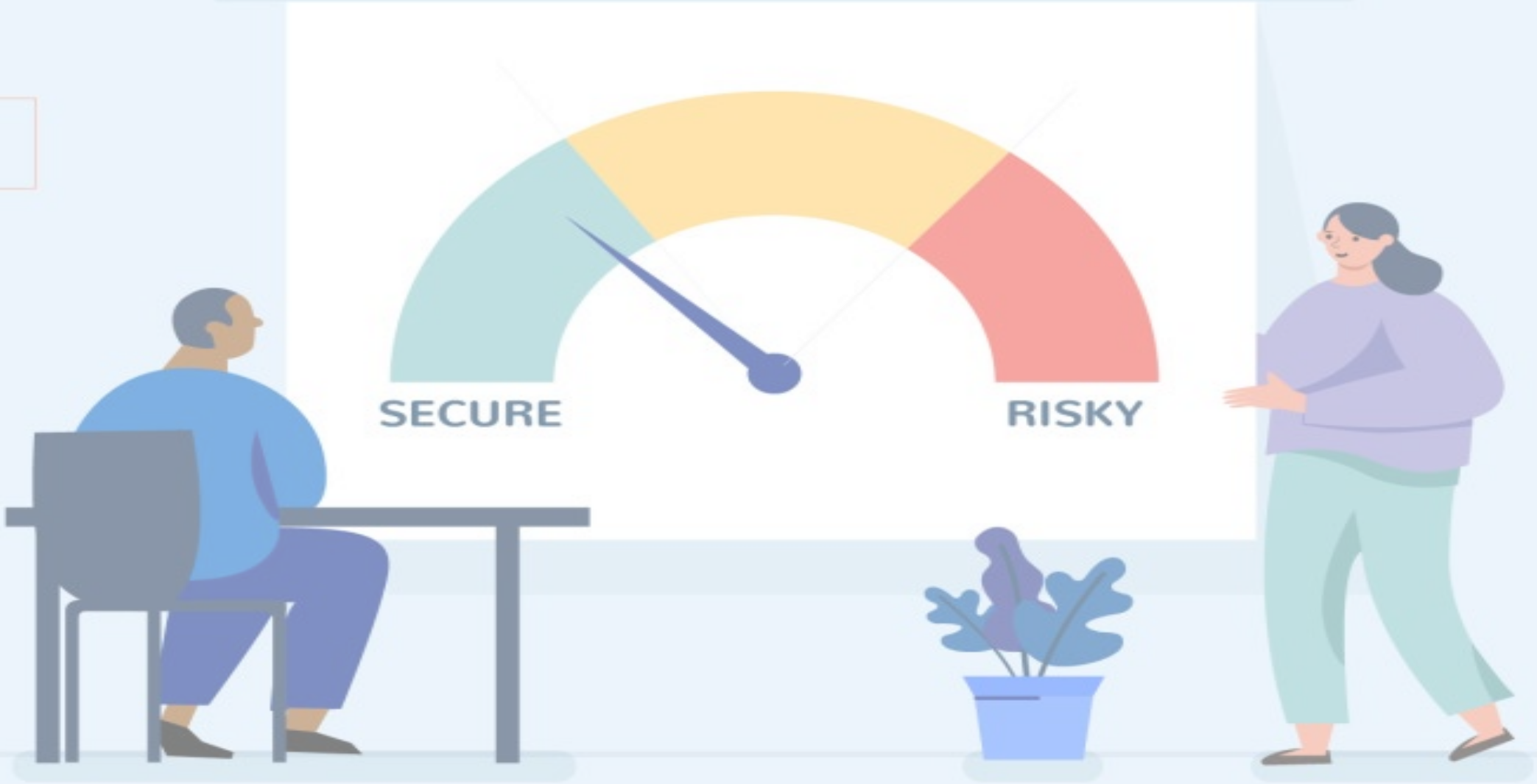
Cybersecurity: A Risky Business



FIRST Regional Symposium for the Pacific
Port Vila, Vanuatu, Sep 22nd 2023

Thanks

PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

CertVU

FIRST Improving Security Together

LONG GOD YUMI STANAP

LONG GOD YUMI STANAP

DEPARTMENT OF STATE · UNITED STATES OF AMERICA

APNIC FOUNDATION

AUSCERT

Take Aways

- Activity Risk = (Inherent Risk) * (Control Failure)

  - Avoid Risk
  - Mitigate Risk
  - Transfer Risk
  - Accept Risk

  - Preventative Controls
  - Detective Control
  - Corrective Controls

- Risk assessment must be a Repeatable process (Qualitative or Quantitative)

AUSCERT

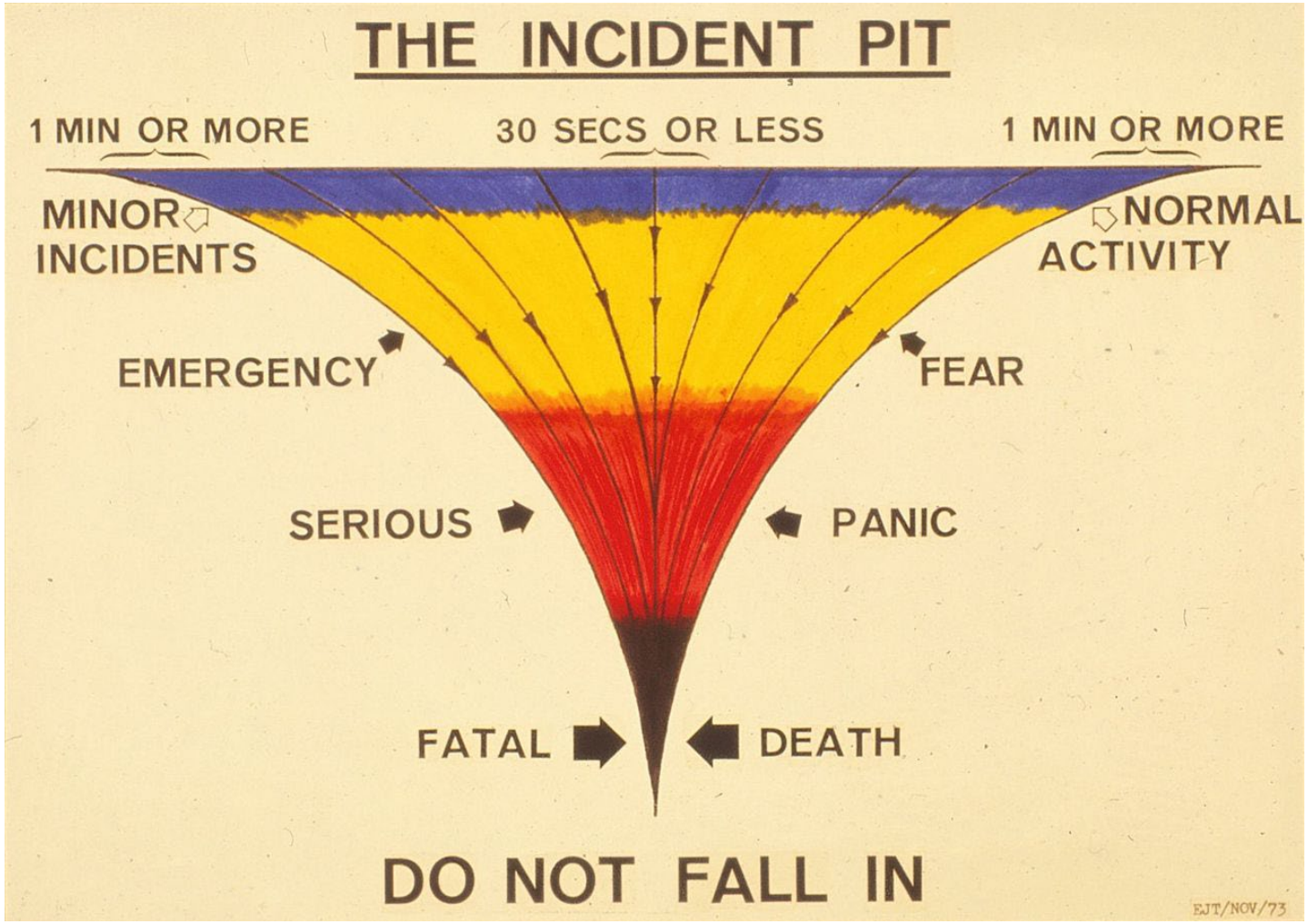
Learning Objectives

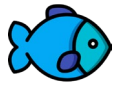
- Understand risks and their role in making an organisation function
- Understand type of controls that can be applied.
- Understand the intent of Govern in CSF 2.0
- Appreciate general steps of process improvement
- Appreciate the different level of process maturity
- For a Given [Country AND OR Industry]
  - Be able to identify documented APT
  - Be able to identify and map the MITRE ATT&K Techniques
  - Be able to list out Detection and Mitigation
  - Be able to fill out CSF 1.0/2.0
  - Be able to describe what needs to be done GOVERN for CSF 2.0
- Apply Risk on a single service (Phish)

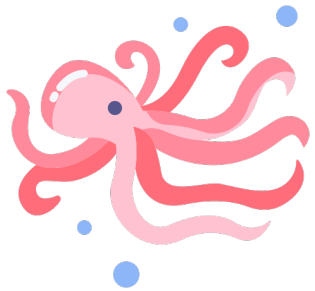

VANUATU
POST
Hideaway Island
Resort & Marine Sanctuary
FgV
BUILT BY FIBREGLASS VANUATU

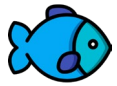
AUSCERT

Incident Pit – Diving



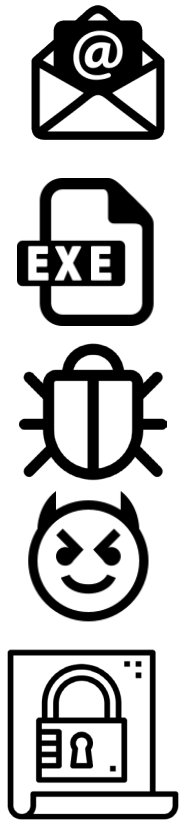


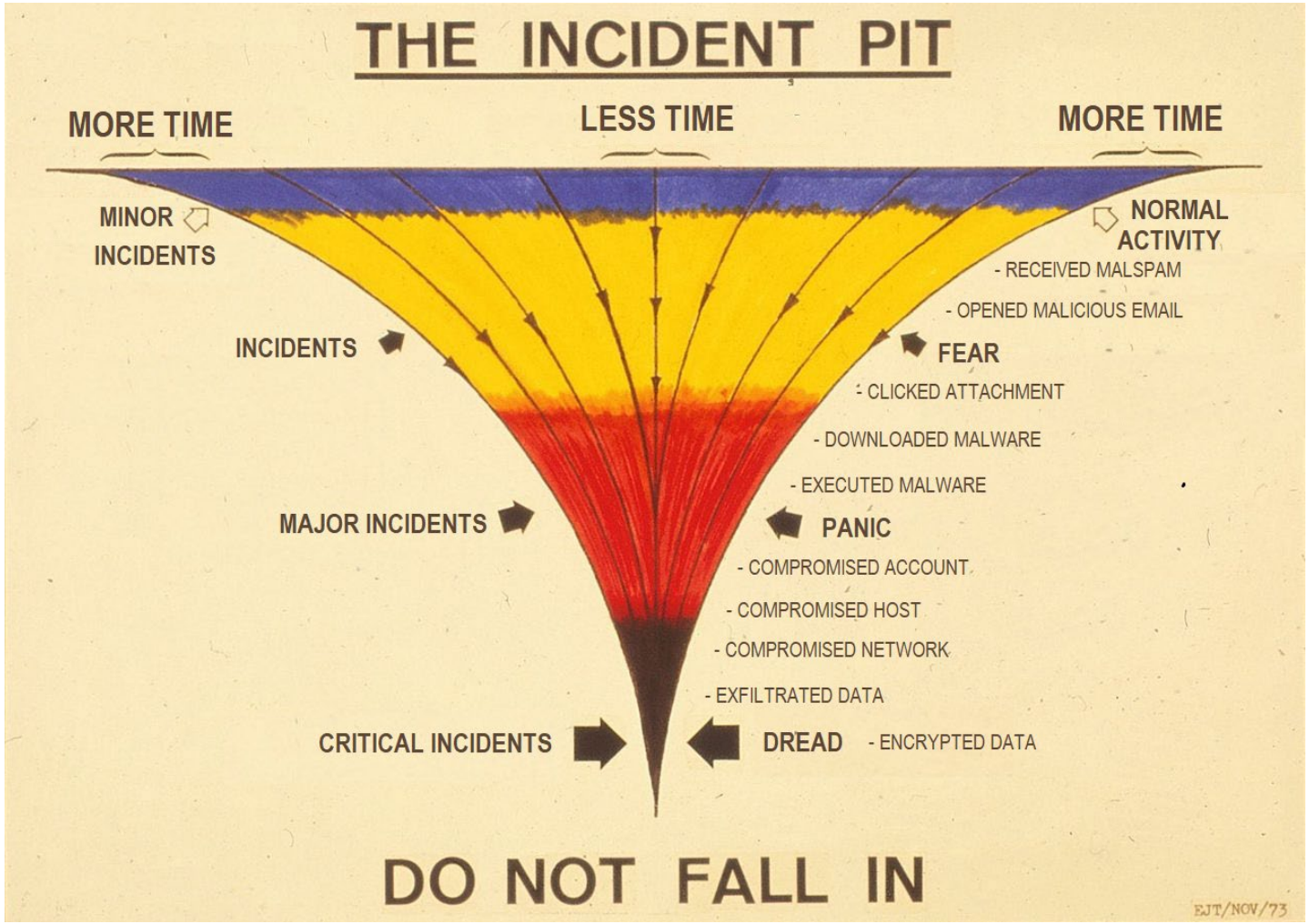




AUSCERT

Incident Pit – Cybersecurity

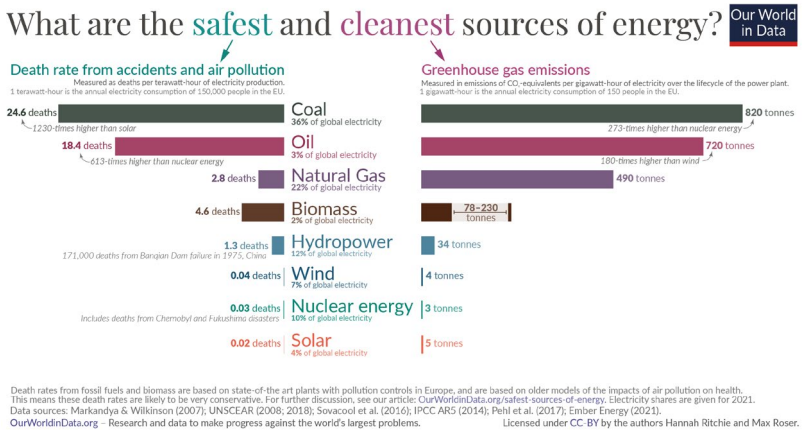


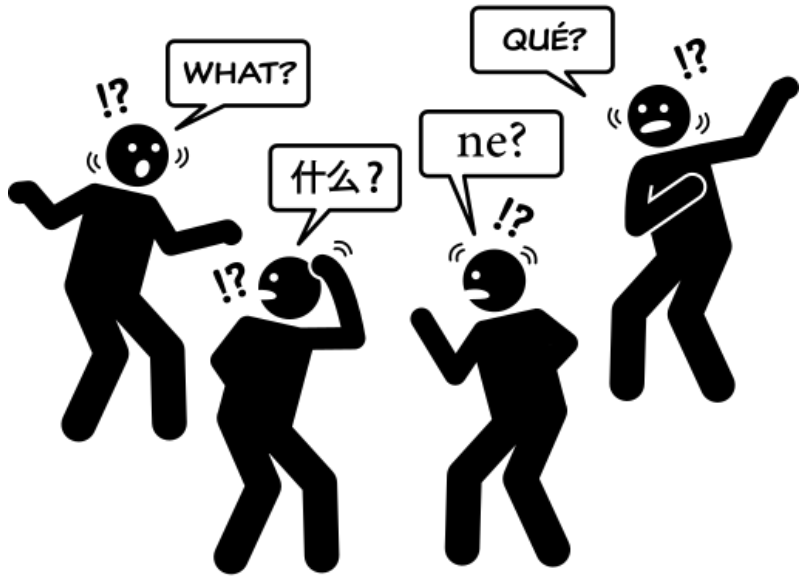


AUSCERT

Disasters are a group effort

- Routine check to see if emergency cooling would work
  - Power Outage
- During test there is a power surge
- Control can’t shut the reactors
- Steam Build up in on reactor
- Roof blown off
- Core exposed
- Material released

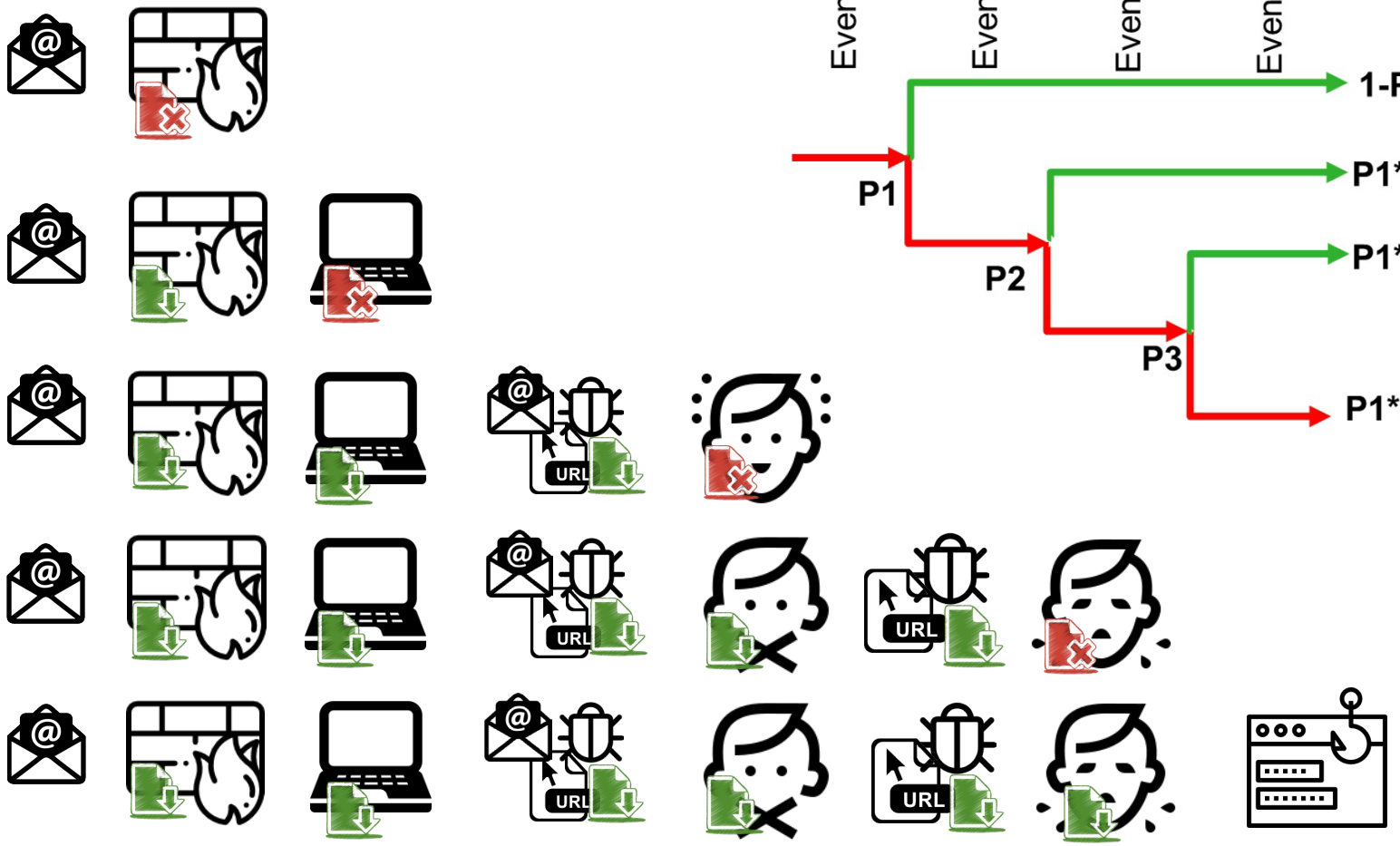




AUSCERT

Progression of Phish

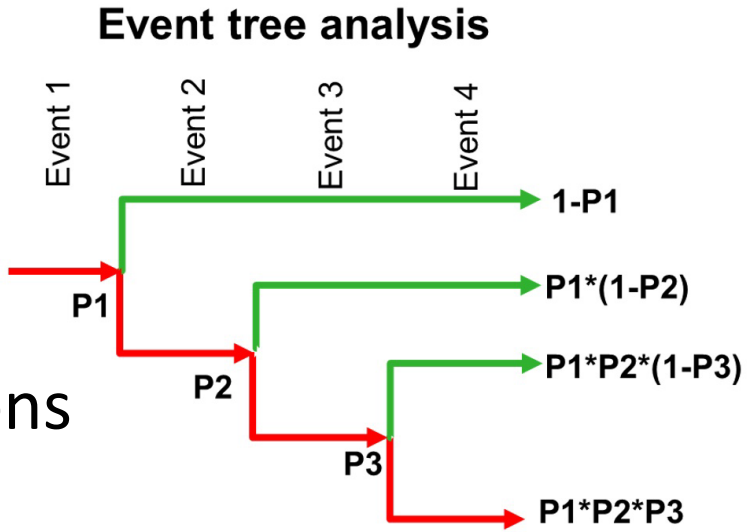
Each stages have tell tale signs



AUSCERT

Compromise is a Group effort

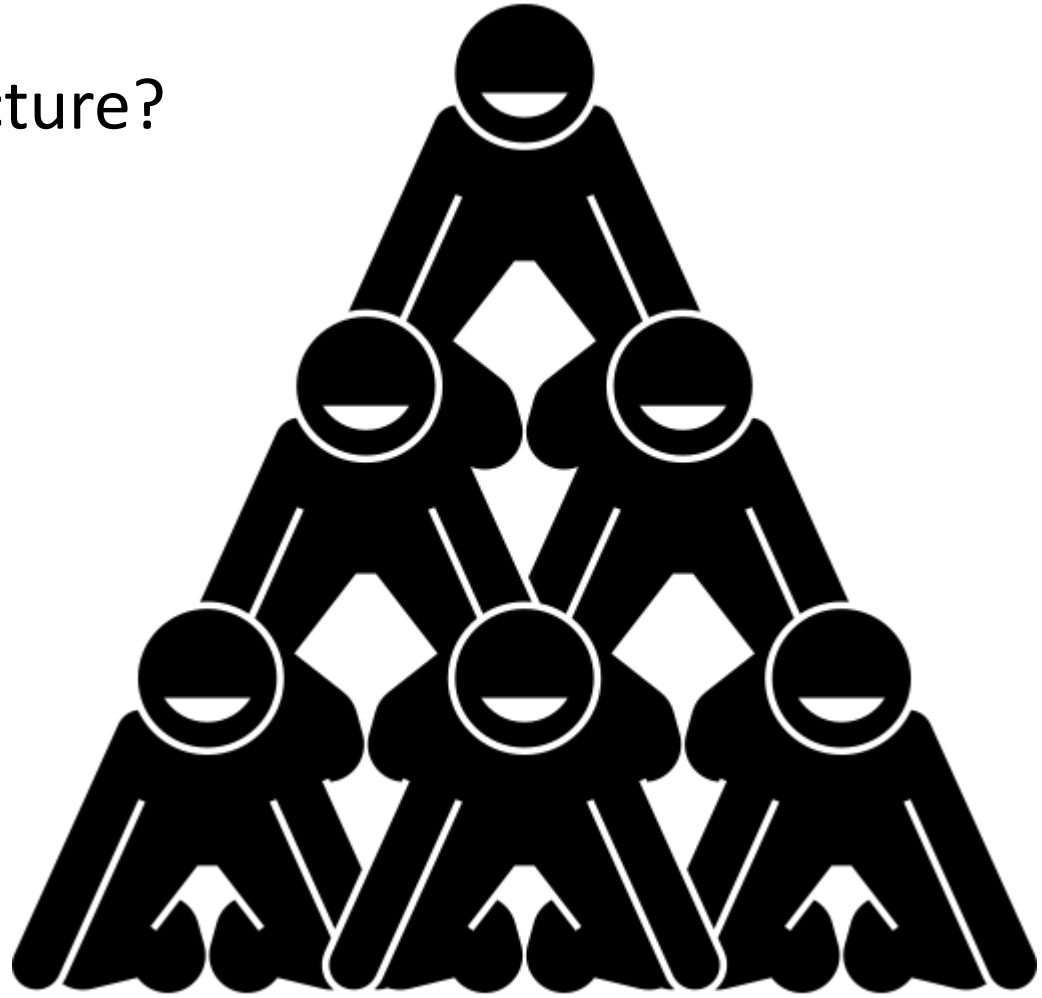
- Vendor Mail protection
- Internal spam filters and solutions (DMARC, DKIM, SPF etc…)
- SOC Threat hunting
- Suspicious email and attachment notification
- Allowing macro
- Report of execution
- Blacklisting by domain age/reputation
- End point scanning solution



AUSCERT

Disasters are avoided by group effort

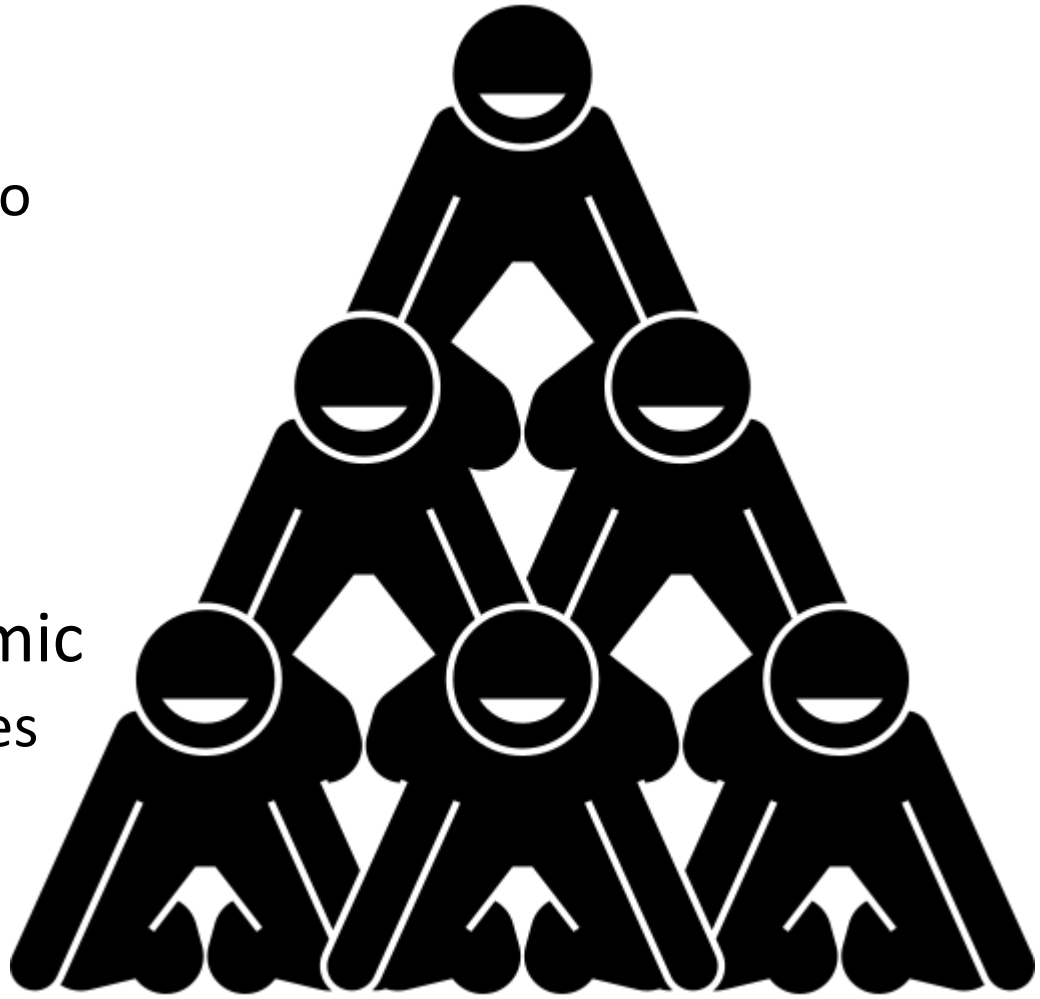
- What do you see in this picture?



AUSCERT

Disasters are avoided by individual effort of the group

- Accomplish a task
  - Something they could not do themselves
- Each Manage a risk
  - From getting squashed
  - To falling
- Each understand the dynamic
  - Individual compensate issues
  - Understand the main idea the master plan

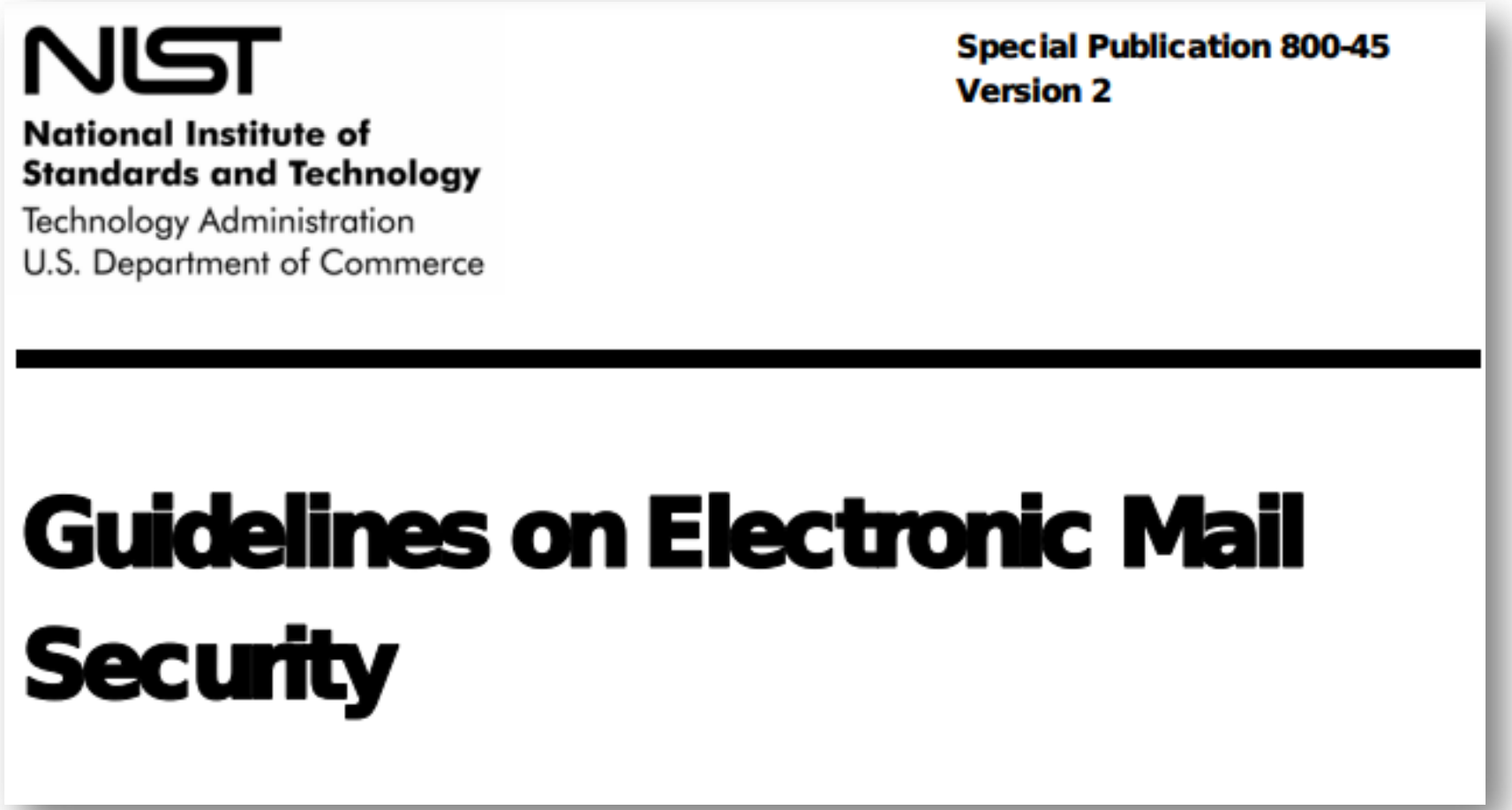


Phish - A few examples

- Policy on email use
- Policy on acceptable risk in use of emails
- Policy on contacting LEA
- Expectation on technical protection (Security architecture)
- Vendor email protection solution monitoring
- Training for SOC analyst
- Incident response plan (including phish and malspam)
- User Awareness training/testing/training
- Asset recovery process (Identity, Data, Money)

