LA TROBE UNIVERSITY

All kinds of clever

CSE5ISM CYBERSECURITY INCIDENT MANAGEMENT Week 3-4

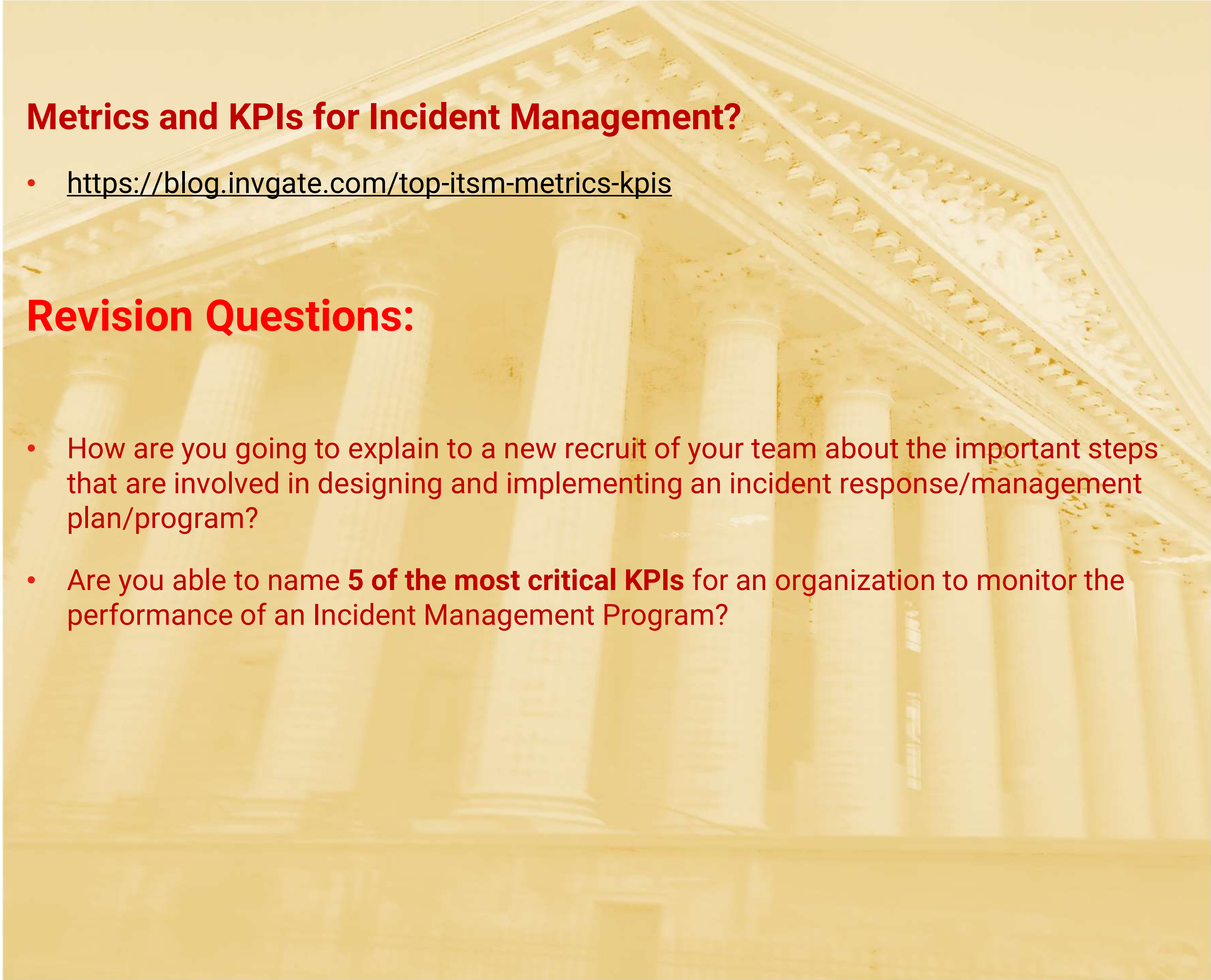
Dr ASM (Kayes) Kayes

March 2025

Week 1-2 Revision

- Difference between Cybersecurity Vs Information Security
- Tasks in the ISACA Information Security Incident Management body of knowledge
- Phases in a typical Incident Response Plan/Framework
- Difference between the ISO/IEC 27035:2016 and the NIST 800-61
- KPIs for incident management

Revision



Metrics and KPIs for Incident Management?

- https://blog.invgate.com/top-itsm-metrics-kpis

Revision Questions:

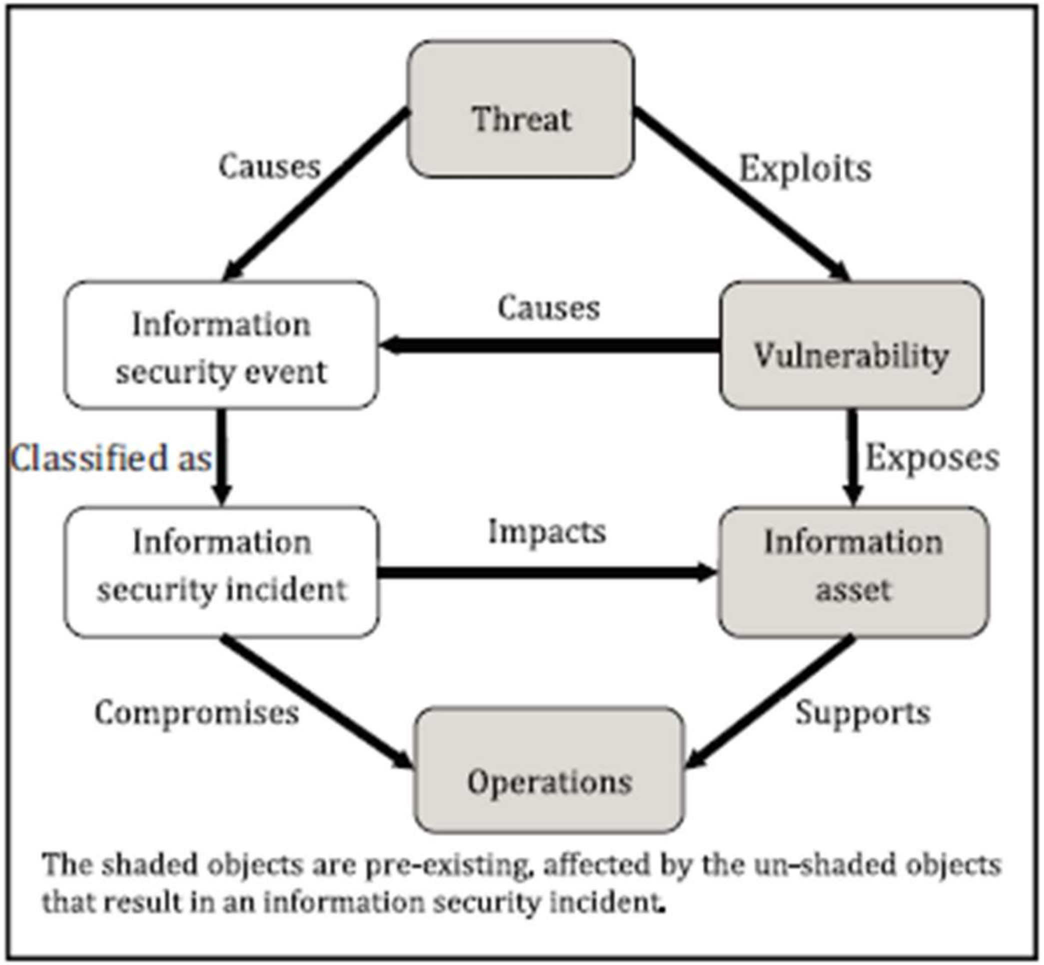
- How are you going to explain to a new recruit of your team about the important steps that are involved in designing and implementing an incident response/management plan/program?
- Are you able to name **5 of the most critical KPIs** for an organization to monitor the performance of an Incident Management Program?

