Collaborative Strategy for the Neutralization of Cyber Threats

July, 2019

Andoni Valverde

About me

Andoni Valverde Villar

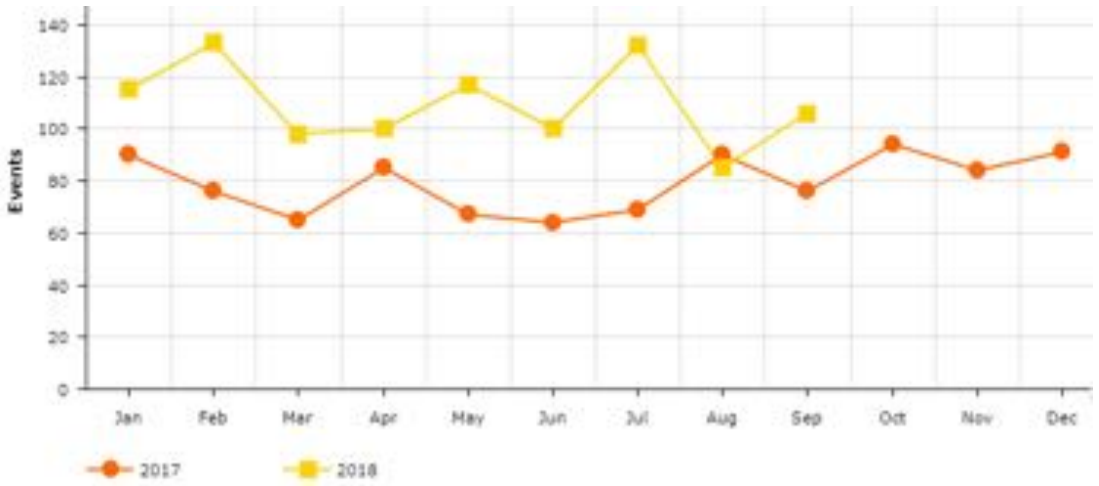
https://www.linkedin.com/in/andoni-valverde-villar/

SIEM, OSINT, SOC/CERT, Deception

Trust affects cybersecurity

Motivation of our adversaries

Trends



Hoja de c·lculo
de Microsoft Exce

2019 Data Breaches

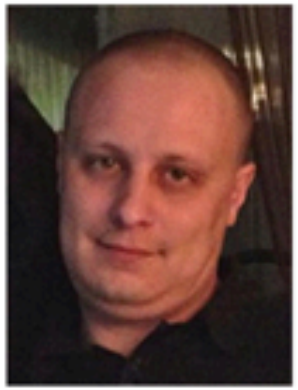
January 2, 2019	Blur
January 3, 2019	Town of Salem Video Game
January 4, 2019	DiscountMugs.com
January 7, 2019	BenefitMall
January 10, 2019	OXO
January 11, 2019	Managed Health Services (MHS) of Indiana
January 16, 2019	Fortnite
January 17, 2019	Oklahoma Department of Securities
January 17, 2019	Collection 1
January 22, 2019	BlackRock Inc.
January 22, 2019	Graeters Ice Cream
January 23, 2019	Online Betting Sites
January 23, 2019	Ascension
January 23, 2019	Alaska Department of Health & Social Services (DHSS)
January 29, 2019	Rubrik
January 31, 2019	Critical Care, Pulmonary & Sleep Associates (CCPSA)
February 1, 2019	Houzz
February 4, 2019	Catawba Valley Medical Center
February 4, 2019	Huddle House
February 6, 2019	EyeSouth Partners
February 12, 2019	Dunkin' Donuts
February 14, 2019	Coffee Meets Bagel
February 15, 2019	500px
February 19, 2019	North Country Business Products
February 20, 2019	Advent Health
February 20, 2019	Coinmama
February 20, 2019	UW Medicine
February 22, 2019	UConn Health
March 1, 2019	Dow Jones
March 4, 2019	Rush University Medical Center
March 6, 2019	Health Alliance Plan
March 12, 2019	Pasquotank-Camden Emergency Medical Services
March 15, 2019	Spectrum Health Lakeland
March 19, 2019	Rutland Regional Medical Center
March 20, 2019	Zoll Medical
March 21, 2019	MyPillow & Amerisleep
March 21, 2019	Facebook
March 21, 2019	Oregon Department of Human Services (DHS)
March 22, 2019	Federal Emergency Management Agency (FEMA)
March 23, 2019	Family Locator
March 25, 2019	Milestone Family Medicine
March 26, 2019	Verity Health Systems
March 29, 2019	Earl Enterprises
March 29, 2019	Verifications.io
April 2, 2019	Georgia Tech
April 2, 2019	Facebook
April 8, 2019	Baystate Health
April 10, 2019	Prisma Health
April 15, 2019	City of Tallahassee
April 15, 2019	Microsoft Email Services
April 19, 2019	Steps to Recovery
April 20, 2019	EmCare
April 22, 2019	Bodybuilding.com
April 25, 2019	Atlanta Hawks
April 29, 2019	Docker Hub
May 2, 2019	Citrix
May 3, 2019	AMC Networks
May 7, 2019	Wyzant
May 9, 2019	Freedom Mobile
May 13, 2019	Pacers Sports & Entertainment (PSE)
May 13, 2019	Uniqlo
May 14, 2019	WhatsApp
May 20, 2019	Instagram
May 23, 2019	Inmediata Health Group
May 24, 2019	First American Financial Corp.
May 24, 2019	Canva
May 29, 2019	Flipboard
May 29, 2019	Checkers
June 3, 2019	Quest Diagnostics
June 4, 2019	LabCorp
June 6, 2019	Opko Health
June 10, 2019	Emuparadise
June 10, 2019	U.S. Customs and Border Protection
June 11, 2019	Evite
June 11, 2019	Total Registration
June 12, 2019	Evernote
June 18, 2019	EatStreet
June 18, 2019	Oregon Department of Human Services
June 20, 2019	Desjardins
June 26, 2019	Dominion National

Cyber’s Most Wanted (https://www.fbi.gov/wanted/cyber)

WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

REMARKS

Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

CAUTION

Evgeniy Mikhailovich Bogachev, using the online monikers "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victims' computers. The

WANTED BY THE FBI

BEHZAD MESRI

Computer Intrusion; Aggravated Identity Theft; Aiding and Abetting; Computer Fraud – Unauthorized Access to a Protected Computer; Wire Fraud; Computer Fraud – Threatening to Impair the Confidentiality of Information; Computer Fraud – Threatening to Damage a Protected Computer/Impair the Confidentiality of Information; Interstate Transmission of an Extortionate Communication

DESCRIPTION

Alias: Skote Vahshat	
Date(s) of Birth Used: August 24, 1988	**Place of Birth:** Naghadeh, Iran
Hair: Brown	**Eyes:** Brown
Height: 5'9"	**Weight:** 175 pounds
Sex: Male	**Race:** White
Nationality: Iranian	**NCIC:** W052433913

REMARKS

Mesri is known to speak Farsi and resides in Iran.

CAUTION

Behzad Mesri is wanted for his alleged involvement in criminal activities to include computer intrusion and aggravated identity theft. Mesri was the CEO of an Iranian entity that allegedly worked at the behest of the Islamic Revolutionary Guard Corps (IRGC) and was allegedly used in furtherance of a malicious cyber campaign targeting current and former members of the United States Intelligence Community. On February 8, 2019, a grand jury in the United States District Court, District of Columbia, indicted Mesri, and others, and a federal arrest warrant was issued for him after he was charged with conspiracy, attempted computer intrusions, and aggravated identity theft. Mesri was previously charged with unauthorized access to computer systems, stealing proprietary data from those systems, and attempted extortion for approximately $6 million in Bitcoin. On November 8, 2017, a grand jury in the United States District Court, Southern District of New York, indicted Mesri and a federal arrest warrant was issued for him after he was charged with Computer Fraud – Unauthorized Access to a Protected Computer; Wire Fraud; Computer Fraud – Threatening to Impair the Confidentiality of Information; Computer Fraud – Threatening to Damage a Protected Computer/Impair the Confidentiality of Information; Interstate Transmission of an Extortionate Communication; and

WANTED BY THE FBI

MOHAMMAD SAEED AJILY

Conspiracy to Commit Computer Fraud; Computer Fraud; Wire Fraud; Violation of International Emergency Economic Powers Act (IEEPA); Violation of International Traffic in Arms Regulations (ITAR)

DESCRIPTION

Aliases: Mohammed Saeed Ajily, Mohammad Ajily	
Date(s) of Birth Used: September 3, 1982	**Place of Birth:** Iran
Hair: Brown	**Eyes:** Brown
Height: 5'7" to 5'10"	**Weight:** 210 to 215 pounds
Build: Medium	**Sex:** Male
Nationality: Iranian	

REMARKS

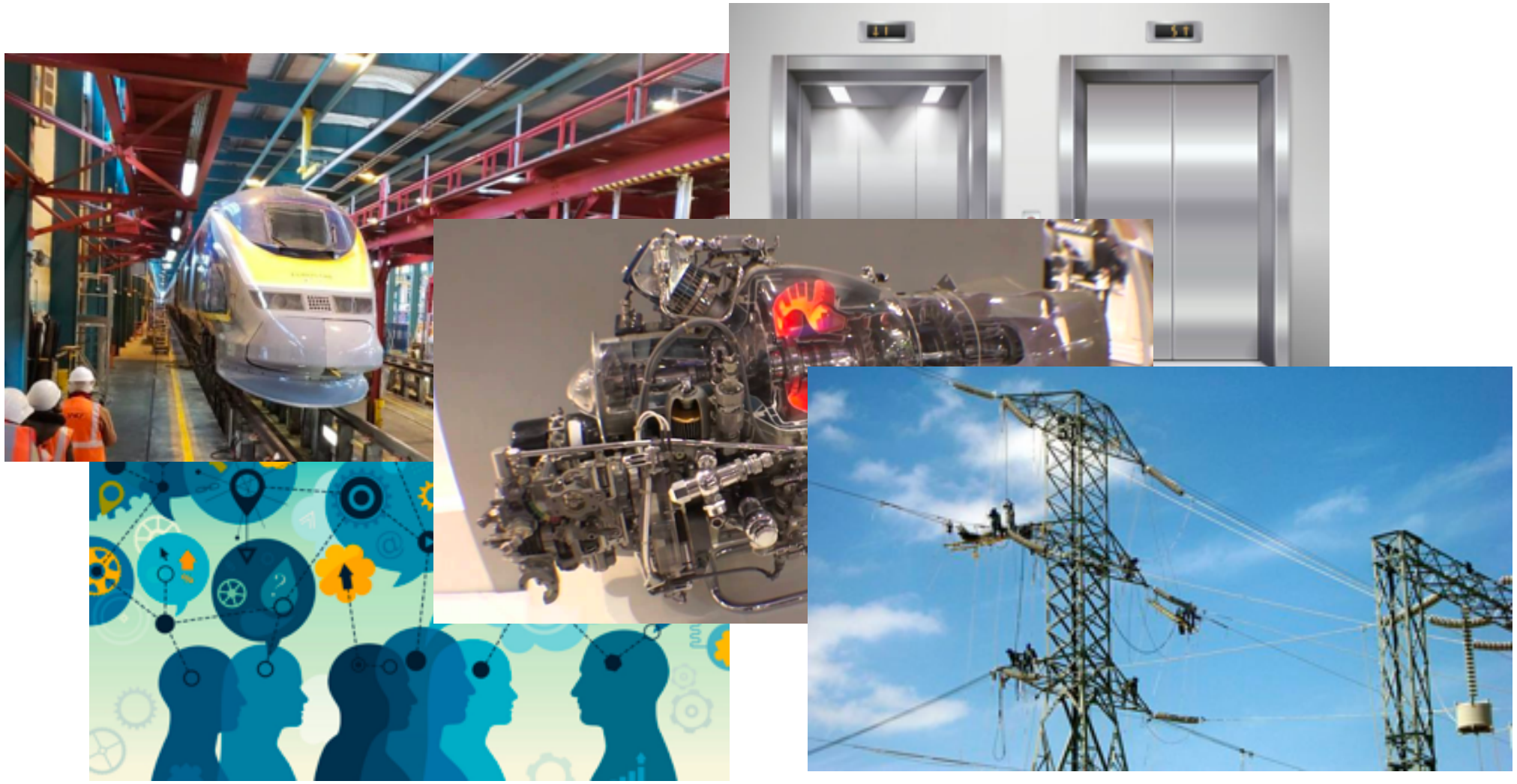
Ajily wears glasses. He is believed to be living in Iran.

