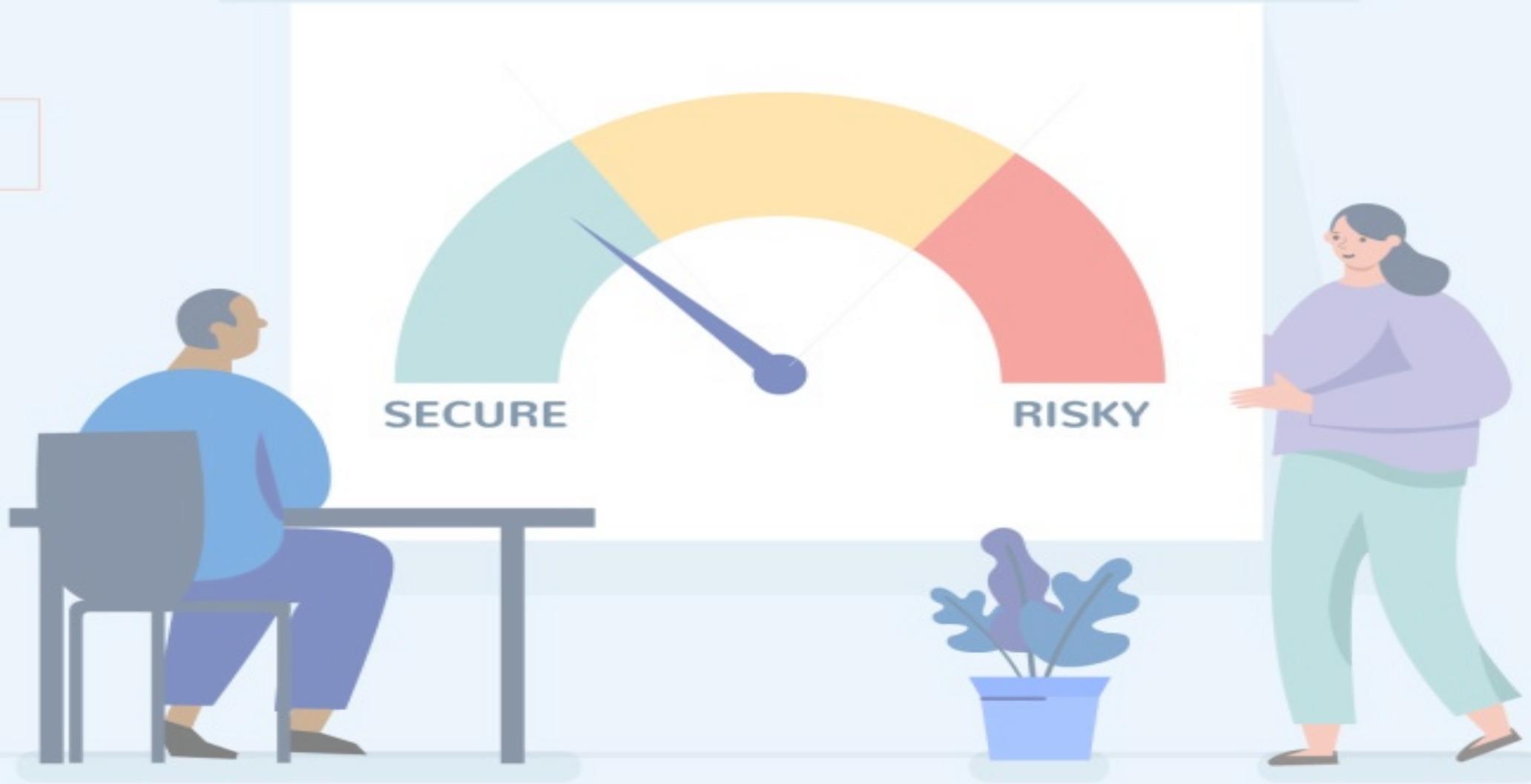


# Cybersecurity: A Risky Business



FIRST Regional Symposium for the Pacific  
Port Vila, Vanuatu, Sep 22<sup>nd</sup> 2023



# PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

# Thanks



# Take Aways

**DON'T  
PANIC**

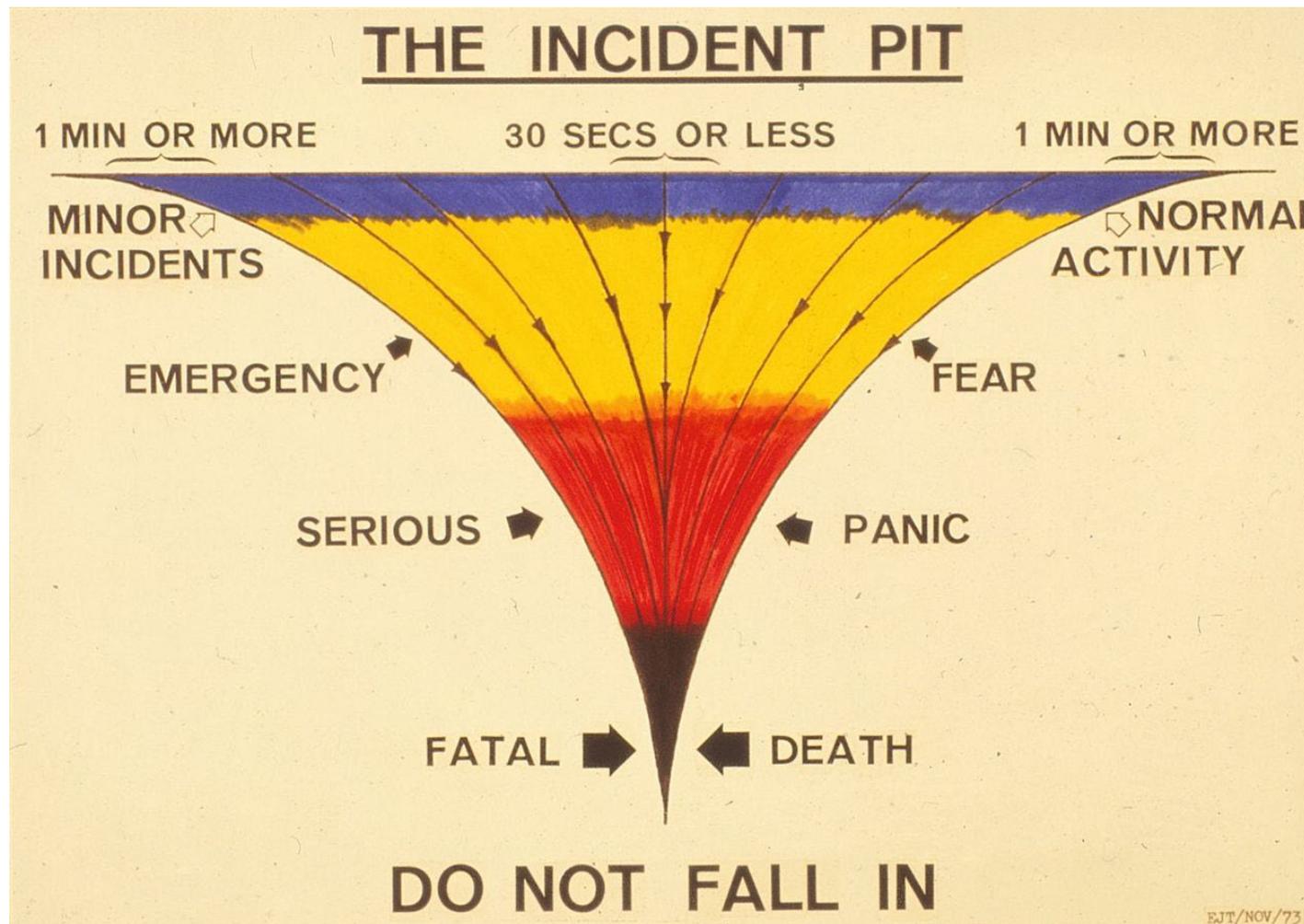
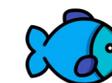
- Activity Risk = (Inherent Risk) \* (Control Failure)
  - Avoid Risk
  - Mitigate Risk
  - Transfer Risk
  - Accept Risk
  - Preventative Controls
  - Detective Control
  - Corrective Controls
- Risk assessment must be a Repeatable process (Qualitative or Quantitative)

# Learning Objectives

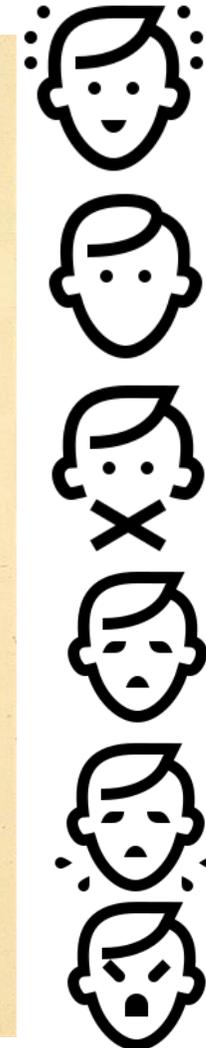
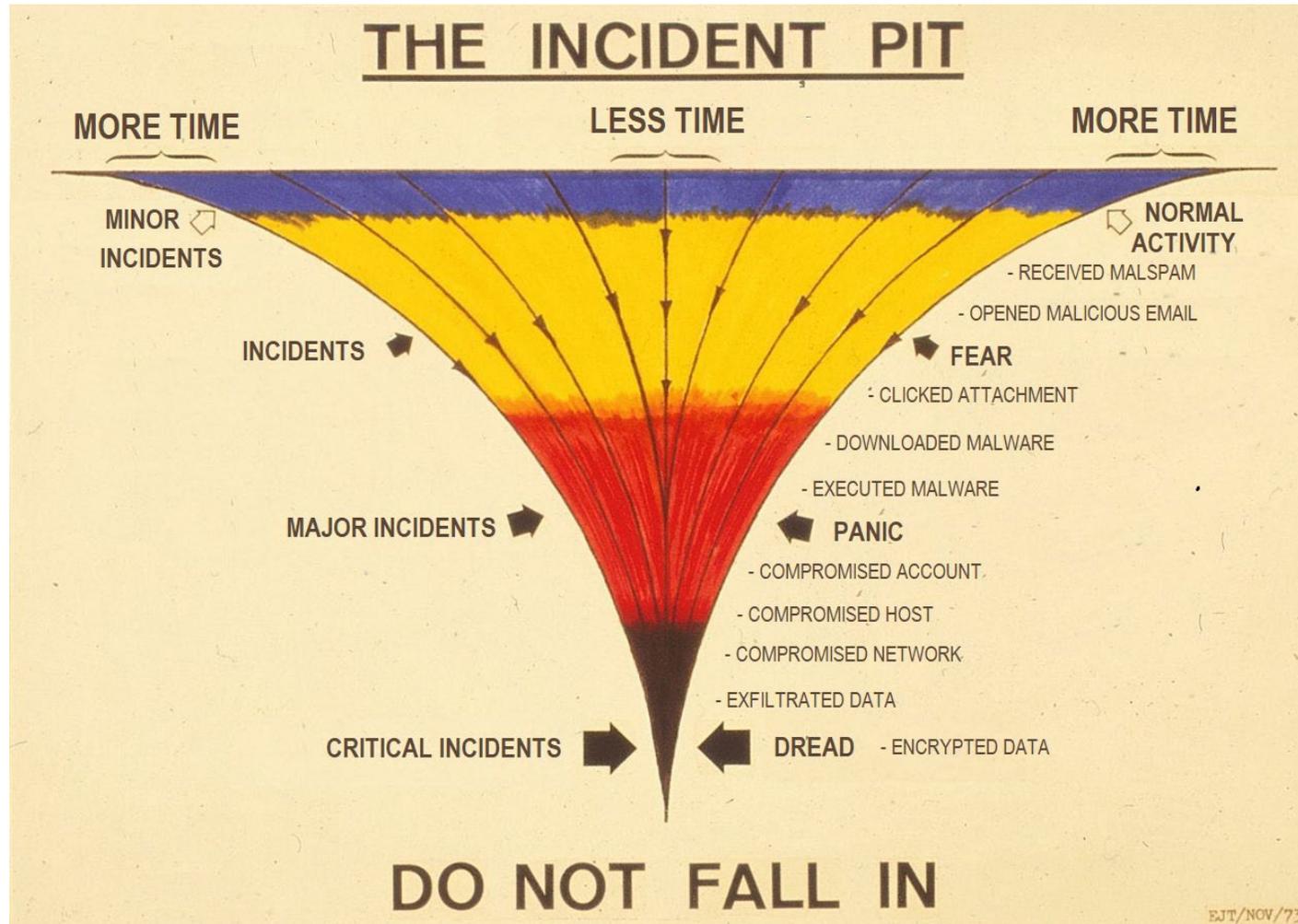
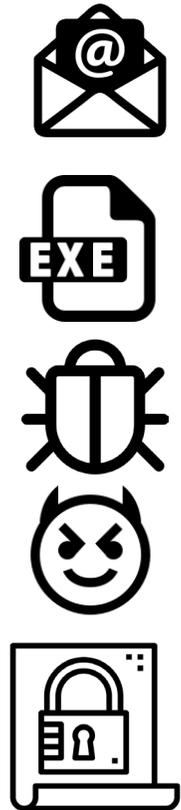
- Understand risks and their role in making an organisation function
- Understand type of controls that can be applied.
- Understand the intent of Govern in CSF 2.0
- Appreciate general steps of process improvement
- Appreciate the different level of process maturity
- For a Given [Country AND OR Industry]
  - 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)



# Incident Pit – Diving



# Incident Pit – Cybersecurity



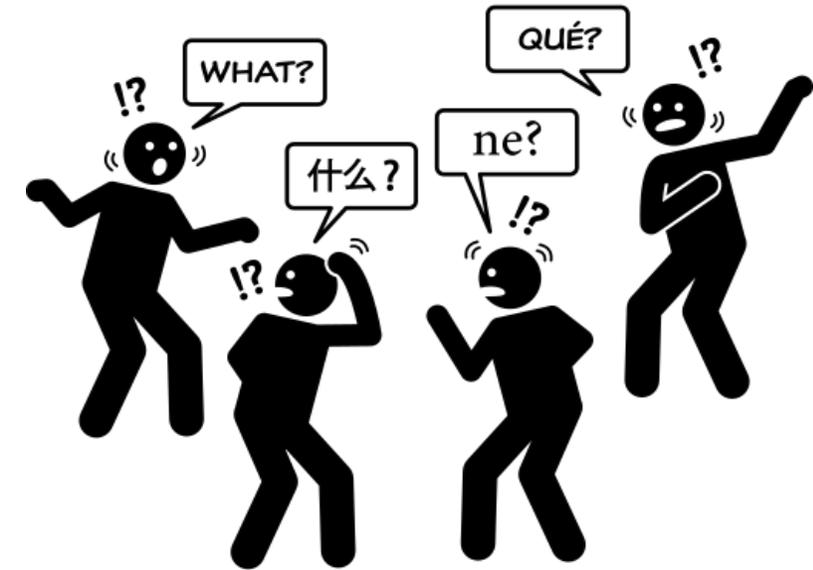
# Disasters are a group effort

-  Routine check to see if emergency cooling would work
  - Power Outage

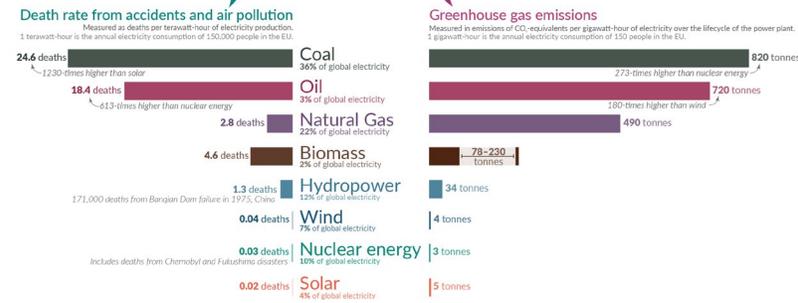
-  During test there is a power surge

-  Control can't shut the reactors
- Steam Build up in on reactor

-  Roof blown off
- Core exposed
-  Material released



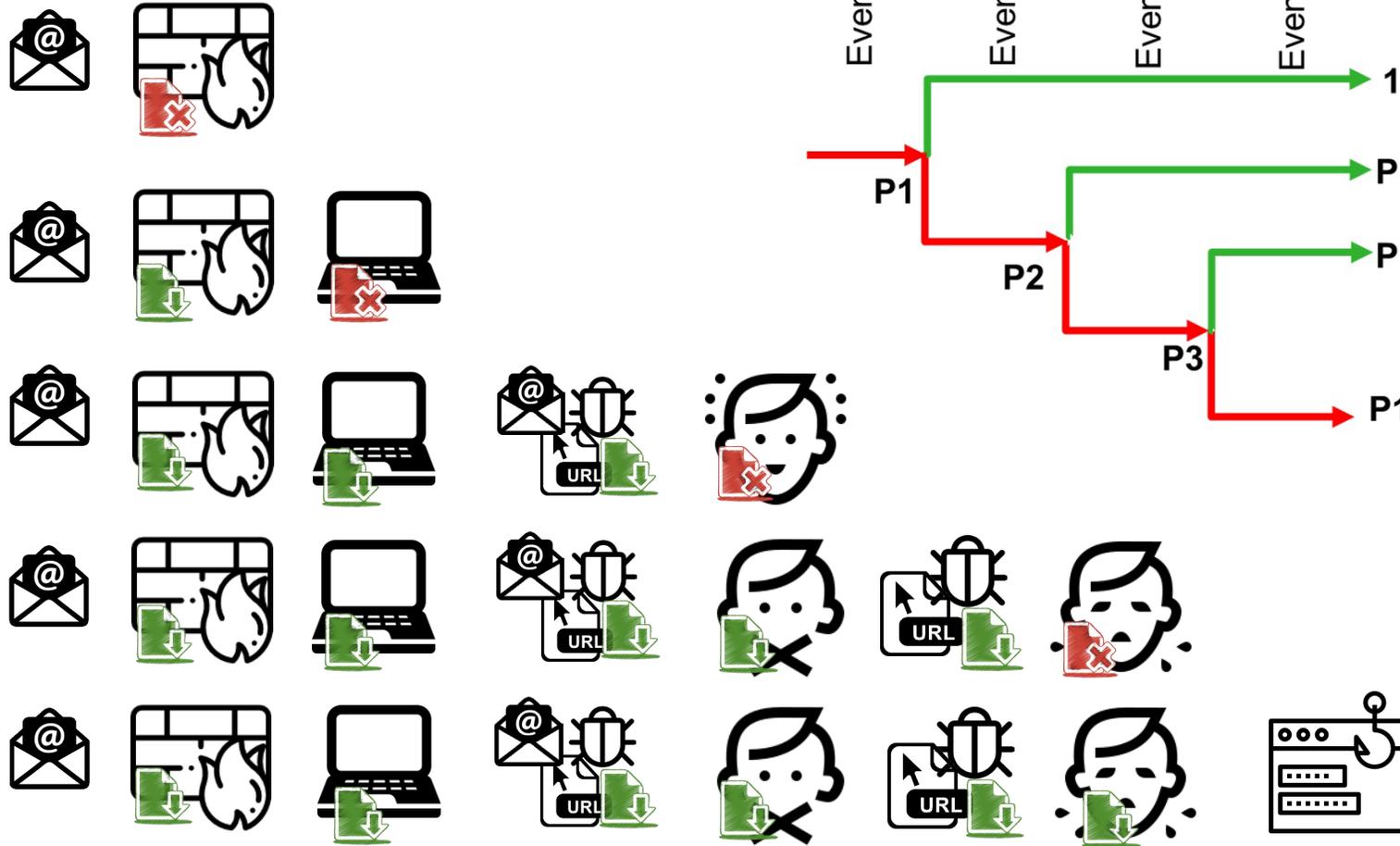
What are the **safest** and **cleanest** sources of energy? 



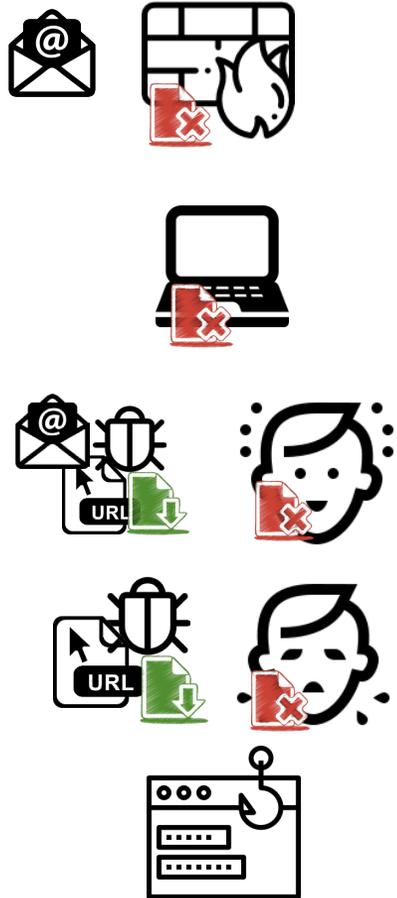
Death rates from fossil fuels and biomass are based on state-of-the-art plants with pollution controls in Europe, and are based on older models of the impacts of air pollution on health. This means these death rates are likely to be very conservative. For further discussion, see our article: [OurWorldInData.org/safest-sources-of-energy](https://ourworldindata.org/safest-sources-of-energy). Electricity shares are given for 2021. Data sources: Markandya & Wilkinson (2007); UNSCEAR (2006, 2018); Sovacool et al. (2016); IPCC AR5 (2014); Pehl et al. (2017); Ember Energy (2021). OurWorldInData.org - Research and data to make progress against the world's largest problems. Licensed under CC BY by the authors Hannah Ritchie and Max Roser.