Week 3-4: Lecture Outline

Business and technical measures in security incident management

- Understand different cyber threat vectors
- Overview of different cyber attack models
  - Cyber Kill Chain
  - Unified Kill Chain
  - The MITRE ATT&CK Framework
- Analysis of vulnerabilities in business processes
- Establish a business process related to the severity of incidents and classification of incidents
- Identify technical measures with the capability to timely detect, investigate, respond to and recover from security incidents to minimize impact to business processes/functions/operations

Relationship of objects in an information security incident



The shaded objects are pre-existing, affected by the un-shaded objects that result in an information security incident.

Source: ISO/IEC 27035 Security incident management

- Threats are Malicious Attempts to gain unauthorised access to and use of an asset
- Exploits Vulnerability and causes Security Event
- Exposes Asset & causes Security Event
- Security Event: classified as Security Incident when the Incident impacts the Asset and compromises Operations

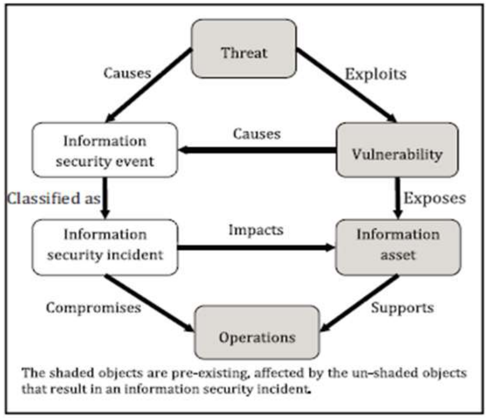
Cyber Threats

“The possibility of a malicious attempt to damage or disrupt a computer network or system” (Oxford Dictionary)

- This definition is incomplete
- It does not include the attempt **to access files and infiltrate or steal data**
- A cyber threat is identified with the actor or adversary attempting to gain access to a system or the information held by the system

Discussion

Types of cyber threats



The shaded objects are pre-existing, affected by the un-shaded objects that result in an information security incident.

- Advanced Persistent Threats
- Phishing / Spear Phishing
- Network traveling Worms
- Virus
- Social Engineered Trojans
- Botnets
- Ransomware
- Distributed Denial of Service (DDoS)
- Wiper Attacks
- Unpatched Software (such as Java, Adobe Reader, Flash) = Zero Day Attack

- Intellectual Property Theft
- Theft of Money
- Root-kit
- Data Manipulation
- Data Destruction
- Spyware/Malware
- Man in the Middle (MITM)
- Drive-By Downloads
- Malvertising
- Rogue Software

Cyber threat vectors (means of attack)

- **Email**
  - Phishing for credentials (including 2 factor SMS codes for simultaneous login by the hacker).
  - Malicious links/attachments.
    - Bulk mailouts = "commodity" malspam campaigns.
    - Targeted mailout = spearphishing.
    - "Business Email Compromise" scams (wire transfer fraud, fake invoices, etc)
- **Web**
  - Drive-by: Commodity background Javascript "exploit kit" redirection and infection of browsing computer while visiting compromised legitimate websites.
  - Watering hole: Compromise of websites known to be visited by the target for selective infection.

Cyber threat vectors (means of attack)…

- **Vulnerable internet-exposed systems**
  - Servers, routers, printers, etc that are not patched / firewalled, can be hacked easily.
  - Targeted introduction of ransomware into critical portions of a compromised organization is becoming common.
- **Supply chain**
  - Trojanized software / firmware / hardware out-of-the-box or via updates.
- **Malicious insider**
  - Rogue staff member or contractor.

