Defending an Organization

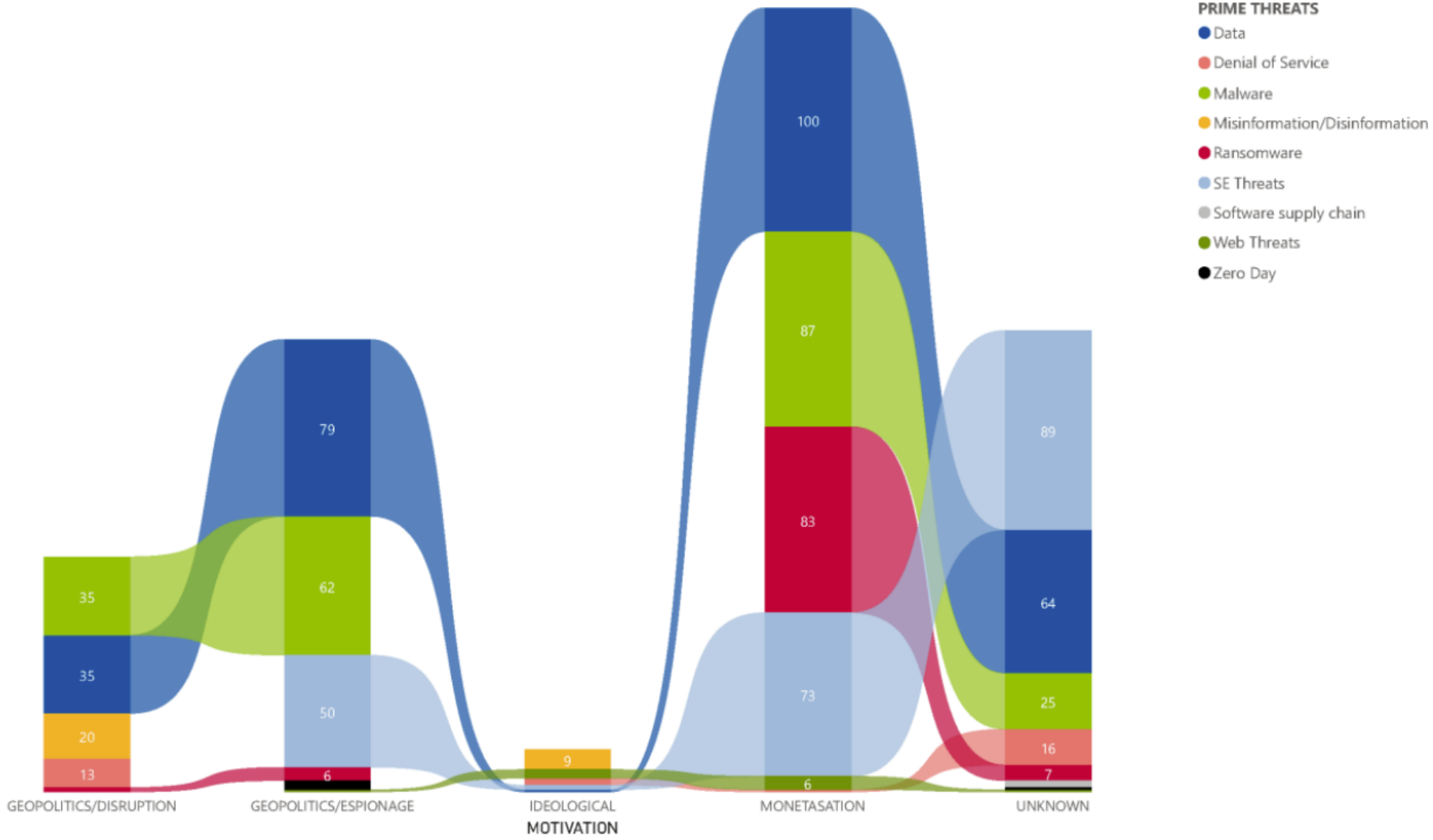
The current organizational landscape

- **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 highly motivated and organized



The current organizational landscape

- **Must comply with new regulatory frameworks**
  - 2016: NIS – Defines basic cybersec requirements
  - 2018: GDPR – Defines requirements for private data
    - Introduces fines for lack of proper data management
  - 2021: DL65 – Defines processes for inventory, reporting, formalize strategy
  - 2024: NIS 2 – Defines cyber teams and processes
    - Introduces fines for lack of security

- **Strategies are based on risk and maturity**
  - Risk: identify assets and determine their risk
  - Maturity: determine organization maturity over multiple áreas
    - Evolve all as adequate

Current requirements

1. **Identify security accountable individual**
   - Responsible for the Security Strategy
   - Typically called CISO: Chief Information Security Officer
   - Will be personally held accountable!
2. **Identify contact points for the organization**
3. **Identify and track the critical assets**
   - Crown Jewels
4. **Have a security plan**
5. **Report relevant incidents and cooperate**

Assets: Crown Jewels Approach

- **Focused on identifying and protecting the most critical assets**
  - To the organization mission!
- **What is a crown jewel?**
  - Sensitive Data
  - Servers
  - Software Systems
  - Any other equipment (HVAC, Generators…)
- **Disruption to the crown jewels will pose a serious impact to the organization mission**
- **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 and Coordination

- **Incident response coordinated by**
  - Relevant incidents must be reported

- **National CSIRT Network facilitates collaboration between entities**
  - https://www.redecsirt.pt

- **Fraud/Crime incidents are reported to authorities**
  - **Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T): unc3t@pj.pt**

Cybersecurity at UA

- **Data: DPO (Data Protection Officer)**
  - https://www.ua.pt/pt/rgpd/page/24346
- **Strategy and Support: Cybersecurity Office**
  - https://www.ua.pt/ciberseguranca
- **Incident Response: the CSIRT@UA part of RNCSIRT**
  - https://www.ua.pt/pt/ciberseguranca/rfc2350
- **Research: several projects and thesis**
- **Education and Training:**
  - Cybersecurity in Teaching Units (DETI)
  - Masters in Cybersecurity (DETI)
  - Higher Professional Training Course in Cybersecurity (ESTGA)
  - Courses with CNCS C-Academy and at UNAVE

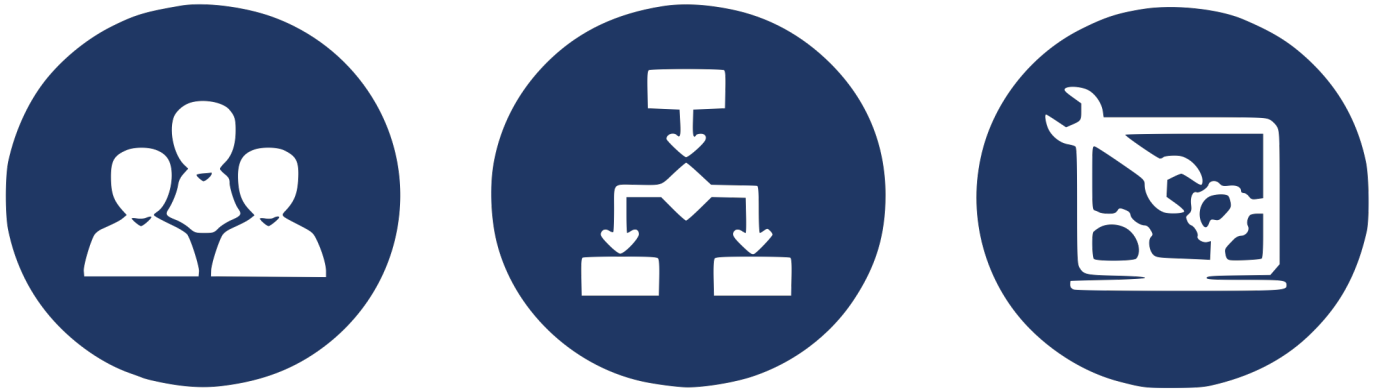
Security Teaming

- **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 defence 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

