



tenable
network security

Outcome Based Security

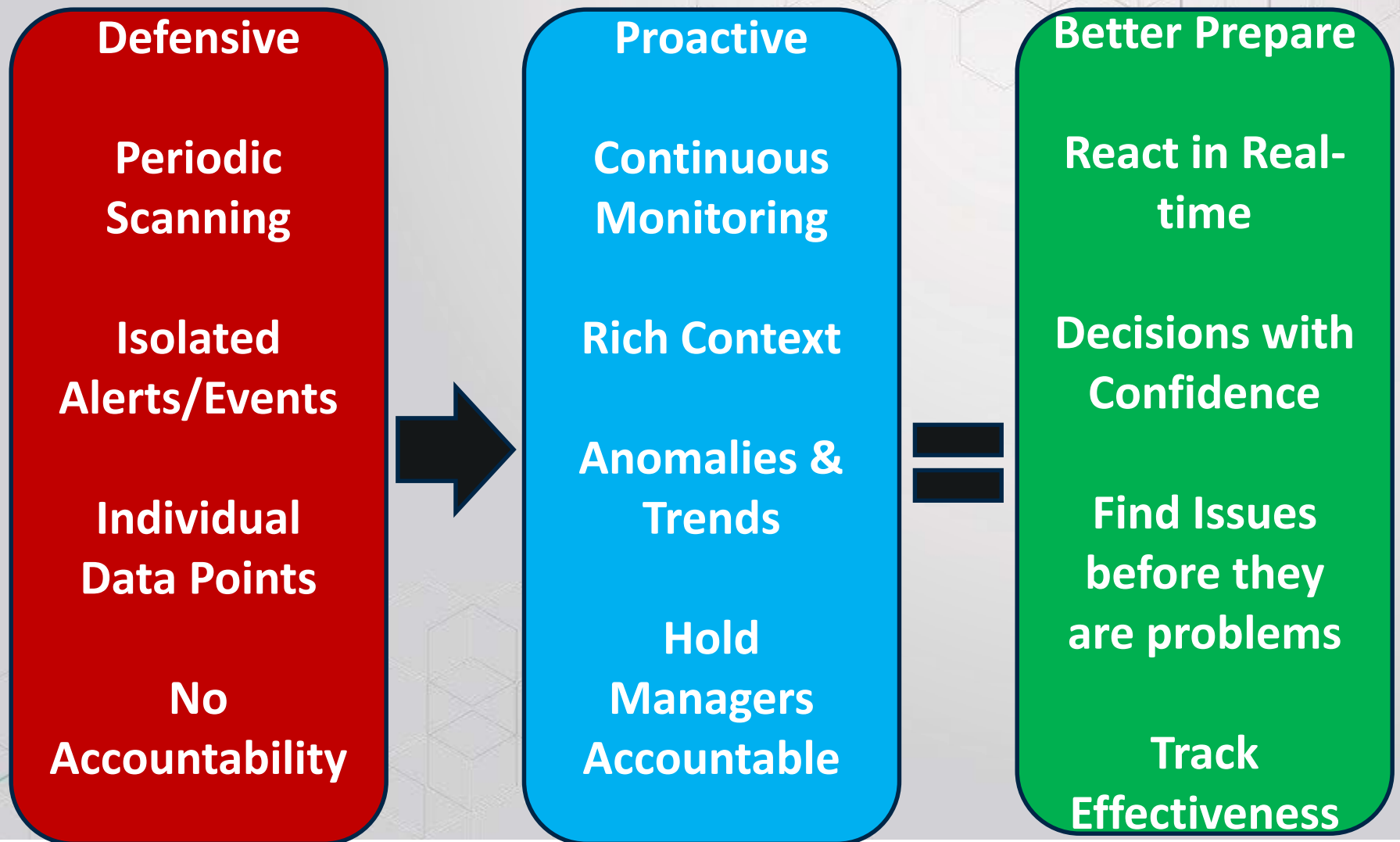
in a Continuous Monitoring World

Background



Traditional Vulnerability Management Programs
are Slow & Ineffective

Outcome-based security is needed...