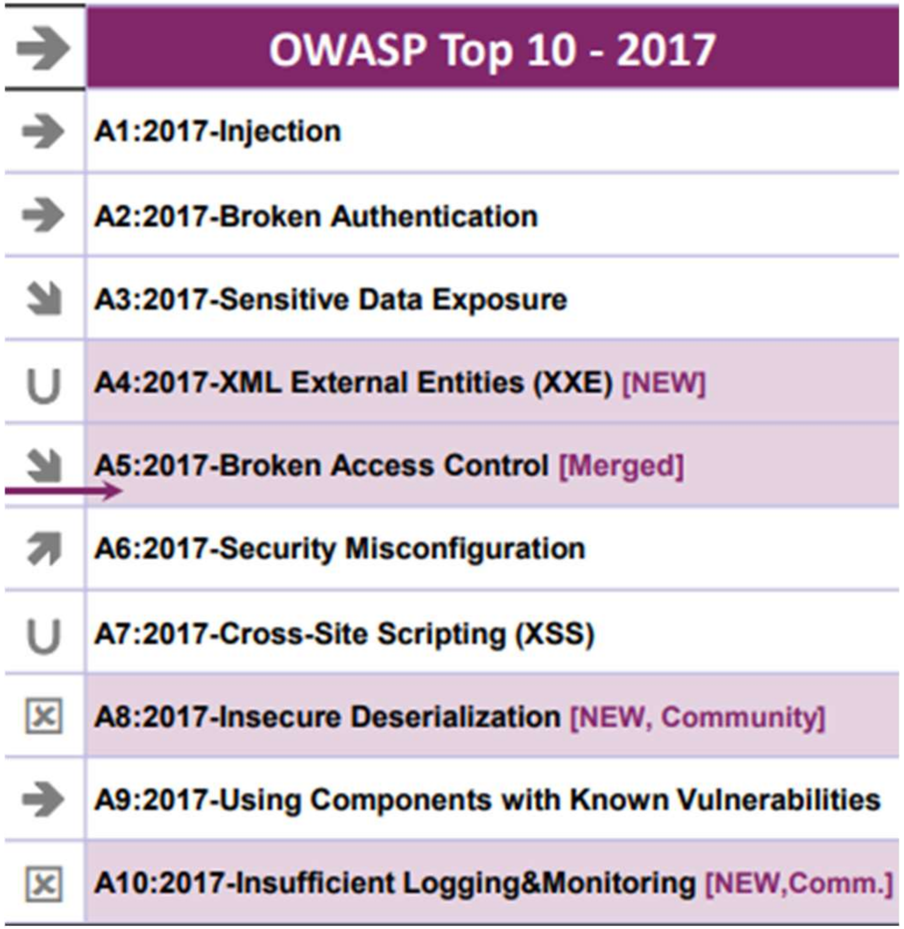
The priority of these vectors may be adjusted according to specific industry/organizational Risk Assessments and **Threat Intelligence (keywords/concepts: threat/attack vector, attack graph, attack surface, cyber threat modelling, threat actor attribution…)** to identify priority threats and to apply appropriate incident response/management approach(s)/framework(s).

Priority threats to infrastructure

- These need <u>fast containment</u> because they can spread through the networks:
  - **Ransomware**
    - Even if only one PC is infected, it will encrypt team file shares, online backup servers...
  - **Worms**
    - Malware that replicates and infects multiple systems.
  - **Destructive malware**
    - Like a worm but with a destructive payload (e.g. Wannacry, Not Petya).

1. **Injection:** untrusted data is sent as part of a command or query
2. **Broken Authentication:** compromised user credentials when authentication and session management
3. **Sensitive or Personal Data Exposure:** compromises to user-inputted data
4. **XML External Entities:** injection-style attack in XML
5. **Broken Access Control:** user without correct permissions
6. **Misconfigured Security:** code-related, or due to user error
7. **Cross-Site Scripting (XSS):** part of the ‘injection’ family, dynamic site elements to hijack the user’s browser and computer
8. **Insecure Deserialization:** untrusted data that is being serialized and deserialized
9. **Insecure Themes, Plugins, and Other Components**
10. **Insufficient Logging and Monitoring Site and Data:** site open to even more malicious attacks and can erode any trust you’ve gained with your user base.

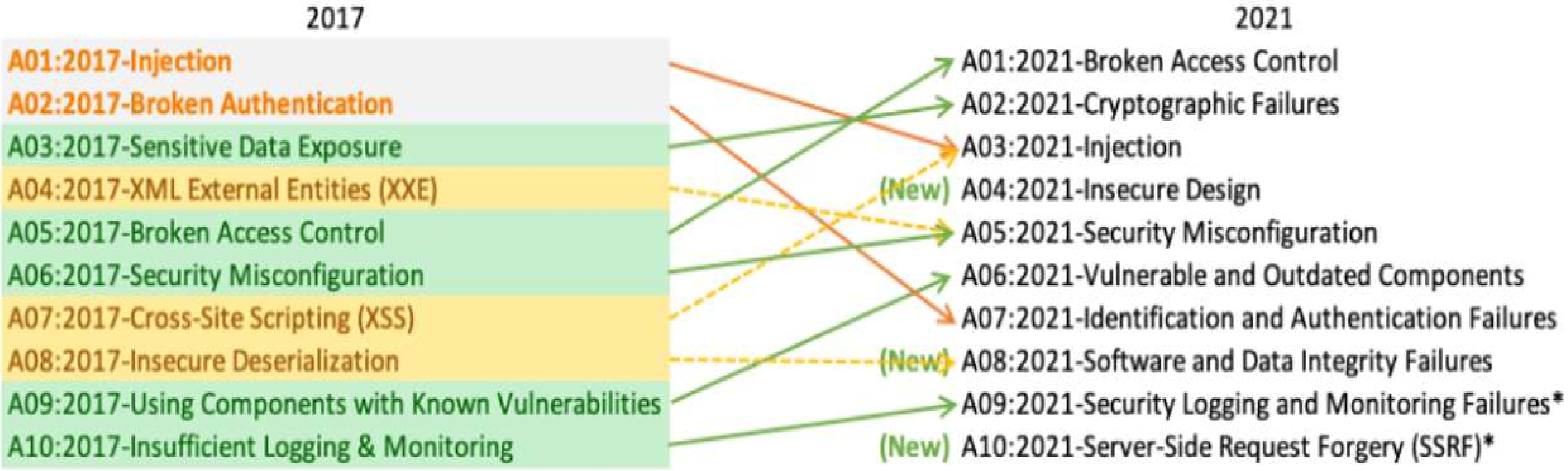
Open Web Application Security Project (OWASP)
Most critical web application security risks/threats



→	OWASP Top 10 - 2017
→	A1:2017-Injection
→	A2:2017-Broken Authentication
↘	A3:2017-Sensitive Data Exposure
∪	A4:2017-XML External Entities (XXE) [NEW]
↘	A5:2017-Broken Access Control [Merged]
↗	A6:2017-Security Misconfiguration
∪	A7:2017-Cross-Site Scripting (XSS)
☒	A8:2017-Insecure Deserialization [NEW, Community]
→	A9:2017-Using Components with Known Vulnerabilities
☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Source: https://www.owasp.org/

Open Web Application Security Project (OWASP)
Most critical web application security risks/threats



2017		2021
A01:2017-Injection		A01:2021-Broken Access Control
A02:2017-Broken Authentication		A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure		A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New)	A04:2021-Insecure Design
A05:2017-Broken Access Control		A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration		A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)		A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New)	A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities		A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New)	A10:2021-Server-Side Request Forgery (SSRF)*

Source: https://owasp.org/www-project-top-ten/

Cyber Attack/Threat Models

- **Attack graphs:** are abstract representations of the different attack scenarios and paths
- **Attack vector:** a means by which a hacker can gain access to a system
- **Diamond model:** an intrusion analysis tool which provides a formalised way to characterise network intrusion

