RSAConference2019

San Francisco | March 4–8 | Moscone Center

SESSION ID:

How to Develop Key Performance Indicators for Security

James Tarala

Principal and Senior Instructor
Enclave Security / The SANS Institute
@isaudit

Laying a Foundation

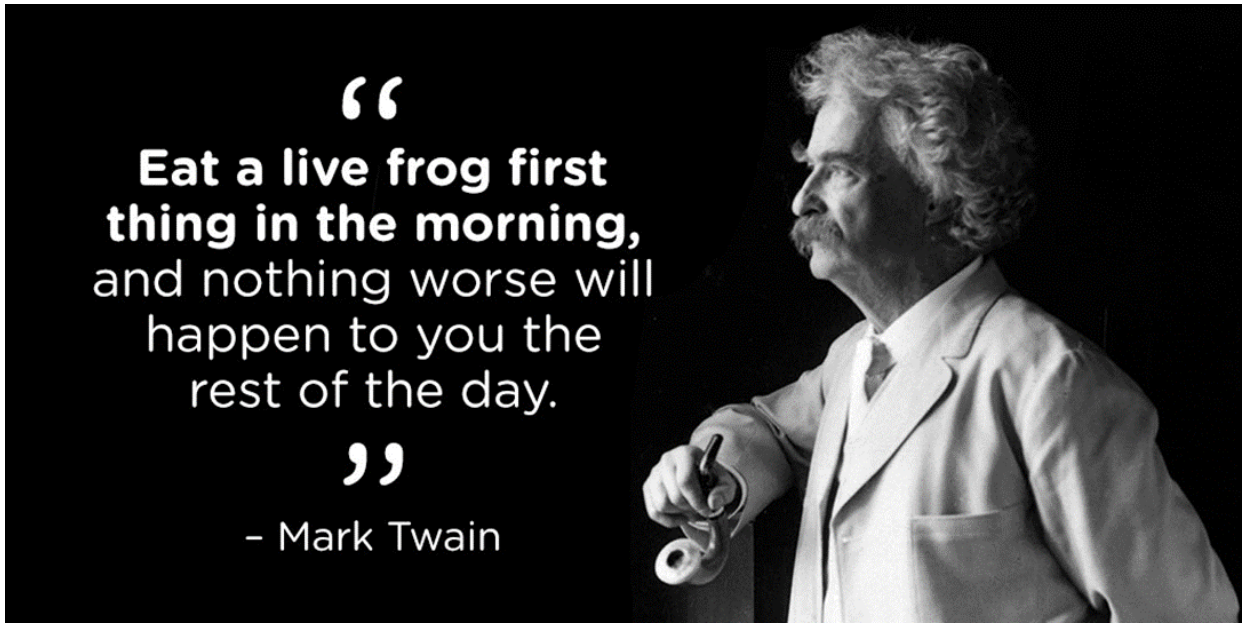
- For metrics to be effective, organizations must define their goals
- Most organizations have not taken the time to define their intentions for security
- We need more detailed metrics than “don’t get breached”
- Before we can define metrics, we have to lay a foundation

An Architecture for Security Program Management

To lay a solid foundation, organizations must:

1. Document a security program charter
2. Empower stakeholders to govern the program
3. Clearly document their intentions (policies)
4. Establish their priorities for defense
5. Create a plan for quality management
6. Define specific measures / metrics for success
7. Regularly report to key stakeholders / leadership

WARNING!



- There are no shortcuts!
- If organizations skip steps in the process, they are bound for frustration, confusion, and failure
- It’s time for our industry to grow up and do the hard things

Defining Appropriate Controls

- Security defenses are generally derived from three places:
  - Regulatory requirements
  - Industry standards
  - Contractual obligations

- It is pointless to define measures, if goals have not been defined

Popular Security Control Standards

CIS Controls™

NIST National Institute of Standards and Technology U.S. Department of Commerce

ISO

PCI Security Standards Council

HIPAA Health Insurance Portability & Accountability Act

FFIEC

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

GDPR

AICPA Service Organization Control Reports AICPA SOC 2 Formerly SAS 70 Reports

The Center for Internet Security (CIS) Controls

- Official home of the Critical Security Controls
- Not-for-Profit group responsible for managing the CIS Controls
- Utilizes a volunteer army of contributors to define defense
- Responsible for maintaining community efforts such as:
  - Security benchmarks
  - Security metrics
  - CIS Controls
  - Managing the MS-ISAC

