Defending an Organization

SIO

deti universidade de aveiro
departamento de eletrónica,
telecomunicações e informática

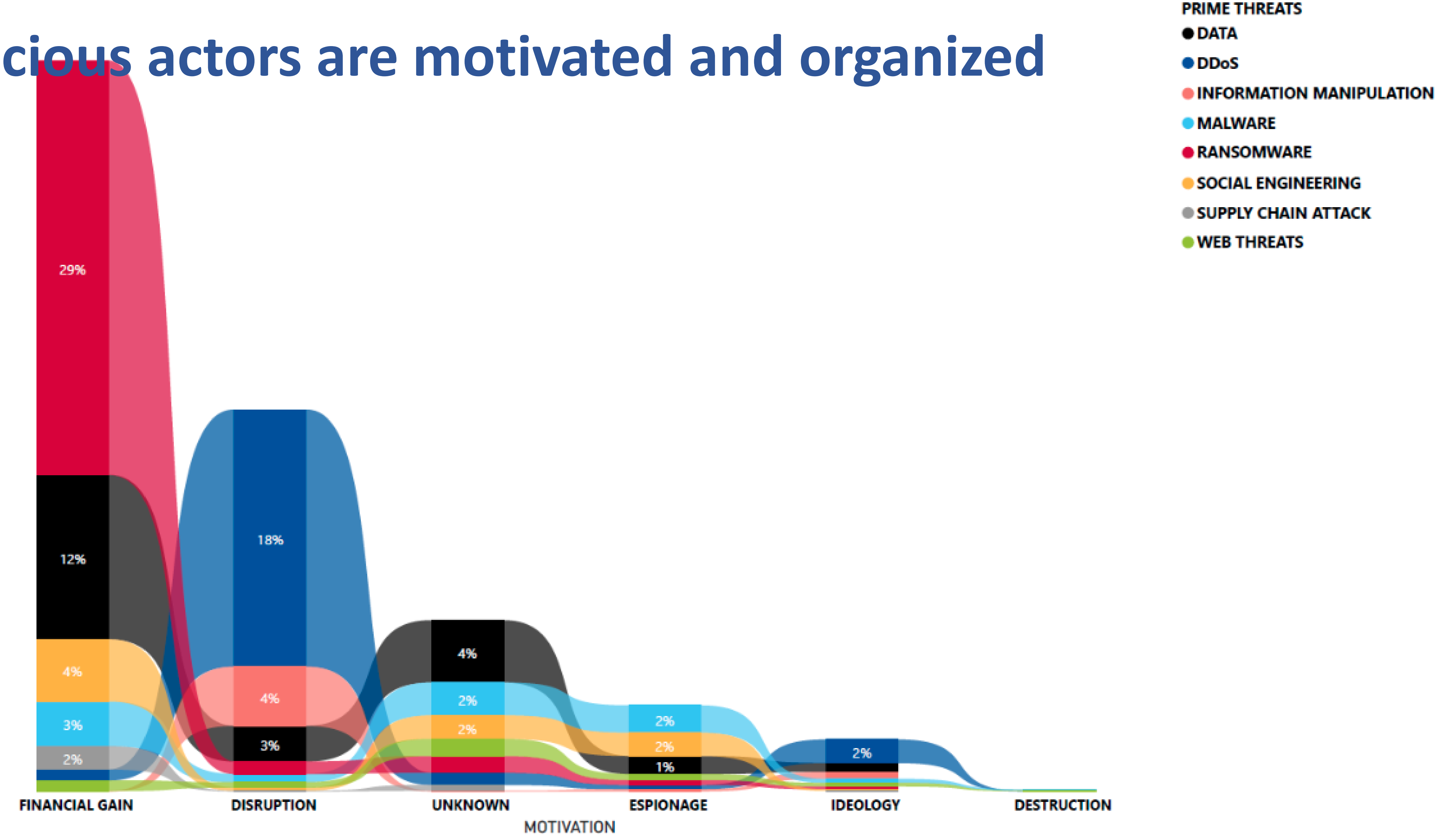
The current organizational landscape

- 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



ENISA Threat Landscape 2023

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.

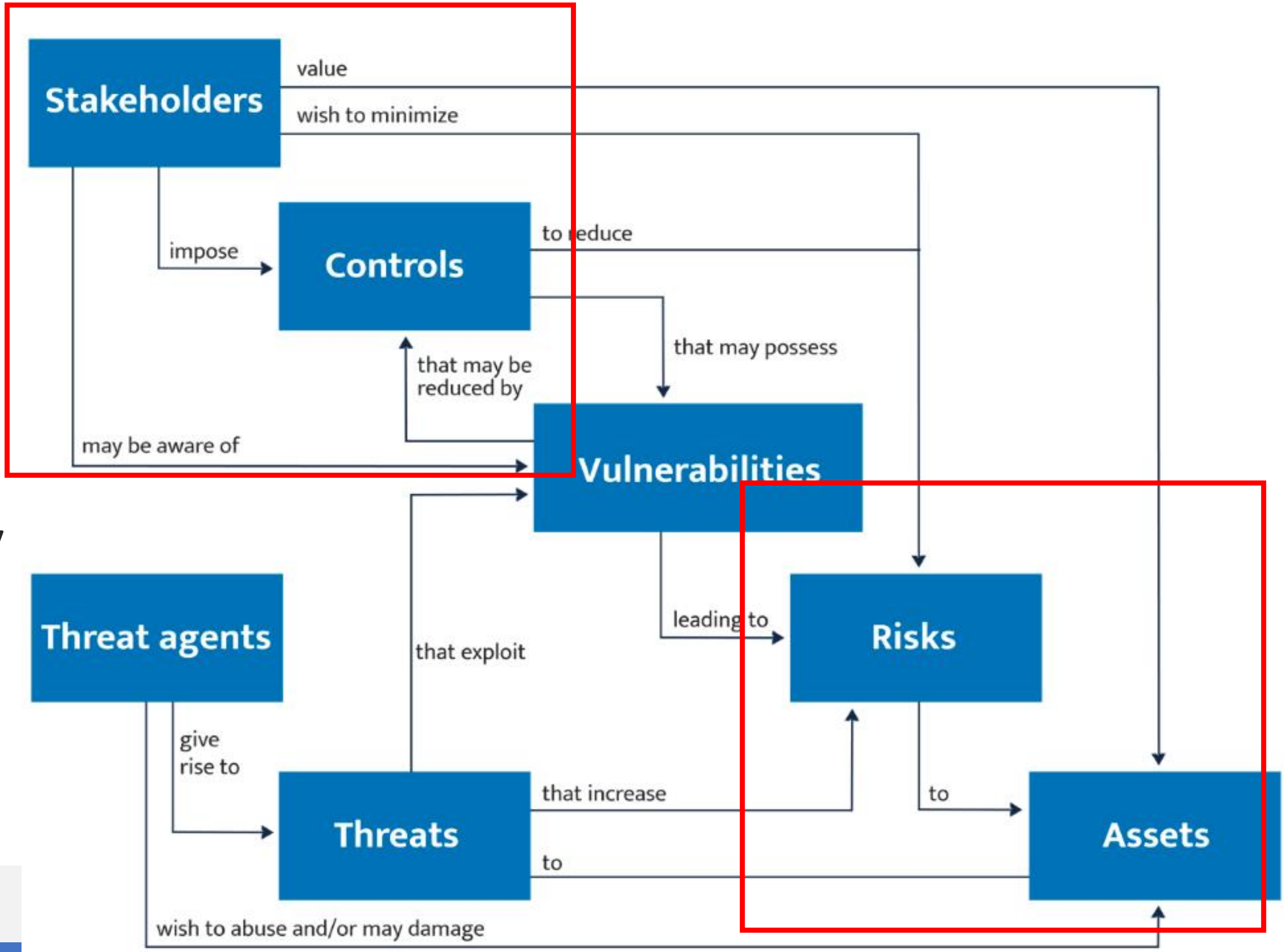
- **Respond**: Definition and implementation of appropriate measures in case of incident detection.

