Center for
Internet Security®

The Cyber OODA Loop:

How Your Attacker Should Help You Design Your Defense

Tony Sager
The Center for Internet Security

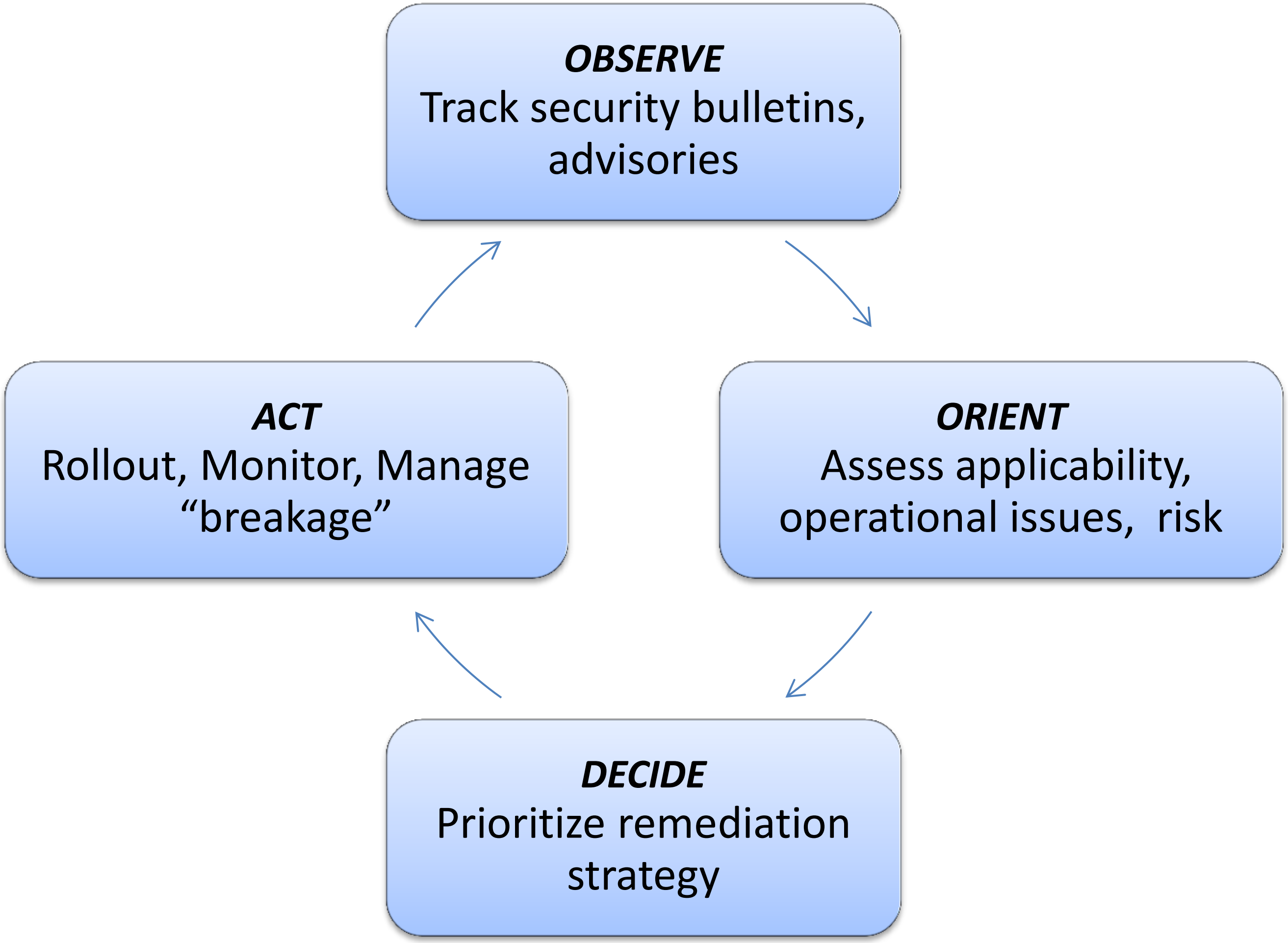
Classic Risk Equation

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

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

"The Fog of More"

