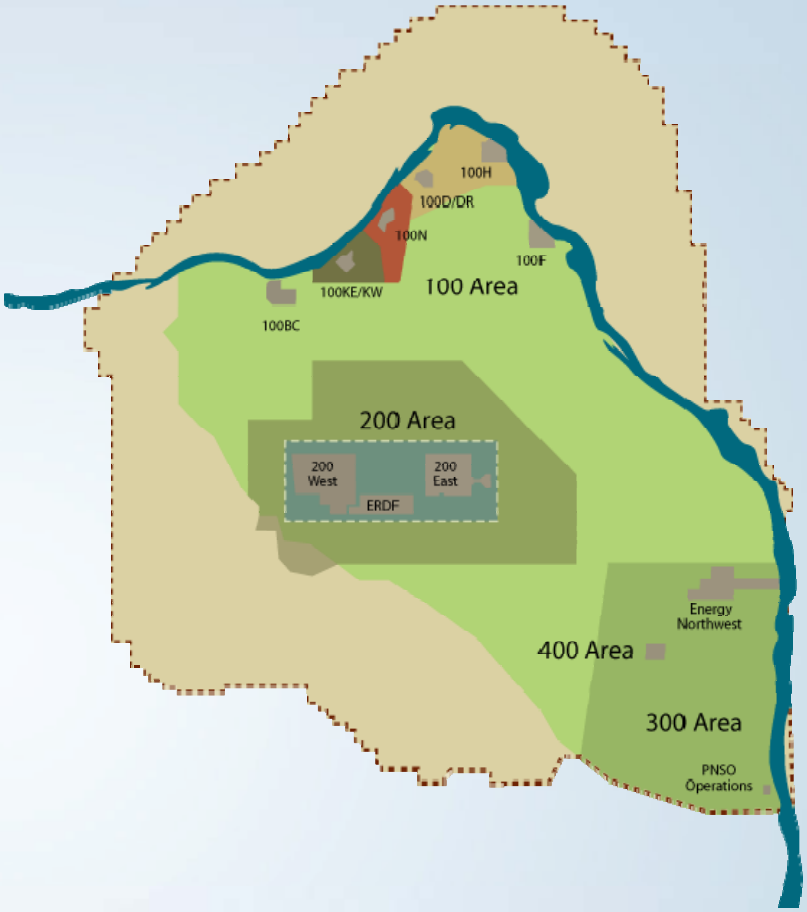
A Report from the Field:

Implementing Cyber Security Metrics that Work

Rick Grandy & Gregg Serene
Cyber Security
MSA/Lockheed Martin

DOE Hanford Site

"To make our customers extraordinarily successful in our unified mission of cleaning up the Hanford Site…"



Hanford Site Scope

- 586 square miles
- 9,000+ PCs
- 500+ servers
- 400+ applications
- 1,000+ miles fiber to 300 bldgs
- 12,500+ phones

Why Metrics?

- How do you know if you're doing well in school?

- How do you know if an athlete is performing well?

Robin Roberts' Career Statistics

Year	Team/League	W	L	PCT	G	SV	IP	H	BB	SO	ERA	BH	AVG
1948	Phillies/N	7	9	.438	20	0	146	148	61	84	3.19	11	.250
1949	Phillies/N	15	15	.500	43	4	226	229	75	95	3.69	5	.075
1950	Phillies/N	20	11	.645	40	1	304	282	77	146	3.02	12	.118
1951	Phillies/N	21	15	.583	44	2	315	284	64	127	3.03	15	.172
1952	Phillies/N	28	7	.800	39	2	330	292	45	148	2.59	14	.125
1953	Phillies/N	23	16	.590	44	2	346	324	61	198	2.75	22	.179
1954	Phillies/N	23	15	.605	45	4	336	289	56	185	2.97	15	.123
1955	Phillies/N	23	14	.622	41	3	305	292	53	160	3.28	27	.252
1956	Phillies/N	19	18	.514	43	3	297	328	40	157	4.45	20	.200
1957	Phillies/N	10	22	.313	39	2	249	246	43	128	4.07	13	.162
1958	Phillies/N	17	14	.548	35	0	269	270	51	130	3.24	20	.202
1959	Phillies/N	15	17	.469	35	0	257	267	35	137	4.27	17	.191
1960	Phillies/N	12	16	.429	35	1	237	256	34	122	4.02	12	.152
1961	Phillies/N	1	10	.091	26	0	117	154	23	54	5.85	3	.091
1962	Orioles/A	10	9	.526	27	0	191	176	41	102	2.78	10	.192
1963	Orioles/A	14	13	.519	35	0	251	230	40	124	3.33	16	.203
1964	Orioles/A	13	7	.650	31	0	204	203	52	109	2.91	9	.132
1965	Orioles/A	5	7	.417	20	0	114	110	20	63	3.38	6	.171
	Astros/N	5	2	.714	10	0	76	61	10	34	1.89	5	.238
1966	Astros/N	3	5	.375	13	1	63	79	10	26	3.82	1	.063
	Cubs/N	2	3	.400	11	0	48	62	11	28	6.14	2	.200
Total		286	245	.539	676	25	4,688	4,582	902	2,357	3.41	255	.167

W = Wins, L = Losses, PCT = Percentage, G = Games, SV = Saves, IP = Innings Pitched, H = Hits, BB = Bases on Balls, SO = Strike Outs, ERA = Earned Run Average, BH = Base Hits, AVG = Average.

- How do you know if you're healthy?
  - Weight, Blood Pressure

Why Metrics?

- Does a FISMA Score of “A” mean…
  - The cyber program is more effective?
  - The cyber program is more efficient?
  - The network is more secure?
  - The network can withstand APT attacks?

- Cyber tends to be a black hole….
  - Management & users don’t understand how it works
  - Visible when cyber puts up road blocks “*No”*
  - “No news is good news”

Our Motivation

- Rick's the new guy
  - Wanted to get a handle on what was going on
  - Was used to IT and business process metrics
  - Wanted data to enable improvement
  - Wanted to be more transparent with management and customer
    - Cyber is complex, let's not make decisions in a vacuum
    - Let them get more engaged with the program
    - Helps build relationships
- Not a DOE Order or contract requirement
  - Proposed to DOE as contract Performance Incentive (PIs)

Our Approach

- ***Keep the metrics meaningful***
  - Tie to cyber program processes
  - Avoid incentivizing the wrong behavior
- ***Keep the metrics reproducible***
  - Develop rigorous, objective definitions
  - Build useful desk procedures/checklists
- ***Keep the metrics manageable***
  - Leverage existing automated sources of data
  - Make practical decisions to narrow scope as needed
- ***Provide an increased level of transparency***

Requirements

- Not a lot of normative guidance
- Metrics are explicitly required in a few areas:
  - Contingency plan (CP-2*)
  - Recovery and restoration procedures (CP-10*)
  - Patch and vulnerability management procedures (CMG-85**)
  - Incident response plan (IR-8*)