CAUTION

Mohammad Saeed Ajily and Mohammad Reza Rezakhah are wanted for allegedly conspiring with others to hack into the network and computers of a United States cleared defense contractor in Vermont in order to steal valuable company software and business information. Ajily and Rezakhah allegedly utilized compromised servers provided by a third co-conspirator to mask their true location and identity, and to launch computer intrusions against victim companies, including the United States cleared defense contractor. As part of this intrusion, which occurred between approximately 2007 and 2013, Ajily and Rezakhah allegedly stole the company's sophisticated software product and other proprietary information.

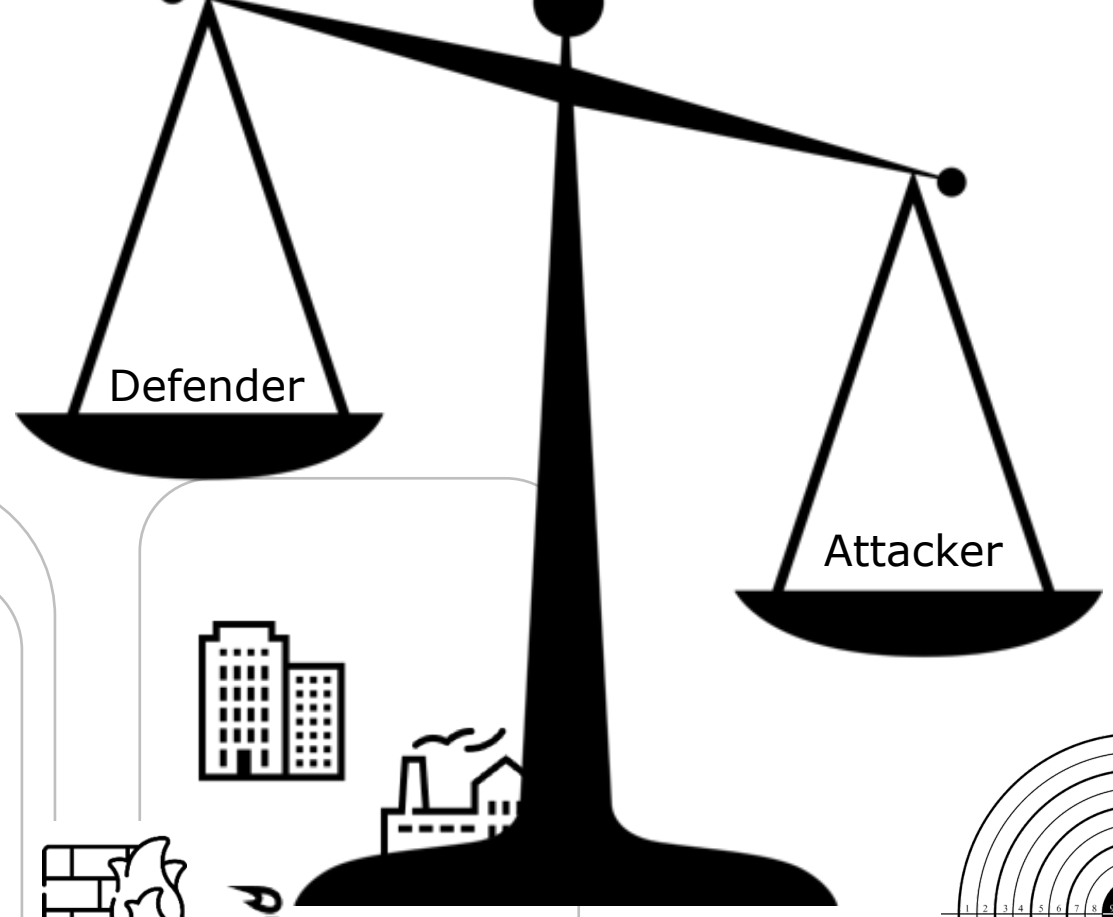
On April 21, 2016, a federal grand jury in the United States District Court, District of Vermont, Burlington, Vermont, indicted Ajily and Rezakhah for their alleged involvement in the conspiracy and a federal warrant was issued for their arrest after they were charged with Conspiracy to Commit Computer Fraud, Computer Fraud, Wire Fraud, Violation of International Emergency Economic Powers Act (IEEPA), and Violation of International Traffic in Arms Regulations (ITAR).

It’s not me! It’s in USA, China or Iran…



Information Sharing

Defend vs. Attack



Cloud

DMZ

VPN

DNS

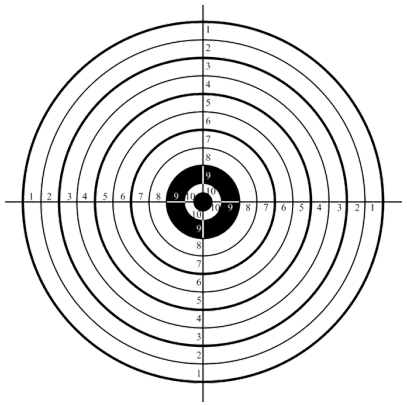
DATACENTER

ADMIN &
VIP USERS

WORKSTATIONS

INTERNAL NETWORK

COMPANY SUBIDIARIES,
CLOUD, OFFICES,
INFRASTRUCTURES…



Sharing

- It is not just a question of Indicators of Compromise
  - We must share experience
  - Which tools are effective for different threats
  - What taxonomies are used and how incidents are classified
  - How you develop communications in a crisis situation
  - …

The Pyramid of Pain

The Pyramid measures **potential usefulness** of your intel

It also measures **difficulty of obtaining** that intel

The higher you are, the **more resources** your adversaries have to expend.

When you quickly detect, respond to and disrupt your adversaries' activities, defense becomes offense.

* David J. Bianco

Hashes

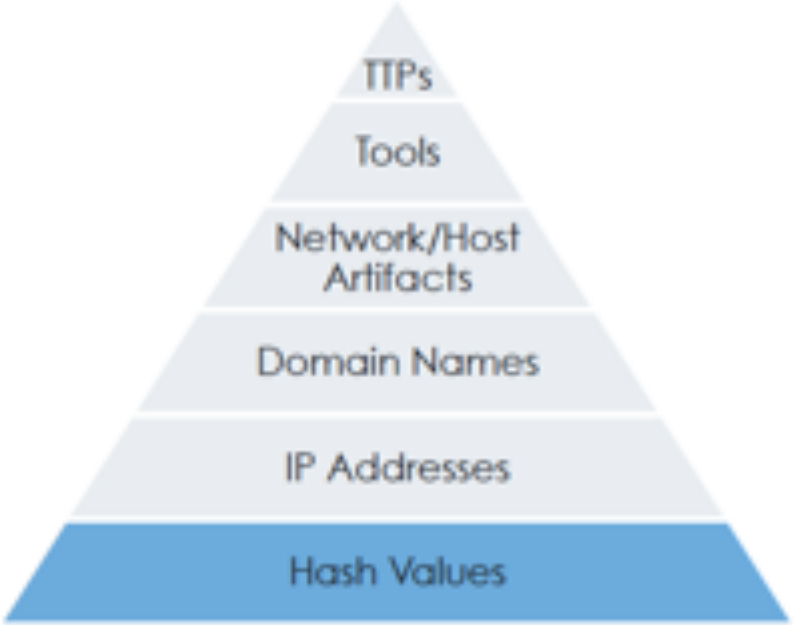
99% of malware hashes are seen for 58 seconds or less

Vast majority of malware only seen once

Hashes are, by far, the highest confidence indicators.

Unfortunately, they are extremely susceptible to change (even accidentally).

Hashes are probably the least useful type of indicators.



MD5
5f6ce162c4b5516670d5a8f1f8f4e57b
SHA1
C8d4c389beaff88811f8fab1965519fce74ffd8a
SHA256
ad690662a1faf97dc41387b73f8fd3415d64f9b0ce66db3e9134385d94e0c01b

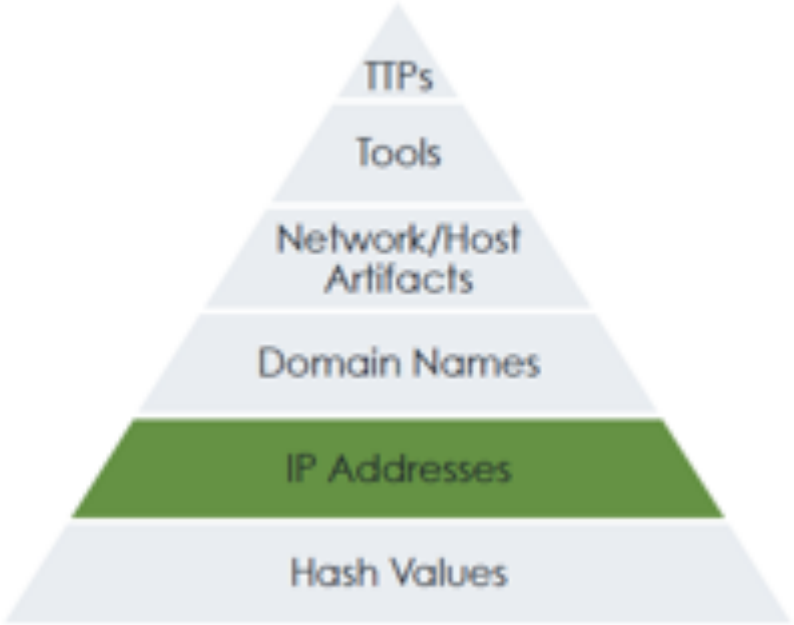
IP addresses

IP reputation sites often rank sites as bad based on badness 6+ months prior

Only n00bs use their own addresses.

VPNs, Tor, open proxies all make it trivial to change your IP.

If it's hardcoded into a config, maybe adversaries have to do a little work to update it.



