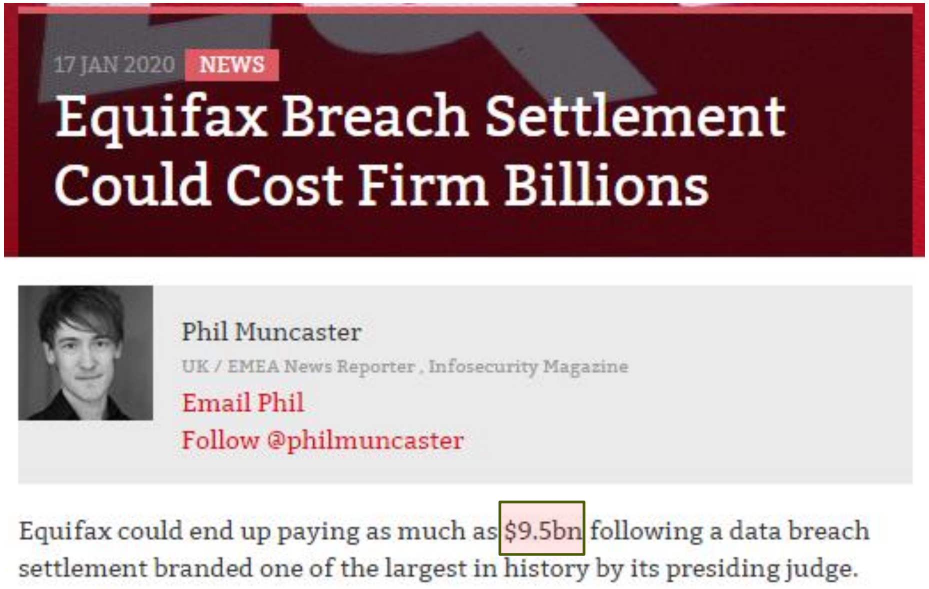
Attack Frameworks

Portland State
Computer Science

Motivation

- Equifax breach (2017)
  - Vulnerability in Java web app leads to 145 million compromised accounts
    - Social Security numbers
    - Birth dates
    - Addresses
    - Driver's license numbers
  - But, not interested in that….



17 JAN 2020 NEWS

Equifax Breach Settlement Could Cost Firm Billions

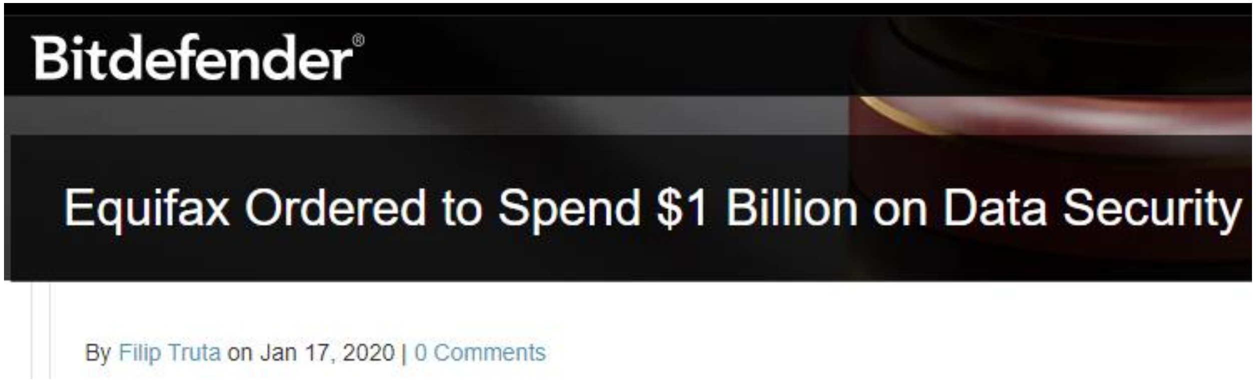
Phil Muncaster

UK / EMEA News Reporter , Infosecurity Magazine

Email Phil

Follow @philmuncaster

Equifax could end up paying as much as $9.5bn following a data breach settlement branded one of the largest in history by its presiding judge.



Bitdefender®

Equifax Ordered to Spend $1 Billion on Data Security

By Filip Truta on Jan 17, 2020 | 0 Comments

Equifax's $1bn problem

- How would we spend their money?
  - Patching?
  - Penetration testing?
  - Phishing training?
  - Data exfiltration detection?
  - Deception?
  - 2FA?
  - Re-write everything in Rust?
  - On you?

Microsoft Patch Tuesday

INSOMNIA SECURITY SPECIALISTS :: REST SECURED

IMMUNITY

INNUENDO

THINKST CANARY

DUO

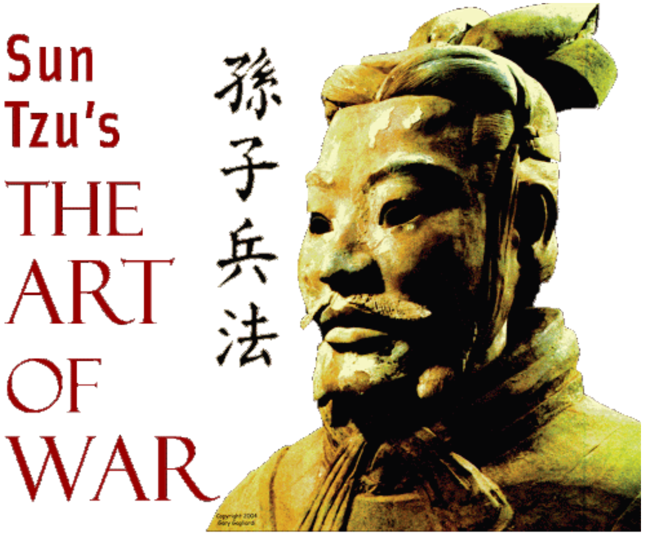
yubico

But…

- How would we know it would work against our adversaries?
- How do we identify what to protect and how to protect it?

