TRANSNET

delivering freight reliably

Cloud-based scanning
17 July 2012
Justin Williams

Cloud Scanning ?

- What
- Why
- How
- Learnings
- Discussion

Not scanning cloud

- Retina CS
  - VMware vCenter
  - Amazon EC2
  - RackSpace
  - GoGrid

PCI Security Standards Council
APPROVED SCANNING VENDOR

eEye Digital Security

Scanning from cloud

- Hosted solution
- Pre-packaged
- Up-to-date / Low hassle
- External scans
- Understand perimeter
- Regular scanning

What's happening?

- Servers running
- Not defaced
- Customers transacting
- Vendors billing us
- Staff working

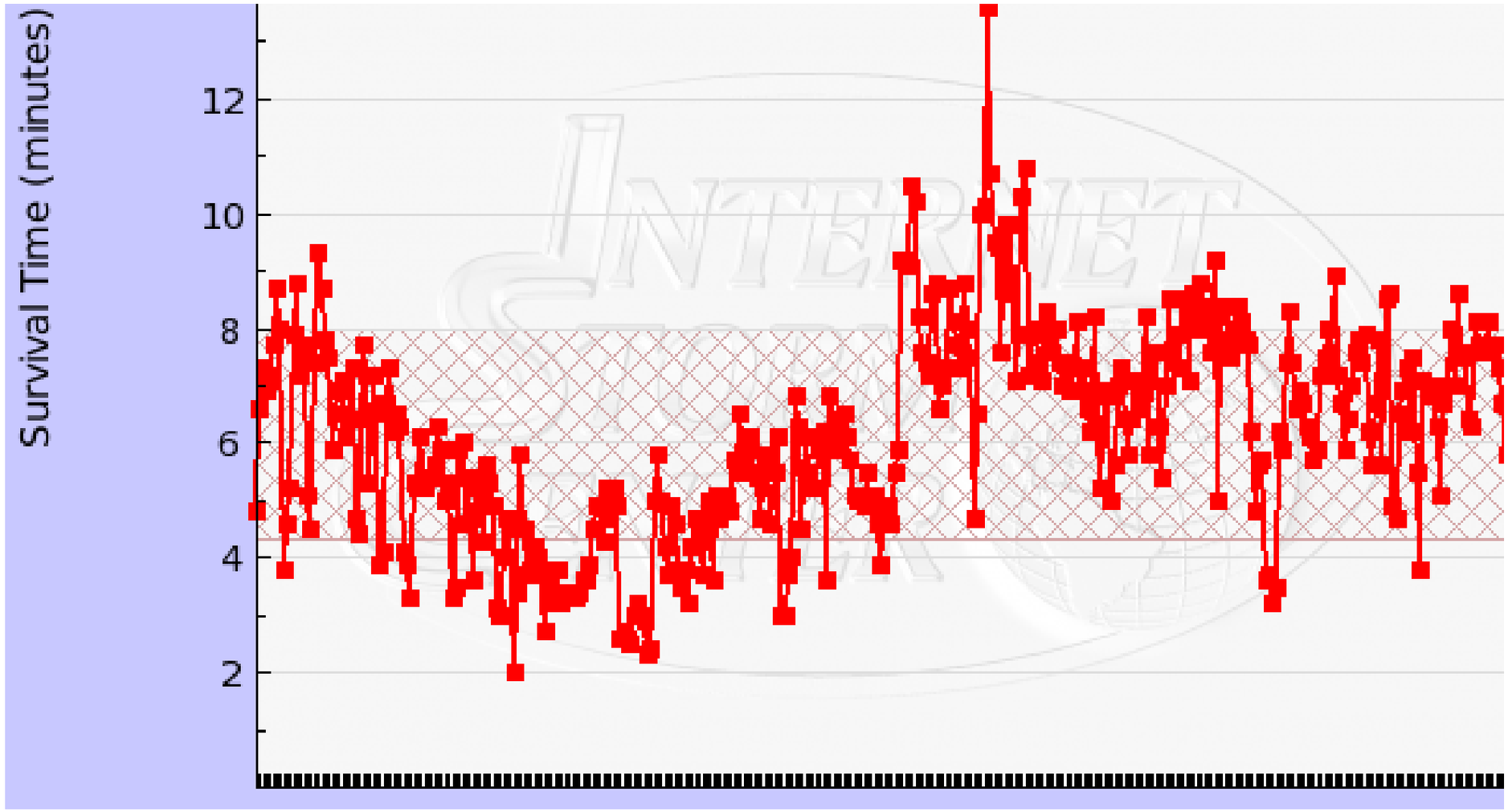

WHO IS
WATCHING?

Really?