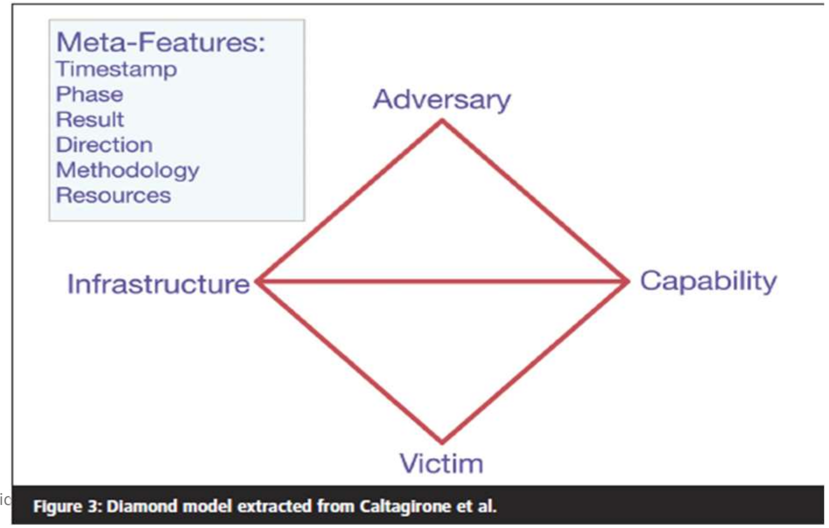


Figure 3: Diamond model extracted from Caltagirone et al.

- **Attack surface:** is the total sum of vulnerabilities that can be exploited to carry out an incident
- **OWASP Threat modelling:** a process for providing a structured representation of the security incident information
- **MITRE ATT&CK™:** is a knowledge base of adversary tactics and techniques
- **Cyber Kill Chain:** an integrated, end-to-end process of adversary attack described as a chain

Hammad et el (2016) Cyber-Attack Modeling Analysis Techniques: An Overview

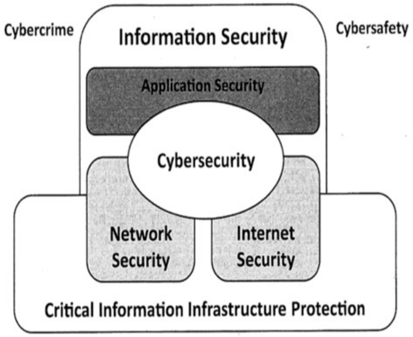


Figure 1 — Relationship between Cybersecurity and other security domains

Cyber Attack Surface

- Physical attack surface: access to all endpoint devices, including desktop systems, laptops, mobile devices, USB ports and improperly discarded hard drives
- Once an attacker was successful in a computing device physically, the exploitation of the digital attack surface begins
- Can be exploited through inside threats, social engineering and intruders posing as staff or service workers
- Can be exploited through external threats including password retrieval, physical break-ins
- Goal is to reduce physical attack surface through access control, surveillance and disaster recovery

Attack surface (Network, Internet, Application / Software, Physical Infrastructure)

- To describe what is being attacked
- Network attack surface: total of all vulnerabilities in connected hardware and software in the network
- Goal is to reduce the number and size of network attack surfaces:
  - Microsegmentation: divide the data center into logical units, each of which has its own unique security policies
  - Policies need to be tied to logical segments: workload migration requires moving the security policies

LA TROBE UNIVERSITY All kinds of clever

Cyber Attack/Threat Models

- **Cyber threat modelling:** a process for providing a structured representation of the security incident information
  - Cyber Kill Chain
  - Unified Kill Chain
  - MITRE ATT&CK™ Framework

Cyber Kill Chain

- Developed by Lockheed Martin to characterize the steps Advanced Persistent Threat (APT) actors generally follow to achieve their objectives.
- The cyber kill chain describes the phases of a targeted attack.
- The goal is to detect and react to an attack.
- The **earlier in the kill chain you can detect / stop the threat actor the better**.
- The kill chain can also help make sense of, and chronologically order, the evidence gathered during an investigation.

- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cyber Kill Chain – 7 Phases

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Action on Objectives

- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cyber Kill Chain

https://www.youtube.com/watch?v=vX8IJ0WTVyU

https://www.youtube.com/watch?v=mhgwtuWlB8I

Cyber Kill Chain

- **Reconnaissance**
  - Used to determine information about the target, e.g.
    - Email and IP addresses.
    - Staff to target.
      - LinkedIn is a great resource for threat actors!
    - Vulnerable systems.
  - Passive recon:
    - Virtually impossible for defenders to spot since there are no actions taken against them directly, e.g. Researching public information.
  - Active recon:
    - Scanning of defender IP address space for vulnerabilities can be spotted if you're logging it, but it may be lost in constant noise of non-targeted scanning.

Harvesting email addresses, conference information, etc.

Cyber Kill Chain

- **Weaponization**
  - Developing and matching the malware payload to the vulnerabilities of the target.
  - May use a contextual lure, e.g. an email about a topic known to be of interest to the target.
    - e.g. a weaponized Microsoft Word document posing as a CV sent to the HR department for a job application.
    - e.g. an Excel file with malware payload macro
    - e.g. an embed object within a PDF file which exploits the vulnerabilities of Adobe Reader

Coupling exploit with backdoor into deliverable payload

Cyber Kill Chain

- **Delivery**
  - Sending the weaponized payload to the target, e.g.
    - Email.
    - Web watering hole.
    - USB sticks left scattered in the staff carpark.
    - Software update from a compromised software vendor.

DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

Cyber Kill Chain

Exploiting a vulnerability to execute code on victim's system

- **Exploitation**
  - The payload exploits a vulnerability on the target system.
  - Keeping software up-to-date with security patches (program updates) helps defend against this phase.
  - Even on patched systems, the vulnerability may be the user who opens a document that runs with user privilege.
  - Zero-day vulnerabilities are those not publicly known or for which a patch has not yet been issued.

Cyber Kill Chain

Installing malware on the asset

- **Installation**
  - Installation of malware / hacking tools on the target system.
  - May be multi-stage using different technologies, e.g.
    - A Word document runs a malicious macro when opened.
    - The macro does a web request to a compromised legitimate website where downloader malware has been pre-positioned.
    - The downloader pulls down and executes a backdoor Remote Access Trojan (RAT) which reaches out to the hacker’s Internet infrastructure and allows them remote control of the infected system.