*NIST SP 800-53 Rev 3 **DOE US PCSP 1.2

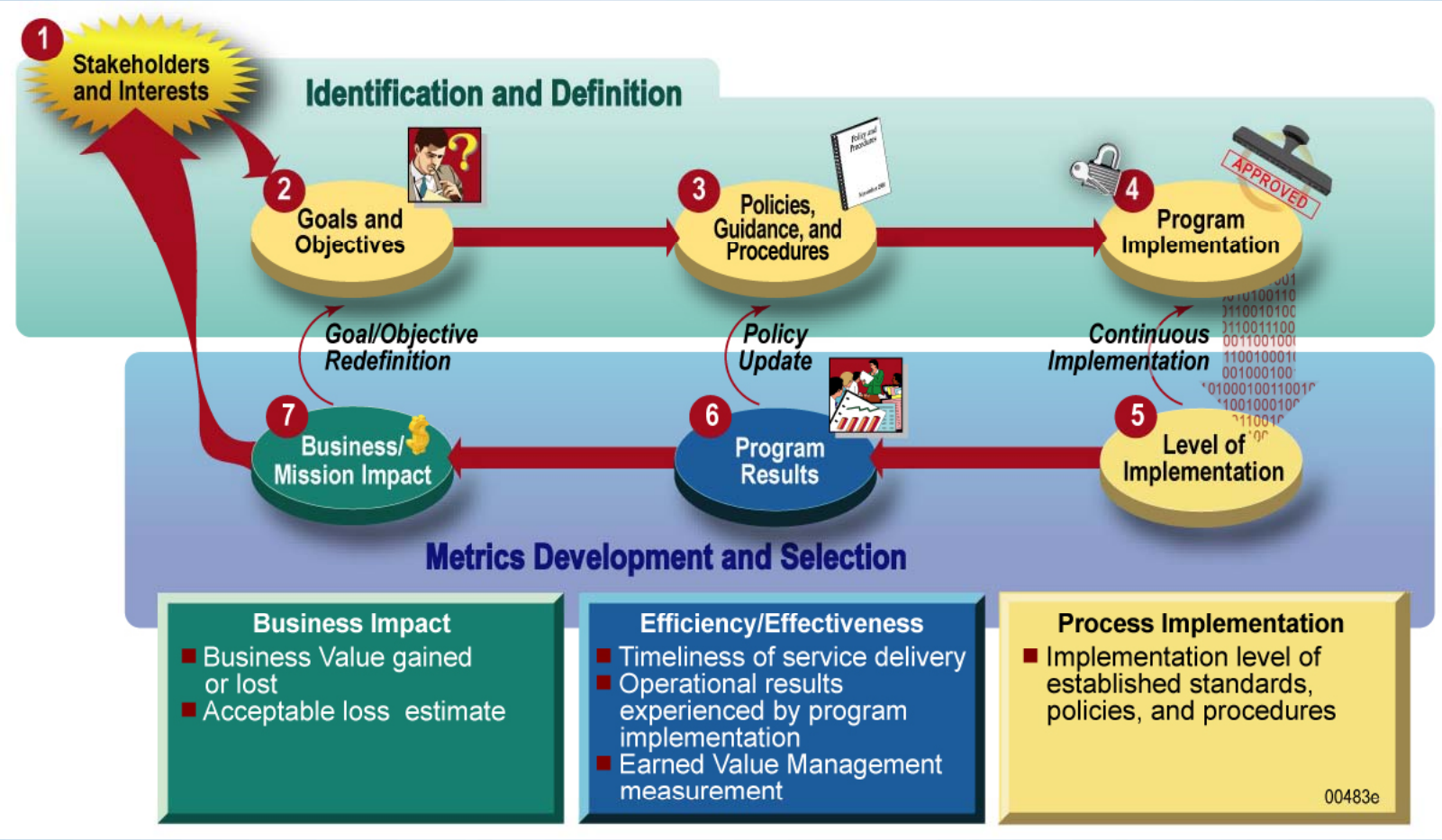
How to Do a Metrics Program

- S. Payne, “A Guide to Security Metrics”
- NIST 800-55 Rev 1, Sections 5.0-6.0
- NIST 800-100, Section 7.0 (summarizes 800-55)

Payne: Seven Steps

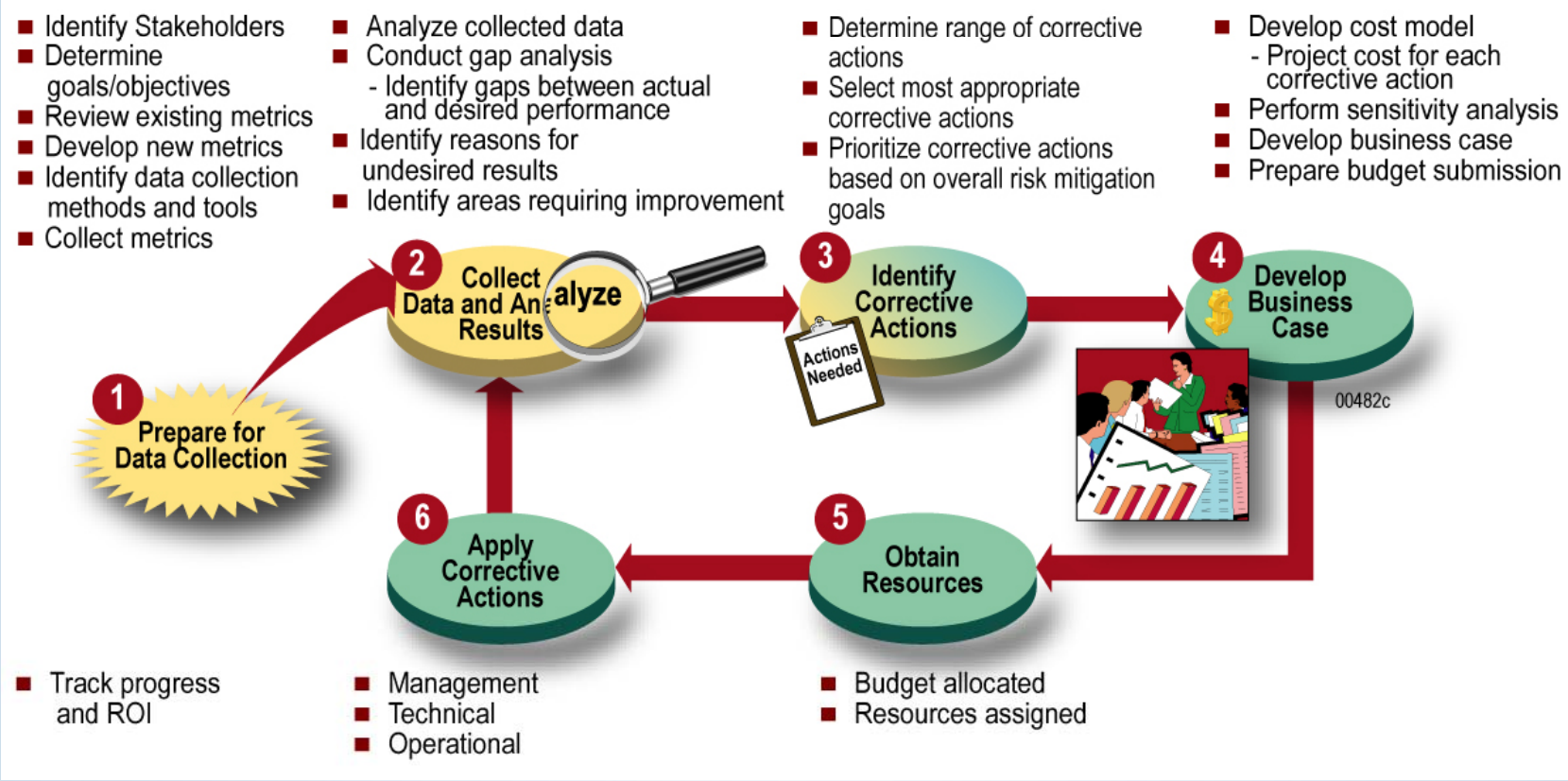
1. Define the metrics program goal(s) and objectives
2. Decide which metrics to generate
3. Develop strategies for generating the metrics
4. Establish benchmarks and targets
5. Determine how the metrics will be reported
6. Create an action plan and act on it, and
7. Establish a formal program review/refinement cycle

