Vulnerability Management That Works
Who Am I?

- Just a Security Guy
- OWASP Orlando
- Bsides Orlando
- FLSEC
- DC407
- Worked internal for 18+ years
- Sr Security Consultant GuidePoint Security
CSIRT vs Vulnerability Mgmt

- Not mutually exclusive
- Consider VM as a CSIRT Program component
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned
Why Do We Care?

• Compliance (I really wish this was farther down the list)
  – PCI DSS
  – HIPAA/Hi-Tech
  – Legislation
  – Others
Who Needs Vulnerability Management?
Whoops.
(Hard) Costs of an incident

- Breach Monitoring Services
- Breach Notification
- Fines
- Lawsuits
- Incident Response/Remediation Services
- Overtime
(Soft) Costs of an Incident

- Reputation Loss (Jury is out on whether this really matters)
- Lost productivity is hard to measure
- A lot of incident related work may never be fully documented
- Taking risks is part of business, becoming too risk adverse stifles innovation
What if there is no impact?

Try Harder

(Hint: There is always impact)
Resistance to VM

- Painful all around
- Ops guys have different priorities
- Security guys often have no authority
- Compliance driven
- Nobody has staffing resources
- Lack of proper QA
- Hard to keep up with VM (virtual machine) creep
- No workflows
But We Have Remediation Reports!
Current State of Vuln Management

• Lots of detection tools
• Really good at telling you how hopeless things are
• Really good at making money for tool vendors
• Huge Reports that aren’t terribly helpful
• Very few tools that actually help us fix anything
Tickets

- Do you find tickets useful?
- Largely Self contained
- Don’t integrate with workflows
- How often does Ops log into VM tools?
- Can we integrate with Remedy already?
Rapid7

- NeXpose Community, Enterprise
- Metasploit Integration
- Very easy to write custom vuln checks (XML format)
- PCI DSS leadership
- Awesome for consultants
- Sales guys not as pushy anymore
Qualys

- SASS model
- Very PCI friendly – most popular ASV tool
- Web scanning - Most do this to some degree
- SSL Research (Ivan Ristic – SSL Labs)
- Reports painful to filter for uninitiated but reporting often listed as a core strength.
nCircle

- Suite of purchased products
- Core developers went to Rapid7
- Support issues
- Excellent Metrics
- Can assign asset values granularly
- Excellent reporting
- Reporting is licensed SEPARATELY!
Retina

- First to market with mobile scanning
- 3rd party patching w/ WSUS and SCCM
- Identity aware with Power Broker
- Easy to create custom checks
- Huge in Federal space – Gold Disk Compliance
- Runs on Windows
- Tends to be a little unstable
Tenable

- Nessus vs Security Center
- Dashboards
- WSUS/Altiris Integration
- Dashboards
- Can rescan from within ticket
- Best workflows
Commercial Webapp Scanners

• AppScan
• Netsparker
• WebInspect
• Acunetix
• Hailstorm
• Burp Suite Pro
Free and Open Source Webapp Scanners

- Burp
- Skipfish
- W3AF
- Arachni
- Vega
- Zed Attack Proxy (OWASP ZAP)
- Specialty tools (Wpscan, joomscan, etc) and many more!
2012 Web App Vuln Scanner Review

2012 Comparison of 49 free and open source scanners

http://sectooladdict.blogspot.co.il/2012/07/2012-web-application-scanner-benchmark.html
Still Left Wanting…

None (or few) of these tools actually help us **fix** anything
Oh Good, It’s Broken. Now what?
How do we Fix it?

• Lifecycle Management (See stages)
• Tracking Vulnerabilities
• Embedding Workflows/ticketing in operations teams
• Metrics reporting to management
• Embedding VM in security incident response team processes
VM is a Lifecycle

- Identify
- Classify
- Mitigate
- Remediate
Identifying Vulnerabilities

• Network Ranges
• Physical Locations
• Inventory Assets
• Classify Assets
• Examine Trust Relationships
• Attack Paths
• What’s Vulnerable?
Classifying Vulnerabilities

Risk = Likelihood * Impact

- Assets already classified
- How likely is the vulnerability to be exploited?
- Does it matter?
If a tree falls in the forest…
Classification Continued

• Vulnerability Scanners may help to identify risk but typically have ZERO context.
• Include business value
• Trust relationships
• Operational impacts
• Need humans to decide
Mitigating Vulnerabilities

• When the Fix is riskier than leaving it alone
• Compensating Controls
• Creating trust zones
• Reducing data footprint
• Reduce focus, wrap controls around the data
• Change Management
Remediating Vulnerabilities

- Patch Management
- Configuration Control
- Writing secure code
Tracking Vulnerabilities

• Centralized repository
• Spreadsheets are better than nothing
• Don’t wait for the perfect solution, start doing SOMETHING today!
• Enter SIEM!
SIEM Monitoring

- Can consume most logs, email events or other tool output.
- Consistent formatting to generate emails into ticketing system
- Single pane of glass to compare and correlate detected vulnerabilities with ongoing events
Custom Applications

• Only useful if people use them
• Need to understand the tools staff are using today and integrate with what's working currently.
• These are operational tasks.
Vulnerability Mgmt Process

Scan/Identify  Prioritize Vuln  Create Workorder  Remediate/Mitigate  Re-scan  Close Workorder
Management Buy-In

• Operations gets their priorities list from above
• We have to educate management
• Metrics help
Metrics that Work

• % of Critical Assets w/significant Vulnerabilities
• Lag time to remediate vulnerabilities
• FTE time or other resources required to fix
• Vulnerabilities contributing to root cause for past incidents or similar
• Correlation between attacks seen and prevented by vuln mgmt
Useless Metrics

• We remediated X number of vulnerabilities.

• Metrics and trending from groups that are also experiencing scope creep or reduction

• Base CVSS scores
Questions?

• Tony Turner
• @tonyllturner
• tony.turner@guidepointsecurity.com
• tony.turner@owasp.org