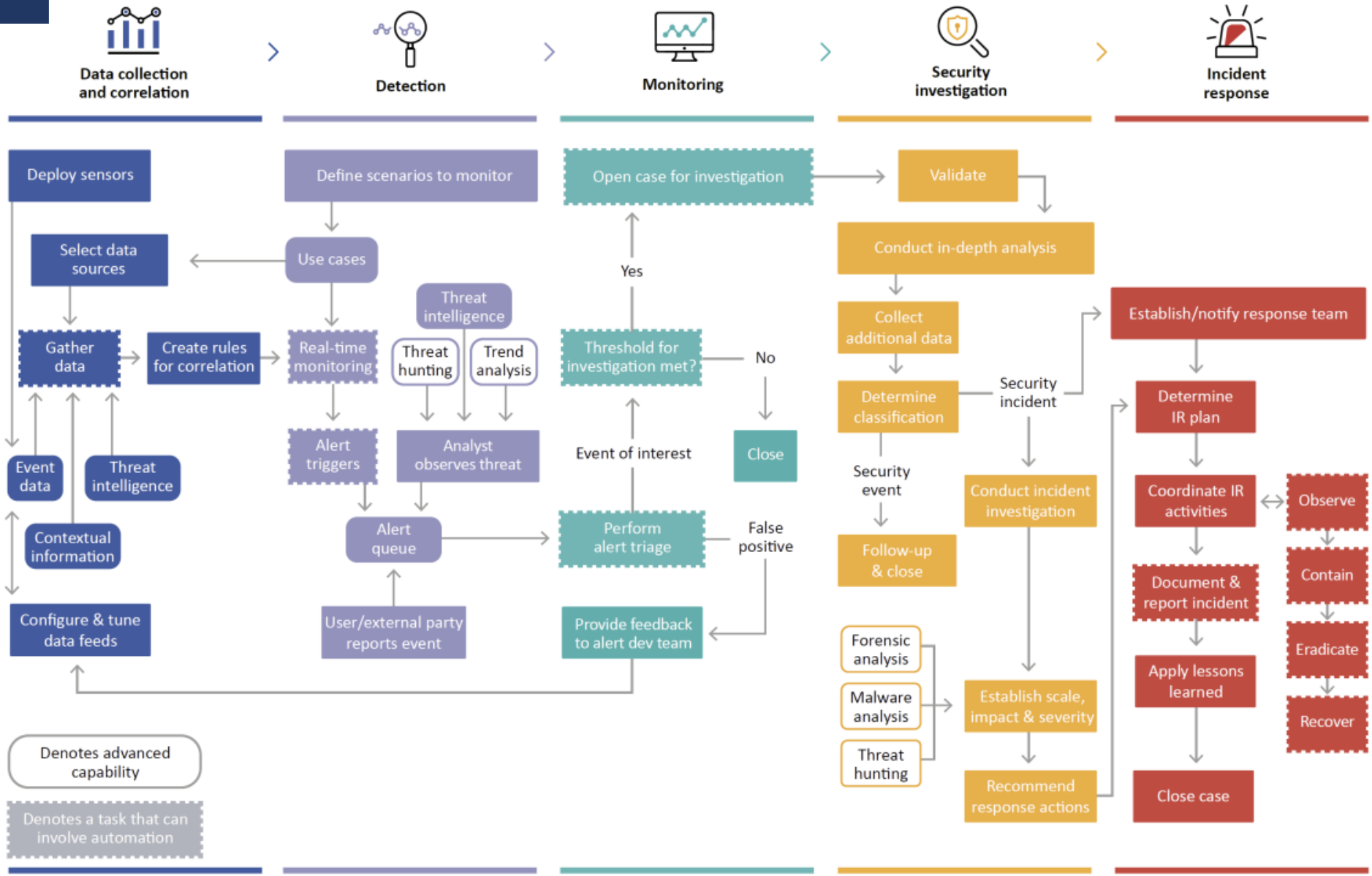
- **Challenging and interesting**
  - Many topics to address: prog, forensics, AI/ML, training…
  - Continuously evolving with new techniques and tools

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
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

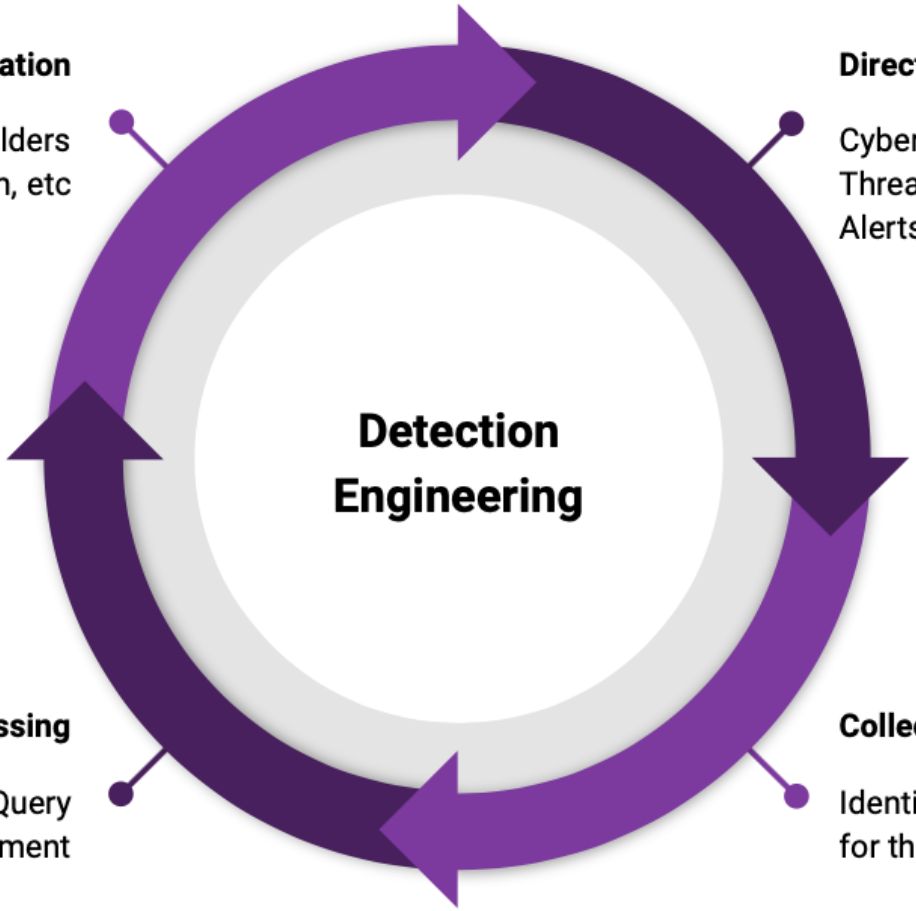
Main concepts

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

- **Incident Response**
  - Have processes to handle incidents
  - Involve stakeholders and communicate

- **Detection Engineering**
  - designing, developing, testing, and maintaining threat detection logic

Detection Engineering

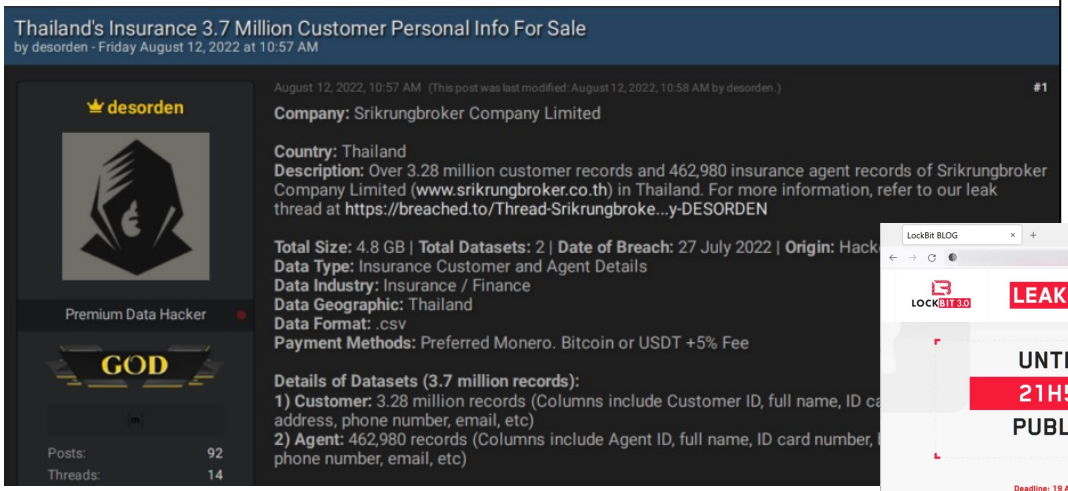


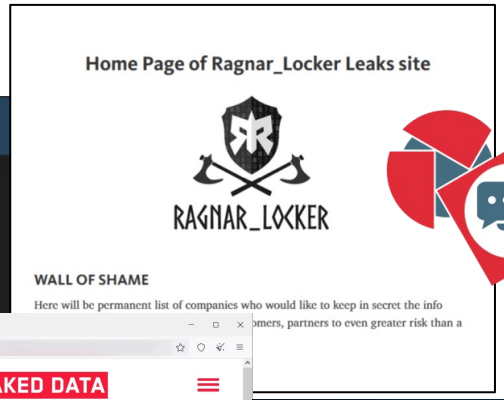
Source: SANS

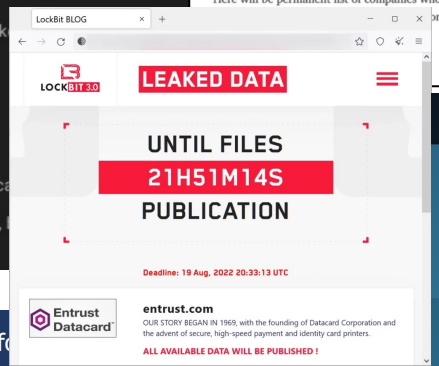
Direction: CTI

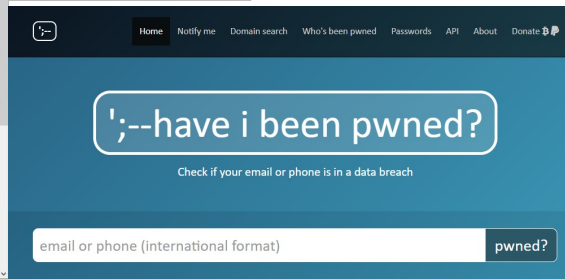
Assess the current threats from CTI

- **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)
  - Attacks to similar organizations





