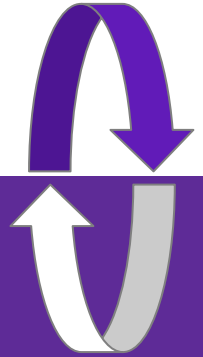
Brain Swap



Thinking Like A Modern Attacker

To Improve Your Defense

Justin Hall
Director, Security Consulting

cbts

Hey, I'm Justin.

Born & Raised in Cincy

Husband & Dad

Director of Security Consulting at CBTS

Agenda

The Problem: Too Many Threats, Too Many Controls

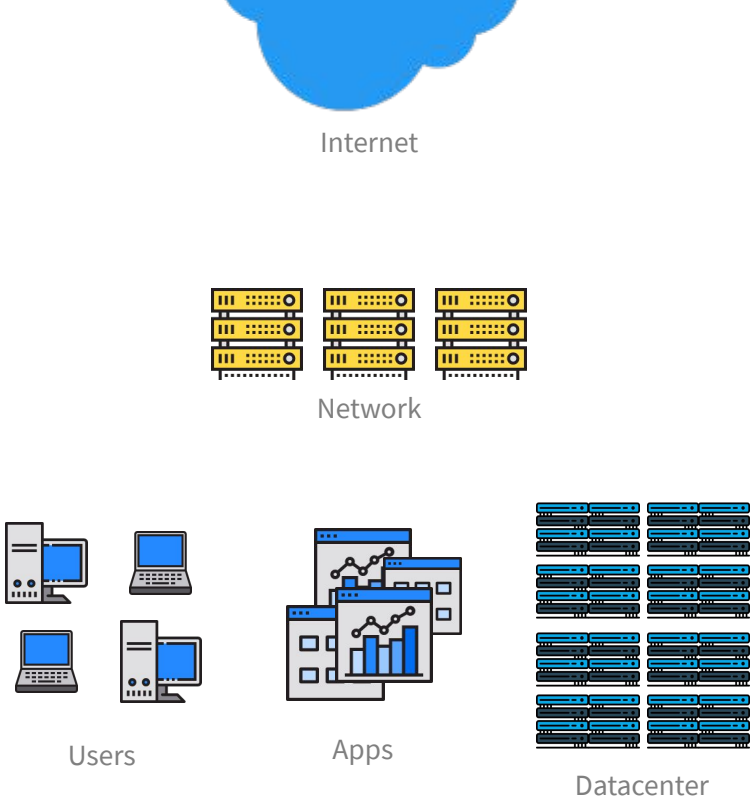
NIST 800-154 & Threat Modeling

