

Defending an Organization

SIO

deti universidade de aveiro
departamento de eletrónica,
telecomunicações e informática

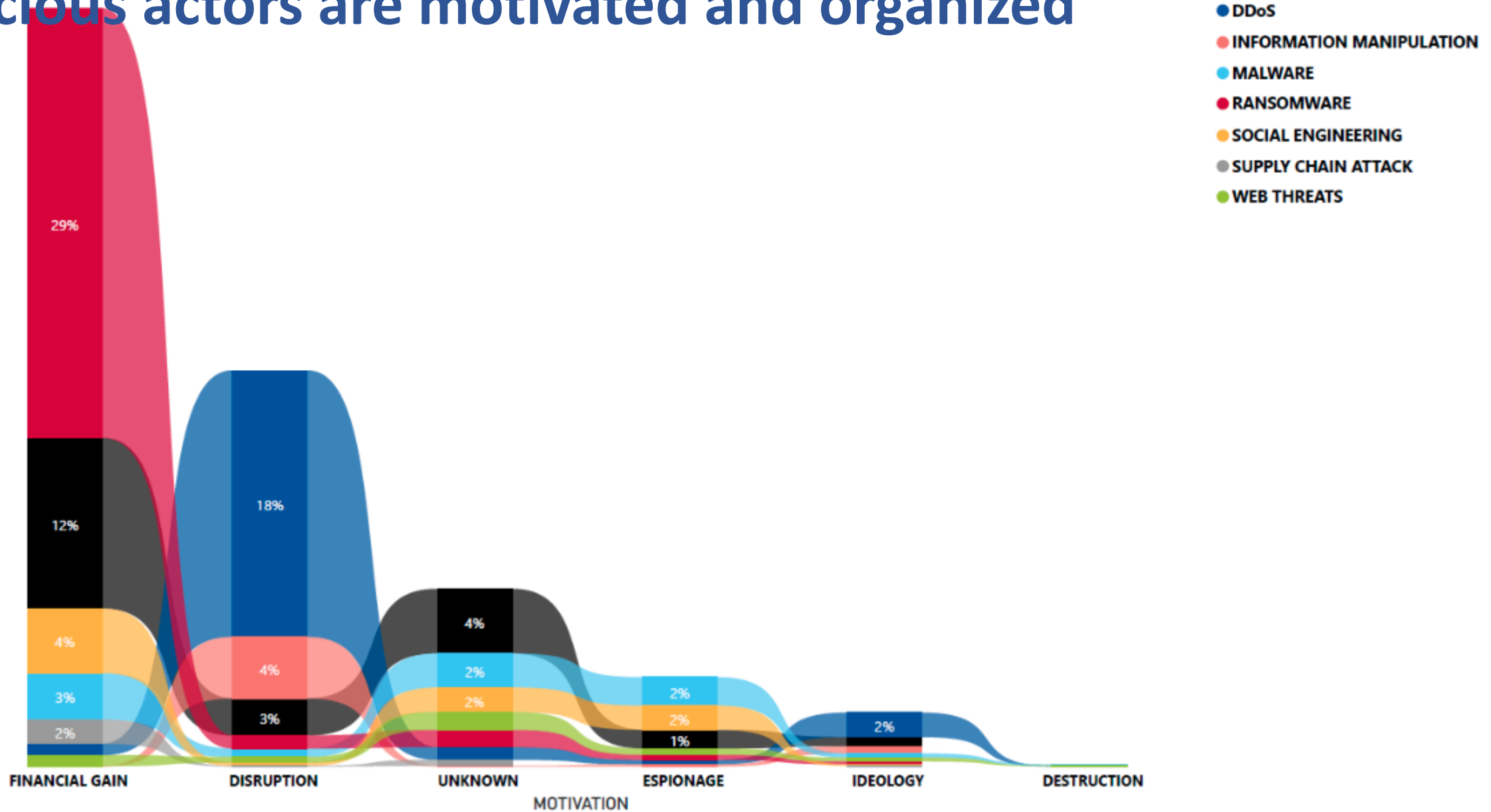
The current organizational landscape

- Organizations are complex and must reach everyone

- **Physical space:** where we live since >10000y BC
 - We know it, it's slow, it involves moving matter around
 - Laws are plentiful and cover most interactions

- **Cyberspace:** to which organizations just tapped into
 - We do not know it, it's fast, there are no barriers
 - Everything can be hidden, laws are limited

Malicious actors are motivated and organized



The current legal landscape

- Must comply with new regulatory frameworks
 - **2016**: NIS – Defines basic cybersecurity requirements
 - **2018**: GDPR – Defines requirements for private data
 - **2018**: RJSC – Legal Framework for the national Cyberspace
 - **2021**: DL65 – Defines processes for inventory, reporting, formalize strategy
 - **2024?**: NIS 2 – Defines cyber teams and processes for critical/essential services
 - **2025**: DORA - Digital Operational Resilience Act – Financial Institutions
- Strategies are based on risk and maturity
 - Risk: identify assets and determine their risk
 - Maturity: determine organization maturity over multiple areas
 - Evolve all as adequate

National Cybersecurity Framework (QNRCS)

Objectives

IDENTIFY



PROTECT



DETECT



RESPOND



RECOVER



<https://www.cncs.gov.pt/pt/quadro-nacional/>

National Cybersecurity Framework (QNRCS)

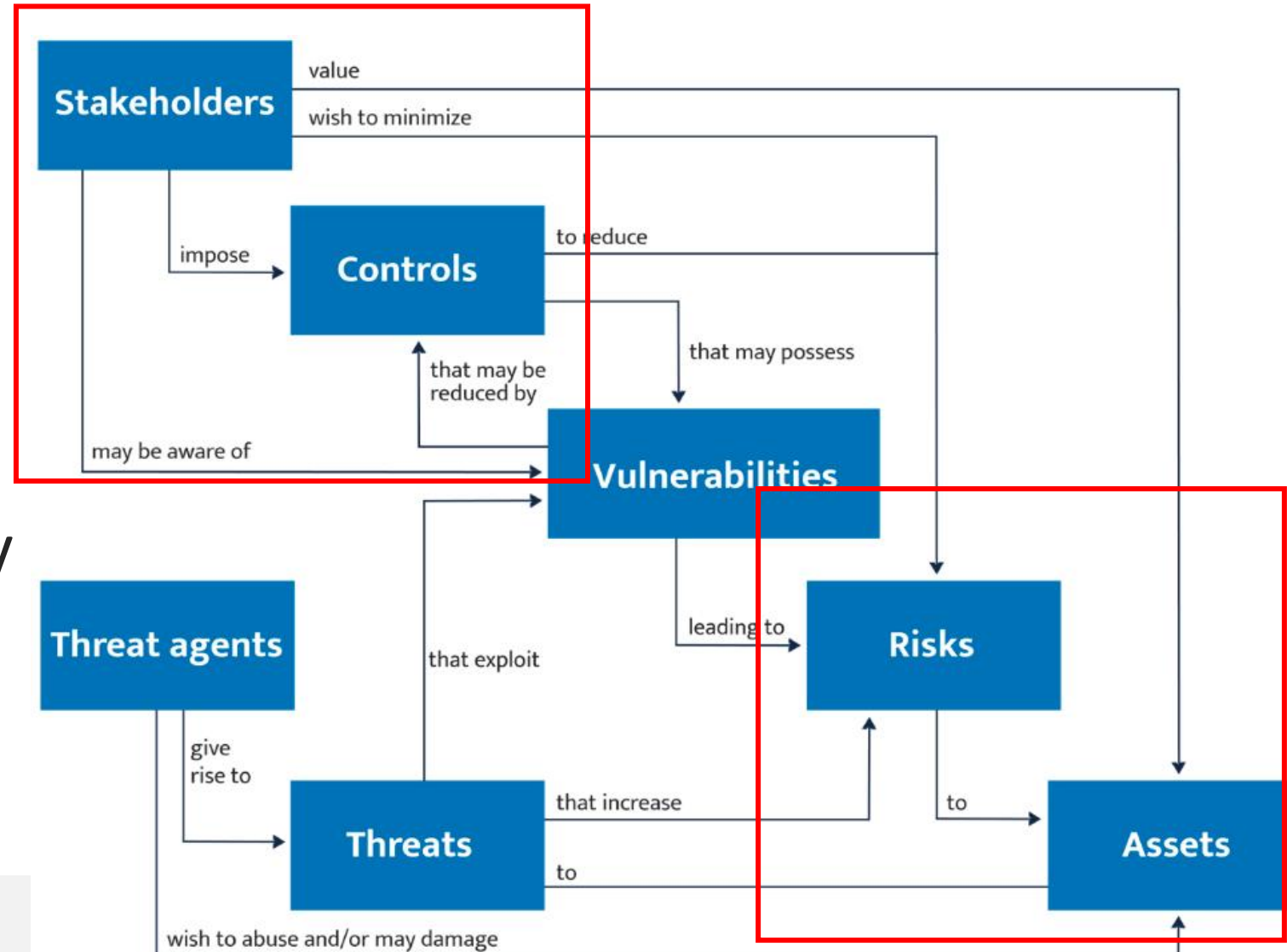
Objectives

- **Identify:** Understanding the organization's context, the assets that support the critical business processes and relevant associated risks.
- **Protect:** Implementation of measures aimed at protecting the business processes and company assets, regardless of their technological nature.
- **Detect:** Definition and implementation of appropriate activities aimed at identifying incidents on time.
- **Respond:** Definition and implementation of appropriate measures in case of incident detection.
- **Recover:** Definition and implementation of activities aimed at managing the recovering plans and actions to restore impaired processes and services...