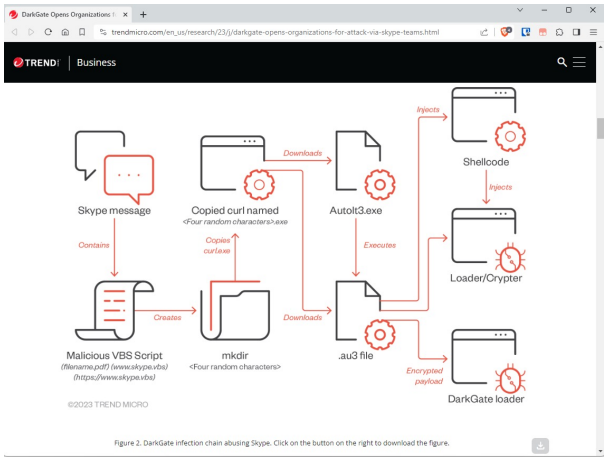


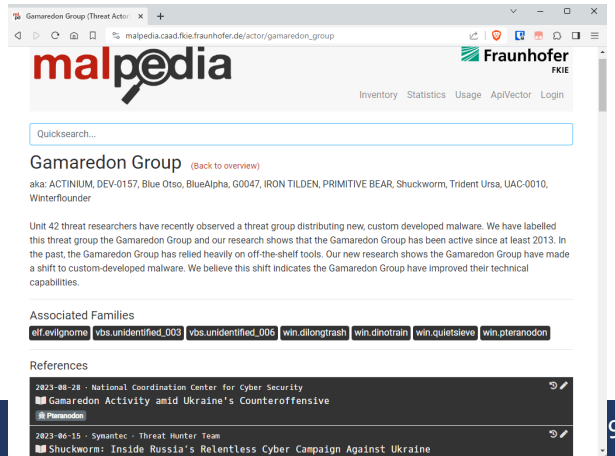


Direction: CTI

Assess the current threats from CTI

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





Direction: Alerts and Incidents

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

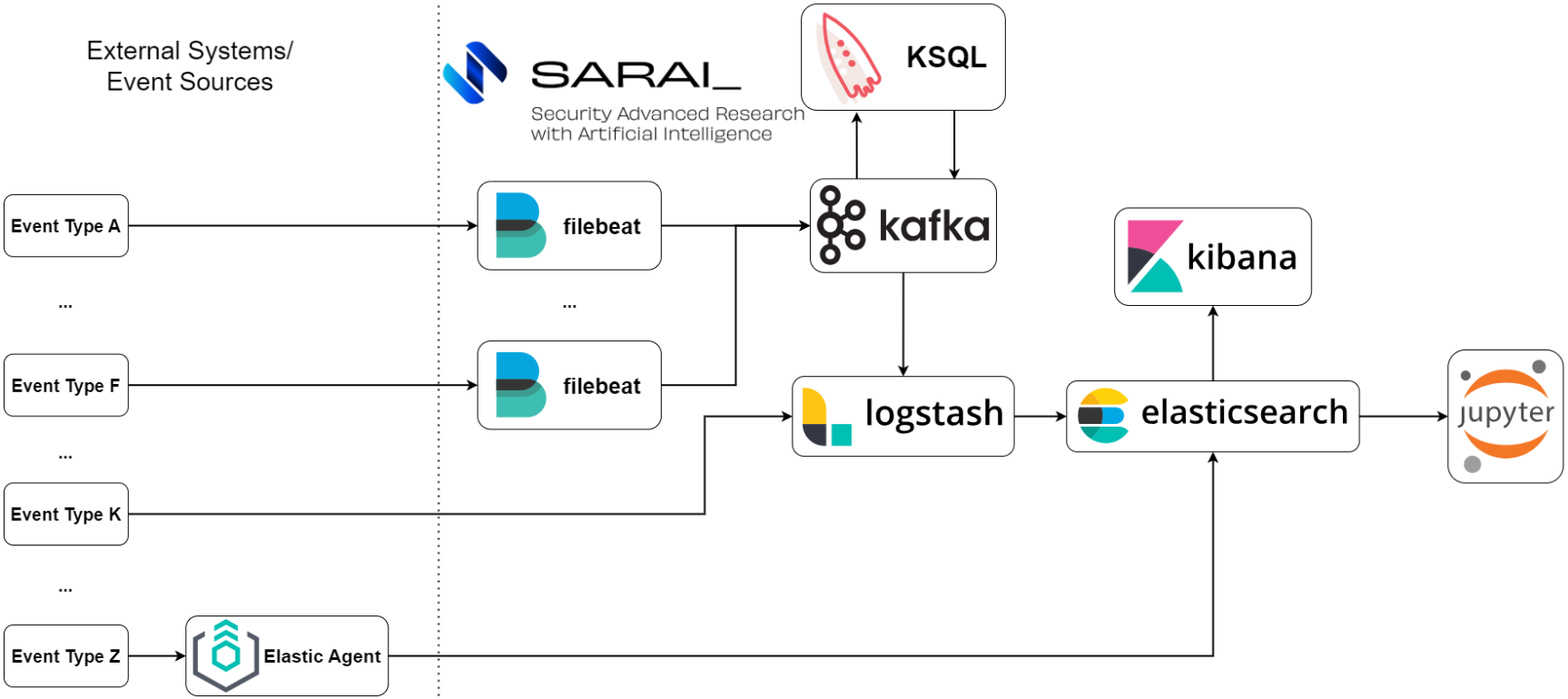
Collection: Data Harvesting