# Progression of Phish

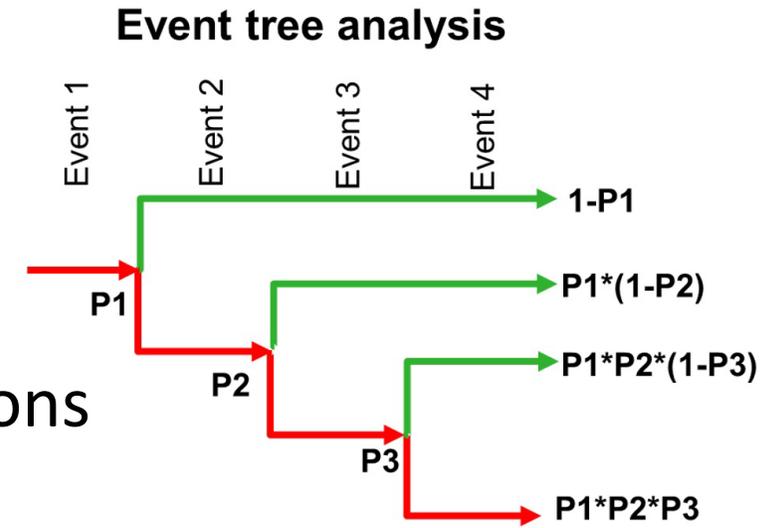
Each stages have tell tale signs



# Compromise is a Group effort

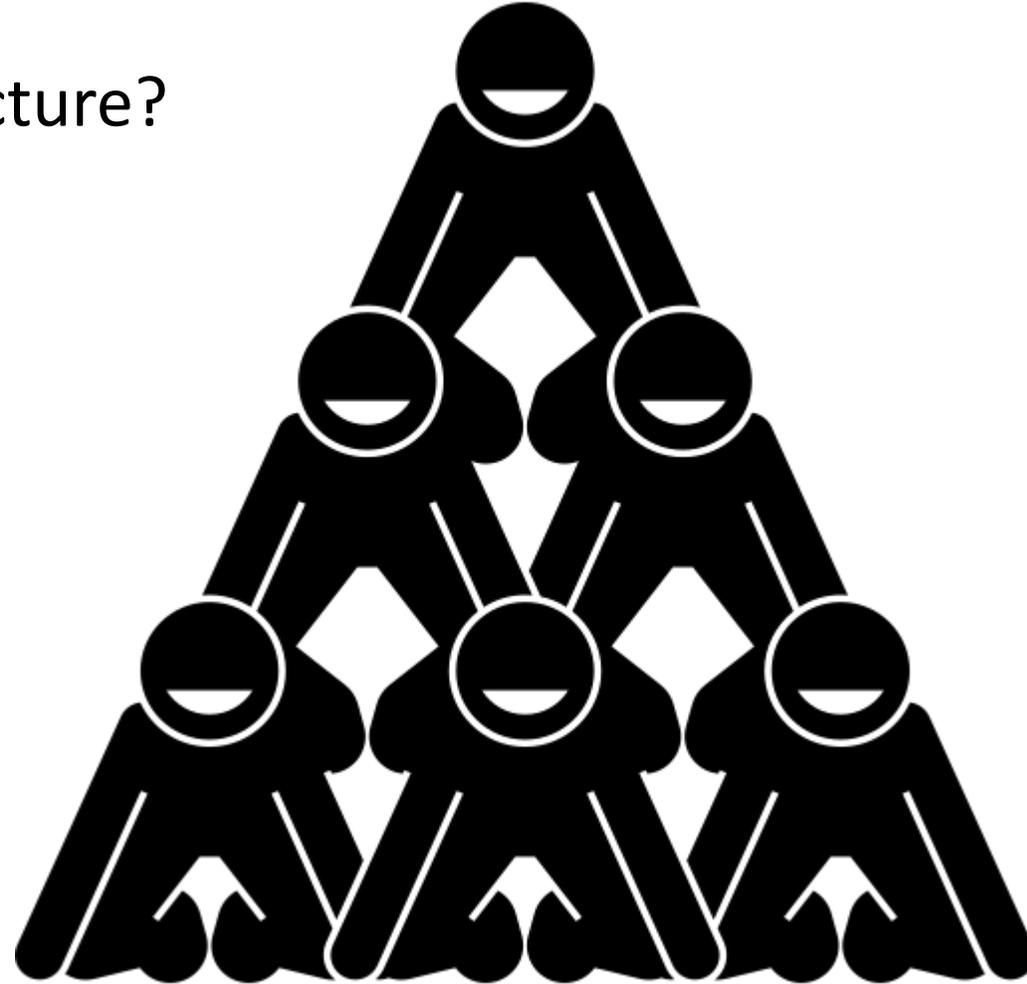


- Vendor Mail protection
- Internal spam filters and solutions (DMARC, DKIM, SPF etc...)
- SOC Threat hunting
- Suspicious email and attachment notification
- Allowing macro
- Report of execution
- Blacklisting by domain age/reputation
- End point scanning solution



# Disasters are avoided by group effort

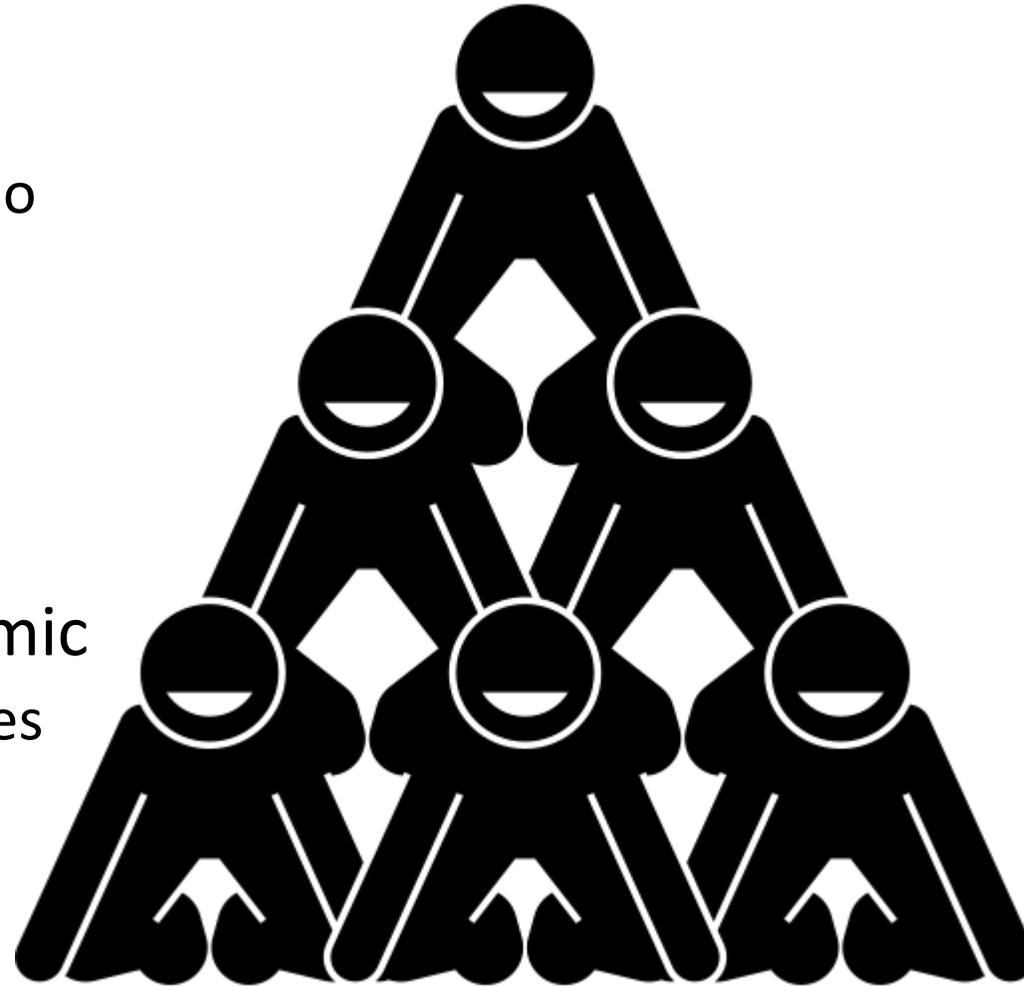
- What do you see in this picture?





# 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**

---

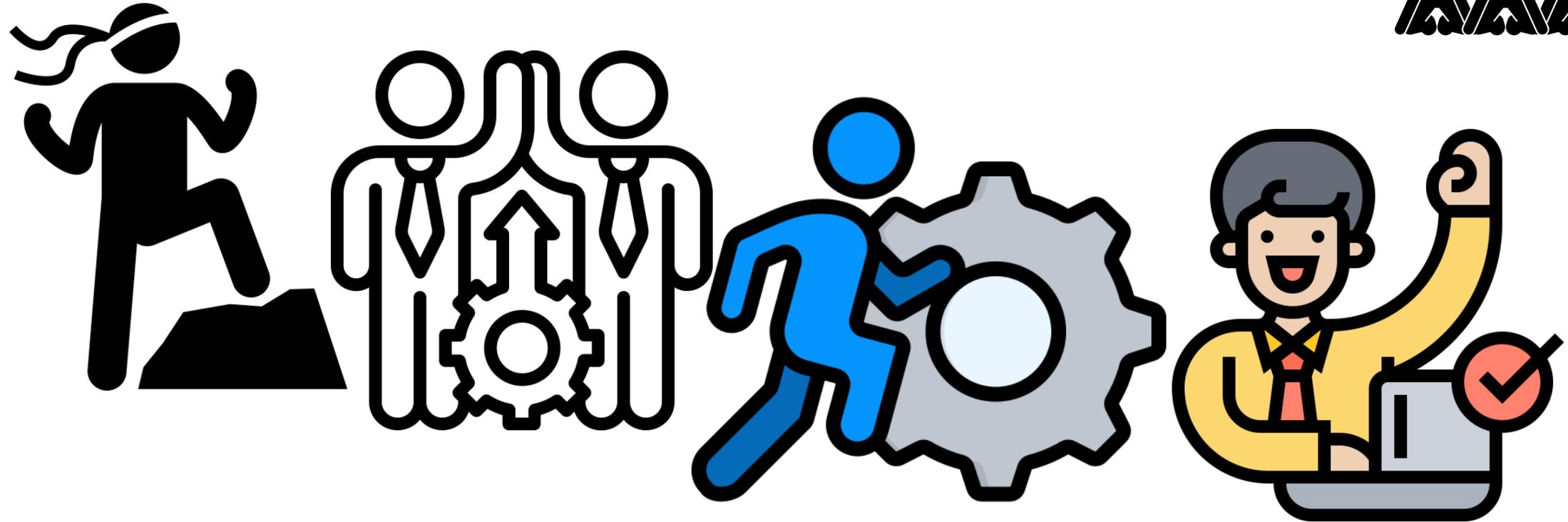
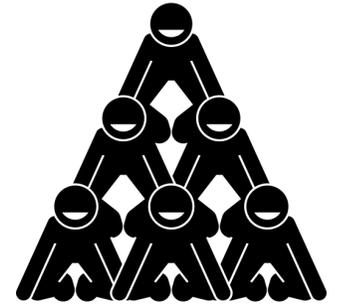
## **Guidelines on Electronic Mail Security**

# Application internally and restriction



AUSCERT

It is a group effort



IDENTIFY

DETECT

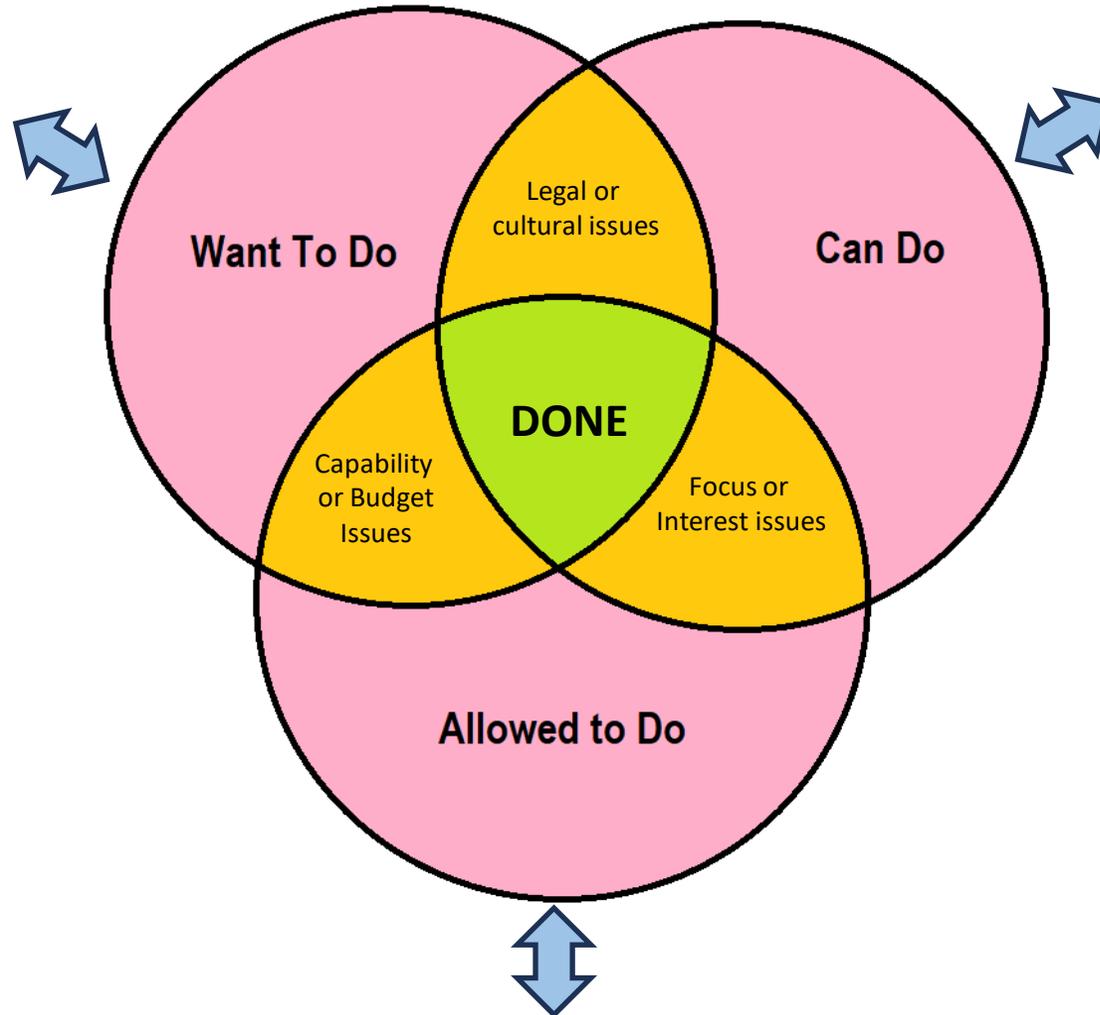
PROTECT

RESPOND

RECOVER

GOVERN

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



# 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”(19<sup>th</sup> 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

# 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. <sup>[8][9]</sup>
G0115	GOLD SOUTHFIELD	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines. <sup>[10]</sup>
S0009	Hikit	Hikit has been spread through spear phishing. <sup>[9]</sup>
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. <sup>[11][12][13]</sup>

# 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. <sup>[14]</sup> [15]
M1017	User Training	Users can be trained to identify social engineering techniques and phishing emails.

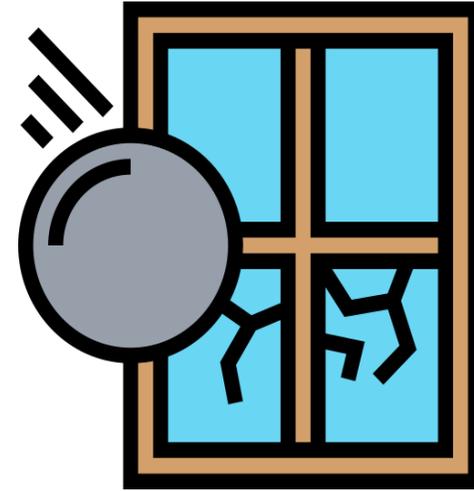
# T1566 – Detection

## 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. <sup>[14][15]</sup> 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. <sup>[14][15]</sup>
		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.

# ATT&CK Framework

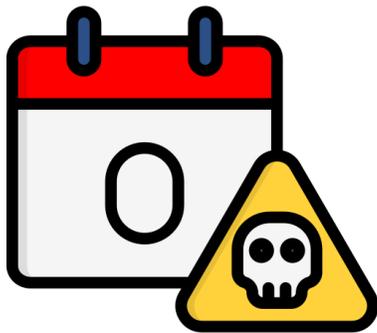
- MITRE ATT&CK<sup>®</sup> is a globally-accessible **knowledge base** of adversary **tactics** and **techniques** based on real-world observations. The ATT&CK knowledge base is used as a **foundation** for the development of **specific threat models** and methodologies in the private sector, in government,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



Revision  
Threats-Vulnerabilities-Risk

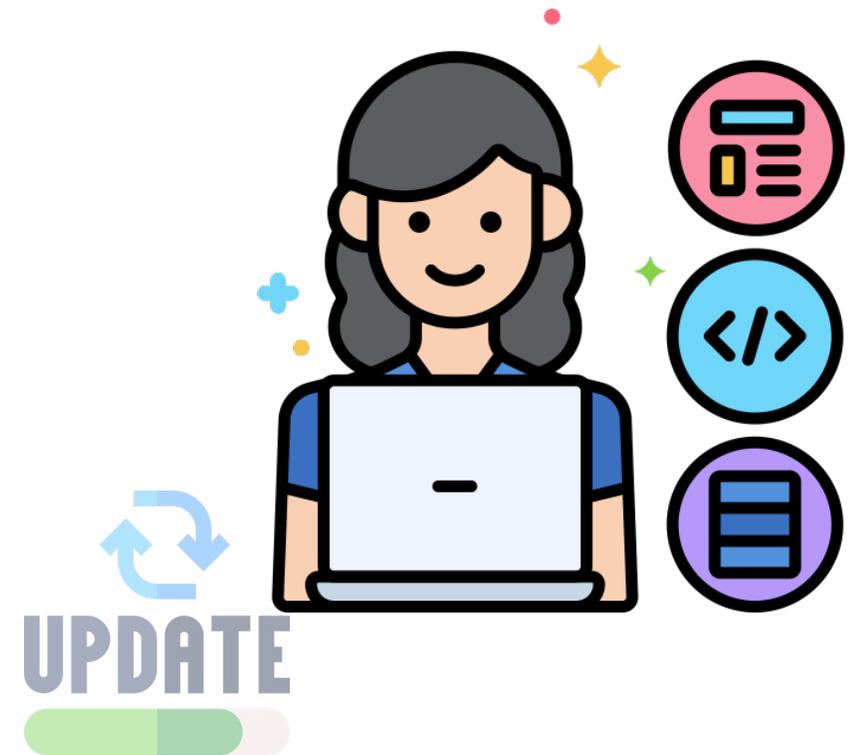
# Vulnerability

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



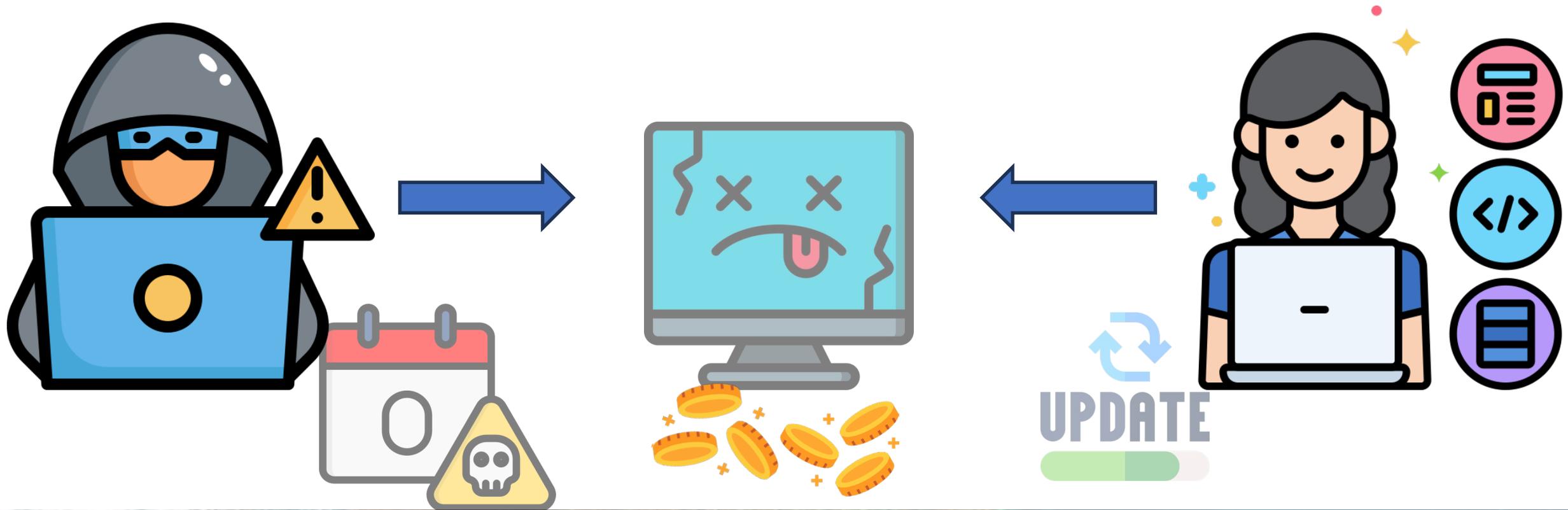
# Threat

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



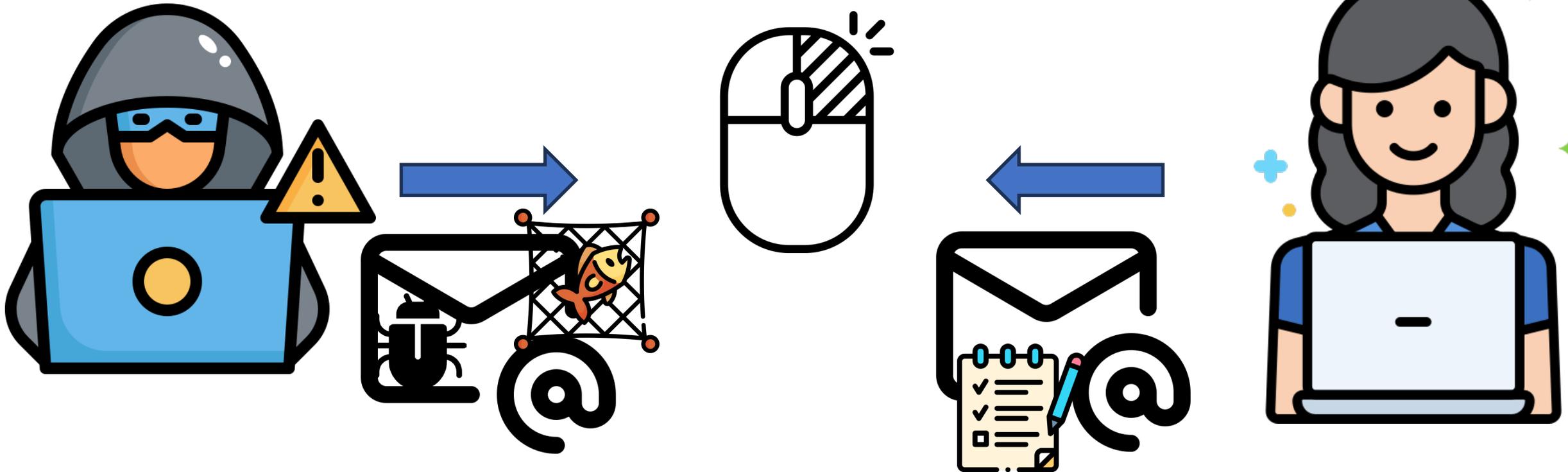
# Risk

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



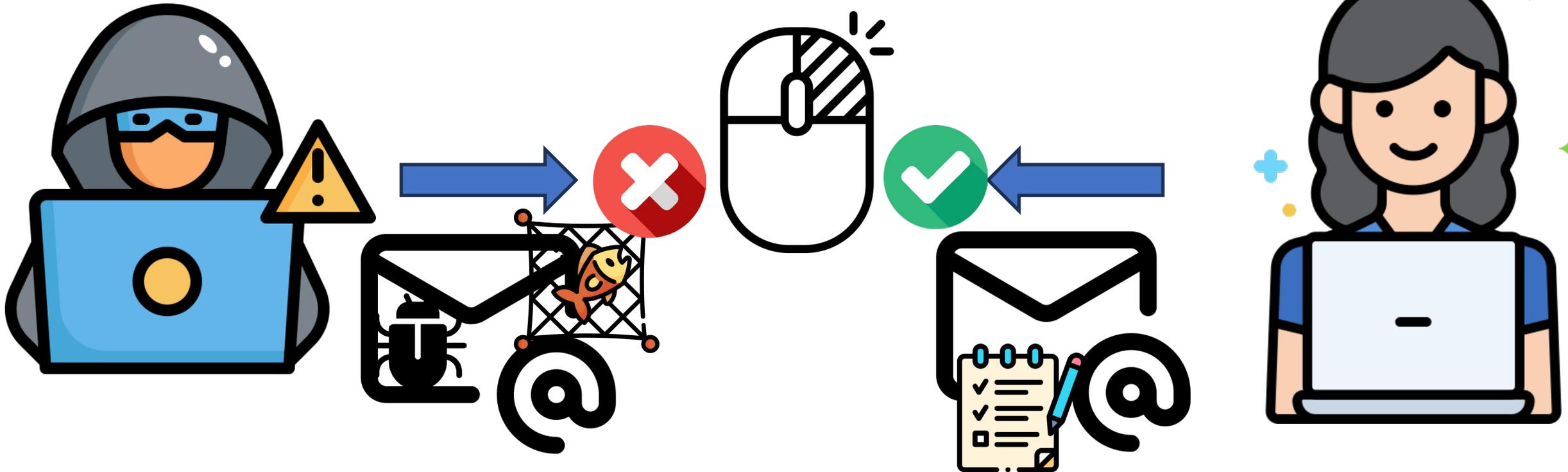
# Risk

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



# 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)



# Risk - Avoid

- Removal of email
  - Replace with something other?