NIST - Recommendations

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-45ver2.pdf => 139 pages



NIST

National Institute of Standards and Technology

Technology Administration

U.S. Department of Commerce

Special Publication 800-45

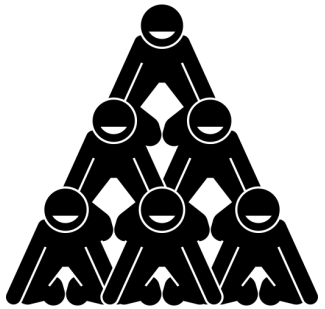
Version 2

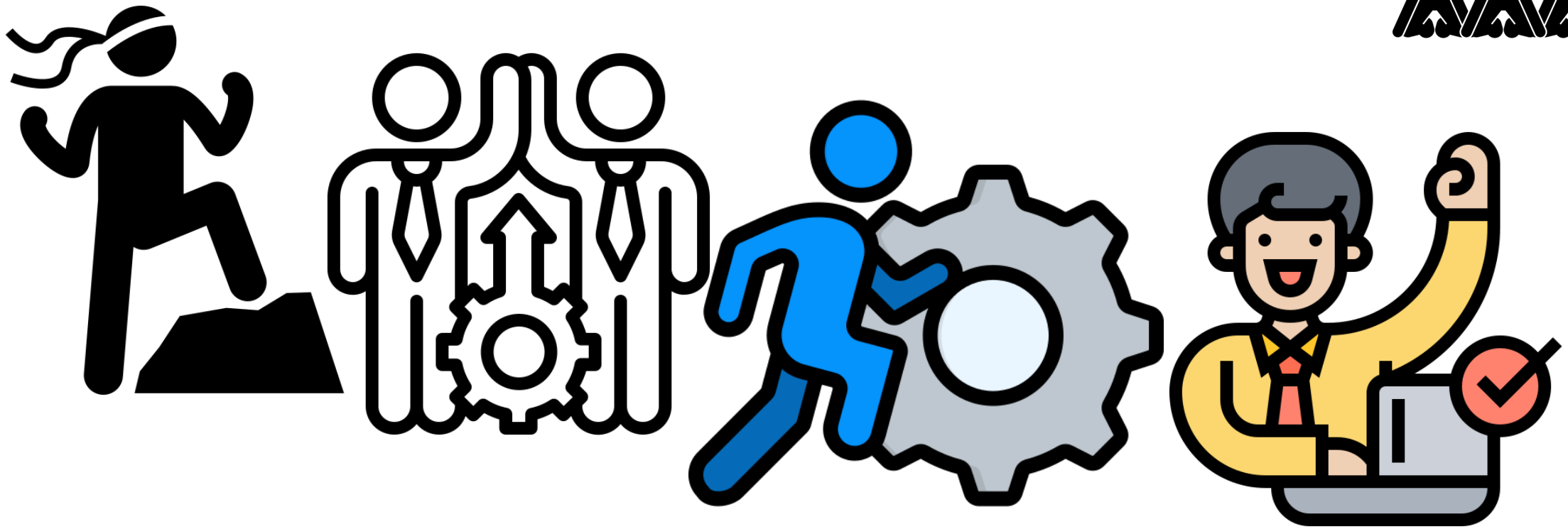
Guidelines on Electronic Mail Security

Application internally and restriction

AUSCERT

It is a group effort

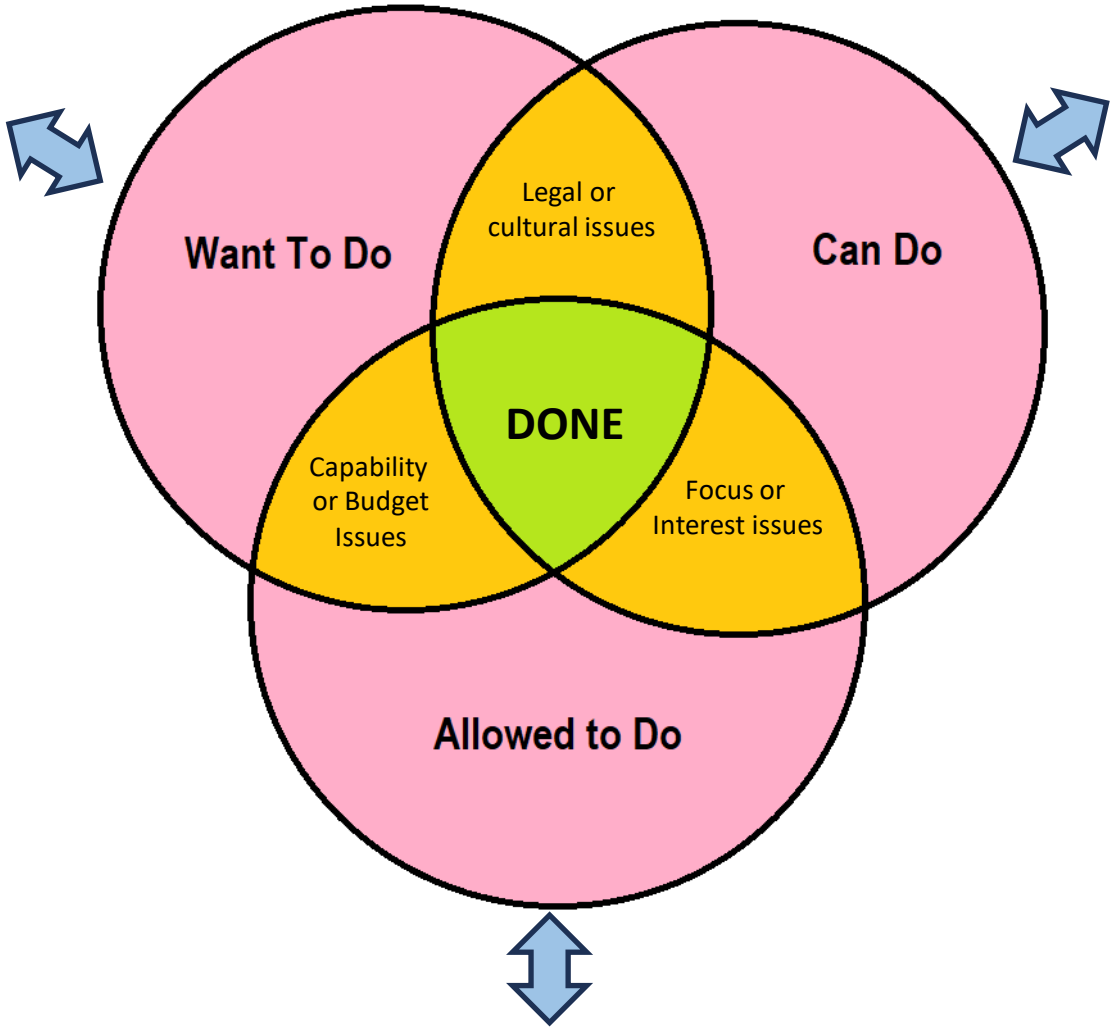




IDENTIFY DETECT PROTECT RESPOND RECOVER

GOVERN

Pressures on what you can (roll out)/(do)



AUSCERT

Risks of CSF incorporated

- Needs of focus and want to write up according to a framework
- Need ability to make policy procedures, instruction and training
- Need to get the culture to accept formalization

- Perhaps legal tools helps in effort of sourcing focus, ability
  - Mandatory Breach Notification (OAIC)
  - Security of Critical Infrastructure Act 2018 (the SOCI Act)
  - “ASIC coming for poorly prepared companies”(19th Sept 2023)

Risks make an organisation work

https://www.youtube.com/watch?v=OGspaYt02Os

Risk, nothing gets done without it!

- All activity has a risk.
  - They can succeed, and fail
- Activities are pursued for their benefits
  - Tangible and Intangible
- Aim to get a positive return on balance of many runs X=(N+M)
  - Return = (N) [Reward of success] – (M) [Cost of failure]
- Aim is to reduce the overall cost of failure to get +’ve return

AUSCERT

Simple Analogy

- Rules
  - Success = 1
  - Failure = 1
  - Note: Cost of run is not included
- Return = (N) [Reward of success] – (M) [Cost of failure]
- Coin Toss N=M Breakeven

- Buttered toast* = M > N Lose

* Buttered toast always seem to land on the buttered side

Email – Simplified example

- Gain
  - Ability to innovate with more people
  - Ability to make more contracts with more clients
  - Ability to reduce cost with more suppliers
- Cost of operation
  - Paid service and maintenance
  - **Cyber security controls**
- Cost
  - Intellectual theft, leakage (non cyber related)
  - Fraudulent transactions (non cyber related)
  - **Cybersecurity attacks**
    - **(Wide and varied costs)**

Phishing

- https://attack.mitre.org/techniques/T1566/
- Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering…
- …Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems…

- Things to read from MITRE ATT&K
  - Procedure Examples
  - Mitigations
  - Detection

T1566 – Procedure Examples

Procedure Examples

ID	Name	Description
G0001	Axiom	Axiom has used spear phishing to initially compromise victims.[8][9]
G0115	GOLD SOUTHFIELD	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines.[10]
S0009	Hikit	Hikit has been spread through spear phishing.[9]
S1073	Royal	Royal has been spread through the use of phishing campaigns including "call back phishing" where victims are lured into calling a number provided through email.[11][12][13]

T1566 – Mitigation

Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can automatically quarantine suspicious files.
M1031	Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.
M1021	Restrict Web-Based Content	Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
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.[14] [15]
M1017	User Training	Users can be trained to identify social engineering techniques and phishing emails.

T1566 – Detection

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 phishing messages to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.[14][15] URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.
DS0022	File	File Creation	Monitor for newly constructed files from a phishing messages 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.[14][15]
		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.

AUSCERT

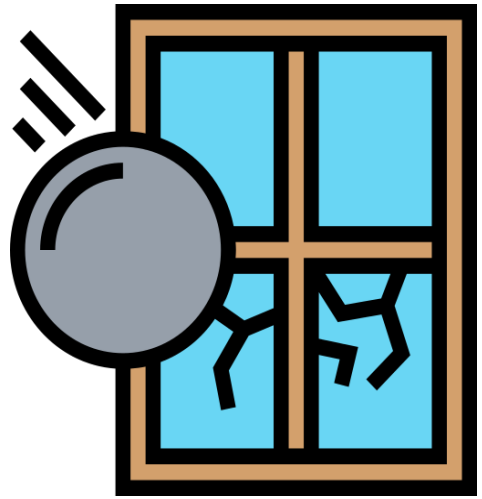
ATT&CK®

ATT&CK Framework

- MITRE ATT&CK® is a globally-accessible **knowledge base** of adversary **tactics** and **techniques** based on real-world observations. The ATT&CK knowledge base is used as a **foundation** for the development **of specific threat models** and methodologies in the private sector, in government, and in the cybersecurity product and service community.

- With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is **open and available** to any person or organization for use at **no charge**.

AUSCERT

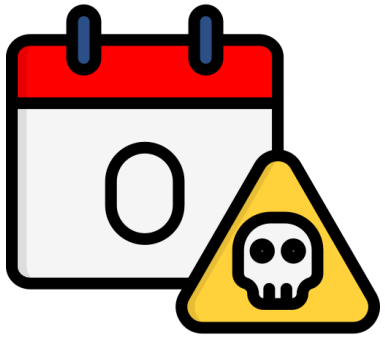


Revision
Threats-Vulnerabilities-Risk

AUSCERT

Vulnerability

- The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.



AUSCERT

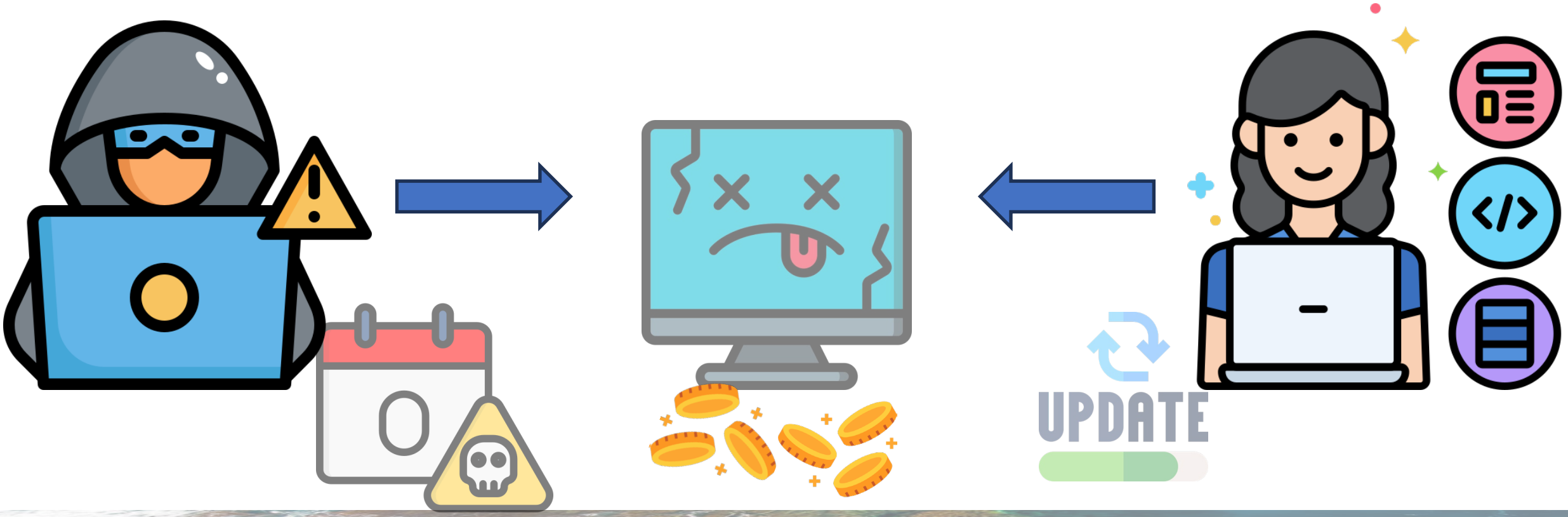
Threat

- a person or thing likely to cause damage or danger.

AUSCERT

Risk

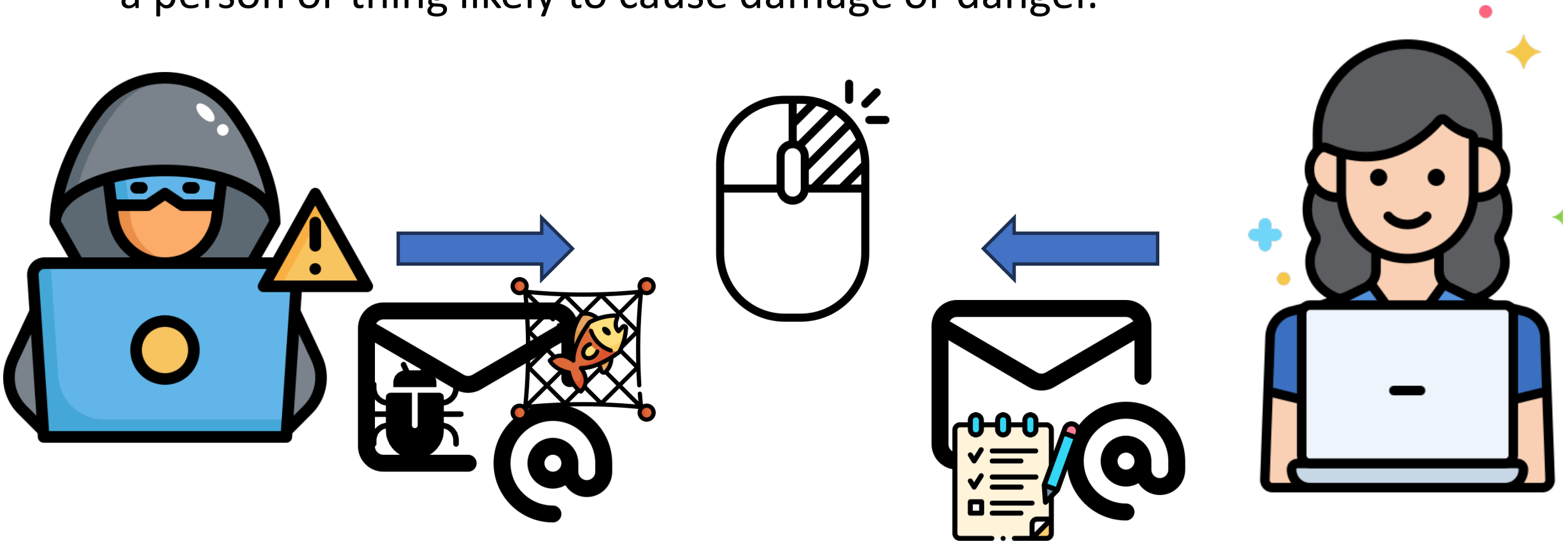
- a person or thing likely to cause damage or danger.



AUSCERT

Risk

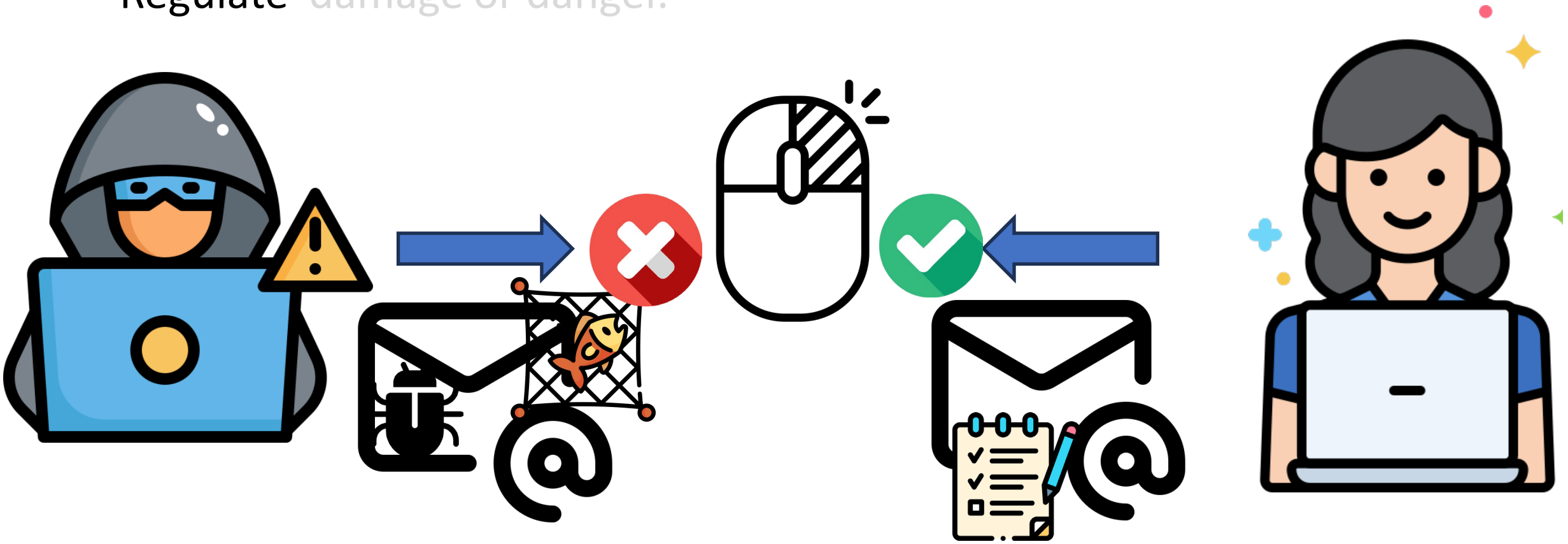
- a person or thing likely to cause damage or danger.



AUSCERT

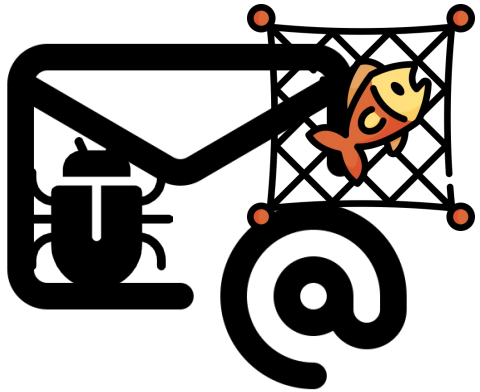
Controls

- Regulate damage or danger.



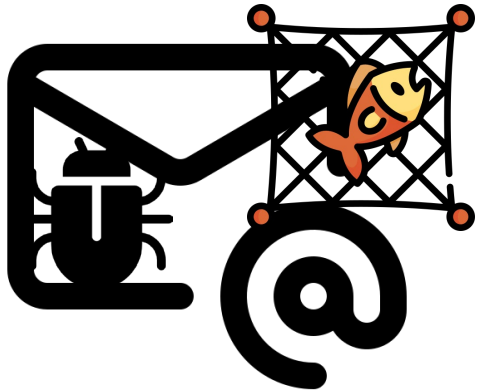
Controls - Detect

- Application Log Content
- File Creation
- Network Traffic Content
- Network Traffic Flow



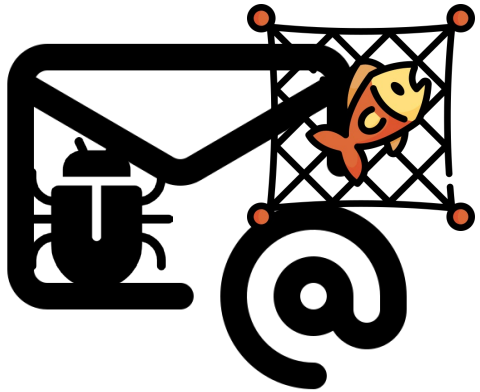
Controls - Prevent

- Reduce the accounts
- Block list
- Internal Advisory



Controls - Correct

- Back up
- External Comms (PR)



AUSCERT

Risk - Avoid

- Removal of email
  - Replace with something other?

AUSCERT

Risk - Mitigate

- Antivirus/Antimalware
- Network intrusion Prevention
- Restrict web-Based Content
- Software Configuration
- User Training

AUSCERT

Risk - Transfer

- Get Insurance
- Get Managed service Provider

AUSCERT

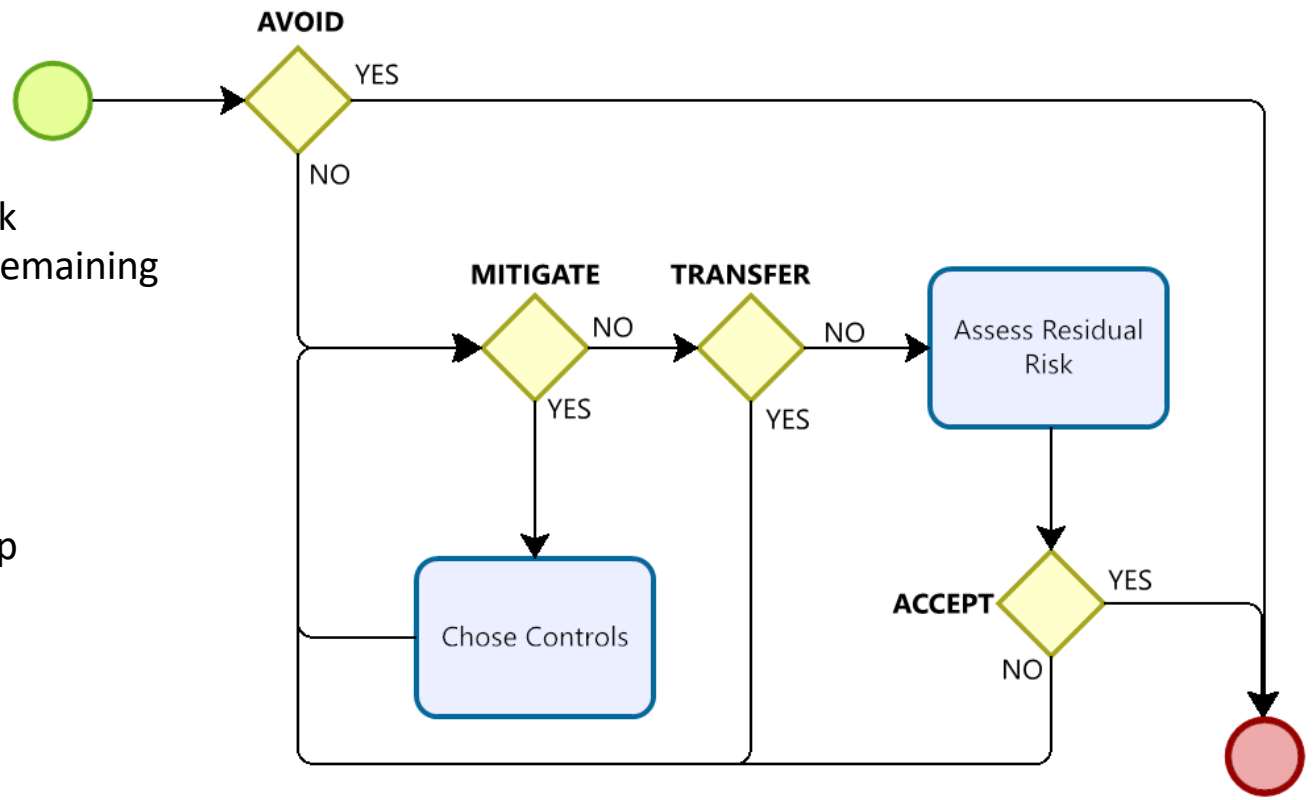
Risk - Accept

- Accept the final risk

AUSCERT

General Approach to RISK

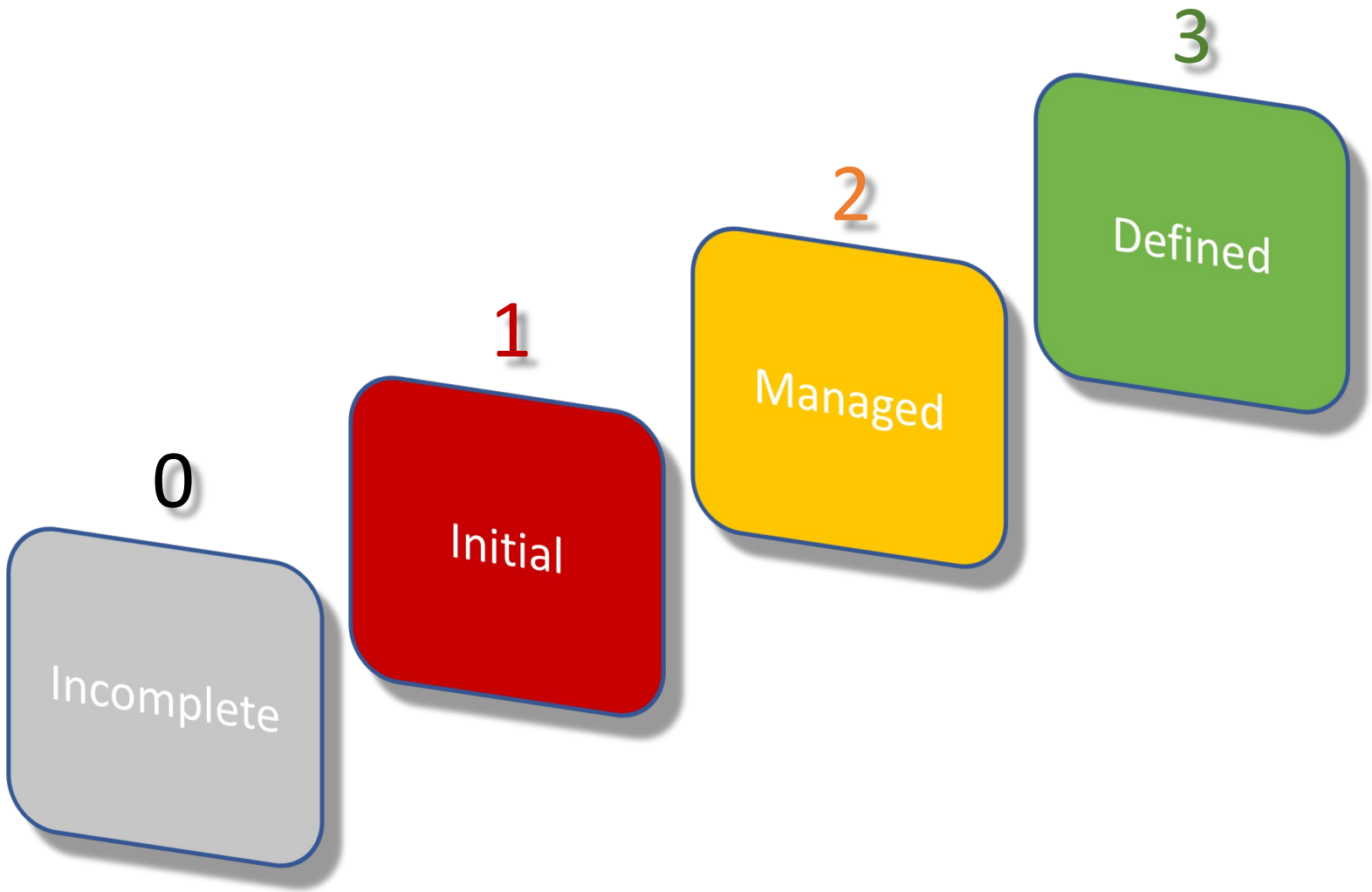
- Can it be AVOIDED completely.
- Can it be MITIGATED with controls
  - If YES then
    - List controls, cost, and expected residual risk
    - Chose controls, recalculate the overall risk remaining
    - Move to next step
  - If NO then
    - Move to next step
- Can it be TRANSFERRED
    - Calculate residual risk and move to next step
- Can it be ACCEPTED
  - If YES then
    - Monitor actual risk
  - If NO then
    - Get a bigger budget and go back to Mitigation



Qualitative Approach

Risk matrix approach

		Impact			
		None	Small	Moderate	High
Frequency	Very High		High	Very High	Very High
	High		Moderate	High	Very High
	Moderate		Low	Moderate	High
	Low		Low	Low	Moderate
	None	No Risk			



Levels of Process Capability

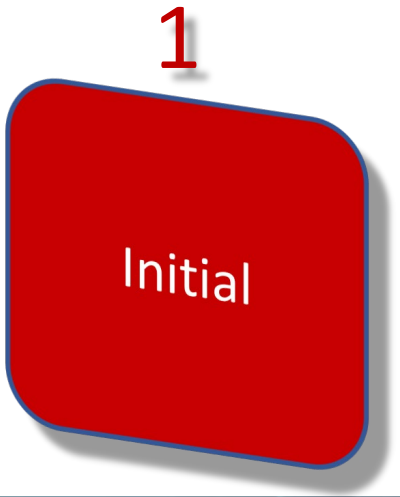
Incomplete

- Indication
  - This is not the first time you heard about this topic
  - It does get, it just gets done by someone ?
  - Not sure who to ask
  - No documents to refer to
  - Not sure if it is effective

0

Initial

- Indication
  - You know someone in your organisation who knows.
  - You seen and know it was and is being done.
  - It is done or handled when it happens
  - But there are not documentation and need to ask a given person how it is done
  - Training would require lots of doing and very little formal training



Managed

- Indication
  - You heard and done the training about it
  - Some one is assigned to the task, given time to perform the task
  - Even someone else does it, you could possibly pick it up as there is a set of material that is defined for training
  - There are reports about the topic

Defined

- Indication
  - You performed the periodic training and got a score recorded
  - Someone is assigned to the task
  - You could do the task but need to read the written instructions
  - You know where the instructions are
  - The instructions are reviewed periodically for suitability
  - The instructions are also authorized by management

  - There is a policy about this process
  - This follows a framework

3

Defined

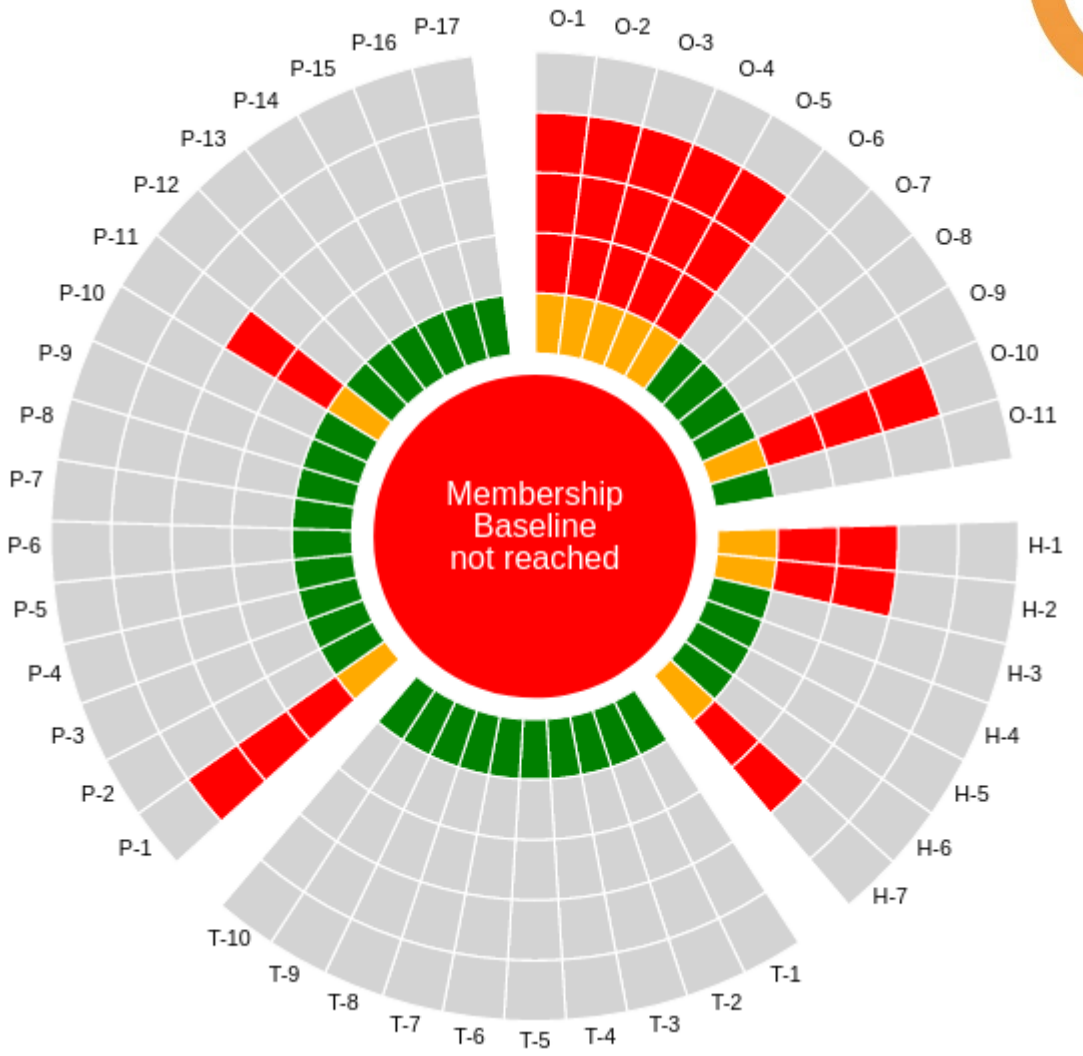
Open CSIRT Foundation

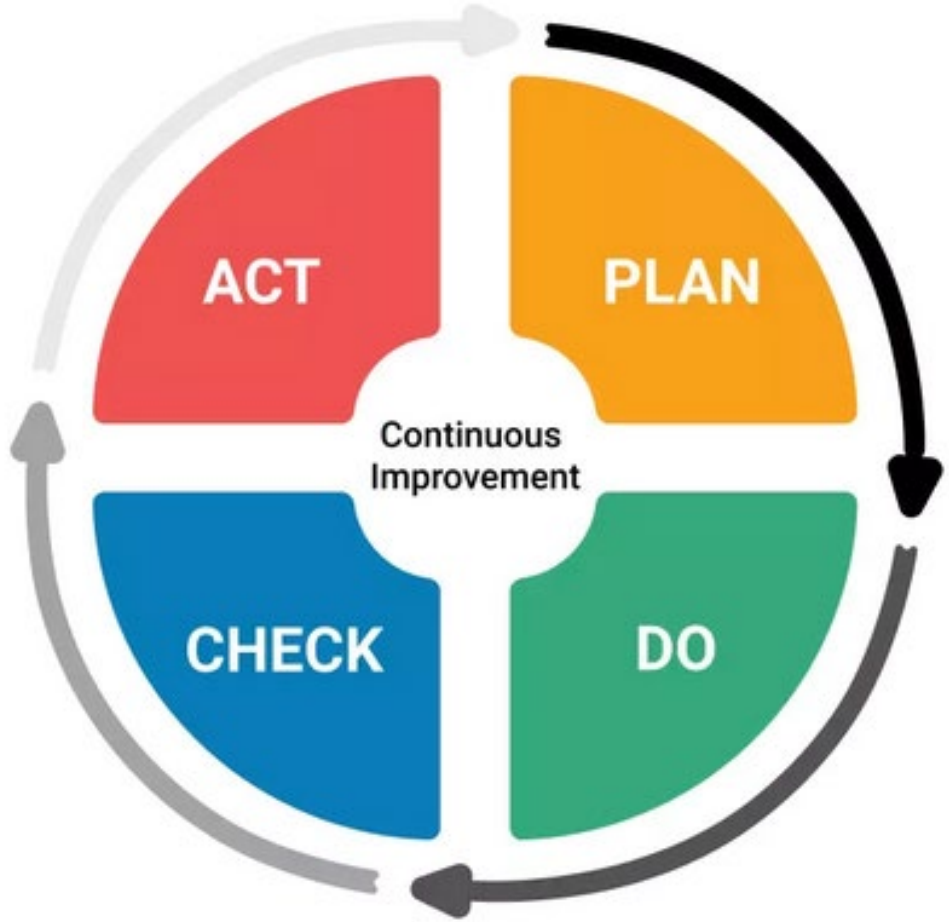
AUSCERT

SIM3

- Organisation
- Human
- Tools
- Processes

- 0 Never really discussed
- 1 Basic understanding
- 2 written but not formal
- 3 written and approved
- 4 written, approved, reviewed