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

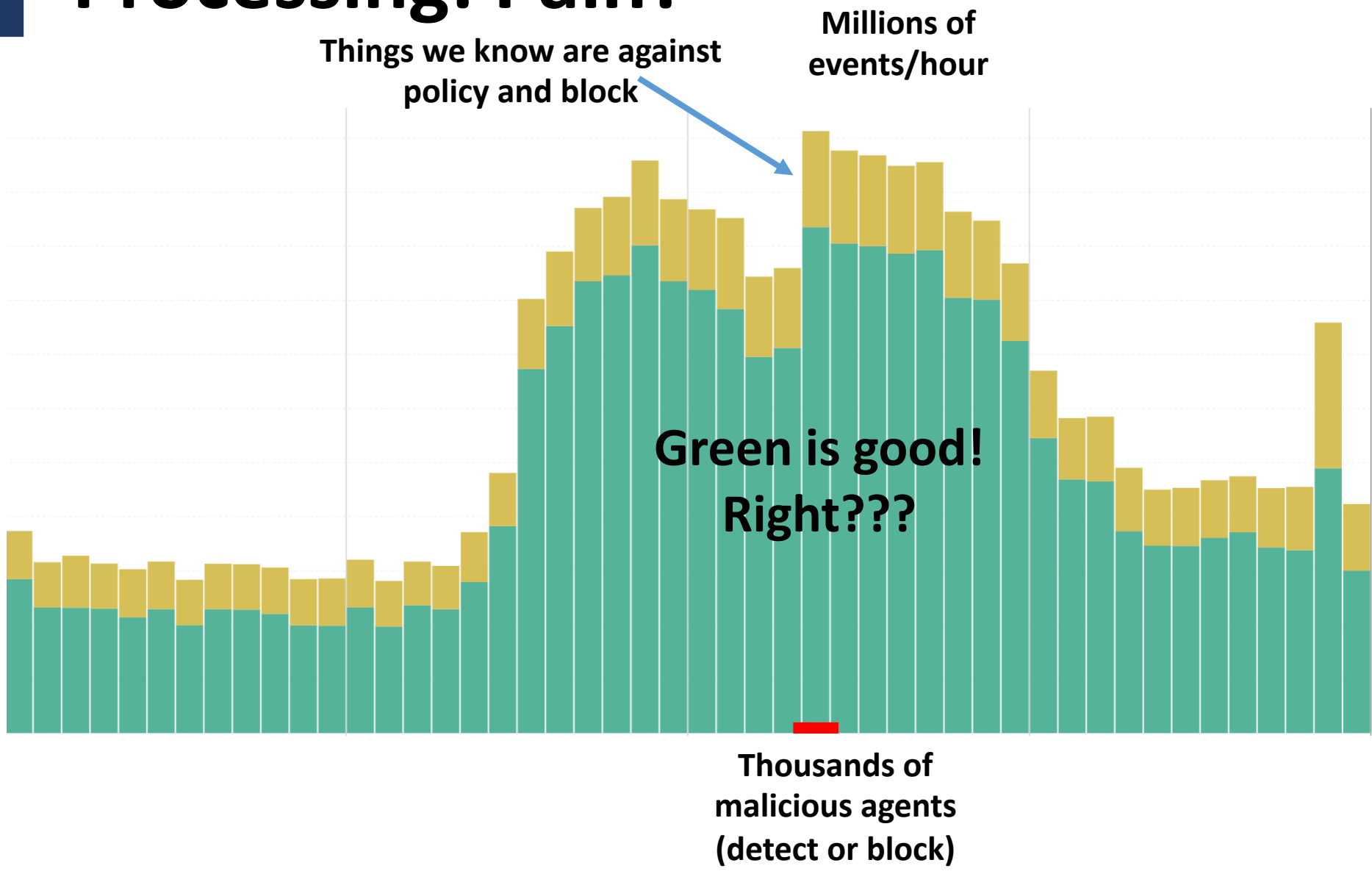
Collection: Data Harvesting

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

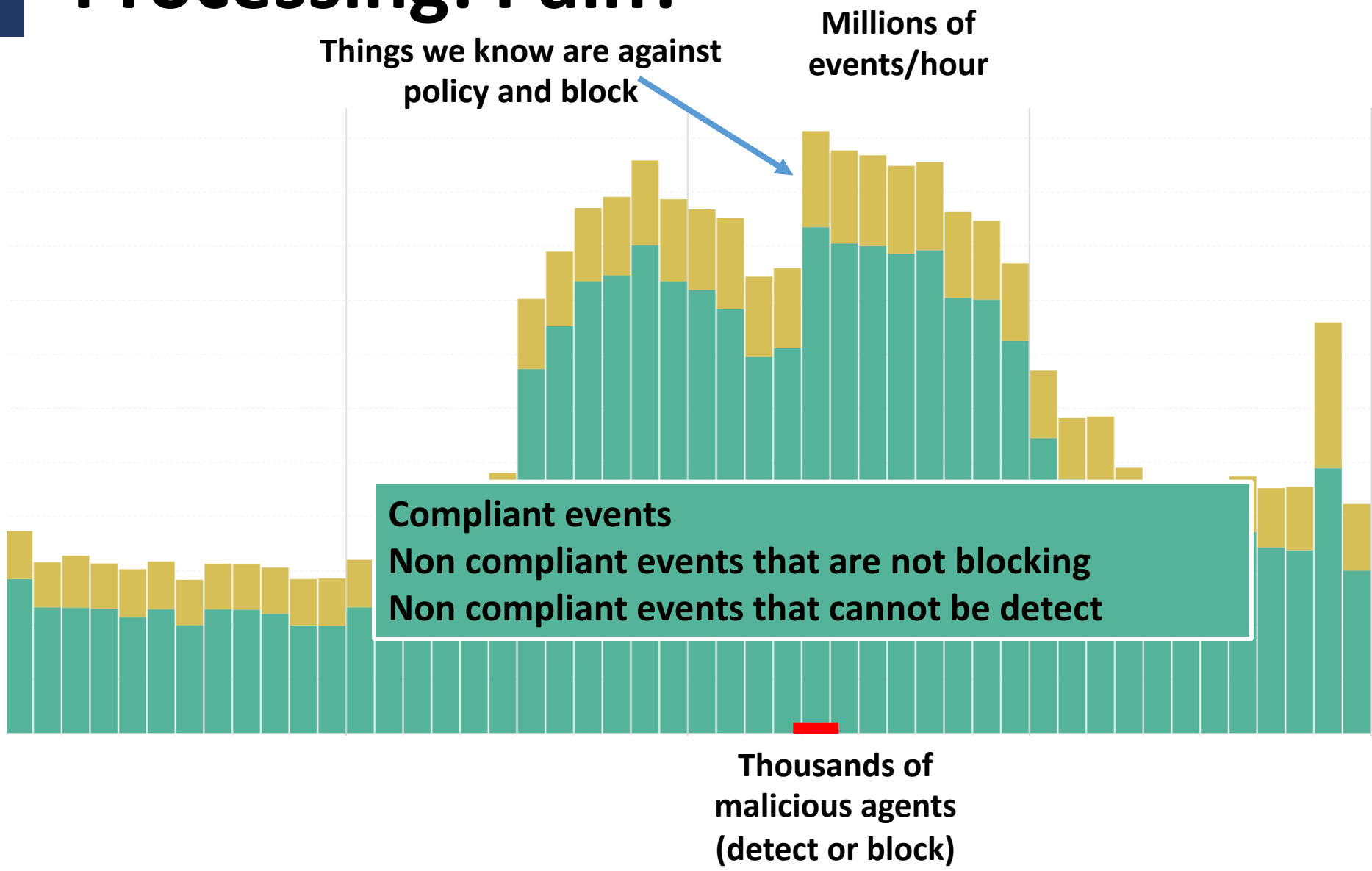


https://github.com/gcsuaveiro/gcs-sarai

Processing: Pain?



Processing: Pain?



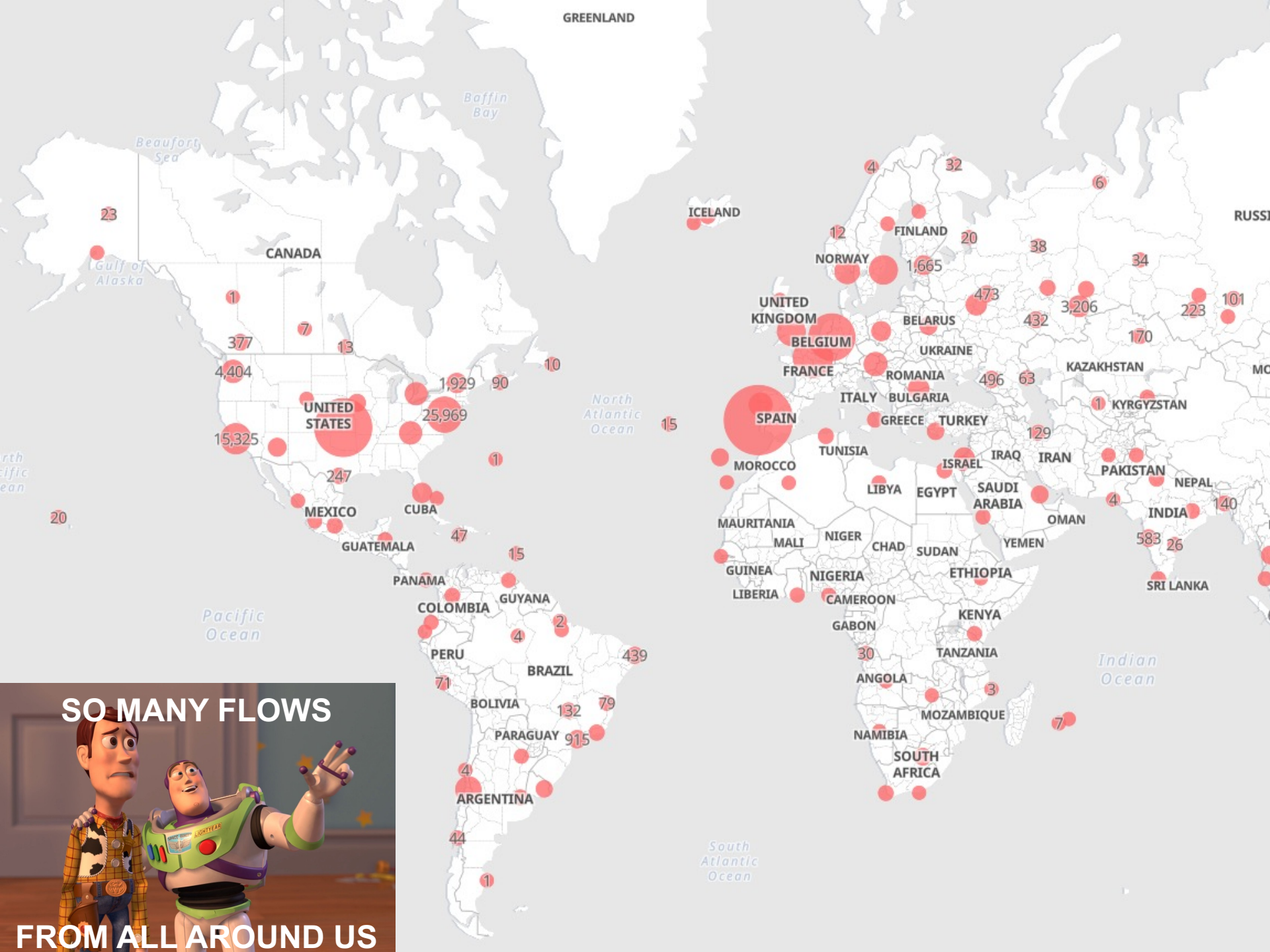
Processing: Pain?