- **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

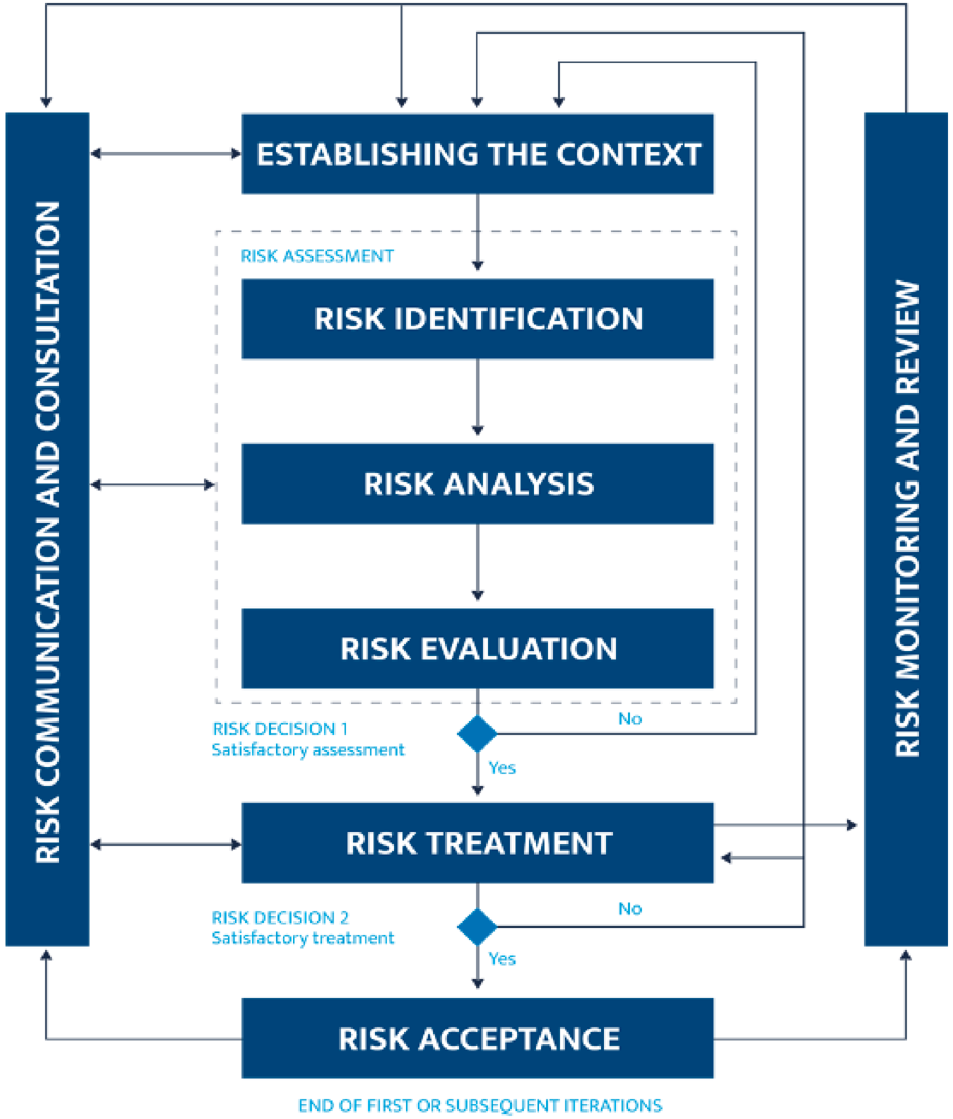
- Risk Based
  - Aims to minimize risk
- Consider Stakeholders
  - Decision Level
- Consider Assets Inventory
  - Services
  - Products



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

SAI NO TESTE 8

- 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

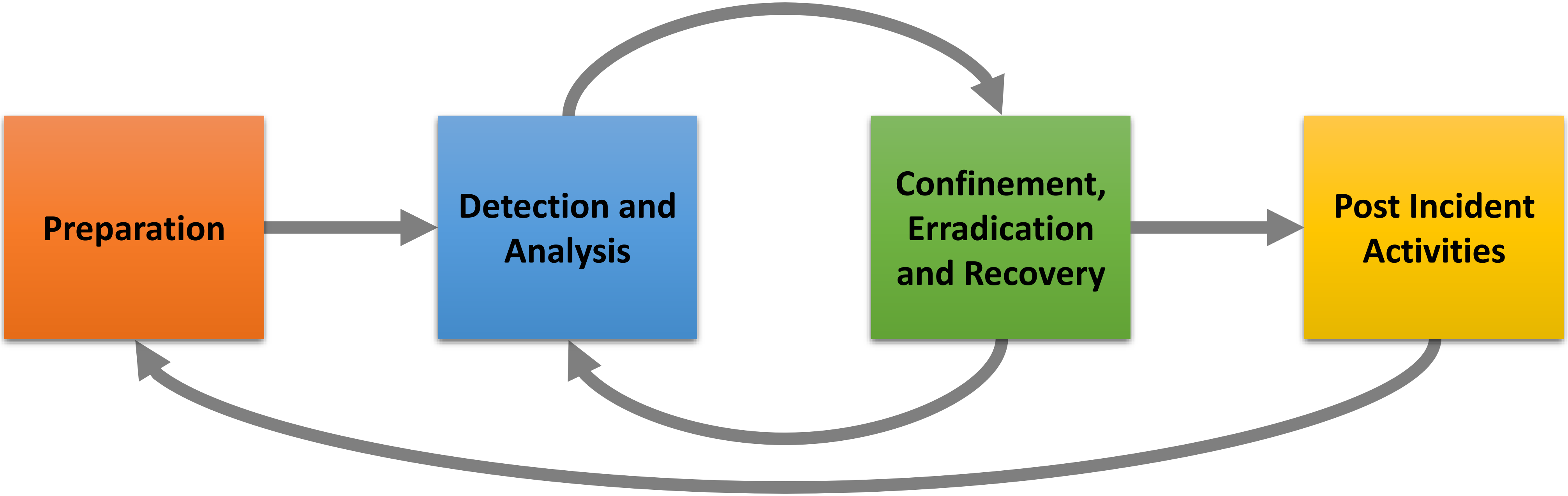
- Live document describing the security posture
  - Allows organizations to know where they are and where they want to go
  - Considers authentication, backups, risk, access control, policies, etc.

- 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

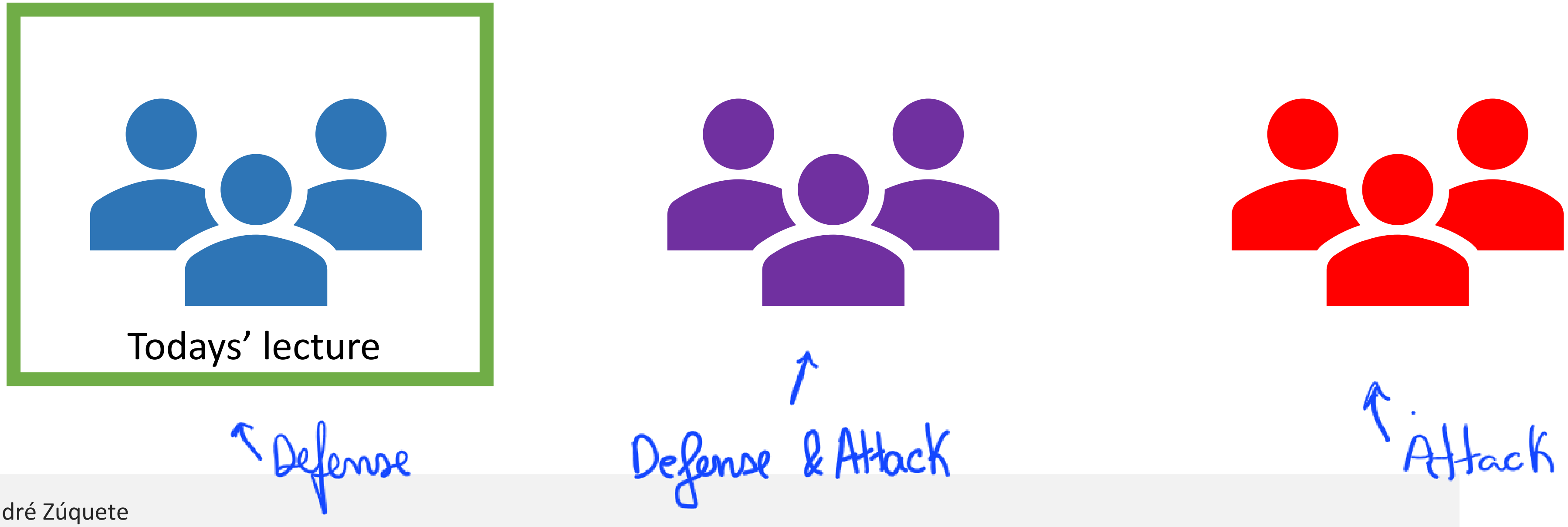
- **Support Activities**
  - Networks, projects
  - E.g. https://www.ccc-centro.pt (Competence Center)
  - Increase the security posture and resilience of organizations
    - Training and awareness
    - Exchange strategies, information, and tools
    - Incident Response
    - Funding