Cyber Kill Chain

Command channel for remote manipulation of victim

- **Command & Control (C2)**
  - The malware "dials home" by connecting to the threat actor's Command & Control server
  - Receive instructions or give the hacker remote access to run commands on the infected system.
  - C2 channels can be via:
    - Web traffic.
    - IRC and other protocols (HTTP proxies help defend against this).
    - DNS requests to the hacker's domain (replies contain instructions).
    - Steganography – instructions hidden in social media posts, memes, etc.

Cyber Kill Chain

With 'Hands on Keyboard' access, intruders accomplish their original goals

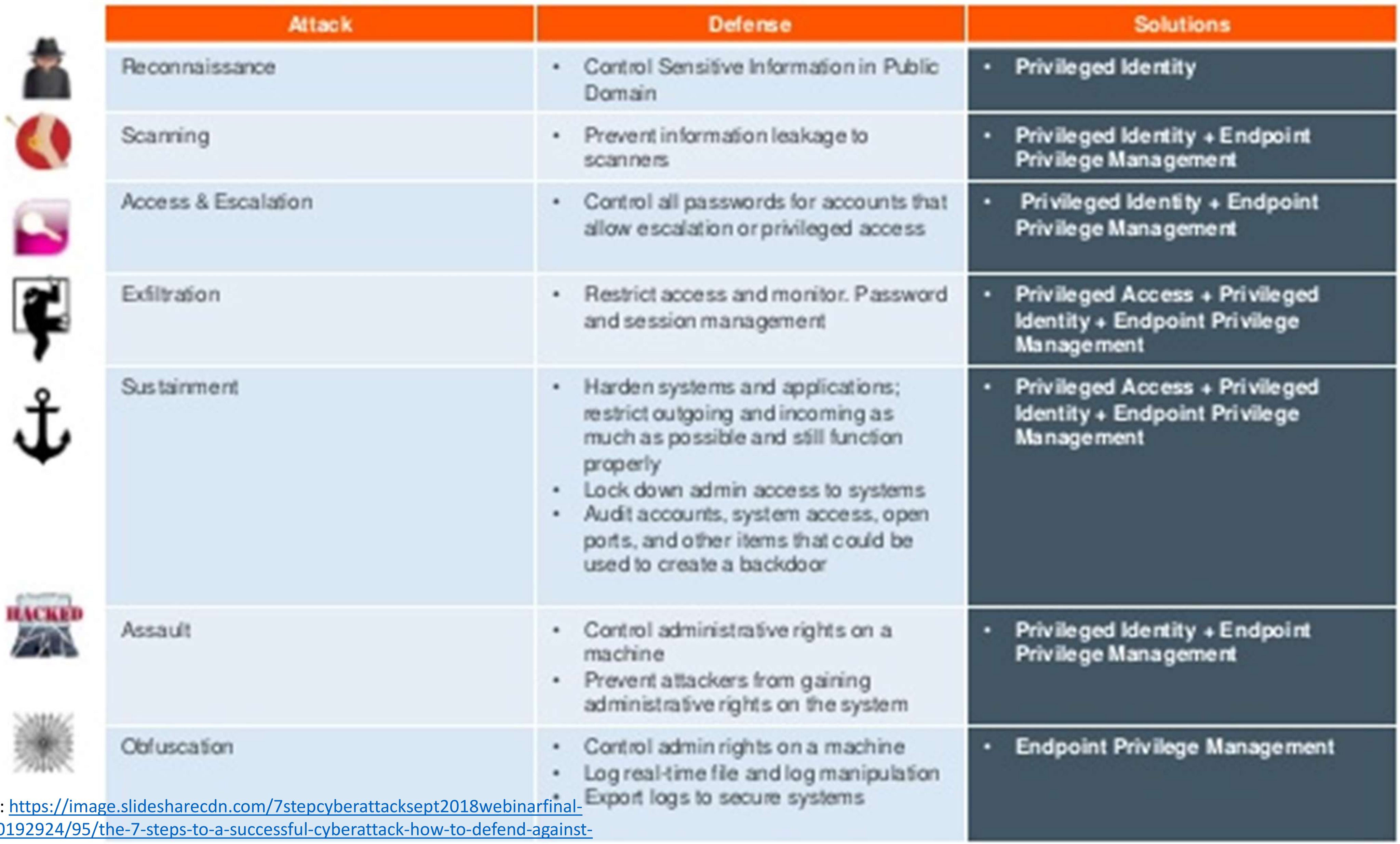
- **Action on Objectives**
  - Lateral movement,
    - pivoting off the initial infection point to compromise other systems in the network.
  - Collecting stolen data on a staging machine (one of the compromised systems).
  - Exfiltration of the data (sending it to the threat actor).

Attacker's viewpoint of steps to success

- Reconnaissance
- Delivery & Exploitation: Initial compromise
- Installation: Establish foothold
  - RAT (Remote Access Trojan)
  - Backdoors
  - Web shells
- Command & Control: Cycle of
  - Escalate privileges
  - Maintain presence
  - Internal reconnaissance
  - Move laterally
- Action of Objective: Exfiltrate data / complete mission / maintain implants in target network for future use

Activity

From the Attacker's and the Defender's viewpoint, discuss about the steps to success in each phase of the cyber kill chain.



Attack	Defense	Solutions
Reconnaissance	• Control Sensitive Information in Public Domain	• Privileged Identity
Scanning	• Prevent information leakage to scanners	• Privileged Identity + Endpoint Privilege Management
Access & Escalation	• Control all passwords for accounts that allow escalation or privileged access	• Privileged Identity + Endpoint Privilege Management
Exfiltration	• Restrict access and monitor. Password and session management	• Privileged Access + Privileged Identity + Endpoint Privilege Management
Sustainment	• Harden systems and applications; restrict outgoing and incoming as much as possible and still function properly • Lock down admin access to systems • Audit accounts, system access, open ports, and other items that could be used to create a backdoor	• Privileged Access + Privileged Identity + Endpoint Privilege Management
Assault	• Control administrative rights on a machine • Prevent attackers from gaining administrative rights on the system	• Privileged Identity + Endpoint Privilege Management
Obfuscation	• Control admin rights on a machine • Log real-time file and log manipulation • Export logs to secure systems	• Endpoint Privilege Management

Source: https://image.slidesharecdn.com/7stepcyberattacksept2018webinarfinal-180920192924/95/the-7-steps-to-a-successful-cyberattack-how-to-defend-against-them-29-638.jpg?cb=1537471822

