# Defending an Organization

SIO

deti universidade de aveiro
departamento de eletrónica, telecomunicações e informática

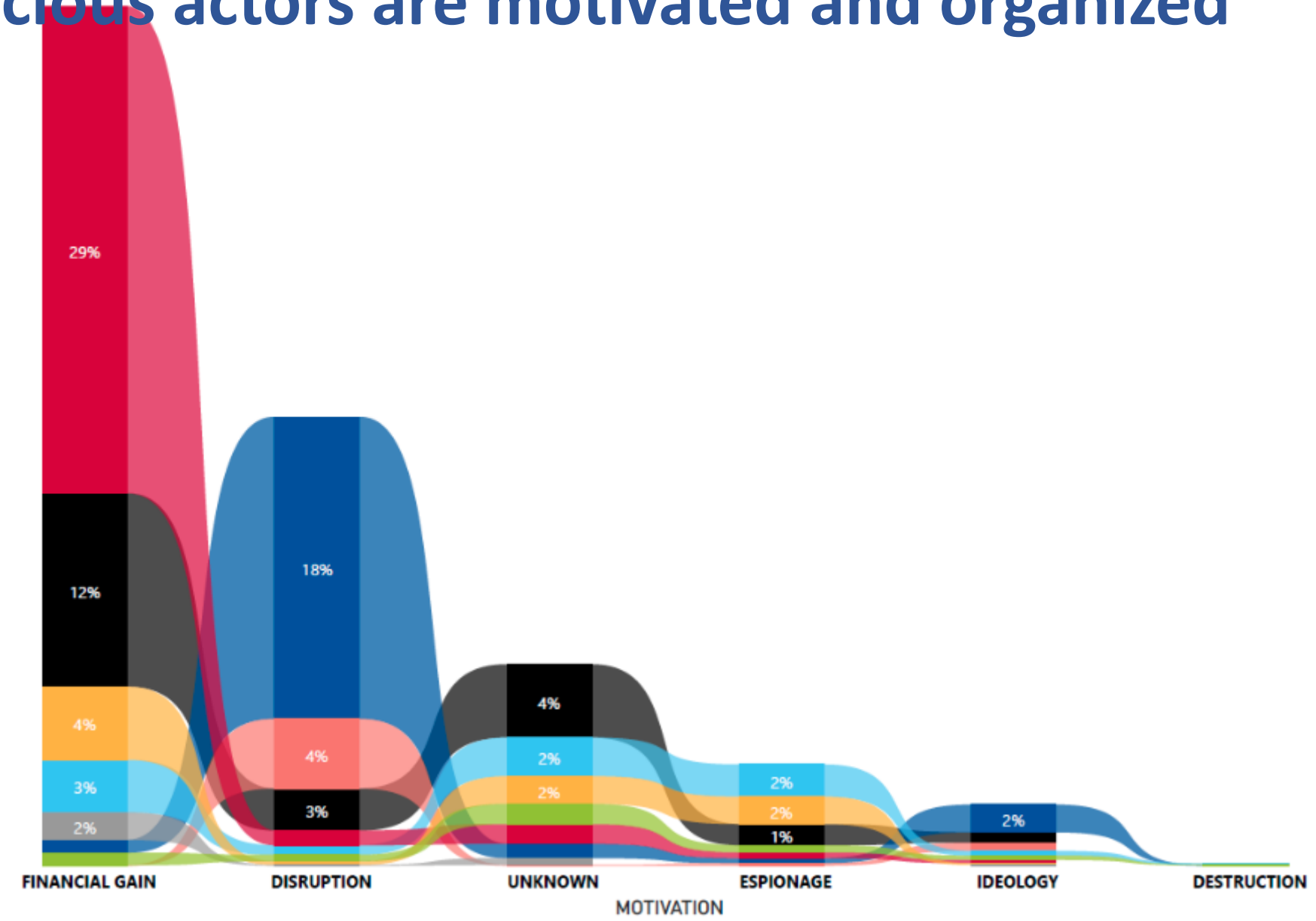
# The current organizational landscape

- 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


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

# National Cybersecurity Framework (QNRCS)

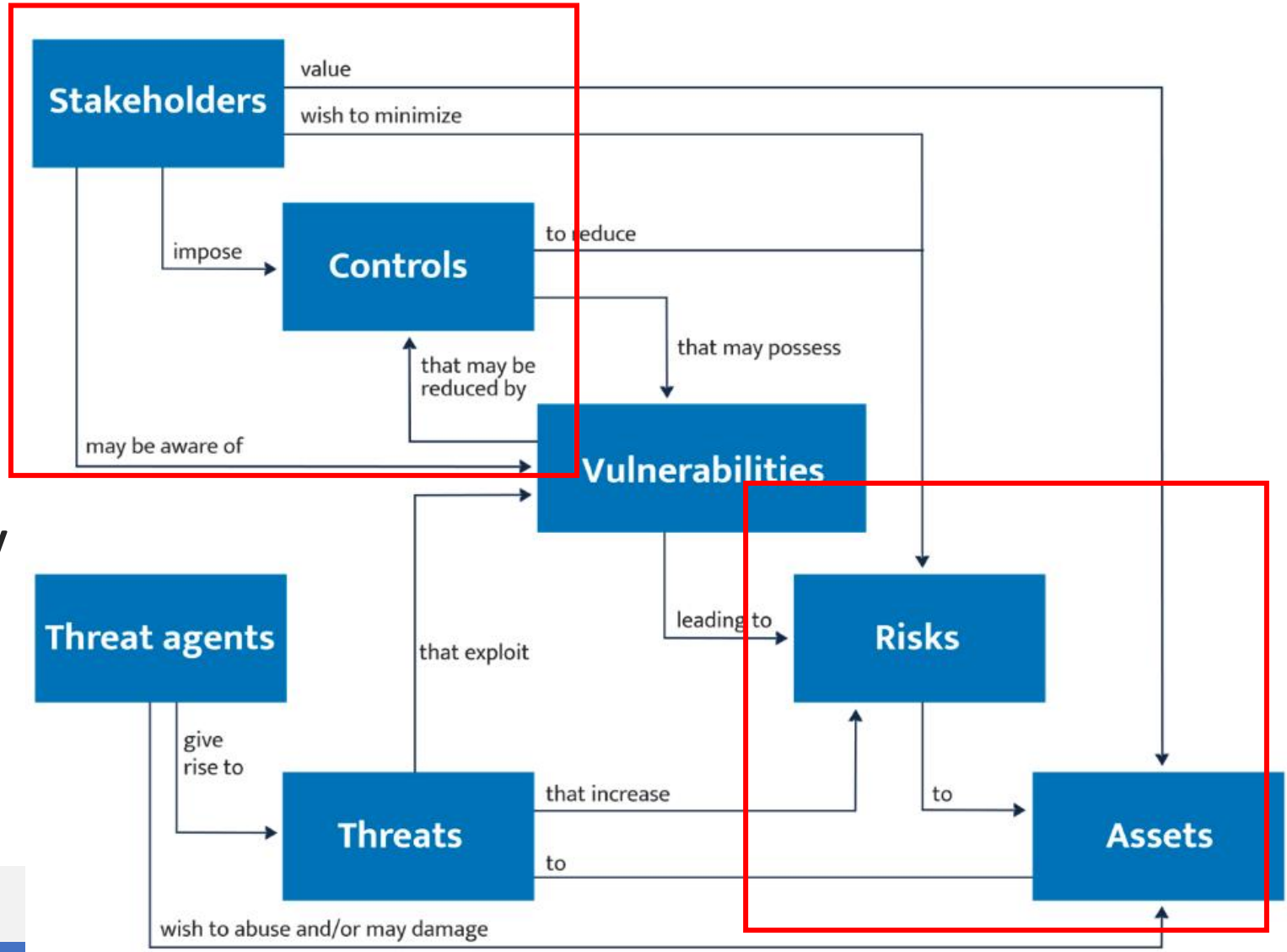
## Objectives

- **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

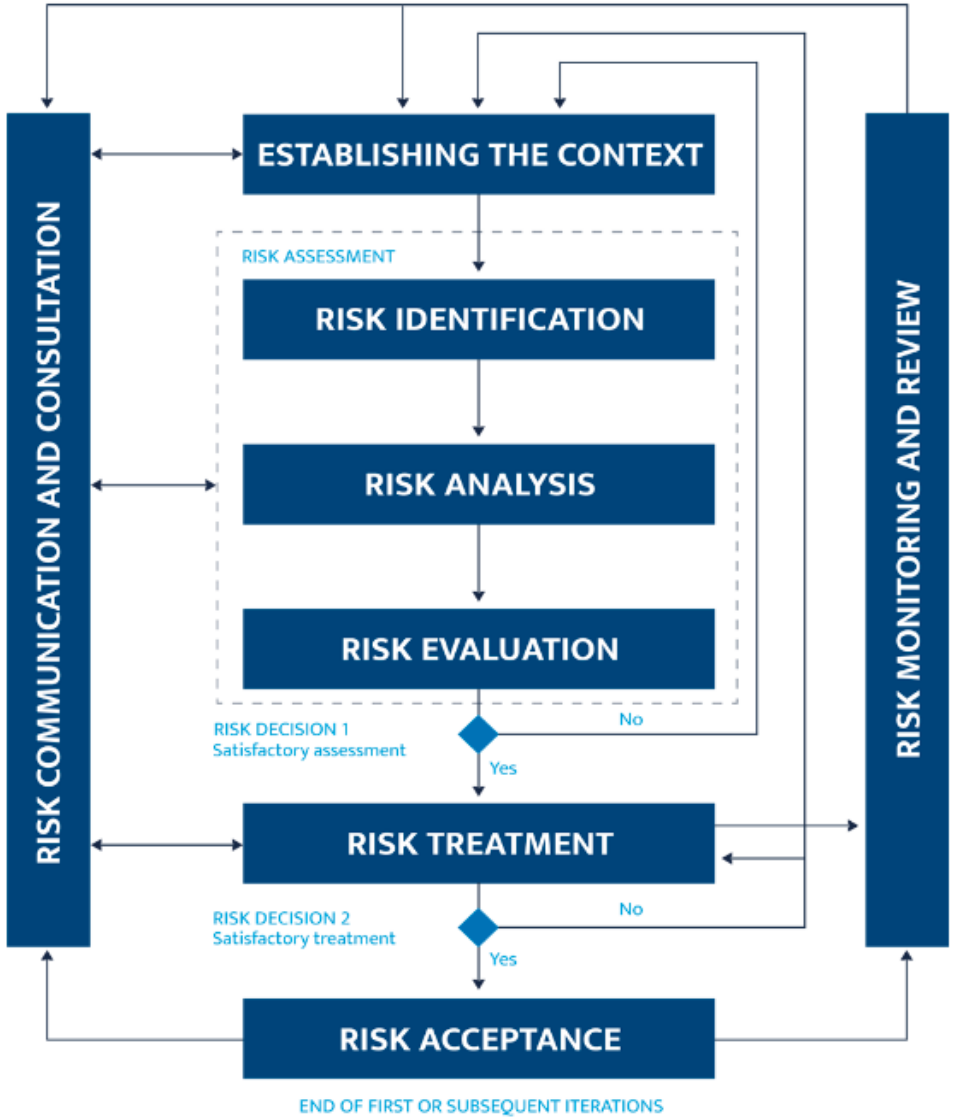
- Risk Based
  - Aims to minimize risk
- Consider Stakeholders
  - Decision Level
- Consider Assets Inventory
  - Services
  - Products



