
IT NATION™
SECURE
hosted by CONNECTWISE

MITRE: Understanding the Cybersecurity Kill Chain

Presented by Harry Perper

IT NATION SECURE

MITRE: Understanding the Cybersecurity Kill Chain

Presented by Harry Perper

MITRE
SOLVING PROBLEMS FOR A SAFER WORLD®

MITRE tackles complex challenges with no commercial interest.

Together with government and public private partnerships, we work to improve the safety, stability, and well-being of our nation.

We apply systems thinking to solve complex national and global problems, bringing an interdisciplinary perspective to R&D.

We operate six federally funded R&D centers, as well as MITRE Labs and an independent research program.

65+ LOCATIONS WORLDWIDE

9,000+ EMPLOYEES

60+ YEARS

260+ PATENTS

MITRE
SOLVING PROBLEMS FOR A SAFER WORLD®

MITRE ATT&CK Introduction

@mitreattack

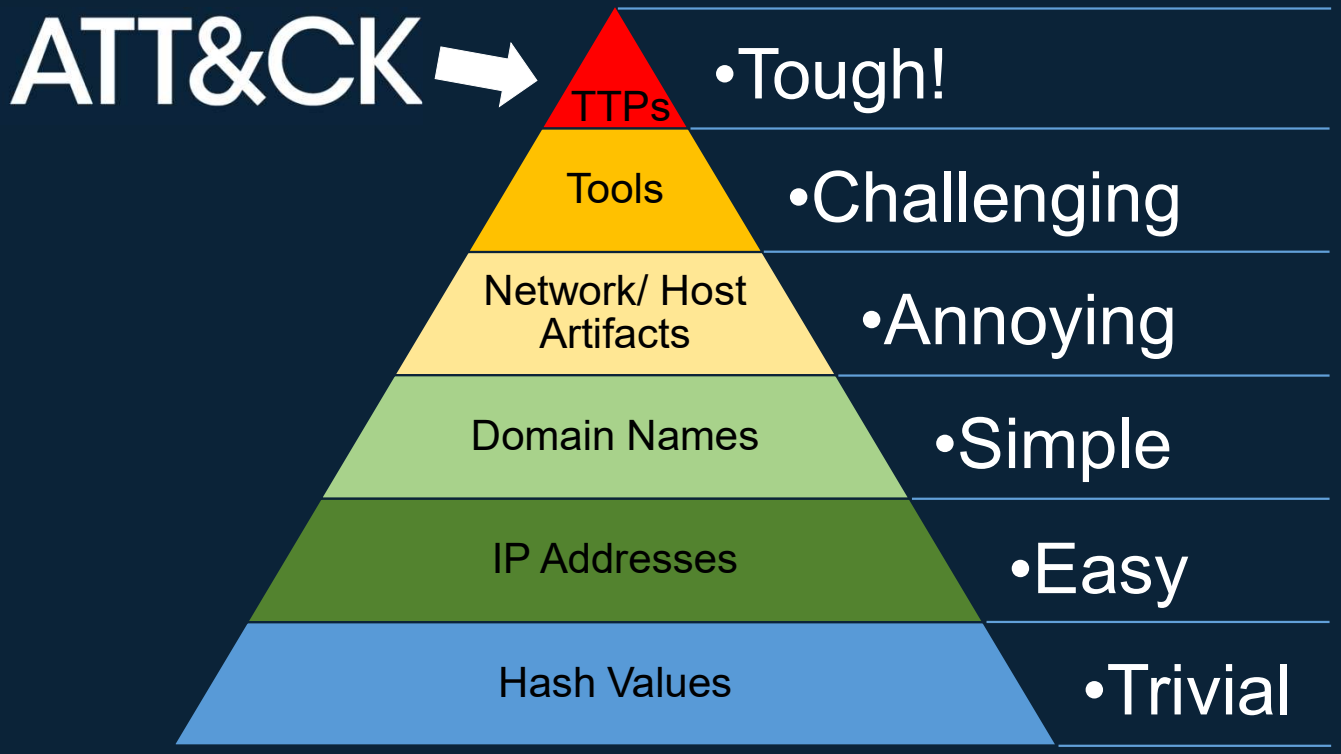
MITRE | ATT&CK®

What is ATT&CK?

A knowledge base of adversary behavior

- ***Based on real-world observations***
- ***Free, open, and globally accessible***
- ***A common language***
- ***Community-driven***

The Difficult Task of Changing TTPs



Source: David Bianco, https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

David Bianco's Pyramid of Pain

ATT&CK Knowledge Base Basics

Tactics: the adversary's technical goals

Techniques: how the goals are achieved

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Valid Accounts					Network Sniffing	System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
Replication Through Removable Media					OS Credential Dumping	Application Window Discovery	Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Trusted Relationship					Input Capture	System Network Configuration Discovery	Replication Through Removable Media	Input Capture	Application Layer Protocol	Data Transfer Size Limits	Service Stop
Supply Chain Compromise					Brute Force	System Owner/User Discovery	Internal Spearphishing	Data Staged	Proxy	Exfiltration Over C2 Channel	Inhibit System Recovery
Hardware Additions					Two-Factor Authentication Interception	System Network Connections Discovery	Use Alternate Authentication Material	Screen Capture	Communication Through Removable Media	Exfiltration Over Physical Medium	Defacement
Exploit Public-Facing Application					Exploitation for Credential Access	Permission Groups Discovery	Lateral Tool Transfer	Email Collection	Web Service	Exfiltration Over Web Service	Firmware Corruption
Phishing					Steal Web Session Cookie	File and Directory Discovery	Taint Shared Content	Clipboard Data	Multi-Stage Channels	Automated Exfiltration	Resource Hijacking
External Remote Services					Unsecured Credentials	Peripheral Device Discovery	Exploitation of Remote Services	Automated Collection	Ingress Tool Transfer	Exfiltration Over Alternative Protocol	Network Denial of Service
Drive-by Compromise					Credentials from Password Stores	Network Share Discovery	Remote Service Session Hijacking	Audio Capture	Data Encoding	Transfer Data to Cloud Account	Endpoint Denial of Service
					Steal or Forge Kerberos Tickets	Password Policy Discovery		Video Capture	Traffic Signaling		System Shutdown/Reboot
					Forced Authentication			Man in the Browser	Remote Access Software		Account Access Removal
					Steal Application Access Token			Data from Information Repositories	Dynamic Resolution		Disk Wipe
								Man-in-the-Middle	Non-Standard Port		Data Manipulation
								Archive Collected Data	Protocol Tunneling		
								Data from Network Shared Drive	Encrypted Channel		
									Non-Application Layer Protocol		

Sub-techniques: More specific techniques

Phishing

Sub-techniques (3)

ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service

Procedures: Adversary technique and sub-technique implementations

Phishing: Spearphishing Attachment

Procedure Examples

Name	Description
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]

Technique: Phishing

Home > Techniques > Enterprise > Phishing

Phishing

Sub-techniques (3)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems or to gather credentials for use of Valid Accounts. Phishing may also be conducted via third-party services, like social media platforms.

Sub-technique: Spearphishing Attachment

Home > Techniques > Enterprise > Phishing > Spearphishing Attachment

Phishing: Spearphishing Attachment

Other sub-techniques of Phishing (3)

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Sub-technique: Spearphishing Attachment

Home > Techniques > Enterprise > Phishing > Spearphishing Attachment

ID: T1566.001

Sub-technique of: T1566

ⓘ Tactic: Initial Access

ⓘ Platforms: Linux, Windows, macOS

Contributors: Philip Winther

Version: 2.2

Created: 02 March 2020

Last Modified: 18 October 2021

Sub-technique: Spearphishing Attachment

Home > Techniques > Enterprise > Phishing > Spearphishing Attachment

Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
M1031	Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
M1021	Restrict Web-Based Content	Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.
M1054	Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.[242][243]
M1017	User Training	Users can be trained to identify social engineering techniques and spearphishing emails.