National Cybersecurity Framework (QNRCS)

ISO/IEC 27032, Basic concepts and high level relationships

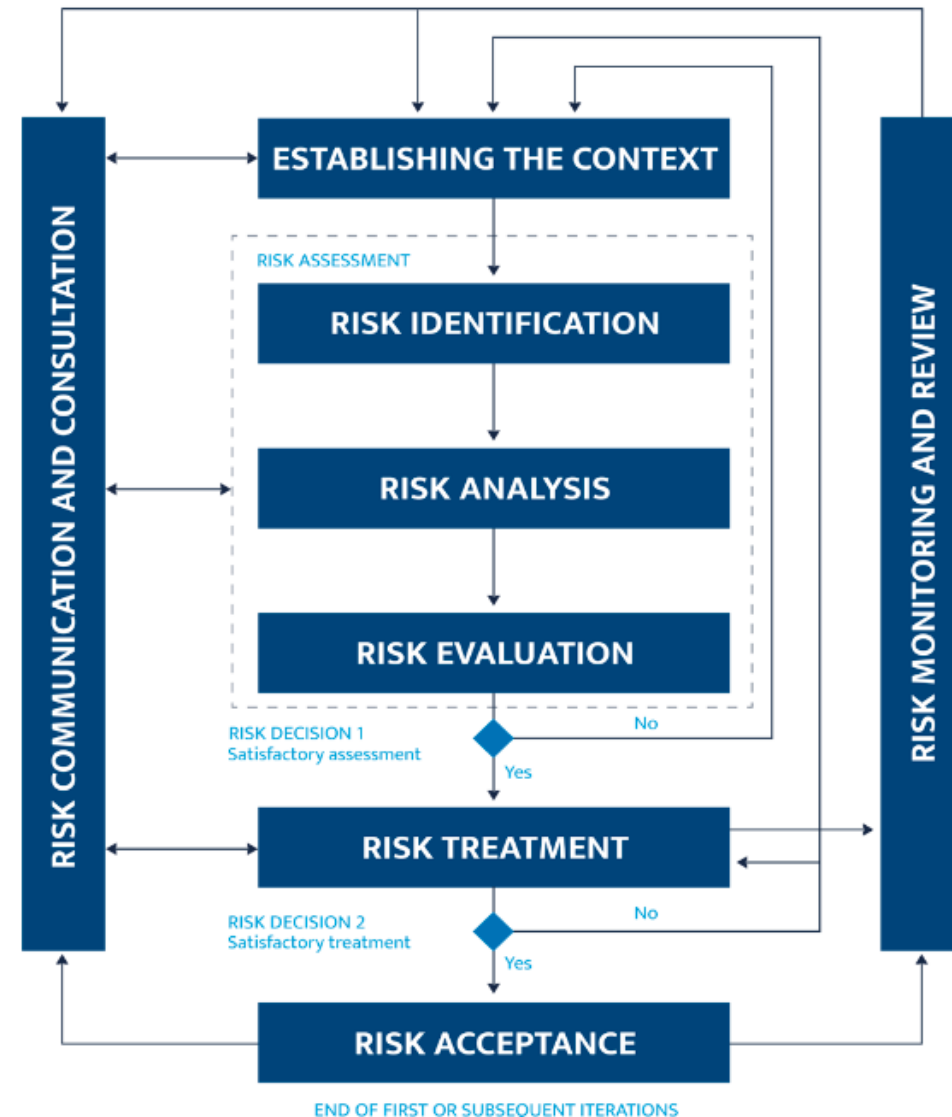
- Risk Based
 - Aims to minimize risk
- Consider Stakeholders
 - Decision Level
- Consider Assets Inventory
 - Services
 - Products



National Cybersecurity Framework (QNRCS)

ISO/IEC 27005, Basic concepts and high level relationships

- Strategy focused on **Risk Management**
- **Risk** used to decide what to address
 - Vulnerabilities to handle
 - Controls do deploy
 - Policies
 - Mechanisms to apply
 - Investment in cybersecurity



Assets: Crown Jewels Approach

- Focused on identifying and protecting the most critical assets
 - To the organization mission!
- What is a crown jewel?
 - Essential Sensitive Data
 - Essential Servers
 - Essential Software Systems
 - Any other asset (HVAC, Generators...)
- Disruption to the crown jewels will pose a serious impact to the organization
- Objective: Protect the crown jewels
 - and grow from there to the rest of the organization
 - based on a risk assessment

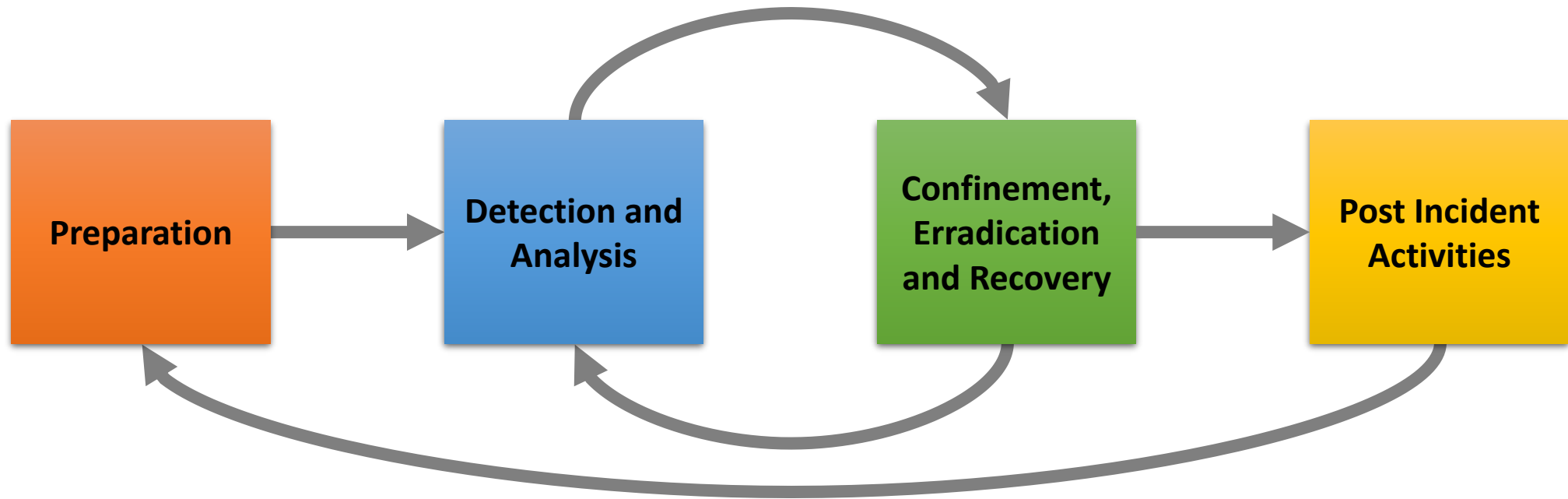


Security Plan

- Live document describing the security posture
 - Allows organizations to know where they are and where they want to go
 - Considers authentication, backups, risk, access control, policies, etc.
- Accepted by the organization, signed by Security Principal
 - Periodically reviewed and improved
- Written and accepted policies implies higher maturity
 - Organizations frequently only have word of mouth or informal frequent practices

Incident Response

Framework NIST SP 800-61r2



NIST SP 800-61r2 – Incident Response Life cycle

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Incident Response

Coordination

- **FIRST: Forum of Incident Response and Security Teams**
 - Global forum of incident response and security teams.
 - Aim to improve cooperation between security teams on handling major cybersecurity incidents.
 - FIRST is an association of incident response teams with **global coverage**.
- **ENISA: European Union Agency for Cybersecurity**
 - Contributes to EU cyber policy, improving trust and resilience
- **CERT: Computer Emergency Response Team**
 - One per country, coordinating



Incident Response

Coordination

- **CERT: Computer Emergency Response Team**
 - One per country, coordinating all significant events
 - Helps companies identifying, preparing and recovering from attacks
- **CSIRT: Computer Security Incident Response Team**
 - One per relevant organization, coordinating the response in coordination with the CERT
 - <https://www.cncs.gov.pt/pt/certpt/>
- **CSIRT Networks: Groups of CSIRTs to facilitate joint actions**
 - E.g. training, taxonomy, Threat information exchange
 - <https://www.redecsirt.pt/>



Incident Response

Coordination

- **Support Activities**

- Networks, projects
- E.g. <https://www.ccc-centro.pt> (Competence Center)
- Increase the security posture and resilience of organizations
 - Training and awareness
 - Exchange strategies, information, and tools
 - Incident Response
 - Funding

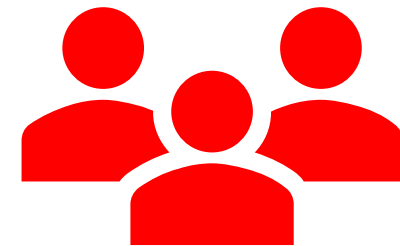
- **Police Authorities**

- Polícia Judiciária
- Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T): unc3t@pj.pt



