Outcome Based Security
in a Continuous Monitoring World
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
- Better Prepare: React in Real-time, Decisions with Confidence, Find Issues before they are problems, Track Effectiveness
Five Steps for Continuous Monitoring

1. Step 1: Scan Daily
2. Step 2: Focus on Attack Readiness
3. Step 3: Fix Daily
4. Step 4: Grade Personally
5. 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
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

![Graph showing supported and unsupported client software trends, critical vulnerabilities, exploitable vulnerabilities, and CVSS score of 10.](image-url)
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
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