Sub-technique: Spearphishing Attachment

Home > Techniques > Enterprise > Phishing > Spearphishing Attachment

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor for third-party application logging, messaging, and/or other artifacts that may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.[242][243] Anti-virus can potentially detect malicious documents and attachments as they're scanned to be stored on the email server or on the user's computer. Monitor for suspicious descendant process spawning from Microsoft Office and other productivity software.[244]
DS0022	File	File Creation	Monitor for newly constructed files from a spearphishing emails with a malicious attachment in an attempt to gain access to victim systems.
DS0029	Network Traffic	Network Traffic Content	Monitor and analyze SSL/TLS traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.[242][243]
		Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

Sub-technique: Spearphishing Attachment

Home > Techniques > Enterprise > Phishing > Spearphishing Attachment

Procedure Examples

Name	Description
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]
APT28	APT28 sent spearphishing emails containing malicious Microsoft Office attachments. [22] [23] [24] [25] [26] [27]

References

1. Sherstobitoff, R., Malhotra, A. (2018, October 18). 'Operation Oceansalt' Attacks South Korea, U.S., and Canada With Source Code From Chinese Hacker Group. Retrieved November 30, 2018.
2. Llimos, N., Pascual, C.. (2019, February 12). Trickbot Adds Remote Application Credential-Grabbing Capabilities to Its Repertoire. Retrieved March 12, 2019.
46. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
47. Counter Threat Unit Research Team. (2017, July 27). The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets. Retrieved February 26, 2018.
48. Carr, N., et al. (2017, April 24). FIN7 Evolution and the Phishing

Group: APT29

Home > Groups > APT29

APT29

APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. [1] [2] This group reportedly compromised the Democratic National Committee starting in the summer of 2015. [3]

ID: G0016

Associated Groups: YTTRIUM, The Dukes, Cozy Bear, CozyDuke

Version: 1.2

Group: APT29

Home > Groups > APT29

Software

ID	Name	References	Techniques
S0054	CloudDuke	[1]	Remote File Copy, Standard Application Layer Protocol, Web Service
S0049	GeminiDuke	[1]	Account Discovery, File and Directory Discovery, Process Discovery, Standard Application Layer Protocol, System Network Configuration Discovery, System Service Discovery

References

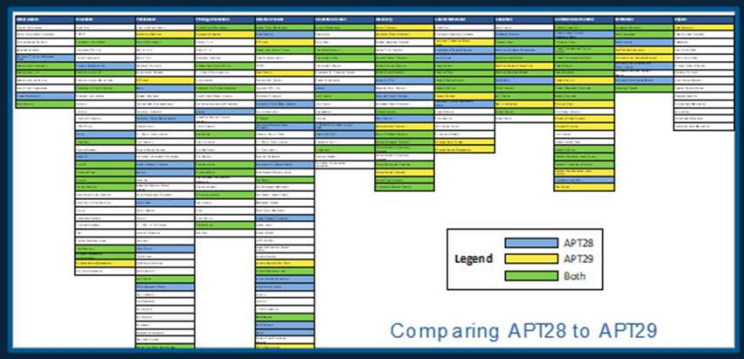
1. F-Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved December 10, 2015.
2. Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity.
6. Dunwoody, M. (2017, March 27). APT29 Domain Fronting With TOR. Retrieved March 27, 2017.
7. Dunwoody, M., et al. (2018, November 19). Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign. Retrieved November 27, 2018.

ATT&CK Use Cases

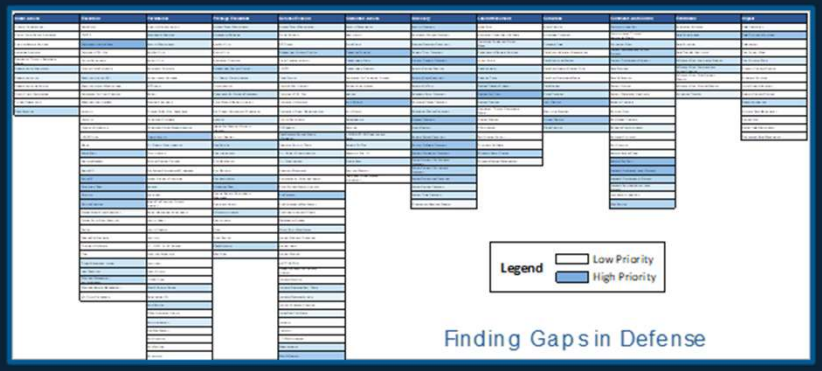
Detection

```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe
== "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and
parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and
reg.hostname == cmd.hostname)
output reg_and_cmd
```

Threat Intelligence



Assessment and Engineering



Adversary Emulation

ATT&CK

https://attack.mitre.org

attack@mitre.org

@mitreattack

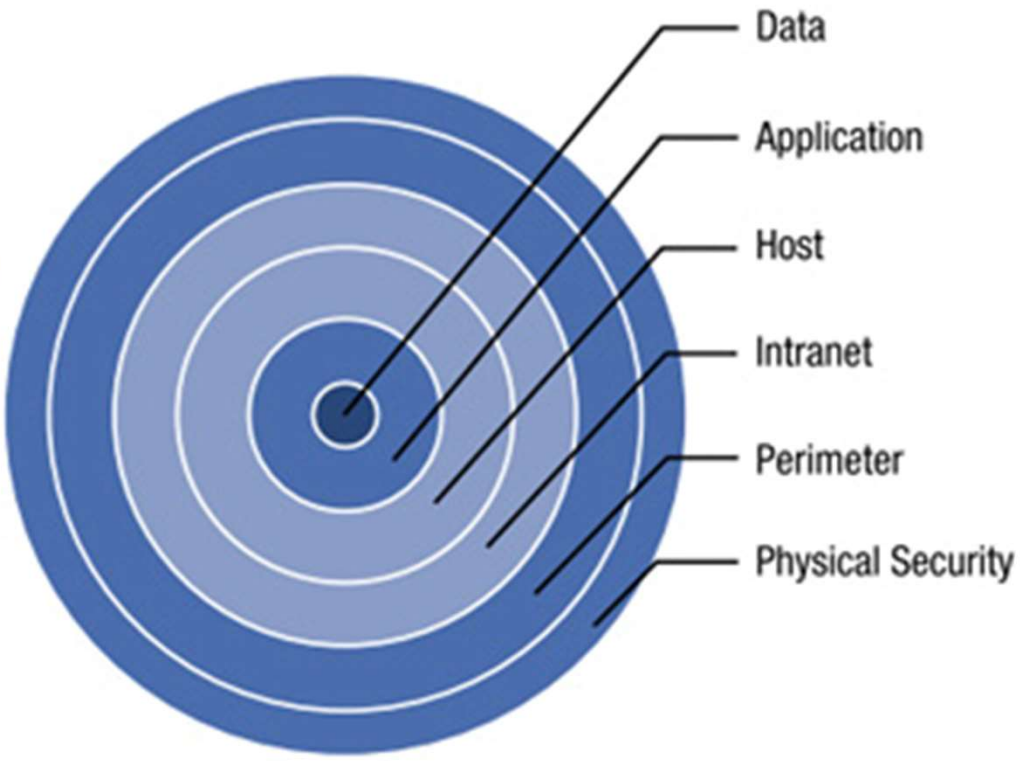
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