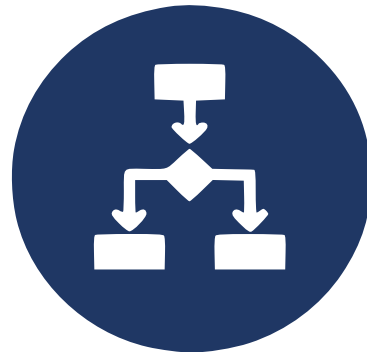
Security Teaming

- Security operations are frequently organized in teams
 - Blue Team: Defends an organization from malicious actors
 - Red Team: Attacks an organization to help finding weak spots
 - Purple Team: Mixed attack defense role
- Each team uses specific tools and methods



Blue Teams

- Defend organizations from malicious actors
 - Abusing and Careless actors, and general failures also
- Typical fundamental tasks to address:
 - People: training, awareness, culture
 - Processes: analysis, investigation, data, reporting
 - Technology: monitoring, detection, scripting, automation



Blue Teams

- **Mandatory** for all organizations!
 - Good amount of job opportunities
 - extreme shortage of professionals
- **Very demanding due to high asymmetry**
 - Attackers must succeed once, using their preferred TTPs
 - Defenders must defend continuously, from all attacks
 - To the entire organization attack surface, using any TTP
- **Challenging and interesting**
 - Many topics to address: prog, forensics, AI/ML, training...
 - Continuously evolving with new techniques and tools

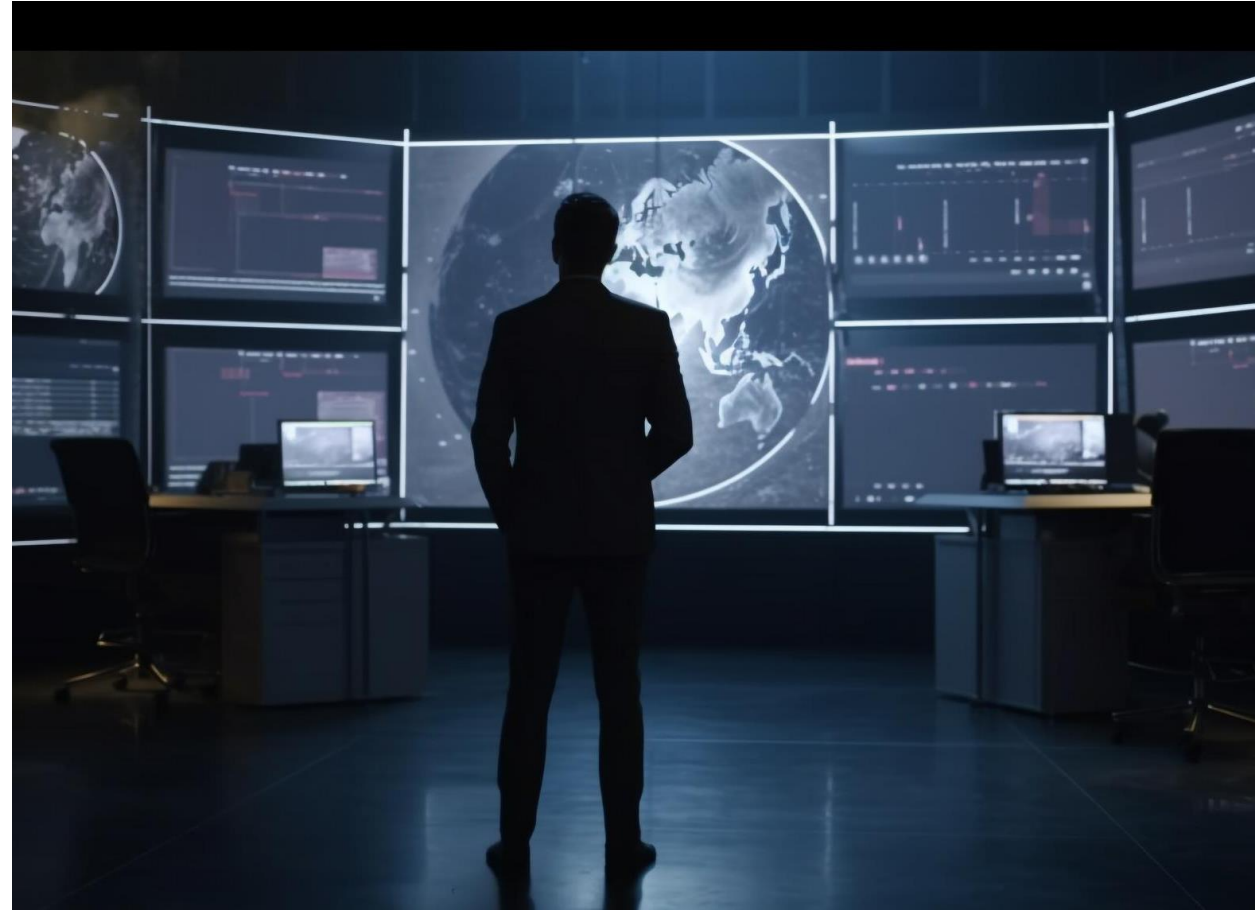
Blue Team Defence Techniques

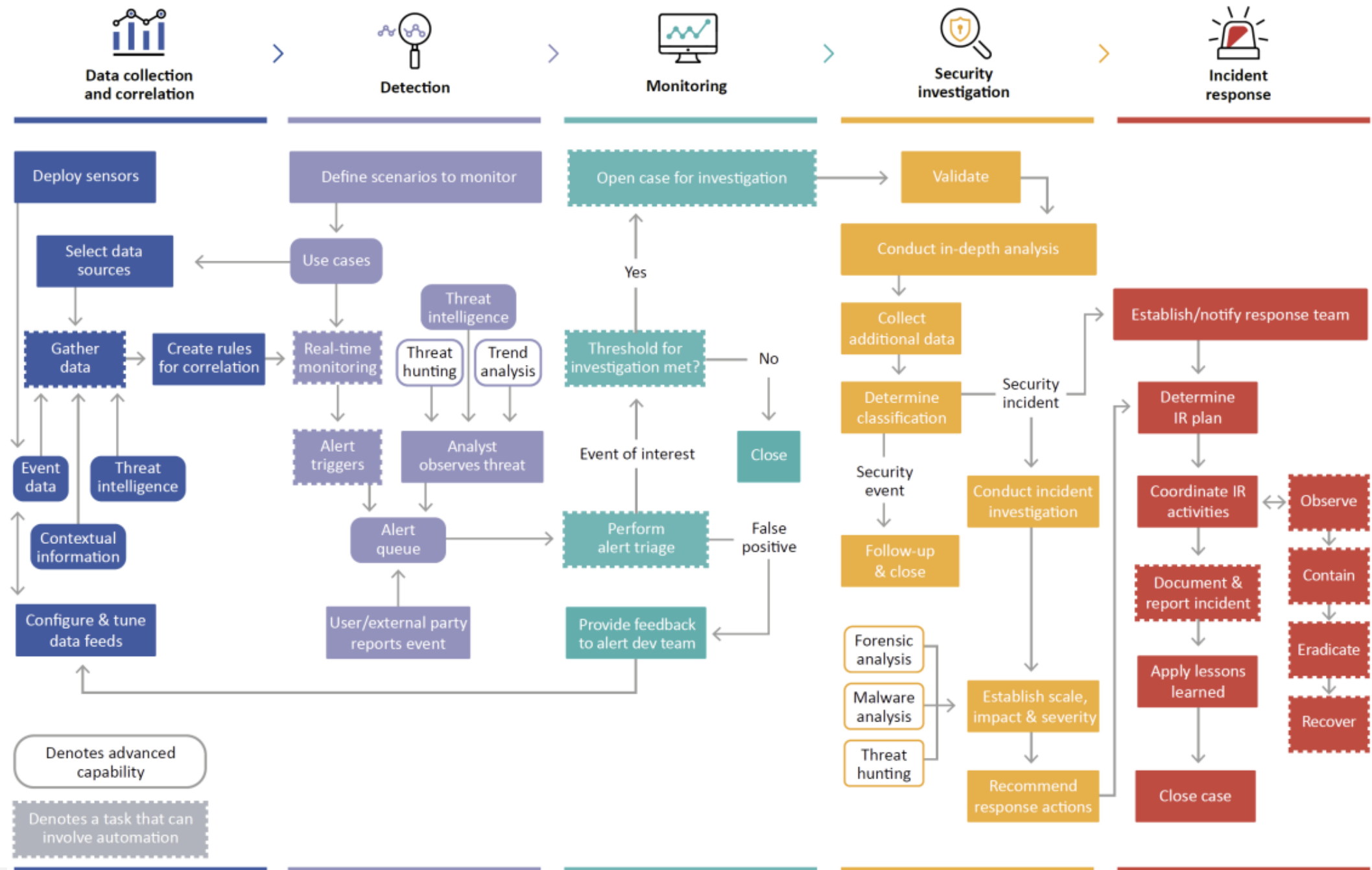
- Everything Everywhere All at Once?
 - No! Prioritize according to the organization mission
- Current approaches focus on:
 - the CIA triad
 - Risk assessment
 - the crown jewels
 - with the least pain
 - security plan



SOC – Security Operations Center

- Responsible for continuously monitoring
 - Organization's digital infrastructure
- Monitor, detect and respond
 - To cybersecurity threats
- Empowered with skilled analysts and technology
 - Security assessments
 - Data protection
 - Incident response