- **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



Todays' lecture

Defense

Defense & Attack

Attack

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

Attackes only need to sucess once, defensors only con fail once //

- 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

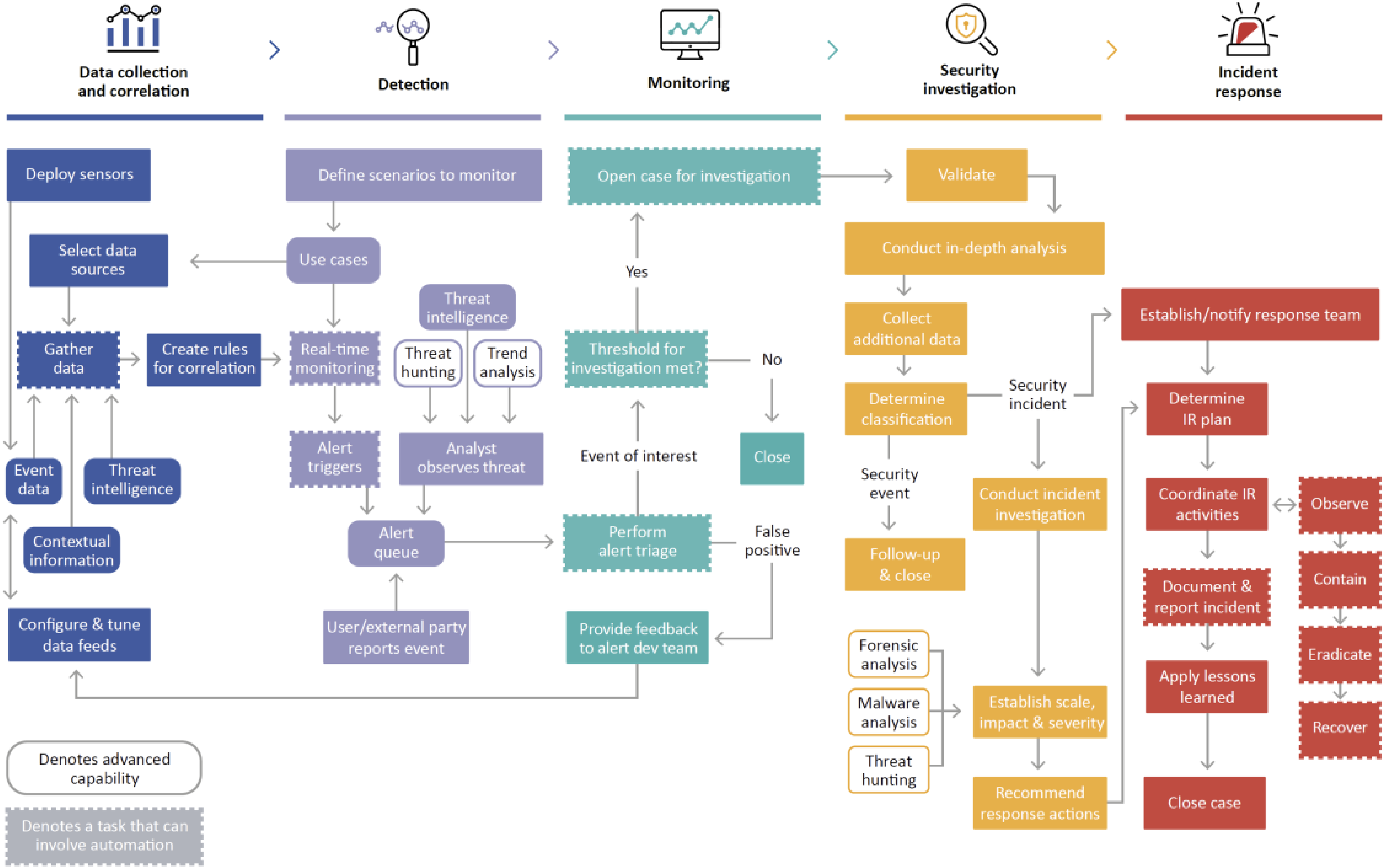
Blue Team Defence Techniques

- 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

Conduct incident investigation

Forensic analysis

Malware analysis

Threat hunting

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

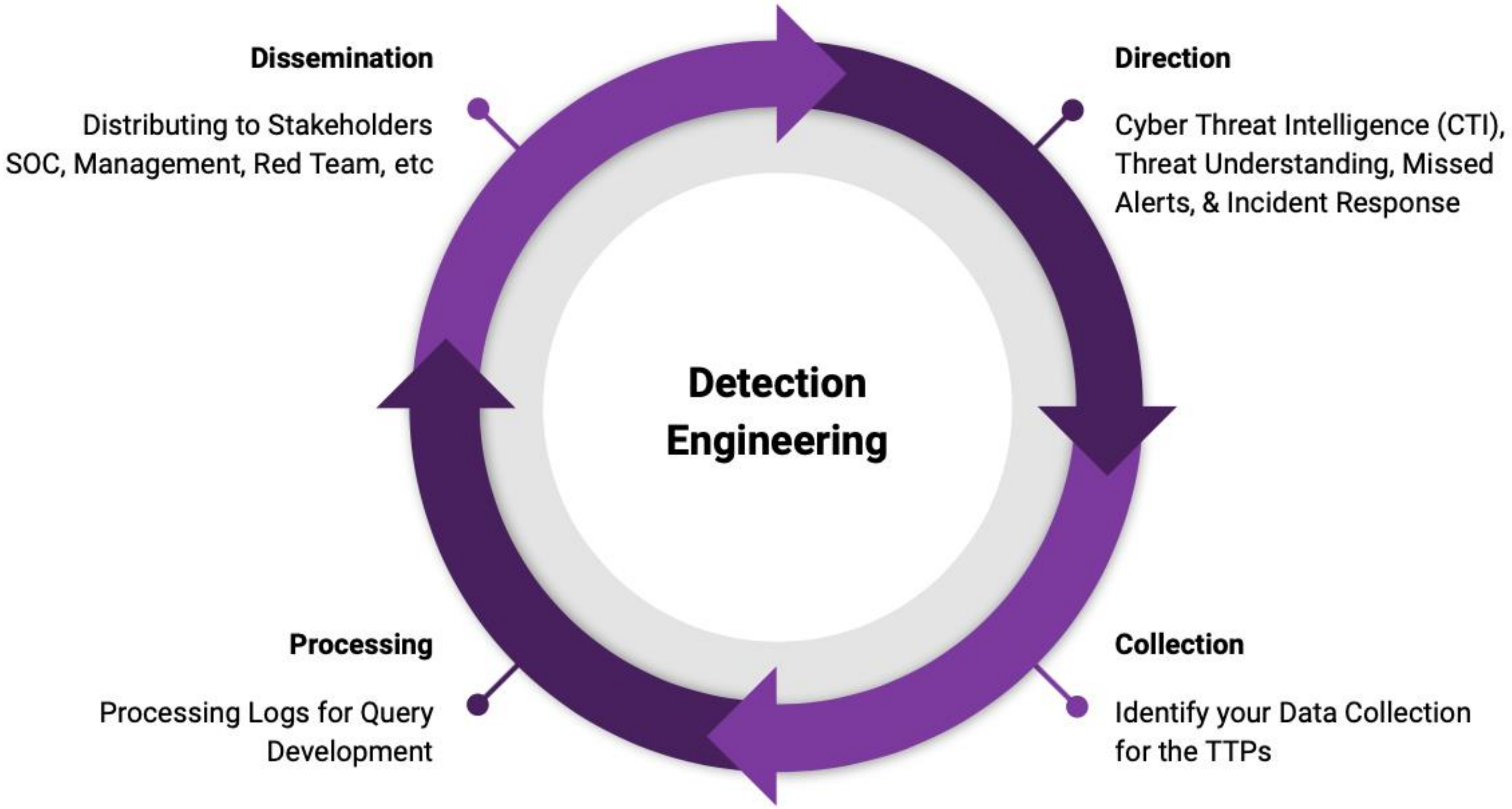
- Defensive Security (Engineering)
  - Firewalls, backups, logs
  - Secure Software Development Lifecycle
  - Security related requirements (e.g., OWASP ASVS)
  - Training and Awareness

Estamos a seguir
as métricas?"

- 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



Dissemination

Distributing to Stakeholders
SOC, Management, Red Team, etc

Direction

Cyber Threat Intelligence (CTI),
Threat Understanding, Missed
Alerts, & Incident Response

Detection Engineering

Collection

Identify your Data Collection
for the TTPs

Processing

Processing Logs for Query
Development

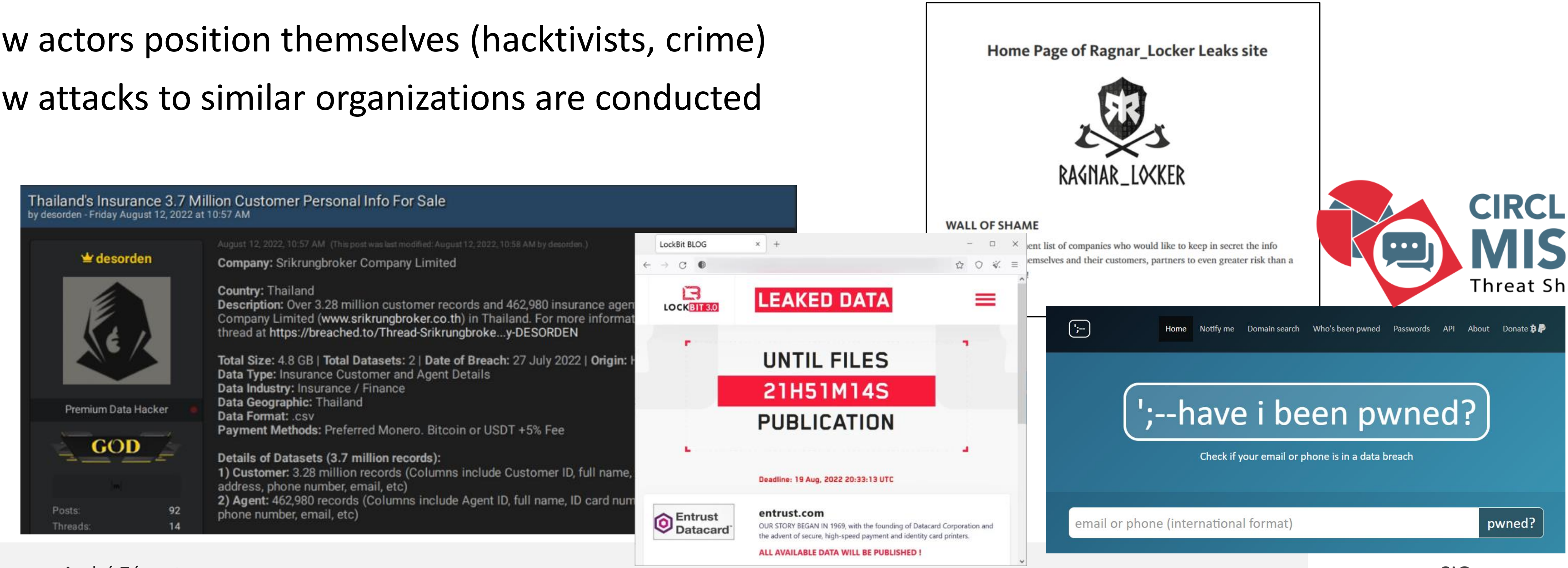
Source: SANS

TTPs: Tactics, Techniques, and Procedures

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

August 12, 2022, 10:57 AM (This post was last modified: August 12, 2022, 10:58 AM by desorden.)