Things we know are against policy and block

Millions of events/hour

Things we know
Things we know we do not know
Things we do not know we do not know

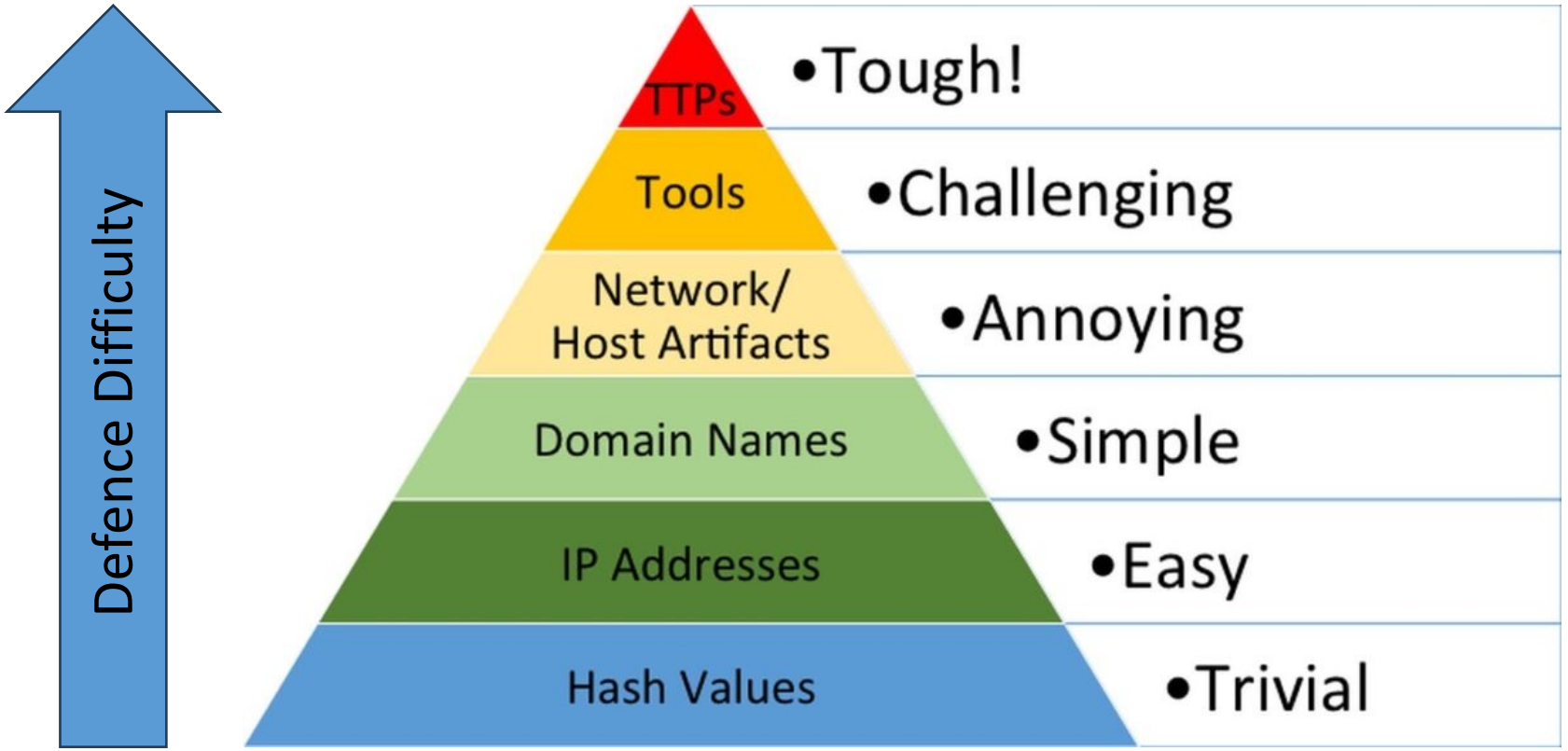
Thousands of malicious agents (detect or block)



SO MANY FLOWS

FROM ALL AROUND US

The Pyramid of Pain



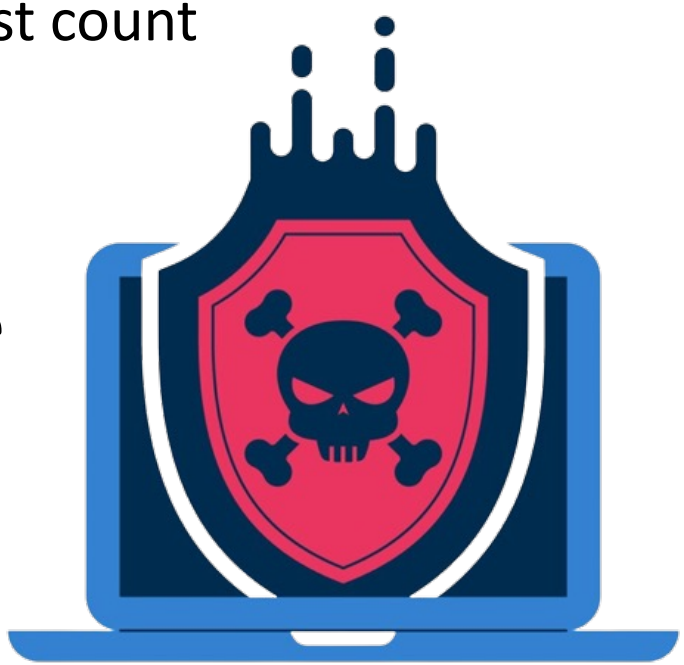
- Increase defence capabilities from the bottom to the top
- Why?
  - Detecting files/emails by comparing hashes is trivial
  - Understanding how actors behave is very difficult

Triage

- **One of an analyst's most important tasks**
  - You will likely never have only one option
- **Think like an ER doctor / emergency dispatcher**
  - Limited resources
  - Multiple problems
- **Where do you start?**
- **Pick the most dangerous alert**
  - Main goal, although it is difficult to chose

Definition of Dangerous

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



How to find threats?

- **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

How to find threats?