Survival times

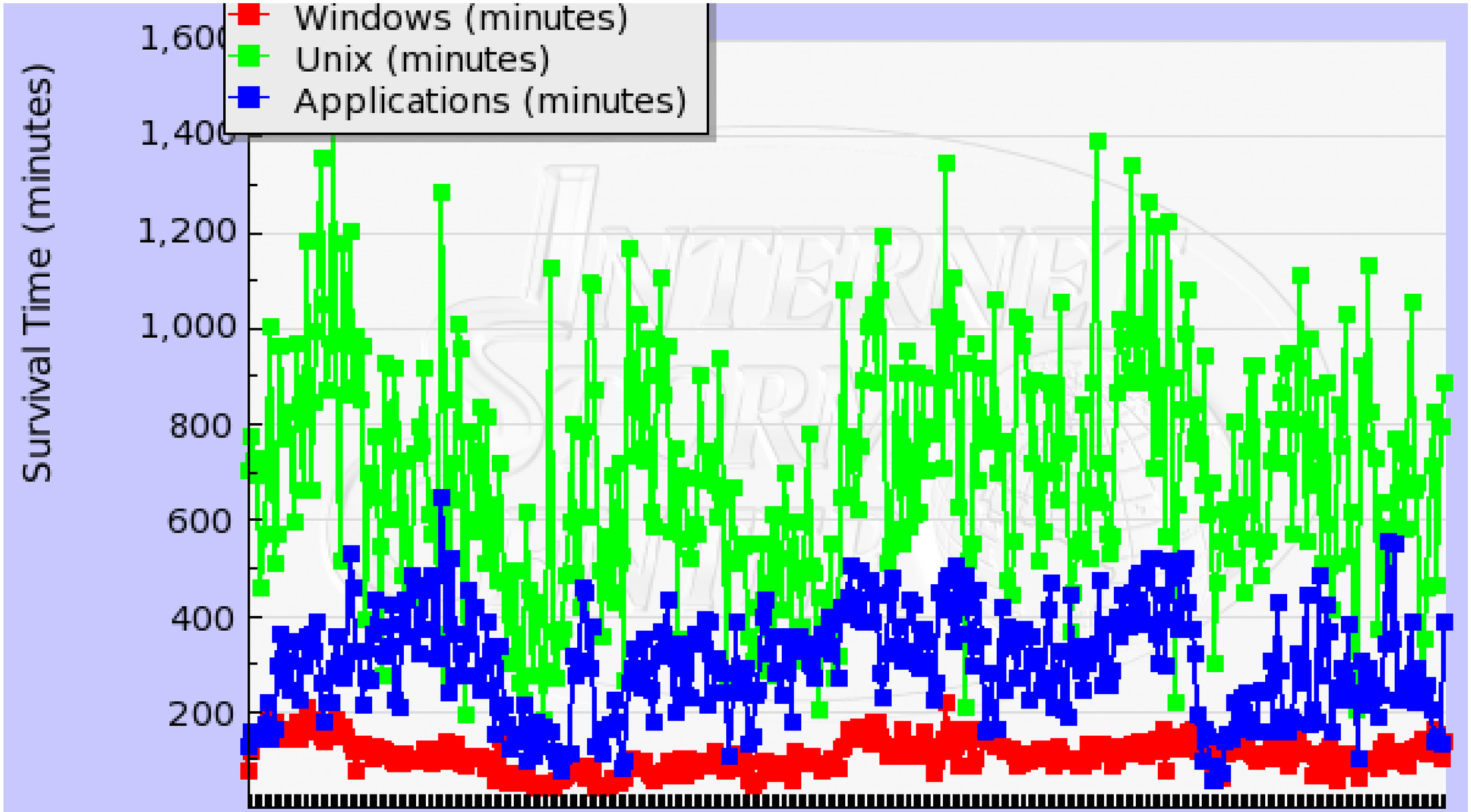
- 40m 2003
- 20m 2004
- 8m 2005

[cnet.com]



- Jan 2005 to July 2012 (Isc.sans.edu)

Platform matters?



Jan 2005 to July 2012 (Isc.sans.edu)

What we need

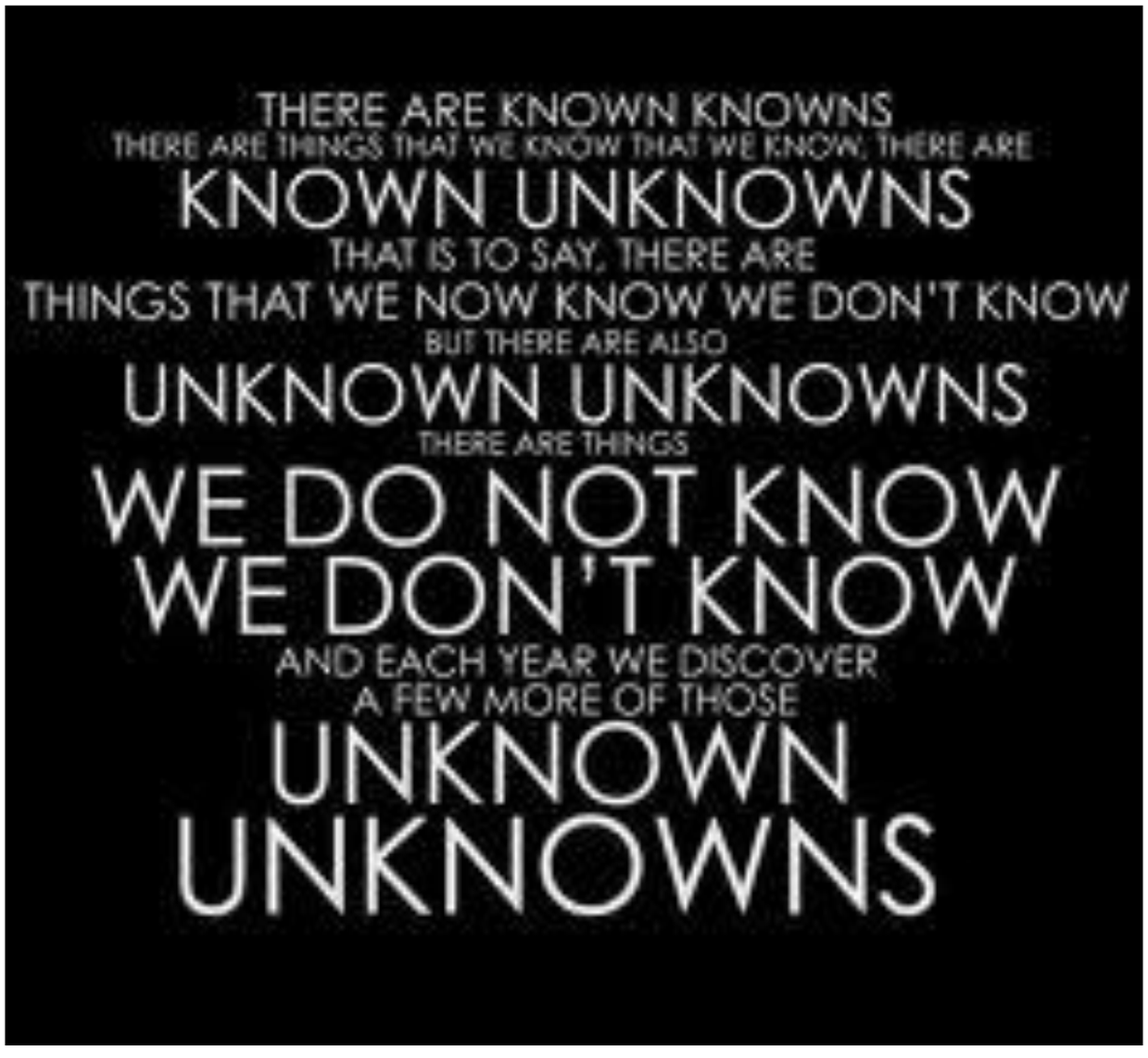
Continuous monitoring

Context of initiative

- Similar deployment internally
- Complexity
  - *Service providers*
  - *Federated*
  - *Heterogeneous*
  - *Documentation*

Need for speed

- Large landscape
- Lots of unknown
- Visibility
- Trust



How?

- DIY
- Cloud infrastructure
- Software as a Service
- Buy a managed service

Options?


Nessus


CLOUD PENETRATOR
WEB VULNERABILITY SCANNER
SECPOINT®
www.secpoint.com


PS


QUALYS®


FREE Security scanner.
Audit your network now!

Rationale

- 3 Quotes
- Walk before run
- Speed of deployment
- Reputation
- Cost
- Accessibility