# 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!

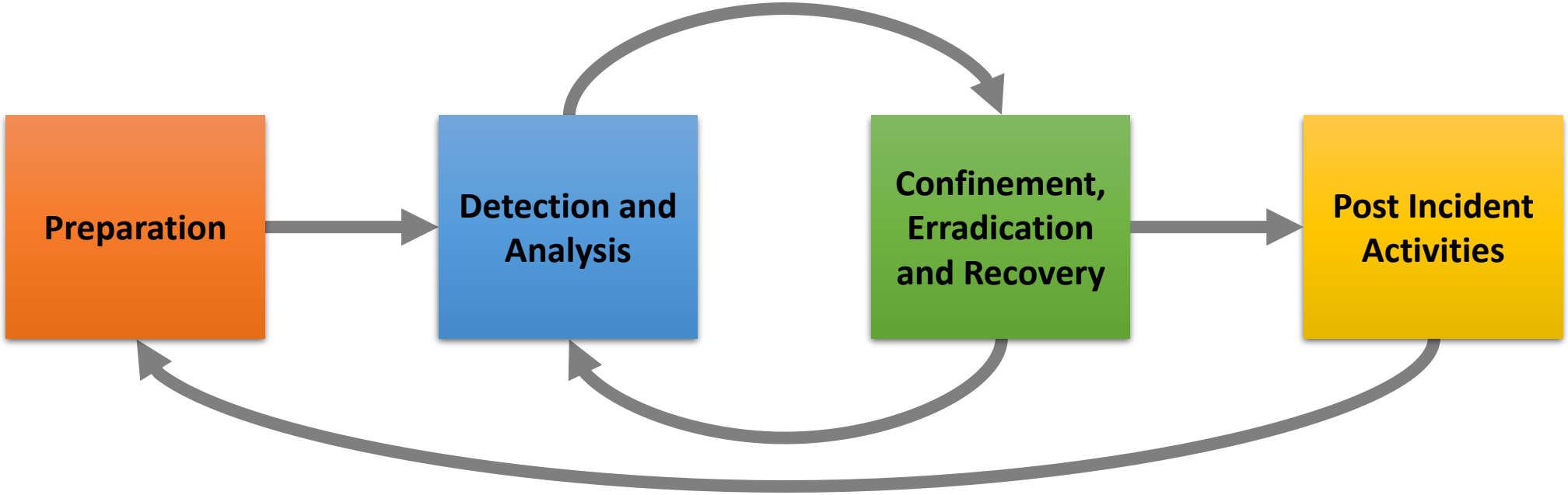
- What is a crown jewel?
  - Essential Sensitive Data
  - Essential Servers
  - Essential Software Systems
  - Any other asset (HVAC, Generators…)
- Disruption to the crown jewels will pose a serious impact to the organization
- Objective: Protect the crown jewels
  - and grow from there to the rest 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

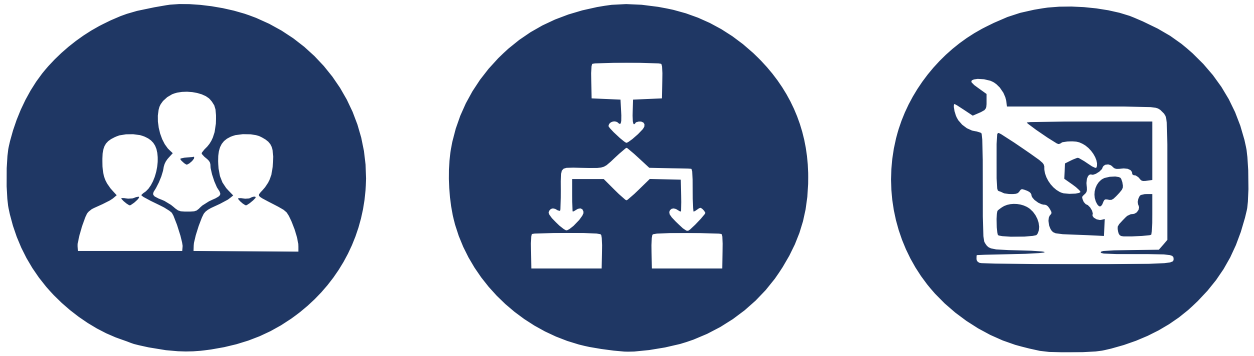
- Security operations are frequently organized in teams
  - Blue Team: Defends an organization from malicious actors
  - Red Team: Attacks an organization to help finding weak spots
  - Purple Team: Mixed attack defense role