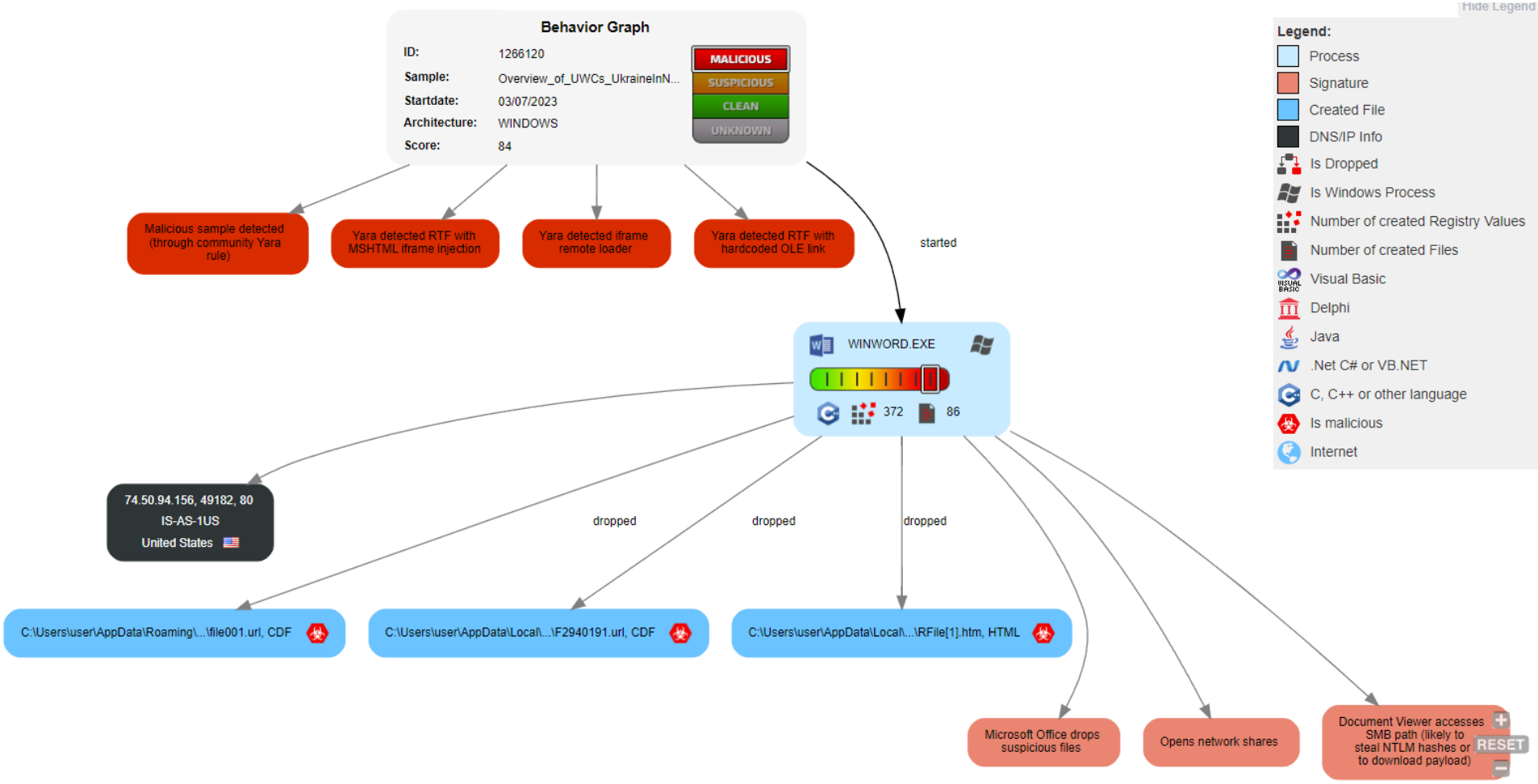
- **What if we do not know if something is malicicous?**
  - What is a malicious website or file?
- **New malware potentially has high impact**
  - It is not detected by Anti-virus
  - Explores unpatched vulnerabilities or flaws (0 day)
- **A new malicious asset is just a new program/website**
  - May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

Threat Research

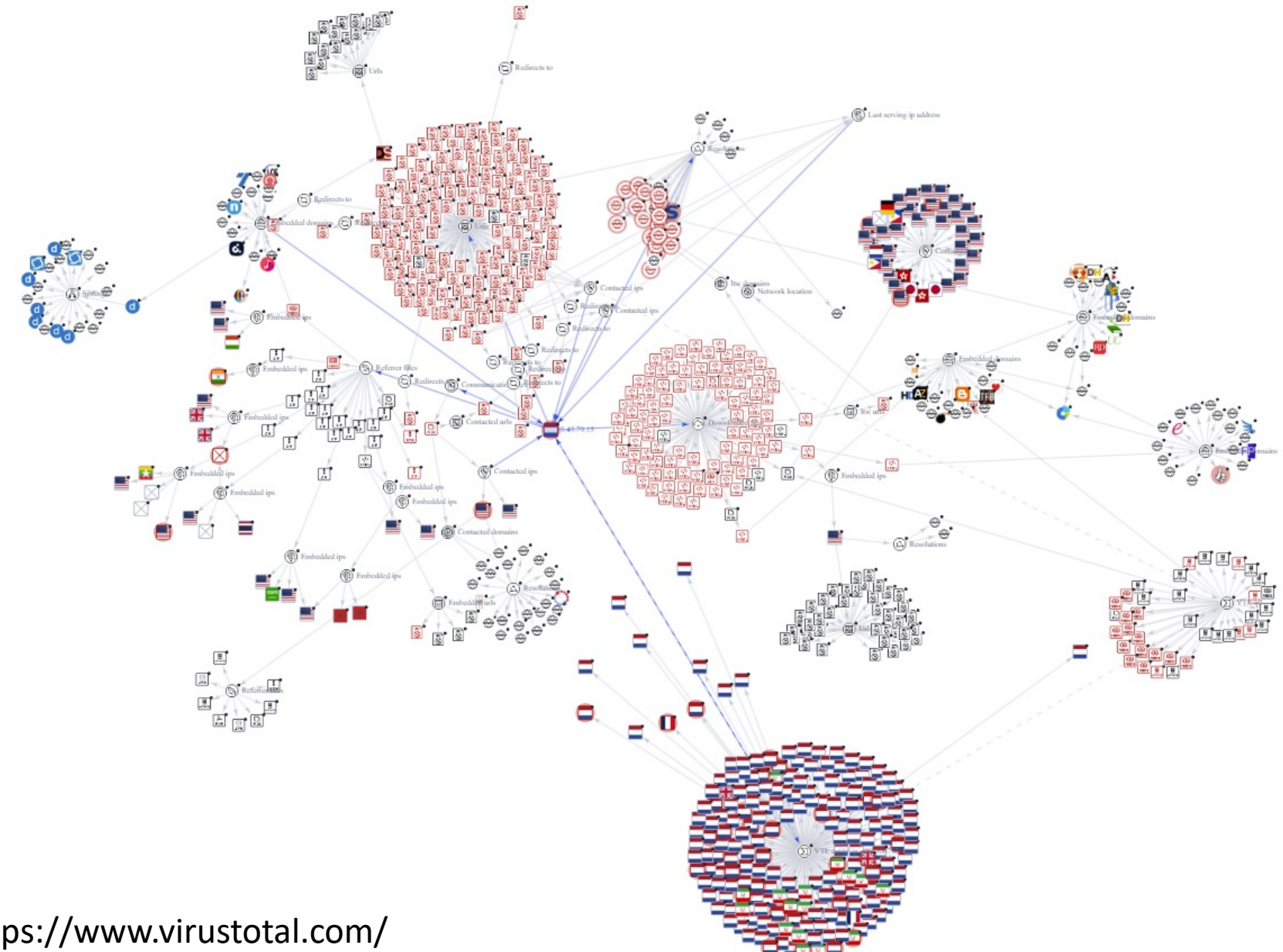
- **Threat Research allows detection of new offenses**
  - Takes a Indicator and determines its risk