Intel TAL

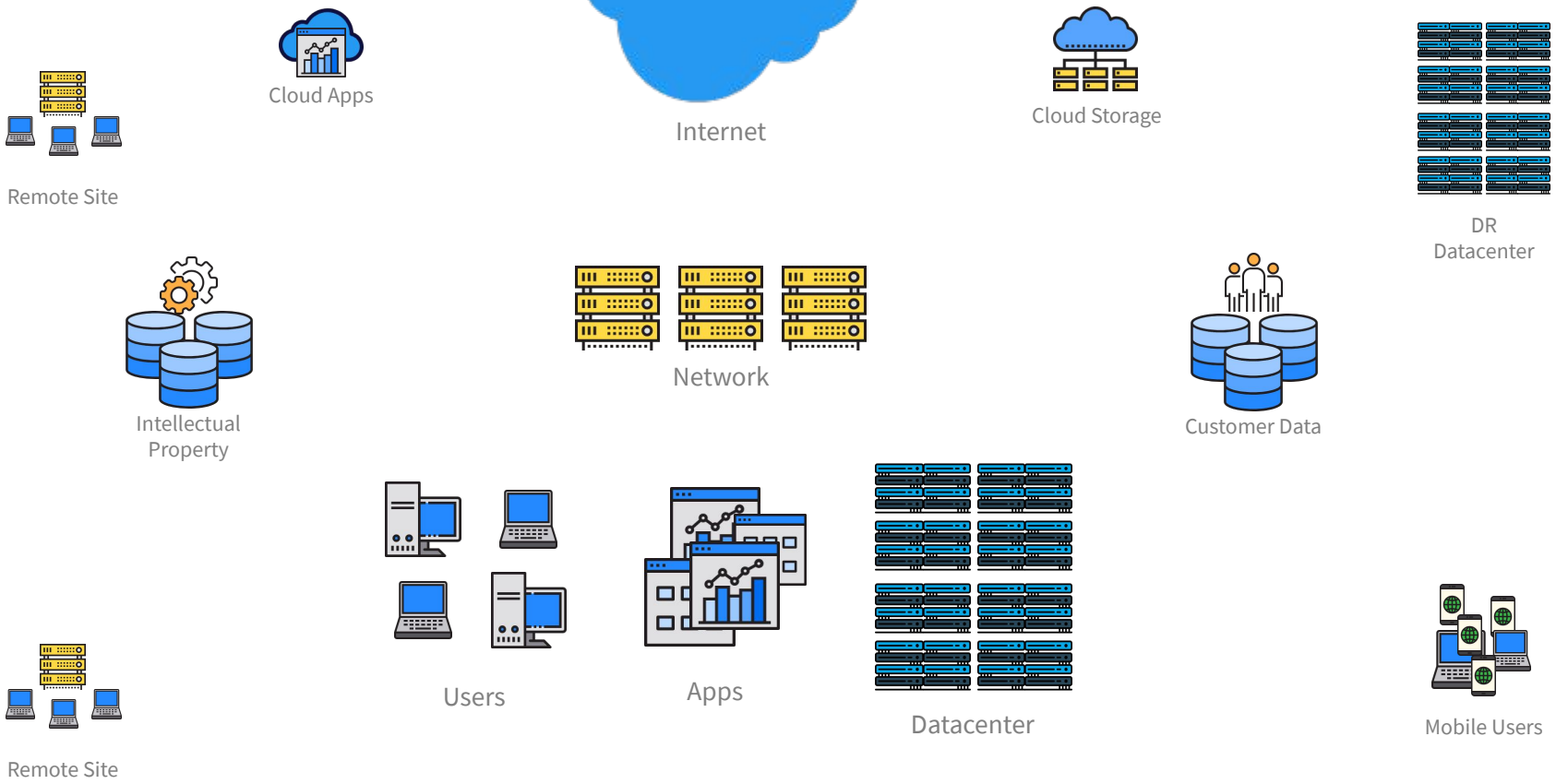
LM CKC/CAL

MITRE ATT&CK

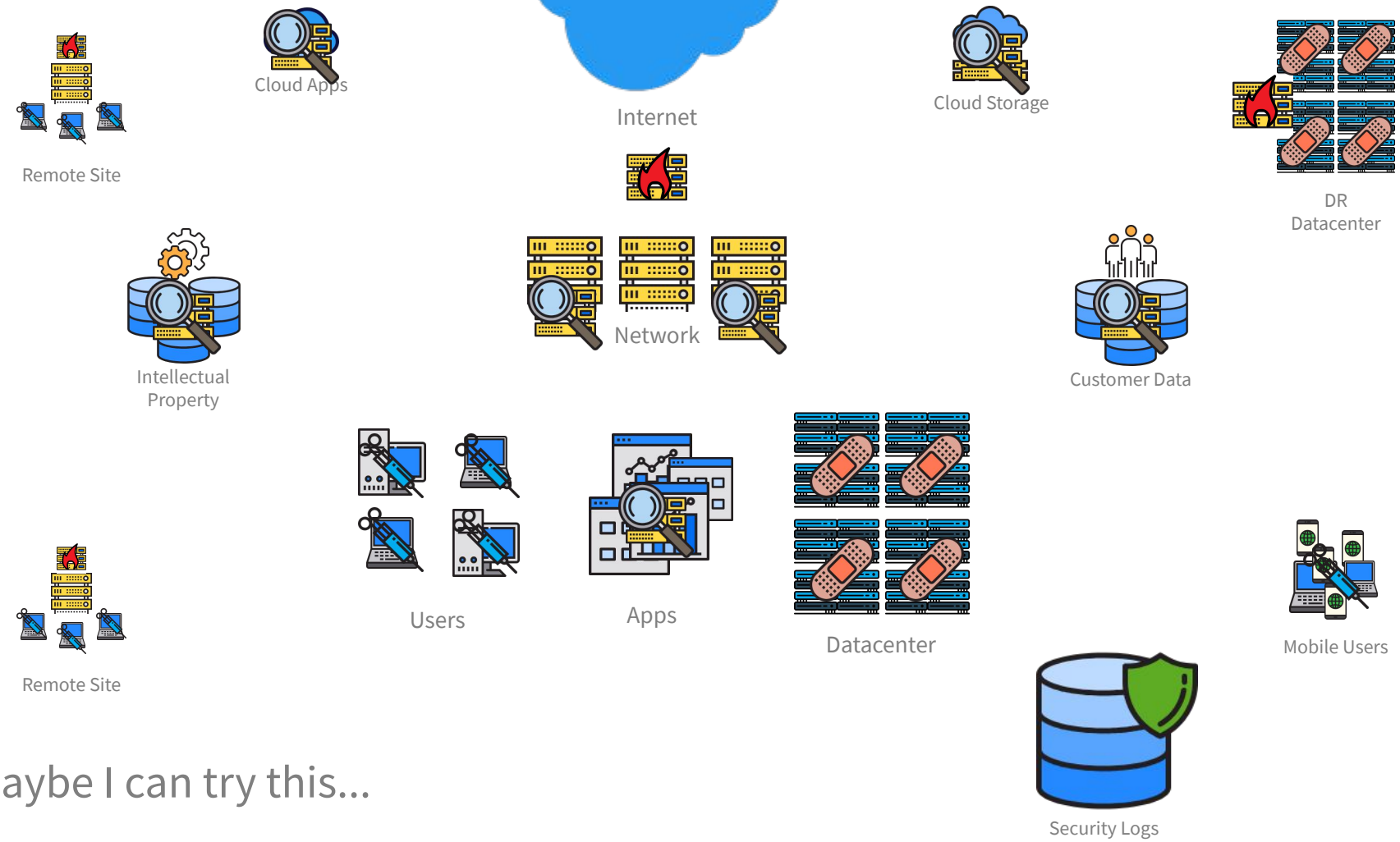
Q&A



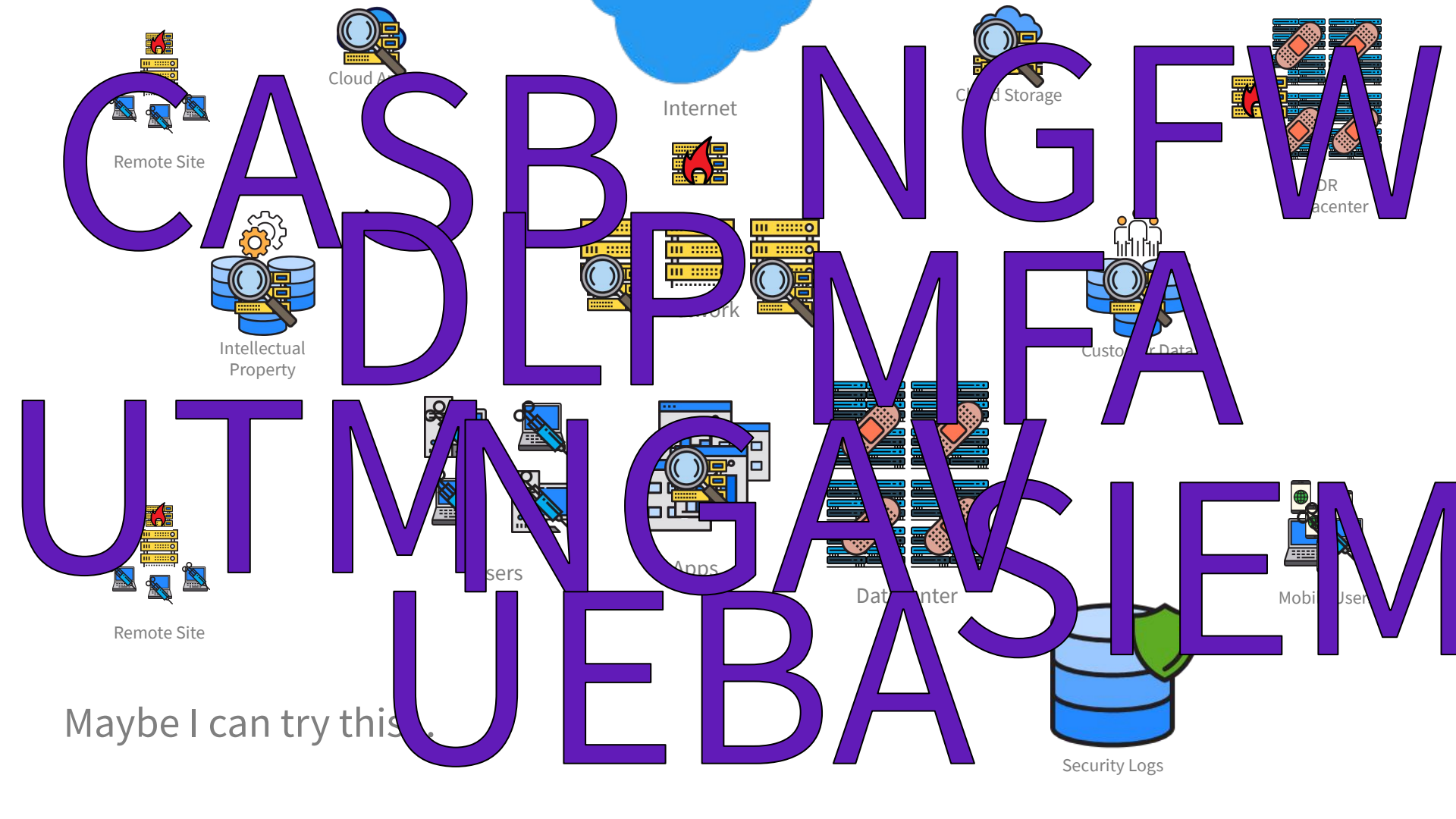
How do I secure this?