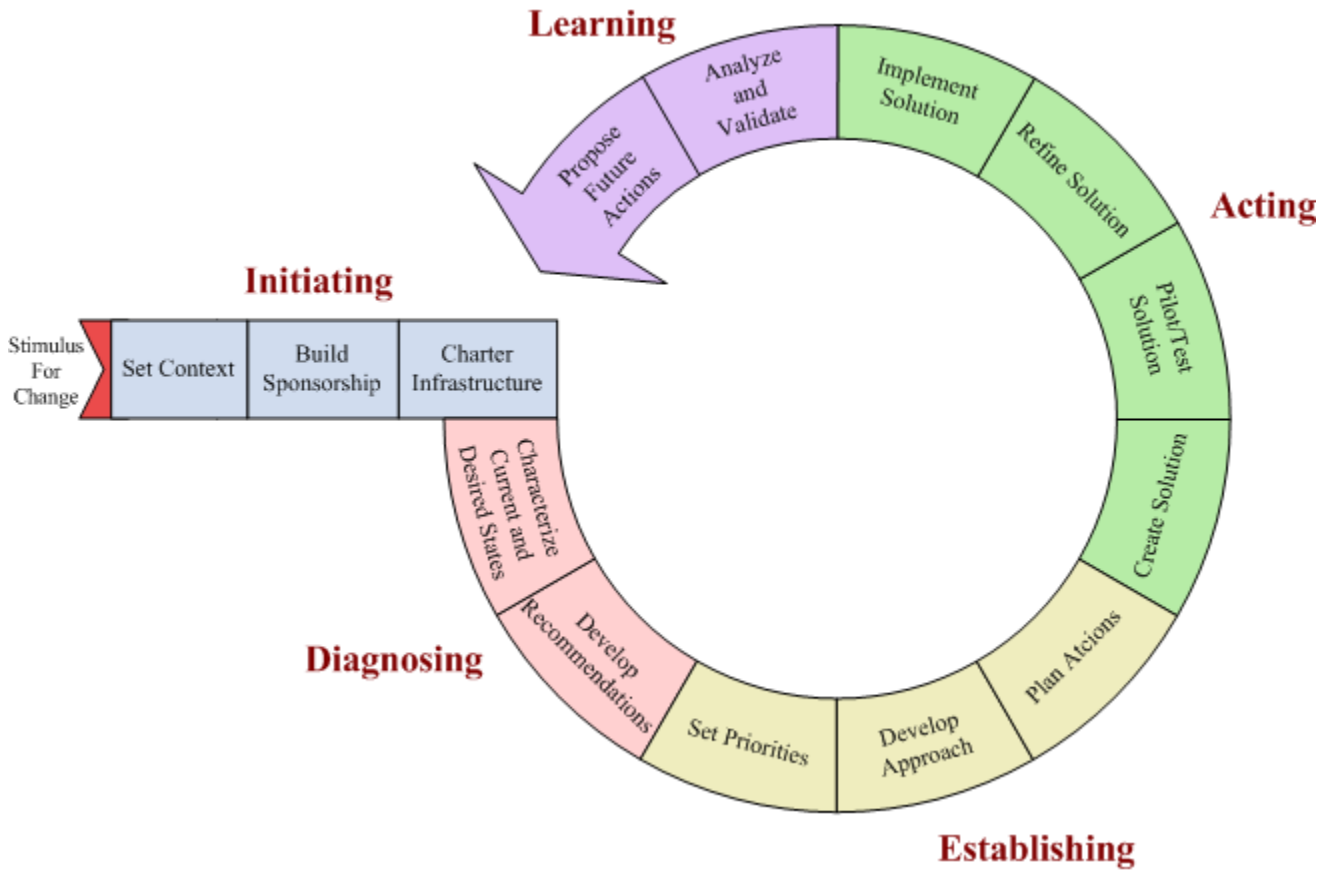


Improvement is Iterative

Deming-Shewhart Model

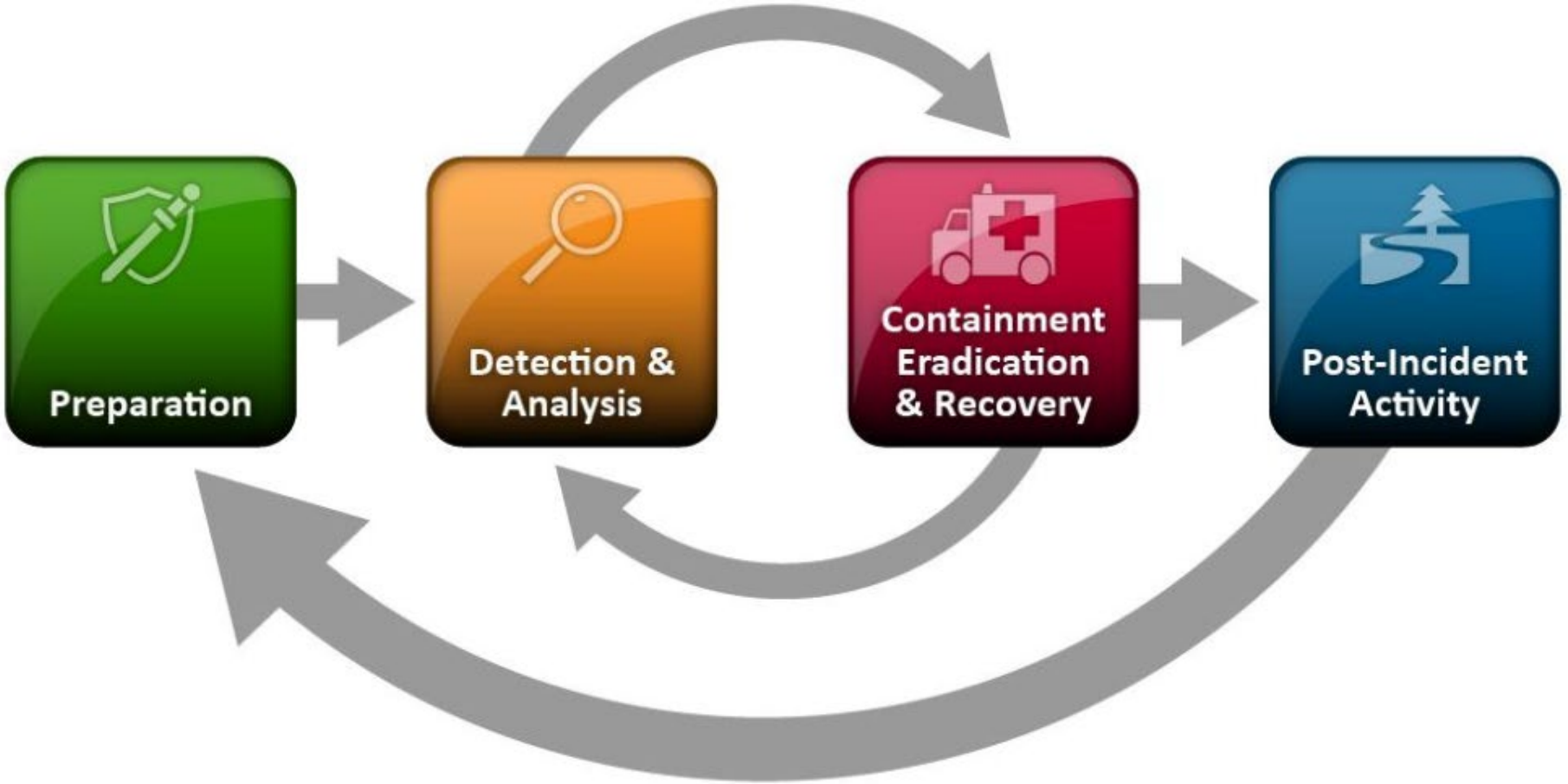
ISO PDCA Model

CMMI IDEAL Model



AUSCERT

NIST



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

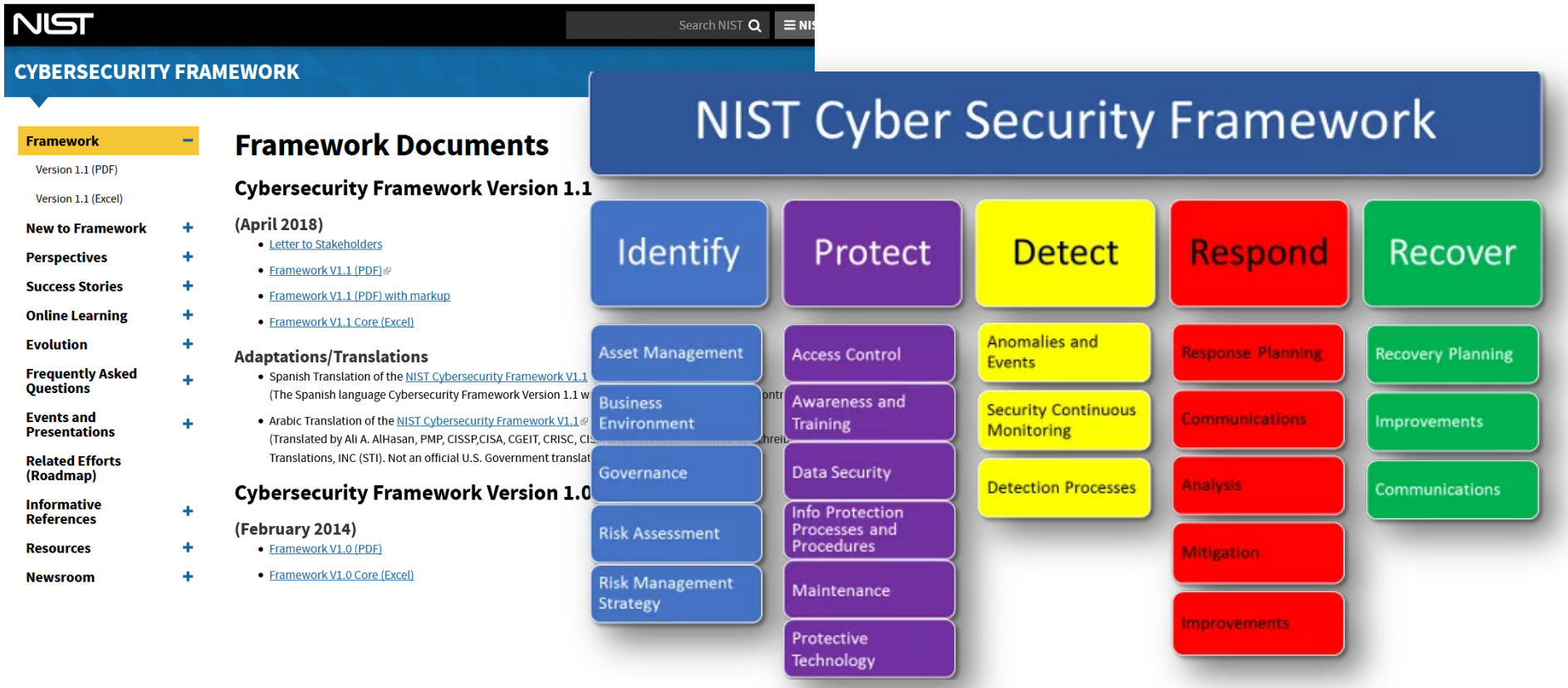
AUSCERT

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework/getting-started/quick-start-guide

AUSCERT

Cybersecurity Framework



AUSCERT

NIST Cybersecuritv Framework 1.0

But.. “Each need to understand the main idea, the master plan”

AUSCERT

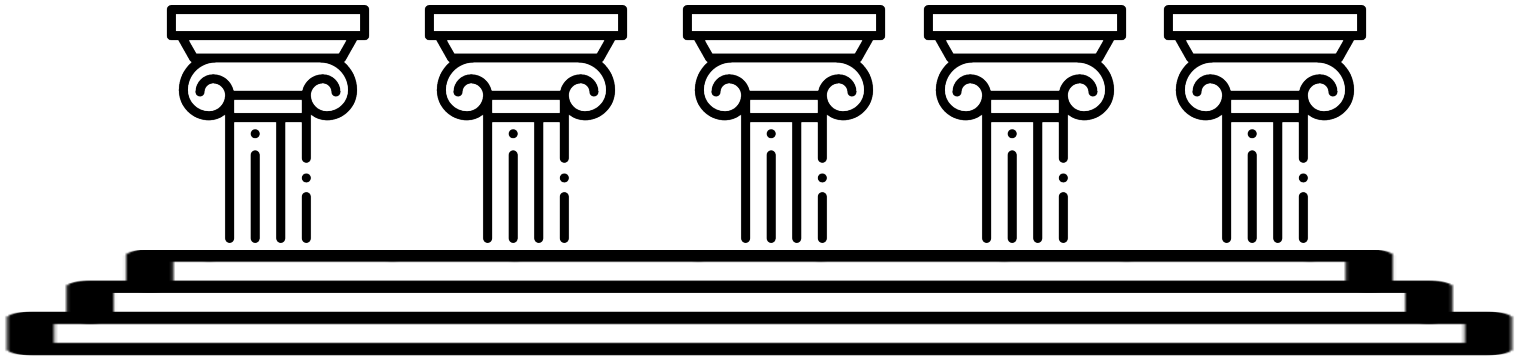
NIST Cybersecurity Framework 2.0

“Each understand the main idea, the master plan”

AUSCERT

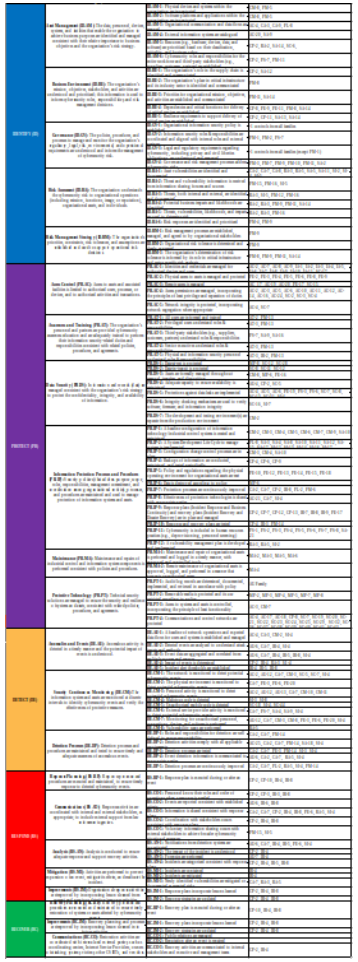
NIST Cybersecurity Framework 2.0

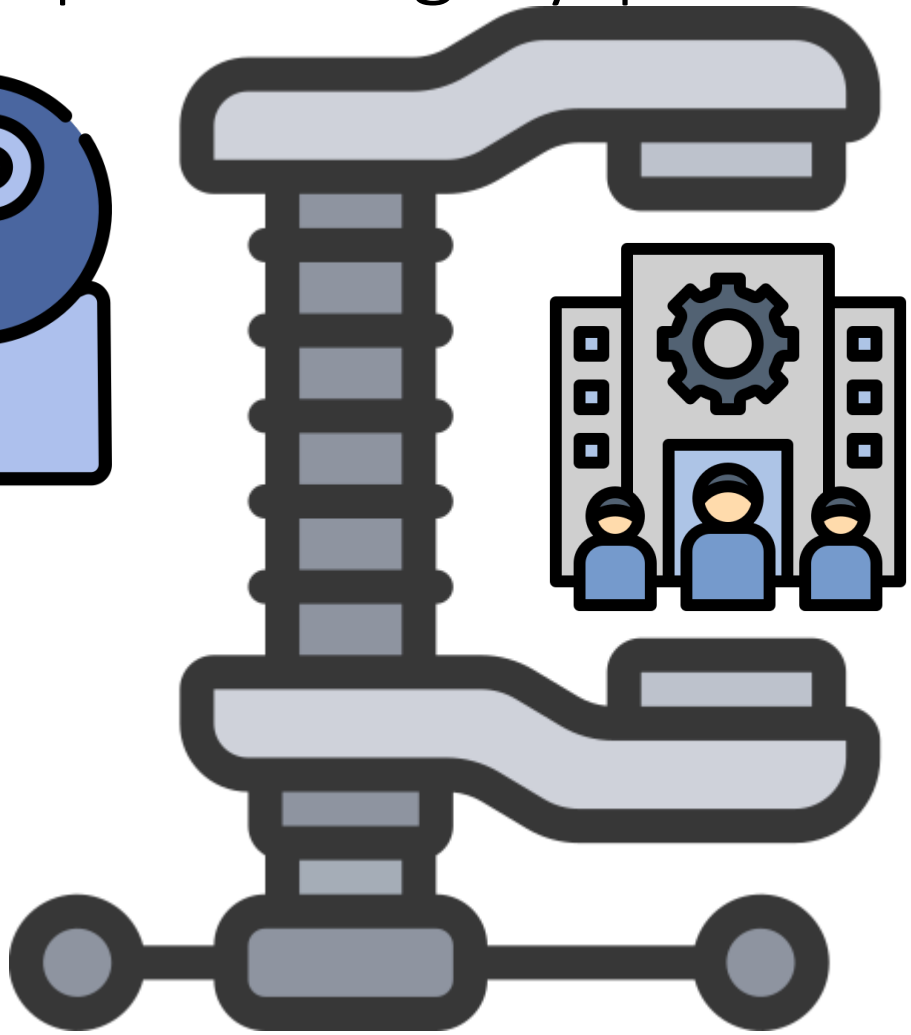
- Scoped expanded for all organisations regardless of type and size.
- Add Govern for senior leadership to the five pillars
  - Identify, Protect, Detect, Respond, Recover
- Added profile to assist applying the CSF to particular situation

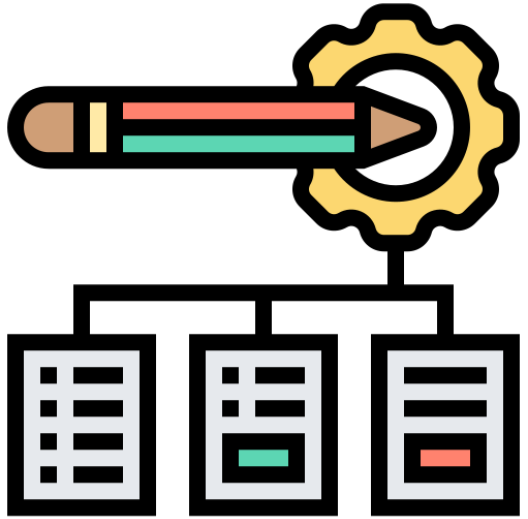


AUSCERT

CSF 1.0 | Category | Subcategory | SP 800-53 Controls

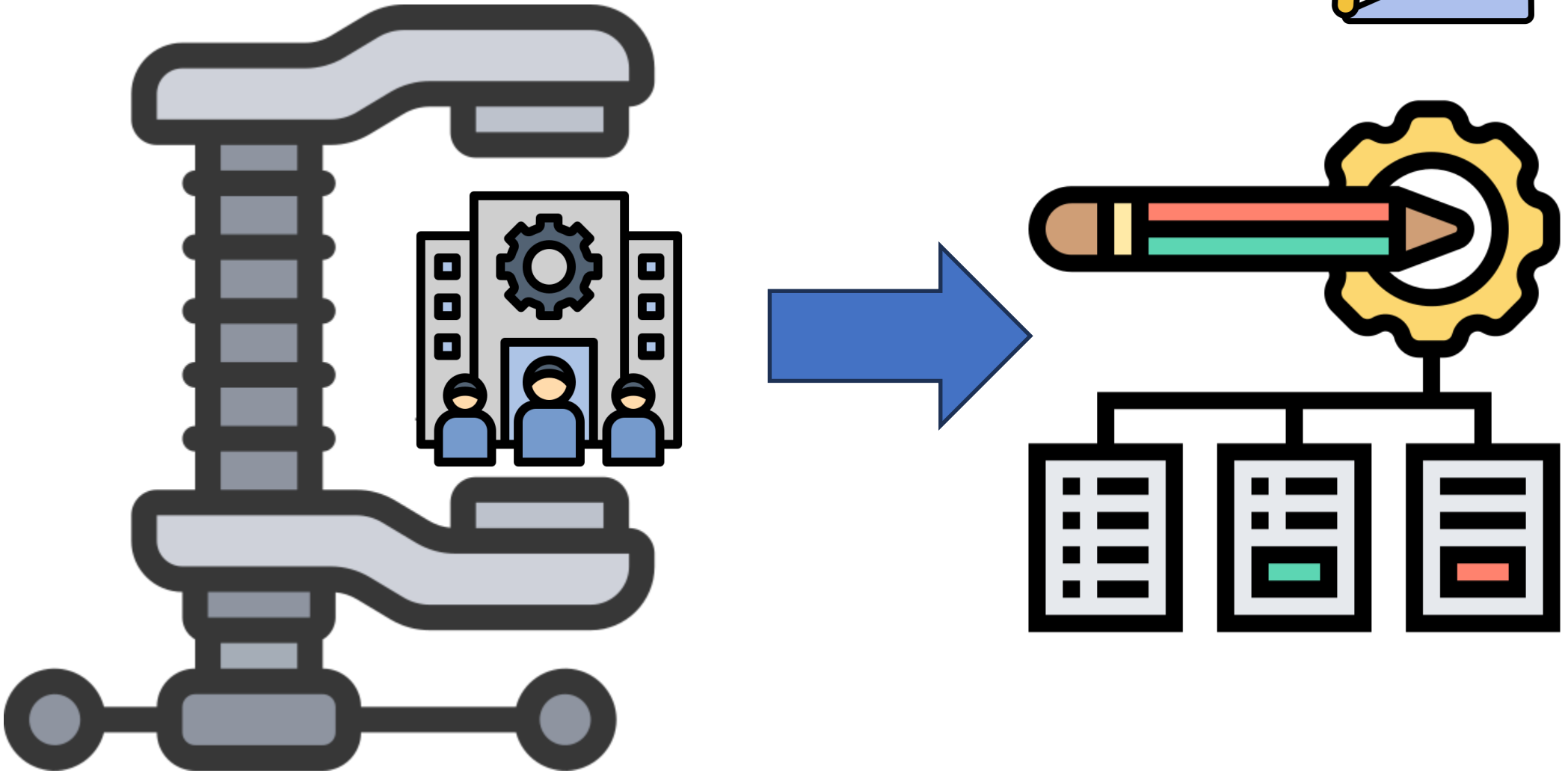






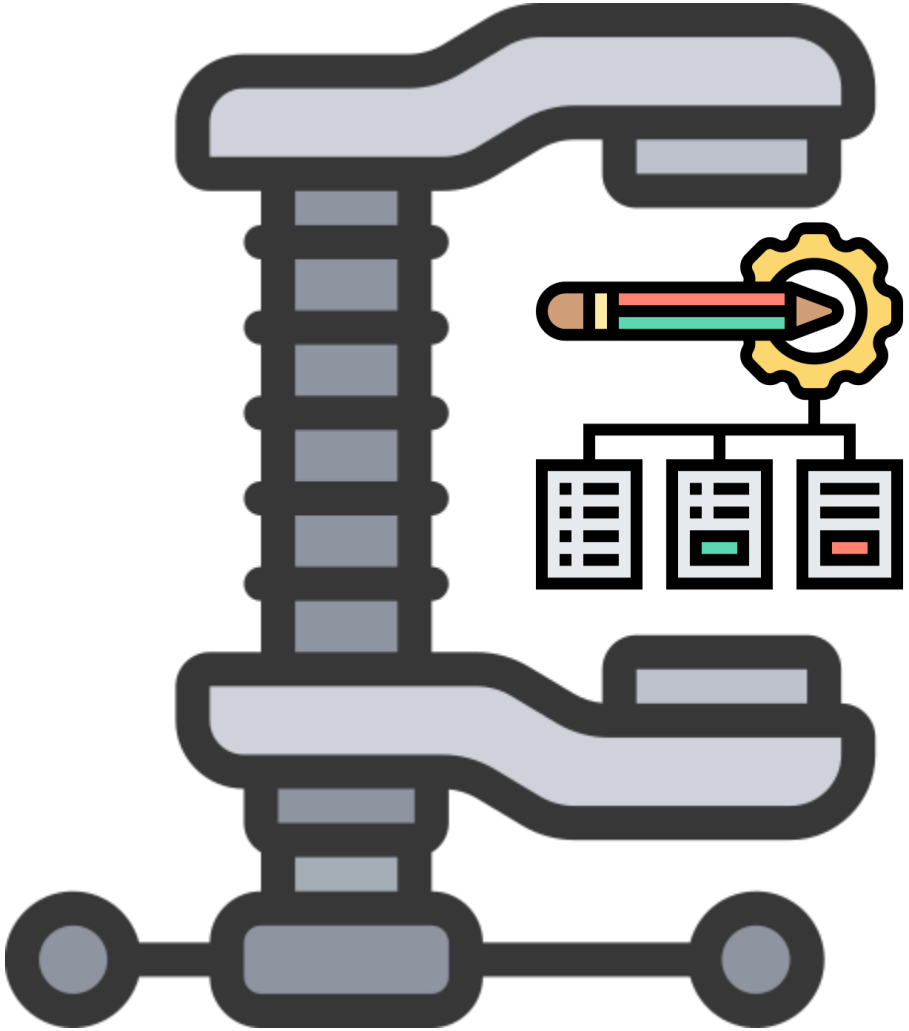
AUSCERT

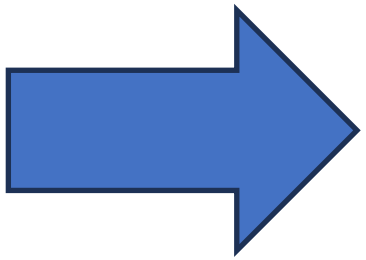
Fit Organisation into a Framework

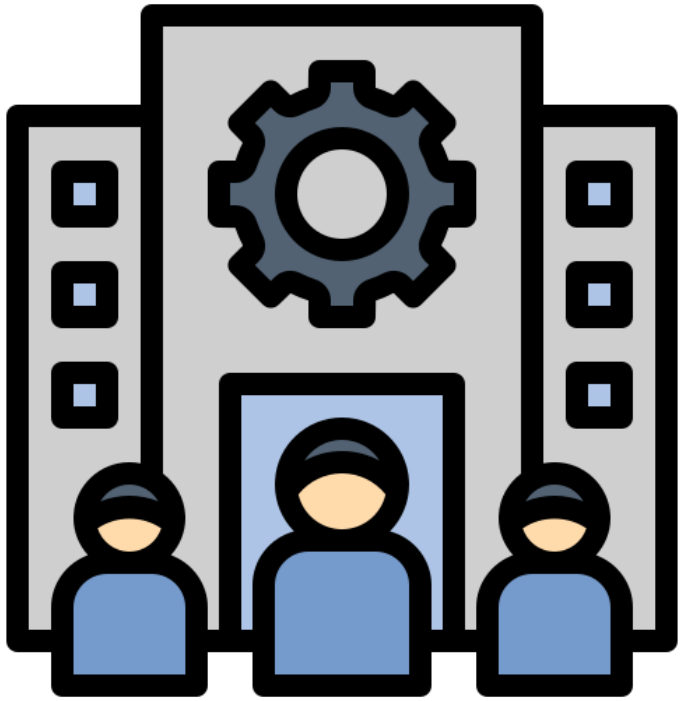


AUSCERT

Fit Framework into an Organisation





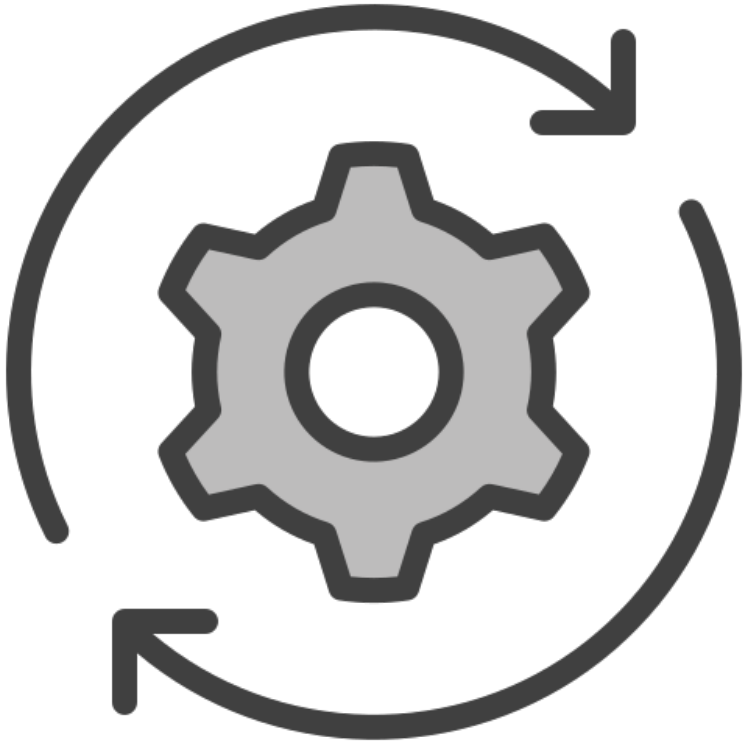


AUSCERT

Profiles for CSF 1.0

- Profiles of industry
  - EV Extreme fast Charging Infrastructure
  - Manufacturing, and Revision 1
  - Election Infrastructure
  - Position Navigation and Timing Services
  - Liquified Natural Gas
  - Hybrid Satellite Network
  - Smart Grid Profile
  - Connected Vehicles Environment
  - Maritime Bulk Liquids
  - Communication Sector

- Profiles of Events
  - Ransom Risk Management
  - BotNet
  - DDos



https://www.nist.gov/cyberframework/examples-framework-profiles

AUSCERT

NIST Cybersecurity Framework 2.0

Summary 1.0

- Identify things to protect you would call asset
- Identify ways to protect these assets (prevent)
- Identify ways to detect these assets are under attack (detect)
- Identify ways to respond to these detection going positive (reduce internally created harm)
- Identify ways to recover (corrective)

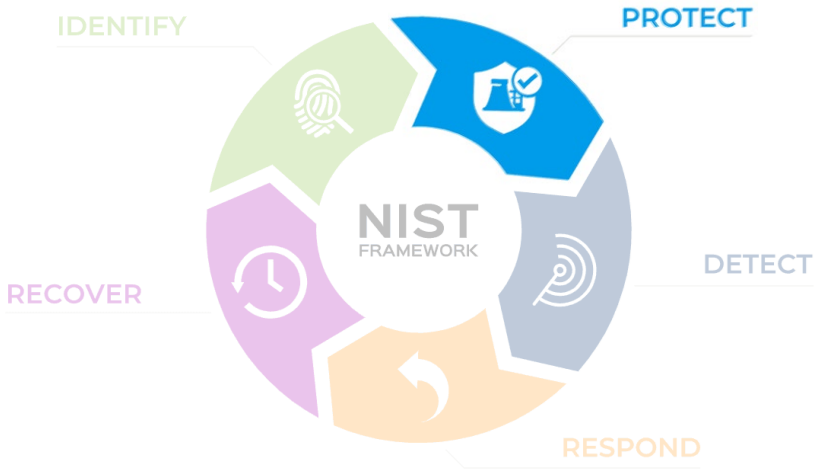
- What's missing for coordination and improvement/dynamic alteration of threat landscape?