# Risk - Mitigate

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



# Risk - Transfer

- Get Insurance
- Get Managed service Provider



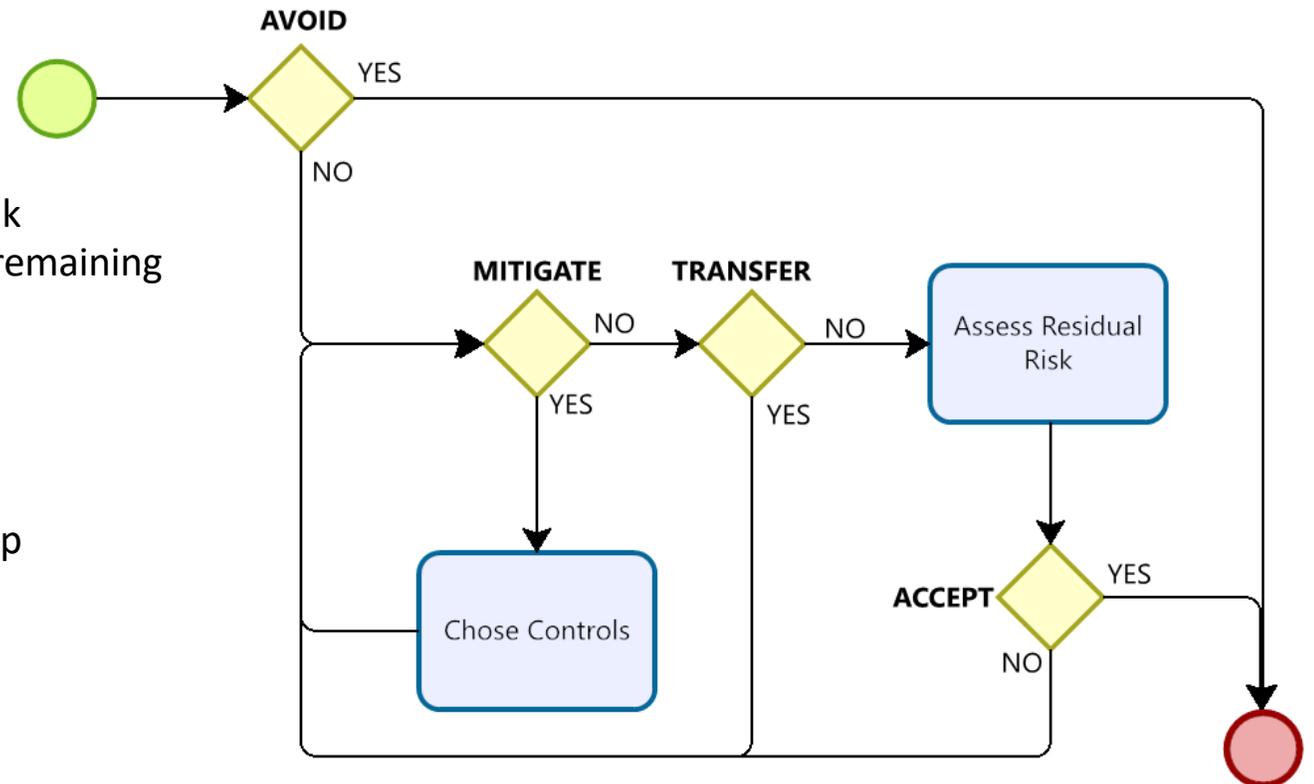
# Risk - Accept

- Accept the final risk



# General Approach to RISK

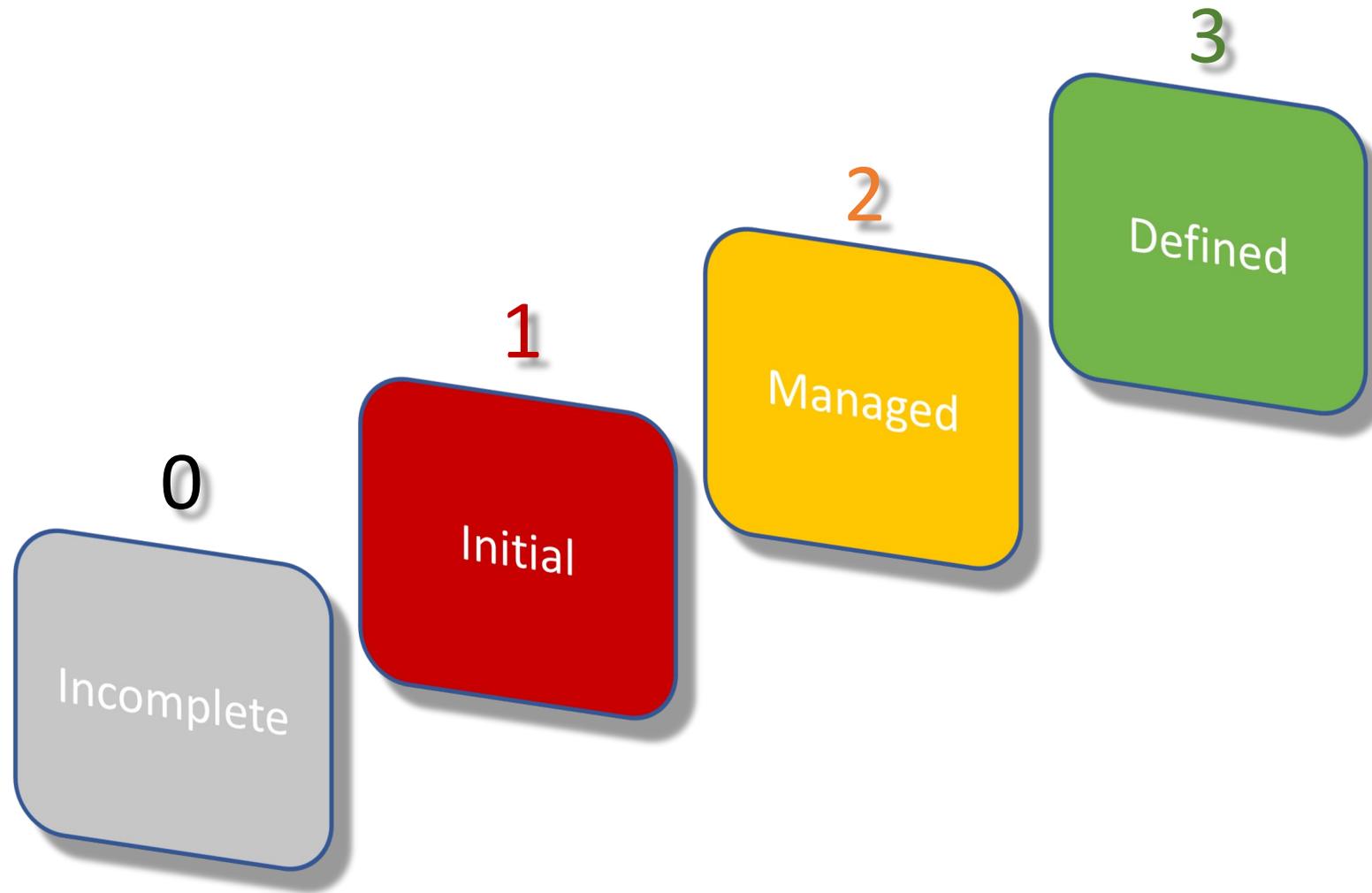
- Can it be **AVOIDED** completely.
- Can it be **MITIGATED** with controls
  - If YES then
    - List controls, cost, and expected residual risk
    - Chose controls, recalculate the overall risk remaining
    - Move to next step
  - If NO then
    - Move to next step
- Can it be **TRANSFERRED**
  - 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

Incomplete

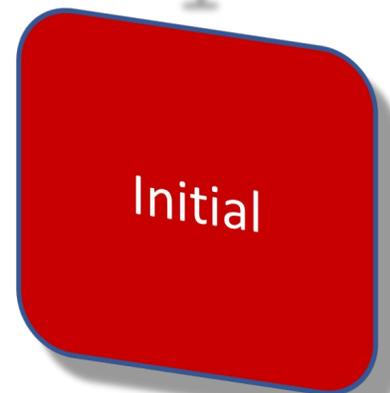
# Initial



- 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

1



# 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

2

Managed

# 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

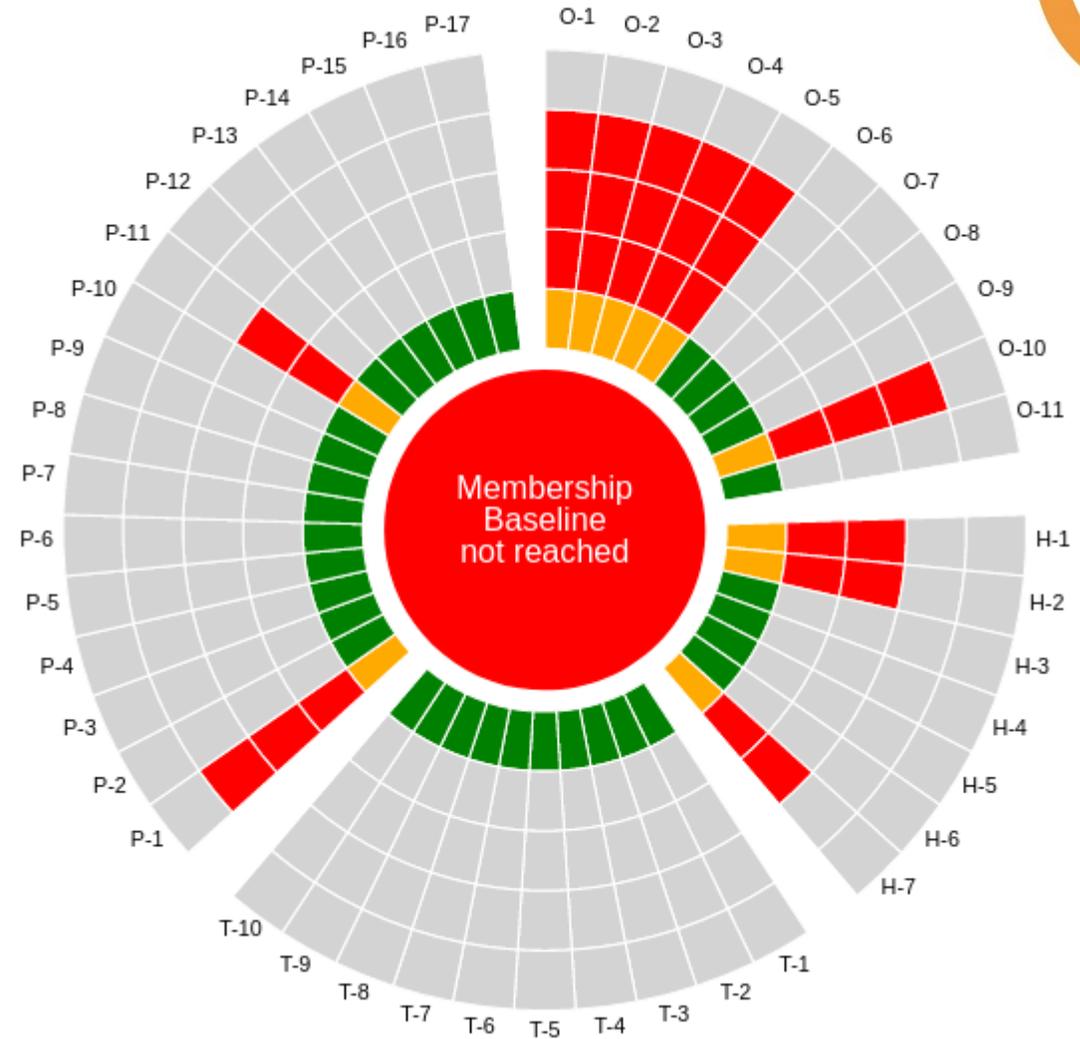


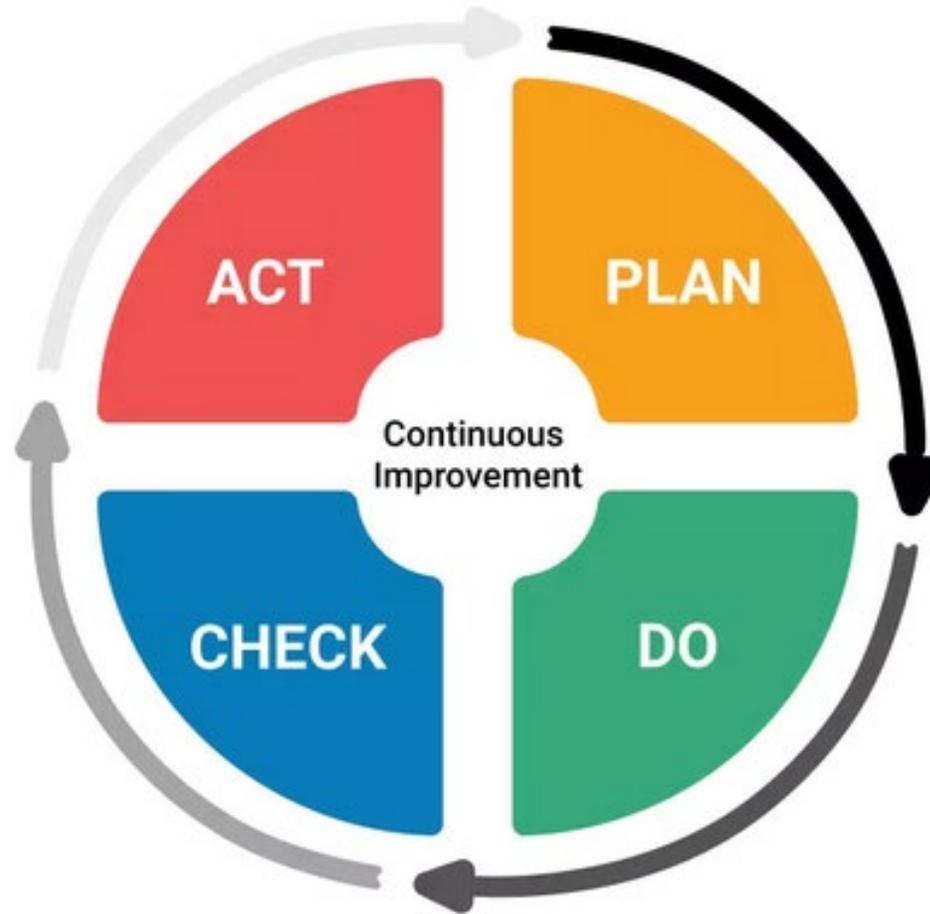


# SIM3



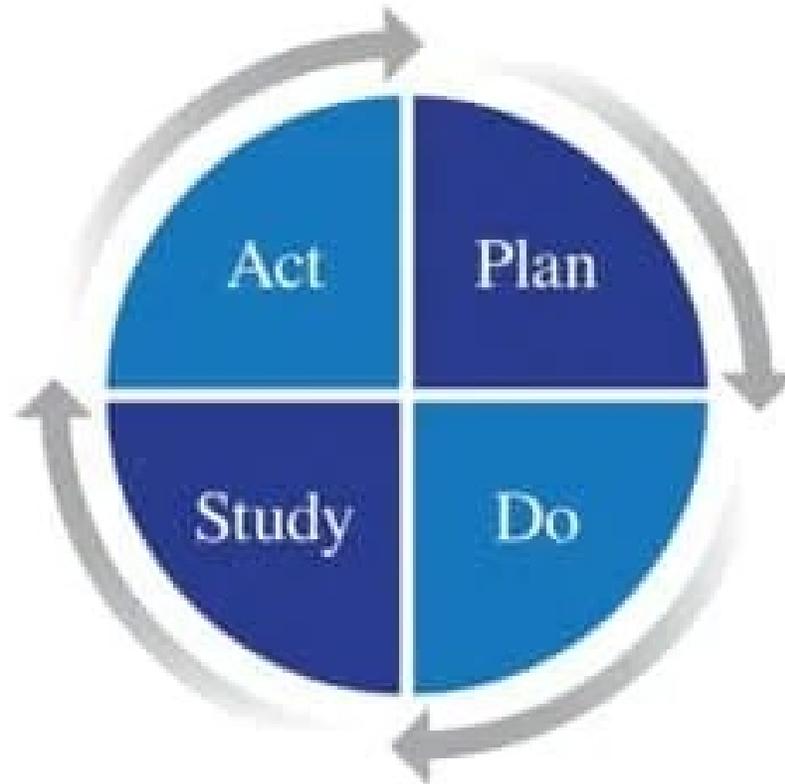
- Organisation
  - Human
  - Tools
  - Processes
- 
- 0 Never really discussed
  - 1 Basic understanding
  - 2 written but not formal
  - 3 written and approved
  - 4 written, approved, reviewed





Improvement is Iterative

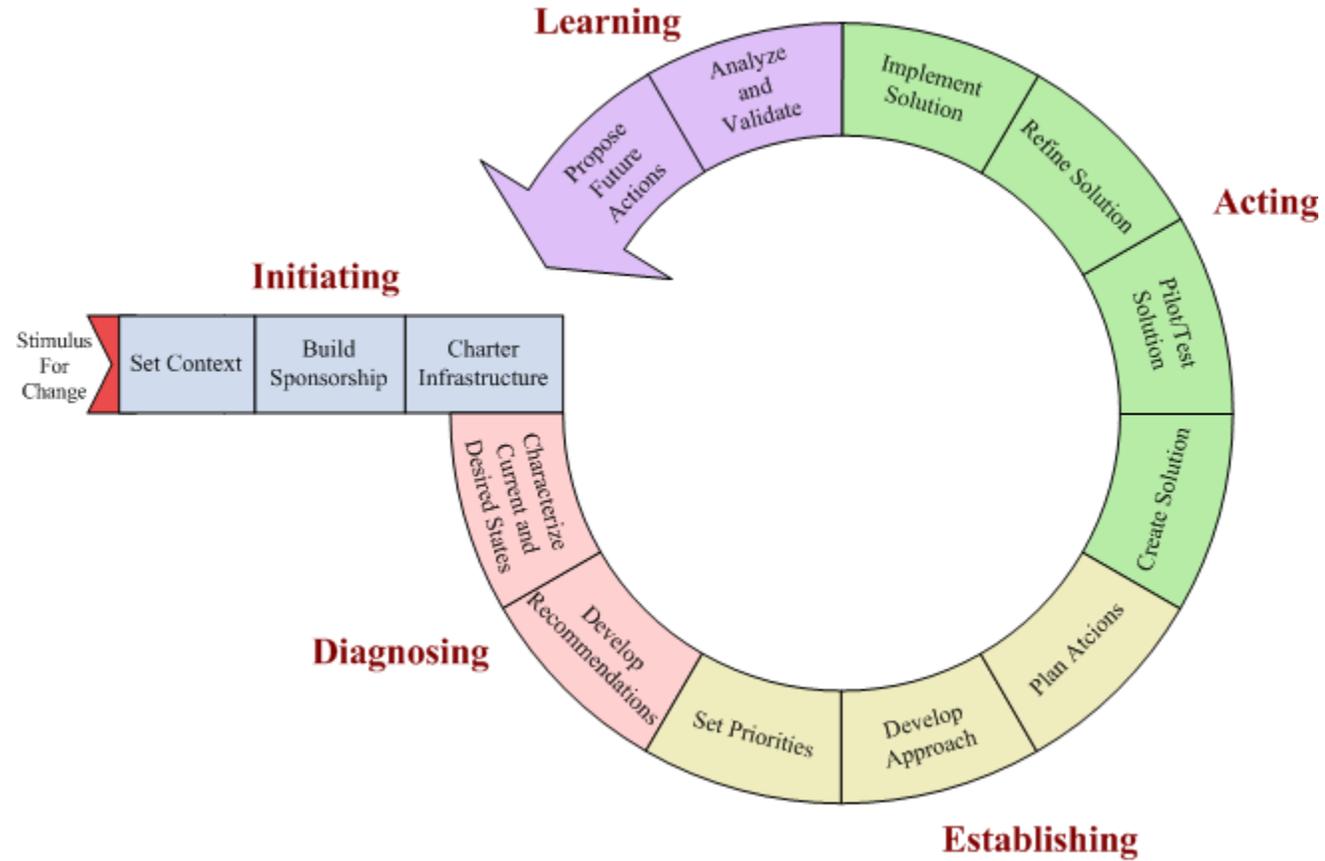
# Deming-Shewhart Model

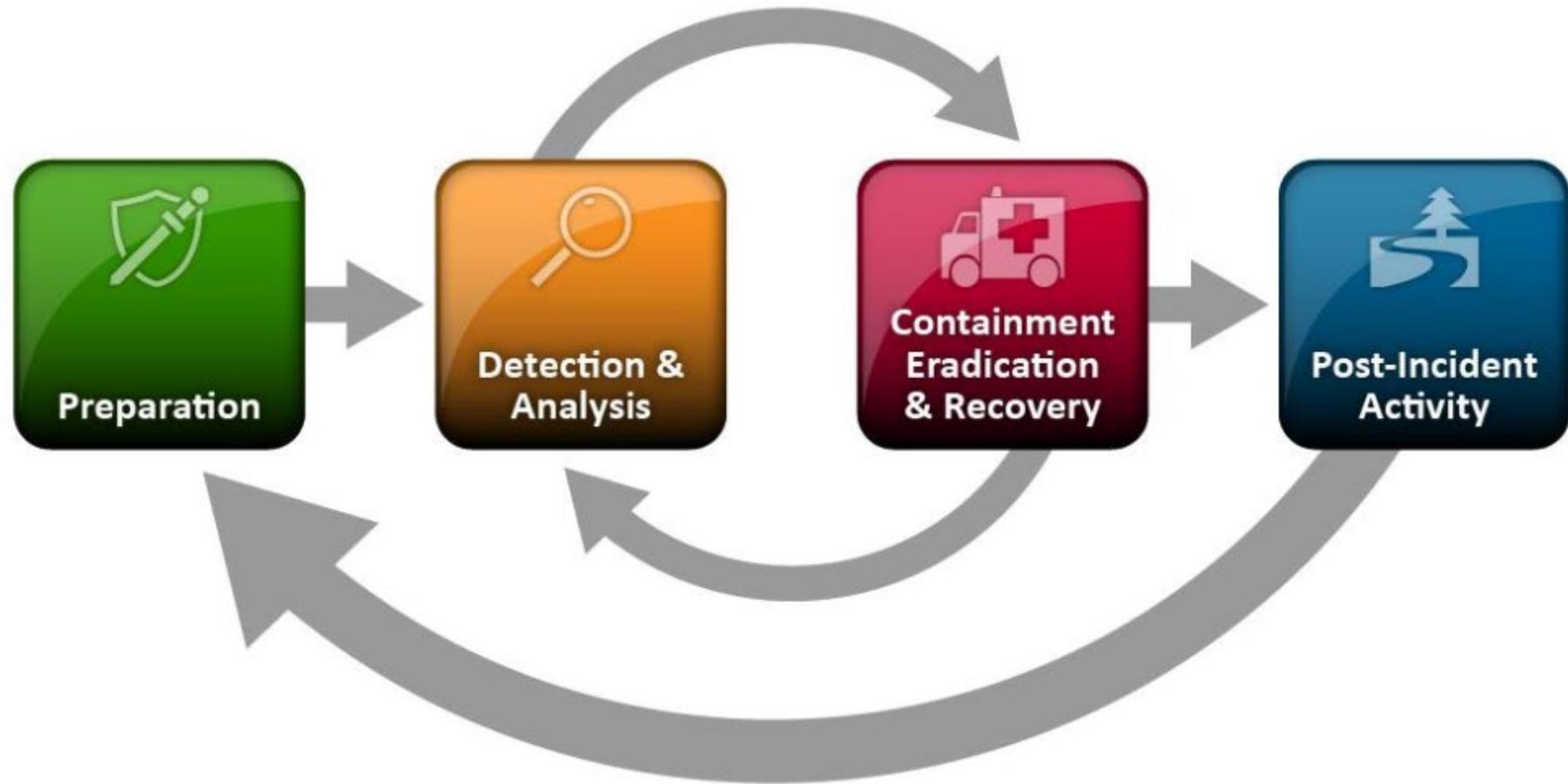


# ISO PDCA Model



# CMMI IDEAL Model





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

# NIST Cybersecurity Framework



# Cybersecurity Framework



**Framework Documents**

**Cybersecurity Framework Version 1.1**  
(April 2018)

- [Letter to Stakeholders](#)
- [Framework V1.1 \(PDF\)](#)
- [Framework V1.1 \(PDF\) with markup](#)
- [Framework V1.1 Core \(Excel\)](#)

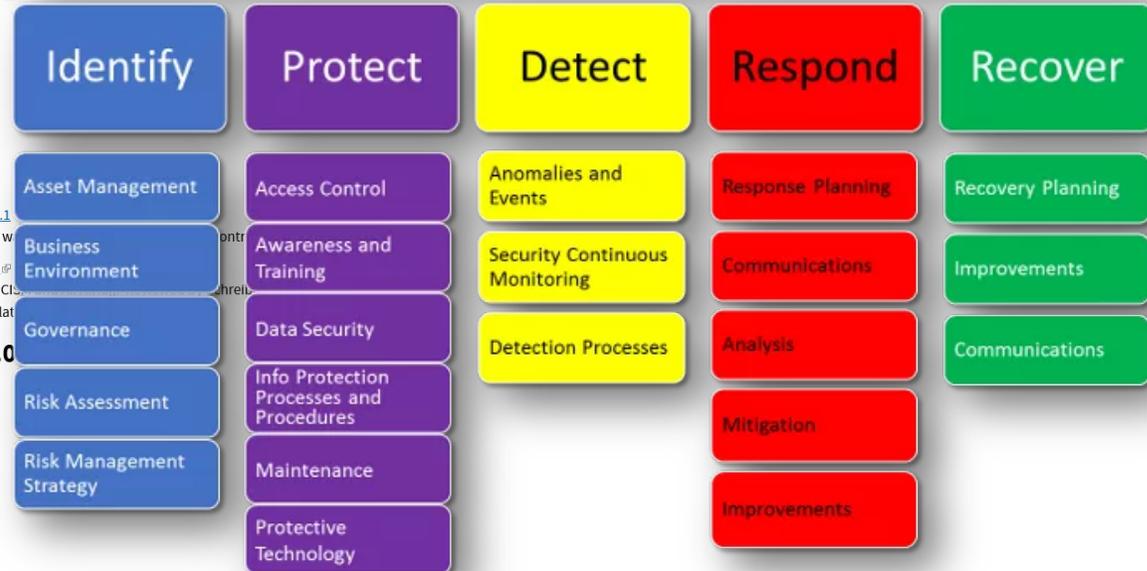
**Adaptations/Translations**

- Spanish Translation of the [NIST Cybersecurity Framework V1.1](#)  
(The Spanish language Cybersecurity Framework Version 1.1 w...
- Arabic Translation of the [NIST Cybersecurity Framework V1.1](#)  
(Translated by Ali A. AlHasan, PMP, CISSP,CISA, CGEIT, CRISC, CISA...  
Translations, INC (STI). Not an official U.S. Government translat...