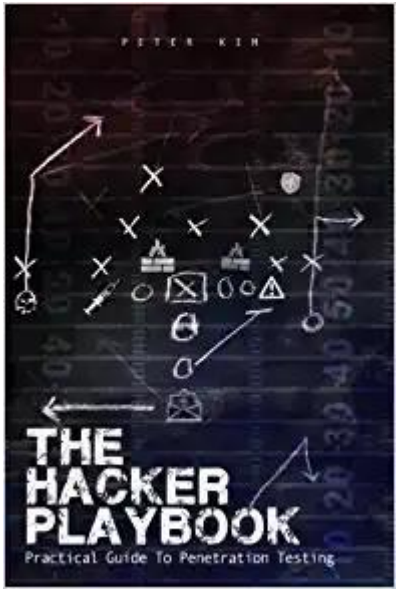
Answers come from the enemy

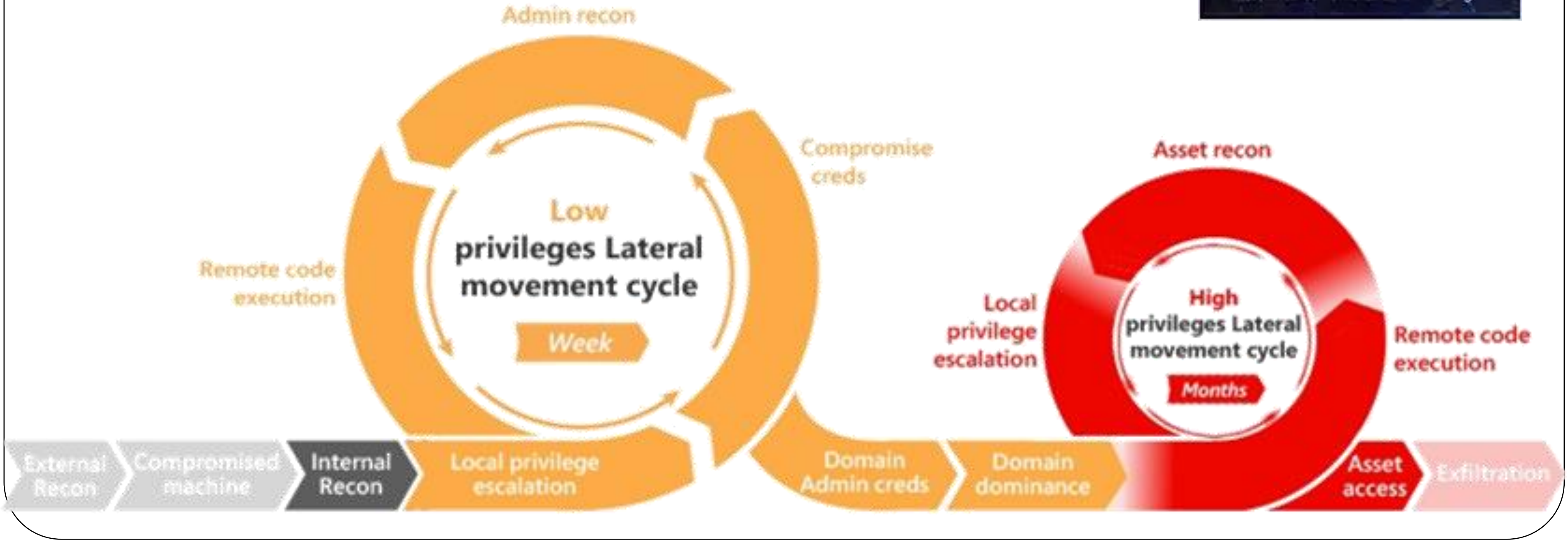
“If you **know** the **enemy** and **know** yourself, you need not fear the result of a hundred battles…If you **know** neither the **enemy** nor yourself, you will succumb in every battle.”



Cyber Kill Chain (2011)

- Lockheed Martin paper
  - Cyber equivalent to military kill chains
  - Model for describing steps attacker must take to carry out a successful attack
  - To disrupt attack, one or more steps must be broken
  - Every hacking group has a playbook to follow based on its capabilities
    - Attack the attacker's playbook!