AUSCERT

Identify

- Develop an organisational understanding to manage cybersecurity risk to: systems, assets, data, capabilities.
  - Identify critical enterprise processes and assets
  - Document information flows
  - Maintain hardware and software inventory
  - Establish policies for cybersecurity that include roles and responsibilities
  - Identify threats, vulnerabilities, and risk to assets

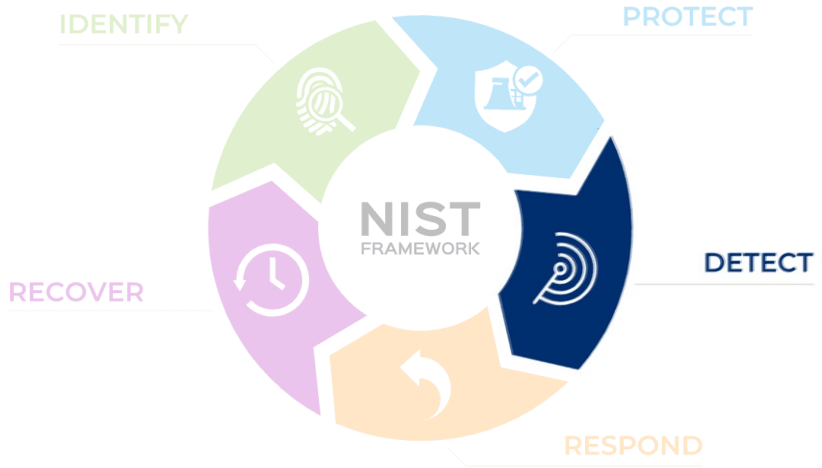
Protect



- Develop and implement the appropriate safeguards to ensure delivery of services
  - Manage access to assets and information
  - Protect sensitive data
  - Conduct regular backups
  - Protect your devices
  - Manage device vulnerabilities
  - Train users

AUSCERT

Detect



- Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
  - Test and update detection processes
  - Maintain and monitor logs
  - Know the expected data flows for your enterprise
  - Understand the impact of cybersecurity events

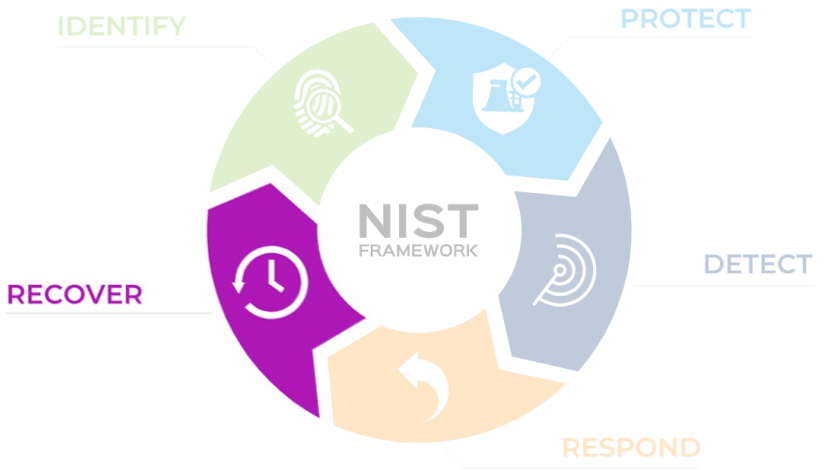
AUSCERT

Respond

- Develop and implement the appropriate activities to take action regarding a detected cyber security event
  - Ensure response plans are tested
  - Ensure response plans are updated
  - Coordinate with internal and external stakeholders

AUSCERT

Recover



- Develop and Implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
  - Communicate with internal and external stakeholders
  - Ensure recovery plans are updated
  - Manage public relations and company reputation

AUSCERT

Govern

- Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy
  - IPDRR has been redefined (slightly)
  - Elements of IPDRR that were govern type were regrouped
  - Some additional items relation to govern has been elaborated

AUSCERT

Summary 2.0

- **Identify**
  Help determine the current cybersecurity risk to the organization
- **Protect**
  Use safeguards to prevent or reduce cybersecurity risk
- **Detect**
  Find and analyze possible cybersecurity attacks and compromises
- **Respond**
  Take action regarding a detected cybersecurity incident
- **Recover**
  Restore assets and operations that were impacted by a cybersecurity incident

- **Govern**
  Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

AUSCERT

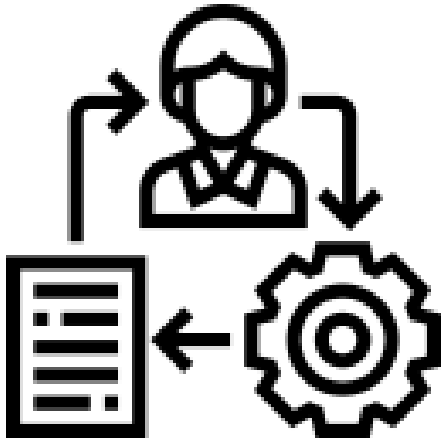
CSF 2.0 Details

- Search term “nist csf 2.0 reference tool”
- Target website : https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters
- Looks Like:

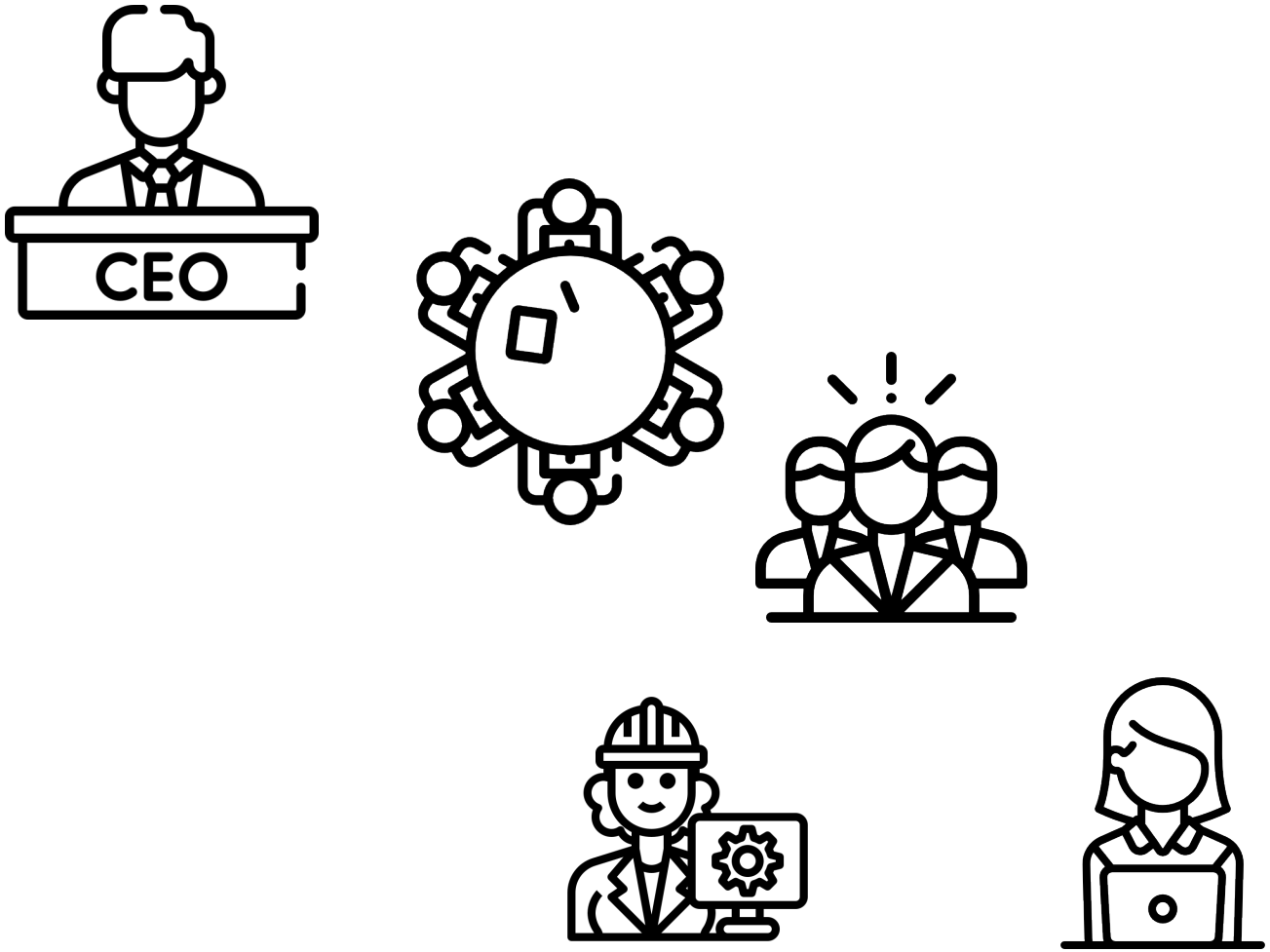
Communication

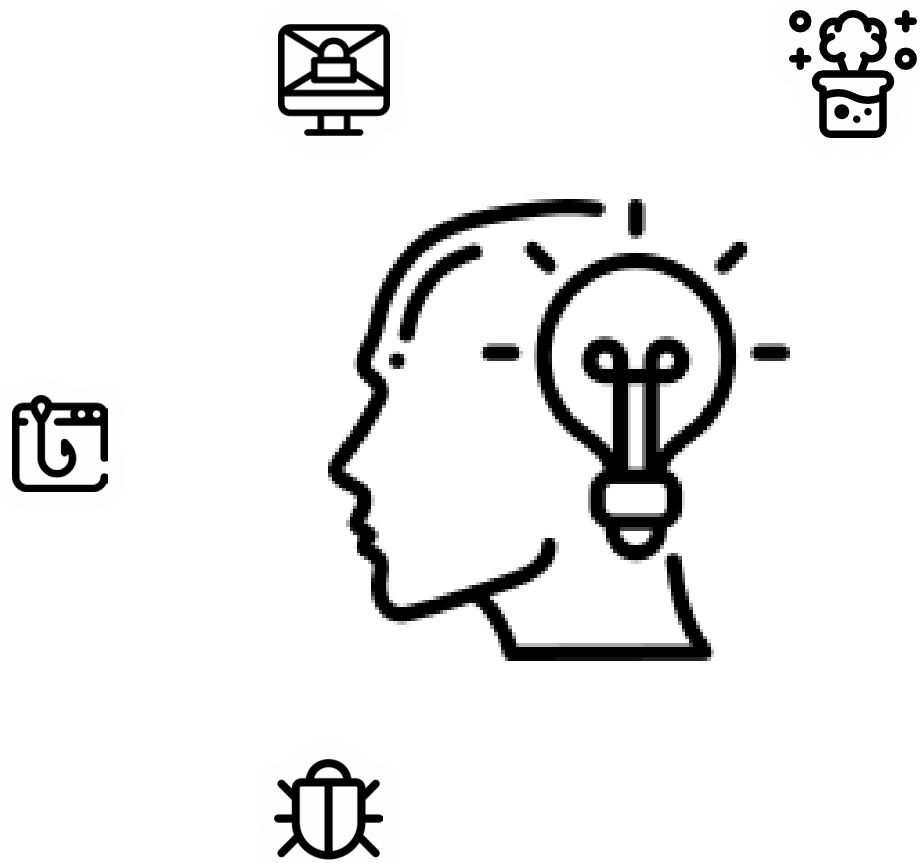
AUSCERT

Message Usefulness



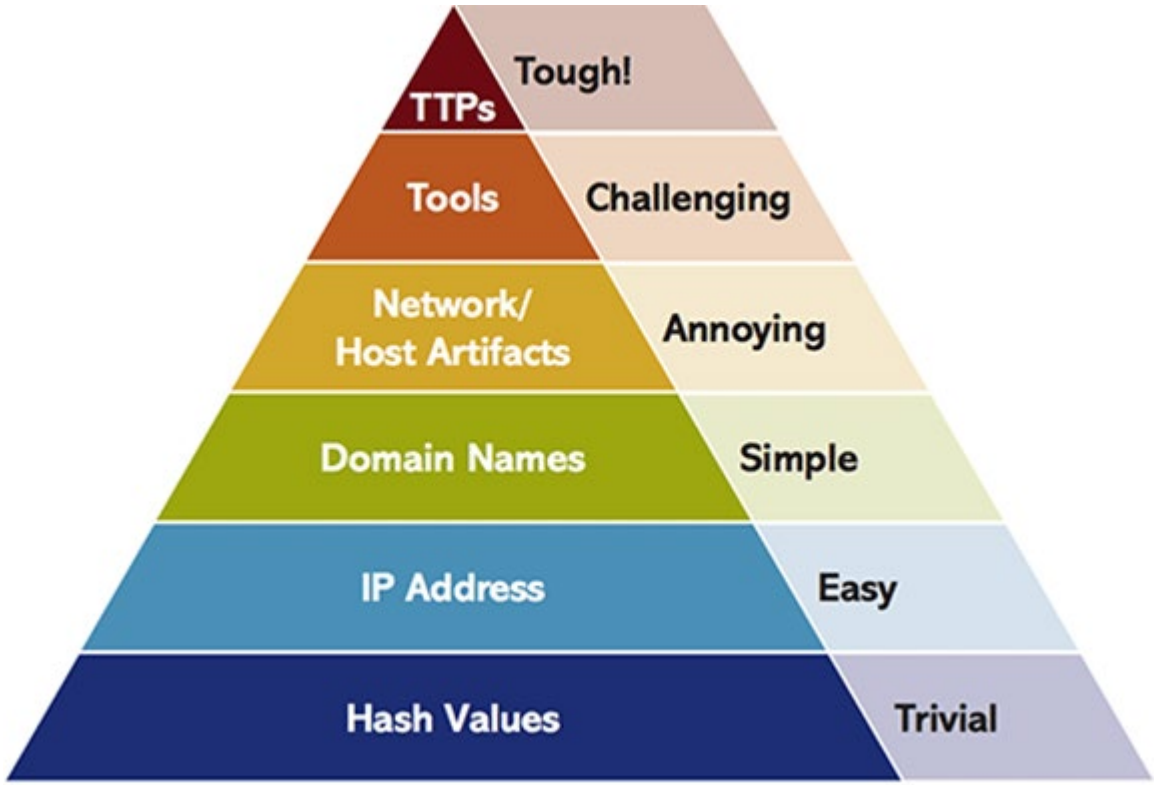
Many Layers “Simultaneously”





Threat Intel

Pyramid of pain



Admiralty Scale

- Reliability
  - A Complete
  - B Usually
  - C Fairly
  - D Not Usually
  - E Unreliable
  - F Not Known

A3

- Credibility
  - 1 Confirmed
  - 2 Probably True
  - 3 Possibly True
  - 4 Doubtful
  - 5 Improbable
  - 6 Not Known

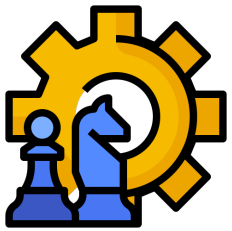
AUSCERT

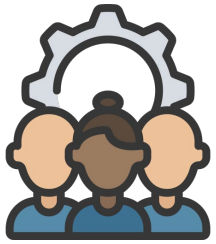
Cyber Threat Intelligence

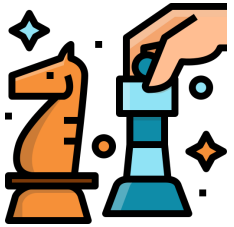
- Types
  - 
    Strategic
    - You need => General Intelligence Requirements
      Information that assist planning of future possible operational threat situations in a predictive manner.
  - 
    Operational
    - You need => Priority Intelligence Requirements
      Information that assist in engaging collective response to ensure operation is protected and can defend from identified threat campaigns.
  - 
    Tactical
    - You need => Specific Intelligence Requirements
      Information that assist in the decision process of detecting and protecting an organisation from a specific threat artefact.

Intelligence requirements

- (GIR) General intelligence requirements
  - Items of interest
- (PIR) Priority intelligence requirements
  - The general question
- (EEI) Essential elements of information
  - Specific questions from the general Q that answers one thing
- Indicators
  - Observables to answer the Specific Question
- (SIR) Specific intelligence requirements
  - Assets that can perform the observations





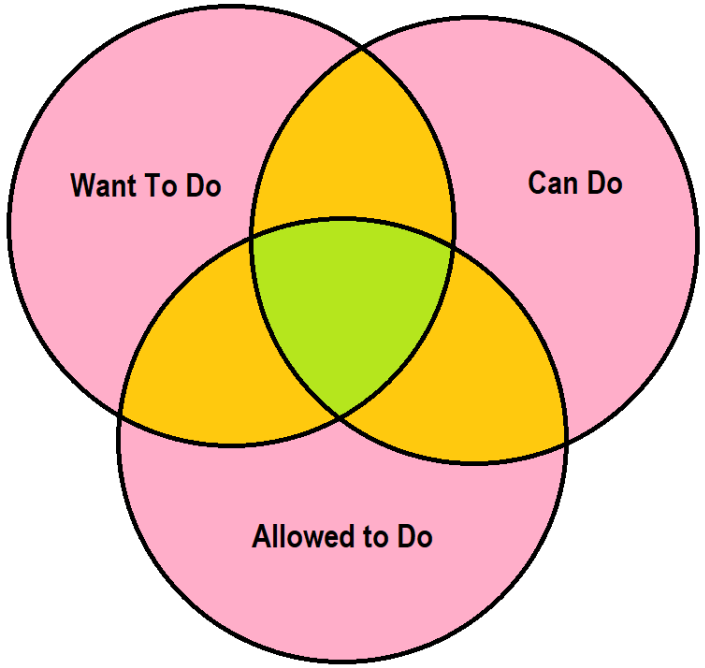


Cyber Threat Intelligence

- Attributes
  - Quality
    - Is this information true and correct to a level that I may use it?
  - Timeliness
    - Is the information current?
  - Scope
    - Target
      - Industry, machine, staff
    - Restraints
      - legal, contractual, distribution ethical.
    - Actionable level
      - Tactical, Operational, Strategic

Distribution

- Traffic light protocol
- Chatam House rules
- Disclosure Agreements
  - Non, Limited



- All ties in with your information classification

Sources – Everything Everywhere All at Once

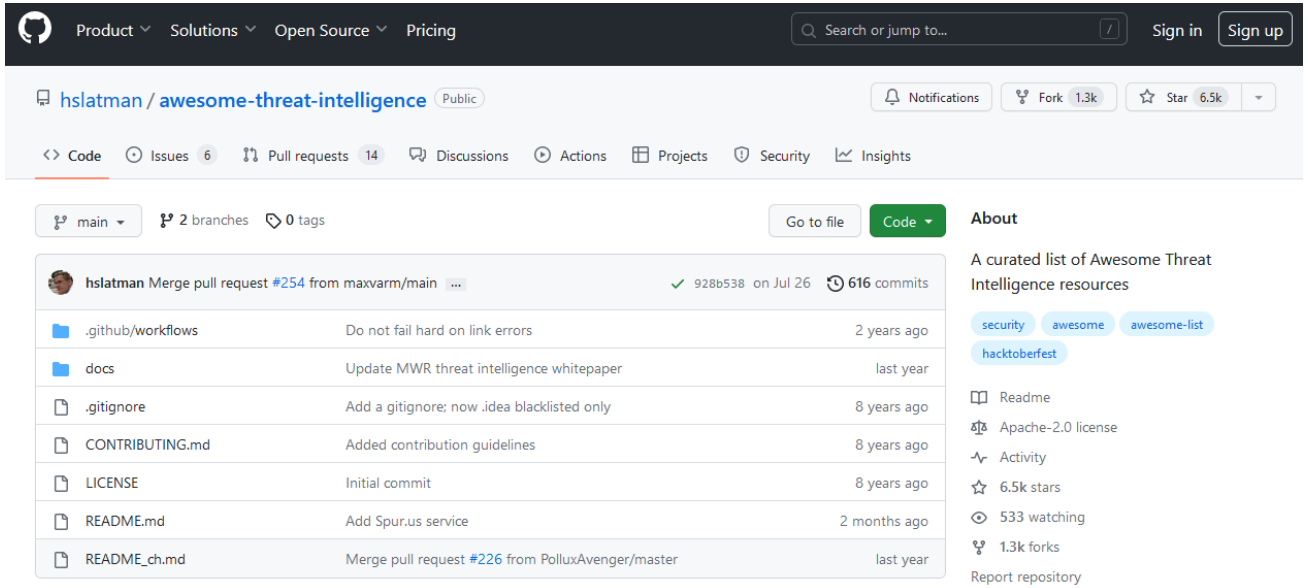
- Too much information to go into details
- Starters
  - CERT/CSIRTS/ISAC
    - CISA, CERT.pl,
  - PSIRST
    - Cisco, Microsoft, Redhat, Atlassian
  - COMMERCIAL
    - Unit 42, Shodan, Talos
  - COMMUNITY
    - Abuse.ch, Alien Vault, Team Cymru, Shadow server

https://ithub.com/hslatman/awesome-threat-intelligence

AUSCERT

Firehoses of Threat Intel

- Search term “curated list of threat intel git”
- Target Link https://github.com/hslatman/awesome-threat-intelligence
- Looks like



AUSCERT

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

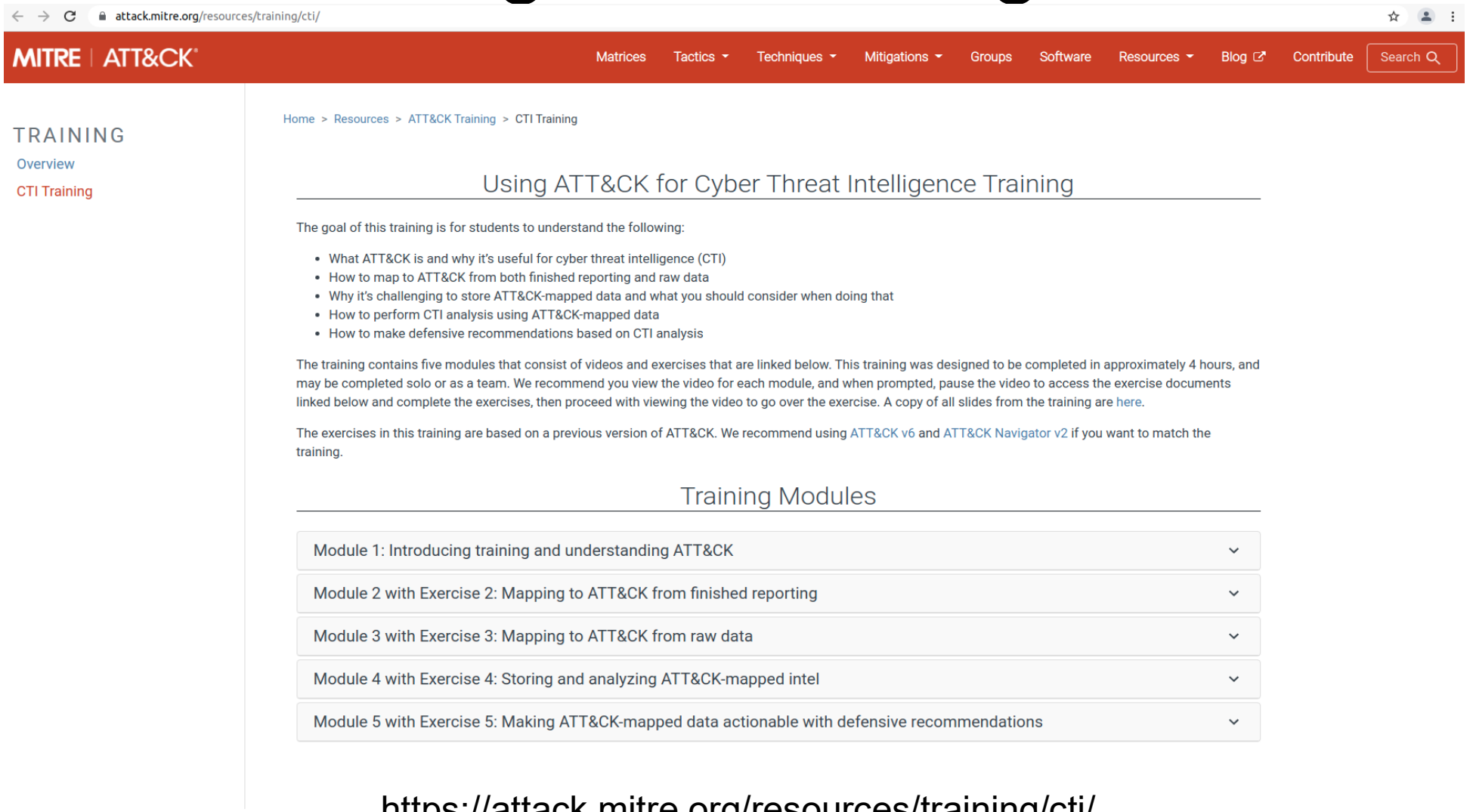
- CISA
  - ALERTS
    - Concise summaries covering cybersecurity topics, such as mitigations that vendors have published for vulnerabilities in their products.
  - ANALYSIS REPORT
    - In-depth analysis of a new or evolving cyber threat, including technical details and remediations.
  - ICS ADVISORY
    - Concise summaries covering industrial control system (ICS) cybersecurity topics, primarily focused on mitigations that ICS vendors have published for vulnerabilities in their products.
  - ICS MEDICAL ADVISORY
    - Concise summaries covering ICS medical cybersecurity topics, primarily focused on mitigations that ICS medical vendors have published for vulnerabilities in their products.
  - CYBERSECURITY ADVISORY
    - In-depth reports covering a specific cybersecurity issue, often including threat actor tactics, techniques, and procedures; indicators of compromise; and mitigations.

Exercise

Using Attack Framework (Minimum Viable Skills)

AUSCERT

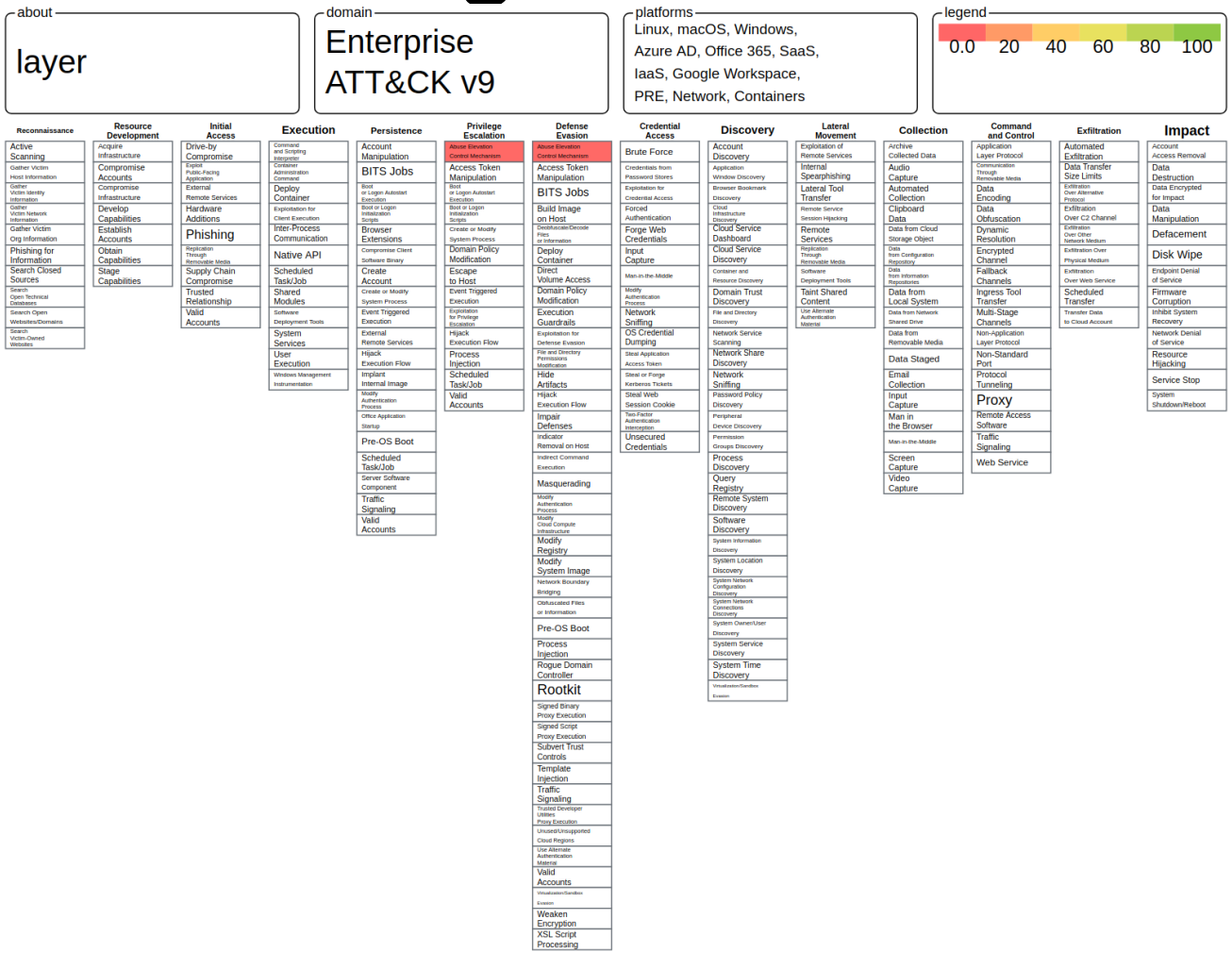
ATT&CK Navigator Training



https://attack.mitre.org/resources/training/cti/

AUSCERT

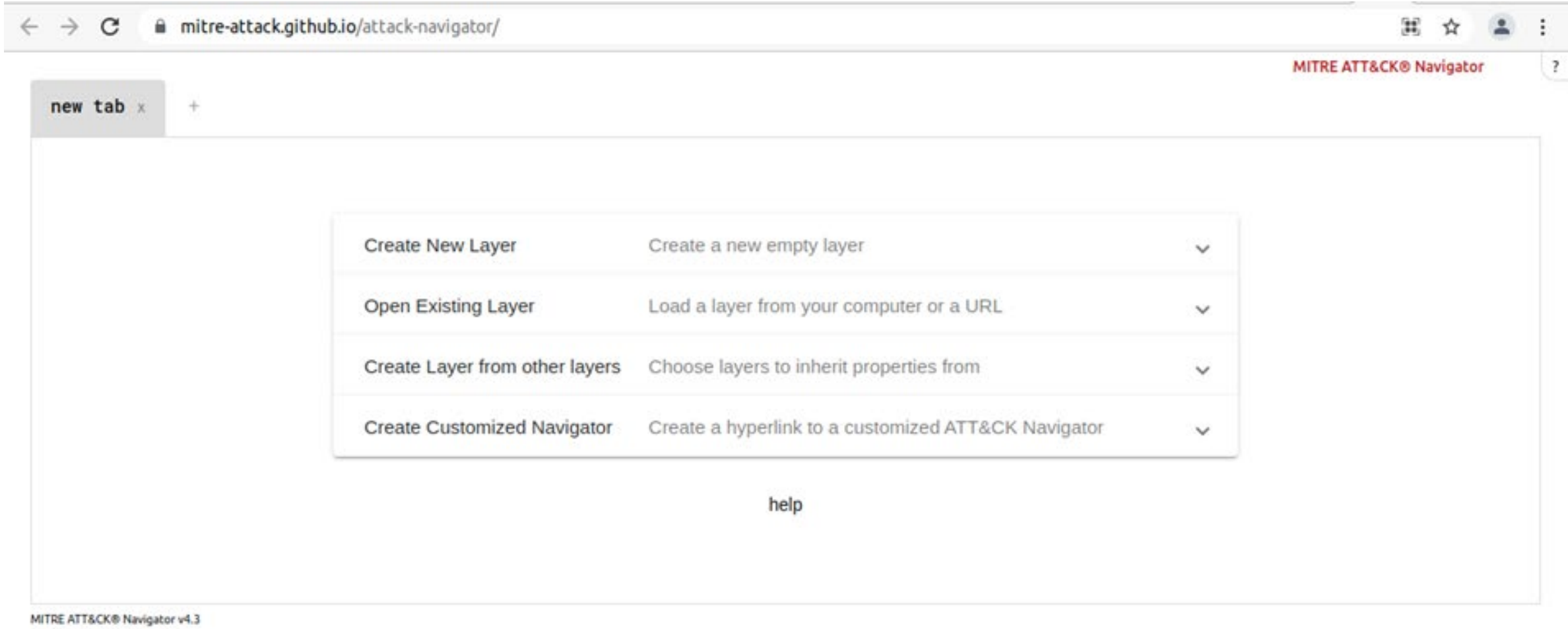
Exercise 1 – Getting used to the Navigator



FIRST Improving Security Together

AUSCERT

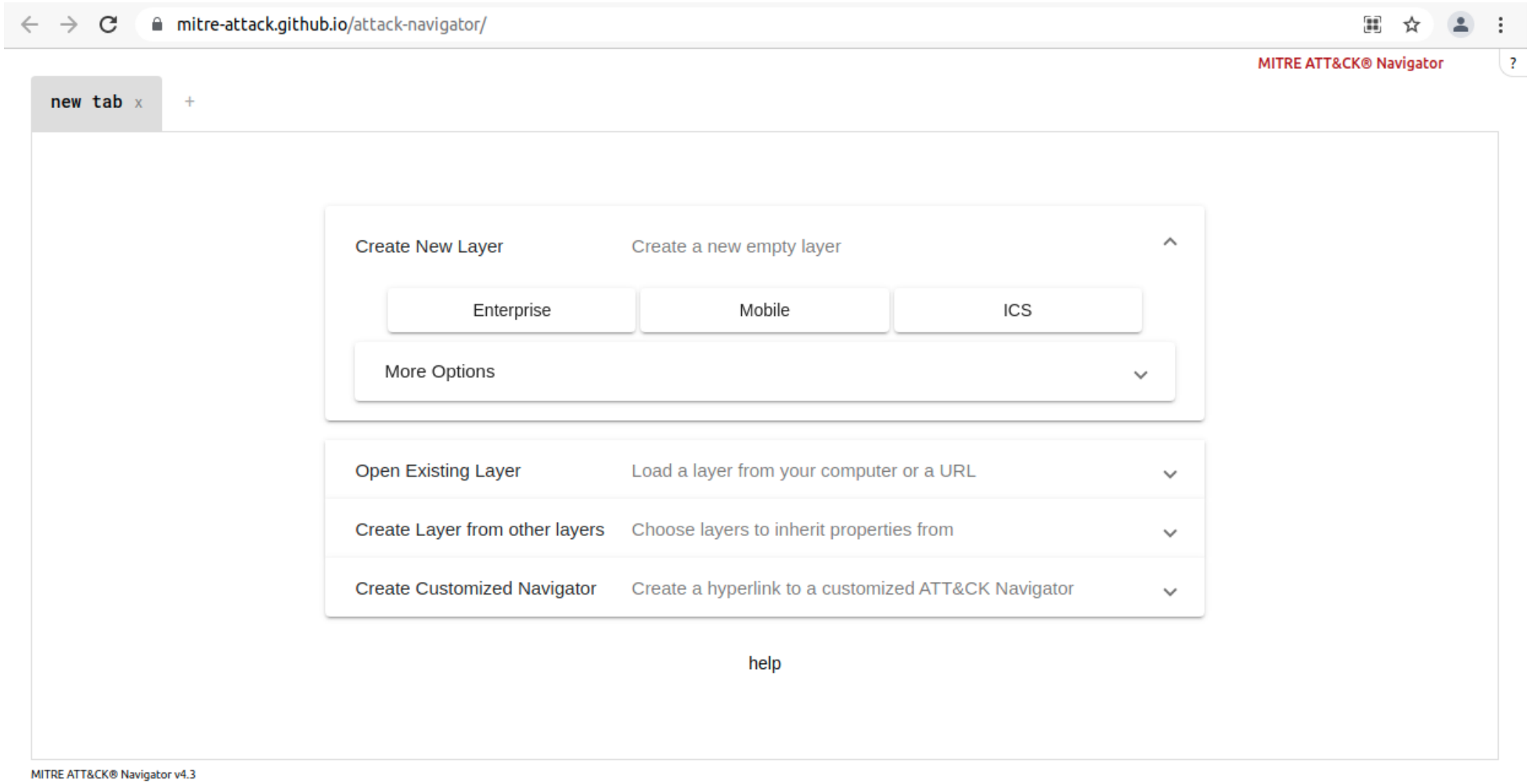
Where is this navigator?



