur mon réseau
  - Savoir ce qui est une cible facile (attaque directe, phishing, APT, etc…)
  - Pouvoir prouver à un tiers que ma surface d'attaque est réduite
  - Etre en mesure de faire des analyses forensics

Federal Information Security Management Act

- NIST 800-53
- DOD 8500.2
- Exemples:
  - AC-1 Access Control
  - AC-18 Wireless Access
  - AU-18 Timestamps
  - CM-1 Config Management
  - CM-2 Config Baselines
  - CM-4 Config Changes
  - IA-2 User Identification
  - RA-5 Vuln Scanning
  - SA-6 Software Usage
  - SC-7 Boundary Protection
  - SI-3 Malicious Code

La première version de la loi oblige les agences gouvernementales US à développer, documenter et implémenter des programmes pour protéger la confidentialité, l'intégrité et la disponibilité de leur parc IT.

tenable network security

CyberScope, en 2013

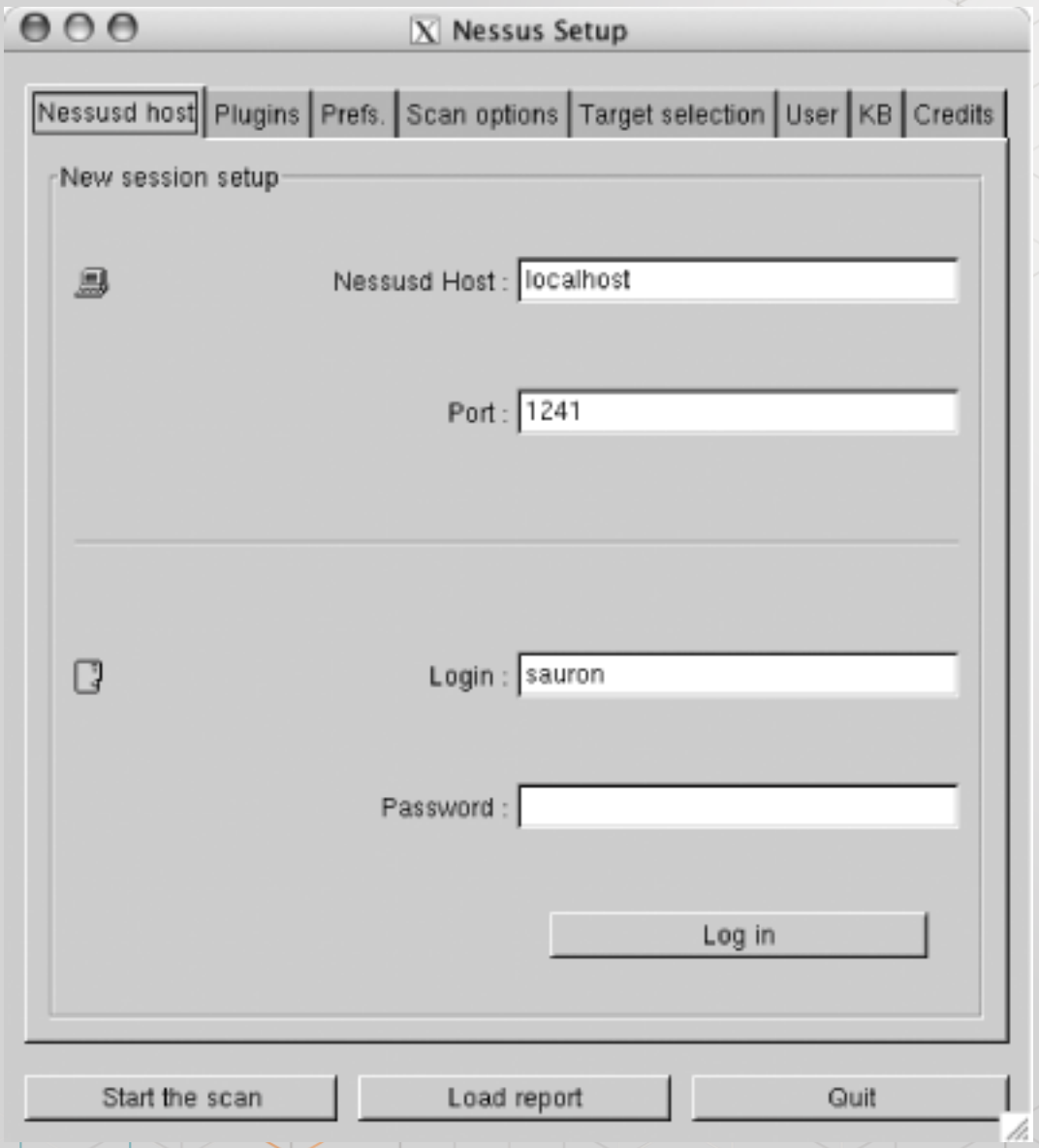
- Les organisations gouv. US doivent envoyer un rapport **tous les 30 jours:**
  - Liste des systèmes
  - Liste des:
    - Vulnerabilités
    - Conformité
    - Types de plateformes
- Format de rapport XML, “LASR”, uploadé sur le portail de DHS

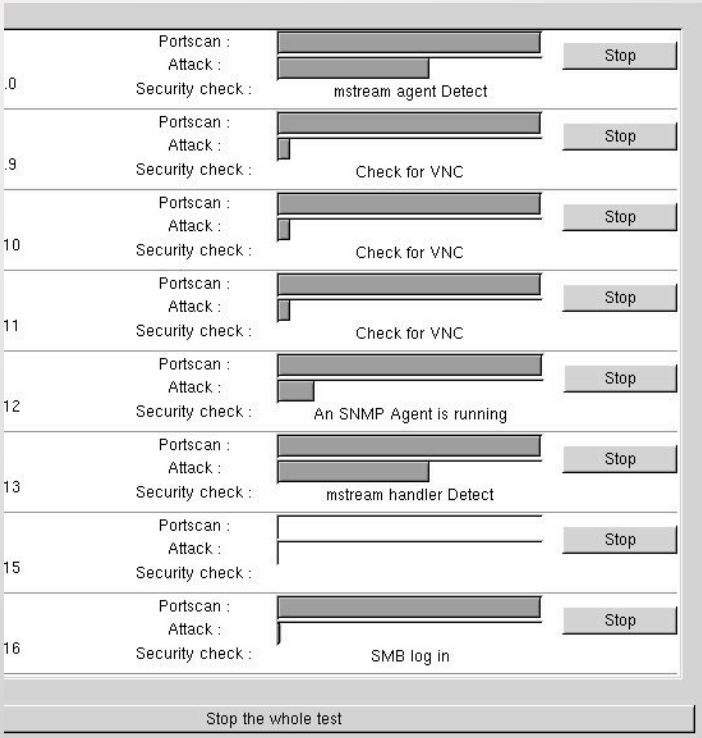
tenable network security

Nessus®

vulnerability scanner

tenable
network security



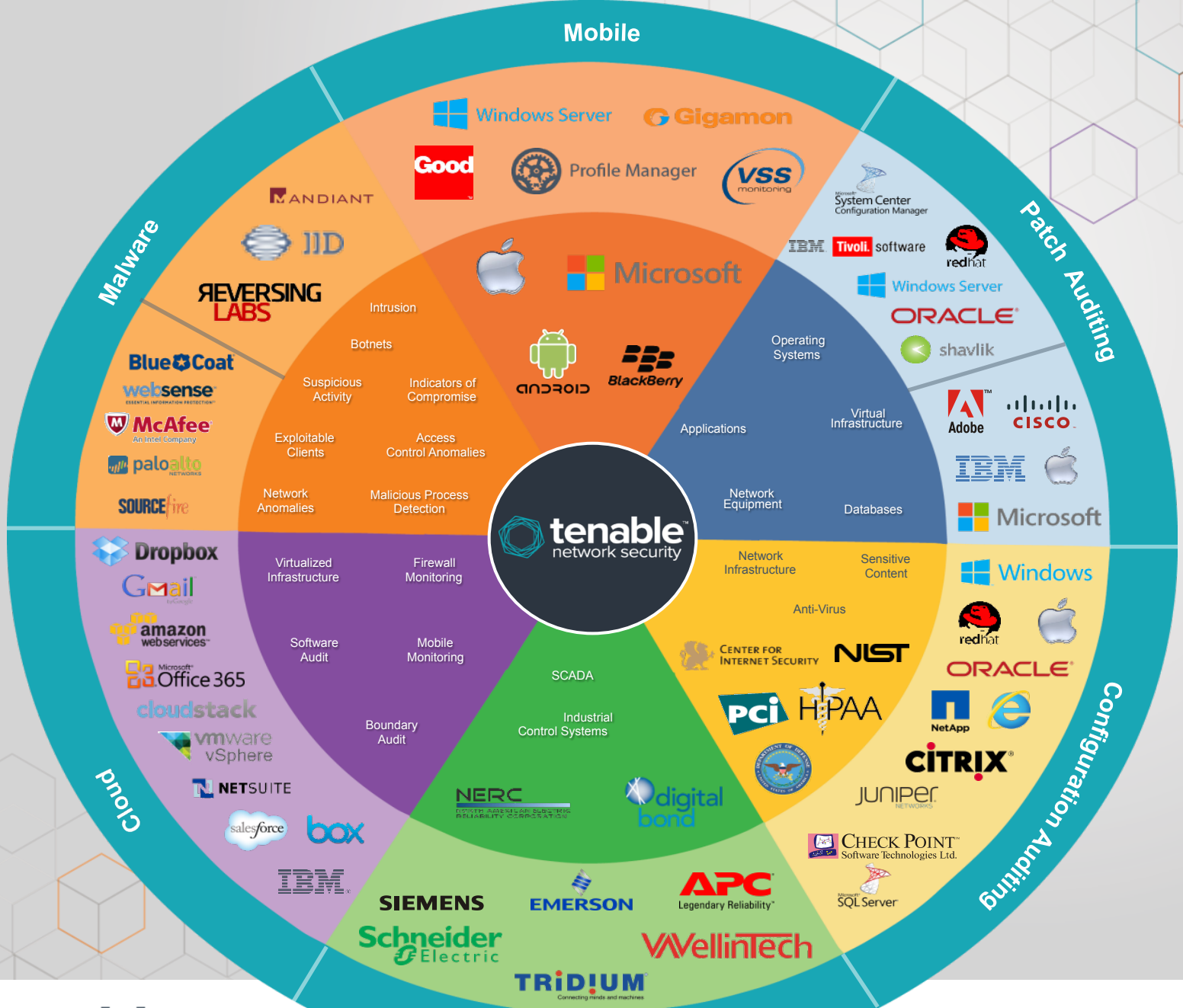


tenable network security

Nessus

- Scanner “actif” de sécurité
- Version actuelle: 5.2

- But: pouvoir faire le meilleur audit possible quel que soit l’environnement en place
  - Qu’est ce qui est sur mon réseau?
  - Qu’est ce qui est vulnérable sur mon réseau?
  - Qu’est ce qui est différent sur mon réseau?



tenable network security

Audit en mode boite noire

- Usage historique
- Detection de services à distance
- Identification de mauvaises configurations (sécurité) et de patches manquants
- Configuration minimale requise

Audit en mode boite blanche

- Fournir les mdps réseaux à Nessus
- Audit local de chaque système:
  - Enumeration de correctifs de sécurité manquants
  - Gain de temps, désengorgement réseau (pas de scan de ports)
  - Auditer non seulement l'OS, mais les applis tierces (ie: Anti-Virus)


redhat


Windows 8


solaris


AIX


ORACLE


JUNOS


Mac OS X


hp UX


MySQL


Microsoft
SQL Server
2008


CentOS
CentOS 5


vmware


amazon
web services


McAfee


CISCO


Check Point
SOFTWARE TECHNOLOGIES LTD.