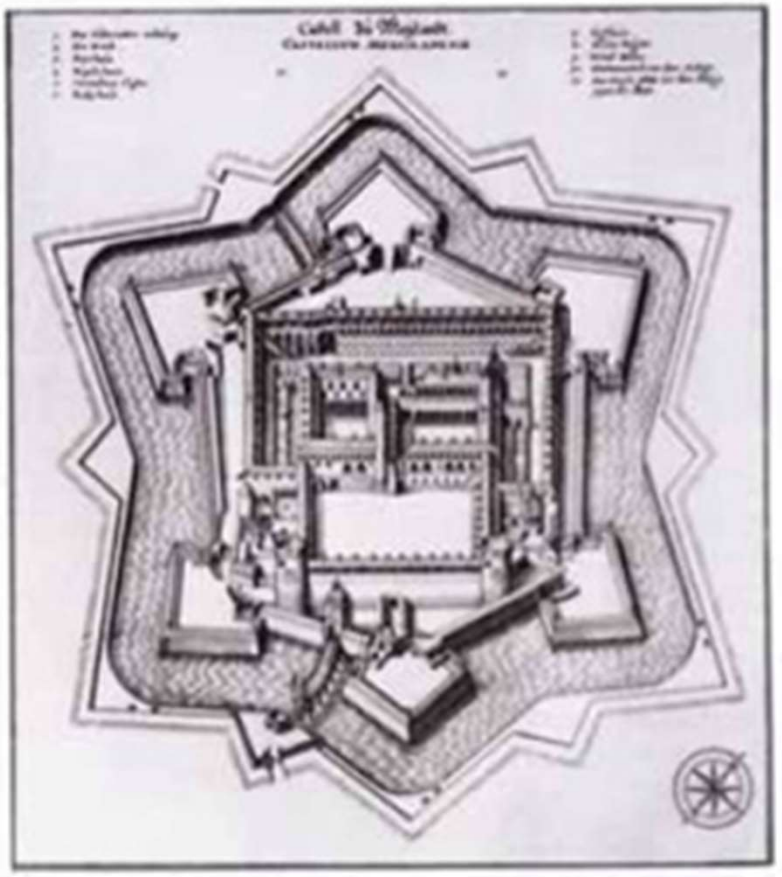
Some Thoughts on Deception

Harry Perper

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

The Limitations of Defense-in-Depth





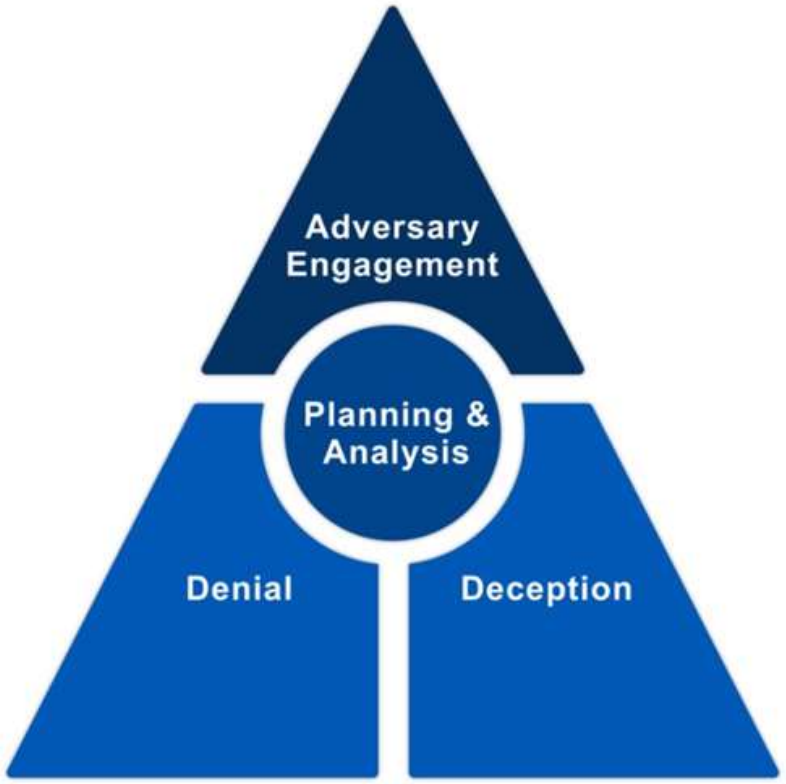
How can we
think differently about
the inside of the castle?

MITRE

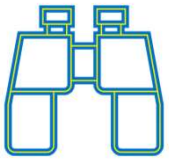
Cyber Denial reveal facts and fictions to prevent or impair the adversary's operations.

Cyber Deception conceal facts and fictions to mislead and confuse the adversary.

When used together with strategic planning and analysis, they provide the pillars of **Adversary Engagement**.



The Goals of Adversary Engagement



Expose

adversaries currently on the network

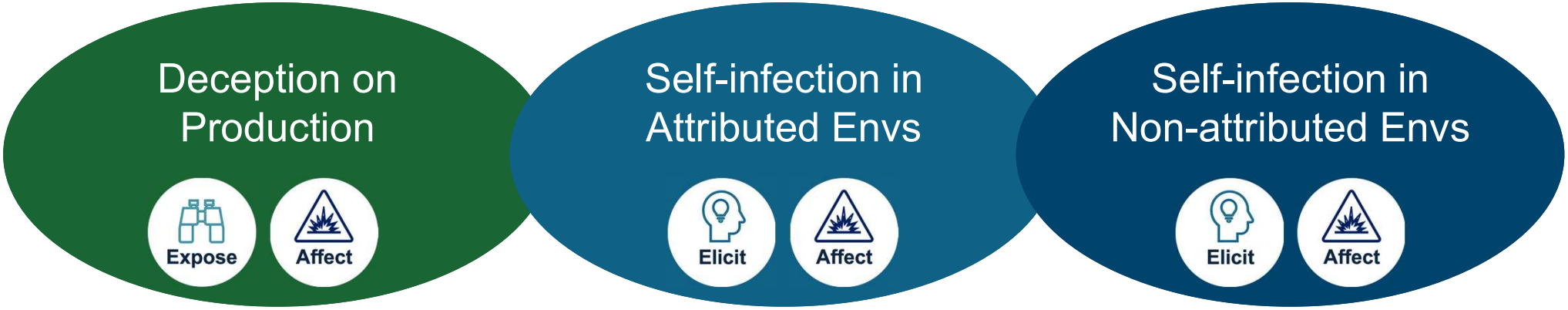
Affect

adversaries by imposing cost on their operations

Elicit

information about adversaries' tactics, techniques, and procedures

Opportunity Space



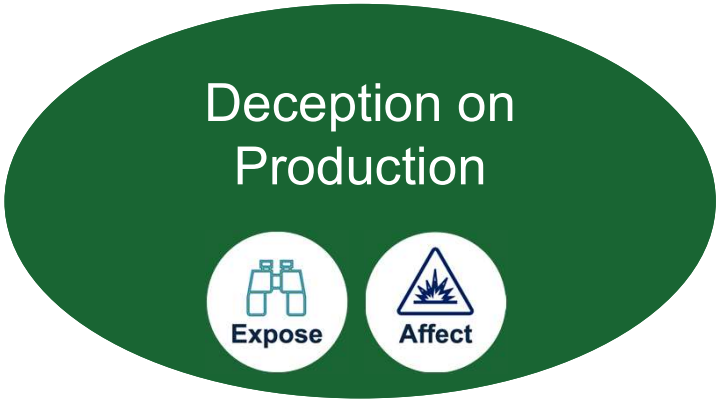
- High-fidelity alerts leading to better analytics using deception for detection
  - Focus on lateral movement, reconnaissance, and stolen credentials
- Obfuscate production network
- Detect insider threats

- Vector threats into deception environment for monitoring
- Gain intelligence on APTs targeting your organization
- Don't want to use gold disk image

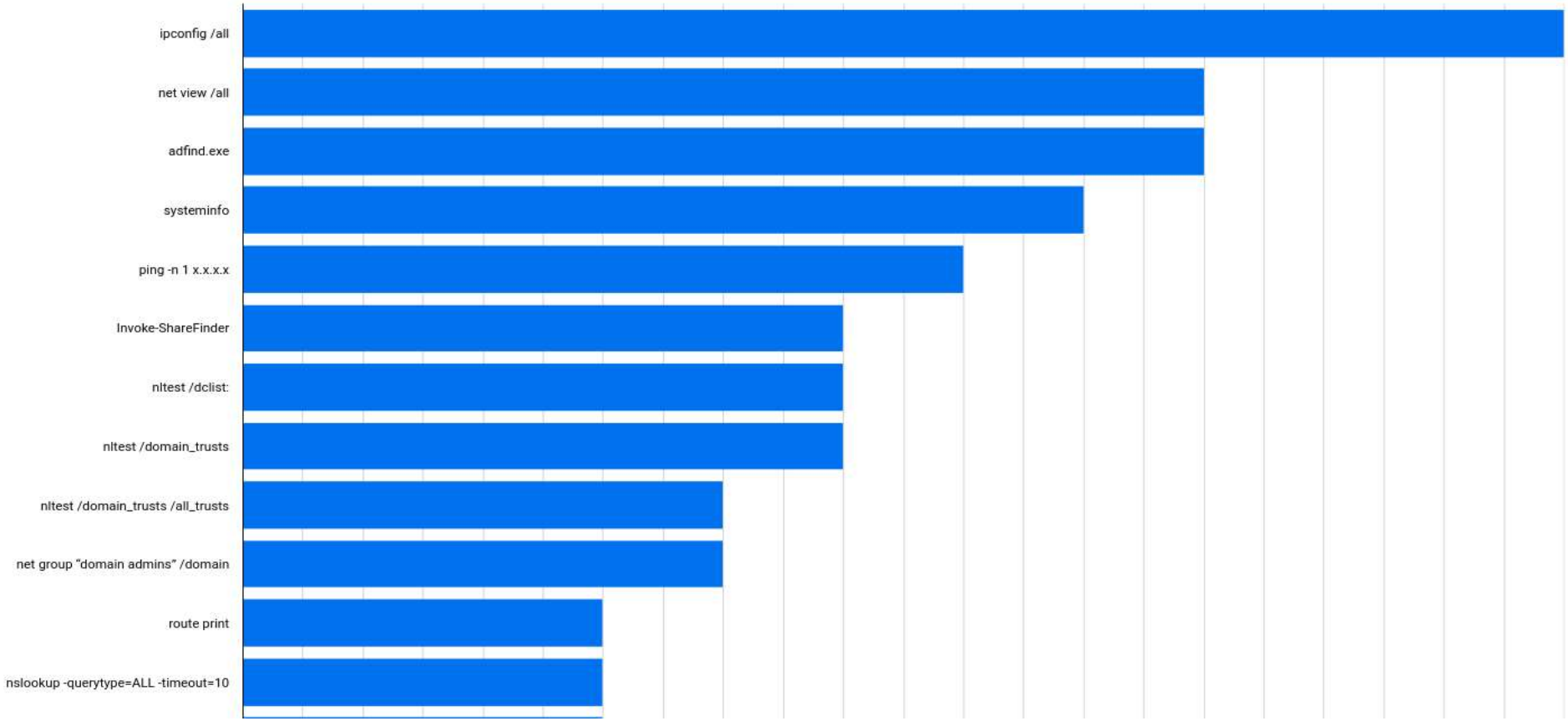
- Elicitation ops to target high-value APTs
- Opportunities for open data sharing
- Can be difficult to get relevant results