Dotted Decimal 192.168.1.1 **Dotted Hex** 0xC0.0xA8.0x01.0x01 **Dotted Octal** 0300.0250.0001.0001	**Decimal** 3232235777 **Hex** 0xC0A80101 **Octal** 030052000401

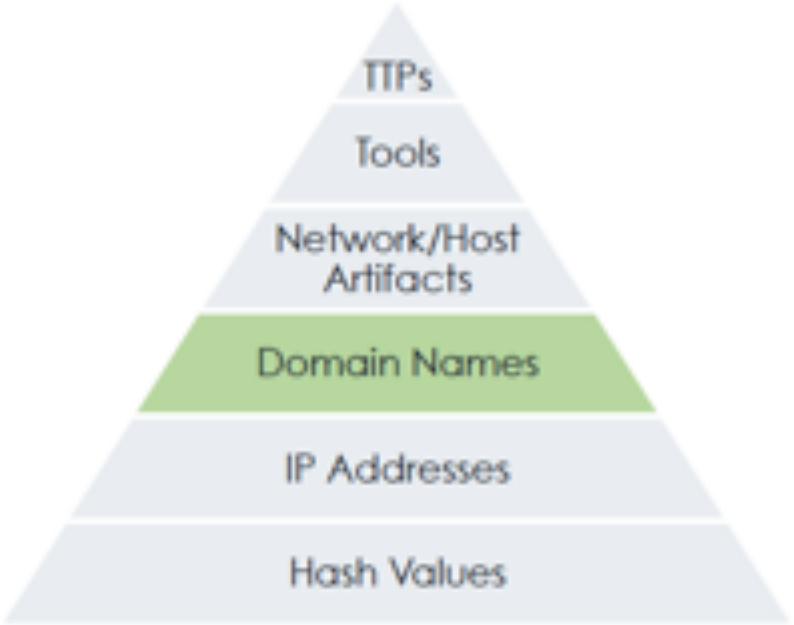
Domain names

84% of phishing sites exist for less than 24 hours

Almost as easy to change as IP addresses.

Domains require pre-registration and (usually) a fee, but there are ways around this.

Dynamic DNS providers even help automate the adversary's update process with helpful APIs.



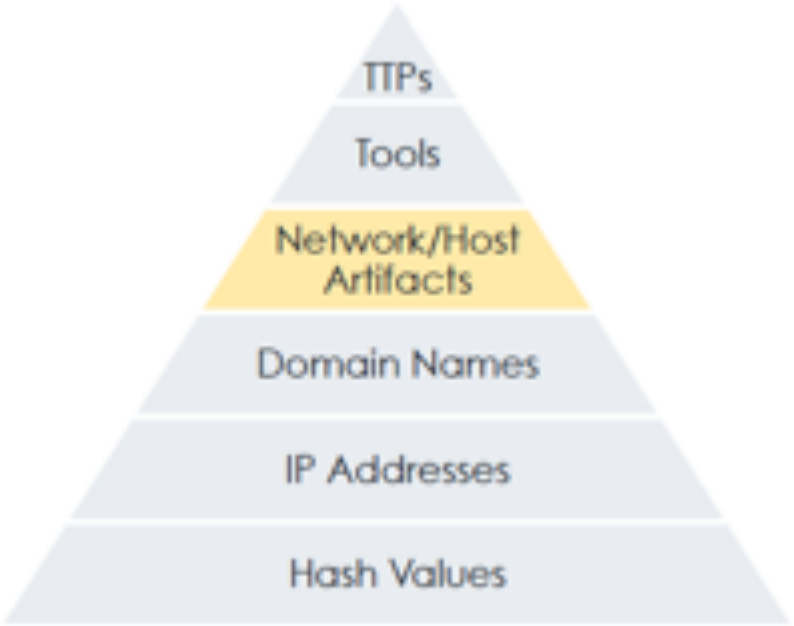
Unicode 邪悪なドメイン.com **Punycode** Xn—q9j5f9d1dzdq306auhtd.com	**Legitimate Domain** rvasec.com **Malicious Homograph** rvasec.com

Network / Host Artifacts

It's very difficult to perform useful activities without leaving some traces.

On hosts, look for files & directories, registry objects, mutexes, memory strings [...]

On the network, check for distinctive transaction values, especially protocol errors or just misinterpretations.



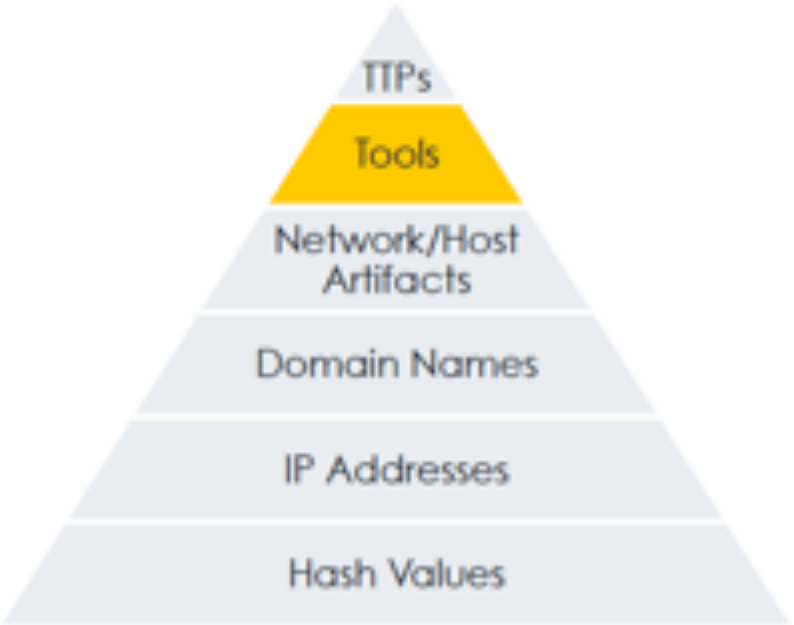
Distinctive URI patterns
/^[A-F0-9]{16}\/\d{3,5}\.{php|aspx}$/
User-Agent Strings
xi/1.0
Typos
Mozilla/5.0 (compatible; MSIE7.0; Windows NT 6.1;)

Tools

If you see the same tool over and over, you eventually get really good at detecting it.

No matter what incidental changes they make, your detection mechanisms can deal with them.

To continue, they need a new tool. With testing & training time, that's a real victory!



Once upon a time, there was an incident response team who encountered the same tool over and over again for more than a year. The tool had a bolt-on network front end, so the attackers could easily change the network protocol, but the back end was always the same. Eventually, the IR team realized that the distinctive keep-alive function was part of the back end, and could be reliably detected. And then everyone (except the attacker) slept well at night and lived happily ever after!

FireEye

TTP – Techniques Tactics Procedures

TTPs are the expression of the attacker's training.

Retraining is probably the hardest thing you can do once, let alone continually.

This becomes so expensive that they have to question their commitment to attacking you. Win!

Data Staging Tactic
Create encrypted RAR and transfer them to the exfiltration point.
Data Staging Technique
AES encryption, files of exactly 650,000 bytes, file copies via SMB
Data Staging Procedure
winrar a –hpqwerty –r vacation_photos.rar *staging_dir*
net use *exfil_server*\photos

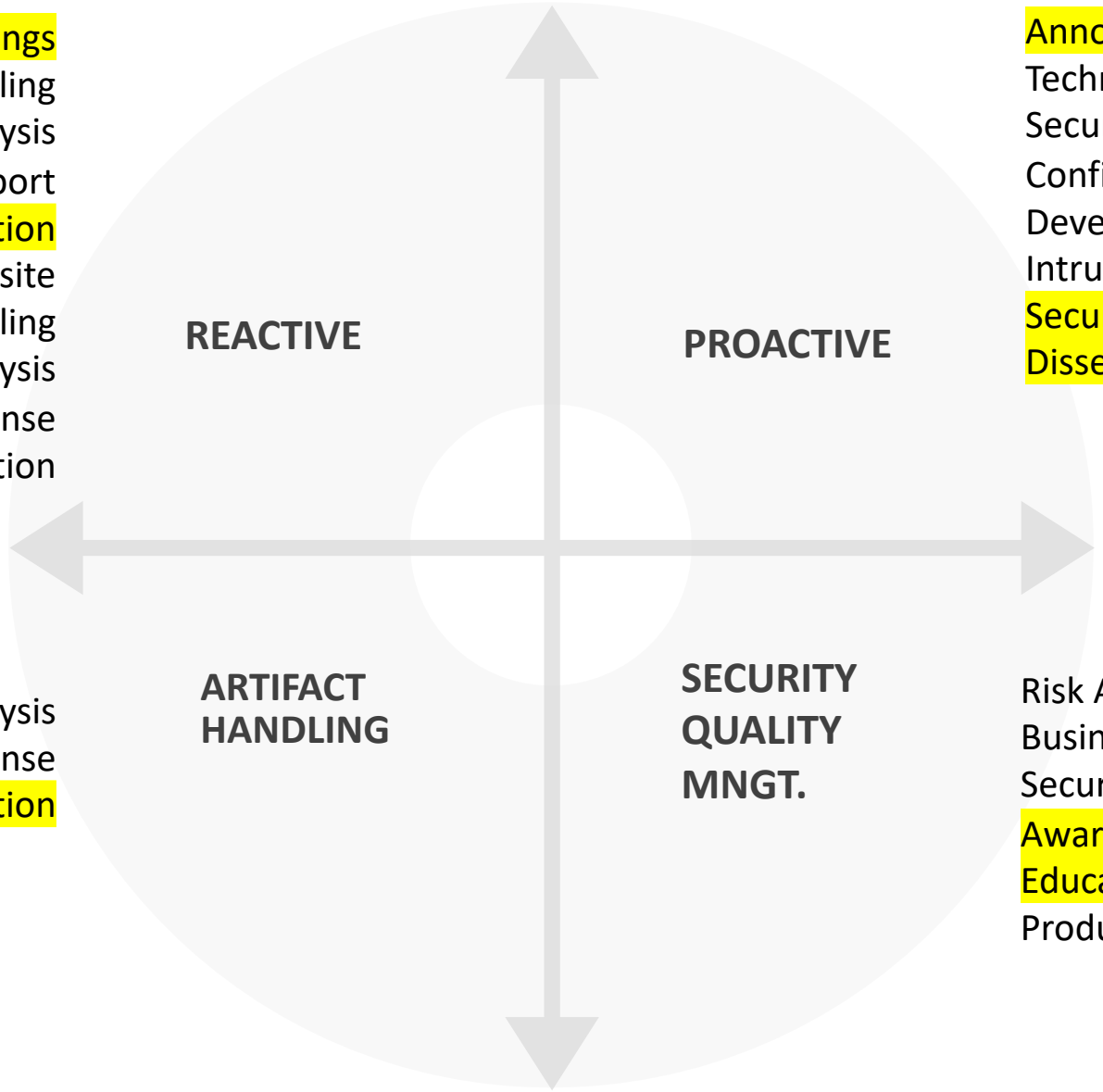
Actively Sharing Organizations

Organizations

- Private organizations from different industries
- Law Enforcement Agents
- Intelligence Companies
- CERTs
- …

Ejemplo de servicios orientados a colaboración

Alerts and Warnings
Incident Handling
Incident analysis
Incident response support
Incident response coordination
Incident response on site
Vulnerability Handling
Vulnerability analysis
Vulnerability response
Vulnerability response coordination