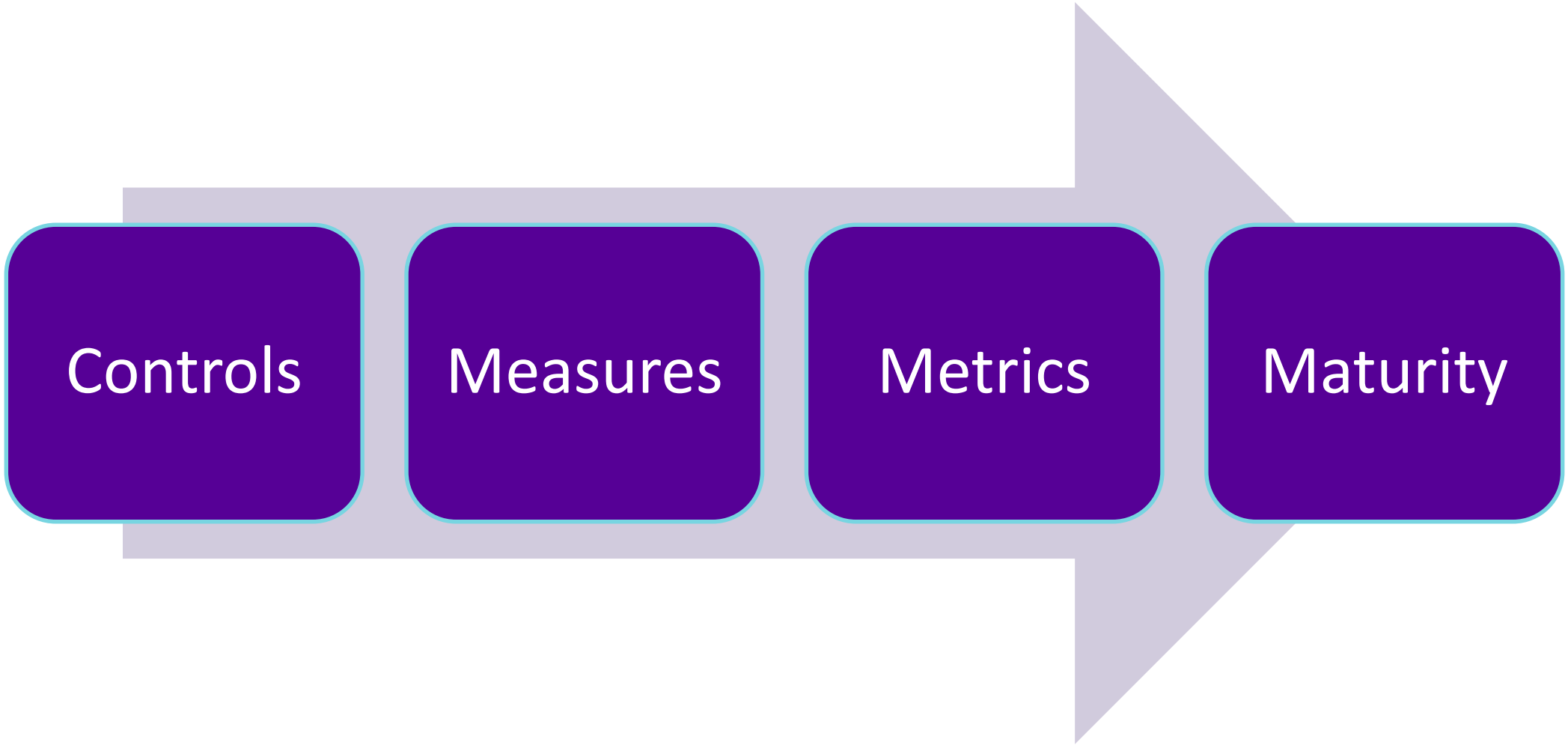
The Center for Internet Security (CIS) Controls (cont)

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Key Principles for Version 7.0 & 7.1