Admin recon

Compromise creds

Remote code execution

Low privileges Lateral movement cycle

Week

Asset recon

Local privilege escalation

High privileges Lateral movement cycle

Months

Remote code execution

External Recon

Compromised machine

Internal Recon

Local privilege escalation

Domain Admin creds

Domain dominance

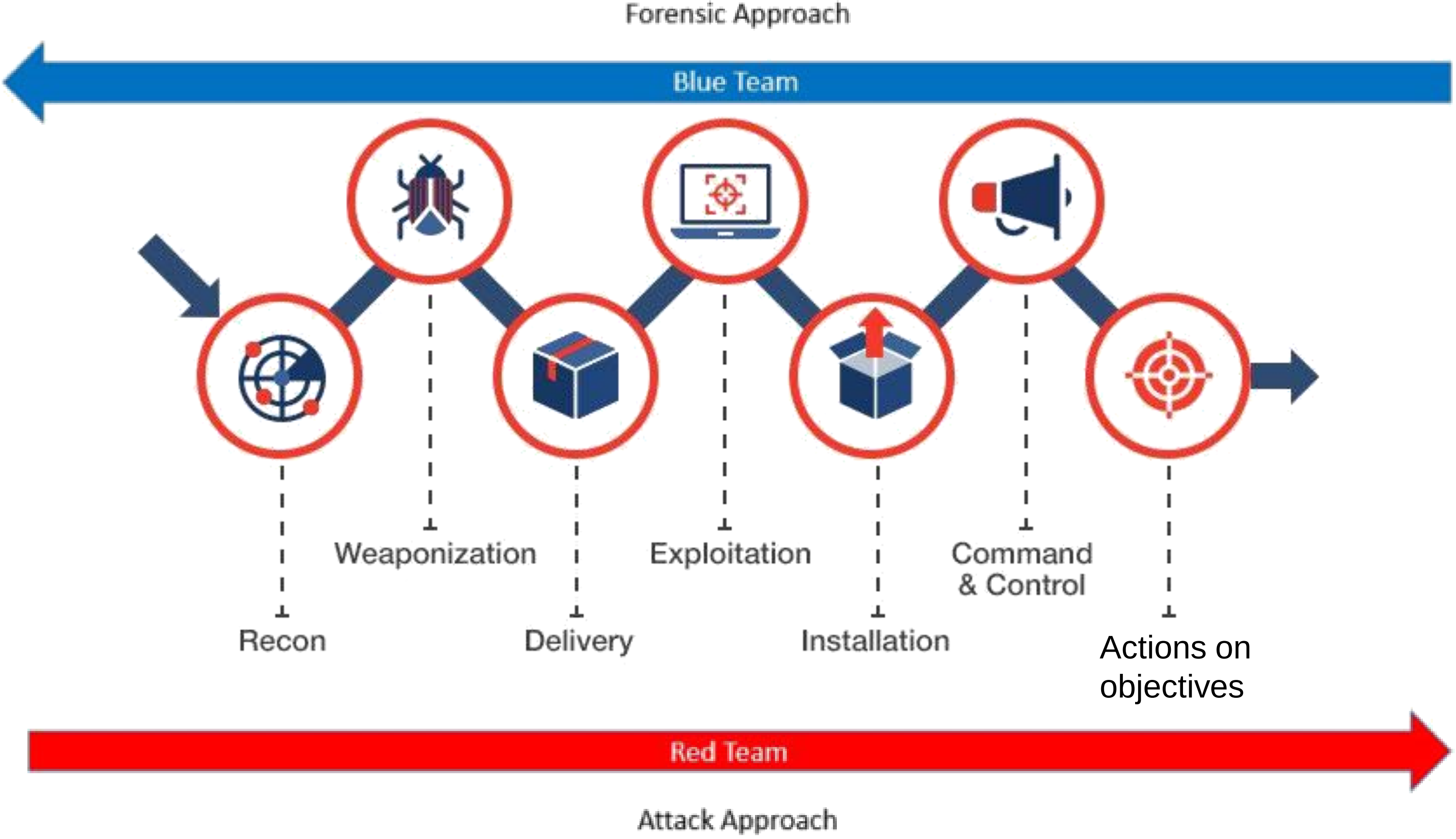
Asset access

Exfiltration

Alternate chain

AWS CloudGoat
ec2_ssrf post-mortem

Portland State
Computer Science



Actions on objectives

MITRE ATT&CK framework

Overview

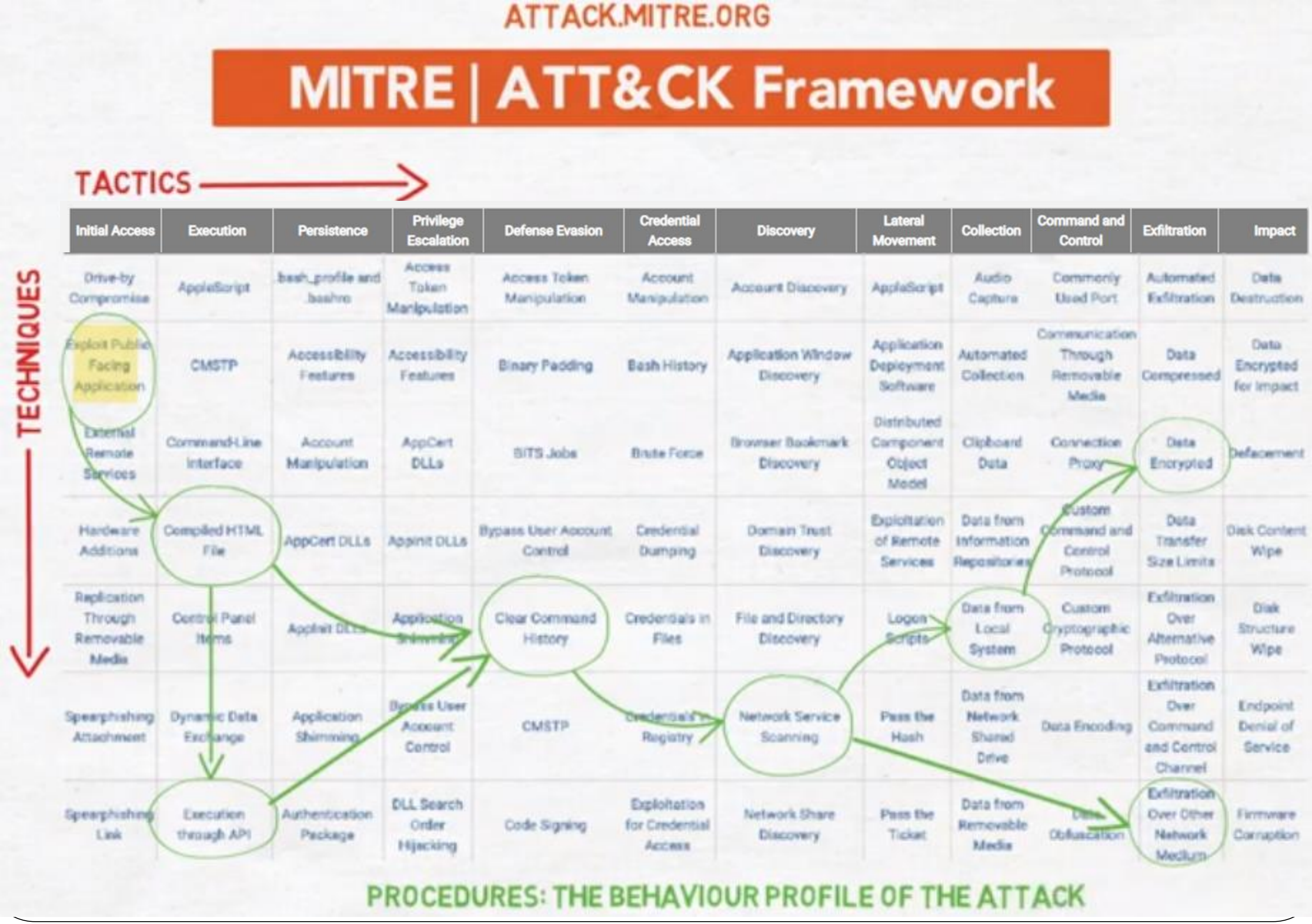
- Common body of knowledge of known attacker behavior
  - A living framework!