Company: Srikrungbroker Company Limited

Country: Thailand
Description: Over 3.28 million customer records and 462,980 insurance agen
Company Limited (www.srikrungbroker.co.th) in Thailand. For more informat
thread at https://breached.to/Thread-Srikrungbroke...y-DESORDEN

Total Size: 4.8 GB | **Total Datasets:** 2 | **Date of Breach:** 27 July 2022 | **Origin:**
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 num
phone number, email, etc)

desorden
Premium Data Hacker
GOD
Posts: 92
Threads: 14

LockBit BLOG

LOCKBIT 3.0

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
emselves and their customers, partners to even greater risk than a
!

CIRCL MISP Threat Sharing

';--have i been pwned?

Check if your email or phone is in a data breach

Direction: CTI

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

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE: HEALTH SECTOR

(January 2021 to March 2023)

JULY 2023

CNCS

Observatório de Cibersegurança

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

Riscos & Conflitos

4ª Edição

JUNHO DE 2023

PRR

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

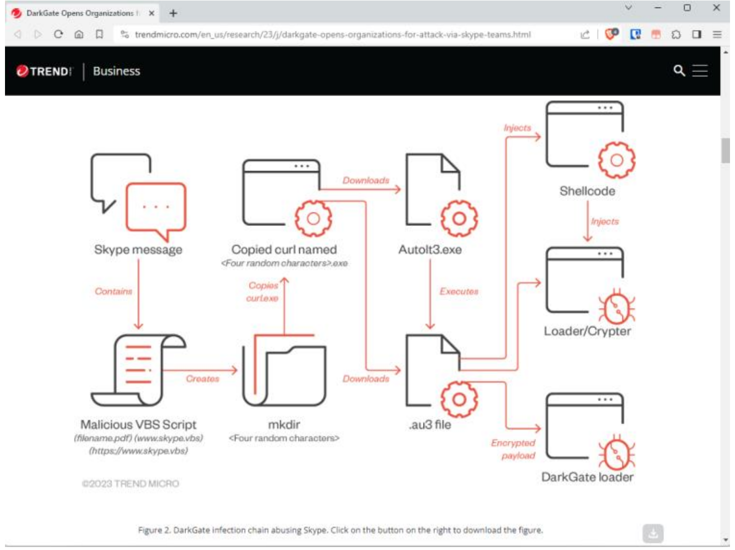
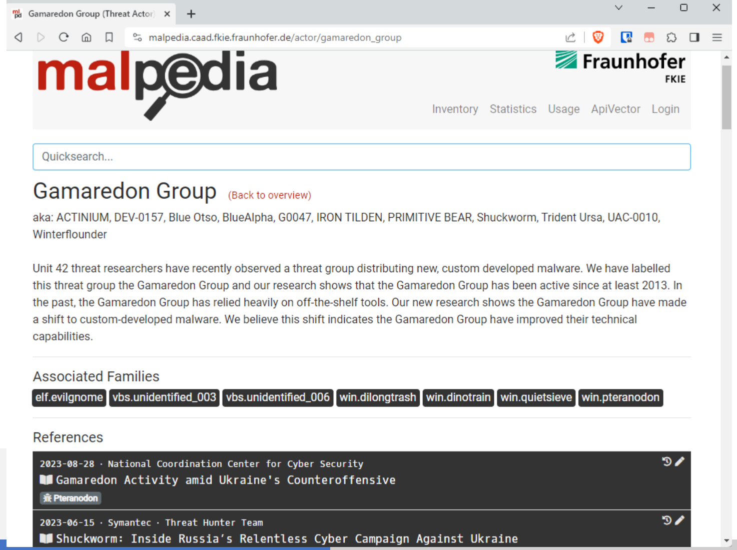


Figure 2. DarkGate infection chain abusing Skype. Click on the button on the right to download the figure.



Gamaredon Group (Threat Actor)
malpedia.caad.fkie.fraunhofer.de/actor/gamaredon_group
malpedia
Fraunhofer FKIE
Inventory
Statistics
Usage
ApiVector
Login
Quicksearch...

Gamaredon Group (Back to overview)

aka: ACTINIUM, DEV-0157, Blue Otso, BlueAlpha, G0047, IRON TILDEN, PRIMITIVE BEAR, Shuckworm, Trident Ursa, UAC-0010, Winterflounder

Unit 42 threat researchers have recently observed a threat group distributing new, custom developed malware. We have labelled this threat group the Gamaredon Group and our research shows that the Gamaredon Group has been active since at least 2013. In the past, the Gamaredon Group has relied heavily on off-the-shelf tools. Our new research shows the Gamaredon Group have made a shift to custom-developed malware. We believe this shift indicates the Gamaredon Group have improved their technical capabilities.

Associated Families

elf.evilgnome vbs.unidentified_003 vbs.unidentified_006 win.dilongtrash win.dinotrain win.quietsieve win.pteranodon

References

2023-08-28 · National Coordination Center for Cyber Security
Gamaredon Activity amid Ukraine's Counteroffensive
Pteranodon

2023-06-15 · Symantec · Threat Hunter Team
Shuckworm: Inside Russia's Relentless Cyber Campaign Against Ukraine

Direction: CTI

Assess the current threats from CTI

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

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE: HEALTH SECTOR

(January 2021 to March 2023)

JULY 2023

CNCS

Observatório de Cibersegurança

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

Riscos & Conflitos

4ª Edição

JUNHO DE 2023

PRR

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

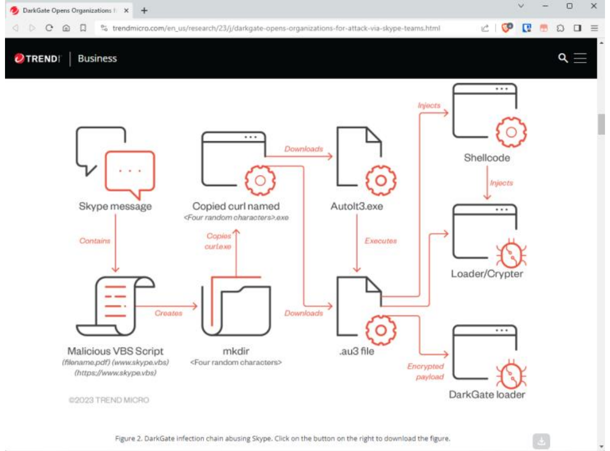
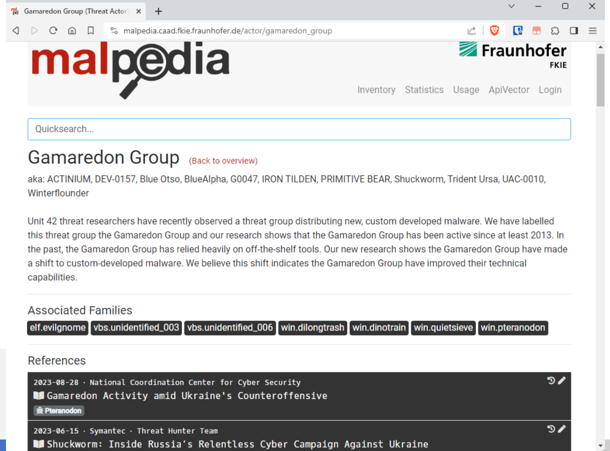


Figure 2. DarkGate infection chain abusing Skype. Click on the button on the right to download the figure.



Gamaredon Group (Threat Actor)
malpedia.caad.fkie.fraunhofer.de/actor/gamaredon_group
malpedia
Fraunhofer FKIE
Inventory
Statistics
Usage
ApiVector
Login
Quicksearch...

Gamaredon Group (Back to overview)

aka: ACTINIUM, DEV-0157, Blue Otso, BlueAlpha, G0047, IRON TILDEN, PRIMITIVE BEAR, Shuckworm, Trident Ursa, UAC-0010, Winterflounder

Unit 42 threat researchers have recently observed a threat group distributing new, custom developed malware. We have labelled this threat group the Gamaredon Group and our research shows that the Gamaredon Group has been active since at least 2013. In the past, the Gamaredon Group has relied heavily on off-the-shelf tools. Our new research shows the Gamaredon Group have made a shift to custom-developed malware. We believe this shift indicates the Gamaredon Group have improved their technical capabilities.