Five Steps for Continuous Monitoring

**Step 1:
Scan Daily**

**Step 2:
Focus on
Attack
Readiness**

**Step 3:
Fix Daily**

**Step 4:
Grade
Personally**

**Step 5:
Hold
Managers
Accountable**

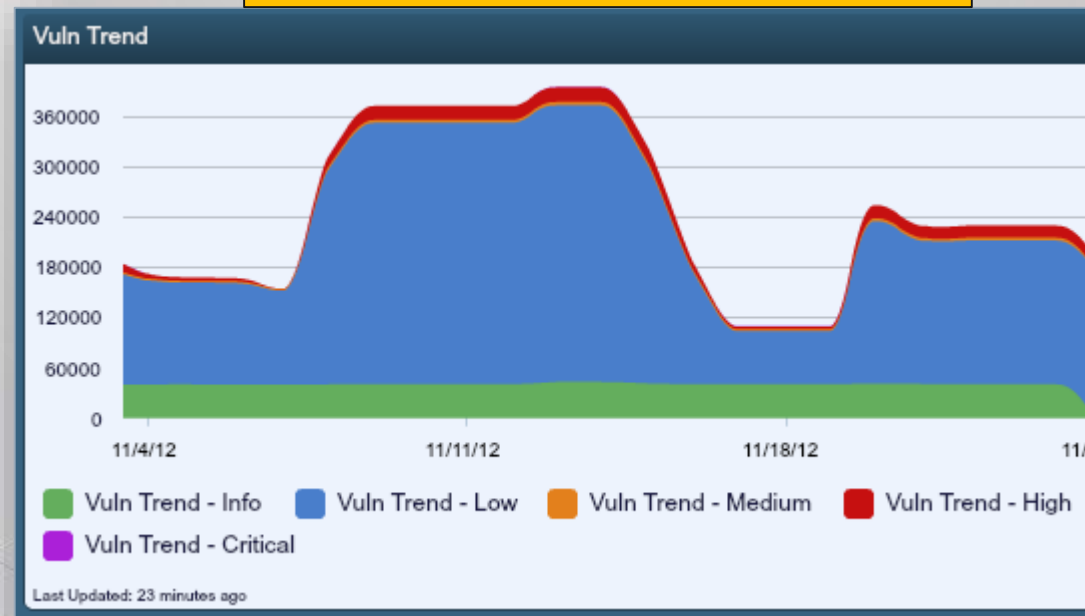
Scan Daily

Step 1: Scan Daily

Need to have...

- Discovery scans
- Real-time vulnerability sniffing
- Credentialed patch and configuration audits
- All managed from single platform

Total Vulnerabilities

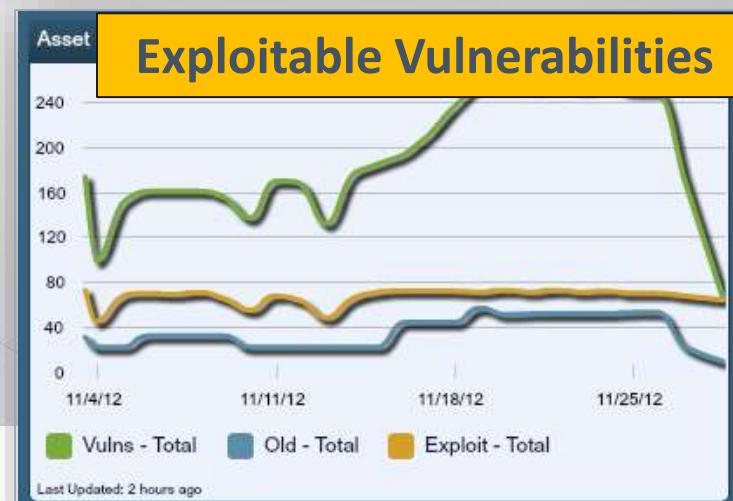
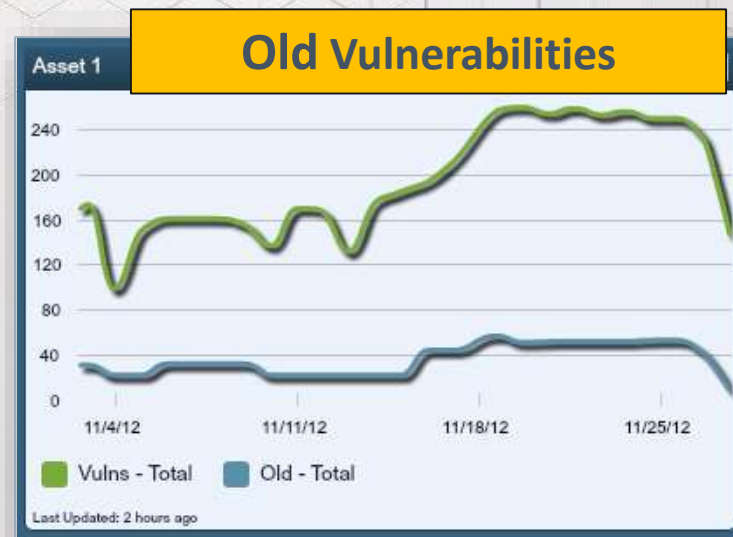


Focus on attack readiness

Step 2: Focus on Attack Readiness

Must identify attack paths in real-time...