Rolling out the solution

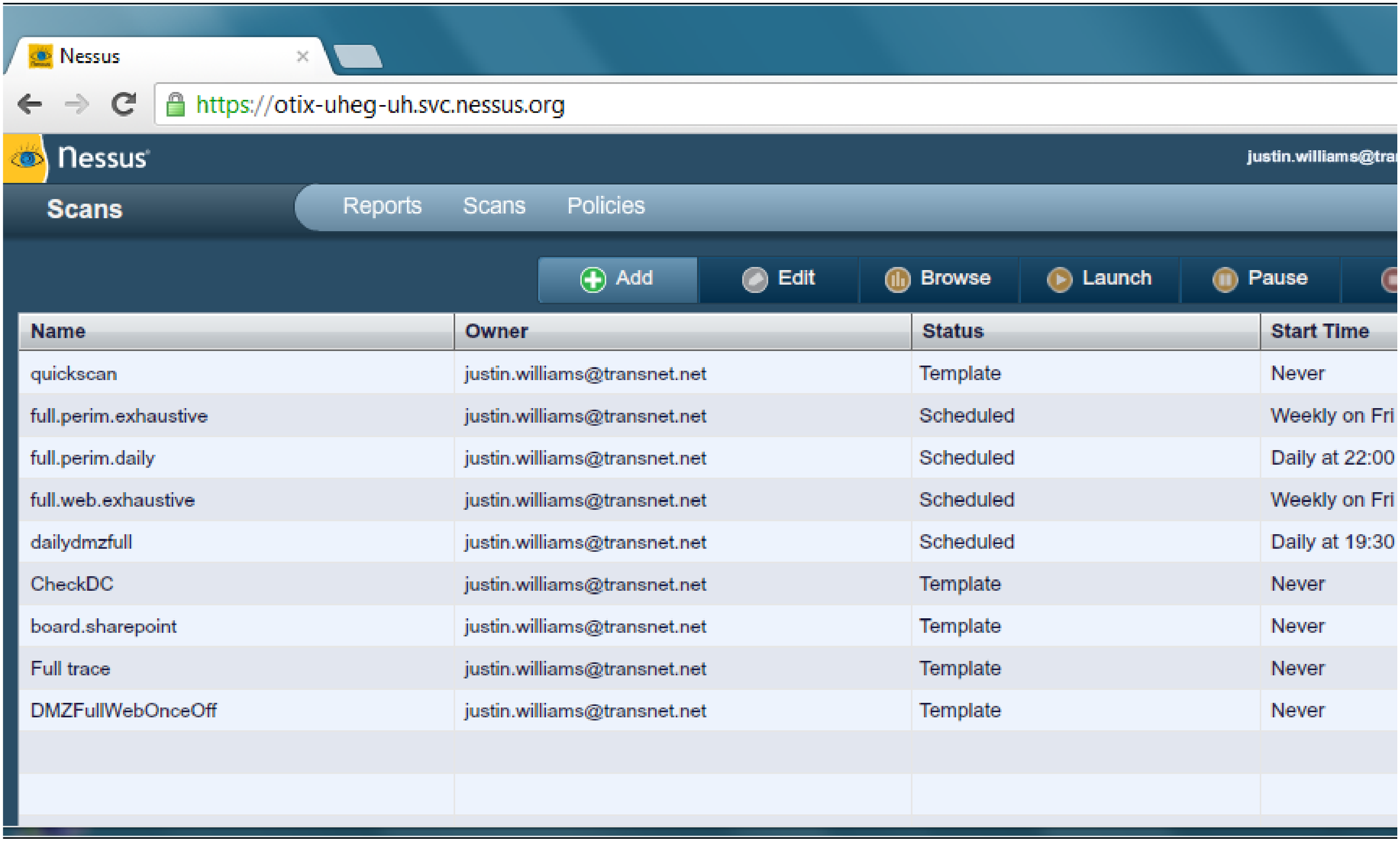
Nessus Perimeter Service

Into action

- Procurement $3600/yr
- Identify targets
- Frequency
- Change request
- Communicate communicate
- Push play

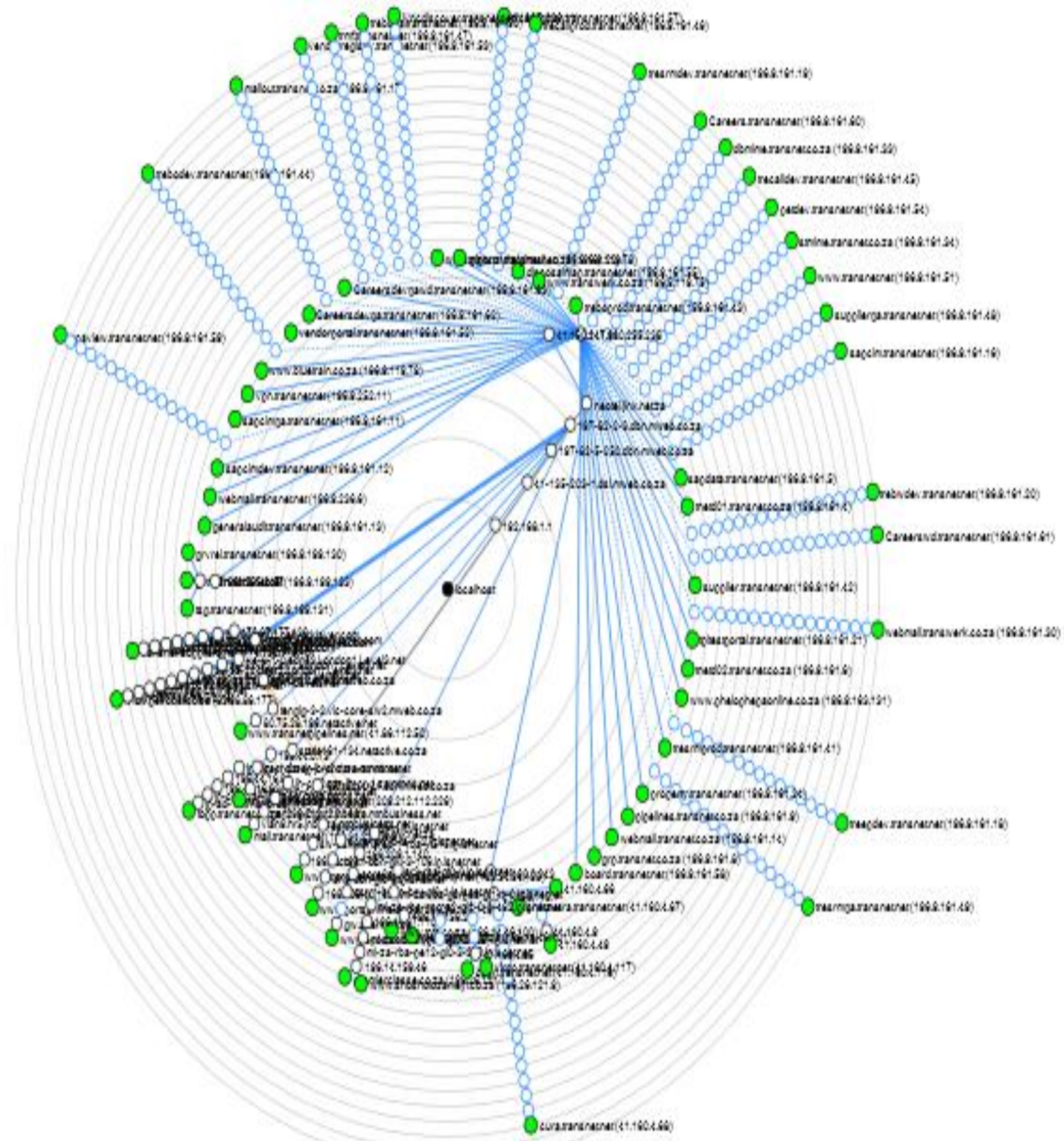
Setup

- Create Policies
  - Predefined
- Create scans
  - Choose Policy
  - Capture addresses
  - Schedule
- Monitor results