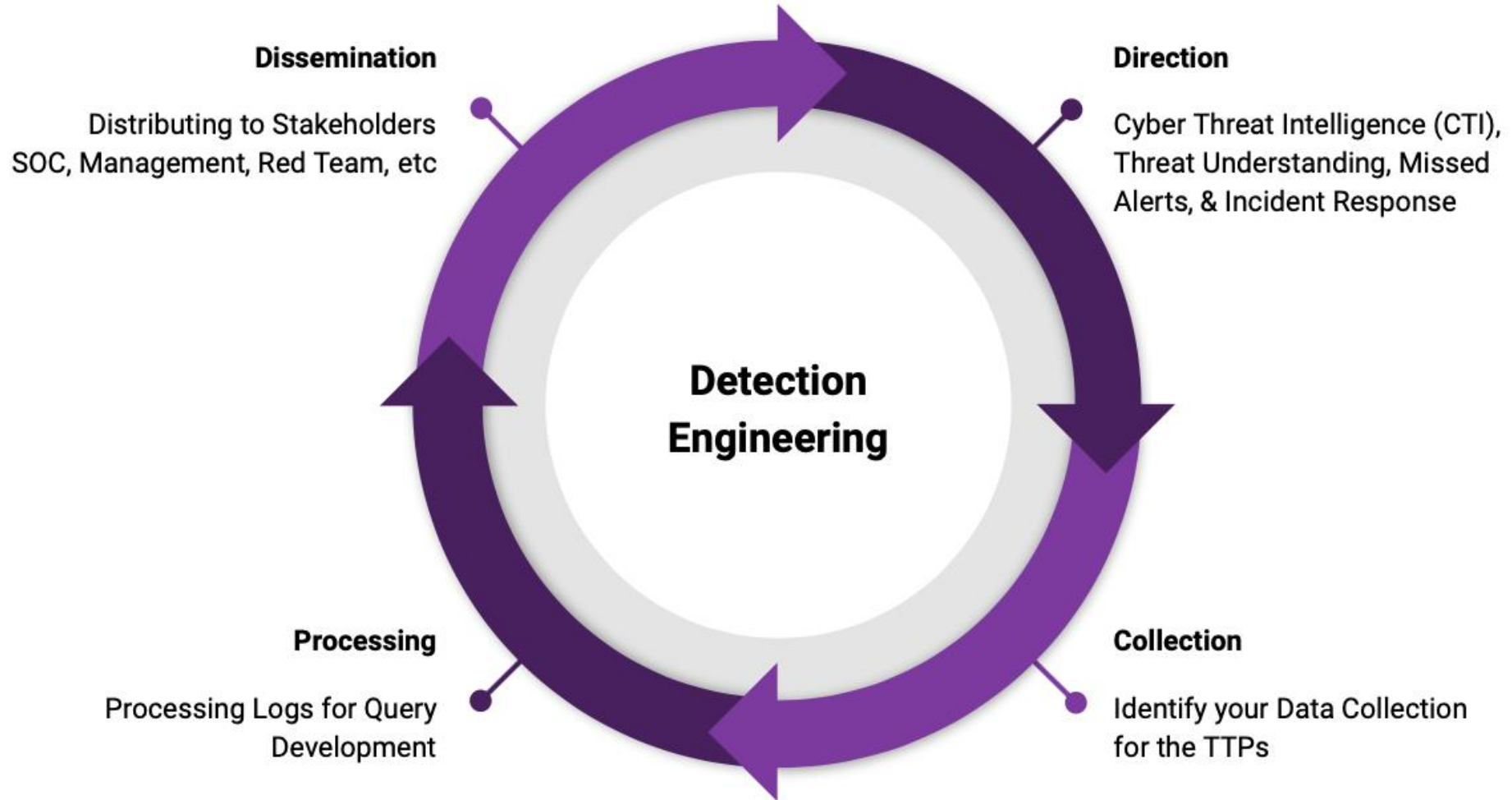




Main concepts

- **Defensive Security (Engineering)**
 - Firewalls, backups, logs
 - Secure Software Development Lifecycle
 - Security related requirements (e.g., OWASP ASVS)
 - Training and Awareness
- **Incident Response**
 - Have processes and procedures to handle incidents
 - Involve stakeholders (Decision maker, Clients, Lawyers) and communicate (Public Relations)
- **Detection Engineering**
 - designing, developing, testing, and maintaining threat detection logic

Detection Engineering



Source: SANS

Direction: CTI

Assess the current threats from Cyber Threat Intelligence

- Cyber Threat Intelligence helps understanding the dynamics
 - The “Dark web”: Tor forums, discords, telegrams, IRC, twitter, pastebins
 - Official reports: Security Researchers (Reversing, analysis)
 - How actors position themselves (hacktivists, crime)
 - How attacks to similar organizations are conducted

Thailand's Insurance 3.7 Million Customer Personal Info For Sale
by desorden - Friday August 12, 2022 at 10:57 AM

desorden
Premium Data Hacker

Company: Srikrungbroker Company Limited
Country: Thailand
Description: Over 3.28 million customer records and 462,980 insurance agent records for Srikrungbroker Company Limited (www.srikrungbroker.co.th) in Thailand. For more information, see the thread at <https://breached.to/Thread-Srikrungbroker...y-DESORDEN>
Total Size: 4.8 GB | Total Datasets: 2 | Date of Breach: 27 July 2022 | Origin: Thailand
Data Type: Insurance Customer and Agent Details
Data Industry: Insurance / Finance
Data Geographic: Thailand
Data Format: .csv
Payment Methods: Preferred Monero. Bitcoin or USDT +5% Fee

Details of Datasets (3.7 million records):
1) Customer: 3.28 million records (Columns include Customer ID, full name, address, phone number, email, etc)
2) Agent: 462,980 records (Columns include Agent ID, full name, ID card number, phone number, email, etc)

LockBit BLOG

LEAKED DATA

UNTIL FILES 21H51M14S PUBLICATION

Deadline: 19 Aug, 2022 20:33:13 UTC

Entrust Datacard
entrust.com
OUR STORY BEGAN IN 1969, with the founding of Datacard Corporation and the advent of secure, high-speed payment and identity card printers.
ALL AVAILABLE DATA WILL BE PUBLISHED !

Home Page of Ragnar_Locker Leaks site

RAGNAR_LOCKER

WALL OF SHAME

ent list of companies who would like to keep in secret the info themselves and their customers, partners to even greater risk than a



Home Notify me Domain search Who's been pwned Passwords API About Donate

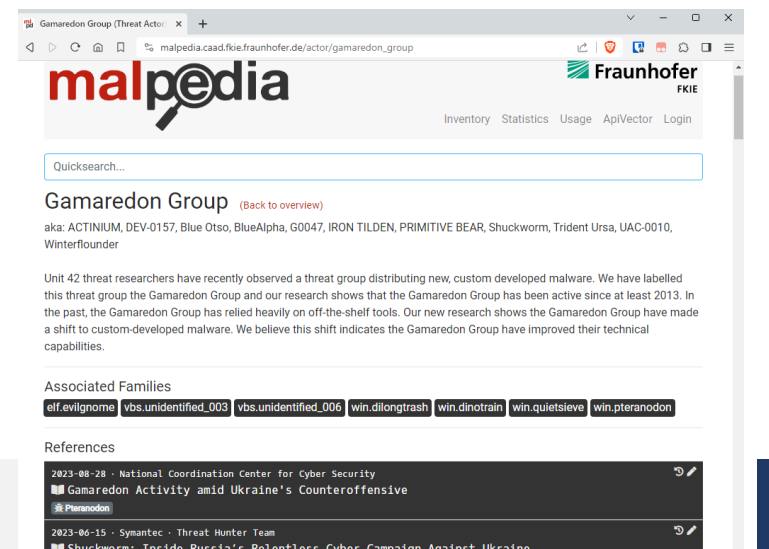
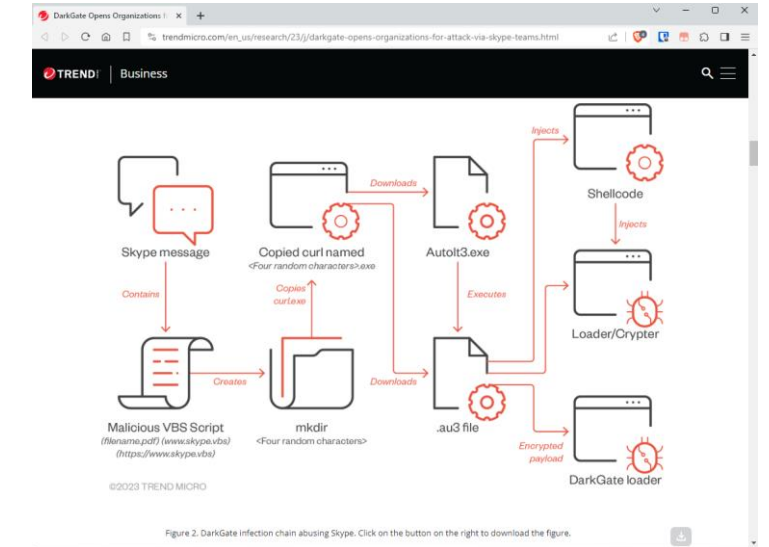
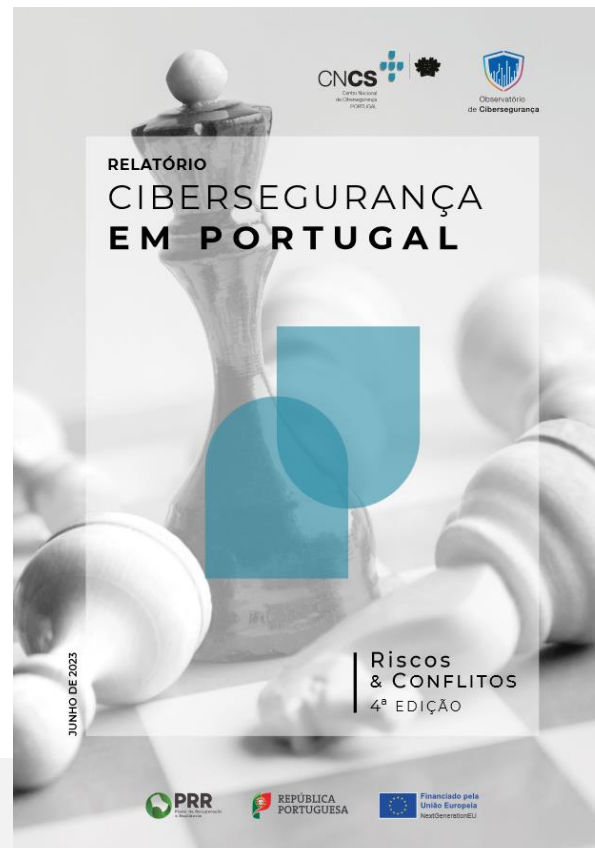
!;--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) **pwned?**