IBM iSeries

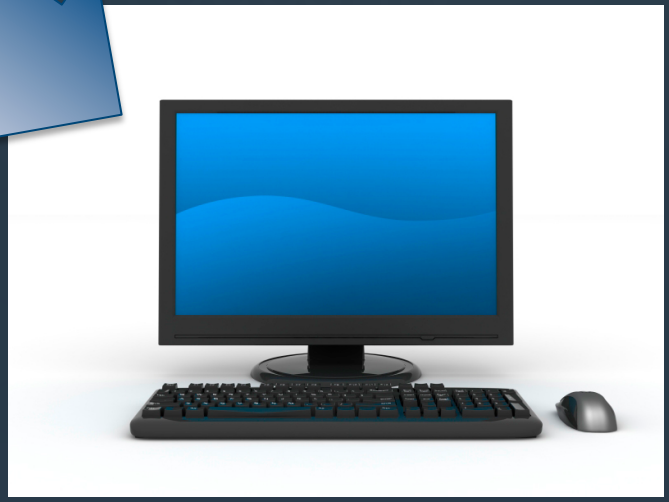

Microsoft Office
SharePoint


TREND
MICRO

Audit en mode “mixte”

- Nessus peut s’interfacer avec votre gestionnaire de patches (SCCM, TEM, WSUS, Red Hat Satellite, Spacewalk)
- Permet d’auditer localement des machines, sans mot de passe
- Avec mdp: permet de confronter les résultats du gestionnaire de patches à ceux de Nessus

Nessus®
vulnerability scanner



tenable
network security

Nessus®
vulnerability scanner

BIGFIX®

Microsoft®
System Center
Configuration Manager

redhat
RED HAT NETWORK
SATELLITE 5.5

tenable
network security

Plugin ID: 58186 **Port / Service:** general/tcp **Severity:** Info

Plugin Name: Patch Management: SCCM Report

Synopsis: This plugin reports a list of missing updates with information or the plugin will report if system is not managed by SCCM.

Description

This plugin parses th
scanned is managed
system. This plugin w
which can be viewed

Solution

n/a

Risk Factor: None

Plugin Output

+ System Information

- ipaddresses : 172.26.22.35, fe80::ddef:8d2
- Netbios name : RE-TEM
- Computer name : NULL
- Domain : TENABLERELAB
- OS : Microsoft Windows NT Advanced Serv
- Caption : Microsoft. Windows Server. 2008

Plugin Output

This system is not managed by Tivoli Endpoint Manager.

Plugin Output

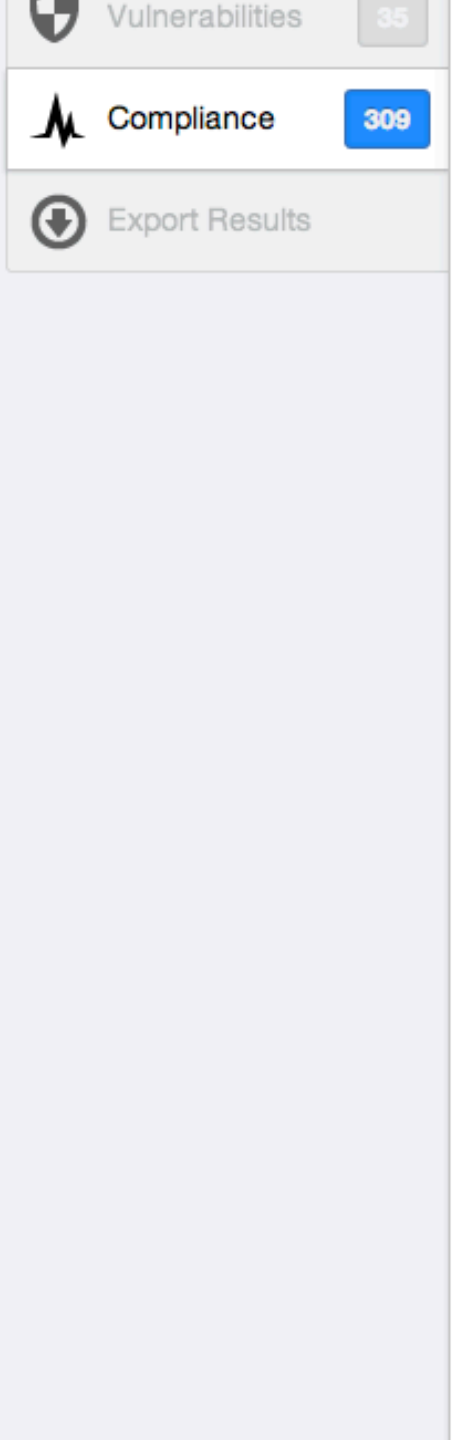
+ The following patch management products report :
- IBM TEM : Vulnerable
- SCCM is NOT reporting vulnerable
- WSUS is NOT reporting vulnerable

- C:\Windows\System32\netapi32.dll has not been patched
Remote version : 6.0.6002.18005
Should be : 6.0.6002.18659

tenable network security

Audit de conformité

- Vérifier que la configuration de la machine est conforme à ce que j'en attends
- Support Windows, Linux, AIX, HP/UX, Solaris, mais aussi Cisco, Juniper, Vmware, Hyper-V, MSSQL, Oracle DB, Apache, etc…
- Tenable fournit des examples d'audits, basés sur CIS (Center for Internet Security), PCI, SANS 20 Critical Controls, etc…



failed	RHEL-06-000505 - OS must conduct backups of system-level	Unix Compliance Checks
failed	RHEL-06-000507 - OS must display to the user the date and ti...	Unix Compliance Checks
failed	RHEL-06-000509 - The system must forward audit records to	Unix Compliance Checks
failed	RHEL-06-000510 - The audit system must take appropriate acti...	Unix Compliance Checks
failed	RHEL-06-000511 - The audit system must take appropriate acti...	Unix Compliance Checks
failed	RHEL-06-000516 - Package management tool must verify	Unix Compliance Checks
failed	RHEL-06-000517 - Package management tool must verify group-	Unix Compliance Checks
failed	RHEL-06-000518 - Package management tool must verify	Unix Compliance Checks
failed	RHEL-06-000521 - The mail system must forward all mail for r...	Unix Compliance Checks
failed	RHEL-06-000523 - Local IPv6 firewall must implement a deny-a...	Unix Compliance Checks
failed	RHEL-06-000524 - The system must provide automated support	Unix Compliance Checks
failed	RHEL-06-000525 - Auditing must be enabled at boot by setting...	Unix Compliance Checks
passed	RHEL-06-000009 - rhnsd service must not be running, unless u...	Unix Compliance Checks
passed	RHEL-06-000013/RHEL-06-000015 - tool must cryptographically	Unix Compliance Checks
passed	RHEL-06-000019 - There must be no .rhosts or hosts.equiv fil...	Unix Compliance Checks

Malware

- Audit d'antivirus (Symantec, Trend, etc…)
- Detection de malware connus tournant sous Windows
- Identification de machines connues pour appartenir à un Botnet
- Identification de processus uniques (13 Oct)
- Collecte d'information permettant une analyse post-mortem (13 Oct)