- 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

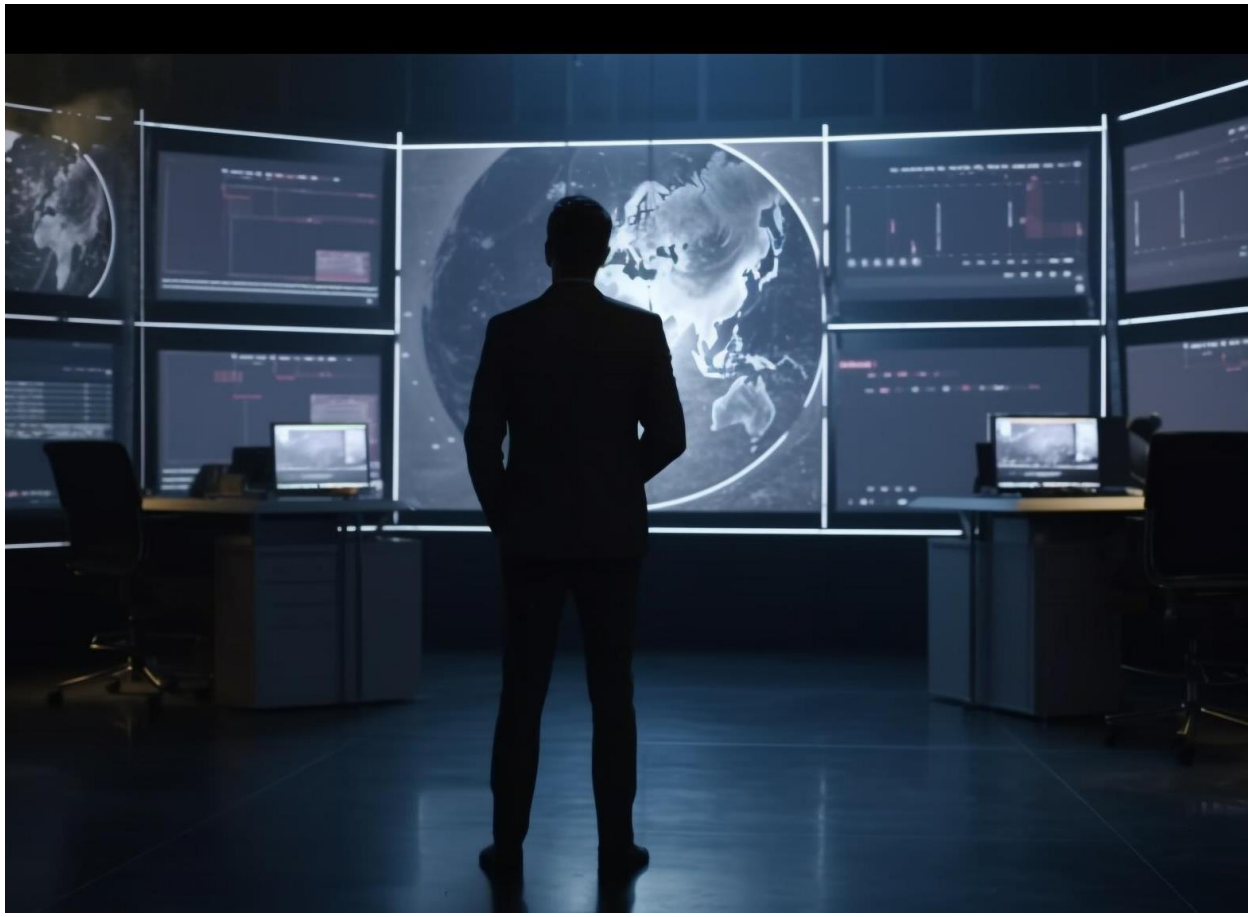
# Blue Team Defence Techniques

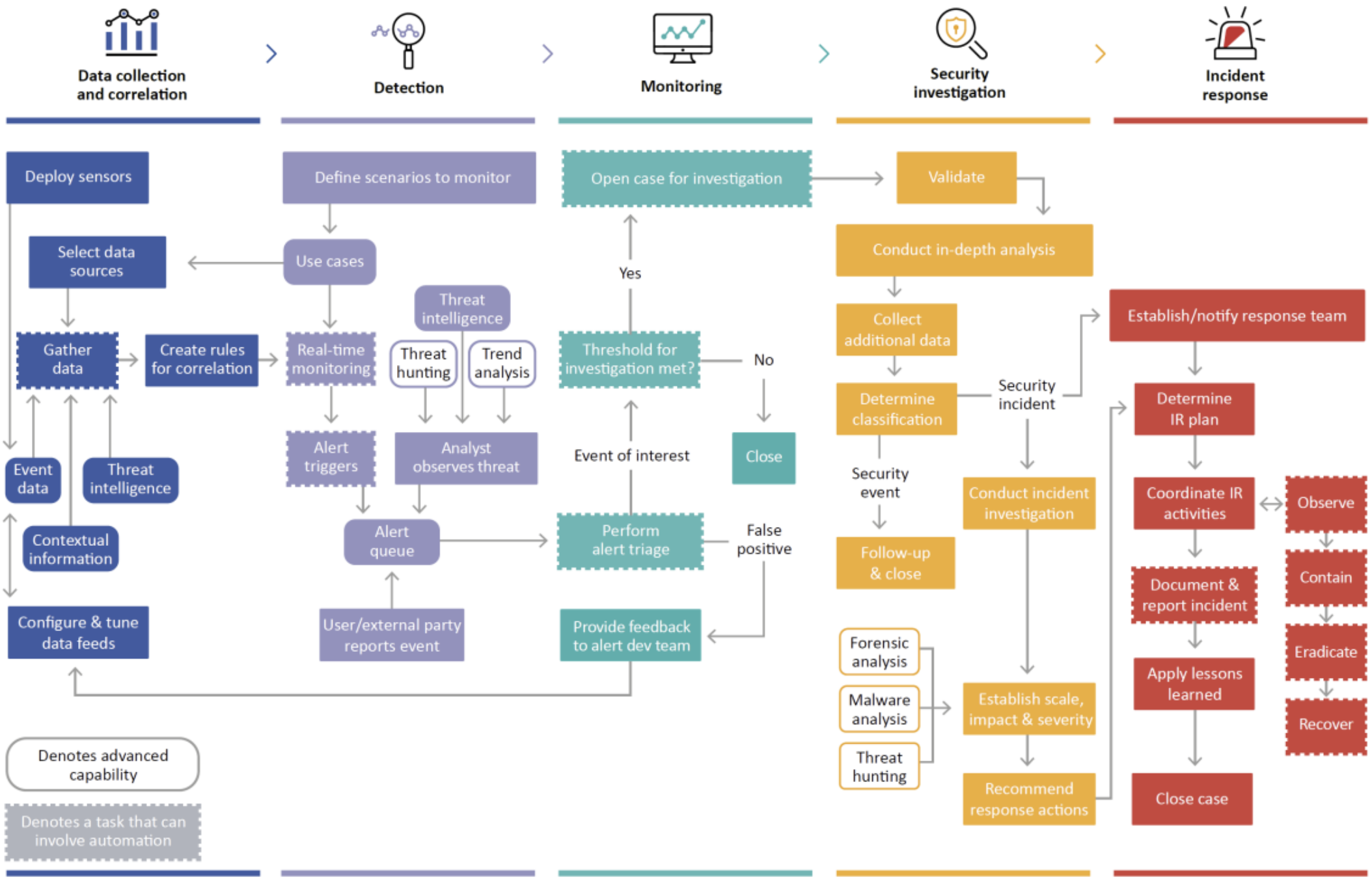
- Everything Everywhere All at Once?
  - No! Prioritize according to the organization mission