- Tactics, techniques, and procedures of adversaries (TTPs)
  - Derived from incident response and threat intelligence communities
  - What are attackers actually using?
  - Expands the last parts of the Cyber Kill Chain

- Tactics
  - Overall behavior
- Techniques
  - Specific approaches to perform tactic
- Procedures
  - Playbook of tactics and techniques used by adversaries to accomplish objective

- Best shown in a matrix…

- Via the CSO Perspective



ATTACK.MITRE.ORG

MITRE | ATT&CK Framework

TACTICS
TECHNIQUES

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption

PROCEDURES: THE BEHAVIOUR PROFILE OF THE ATTACK

12 tactics

- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- Command & Control
- Exfiltration
- Impact

1. Initial access

- Attacker gains foothold in environment (starting point)
- Examples
  - Vulnerable public-facing web application, valid account compromise
  - Spear phishing attachment that executes when clicked
- Detection
  - Web access and log-in analytics
  - Scanning attachments
- Mitigations
  - Patching
  - Browser protections against phishing/malware sites
  - Multi-factor authentication

2. Execution

- Attacker-controlled code run within environment
- Examples
  - Shells (command injection, buffer overflow)
  - Victim executes payloads directly
- Detection
  - Process monitoring, sandbox execution
- Mitigations
  - Whitelisted software execution
  - Data-execution prevention (DEP/NX)
  - Chroot jails and containers

3. Persistence

- Action or change to a compromised system to maintain access
- Examples
  - Registry run keys, start-up folders (e.g. `/etc/init.d`), binary and library replacement, malicious browser extensions
- Detection
  - File and registry integrity tools
- Mitigations
  - Executing at least privileges
  - Code signing enforcement

4. Privilege escalation

- Obtaining elevated or administrator access on a machine, network, or domain
- Examples
  - Cloud projects with misconfigured IAM policies or exposed keys
  - Vulnerable `setuid` programs, library hijacking
- Detection
  - Audit logs to detect anomalous behavior (CloudTrail, Stackdriver, SIEMs, Blackberry/Cylance)
  - `sudo` logs
- Mitigations
  - Application and machine whitelisting
  - Hardening endpoints (Linux seccomp)
  - Isolation (containers)

5. Defense evasion

- Avoiding detection and other deployed counter-measures
- Examples
  - Polymorphism/obfuscation to bypass signatures
  - Giving AV the halting problem (e.g. 600 second delay bypass)
  - Rootkit techniques for compromising kernel
  - Disabling security controls (code-signing, anti-virus, software updates)
  - DNS/web mimicry of traffic
  - Tampering with log files
- Detection/Mitigations
  - Monitoring defenses to ensure they're running (not Equifax 2017)
  - Monitoring endpoint changes
  - Sending audit logs to a centralized location (e.g. append-only logs)

6. Credential access

- Gaining control over authentication information for a user, system, domain, or service.
- Examples
  - Exposed API/account keys and passwords/hashes
  - Credential spraying/stuffing, credential dumping, stolen session cookies
  - Keyboard loggers
- Detection
  - Auditing access to perform analytics like credit cards (location, concurrence)
  - Canary tokens
- Mitigations
  - Rate-limiting authentication attempts (!Instagram 2FA)
  - 2FA, Password managers, strong password policies
  - Strong password hashing
  - Elimination of credential sharing (e.g. shared admin account)
  - Key rotation

7. Discovery

- Gaining knowledge about target environment such as its software, its networks, its users, and its processes for future targeting
- Examples
  - Accounts, files, directories, processes, security software, system information, etc.
  - Passive network sniffing, active network scanning
  - Examining service quotas on vulnerable cloud projects ☺
- Detection
  - Monitoring histories (e.g. .bash_history, files in "Recent" directory)
  - Network traffic analysis, honeypots
- Mitigations
  - Canaries and honey tokens
  - Traffic filtering, network segmentation

8. Lateral movement

- Pivoting over the network from one compromised system to another to obtain additional footholds
- Examples
  - Exploit remote services (e.g. domain controller, admin machine, or database server)
  - Shared drives
  - `ssh` hijacking (forwarding)
- Detection
  - Traffic analytics
  - Auditing for behavioral anomalies
- Mitigations
  - Tarpits, honeypots
  - Network segmentation

9. Collection

- Gathering sensitive data from target environment prior to exfiltration
- Examples
  - Credit-card information
  - Screen grabs
  - Web cam captures (Dutch outing of FancyBear)
  - Shared drives
- Detection
  - Detailed inventory of sensitive data coupled with logging of all access (the 'new' perimeter)
- Mitigations
  - Least privilege to protect sensitive data
  - Encryption of information at rest and in transit

10. Command and Control (C&C or C2)

- Communication to an attacker-controlled remote location in order to obtain additional instructions from or delivering compromised data to.
- Examples
  - Set of addresses or URLs to connect to
  - Connections to anonymizing networks, connections on high network ports to C&C servers
- Detection
  - Proxies on incoming and outgoing connections (e.g. scan both directions of HTTP and HTTPS)
  - Connection logging in SIEMs (ELK, Splunk, cloud audit logs)
- Mitigations
  - Network segmentation
    - e.g. PoS machines configured to only communicate with specific destinations

11. Exfiltration

- Transferring sensitive information out of target environment
- Examples
  - Disk snapshots
  - Web, DNS exfiltration
  - USB drives (insider threat)
- Detection
  - Data loss prevention (DLP) tools
  - Device usage history
- Mitigations
  - Encryption at rest
  - Least-privilege access control
  - Eliminating USB access

12. Impact

- Manipulate, interrupt, or destroy systems or data to compromise a target's integrity and availability
  - CIA properties
    - Exfiltration => confidentiality
    - Impact => integrity and availability
- Examples
  - Backdoor insertion
  - Ransomware
- Detection
  - Integrity checks
  - Backups