Plugin Output

172.20.5.18 1

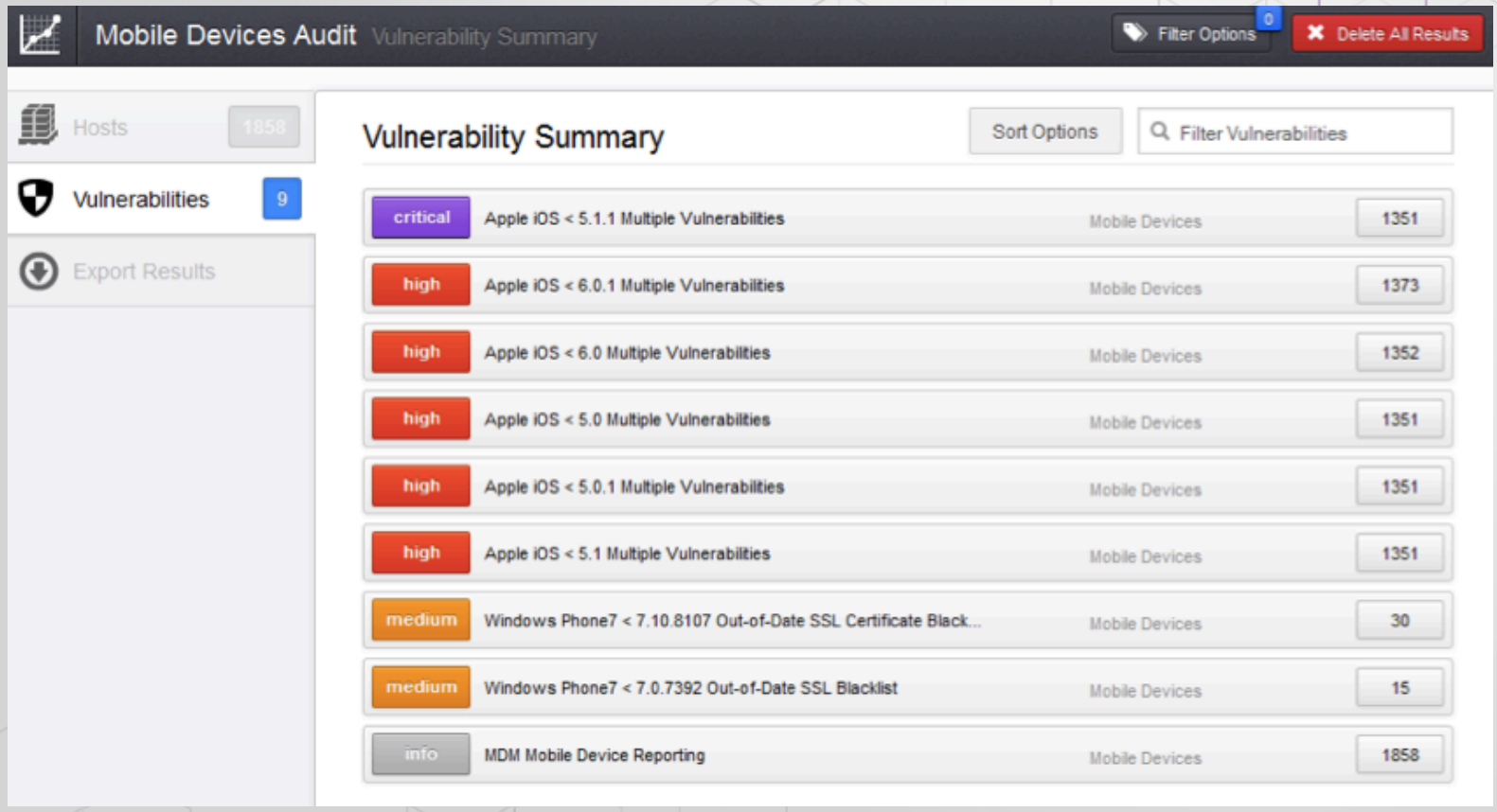
445 / tcp

Service: cifs

```
3D2003FEEEC75B7A7CA7E889553F61F1 matches a known malware md5sum.

File Path                          :
C:\Users\Administrator\AppData\Local\Temp\2\Rar$EX77.176\WinArpAttacker.exe
Associated PID(s) during check     : 2960

The following are some of the tested AntiVirus products that consider this
executable to be malware:
Avast
BitDefender
ClamAV
DrWeb
EsetNOD32
Fortinet
F-Prot
McAfee
Microsoft
Panda
Sophos
Symantec
TrendMicro

Number of AVs reporting malware    : 21

Number of AVs tested               : 25

For more information visit
https://malwaredb.nessus.org/malware/4a6cd2168cb074a4fa82fa0c0143b9d4
```

BYOD

- Identification des mobiles / tablettes via Exchange (ActiveSync)…
- .. et MDM (Apple Profile Manager, GOOD for Enterprise, et bientôt Tivoli, Mobile Iron et Airwatch)
- Qui utilise un mobile sur mon réseau? (ou accède aux ressources de l'entreprise)
- Quels mobiles ne sont pas gérés par mon MDM?
- Ces mobiles sont-ils à jour?



tenable
network security

Nessus – le produit

Interface web (html5) integrée avec gestion des résultats

- Moteur performant
- Analyse “intelligente” des résultats
- Sécurité: fichiers chiffrés, language sécurisé, etc…
- “Chantier” en cours: simplification de l’interface et des configurations (Nov.)
- $1500/an, nombre d’IP illimité

Web Sweep2 Vulnerability Summary

Filter Options 0

This result set contains 1 note. Please click this notification dialog for more information.

- Hosts 16
- Vulnerabilities 71
- Export Results

Vulnerability Summary

Sort Options

high	Microsoft Windows SMB Shares Unprivileged Access	Windo
medium	SSL Certificate Cannot Be Trusted	Gener
medium	SSL Self-Signed Certificate	Gener
medium	SMB Signing Disabled	Misc
medium	SSL Certificate Expiry	Gener
medium	SSL Certificate Signed using Weak Hashing Algorithm	Gener
medium	Terminal Services Doesn't Use Network Level Authentication (...	Misc
medium	Terminal Services Encryption Level is Medium or Low	Misc
medium	Mac OS X 10.7 / 10.8 Unauthorized File Access (remote check)	

PVS

passive
vulnerability
scanner™

tenable
network security

PVS

- Scan avec Nessus: vision “exhaustive” mais à un instant t donné ;
- Que se passe-t-il entre deux scans?
- Que se passe-t-il sur les réseaux que je n’ai pas le droit de scanner?

PVS

- Scanner “passif”
  - Sniffe les connexions
  - En déduit des failles (ie: Chrome 24 utilisé contre Apache 1.3.26)
  - Identification des protocoles
  - Identification des applications utilisées sur chaque machine
  - Temps réel

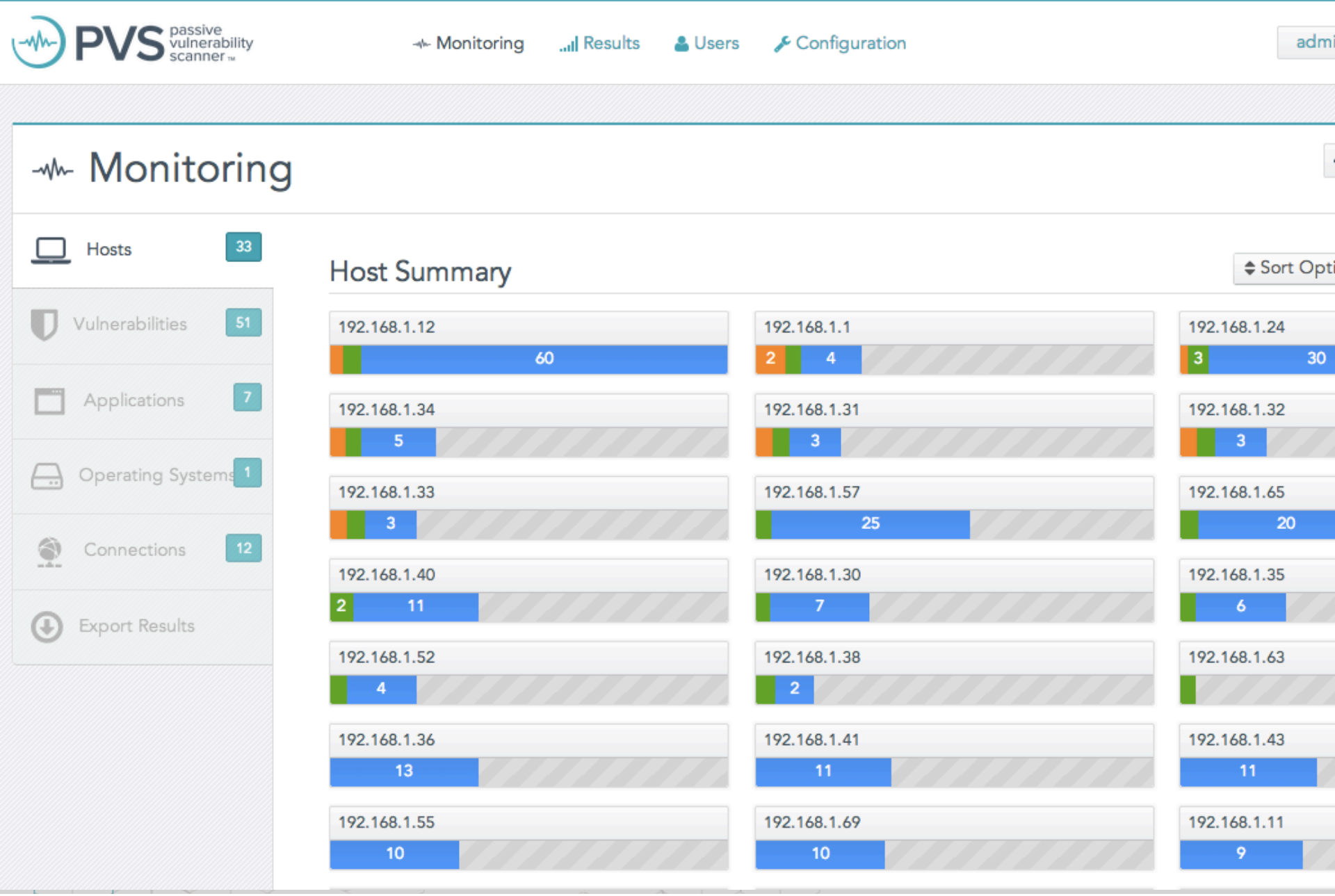
PVS: BYOD

- Quels équipements mobiles non-autorisés utilisent mon infrastructure pour sortir sur internet?
- Sont-ils à jour?
- Identification d'app iPhone/Android