What about this?



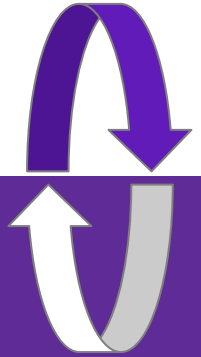
Maybe I can try this...



Maybe I can try this.

Yikes.

We can’t deploy every control.



We need a strategy.

> Threat modeling is a form of risk assessment that **models aspects of the attack and defense sides of a particular logical entity**, such as a piece of data, an application, a host, a system, or an environment.

NIST SP 800-154 Draft, Souppaya & Scarfone, Dec 2016

“Unless you're the NSA, attribution doesn't matter.”

Unnamed Security Leader

Source:
https://www.cnbc.com/2019/03/18/heres-how-cybersecurity-vendors-drive-the-hacking-news-cycle.html

“Unl[illegible]s you[illegible] the NS[illegible]on does[illegible]tter.”

U[illegible]ect[illegible]er

Source:
https://www.cnb[illegible]om/2019/03/18/here[illegible]w-cybersecurity-vendors-drive-the-hacking-news-cycle.html

Attribution matters:

Who’s got your data → **What** they will do with it

Who’s in your network → If they’re still there, how to **find them**, how to **stop them** from returning

Why do threat modeling?