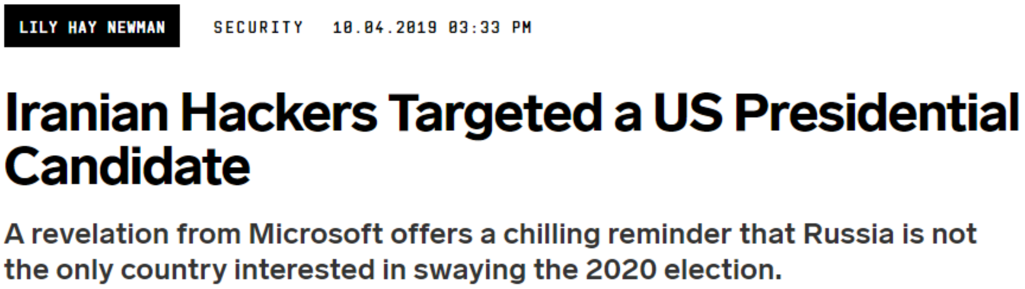
Tactics drive defense

- Threat informed defensive strategy to guide investment into controls
- Threat modeling: 2 approaches
  - Start at Impact to fix the threat you've prioritized to prevent
    - Work backwards to make sure controls applied stop all procedures that lead to it
  - Start with TTPs of attackers
    - Work towards removing plays out of their playbook

- A good way for Equifax to prioritize its $1B spend?

Demo of use

- Say you want to protect our upcoming election from methods of attack used in 2016…
  - APT 28 (Cozy Bear)
    - Backed by Russian Foreign Intelligence Service (e.g. CIA)
    - Pentagon (2015), DNC (2016), Petya/NotPetya (2017)
  - APT 29 (Fancy Bear)
    - Backed by Russian Military Intelligence (e.g. DoD/NSA)
    - Also DNC (2016), French elections (2017), US Conservative groups (2018)
- And also from other rogue states
  - APT 38 (Lazarus Group)
    - Links to N. Korea
    - WannaCry (2017)
  - APT 35 (C. Kittens)
    - Iran



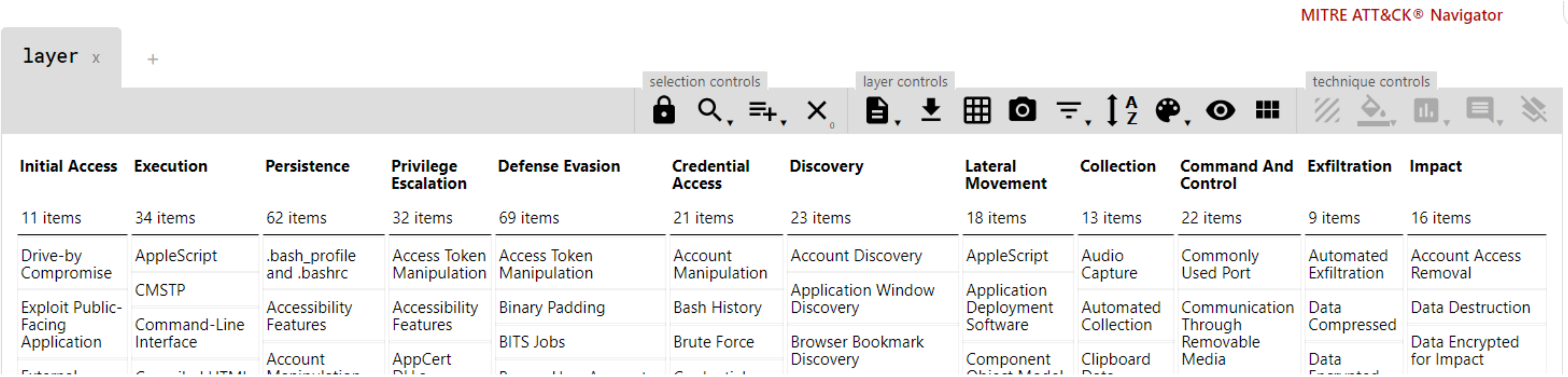
LILY HAY NEWMAN SECURITY 10.04.2019 03:33 PM

Iranian Hackers Targeted a US Presidential Candidate

A revelation from Microsoft offers a chilling reminder that Russia is not the only country interested in swaying the 2020 election.

Demo

- https://mitre-attack.github.io/attack-navigator/enterprise
  - APT 28, 29, CopyKittens, Lazarus Group



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
	Command-Line Interface	Account	AppCert	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component	Clipboard		Data	Data Encrypted for Impact

- Idea for your presentations
  - Cover all of the techniques used by particularly prolific APTs
  - FIN7?

Now what?

- Have the TTPs prioritized

- Must deploy controls to
  - Detect
  - Deny
  - Disrupt
  - Degrade
  - Deceive

- Center for Internet Security (CIS) controls enumeration

20 CIS controls to detect and mitigate

Basic controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
6. Maintenance, Monitoring, and Analysis of Audit Logs

Foundational controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Lots of controls out there, but not all implementations are created equally!

How to choose?

Based on the Pyramid of pain

- How easy is it to bypass control?

Preventing entire TTP (entry in matrix)