NIST: Integrated Program



Source: NIST SP 800-100, Figure 7-1

Collecting and Analyzing Data



Source: NIST SP 800-100, Figure 7-2

The Chicken and the Egg

- Metrics must be focused on specific things you want to measure
- You need metrics to know what you need to focus on

Problem: *You don't know what you don't know!*

Our Situation

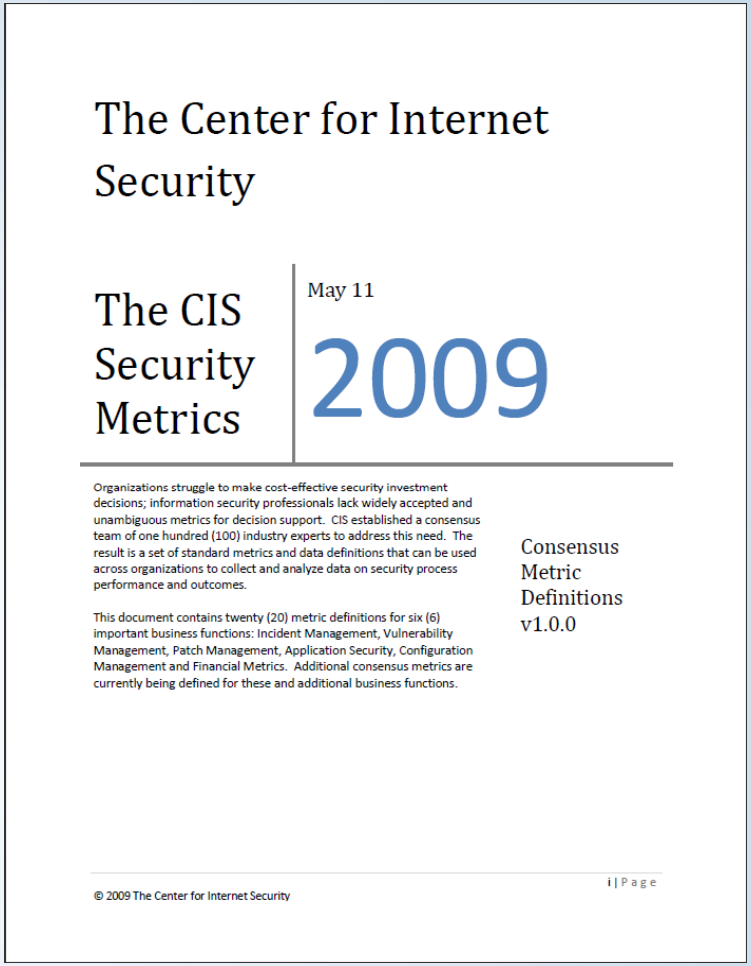
- Few specific requirements
  - So it's mostly up to us
- No experience with security metrics
  - Not sure what the pitfalls will be
- Not much time or money
  - A "5-year plan" is not an option

Our Approach

- Start small
- Use exploratory, iterative approach
- Look for expertise to rely on

CIS Security Metrics

- Well-defined and documented
- Reasonably broad in scope (incident, vulnerability, patch, application, CM, financial)



The Center for Internet Security

The CIS Security Metrics

May 11

2009

Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS established a consensus team of one hundred (100) industry experts to address this need. The result is a set of standard metrics and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes.

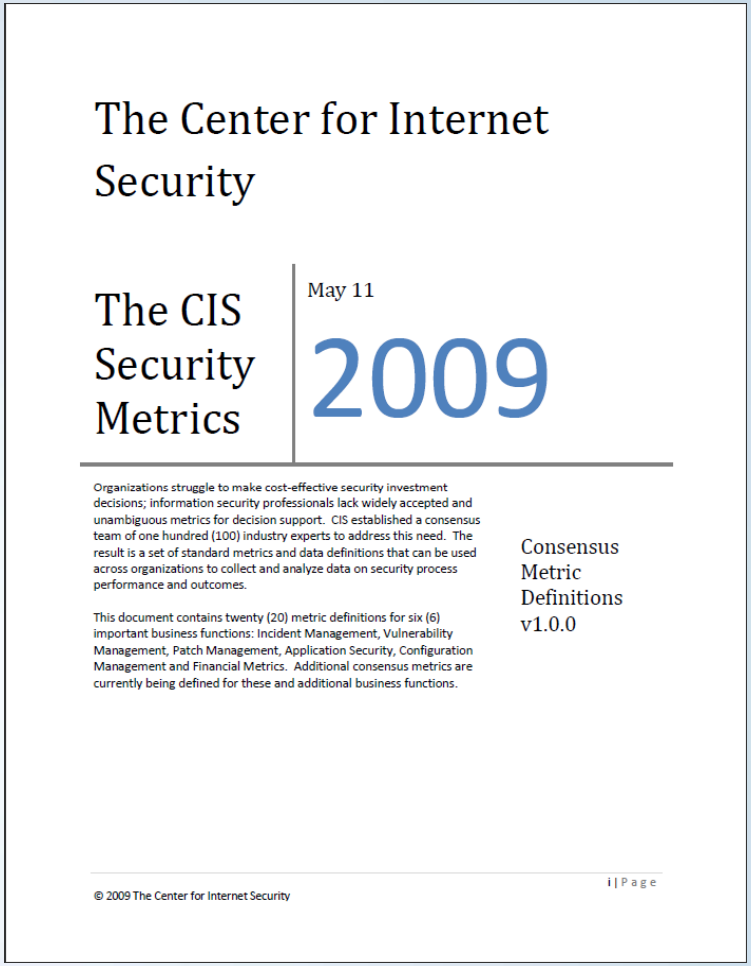
This document contains twenty (20) metric definitions for six (6) important business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management and Financial Metrics. Additional consensus metrics are currently being defined for these and additional business functions.