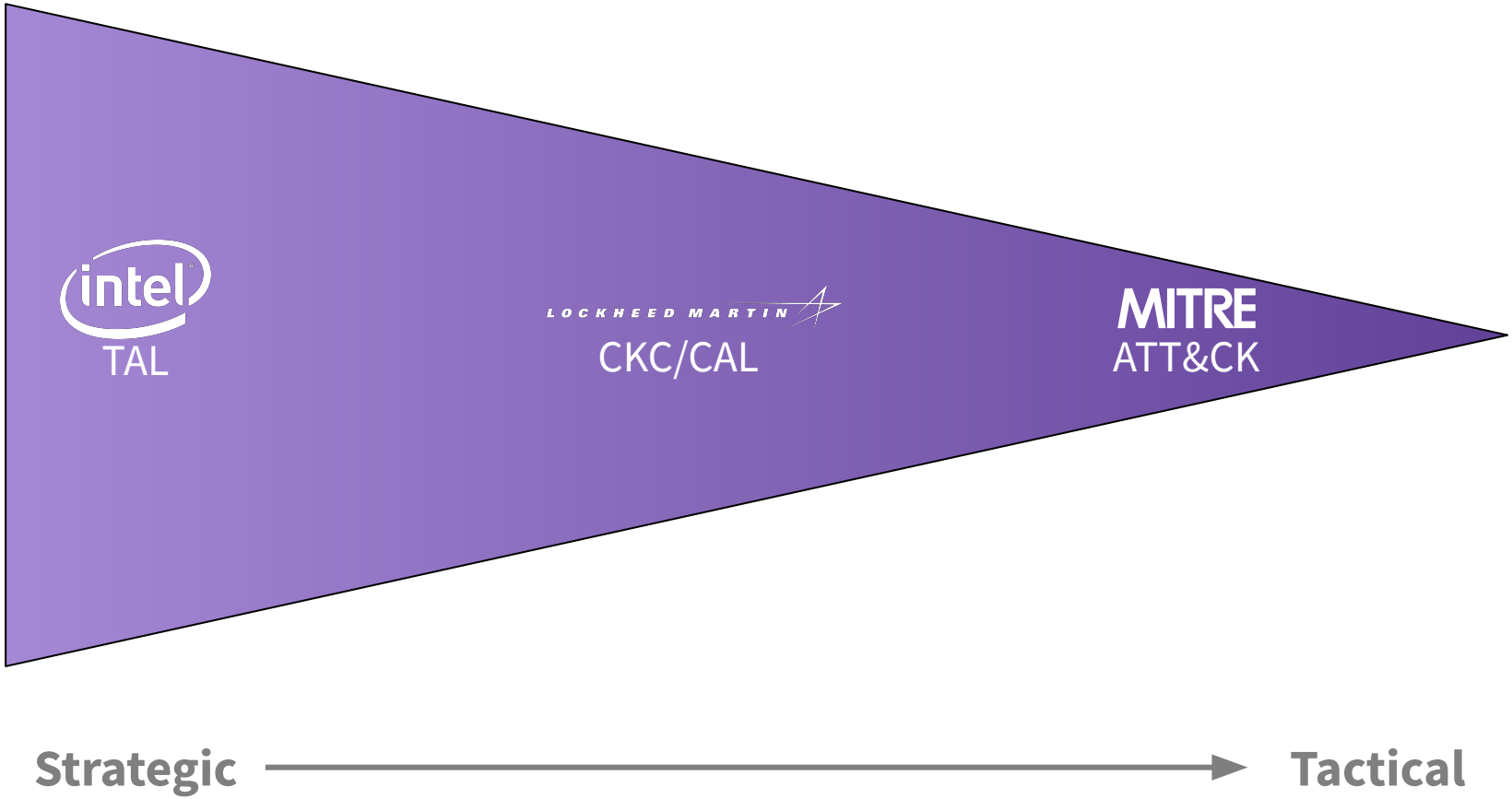
- Risk management efforts require a **clear understanding of the threats** we face and how they operate
- Rolling out, managing, and watching every security control is **costly, complex and noisy**
- Enumerating attacker behavior can help qualify threats when **educating users**

800-154's Threat Modeling At A High Level

1. Identify and characterize **the system and data of interest**;
2. Identify and select **the attack vectors to be included** in the model;
3. **Characterize the security controls** for mitigating the attack vectors; and
4. Analyze the **threat model**.

800-154's Threat Modeling At A High Level

1. Identify and characterize **the system and data of interest**;
2. Identify and select **the attack vectors to be included** in the model;
3. **Characterize the security controls** for mitigating the attack vectors; and
4. Analyze the **threat model**.


intel
TAL
LOCKHEED MARTIN
CKC/CAL
MITRE
ATT&CK
Strategic
Tactical

Which threats should concern me?