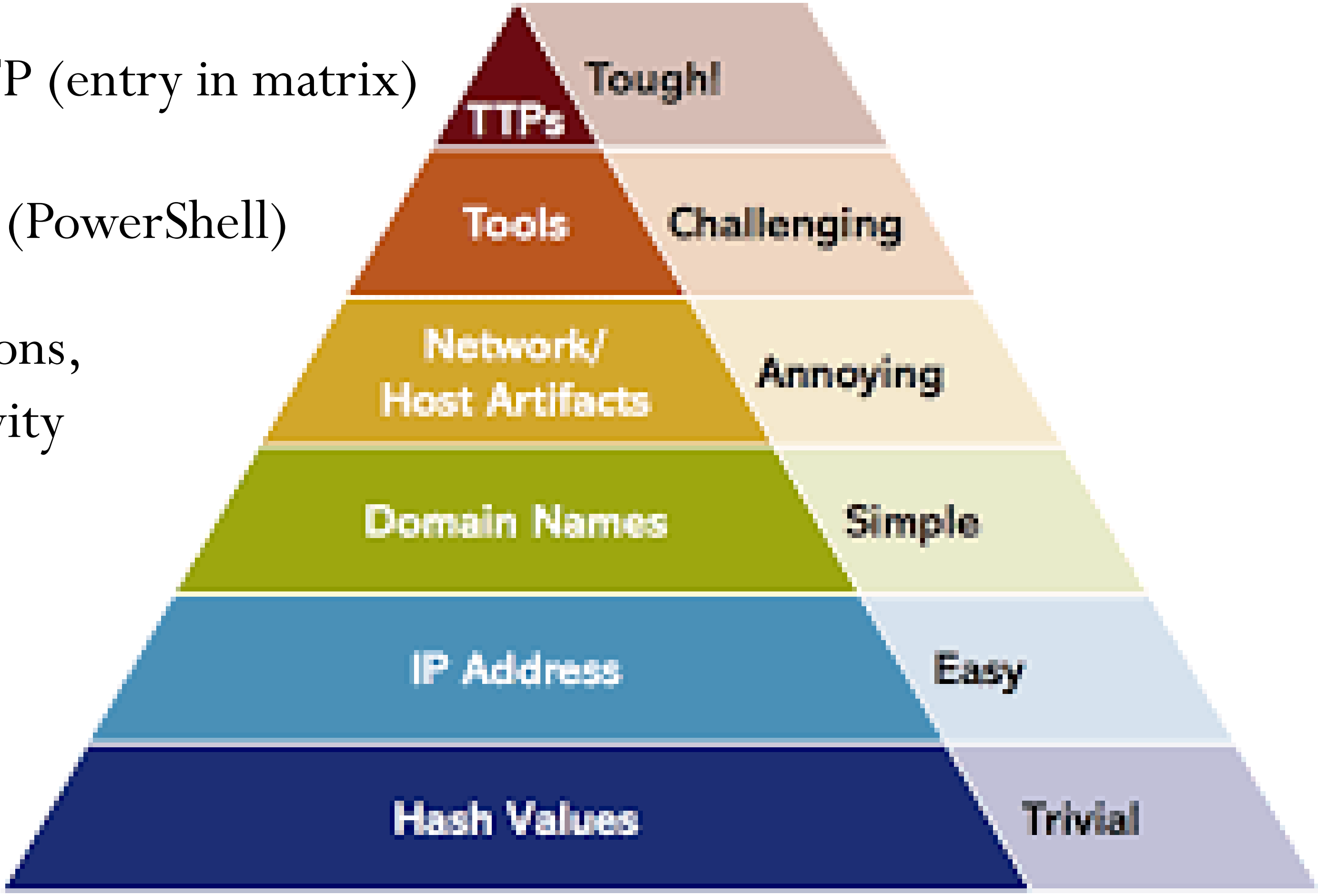
Restricting software (PowerShell)

Restricting connections,
file and registry activity

DNS blocking

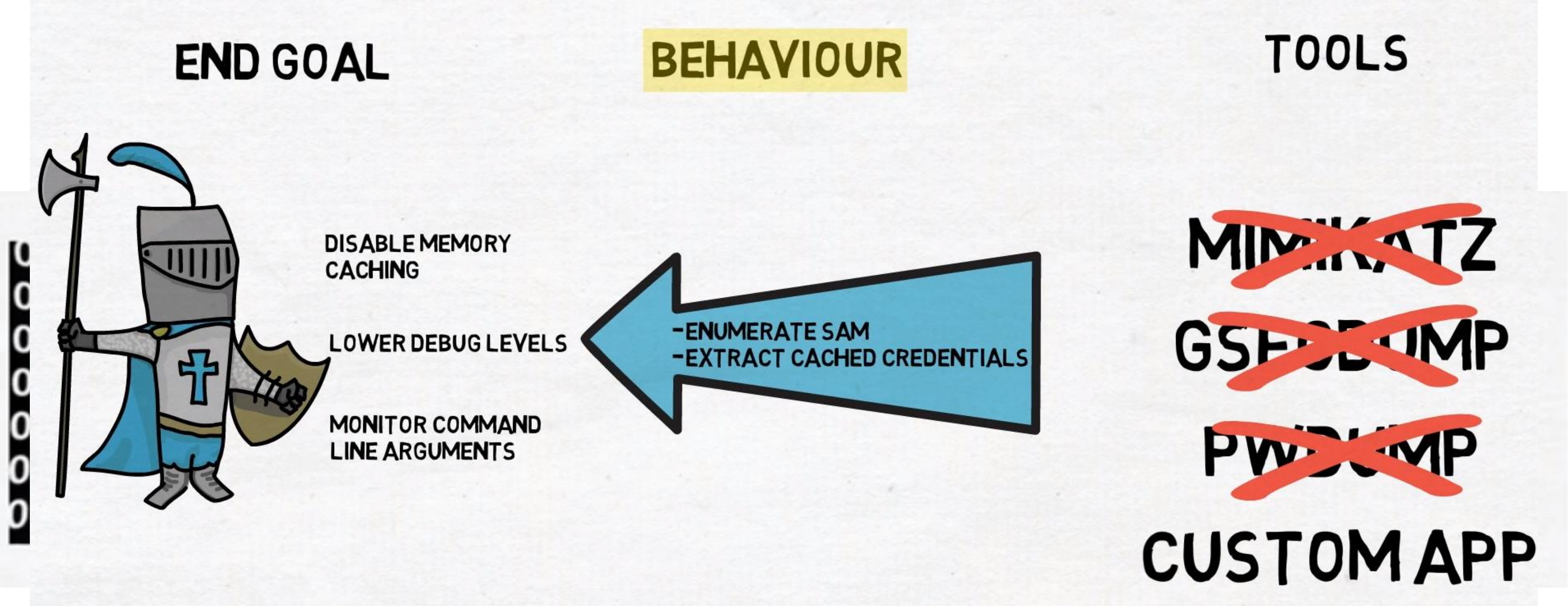
Firewall filtering

Anti-virus signatures



Focus on controls that target the top!