Consensus Metric Definitions v1.0.0

i | Page

CIS Security Metrics

- Actionable, for the most part
- Not too big (20 metrics)



The Center for Internet Security

The CIS Security Metrics

May 11

2009

Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS established a consensus team of one hundred (100) industry experts to address this need. The result is a set of standard metrics and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes.

This document contains twenty (20) metric definitions for six (6) important business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management and Financial Metrics. Additional consensus metrics are currently being defined for these and additional business functions.

Consensus Metric Definitions v1.0.0

i | Page

CIS Security Metrics

Function	Management Perspective	Defined Metrics
Incident Management	How well do we detect, accurately identify, handle, and recover from security incidents?	• Mean Time to Incident Discovery • Number of Incidents • Mean Time Between Security Incidents • Mean Time to Incident Recovery
Vulnerability Management	How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities?	• Vulnerability Scanning Coverage • Percent of Systems with No Known Severe Vulnerabilities • Mean Time to Mitigate Vulnerabilities • Number of Known Vulnerabilities
Patch Management	How well are we able to maintain the patch state of our systems?	• Patch Policy Compliance • Patch Management Coverage • Mean Time to Patch
Application Security	Can we rely on the security model of business applications to operate as intended?	• Number of Applications • Percent of Critical Applications • Risk Assessment Coverage • Security Testing Coverage
Configuration Management	How do changes to system configurations affect the security of the organization?	• Mean Time to Complete Changes • Percent of Changes with Security Reviews • Percent of Changes with Security Exceptions
Financial Metrics	What is the level and purpose of spending on information security?	• IT Security Spending as % of IT Budget • IT Security Budget Allocation

Source: CIS CMD v1.0.0, p. 2.

Example CIS Definition

Vulnerability Scan Coverage

Objective

Vulnerability Scan Coverage (VSC) indicates the scope of the organization's vulnerability identification process. Scanning of systems known to be under the organization's control provides the organization the ability to identify open known vulnerabilities on their systems. Percentage of systems covered allows the organization to become aware of areas of exposure and proactively remediate vulnerabilities before they are exploited.

Table 10: Vulnerability Scan Coverage

Metric Name	Vulnerability Scan Coverage
Version	1.0.0
Status	Final
Description	Vulnerability Scanning Coverage (VSC) measures the percentage of the organization's systems under management that were checked for vulnerabilities during vulnerability scanning and identification processes. This metric is used to indicate the scope of vulnerability identification efforts.
Audience	Management, Operations

Example CIS Definition

Question	What percentage of the organization's total systems has been checked for known vulnerabilities?
Answer	Positive integer value that is greater than or equal to zero but less than or equal to 100%. A value of "100%" indicates that all systems are covered by the vulnerability scanning process.
Formula	Vulnerability Scanning Coverage is calculated by dividing the total number of systems scanned by the total number of systems within the metric scope such as the entire organization: $$VSC = \frac{Count(Scanned\_Systems)}{Count(All\_Systems\_Within\_Organization)} * 100$$
Units	Percentage of systems
Frequency	Weekly, Monthly, Quarterly, Annually
Targets	VSC values should trend higher over time. Higher values are obviously better as it means more systems have been checked for vulnerabilities. A value of 100% means that all the systems are checked in vulnerability scans. For technical and operational reasons, this number will likely be below the theoretical maximum.

Preliminary Tasks

- Didn’t just implement CIS
- Analyzed each metric to see what data are required
- Conducted interviews with managers, the ISSO, developers, and system admins to determine if data existed
- Identified possible scope restrictions to reduce cost of data collection

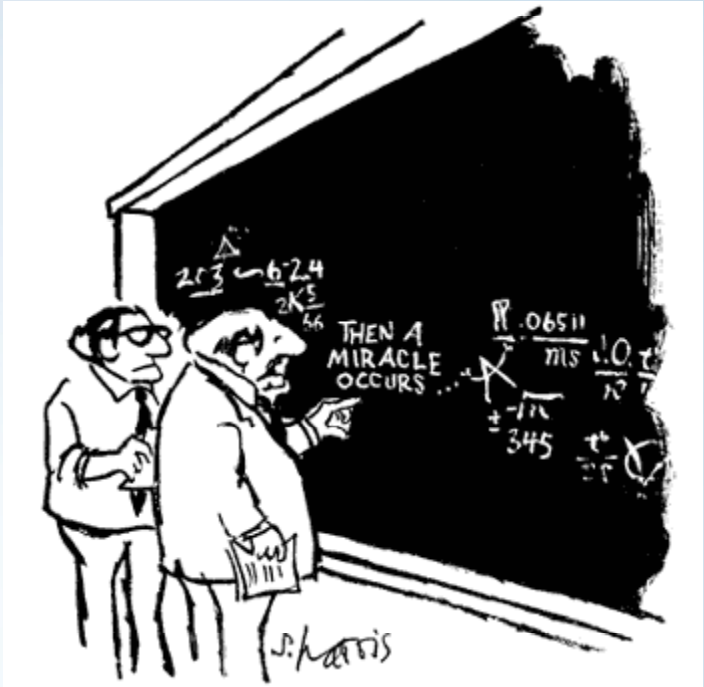
Preliminary Tasks

- Brainstorming session with security staff helped to identify:
  - What kinds of metrics were perceived as most important
  - Existing sources of data we weren't aware of

And Then…

Ultimately, someone had to decide which metrics we were going to use (that would be Rick).

And then we implemented them…



"I think you should be more explicit here in step two."

