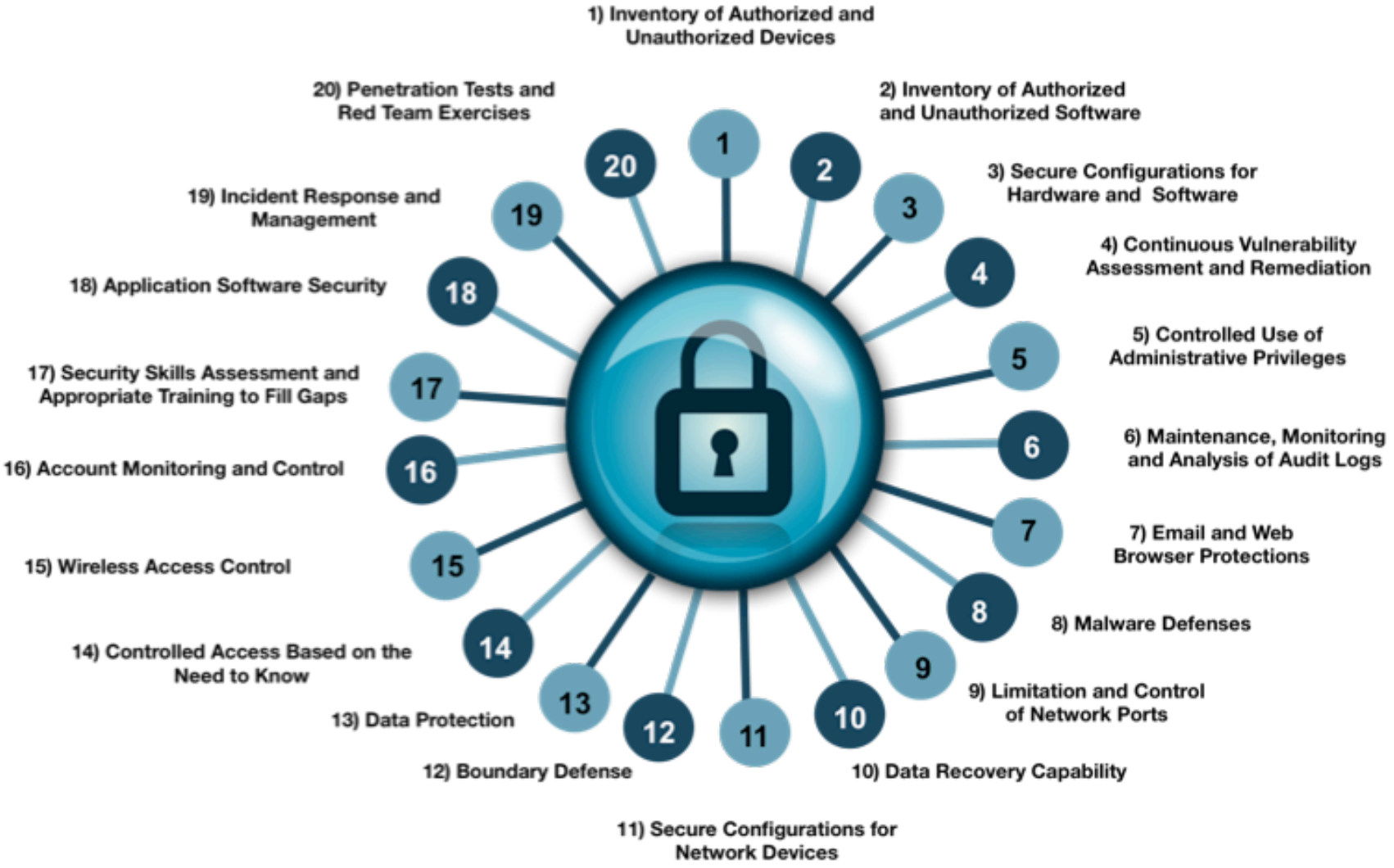
Center for
Internet Security®

A Community Attack Model

How Attackers Can Help You Design Your Defenses

Tony Sager
The Center for Internet Security

CIS Critical Security Controls (Version 6)



How did we get here?

NSA/DoD Project (2008)

Center for Strategic and International Studies (2008)
"The Consensus Audit Guidelines"

The SANS Institute (2009)
"The SANS Top 20 Critical Controls"

Council on CyberSecurity (2013; non-profit)
"The Critical Security Controls"

Center for Internet Security (2015, integration)
"The CIS Critical Security Controls"

"Offense Informs Defense"

- Gather a few friends that I trust
- Add thousands of friends
  - and repeat
- Translate/map from authoritative sources of data
  - Verizon DBIR, Symantec ISTR, HP Annual Report….
- Build and operate an open, repeatable process
- A "Community Attack Model"
  - Standardize language, workflow, "refresh cycle"
  - Align with Risk Management Frameworks, other models

Why a Community Attack Model?