Associated Families

elf.evilgnome vbs.unidentified_003 vbs.unidentified_006 win.dilongtrash win.dinotrain win.quietsieve win.pteranodon

References

2023-08-28 · National Coordination Center for Cyber Security
Gamaredon Activity amid Ukraine's Counteroffensive
Pteranodon

2023-06-15 · Symantec · Threat Hunter Team
Shuckworm: Inside Russia's Relentless Cyber Campaign Against Ukraine

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

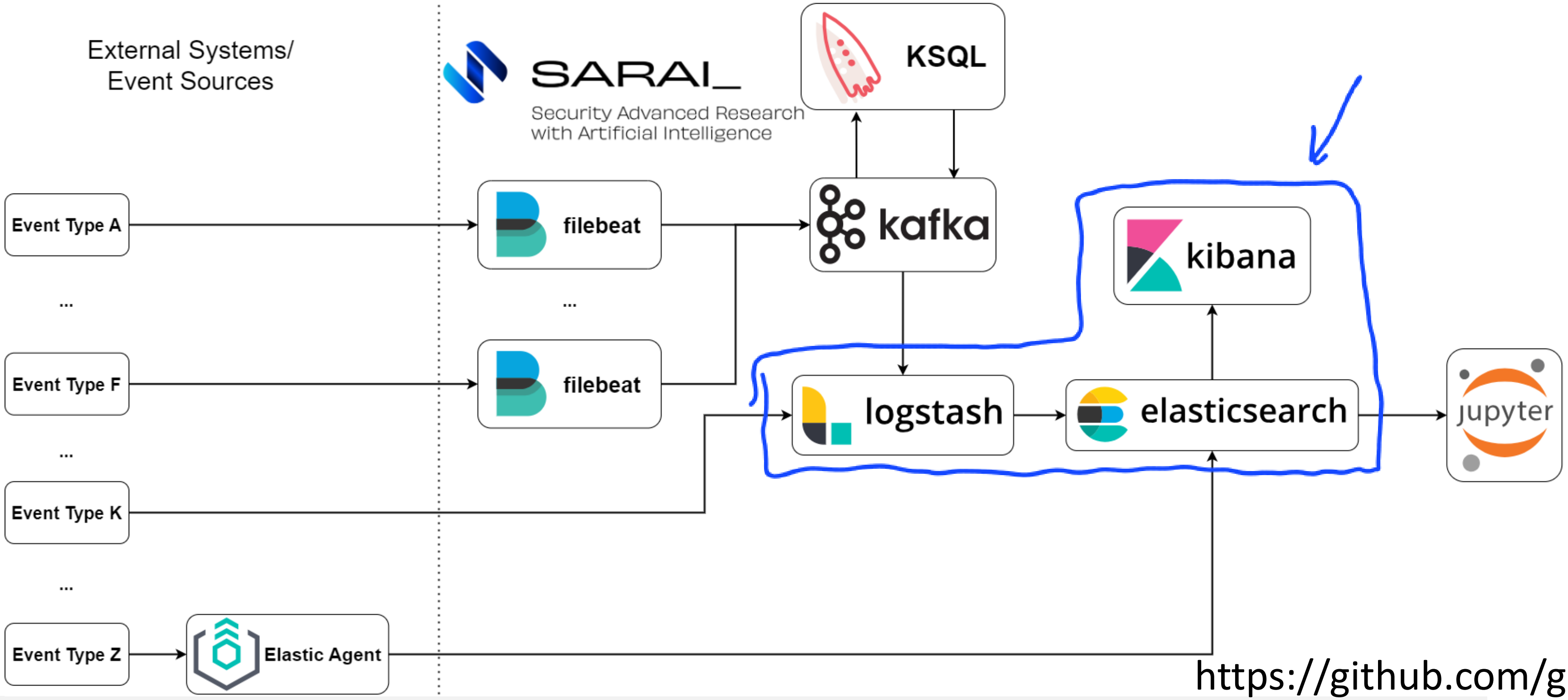
- Focus on relevant data sources to address threats
  - Cannot get all data
  - Visiblity will be limited

- 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

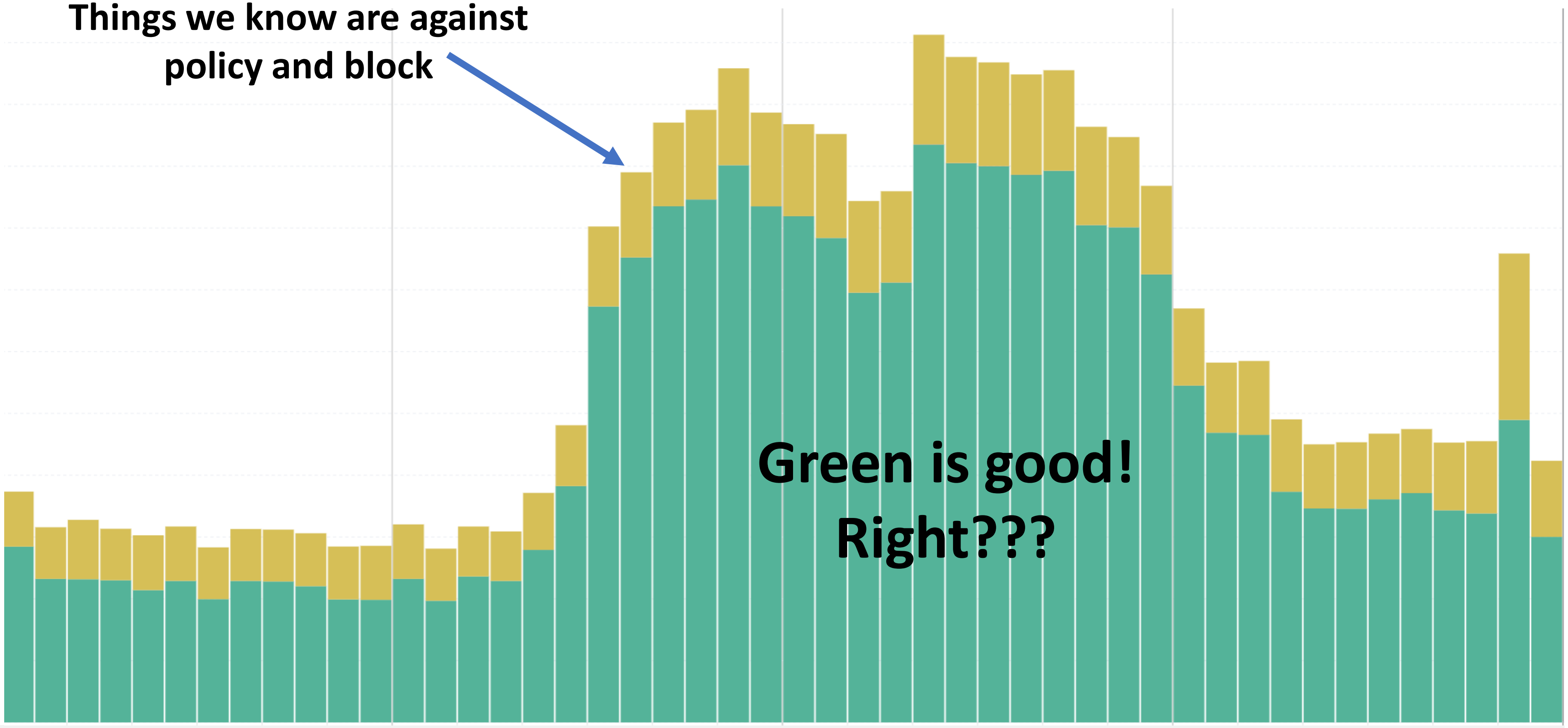


https://github.com/gcsuaveiro/gcs-sarai

Collection: Data Harvesting

Processing: Pain?

Millions of events/hour



Things we know are against policy and block

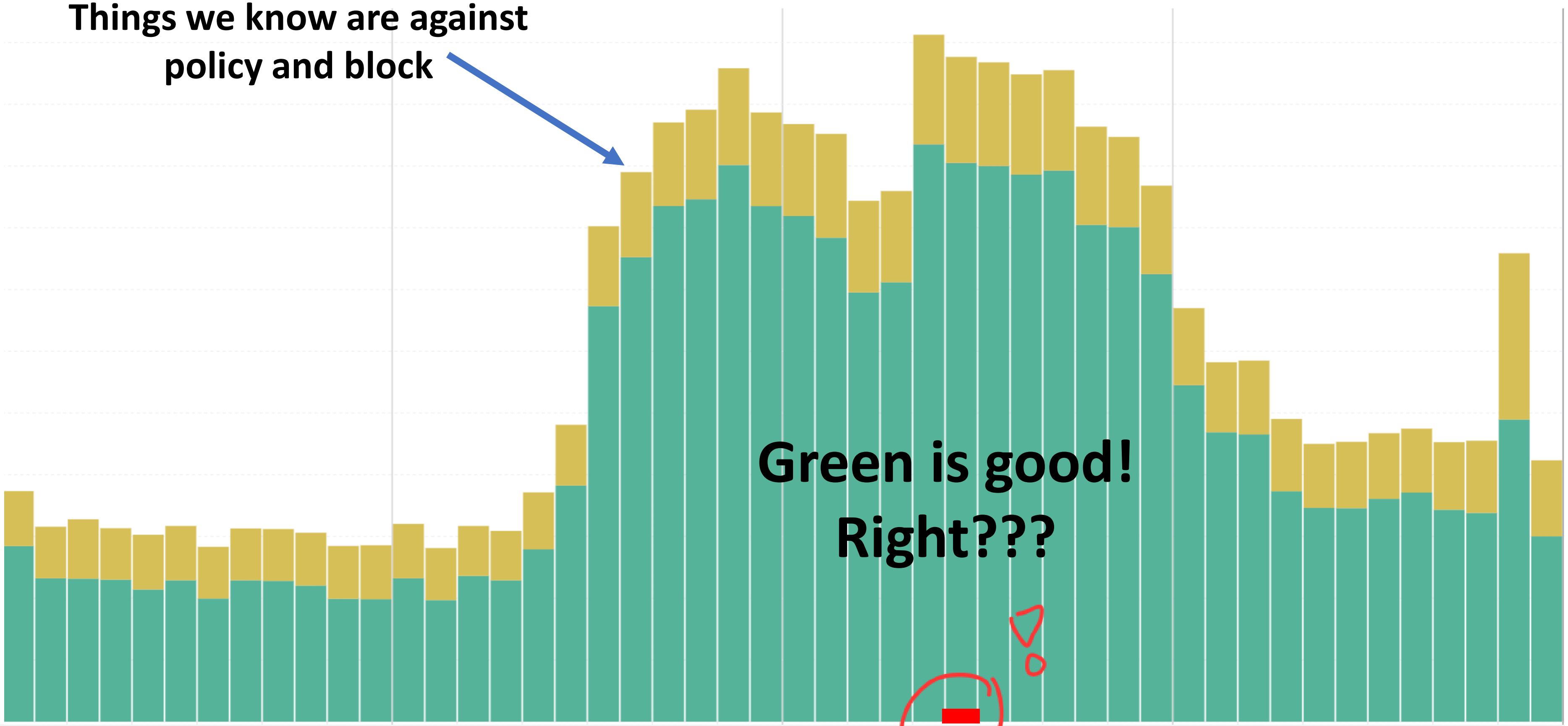
Green is good! Right???