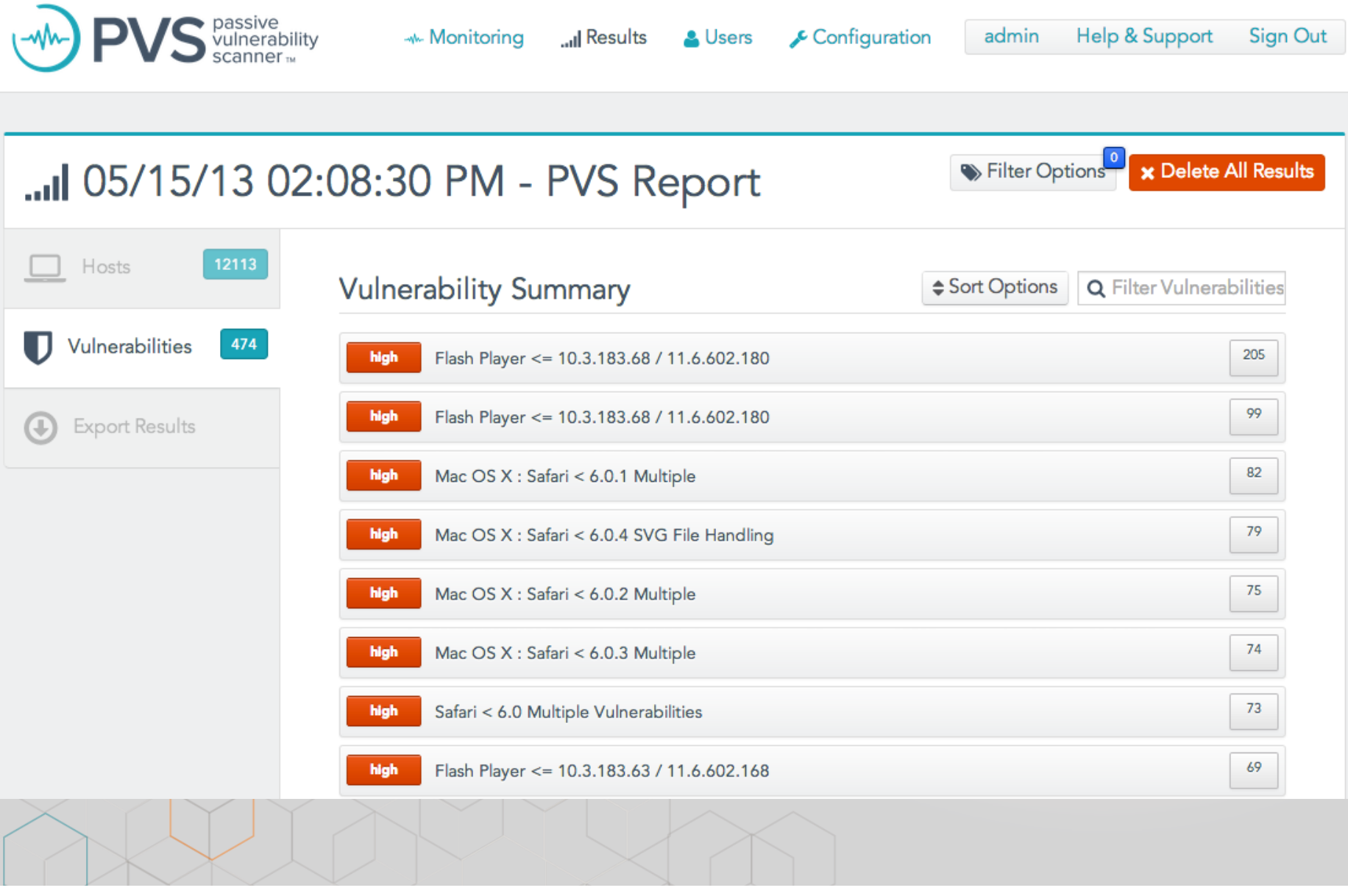
PVS

- PVS n’est pas un IDS
  - Pas de détection d’attaque, mais de présence de vulnérabilités

- PVS peut générer des syslogs permettant de palier à un manque de monitoring (ex: lookups DNS des clients, accès web, etc…)



tenable network security



tenable network security

PVS

- Interface web (html5)
- Rapports chiffrés
- Déploiement facile
- Windows, Linux (RHEL)
- $1800/an, IP illimité

tenable
network security

LCE log correlation engine ™

tenable network security

LCE (Log Correlation Engine)

- Agrégration de logs
- Corrélation
- But: donner du contexte à une machine auditée
  - Que fait-elle sur le réseau?
  - Quels évenements système ont été générés?

LCE: Aggrégation, normalisation de logs

Normalisation de logs de centaines de produits (Unix, Windows, etc…)

Agents (Windows, Linux, Mac OS X) permettant la collecte d'informations locale (process accounting, logs locaux, monitoring de fichiers, détection de malware dans la table des processus)

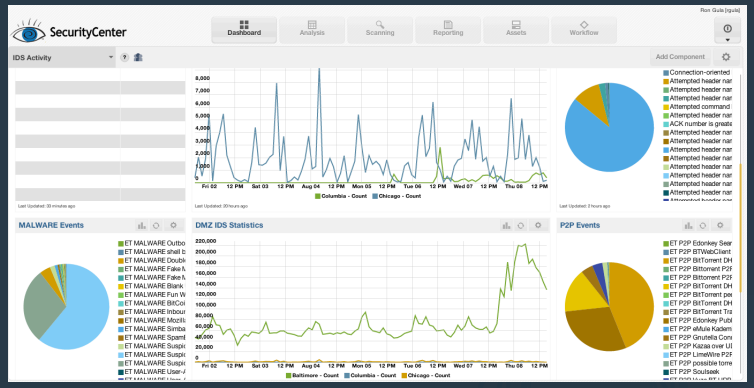
LCE: Corrélation de logs

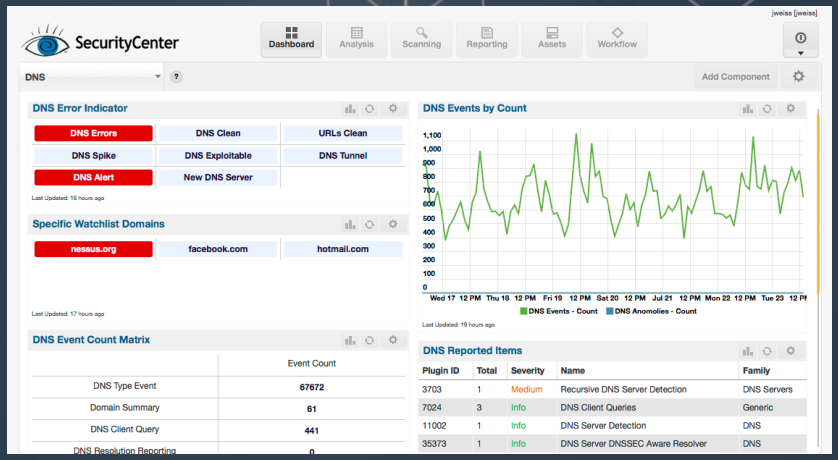
- Language de script permettant de créer des scénarios plus ou moins complexes
- Analyse statistique (client devenant serveur, pic d'évenements nouveaux, etc…)

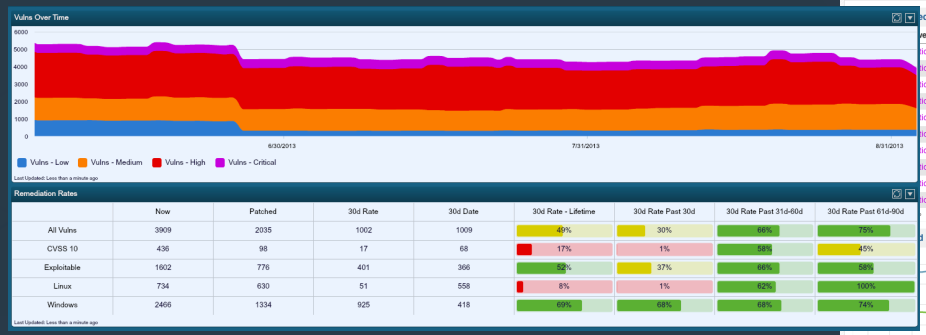
LCE: Audit de vulnérabilité

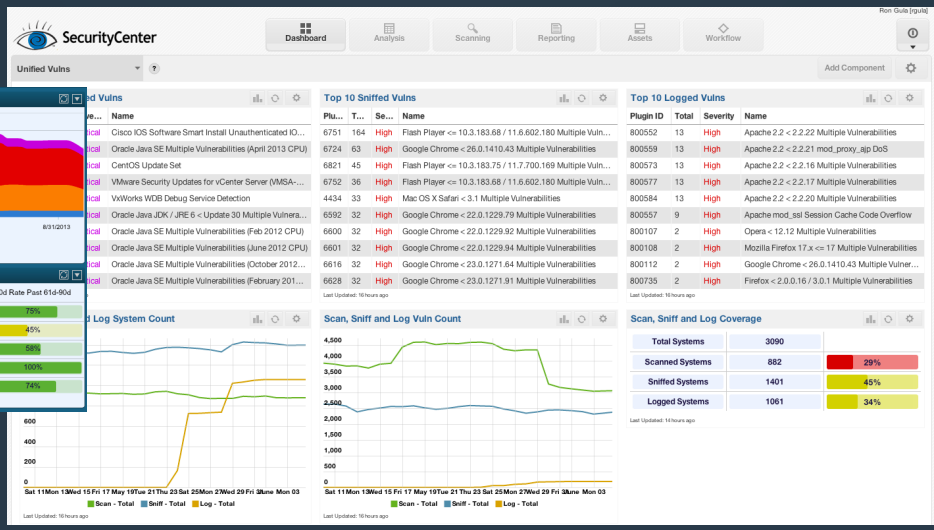
- Détection de failles à partir des logs
  - `Jun 11 18:47:03 macbookair.local ReportCrash[2880]: Saved crash report for airportd[2715] **version 840.22.1** to /Library/Logs/DiagnosticReports/airportd_2013-06-11-184703_macbookair.crash`
  - `/var/log/anaconda.log:10:57:42 DEBUG : Adding Package **libtermcap-2.0.8-46.1.x86_64** in mode u`