https://mitre-attack.github.io/attack-navigator/

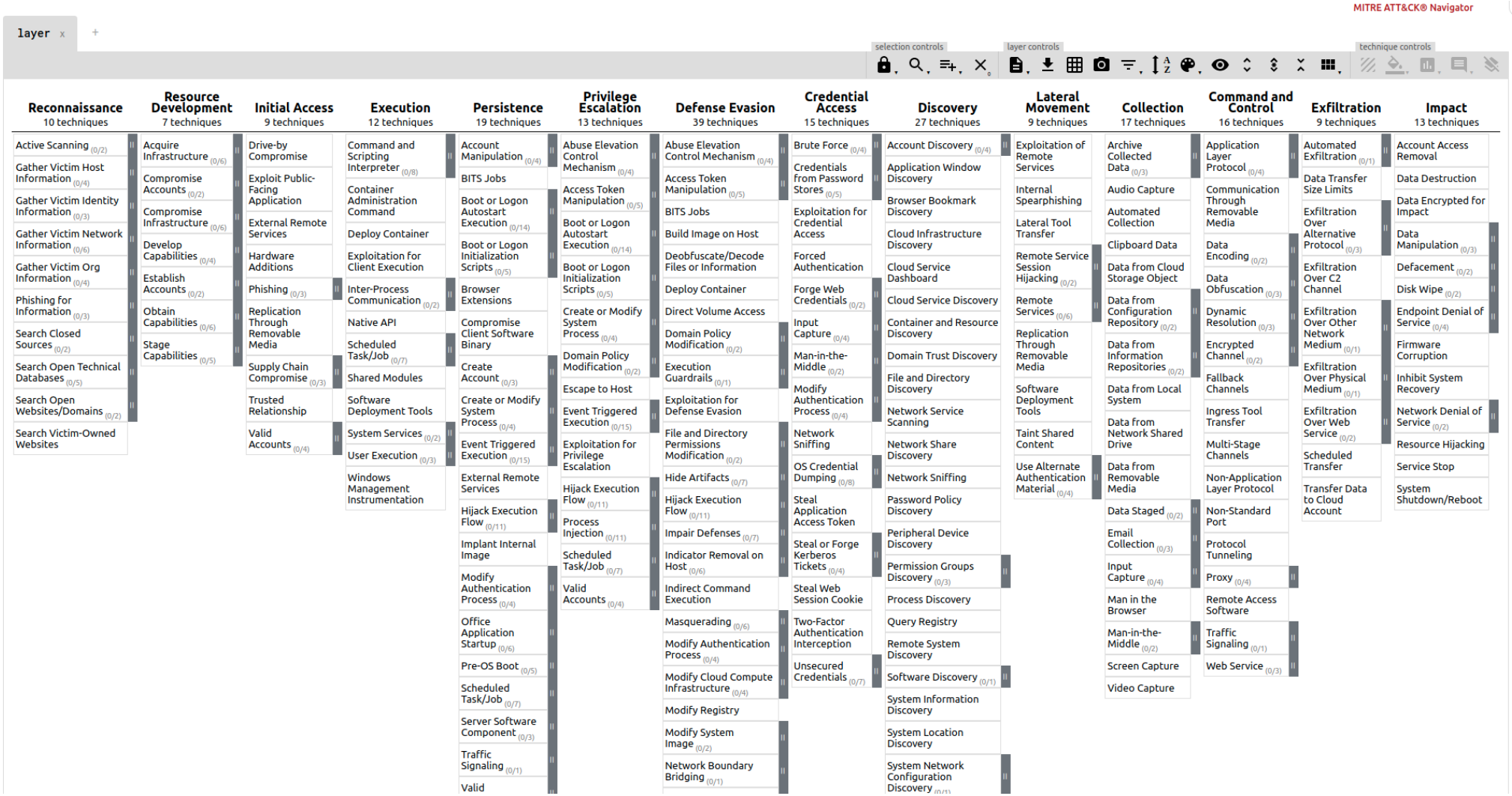
AUSCERT

Create A New Layer - Enterprise



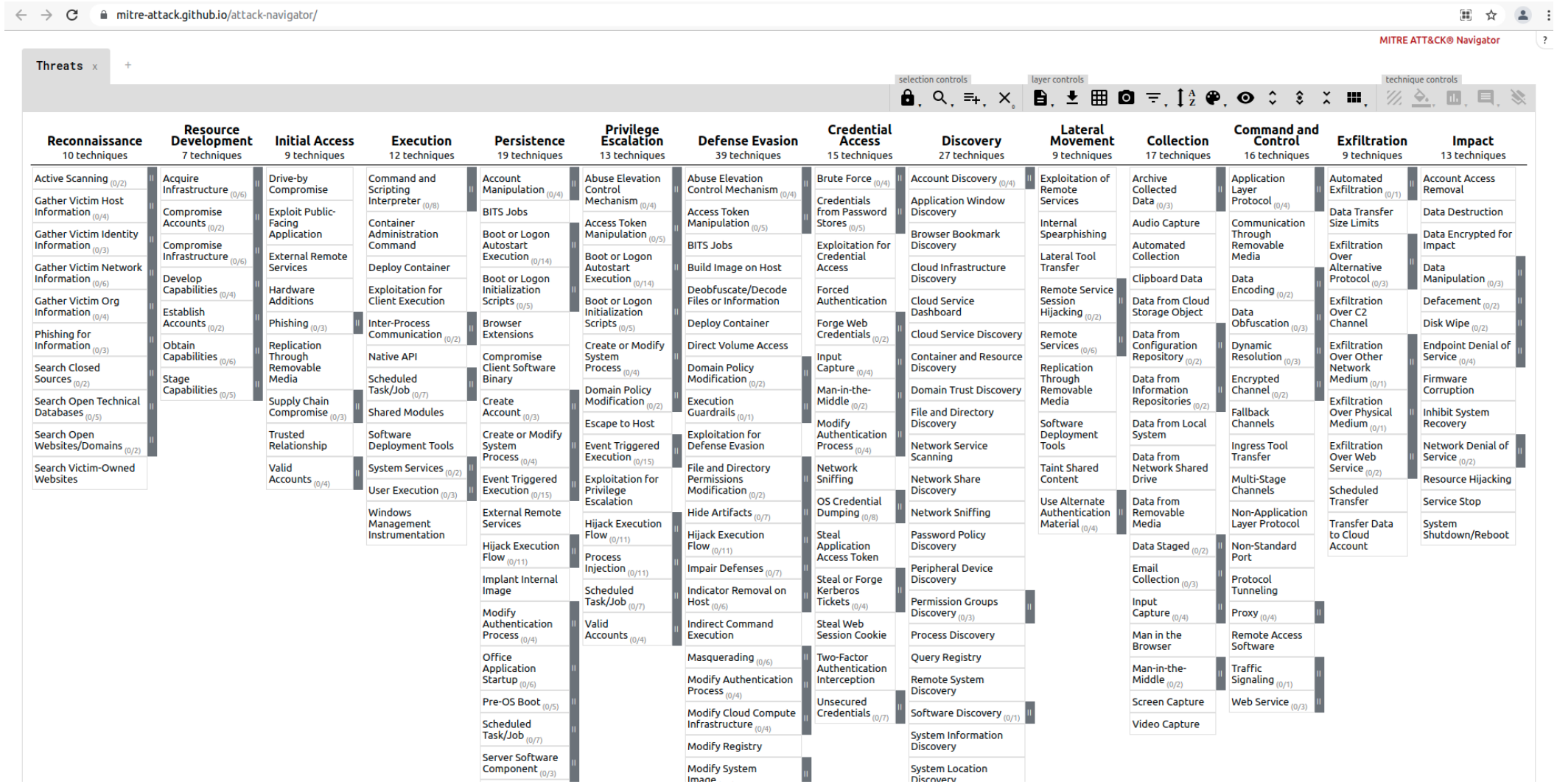
AUSCERT

Change the Layer name

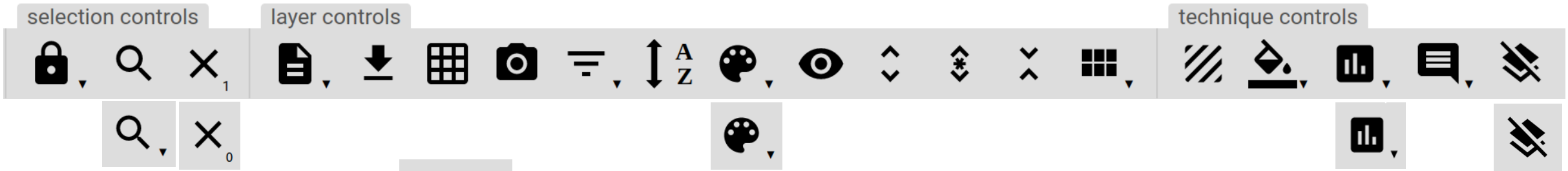


AUSCERT

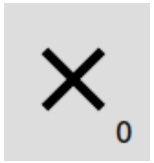
Next… will be toolbar navigation



ATT&CK Navigator toolbar



- Search



- Deselect

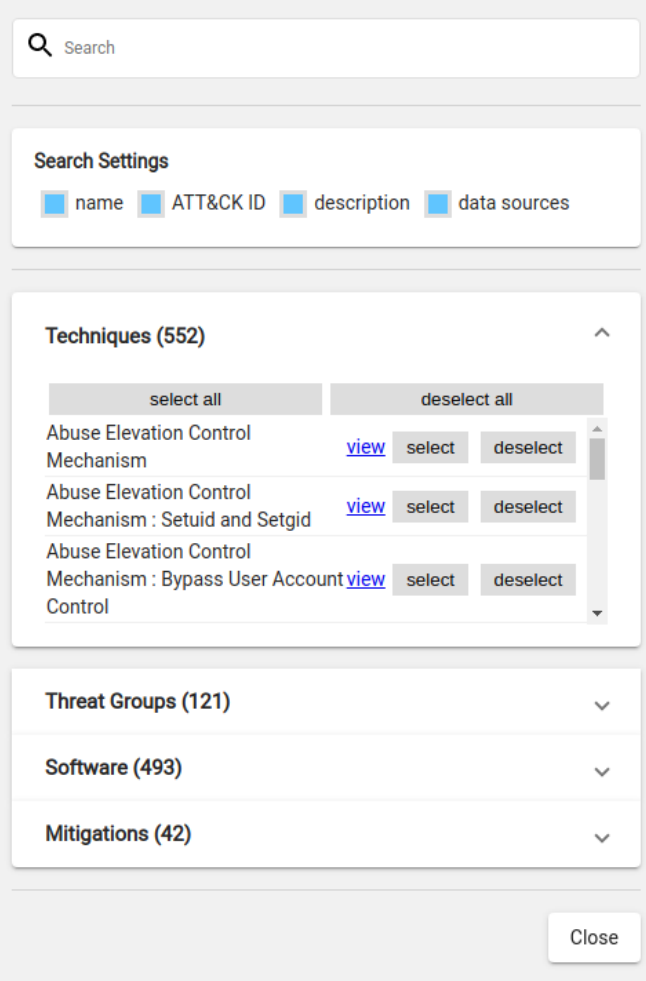
- Color setup

- Scoring

- Clear Annotation

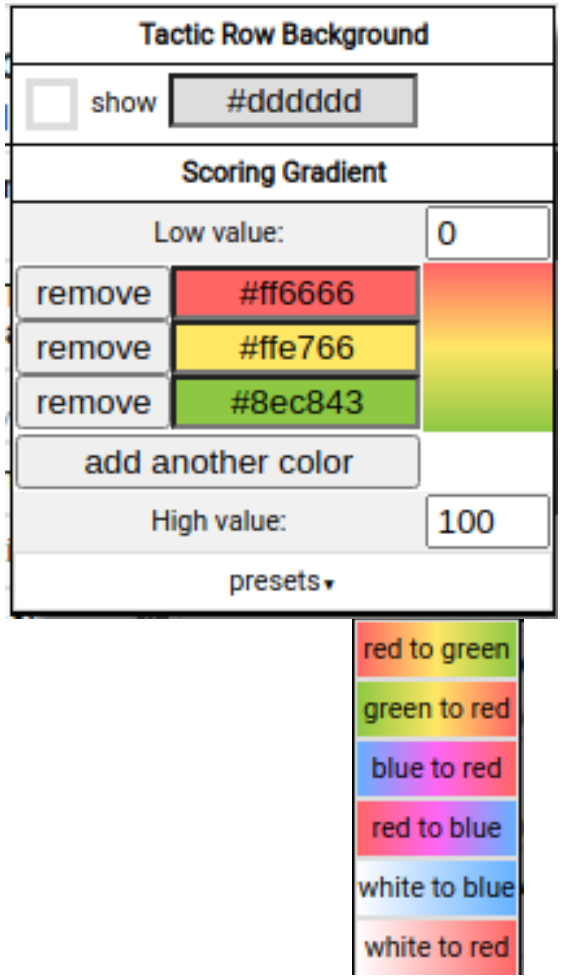
AUSCERT

SEARCH



- Search Text field
- Search Settings
  - Will be using “name” and “description”
- Techniques
  - Menu selection of items to include from Searching
  - Select “Abuse Elevation Control Mechanism”
- Threat Groups
  - Multi-selects threats associated with Group
- Software
  - Multi-selects threat posed by Software
- Mitigation
  - Multi-selects threat treated by the Mitigation

Color Setup



- Choice of color arrangement
- Can select and tri-color match
  - Or add more colors as you wish
- Default to Red-Yellow-Green is our Choice

AUSCERT

scoring

- Score the selected techniques to paint them with a colour
  - Score with “1” to get RED
  - Score with “50” to get YELLOW
  - Score with “100” to get GREEN

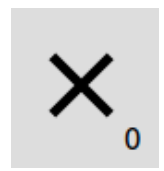
- Decide on what color you will need to state what
  - RED will be techniques Selected or multi-selected by Threat Group
  - YELLOW will be techniques from Software
  - GREEN will techniques covered by Mitigation

Test it Out – Interim results

- Select Techniques

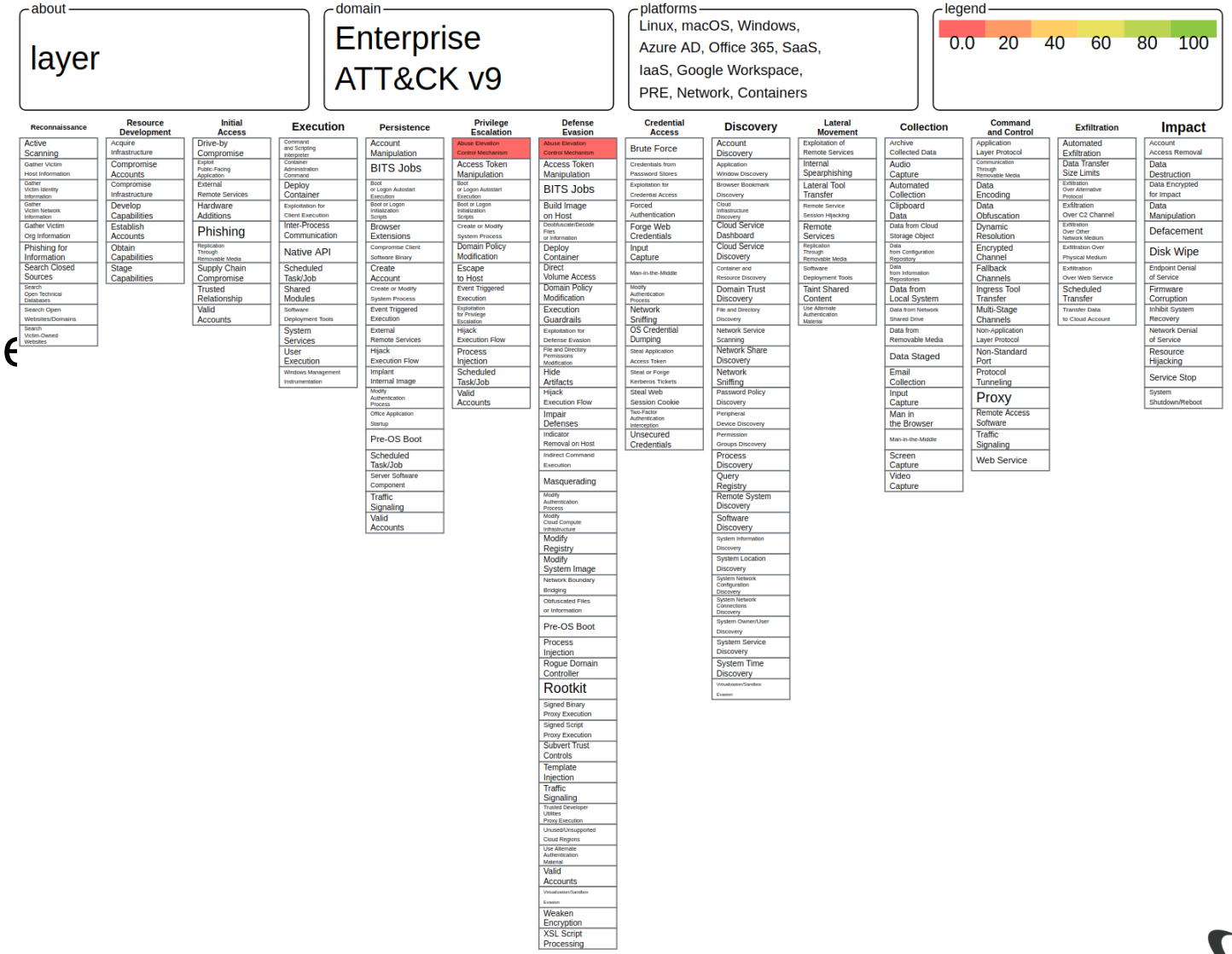
- Choose Color Sche

- Provide a score

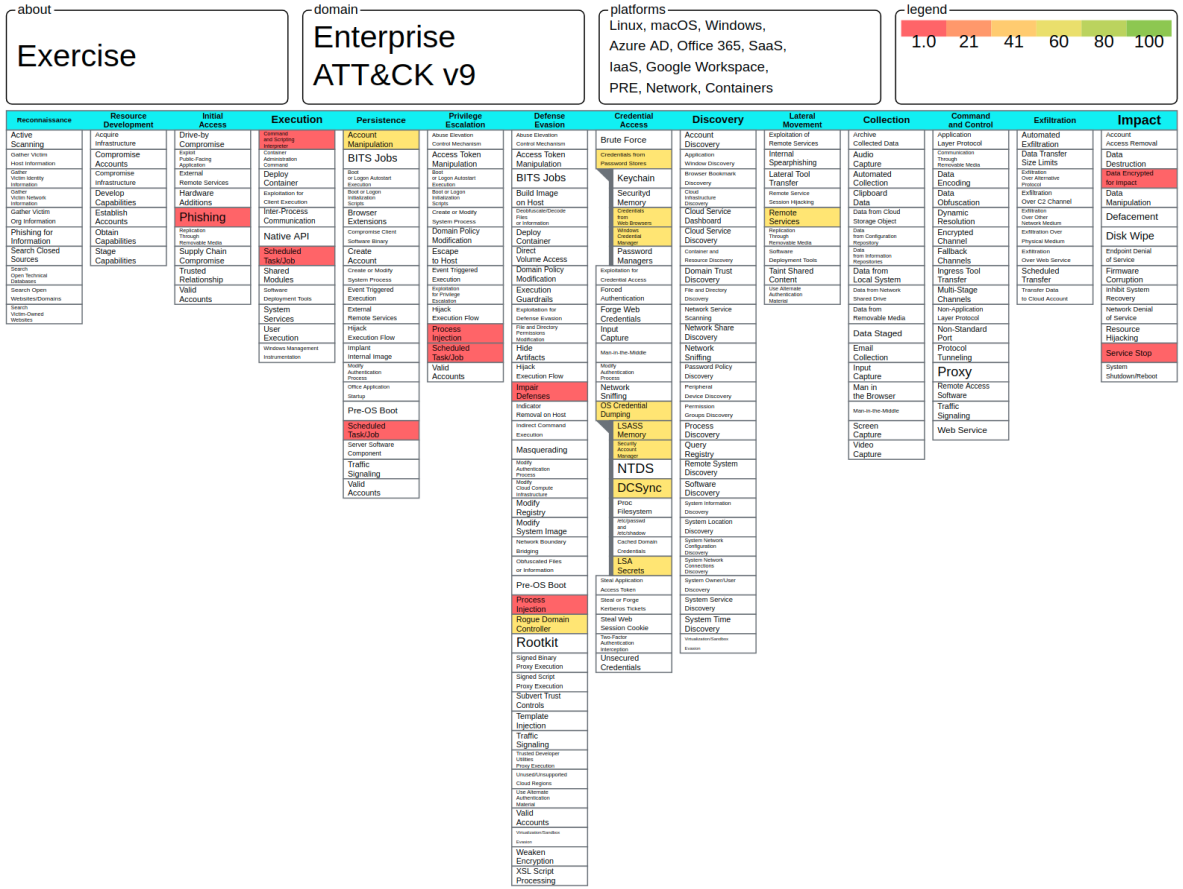


- Deselect

- Clear Annotation



Exercise 2 – Getting Statement into Navigator



Statement of Focus

- Find one on the internet https://forums.whirlpool.net.au/thread/3xv6604y
- Consists of
  - Statement of event
  - Statement of learning
- This is a simple and semi-clean statement.

this post was **edited** O.P.

I'm sharing my learnings after ransomware. I look after a system that supports 500 users and 16x7x365 operations.

Old ransomware was someone clicking on something executable and the ransomware happening immediately to encrypt files. Today's ransomware is targeted, sophisticated compromise using vulnerabilities, attacker dwell time in systems then ransomware and likely taking data to threaten to expose too.

The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend. The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical.

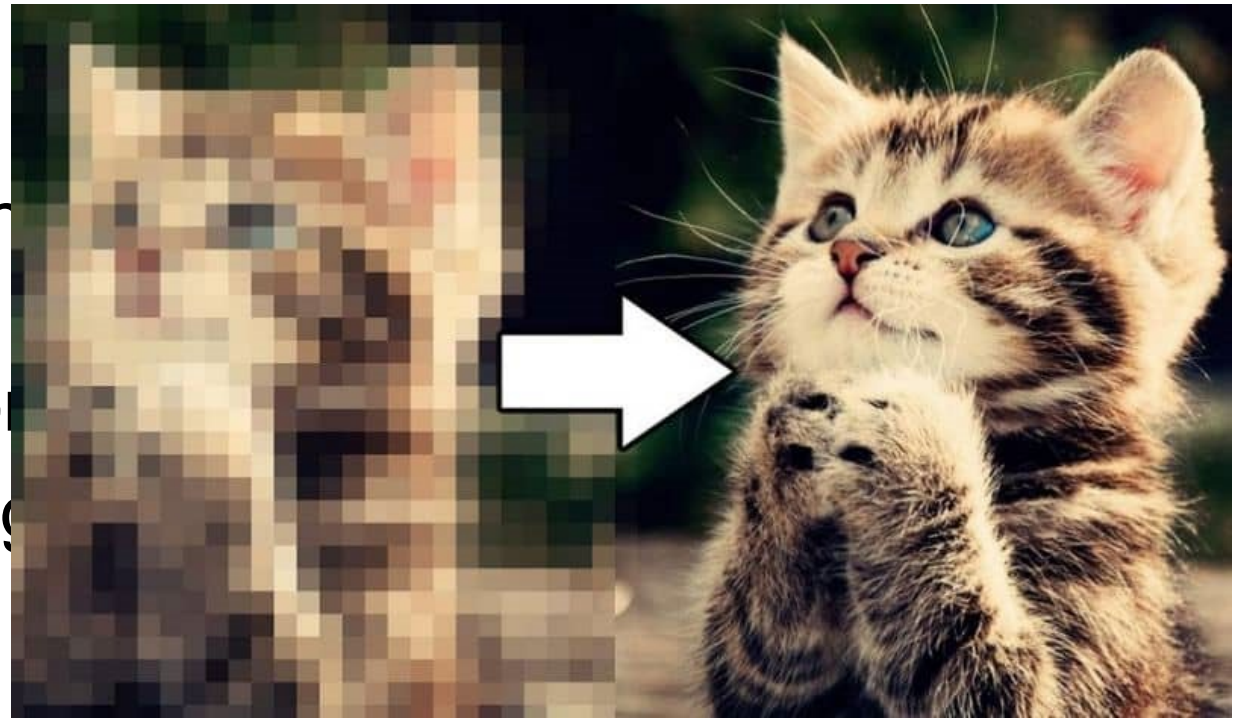
Learnings:
- Be prepared for the forensics to find out what happened, if the attack is ongoing and to detect new attacks or you have NO HOPE of stopping it and quickly detecting a new attack (follow-up attacks are extremely likely)
So logging to an intelligent SIEM with 24x7 alerting, enabling sysmon logging on servers.

- There might not be malicious files.
Today's attackers use in-memory tools, Windows scripts, Windows executables, open source security tools and AV might not detect anything.

- Be prepared to change every password in AD and on computers.

When and how do you get statements

- Make it as iterative as you can
- Start as early as possible
- Jot down notes if that all you can start
- Or work direct into the Framewo
- Sooner or later someone is going happened



AUSCERT

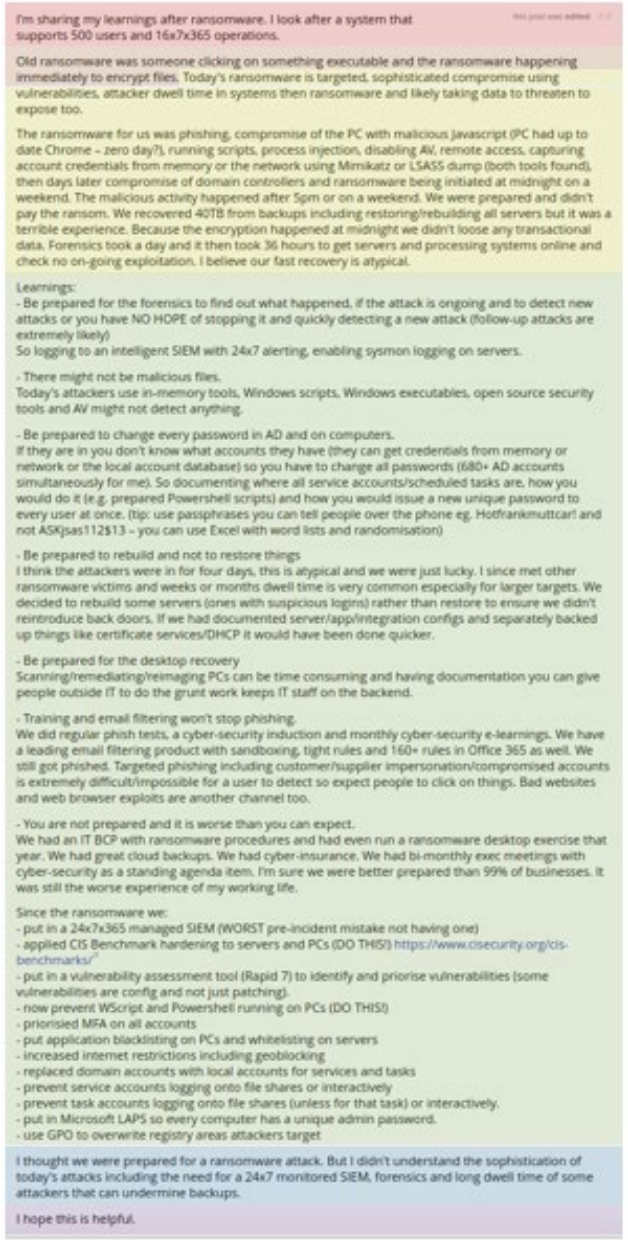
FIRST Improving Security Together

Decomposition of Target Statement

Narrative structure in this statement:

Exposition (RED)
Rising Action (ORANGE)
Climax (YELLOW)
Falling Action (GREEN)
Resolution (BLUE)

And a signoff (VIOLET)



I'm sharing my learnings after ransomware. I look after a system that supports 500 users and 16x7x365 operations.

Old ransomware was someone clicking on something executable and the ransomware happening immediately to encrypt files. Today's ransomware is targeted, sophisticated compromise using vulnerabilities, attacker dwell time in systems then ransomware and likely taking data to threaten to expose too.

The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend. The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical.

Learnings:
- Be prepared for the forensics to find out what happened, if the attack is ongoing and to detect new attacks or you have NO HOPE of stopping it and quickly detecting a new attack (follow-up attacks are extremely likely)
So logging to an intelligent SIEM with 24x7 alerting, enabling sysmon logging on servers.

- There might not be malicious files.
Today's attackers use in-memory tools, Windows scripts, Windows executables, open source security tools and AV might not detect anything.

- Be prepared to change every password in AD and on computers.
If they are in you don't know what accounts they have (they can get credentials from memory or network or the local account database) so you have to change all passwords (680+ AD accounts simultaneously for me). So documenting where all service accounts/scheduled tasks are, how you would do it (e.g. prepared Powershell scripts) and how you would issue a new unique password to every user at once. (tip: use passphrases you can tell people over the phone eg. Hotfrankmuttcar! and not ASKjsas112$13 – you can use Excel with word lists and randomisation)

- Be prepared to rebuild and not to restore things
I think the attackers were in for four days, this is atypical and we were just lucky. I since met other ransomware victims and weeks or months dwell time is very common especially for larger targets. We decided to rebuild some servers (ones with suspicious logins) rather than restore to ensure we didn't reintroduce back doors. If we had documented server/app/integration configs and separately backed up things like certificate services/DHCP it would have been done quicker.

- Be prepared for the desktop recovery
Scanning/remediating/reimaging PCs can be time consuming and having documentation you can give people outside IT to do the grunt work keeps IT staff on the backend.

- Training and email filtering won't stop phishing.
We did regular phish tests, a cyber-security induction and monthly cyber-security e-learnings. We have a leading email filtering product with sandboxing, tight rules and 160+ rules in Office 365 as well. We still got phished. Targeted phishing including customer/supplier impersonation/compromised accounts is extremely difficult/impossible for a user to detect so expect people to click on things. Bad websites and web browser exploits are another channel too.

- You are not prepared and it is worse than you can expect.
We had an IT BCP with ransomware procedures and had even run a ransomware desktop exercise that year. We had great cloud backups. We had cyber-insurance. We had bi-monthly exec meetings with cyber-security as a standing agenda item. I'm sure we were better prepared than 99% of businesses. It was still the worse experience of my working life.

Since the ransomware we:
- put in a 24x7x365 managed SIEM (WORST pre-incident mistake not having one)
- applied CIS Benchmark hardening to servers and PCs (DO THIS!) https://www.cisecurity.org/cis-benchmarks/
- put in a vulnerability assessment tool (Rapid 7) to identify and priorise vulnerabilities (some vulnerabilities are config and not just patching).
- now prevent WScript and Powershell running on PCs (DO THIS!)
- priorisied MFA on all accounts
- put application blacklisting on PCs and whitelisting on servers
- increased internet restrictions including geoblocking
- replaced domain accounts with local accounts for services and tasks
- prevent service accounts logging onto file shares or interactively
- prevent task accounts logging onto file shares (unless for that task) or interactively.
- put in Microsoft LAPS so every computer has a unique admin password.
- use GPO to overwrite registry areas attackers target

I thought we were prepared for a ransomware attack. But I didn't understand the sophistication of today's attacks including the need for a 24x7 monitored SIEM, forensics and long dwell time of some attackers that can undermine backups.

I hope this is helpful.

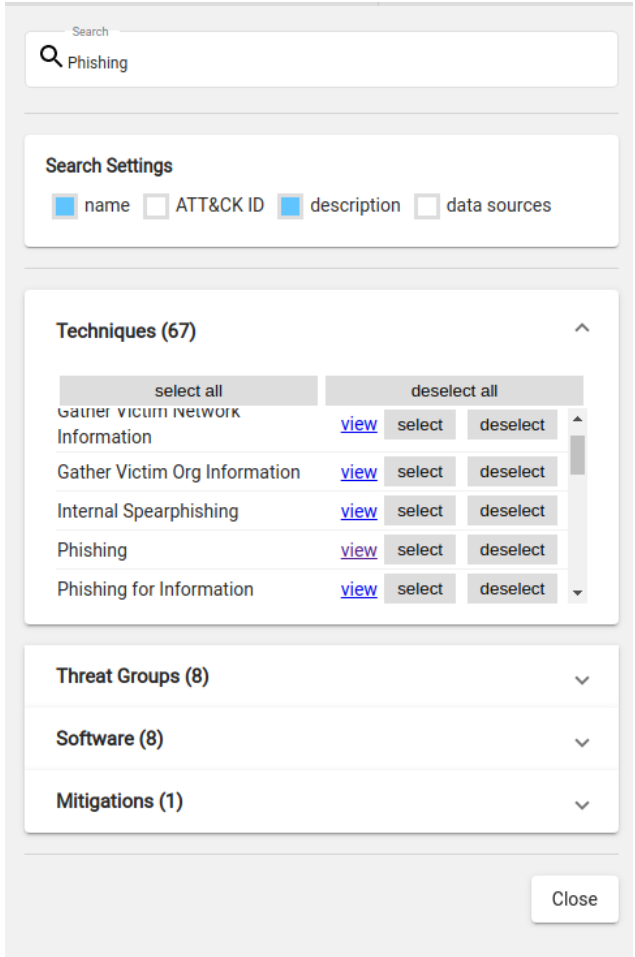
We just want the action that happened

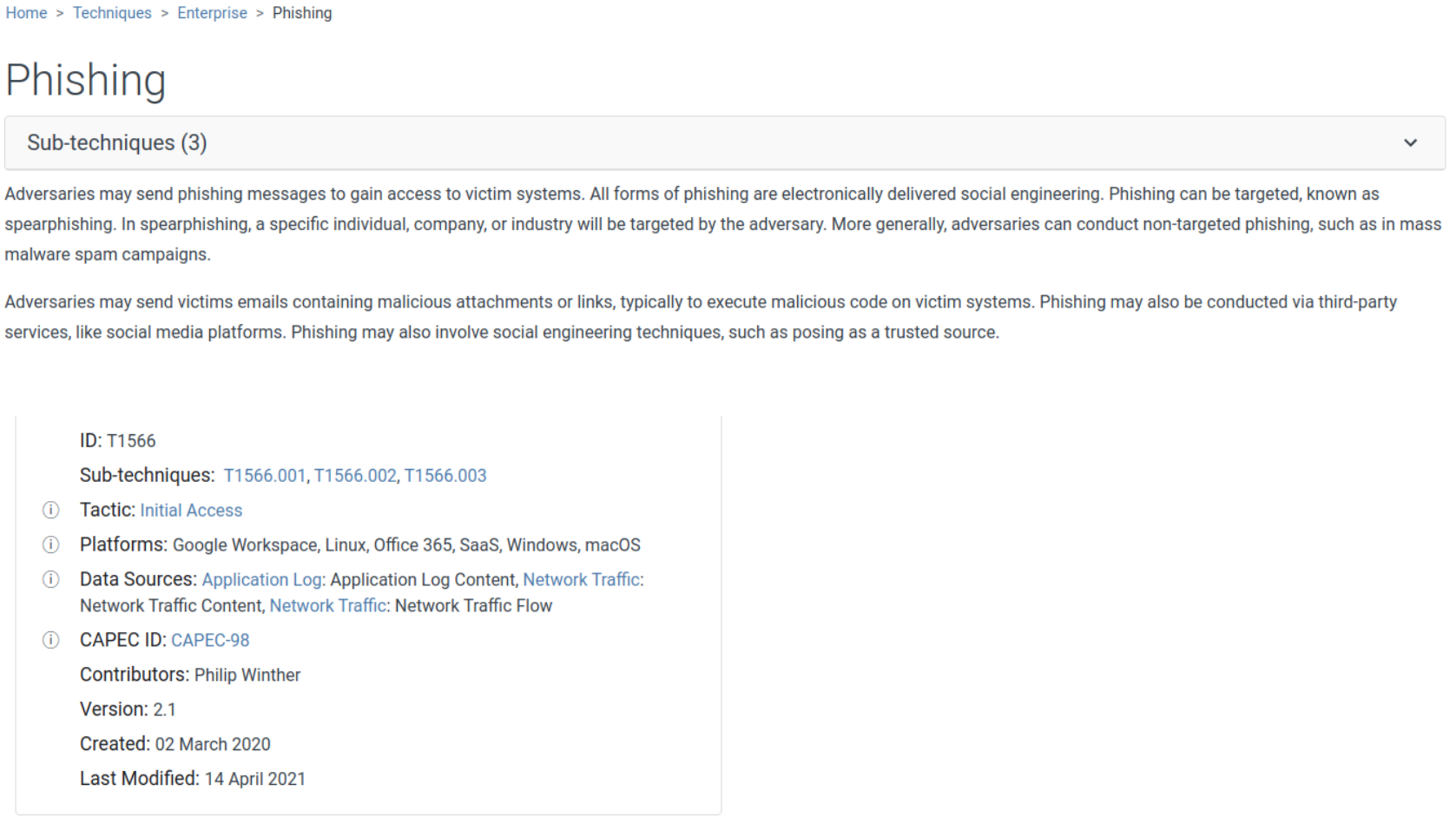
- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

Is a phish a phish by any other name?