Collection: Data Harvesting

Processing: Pain?

Millions of events/hour

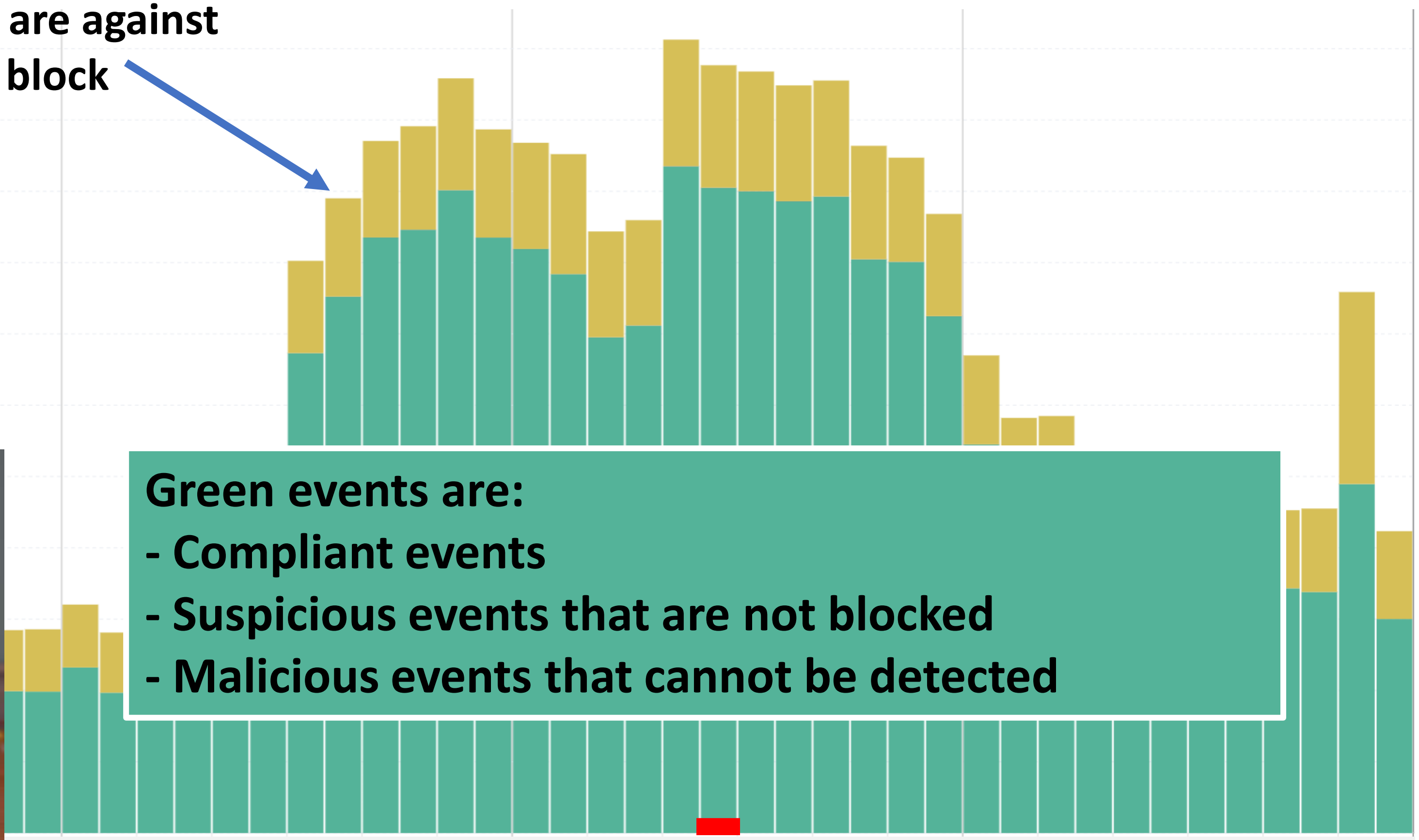
Things we know are against policy and block



Thousands of malicious agents (detect or block)

Collection: Data Harvesting

Processing: Pain?

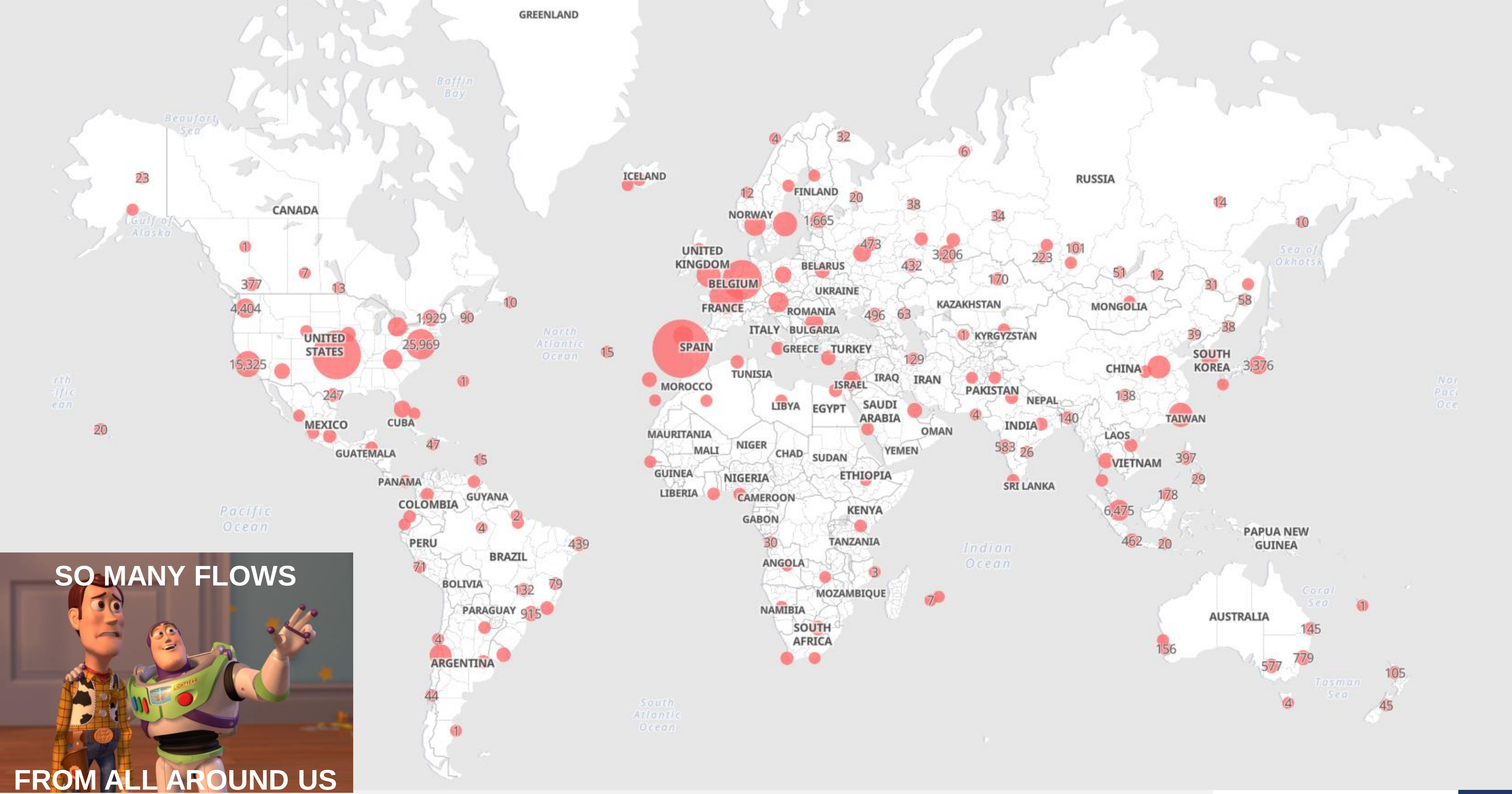


Millions of events/hour

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)