**Cybersecurity Framework Version 1.0**  
(February 2014)

- [Framework V1.0 \(PDF\)](#)
- [Framework V1.0 Core \(Excel\)](#)

## NIST Cyber Security Framework



# NIST Cybersecurity Framework 1.0



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

# NIST Cybersecurity Framework 2.0

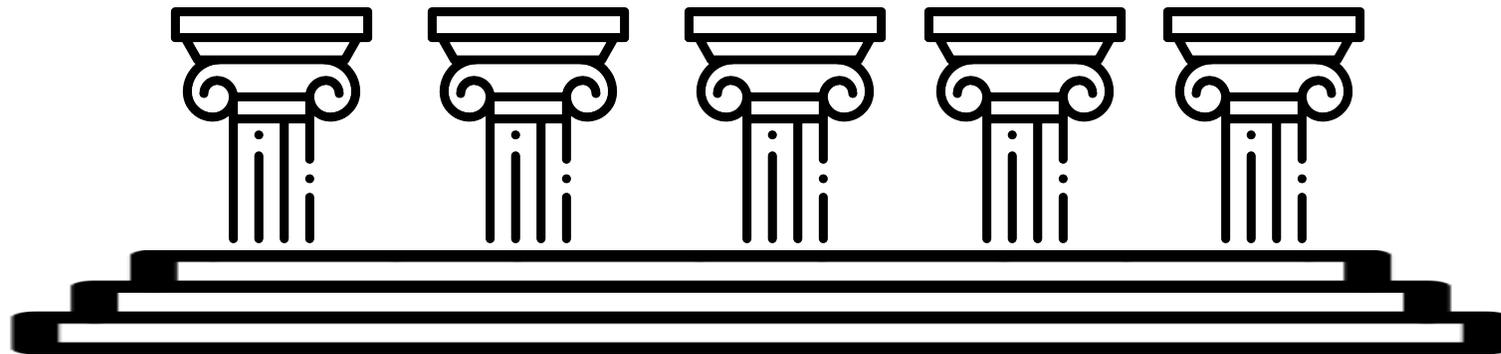


“Each understand the main idea, the master plan”



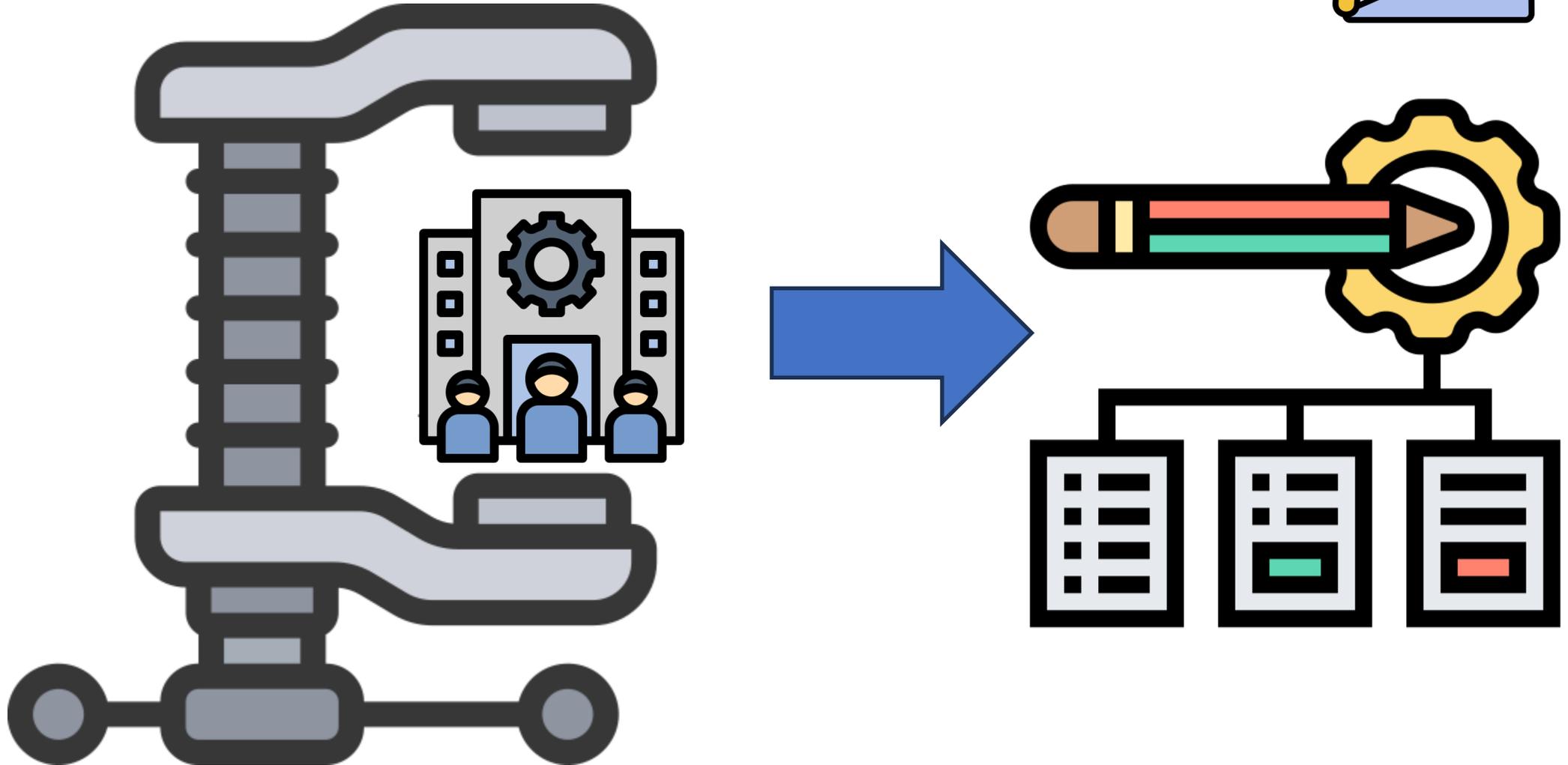
# NIST Cybersecurity Framework 2.0

- 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

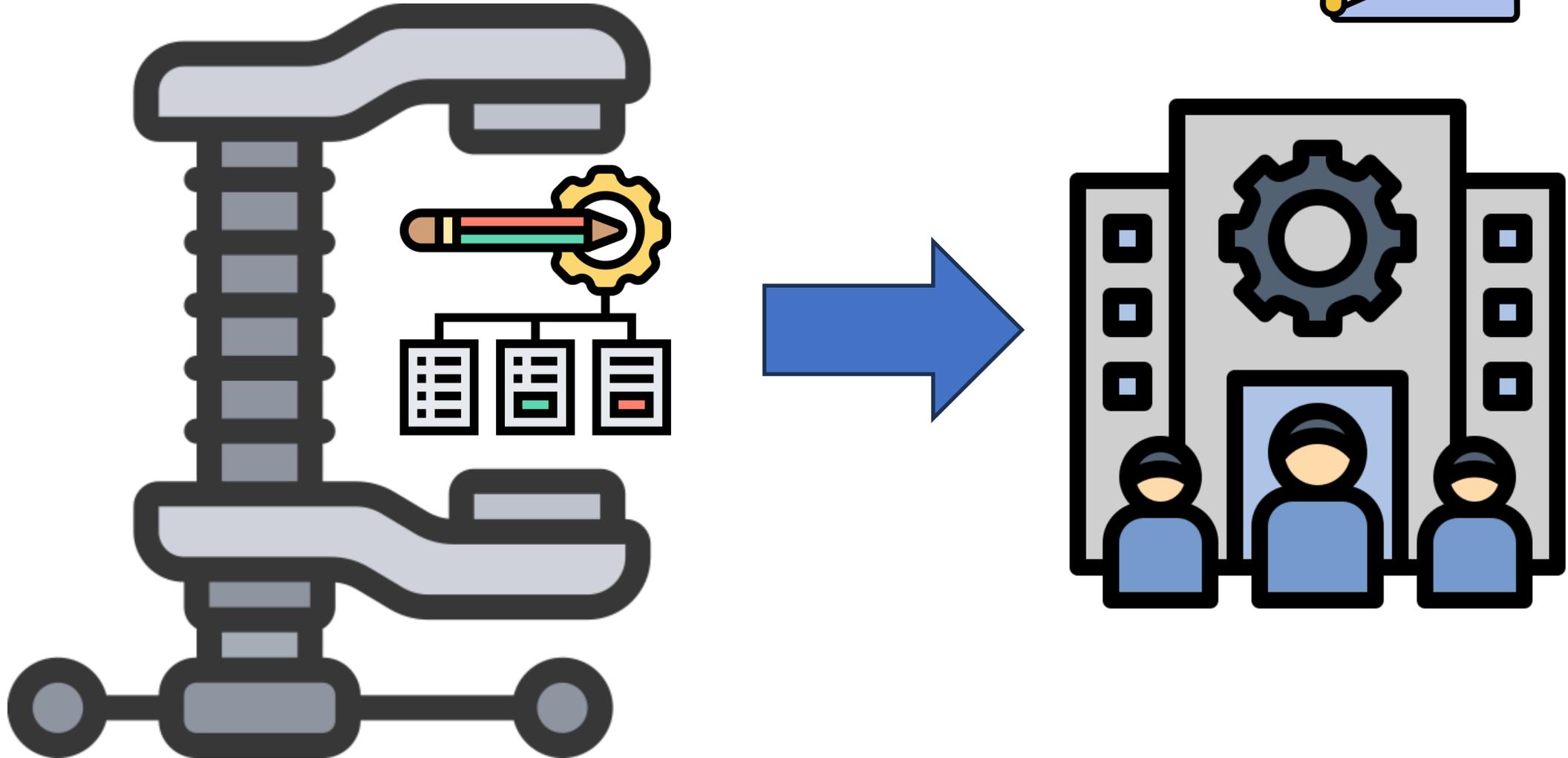




# Fit Organisation into a Framework

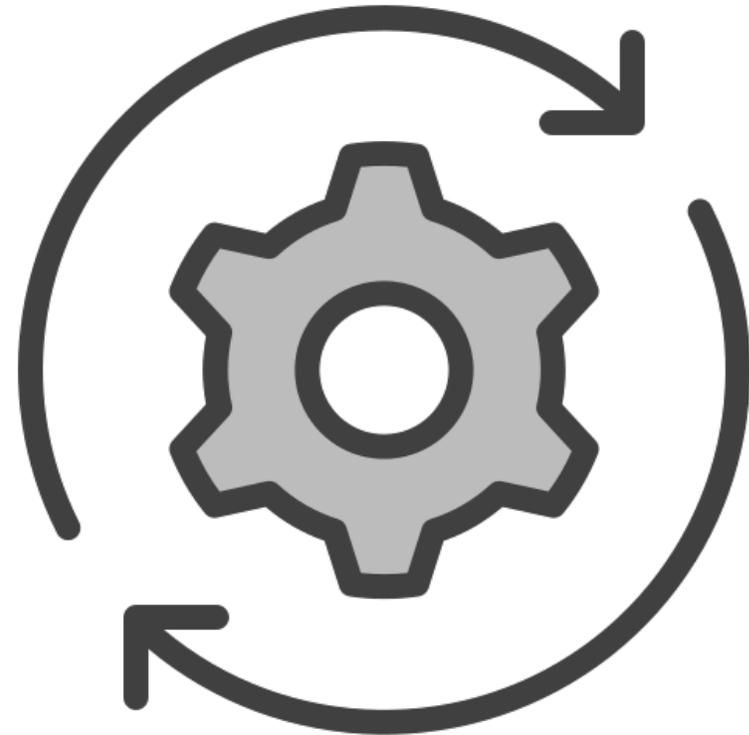


# Fit Framework into an Organisation



# Profiles for CSF 1.0

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



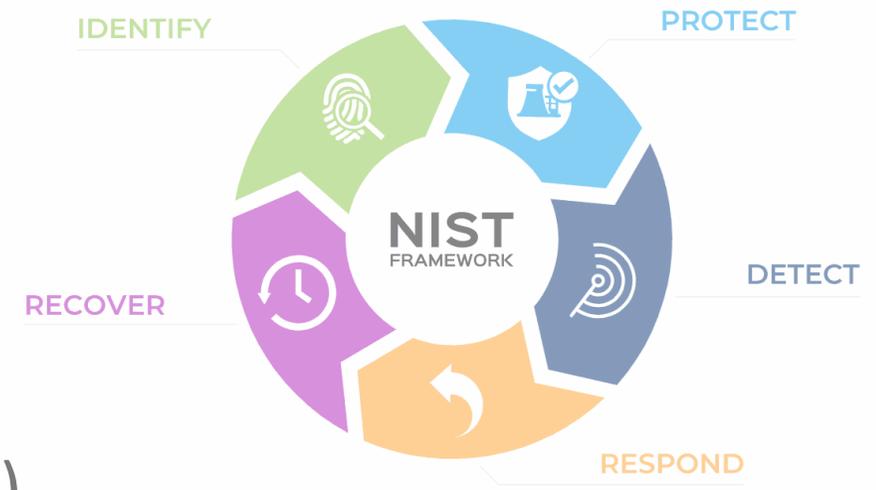
# NIST Cybersecurity Framework 2.0





# 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?

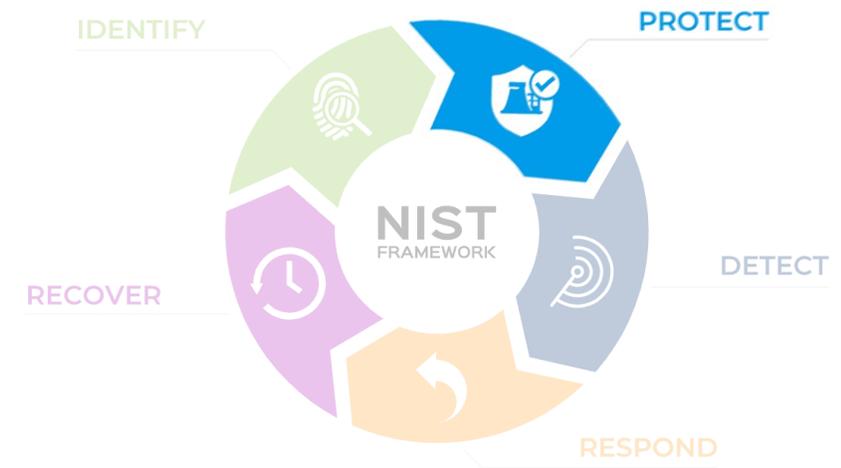


# Identify



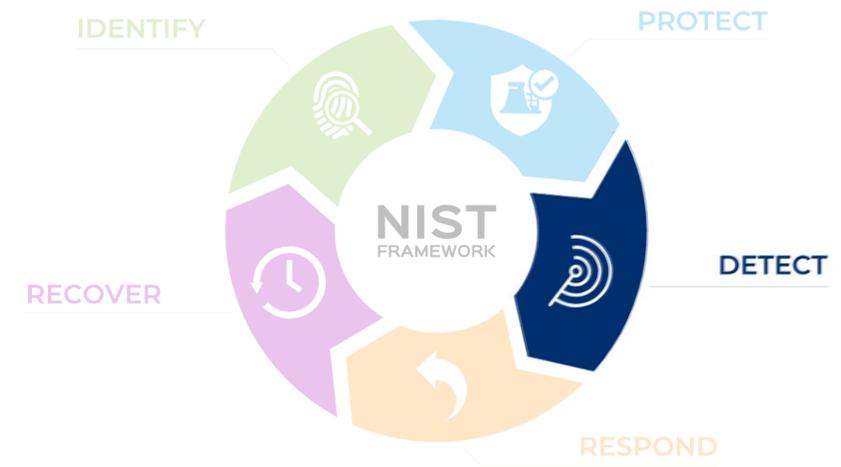
- Develop an organisational understanding to manage cybersecurity risk to: systems, assets, data, capabilities.
  - Identify critical enterprise processes and assets
  - Document information flows
  - Maintain hardware and software inventory
  - Establish policies for cybersecurity that include roles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

# 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

# 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

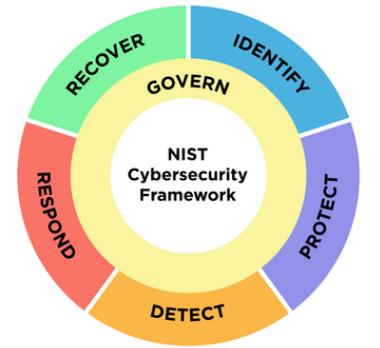
# Recover



- 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

# 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



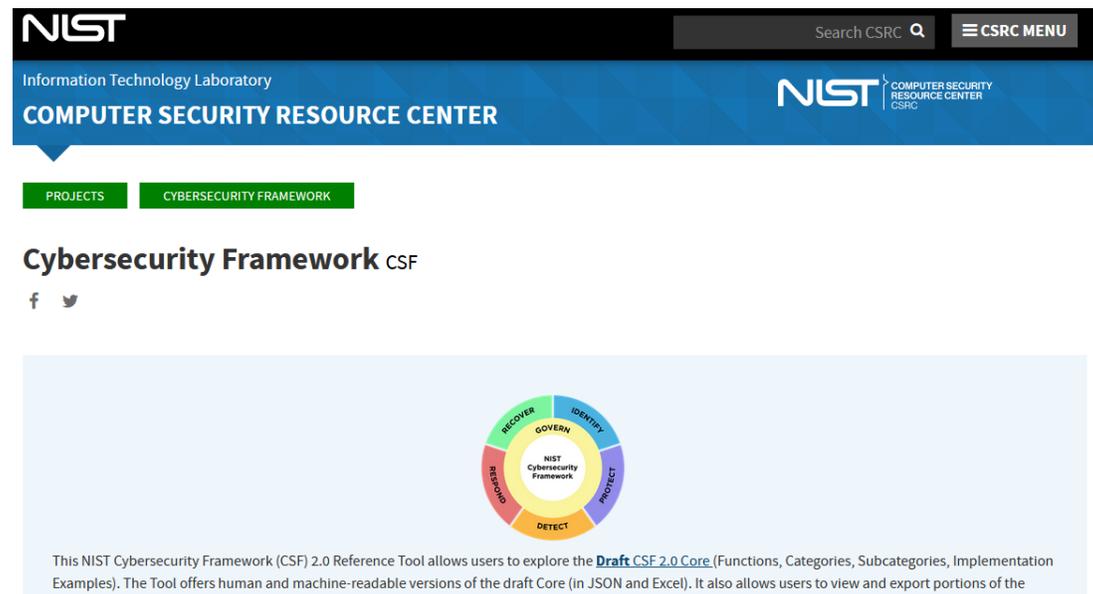
# Summary 2.0



- **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

# 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:

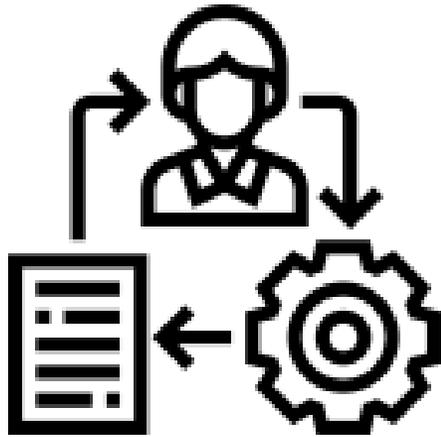


The screenshot shows the NIST Computer Security Resource Center (CSRC) website. The header includes the NIST logo, the text "Information Technology Laboratory" and "COMPUTER SECURITY RESOURCE CENTER", and a search bar labeled "Search CSRC" and a "CSRC MENU" button. Below the header, there are two green buttons: "PROJECTS" and "CYBERSECURITY FRAMEWORK". The main content area is titled "Cybersecurity Framework CSF" and includes social media icons for Facebook and Twitter. A central graphic displays the NIST Cybersecurity Framework (CSF) 2.0 Reference Tool, which is a circular diagram with five segments: GOVERN (top), IDENTIFY (right), PROTECT (bottom right), DETECT (bottom), and RECOVER (left). Below the diagram, a paragraph of text reads: "This NIST Cybersecurity Framework (CSF) 2.0 Reference Tool allows users to explore the [Draft CSF 2.0 Core](#) (Functions, Categories, Subcategories, Implementation Examples). The Tool offers human and machine-readable versions of the draft Core (in JSON and Excel). It also allows users to view and export portions of the

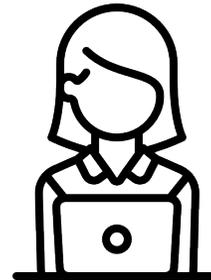
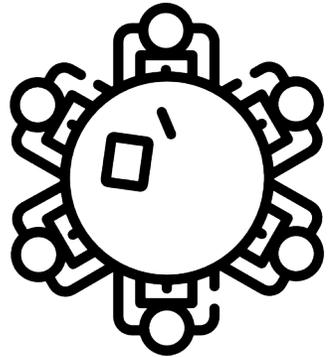


