

# Outcome Based Security in a Continuous Monitoring World



# Background



**Traditional Vulnerability Management Programs** 

are Slow & Ineffective



### Outcome-based security is needed...

Defensive Periodic Scanning Isolated **Alerts/Events** Individual **Data Points** No Accountability

#### Proactive

Continuous Monitoring

**Rich Context** 

Anomalies & Trends

Hold Managers Accountable React in Realtime

**Better Prepare** 

Decisions with Confidence

Find Issues before they are problems

Track Effectiveness



### **Five Steps for Continuous Monitoring** Step 2: Step 3: Step 1: **Focus on Fix Daily Scan Daily** Attack Readiness Step 5: Step 4: Hold Grade Managers **Personally** Accountable



# Scan Daily

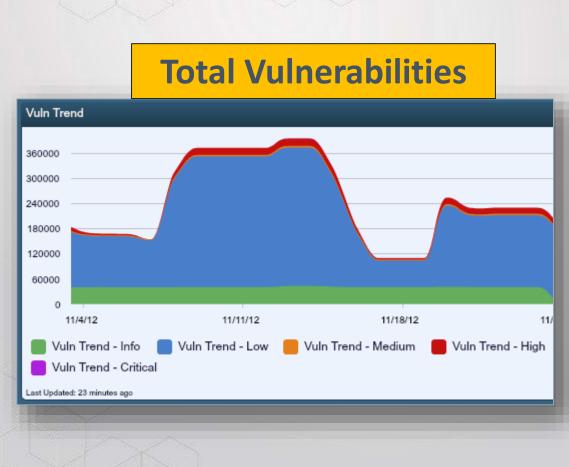




# Step 1: Scan Daily

### Need to have...

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





# Focus on attack readiness

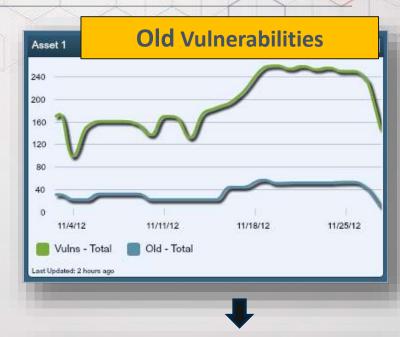


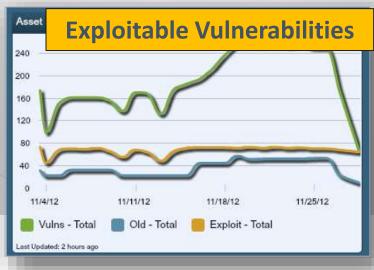
# Step 2: Focus on Attack Readiness

# 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)

		Accete					Exploitable Assets			
Assets		Assets	E D III	Exploitable As	Exploitable Assets		Exploitable Assets			
Asset Score To	otal Vu	ulnerabilities		Asset	Score	Total	Vulnerabiliti	es		
Boston 30064 27	7494	25903		San Fran	1356	261	55		171	
London 6993 73	319	5552	1637	Boston	1197	123		108	12	
San Fran 5799 13	3976	112	85	London	1126	78	18	34	22	
Chicago 2342 26	677	1466 1052		Chicago	124	18	10	8		
New York 394 36	អ 📒	355		New York	0	0				
ast Updated: 2 minutes ago				Last Updated: 1 minu	ute ago					
Assets with 90+ Day Old Vulns 👔 🗸 💌				Assets With E	Assets With External Services					
Asset Score To	otal Vu	ulnerabilities		Asset	Score	Total	Vulnerabiliti	es		
San Fran 1775 80	001	74	07	San Fran	293	94	21	5	68	
Boston 1369 16	518	751 80	0	Boston	21	21		21		
London 485 44	11	173 222		Chicago	4	4	4			
London 485 44 Chicago 225 79		173 222 680		London	0	0	4			

# 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

Alerts Home	e Analysis Scanning	Reporting Support	Users Workflow	Plugins					
						🕀 Add	🗲 Edit 🚺 🜔 Evaluate	e 🔘 De	tail
Name	Action Type	Fromionov		State	▼ Last	Evaluated	Last Triggered		Status
ondon - 30 Day Patch Alert 1 Email		Notify Asset		Ownor	2 minutes ago		2 minutes ago		Active
Chicago - 30 Day Patch Alert	1 Email	NOtify	ASSEL	Owner	2 mi	nutes ago	2 minutes ago		Active
Boston - 30 Day Patch Alert 🧹			Every Day	Triggered	2 mi	nutes ago	2 minutes ago		Active
London - Scan older then 3 days	1 Email		Every Day	Triggered	1 mi	nute ago	1 minute ago		Active
San Fran - 30 Day Patch Alert	1 Email		Every Day	Triggered	2 mi	nutes ago	2 minutes ago		Active
New Y						1.			
Chicas Boston - 30 Day Pa	1 Email			Every Day		Triggered			
<sup>Bostor</sup> New Y London - Scan old	1 Em	1 Email			Every Day			Triggered	
San Fran - 30 Day	1 Em	1 Email			Every Day			Triggered	



"Outcome-based" security provides... Proactive vulnerability management o 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