- Real-time detection of vulnerabilities
- Correlated to public exploit from penetration testing tools
- Exploitable vulnerabilities
- Tied to existing assets (patching, firewalls, proxies)

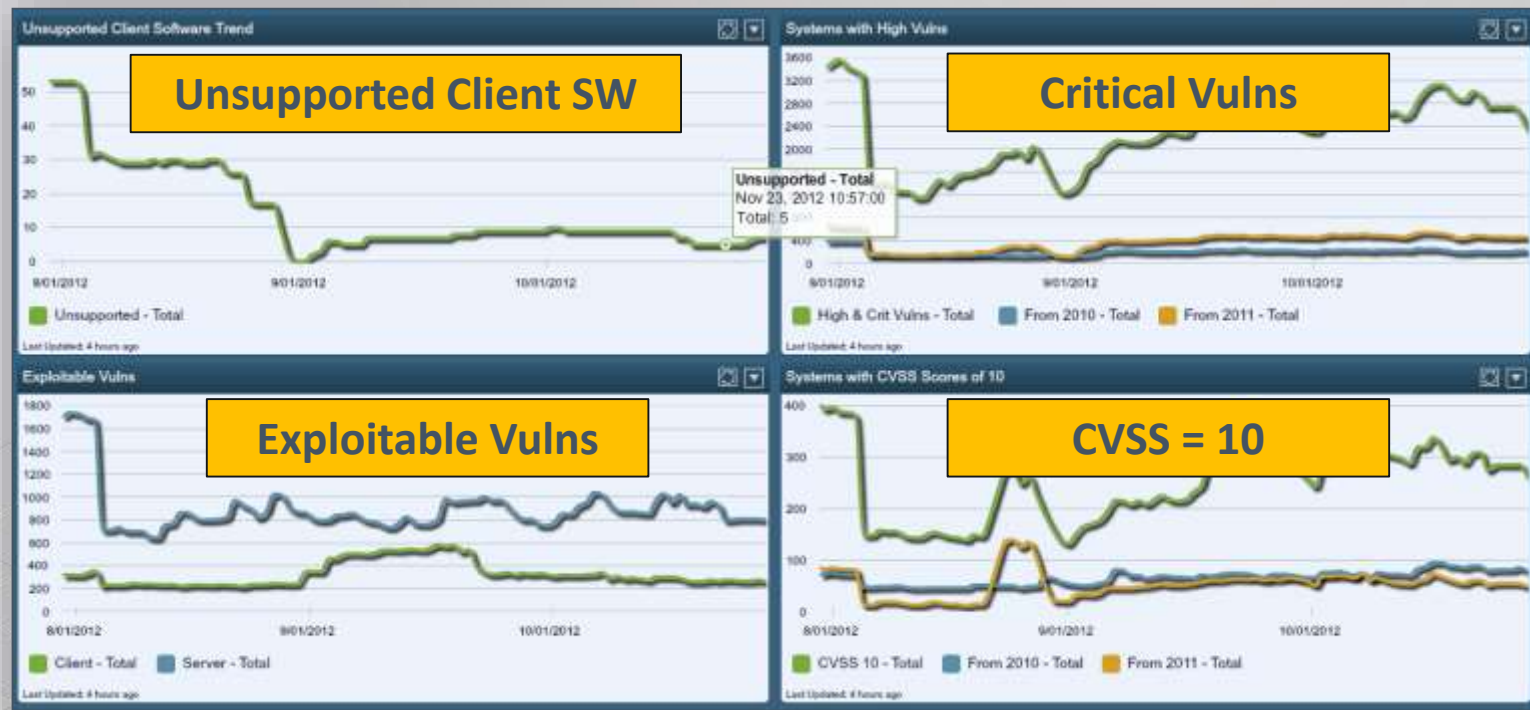


Fix daily

Step 3: Fix Daily

With patching data and long term trending...