SecurityCenter™









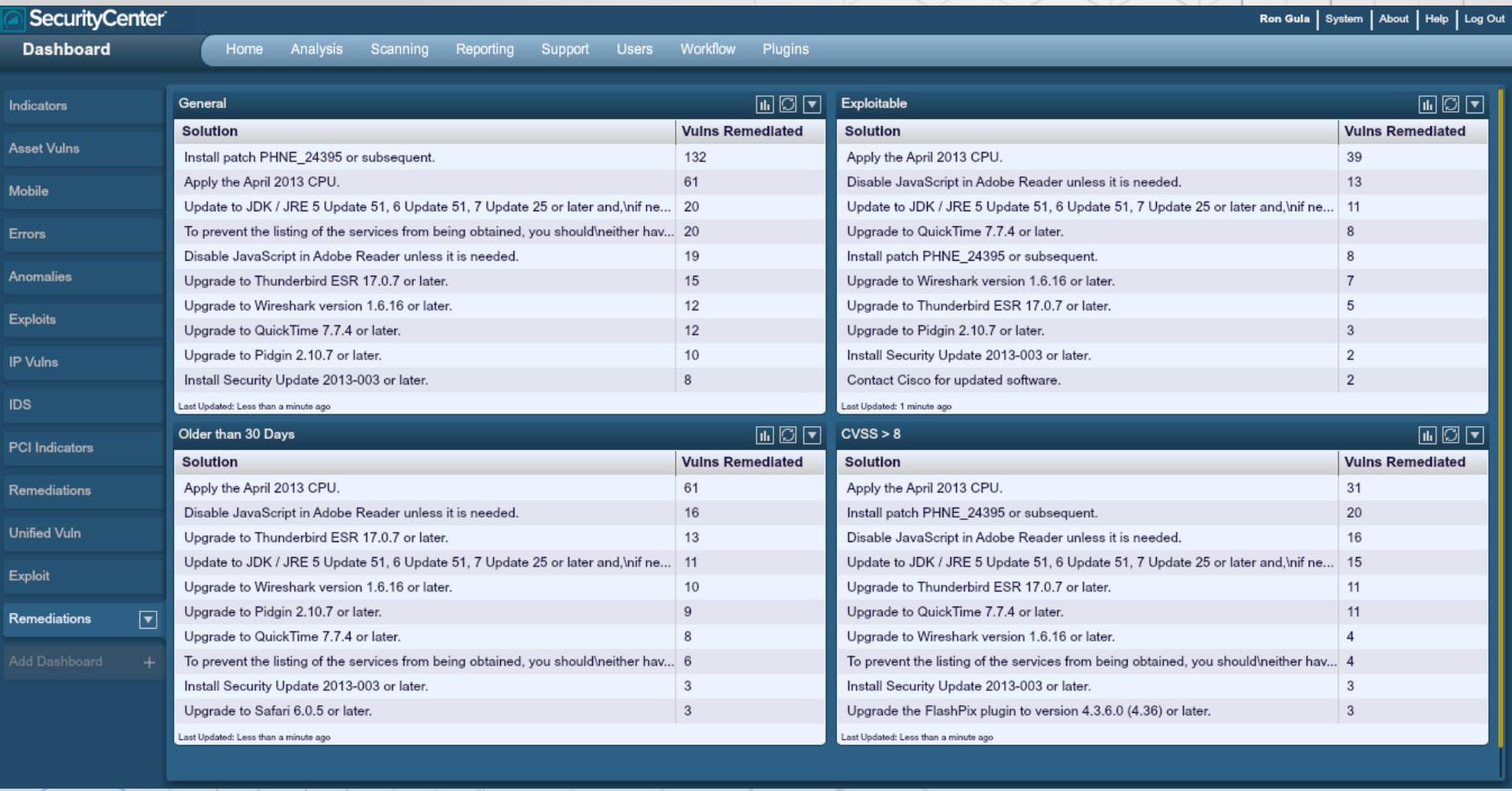
SecurityCenter

- Console de gestion de plusieurs scanners Nessus, PVS, LCE
- Permet de centraliser les audits
- Une base unique de résultats
- Roles, ACL pour chaque utilisateur

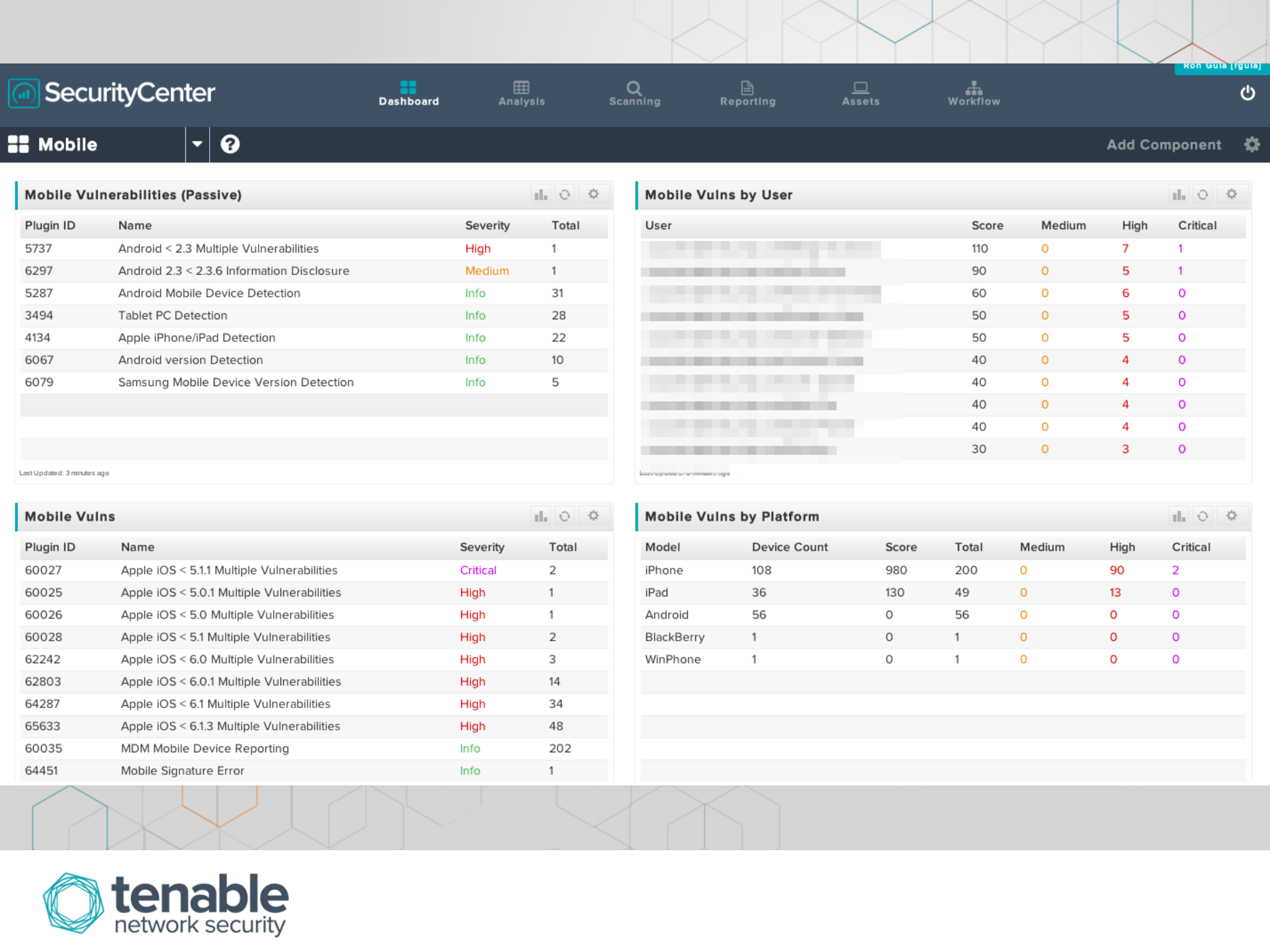
Remediation Summary Edit Filters Save Query

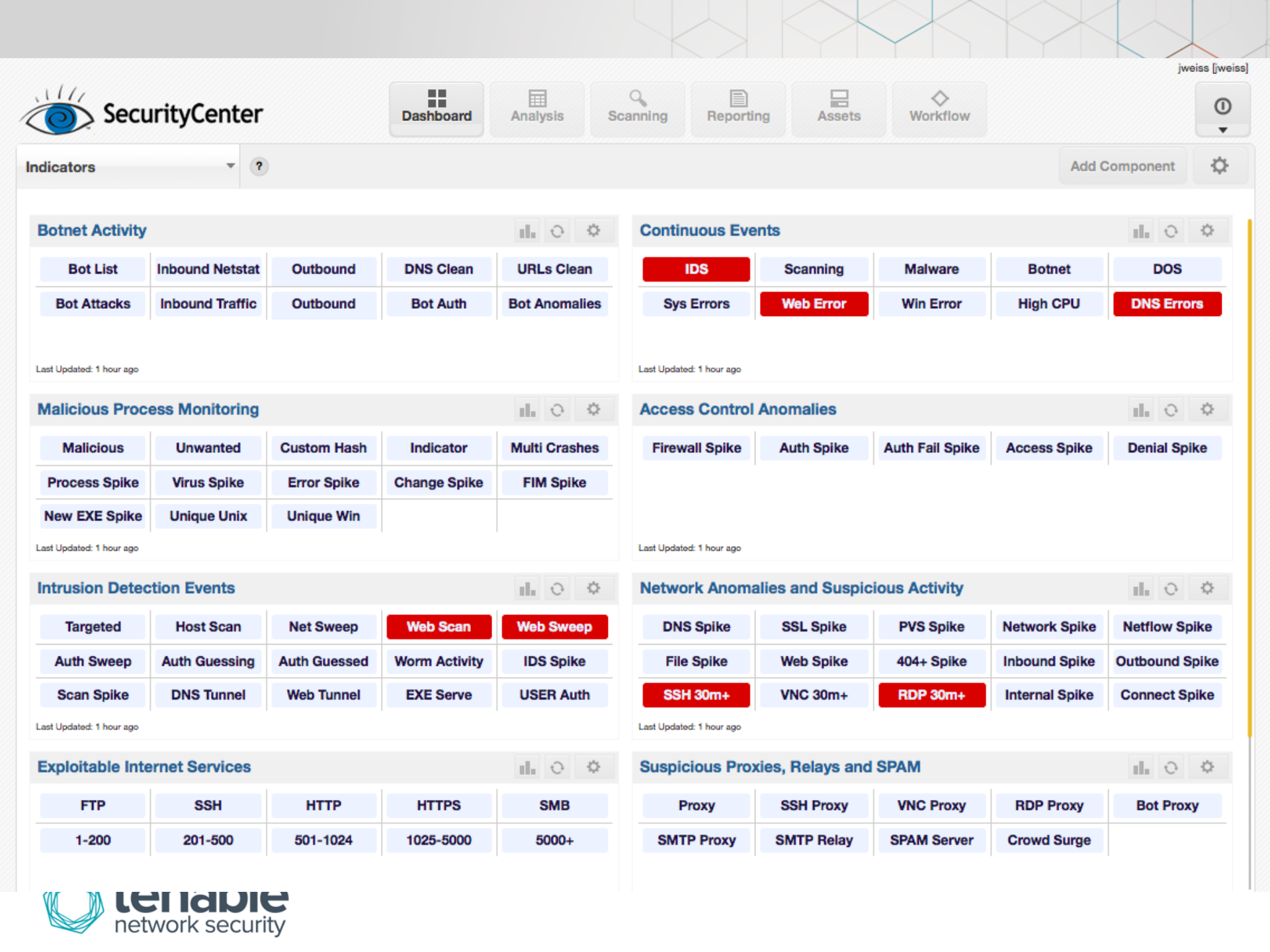
Viewing results 1 - 27 out of 47

Solution	Risk Re... ▼	Hosts Affe...	Vulns	CVEs
Update to JDK / JRE 5 Update 51, 6 Update 51, 7 Update 25 or later and, if necessary, remov...	35.55%	1	11	175
Update to JDK / JRE 5 Update 51, 6 Update 51, 7 Update 25 or later and, if necessary, remov...	26.28%	1	5	139
Upgrade to Adobe AIR 3.8.0.1430 or later.	17.00%	1	12	89
Install Security Update 2013-004 or later.	6.18%	4	12	28
Upgrade to Sophos Anti-Virus version 10.0.9 / 10.2.1 or later.	6.18%	1	1	0
Upgrade to Adobe Flash Player version 11.7.700.242 / 11.8.800.168 or later, or Google Chrom...	1.55%	6	7	4
Upgrade to Adobe Reader 11.0.4 / 10.1.8 or later.	1.55%	2	4	8
Update the affected kernel packages.	0.46%	1	1	6



