RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-W03

Pragmatic Metrics for Building Security Dashboards

James Tarala

Principal Consultant
Enclave Security
@isaudit

Problem Statement

- “What’s measured improves.” – Peter Drucker
- In an era of security breaches we tend to have only one metric – Have my systems been compromised?
- But how do our organization’s measure progress?
- How do we know if we’ve accepted a reasonable level of risk?
- And why are security engineers making so many business decisions for our organizations?

Suggested Solution

- Proposed Solution = Meaningful Metrics

- Organizations need a way to measure security risk in a meaningful way
- Better communication is necessary between business owners and security teams
- Business leaders need information to make better decisions

Why are Metrics Needed?

- Businesses use metrics to facilitate decision making
- Better data leads to better decisions & allows organizations to set appropriate priorities
- Measurement allows comparison:
  - Between our organization and industry benchmarks
  - Between our organization and other organizations risk levels
  - Between levels of accepted risk over time
  - Between business units within an organization

Metrics from the Business World

- The business world uses metrics all the time
- Consider the following examples:
  - Price to Earnings Ratio
  - Profit & Loss Statements
  - Product Sales Quotas
  - Number of Safety Incidents
  - Unit Production
  - Number of Facebook “Likes” per Post

Metrics in Technology

- Organizations even commonly use metrics to help measure the performance of technology systems as well
- Consider the following examples:
  - System uptime
  - CPU Utilization Percentage
  - Average Email Mailbox Size
  - Support Technician to Computer Node Ratio
  - Help Desk Ticket Time to Resolution

IS Metrics: Too Broad?

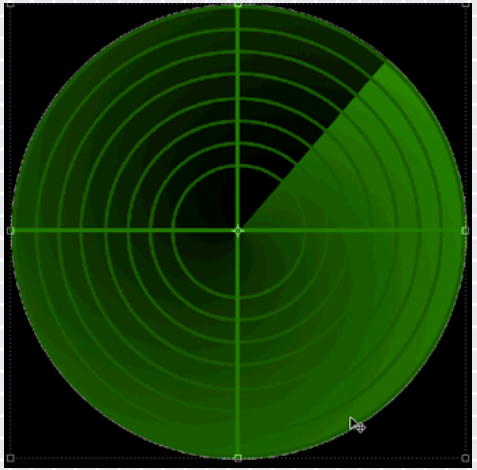
- The first question we need to ask is, “What do we mean by the term Information Security metrics?”
- IS Metrics is too broad of a term
- **“Begin with the end in mind.”** – Stephen Covey
- Measurement for measurement’s sake helps no one
- Organizations must be specific on what they are measuring and the benefits they hope to achieve from it

Potential Metrics Categories

- In the realm of information security, organizations may want to consider measuring:
  - System availability / performance metrics
  - Network utilization metrics
  - Incident management metrics
  - Security budget metrics
  - Software development risk metrics
  - System defense metrics

Metrics for System Defense

- Most of you are looking for cool dashboards & system defense metrics
- You read the Wall Street Journal & Financial Times, and you want to keep bad actors off your systems
  - Advanced Persistent Threat = Scary
  - Nation State Attacks = Scary
  - Cyberwar = Scary
- **So what metrics should you choose?!?**



Current Research Projects

- NIST Special Publication 800-55 (rev 1): Performance Measurement Guide for Information Security
- Security Content Automation Protocol (SCAP) / Common Vulnerability Scoring System (CVSS)
- CIS / SANS Critical Security Controls
- Center for Internet Security (CIS) Consensus Information Security Metrics
- Incident Management Capability Metrics (Carnegie Mellon Software Engineering Institute)
- Verizon Incident Sharing framework (VERIS)
- Systems Security Engineering – Capability Maturity Model (SSE-CMM)

Example: Critical Security Control #1

- **Inventory of Authorized and Unauthorized Devices**

- Exploit this Control is Meant to Stop:
  - Exploits due to lack of implemented controls on unknown (un-inventoried) devices
- Business goal of this control:
  - Only authorized systems should be on the agency's network.