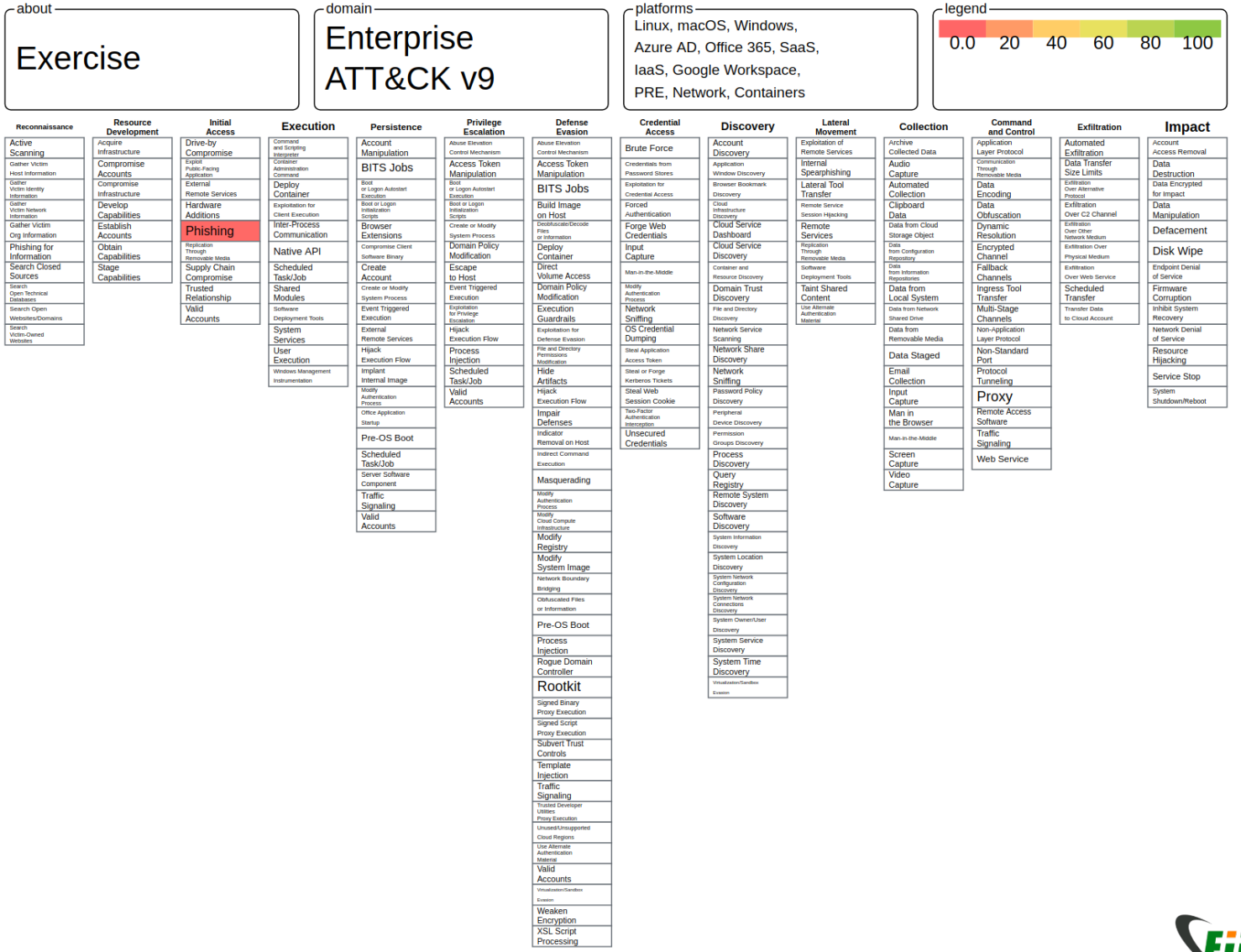
We just want the action

T1566 - Phishing

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

Navigator Entry

- Search select “Phishing”
- Score “1” (Red)
- Deselect
- Move on to the next one



AUSCERT

FIRST Improving Security Together

We just want the action

No Match – It is not a technique, but a result

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1059-007 – Command Scripting Interpreter - Javascript

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1059-007 – Command Scripting Interpreter: Javascript

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want th[illegible]on

T1059 – Command Scripting Interpreter

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1055 – Process Injection

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1562-001 – Impair Defenses: Disable or Modify Tools

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1201 – Remote Services

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want th[redacted]on

T1201-002 – Credentials from Password Stores: Securityd Memory

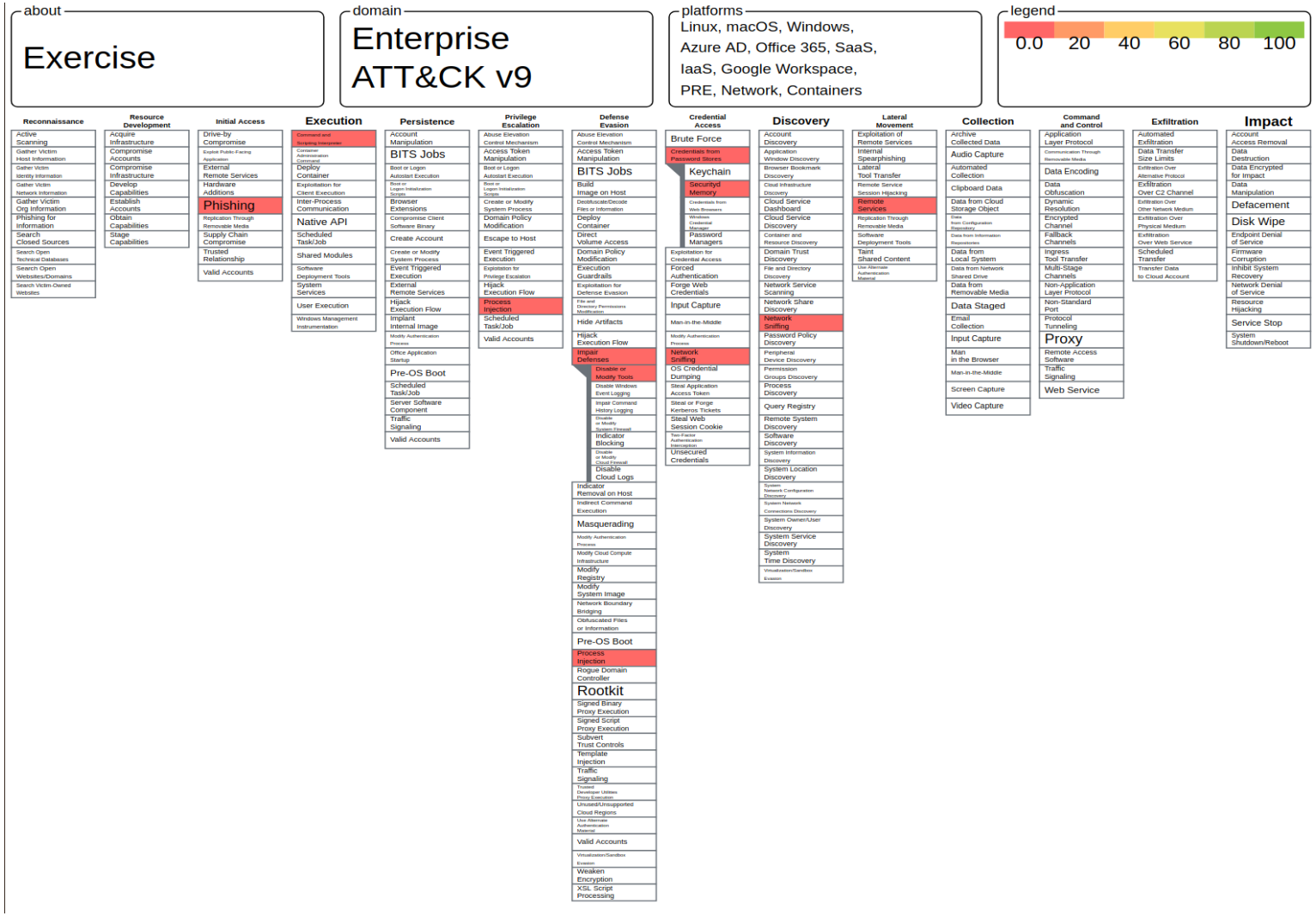
- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want th[illegible]on

T1040 – Network Sniffing

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

How it should look so far



AUSCERT

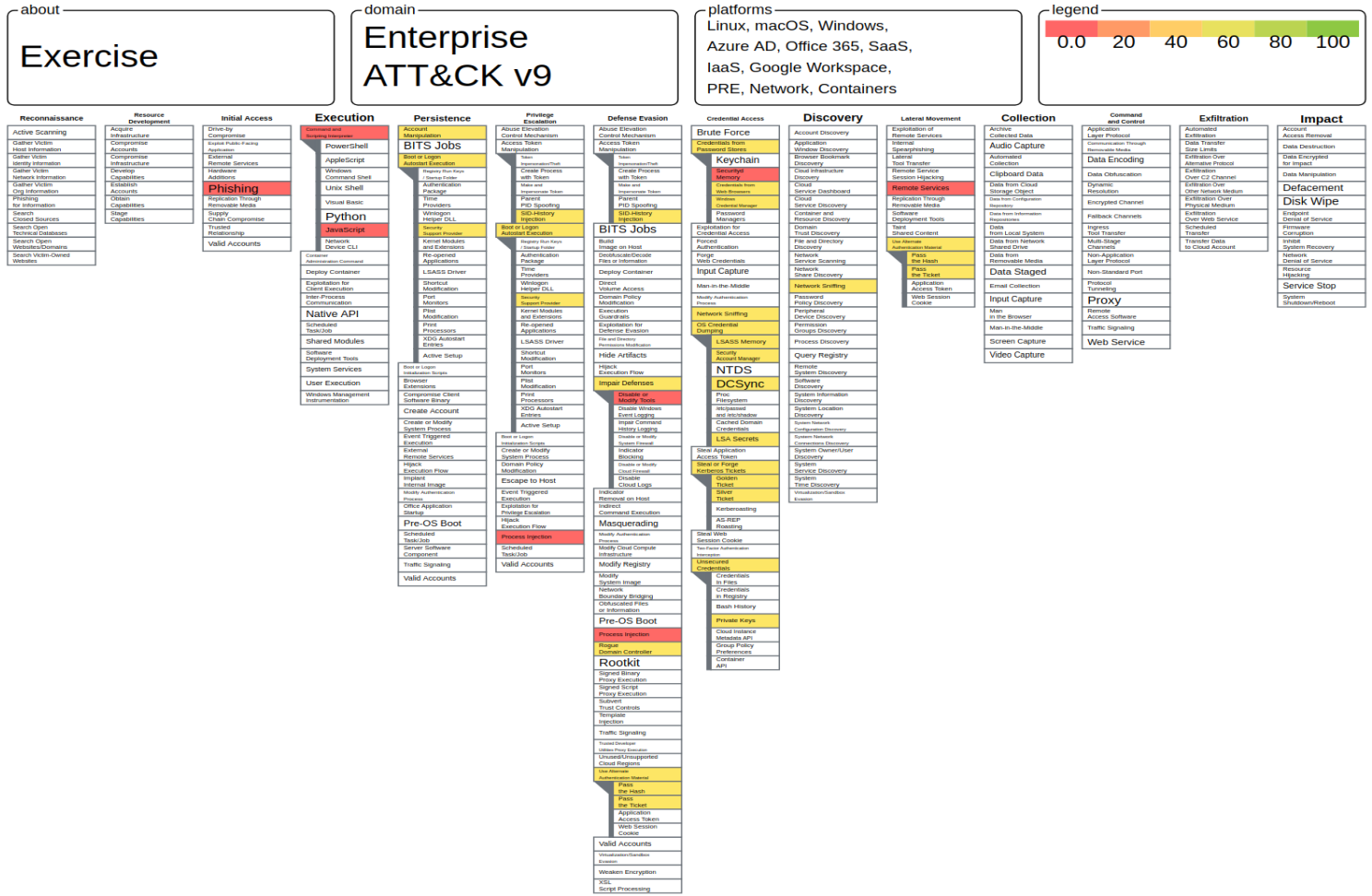
FIRST Improving Security Together

We just want the action

S0002 – Mimikatz

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

With Mimikatz



AUSCERT

FIRST Improving Security Together

We just want the action

T1003-001 – OS Credential Dumping: LSASS Memory

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1207 – Rogue Domain Controller

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1486 – Data Encrypted For Impact

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1053 – Scheduled Task/Job

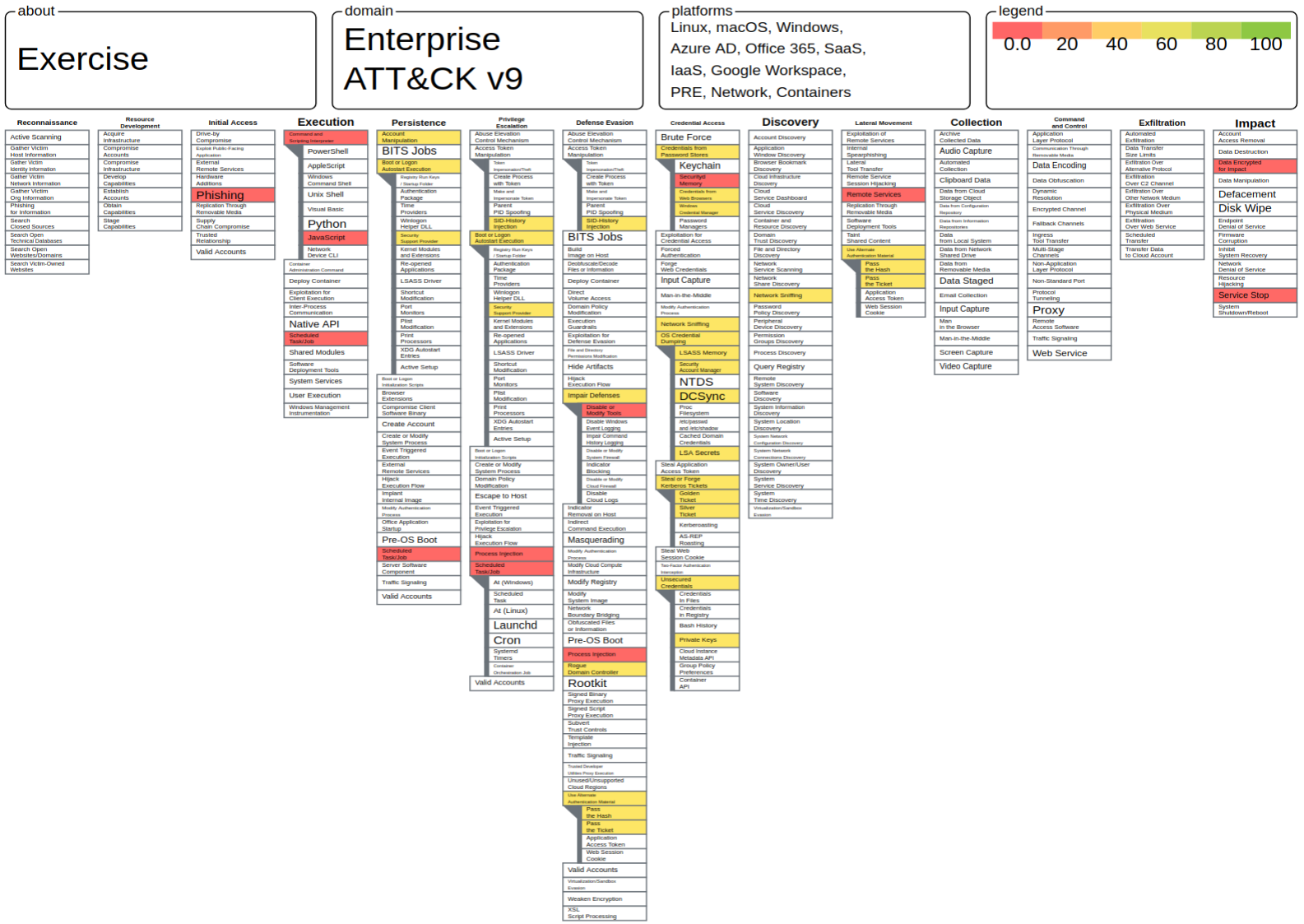
- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

We just want the action

T1489 – Service Stop

- The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend . The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical

Threat Event Completed

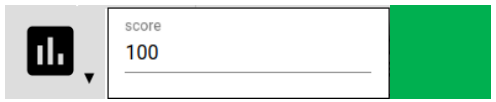


AUSCERT

FIRST Improving Security Together

WHAT ABOUT THE LESSONS LEARNT

https://forums.whirlpool.net.au/thread/3xv6604y



I'm sharing my learnings after ransomware. I look after a system that supports 500 users and 16x7x365 operations.

Old ransomware was someone clicking on something executable and the ransomware happening immediately to encrypt files. Today's ransomware is targeted, sophisticated compromise using vulnerabilities, attacker dwell time in systems then ransomware and likely taking data to threaten to expose too.

The ransomware for us was phishing, compromise of the PC with malicious Javascript (PC had up to date Chrome – zero day?), running scripts, process injection, disabling AV, remote access, capturing account credentials from memory or the network using Mimikatz or LSASS dump (both tools found), then days later compromise of domain controllers and ransomware being initiated at midnight on a weekend. The malicious activity happened after 5pm or on a weekend. We were prepared and didn't pay the ransom. We recovered 40TB from backups including restoring/rebuilding all servers but it was a terrible experience. Because the encryption happened at midnight we didn't loose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check no on-going exploitation. I believe our fast recovery is atypical.

Learnings:
- Be prepared for the forensics to find out what happened, if the attack is ongoing and to detect new attacks or you have NO HOPE of stopping it and quickly detecting a new attack (follow-up attacks are extremely likely)
So logging to an intelligent SIEM with 24x7 alerting, enabling sysmon logging on servers.

- There might not be malicious files.
Today's attackers use in-memory tools, Windows scripts, Windows executables, open source security tools and AV might not detect anything.

- Be prepared to change every password in AD and on computers.
If they are in you don't know what accounts they have (they can get credentials from memory or network or the local account database) so you have to change all passwords (680+ AD accounts simultaneously for me). So documenting where all service accounts/scheduled tasks are, how you would do it (e.g. prepared Powershell scripts) and how you would issue a new unique password to every user at once. (tip: use passphrases you can tell people over the phone eg. Hotfrankmuttcar! and not ASKjsas112$13 – you can use Excel with word lists and randomisation)

- Be prepared to rebuild and not to restore things
I think the attackers were in for four days, this is atypical and we were just lucky. I since met other ransomware victims and weeks or months dwell time is very common especially for larger targets. We decided to rebuild some servers (ones with suspicious logins) rather than restore to ensure we didn't reintroduce back doors. If we had documented server/app/integration configs and separately backed up things like certificate services/DHCP it would have been done quicker.

- Be prepared for the desktop recovery
Scanning/remediating/reimaging PCs can be time consuming and having documentation you can give people outside IT to do the grunt work keeps IT staff on the backend.

- Training and email filtering won't stop phishing.
We did regular phish tests, a cyber-security induction and monthly cyber-security e-learnings. We have a leading email filtering product with sandboxing, tight rules and 160+ rules in Office 365 as well. We still got phished. Targeted phishing including customer/supplier impersonation/compromised accounts is extremely difficult/impossible for a user to detect so expect people to click on things. Bad websites and web browser exploits are another channel too.

- You are not prepared and it is worse than you can expect.
We had an IT BCP with ransomware procedures and had even run a ransomware desktop exercise that year. We had great cloud backups. We had cyber-insurance. We had bi-monthly exec meetings with cyber-security as a standing agenda item. I'm sure we were better prepared than 99% of businesses. It was still the worse experience of my working life.

Since the ransomware we:
- put in a 24x7x365 managed SIEM (WORST pre-incident mistake not having one)
- applied CIS Benchmark hardening to servers and PCs (DO THIS!) https://www.cisecurity.org/cis-benchmarks/
- put in a vulnerability assessment tool (Rapid 7) to identify and priorise vulnerabilities (some vulnerabilities are config and not just patching).
- now prevent WScript and Powershell running on PCs (DO THIS!)
- priorisied MFA on all accounts
- put application blacklisting on PCs and whitelisting on servers
- increased internet restrictions including geoblocking
- replaced domain accounts with local accounts for services and tasks
- prevent service accounts logging onto file shares or interactively
- prevent task accounts logging onto file shares (unless for that task) or interactively.
- put in Microsoft LAPS so every computer has a unique admin password.
- use GPO to overwrite registry areas attackers target

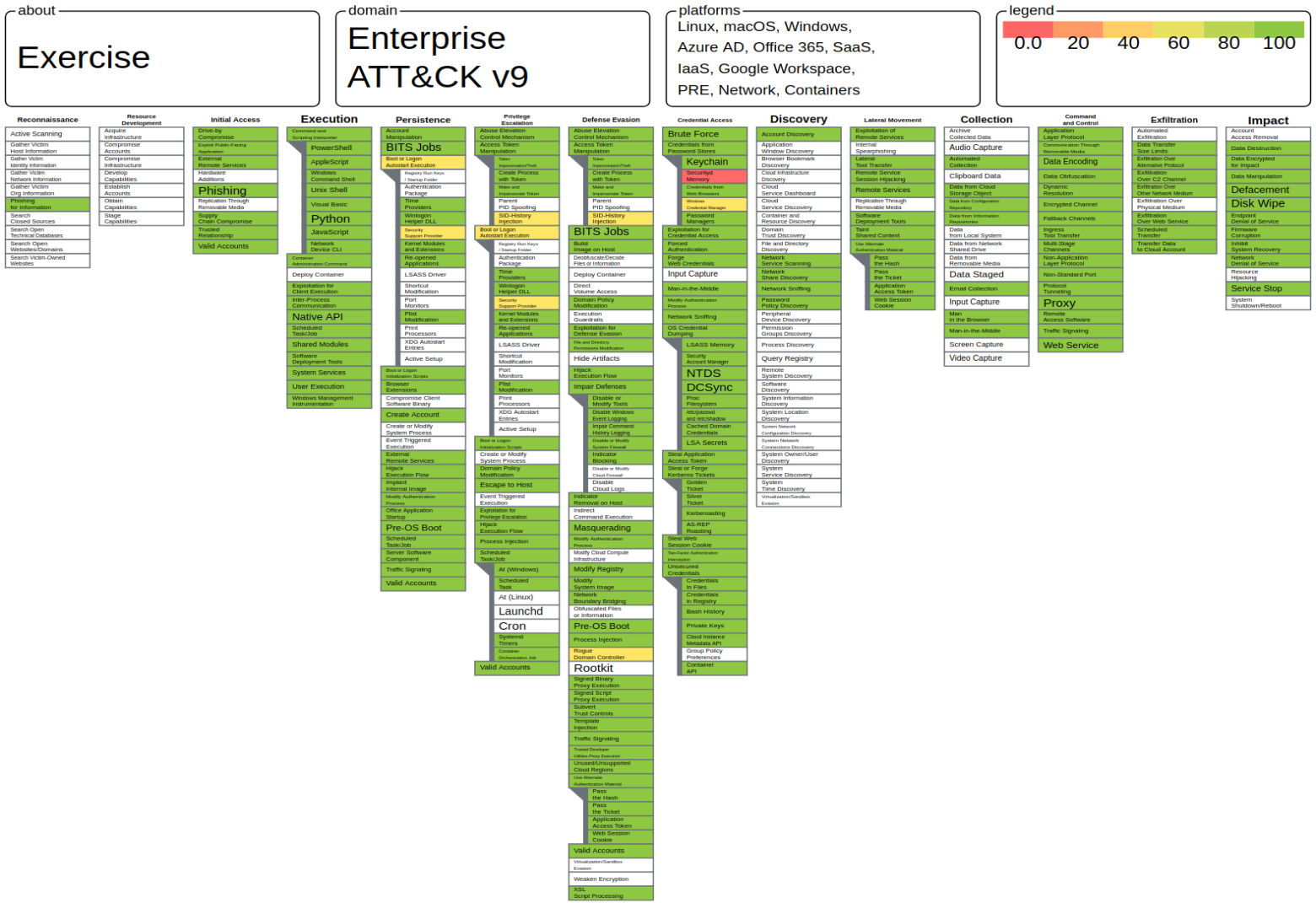
I thought we were prepared for a ransomware attack. But I didn't understand the sophistication of today's attacks including the need for a 24x7 monitored SIEM, forensics and long dwell time of some attackers that can undermine backups.

I hope this is helpful.

MITIGATIONS

Lessons learnt		
logging to an intelligent SIEM	Remote Data Storage	https://attack.mitre.org/mitigations/M1029/
to an intelligent SIEM	Network Intrusion Prevention	https://attack.mitre.org/mitigations/M1031/
change every password in AD and on computers.	Password Policies	https://attack.mitre.org/mitigations/M1027/
get credentials from memory or network or the local account database	OS Credential Dumping	https://attack.mitre.org/techniques/T1003/
get credentials from memory or network or the local account database	Network Boundary Bridging	https://attack.mitre.org/techniques/T1599/
get credentials from memory or network or the local account database	OS Credential Dumping	https://attack.mitre.org/techniques/T1003/
training	User Training	https://attack.mitre.org/mitigations/M1017/
filtering	Filter Network Traffic	https://attack.mitre.org/mitigations/M1037/
sandboxing	Application Isolation and Sandboxing	https://attack.mitre.org/mitigations/M1048/
Bad websites and web browser exploits	Drive-by Compromise	https://attack.mitre.org/techniques/T1189/
backups	Data Backup	https://attack.mitre.org/mitigations/M1053/
vulnerability assessment tool	Vulnerability Scanning	https://attack.mitre.org/mitigations/M1016/
some vulnerabilities are config	Operating System Configuration	https://attack.mitre.org/mitigations/M1028/
	Software Configuration	https://attack.mitre.org/mitigations/M1054/
	User Account Control	https://attack.mitre.org/mitigations/M1052/
prevent WScript and Powershell running on PCs	Execution Prevention	https://attack.mitre.org/mitigations/M1038/
MFA	Multi-factor authentication	https://attack.mitre.org/mitigations/M1032/
increased internet restrictions including geoblocking	Restrict Web-Based Content	https://attack.mitre.org/mitigations/M1021/
replaced domain accounts with local accounts for services and tasks	Privileged Account Management	https://attack.mitre.org/mitigations/M1026/
prevent service accounts logging onto file shares or interactively	Remote Data Storage	https://attack.mitre.org/mitigations/M1029/
prevent task accounts logging onto file shares (unless for that task) or interactively.	Remote Data Storage	https://attack.mitre.org/mitigations/M1029/
put in Microsoft LAPS so every computer has a unique admin password	Privileged Account Management	https://attack.mitre.org/mitigations/M1026/
overwrite registry areas attackers target	Restrict Registry Permissions	https://attack.mitre.org/mitigations/M1024/

Masking with the Mitigations



AUSCERT

FIRST Improving Security Together

What we did not cover

- Layering the data
  - Initial techniques identified
  - Initial software
  - Lessons learnt mitigation
  - Lessons learnt technique expansion

- A lot of other features of the Navigator

- Refine the Broad brush used
  - E.g. Privilege Account Management M1026 => VERY BROAD BRUSH INDEED

  - **Missing items in ATT&CK**
  - The case of double extortion
  - There is: T1486 Data Encrypted for Impact
  - But there is no “Devaluation of Documented Assets – public release”

Homework

- TASK 1 – Statement into Framework Navigator

Statement : https://forums.whirlpool.net.au/thread/3xv6604y

Framework : https://mitre-attack.github.io/attack-navigator/

Directions:
Do the same as you have been shown and then expand perhaps on

o Using different layers
o Saving into a JSON file
o Loading the JSON file

- TASK 2 – CONTI Playbook into Framework Navigator

o Distil/Summarise the commands into techniques

o Make a table of key words you searched and the matching techniques

o Add the Techniques into the ATT&CK Navigator.

Framework : https://mitre-attack.github.io/attack-navigator/

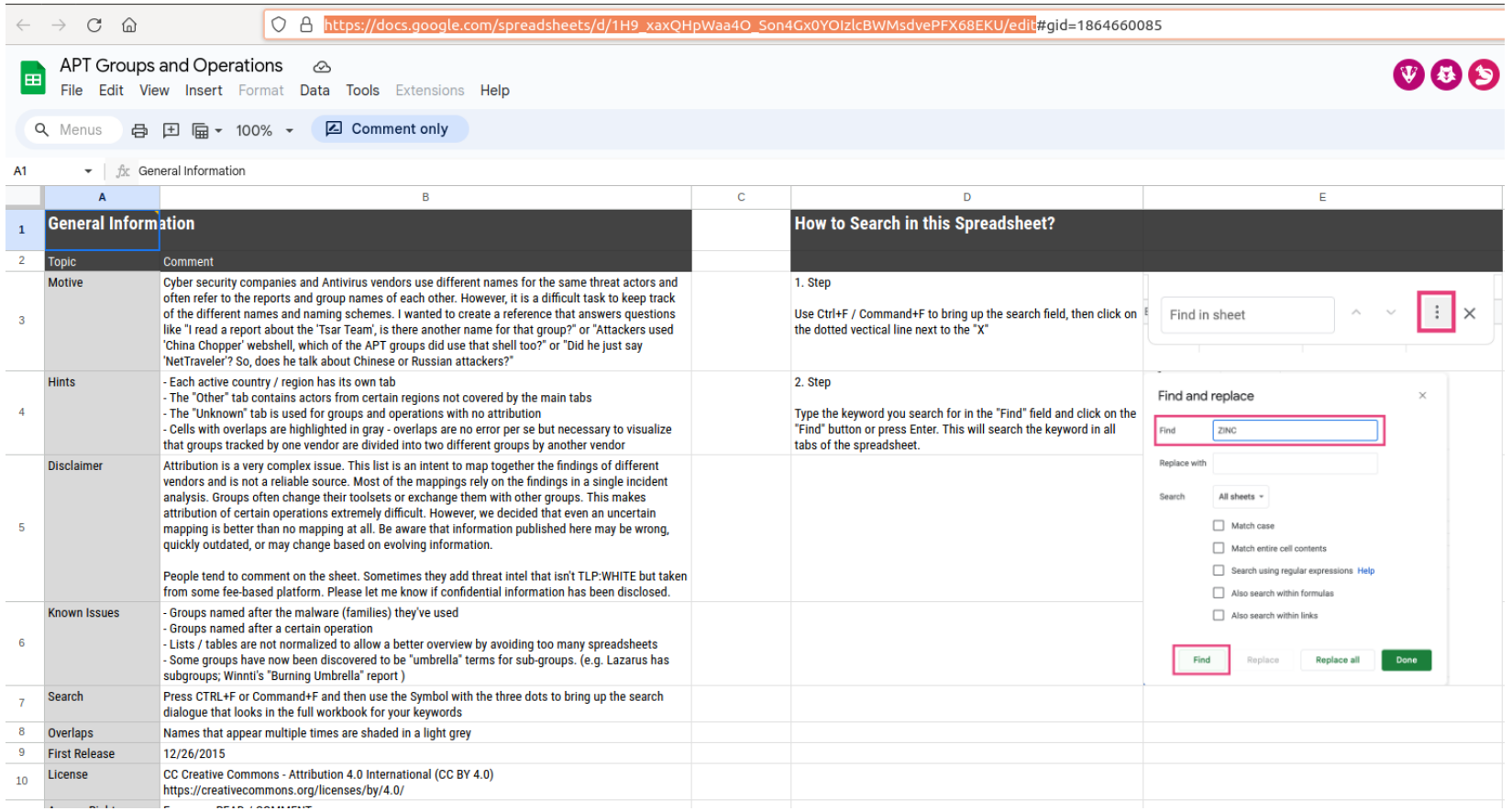
Playbook : Conti Playbook

Cheetsheet: https://github.com/DISREL/Conti-Leaked-Playbook-TTPs/blob/main/Conti-Leaked-Playbook-TTPs.pdf
https://github.com/j91321/conti-manuals-analysis

Exercise

Filling up the Cybersecurity Framework covering an industry

APT Group and Operations



https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085

APT Groups and Operations

File Edit View Insert Format Data Tools Extensions Help

Menus 100% Comment only

A1 General Information

	A	B	C	D	E
1	**General Information**			**How to Search in this Spreadsheet?**	
2	Topic	Comment			
3	Motive	Cyber security companies and Antivirus vendors use different names for the same threat actors and often refer to the reports and group names of each other. However, it is a difficult task to keep track of the different names and naming schemes. I wanted to create a reference that answers questions like "I read a report about the 'Tsar Team', is there another name for that group?" or "Attackers used 'China Chopper' webshell, which of the APT groups did use that shell too?" or "Did he just say 'NetTraveler'? So, does he talk about Chinese or Russian attackers?"		1. Step Use Ctrl+F / Command+F to bring up the search field, then click on the dotted vectical line next to the "X"	
4	Hints	- Each active country / region has its own tab - The "Other" tab contains actors from certain regions not covered by the main tabs - The "Unknown" tab is used for groups and operations with no attribution - Cells with overlaps are highlighted in gray - overlaps are no error per se but necessary to visualize that groups tracked by one vendor are divided into two different groups by another vendor		2. Step Type the keyword you search for in the "Find" field and click on the "Find" button or press Enter. This will search the keyword in all tabs of the spreadsheet.	
5	Disclaimer	Attribution is a very complex issue. This list is an intent to map together the findings of different vendors and is not a reliable source. Most of the mappings rely on the findings in a single incident analysis. Groups often change their toolsets or exchange them with other groups. This makes attribution of certain operations extremely difficult. However, we decided that even an uncertain mapping is better than no mapping at all. Be aware that information published here may be wrong, quickly outdated, or may change based on evolving information. People tend to comment on the sheet. Sometimes they add threat intel that isn't TLP:WHITE but taken from some fee-based platform. Please let me know if confidential information has been disclosed.			
6	Known Issues	- Groups named after the malware (families) they've used - Groups named after a certain operation - Lists / tables are not normalized to allow a better overview by avoiding too many spreadsheets - Some groups have now been discovered to be "umbrella" terms for sub-groups. (e.g. Lazarus has subgroups; Winnti's "Burning Umbrella" report)			
7	Search	Press CTRL+F or Command+F and then use the Symbol with the three dots to bring up the search dialogue that looks in the full workbook for your keywords			
8	Overlaps	Names that appear multiple times are shaded in a light grey			
9	First Release	12/26/2015			
10	License	CC Creative Commons - Attribution 4.0 International (CC BY 4.0) https://creativecommons.org/licenses/by/4.0/			

https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit

AUSCERT

Threat card

ETDA

IDENTIFY

ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Electronic Transactions Development Agency

Groups Tools Search Statistics

Home Search

Threat Group Cards: A Threat Actor Encyclopedia

Main menu

- Browse threat groups
- Browse their tools
- Search
- Statistics

AUSCERT

ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Electronic Transactions Development Agency

IDENTIFY

Groups Tools Search Statistics

Home > Search

Threat Group Cards: A Threat Actor Encyclopedia

Database search

Actor

Source country: ...