tenable network security


SecurityCenter
Dashboard
Analysis
Scanning
Reporting
Assets
Workflow
Mobile
Add Component
Mobile Vulnerabilities (Passive)
Plugin ID Name Severity Total
5737 Android < 2.3 Multiple Vulnerabilities High 1
6297 Android 2.3 < 2.3.6 Information Disclosure Medium 1
5287 Android Mobile Device Detection Info 31
3494 Tablet PC Detection Info 28
4134 Apple iPhone/iPad Detection Info 22
6067 Android version Detection Info 10
6079 Samsung Mobile Device Version Detection Info 5
Last Updated: 3 minutes ago
Mobile Vulns by User
User Score Medium High Critical
110 0 7 1
90 0 5 1
60 0 6 0
50 0 5 0
50 0 5 0
40 0 4 0
40 0 4 0
40 0 4 0
40 0 4 0
30 0 3 0
Mobile Vulns
Plugin ID Name Severity Total
60027 Apple iOS < 5.1.1 Multiple Vulnerabilities Critical 2
60025 Apple iOS < 5.0.1 Multiple Vulnerabilities High 1
60026 Apple iOS < 5.0 Multiple Vulnerabilities High 1
60028 Apple iOS < 5.1 Multiple Vulnerabilities High 2
62242 Apple iOS < 6.0 Multiple Vulnerabilities High 3
62803 Apple iOS < 6.0.1 Multiple Vulnerabilities High 14
64287 Apple iOS < 6.1 Multiple Vulnerabilities High 34
65633 Apple iOS < 6.1.3 Multiple Vulnerabilities High 48
60035 MDM Mobile Device Reporting Info 202
64451 Mobile Signature Error Info 1
Mobile Vulns by Platform
Model Device Count Score Total Medium High Critical
iPhone 108 980 200 0 90 2
iPad 36 130 49 0 13 0
Android 56 0 56 0 0 0
BlackBerry 1 0 1 0 0 0
WinPhone 1 0 1 0 0 0
tenable
network security


jweiss [jweiss]
SecurityCenter
Dashboard
Analysis
Scanning
Reporting
Assets
Workflow
Indicators
Add Component
Botnet Activity
Bot List
Inbound Netstat
Outbound
DNS Clean
URLs Clean
Bot Attacks
Inbound Traffic
Outbound
Bot Auth
Bot Anomalies
Last Updated: 1 hour ago
Continuous Events
IDS
Scanning
Malware
Botnet
DOS
Sys Errors
Web Error
Win Error
High CPU
DNS Errors
Last Updated: 1 hour ago
Malicious Process Monitoring
Malicious
Unwanted
Custom Hash
Indicator
Multi Crashes
Process Spike
Virus Spike
Error Spike
Change Spike
FIM Spike
New EXE Spike
Unique Unix
Unique Win
Last Updated: 1 hour ago
Access Control Anomalies
Firewall Spike
Auth Spike
Auth Fail Spike
Access Spike
Denial Spike
Last Updated: 1 hour ago
Intrusion Detection Events
Targeted
Host Scan
Net Sweep
Web Scan
Web Sweep
Auth Sweep
Auth Guessing
Auth Guessed
Worm Activity
IDS Spike
Scan Spike
DNS Tunnel
Web Tunnel
EXE Serve
USER Auth
Last Updated: 1 hour ago
Network Anomalies and Suspicious Activity
DNS Spike
SSL Spike
PVS Spike
Network Spike
Netflow Spike
File Spike
Web Spike
404+ Spike
Inbound Spike
Outbound Spike
SSH 30m+
VNC 30m+
RDP 30m+
Internal Spike
Connect Spike
Last Updated: 1 hour ago
Exploitable Internet Services
FTP
SSH
HTTP
HTTPS
SMB
1-200
201-500
501-1024
1025-5000
5000+
Suspicious Proxies, Relays and SPAM
Proxy
SSH Proxy
VNC Proxy
RDP Proxy
Bot Proxy
SMTP Proxy
SMTP Relay
SPAM Server
Crowd Surge
tenable
network security

Vulnerability Summary | Edit Filters

Viewing results 28 - 54 out of 814

Save Query | Save Asset | Open Ticket | More

View Settings

Plugin ID	Name	Family	Severity	Total
57462	FreeBSD 'telnetd' Daemon Remote Buffer Overflow	Gain a shell remotely	Critical	1
42367	Default Password (alpine) for 'root' Account	Default Unix Accounts	Critical	1
51418	HP StorageWorks MSA P2000 Default Credentials	Gain a shell remotely	Critical	1
61646	Oracle Integrated Lights Out Manager Default Crede...	Misc.	Critical	1
13659	l2tpd < 0.69 control.c write_packet Function Remote ...	Gain a shell remotely	Critical	1
19948	X11 Server Unauthenticated Access	Misc.	Critical	1
40987	Random password for 'root' account	Gain a shell remotely	Critical	1
14319	MySQL < 4.0.21 mysql_real_connect() Function Rem...	Databases	Critical	1
49691	IBM WebSphere Application Server 6.1 < 6.1.0.33 Mu...	Web Servers	Critical	1
57607	IBM WebSphere Application Server 6.1 < 6.1.0.41 Mu...	Web Servers	Critical	1
58327	Samba 'AndX' Request Heap-Based Buffer Overflow	Misc.	Critical	1
63623	Oracle Database, January 2013 Critical Patch Update	Databases	Critical	1
58966	PHP < 5.3.11 Multiple Vulnerabilities	CGI abuses	High	36
58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	CGI abuses	High	36
57537	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses	High	35
55976	Apache HTTP Server Byte Range DoS	Web Servers	High	31
11169	SSH Secure Shell without PTY setsid() Function Privi...	Misc.	High	26
52669	Host is Listed in Known Bot Database	General	High	26
41028	SNMP Agent Default Community Name (public)	SNMP	High	23
41014	PHP < 5.2.11 Multiple Vulnerabilities	CGI abuses	High	17
35067	PHP < 5.2.8 Multiple Vulnerabilities	CGI abuses	High	16
48244	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CGI abuses	High	14
66175	Plesk Horde Detection	CGI abuses	High	12
34460	Unsupported Web Server Detection	Web Servers	High	11
42052	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers	High	10
33849	PHP < 4.4.9 Multiple Vulnerabilities	CGI abuses	High	9
6718	Apple iOS < 6.1.3 Multiple Vulnerabilities	Web Clients [PVS]	High	7

Ron Gula [rongula]

SecurityCenter

Dashboard | Analysis | Scanning | Reporting | Assets | Workflow

Compliance ?

Add Component

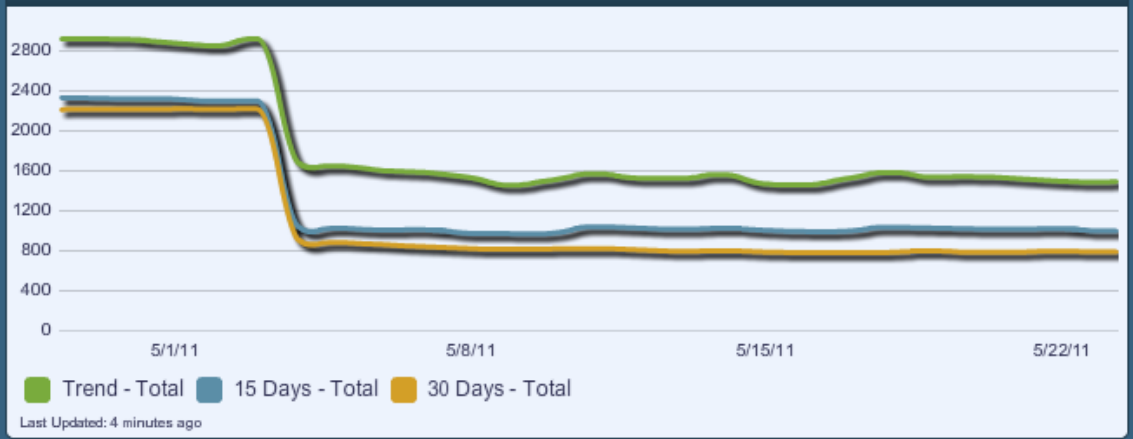
Compliance Status

	% Settings	% PCI	% HIPAA	% CyberScope
NY	52%	59%	69%	34%
Chicago	54%	58%	48%	47%
DC	48%	48%		22%
SF	35%	35%		32%
Boston	52%	59%	69%	34%
London	66%	80%		29%
Paris	52%	55%	59%	37%