An OODA Loop - Patching



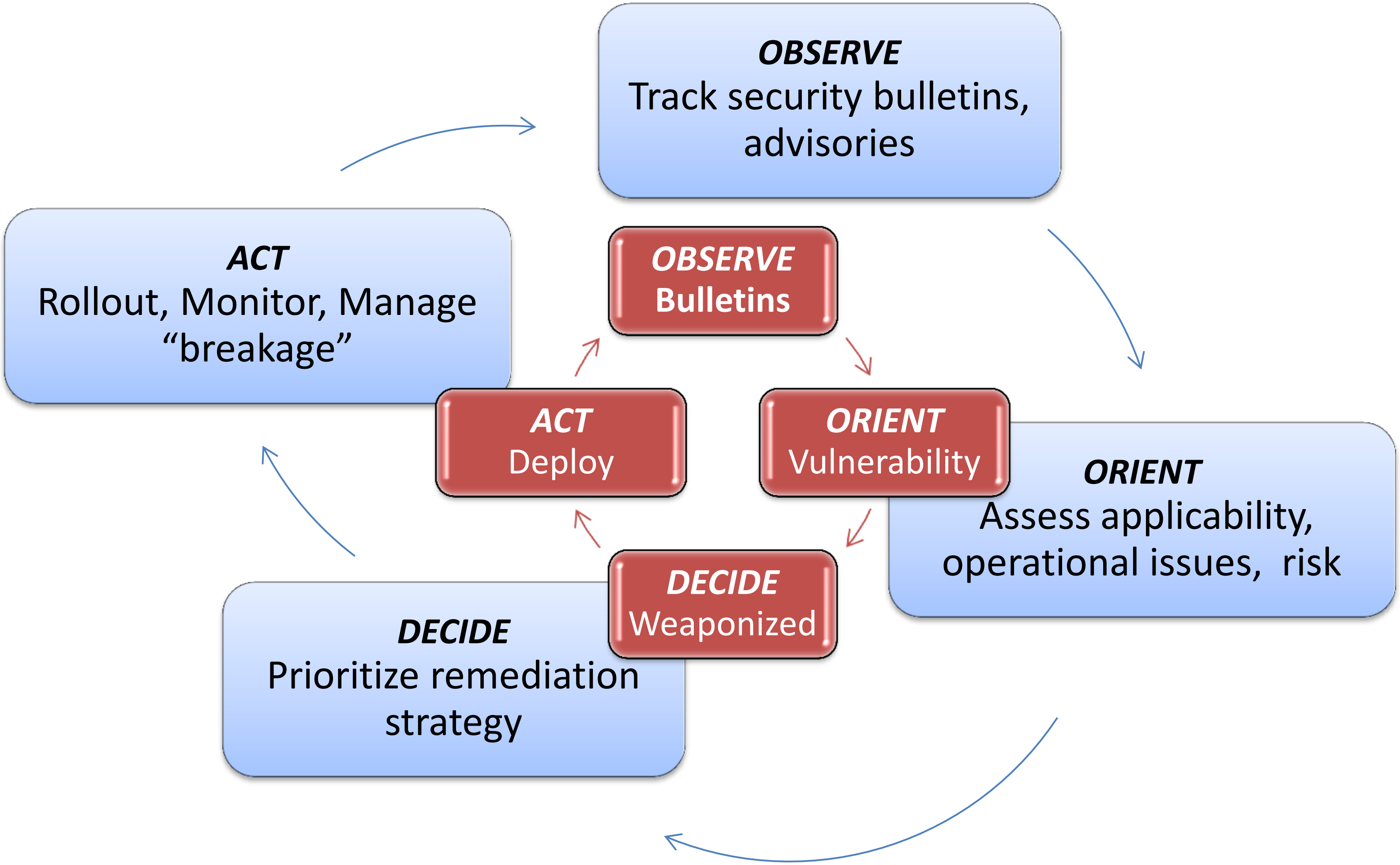
OBSERVE
Track security bulletins, advisories

ORIENT
Assess applicability, operational issues, risk

DECIDE
Prioritize remediation strategy

ACT
Rollout, Monitor, Manage "breakage"

“Dueling’ OODAs”



OBSERVE
Track security bulletins, advisories

ORIENT
Assess applicability, operational issues, risk

DECIDE
Prioritize remediation strategy

ACT
Rollout, Monitor, Manage “breakage”