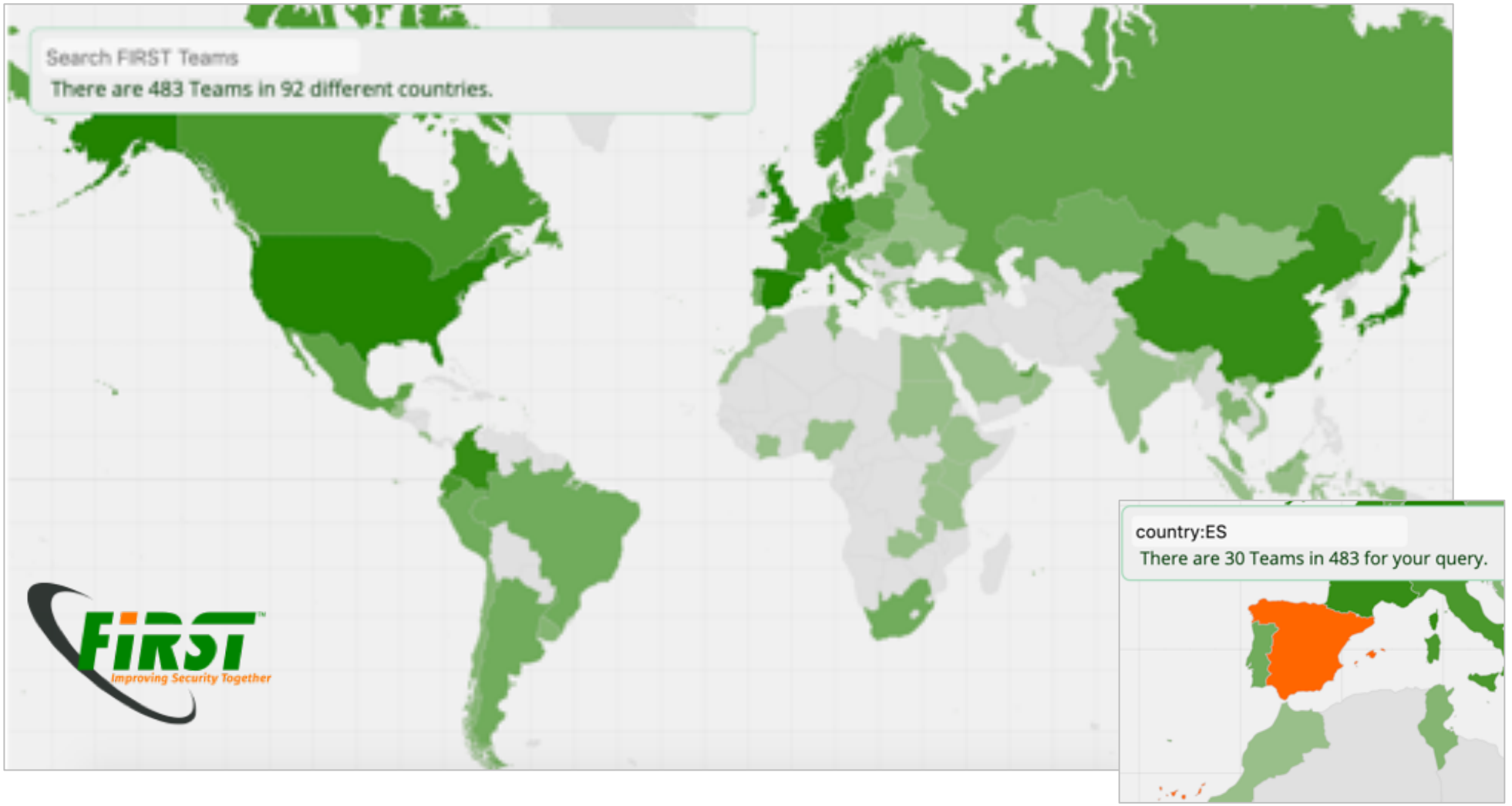


Announcements
Technology Watch
Security Audits or Assessments
Configuration and Maintenance of Security
Development of Security Tools
Intrusion Detection Services
Security-Related Information Dissemination

Artefact analysis
Artefact response
Artefact response coordination

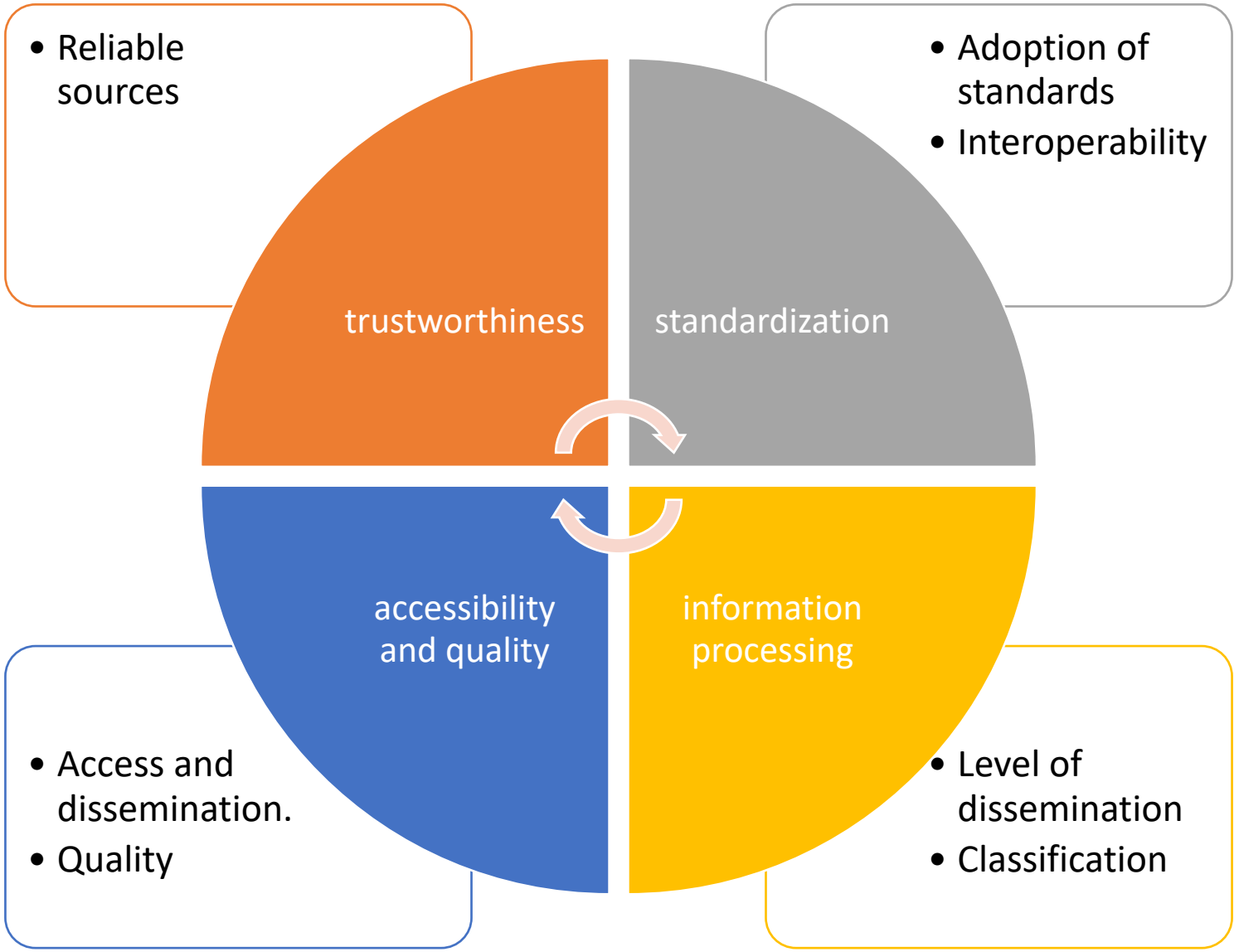
Risk Analysis
Business Continuity and Disaster Recovery
Security Consulting
Awareness Building
Education/Training
Product Evaluation or Certification

First - Forum of Incident Response and Security Teams



- BBVA CERT
- BCSC
- CaixaBank Team
- CCN-CERT
- CERT OESÍA
- CESICAT-CERT
- CiberSOC
- Cipher CERT
- CSA-CSIRT
- CSIRT-CV
- Deloitte EDC
- DXC Technology Iberia CSIRT
- Entelgy Innotec CSIRT
- ERIS-CERT
- esCERT-UPC
- eSOC Ingenia
- ESP DEF CERT
- EULEN-CCSI-CERT
- everis CERT
- IBERDROLA CSIRT
- INCIBE-CERT
- ITS-CERT
- MAPFRE-CCG-CERT
- Mnsait CSIRT
- NestleSOC

Sharing procedure



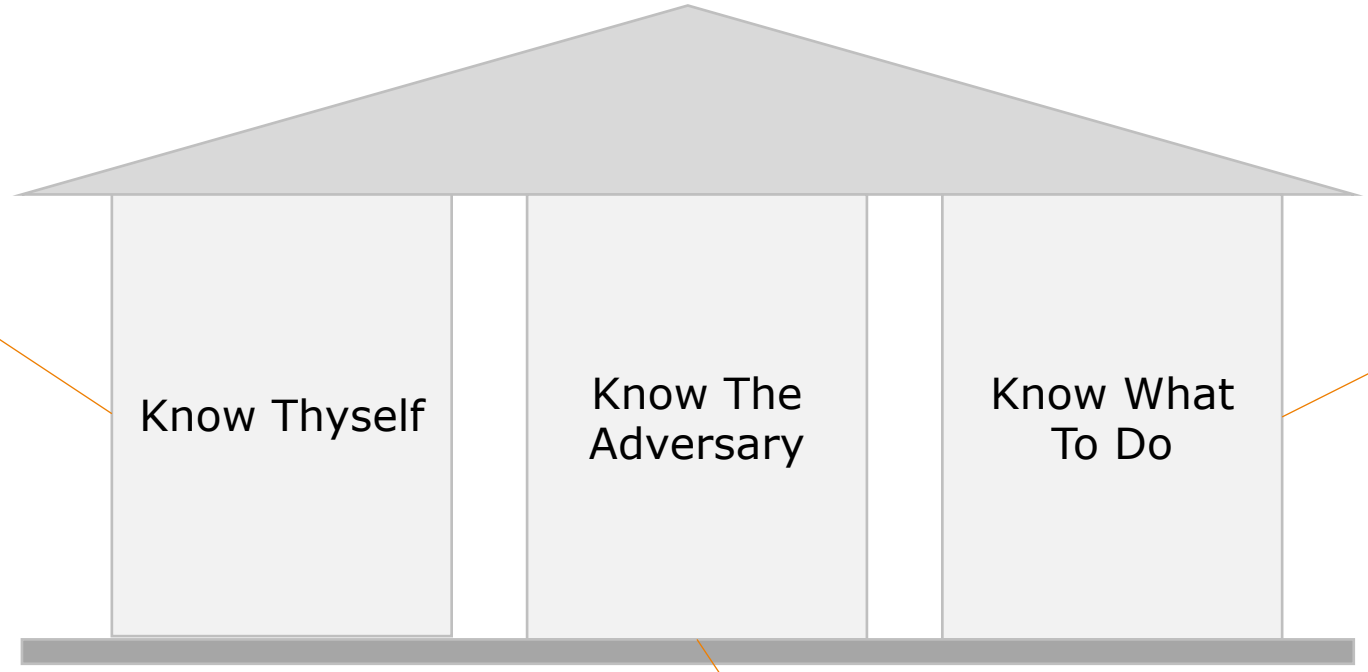
Traffic Light Protocol (TLP)

- The author must check the information with appropriate color to indicate scope TLP is the dissem