Last Updated: 7 minutes ago

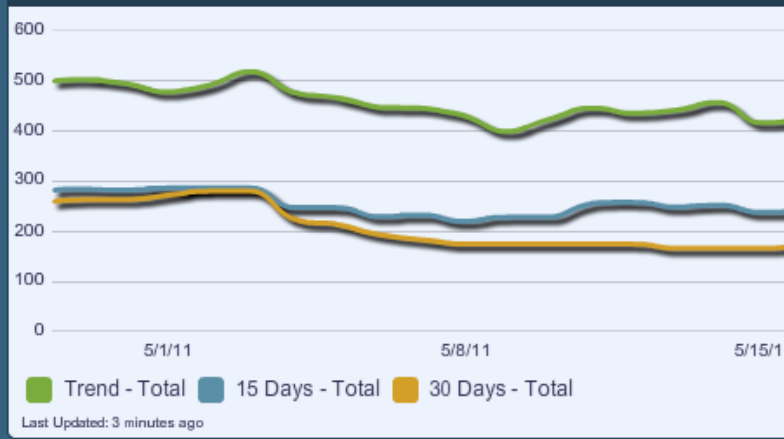
tenable network security

Group 1



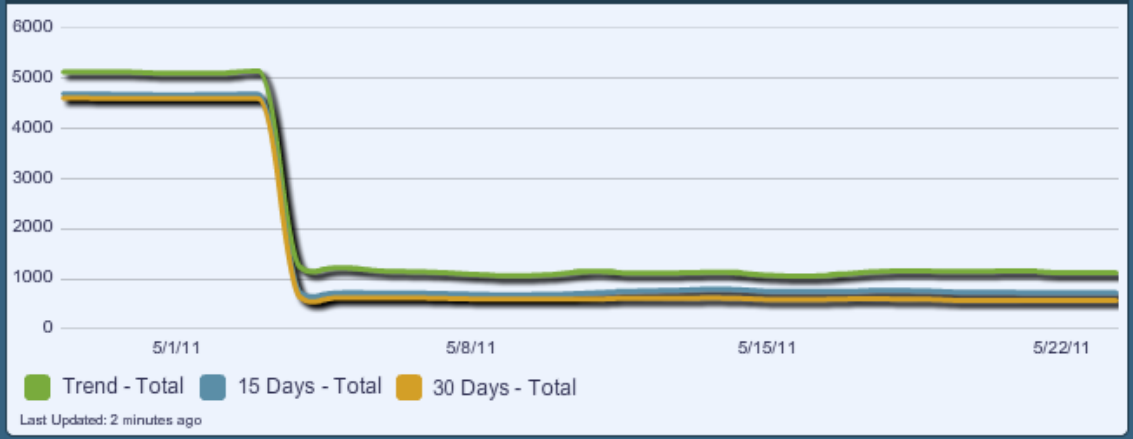
Last Updated: 4 minutes ago

Group 1 - High Vulns



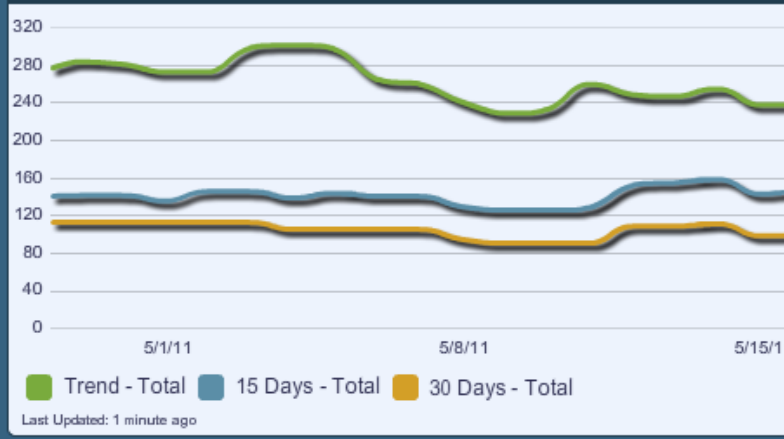
Last Updated: 3 minutes ago

Group 2



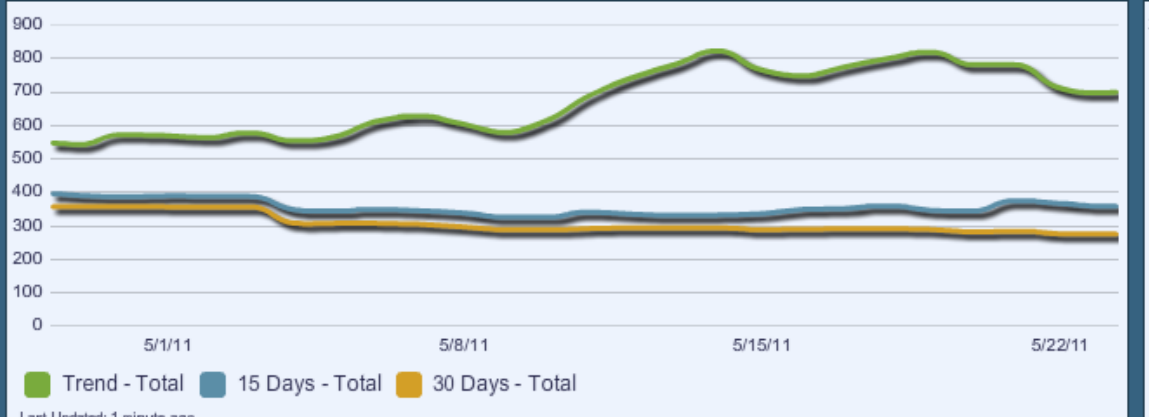
Last Updated: 2 minutes ago

Group 2 - High Vulns

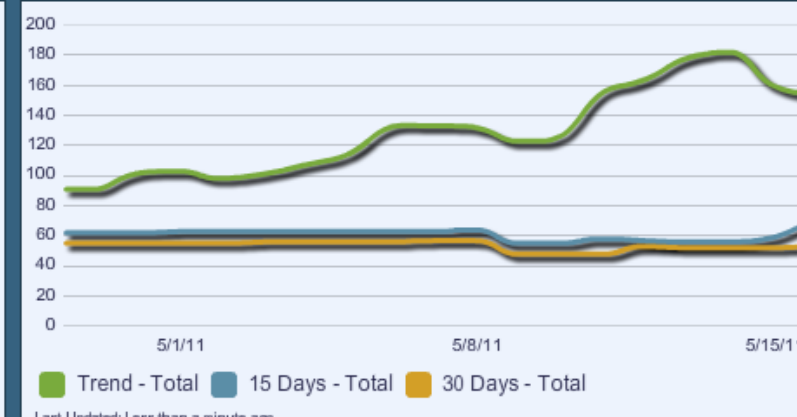


Last Updated: 1 minute ago

Group 3



Group 3 - High Vulns



Top 10 Scanned Vulns

Plug...	...	Seve...	Name
65891	11	Critical	Cisco IOS Software Smart Install Unauthenticated IO...
65995	9	Critical	Oracle Java SE Multiple Vulnerabilities (April 2013 CPU)
44340	5	Critical	CentOS Update Set
66274	4	Critical	VMware Security Updates for vCenter Server (VMSA-...
48264	4	Critical	VxWorks WDB Debug Service Detection
57290	4	Critical	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnera...
57959	4	Critical	Oracle Java SE Multiple Vulnerabilities (Feb 2012 CPU)
59462	4	Critical	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)
62593	4	Critical	Oracle Java SE Multiple Vulnerabilities (October 2012...
64454	4	Critical	Oracle Java SE Multiple Vulnerabilities (February 201...

Last Updated: 16 hours ago

Top 10 Sniffed Vulns

Plu...	T...	Se...	Name
6751	164	High	Flash Player <= 10.3.183.68 / 11.6.602.180 Multiple Vuln...
6724	63	High	Google Chrome < 26.0.1410.43 Multiple Vulnerabilities
6821	45	High	Flash Player <= 10.3.183.75 / 11.7.700.169 Multiple Vuln...
6752	36	High	Flash Player <= 10.3.183.68 / 11.6.602.180 Multiple Vuln...
4434	33	High	Mac OS X Safari < 3.1 Multiple Vulnerabilities
6592	32	High	Google Chrome < 22.0.1229.79 Multiple Vulnerabilities
6600	32	High	Google Chrome < 22.0.1229.92 Multiple Vulnerabilities
6601	32	High	Google Chrome < 22.0.1229.94 Multiple Vulnerabilities
6616	32	High	Google Chrome < 23.0.1271.64 Multiple Vulnerabilities
6628	32	High	Google Chrome < 23.0.1271.91 Multiple Vulnerabilities

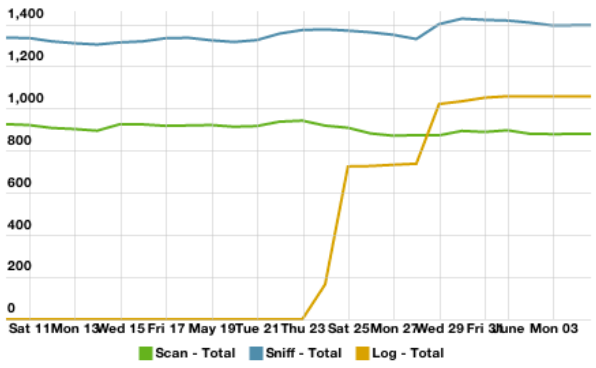
Last Updated: 16 hours ago

Top 10 Logged Vulns

Plugin ID	Total	Severity	Name
800552	13	High	Apache 2.2 < 2.2.22 Multiple Vulnerabilities
800559	13	High	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS
800573	13	High	Apache 2.2 < 2.2.16 Multiple Vulnerabilities
800577	13	High	Apache 2.2 < 2.2.17 Multiple Vulnerabilities
800584	13	High	Apache 2.2 < 2.2.20 Multiple Vulnerabilities
800557	9	High	Apache mod_ssl Session Cache Code Overflow
800107	2	High	Opera < 12.12 Multiple Vulnerabilities
800108	2	High	Mozilla Firefox 17.x <= 17 Multiple Vulnerabilities
800112	2	High	Google Chrome < 26.0.1410.43 Multiple Vulner...
800735	2	High	Firefox < 2.0.0.16 / 3.0.1 Multiple Vulnerabilities