Intel Threat Agent Library (TAL)

"A single standardized set of **archetypal agent definitions** ranging from government spies to untrained employees"

"**Eight common agent attributes**… and **22 agents** based on unique combinations of these attributes"

- Hostile or not?
- Access method
  - Internal or External?
- Desired outcome
  - E.g. Theft, Embarrassment, Competitive Advantage
- Legal & Ethical Limits
  - Inside or outside the law?
- Resources
  - Individual -> Community -> Organization
- Skills
  - Skids or APT?
- Objectives
  - Actions that achieve outcome
- Visibility
  - Overt, covert, clandestine

"Threat Agent Library Helps Identify Information Security Risks", Intel Corp, 2007

	Intent	NON-HOSTILE			HOSTILE																	
		Employee Reckless	Employee Untrained	Info Partner	Anarchist	Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyberwarrior	Government Spy	Internal Spy	Irrational Individual	Legal Adversary	Mobster	Radical Activist	Sensationalist	Terrorist	Thief	Vandal	Vendor
Access (1)	Internal	■	■	■						■		■	■							■		■
	External				■	■	■	■	■		■			■	■	■	■	■	■		■	
Outcome (1-2)	Acquisition/Theft												■			■				■		
	Business Advantage						■	■	■			■			■							■
	Damage	■	■	■	■					■	■			■			■	■	■		■	
	Embarrassment	■	■	■		■				■	■			■	■		■	■				
	Tech Advantage						■	■	■			■	■									■
Limits (max)	Code of Conduct		■	■																		
	Legal	■													■							■
	Extra-legal, minor					■	■	■	■				■				■	■		■	■	
	Extra-legal, major				■					■	■	■		■		■			■			
Resources (max)	Individual	■	■	■						■				■						■		
	Club				■													■				
	Contest																				■	
	Team								■													■
	Organization					■	■						■		■	■	■		■			
	Government							■			■	■										
Skills (max)	None				■									■						■		
	Minimal		■															■				
	Operational			■						■											■	■
	Adept	■				■	■	■	■		■	■	■		■	■	■		■			
Objective (1 or more)	Copy					■	■		■			■	■		■							■
	Deny							■			■											
	Destroy				■					■	■								■			
	Damage									■	■								■			
	Take														■	■			■	■		
	All of the Above/ Don't Care	■	■	■										■			■	■			■	
Visibility (min)	Overt		■		■			■							■		■	■				
	Covert	■				■										■			■		■	
	Clandestine			■			■		■			■	■							■		■
	Multiple/Don't Care									■	■			■								

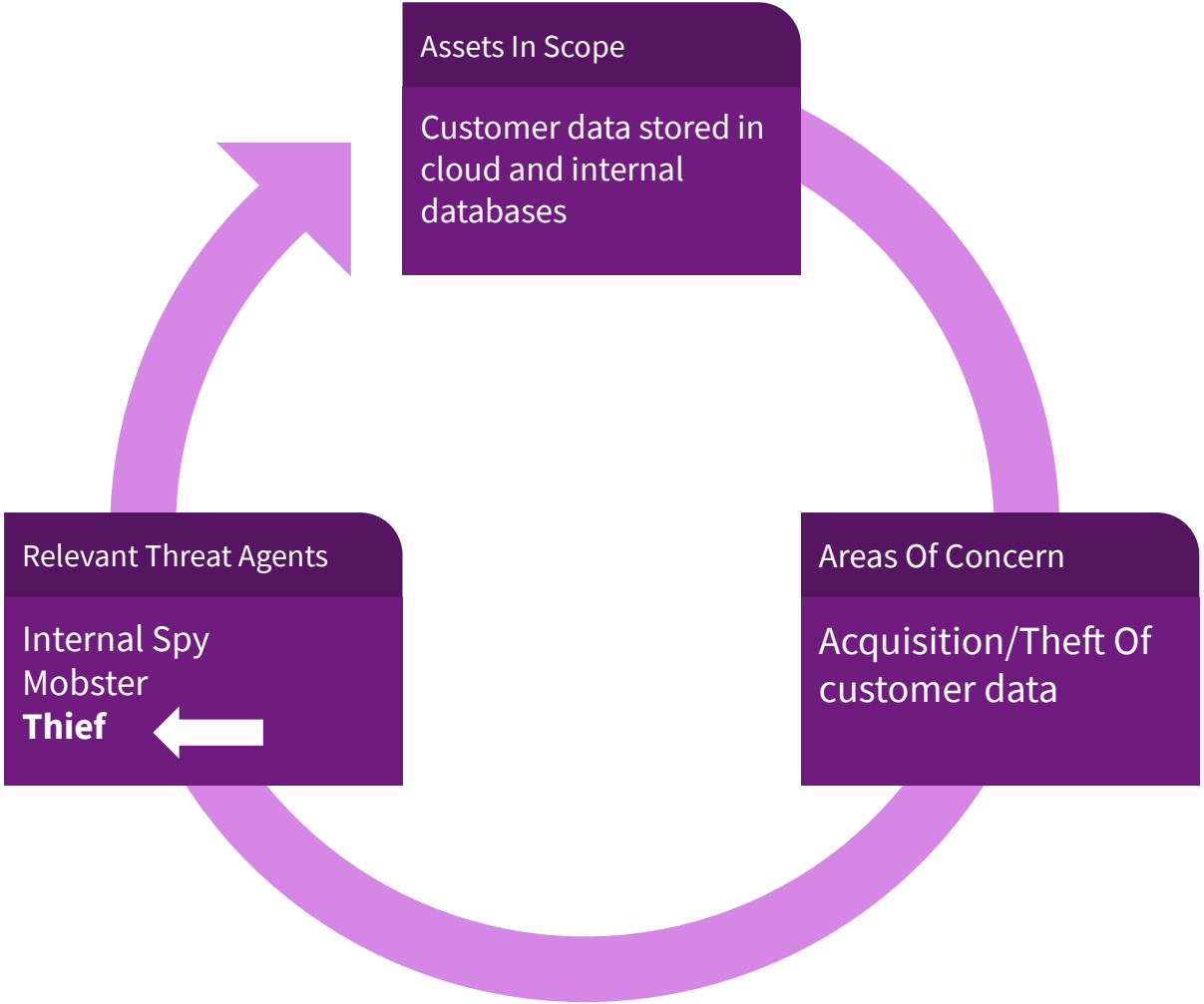
Source: Intel IT Threat Assessment Group, 2007