- Current approaches focus on:
  - the CIA triad
  - the crown jewels
    - Risk assessment
  - 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

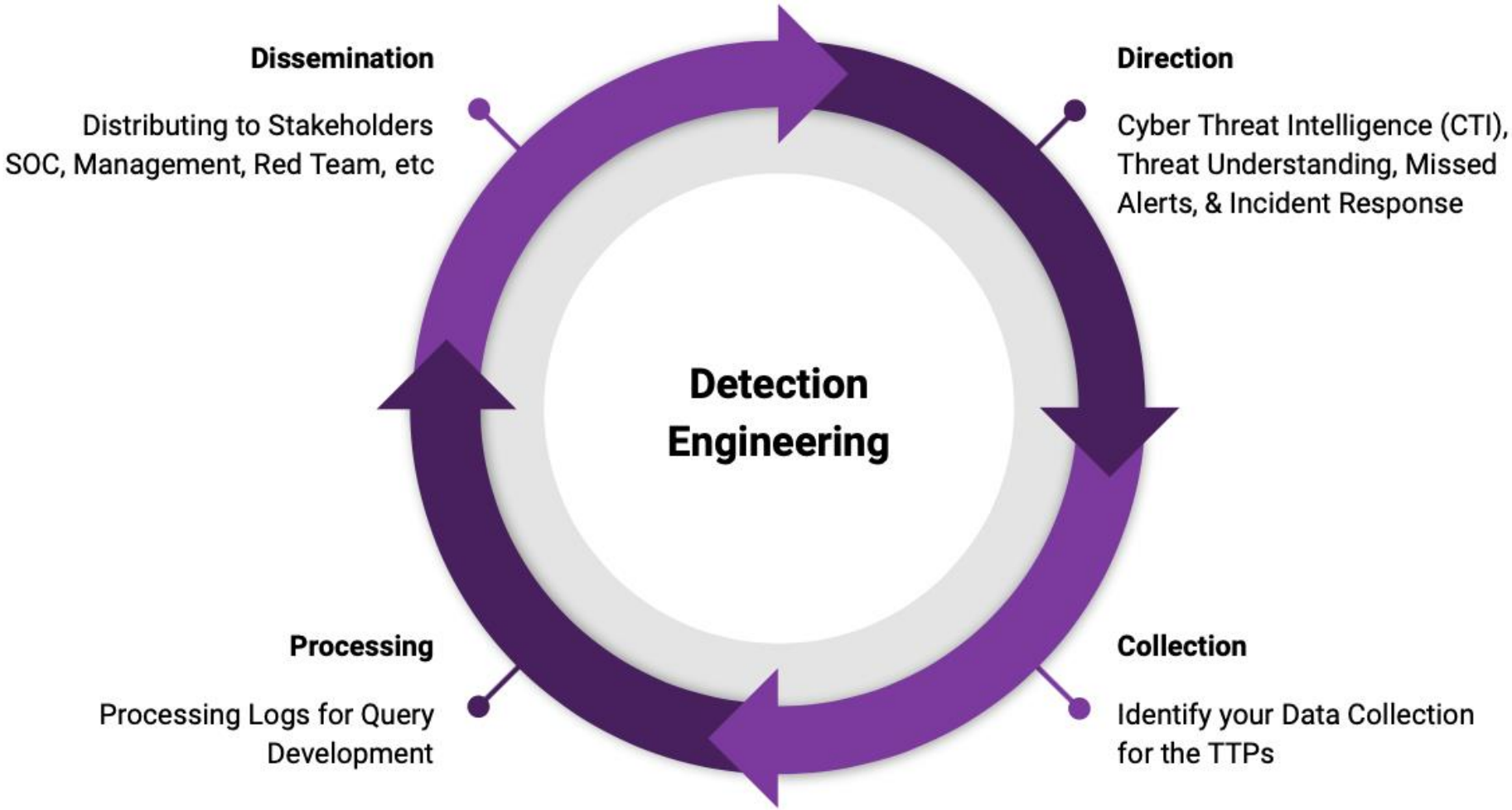



Data collection and correlation
Detection
Monitoring
Security investigation
Incident response
Deploy sensors
Select data sources
Gather data
Create rules for correlation
Event data
Threat intelligence
Contextual information
Configure & tune data feeds
Define scenarios to monitor
Use cases
Real-time monitoring
Threat intelligence
Threat hunting
Trend analysis
Alert triggers
Analyst observes threat
Alert queue
User/external party reports event
Open case for investigation
Yes
Threshold for investigation met?
No
Close
Event of interest
Perform alert triage
False positive
Provide feedback to alert dev team
Validate
Conduct in-depth analysis
Collect additional data
Determine classification
Security incident
Security event
Follow-up & close
Forensic analysis
Malware analysis
Threat hunting
Conduct incident investigation
Establish scale, impact & severity
Recommend response actions
Establish/notify response team
Determine IR plan
Coordinate IR activities
Observe
Contain
Eradicate
Recover
Document & report incident
Apply lessons learned
Close case
Denotes advanced capability
Denotes a task that can involve automation