1. Improve the consistency and simplify the wording of each sub-control
2. Implement “one ask” per sub-control
3. Bring more focus on multi-factor authentication and application whitelisting
4. Account for improvements in security technology and emerging security problems
5. Better alignment with other frameworks (e.g., the NIST CSF)
6. Support for the development of related products (e.g. measurements/metrics, governance, and implementation guides)
7. Definition of control levels based on organizational demographics

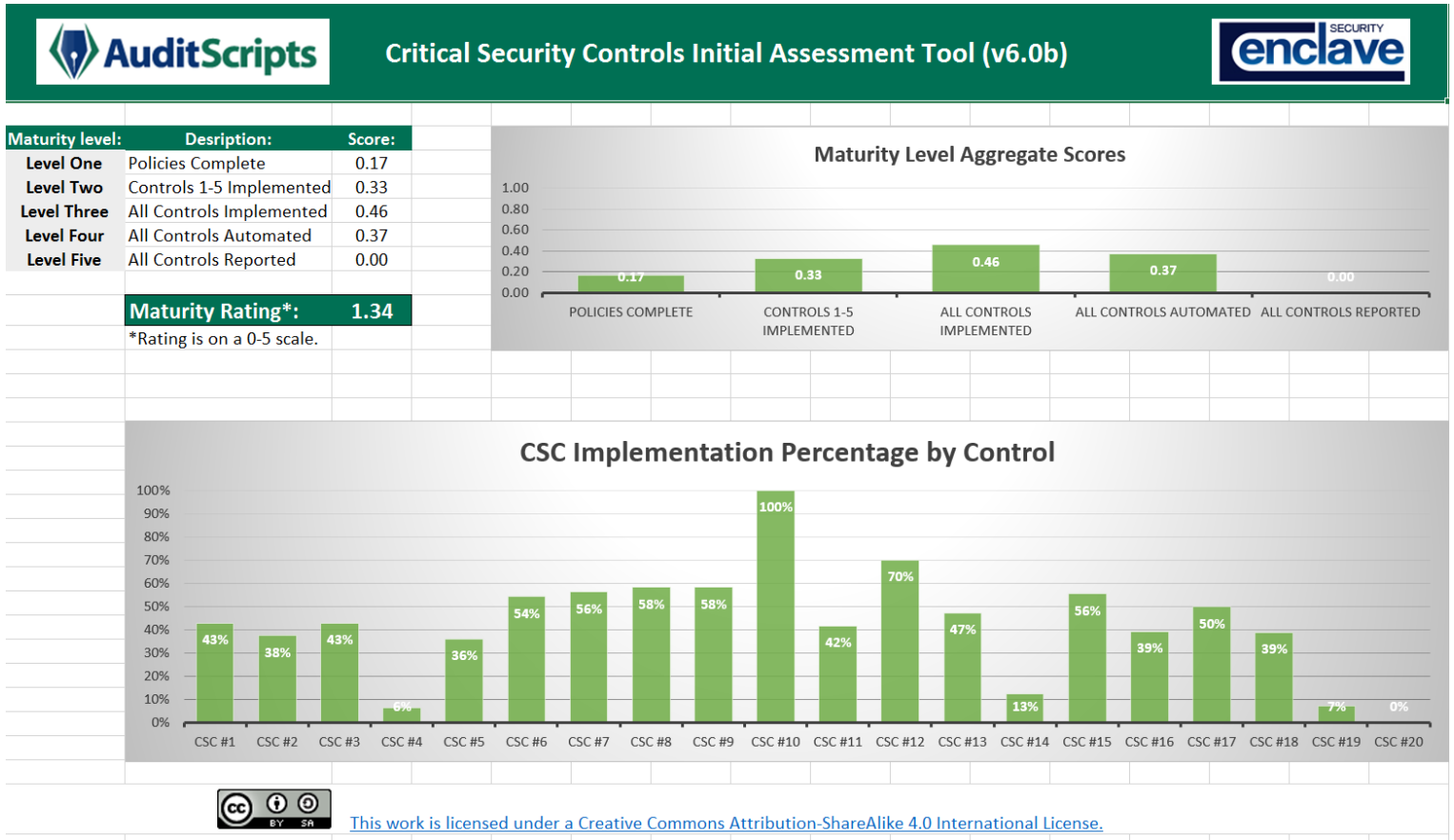
Controls, Measures, Metrics, Maturity



Start with Attestations

- Start the process with simple interviews
- There's no reason for a deep dive if the basics are not done
- Tool available at:

www.auditscripts.com



Six Sigma and the CIS Controls

- Starting in version 7.0 of the CIS Controls, Six Sigma was adopted to be the quality management program for the controls
- “Six Sigma is a quality program that, when all is said and done, improves your customer’s experience, lowers your costs, and builds better leaders.”