OBSERVE
Bulletins

ORIENT
Vulnerability

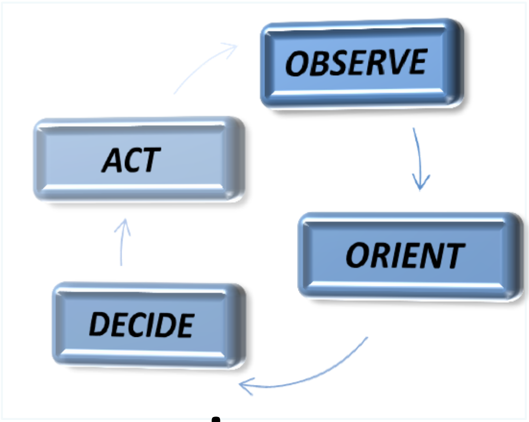
DECIDE
Weaponized

ACT
Deploy

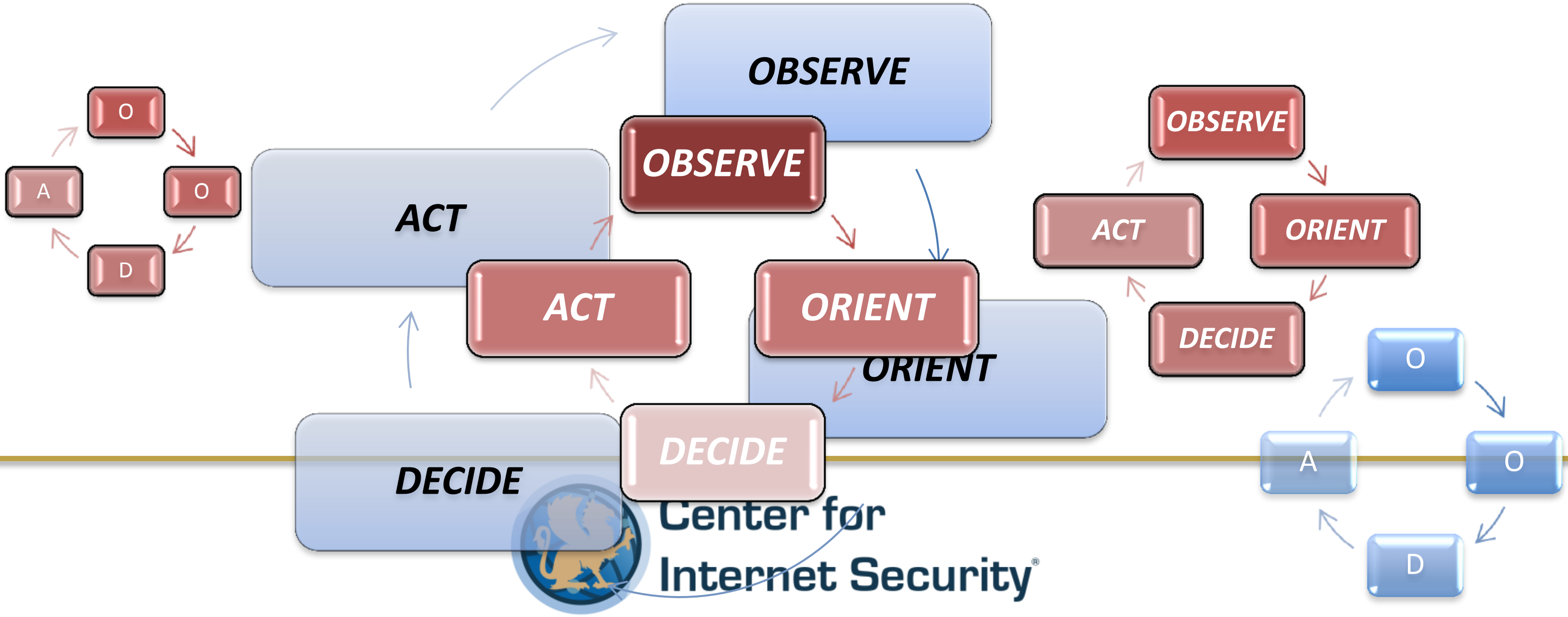
Center for Internet Security

Threat Intelligence

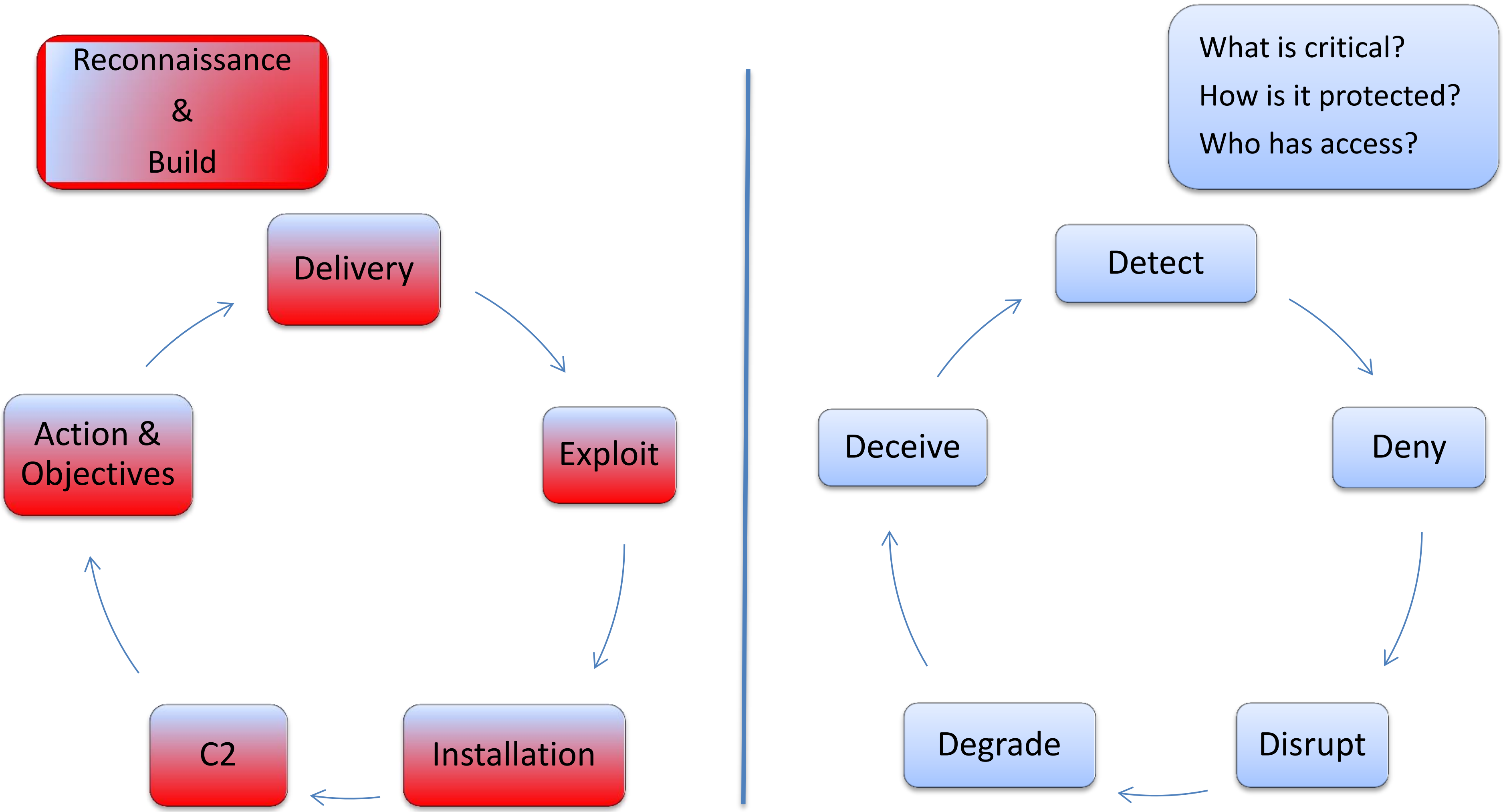
- There are many loops
  - Tactical AND Strategic
  - Often connected
- “farther in space, earlier in time”



- The Bad Guy’s loop is also an opportunity



Attack & Defend



Reconnaissance
&
Build

Delivery

Exploit

Installation

C2

Action & Objectives

What is critical?
How is it protected?
Who has access?