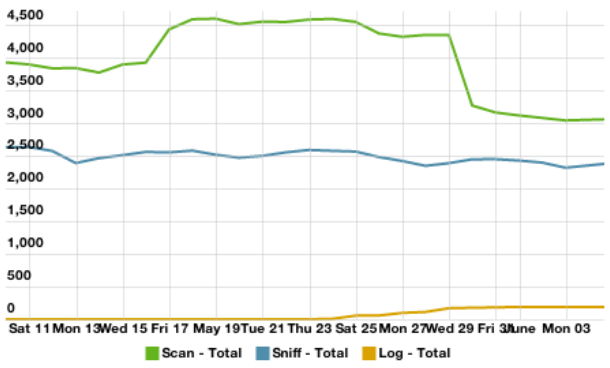
Last Updated: 16 hours ago

Scan, Sniff and Log System Count



Last Updated: 16 hours ago

Scan, Sniff and Log Vuln Count



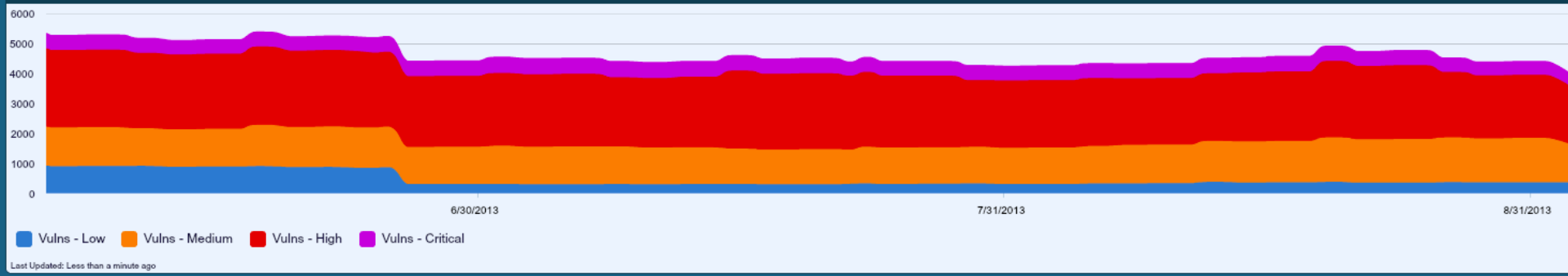
Last Updated: 16 hours ago

Scan, Sniff and Log Coverage

Total Systems	3090	
Scanned Systems	882	29%
Sniffed Systems	1401	45%
Logged Systems	1061	34%

Last Updated: 14 hours ago

Vulns Over Time



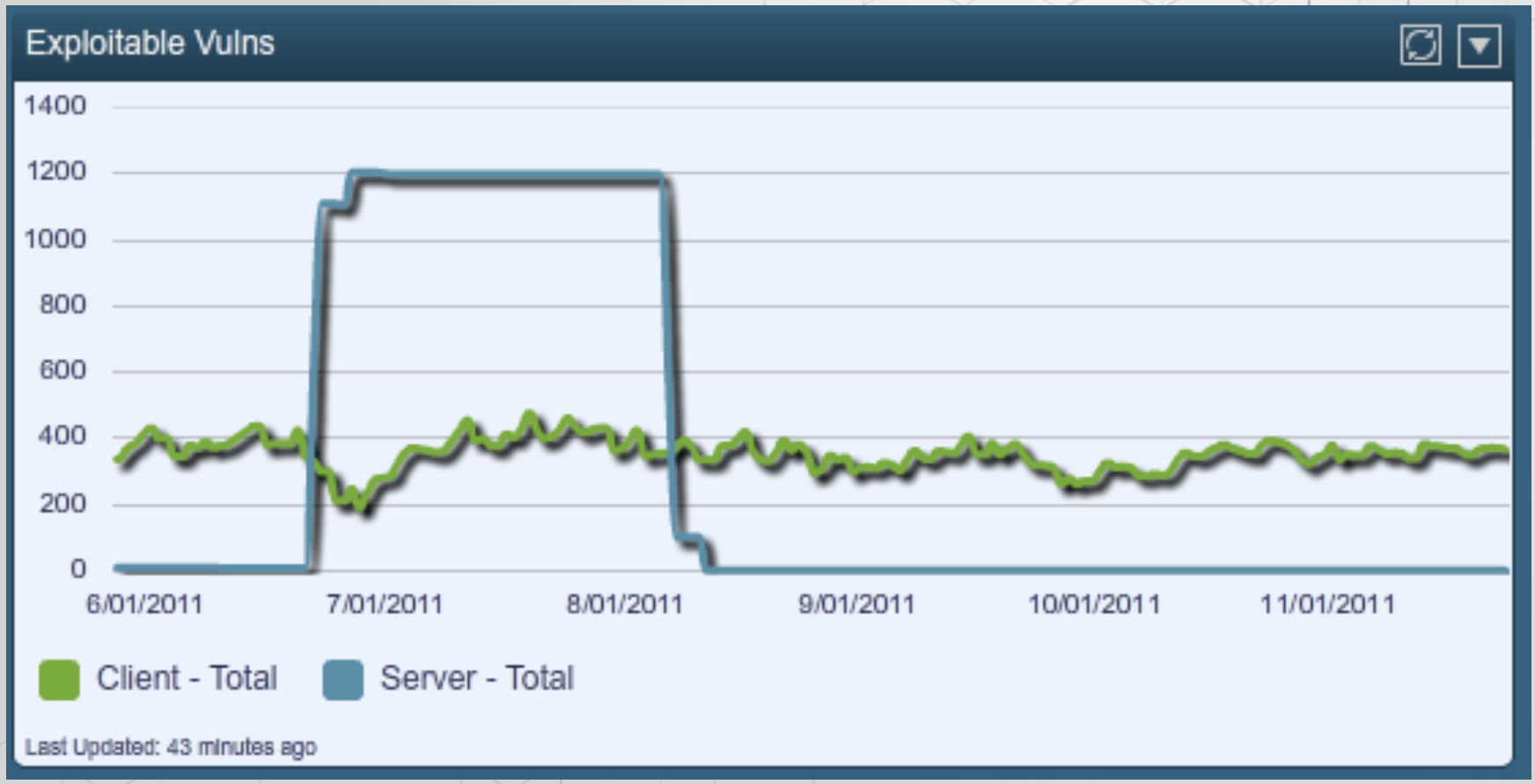
Last Updated: Less than a minute ago

Remediation Rates

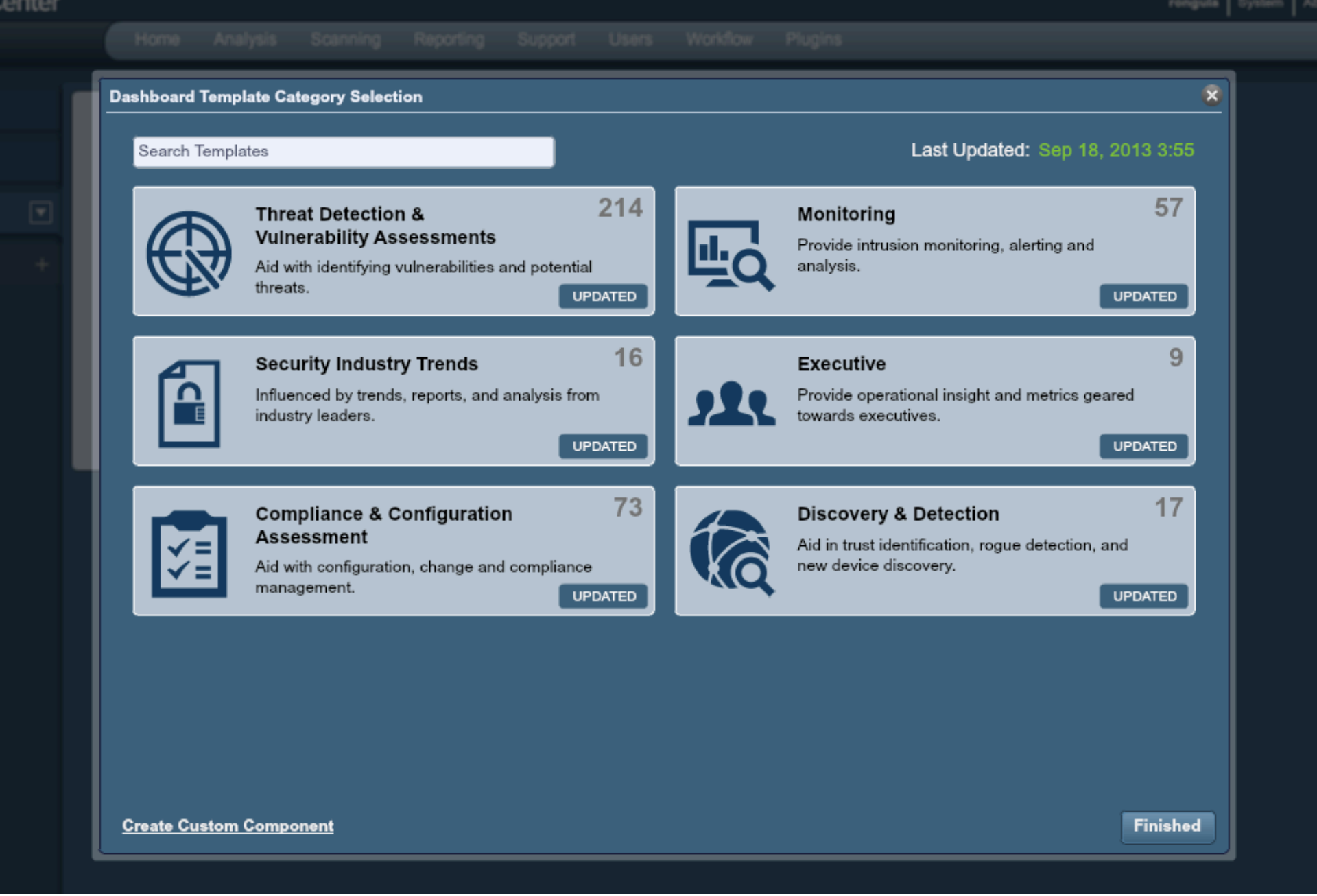
	Now	Patched	30d Rate	30d Date	30d Rate - Lifetime	30d Rate Past 30d	30d Rate Past 31d-60d	30d Rate Past 61d-90d
All Vulns	3909	2035	1002	1009	49%	30%	66%	75%
CVSS 10	436	98	17	68	17%	1%	58%	45%
Exploitable	1602	776	401	366	52%	37%	66%	58%
Linux	734	630	51	558	8%	1%	62%	100%
Windows	2466	1334	925	418	69%	68%	68%	74%

Last Updated: Less than a minute ago

tenable network security



tenable
network security



tenable network security

Questions?

rderaison@tenable.com

tenable
network security