  — Jack Welch, GE

- Purpose was to define thresholds for maturity for each defined measure
- Organizations do not need to be perfect, but this allows them to define a standard for what is acceptable risk

Controls, Measures, and Metrics Example

Maintain detailed asset inventory

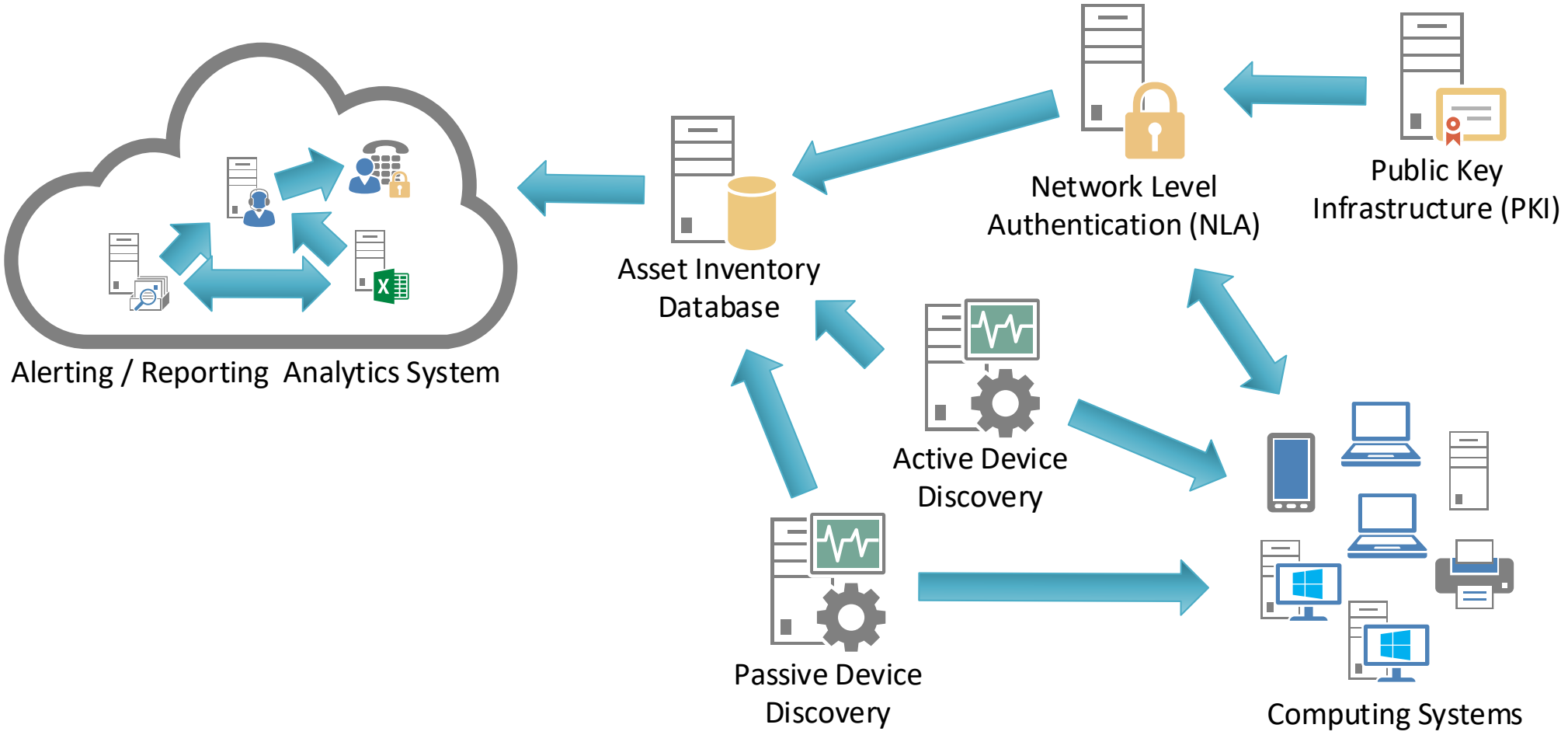
What percentage of the organization's hardware assets are not presently included in the organization's asset inventory?