- **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

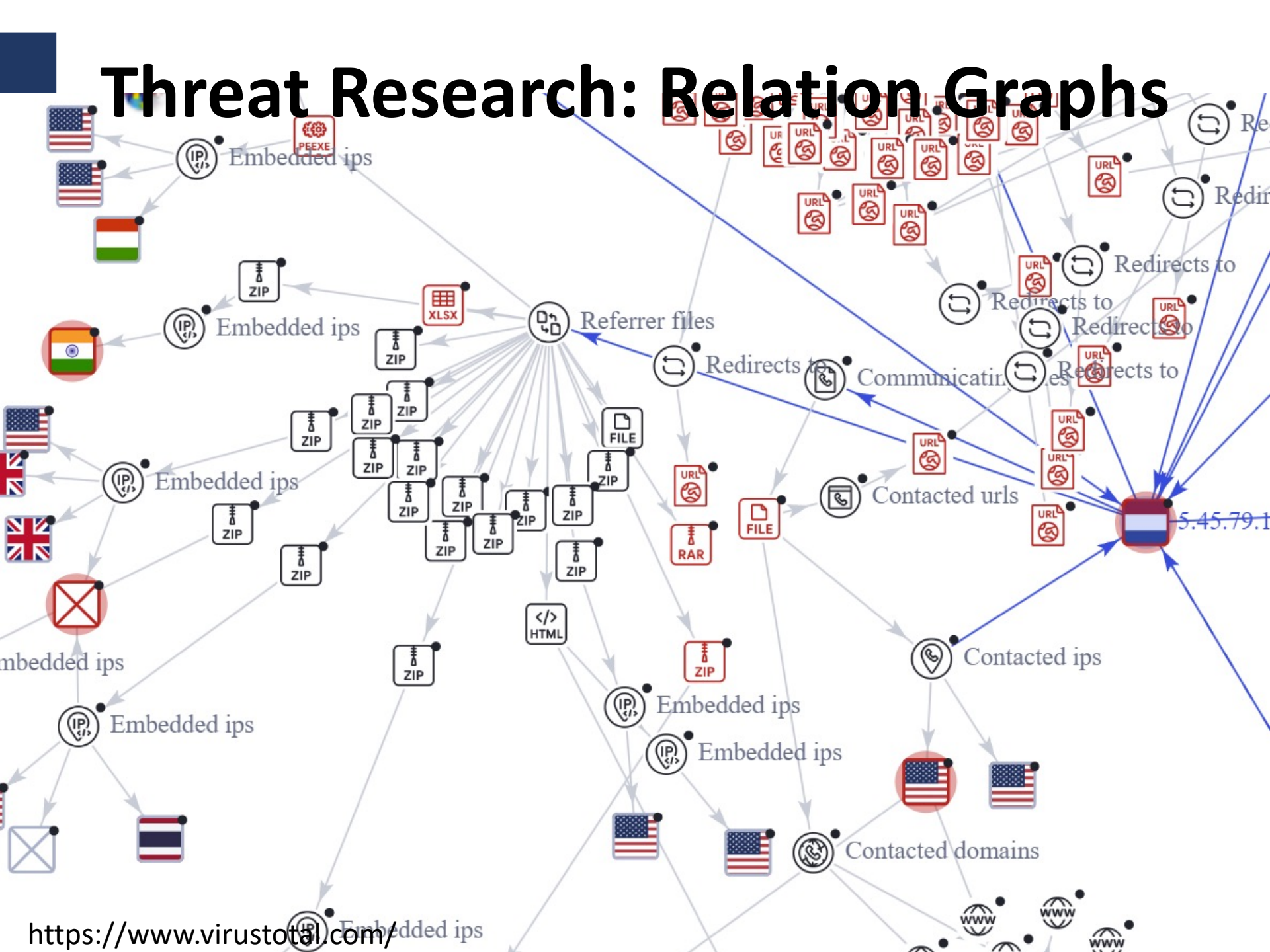


Threat Research: Relation Graphs



https://www.virustotal.com/

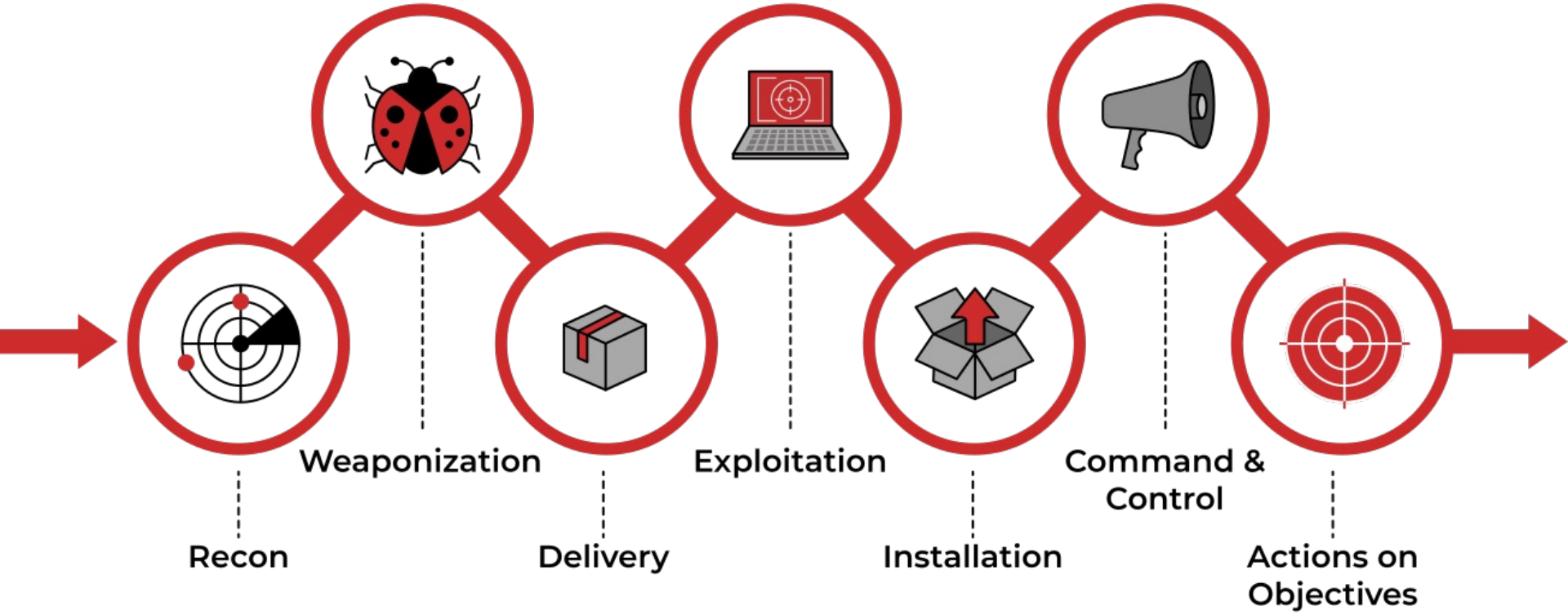
Threat Research: Relation Graphs



https://www.virustotal.com/

Think like a hacker

- **Lockheed Martin Cyber Kill Chain**
  - Helps understand and combat ransomware, security breaches, and advanced persistent attacks (APTs)

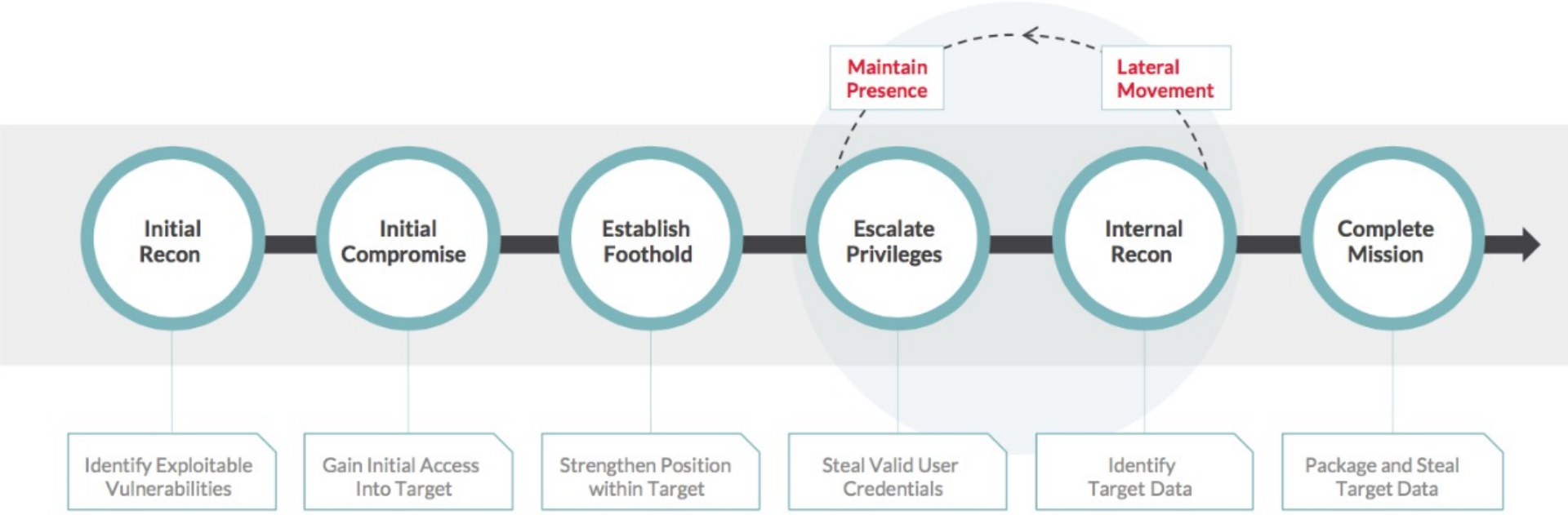


Think like a hacker

1. Enumerating employees, services, among others
2. Creating file with exploit included
3. Transferring exploit to victim
4. Asset exploited, unauthorized code run
5. Malicious code executes/installs
6. Remote control of asset
7. Exfil/destroy data, disrupt process, etc.