Code	When to use it	How to share it	Color	Background
TLP:RED	**TLP:RED** should be used when the information is limited to specific individuals, and could have an impact on privacy, reputation or operations if misused.	Recipients should not share information designated as **TLP:RED** with any third party outside the area where it was originally exposed.	#ff0033	#000000
TLP:AMBER	**TLP:AMBER** should be used when information needs to be distributed to a limited extent, but poses a risk to the privacy, reputation or operations if shared outside the organization.	Recipients can share information indicated as **TLP:AMBER** only with members of their own organization who need to knowand with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.	#ffc000	#000000
TLP:GREEN	**TLP:GREEN** when the information is useful for all organizations involved, as well as with community or sector.	Recipients can share information indicated as **TLP:GREEN** with affiliated organizations or members of the same sector, but never through public channels.	#33ff00	#000000
TLP:WHITE	when information poses no risk of misuse, within the rules and procedures for public dissemination.	information can be distributed without restrictions, but still subject to Copyright controls	#ffffff	#000000

Threat Intelligence: How to…

Pillars of Threat Intelligence

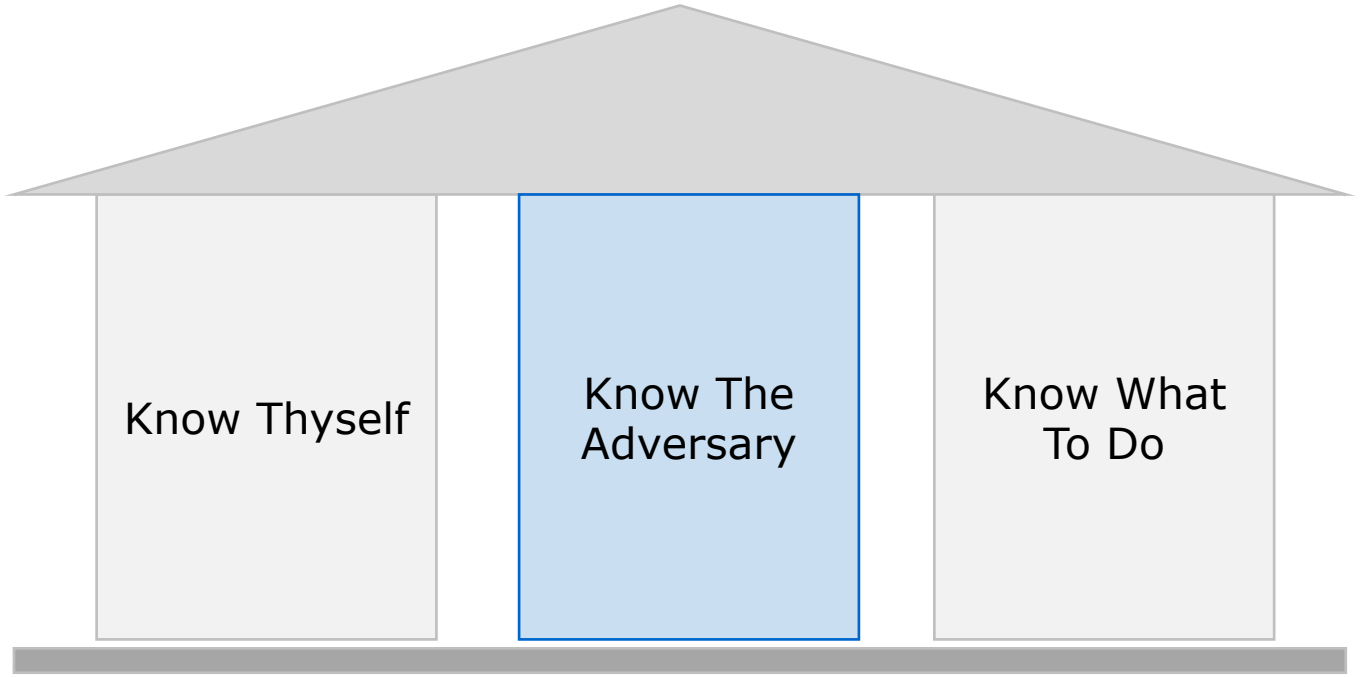


- Network
- Employees
- Supply chain
- Vulnerabilities
- Assets
- Data
- …

- Sequence of events
- Flags
- …

- Motives
- Weapons
- Capability / Opportunity / Intent
- TTPs
- …

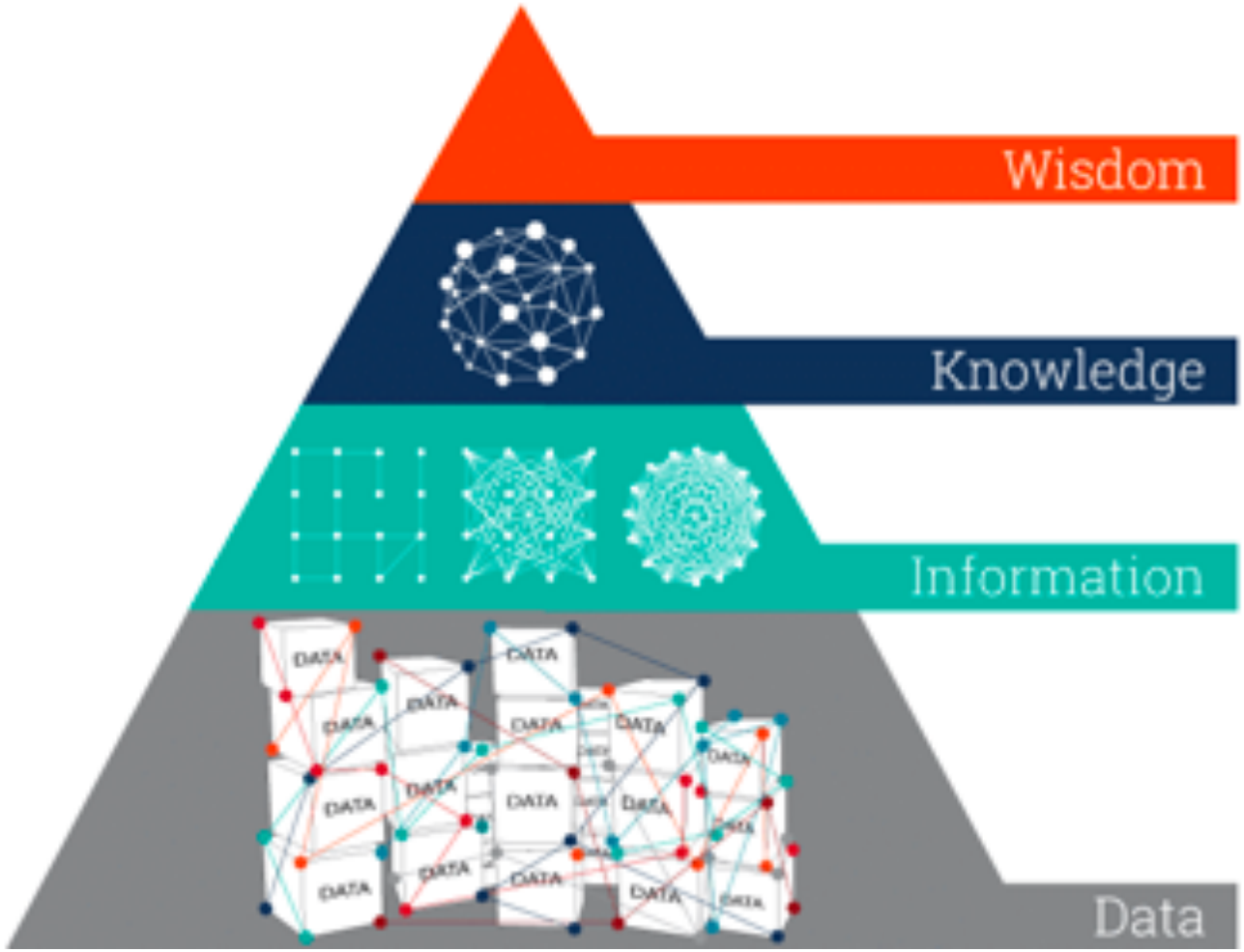
Know the adversary



Cyber-Threat

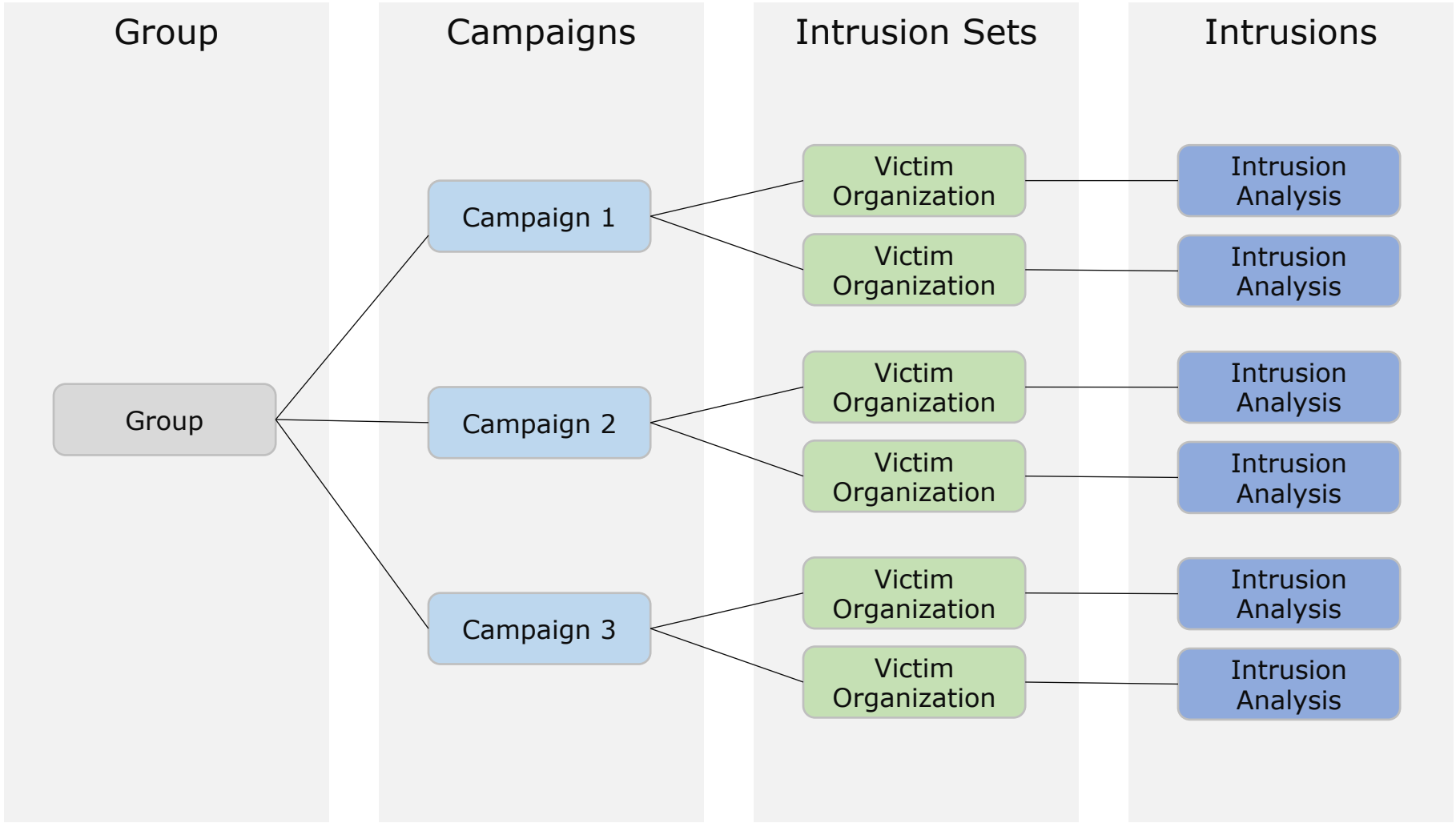
- Organizations must know what their threats are to accurately collect and use threat intelligence
- Threats can be established by evaluating Capability + Intent + Opportunity

DIKW Pyramid



Each step up the pyramid answers questions about and adds value to the initial data.