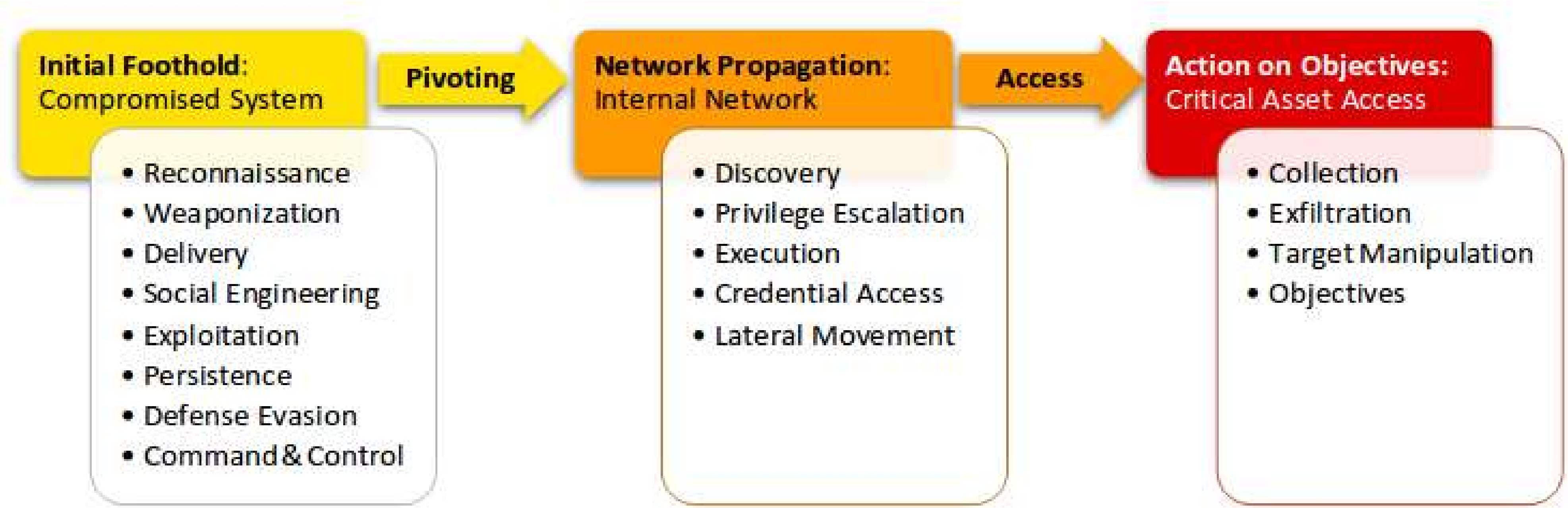
Cyber Kill Chain – 7 Phases

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Action on Objectives

- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Unified Kill Chain

- A more detailed kill chain has been proposed that better illustrates the multitude of ongoing phases typically taking place while threat actors are operating within a target network.



Initial Foothold: Compromised System

- Reconnaissance
- Weaponization
- Delivery
- Social Engineering
- Exploitation
- Persistence
- Defense Evasion
- Command & Control

Network Propagation: Internal Network

- Discovery
- Privilege Escalation
- Execution
- Credential Access
- Lateral Movement

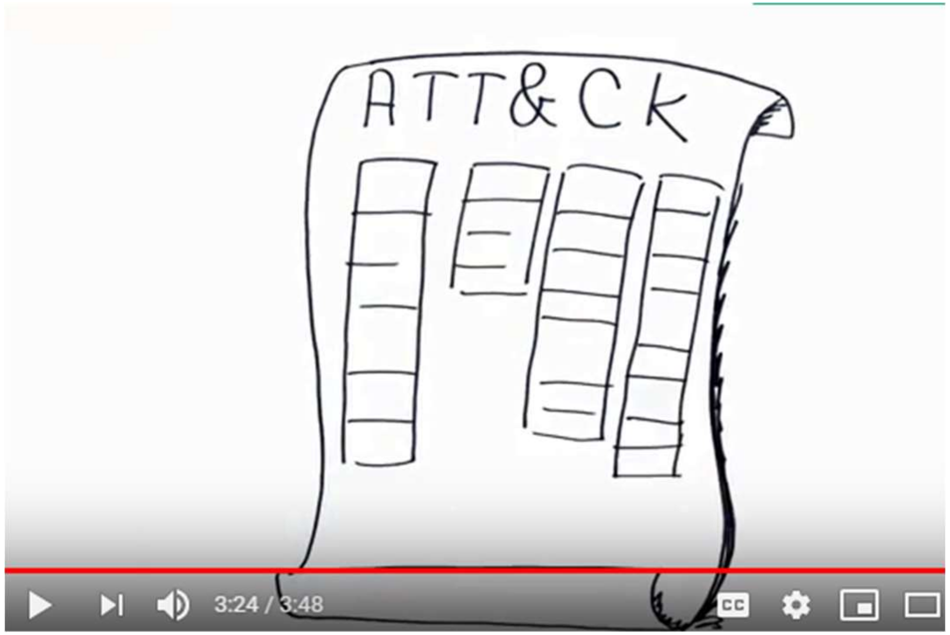
Action on Objectives: Critical Asset Access

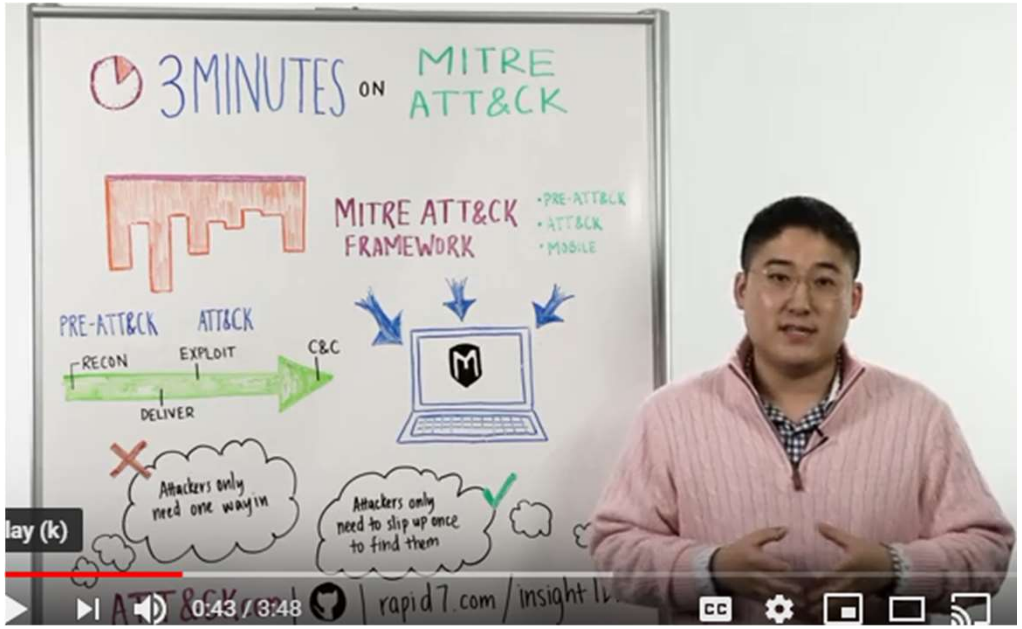
- Collection
- Exfiltration
- Target Manipulation
- Objectives