# 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

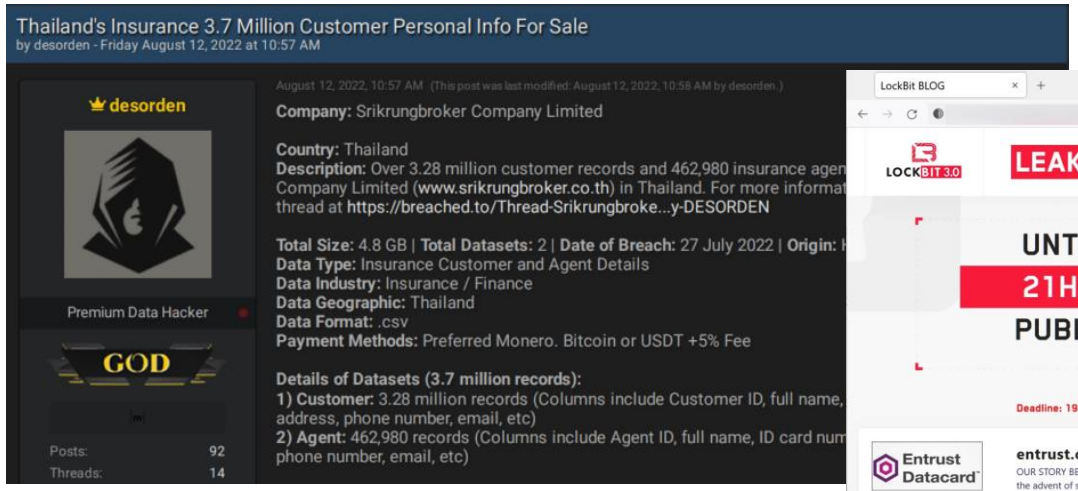


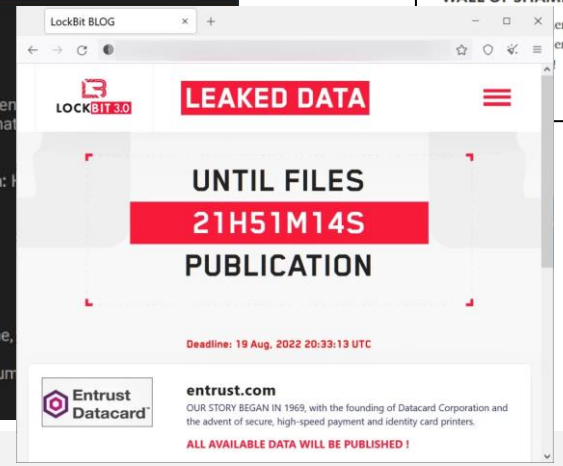

Source: SANS

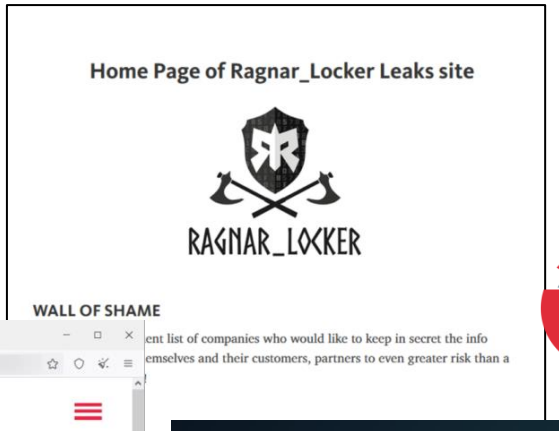
# Direction: CTI

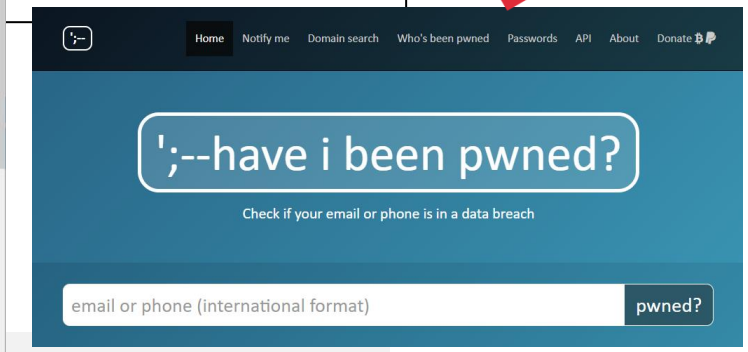
## Assess the current threats from Cyber Threat Intelligence

- 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



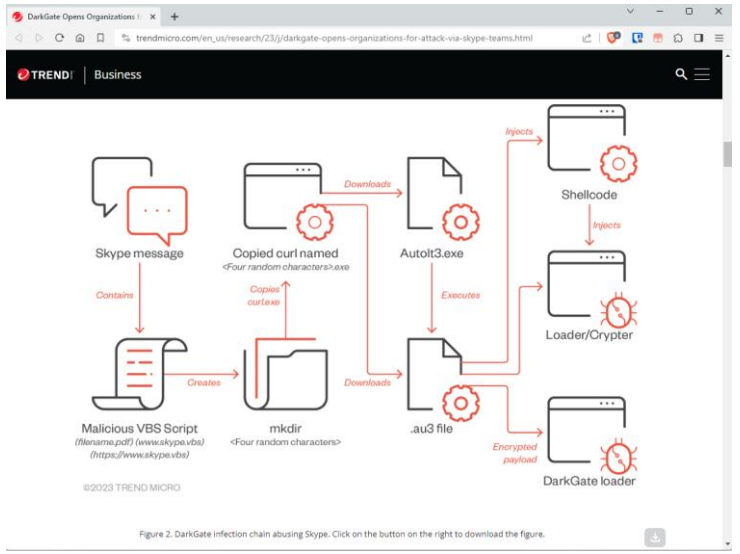



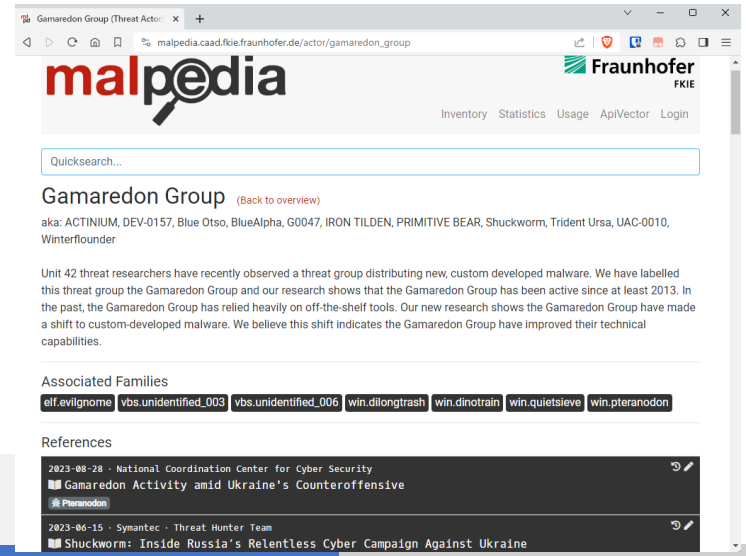

CIRCL MISP Threat Sharing

# Direction: CTI

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





# Direction: CTI

## Assess the current threats from CTI

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



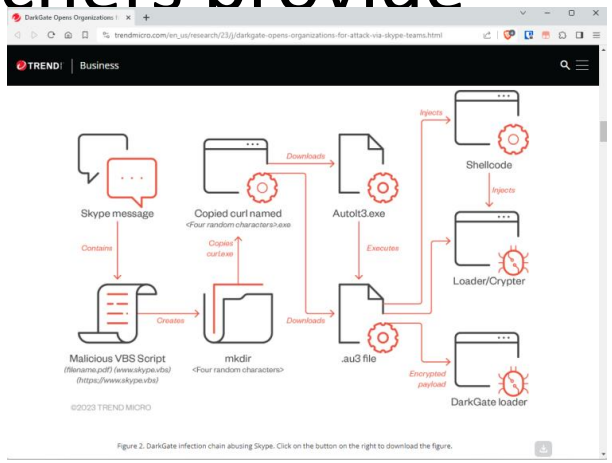
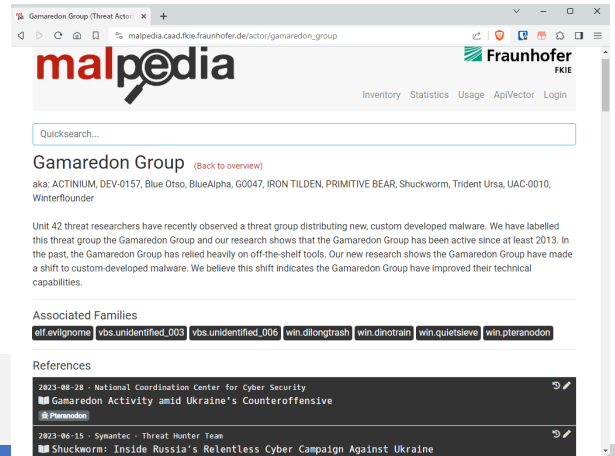



Figure 2. DarkGate infection chain abusing Skype. Click on the button on the right to download the figure.