The Making of an Activity Group

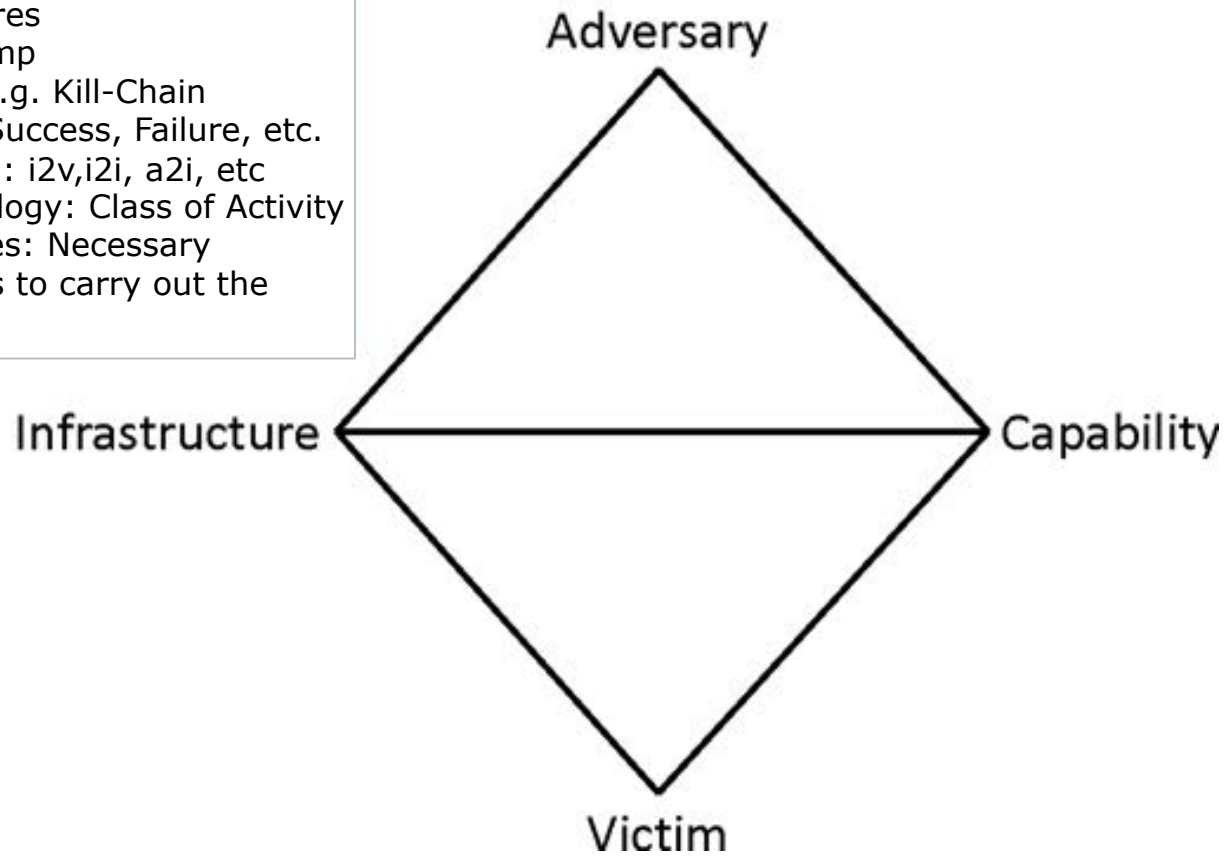


Diamond Model of Intrusion Analysis

An adversary deploys a capability over some infrastructure against a victim

- Events=Diamonds
- Each Event is characterized by and requires four Core Features (aka nodes, vertices):

Meta-Features
- Timestamp
- Phase: e.g. Kill-Chain
- Result: Success, Failure, etc.
- Direction: i2v,i2i, a2i, etc
- Methodology: Class of Activity
- Resources: Necessary elements to carry out the event.



{{Adversary, $Confidence_{adversary}$},
{Capability, $Confidence_{capability}$},
{Infrastructure, $Confidence_{infrastructure}$},
{Victim, $Confidence_{victim}$},
{$Timestamp_{start}$, $Confidence_{timestamp_{start}}$},
{$Timestamp_{end}$, $Confidence_{timestamp_{end}}$},
{Phase, $Confidence_{phase}$},
{Result, $Confidence_{result}$},
{Direction, $Confidence_{direction}$},
{Methodology, $Confidence_{methodology}$},
{Resources, $Confidence_{resources}$}}

Core Features

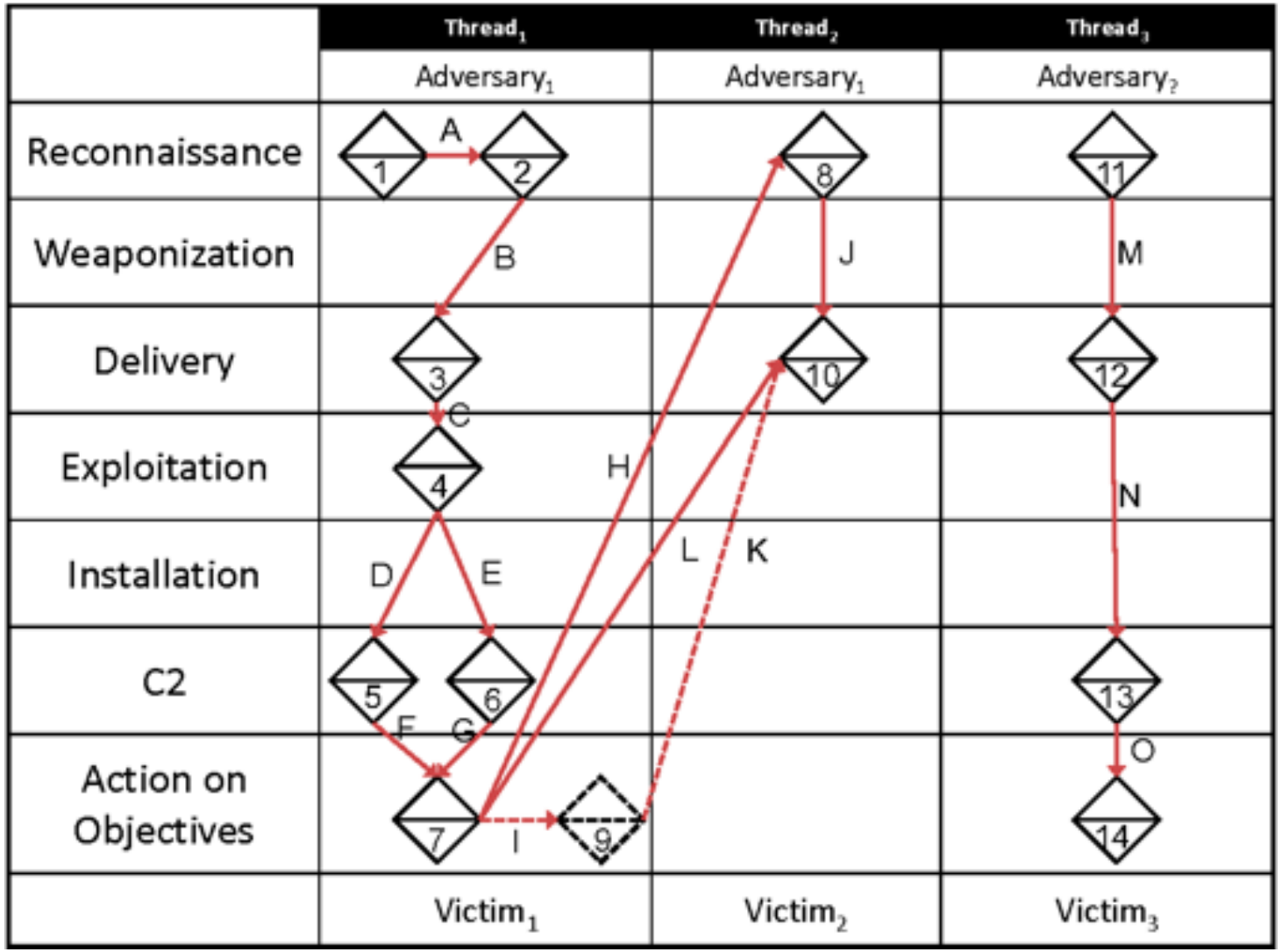
Meta Features

Activity Threads

An example visualization of activity threads illustrating Diamond events being linked:

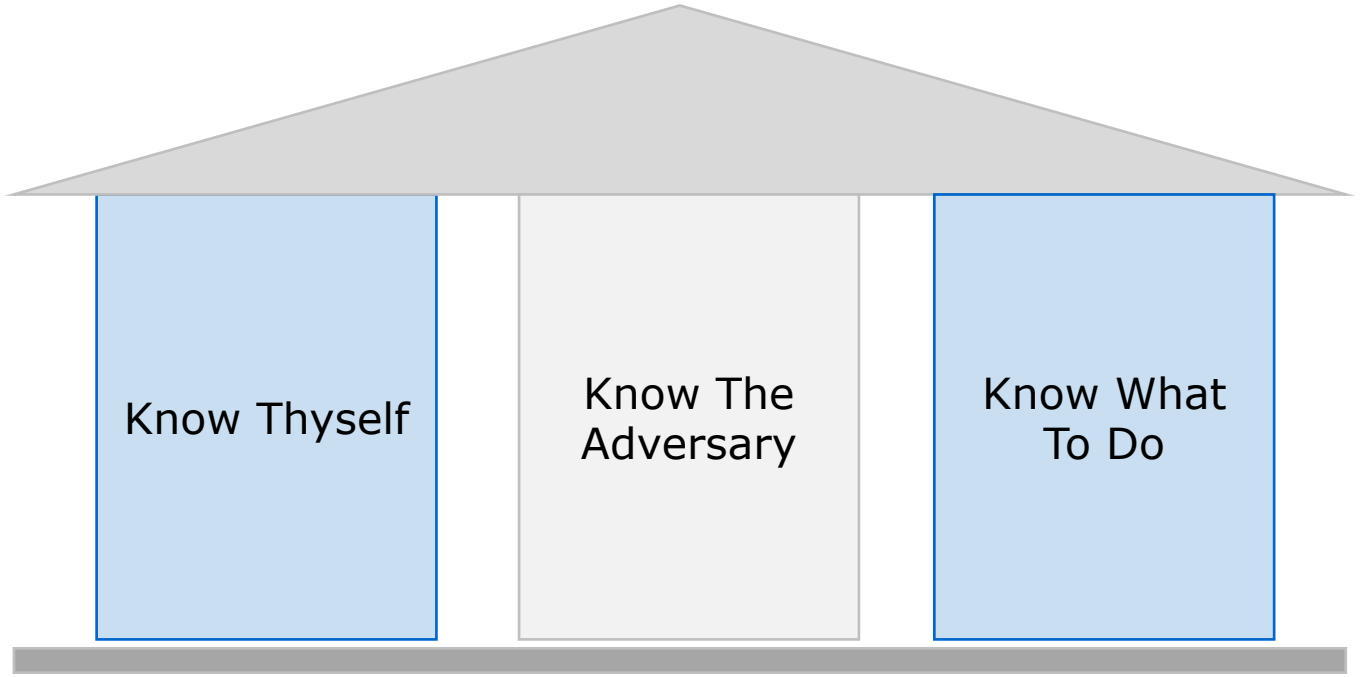
- **Vertically** (within a single victim), IR Process of identifying causal events.
- **Horizontally** (across victims) via directed **arcs** designating a causal relationship between the events (i.e., this event occurred because of, and subsequent to, this event)

- Solid lines represent actual element of information supported by evidence
- Dashed lines represent hypothesized elements.