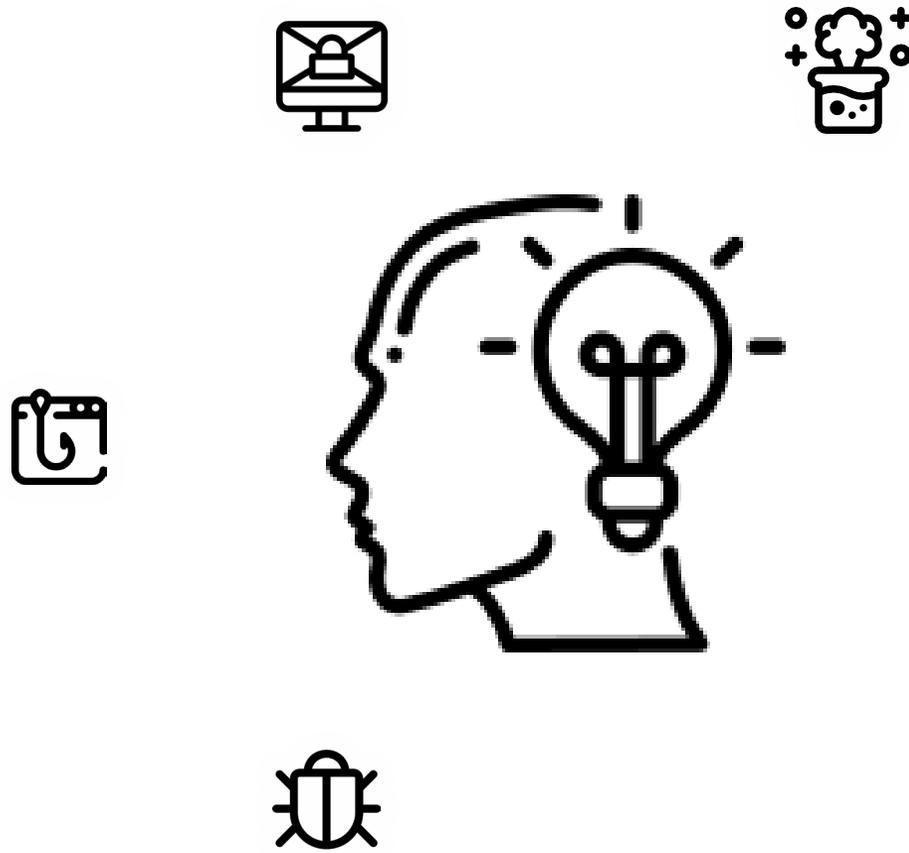
Communication

# Message Usefulness



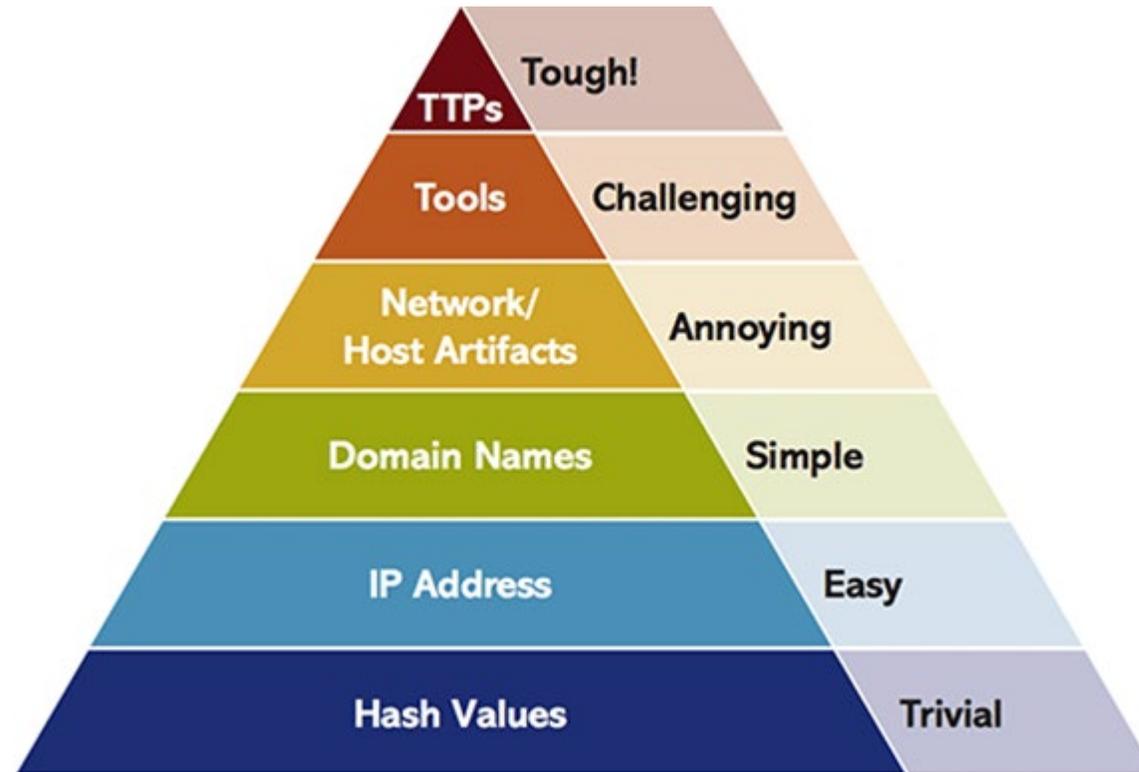
# Many Layers “Simultaneously”





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



# 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.

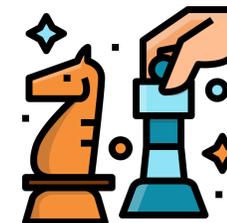
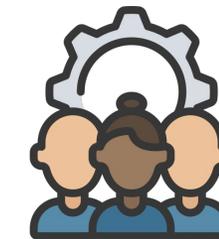
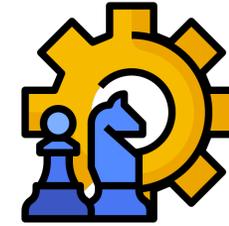


- Tactical

- 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

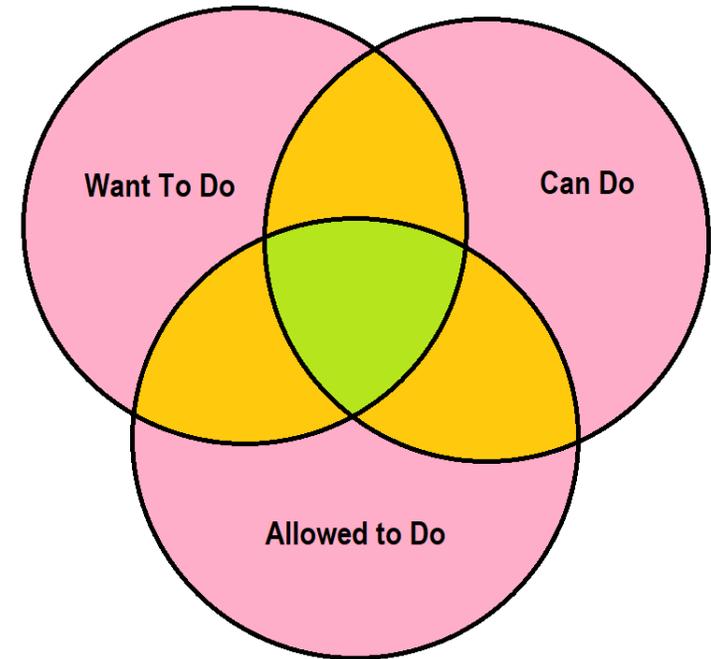


# Cyber Threat Intelligence

- 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>

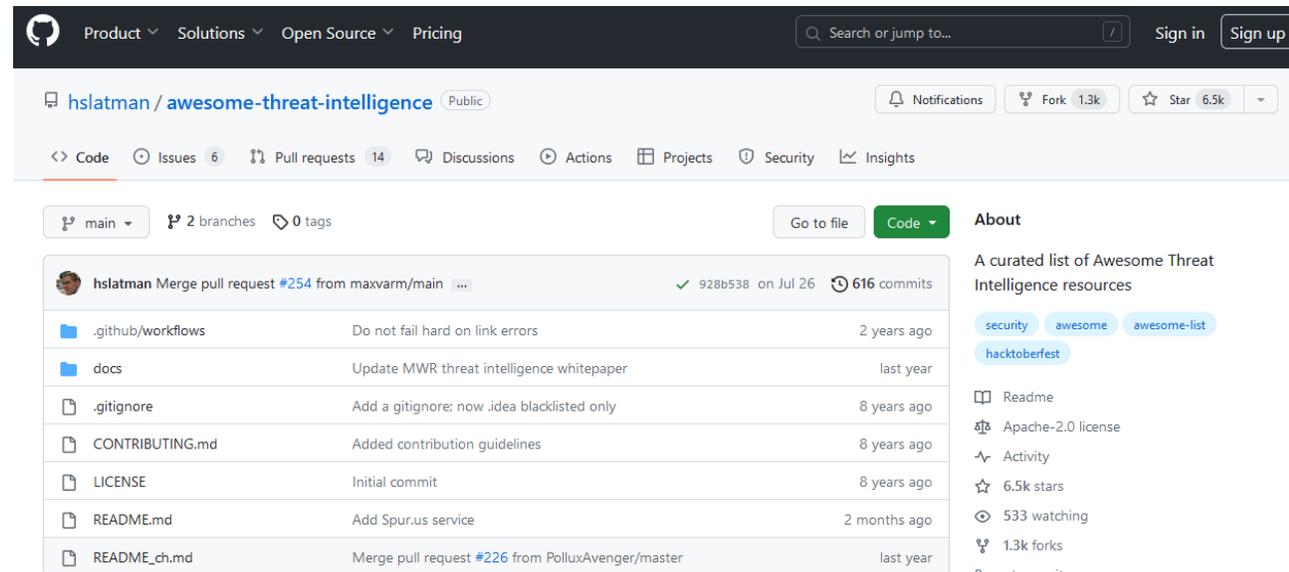
# Firehoses of Threat Intel

- Search term “curated list of threat intel git”

- Target Link

<https://github.com/hslatman/awesome-threat-intelligence>

- Looks like



The screenshot shows the GitHub repository page for `hslatman/awesome-threat-intelligence`. The repository is public and has 6.5k stars and 1.3k forks. The main branch is `main` with 2 branches and 0 tags. The repository contains a curated list of Awesome Threat Intelligence resources, including a README.md, a LICENSE, and a CONTRIBUTING.md. The repository is licensed under Apache-2.0 and has 533 watchers and 1.3k forks.

File	Description	Last Commit
<code>.github/workflows</code>	Do not fail hard on link errors	2 years ago
<code>docs</code>	Update MWR threat intelligence whitepaper	last year
<code>.gitignore</code>	Add a gitignore; now .idea blacklisted only	8 years ago
<code>CONTRIBUTING.md</code>	Added contribution guidelines	8 years ago
<code>LICENSE</code>	Initial commit	8 years ago
<code>README.md</code>	Add Spur.us service	2 months ago
<code>README_ch.md</code>	Merge pull request #226 from PolluxAvenger/master	last year

- 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)

# ATT&CK Navigator Training

## TRAINING

[Overview](#)

[CTI Training](#)

[Home](#) > [Resources](#) > [ATT&CK Training](#) > [CTI Training](#)

## Using ATT&CK for Cyber Threat Intelligence Training

The goal of this training is for students to understand the following:

- What ATT&CK is and why it's useful for cyber threat intelligence (CTI)
- How to map to ATT&CK from both finished reporting and raw data
- Why it's challenging to store ATT&CK-mapped data and what you should consider when doing that
- How to perform CTI analysis using ATT&CK-mapped data
- How to make defensive recommendations based on CTI analysis

The training contains five modules that consist of videos and exercises that are linked below. This training was designed to be completed in approximately 4 hours, and may be completed solo or as a team. We recommend you view the video for each module, and when prompted, pause the video to access the exercise documents linked below and complete the exercises, then proceed with viewing the video to go over the exercise. A copy of all slides from the training are [here](#).

The exercises in this training are based on a previous version of ATT&CK. We recommend using [ATT&CK v6](#) and [ATT&CK Navigator v2](#) if you want to match the training.

## Training Modules

Module 1: Introducing training and understanding ATT&CK	▼
Module 2 with Exercise 2: Mapping to ATT&CK from finished reporting	▼
Module 3 with Exercise 3: Mapping to ATT&CK from raw data	▼
Module 4 with Exercise 4: Storing and analyzing ATT&CK-mapped intel	▼
Module 5 with Exercise 5: Making ATT&CK-mapped data actionable with defensive recommendations	▼

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

# Exercise 1 – Getting used to the Navigator

about  
layer

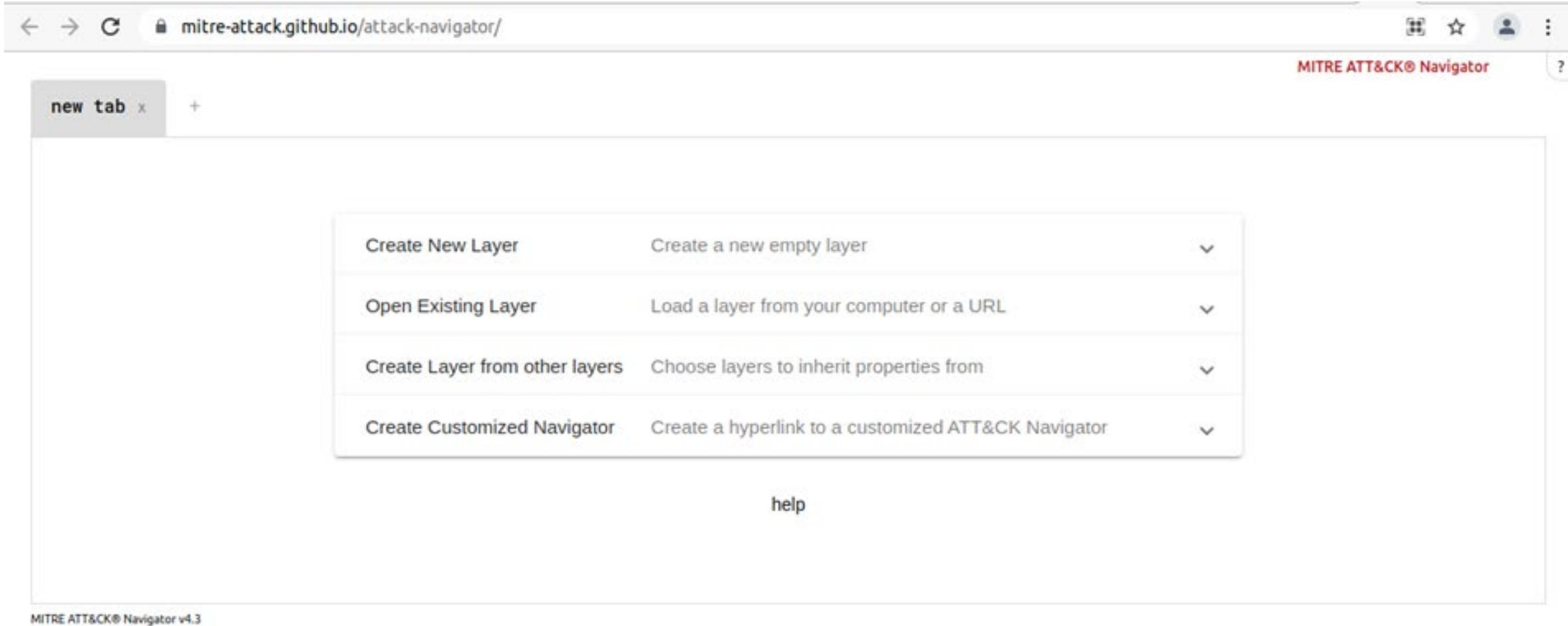
domain  
**Enterprise  
ATT&CK v9**

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

legend  
0.0 20 40 60 80 100

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning Gather Victim Host Information Tech Identity Information Gather Victim Network Information Gather Victim Org Information Phishing for Information Search Closed Sources Search Open Websites/Domains Search Video/Owned Websites	Acquire Infrastructure Compromise Accounts Compromise Infrastructure Develop Capabilities Establish Accounts Obtain Capabilities Stage Capabilities	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing Redirection Through Disposable Media Supply Chain Compromise Trusted Relationship Valid Accounts	Command and Emping Applications Container Allocation Container Deployment Container Exploitation for Client Execution Inter-Process Communication Native API Scheduled Task/Job System Process Event Triggered Execution Software Deployment Tools System Services User Execution Written Management Instrumentation	Account Manipulation BITS Jobs Boot or Login Assesstion Execution Deploy Container Browser Extensions Compromised Client Create Account Create or Modify System Process Event Triggered Execution External Remote Services Hijack Execution Flow Implant Internal Image Modify Administrative Process Office Application Startup Pre-OS Boot Scheduled Task/Job Server Software Component Traffic Signaling Valid Accounts	Local Manipulation Access Token Manipulation BITS Jobs Build Image on Host Deploy Container Direct Volume Access Domain Policy Modification Escape to Host Event Triggered Execution Hijack Execution Flow Process Injection Scheduled Task/Job Valid Accounts	Secure Execution Access Token Manipulation BITS Jobs Build Image on Host Deploy Container Direct Volume Access Domain Policy Modification Escape to Host Event Triggered Execution Hijack Execution Flow Process Injection Scheduled Task/Job Valid Accounts	Brute Force Credentials from Password Bases Exploitation for Credential Access Forged Authentication Input Capture Man-in-the-Middle Modify Administrative Process Network Sniffing OS Credential Dumping Steal Application Access Token Steal or Forge Hardware Tokens Hijack Session Cookie Impair Authentication Interception Unsecured Credentials Masquerading Modify Authentication Process Steal Computer Infrastructure Modify Registry Modify System Image Network Discovery Bringing Obfuscated Files or Information Pre-OS Boot Process Injection Rogue Domain Controller Rootkit Signed Binary Proxy Execution Signed Script Proxy Execution Subvert Trust Controls Template Injection Traffic Signaling Trusted Developer Utilities Proxy Execution Untrusted/Unsupported Cloud Regions Use Alternate Authentication Material Valid Accounts Virtualization/Container Weaken Encryption XSL Script Processing	Account Discovery Application Windows Discovery Automated Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery System Location Discovery System Network Configuration Discovery System Network Connections System Owner/User Discovery System Service Discovery System Time Discovery	Exploitation of Remote Services Internal Spearfishing Lateral Tool Transfer Remote Service Session Hijacking Remote Services Registration Through Disposable Media Software Deployment Tools Taint Shared Content User Message Authentication Material Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery System Location Discovery System Network Configuration Discovery System Network Connections System Owner/User Discovery System Service Discovery System Time Discovery	Archive Collected Data Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Configuration Repository Data from Information Repository Data from Local System Data from Removable Media Data Staged Email Collection Input Capture Man in the Browser Man in the Middle Screen Capture Video Capture	Application Layer Protocol Communication Through Removable Media Data Encoding Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-application Layer Protocol Non-Standard Port Protocol Tunneling Proxy Remote Access Software Traffic Signaling Web Service	Automated Exfiltration Data Transfer Data Limits Data Retention Data Encrypted for Impact Data Manipulation Exfiltration Over C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium Exfiltration Over Web Service Scheduled Transfer Transfer Data to Cloud Account Network Denial of Service Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Disk Wipe Endpoint Denial of Service Firmware Corruption Inhibit System Recovery Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot

# Where is this navigator?



The screenshot shows a web browser window with the address bar displaying `mitre-attack.github.io/attack-navigator/`. The page title is "MITRE ATT&CK® Navigator". A "new tab" button is visible in the top left. The main content area features a central menu with four options, each with a description and a dropdown arrow:

Create New Layer	Create a new empty layer	▼
Open Existing Layer	Load a layer from your computer or a URL	▼
Create Layer from other layers	Choose layers to inherit properties from	▼
Create Customized Navigator	Create a hyperlink to a customized ATT&CK Navigator	▼

Below the menu is a "help" link. At the bottom left of the page, the text "MITRE ATT&CK® Navigator v4.3" is displayed.

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

# Create A New Layer - Enterprise

← → ↻ [mitre-attack.github.io/attack-navigator/](https://mitre-attack.github.io/attack-navigator/)    

MITRE ATT&CK® Navigator 

new tab x +

Create New Layer      Create a new empty layer      ^

Enterprise      Mobile      ICS

More Options      v

Open Existing Layer      Load a layer from your computer or a URL      v

Create Layer from other layers      Choose layers to inherit properties from      v

Create Customized Navigator      Create a hyperlink to a customized ATT&CK Navigator      v

help



AUSCERT

# Change the Layer name

MITRE ATT&CK® Navigator

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Data Manipulation (0/3)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Defacement (0/2)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Direct Volume Access	Input Capture (0/4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Disk Wipe (0/2)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Man-in-the-Middle (0/2)	Container and Resource Discovery	Taint Shared Content	Data from Information Repositories (0/2)	Fallback Channels	Endpoint Denial of Service (0/4)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Trusted Relationship	Software Deployment Tools	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Modify Authentication Process (0/4)	File and Directory Discovery	Use Alternate Authentication Material (0/4)	Data from Local System	Ingress Tool Transfer	Firmware Corruption	Firmware Corruption
Search Open Websites/Domains (0/2)	Valid Accounts (0/4)	System Services (0/2)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing (0/8)	File and Directory Permissions Modification (0/2)	Software Deployment Tools	Data from Network Shared Drive	Multi-Stage Channels	Inhibit System Recovery	Inhibit System Recovery
Search Victim-Owned Websites	User Execution (0/3)	User Execution (0/3)	System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	Hide Artifacts (0/7)	Taint Shared Content	Data from Network Shared Drive	Non-Application Layer Protocol	Network Denial of Service (0/2)	Network Denial of Service (0/2)
	Windows Management Instrumentation	Hijack Execution Flow (0/11)	User Execution (0/3)	Hijack Execution Flow (0/11)	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Exploitation for Defense Evasion	Use Alternate Authentication Material (0/4)	Data from Removable Media	Non-Standard Port	Resource Hijacking	Resource Hijacking
		Implant Internal Image	System Services (0/2)	Process Injection (0/11)	Scheduled Task/Job (0/7)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data Staged (0/2)	Protocol Tunneling	Service Stop	Service Stop
		Modify Authentication Process (0/4)	System Services (0/2)	Scheduled Task/Job (0/7)	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Network Share Discovery	Use Alternate Authentication Material (0/4)	Email Collection (0/3)	Proxy (0/4)	System Shutdown/Reboot	System Shutdown/Reboot
		Office Application Startup (0/6)	System Services (0/2)	Valid Accounts (0/4)	Indirect Command Execution	Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	OS Credential Dumping (0/8)	Use Alternate Authentication Material (0/4)	Input Capture (0/4)	Remote Access Software		
		Pre-OS Boot (0/5)	System Services (0/2)	Valid Accounts (0/4)	Masquerading (0/6)	Indirect Command Execution	Unsecured Credentials (0/7)	Password Policy Discovery	Use Alternate Authentication Material (0/4)	Man in the Browser	Traffic Signaling (0/1)		
		Scheduled Task/Job (0/7)	System Services (0/2)	Valid Accounts (0/4)	Modify Authentication Process (0/4)	Indirect Command Execution	Unsecured Credentials (0/7)	Peripheral Device Discovery	Use Alternate Authentication Material (0/4)	Man-in-the-Middle (0/2)	Web Service (0/3)		
		Server Software Component (0/3)	System Services (0/2)	Valid Accounts (0/4)	Modify Cloud Compute Infrastructure (0/4)	Indirect Command Execution	Unsecured Credentials (0/7)	Permission Groups Discovery (0/3)	Use Alternate Authentication Material (0/4)	Screen Capture			
		Traffic Signaling (0/1)	System Services (0/2)	Valid Accounts (0/4)	Modify Registry (0/4)	Indirect Command Execution	Unsecured Credentials (0/7)	Process Discovery	Use Alternate Authentication Material (0/4)	Video Capture			
		Valid	System Services (0/2)	Valid Accounts (0/4)	Modify System Image (0/2)	Indirect Command Execution	Unsecured Credentials (0/7)	Query Registry	Use Alternate Authentication Material (0/4)				
			System Services (0/2)	Valid Accounts (0/4)	Network Boundary Bridging (0/1)	Indirect Command Execution	Unsecured Credentials (0/7)	Remote System Discovery	Use Alternate Authentication Material (0/4)				
			System Services (0/2)	Valid Accounts (0/4)	Valid	Indirect Command Execution	Unsecured Credentials (0/7)	Software Discovery (0/1)	Use Alternate Authentication Material (0/4)				
			System Services (0/2)	Valid Accounts (0/4)	Valid	Indirect Command Execution	Unsecured Credentials (0/7)	System Information Discovery	Use Alternate Authentication Material (0/4)				
			System Services (0/2)	Valid Accounts (0/4)	Valid	Indirect Command Execution	Unsecured Credentials (0/7)	System Location Discovery	Use Alternate Authentication Material (0/4)				
			System Services (0/2)	Valid Accounts (0/4)	Valid	Indirect Command Execution	Unsecured Credentials (0/7)	System Network Configuration Discovery (0/1)	Use Alternate Authentication Material (0/4)				