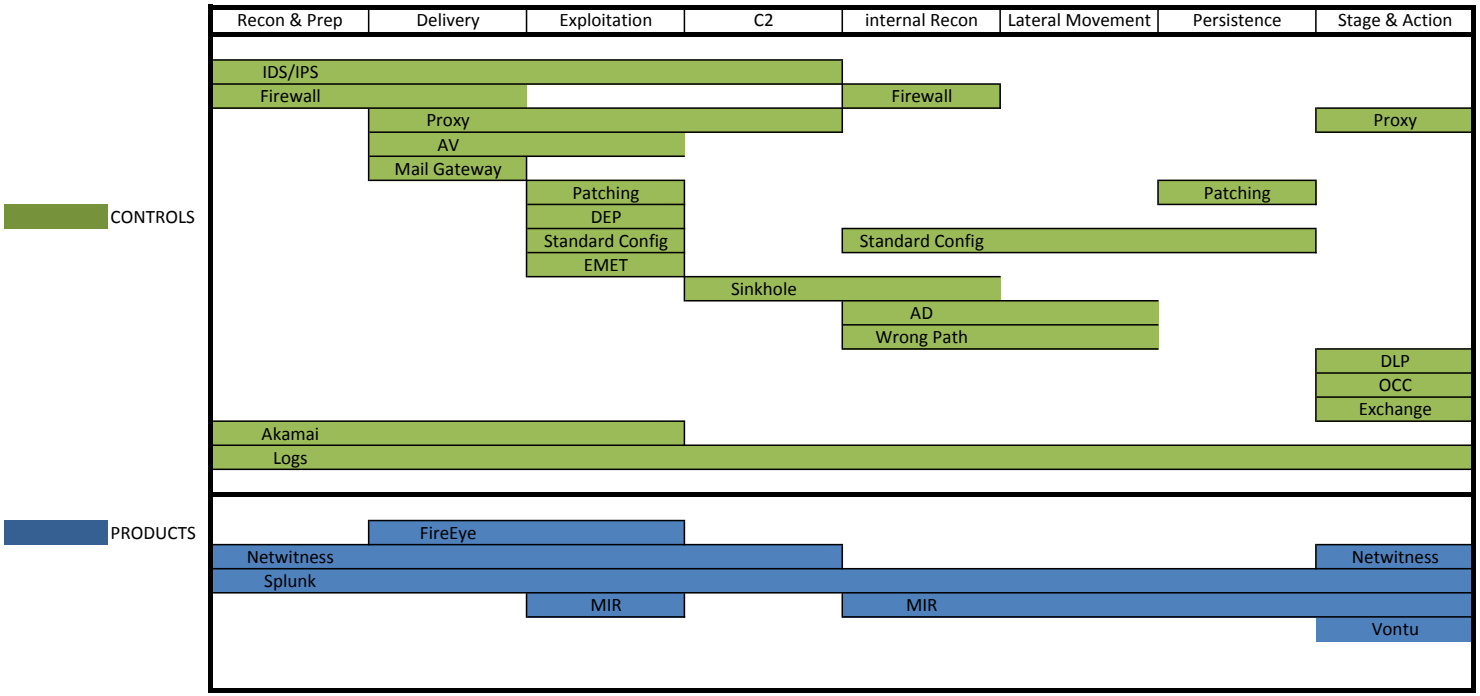
- Extend our information reach
  - *"volume, velocity, variety"*
- Most Enterprises can't do it on their own
  - *or cannot do it more than once*
- And even if you could, does that make sense…
  - *in a dynamic, connected world?*
  - *where trust and risk are dynamic, and must be negotiated?*

An Attack Model is about *Action*

- ***What*** do Attackers do, ***When***?
- ***Where*** are the opportunities to see, stop, etc.?
- ***What*** things should I put in place, ***Where,*** to help me the most effectively?

Sample 1: based on LM Kill Chain

A notional use of the Lockheed Kill Chain: mapping Controls to the Kill Chain; then mapping specific tool choices to the Kill Chain



Sample 2: based on Mandiant APT1 and JP 3-13

A notional use of the Mandiant APT1 model; mapping Controls to the Adversary model; then mapping specific tool choice

SOURCE: http://www.appliednsm.com/making-mandiant-apt1-report-actionable/

from Joint Pub JP 3-13, 2006

from JP 3-13	Recon	Delivery	Exploitation	Installation	C2	Actions or Objectives
DETECT	NIDS Router Logs Web Logs	NIDS HIDS Vigilant User AV	NIDS HIDS AV	HIDS Application Logs AV	HIDS NIDS AV	
DENY	Firewall ACL	Mail Filter Web Filter	HIPS AV Hardened Systems	App Whitelisting Block Execution	Egress Filter Firewall ACL Sinkhole	Egress Filter Firewall ACL NW Segmentation
DISRUPT	Active Defenses	Web Filter Mail Filter	HIPS AV Hardened Systems	AV HIPS	DEP Sinkhole	NW Segmentation DEP HIPS
DEGRADE	Honeypot Redirect Loops Active Defenses	Sinkhole Combo of Deny/Disrupt	Restrict User Accou	Combo of Deny/Dis	Sinkhole	NW Segmentation
DECEIVE	Honeypot Redirect Loops Active Defenses	Honeypot `	Honeypot	Honeypot	Honeypot Sinkhole	Honeypot
(DESTROY)	N/A	N/A	N/A	N/A	N/A	N/A

CIS Community Attack Model - Structure

		Attack Stages								
	Controls	Initial Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
Functions	Identify									
	Protect									
	Detect									
	Respond									
	Recover									

Each cell contains controls that ***Identify, Protect, Detect, Respond, Recover*** *against specific attack stages*

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	

Running an Operational Process

- Support the evolution of CIS Critical Security Controls
- Basis for mapping from Attack Summaries
  - And a baseline for effective use of Threat Intelligence
- Working with “closed systems”
- Operate an ongoing refresh cycle (is the model still good? Priority within the model?)

Contact

- Website: www.cisecurity.org
- Email: contact@cisecurity.org
- Twitter: @CISecurity
- Facebook: Center for Internet Security
- LinkedIn: The Center for Internet Security ; Critical Security Controls
- Addresses:

Mid-Atlantic Headquarters
1700 N. Moore Street, Suite 2100
Arlington, VA 22209

Northeast Headquarters
31 Tech Valley Drive, Suite 2
East Greenbush, NY 12061