TAL's Library of Threat Agents & Characteristics

"Threat Agent Library Helps Identify Information Security Risks", Intel Corp, 2007

Practical Use Of The TAL

1. Consider **assets in scope**
2. Identify **areas of concern**
3. Map to **threat agents**



What is their strategy?

LOCKHEED MARTIN

Cyber Kill Chain®

Lockheed Martin Cyber Kill Chain®

A “Kill Chain” is:

“...a systematic process to target and engage an adversary to create desired effects.”

Translated to the “Cyber Kill Chain”:

“... the aggressor must **develop a payload** to breach a trusted boundary, **establish a presence inside** a trusted environment, and from that presence, **take actions towards their objectives**, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment.”

“Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, Hutchens et al, 2011

The 7 Phases of the CKC/CAL

Reconnaissance	Weaponization	Delivery	Exploit	Install	C2	Actions On Objectives
Research, identification and selection of targets	Coupling a remote access trojan with an exploit into a deliverable payload	Transmission of the weapon to the targeted environment	After the weapon is delivered to victim host, exploitation triggers intruders' code.	Installation of a remote access trojan or backdoor on the victim system	Compromised hosts beacon outbound to an Internet controller server to establish a command and control (C2) channel	Intruders take actions to achieve their original objectives.

"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Hutchens et al, 2011

When Is The CKC/CAL Model Appropriate?

The attacker must:

- Breach a “trusted” boundary
- Establish an internal presence
- Use that presence to take actions on their objectives

Phishing & Social Engineering
Man-In-The-Middle
External Web App Exploitation
Drive By & Watering Hole

Remote Access Trojans
Autoruns, Services, Stages

Lateral Movement
Data Theft/Exfiltration
Data Destruction/Encryption

What are their tactics?