Detect

Deny

Disrupt

Degrade

Deceive

Samples of Attack Models

- ***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

🟩 CONTROLS

🟦 PRODUCTS

	Recon & Prep	Delivery	Exploitation	C2	internal Recon	Lateral Movement	Persistence	Stage & Action
IDS/IPS	🟩	🟩	🟩	🟩				
Firewall	🟩	🟩			🟩			
Proxy		🟩	🟩	🟩				🟩
AV		🟩	🟩					
Mail Gateway		🟩						
Patching			🟩				🟩	
DEP			🟩					
Standard Config			🟩		🟩	🟩	🟩	
EMET			🟩					
Sinkhole				🟩	🟩			
AD					🟩	🟩		
Wrong Path					🟩	🟩		
DLP								🟩
OCC								🟩
Exchange								🟩
Akamai	🟩	🟩	🟩					
Logs	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
FireEye		🟦	🟦					
Netwitness	🟦	🟦	🟦	🟦				🟦
Splunk	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
MIR			🟦		🟦	🟦	🟦	🟦
Vontu								🟦

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

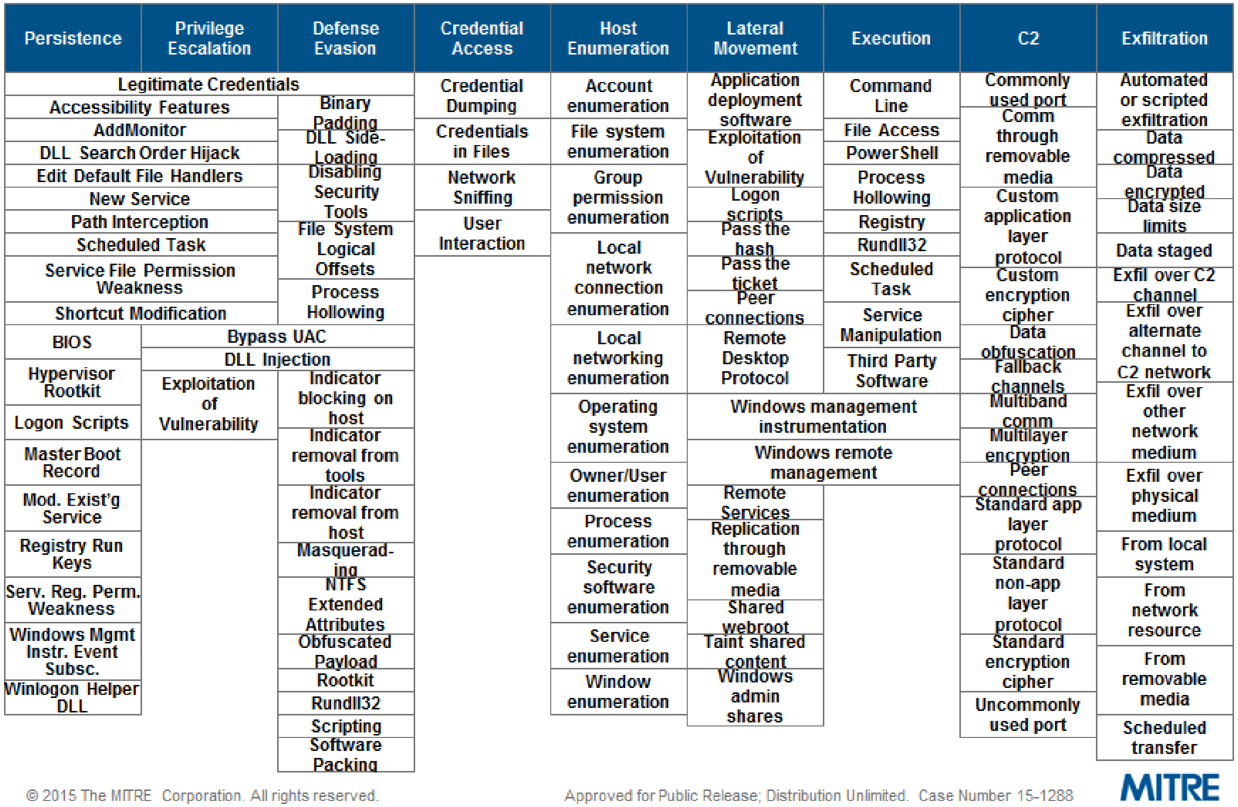
from JP 3-13	Recon	Delivery	Exploitation	Installation	C2	Actions on Objectives
DETECT	NIDS Router Logs Web Logs	NIDS HIDS Vigilant User AV	NIDS HIDS AV	HIDS Application Logs AV	HIDS NIDS AV	
DENY	Firewall ACL	Mail Filter Web Filter	HIPS AV Hardened Systems	App Whitelisting Block Execution	Egress Filter 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

