MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

MAKING COMMUNITY BEST PRACTICE… *COMMON* PRACTICE

Tony Sager

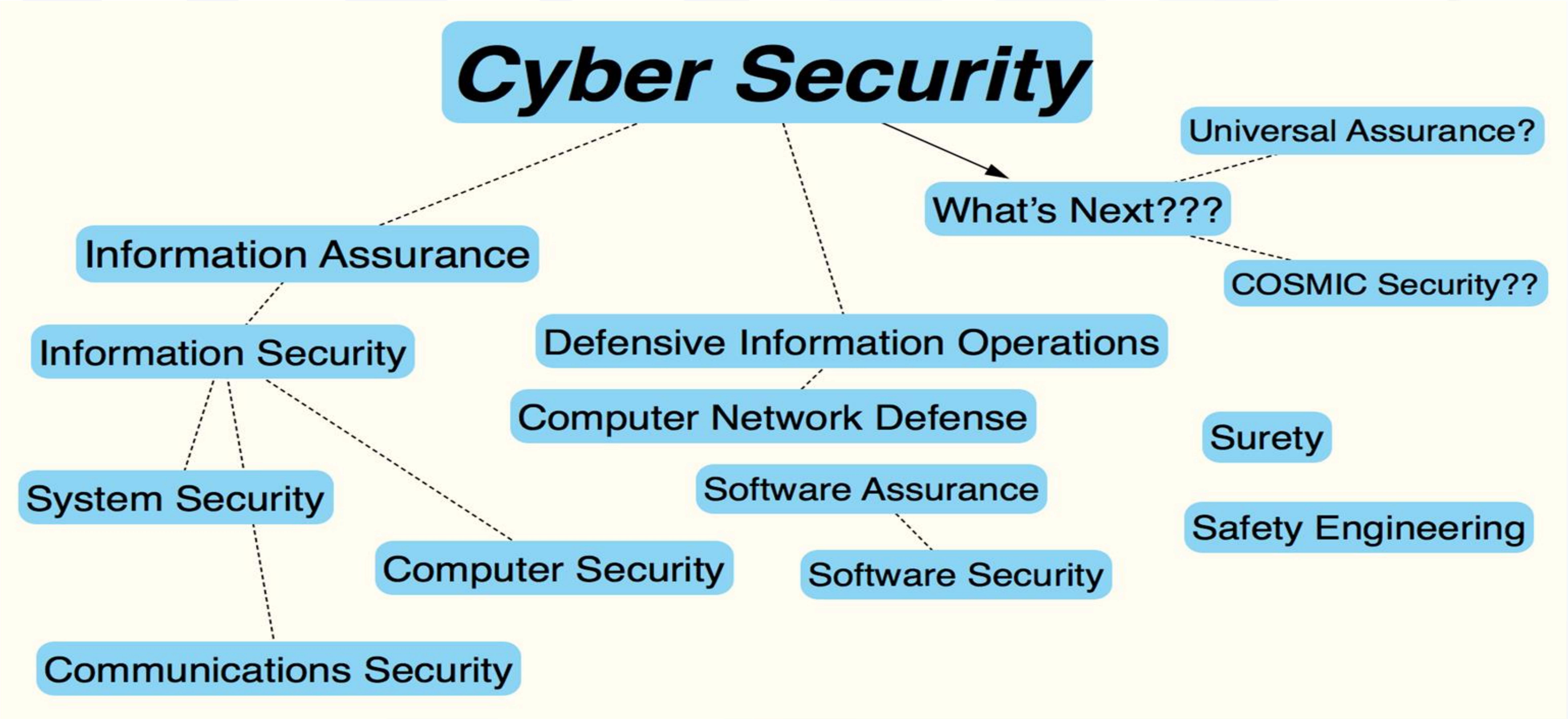
Senior Vice President & Chief Evangelist

CIS (the Center for Internet Security)

CLASSIC RISK EQUATION

$$\text{Risk} = \left\{ \frac{\textbf{Vulnerability, Threat, Consequence}}{\text{countermeasures}} \right\}$$

THE LONG AND WINDING ROAD THAT LEADS TO…….