- Credential dumping example (CSO Perspective)
  - Go after Tools (e.g. prevent installation of Mimikatz or Metasploit)
  - Take out the entire technique of in-memory credential dumps



Validation

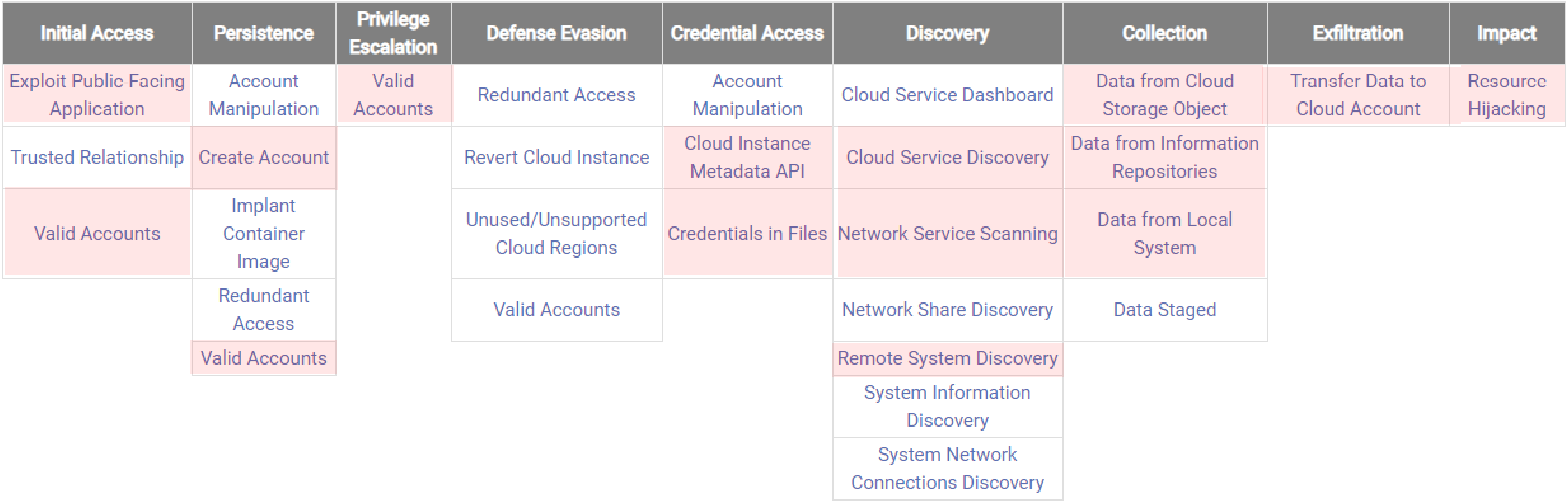
- Knowing yourself
  - How can you tell how well a control is working?
  - How can you identify where you are weakest?

- Automated Attack validation
  - AttackIQ, Mitre's Caldera, Canary's Red Team Automation
  - Measure whether TTPs get detected by the control that is assigned
  - Measure coverage across attack matrix to evaluate what an organization needs

- Mostly for enterprise and legacy deployments

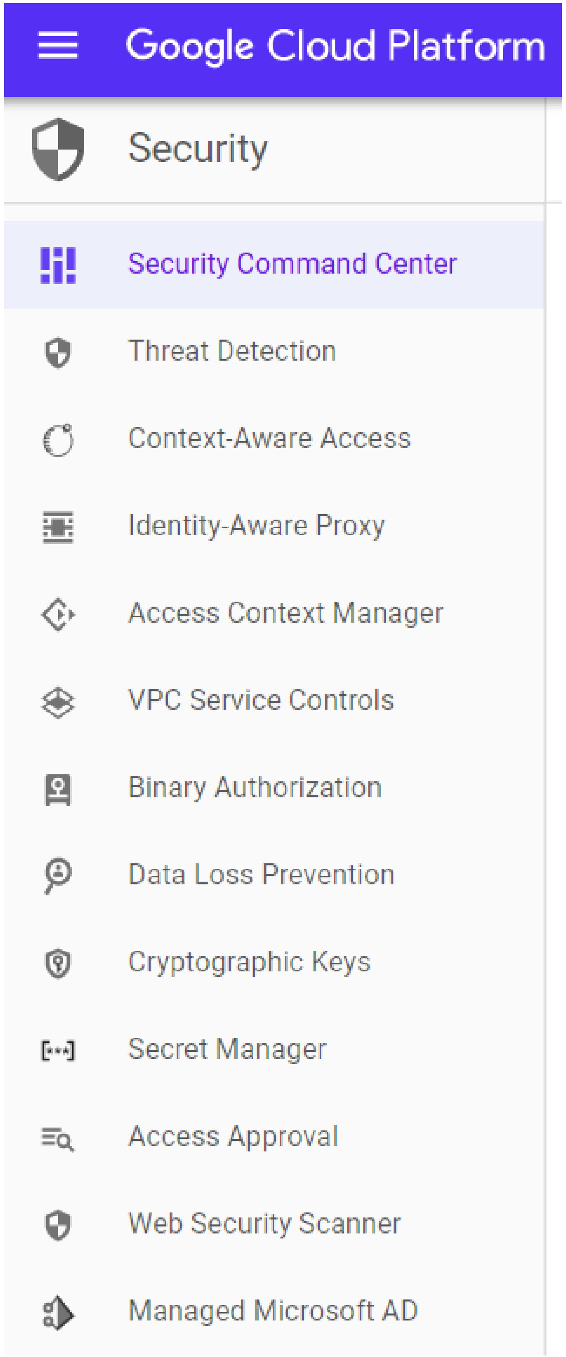
What about the cloud?