MITRE

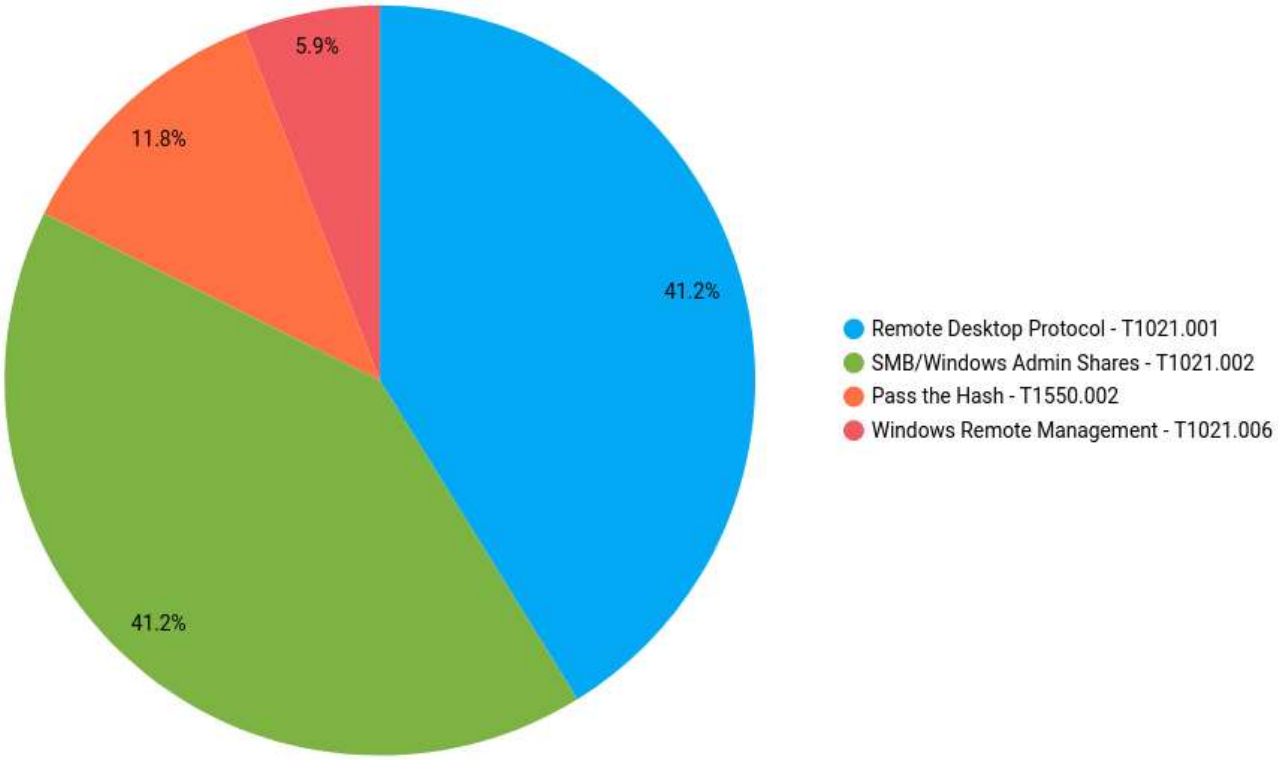
Let’s Zoom in on the Opportunity Space in Production