Cyber Security

Universal Assurance?

What's Next???

COSMIC Security??

Information Assurance

Information Security

Defensive Information Operations

Computer Network Defense

Surety

System Security

Software Assurance

Safety Engineering

Computer Security

Software Security

Communications Security

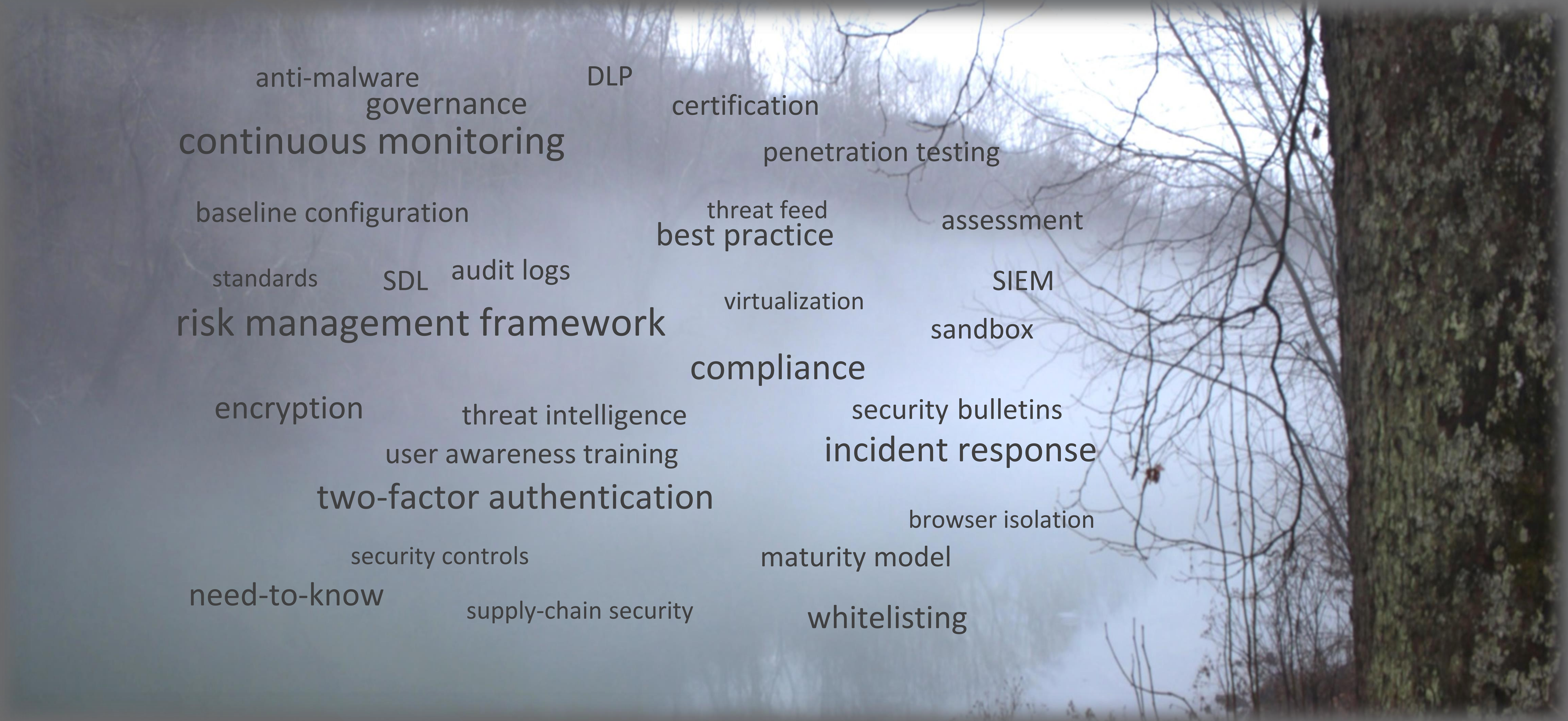
CALABRESE’S RAZOR

“I’ve long held the opinion that the community of ‘Information Security Experts agree with each other 90% of the time…

…but waste 90% of their time arguing to the death with other InfoSec Experts about the remaining 10%.”