# Next... will be toolbar navigation

mitre-attack.github.io/attack-navigator/ MITRE ATT&CK® Navigator

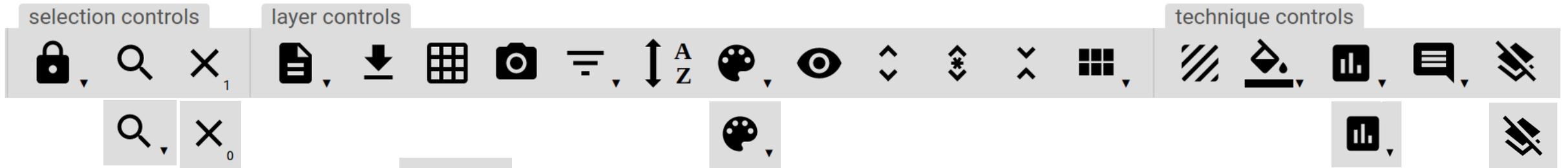
Threats x +

selection controls    layer controls    technique controls

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials From Password Stores (0/5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/5)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Dynamic Resolution (0/3)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Dashboard	Replication Through Removable Media	Data from Cloud Storage Object	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/5)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Service Discovery	Software Deployment Tools	Data from Configuration Repository (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (0/2)	Container and Resource Discovery	Taint Shared Content	Data from Information Repositories (0/2)	Encrypted Channel (0/2)	Firmware Corruption	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Domain Policy Modification (0/2)	Modify Authentication Process (0/4)	File and Directory Discovery	Use Alternate Authentication Material (0/4)	Data from Local System	Fallback Channels	Inhibit System Recovery	Endpoint Denial of Service (0/4)
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Network Sniffing	File and Directory Permissions Modification (0/2)		Data from Network Shared Drive	Ingress Tool Transfer	Network Denial of Service (0/2)	Resource Hijacking
Search Victim-Owned Websites			System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	Exploitation for Defense Evasion	OS Credential Dumping (0/8)	File and Directory Permissions Modification (0/2)		Data from Removable Media	Multi-Stage Channels	Scheduled Transfer	Service Stop
			User Execution (0/3)	Hijack Execution Flow (0/11)	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot
			Windows Management Instrumentation	Process Injection (0/11)	Scheduled Task/Job (0/7)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Password Policy Discovery		Data Staged (0/2)	Non-Standard Port		
				Scheduled Task/Job (0/7)	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Peripheral Device Discovery		Email Collection (0/3)	Protocol Tunneling		
				Office Application Startup (0/6)	Masquerading (0/6)	Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Permission Groups Discovery (0/3)		Input Capture (0/4)	Proxy (0/4)		
				Pre-OS Boot (0/5)	Modify Authentication Process (0/4)	Indirect Command Execution	Unsecured Credentials (0/7)	Process Discovery		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/7)	Modify Cloud Compute Infrastructure (0/4)	Masquerading (0/6)	Modify System Image	Query Registry		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component (0/3)	Modify Registry	Modify Authentication Process (0/4)		Remote System Discovery		Screen Capture	Web Service (0/3)		
					Modify System Image	Modify Cloud Compute Infrastructure (0/4)		Software Discovery (0/1)		Video Capture			
						Modify Registry		System Information Discovery					
						Modify System Image		System Location Discovery					



# CK Navigator toolbar



- Search



- Deselect



- Color setup



- Scoring



- Clear Annotation

# SEARCH

Q Search

Search Settings

name  ATT&CK ID  description  data sources

Techniques (552) ^

select all      deselect all

Abuse Elevation Control Mechanism	<a href="#">view</a>	select	deselect
Abuse Elevation Control Mechanism : Setuid and Setgid	<a href="#">view</a>	select	deselect
Abuse Elevation Control Mechanism : Bypass User Account Control	<a href="#">view</a>	select	deselect

Threat Groups (121) v

Software (493) v

Mitigations (42) v

Close

- 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

Tactic Row Background	
<input type="checkbox"/> show	#dddddd
Scoring Gradient	
Low value:	0
remove	#ff6666
remove	#ffe766
remove	#8ec843
add another color	
High value:	100
presets ▾	

- red to green
- green to red
- blue to red
- red to blue
- white to blue
- white to red

- 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

 scoring

score  
1



score  
50



score  
100



- 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





# 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.

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

this post was edited O.P.

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 lose 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.

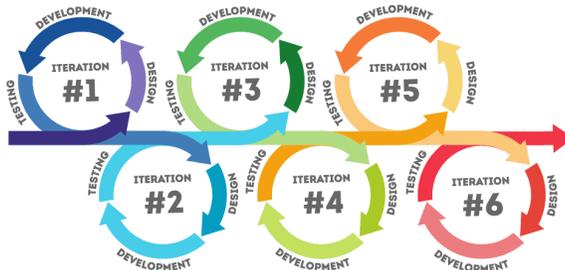
- There might not be malicious files.

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 Framework
- Sooner or later someone is going to be wrong and something is going to have happened



# 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 syslog 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. HotFrankfurtcarl and not ASKjsas112313 - 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-learning. 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 prioritise vulnerabilities (some vulnerabilities are config and not just patching).
- now prevent WScript and Powershell running on PCs (DO THIS!)
- prioritised 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 lose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check for 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 lose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check for on-going exploitation. I believe our fast recovery is atypical

# Is a phish a phish by any other name?

Search  
Phishing

Search Settings  
 name  ATT&CK ID  description  data sources

Techniques (67)

	select all		deselect all
Gather Victim Network Information	<a href="#">view</a>	select	deselect
Gather Victim Org Information	<a href="#">view</a>	select	deselect
Internal Spearphishing	<a href="#">view</a>	select	deselect
Phishing	<a href="#">view</a>	select	deselect
Phishing for Information	<a href="#">view</a>	select	deselect

Threat Groups (8) ▼

Software (8) ▼

Mitigations (1) ▼

Close

Home > Techniques > Enterprise > Phishing

## Phishing

Sub-techniques (3) ▼

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

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source.

ID: T1566

Sub-techniques: [T1566.001](#), [T1566.002](#), [T1566.003](#)

- ① **Tactic:** [Initial Access](#)
- ① **Platforms:** Google Workspace, Linux, Office 365, SaaS, Windows, macOS
- ① **Data Sources:** [Application Log:](#) Application Log Content, [Network Traffic:](#) Network Traffic Content, [Network Traffic:](#) Network Traffic Flow
- ① **CAPEC ID:** [CAPEC-98](#)

Contributors: Philip Winther

Version: 2.1

Created: 02 March 2020

Last Modified: 14 April 2021

# 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 lose 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

about

**Exercise**

domain

**Enterprise ATT&CK v9**

platforms

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

legend

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Spying	Account Manipulation	Abuse Elevation	Abuse Elevation	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Public-Facing Application	Exploit	BITS Jobs	Control Metasploit	Control Metasploit	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Infrastructure Compromise	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Access Token Manipulation	Access Token Manipulation	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Processes	Desktop/Local Decode File or Information	Forge Web Credentials	Cloud Service Dashboard	Remote Services	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Network Medium	Defacement
Search Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client	Domain Policy Modification	Deploy Container	Input Capture	Cloud Service Discovery	Registration Through Removable Media	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Software Binary	Escape to Host	Direct Volume Access	Man-in-the-Middle	Container and Resource Discovery	Software Employment Tools	Data from Information Repository	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Gateways		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Domain Policy Modification	Modify Authentication Process	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	System Services	Event Triggered Execution	Exploitation for Defense Evasion	Execution Guardrails	Network Sniffing	File and Directory Discovery	User Alternate Authentication Methods	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Resource Hijacking
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow	OS Credential Dumping	OS Credential Dumping	Network Service Scanning		Data from Removable Media	Non-Standard Port		Network Denial of Service
			User Execution	Hijack Execution Flow	Process Injection	File and Directory Permissions Modification	Steal Application Access Token	Network Share Discovery		Data Staged	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Hide Artifacts	Steal or Forge Browser Cookies	Network Sniffing		Email Collection	Proxy		System Shutdown/Reboot
				Modify Authentication Process	Valid Accounts	Hijack Execution Flow	Steal Web Session Cookie	Password Policy Discovery		Input Capture	Remote Access Software		
				Office Application Setup		Impair Defenses	Two-Factor Authentication	Peripheral Device Discovery		Man in the Browser	Traffic Signaling		
				Pre-OS Boot		Indicator Removal on Host	Unsecured Credentials	Process Discovery		Man-in-the-Middle	Web Service		
				Scheduled Task/Job		Indirect Command Execution		Query Registry		Screen Capture			
				Server Software Component		Masquerading		Registry		Video Capture			
				Traffic Signaling		Modify Authentication Process		Remote System Discovery					
				Valid Accounts		Modify System Image		Software Discovery					
						Network Boundary Bridging		System Information Discovery					
						Obfuscated Files or Information		System Location Discovery					
						Pre-OS Boot		System Network Discovery					
						Process Injection		System Network Connectors Discovery					
						Rogue Domain Controller		System Owner/User Discovery					
						Rootkit		System Service Discovery					
						Signed Binary		System Time Discovery					
						Proxy Execution		Virtualization/Sandbox Evasion					
						Signed Script							
						Privilege Escalation							
						Solvent Trust Controls							
						Template Injection							
						Traffic Signaling							
						Trusted Developer JARs							
						Proxy Execution							
						Universal/Unsupported Client Programs							
						User Alternate Authentication Methods							
						Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							

# 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 lose 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 lose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check for on-going exploitation. I believe our fast recovery is atypical

# We just want th 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 lose 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 lose 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 lose 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 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 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



# 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 lose 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



## 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 lose 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 lose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check for 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 lose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check for 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 lose any transactional data. Forensics took a day and it then took 36 hours to get servers and processing systems online and check for on-going exploitation. I believe our fast recovery is atypical



# 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 16kx365 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. Hotfrankmutter! and not ASKjsat112&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-learning. 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 prioritise vulnerabilities (some vulnerabilities are config and not just patching)
- now prevent WScript and Powershell running on PCs (DO THIS)
- prioritised 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

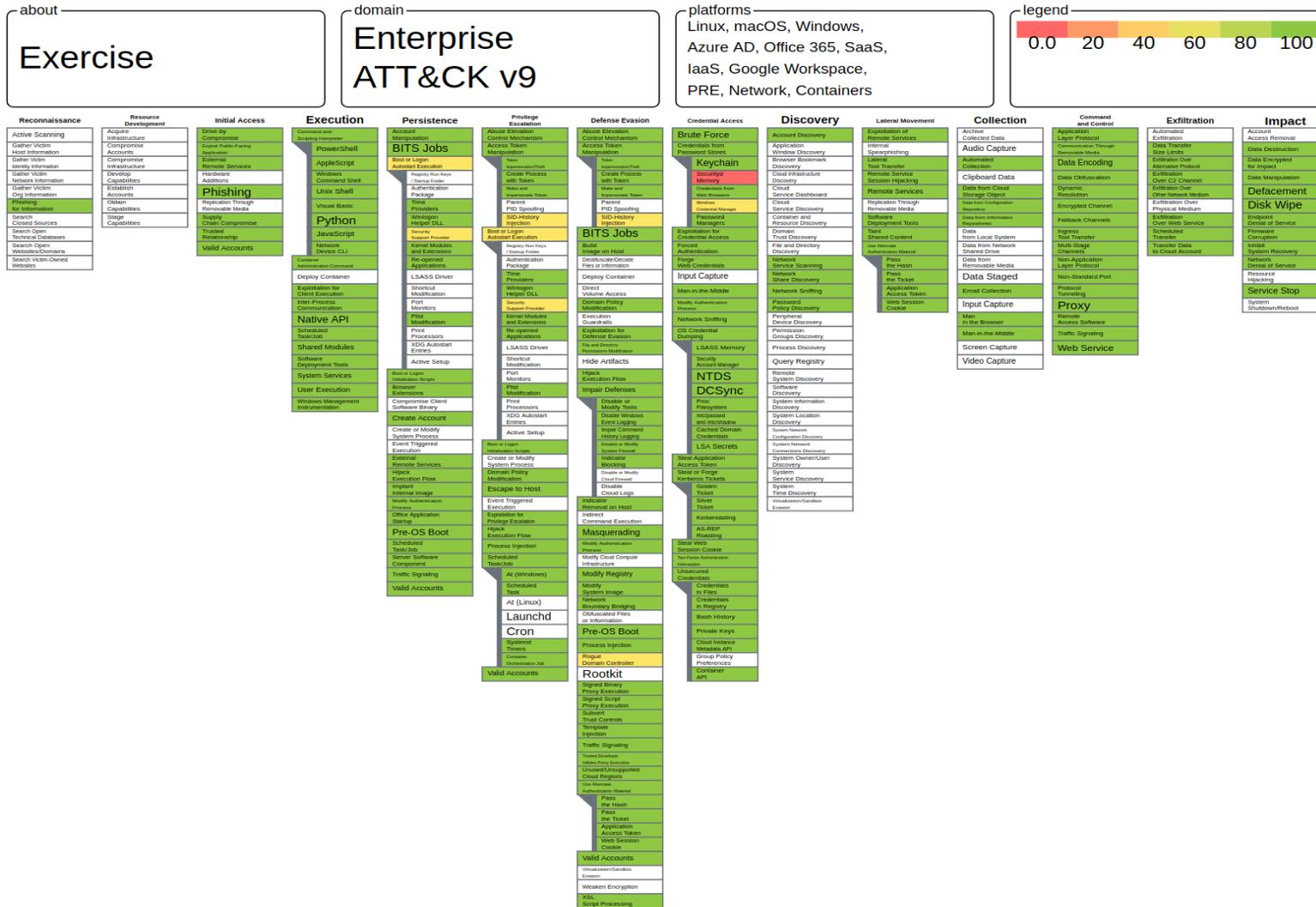
I thought we were prepared for a ransomware attack. But I didn't understand the sophistication of today's attacks including the need for a 24x7 monitored SIEM, forensics and long dwell time of some attackers that can undermine backups.

I hope this is helpful.

# MITIGATIONS

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

# Masking with the Mitigations



# 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

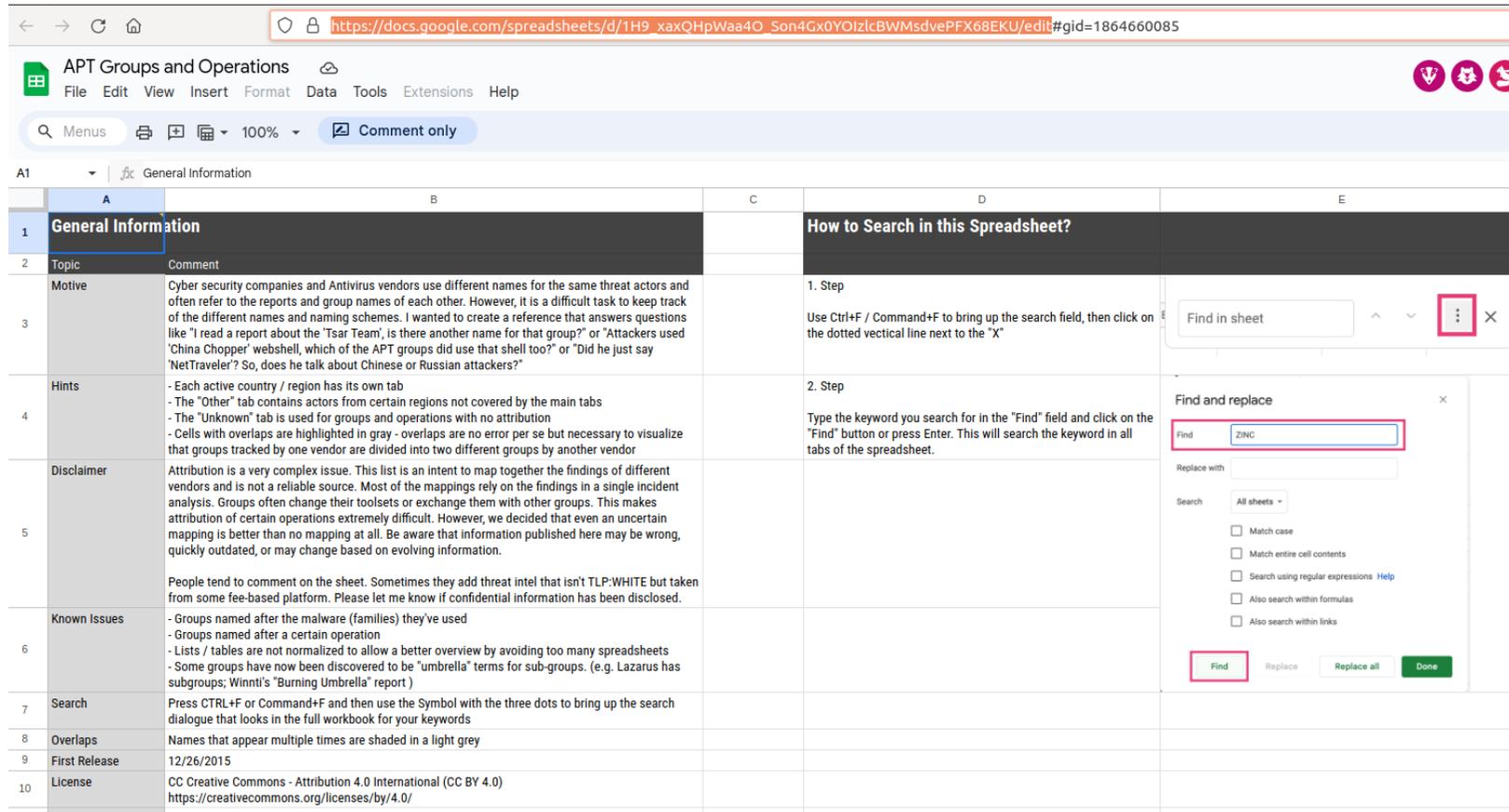
Cheatsheet: <https://github.com/DISREL/Conti-Leaked-Playbook-TTPs/blob/main/Conti-Leaked-Playbook-TTPs.pdf>  
<https://github.com/j91321/conti-manuals-analysis>

# Exercise

Filling up the Cybersecurity Framework covering an industry



# APT Group and Operations



The screenshot shows a Google Sheet with the following content:

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 vertical 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 dialog 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) <a href="https://creativecommons.org/licenses/by/4.0/">https://creativecommons.org/licenses/by/4.0/</a>		

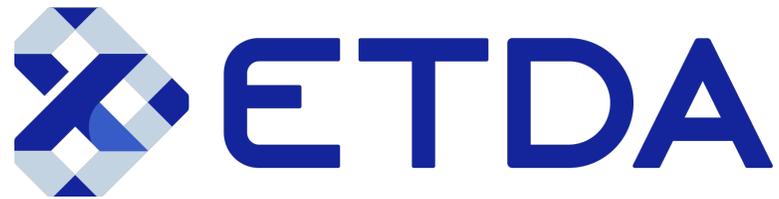
Overlaid on the right side of the spreadsheet are two search tool windows:

- Find in sheet:** A search bar with a dropdown arrow and a three-dot menu icon highlighted with a red box.
- Find and replace:** A dialog box with a "Find" field containing the text "ZINC" (highlighted with a red box), a "Replace with" field, and search options like "Match case", "Match entire cell contents", etc. The "Find" button is also highlighted with a red box.



[https://docs.google.com/spreadsheets/d/1H9\\_xaxQHpwaa4O\\_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit](https://docs.google.com/spreadsheets/d/1H9_xaxQHpwaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit)

# Threat card



IDENTIFY



[Groups](#) [Tools](#) [Search](#) [Statistics](#)



[Home](#)

[Search](#)

## Threat Group Cards: A Threat Actor Encyclopedia

### Main menu

- [Browse threat groups](#)
- [Browse their tools](#)
- [Search](#)
- [Statistics](#)



[Groups](#) [Tools](#) [Search](#) [Statistics](#)



[Home](#) > [Search](#)

## Threat Group Cards: A Threat Actor Encyclopedia



### Database search

<b>Actor</b>	Source country	...	▼
	Victim country	...	▼ <input type="checkbox"/> or Worldwide
	Victim sector	Government	▼
	Motivation	...	▼
	Free text search	<input type="text"/> (can use '*' and '?' wildcards)	
		<input type="button" value="Search!"/>	



[Home](#) > [List all groups](#) > List all groups targeting sector Government

[Search](#)

## Threat Group Cards: A Threat Actor Encyclopedia

### All groups targeting sector Government

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Aggah</a>	[Unknown]	2018-Jun 2022
	<a href="#">Anchor Panda, APT 14</a>		2012
	<a href="#">Aoqin Dragon</a>		2013
	<a href="#">APT 4, Maverick Panda, Wisp Team</a>		2007-Oct 2018
	<a href="#">APT 6</a>		2011
	<a href="#">APT 12, Numbered Panda</a>		2009-Nov 2016

IDENTIFY



# 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™**



## 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](#)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques
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 (3)
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)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automate 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 (5)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery		Data from Cloud Storage
Search Open Sources (2)	Stage Capabilities (6)					Direct Volume Access		Container and Resource Discovery		Data from Cloud Storage

# Navigator

## MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

[help](#) [changelog](#) [theme ▼](#)

Create New Layer	Create a new empty layer	^
<input type="button" value="Enterprise"/>	<input type="button" value="Mobile"/>	<input type="button" value="ICS"/>
<input type="button" value="More Options"/>		▼
Open Existing Layer	Load a layer from your computer or a URL	▼
Create Layer from other layers	Choose layers to inherit properties from	▼
Create Customized Navigator	Create a hyperlink to a customized ATT&CK Navigator	▼



# Initial Access

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

Initial Access 9 techniques	
Drive-by Compromise	
Exploit Public-Facing Application	
External Remote Services	
Hardware Additions	
Phishing (3/3)	
Replication Through Removable Media	
Supply Chain Compromise (0/3)	
Trusted Relationship	
Valid Accounts (3/4)	

Application of Risk on a Service

# CSIRT Services

- Search Term “CSIRT Service Framework 2.1”
- Target Link :  
[https://www.first.org/standards/frameworks/csirts/csirt\\_services\\_framework\\_v2.1](https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)

- Looks Like



The screenshot shows the FIRST website's navigation and content for the CSIRT Services Framework. The top navigation bar includes links for About FIRST, Membership, Initiatives, Standards & Publications, Events, Education, and Blog, along with a Sign in button. The main content area is titled "FIRST CSIRT Services Framework" and features a "Version 2.1" label with a PDF download link. The page is structured with a left sidebar for navigation, a central main content area, and a right sidebar for a Table of Contents.

**Standards & Publications**

- Standards
  - Common Vulnerability Scoring System (CVSS-SIG)
  - Traffic Light Protocol (TLP)
  - Service Frameworks
    - CSIRT Services Framework**
    - PSIRT Services Framework
  - Information Exchange Policy (IEP)
  - Passive DNS Exchange
  - Exploit Prediction Scoring System (EPSS)
- Publications
  - Best Practices Guide (BPGL)
  - Security Reference Index

**FIRST CSIRT Services Framework**

*Version 2.1*  
Also available in [PDF](#)

**Computer Security Incident Response Team (CSIRT) Services Framework**

**1 Purpose**

The Computer Security Incident Response Team (CSIRT) Services Framework is a high-level document describing in a structured way a collection of cyber security services and associated functions that Computer Security Incident Response Teams and other teams providing incident management related services may provide. The framework is developed by recognized experts from the FIRST community with strong support from the Task Force CSIRT (TF-CSIRT) Community, and the International Telecommunications Union (ITU).