# 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

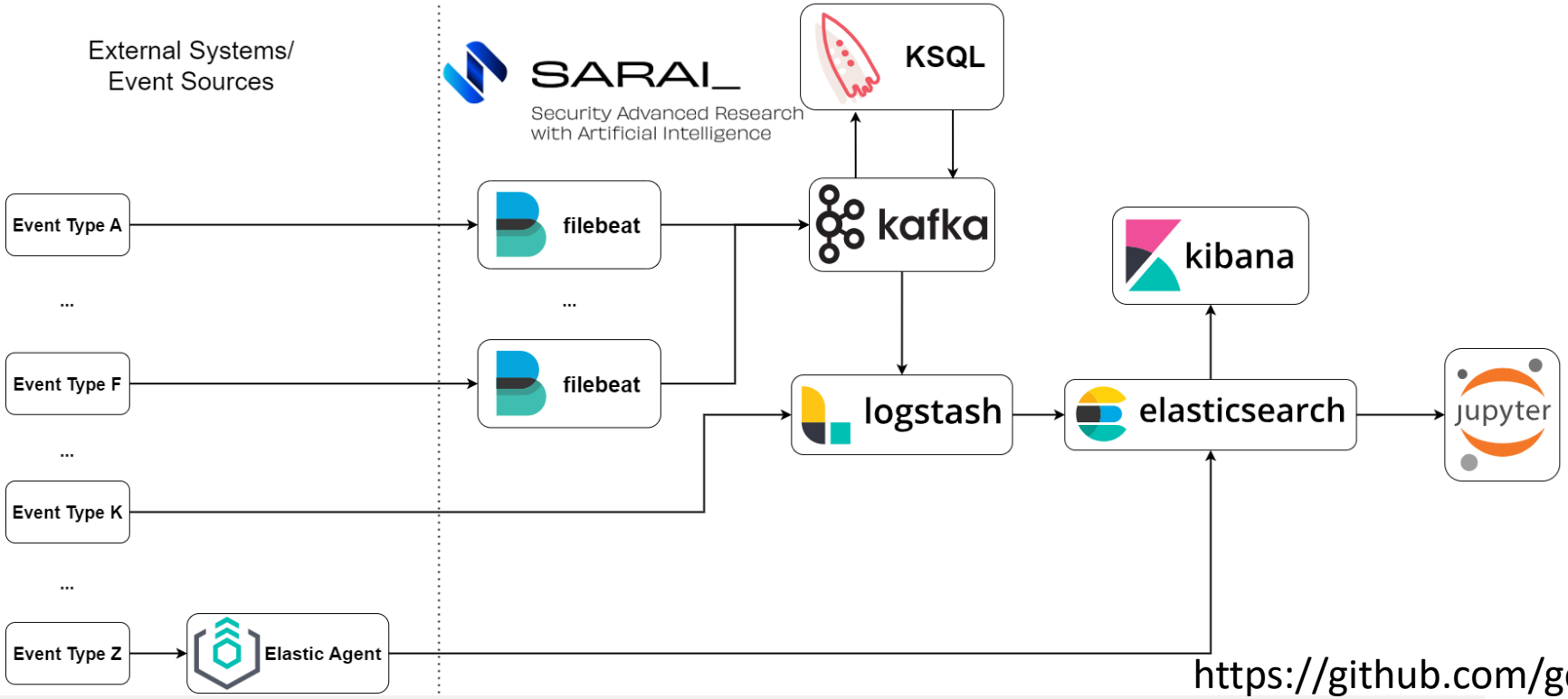
- Focus on relevant data sources to address threats
  - Cannot get all data
  - Visiblity will be limited

- Potential targets
  - Servers: AD, email, HTTP, Databases
  - Wireless Controllers
  - VPN access
  - Firewalls
  - Endpoints: Laptops, VMs, IoT devices

# Collection: Data Harvesting

## Engineer Data Collection

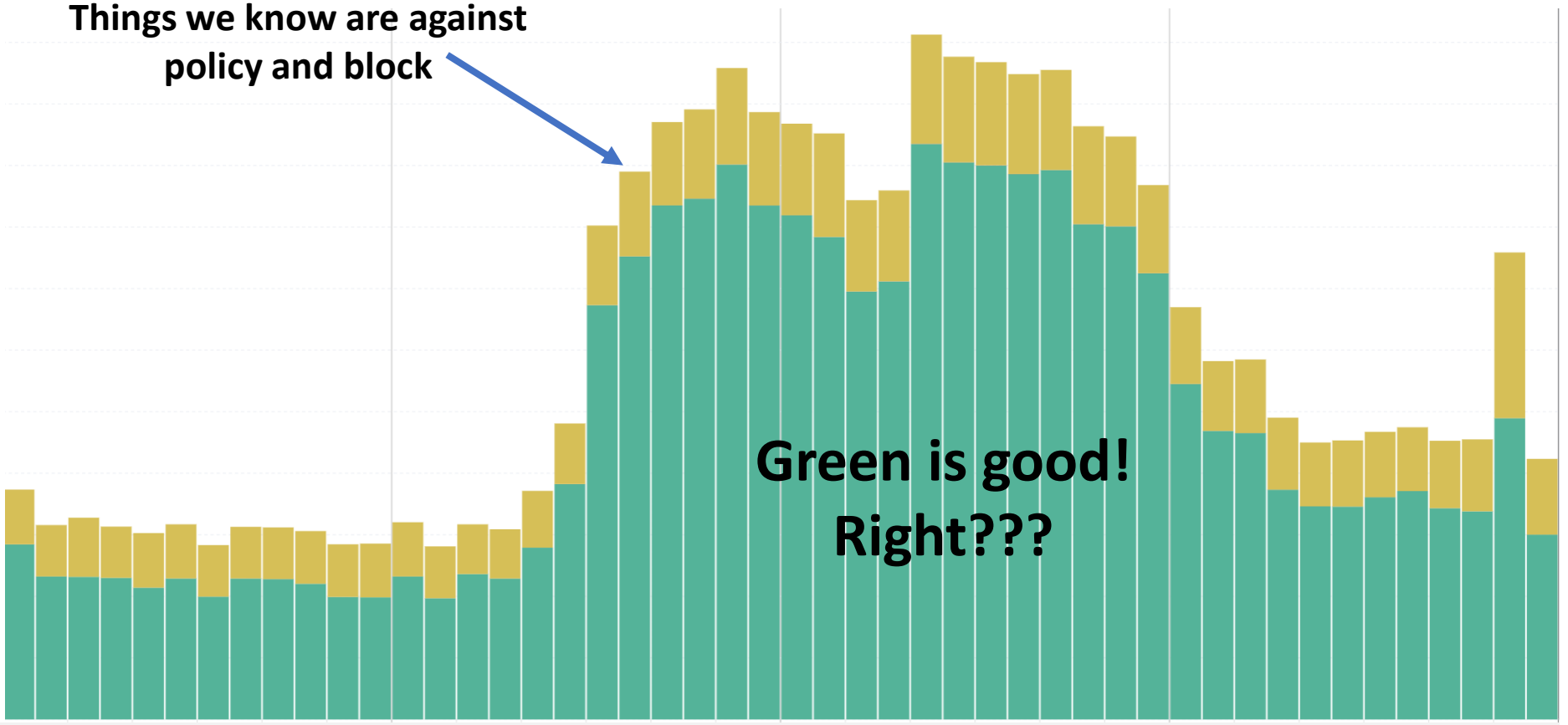
- Current approaches focus on a large data lake
  - Algorithms match rules, ML models, signatures, behavior