Nessus
https://otix-uheg-uh.svc.nessus.org
Nessus
justin.williams@tra
Scans
Reports
Scans
Policies
Add
Edit
Browse
Launch
Pause
Name
Owner
Status
Start Time
quickscan
justin.williams@transnet.net
Template
Never
full.perim.exhaustive
justin.williams@transnet.net
Scheduled
Weekly on Fri
full.perim.daily
justin.williams@transnet.net
Scheduled
Daily at 22:00
full.web.exhaustive
justin.williams@transnet.net
Scheduled
Weekly on Fri
dailydmzfull
justin.williams@transnet.net
Scheduled
Daily at 19:30
CheckDC
justin.williams@transnet.net
Template
Never
board.sharepoint
justin.williams@transnet.net
Template
Never
Full trace
justin.williams@transnet.net
Template
Never
DMZFullWebOnceOff
justin.williams@transnet.net
Template
Never

Initial runs

- Timing conflicts
- Flakey iPad app
- Large reports
  - CSV, PDF, Nessus
- Vulnerabilities
- False positives
- Duplicate IPs


localhost

Nessus

https://otix-uheg-uh.svc.nessus.org

Nessus

justin.williams@transnet.net | Help | About | Log out

Reports | Reports | Scans | Policies

dailydmzfull (scheduled) **Vulnerability Summary** | Host Summary

Completed: Jul 8, 2012 21:23 (1 Error)

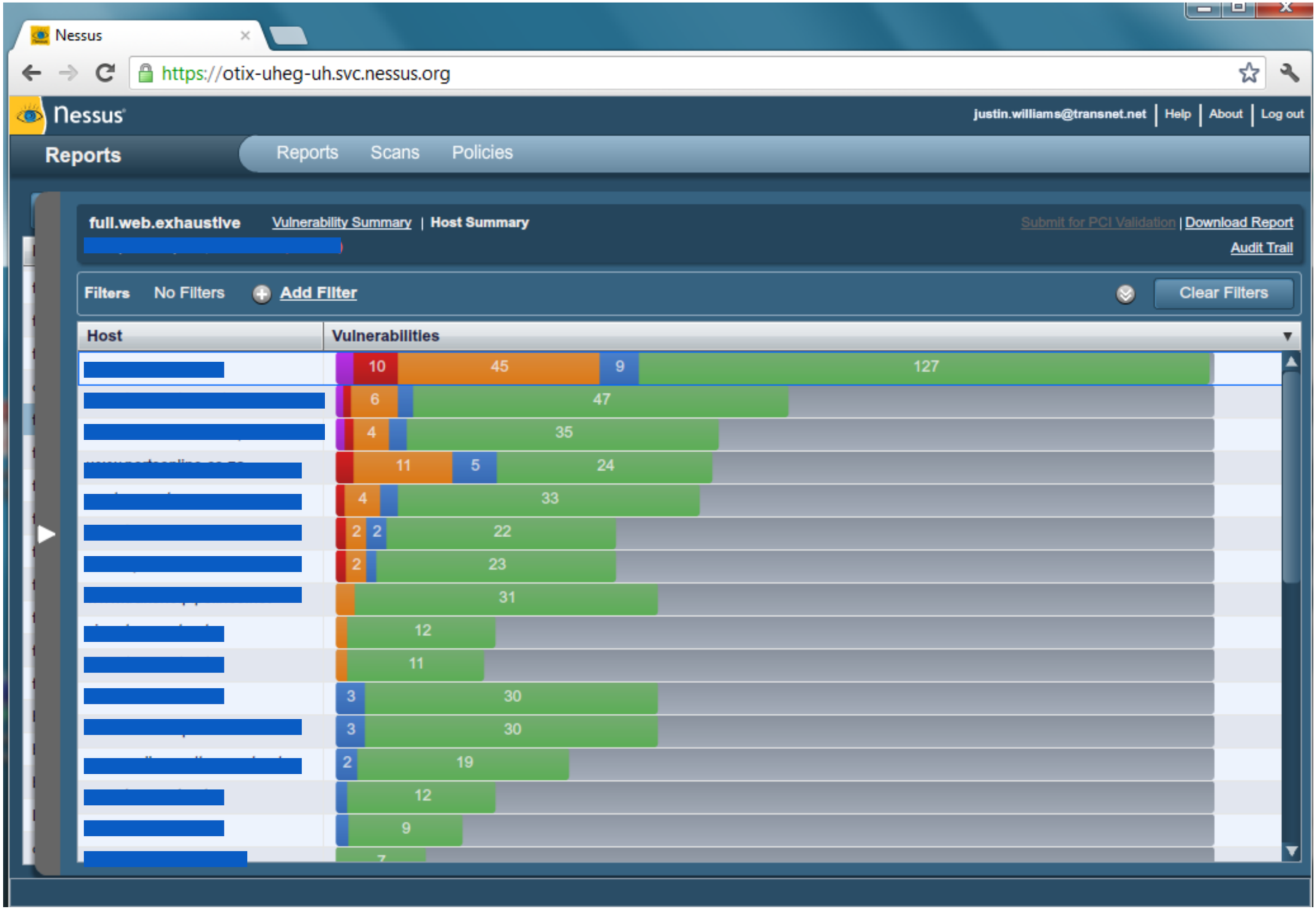
Submit for PCI Validation | Download Report