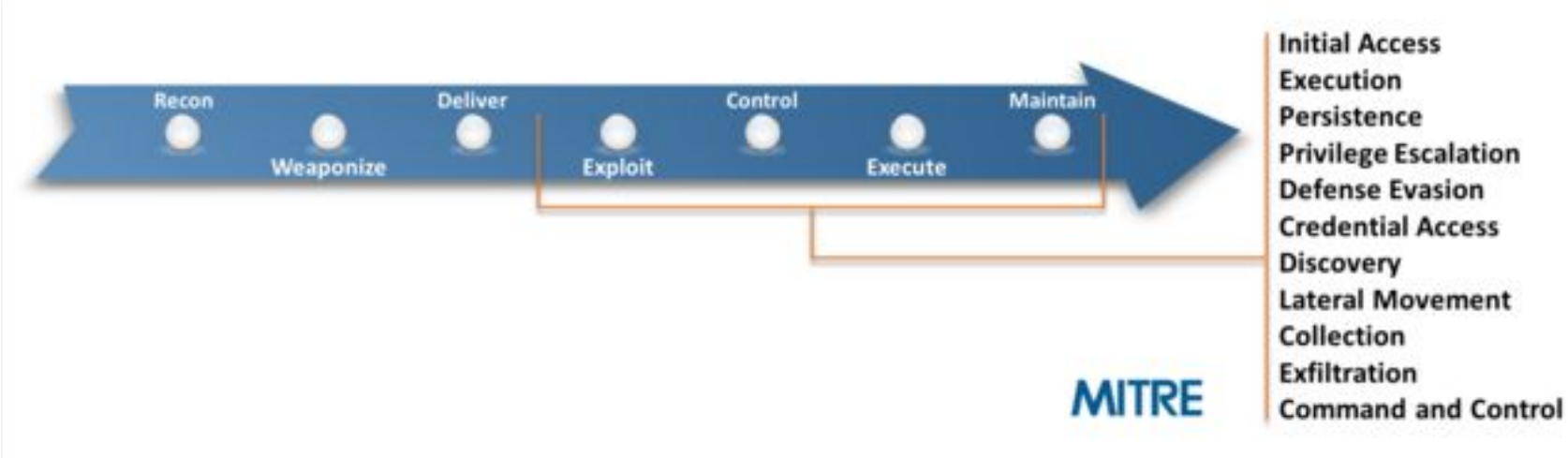
MITRE

ATT&CK Framework™

MITRE ATT&CK Framework™

Adversarial Tactics, Techniques & Common Knowledge

"...a **curated knowledge base** and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target."



"Adversarial Tactics, Techniques & Common Knowledge", MITRE Corp, 2018

ATT&CK: Tactics → Techniques

Tactics describe **a specific goal or objective** of the attacker.

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion

Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

“Adversarial Tactics, Techniques & Common Knowledge”, MITRE Corp, 2018

ATT&CK: Tactics → Techniques

Techniques describe the **observable technical activity** performed to achieve the goal.

Initia
Execu
Persi
Privil
Defe

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- **Exfiltration Over Alternative Protocol**
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

"Adversarial Tactics, Techniques & Common Knowledge", MITRE Corp, 2018

Technique Example: Exfiltration

Exfiltration Over Alternative Protocol

Data exfiltration is performed with a different protocol from the main command and control protocol or channel. The data is likely to be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, or some other network protocol. Different channels could include Internet Web services such as cloud storage.

Contents [hide]

Exfiltration Over Alternative Protocol	
Technique	
ID	T1048
Tactic	Exfiltration
Platform	Linux, macOS, Windows
Data Sources	User interface, Process monitoring, Process use of network, Packet capture, Netflow/Enclave netflow, Network protocol analysis
Requires Network	Yes

Examples

- FIN8 has used FTP to exfiltrate collected data.[1]
- Lazarus Group malware SierraBravo-Two generates an email message via SMTP containing information about newly infected victims.[2]
- OilRig has exfiltrated data over FTP separately from its primary C2 channel over DNS.[3]
- can be used to create BITS Jobs to upload files from a compromised host.[4]
- Cherry Picker exfiltrates files over FTP.[5]
- CosmicDuke exfiltrates collected files over FTP or WebDAV. Exfiltration servers can be separately configured from C2 servers.[6]

Threat Modeling Process Example

We are concerned about **customer data being stolen**

Risk

3 Threat Agents whose desired outcomes are **theft**

Threat

Threat Agent Strategy matches **CAL**

Strategy

Threat Agent Tactic includes **Exfiltration**

Tactic

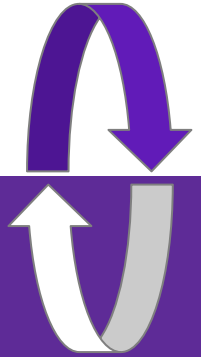
Technique: Exfil over Alternative Protocol

Technique

Resources

http://bit.ly/ThreatModeling

Thanks for listening!



Questions?

Justin Hall @justinhall justin.hall@cbts.com