Hal Pomeranz, Deer Run Associates
February 26, 2009

“THE FOG OF MORE”



anti-malware
DLP
governance
certification
continuous monitoring
penetration testing
baseline configuration
threat feed
best practice
assessment
standards
SDL
audit logs
SIEM
virtualization
risk management framework
sandbox
compliance
encryption
threat intelligence
security bulletins
user awareness training
incident response
two-factor authentication
browser isolation
security controls
maturity model
need-to-know
supply-chain security
whitelisting

A LIFETIME OF CYBERSECURITY LESSONS

- Knowing about vulnerabilities doesn’t get them fixed
- The Bad Guy doesn’t perform magic
- There’s a large but limited number of defensive choices
  - the 80/20 rule applies (The Pareto Principle)
- Cybersecurity => Information Management *(not Threat Sharing)*
  - when you hear “*share*”, think “*translate*” and “*execute*”
- Few people/enterprises make *security* decisions
  - they make economic and social decisions
- Cybersecurity is more like **Groundhog Day** than **Independence Day**

THE DEFENDER’S DILEMMA

1. What’s the right thing to do
   - and how much do I need to do?
2. How do I actually do it?
3. And how can I demonstrate to others that I have done the right thing?

FROM BEST PRACTICE → COMMON PRACTICE

How do we know what is "best"?

- Based on Data? Solution to the worst problem? Trusted source?

What is a "practice"?

- How specific? How do I actually do it? What do I need to do this?

What are the barriers?

- Knowledge? Cost? Tools? Training? Enforcement? Misalignment? Repeatability?

It takes more than a list of practices

- Marketplace of tools, training; community-building; sharing of ideas; alignment of practices with oversight, auditing, compliance.

HEALTH & HUMAN SERVICES - BEST PRACTICES

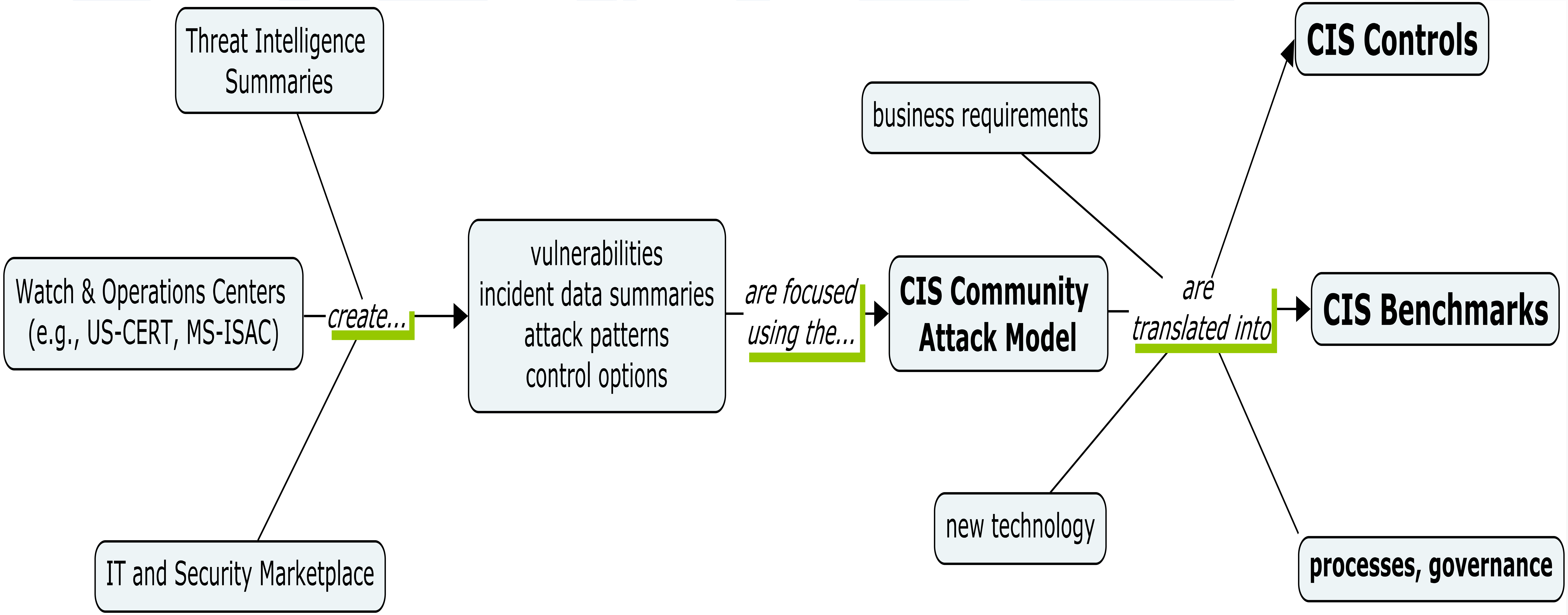
Where are we today in cyberdefense?