Think like a hacker

- Similar to the Lockheed Martin Cyber Kill Chain
- Emphasizes the iterative nature of compromise
- More literal steps

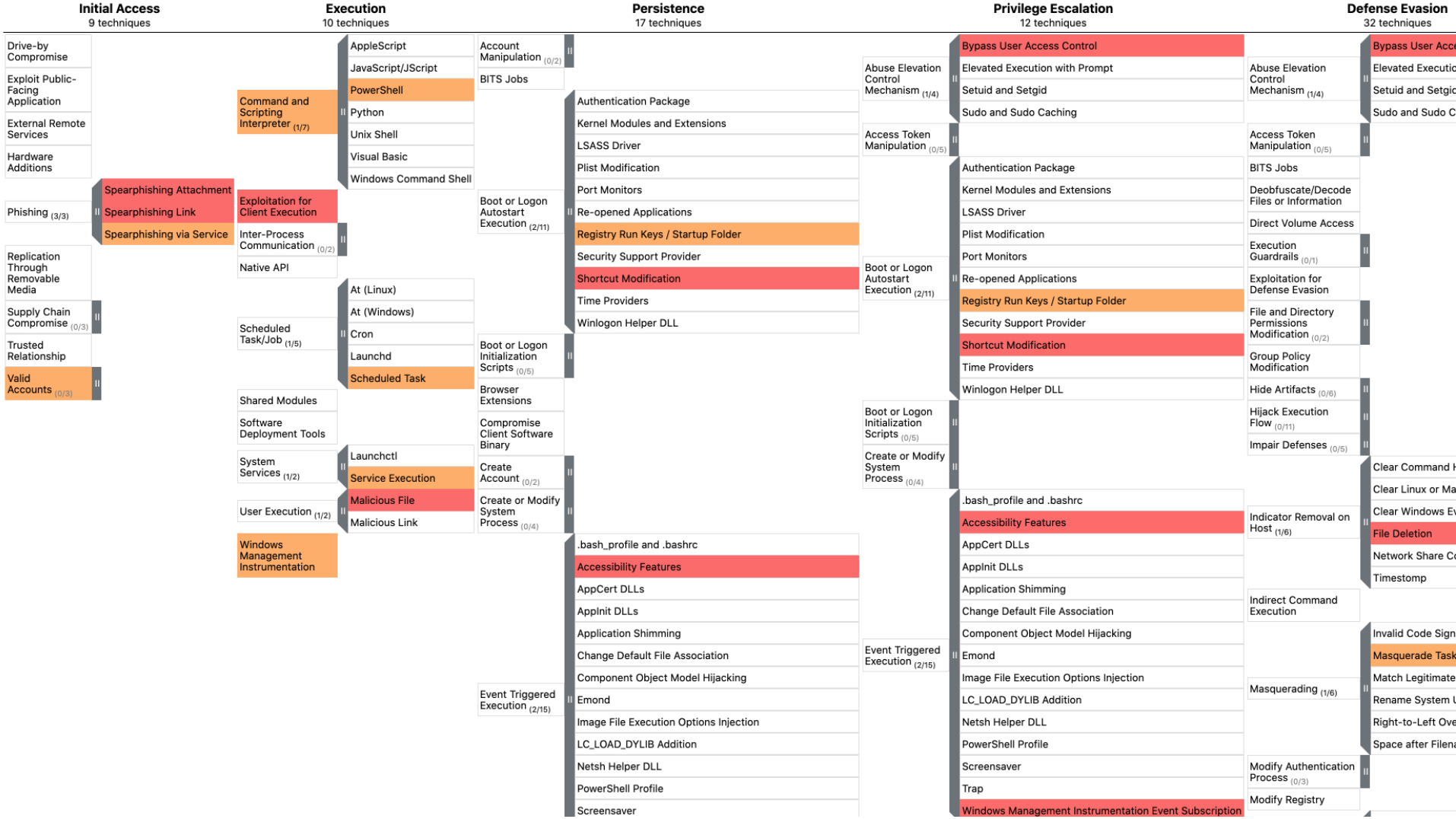


MITRE Att&ck Matrix

- **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

https://attack.mitre.org


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)
.bash_profile and .bashrc
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Change Default File Association
Component Object Model Hijacking
Event Triggered Execution (2/15)
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)
.bash_profile and .bashrc
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Change Default File Association
Component Object Model Hijacking
Event Triggered Execution (2/15)
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 Executio
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 H
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

Data exfiltration clues

- **High-volume of traffic**
  - DNS tunnelling
  - From unusual source
  - Long connection time to odd destination
- **Questionable compressed archive creation**
- **Multiple port firewall denies outbound from a single source**
- **URLs with long unexplained parameters**
- **DLP alerts**
  - Data Loss Prevention tools
- **UEBA alerts**
  - User Entity and Behaviour Analytics

Data destruction clues

- Compromise of patching servers
- Unusual file deletions
- Sudden system slowness or crashes
- Abnormal system and network behaviour

Attack identification

- **Domains, IP addresses or URLs**
  - Matching to APT
  - Domains unknown
    - To all OSINT sources
- **Email tailored to a specific person**
- **Suspicious information about business**
- **New executables**
  - Never been seen before anywhere
  - Customized attack files

Exploit alert triage

- **Prioritization**
  - How to do it? Which alerts we should prioritize?

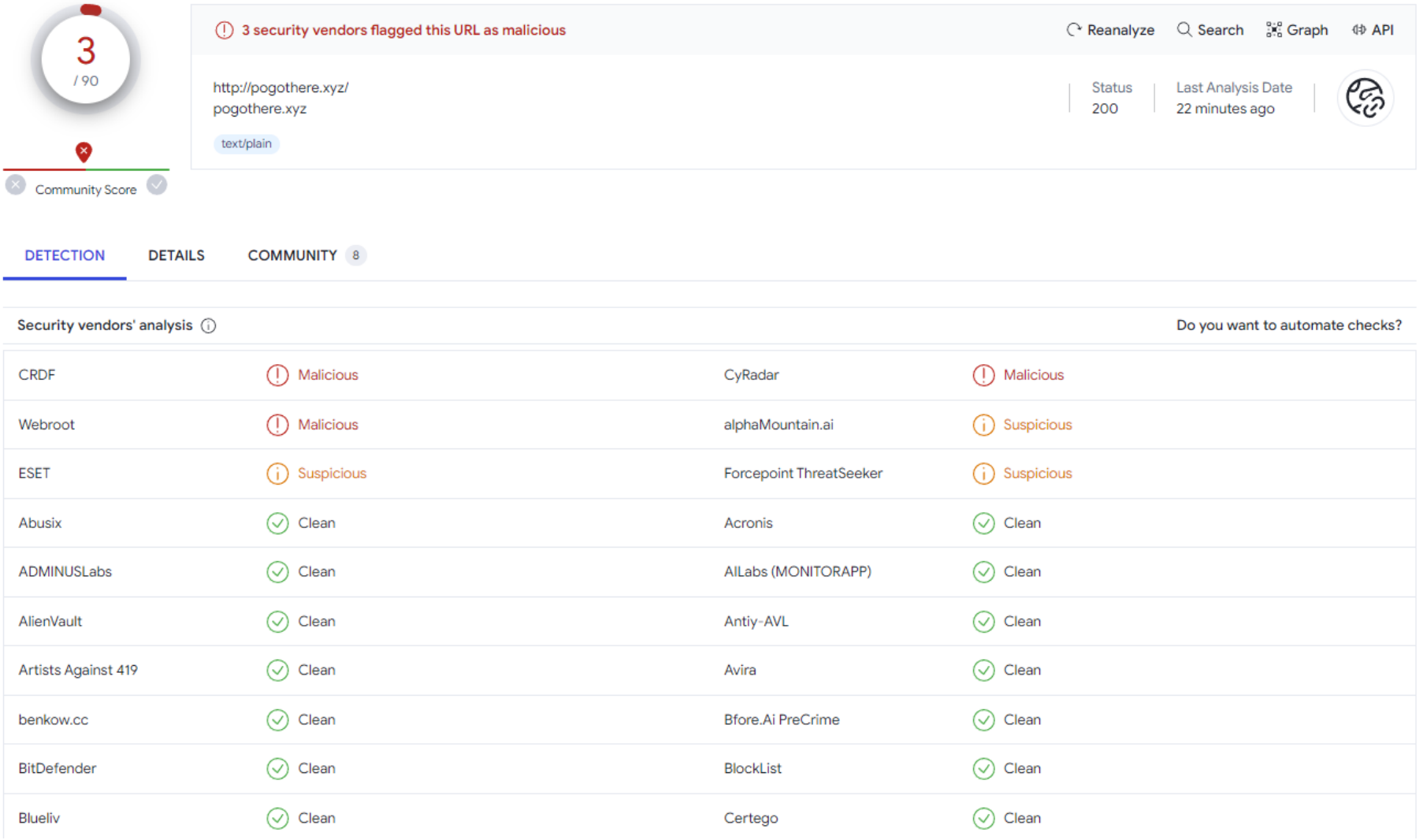
- **Ask yourself…**
  - What does the exploit do?
    - Give admin or user access? DoS?
  - Did the exploit work?
    - Is there evidence of install afterwards? Command and control?
  - What type of asset?
    - Internal? External? Desktop? Server?
    - Where is the asset located? DMZ? Sensitive server subnet?
    - Who is the user? Do they have admin access, critical data access?

Dissemination

- **When a threat is found information is disseminated**
  - Inside closed communities: MISP
  - To the public: Virustotal, AbuseCH, OTX, MISP…
- **Security software will include this information to protect organizations**
  - Current systems update signatures/rules dynamically
    - Several times per day
- **Golden rule: update!**

MISP: Global platform to share indicators of compromise

Is this site malicious?



https://www.virustotal.com/gui/url/9bfdba5d503dc46919a917a80885ebc442b1b88eb29d46898793c995abae5530

SOAR

- **Security Orchestration, Automation and Response**
  - Software that enables security teams to integrate and coordinate separated tools into streamlined threat response workflows