



Scanning Tools

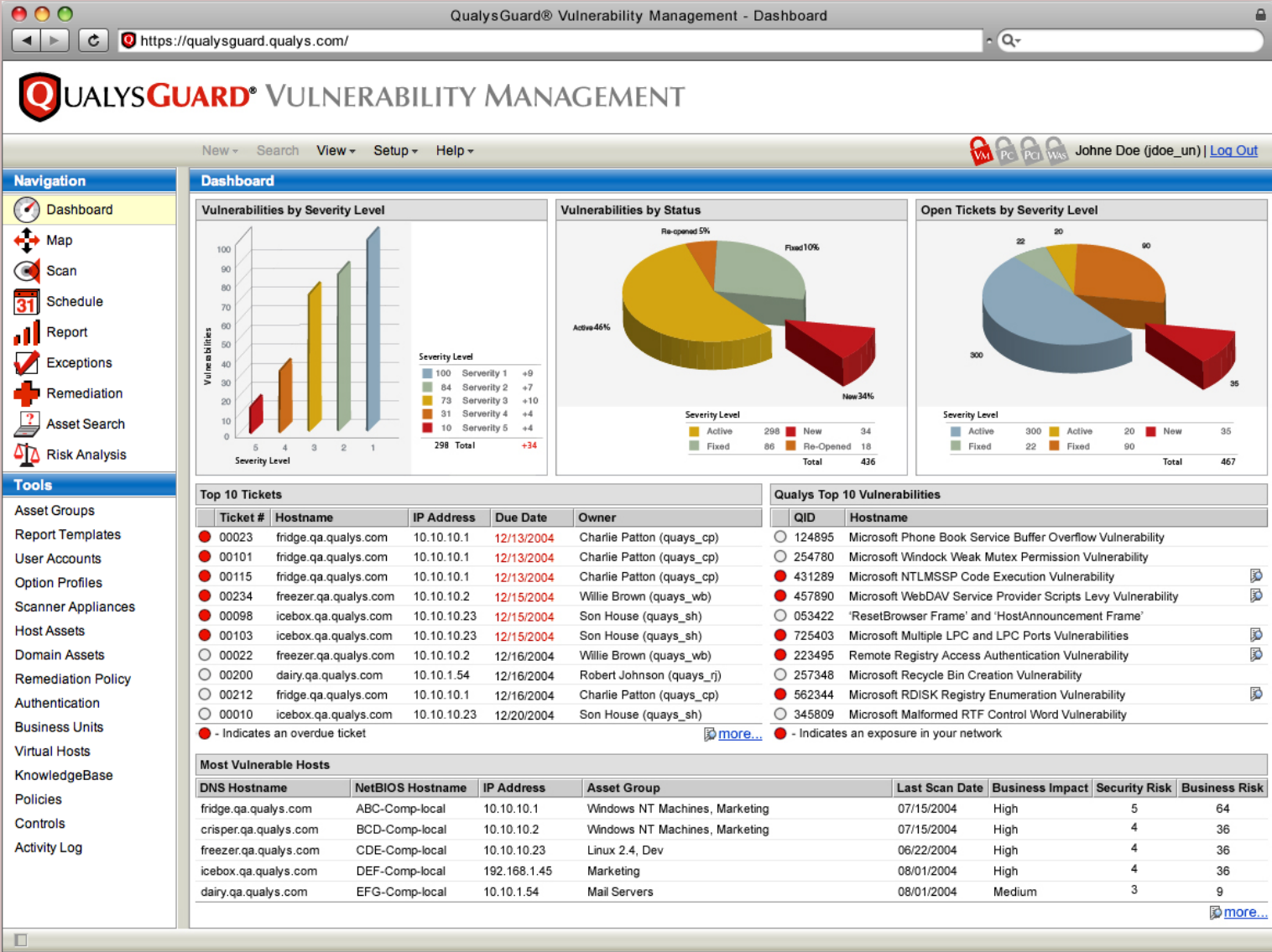
VULNERABILITY MANAGEMENT

Vulnerability Scanning Tools

- QualysGuard
- Tenable's Nessus
- Rapid7's Nexpose
- OpenVAS
- Nikto Web Application scanner
- Microsoft Baseline Security Analyzer



QualysGuard Vulnerability Scanner



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



Tenable's Nessus Vulnerability Scanner

Nessus - Windows Internet Explorer

https://localhost:8834/flash.html

File Edit View Favorites Tools Help

Nessus

Nessus user | Help | About | Log out

Reports Reports Mobile Scans Policies Users Configuration

Keene_policy Vulnerability Summary | Host Summary

Completed: Feb 9, 2015 15:32 (1 Error) [Download Report](#) [Remove Vulnerability](#) [Audit Trail](#)

Filters No Filters + Add Filter Clear Filters

Plugin ID	Count	Host	Port
11808	1	10.3.1.6	445 / tcp
11835	1		
12054	1		
12209	1		
22194	1		
34477	1		
35362	1		
22034	1		
26920	1		
57608	1		
11219	5		
10736	4		
11011	2		

Plugin ID: 34477 Port / Service: cifs (445/tcp) Severity: **Critical**

Plugin Name: MS08-067: Microsoft Windows Server Service Crafted RPC Request Han...