**Table of Contents**

- 1 Purpose
- 2 Introduction and Background
- 3 The Difference Between a CSIRT and a PSIRT
- 4 CSIRT Services Framework Structure
- 5 Service Area: Information Security Event Management
  - 5.1 Service: Monitoring and detection
  - 5.2 Service: Event analysis
- 6 Service Area: Information Security Incident Management

# 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>

# Domains



Centralised Zone  
Data Service



Delegation Record

URL to Registration service

Domain Registrar

Domain Registrar  
Domain Registrar

# Domain Data repositories (simplification)

## japan-ja1.jp



Domain NIC

Certificate  
Transparency



A-Record  
(online)

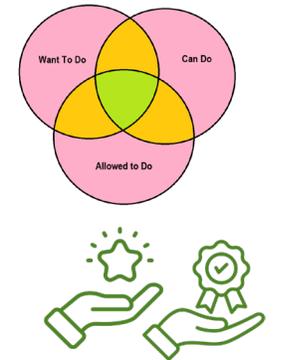
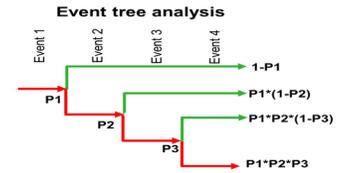
Analysis  
Repositories



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

# 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



Domain NIC

Certificate  
 Transparency



A-Record  
 (online)

Analysis  
 Repositories



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

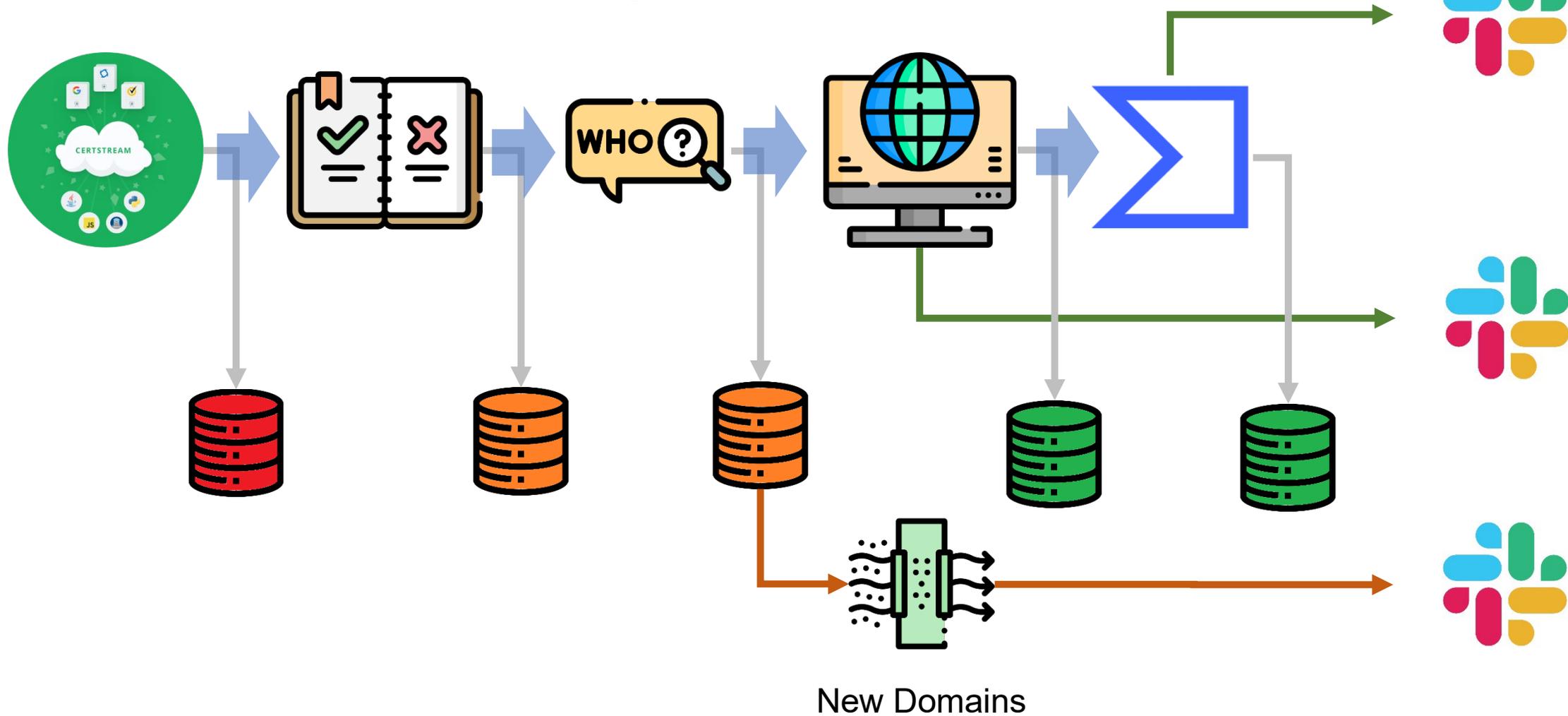


# Certstream Recap

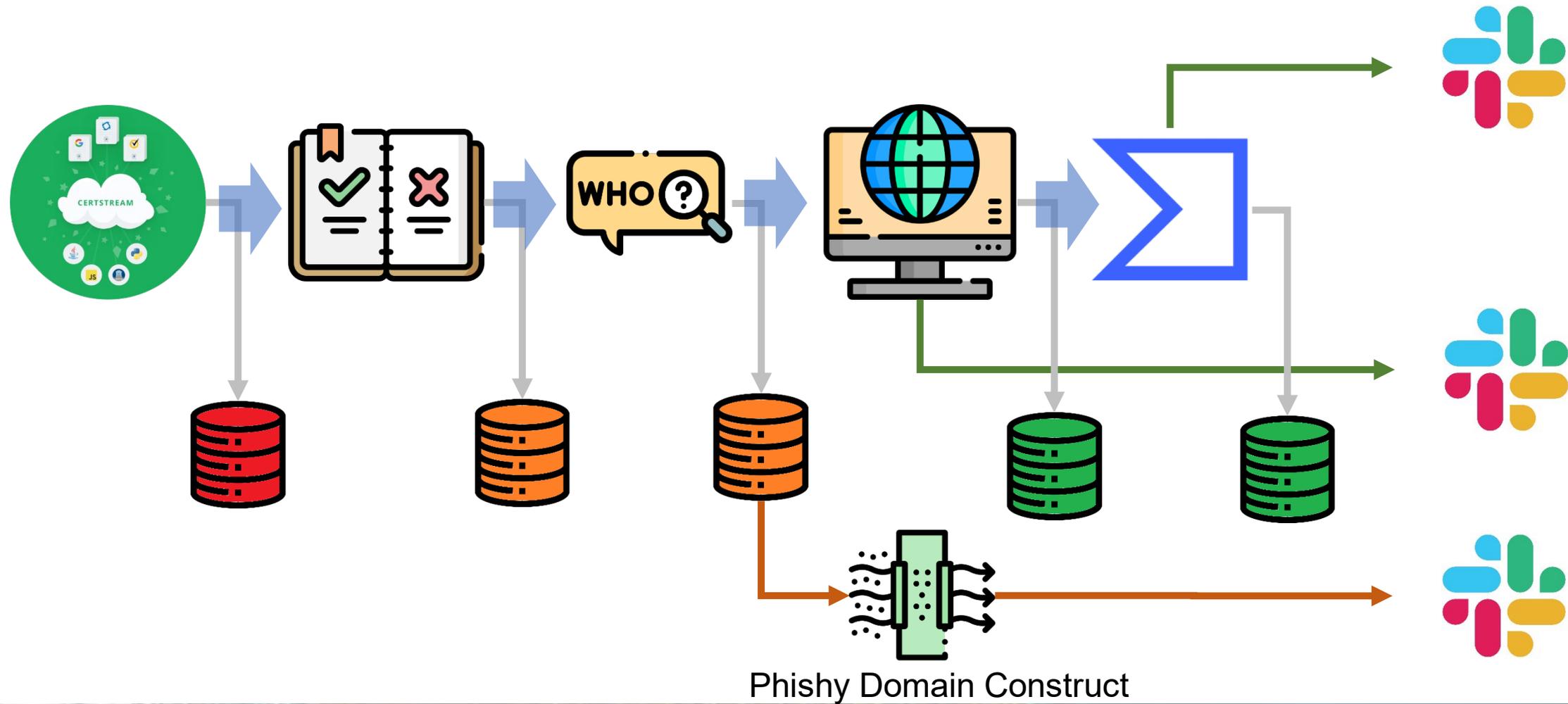
Can it really be done?



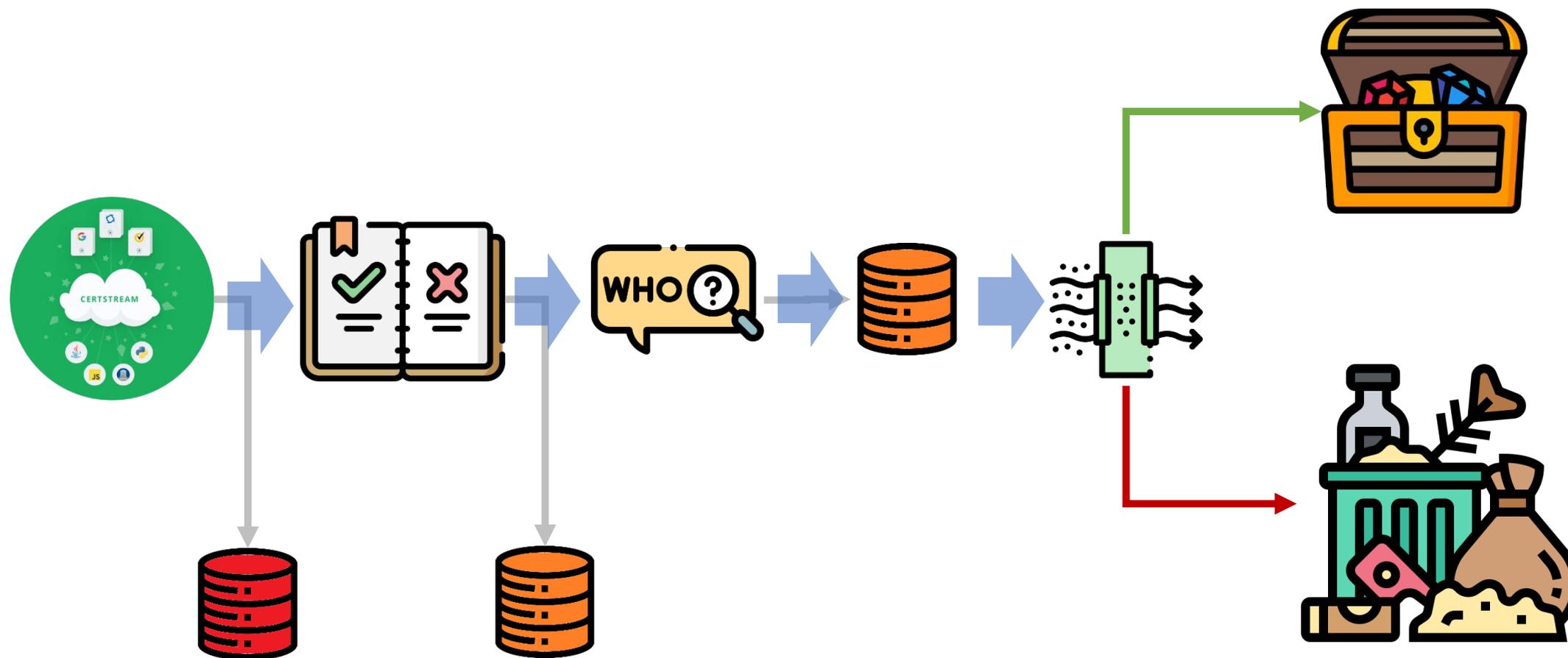
# How we used to process Certstream



# How we should to process Certstream



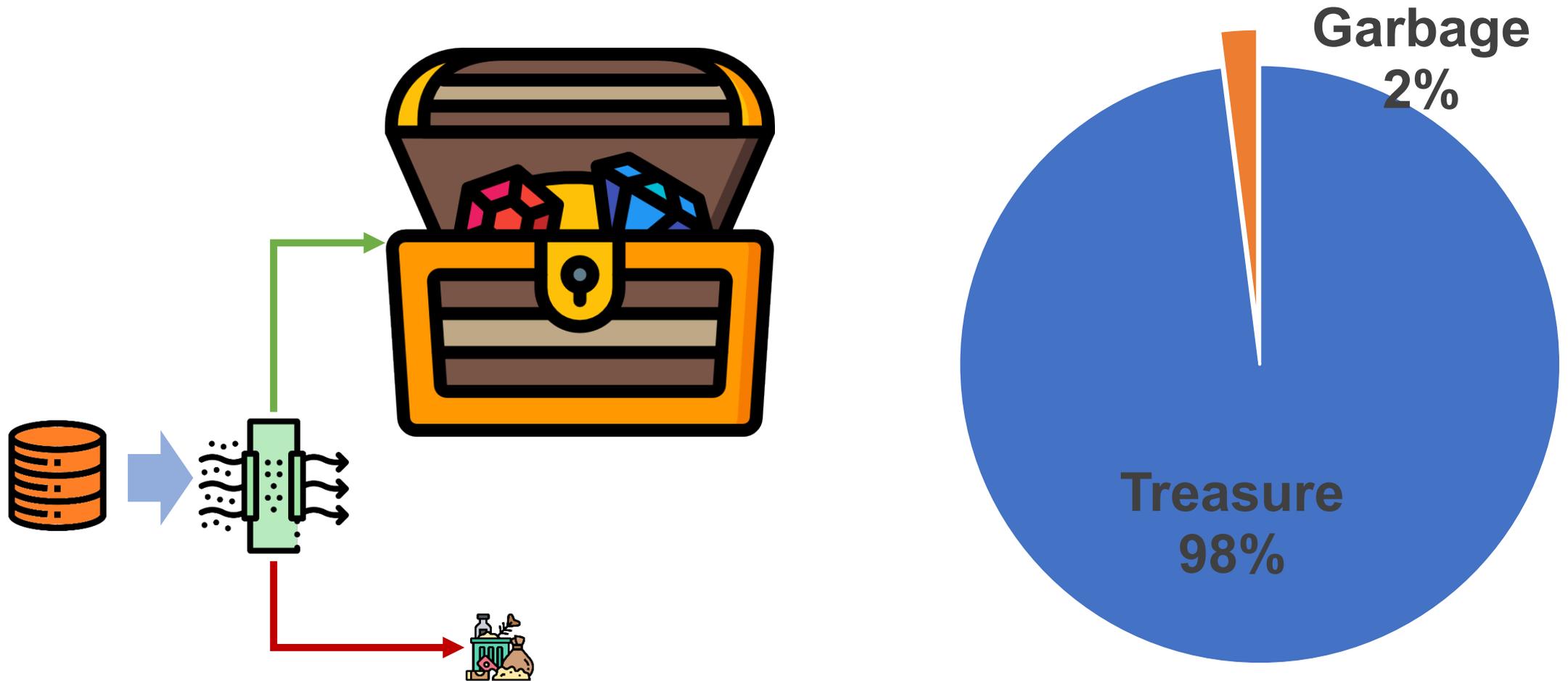
# How we should process phishy domains



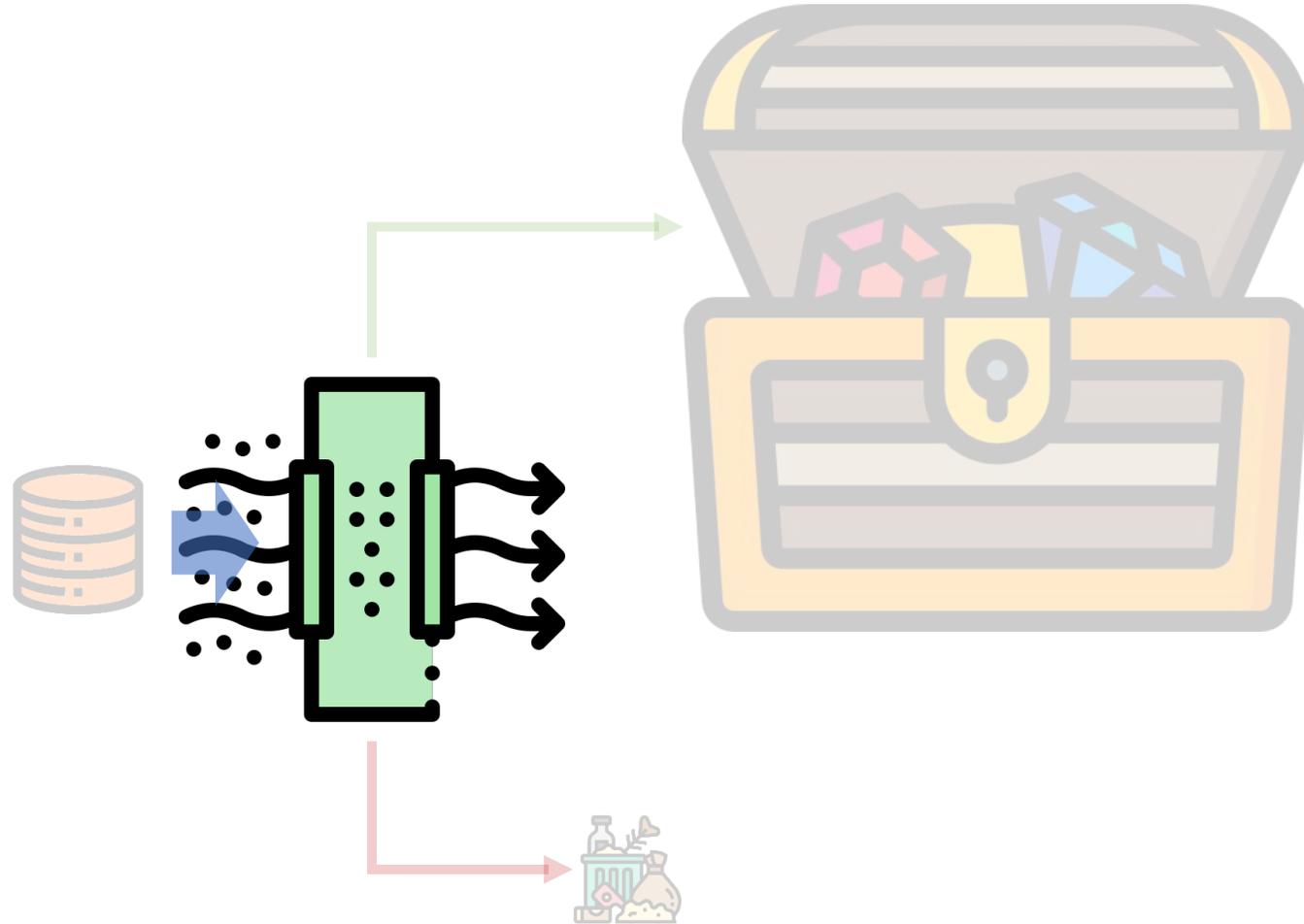
# Treasure Vs Garbage (Rules Based)



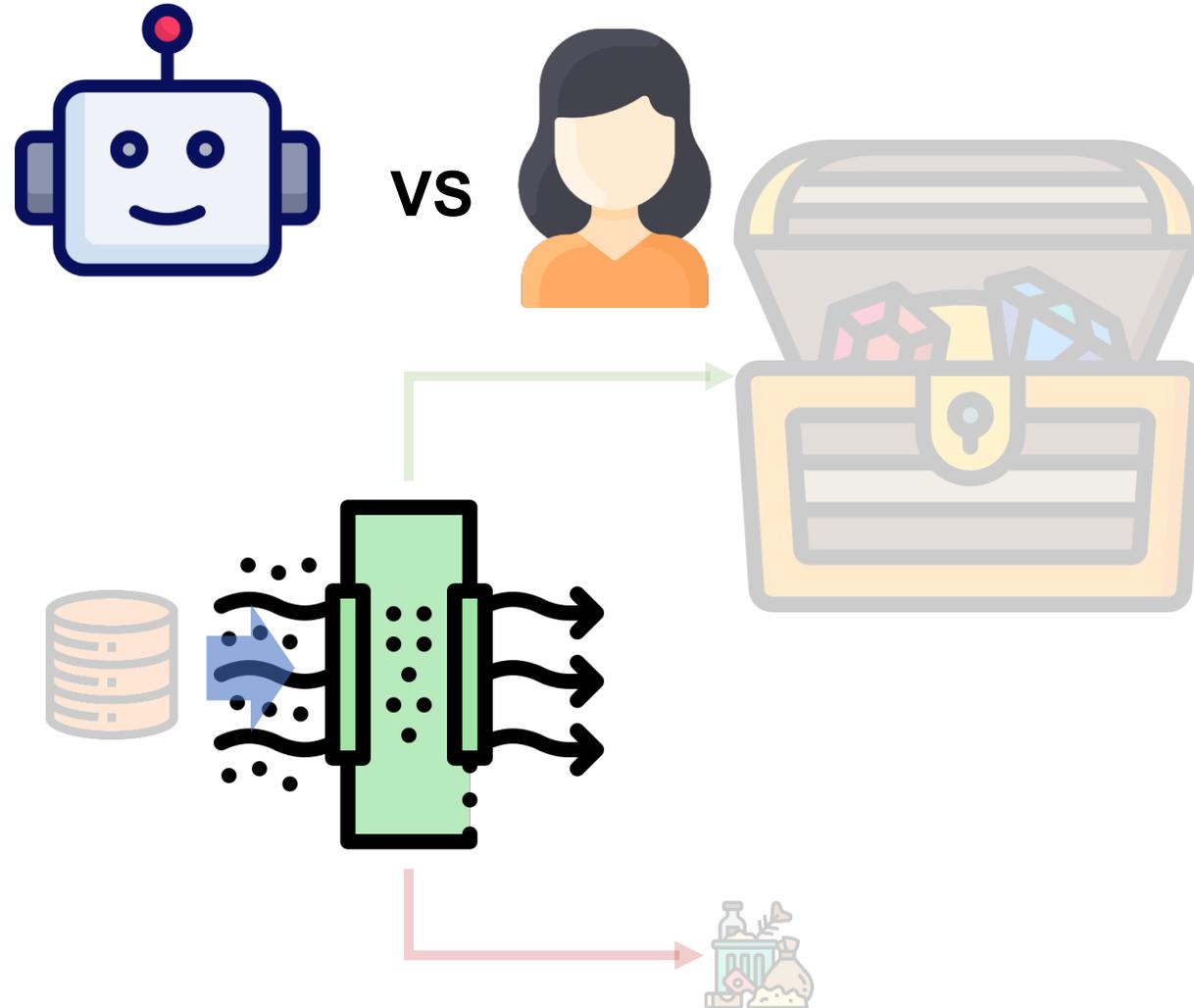
# Treasure Vs Garbage (Required Filter)