Victim country: ... or Worldwide

Victim sector: Government

Motivation: ...

Free text search: (can use '*' and '?' wildcards)

Search!

AUSCERT ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ Electronic Transactions Development Agency

IDENTIFY

Groups Tools Search Statistics

Threat Group Cards: A Threat Actor Encyclopedia

All groups targeting sector Government

Changed	Name	Country	Observed
APT groups			
	Aggah	[Unknown]	2018-Jun 2022
	Anchor Panda, APT 14		2012
	Aoqin Dragon		2013
	APT 4, Maverick Panda, Wisp Team		2007-Oct 2018
	APT 6		2011
	APT 12, Numbered Panda		2009-Nov 2016

Result

- APT group: APT 29, Cozy Bear, The Dukes
- APT group: Bad Magic, RedStinger
- APT group: ChamelGang
- Permanent link APT group: Volt Typhoon
- APT group: Reaper, APT 37, Ricochet Chollima, ScarCruft
- APT group: Mustang Panda, Bronze President
- APT group: MuddyWater, Seedworm, TEMP.Zagros, Static Kitten
- APT group: Magic Hound, APT 35, Cobalt Illusion, Charming Kitten
- APT group: Lazarus Group, Hidden Cobra, Labyrinth Chollima
- APT group: Kimsuky, Velvet Chollima
- APT group: Donot Team

MITRE ATT&CK™

AUSCERT

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Campaigns | Resources | Blog | Contribute | Search

MATRICES

- Enterprise
  - PRE
  - Windows
  - macOS
  - Linux
  - Cloud
  - Network
  - Containers
- Mobile
- ICS

Home > Matrices > Enterprise

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

View on the ATT&CK® Navigator

Version Permalink

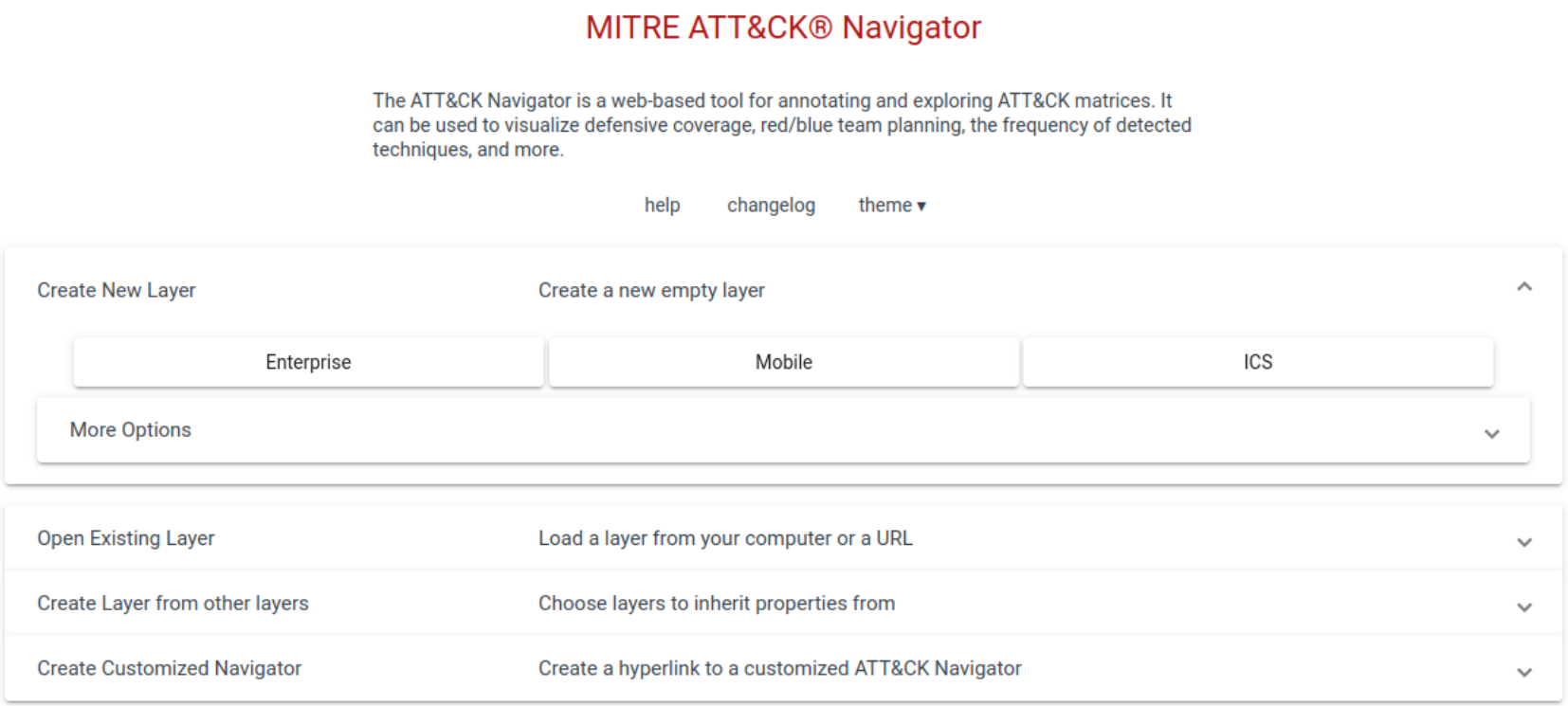
layout: side | show sub-techniques | hide sub-techniques | help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collec
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techn
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Access Token Manipulation (5)	BITS Jobs	Credentials from Password Stores (5)	Browser Information Discovery	Lateral Tool Transfer	Audio Cap
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (7)	Browser Session Hijacking
Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard
Search Closed Sources (2)	Obtain Capabilities (6)	Supply Chain	Native API	Create Account	Domain Policy Modification (2)	Deploy Container	Input Capture	Cloud Storage Object Discovery		Data from Cloud Sto
Search Open	Stage Capabilities					Direct Volume Access		Container and Resource Discovery		Data from
						Domain Policy Modification (2)				

FIRST

AUSCERT

Navigator



https://mitre-attack.github.io/attack-navigator/

AUSCERT

about

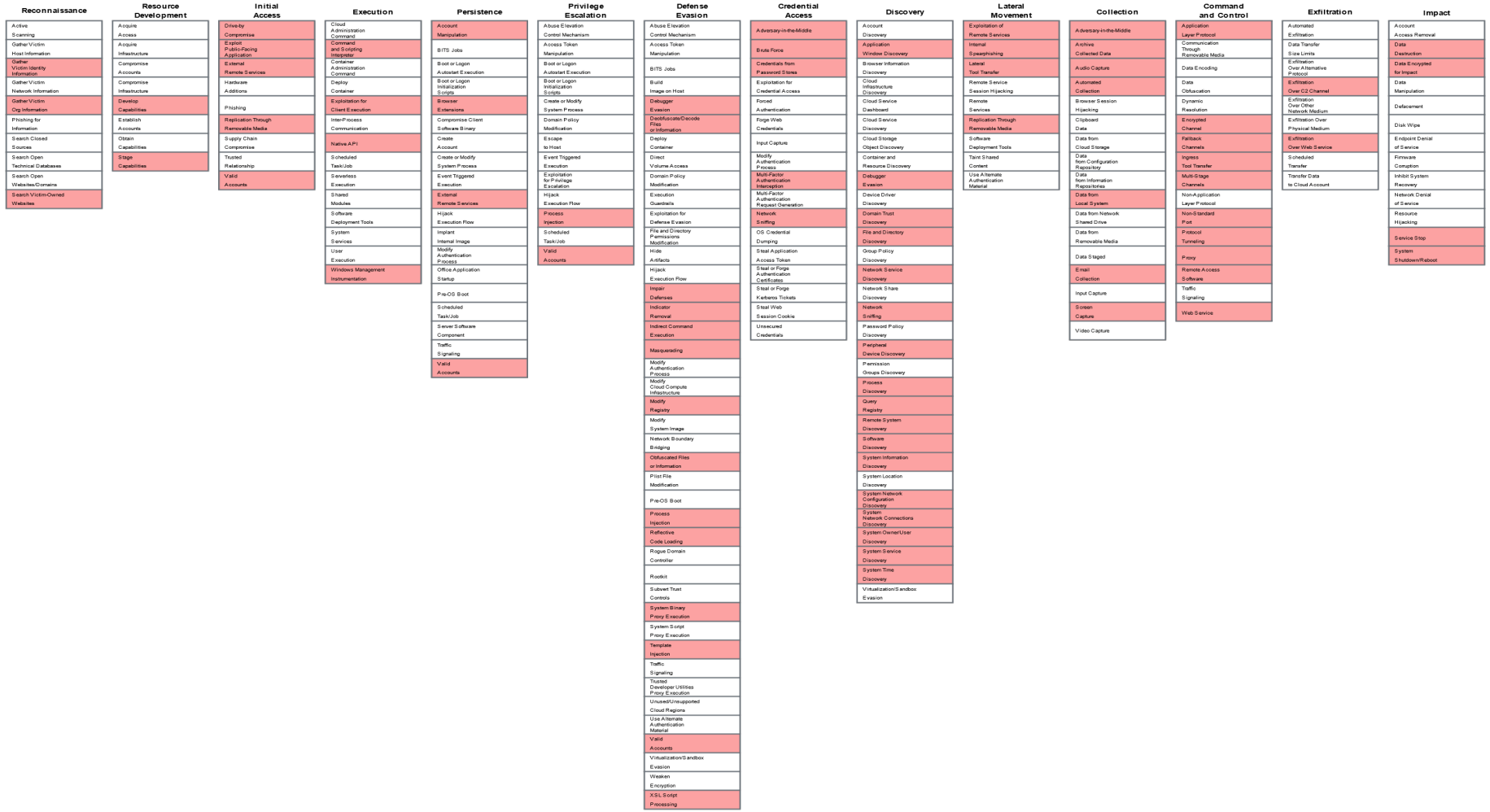
Government

domain

Enterprise ATT&CK v13

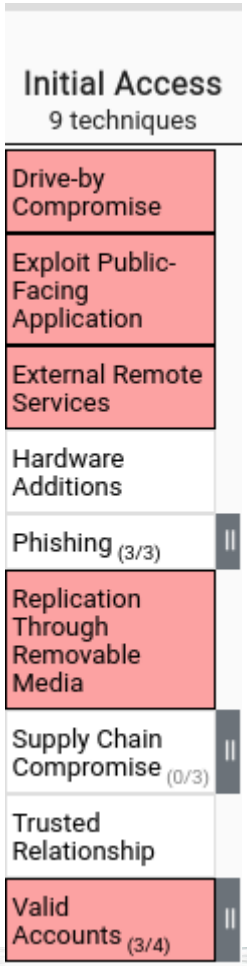
platforms

Linux, macOS, Windows,
Network, PRE, Containers, Office 365,
SaaS, Google Workspace, IaaS, Azure AD



AUSCERT

Initial Access



- (T1189) Drive by Compromise
- (T1190) Exploit Public facing Application
- (T1133) External Remote Service
- (T1091) Replication Through Removable Media
- (T1078) Valid Accounts

Application of Risk on a Service

AUSCERT

CSIRT Services

- Search Term “CSIRT Service Framework 2.1”
- Target Link : https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- Looks Like

AUSCERT

Malicious Domain Notification

- When the CSIRT knows of a domain that is Malicious and requests a corrective action from the domain registrar.
- Specific condition of a “take down request”
  - Different than a content take down
  - Different than a host take down

japan-ja1.jp

Source: https://github.com/JPCERTCC/phishurl-list/blob/main/2023/202306.csv

AUSCERT

Domains

Centralised Zone Data Service

Delegation Record

URL to Registration service

Domain Registrar

Domain Registrar
Domain Registrar

AUSCERT

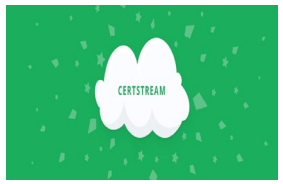
Domain Data repositories (simplification)

japan-ja1.jp

ICANN CZDS

Domain NIC

Certificate Transparency



A-Record (online)

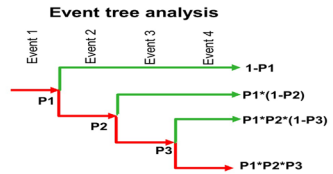
Analysis Repositories

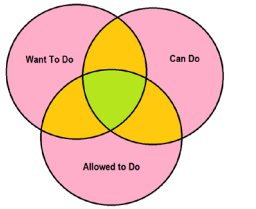
PhishTank®

“60% of all phishing domains stay alive for only 10 minutes.” - google

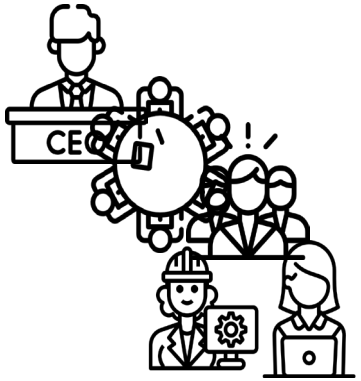
AUSCERT

When can you make a notice?





anz-co-nz.com
anz-mobile.secur4unlock-au.online
ato-augov.org
atotaxfile-mygov.site
aumygovtxrefund.info
auspost-australia-online.com
centre1ink00rev1ew.top
mail.mygovid-account.com
verify0centrelink09.info
www.commbankaustralia.com

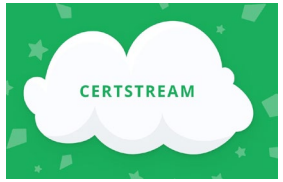


ICANN

CZDS

Domain NIC

Certificate Transparency



A-Record (online)

Analysis Repositories

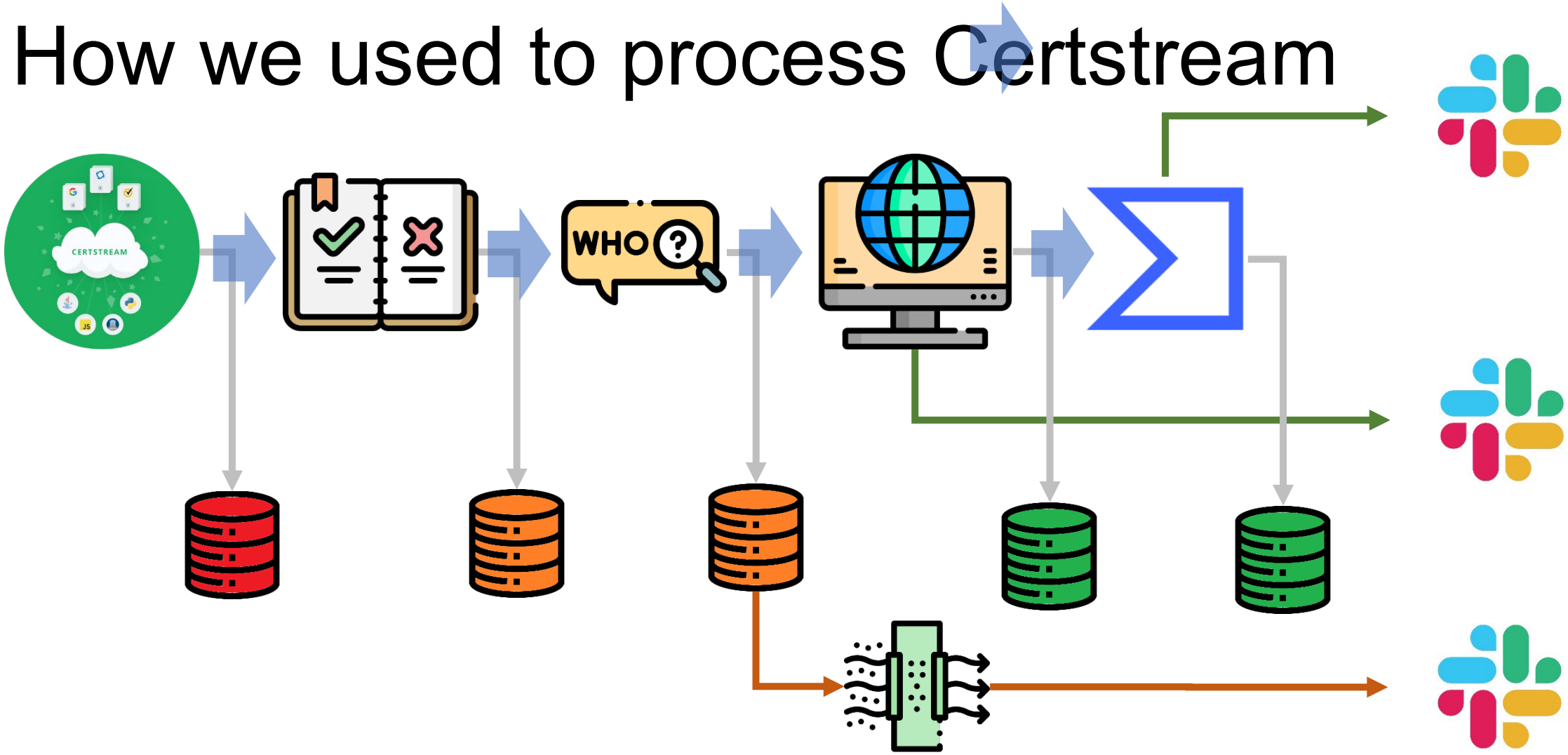
"60% of all phishing domains stay alive for only 10 minutes." - google

PhishTank®

Certstream Recap

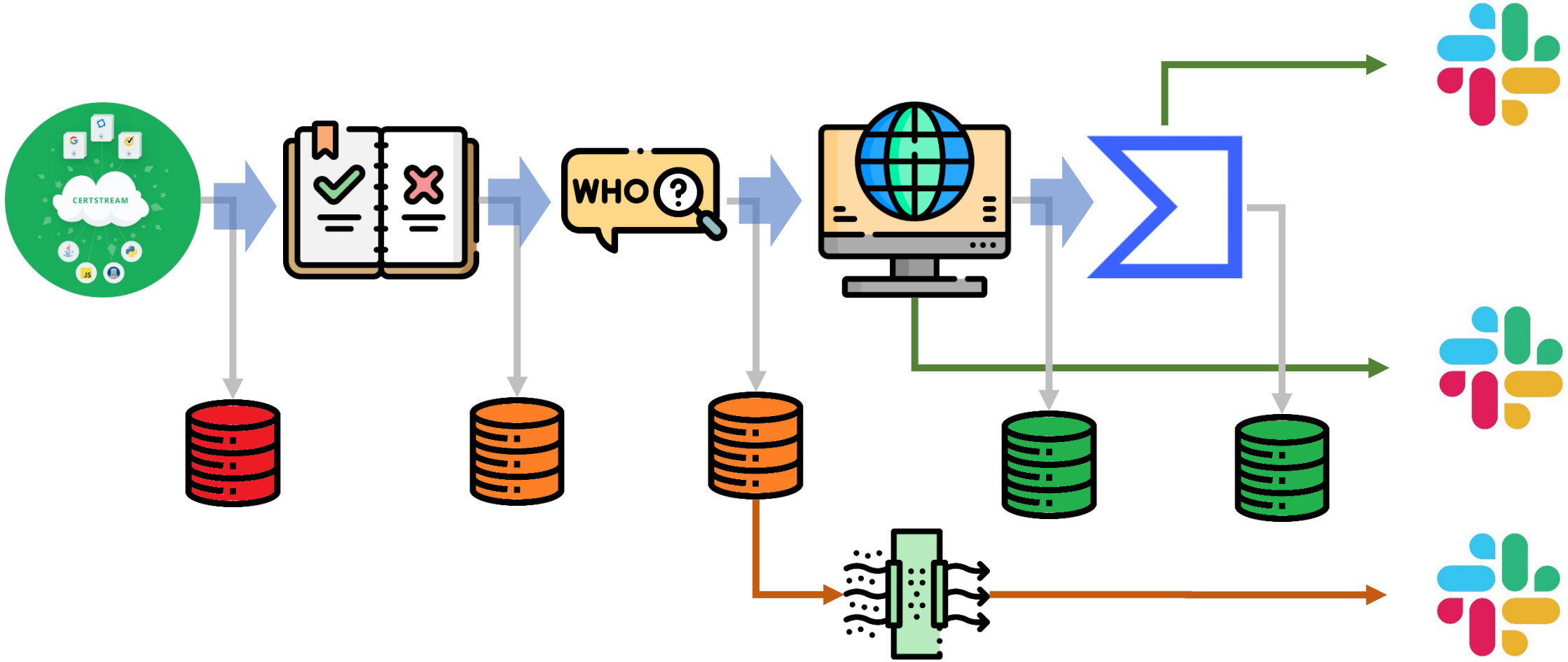
Can it really be done?

How we used to process Certstream

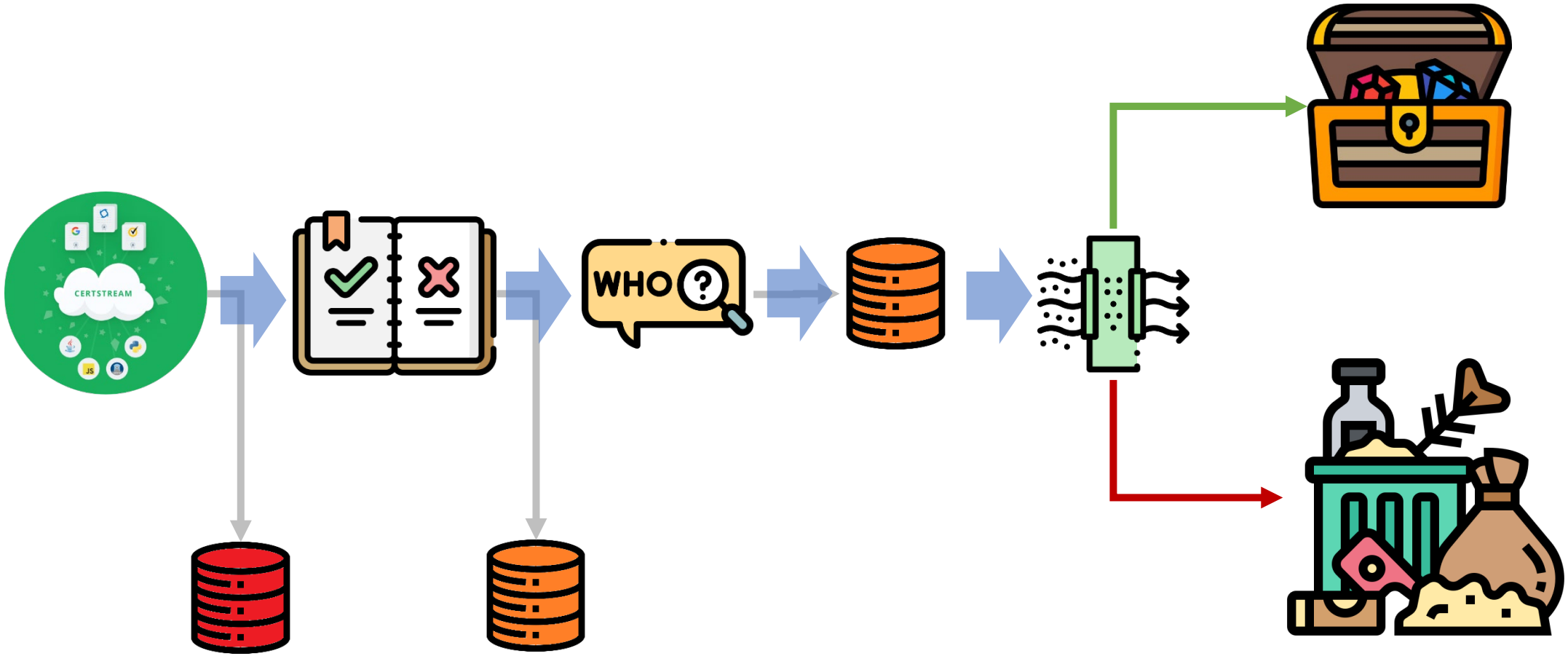


AUSCERT

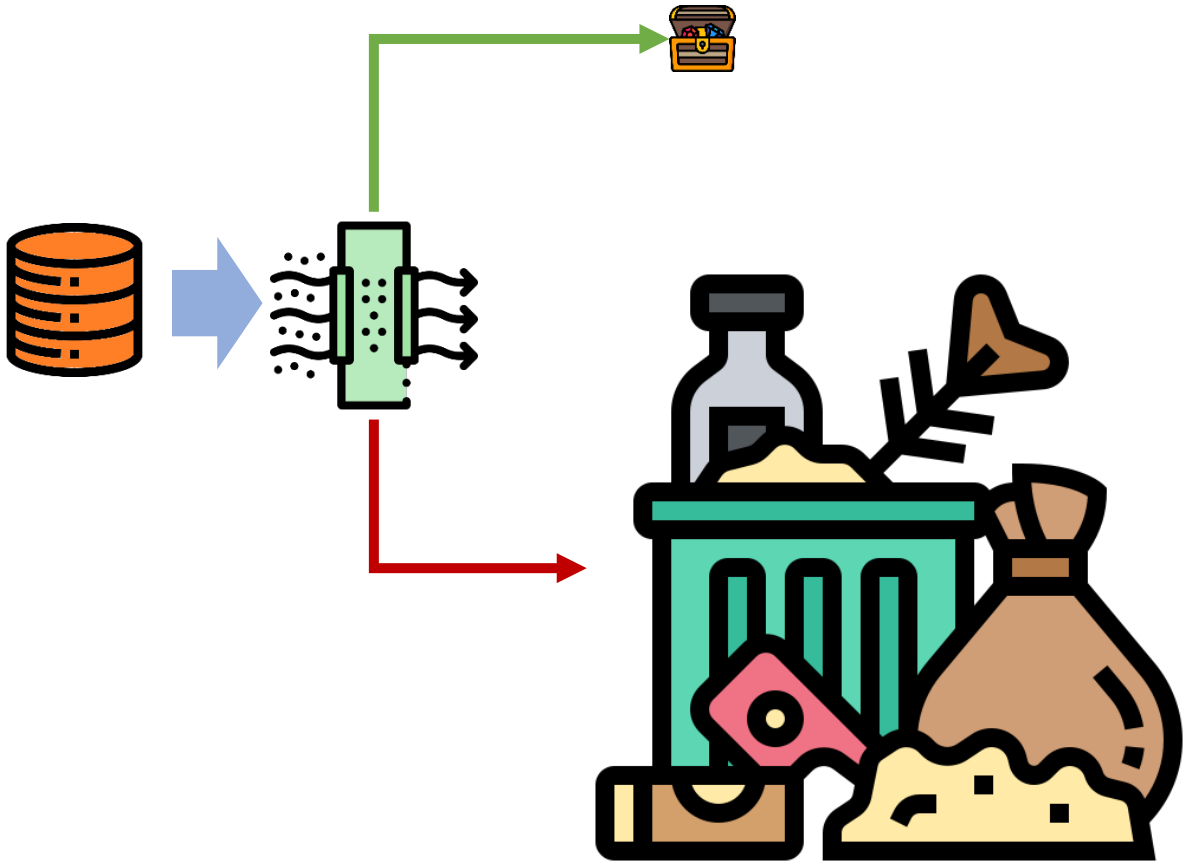
How we should to process Certstream

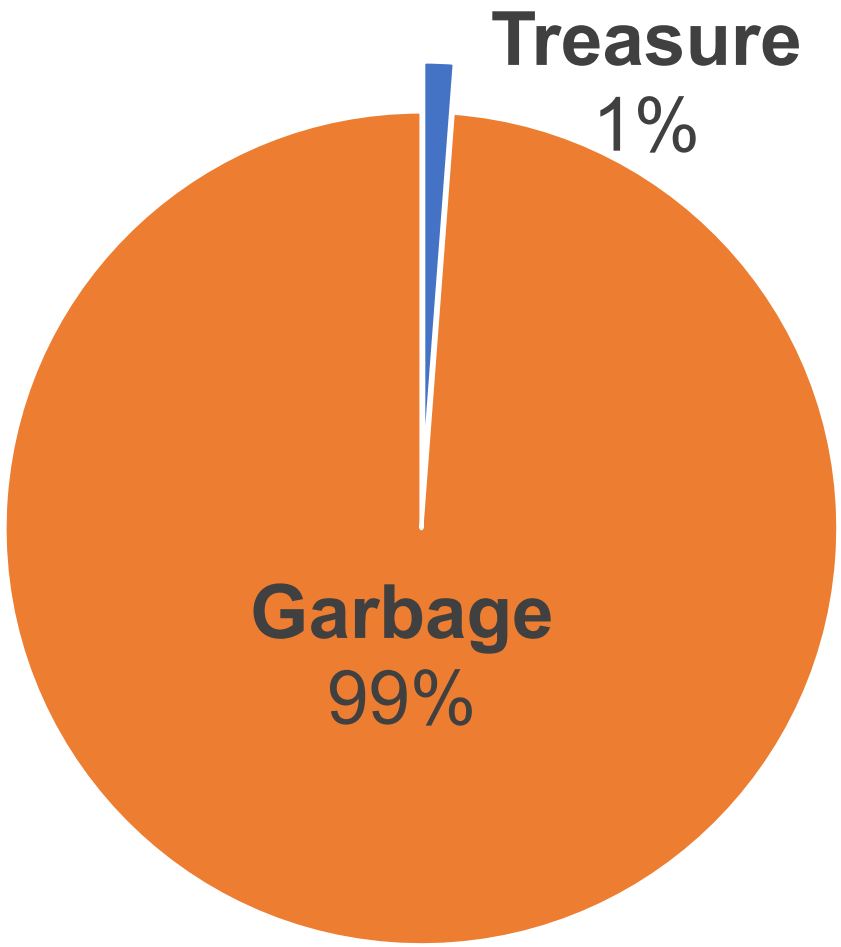


How we should process phishy domains

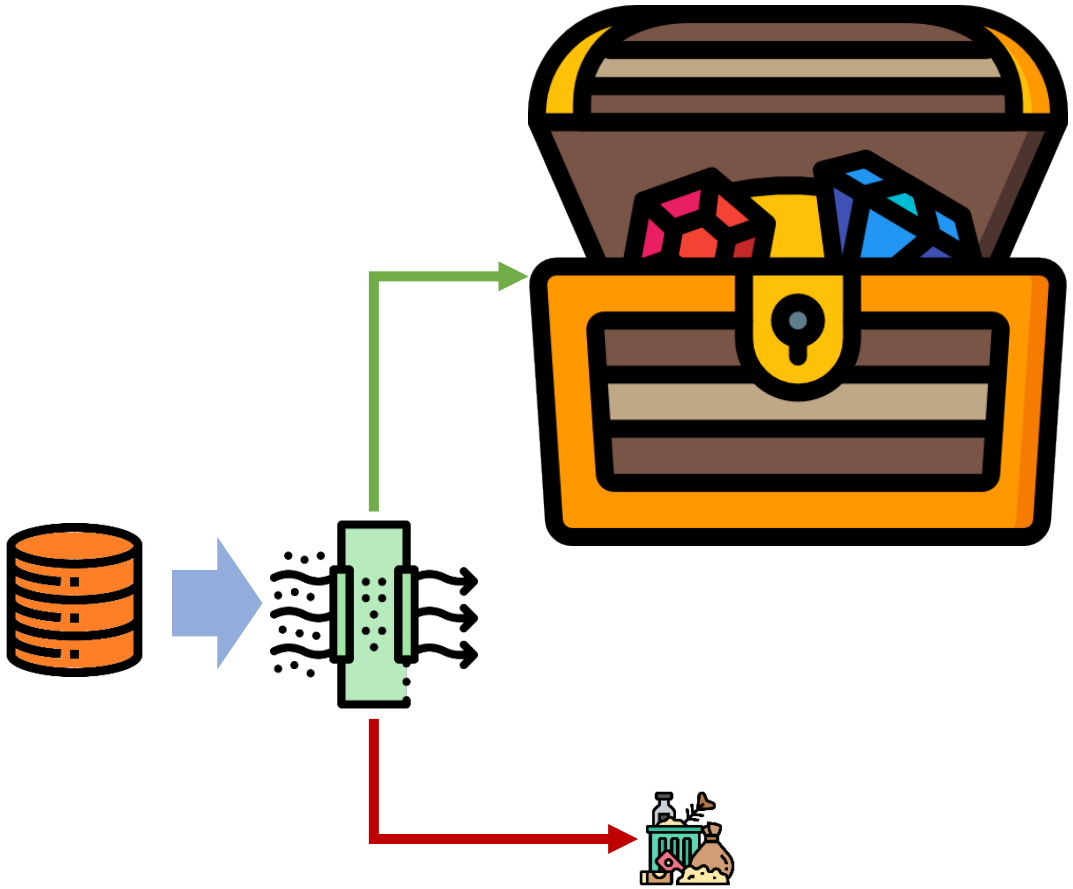


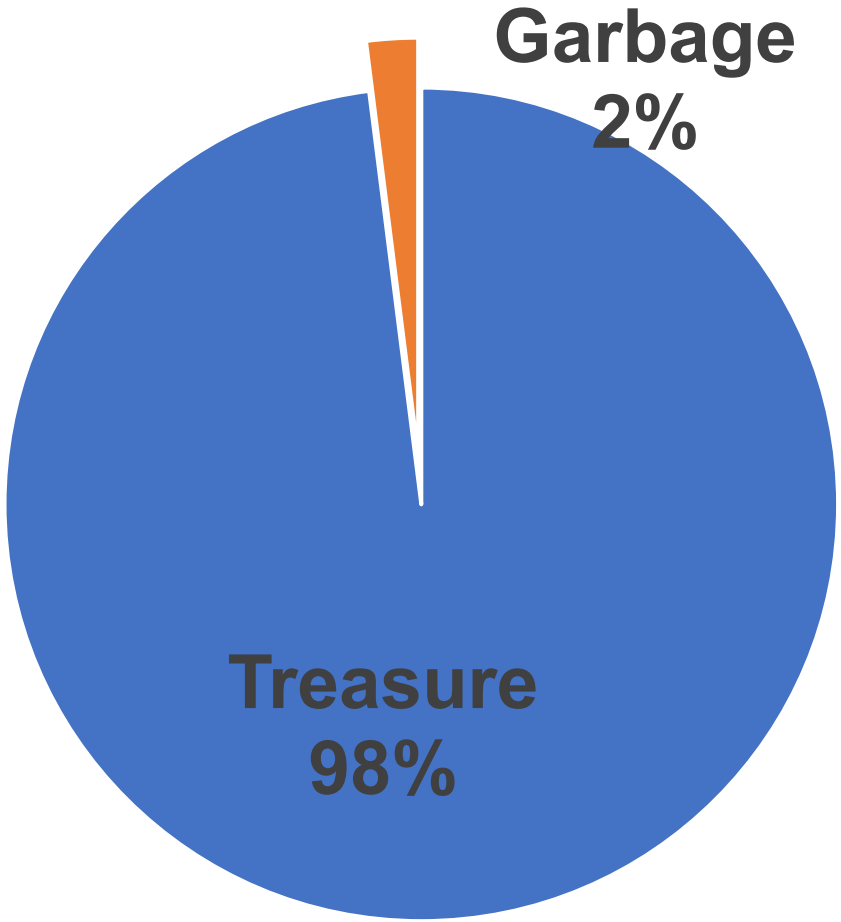
Treasure Vs Garbage (Rules Based)