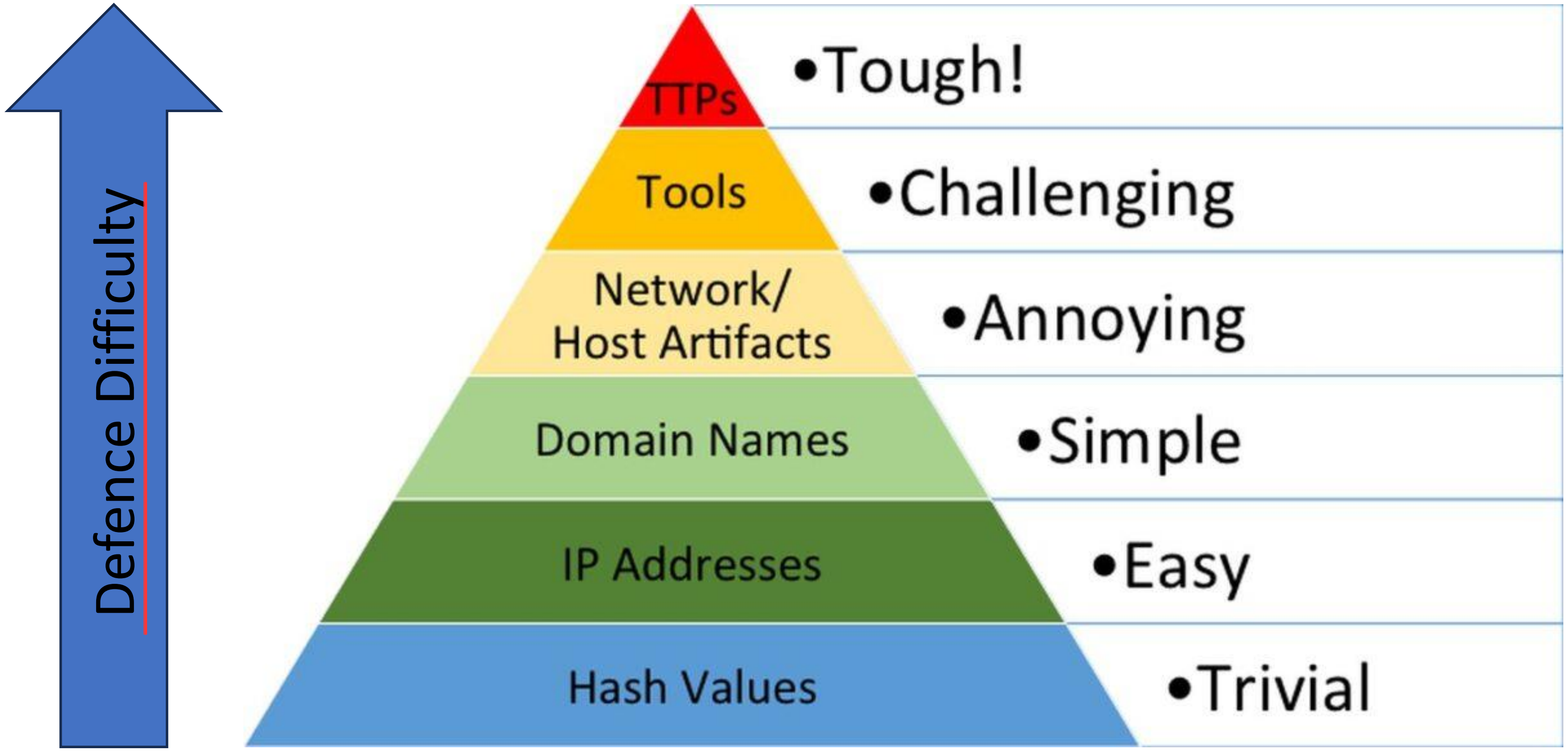
Concepts of Us (Internal) vs others (External) is not robust

“The Pyramid of Pain” (Bianco, 2013)

The Pyramid of Pain

SAI NO TESTE !

Para detetar . . .



Implementar o mais fácil

- 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

TESTE

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

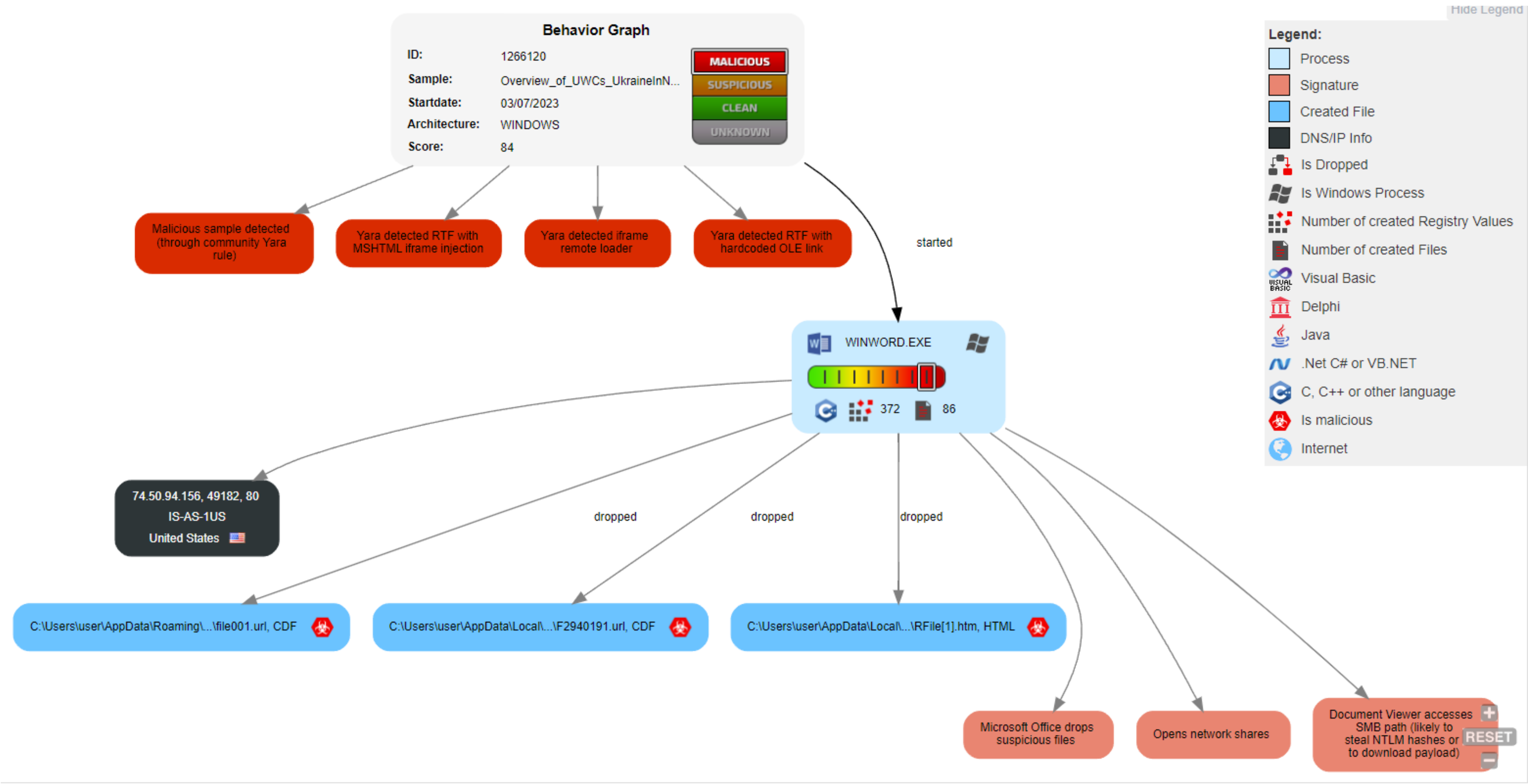
Threat Research

- 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

Joe Sandbox



Behavior Graph

ID: 1266120

Sample: Overview_of_UWCs_UkraineInN...