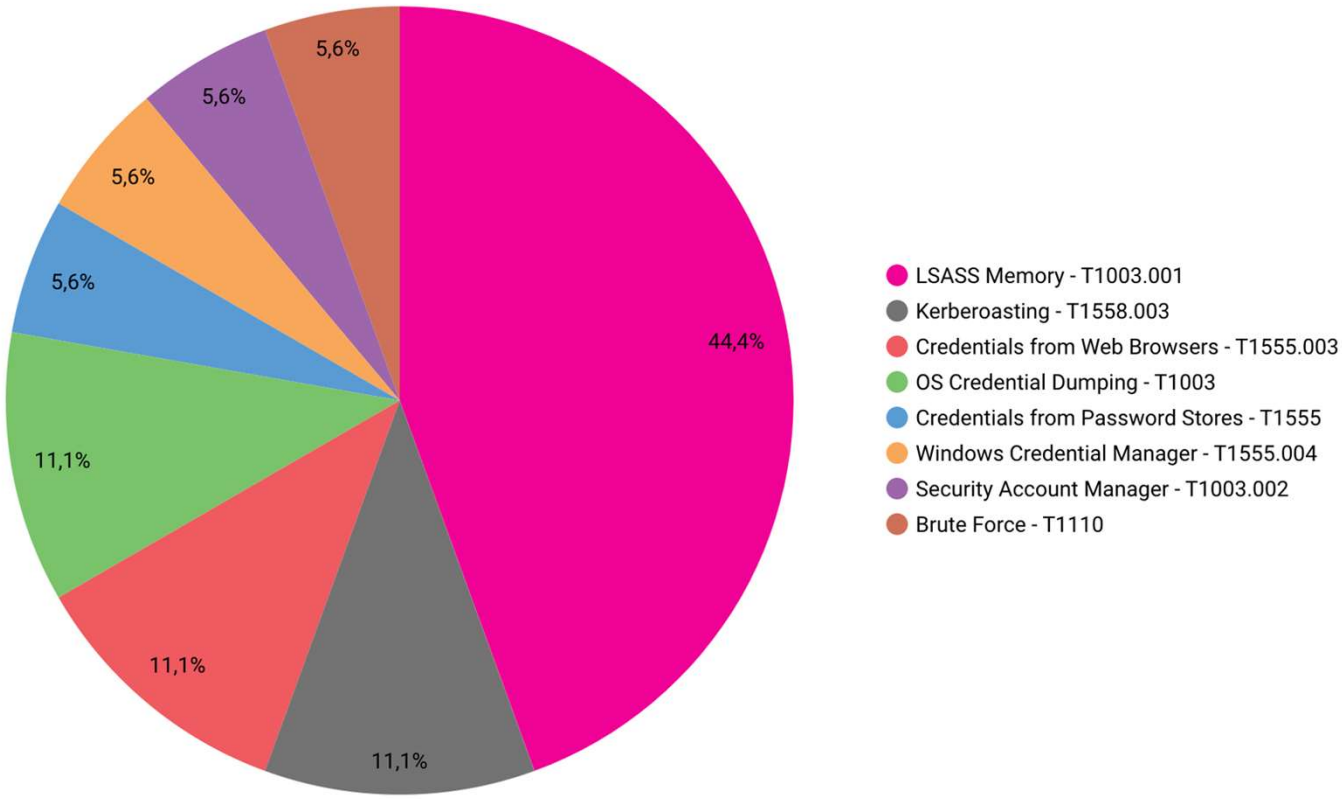
Reconnaissance



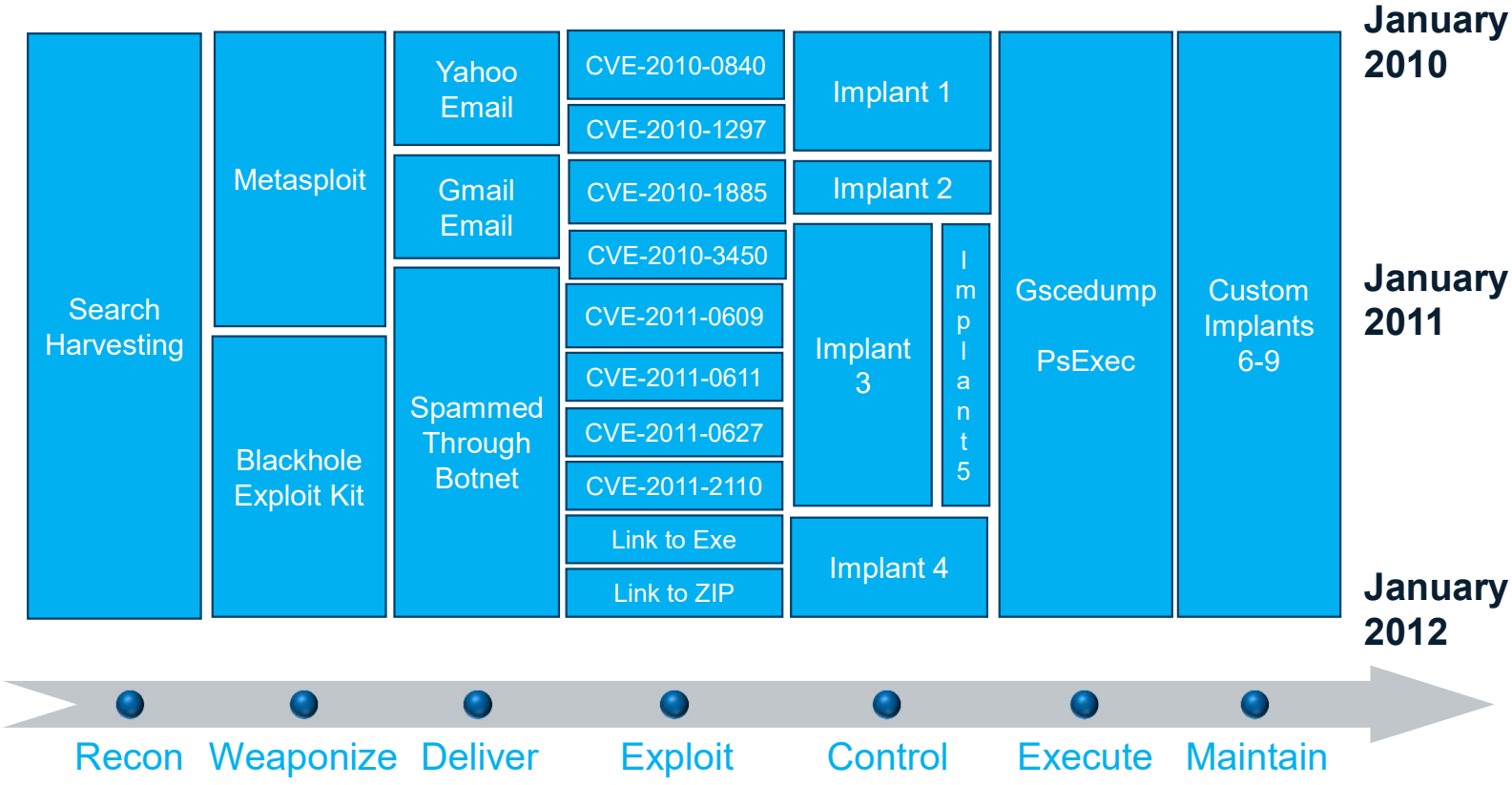
Lateral Movement



Stolen Credentials



Long term study of APT group from 2010-2012



Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense
Kristin E.Heckman
Frank J.Stech
Roshan K.Thomas
Ben Schmoker
Alexander W.Tsow
Springer International Publishing - 2015

Even basic IOCs can be valuable ROI

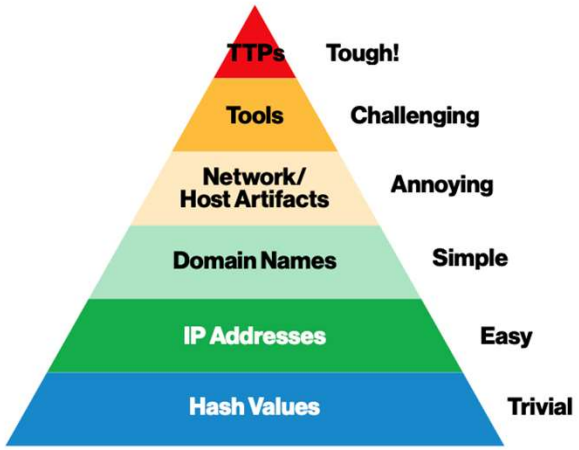


Figure 45. Pyramid of Pain

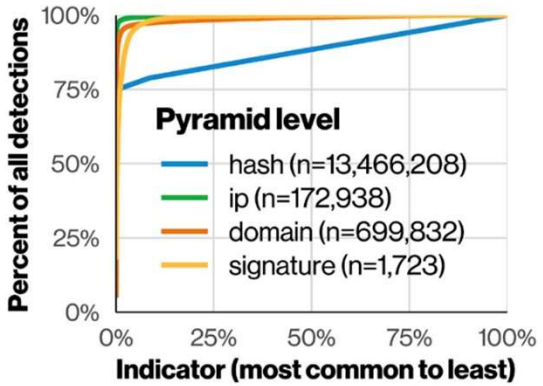
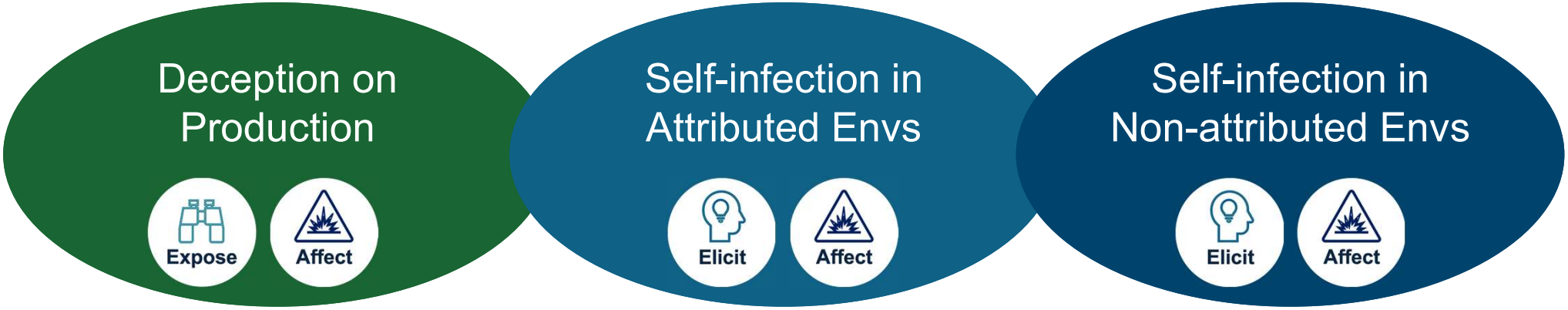
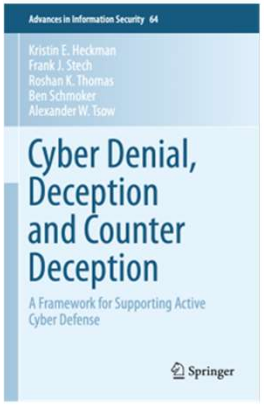


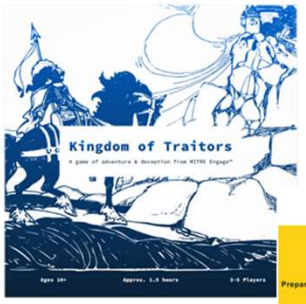
Figure 46. Cumulative sum of indicators

"Other than hashes, most indicators in the Pyramid of Pain have pretty high Gini coefficients. That means that if you block the first few percent of that indicator, you stop most of the malice. Frankly we expected that the Gini coefficient would go up as we went up the pyramid, but from IP addresses on up, they are all about the same." 2022 DIBR

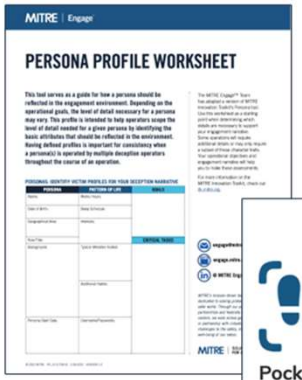
MITRE Offerings in the Opportunity Space