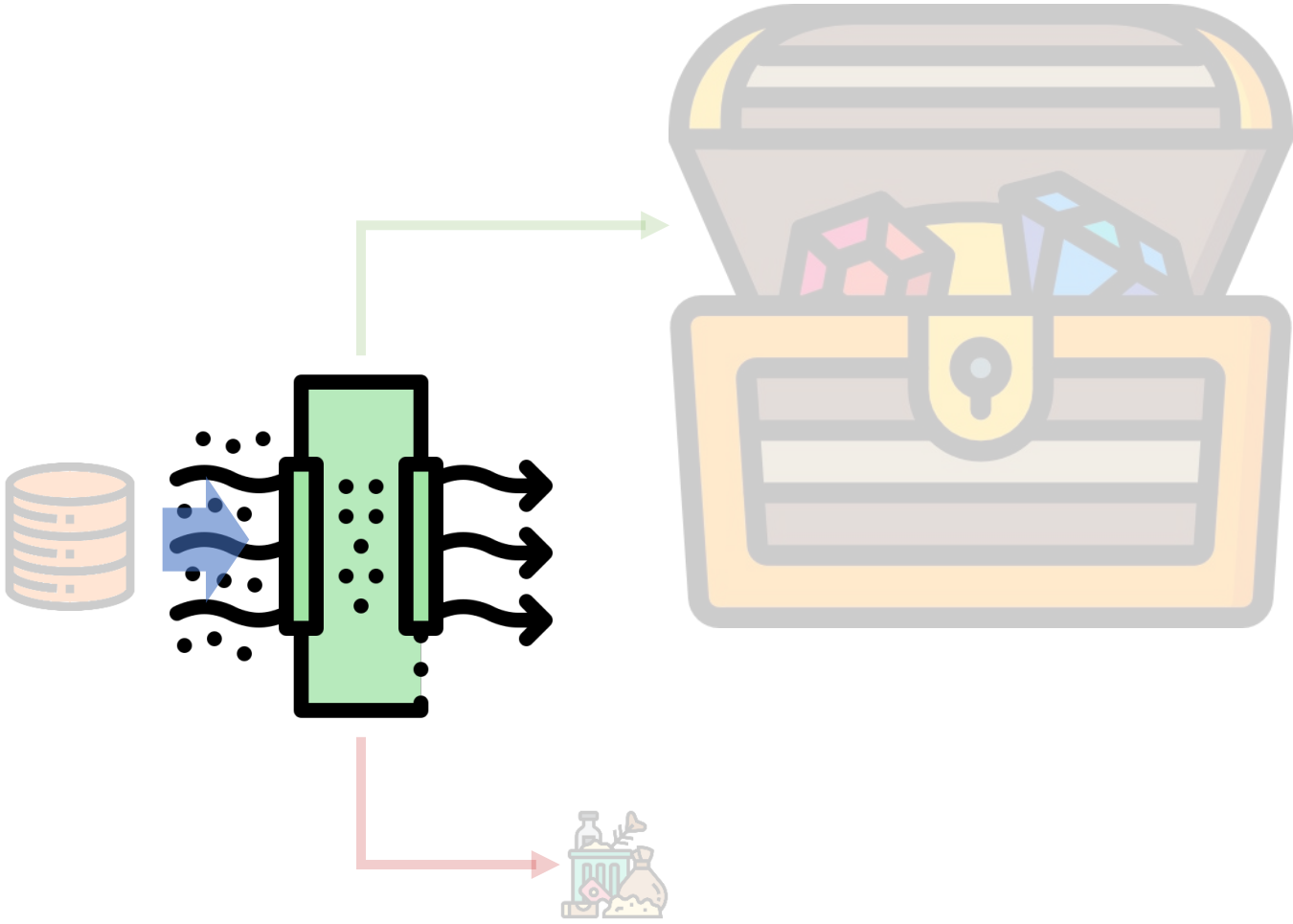


Treasure Vs Garbage (Required Filter)

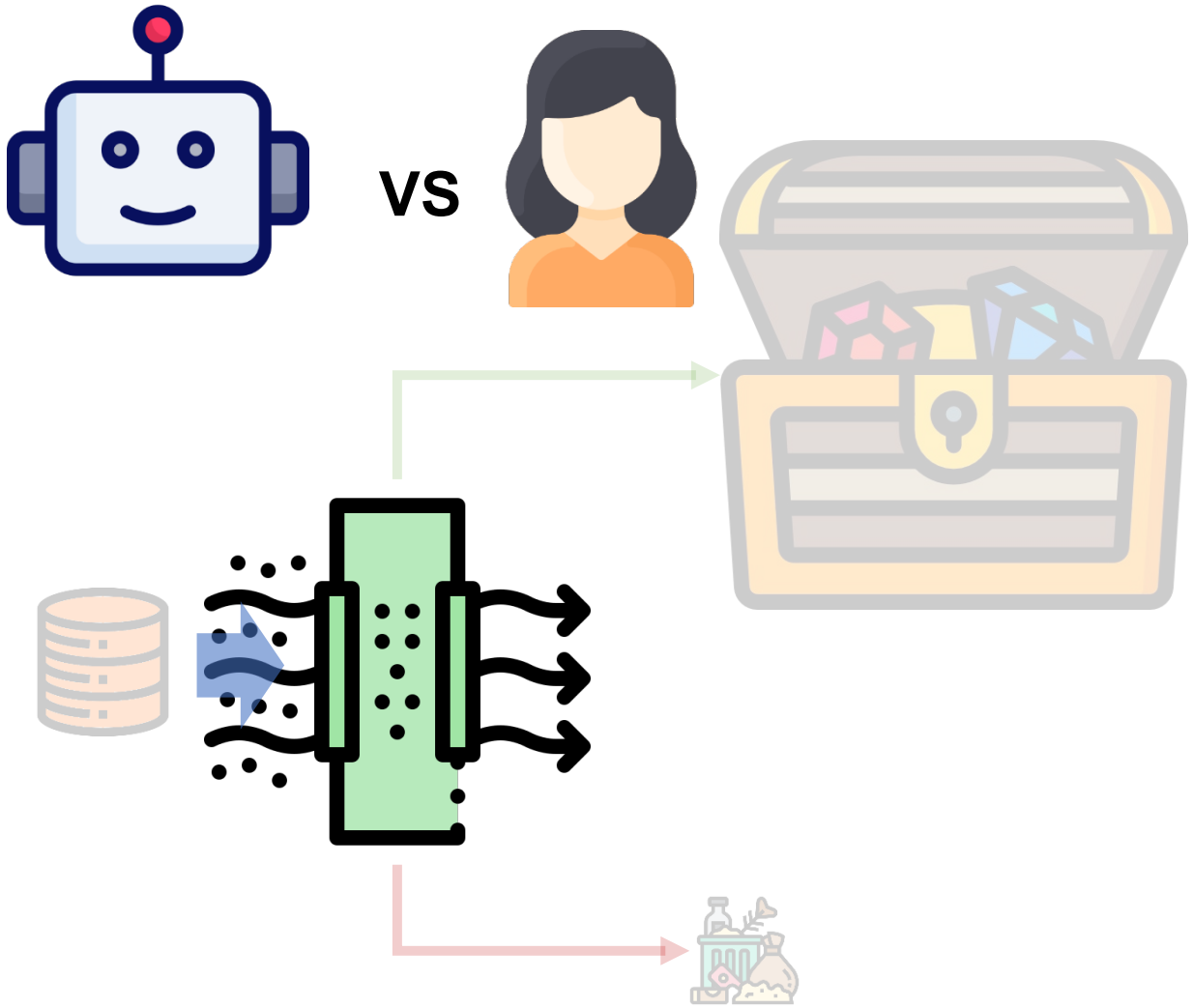




Filter of Treasure Vs Garbage

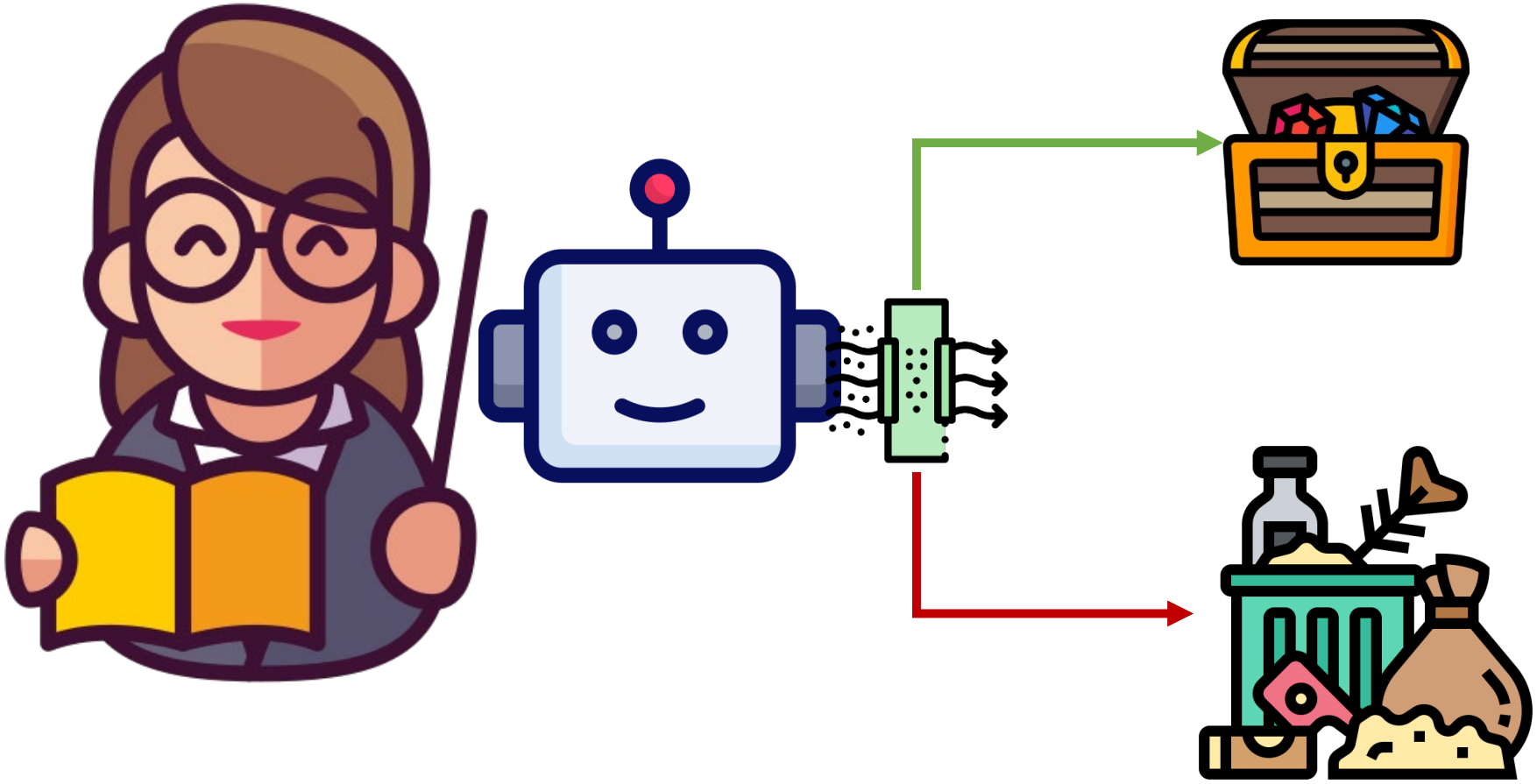


Machine - Human



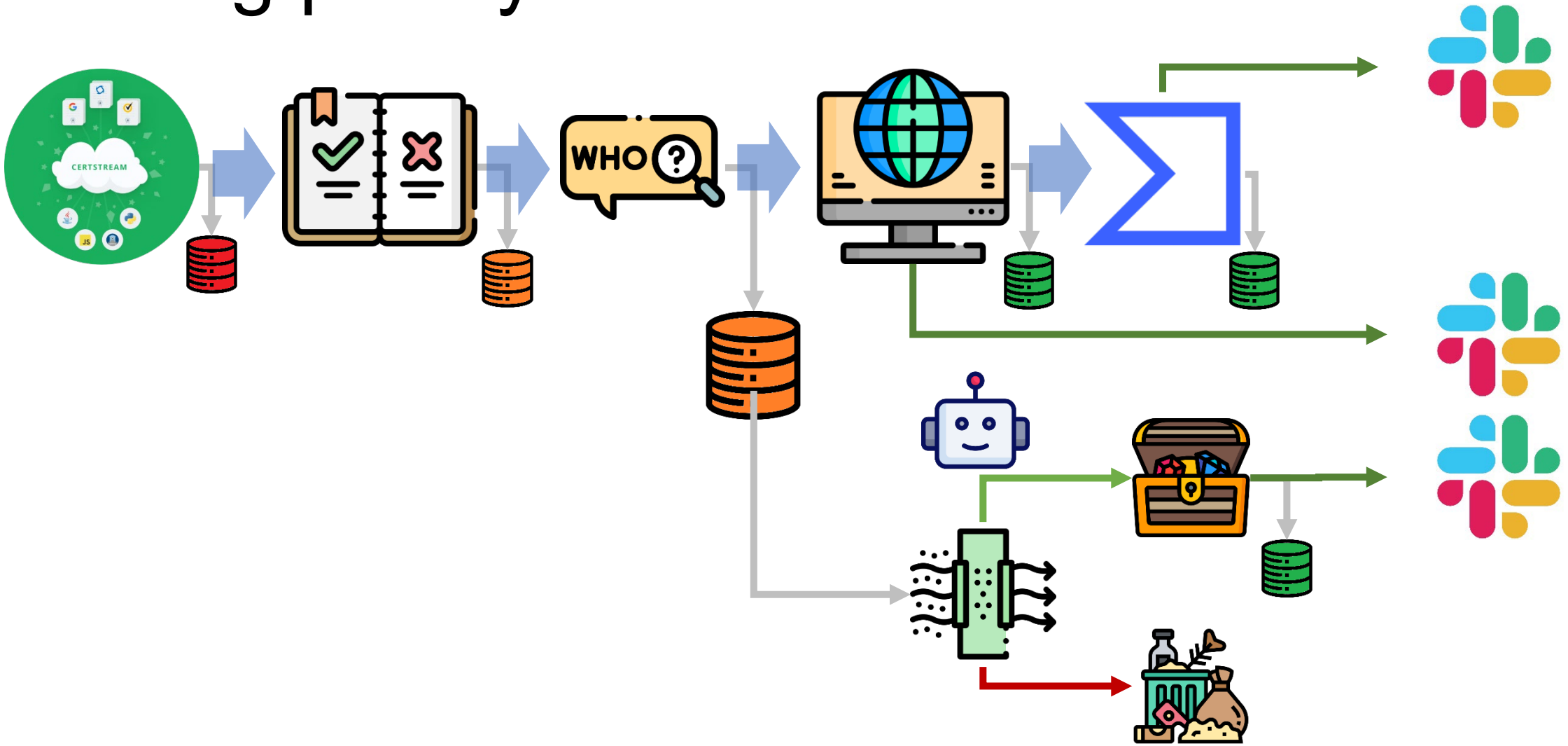
AUSCERT

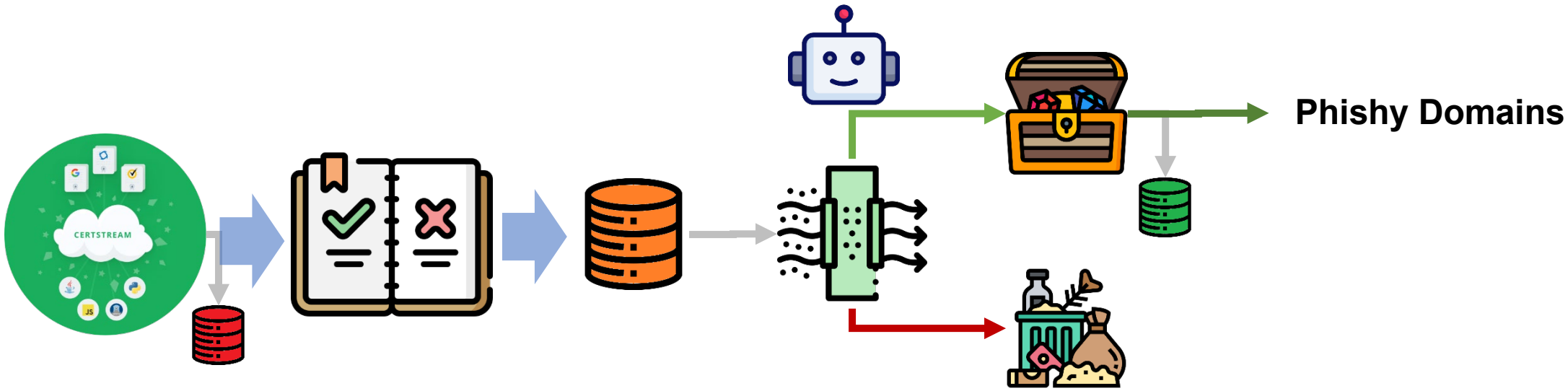
Teaching the Machine



AUSCERT

Getting phishy domains before online





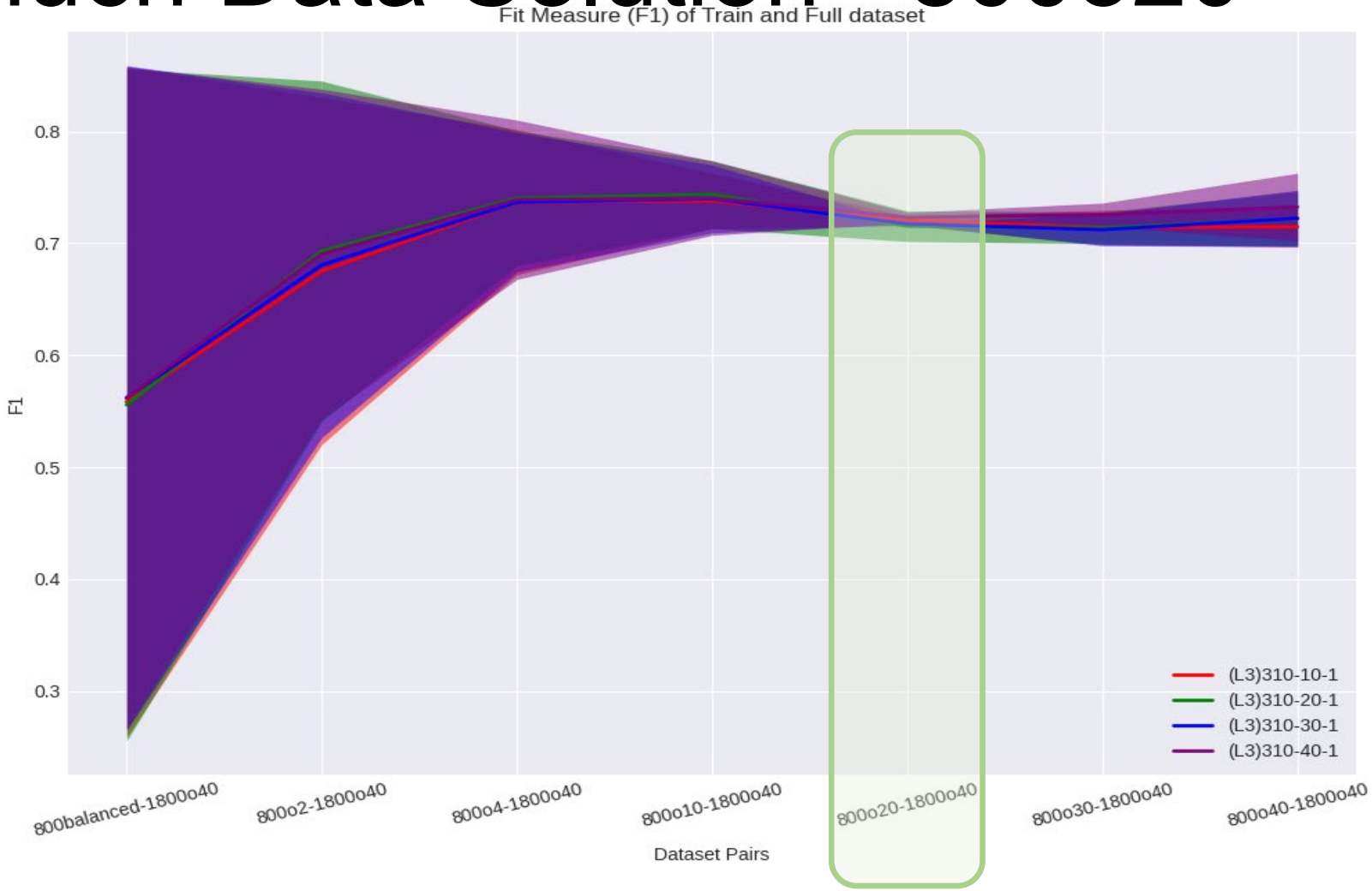
High volume / Low confidence data

Medium volume / Medium confidence data

Low volume / High confidence data

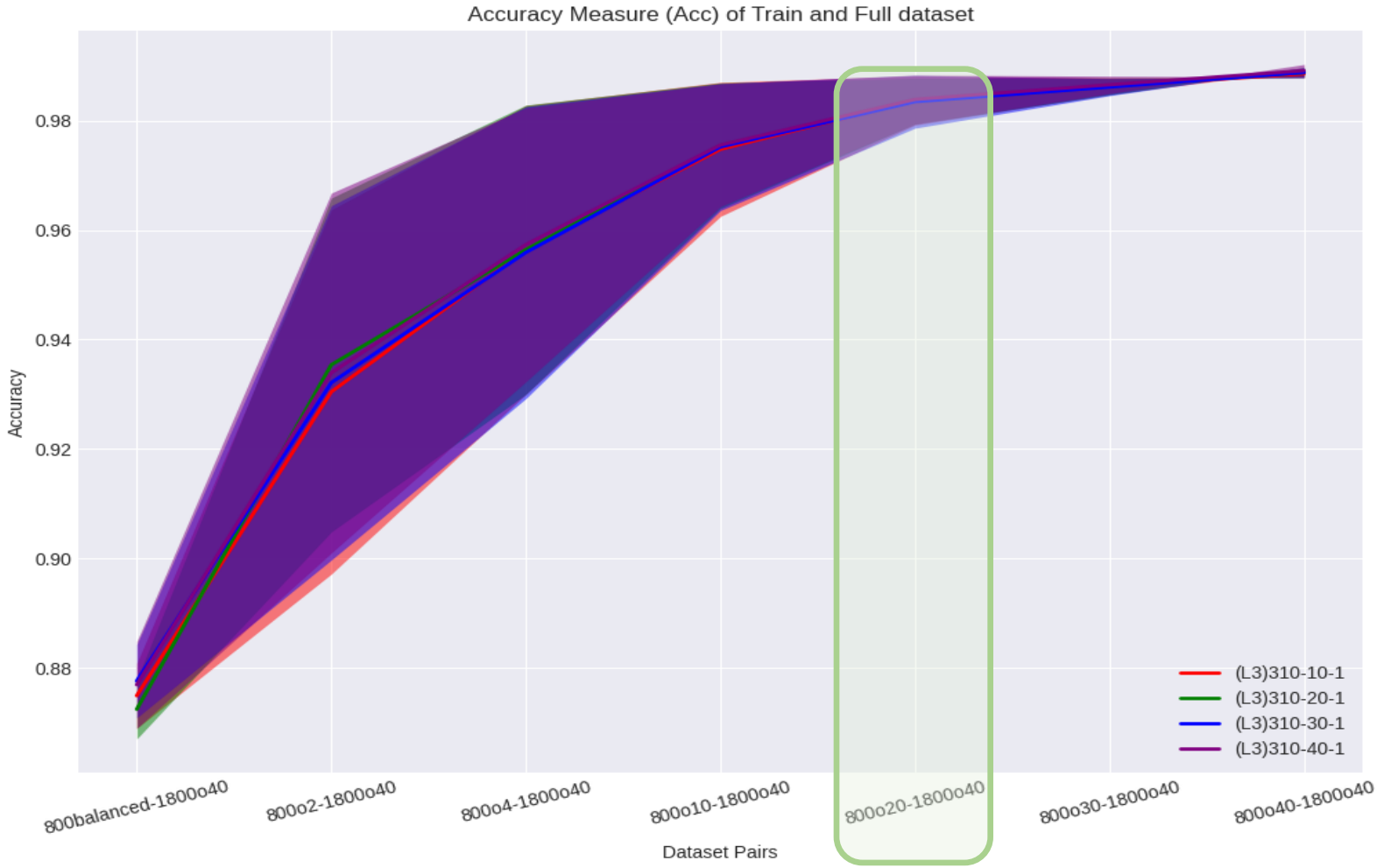
AUSCERT

How Much Data Solution ~800o20



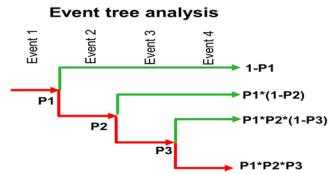
AUSCERT

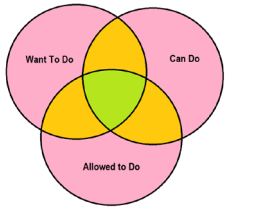
How Much Data Solution ~800o20



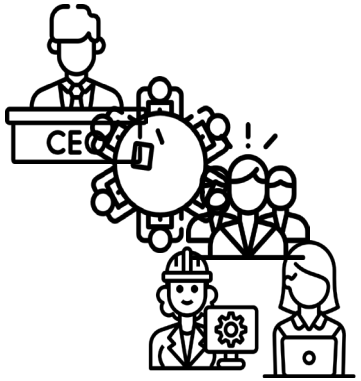
AUSCERT

When can you make a notice?





anz-co-nz.com
anz-mobile.secur4unlock-au.online
ato-augov.org
atotaxfile-mygov.site
aumygovtxrefund.info
auspost-australia-online.com
centre1ink00rev1ew.top
mail.mygovid-account.com
verify0centrelink09.info
www.commbankaustralia.com

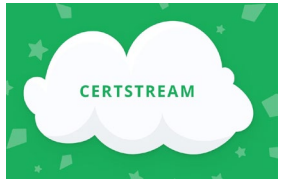


ICANN

CZDS

Domain NIC

Certificate Transparency



A-Record (online)

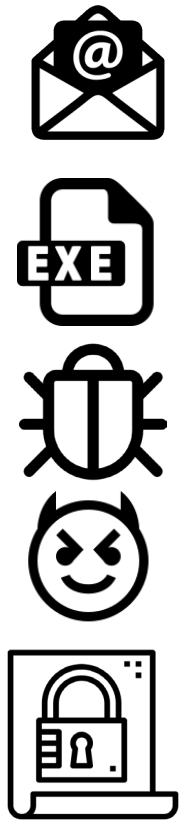
Analysis Repositories

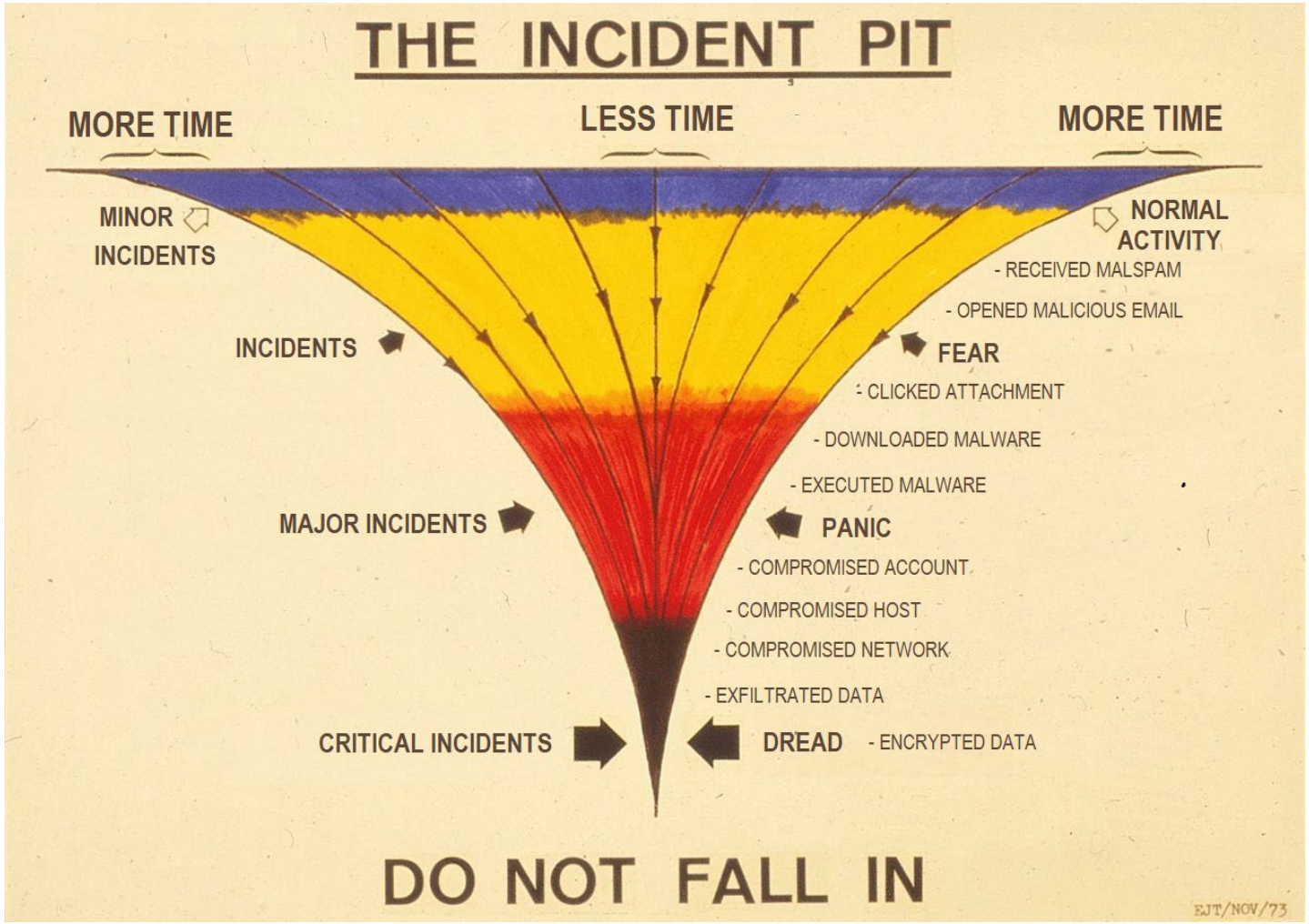
"60% of all phishing domains stay alive for only 10 minutes." - google

PhishTank®

AUSCERT

Incident Pit – Cybersecurity





AUSCERT

Take Aways

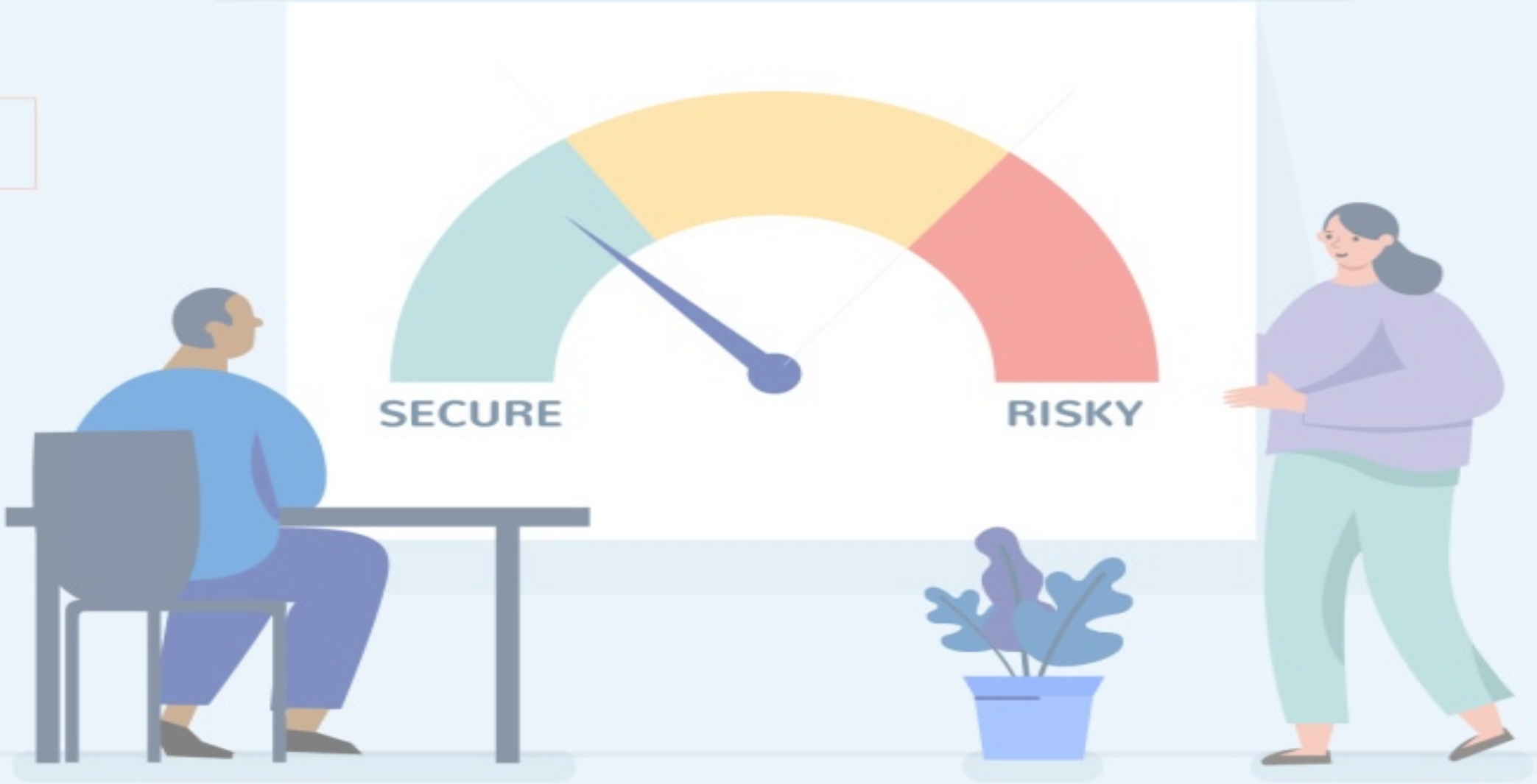
- Activity Risk = (Inherent Risk) * (Control Failure)

  - Avoid Risk
  - Mitigate Risk
  - Transfer Risk
  - Accept Risk

  - Preventative Controls
  - Detective Control
  - Corrective Controls

- Risk assessment must be a Repeatable process (Qualitative or Quantitative)

Cybersecurity: A Risky Business



FIRST Regional Symposium for the Pacific
Port Vila, Vanuatu, Sep 22nd 2023