https://github.com/gcsuaveiro/gcs-sarai

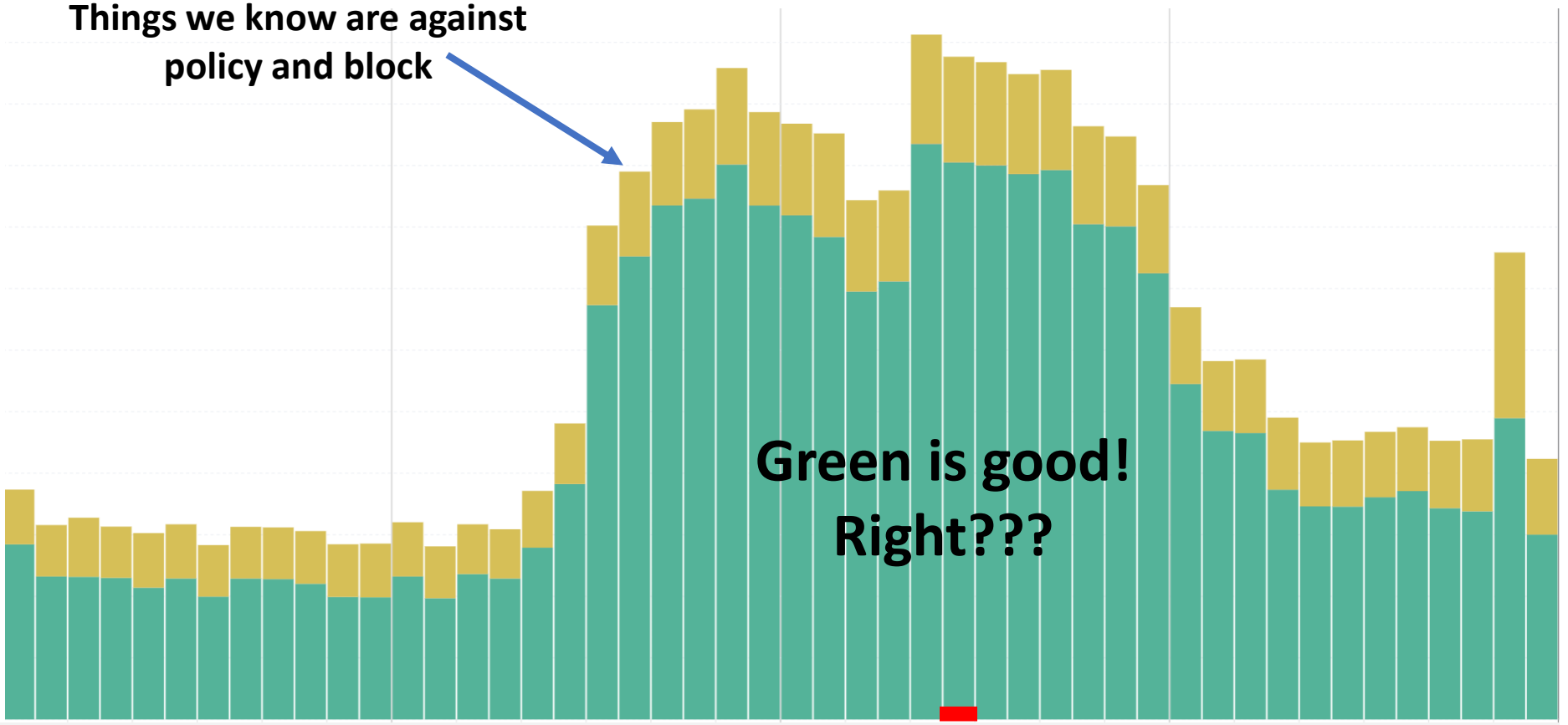
# Collection: Data Harvesting

## Processing: Pain?



# Collection: Data Harvesting

## Processing: Pain?



# Collection: Data Harvesting

## Processing: Pain?

Millions of events/hour

Things we know are against policy and block

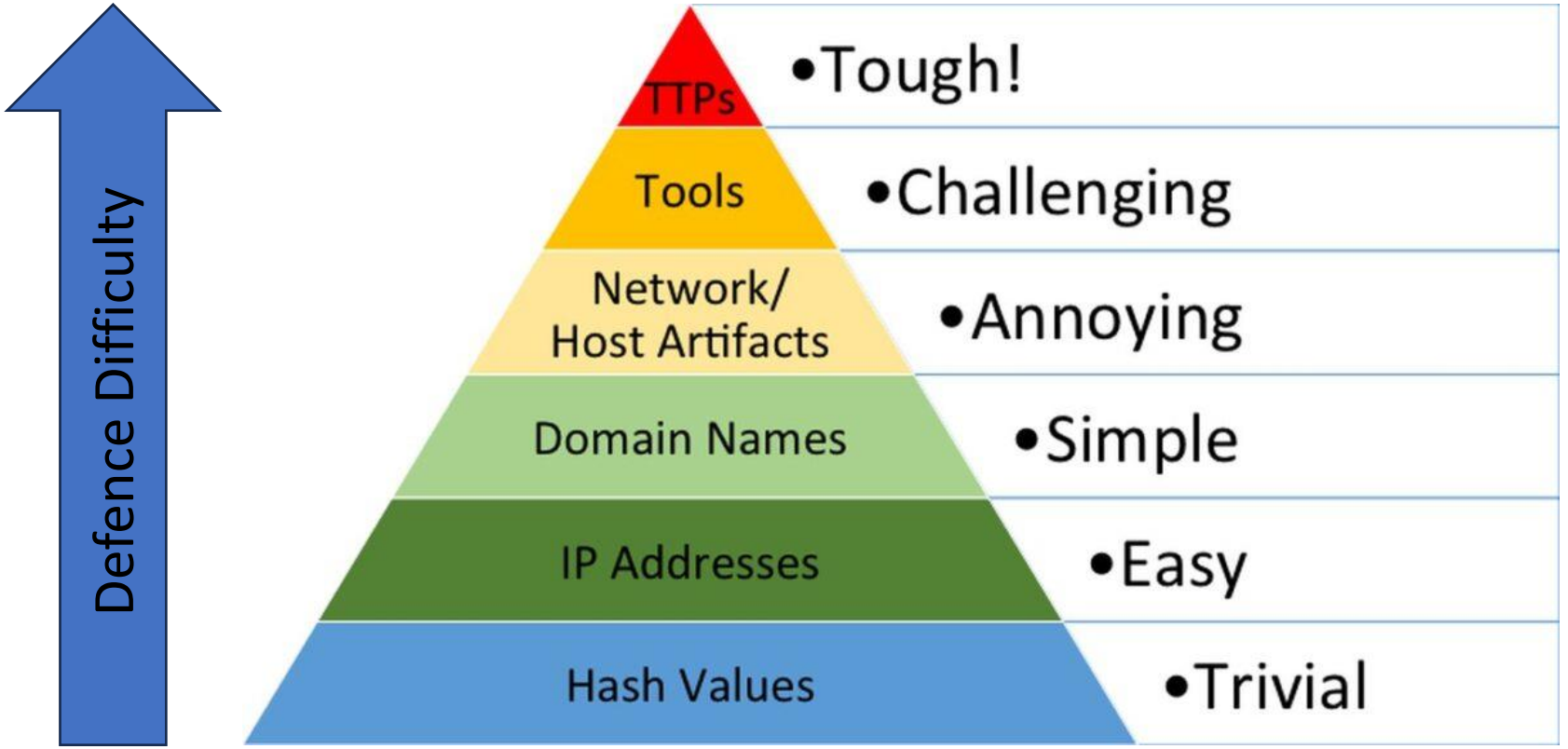

Green events are:
- Compliant events
- Suspicious events that are not blocked
- Malicious events that cannot be detected

Thousands of malicious agents (detect or block)


Concepts of Us (Internal) vs others (External) is not robust

# The Pyramid of Pain

"The Pyramid of Pain" (Bianco, 2013)




- 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
  - Anomally 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 be vendor software
  - Challenge: **Unknown**/Tailored threats

# (Fantastic) Threats and Where to Find Them?

- What if we do not know if something is malicicous?
  - What is a malicious website or file?
  - Most dangerous threats are not classified are Malware.