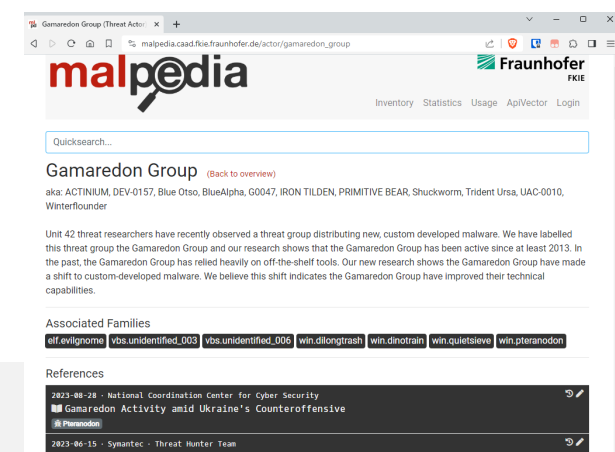
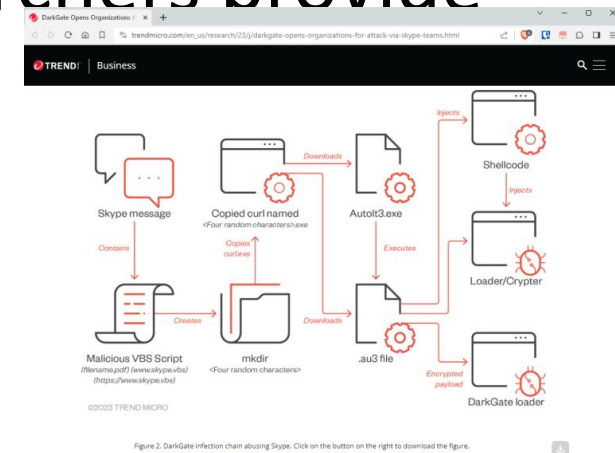
Direction: CTI

- Threat Intelligence provide analysis and forecasts
 - Official entities, private orgs
 - Police Authorities
 - Government Ministries



Assess the current threats from CTI

- Threat Intelligence from researchers provide analysis and forecasts
 - Official entities, private orgs



Direction: Alerts and Incidents

- Current alerts will tailor future rules
 - Identify popular threat actions
 - Reduce false positives
 - Keep the capability to detect new threats
 - Includes conducting controlled attacks to validate rules

- Incident resolution impact resolution playbooks
 - One a threat is found, what can the organization do?
 - Deficiencies in incident response define future improvements
 - Includes simulated incidents to test processes

Collection: Data Harvesting

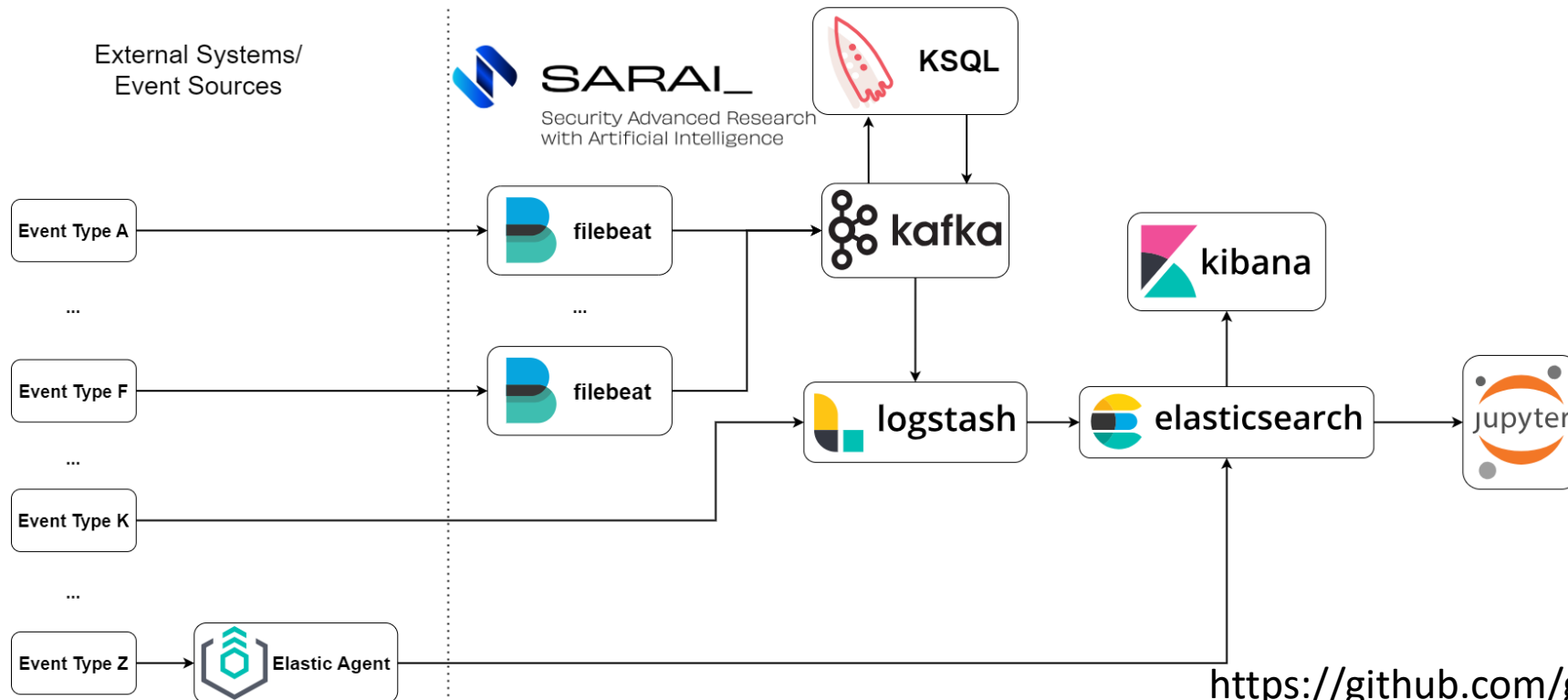
Engineer Data Collection

- Focus on relevant data sources to address threats
 - Cannot get all data
 - Visibility will be limited
- Potential targets
 - Servers: AD, email, HTTP, Databases
 - Wireless Controllers
 - VPN access
 - Firewalls
 - Endpoints: Laptops, VMs, IoT devices