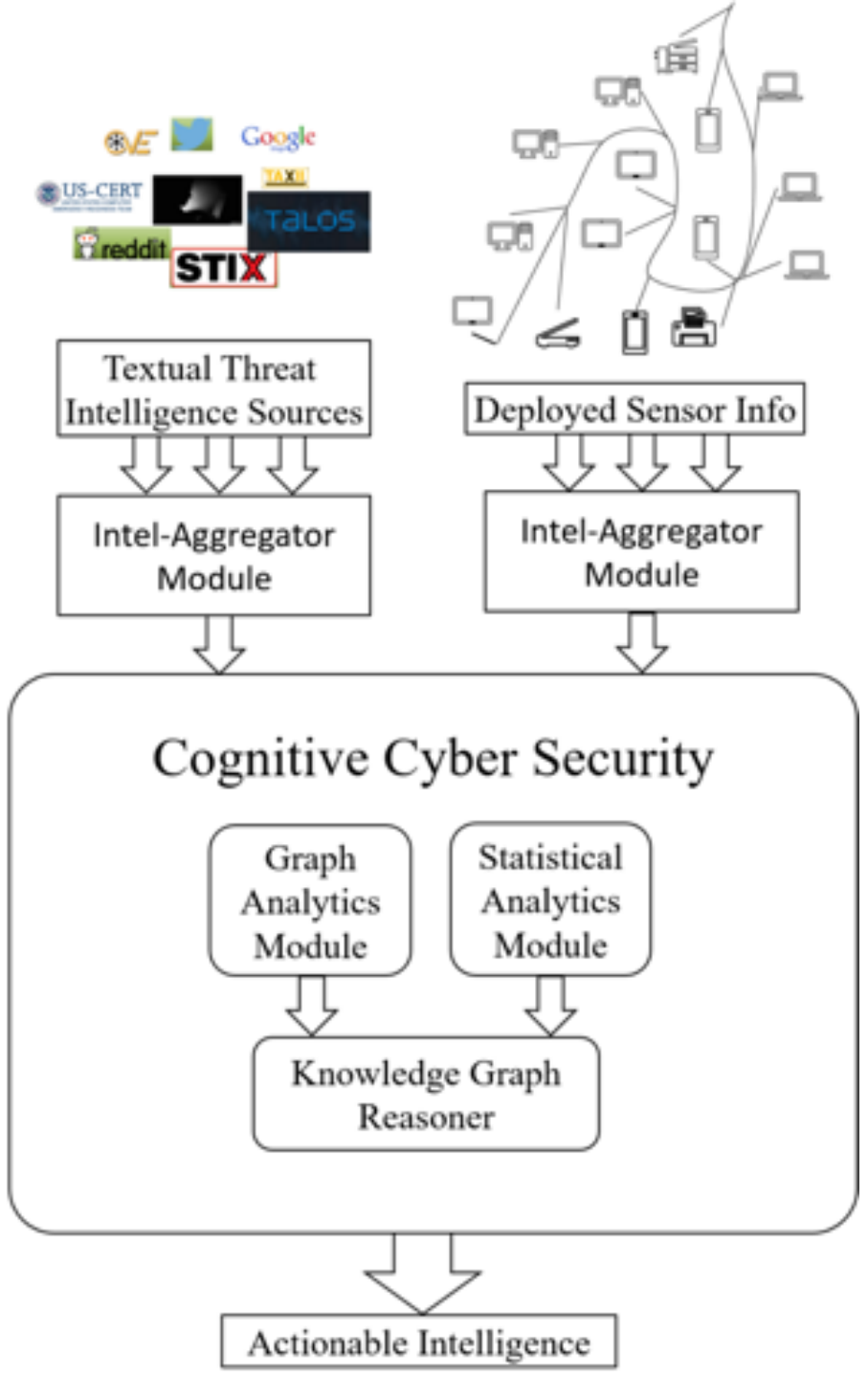

“Actionable” Intelligence

Pillars of Threat Intelligence



Cognitive CyberSecurity Architecture

- External
  - Textual Threat Intelligence Sources
  - Deception / Honeypot
  - Pastebin, Shodan, Twitter…
  - …
- Internal
  - Logs
  - IPS (sensors)
  - Incident data
  - Deception / Honeypot
  - Malware analysis
  - Malicious / Phishing email analysis
  - …



Textual Threat Intelligence Sources (IoC / IoA)

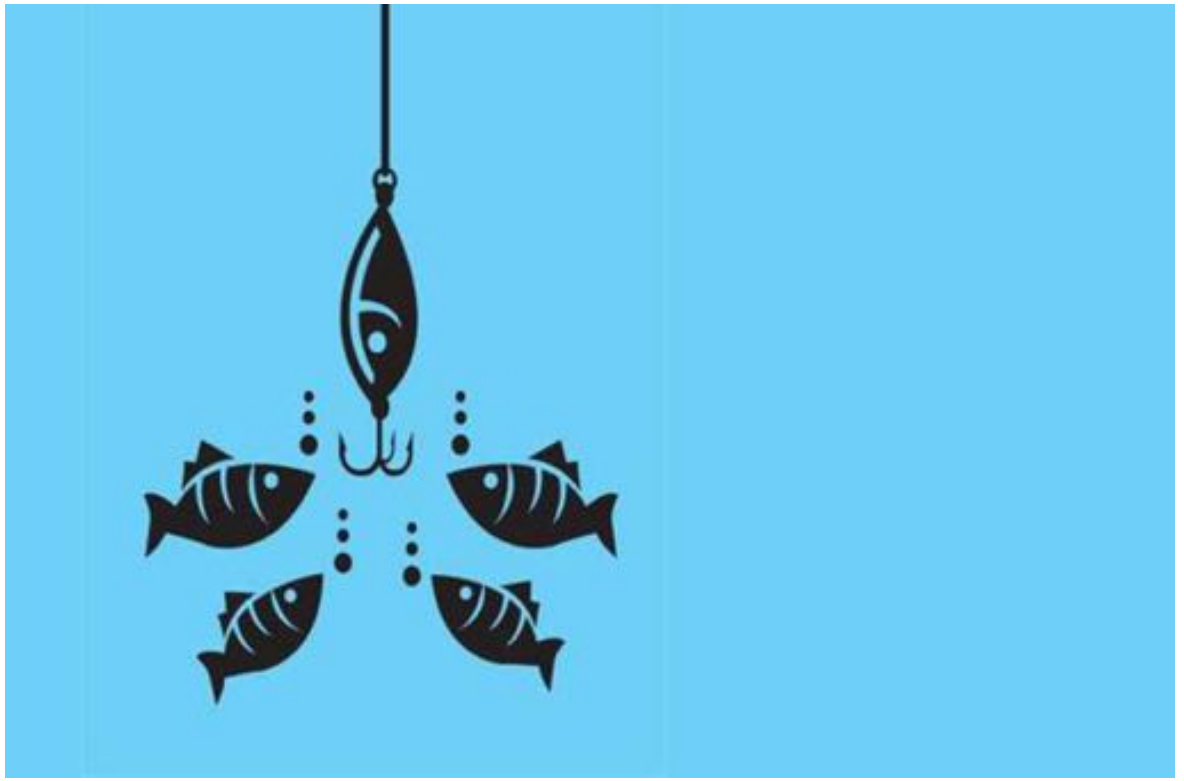
- Data without context is just data
- Threat intelligence with no association to your organization is (mostly) useless

- ~~Get better indicators faster~~
- ~~Share more~~

- Get only good indicators
  - High confidence level
  - More is not necessarily better

Phishing / Business Email Compromise (BEC)

- CEO Fraud
- Account Compromise
- Attorney Impersonation
- Data Theft
- …



Log analysis

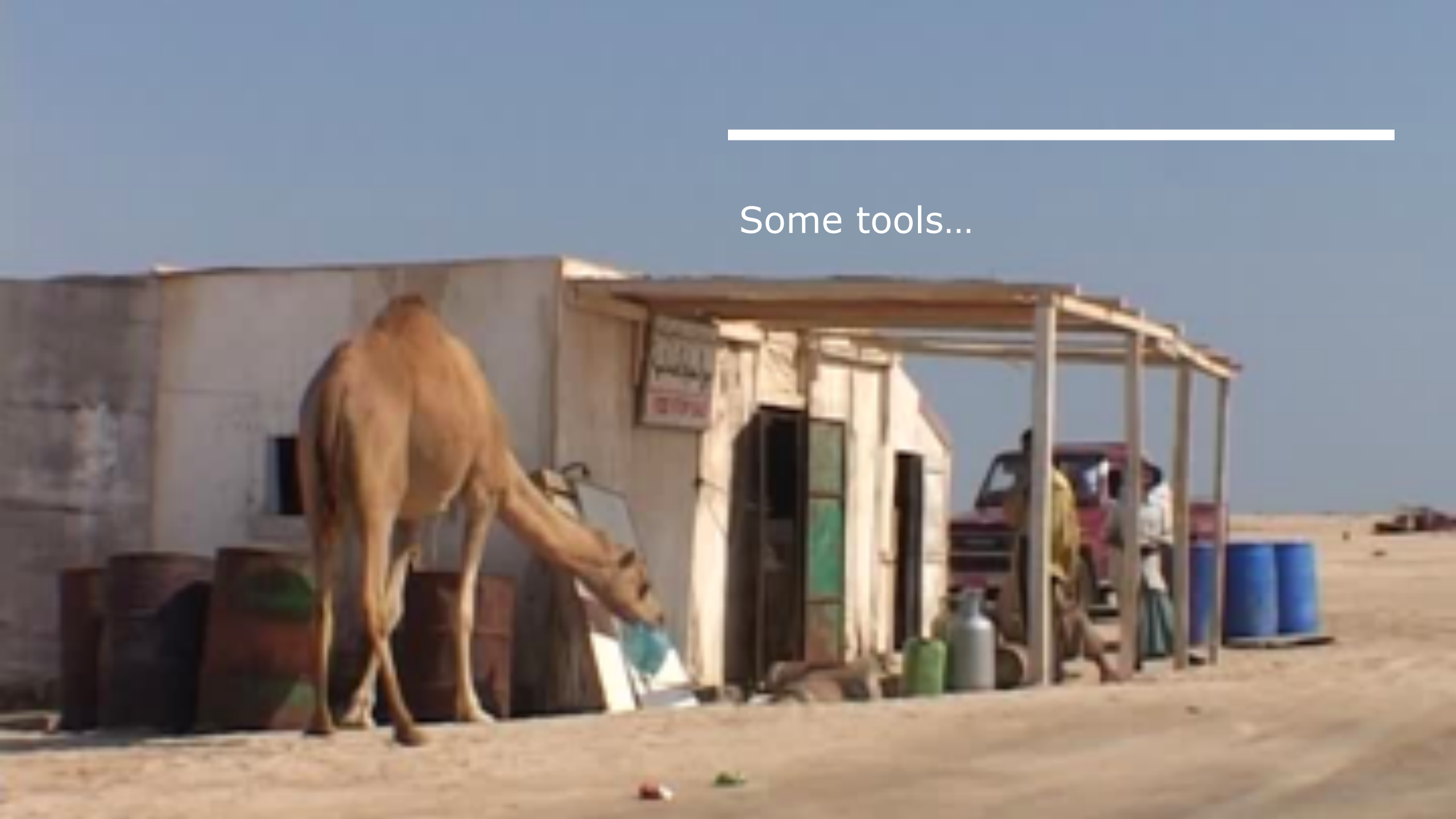
Malware analysis
Using malware to Identify Threat Actors

- When malware is the source of a breach, knowledge of its capabilities and behavior are crucial to effective incident response.
- Quick and reliable malware analysis can reveal the functionality of the malicious code. It can identify any changes the malware may have made to affected systems, and it can provide preliminary host- and networkbased indicators for detection signatures.