- Organizations can track daily progress for more effective security and compliance profile



Grade personally

Step 4: Grade Personally

Associate people with IT assets

- Defined by list of IP addresses or DNS names
- Groups assets to identify intersecting points (Vulnerable Windows hosts vs. Assets of Windows domains)
- Multiple repositories of vulnerability data from different types of scans (External vs. Internal scan)

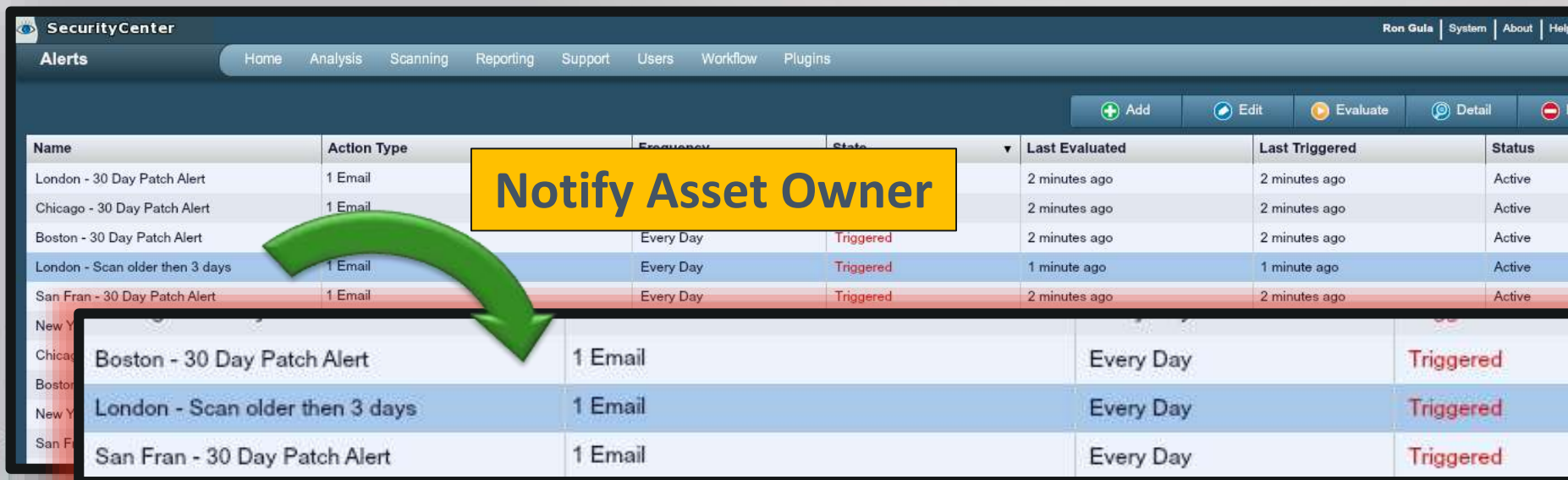


Hold managers accountable

Step 5: Hold Managers Responsible

“Outcome based” auditing in real-time...

- Who owns what systems? Define desired security posture and track deviation against it
- Inform asset owners and admins in real-time when out of compliance



The screenshot shows the Tenable SecurityCenter Alerts interface. The top navigation bar includes 'Home', 'Analysis', 'Scanning', 'Reporting', 'Support', 'Users', 'Workflow', and 'Plugins'. The main content area displays a table of alerts with columns for Name, Action Type, Frequency, State, Last Evaluated, Last Triggered, and Status. A yellow callout box with the text 'Notify Asset Owner' and a green arrow points to the 'Action Type' column of the 'Boston - 30 Day Patch Alert' row.

Name	Action Type	Frequency	State	Last Evaluated	Last Triggered	Status
London - 30 Day Patch Alert	1 Email			2 minutes ago	2 minutes ago	Active
Chicago - 30 Day Patch Alert	1 Email			2 minutes ago	2 minutes ago	Active
Boston - 30 Day Patch Alert	1 Email	Every Day	Triggered	2 minutes ago	2 minutes ago	Active
London - Scan older then 3 days	1 Email	Every Day	Triggered	1 minute ago	1 minute ago	Active
San Fran - 30 Day Patch Alert	1 Email	Every Day	Triggered	2 minutes ago	2 minutes ago	Active

Boston - 30 Day Patch Alert	1 Email	Every Day	Triggered
London - Scan older then 3 days	1 Email	Every Day	Triggered
San Fran - 30 Day Patch Alert	1 Email	Every Day	Triggered

Conclusions

“Outcome-based” security provides...

- **Proactive** vulnerability management
- **Ability to react in real-time** to new vulnerabilities and threats
- **Drives better decisions** through context
- **Identifies trends** before they are problems
- **Makes asset owners more accountable** for systems they manage

For more information...

Whitepaper



“Outcome Based Security Monitoring in a Continuous Monitoring World”

<http://www.tenable.com/expert-resources/whitepapers>

Additional Resources:



Blog

blog.tenable.com



YouTube

youtube.com/tenablesecurity



Website

tenable.com



Discussions

discussions.nessus.org



tenable
network security