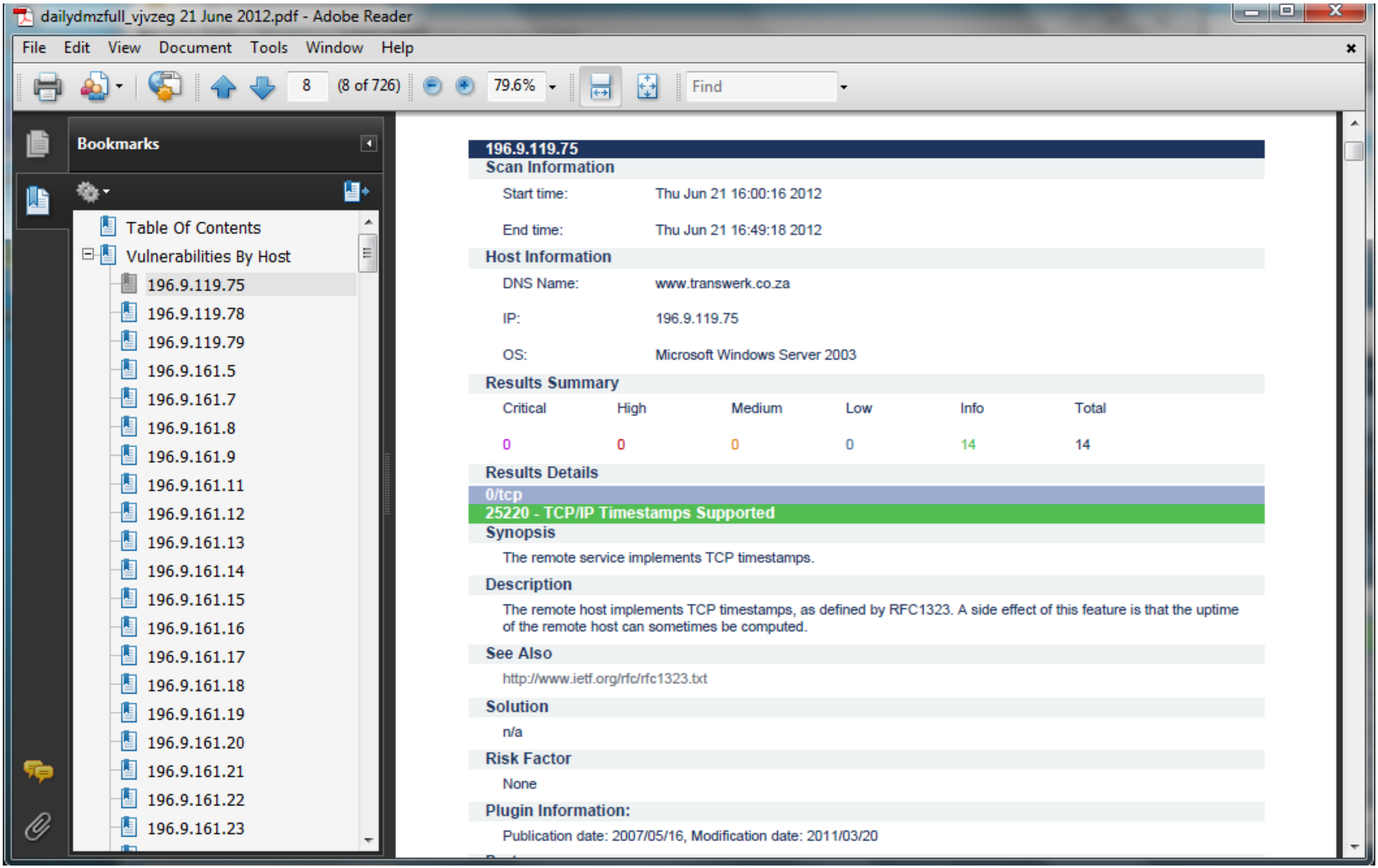
Remove Vulnerability | Audit Trail

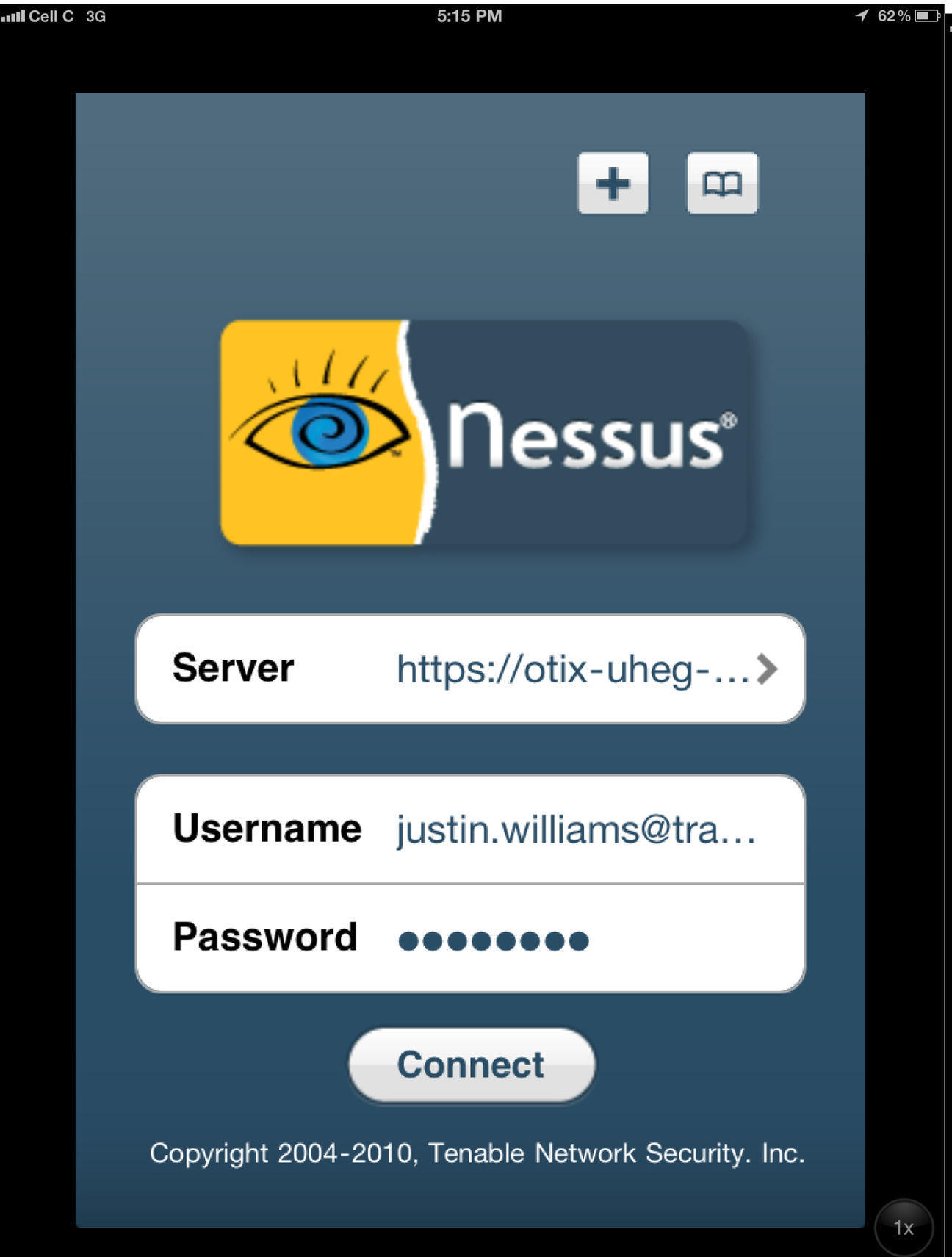
Filters No Filters Add Filter Clear Filters

Plugin ID	Count	Severity	Name	Family
46802	2	Critical	SBLIM-SFCB Multiple Buffer Overflows	Web Servers
51369	2	Critical	HP StorageWorks MSA P2000 Hidden 'admin' User Default Credentials	Gain a shell remotely
51418	2	Critical	HP StorageWorks MSA P2000 Default Credentials	Gain a shell remotely
58183	2	High	Dropbear SSH Server Channel Concurrency Use-after-free Remote Code Execut	Misc.
42873	20	Medium	SSL Medium Strength Cipher Suites Supported	General
20007	10	Medium	SSL Version 2 (v2) Protocol Detection	Service detection
51192	10	Medium	SSL Certificate Cannot Be Trusted	General
26928	8	Medium	SSL Weak Cipher Suites Supported	General
57582	8	Medium	SSL Self-Signed Certificate	General
11213	7	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
15901	5	Medium	SSL Certificate Expiry	General
10815	3	Medium	Web Server Generic XSS	CGI abuses : XSS
35291	3	Medium	SSL Certificate Signed using Weak Hashing Algorithm	General
57792	3	Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers
10882	2	Medium	SSH Protocol Version 1 Session Key Retrieval	General