Attribution of attacks - Threat Intelligence

- **Attributing the attack to a specific threat actor group or individual is usually very hard**.
- Some threat actors plant “false flags” in their malware, e.g.
  - Configuring malware to look like it uses the language of the country the true threat actor wants to implicate.
  - Reusing code known to be attributed to another actor group.
- Most organizations don’t have the visibility of evidence (e.g. logs) and sufficient resources to track actor Tools, Tactics and Procedures (TTPs) in order to do attribution.

MITRE ATT&CK





https://youtu.be/0BEf6s1iu5g

https://youtu.be/giHof1SoZv4

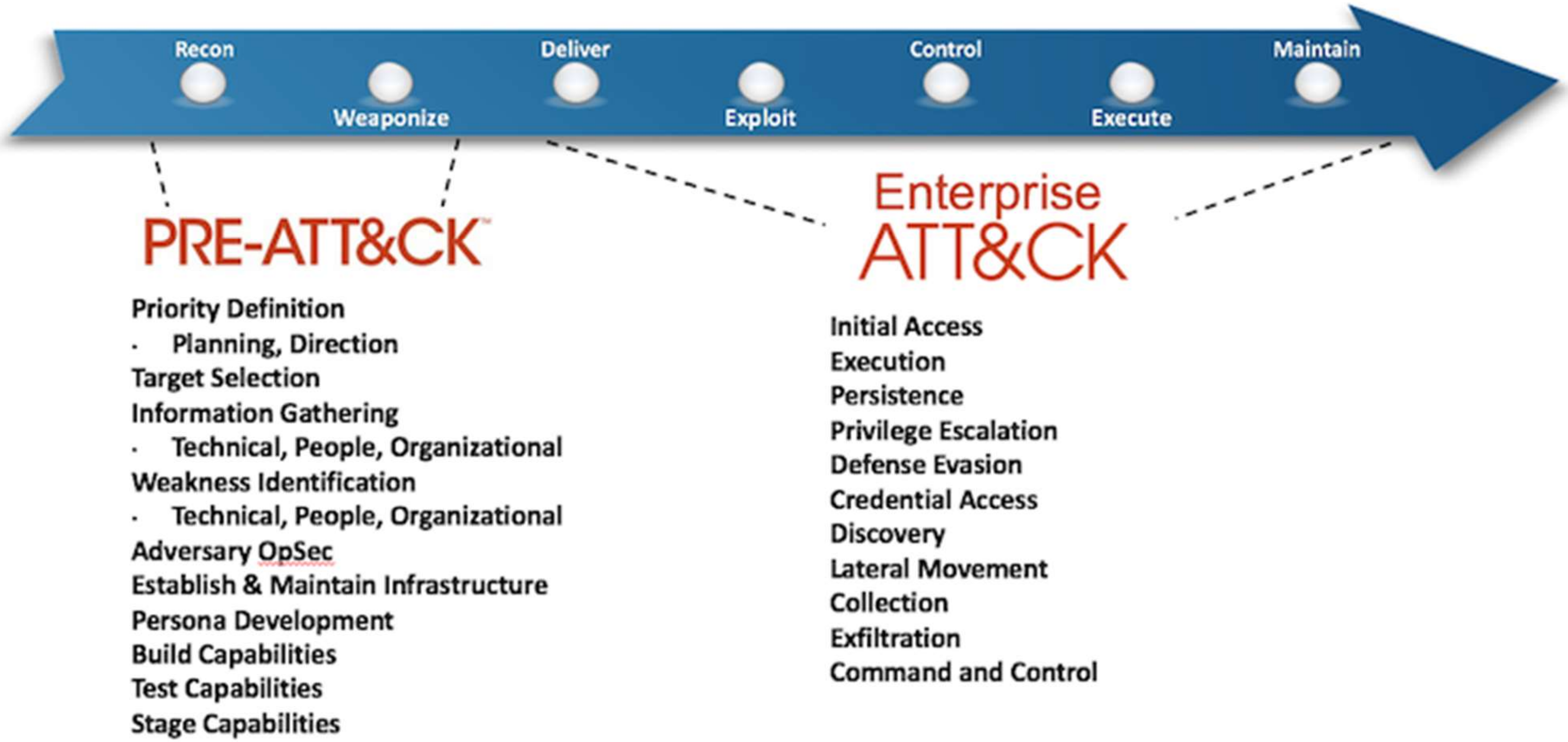
MITRE ATT&CK Framework

- MITRE **ATT&CK**™ ("*Adversarial Tactics, Techniques, and Common Knowledge*") is a repository of adversary tactics and techniques based on real-world observations of threat actor methods
- It contains very detailed classifications of:
  - **Tactics**, e.g.
    - Defence Evasion, Lateral Movement, Exfiltration.
  - Within **each Tactic it describes multiple techniques and, where known, which threat actor group use the technique**.
  - It provides a very granular breakdown of the later stages of the kill chain.
- The framework can possibly help with attribution to some extent.

https://attack.mitre.org/

MITRE PRE-ATT&CK

- Pre-ATT&CK covers the first two stages of the kill chain
- Enterprise ATT&CK deals with the next five stages of the kill chain