Collection: Data Harvesting

Engineer Data Collection

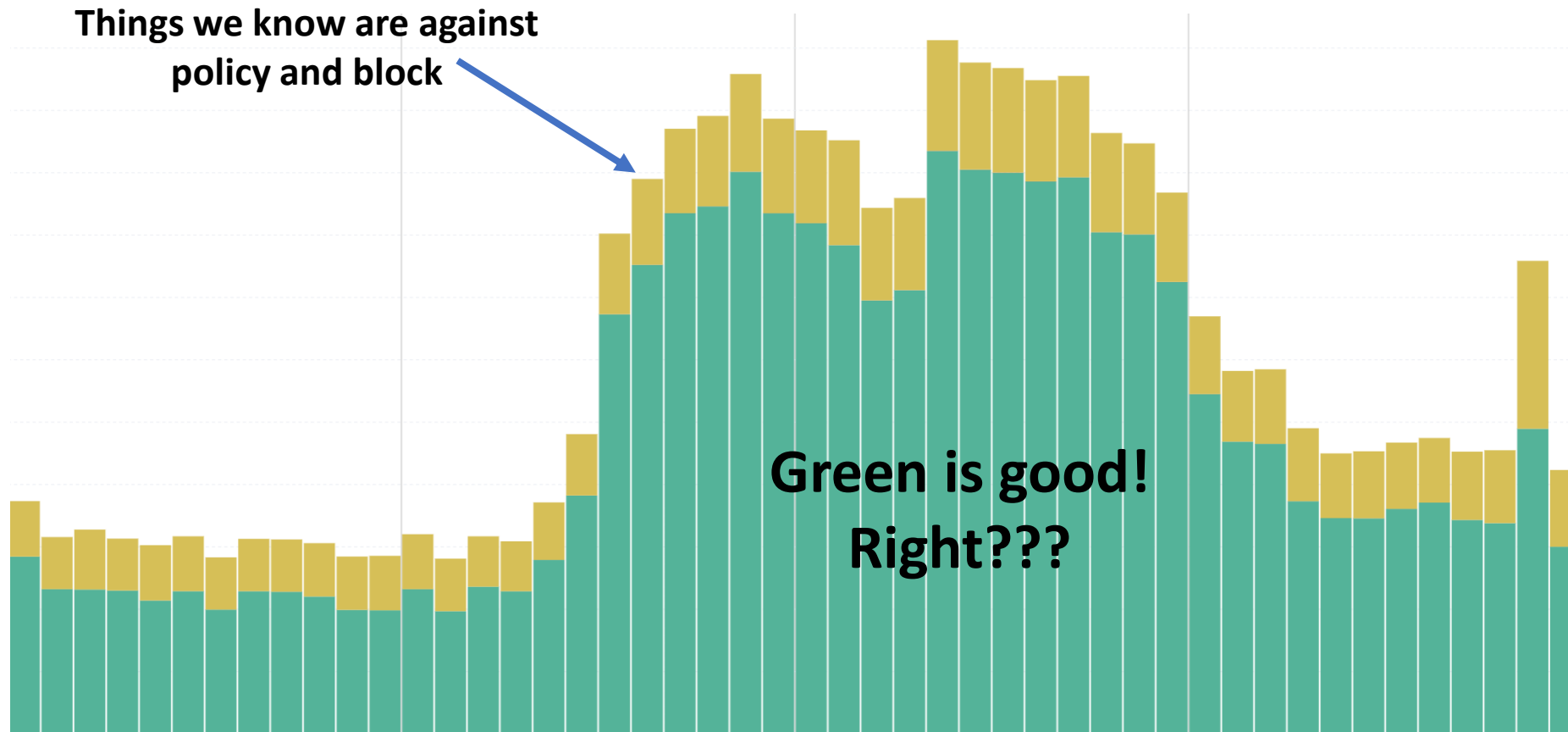
- Current approaches focus on a large data lake
 - Algorithms match rules, ML models, signatures, behavior



Collection: Data Harvesting

Processing: Pain?

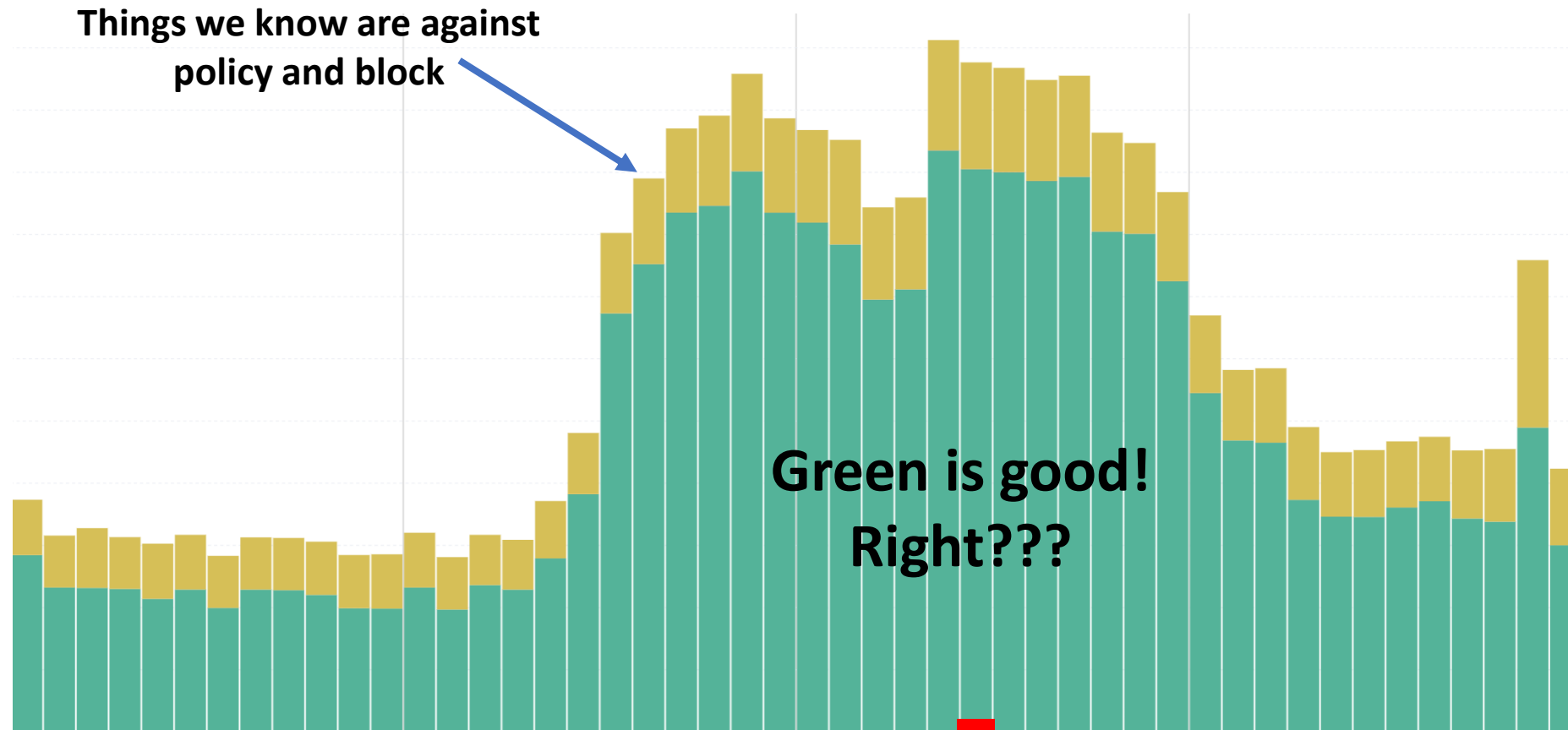
Millions of events/hour



Collection: Data Harvesting

Processing: Pain?

Millions of events/hour

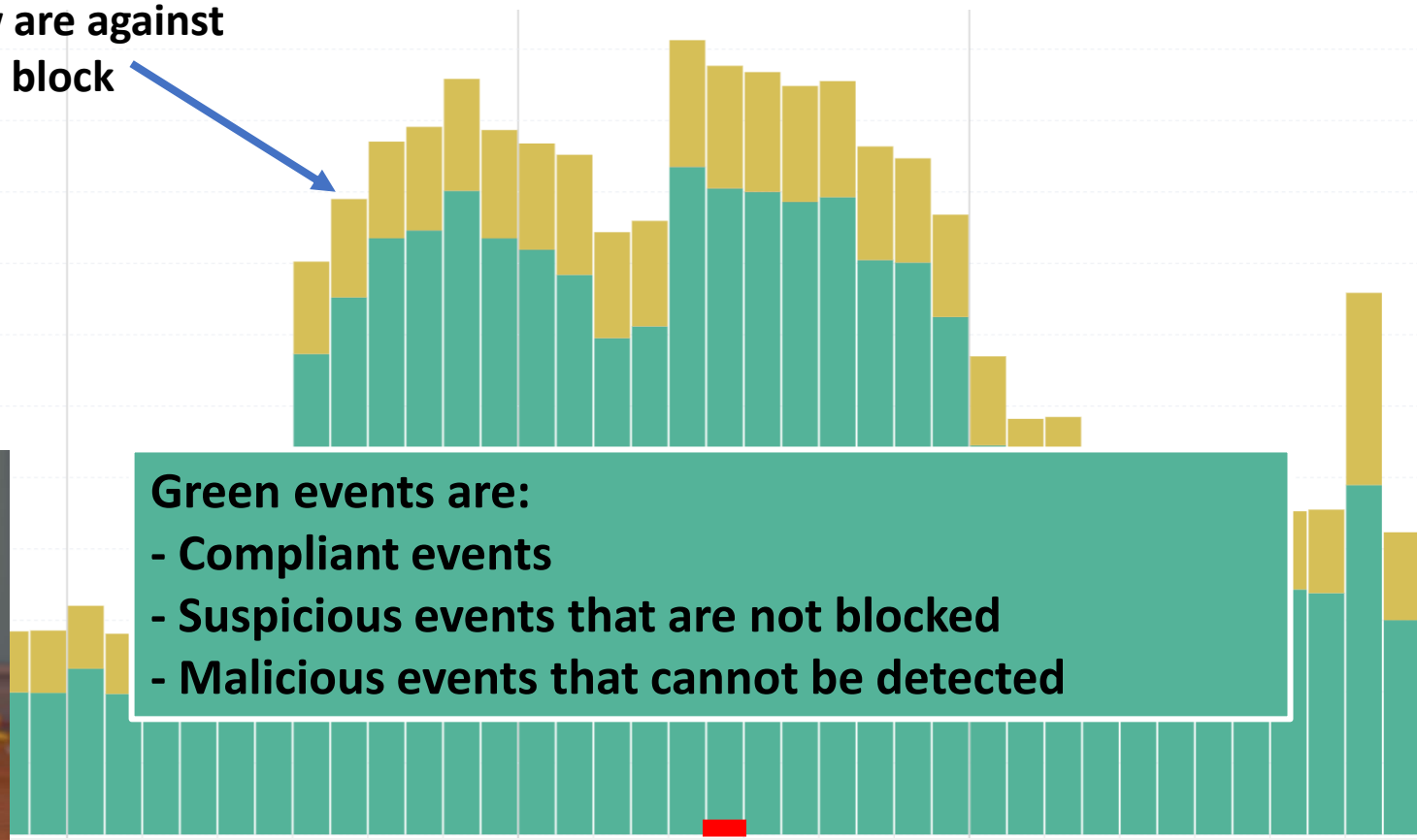
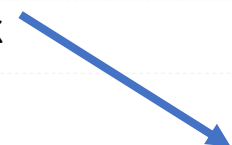


Collection: Data Harvesting

Processing: Pain?