Sample 3: MITRE ATT&CK Model (no controls)

The MITRE ATT&CK Matrix™ is a overview of the tactics and techniques described in the ATT&CK model.
It visually aligns individual techniques under the tactics in which they can be applied.
Some techniques span across more than one tactic because they can be used for different purposes.
SOURCE: https://attack.mitre.org/wiki/Main_Page

TACTICS ->

TECHNIQUES
|
V



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features	Accessibility Features	Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor	AddMonitor	DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack	DLL Search Order Hijack	Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers	Edit Default File Handlers	File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service	New Service	Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception	Path Interception	Bypass UAC		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task	Scheduled Task	DLL Injection		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness	Service File Permission Weakness	Indicator blocking on host		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification	Shortcut Modification	Indicator removal from tools		Service enumeration	Remote Services	Windows management instrumentation	Standard app layer protocol	From local system
BIOS	Bypass UAC	Indicator removal from host		Window enumeration	Replication through removable media	Windows remote management	Standard non-app layer protocol	From network resource
Hypervisor Rootkit	DLL Injection	Masquerading			Shared webroot		Standard encryption cipher	From removable media
Logon Scripts	Exploitation of Vulnerability	NTFS Extended Attributes			Taint shared content		Uncommonly used port	Scheduled transfer
Master Boot Record		Obfuscated Payload			Windows admin shares			
Mod. Exist'g Service		Rootkit						
Registry Run Keys		Rundll32						
Serv. Reg. Perm. Weakness		Scripting						
Windows Mgmt Instr. Event Subsc.		Software Packing						
Winlogon Helper DLL								

© 2015 The MITRE Corporation. All rights reserved.