Loading Scans


Nessus
https://otix-uheg-uh.svc.nessus.org
Nessus
justin.williams@transnet.net | Help | About | Log out
Reports
Reports Scans Policies
full.web.exhaustive Vulnerability Summary | Host Summary
Submit for PCI Validation | Download Report
Audit Trail
Filters No Filters Add Filter
Clear Filters
Host
Vulnerabilities
10 45 9 127
6 47
4 35
11 5 24
4 33
2 2 22
2 23
31
12
11
3 30
3 30
2 19
12
9


dailydmzfull_vjvzeg 21 June 2012.pdf - Adobe Reader
File Edit View Document Tools Window Help
8 (8 of 726)
79.6%
Find
Bookmarks
Table Of Contents
Vulnerabilities By Host
196.9.119.75
196.9.119.78
196.9.119.79
196.9.161.5
196.9.161.7
196.9.161.8
196.9.161.9
196.9.161.11
196.9.161.12
196.9.161.13
196.9.161.14
196.9.161.15
196.9.161.16
196.9.161.17
196.9.161.18
196.9.161.19
196.9.161.20
196.9.161.21
196.9.161.22
196.9.161.23
196.9.119.75
Scan Information
Start time: Thu Jun 21 16:00:16 2012
End time: Thu Jun 21 16:49:18 2012
Host Information
DNS Name: www.transwerk.co.za
IP: 196.9.119.75
OS: Microsoft Windows Server 2003
Results Summary
Critical High Medium Low Info Total
0 0 0 0 14 14
Results Details
0/tcp
25220 - TCP/IP Timestamps Supported
Synopsis
The remote service implements TCP timestamps.
Description
The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.
See Also
http://www.ietf.org/rfc/rfc1323.txt
Solution
n/a
Risk Factor
None
Plugin Information:
Publication date: 2007/05/16, Modification date: 2011/03/20


Cell C 3G
5:15 PM
62%
Nessus®
Server
https://otix-uheg-…
Username
justin.williams@tra…
Password
Connect
Copyright 2004-2010, Tenable Network Security. Inc.
1x


Cell C 3G
5:15 PM
62%
Logout
Nessus®
Welcome justin.williams@transnet.net!
IP: 4.79.179.86
Scans
Reports
1x

Cell C 3G 5:16 PM 62%

Scans

Add

2 Scans Running

11 Scans in Total

board.sharepoint
justin.williams@transnet.net
Never
Template

CheckDC
justin.williams@transnet.net
Never
Template

dailydmzfull
justin.williams@transnet.net
Never
Template

DMZFullWebOnceOff
justin.williams@transnet.net
Never
Template

1x

Cell C 3G 5:16 PM 62%

Reports

Search Scans

full.perim.daily (scheduled)
Jul 06, 2012 21:55 PM
Running

dailydmzfull (scheduled)
Jul 06, 2012 21:21 PM
Completed

full.perim.exhaustive (scheduled)
Jul 06, 2012 19:49 PM
Completed

full.web.exhaustive (scheduled)
Jul 06, 2012 16:54 PM
Running

1x

Reports
Host Results
Filters
0 Filters Applied
Report dailydmzfull (scheduled) 109 Results

Host 152.108.194.131
Completed
Total 10
Open Port 0
0 0

Host 152.108.194.133
Completed
Total 9
Open Port 0
0 0

Host 152.108.194.134
Completed
Total 9
Open Port 0
0 0

Host 152.108.194.135
Completed
Total 9
Open Port 0
0 0

Cell C 3G 5:20 PM 61 %

Reports
Port Details
Filters
0 Filters Applied
Report dailydmzfull (scheduled)
Host 41.160.22.11
Port 22
7 Results

List Details

Plugin ID 22964
Name Service Detection
Port Ssh (22/Tcp)
Severity Low

Plugin ID 11219
Name Nessus SYN scanner
Port Ssh (22/Tcp)
Severity Low

Plugin ID 10267
Name SSH Server Type and Version Information
Port Ssh (22/Tcp)
Severity Low

Plugin ID 58183

Cell C 3G 5:20 PM 61 %

Reports
Port Details
Filters
0 Filters Applied
Report dailydmzfull (scheduled)
Host 41.160.22.11
Port 22
5 of 7 Results

List Details

Plugin ID 51418
Name HP StorageWorks MSA P2000 Default Cr...
Port Ssh (22/Tcp)
Severity High

The remote device appears to be a HP StorageWorks MSA P2000 series. One or more accounts are secured with a default password.

A remote, unauthenticated attacker could exploit this to gain administrative access to the management interface.

Solution
Secure all accounts with a strong password.

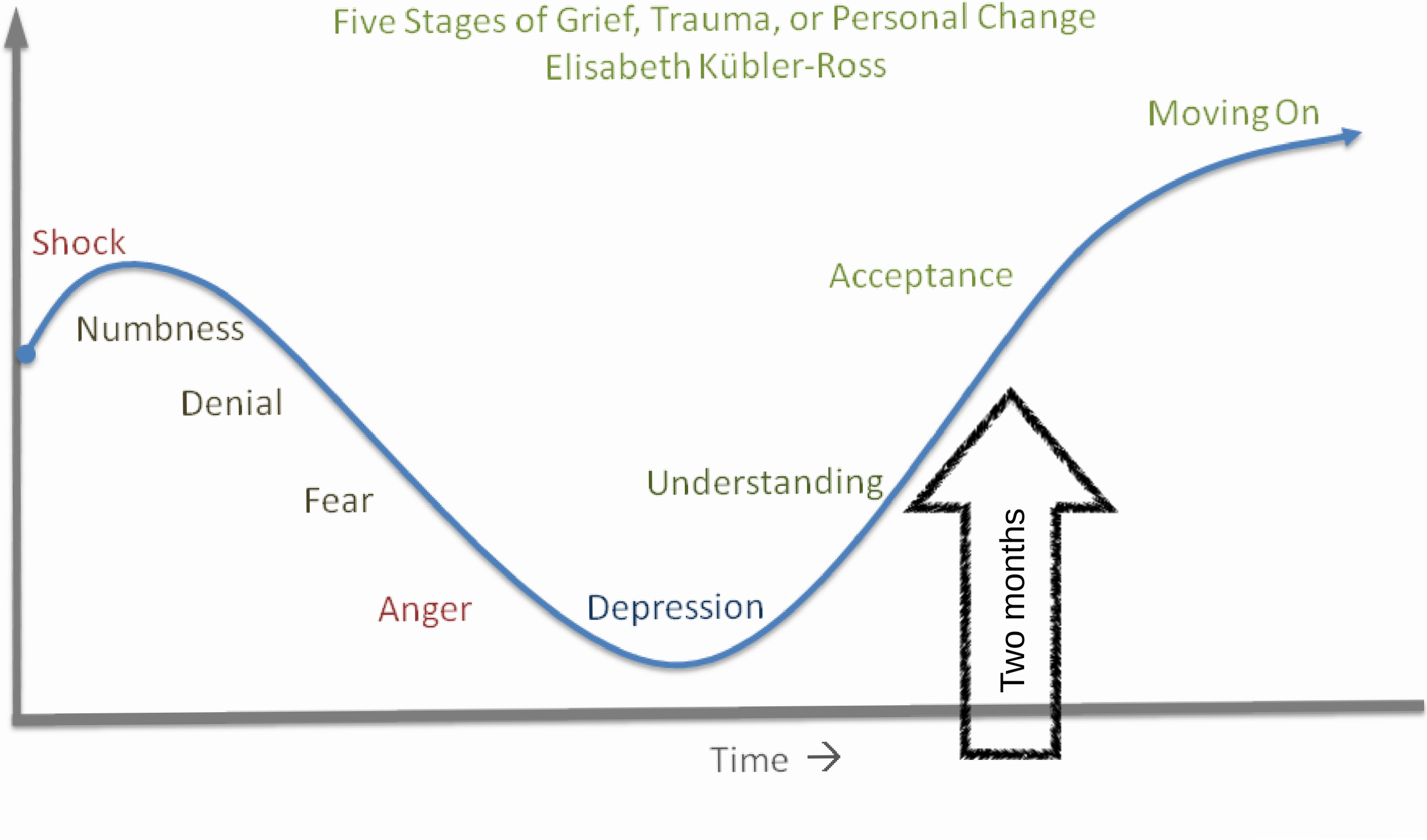
Plugin_Output
Username : manage
Password : !manage