Honeypots

- If you installed a honeynet on your network and obtained intelligence locally

Some tools…



Threat Intelligence Frameworks

- You need a framework
- Data comes in a multitude of formats
- Different distribution methods
- You need the ability to take disparate datasets and converge them into usable and actionable intelligence

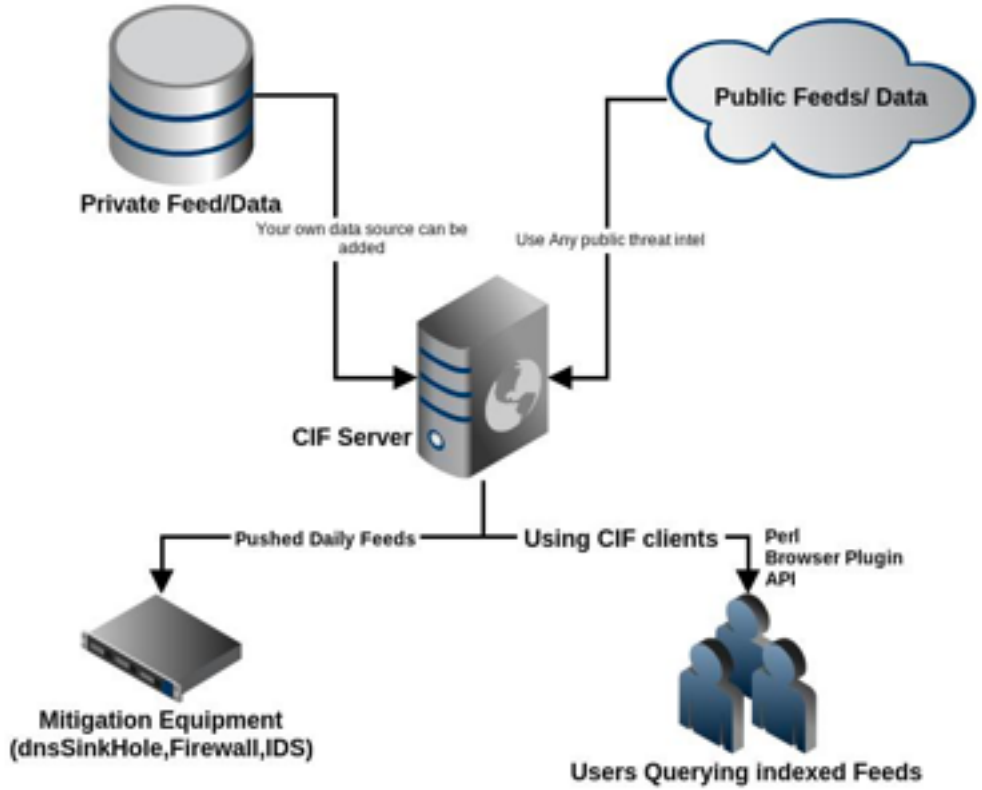
spiderfoot

SpiderFoot is a reconnaissance tool that automatically queries over 100 public data sources (OSINT) to gather intelligence on IP addresses, domain names, e-mail addresses, names and more.

- Honeypot Checker
- SHODAN
- VirusTotal
- IBM X-Force Exchange
- MalwarePatrol
- BotScout
- Cymon.io
- Censys.io
- Hunter.io
- AlienVault OTX
- Clearbit
- BuiltWith
- FraudGuard
- IPinfo.io
- CIRCL.LU
- SeccurityTrails
- FullContact.com
- RiskIQ
- Citadel.pw

Collective Intelligence Framework (CIF)

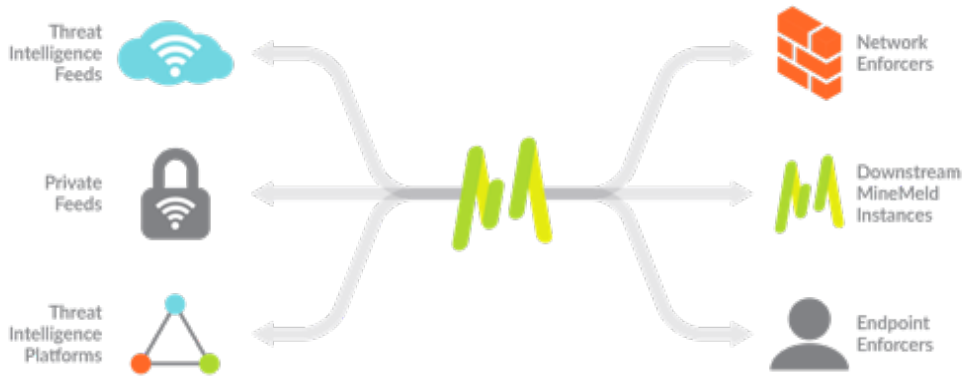
- REN-ISAC project
- Aggregates private and public feeds
- CLI and RESTful API
- Comes pre-configured with feeds
- Version
  - CIFv3 [Production Ready]
  - CIFv4 [Technology Preview]



MINEMELD

MineMeld supports a variety of use cases, with more being added each day by the community, including:

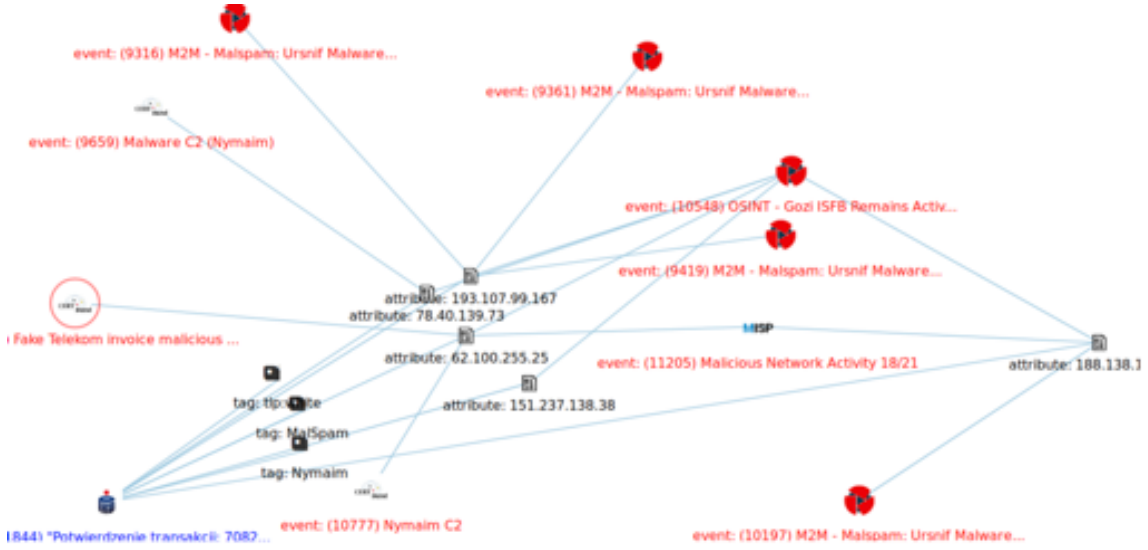
- Aggregation and correlation of threat intelligence feeds
- Enforcement of new prevention controls, including IP blacklists.
- Evaluate the value of a specific threat intelligence feed for your environment.
- Extract indicators from Palo Alto Networks device logs and share them with other security tools.
- Share indicators with trusted peers.
- Identify incoming sessions from Tor exit nodes for blocking or strict inspection.
- Track Office365 URLs and IPs



CIRCL MISP Threat Sharing

Co-financed by the European Union
Connecting Europe Facility

- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by a wide range of military or intelligence communities, private companies, the financial sector, National CERTs and LEAs globally.
- MISP is a threat information sharing free & open source software.
- CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing.
- A rich set of MISP modules to add expansion, import and export functionalities. A strong integration with other open source security projects such as TheHive, Cortex, cve-search,…



Other resources

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

References

Referencias

- INCIBE
  https://www.incibe-cert.es
- CCN-CERT
  https://www.ccn-cert.cni.es
- Bianco Piramid of Pain
  https://rvasec.com/slides/2014/Bianco_Pyramid%20of%20Pain.pdf
- Cyber's Most Wanted
  https://www.fbi.gov/wanted/cyber
- InfoTechnology
  https://www.infotechnology.com/online/Que-crimenes-cometieron-los-hackers-mas-buscados-del-FBI-piden-hasta-US-3-millones-20180725-0002.html
- MISP
  https://www.misp-project.org/
- Herman Slatman – Resource compilation (github)
  https://github.com/hslatman/awesome-threat-intelligence
- Ontotext
  https://www.ontotext.com/knowledgehub/fundamentals/dikw-pyramid/
- Sans - ThreatConnect
  https://digital-forensics.sans.org/summit-archives/cti_summit2014/The_Diamond_Model_for_Intrusion_Analysis_A_Primer_Andy_Pendergast.pdf

Referencias

- Software Engineering Institute. Carnegie Mellon University
  https://resources.sei.cmu.edu/asset_files/Presentation/2015_017_001_432139.pdf
- ICS Threat Intelligence and Active Defense, Dragos
  https://midwestreliability.org/MRODocuments/ICS%20Threat%20Intelligence%20and%20Active%20Defense%20%20Robert%20Lee.pdf
- How to use cyber kill chain model to build cybersecurity? Ireneusz Tarnowski
  https://tnc17.geant.org/getfile/3513
- List of data breaches
  https://en.wikipedia.org/wiki/List_of_data_breaches
- Tool compilation by hslatman/awesome-threat-intelligence (Github)
  https://github.com/hslatman/awesome-threat-intelligence
- Cognitive Techniques for Early Detection of Cybersecurity Events (umbc.edu)
  https://arxiv.org/pdf/1808.00116.pdf
- Collective Intelligence Framework
  https://csirtgadgets.com/collective-intelligence-framework
- Threat Intelligence on the Cheap, OWASP
  https://www.owasp.org/images/b/b2/OWASP_LA_Threat_Intel_Shane_MacDougall_2017_05.pdf
- OpenCTI
  https://www.opencti.io/en/
- Intelligence Preparation of the Cyber Environment - SANS Cyber Threat Intelligence Summit 2018
  https://www.youtube.com/watch?v=3bXr-CF9NBI&feature=youtu.be


Gracias!
Mila esker!