Millions of events/hour

Things we know are against policy and block



SO MANY FLOWS

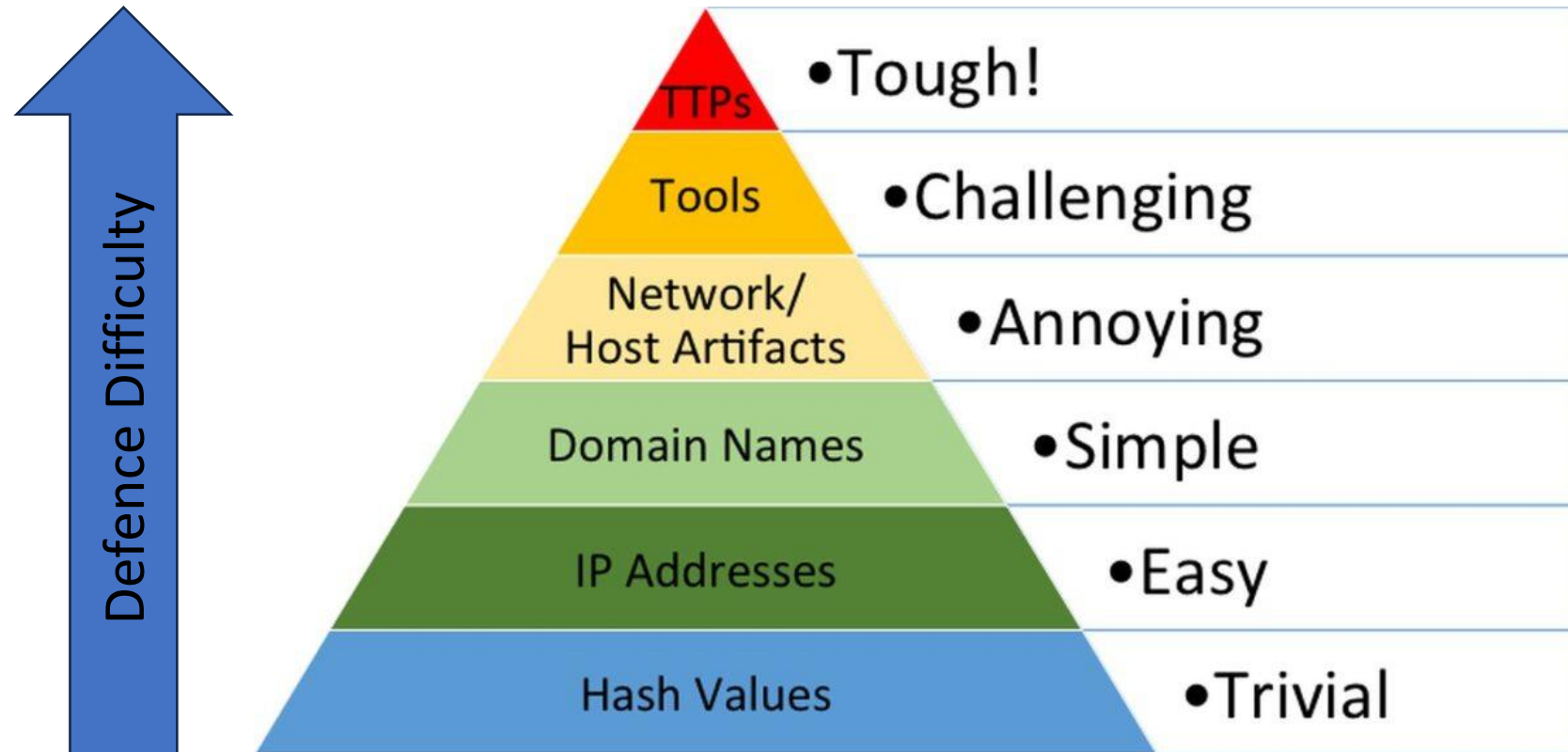


Green events are:

- Compliant events
- Suspicious events that are not blocked
- Malicious events that cannot be detected

Thousands of malicious agents (detect or block)

The Pyramid of Pain



- Increase defence capabilities **from the bottom to the top**
- Why?
 - Detecting URLs/files/emails by comparing hashes is trivial
 - Understanding how actors behave is very very difficult

Triage

Or how to select relevant events?

- Could be one of several definitions
 - Attack near completion
 - Targeting / affecting high-value items
 - Critical hosts, business processes, users, data
 - Advanced targeted attackers or simple attacks
 - Unique, never fired before or lowest count
- Will depend on the organization



Definition of Dangerous

- Could be one of several definitions
 - Attack near completion
 - Targeting / affecting high-value items
 - Critical hosts, business processes, users, data
 - Advanced targeted attackers
 - Unique, never fired before or lowest count
- Will depend on the organization
- Anything that will cause relevant damage
 - It has a high cost to recover from
 - Or it is difficult to remedy



(Fantastic) Threats and Where to Find Them?

- Behavior matching: mostly ML
 - Known patterns
 - Anomaly detection
- Signature matching: **YARA**
 - Signatures for malware are created and disseminated
- Reputation evaluation: **IP addresses /domains**
 - Low reputation addresses may generate alert or block
- Known threats are identified by vendor software
 - Challenge: **Unknown**/Tailored threats

(Fantastic) Threats and Where to Find Them?

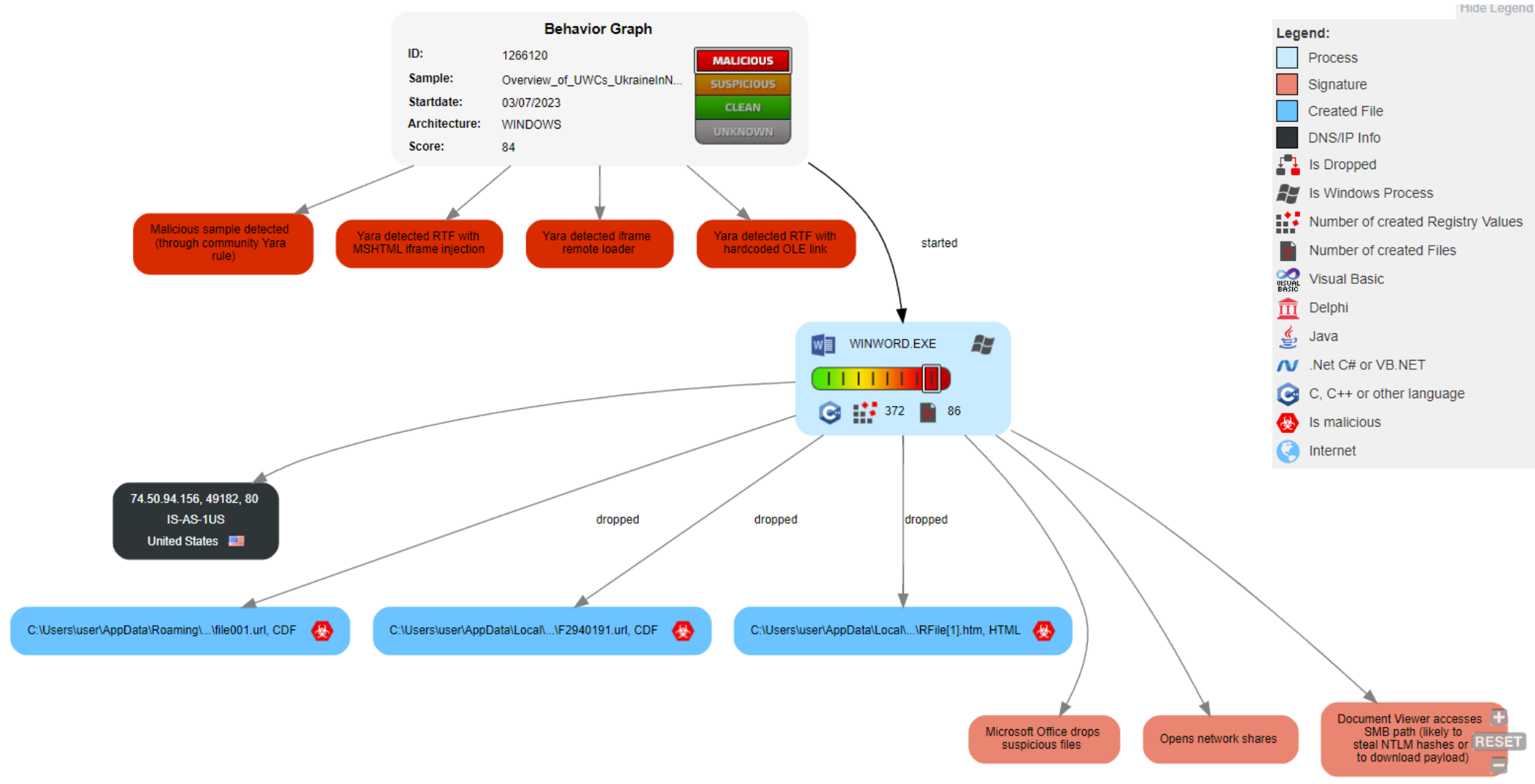
- What if we do not know if something is malicious?
 - What is a malicious website or file?
 - Most dangerous threats are not classified as Malware.
- New malware potentially has high impact
 - It is not detected by Anti-virus
 - Explores unpatched vulnerabilities or flaws (0 day)
- A new malicious asset is just a **new program/website**
 - May be a variation of an existing malware
 - Different language/obfuscated/encrypted/packed
 - May simply bypass existing signatures
 - There is a robust market selling malware