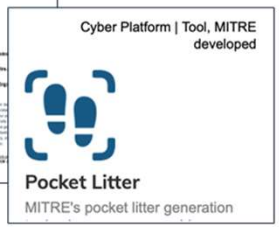


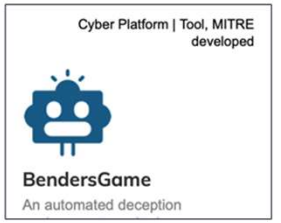




Knowledge of Vendor Space



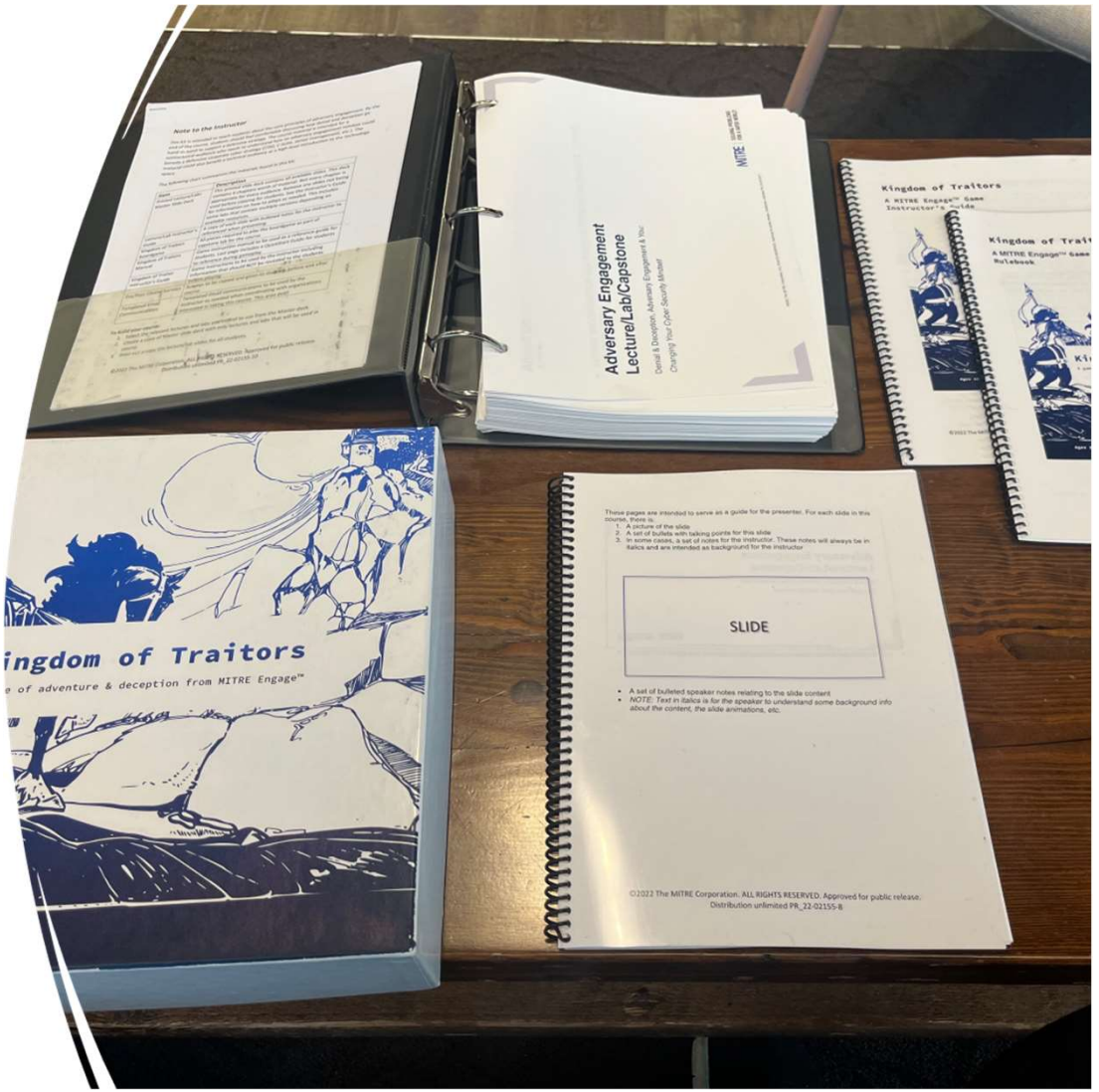




Engage in a Box

- A nontechnical Train the Trainer Kit designed to help organizations ***think*** differently about adversary engagement

- Contains:
  - Labs
  - Lectures
  - An educational boardgame

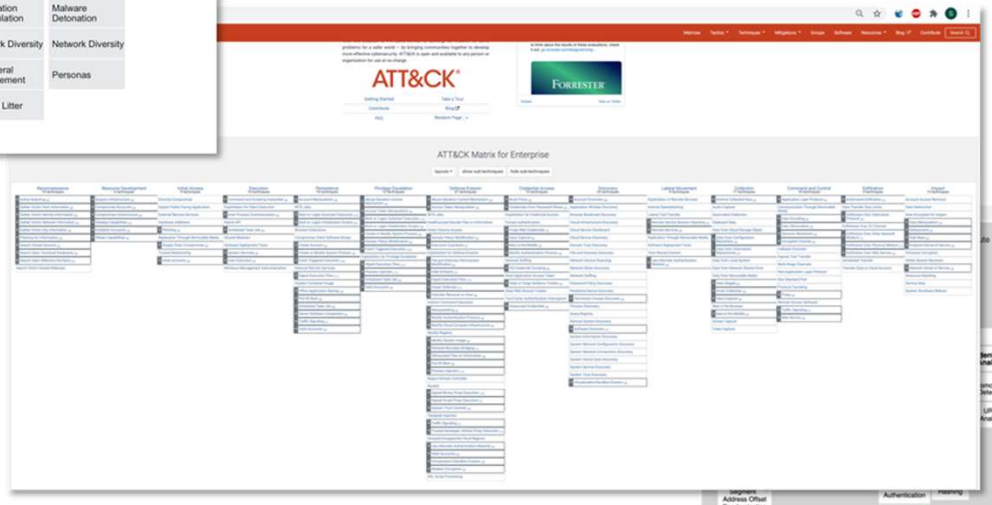


MITRE's many frameworks!

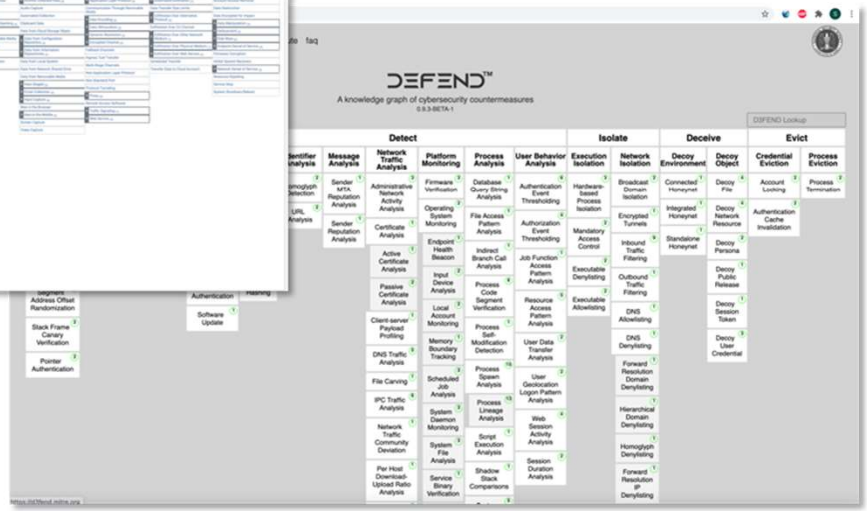
How do we engage with them?

Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	Cyber Threat Intelligence
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	After-Action Review
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

How do we document them?

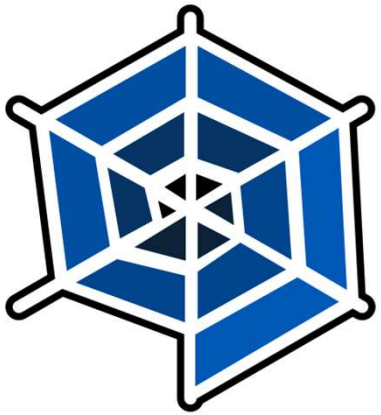


How do we counter them?



MITRE

MITRE Engage



MITRE Engage is a **framework**

for **planning and discussing adversary engagement activities**

that **enables operations** within and across **the public and private sectors**.

Engage Focus Areas

MATRIX

A shared reference that **bridges the gap** between defenders, decision-makers, and vendors.

PLAYBOOK

Actionable and pragmatic guidance for integrating adversary engagement.

PROCESS

Methods to plan and learn from engagements, **building capabilities** with every operation.

COMMUNITY

Cyber professionals **contributing expertise and sharing insights** into adversary behaviors.

STANDARDS

Standards and terminology to **apply, assess, and validate** engagement operations and tools.

MINDSET

Empowering you to **redefine what security means** and **rethink how to achieve it**.

MITRE

Exemplar Infrastructure Suggestions

- Small business environment
  - Managed endpoint with centrally authenticated user account(s)
- Medium business environment
  - Small and on-site webapp and file server to offer lateral movement

Using Cyber Resiliency to Improve Your Skills

Focus – Data Back-up and Disaster Recovery

MITRE

Agenda

1. Introduction
2. Cyber Resiliency Engineering
   - What it is and is not
3. Disaster Recovery and Data Back-up
   - Risk tolerance
   - Planning
   - Implementation
   - Testing