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

MITRE

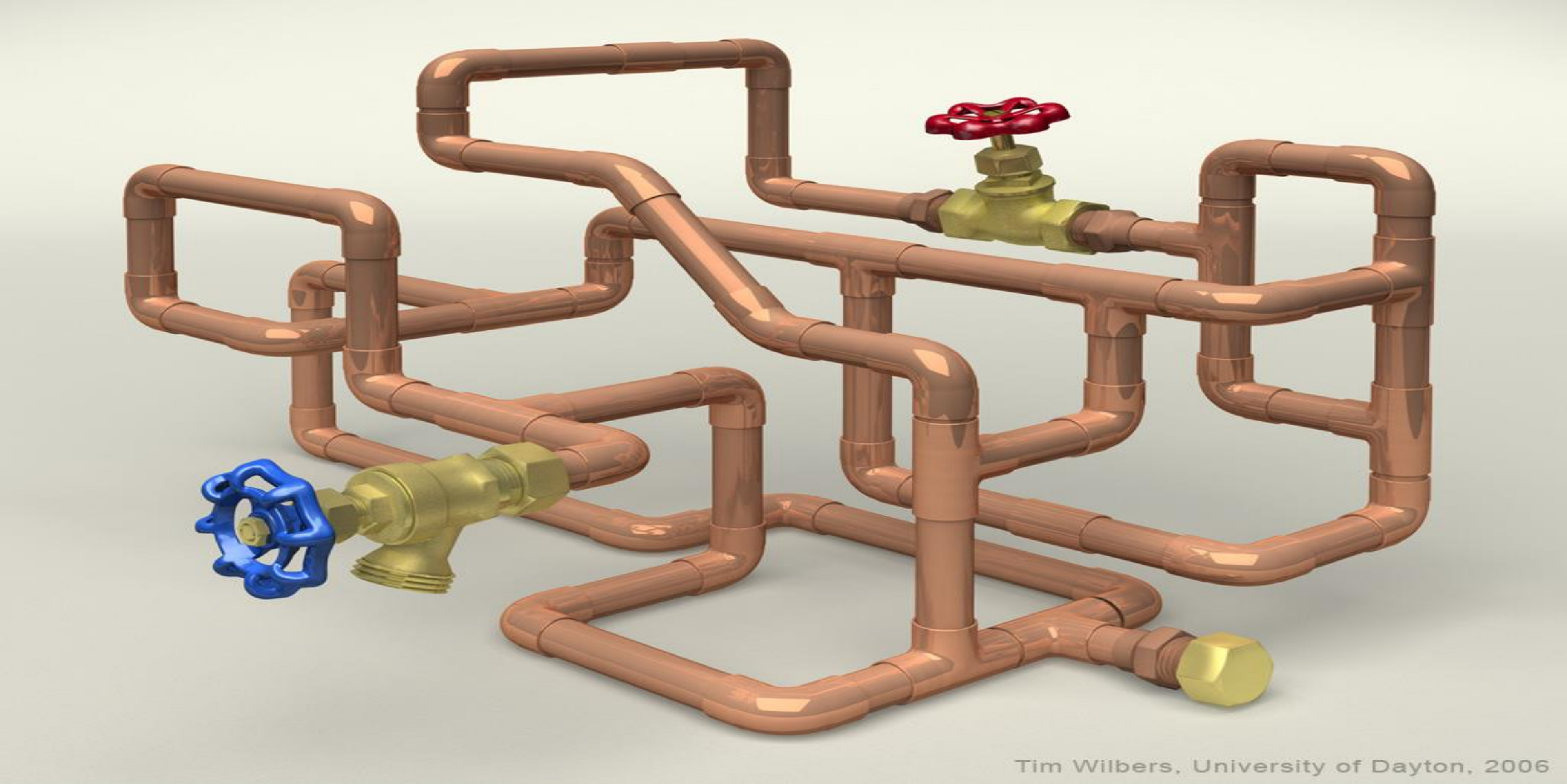
Center for Internet Security®

Sample 4: NIST CSF, LM Kill Chain, CSCs

NIST Cybersecurity Framework (V1.0)		CSC	Recon & Prep	Delivery	Exploitation	C2	internal Recon	Lateral Movement	Persistence	Stage & Action
Functions	Categories	Control #								
Identify	Asset Management (AM)	1,2	x				x	x		
	Business Environment (BE)									
	Governance (GV)									
	Risk Assessment (RA)	4	x	x	x		x	x	x	x
	Risk Management Strategy (RM)									
Protect	Access Control (AC)	7, 12, 15, 16		x			x	x		
	Awareness and Training (AT)	9	x	x						
	Data Security (DS)	17			x	x			x	x
	Information Protection Processes and Procedures (IP)	3, 6, 10, 11, 19	x		x	x			x	x
	Maintenance (MA)									
	Protective Technology (PT)	5	x	x	x	x	x	x	x	x
Detect	Anomalies and Events (AE)	14, 18			x				x	x
	Security Continuous Monitoring (CM)	4, 5, 16	x	x	x	x	x	x	x	x
	Detection Processes (DP)	13	x						x	x
Respond	Response Planning (RP)	18						x	x	x
	Communications (CO)									
	Analysis (AN)	14				x				x
	Mitigation (MI)	4	x	x			x	x		
	Improvements (IM)	20			x				x	x
Recover	Recovery Planning (RP)	8			x	x			x	x
	Improvements (IM)	20	x	x	x	x	x	x	x	x
	Communications (CO)									