Threat Research

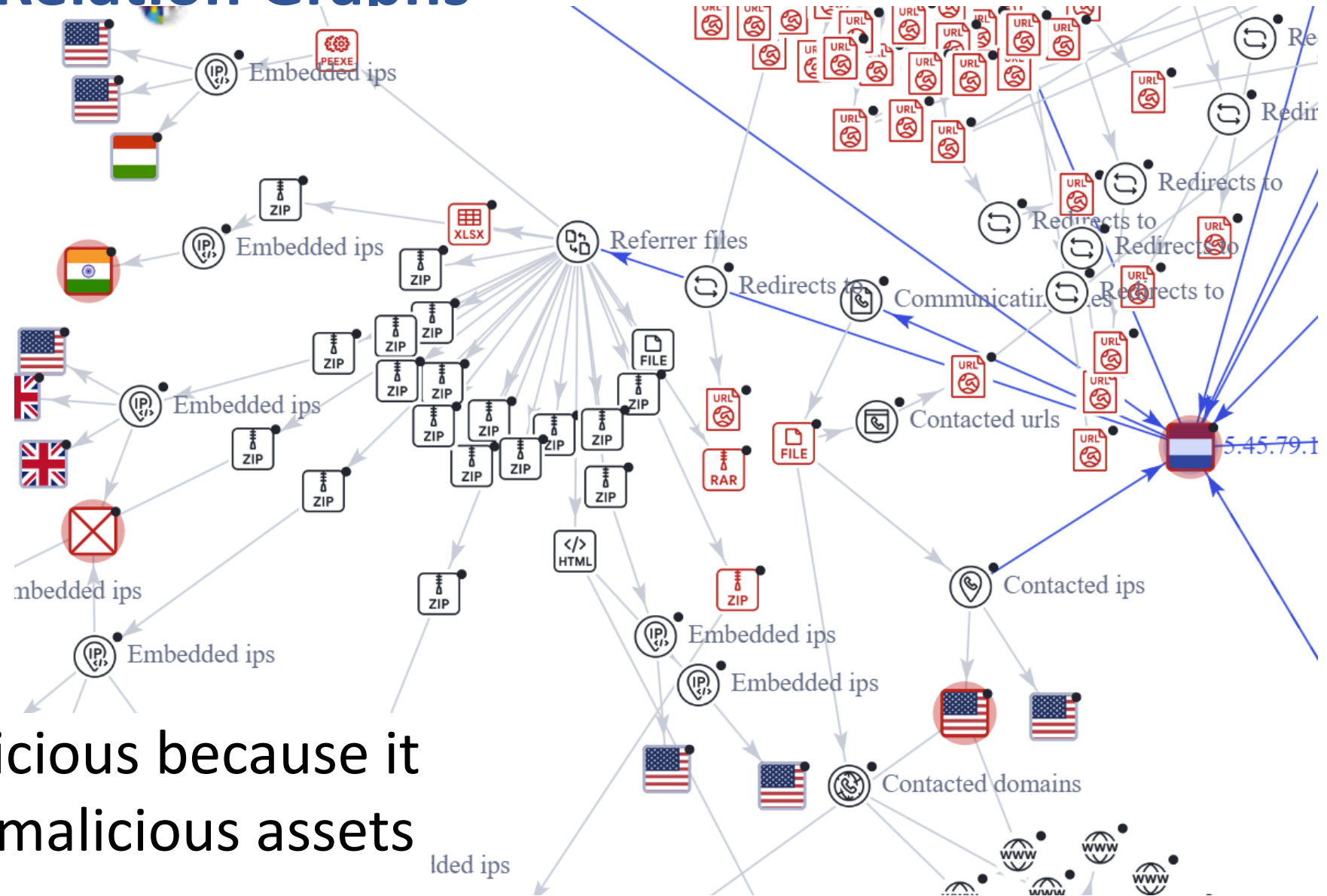
- Threat Research allows detection of **new offenses**
 - Takes a Indicators and determines its behavior

- Includes several knowledge areas
 - Open Source Intelligence
 - Social Networks, DNS/TLS Records, Dark Web
 - Reverse Engineering
 - Networking concepts
 - Network traffic analysis
 - Cryptography
 - Machine Learning

Threat Research: Execution Graphs



Threat Research: Relation Graphs



- Some become suspicious because it contacts/has other malicious assets

MITRE Att&ck Matrix

- A globally-accessible knowledge base of adversary tactics and techniques
 - based on real-world observations.

- Allows organizations to map actions to a kill chain
 - Also facilitates tracking the Actor or how it evolves
 - Actors will reuse tools, tactics and techniques

MITRE Att&ck Matrix

Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques
Drive-by Compromise	AppleScript	Account Manipulation (0/2)	Bypass User Access Control	Bypass User Access Control
Exploit Public-Facing Application	JavaScript/JScript	BITS Jobs	Elevated Execution with Prompt	Elevated Execution with Prompt
External Remote Services	PowerShell	Boot or Logon Autostart Execution (2/11)	Setuid and Setgid	Setuid and Setgid
Hardware Additions	Python	Authentication Package	Sudo and Sudo Caching	Sudo and Sudo Caching
Phishing (3/3)	Unix Shell	Kernel Modules and Extensions	Authentication Package	Access Token Manipulation (0/5)
Spearphishing Attachment	Visual Basic	LSASS Driver	Kernel Modules and Extensions	BITS Jobs
Spearphishing Link	Windows Command Shell	Plist Modification	LSASS Driver	Deobfuscate/Decode Files or Information
Spearphishing via Service	Exploitation for Client Execution	Port Monitors	Plist Modification	Direct Volume Access
Replication Through Removable Media	Inter-Process Communication (0/2)	Re-opened Applications	Port Monitors	Execution Guardrails (0/1)
Supply Chain Compromise (0/3)	Native API	Registry Run Keys / Startup Folder	Re-opened Applications	Exploitation for Defense Evasion
Trusted Relationship	Scheduled Task/Job (1/5)	Security Support Provider	Registry Run Keys / Startup Folder	File and Directory Permissions Modification (0/2)
Valid Accounts (0/3)	At (Linux)	Shortcut Modification	Security Support Provider	Group Policy Modification
	At (Windows)	Time Providers	Time Providers	Hide Artifacts (0/6)
	Cron	Winlogon Helper DLL	Winlogon Helper DLL	Hijack Execution Flow (0/11)
	Launchd	Browser Extensions	Boot or Logon Autostart Execution (2/11)	Impair Defenses (0/5)
	Scheduled Task	Compromise Client Software Binary	Boot or Logon Initialization Scripts (0/5)	Clear Command Line
	Shared Modules	Create Account (0/2)	Create or Modify System Process (0/4)	Clear Linux or Mac System Files
	Software Deployment Tools	Create or Modify System Process (0/4)	Event Triggered Execution (2/15)	Clear Windows Event Logs
	System Services (1/2)	Event Triggered Execution (2/15)	.bash_profile and .bashrc	File Deletion
	User Execution (1/2)	Event Triggered Execution (2/15)	Accessibility Features	Network Share Content Removal
	Windows Management Instrumentation	Event Triggered Execution (2/15)	AppCert DLLs	Timestomp
		Event Triggered Execution (2/15)	Appninit DLLs	Invalid Code Signing
		Event Triggered Execution (2/15)	Application Shimming	Masquerade Task
		Event Triggered Execution (2/15)	Change Default File Association	Match Legitimate Processes
		Event Triggered Execution (2/15)	Component Object Model Hijacking	Rename System Files
		Event Triggered Execution (2/15)	Component Object Model Hijacking	Right-to-Left Override
		Event Triggered Execution (2/15)	Emond	Space after Filenames
		Event Triggered Execution (2/15)	Image File Execution Options Injection	
		Event Triggered Execution (2/15)	LC_LOAD_DYLIB Addition	
		Event Triggered Execution (2/15)	Netsh Helper DLL	
		Event Triggered Execution (2/15)	PowerShell Profile	
		Event Triggered Execution (2/15)	Screensaver	
		Event Triggered Execution (2/15)	Trap	
		Event Triggered Execution (2/15)	Windows Management Instrumentation Event Subscription	