Startdate: 03/07/2023

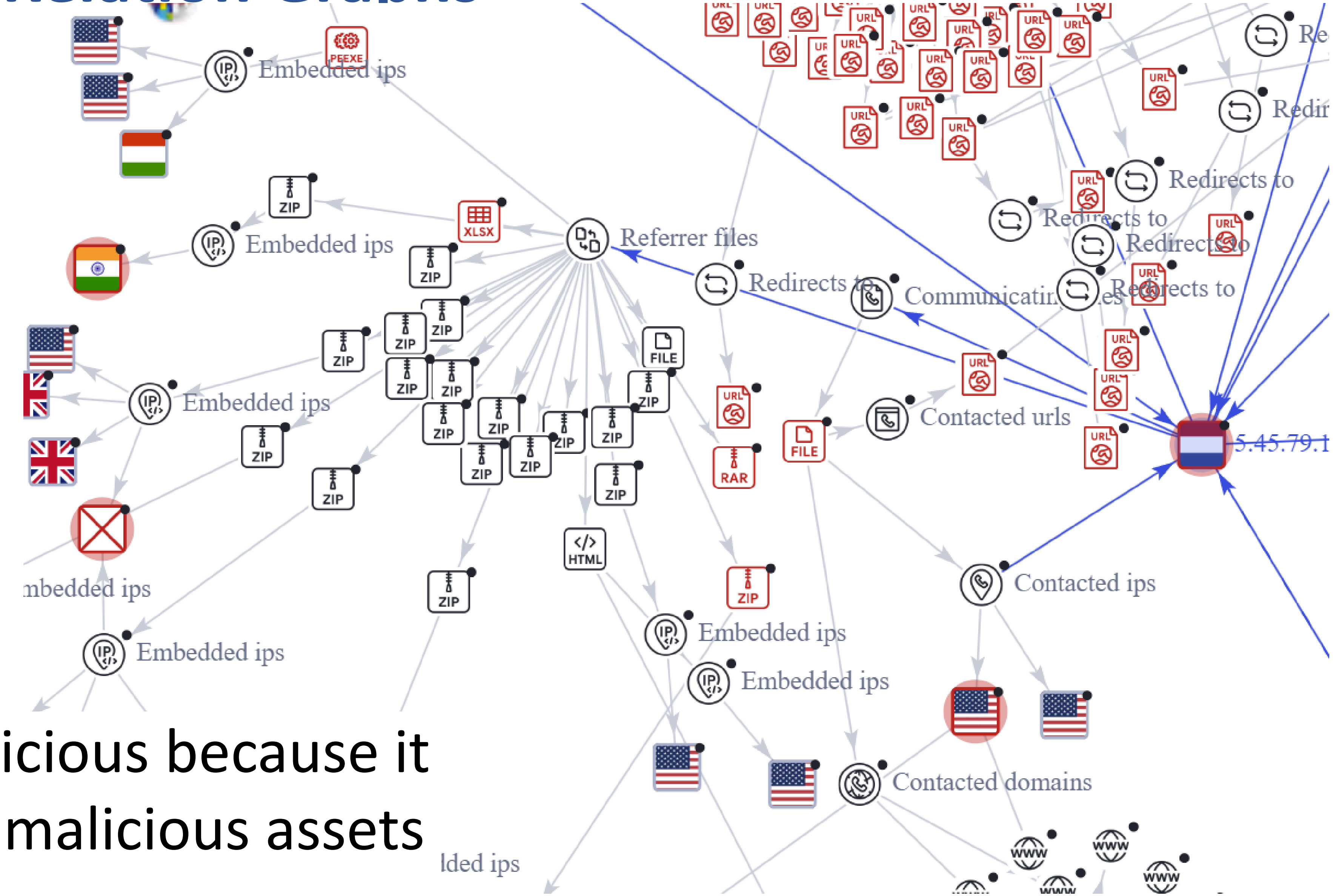
Architecture: WINDOWS

Score: 84

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Malicious sample detected (through community Yara rule)
Yara detected RTF with MSHTML iframe injection
Yara detected iframe remote loader
Yara detected RTF with hardcoded OLE link
started
WINWORD.EXE
372
86
74.50.94.156, 49182, 80
IS-AS-1US
United States
dropped
dropped
dropped
C:\Users\user\AppData\Roaming\...\file001.url, CDF
C:\Users\user\AppData\Local\...\F2940191.url, CDF
C:\Users\user\AppData\Local\...\RFile[1].htm, HTML
Microsoft Office drops suspicious files
Opens network shares
Document Viewer accesses SMB path (likely to steal NTLM hashes or to download payload)
RESET
Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

Threat Research: Relation Graphs

Virus Total



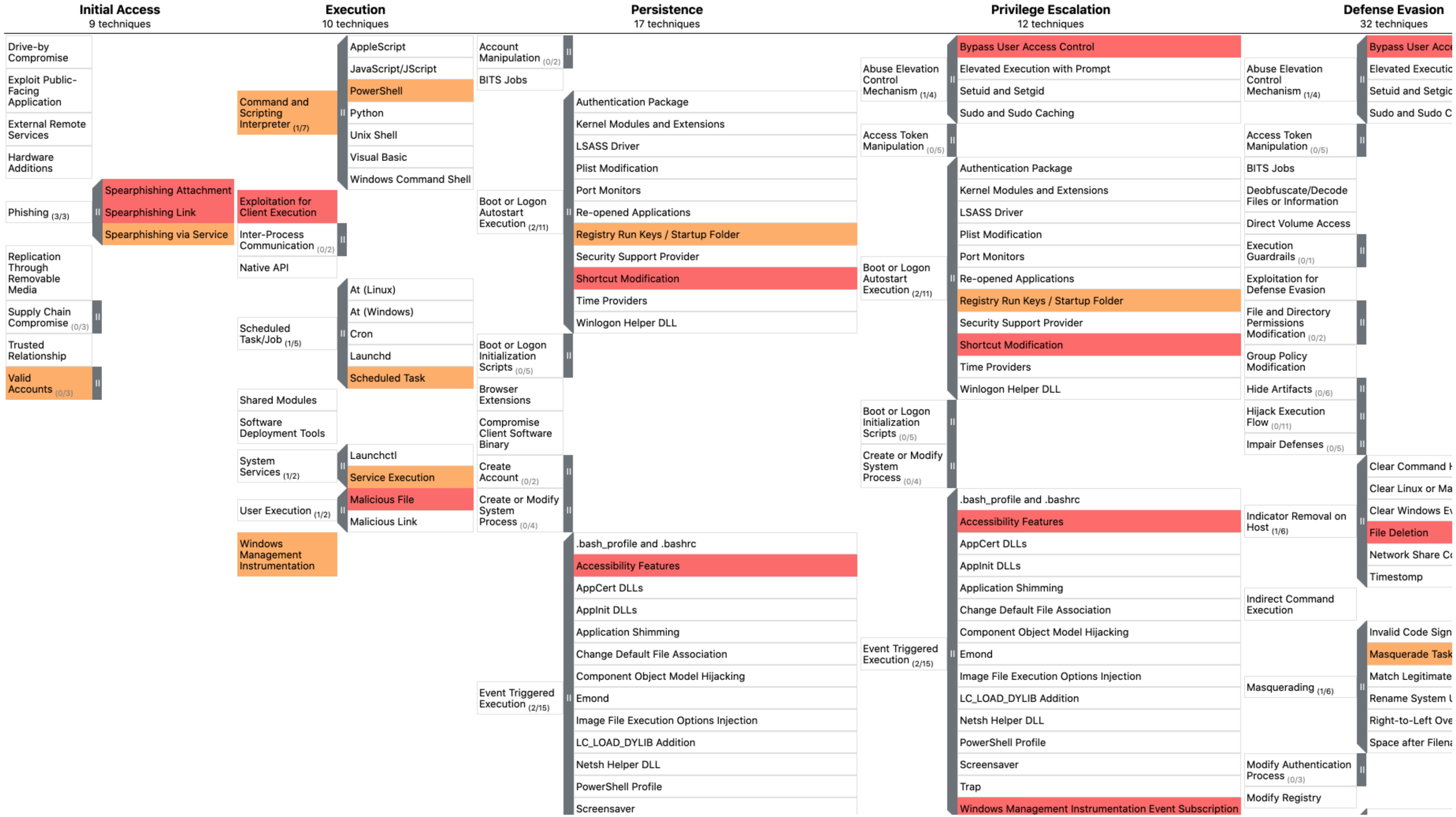
- Some become suspicious because it contacts/has other malicious assets

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

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution
10 techniques

- Command and Scripting Interpreter (1/7)
  - AppleScript
  - JavaScript/JScript
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (1/5)
  - At (Linux)
  - At (Windows)
  - Cron
  - Launchd
  - Scheduled Task
- Shared Modules
- Software Deployment Tools
- System Services (1/2)
  - Launchctl
  - Service Execution
- User Execution (1/2)
  - Malicious File
  - Malicious Link
- Windows Management Instrumentation

Persistence
17 techniques

- Account Manipulation (0/2)
- BITS Jobs
- Boot or Logon Autostart Execution (2/11)
  - Authentication Package
  - Kernel Modules and Extensions
  - LSASS Driver
  - Plist Modification
  - Port Monitors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/15)
  - .bash_profile and .bashrc
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Change Default File Association
  - Component Object Model Hijacking
  - Emond
  - Image File Execution Options Injection
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - PowerShell Profile
  - Screensaver

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (1/4)
  - Bypass User Access Control
  - Elevated Execution with Prompt
  - Setuid and Setgid
  - Sudo and Sudo Caching
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (2/11)
  - Authentication Package
  - Kernel Modules and Extensions
  - LSASS Driver
  - Plist Modification
  - Port Monitors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/15)
  - .bash_profile and .bashrc
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Change Default File Association
  - Component Object Model Hijacking
  - Emond
  - Image File Execution Options Injection
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - PowerShell Profile
  - Screensaver
  - Trap
  - Windows Management Instrumentation Event Subscription

Defense Evasion
32 techniques

- Abuse Elevation Control Mechanism (1/4)
  - Bypass User Acce
  - Elevated Executic
  - Setuid and Setgic
  - Sudo and Sudo C
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/6)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/5)
- Indicator Removal on Host (1/6)
  - Clear Command I
  - Clear Linux or Ma
  - Clear Windows Ev
  - File Deletion
  - Network Share Co
  - Timestomp
- Indirect Command Execution
- Masquerading (1/6)
  - Invalid Code Sign
  - Masquerade Task
  - Match Legitimate
  - Rename System U
  - Right-to-Left Ove
  - Space after Filena
- Modify Authentication Process (0/3)
- Modify Registry