Implementation

- Used CIS Security Metrics document as a template for creating our own metrics definitions
- Worked with management to identify who would be the point of contact (POC) for each metric
- Taught administrative staff how to collect data and create monthly report

Implementation

- Met with each metric POC (some multiple times) and determined how each metric would be calculated
- Allowed several months of dry runs before delivering reports to customer
- Worked with POCs to develop short desk procedures for each metric

CM-1, Number of Devices

- The number of devices that were connected to the HLAN during the reporting period, broken down into clients, servers, network devices, and other
- Used as the denominator for VM-1, Vulnerability Scanning Coverage
- Conceptually simple, difficult in practice

Possible Sources for CM-1

Source	Limitation
Network management tools	Only track systems being actively managed
Patch tools	Only cover Windows clients and servers
Address Resolution Protocol (ARP) tables	Limited data (IP address, hostname, MAC address)

Solution for CM-1

- Only ARP data was complete enough to give a reasonably accurate count of devices on the network
- Data is pulled hourly by a cron job
- We rely on heuristics based on host naming conventions and IP ranges to distinguish clients, servers, network devices, and other

Hanford Cyber Security Metrics

Process Area	Defined Metrics
Vulnerability Management	VM-1: Vulnerability Scan Coverage VM-2: Percent of Systems Without Known High Vulnerabilities VM-3: Number of Known Vulnerability Instances (High, Med, Low)
Patch Management	PM-1: Mean Time to Patch Covered Systems (Clients, Servers) PM-2: Number of Patches Deployed
Configuration Management	CM-1: Number of Devices (Clients, Servers, Network, Other) CM-2: Number of Internet Emails (Sent, Received) CM-3: Number of Blocked Internet Emails CM-4: Number of Blocked Internet Access Attempts
Incident Management	IM-1: Number of Investigative Support Requests IM-2: Number of Incidents IM-3: Number of Discovered Malware Types IM-4: Number of Malware Agents Remediated IM-5: Number of Compromised Clients
Risk Management	RM-1: Number of Risk Assessments RM-2: List of Risk Assessments Completed (during quarter) RM-3: Number of CIRC AWAREs RM-4: Number of CIRC Bulletins
Awareness and Training	AT-1: Number of Awareness Briefings/Communications
Program Management	PG-1: Number of POA&Ms (Open, Closed, In Progress) PG-2: List of Audits (YTD with # of Findings, …) PG-3: List of Interconnection Security Agreements

Scan Coverage

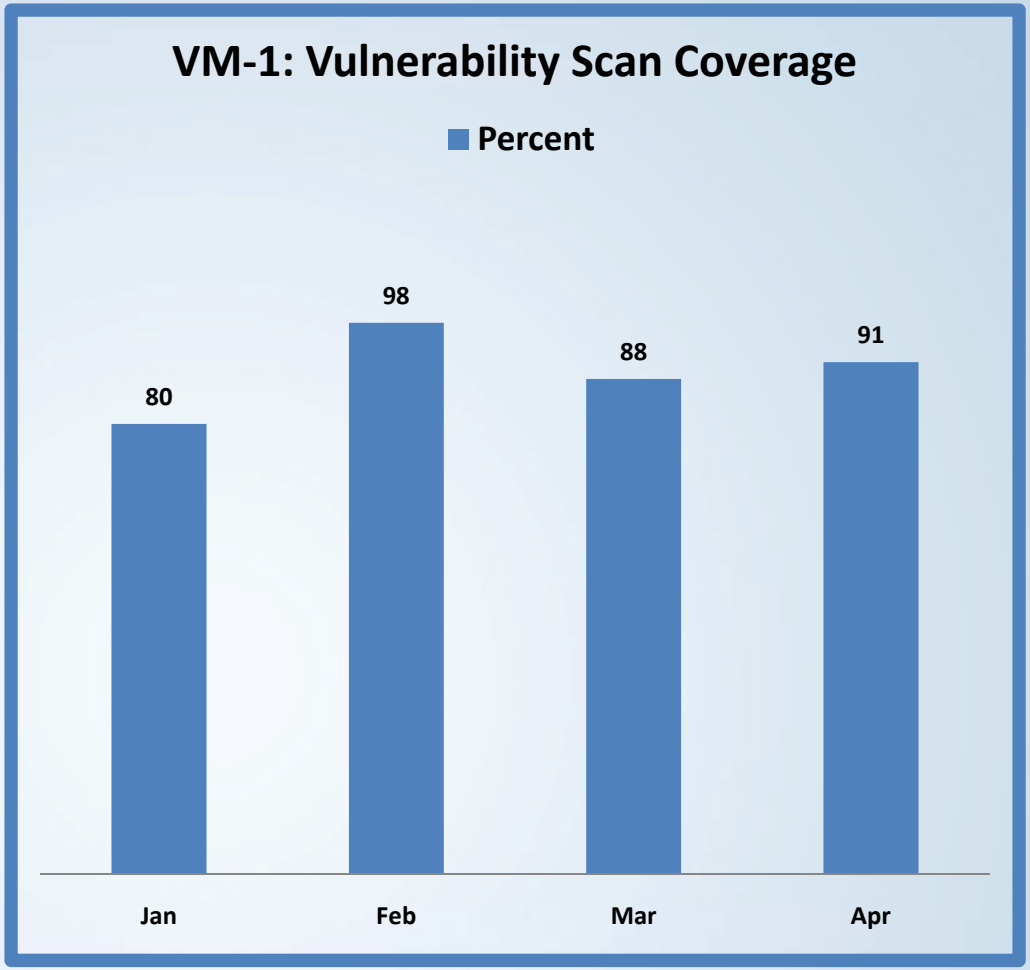
VM-1

- Measures the % of systems covered by vulnerability scans (Nessus)

- Dependant on CM-1: Number of Devices

- Never expect to reach 100%
  - Refresh PCs, laptops on travel, classroom PCs, …)

- **Cyber Goal:**
  - Understand the gap between VM-1 & 100%
  - Look for a consistent %