CPE
cpe:/o:microsoft:windows

CVE
[CVE-2008-4250](#)

BID
[31874](#)

Cross-References
[OSVDB:49243](#)
IAVA:2008-A-0081
MSFT:MS08-067
CWE:94

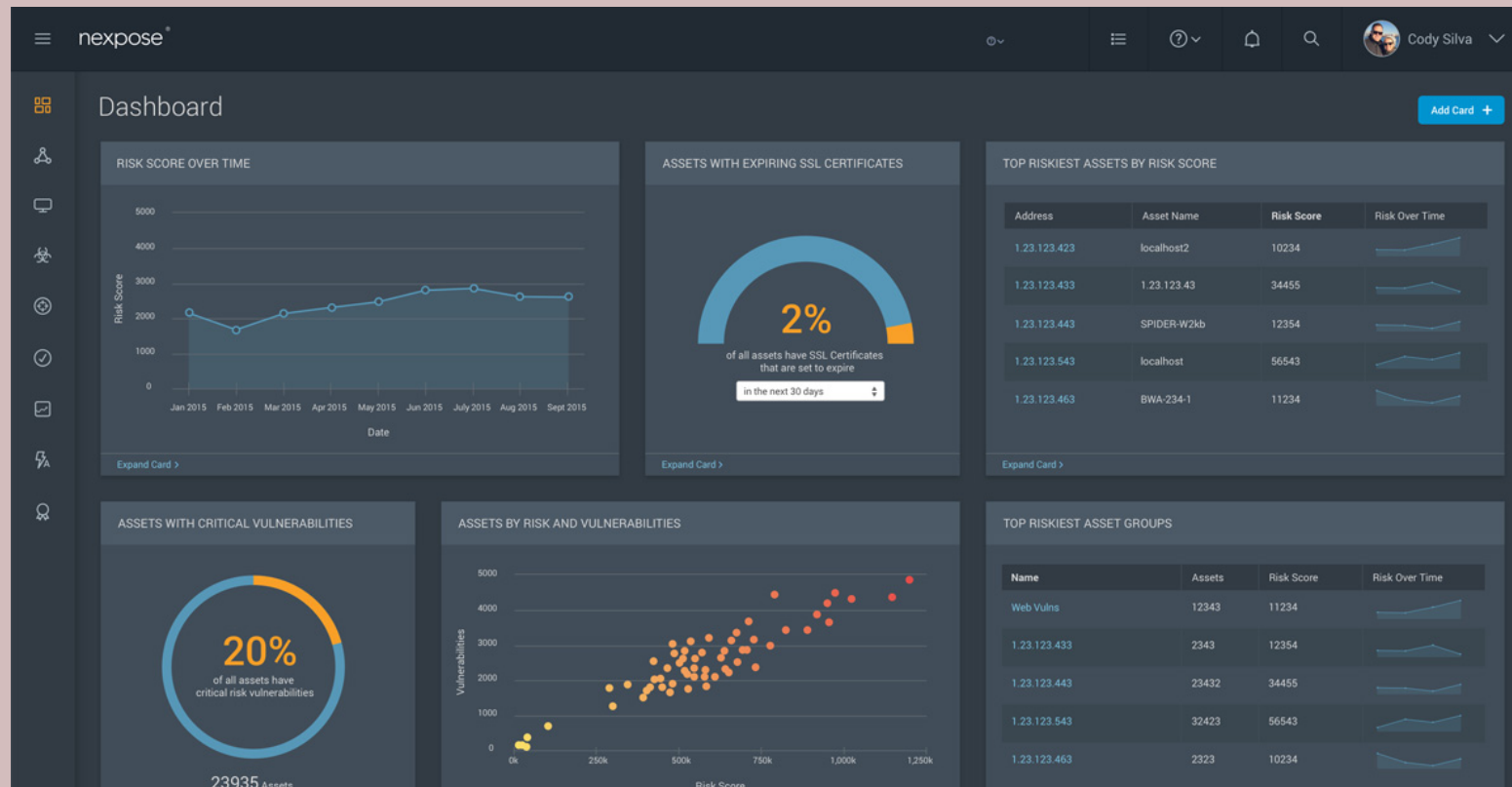
Plugin Publication Date: 2008/10/23

Plugin Last Modification Date: 2012/09/14

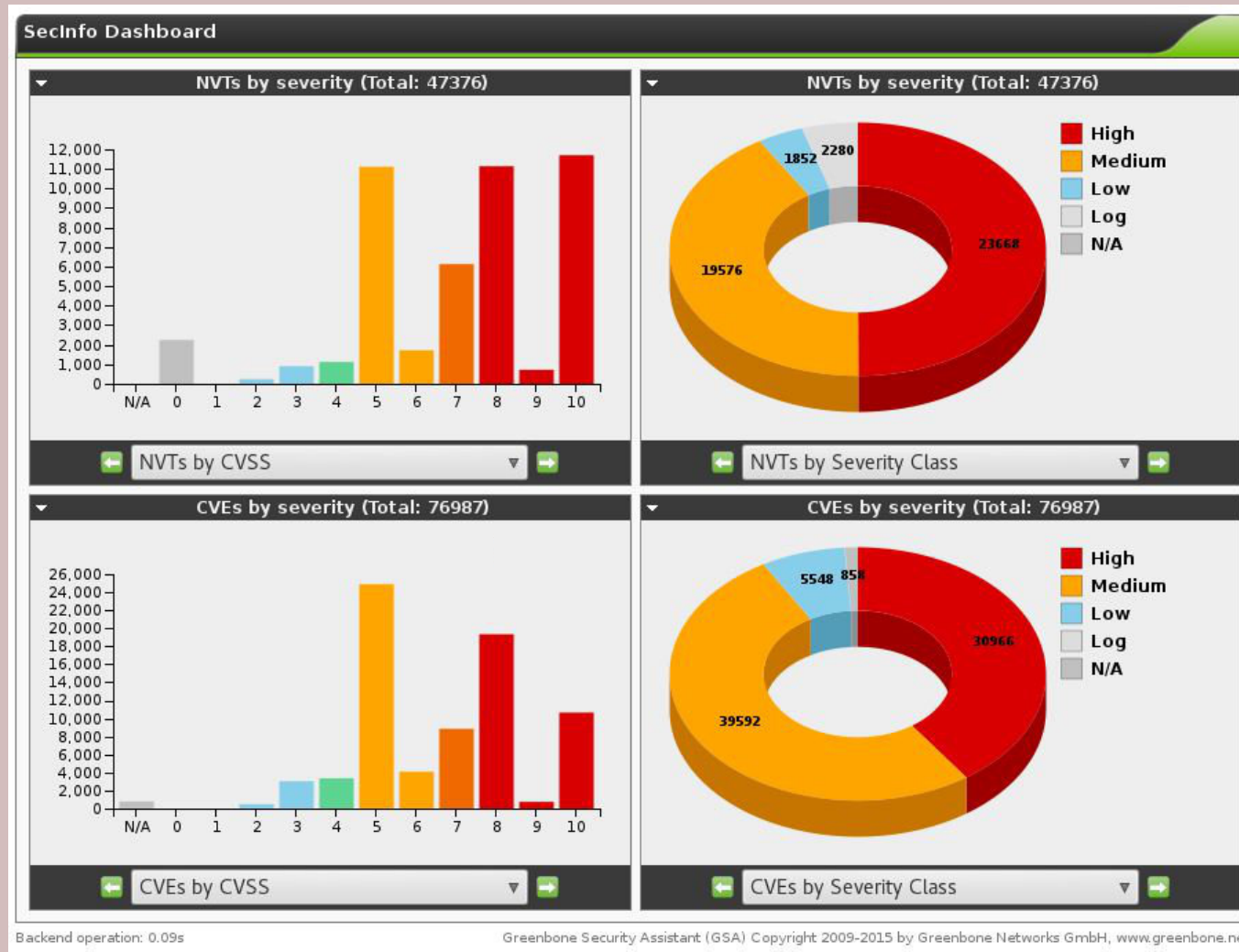
Done Local intranet | Protected Mode: Off 100%



Rapid7's Nexpose



OpenVAS (Open-source Scanner)



Nikto (Web Application Scanner)

```
- Nikto v2.1.6
-----
+ Target IP:      87.229.144.34
+ Target Hostname: google.ru
+ Target Port:    80
+ Start Time:     2015-02-26 14:51:38 (GMT6)
-----
+ Server: gws
+ Uncommon header 'alternate-protocol' found, with contents: 80:quic,p=0.08
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: http://www.google.ru/
+ Server banner has changed from 'gws' to 'sfpe' which may suggest a WAF, load b
alancer or proxy is in place
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-5737: WebLogic may reveal its internal IP or hostname in the Location he
ader. The value is "http://87.229.144.34/".
```



Microsoft's Baseline Security Analyzer