- New malware potentially has high impact
  - It is not detected by Anti-virus
  - Explores unpatched vulnerabilities or flaws (0 day)

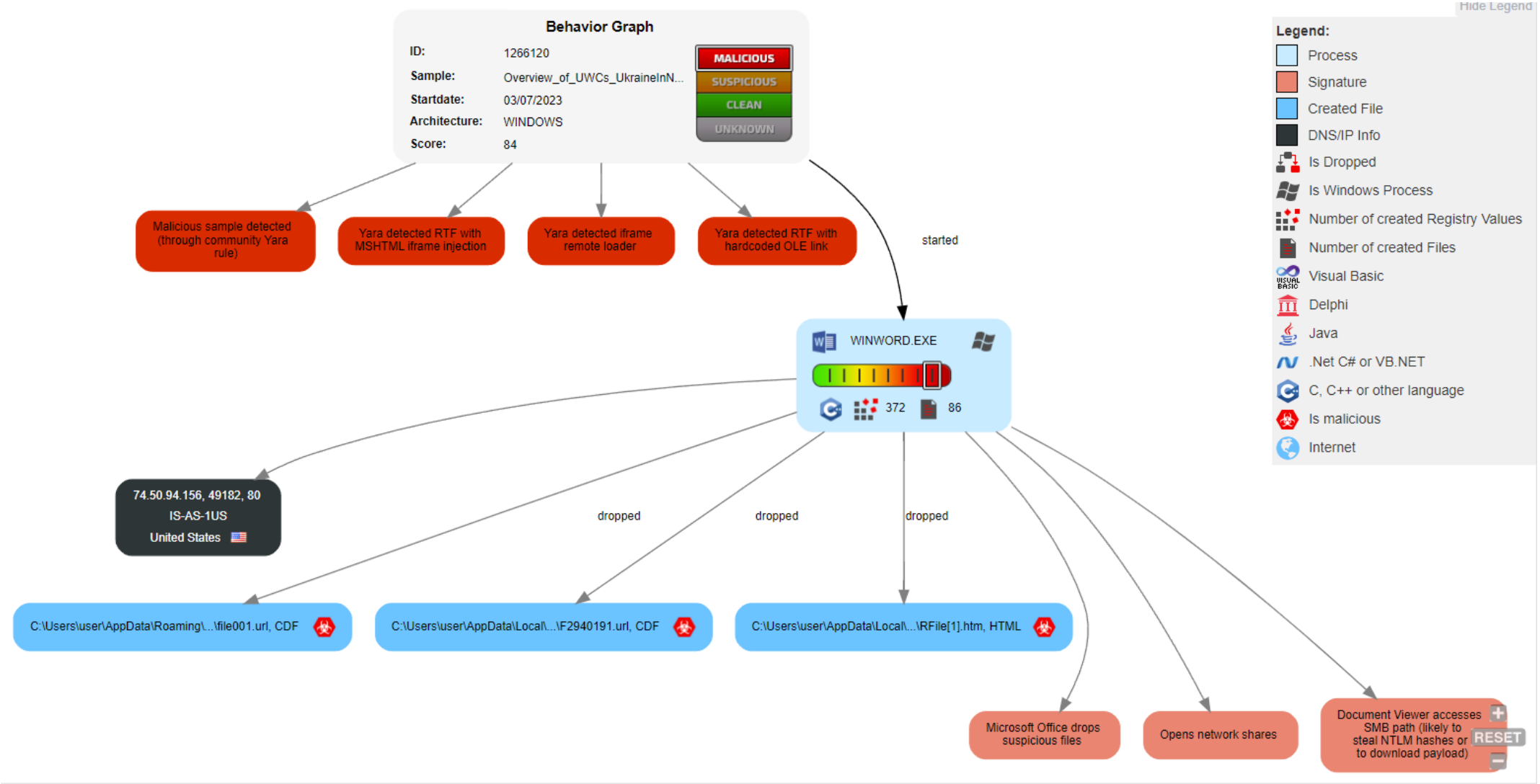
- A new malicious asset is just a **new program/website**
  - May be a variation of a existing malware
    - Different language/obfuscated/encrypted/packed
  - May simply bypass existing signatures
  - There is a robust market selling malware

# Threat Research

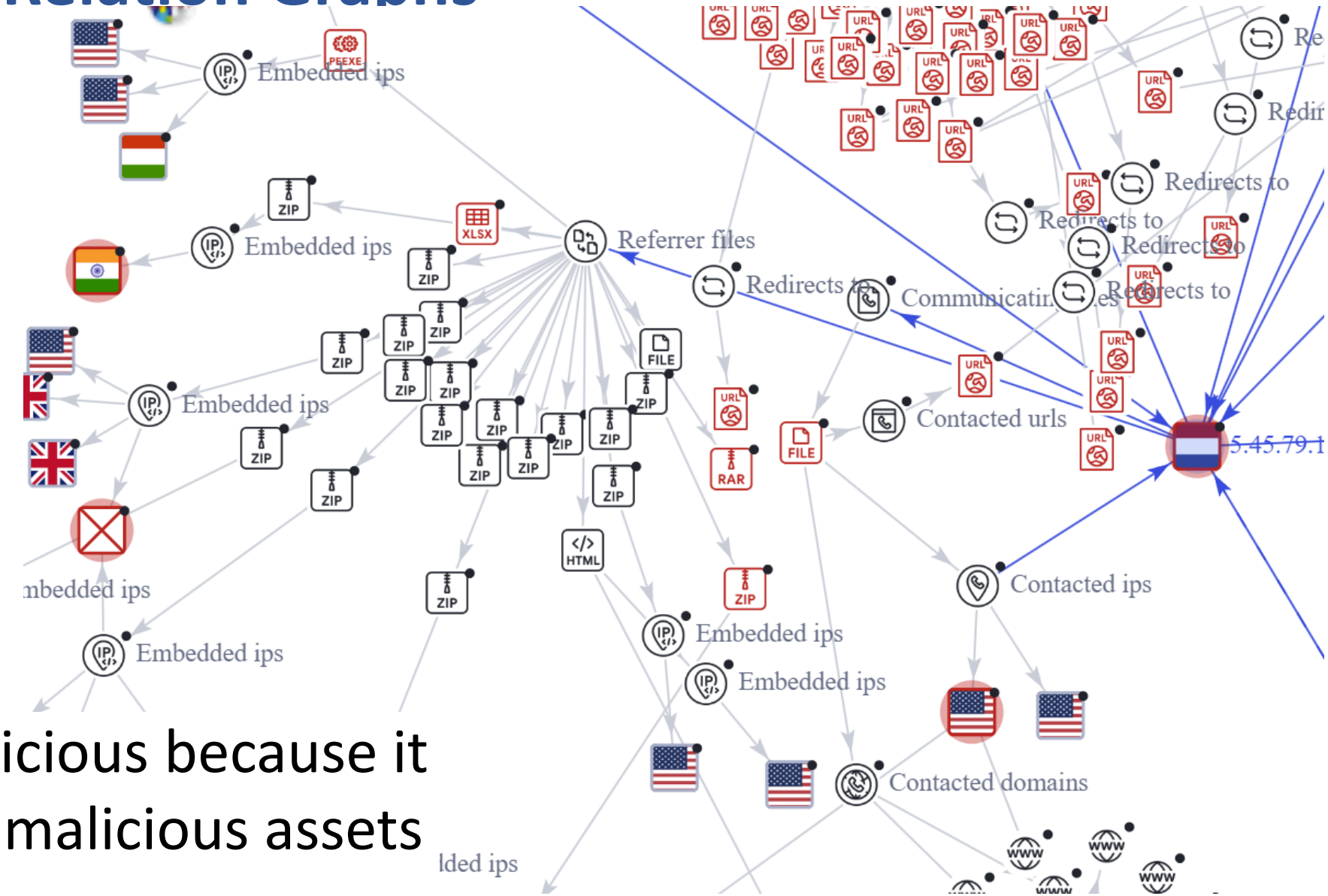
- Threat Research allows detection of **new offenses**
  - Takes a Indicators and determines its behavior

- 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