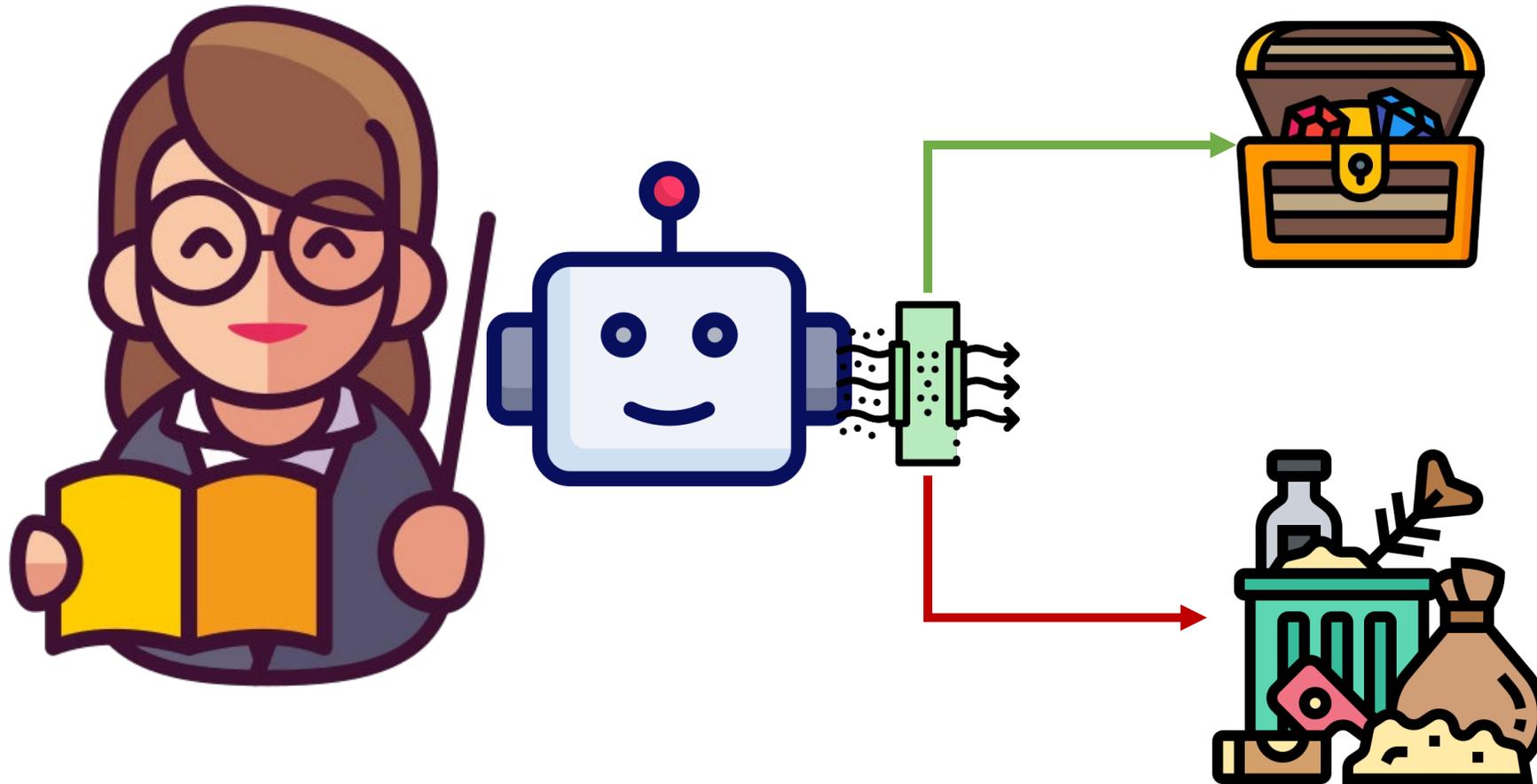
# Filter of Treasure Vs Garbage



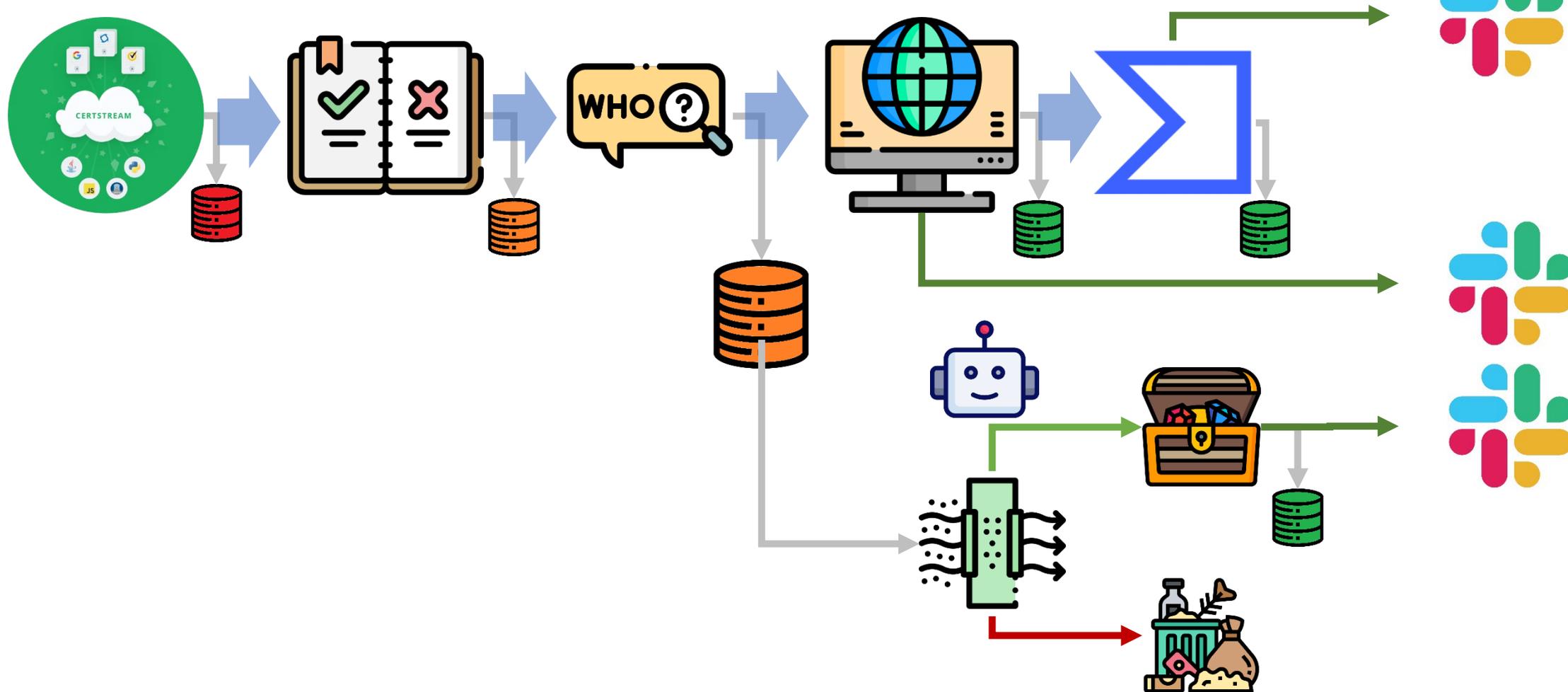
# Machine - Human

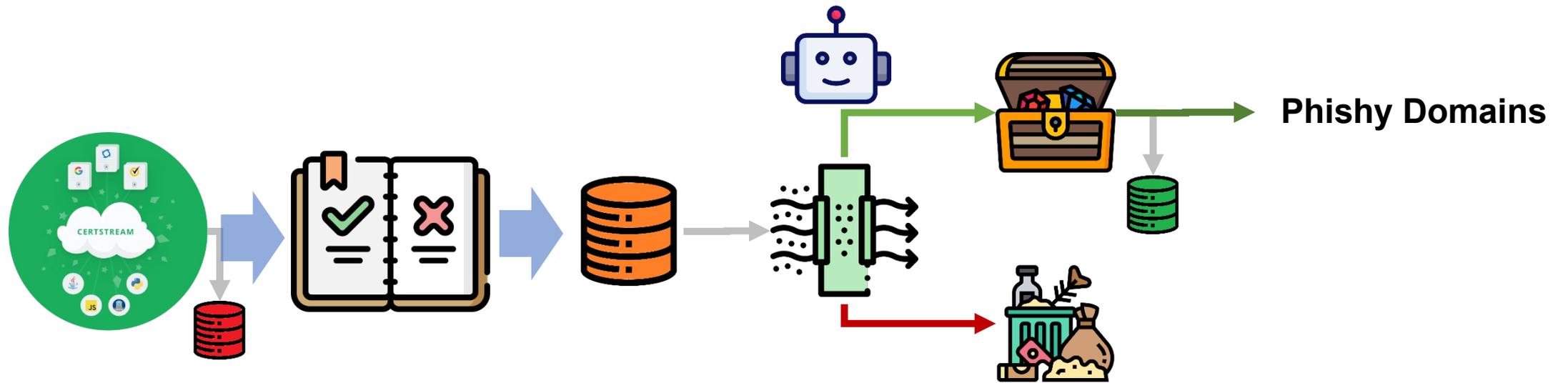


# Teaching the Machine



# Getting phishy domains before online

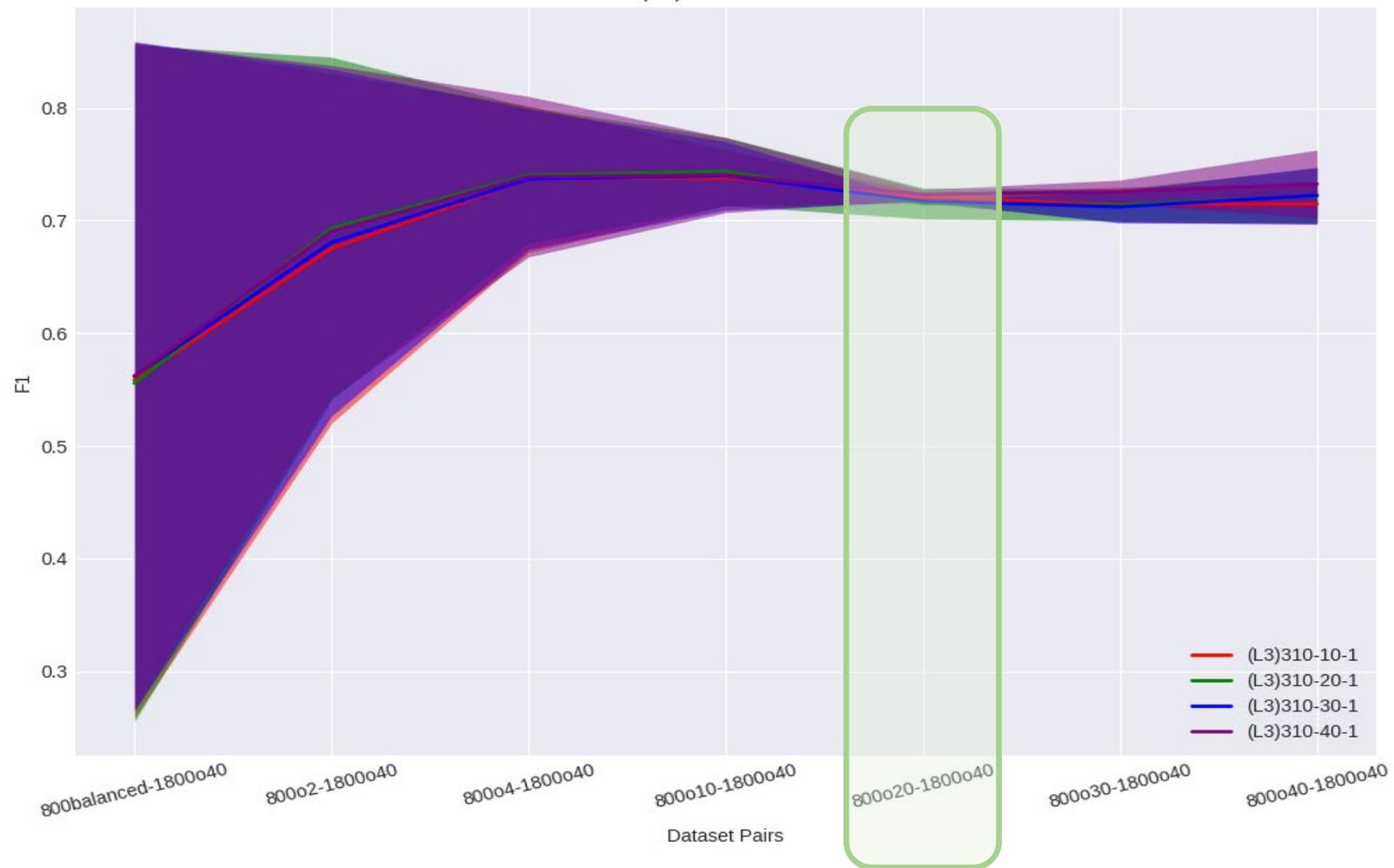




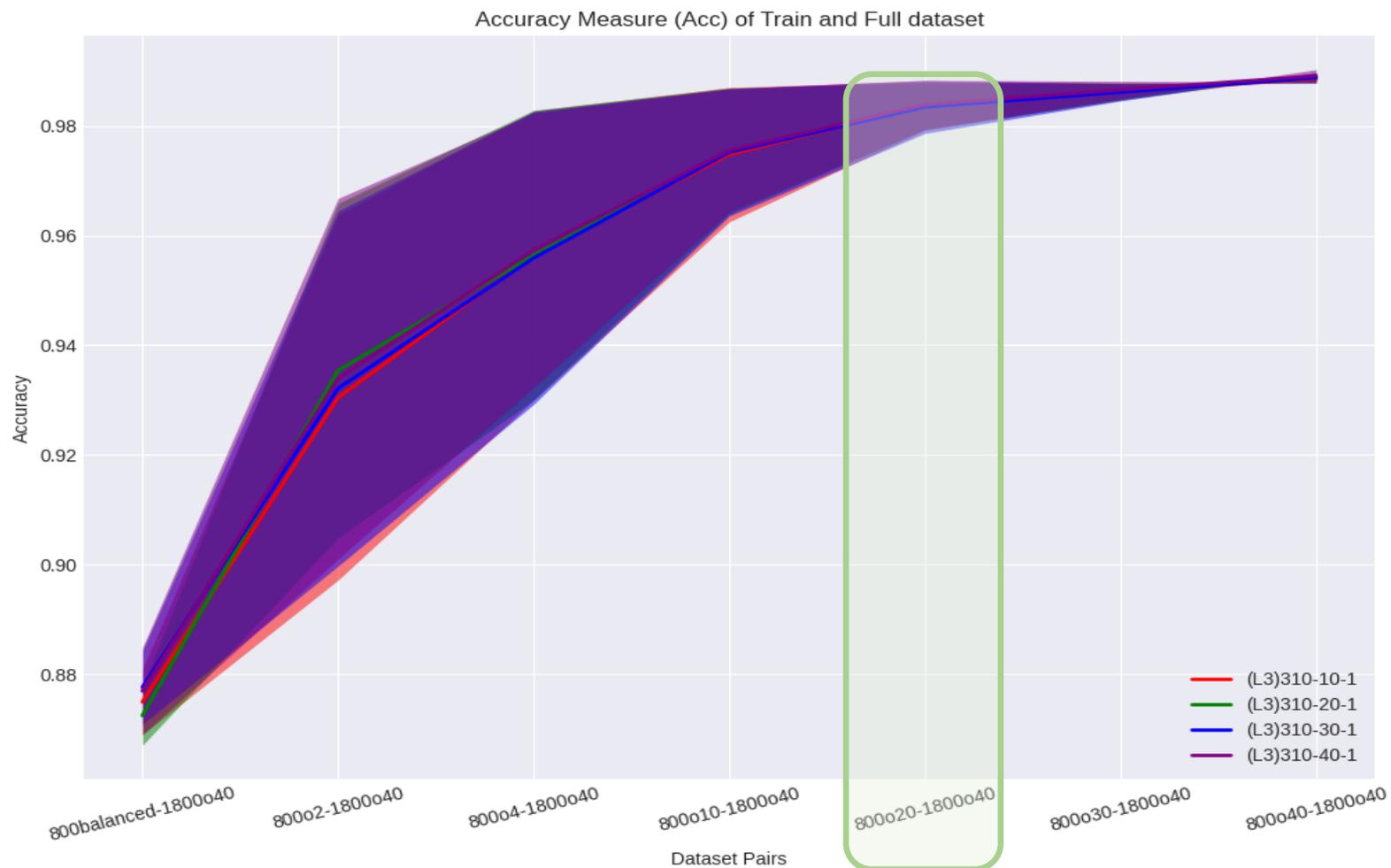
-  High volume / Low confidence data
-  Medium volume / Medium confidence data
-  Low volume / High confidence data

# How Much Data Solution ~800o20

Fit Measure (F1) of Train and Full dataset

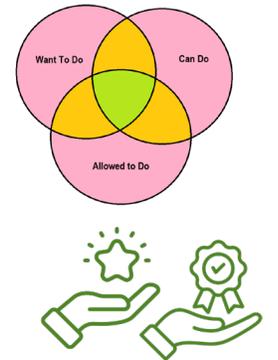
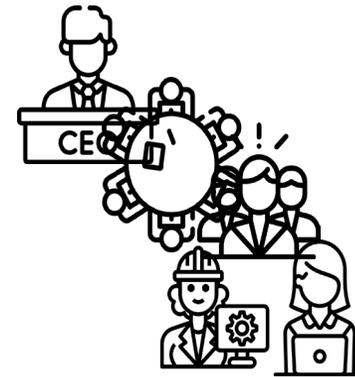
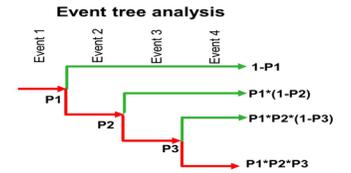


# How Much Data Solution ~800o20



# 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



Domain NIC

Certificate  
Transparency



A-Record  
(online)

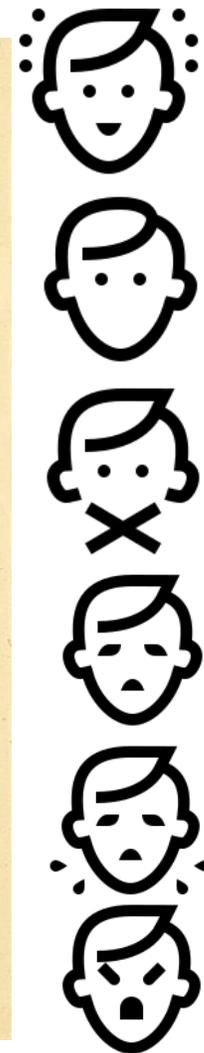
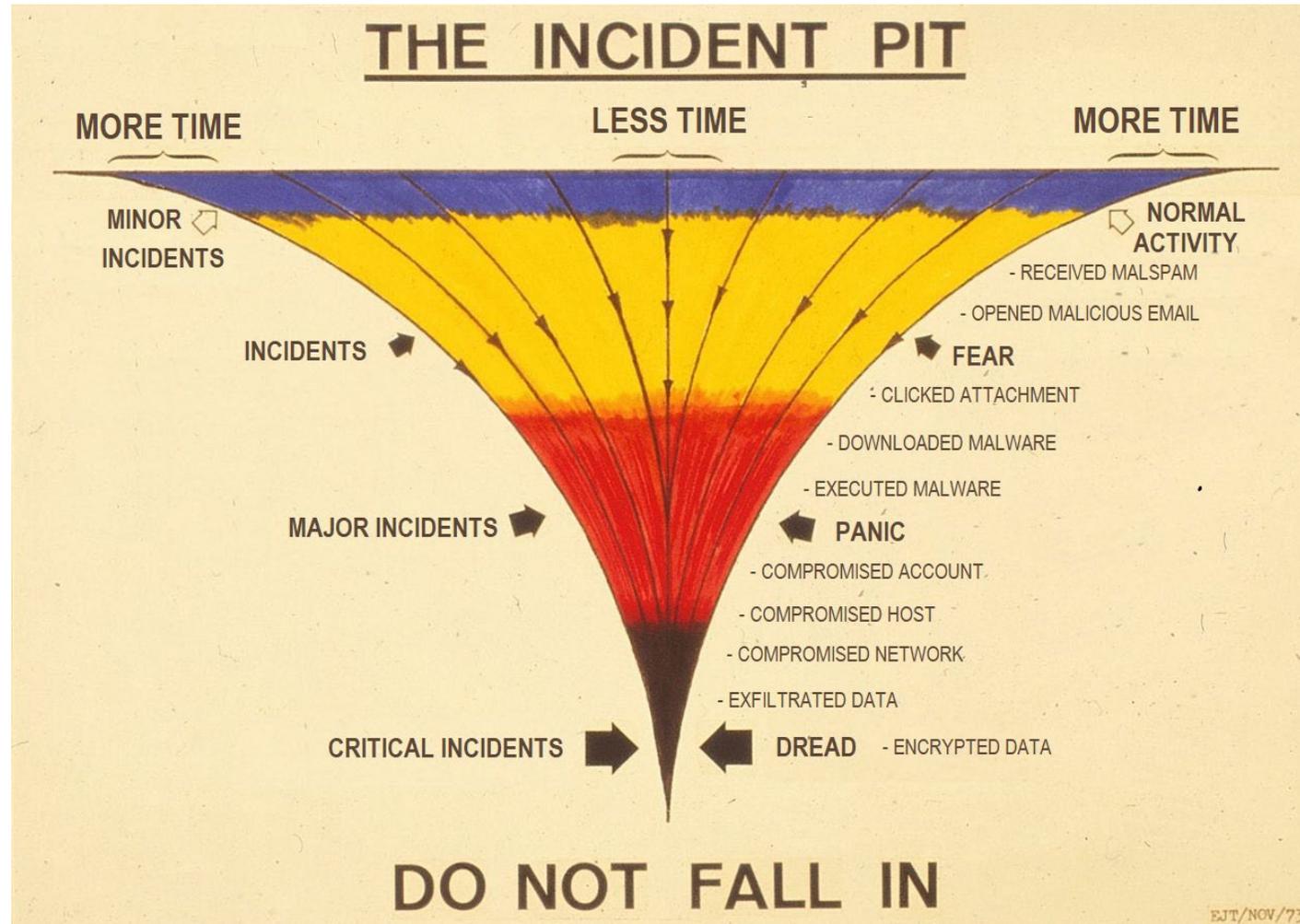
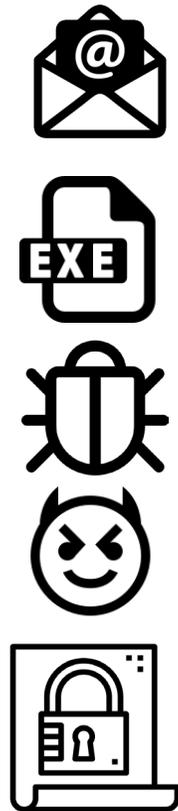
Analysis  
Repositories



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



# Incident Pit – Cybersecurity

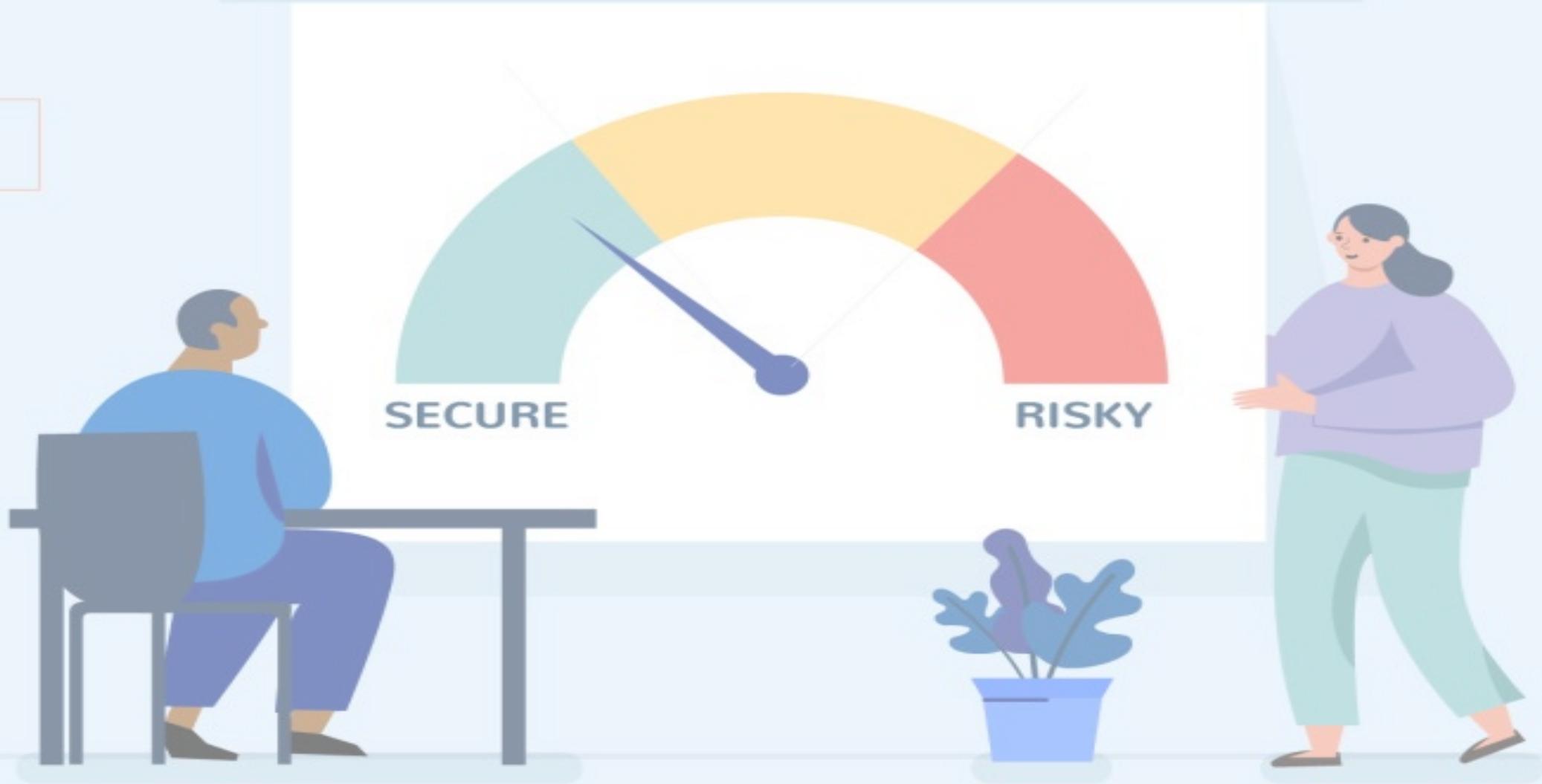


# Take Aways

**DON'T  
PANIC**

- 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 22<sup>nd</sup> 2023