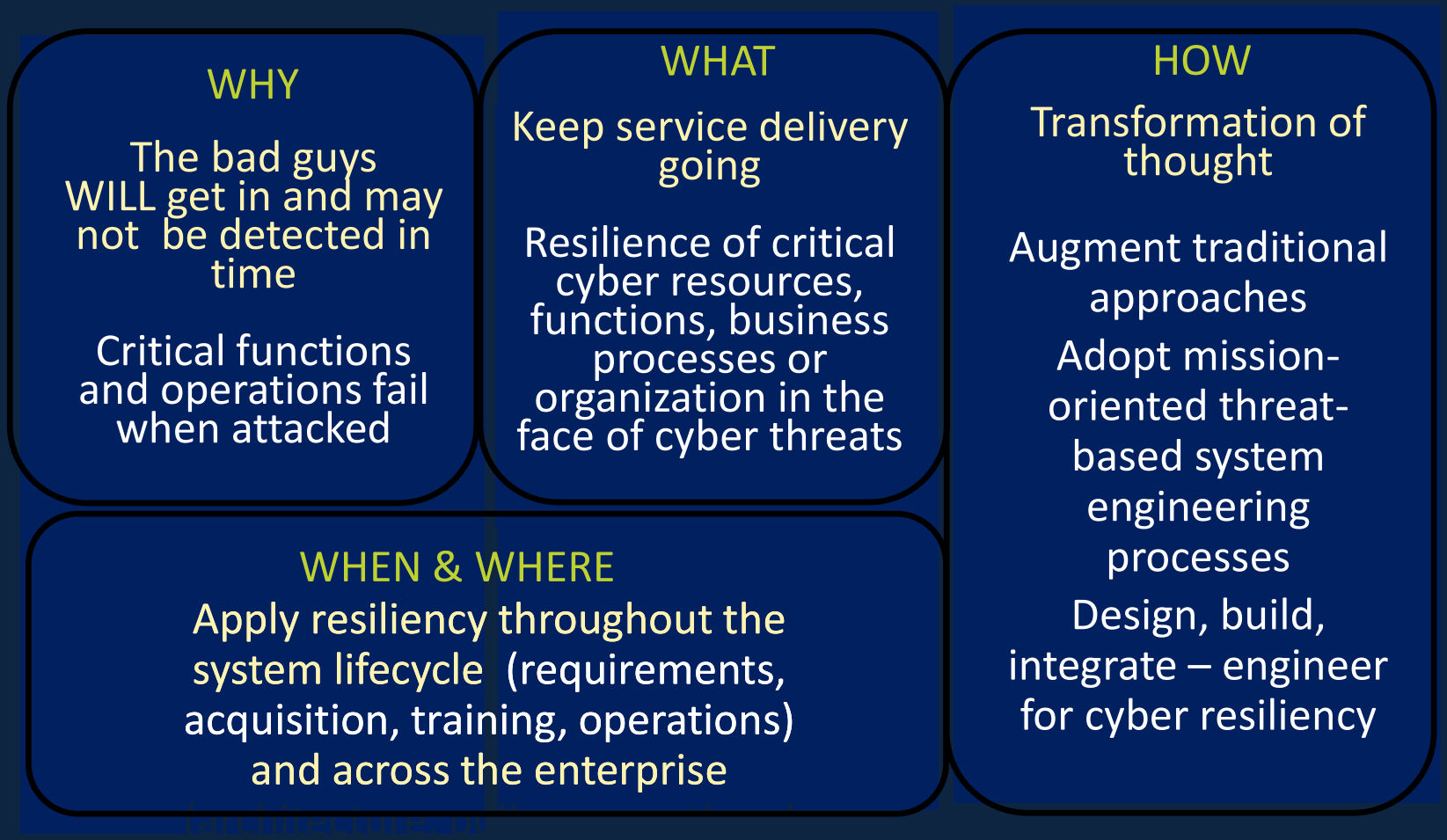
Cyber Resiliency Overview

Cyber Resiliency

How does it relate to cybersecurity?

Cyber Resiliency: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources

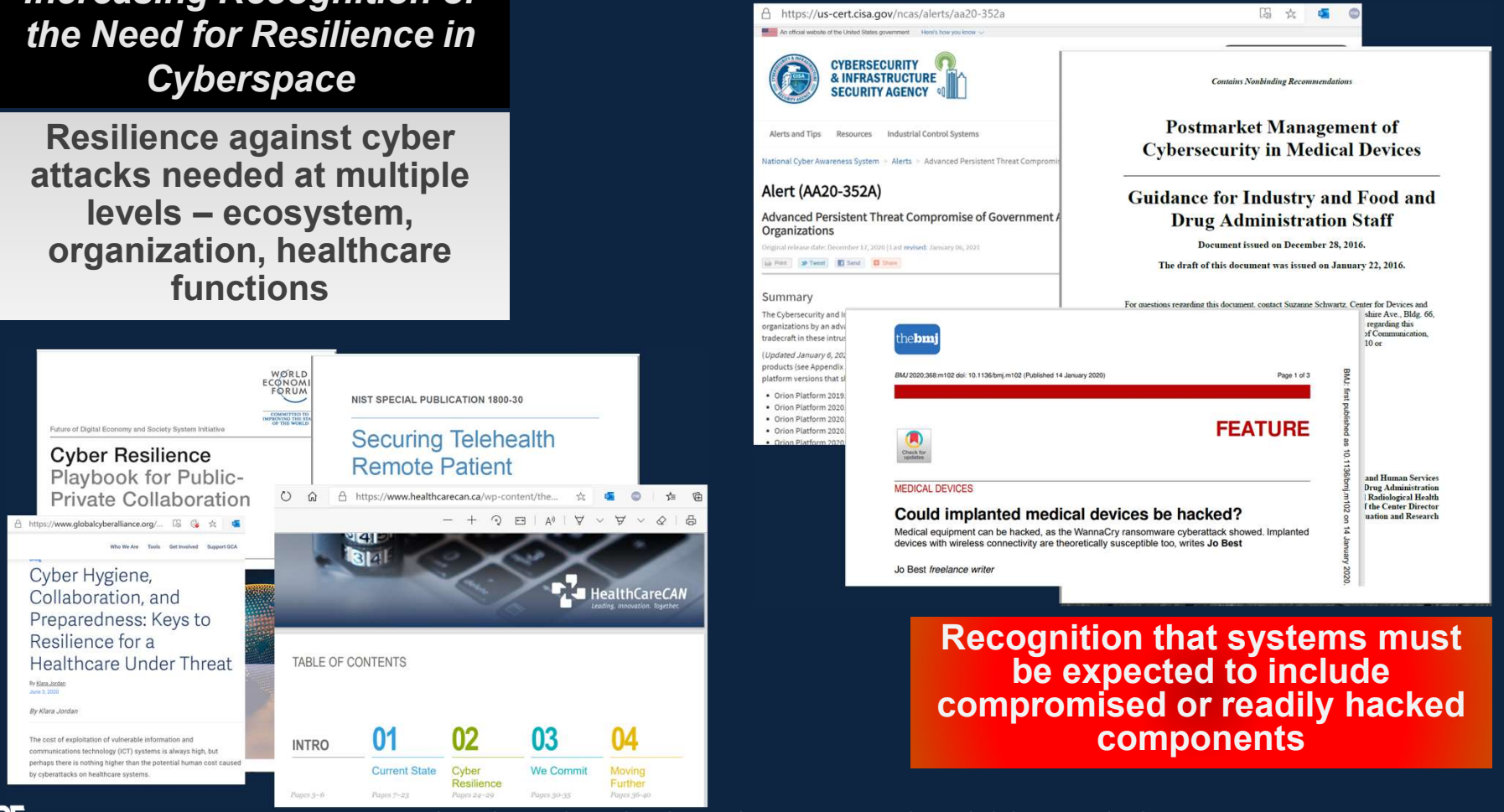
Cyber Resiliency – "Why" Drives What, How, When, and Where



Recognized need: Cyber Dependence and Cyber Threats

Increasing Recognition of the Need for Resilience in Cyberspace

Resilience against cyber attacks needed at multiple levels – ecosystem, organization, healthcare functions



Recognition that systems must be expected to include compromised or readily hacked components

What Is the Relationship Between Cybersecurity and Cyber Resiliency?

Limitations with Conventional Cyber Security Practices

Traditional Cybersecurity Practices	Limitations
Establish an effective security perimeter	No perimeter is 100% effective at keeping adversaries out
Use up-to-date A/V s/w to detect malware	A/V is ineffective against zero-day attacks
Encrypt data while at rest and in transit	Encrypted traffic is a great place for adversary activity to hide
Monitor and audit all user activity	Audit logs are rarely checked due to lack of time and resources, focused on individual components and do not provide big picture view of adversary activities
back-up plans, contingency plans, IA policies, accreditations, etc.	deal with natural disasters, thus are ineffective against the APT who will apply the same attacks against back-ups

Threat assumptions, adversary presence, compromise focus differ for resiliency

	Conventional Cyber Security	Cyber Resiliency
Threat Assumptions with respect to Adversary	**Capabilities: Limited Intent: Self aggrandizement, personal benefits Targeting: Targets of opportunity Timeline: Episodic Stealthy: No**	**Capabilities: Sophisticated, well resourced Intent: Establish & maintain ability to undermine mission Targeting: High value targets, very persistent Timeline: Long term campaigns Stealthy: Very**
Adversary Presence	**Assumes can be kept out or can quickly be detected and removed**	**Assumes adversary has established a foothold**
Focus of Type of	**Limited duration events, natural**	**Ongoing attacks, long term adversary presence,**
	present to impede recovery	**despite presence of adversary**
Goals	**Protect, Detect, React**	**Anticipate, Withstand, Recover, Evolve**

Cyber resiliency measures can complement or sometimes replace conventional cyber security measures

Illustrative Scenario – Traditional Cybersecurity

1) Attacker uses 0-day exploit to penetrate systems at local facility
2) Malware spreads within local facility; user accounts compromised
3) Malware takes advantage of homogeneous software environment, compromised accounts to spread to corporate network
4) Static host environment enables attacker to maintain foothold

Traditional defenses (boundary protection and patching) are insufficient

Illustrative Scenario with Cyber Resiliency Applied

Resiliency enables the enterprise to complete missions, provide essential services, or perform essential functions *despite* successful attacks.

- Segmentation: distinct internal enclaves → *Contain adversary's advance*
- Diversity: run IE, Chrome, Firefox, etc. → *Negate adversary's assumptions*
- Non-Persistence: reimage software periodically → *Expunge malware (foothold lost)*
- Substantiated Integrity: quality / consistency checks → *Detect corruption, limit its effects*
- Deception: detonation chambers, honeynets → *Detect malware, divert adversary*
- Unpredictability: ASLR, randomizing compiler, … → *Delays attack progression*

Knowledge of specific attack not required Patching of vulnerabilities not the focus
Detection of adversaries is helpful but not required AND It's not just about technology – includes defender TTPs

MITRE

Moving from Cybersecurity to Cyber Resiliency?