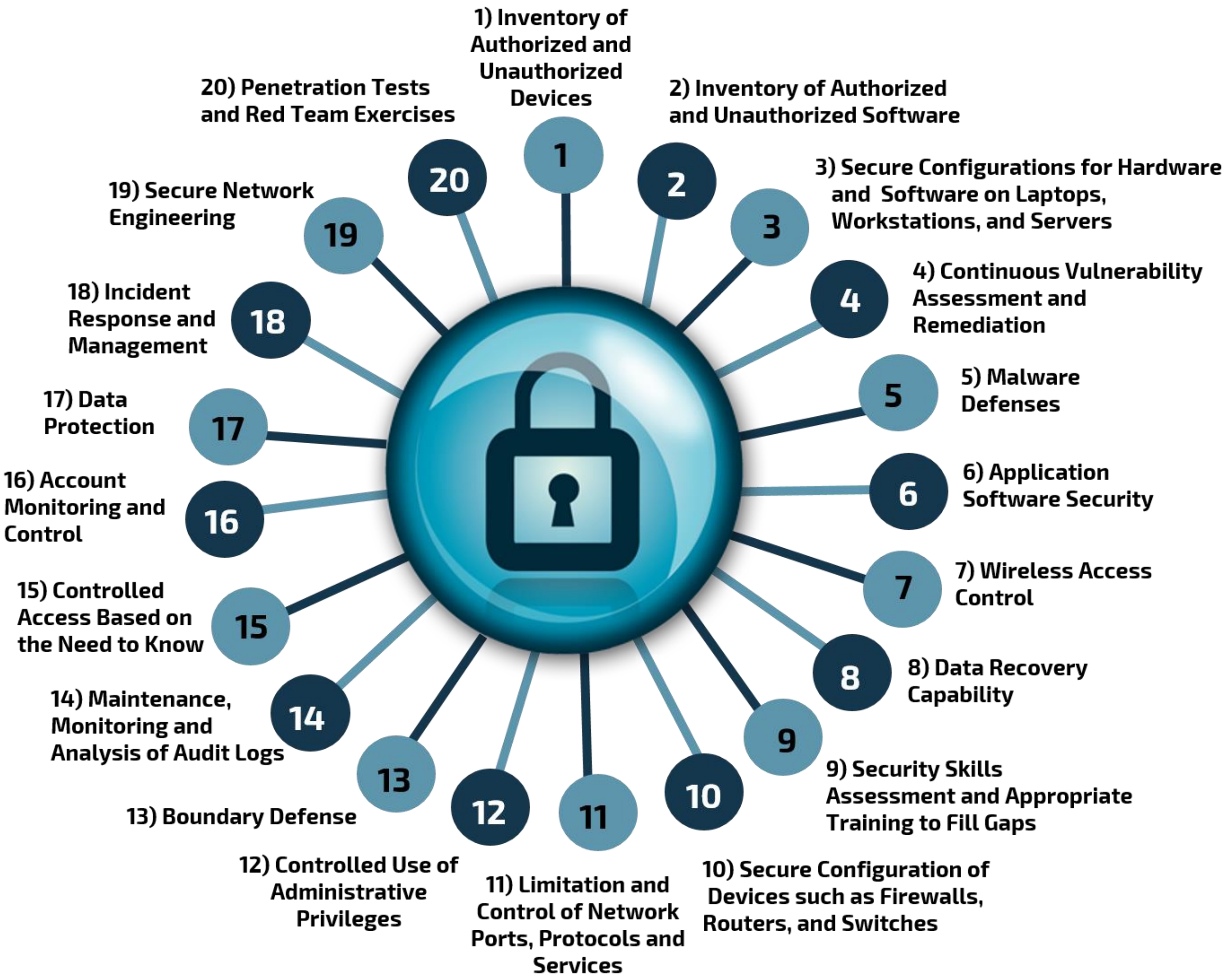
20 Critical Security Controls (V5.1)
CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configuration of End user devices
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Malware Defense
CSC 6: Application Software Security
CSC 7: Wireless Access Control
CSC 8: Data Recovery Capability
CSC 9: Security Skills Assessment and Appropriate Training
CSC 10: Secure Configuration of Network Devices
CSC 11: Limitation and Control of Network Ports, Protocols, and Service
CSC 12: Controlled Use of Administrative Privileges
CSC 13: Boundary Defense
CSC 14: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 15: Controlled Access Based on Need to Know
CSC 16: Account Monitoring and Control
CSC 17: Data Protection
CSC 18: Incident Response and Management
CSC 19: Secure Network Engineering
CSC 20: Penetration Tests and Red Team Exercises

Cybersecurity "Plumbing"



Tim Wilbers, University of Dayton, 2006

Critical Security Controls



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

4) Continuous Vulnerability Assessment and Remediation

5) Malware Defenses

6) Application Software Security

7) Wireless Access Control

8) Data Recovery Capability

9) Security Skills Assessment and Appropriate Training to Fill Gaps

10) Secure Configuration of Devices such as Firewalls, Routers, and Switches

11) Limitation and Control of Network Ports, Protocols and Services

12) Controlled Use of Administrative Privileges

13) Boundary Defense

14) Maintenance, Monitoring and Analysis of Audit Logs

15) Controlled Access Based on the Need to Know

16) Account Monitoring and Control

17) Data Protection

18) Incident Response and Management

19) Secure Network Engineering

20) Penetration Tests and Red Team Exercises

Center for Internet Security®

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