Sigma Level One	Sigma Level Two	Sigma Level Three	Sigma Level Four	Sigma Level Five	Sigma Level Six
69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less

More Sample Measures / Metrics (CIS Control #1)

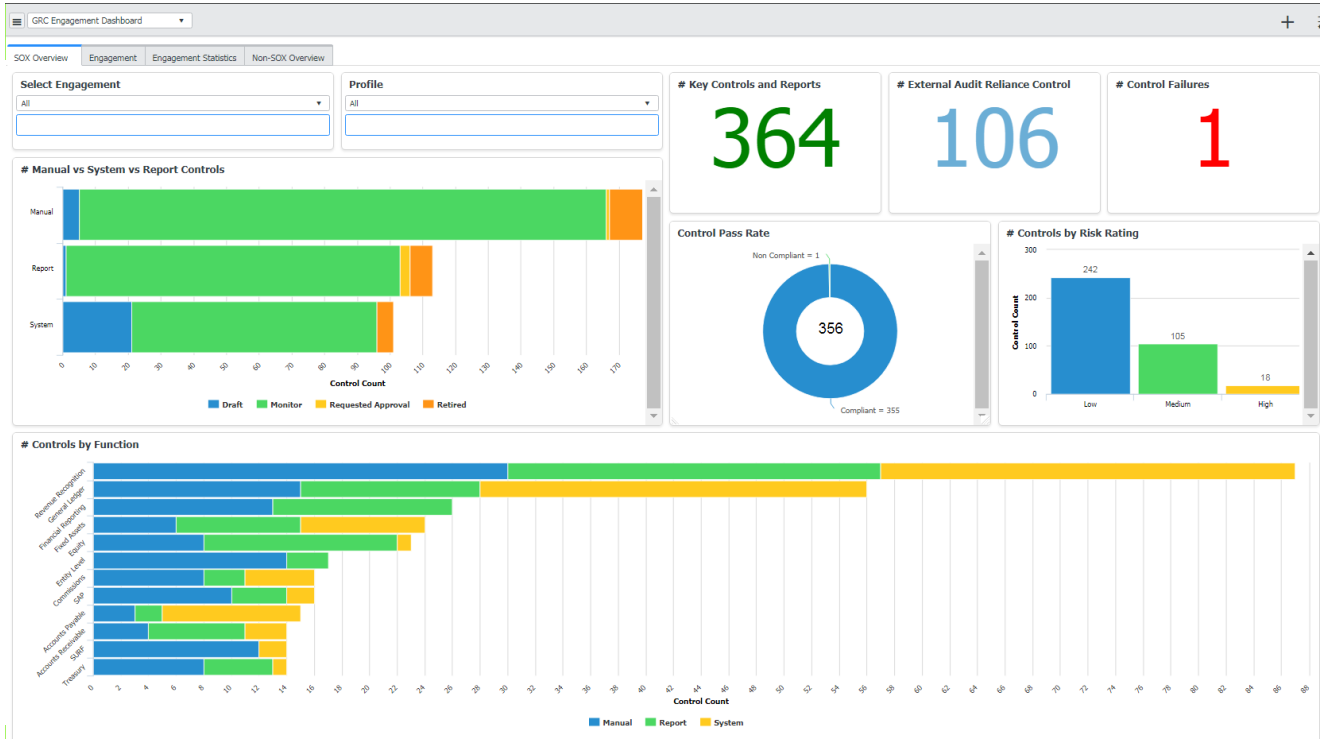
Measure	Sigma Level One	Sigma Level Two	Sigma Level Three	Sigma Level Four	Sigma Level Five	Sigma Level Six
What percentage of the organization's networks have not recently been scanned by an active asset discovery tool?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
What percentage of the organization's networks are not being monitored by a passive asset discovery tool?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
What percentage of the organization's DHCP servers do not have logging enabled?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
What percentage of the organization's hardware assets are not presently included in the organization's asset inventory?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
What percentage of the organization's hardware assets as a whole are not documented in the organization's asset inventory with the appropriate network address, hardware address, machine name, data asset owner, and department for each asset?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
What percentage of the organization's unauthorized assets have not been removed from the network, quarantined or added to the inventory in a timely manner?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
What percentage of the organization's network switches are not configured to require network-based port level access control for all client connections?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
What percentage of the organization's network switches are not configured to require network-based port level access control utilizing client certificates to authenticate all client connections?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less