Evaluation Test for Control #1

- Place ten unauthorized devices on various portions of the organization's network unannounced to see how long it takes for them to be detected
  - They should be placed on multiple subnets
  - Two should be in the asset inventory database
  - Devices should be detected within 24 hours
  - Devices should be isolated within 1 hour of detection
  - Details regarding location, department should be recorded

Core Effectiveness Metrics for CSC #1

ID	Testing / Reporting Metric	Response
1a	How long does it take to detect new devices added to the organization's network?	Time in Minutes
1b	How long does it take the scanners to alert the organization's administrators that an unauthorized device is on the network?	Time in Minutes
1c	How long does it take to isolate / remove unauthorized devices from the organization's network?	Time in Minutes
1d	Are the scanners able to identify the location, department, and other critical details about the unauthorized system that is detected?	Yes/No

Automation Metrics for CSC #1

1. How many unauthorized devices are presently on the organization's network (by business unit)?
2. How long, on average, does it take to remove unauthorized devices from the organization's network (by business unit)?
3. What is the percentage of systems on the organization's network that are not utilizing Network Access Control (NAC) to authenticate to the organization's network (by business unit)?
4. What is the percentage of systems on the organization's network that are not utilizing Network Access Control (NAC) with client certificates to authenticate to the organization's network (by business unit)?

Australian DSD Top 35 / “Sweet Spot”

- Australian Top 35 Mitigation Strategies, Australian Department of Defence
- Defensive controls to block over 85% of attacks directed against their systems
- They are ranked in order of overall effectiveness
- Rankings are based on DSD’s analysis of reported security incidents and vulnerabilities detected by DSD
- They also define 4 top controls as their “sweet spot”

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Aus DSD #1: Application Whitelisting

- **Specific Australian DSD Top 35 Control:**

  "Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker." – Australian DSD

- **Business Purpose:**

  To limit the likelihood of successful vulnerabilities being exploited by limiting the allowable application binaries that are allowed to execute on a system.

Aus DSD #1: Application Whitelisting (cont)

- Potential Metric:

  Establish a baseline of all necessary binaries that would run on a system by system and business unit & establish a risk score for all binaries that execute successfully that are not on the approved binaries baseline

- US Dept of State iPost Formula:

  Product SOE Score = 5.0 (for each product)

  Host SOE Score = SUM(SOE scores for each product)

Aus DSD #2: Patch Applications

- **Specific Australian DSD Top 35 Control:**

  “Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications.” – Australian DSD

- **Business Purpose:**

  To limit the vulnerabilities attackers can exploit by eliminating software application vulnerabilities on enterprise systems.

Aus DSD #2: Patch Applications (cont)

- **Potential Metric:**

  Gather the composite Common Vulnerability Scoring System (CVSS) score of all systems by business unit, according to your vulnerability scanning software

- **US Dept of State iPost Formula:**

  DoS VUL Score = (CVSS Score)N / 10(N-1) where N=3

  Host VUL Score = SUM(VUL scores of all detected vulnerabilities)

  Host PAT Score = SUM(PAT scores of all incompletely installed patches)

Aus DSD #3: Patch OSs

- **Specific Australian DSD Top 35 Control:**

  “Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version.” – Australian DSD

- **Business Purpose:**

  To limit the vulnerabilities attackers can exploit by eliminating operating system coding vulnerabilities on enterprise systems.

Aus DSD #3: Patch OSs (cont)

- **Potential Metric:**

  Gather the composite Common Vulnerability Scoring System (CVSS) score of all systems by business unit, according to your vulnerability scanning software

- **US Dept of State iPost Formula:**

  DoS VUL Score = (CVSS Score)N / 10(N-1) where N=3

  Host VUL Score = SUM(VUL scores of all detected vulnerabilities)

  Host PAT Score = SUM(PAT scores of all incompletely installed patches)

Aus DSD #4: Limit Admin Rights

- **Specific Australian DSD Top 35 Control:**

  “Minimize the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.” – Australian DSD

- **Business Purpose:**

  To limit the likelihood of successful vulnerabilities being exploited by limiting the rights of users on operating systems.

