

RSA® Conference 2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: GRC-R04

CUT THROUGH THE CONFUSION: 2018 UPDATES TO CIS CONTROLS

MODERATOR: **James Tarala**

Principal Consultant, Enclave Security
@isaudit

PANELISTS:

Kelli Tarala

Principal Consultant
Enclave Security
@kellitarala

Philippe Langlois

Controls Technical Product Manager
Center for Internet Security
@langlois925



#RSAC

Goals for the CIS Controls (v7.0) Release



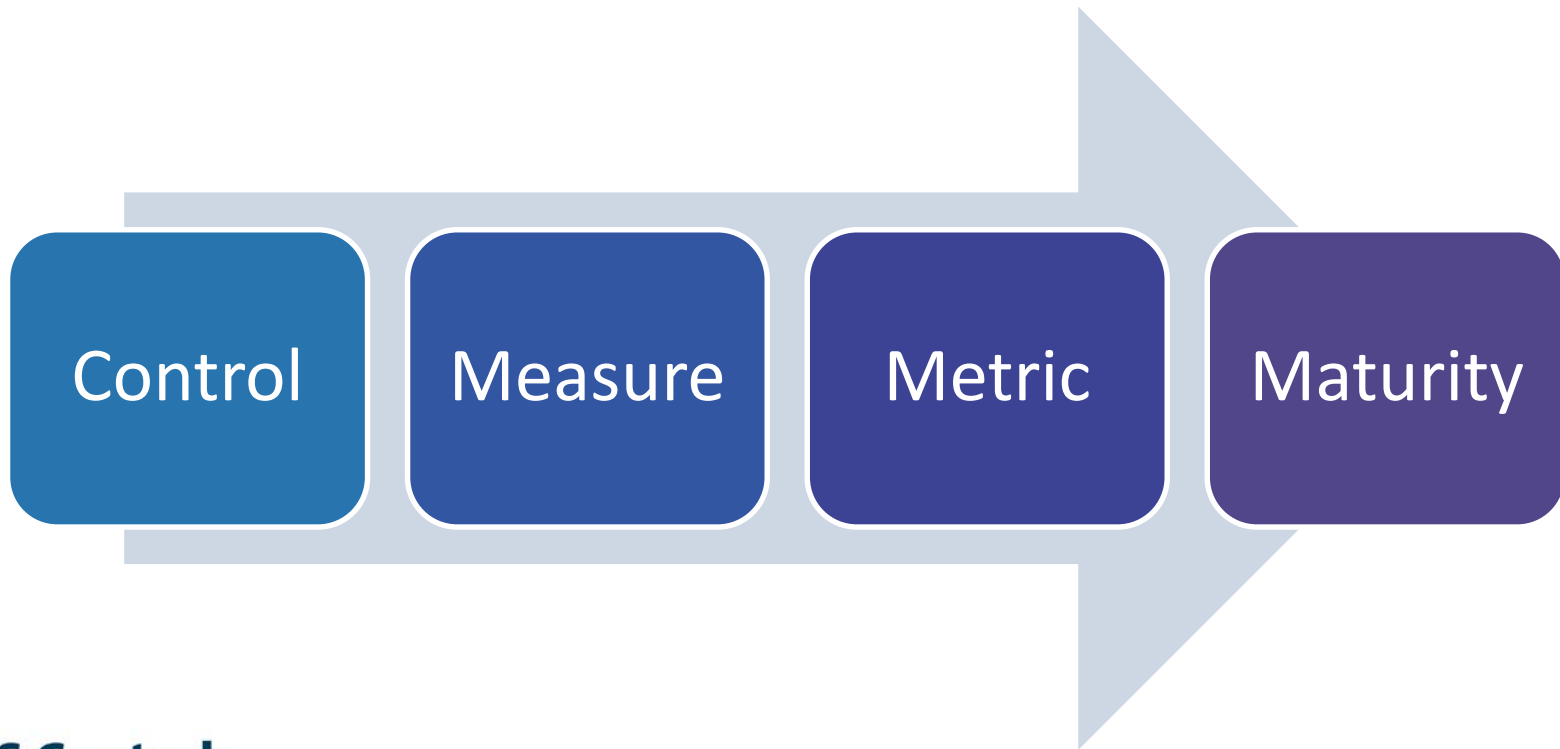
- Improve the consistency and simplify the wording of each sub-control
- Implement “one ask, one measure” principle per sub-control
- Account for improvements in security technology and emerging security problems
- Better alignment with other frameworks (e.g., the NIST CSF)
- Support for the development of related products (e.g. measurements/metrics, governance, and implementation guides)

Major Changes to Version 7.0



- Re-ordered CIS Controls 3, 4, & 5 to reflect changing priorities
- Additional emphasis and specificity related to:
 - Multi-Factor Authentication (MFA)
 - Application Whitelisting
 - Defenses Against Microsoft PowerShell Abuses
- More detailed measures and integration of a quality management program (Six-Sigma)

Understanding Measures and Metrics



2018 CIS Controls (version 7.0)



#RSAC

Basic

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

Foundational

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

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Applying What You Learned



- Download the latest version of the CIS Controls:
<https://www.cisecurity.org/>
- Review the controls and explore the available practice aids
- Evaluate your organization, are there defenses missing?
- Share what you have learned this week with coworkers back home

If You Have Further Questions



- James Tarala

James.tarala@enclavesecurity.com

- Kelli Tarala

Kelli.tarala@enclavesecurity.com

- Philippe Langlois

Philippe.Langlois@cisecurity.org



<https://www.cisecurity.org>