- GCP
  - https://attack.mitre.org/matrices/enterprise/cloud/gcp/
- AWS
  - https://attack.mitre.org/matrices/enterprise/cloud/aws/
- Covered by https://thunder-ctf.cloud and CloudGoat/flaws.cloud

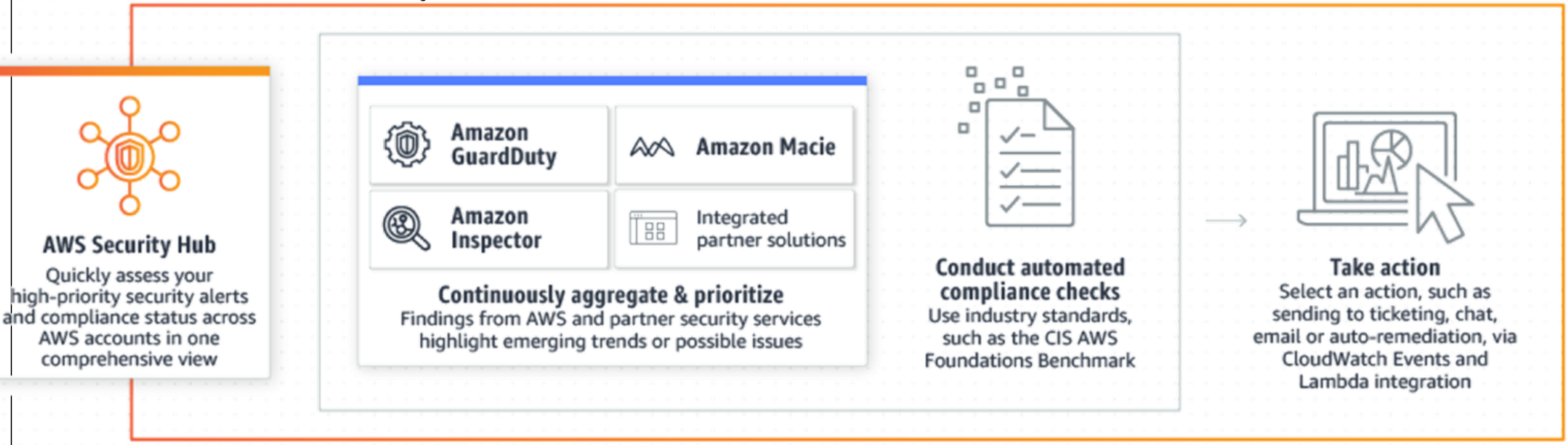


Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

- GCP's Security Command Center (4/2019)
  - Centralize controls for a project



- AWS's Security Hub (6/2019)



AWS Security Hub

Quickly assess your high-priority security alerts and compliance status across AWS accounts in one comprehensive view

Continuously aggregate & prioritize

Findings from AWS and partner security services highlight emerging trends or possible issues

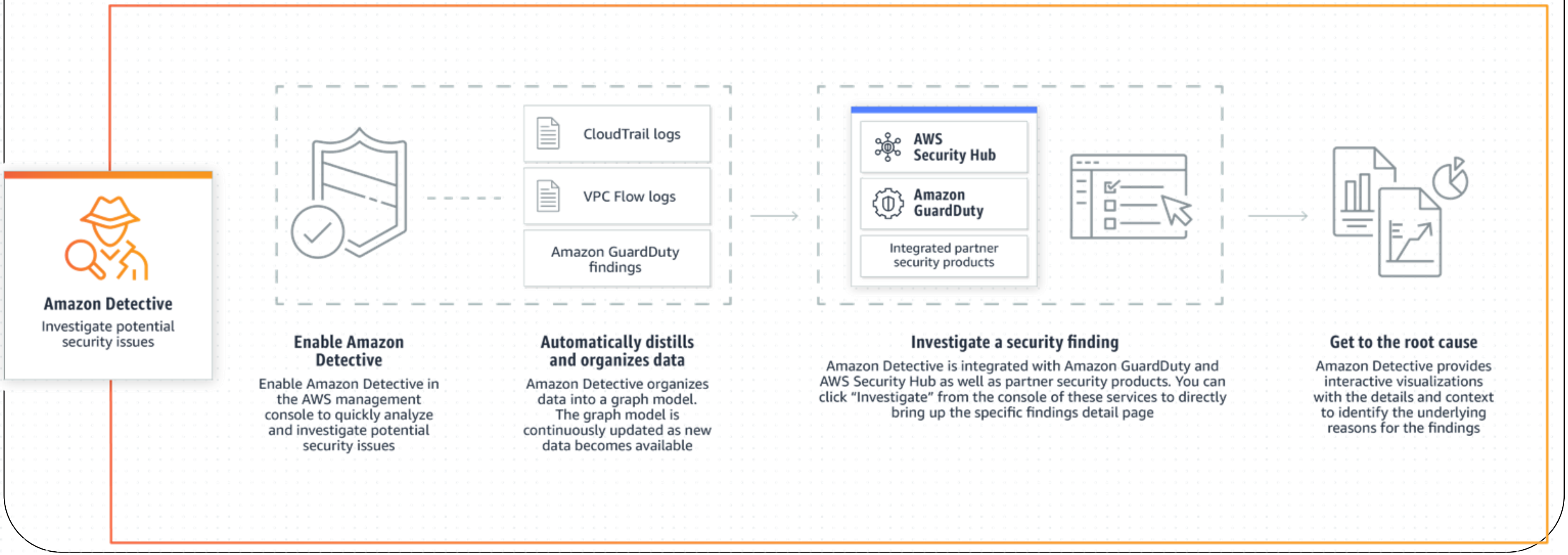
Conduct automated compliance checks

Use industry standards, such as the CIS AWS Foundations Benchmark

Take action

Select an action, such as sending to ticketing, chat, email or auto-remediation, via CloudWatch Events and Lambda integration

- Last week: Incident response with AWS Detective (4/2020)



Amazon Detective

Investigate potential security issues

CloudTrail logs
VPC Flow logs
Amazon GuardDuty findings
AWS Security Hub
Amazon GuardDuty
Integrated partner security products

Enable Amazon Detective

Enable Amazon Detective in the AWS management console to quickly analyze and investigate potential security issues

Automatically distills and organizes data

Amazon Detective organizes data into a graph model. The graph model is continuously updated as new data becomes available

Investigate a security finding

Amazon Detective is integrated with Amazon GuardDuty and AWS Security Hub as well as partner security products. You can click "Investigate" from the console of these services to directly bring up the specific findings detail page

Get to the root cause

Amazon Detective provides interactive visualizations with the details and context to identify the underlying reasons for the findings