Defined Measures / Metrics Lead to Automation



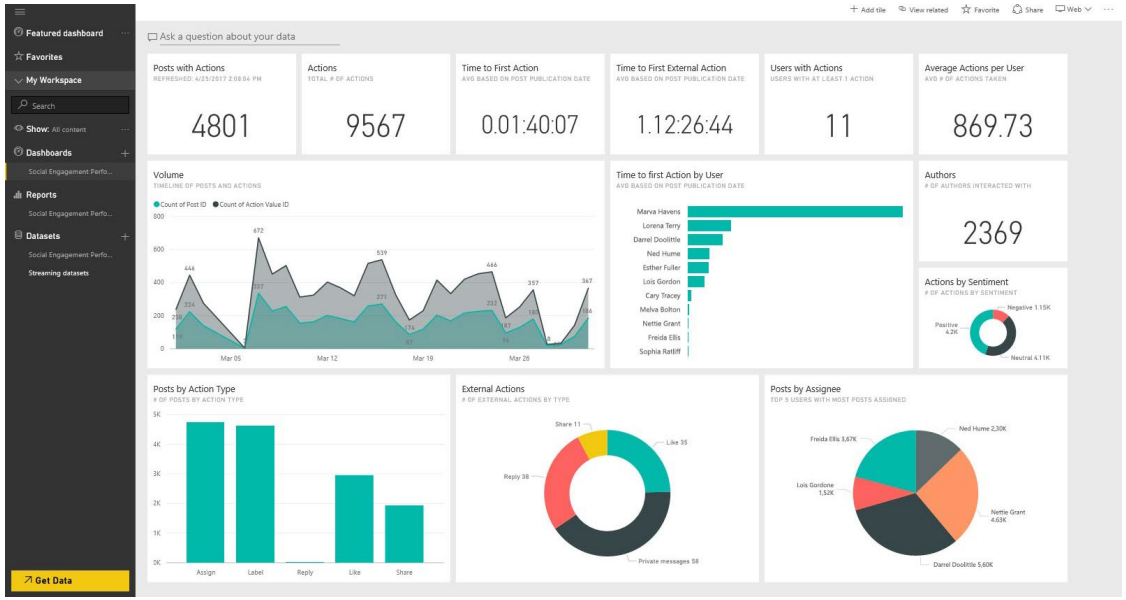
Automation Leads to Reporting

- Automated measures can be aggregated and reported to leadership using standardized software platforms



The Future of Information Security

- Cyber hygiene has been defined
- We have standards of care



- Information security is a business intelligence problem
- Automated measures show the way

Call to Action

- Every organization is at a different place in the journey
- Remember the basics:
  1. Document a security program charter
  2. Empower stakeholders to govern the program
  3. Clearly document their intentions (policies)
  4. Establish their priorities for defense
  5. Create a plan for quality management
  6. Define specific measures / metrics for success
  7. Regularly report to key stakeholders / leadership

Operationalizing Security Program Metrics

- Next week you should:
  - Download the free resources at cisecurity.org & auditscripts.com
  - Decide which standards will drive your security program
- In the first three months following this presentation you should:
  - Create / review your security program charter
  - Evaluate / update your security policy library to reflect your goals
- Within six months you should:
  - Choose 5-10 measures to report to senior leadership

For More Information

- James Tarala
  - E-mail: james.tarala@enclavesecurity.com
  - Twitter: @isaudit

- Resources for further study:
  - The Center for Internet Security Resources (www.cisecurity.org)
  - AuditScripts.com Resources (www.auditscripts.com)
  - SANS – CIS Controls Courses – SEC 440 / 566
  - The Project Management Institute Resources (www.pmi.org)