Research Validated Best Practice	A program, activity or strategy ….. that has the highest degree of **proven effectiveness** supported by **objective and comprehensive research and evaluation.**
Field Tested Best Practice	….. that has been **shown to work effectively and produce successful outcomes** and is supported to **some degree by subjective and objective da**ta sources.
Promising Practice	….. that **has worked within one organization and shows promise** during its early stages for becoming a best practice with long term sustainable impact. … must have **some objective bas**is for claiming effectiveness and must have **the potential for replication** among other organizations.

AN EFFECTIVE CYBERDEFENSE “MACHINE” SHOULD BE…

- based on a model of Attacks, Attackers, and defensive choices
  - focused on categories, types, patterns, templates, etc.
- driven by data/information
- managed within an open, standards-based framework
- account for “community risk”, but be tailorable
- repeatable, dynamic, feedback-driven
- demonstrable, negotiable for real people

CIS BEST PRACTICE WORKFLOW



Threat Intelligence Summaries

Watch & Operations Centers (e.g., US-CERT, MS-ISAC)

IT and Security Marketplace

create…

vulnerabilities
incident data summaries
attack patterns
control options

are focused using the…

CIS Community Attack Model

business requirements

new technology

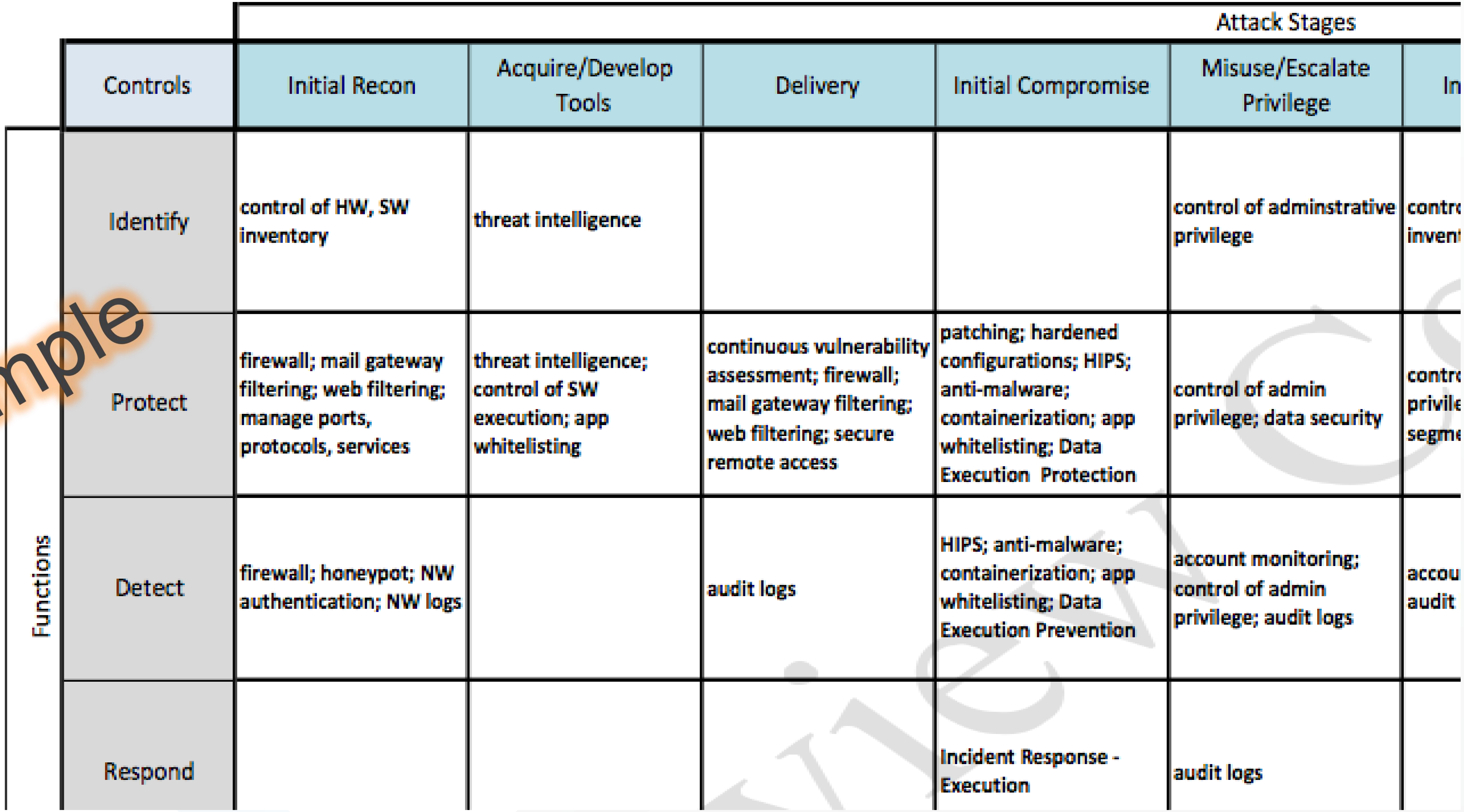
are translated into

CIS Controls

CIS Benchmarks

processes, governance

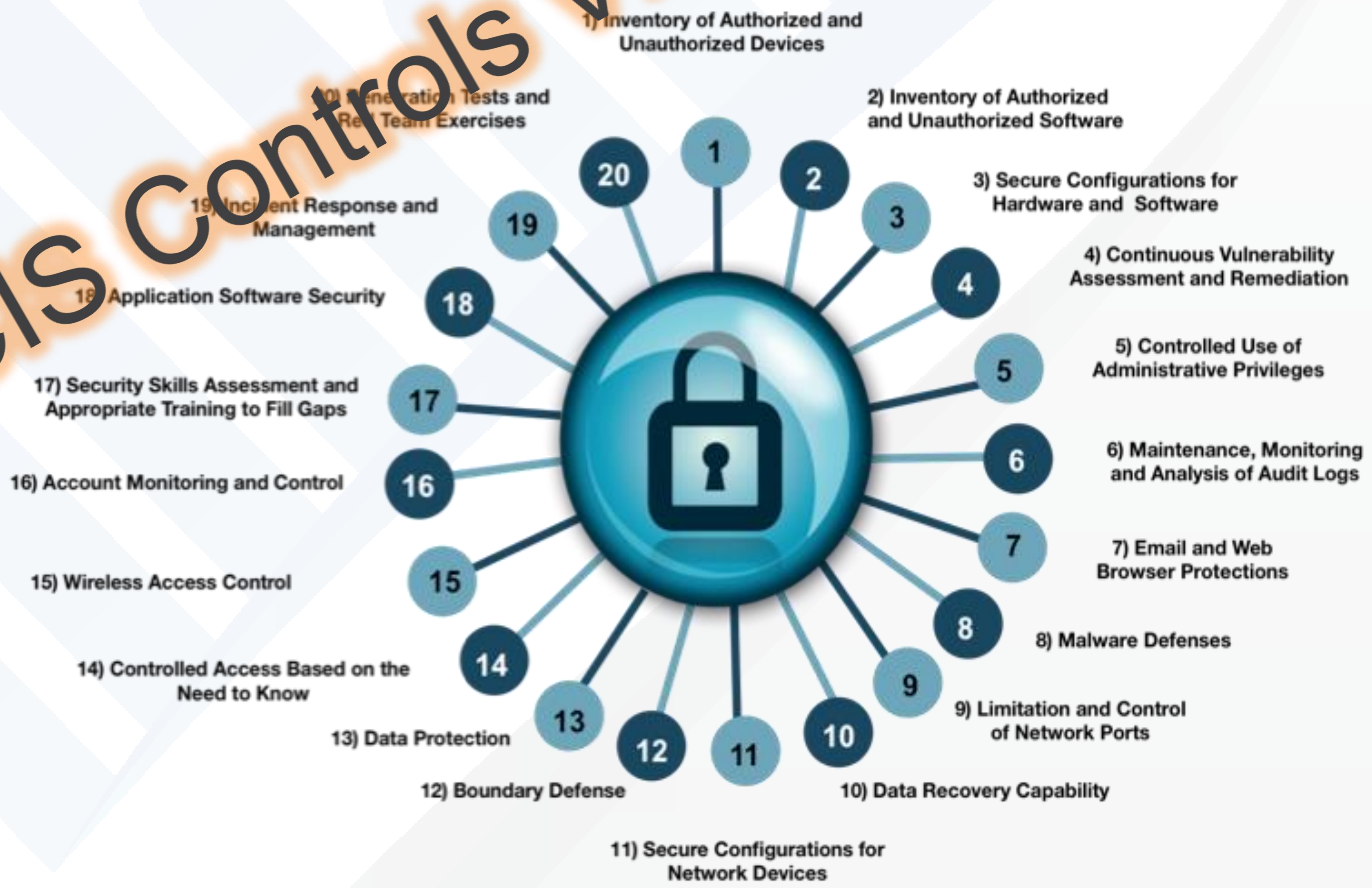
CIS COMMUNITY ATTACK MODEL – CHOOSING CONTROLS



		Attack Stages					
	Controls	Initial Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	In
Functions	Identify	control of HW, SW inventory	threat intelligence			control of adminstrative privilege	contr invent
	Protect	firewall; mail gateway filtering; web filtering; manage ports, protocols, services	threat intelligence; control of SW execution; app whitelisting	continuous vulnerability assessment; firewall; mail gateway filtering; web filtering; secure remote access	patching; hardened configurations; HIPS; anti-malware; containerization; app whitelisting; Data Execution Protection	control of admin privilege; data security	contr privile segme
	Detect	firewall; honeypot; NW authentication; NW logs		audit logs	HIPS; anti-malware; containerization; app whitelisting; Data Execution Prevention	account monitoring; control of admin privilege; audit logs	accou audit
	Respond				Incident Response - Execution	audit logs	

THE CIS CONTROLS

MARCH 19th - CIS Controls V7 !!!



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

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) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

A COMMUNITY APPROACH TO CYBERDEFENSE

1. ~~Sing Kumbaya~~
2. ~~Wait for … {*Pick One*: "the cloud", AI, advanced analytics, magic boxes, threat sharing, the government} … to save me~~

- Recognize "Community Risk," which implies Community Action
- Share the work of translation to Action
- Support the work to create Community products
- Use a common model from enterprise level, to action/attack level
- Streamline systems for assessment, auditing, compliance, reporting

MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Tony Sager

Senior Vice President & Chief Evangelist

CIS (the Center for Internet Security)