PRE-ATT&CK™

Priority Definition

- Planning, Direction

Target Selection

Information Gathering

- Technical, People, Organizational

Weakness Identification

- Technical, People, Organizational

Adversary OpSec

Establish & Maintain Infrastructure

Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

Enterprise ATT&CK

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

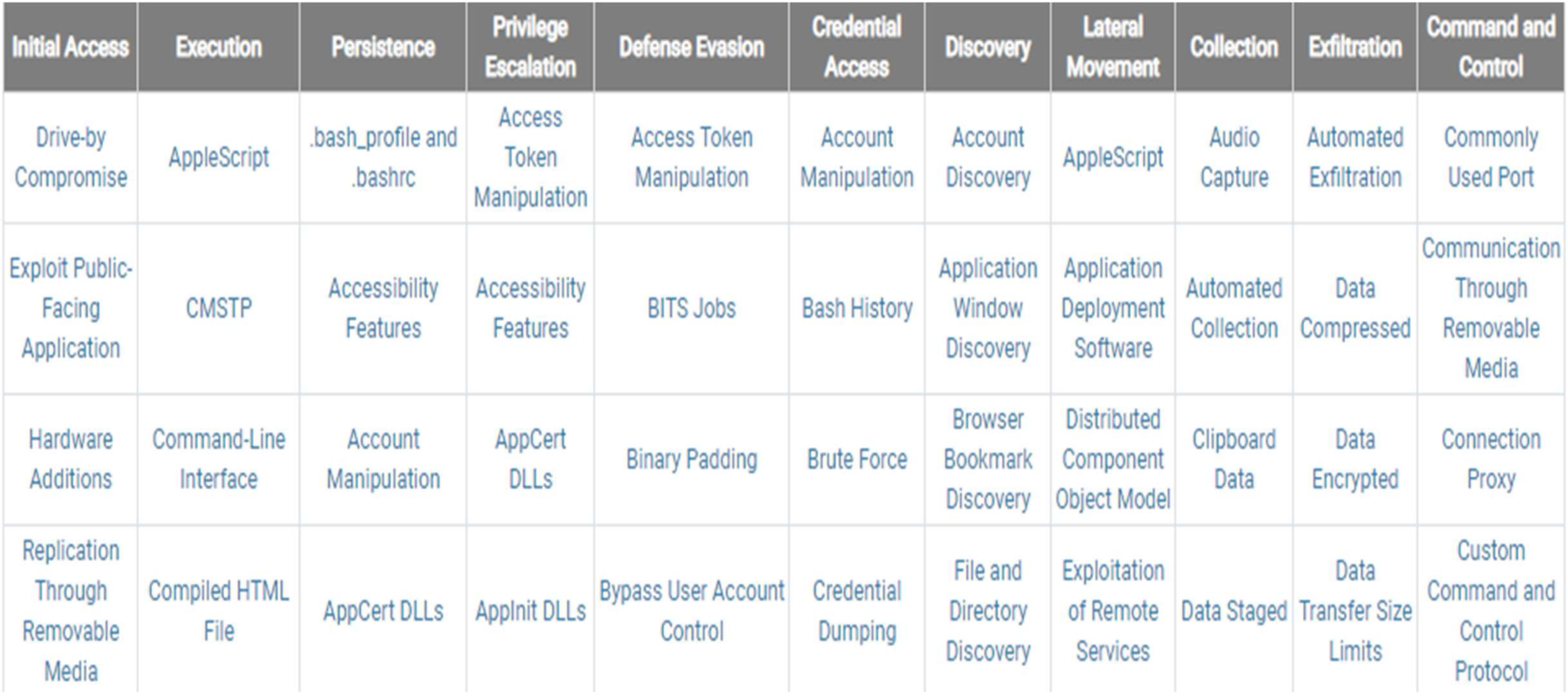
Lateral Movement

Collection

Exfiltration

Command and Control

Example of ATT&CK Matrix™



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol

Australian Cybersecurity agencies

- **AusCERT**
  - Australia's **first *Computer Emergency Response Team* (CERT),** a not-for-profit security group based at the University of Queensland.
- **Australian Signals Directorate** (ASD)
  - Historically the Australian Defence Force's **Signals Intelligence function**, it is now also the nation's primary cybersecurity agency. The ASD also **does Incident Response for Government departments**.
- **CERT Australia**
  - The Australian **Government's first CERT**.
- **Australian Cyber Security Centre** (ACSC) (https://www.cyber.gov.au/)
  - Based in Canberra, the centre **co-locates cyber related government departments** like the AFP, ASD and CERT Australia.
- **Joint Cyber Security Centres** (JCSC)
  - Offices based in each capital city as **"branches" of the ACSC for liaison between Government and Business**.

Australian Cybersecurity agencies…

- In mid 2018, CERT Australia and the ACSC became part of the ASD and are in the process of collectively rebranding as “cyber.gov.au”
- The ACSC:
  - Responds to cyber security threats and incidents as Australia’s Computer Emergency Response Team (CERT)
  - Monitor cyber threats across the globe to alert Australians
  - Provide advice and information about cybersecurity to individuals and business online
  - Work business, government and academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats
- https://www.cyber.gov.au/about

Other Australian agencies

- The new government cybersecurity agencies come under the Department of Home Affairs.
  - https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security
- Within Home Affair’s Cybersecurity portfolio is the Trusted Information Sharing Network (TISN), an environment where business and government can share information on critical infrastructure vulnerabilities and techniques to assess and mitigate risk.
  - https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience

Other Australian agencies…

- Law enforcement
  - Australian Federal Police (AFP)
  - State Police
  - Australian Criminal Intelligence Commission (ACIC)
    - Each have cybercrime units
    - They also liaise with counterparts overseas

Other Australian agencies…

- Australian Transaction Reports and Analysis Centre (**AUSTRAC**)
  - Australia's financial intelligence agency with regulatory responsibility for anti-money laundering and counter-terrorism financing.
  - (Note that some cyberattacks are used to fund terrorism).
- Australian Cybercrime Online Reporting Network (**ACORN**)
  - The government’s central portal for reporting cybercrime (Police refer victims to it).

Cyber Threat Intelligence

- **Threat Intelligence (threat/attack vector, attack graph, attack surface, cyber threat modelling, threat actor attribution…)**
- There are a number of formal, informal and industry based groups globally that share **cyber threat intelligence** such as:
  - Attack campaign sightings.
  - Threat actor attribution information.
  - Threat actor **T**ools, **T**actics and **P**rocedures.
  - Indicators of Compromise (bad domain names, IP addresses, malware fingerprints, etc).
- Much of the information has a limited tactical shelf life as threat actors vary their TTPs and infrastructure.
- Nevertheless, Threat Intelligence can aid Incident Response investigations.
- Explore these: OWASP, APWG (anti-phishing working group).

LA TROBE UNIVERSITY

See You

Next Session

latrobe.edu.au

La Trobe University
CRICOS Provider Code Number 00115M