Reaction

- Denial
- Anger
- Avoidance
- Blame
- Confessions
- Additions

Change management

- Denial,fear, anger
- It's expected
- Give it time
- Be strong
  - Don't give in
  - Don't allow exceptions
- Keep communicating

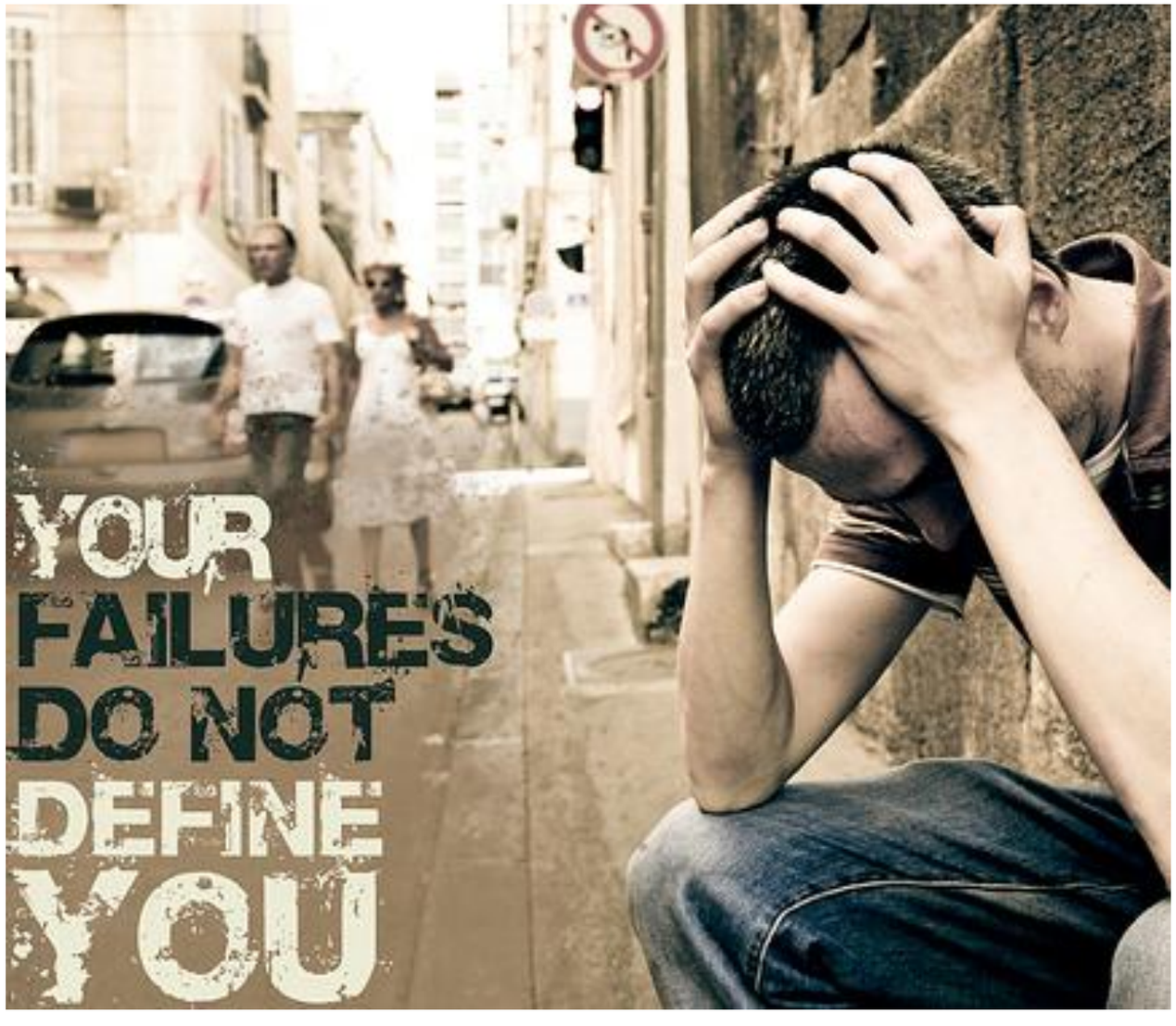

Five Stages of Grief, Trauma, or Personal Change
Elisabeth Kübler-Ross
Shock
Numbness
Denial
Fear
Anger
Depression
Understanding
Acceptance
Moving On
Two months
Time →

Learnings

What worked? What didn't?

What we found...

- Wrong DNS
- Remote admin
- Misconfigurations
- Outdated software
- Legacy
- Firewall issues
- Failed IDS



Root causes

- Patching
- Responsibility
- Business vs IT
- Vendor trust
- CMDB
- Respect

Response ...

- Report and monitor
- CIOs
- Infrastructure support
- Business
- Vendors
- Continuous monitoring

Adjustments

- Firewall rules
- IDS reconfig
- Policy changes
- Server config
- Responsibilities