Implement conventional cybersecurity / resilience capabilities in a novel or enhanced ways (e.g., use AI to enhance intrusion detection, employ micro-segmentation)

Active threats use case analogies (e.g., sports and military) (e.g., provide misleading information and use deception environments to confuse adversaries, change behavior or states at random times)

Conventional Cybersecurity

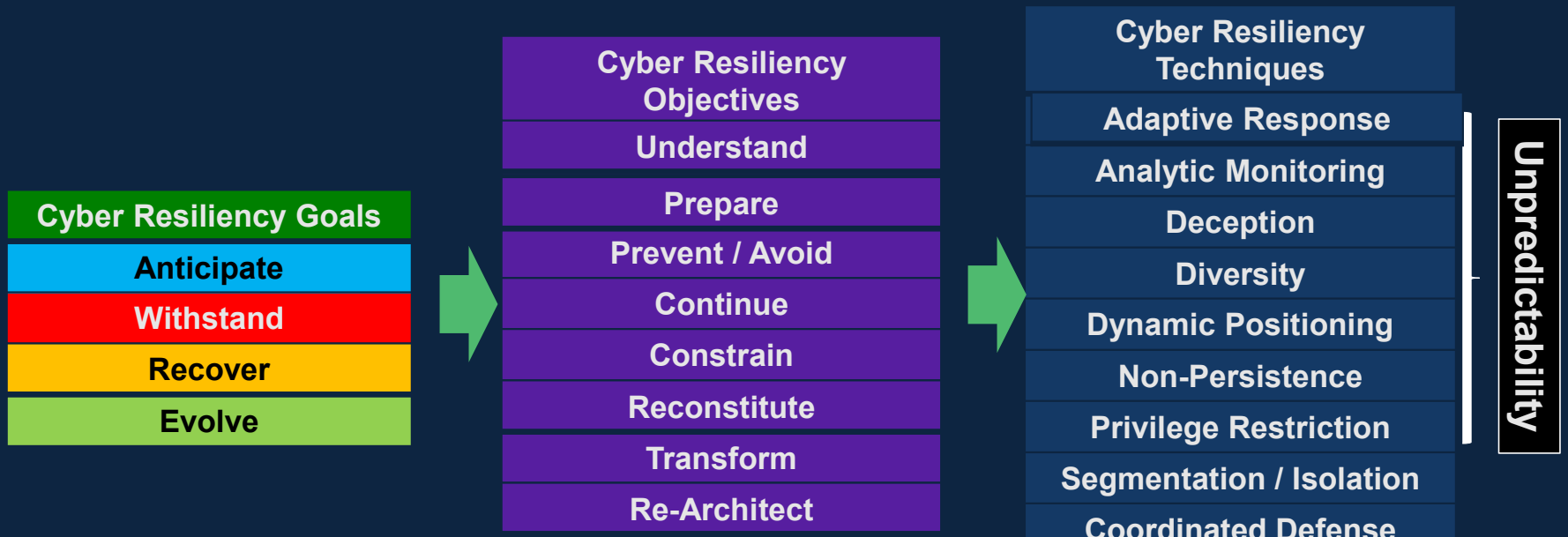
Cyber Resiliency

Apply minor tweaks to conventional cybersecurity and resilience (e.g., ensure backups are protected)

Non-adversarial threats use case analogies (e.g., safety and survivability) (e.g., use randomizing compilers, multiple OSs, employ virtualization to support non-persistent services to flush out malware)

Cyber Resiliency Engineering Framework (CREF):

A Structured Way to Understand the Domain



Objectives support goals.
Techniques support objectives.
Different stakeholders will be more concerned about different goals & objectives.
Techniques vary in maturity, applicability, and suitability
no system can (or should) apply them all.

Cyber Resilience Summary

Traditional Cybersecurity	Cyber Resiliency
Fragile approach	Designed to absorb attacks
Based on known attack patterns	Mission success focused
Slow to adjust to new attack patterns	Incorporates principles of safety, high availability, and agility
Typically added onto existing IT infrastructure	Designed in upfront. (like a bridge or building)

Cybersecurity
Disaster Recovery – Data Back-up

MITRE

Planning

Source: MITRE

Define your disaster

- Natural
  - Flood, wildfire, storm
- Facility
  - Fire
  - Physical damage
  - Theft
- IT
  - Ransomware
  - Hardware failure
  - Software failure

Planning

Answers to these questions drive the IT recover planning decisions

Source: MITRE

Authorities and Responsibilities

Recovery approach

- Relocate to back-up facility
- On-site spares
- Off-site spares
- Outsource/Insource

Acknowledge Risk Tolerance

- Minimum acceptable levels of operation
  - # systems, people, customer response times, payroll
- Maximum acceptable exposure
  - Time to restore to minimum operations
  - Customer loss potential

Planning

Source: MITRE

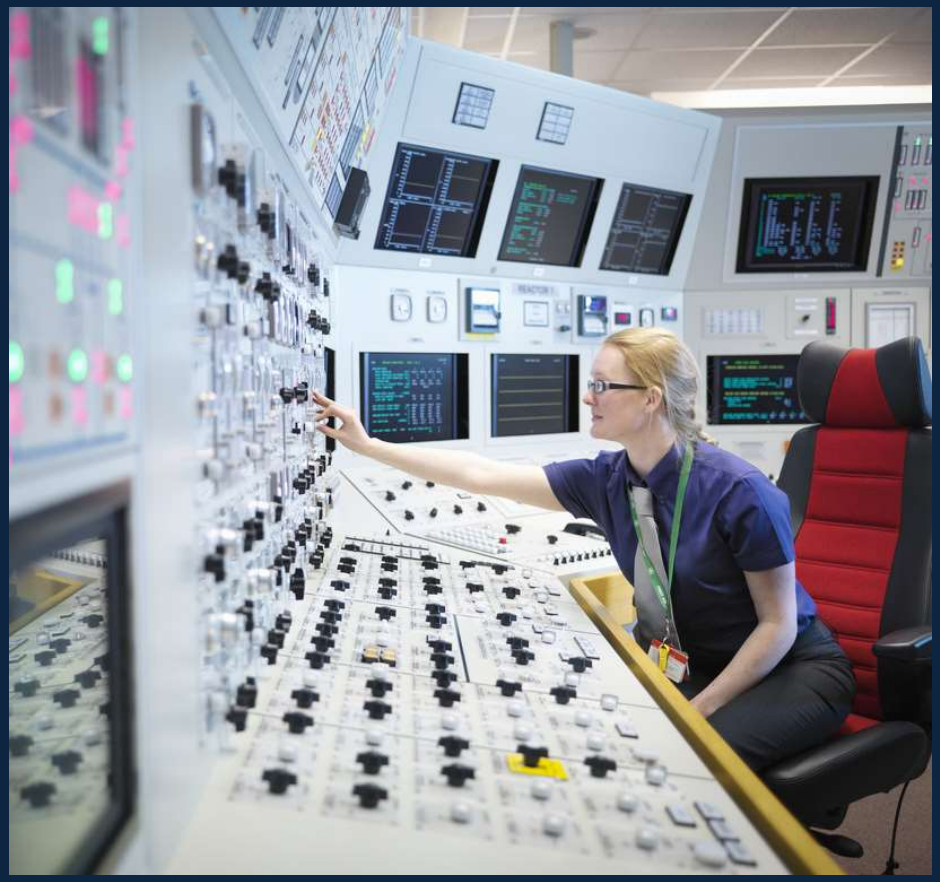
Know your data

- value (short and long term)
- regulations
- retention duration
- location
- volume

Restoral needs

- Cycle time to refresh back-ups
- Restoral time targets
- Geographic diversity
- Protection of backed-up data (encryption, offline) encryption key storage/safety

Implementation Considerations



- Automate as much as possible.
- Integrate back-up systems with operations (seamless)
- Offline back-ups
- Online back-ups
- Determine on-line and off-line back-up restoration procedures and test plans

Source: MITRE

Test and Monitor Considerations (rinse and repeat)

Source: MITRE

- **Are back-ups useable?**
- **Verify back-up integrity**
- **Verify processes and procedures**
- **Use lessons learned**
  - Time to restore (sufficient)
  - Time to test
  - Time to rebuild
  - Make adjustments
- **Check on back-up status regularly**

Conclusions

1. Cyber resilience is related Cybersecurity
2. Cyber resilience builds on cybersecurity
3. Cyber resilience ensures IT supports the mission even under attack/duress

1. Disaster recovery and back up success requires planning
2. Planning decisions are based on risk tolerance
3. Restoral approach decisions based on planning decisions
4. Testing and monitoring back-up files/system maximize the chance* they are safe and useful to restore operations

* Never plan for 100%

References

NIST – Protecting data from Ransomware
https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-extended.pdf

NIST - Secure Systems Engineering SP 800-160 Vol. 2
https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final

NIST – National Cybersecurity Center of Excellence
https://www.nccoe.nist.gov/

Questions?

Harry Perper

harry@mitre.org

Twitter: @hperper

Linkedin: linkedin.com/in/hperper