Aus DSD #4: Limit Admin Rights (cont)

- **Potential Metric:**

  Create secondary accounts (admin) for anyone needed elevated rights, establish a baseline of the admin accounts created, & establish a risk score every time a non-baselined admin account or standard user account is configured as an administrator on each system

- **US Dept of State iPost Formula:**

  SCM Score for a check = score of the check's Security Setting Category

  Host SCM Score = SUM(SCM scores of all Failed checks)

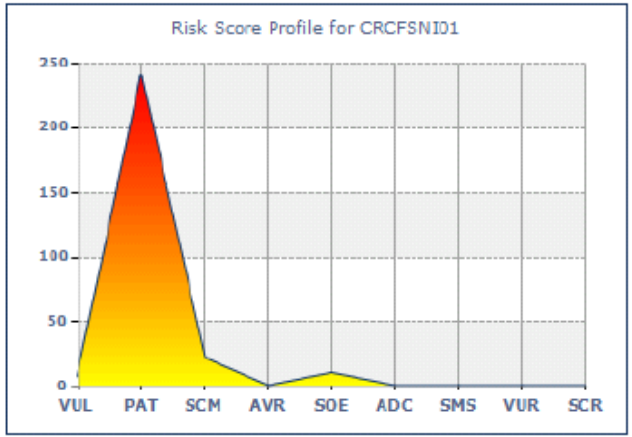
Sample DoS iPost Reporting

Configuration | Software | Services | Compliance | Vulnerabilities | Patches | SOE | AD Info | Risk Scores

Server Workstation [redacted]

Risk Scores for Host: [redacted]

Risk Score Component	Risk Score	Additional Information
Vulnerability	8.04	Vulnerabilities: 10
Patch	240.00	Unapplied Patches: 1
Security Compliance	21.29	Failed Checks: 37
Anti-Virus	0.00	Definition Date: Mar 10, 2010
SOE Compliance	10.00	Non-Compliant Products: 2
AD Computers	0.00	Computer Pwd Age: 1 Days
SMS Reporting	0.00	SMS Errors: 0
Vulnerability Reporting	0.00	Last Scan: Mar 10, 2010
Security Compliance Reporting	0.00	Last Scan: Feb 26, 2010
Total Risk Score:	**279.33**	



http://www.state.gov/documents/organization/156865.pdf

Maturity Model

- These steps move us towards an overall implementation & assessment maturity model:
  - **Level #0:** Project Initiation / Policy Defined
  - **Level #1:** Policies Formalize Statements of Management Intent
  - **Level #2:** Critical Security Controls 1-5 Implemented & Audited
  - **Level #3:** All Critical Security Controls Implemented & Audited
  - **Level #4:** All Critical Security Controls Automated
  - **Level #5:** All Critical Security Controls Reported to Business Leaders

Our Primary Recommendation

1. Start small, excel at gathering a small number of metrics
2. Integrate these metrics into your business process
3. Grow the number of metrics you collect

United States Department of State iPost began with only three data sensors:

- Tenable Nessus
- Microsoft Active Directory
- Microsoft System Management Server (System Center)

Apply Practical Steps: Base

- To create an effective, sustainable program to implement metrics, don't start by creating metrics
- Out recommendation would be:
  1. Obtain a security management charter from senior management
  2. Create an organization wide IS Steering Committee
  3. Document your organization's overall security goals
  4. Create & approve appropriate security policies, procedures, & standards
  5. Educate your organization on those documents

Apply Practical Steps: Phase I

- Once a base or foundation for information assurance is laid, then you can begin with metrics
- The next phase would be to:
  1. Identify what information security sensors you have already successfully deployed
  2. Determine what meaningful metrics can be gleaned from these sensors
  3. Deploy a tool that can centrally aggregate, normalize, and report on the data collected by the sensors
  4. Create basic reports based on the metrics from strep #2
  5. Work with business owners to remediate risk

Apply Practical Steps: Phase II

- Now you are ready for continuous process improvement
- The last steps are to refine your effort, gather more data, and remediate more risk:
  1. Deploy additional sensors & aggregate the results
  2. Determine meaningful metrics that new sensors can bring
  3. Collaborate with business owners to make metrics more meaningful
  4. Remediate new risks as they are discovered
  5. Automate the response to as many metrics as possible

Bare Minimum Response

1. Create an asset inventory
2. Assign data owners to all of your systems
3. Deploy a vulnerability scanner & scan all of your hosts on a regular basis
4. Create overall CVSS risk scores, by business unit, and publish those scores to key business owners
5. Remediate the risk you discover

- Focus on the basics, then improve your efforts
- Run a 5K first, then try a marathon