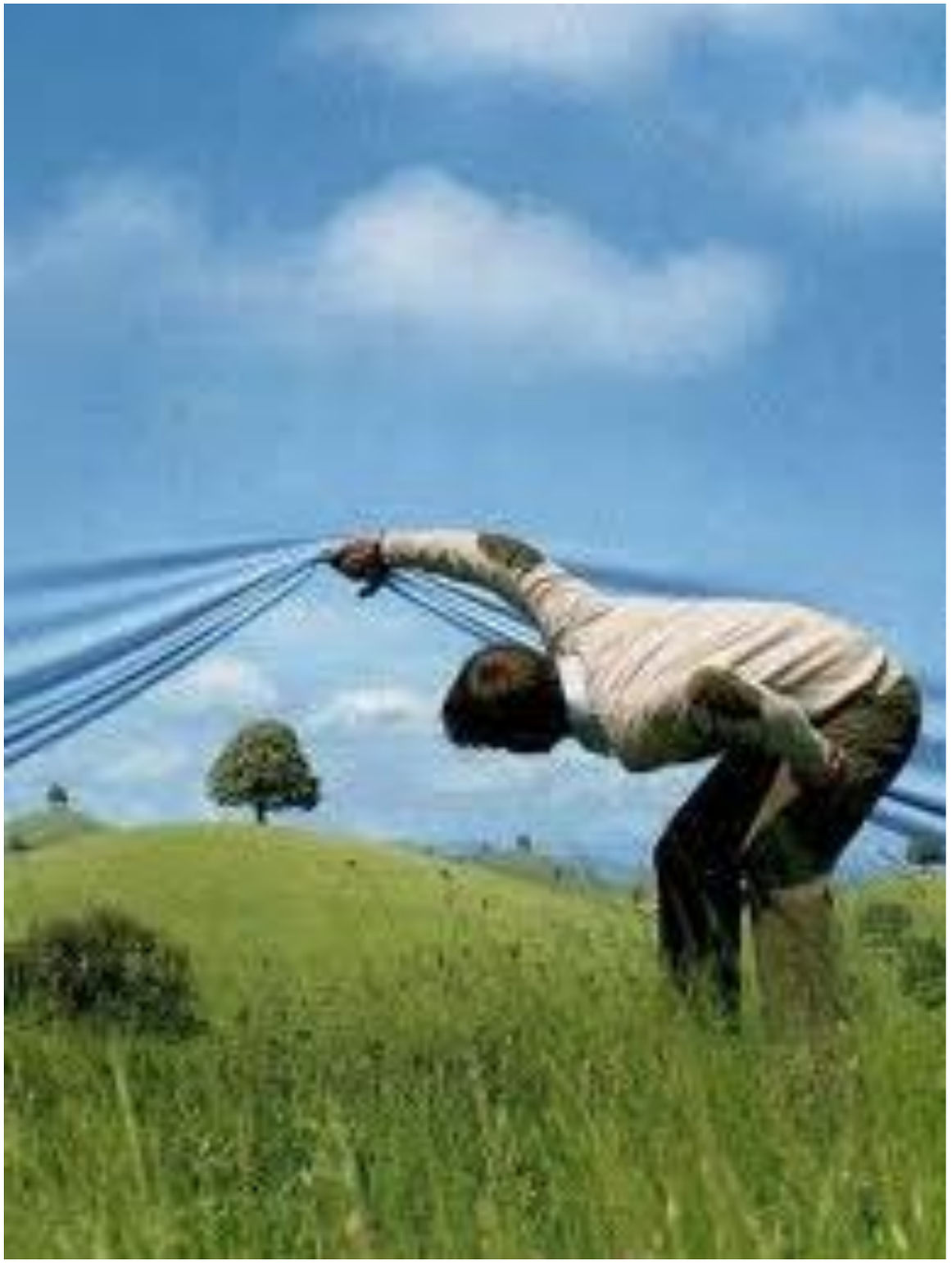
What could we have done better?

- Started sooner
- Buy-in
- Reacted faster
- Logged incidents
- Escalated faster

And now?

> Most users aren't maliciously violating their company security policies, but simply seeking ways to get their jobs done.
>
> - Rene Bonvanie, Palo Alto Networks 2010

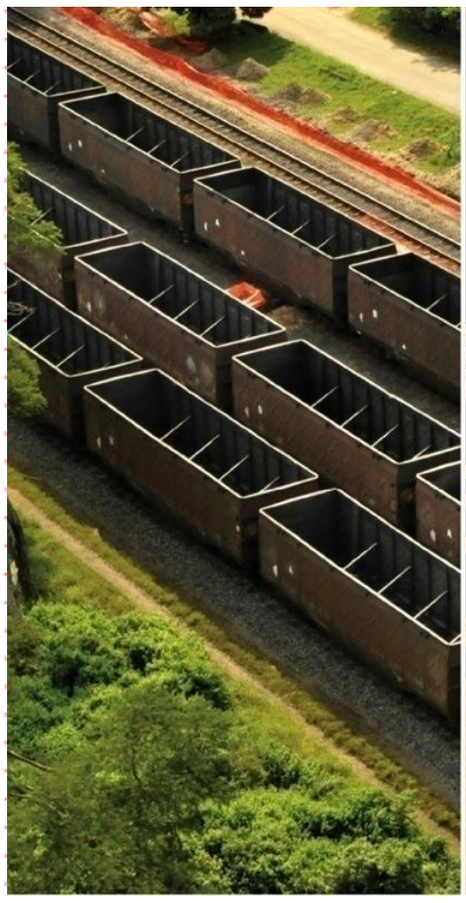
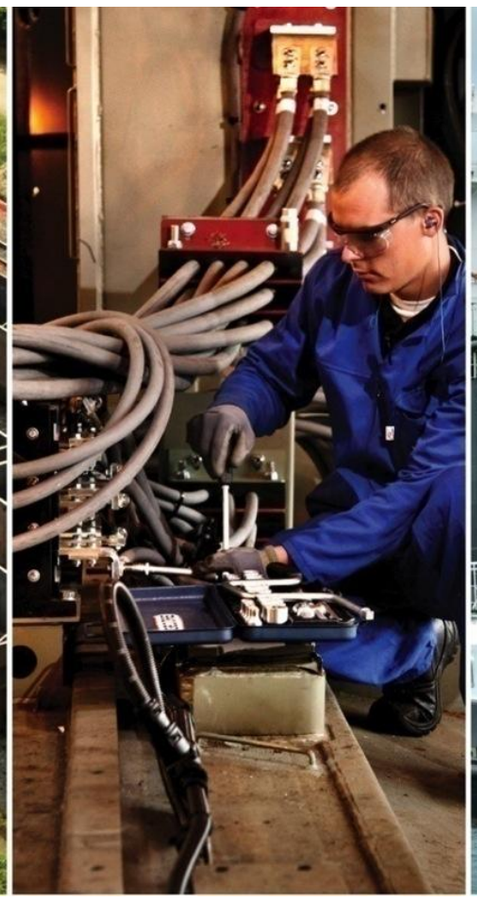
- Continue to be vigilant
- Adjust scanning schedules
- Asset database + notifications
- Differential scans
- More mature solution
- Targeted attack and penetration

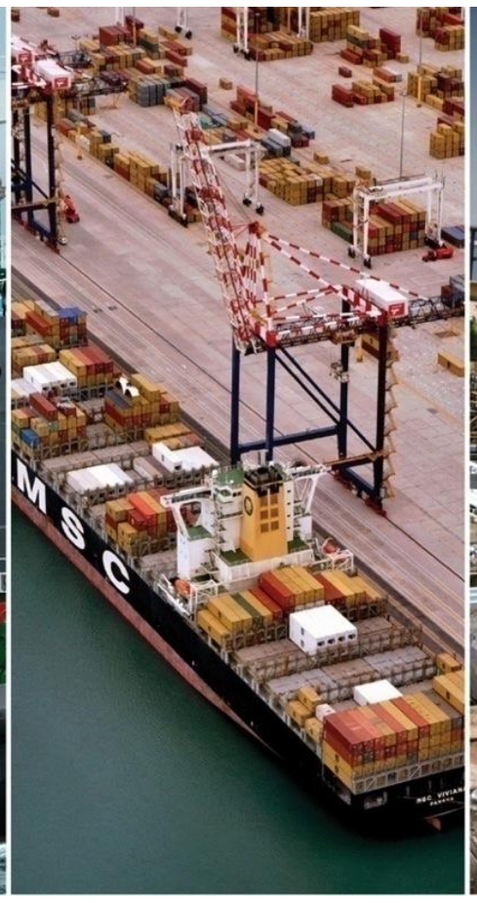


Q&A

TRANSNET

delivering freight reliably



justin.williams@transnet.net
twitter: @jjza
copy of presentation : http://j-j.co.za