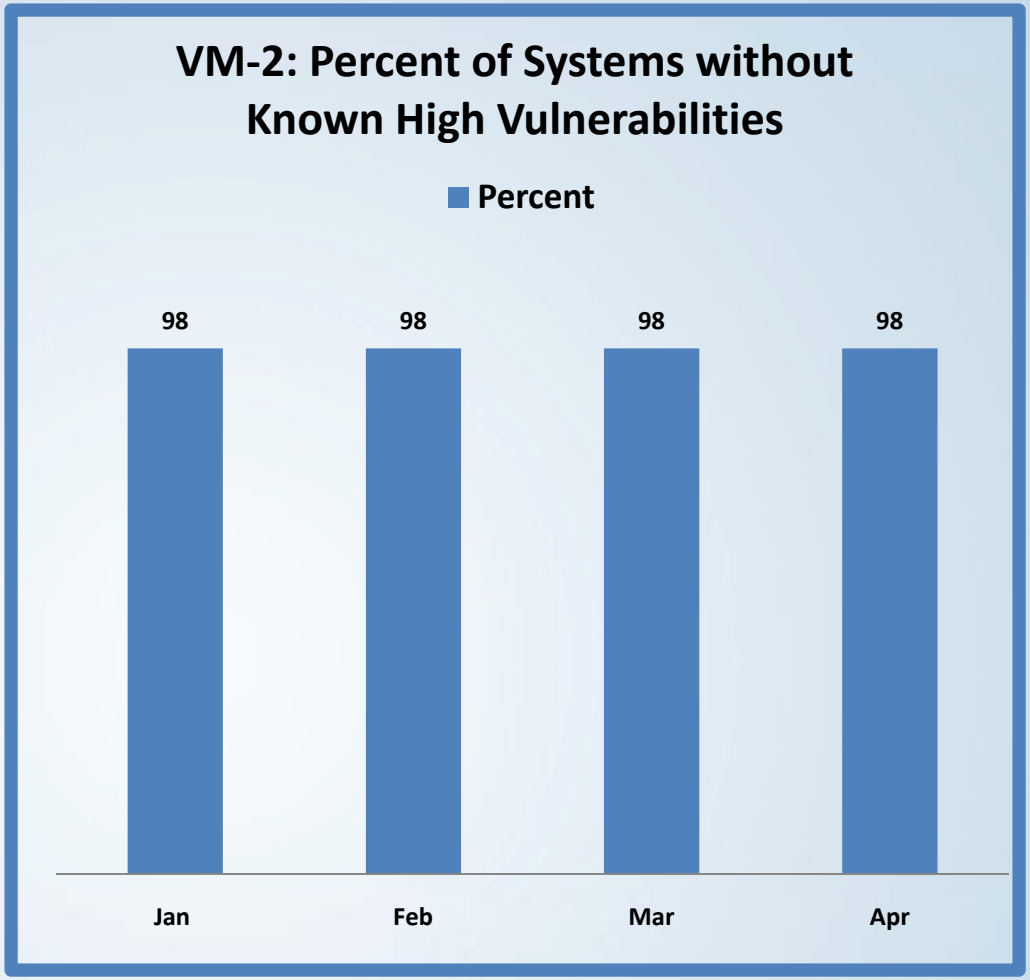
Systems w/out High Vulnerabilities

VM-2

- Measures the % of systems without known high vulnerabilities

- Ideal would be 100%

- **Cyber Goal:**
  - Understand the 2%
  - Look for a consistent %



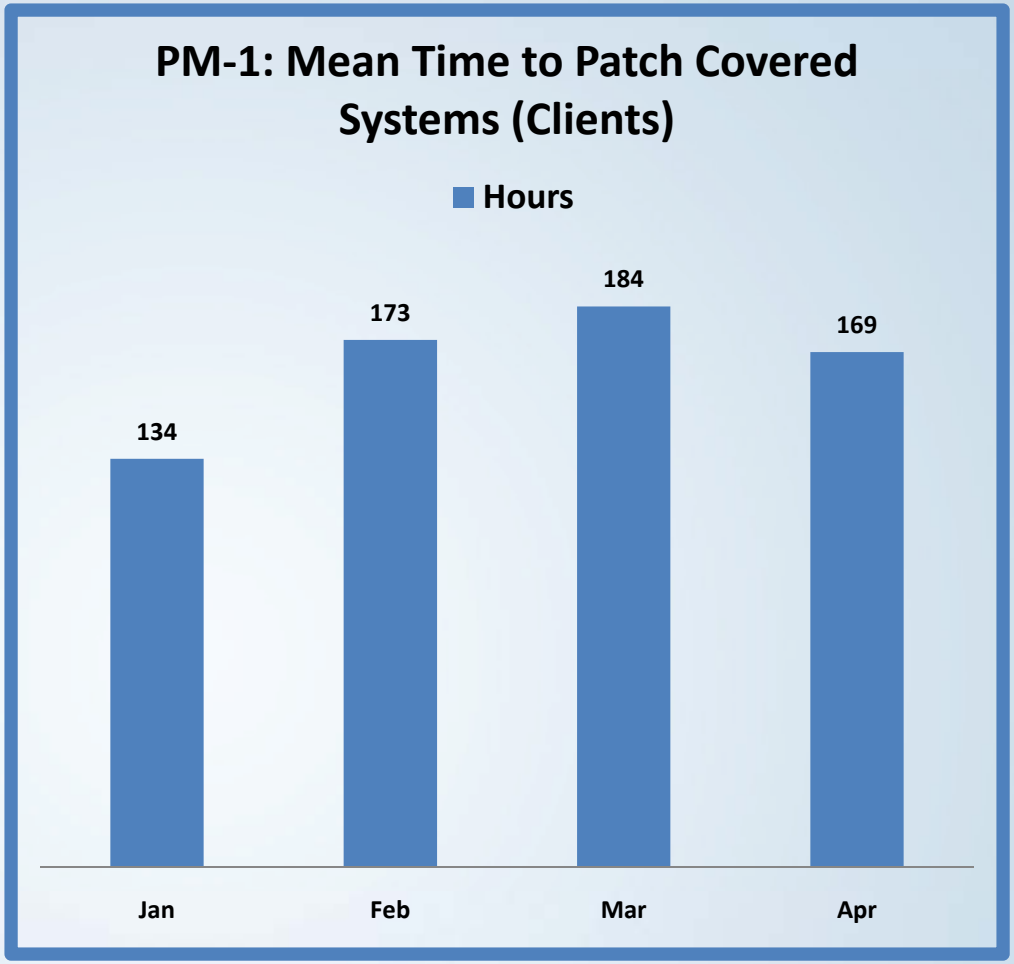
Time to Patch Systems

PM-1

- Measures the time, in hours, to patch covered systems
  - Only clients shown here
- Definition of metric is key to understanding what this really means!

•Cyber Goal:

- Team with IT to reduce the number
- Look for a consistent number



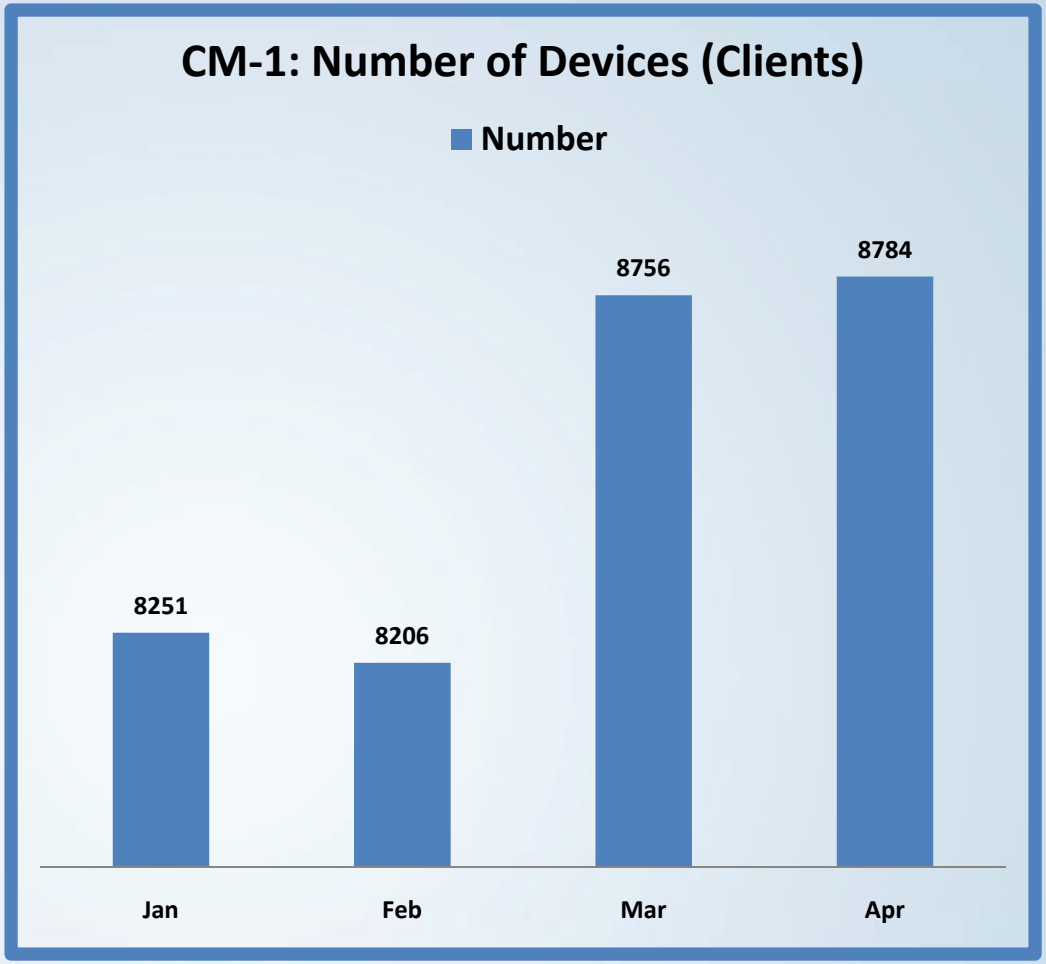
Number of Devices (Clients)

CM-1

- Measures the number of devices on the network
  - Only clients shown here

- CM-1 is the denominator for VM-1 (scan coverage)

- **Cyber Goal:**
  - Understand what's being counted & and not being counted
  - Look for a consistent count



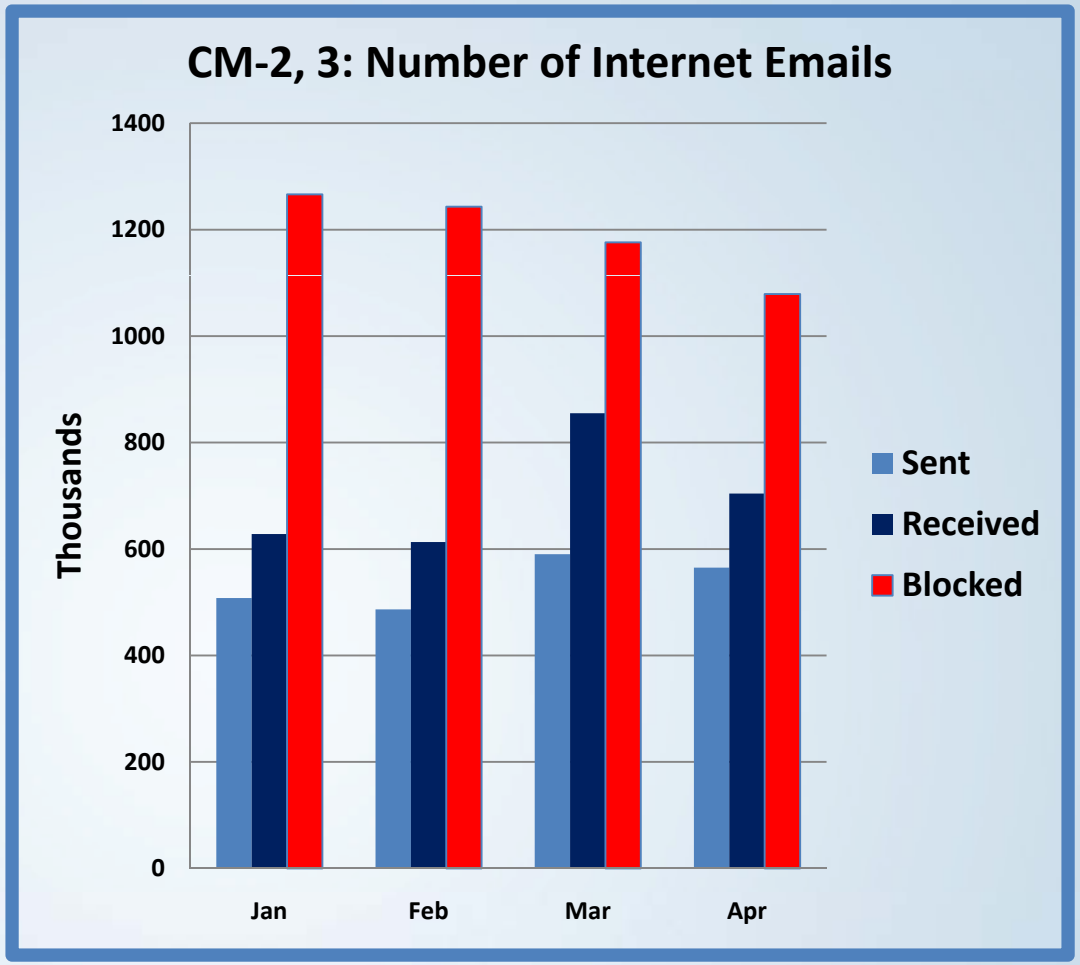
Internet Emails

CM-2,3

- Measures the number of Internet emails sent, received and blocked (inbound)

•Cyber Goal:

- Look into broad data swings
- Understand the security context



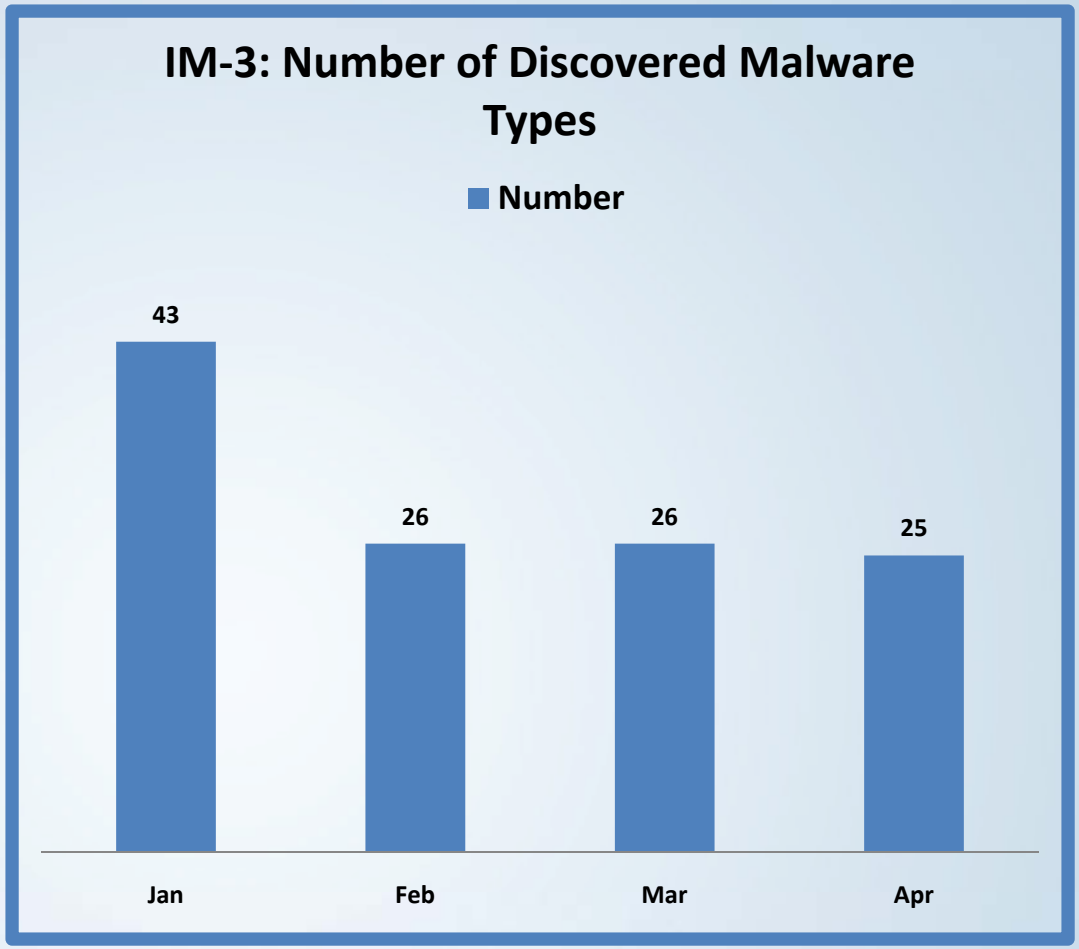
Malware Types

IM-3

- Measures the number of unique malware types discovered

•Cyber Goal:

- Understand the security context



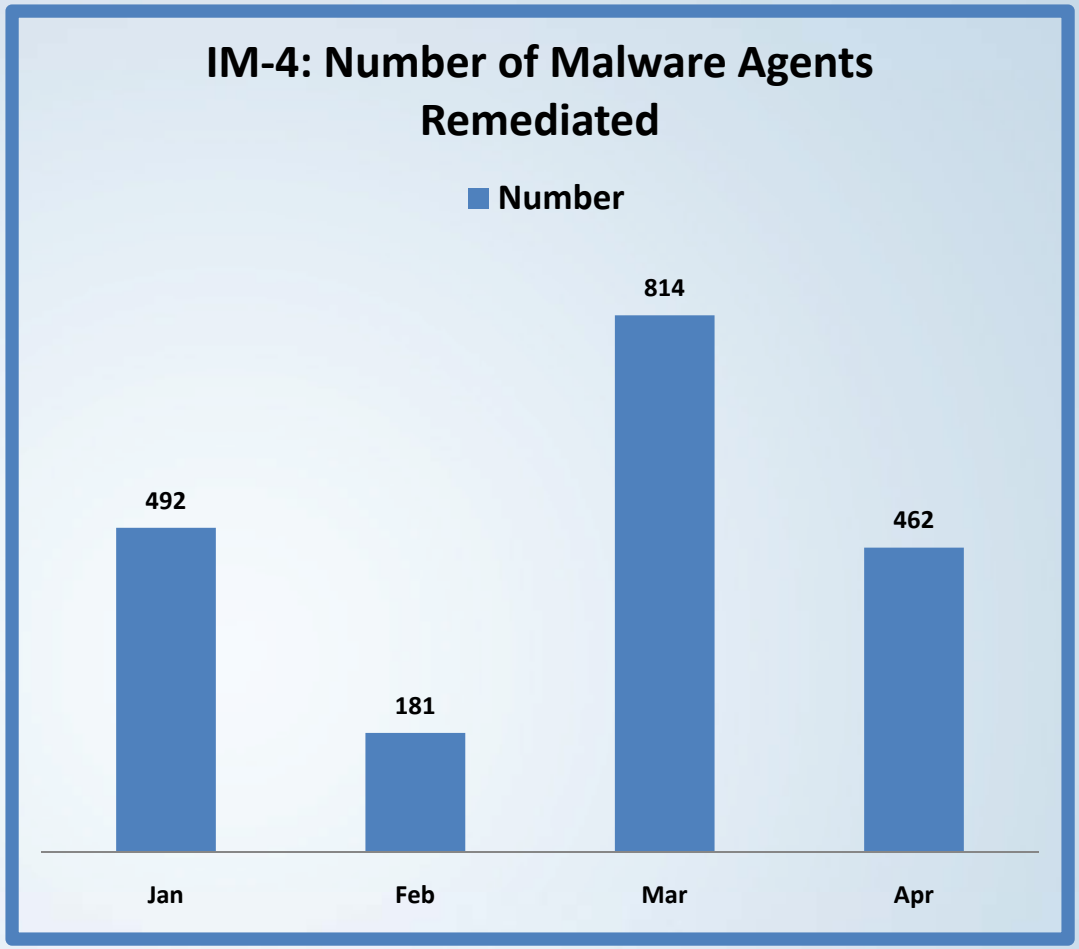
Malware Types

IM-4

- Measures the number of unique malware instances remediated

•Cyber Goal:

- •Look into broad data swings
- •Understand the security context



Results

- Some I expected
  - Extensive effort for initial implementation, moderate effort to maintain
  - Rigorous metric definitions very helpful
- Some I didn't expect
  - People care about what gets inspected
  - Increased insight into how the IT and cyber processes work
    - "I didn't know it worked like that"
  - Exceeded customer expectations
    - But created "metrics envy"

What's next?

- Refine the process for regular analysis
  - Ensure we get value from the data
  - Requires both Cyber and IT staff

    "Remember: Cyber security is a team sport"

- Tweak the metrics for next year

- Looking hard at
  - Consensus Audit Guidelines (CAG)
  - Recent OMB Draft/Guidance
  - Note the shift in orientation from **artifact-based compliance** to **measurement-based performance**

Contact Info

Rick Grandy
Richard_S_Grandy@RL.GOV
Lockheed Martin

Gregg Serene
Gregg_A_Serene@RL.GOV
Lockheed Martin

References

NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html

DOE Office of the Under Secretary of Energy, *Program Cyber Security Plan*, Ver. 1.2: You probably already have a copy

S. Payne, "A Guide to Security Metrics": http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

Center for Internet Security, "CIS Security Metrics": http://cisecurity.org/en-us/?route=downloads.browse.category.metrics

A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. ISBN 9780321349989.

S. Berinato, "A Few Good Info Sec Metrics": http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics