TF-CSIRT

TRANSITS I

Operational Module

07.12.2023

TBA Workshop, Abuja, Nigeria

Kamil Gapiński

Authors: Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis, Kamil Gapiński

Version: 7.3c

TF-CSIRT

Section 1: Introduction to Incident Management

Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis

TF-CSIRT

- Incident Handling
- Incident Response
- Incident Management
- Crisis Management

Photo by Jon Tyson on Unsplash

2. Incident Handling
1 – Incident Response *versus* Incident Handling

TF-CSIRT

- Complementary roles
  - Incident Response
    - Analysis and Containment
  - Incident Handling
    - Logistics and Communication
    - Planning and Coordination
    - Processes and Procedures
  - Incident Management
    - More high-level view, covers response and handling
    - Ability to provide and ensure start-to-finish management of incidents in repeatable, effective manner, in allign with the enterprise strategy.
- Different skill sets
- The bigger the incident, the more complex it will be:
  - Organize the activities
  - Hands-on analysis and technical work requires a dedicated mind
  - Provide support to the Incident responder

Photos by Julian Hochgesang and Kal Visuals on Unsplash

2. Incident Handling
2 – Incident Response *versus* Incident Handling

TF-CSIRT

- Real-time activities
  - Detection
  - Incident Handling
  - Incident Recovery
  - Investigation
  - Management
  - Legal
  - Communications

- Off-line activities
  - Policy
  - Preparation
  - Procedures for incident information tracking, incident reporting and handling
  - Post-mortem

Photo by Neonbrand on Unsplash

2. Incident Handling
3 – Passive vs. Active defense

TF-CSIRT

- **Passive defense**:
  - Firewalls
  - AV Solution, EDR, XDRs
  - SIEM
  - WAF

- **Active defense**:
  - Adapting to the current threat
  - Adjusting filters upon analysis results
  - Threat intelligence

- **Active defense is NOT 'hacking back'**
  - We act / react to the current threat
  - But we stay within the legal boundaries

Photo by Will Porada on Unsplash

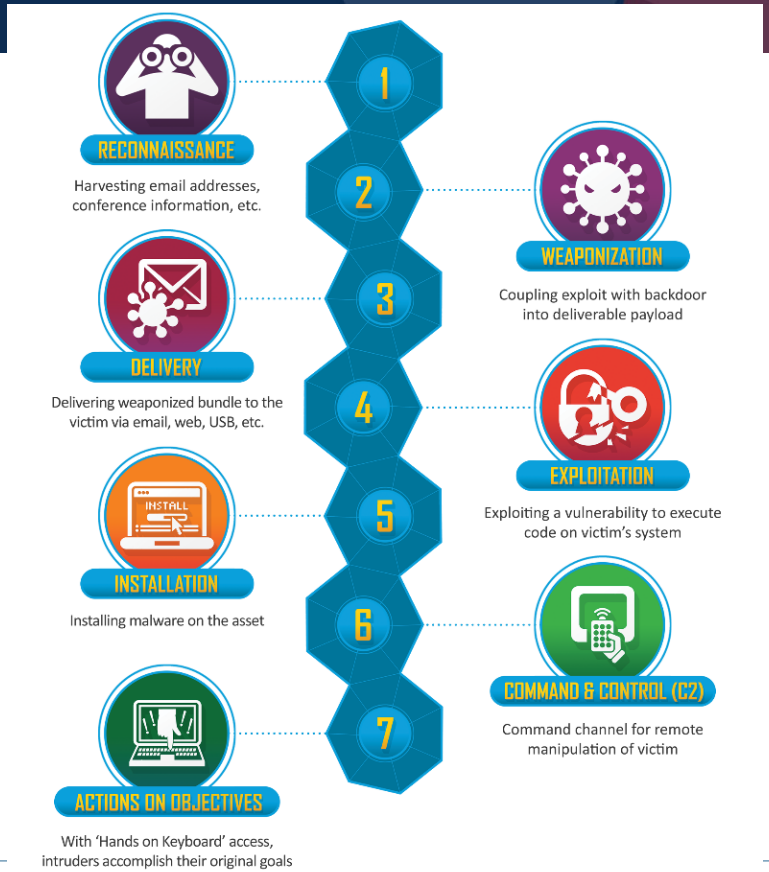
2. Incident Handling
4 – For smaller teams

TF-CSIRT

- Some incident handling teams are **as little as 2 people**
  - Simple tools for coordination and logging
  - No dimensioning issues
  - Excel spreadsheets, Wiki
- Split between Incident Response and Incident Handling
  - IR: Technical matters
  - IH: taking care of the constituency/executive/management
- Coordination
- Even more important to protect Incident Responder(s) from everything else
  - Don't bother ”hands-on” staff
  - Remember fire-workers or police officers

Photo by David Von Diemar on Unsplash

2. Incident Handling
5 – Cyber Kill Chain



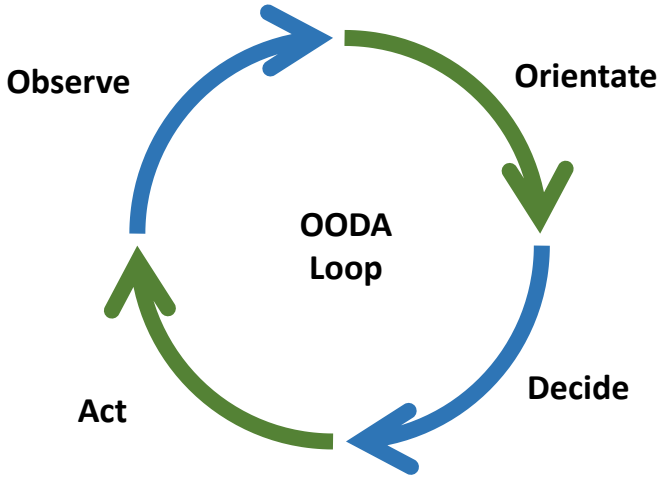
- **Crisis** is an unexpected threat to your constituency that demands decisions to be taken quickly and **out of usual procedures**.
- Incident response can be a part of the larger crisis management plan.
- The ultimate goals of the organisation are to keep essential services running and limit damages.

- Crisis will affect:
  - Roles in incident management
  - Level of services provided
  - Who you respond to
  - Decision making process
  - Availability of resources

- Various flavors
    - Observe Orientate Decide Act (OODA loop) → June 1995, John R. Boyd
    - “Computer Incident Response Guidebook” → US Navy, August 1996

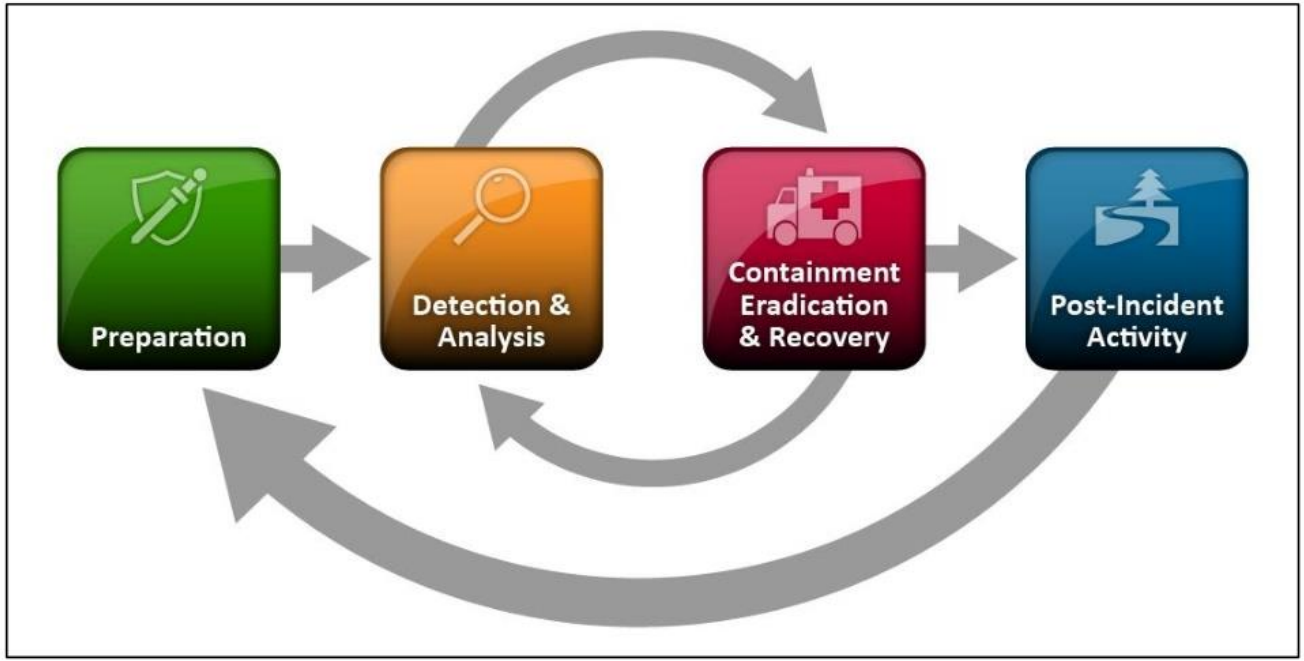
- 3 best known models
    - SANS “6-steps Incident Handling” → Early 1990s
    - NIST SP800-61 “Computer Security Incident Handling Guide”
        - January 2004, latest update in August 2012 (release v2)
    - ENISA ”Good Practice Guide for Incident Management” → December 2010

OODA Loop: Observe - Orientate - Decide - Act



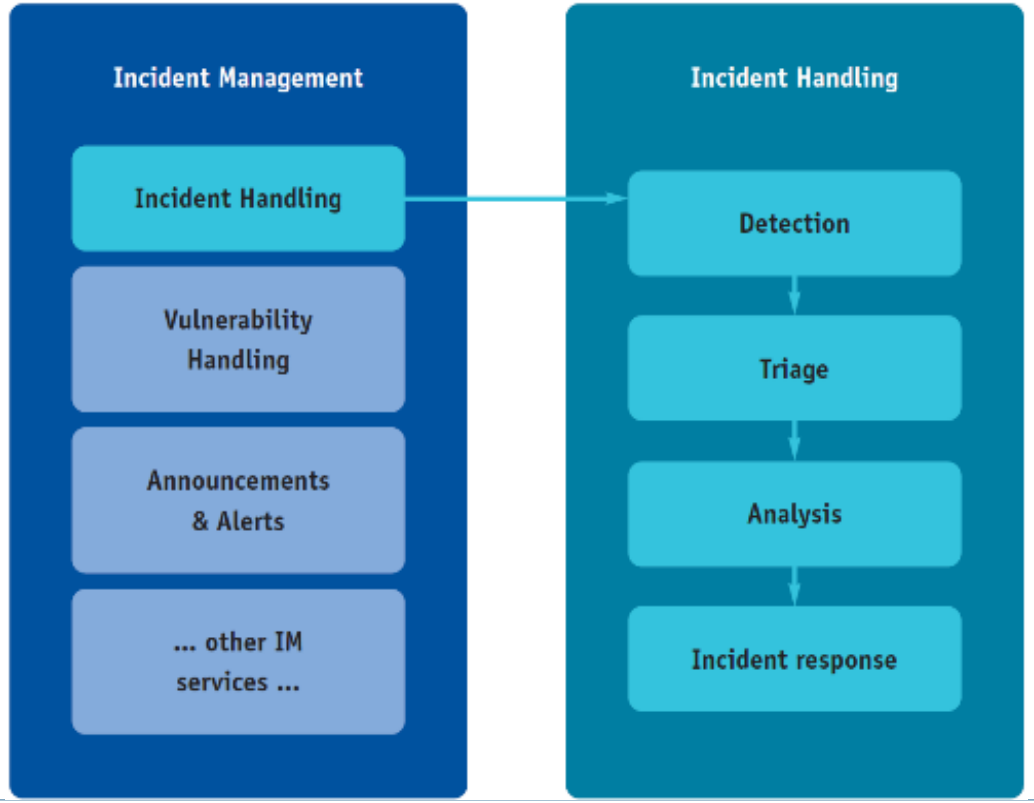
TF-CSIRT

NIST SP 800-61 rev 2 (2012)



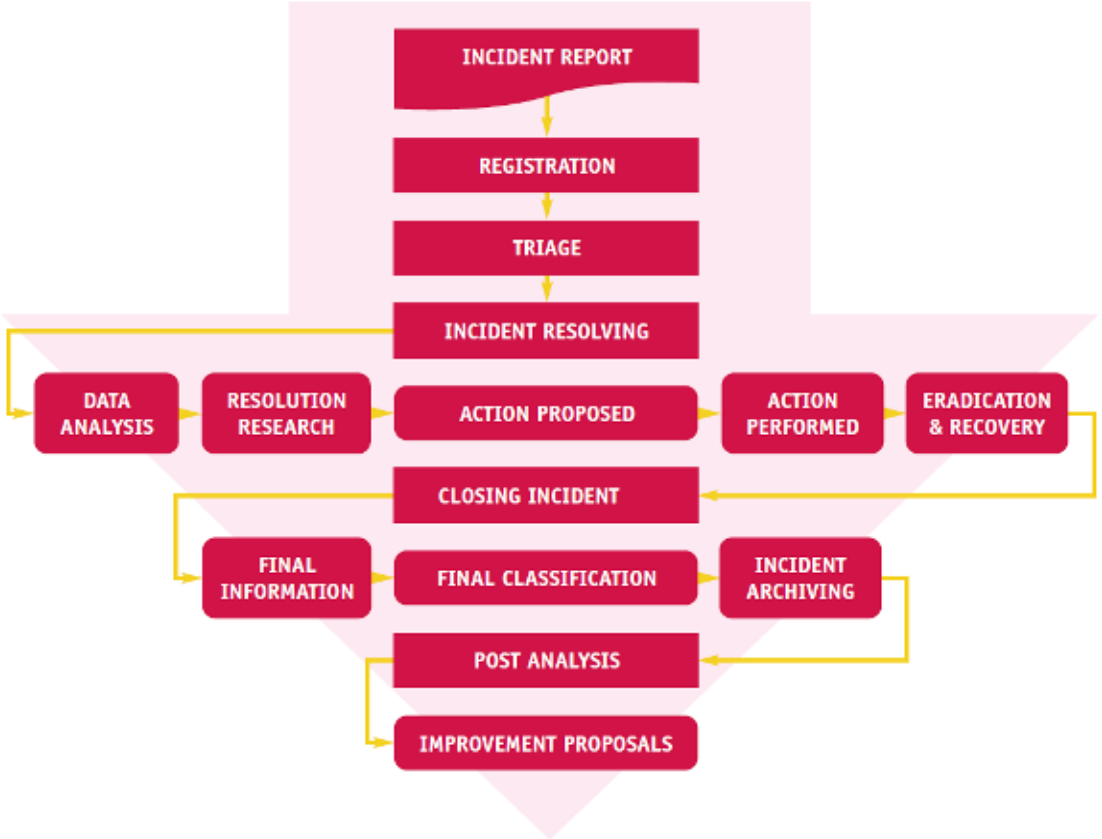
TF-CSIRT

ENISA Model for Incident Management



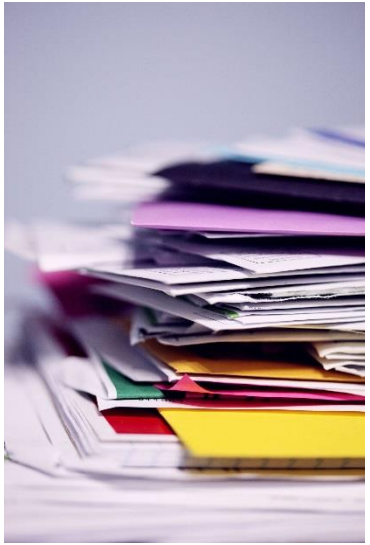
TF-CSIRT

ENISA “Good Practice Guide for Incident Management” (p.34)



TF-CSIRT

- Understand Incident handlers' work
  - *Know your team*
  - *Know your perimeter*
  - *Know the processes*



- 3 Stages
  - *Preparation* → be ready
  - *Run* → follow the rules
  - *Capitalize* → improve the preparation and process(es) – get faster

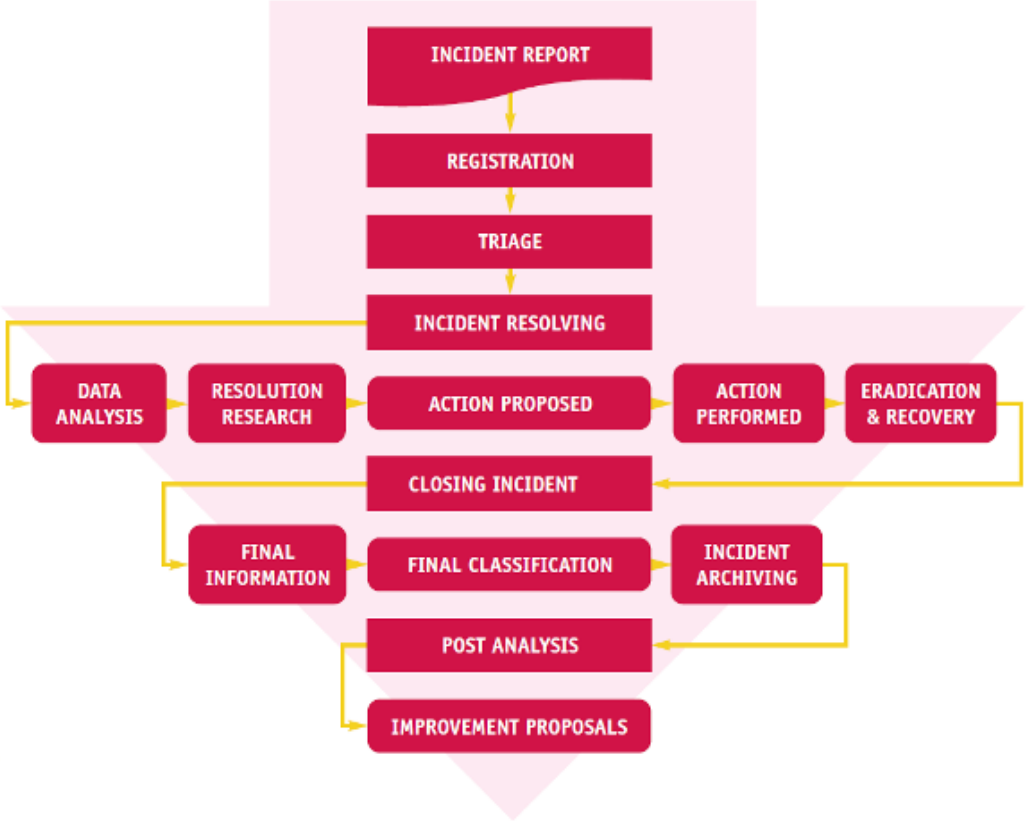
TF-CSIRT

Section 2: Incident Handling

ENISA Approach

Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis

Section 2: Incident Handling
ENISA Workflow Overview

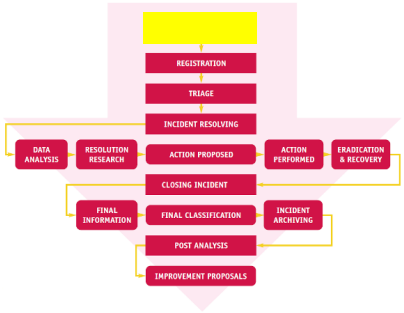


TF-CSIRT

- Initial input
  - Issue/problem/incident received by the CSIRT
  - Must offer multiple way to reach the CSIRT, in case of outages, attacks...

- Aim:
  - Getting the best at first
  - Aggregating data fast
  - Keep it easy for the submitters, read “simple emails”

INCIDENT REPORT



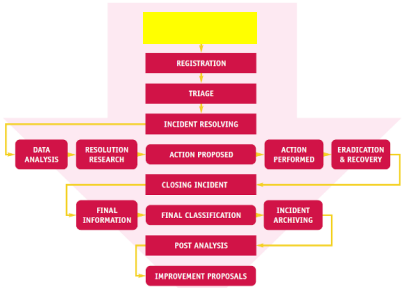
TF-CSIRT

- Automate the incident report intake process as much as you can.
- Full automation to input of incident details looks like a dream… but

1. Needs to find a commonly agreed terminology that fits everyone, every case, every tool...

2. Evaluate the number of incidents reported on a standard day... and see if it's worth it

INCIDENT REPORT

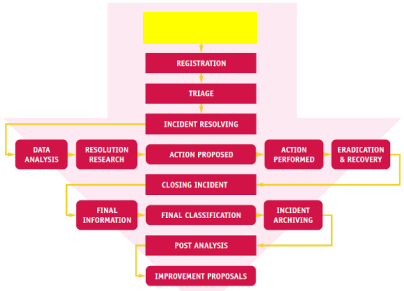


TF-CSIRT

- Feeds (detection, threat intelligence…)
- Noise reduction
- Integration with ticketing system – set-up a link between the email handling system and incident handling system
- Move from a **reactive posture** (waiting for e-mails) to a **proactive one**:
  - Integrate tools (IDS probes, scanners, feeds, …)
  - Integrate third-parties to (automatically) report incidents
  - Integrate information collected on the web (forums, file repository, …)

This is a SOC

INCIDENT REPORT



TBA CSIRT OPERATIONS EXERCISE: CSIRT/SOC Report Intake Channels Exercise

In this exercise, you will identify and analyze all possible channels through which reports can be received by a Computer Emergency Response Team (CERT) and Security Operations Center (SOC). Understanding these channels is crucial for effectively capturing and responding to security incidents.

1. **Understanding intake channels**

   Intake channels are the various means through which CERTs and SOCs receive reports about potential security incidents. These channels are vital for the initial detection and subsequent management of incidents.

2. **Brainstorming session**

   - Individually or in small groups, brainstorm all potential intake channels that CERTs and SOCs might use. Think broadly and consider both traditional and innovative methods.
   - Consider channels that vary in formality, speed, and source.

3. **Listing possible channels**

   - Compile a comprehensive list of these channels. Examples might include email alerts, phone calls, …
   - Analyze each channel for its effectiveness, reliability, speed of communication, and the type of information typically received through it.

4. **Discussion and presentation**:

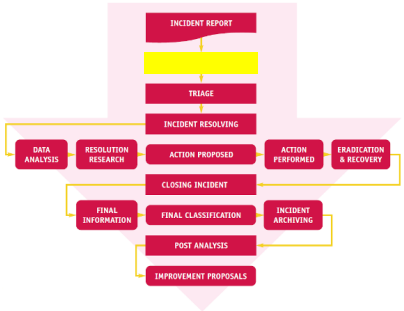
   - Discuss within your group and Prepare your findings, highlighting the most effective channels for different types of incidents and events.

Section 2: Incident Management Models – ENISA
2 – Registration

TF-CSIRT

- Registration process is easier with an incident report registration form and ticketing system
  - Define the most useful/required fields
- Assign a unique number for tracking
- Leave ground for aggregating/merging various tickets dealing with a single incident...
- … but what appears to be a single incident at first may turn out to be different cases
- What if we have a lot of systems where we can register an incident? (ticketing system, SIEM, SOAR, spreadsheets?!)

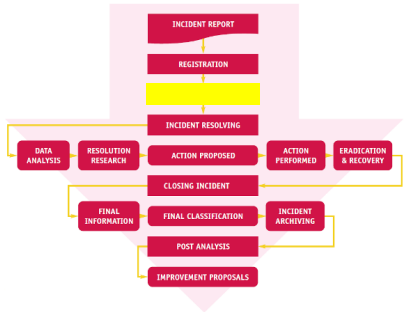
REGISTRATION



TF-CSIRT

- Triage comes from a French medical term
  - When confronted with a massive arrival of victims, with only a few medical resources
  - You need a way to handle all cases in the best way
  - In a limited amount of time

TRIAGE



TF-CSIRT

- Triage has 4 Steps
  - Verification
  - Initial Classification
  - Assign severity and priority
  - Assignment to an incident handler (or self-assingment…)

TRIAGE

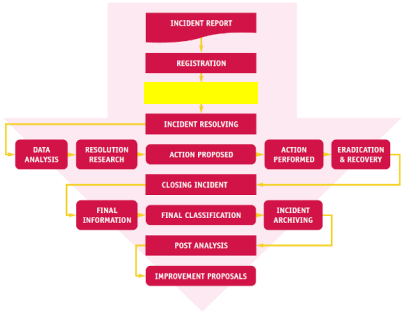


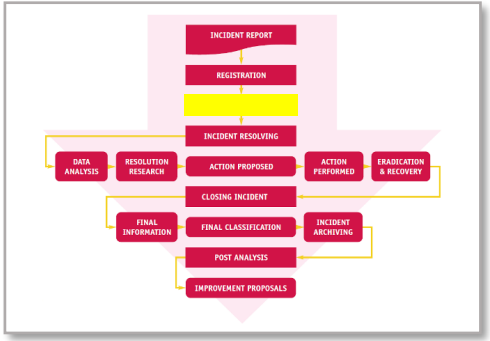
Photo by Erika Giraud on Unsplash

TF-CSIRT

- Verification
  - Is it out of scope / out of perimeter
    - Messages written in a foreign or cryptic alphabet
    - Event not considered an incident by CSIRT standards
    - Component is not part of the CSIRT constituency
    - Dubious source of the notification
  - What is the policy for notification of no interest?

- **Are you ready to send an ACK?**
- **Do you need additional details?**

TRIAGE

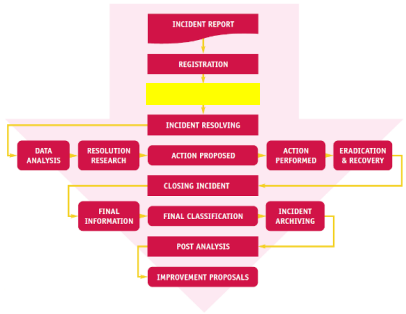


TF-CSIRT

- Incident Initial Classification
- Severity Assessment
- The Initial classification may not be the right one
  - Additional details may suggest to change classification

- Possible to send an ACK to the notification reporter
  - Ticket number
  - Hints on the following steps
- Prioritization
  - Dealing with the most severe cases first

TRIAGE

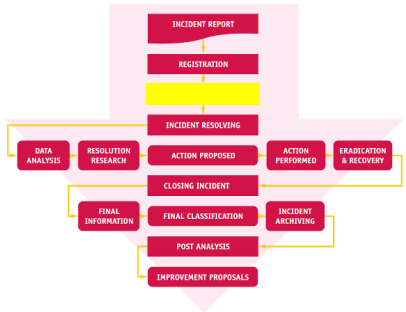


Section 2: Incident Management Models – ENISA
3 – Triage

TF-CSIRT

- Incident initial classification / severity assessment / prioritization
  - Some criteria for prioritization
    - Security requirements of the target
    - Business impact
    - Type of attacks
    - Strength of the attacks
    - Standalone attack or multiple attacks
    - SLA with the constituency
- Criteria may vary depending on the CSIRTs role and activities
  - Gov CSIRT versus commercial CSIRT
  - Internal CSIRT versus product-oriented CSIRT
- Classification may decide on the amount of effort that will be allocated to the handling of the incident

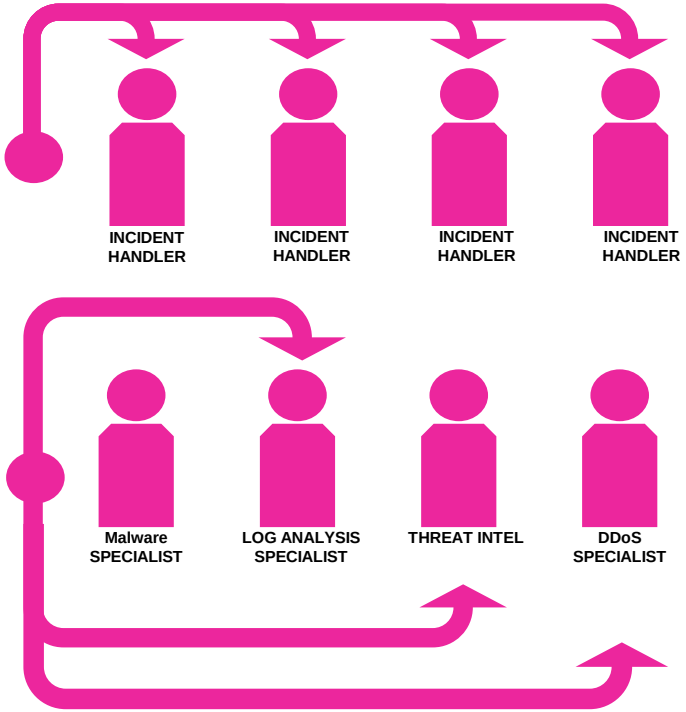
TRIAGE



Section 2: Incident Management Models – ENISA 3 – Triage

TF-CSIRT

- Incident Assignment
  - The Ticket can be assigned to an Incident Handler
  - Criteria for assignment
    - Expertise or capabilities,
    - Resource availability
    - Knowledge
    - Soft vs hard skills
- Roles and tasks
  - Must be defined according to the procedures – who decides on what?
  - Split technical, reporting and/or communication roles



TF-CSIRT

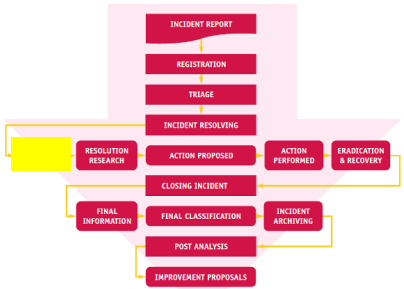
- Gather more data:
  - Look for details to support the effort of incident handling
  - Readily available data in the notification form, including point of contacts, date, targeted environments
  - Incident knowledge base
  - Live data from sensors and monitoring systems
  - Logs from security components

- May discover other victims that are not yet aware of the incident
- May deduce the next potential victim

INCIDENT RESOLUTION

-

DATA ANALYSIS



TF-CSIRT

- May require to liaise with **technical** partners
  - Hosting companies, ISP, content providers
  - HW/SW suppliers, application vendors
  - Service providers
- May require to liaise with **business** partners
  - Partners, sub-contractors
  - Service providers
- May require to liaise with **authorities**
  - Law enforcement agencies (LEA)
- Airport approach, fast overlook, more and more detailed when reaching the point of interest

Digging and analyzing down to details *versus* adapting the level of analysis

INCIDENT RESOLUTION

-

DATA ANALYSIS

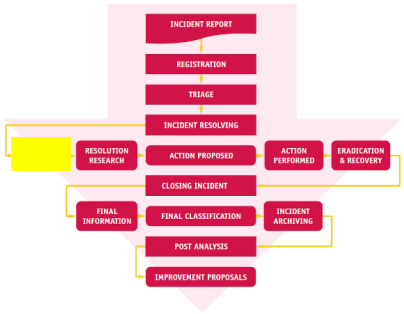


Photo by Sebastian Grochowicz on Unsplash

TF-CSIRT

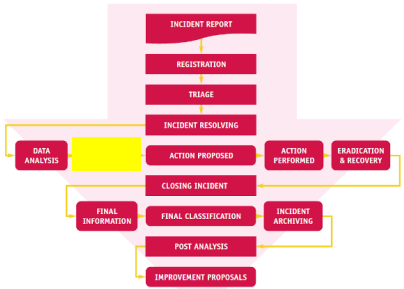
- Review data, analyze and see if it points to a resolution
- SOPs: Standard Operations Procedures (aka playbooks)
- Be prepared to get more expertise onboard
- Usually collection of 20-30% of possible information gives you potentially about 80% of answers

- Global research approach with tracks
  - Independent tracks and researches
  - Project management, brainstorming, tasks, meetings
- Review sessions are very important
  - Key role of the incident manager

INCIDENT RESOLUTION

-

RESOLUTION RESEARCH



Section 2: Incident Management Models – ENISA
7 – Action Proposed

TF-CSIRT

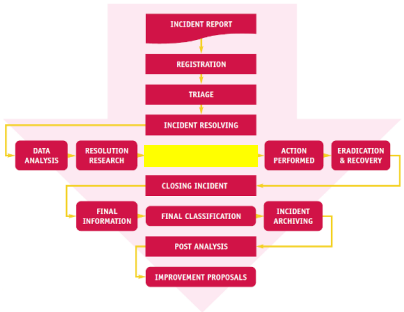
- Present the next steps to the business managers or decision makers
- Proposed actions must be explained according to the audience
  - Technical, business, legal, human resources, …

- Examples:
  - Looking for the origin of the attack
  - Stopping versus mitigation an attack
  - Moving to a backup environment

INCIDENT RESOLUTION

-

ACTIONS PROPOSED



Section 2: Incident Management Models – ENISA
8 – Actions Performed

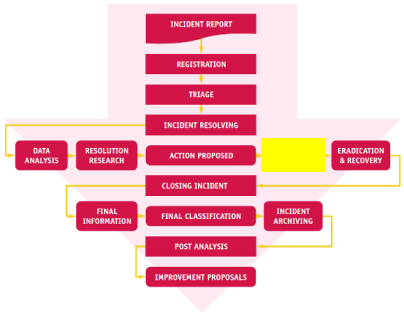
TF-CSIRT

- Actions can be performed by incident team, responders (e.g. administrators) or subcontracted to third-parties
- In all cases, everyone must stick to the plan
- Results may influence choices
- Check if an action has been performed (correctly)
- Document (what has been done and when)
- Communicate

INCIDENT RESOLUTION

-

ACTIONS PERFORMED



TF-CSIRT

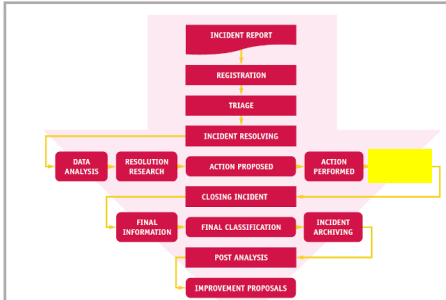
- Main goal: getting rid of the incident
- Eradication
  - No more effects
  - No risk of new compromise
- Recovery
  - Getting back to the pre-incident context
- Business restoration
  - RTO: recovery time objective
  - RPO: recovery point objective

INCIDENT RESOLUTION

-

ERADICATION

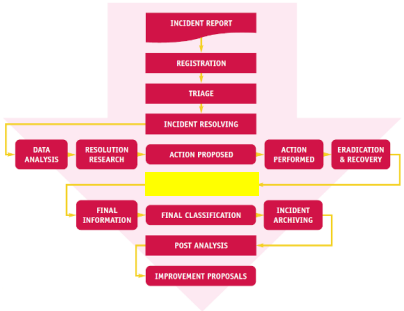
& RECOVERY



TF-CSIRT

- Keep an eye on open tickets or updated events updates might change the game.
- Spend 10 seconds more on data gathering, diagnosing and team planning and save time and improve safety for the next 10 minutes.

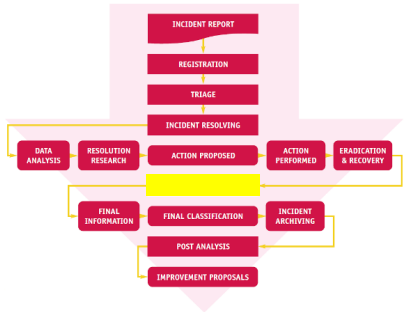
INCIDENT RESOLUTION



TF-CSIRT

- Last but not least, this is the end of the incident
- No longer an issue
- Who decides the incident is closed?
- What if there is a legal action?
- Were sensors and attack detectors added and/or tuned? Should you keep the current settings or change them?

INCIDENT CLOSING

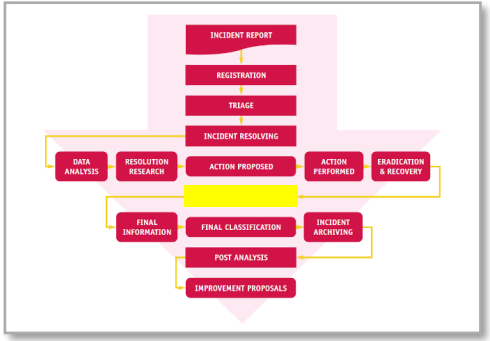


TF-CSIRT

- An incident is finished for the **incident handler**, when …
  - All tasks have been fulfilled
  - Activities have been documented
  - The incident ticket is closed with all required details

- An incident is finished for the **incident manager**, when …
  - The required incident handling tasks have all been done
  - The incident ticket is not re-opened within a give amount of time
  - The closure of the ticket can be validated
  - The artifacts, collected items, logs and documentation have been indexed and secured

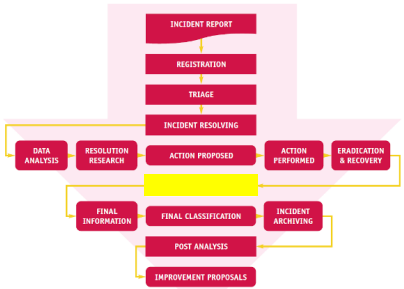
INCIDENT CLOSING



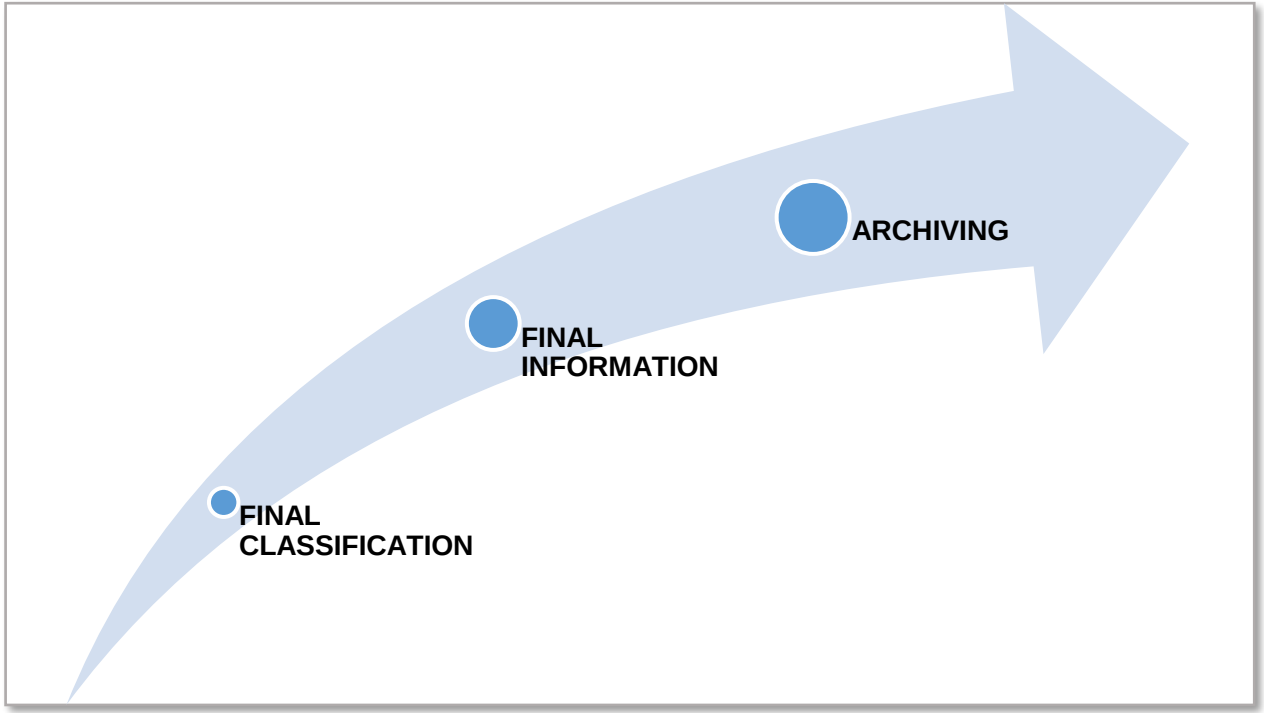
TF-CSIRT

- An incident is finished for the **victim**, when …
  - Business is back to usual
  - The victim
    - Knows the basic actions to take if ever the same incident (or similar) happens again
    - Knows for sure who to contact if ever the same incident (or similar) happens again
    - The victim receives a formal notification of the closure

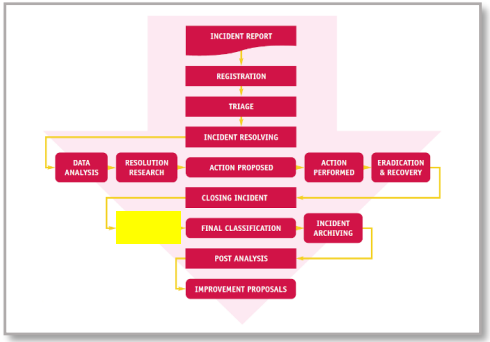
INCIDENT CLOSING



Section 2: Incident Management Models – ENISA
10 – Incident Closing



INCIDENT CLOSING



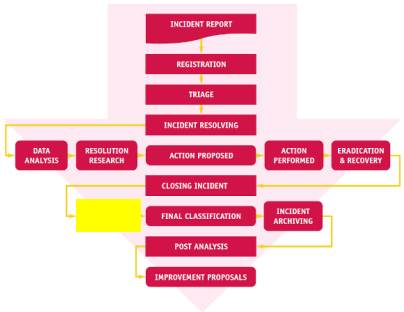
TF-CSIRT

- What are the messages to release
  - Targets, potential and real impacts, current status
  - Main findings
  - Summary of the issues encountered and work done
  - Level of understanding and complexity of the attack
  - New assessed security level
  - Recommendations, follow-up steps
  - Adjust the message to the audience
- Who should deliver the message?
  - The incident manager or the CSIRT leader
  - Able to use different levels of explanations
- Who should support afterward?

INCIDENT CLOSING

-

FINAL INFORMATION



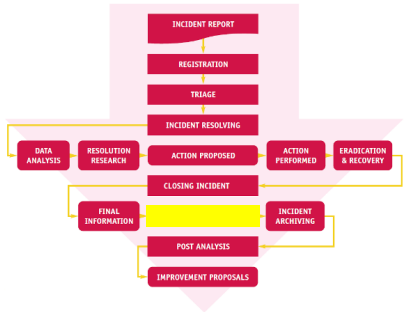
TF-CSIRT

- Final classification may be different from the initial one
  - Initial: based on elements available at the start
  - Resolution step: during the action phase, while tackling the issue
  - Final: global and final understanding of the incident
- Classification can be useful to speed up the triage phase
  - Helps starting in the right direction thanks to additional details
- Risk of final classification
  - Focusing on the classification sub-categories
  - Instead of spending time on extending the criteria and details that help classify

INCIDENT CLOSING

-

FINAL CLASSIFICATION



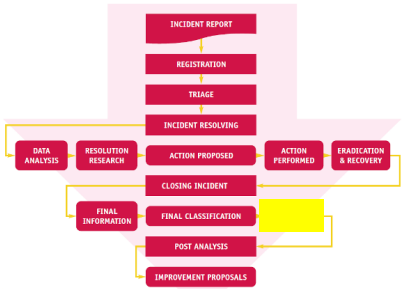
TF-CSIRT

- Archives
  - Accessible for the team members
  - If an incident occurs again, easier to follow a path that worked
  - Archive contain all steps to solve the incident
- Built-in function
  vs. CSIRT dedicated solution
  vs. Organization-wide solution
- Privacy regulations and data retention aspects

INCIDENT CLOSING

-

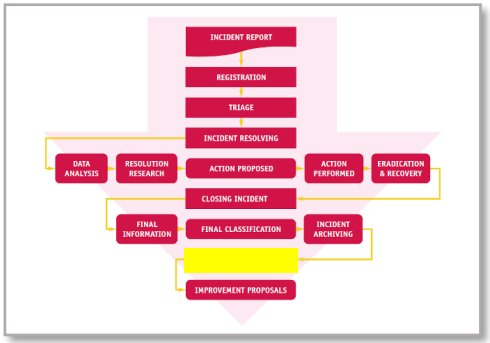
ARCHIVING



Section 2: Incident Management Models – ENISA
14 – Post Analysis

TF-CSIRT

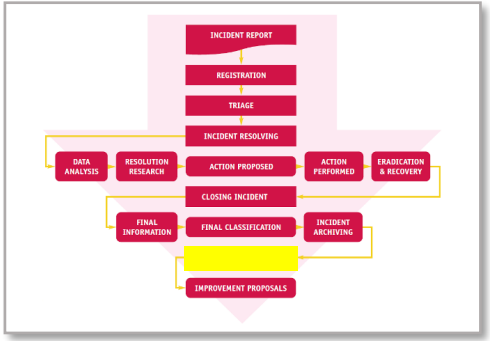
Post Analysis



TF-CSIRT

- Should only start **after** the incident is closed
  - Resistance from IHs:
    - As it is closed, why waste more time on it?
    - We did it, so why are you investigating our own activities?
    - We have other incidents to deal with!
    - Hummm … you do paper work, we do real work …
    - Off-line quality versus live incidents
- How can this be organized?
  - Have dedicated people follow the incident handling from its start
  - Organize regular post-incident analysis and feedback sessions
- Should post analysis be performed for all incidents?

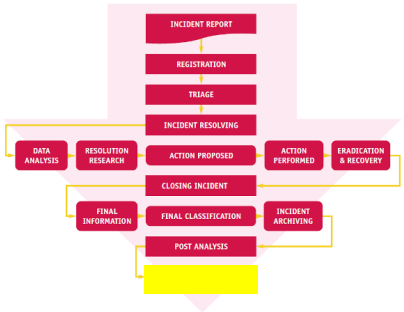
POST ANALYSIS



TF-CSIRT

- Based on previous post-analysis sessions
  - What went wrong?
  - What should have been done to prevent that?
  - Who may benefit from these improvements?
    - Internal team
    - External team
- Benefits
  - Better incident handling process
  - Easier relationships with CSIRTs and other stakeholders

FINAL RECOMMENDATIONS



TBA CSIRT OPERATIONS EXERCISE: Developing Final Incident Report Template

Your goal is to create a final report template that is both comprehensive and practical. The report will be consulted both by technical people, business owners and management.

1. Team collaboration

   - Work collaboratively within your group to discuss and decide on the key elements your template will include.
   - Consider the flow of information in the report and how each section will contribute to a clear understanding of the incident. Use the knowledge and insights from the incident handling process explained by the trainee.

2. Developing the template

   - Start by outlining the main sections and sub-sections your report will contain, discuss and define what specific information each section should capture.

3. Consideration of different scenarios

   - Think about various incident types (e.g., data breaches, malware attacks) and ensure your template is versatile enough to accommodate different scenarios.

4. Presentation

   - Prepare to present your template to the other groups, explain the rationale behind the structure and content choices in your template.

TF-CSIRT

Section 3: Incident Management

Real world challenges in Incident Management / Incident Handling

Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis, Kamil Gapiński

Section 3: Real world challenges
CSIRT vs SOC

TF-CSIRT

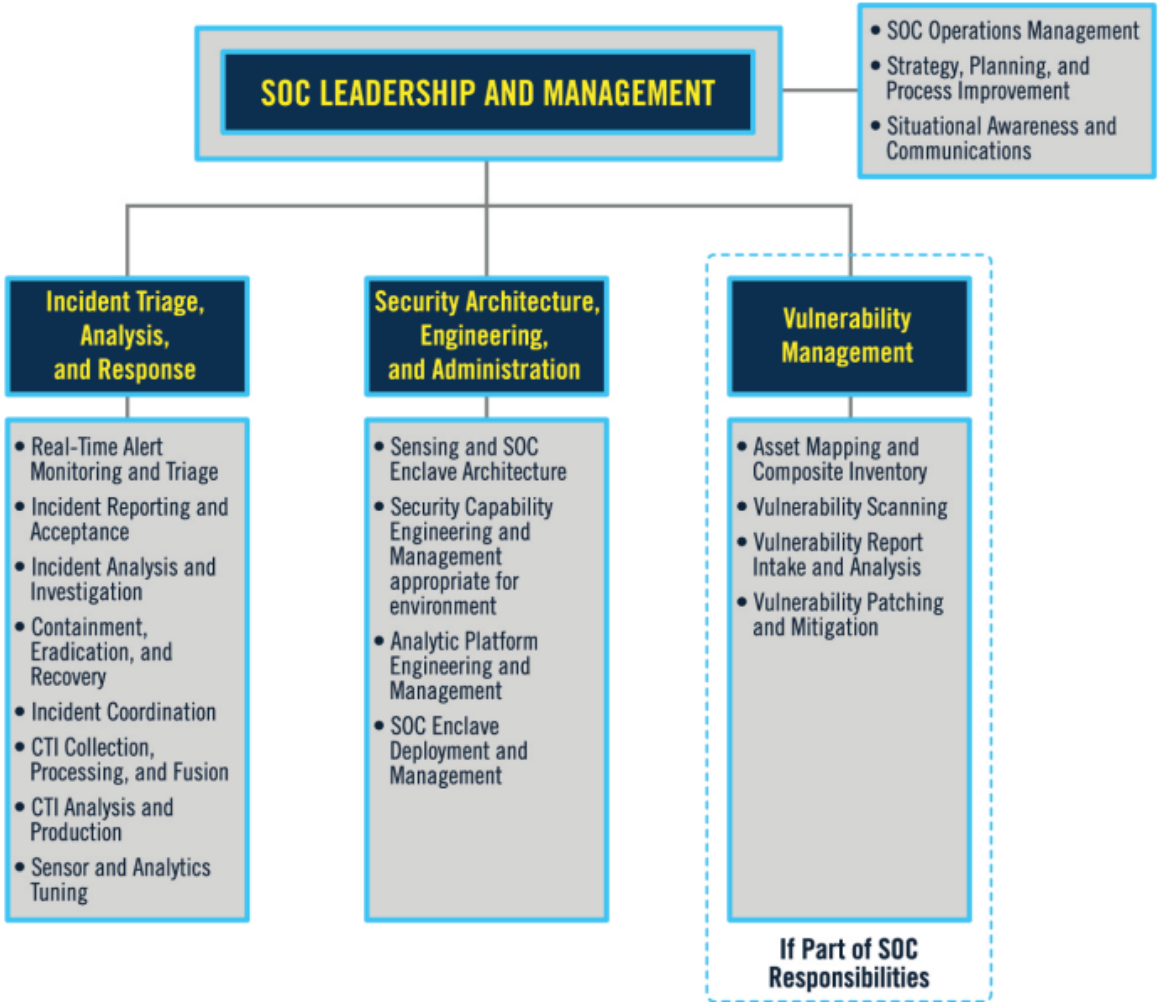
CSIRT services (FIRST.org CSIRT service framework)

Information Security Event Management	Information Security Incident Management	Vulnerability Management	Situational Awareness	Knowledge Transfer
•Monitoring and Detection •Analyzing	•Accepting Reports •Analyzing Incidents •Analyzing Artefacts and Forensic Evidence •Mitigation and Recovery •Coordination	•Vulnerability Discovery •Report Intake •Analysis •Coordination •Disclosure •Response	•Data Acquisition •Analysis and Synthesis •Communication	•Awareness Building •Training and Education •Exercises •Technical and Policy Advisory

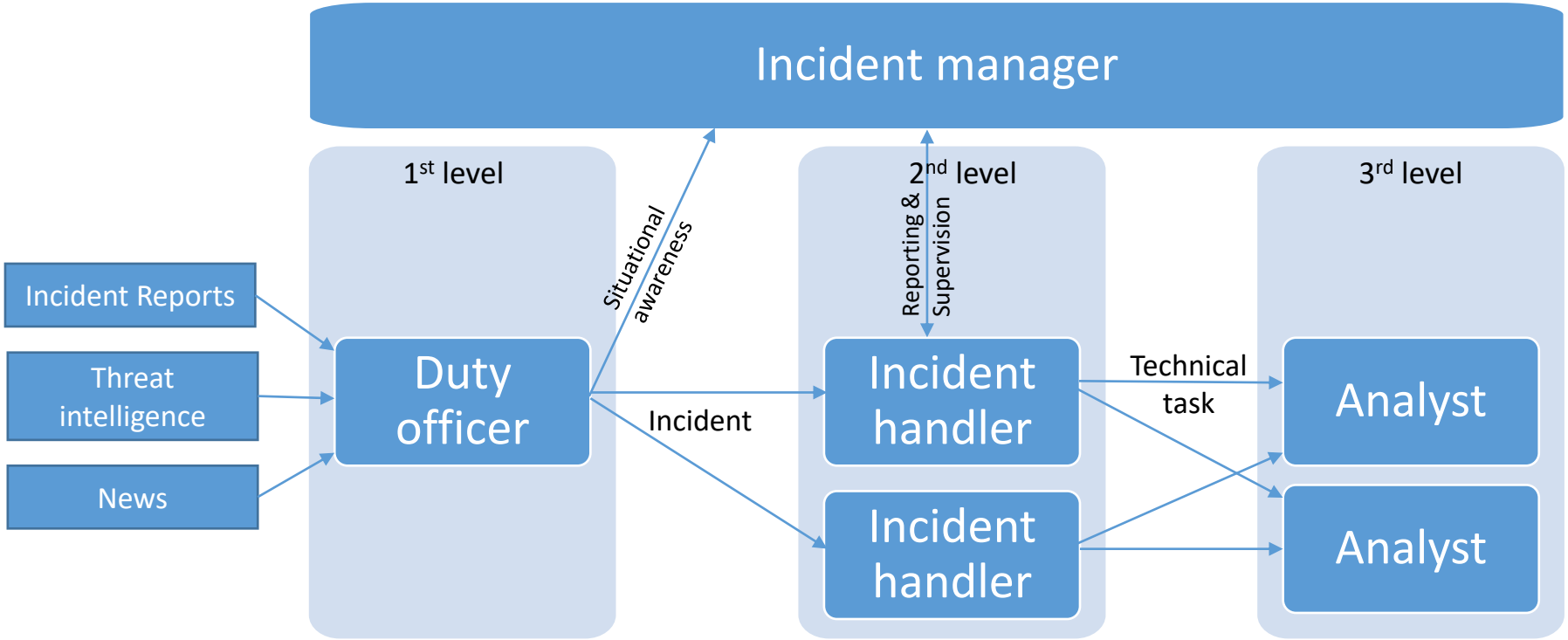
SOC services (SOC-CMM)

Security Monitoring	Security Incident Management	Security Analysis & Forensics	Threat Intelligence	Threat hunting	Vulnerability Management	Log Management

Section 3: Real world challenges
CSIRT vs SOC



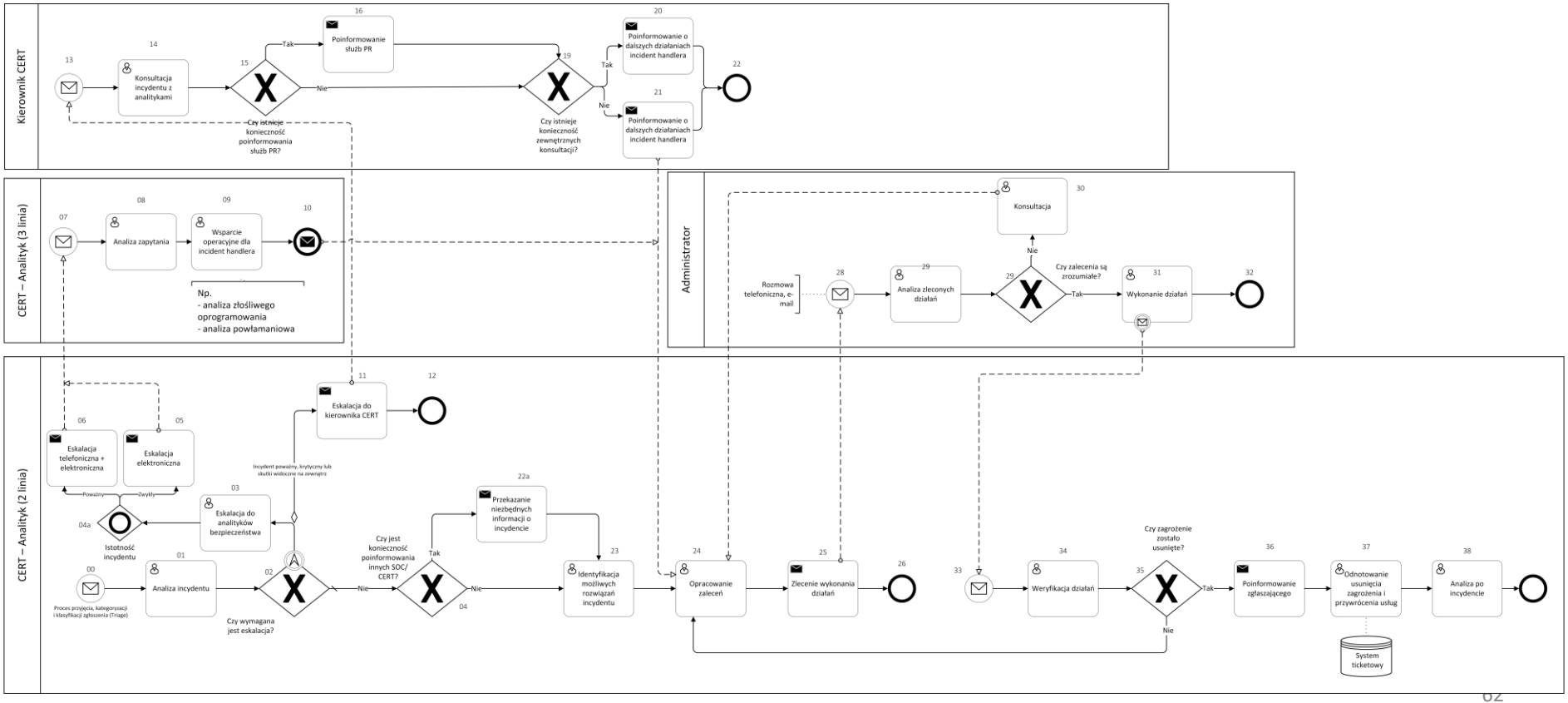
TF-CSIRT


Incident manager
1st level
2nd level
3rd level
Situational awareness
Reporting & Supervision
Incident Reports
Threat intelligence
News
Duty officer
Incident
Incident handler
Incident handler
Technical task
Analyst
Analyst

- Triage officer
- Communication officer
- PR officer
- Legal officer
- Team Manager
- Any others?

- Not all roles require strong technical skills – communication is essential, too!
- Split roles as the number of tasks and the size of the team grow.
- People are more motivated and efficient when they do what they are best at.

Section 3: Real world challenges
Detailed workflow



Governance issue #1:

You want to handle the incident, but what does the victim want?

> Incident handling may not be key to the victims
> Victims may rather wish to restart operation ASAP...
> ...with the risk of deleting or spoiling artifacts

Business driven criteria & decisions – Management's enforcement

Governance issue #2:

What drives incident handling?

Recovering from the incident and going back to business?
Preventing the incident from spreading any further?
Determining the origin of the incident?

Business driven criteria & decisions – Management's enforcement

Governance issue #3:

What can be said about the incident?

Keep it under the carpet
(Possibly limited) Notification is compulsory by law or regulation
Share with peers
General public communication

Business driven criteria & decisions – Management's enforcement

Governance issue #4:
Crisis Management

What if there is a crisis, what is the role of the CSIRT

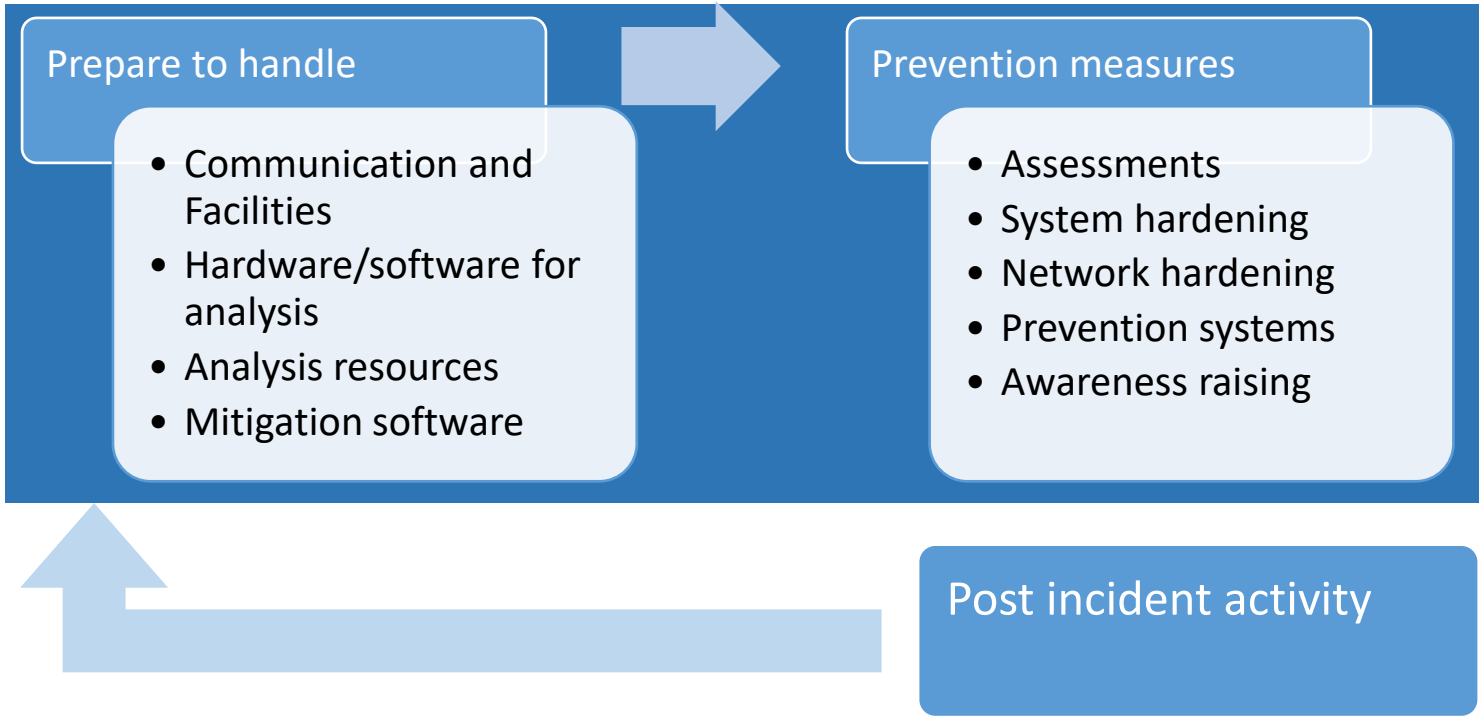
Business driven criteria & decisions – Management's enforcement

Governance issue #5:
Information leakage

What if some press agency announces a public report right now – or in the coming days – but you still want to investigate / monitor the attacker(s)?

Business driven criteria & decisions – Management's enforcement

TF-CSIRT


Prepare to handle
Communication and Facilities
Hardware/software for analysis
Analysis resources
Mitigation software
Prevention measures
Assessments
System hardening
Network hardening
Prevention systems
Awareness raising
Post incident activity

TF-CSIRT

- Establish ground rules
- Never pay for ransomware attack
- Always report to the police

Photo by Joshua Rodriguez on Unsplash

TF-CSIRT

- How to keep working when everything falls apart
- When not to keep working

Photo by Nadine Shaabana on Unsplash

- If you are under attack you might not …
  - be able to use e-mail
  - be able to use your phone system
- How do you communicate?
  - Think about address books and contacts
  - PGP keyrings
  - Access to your tools

- If your own tooling is the target?

- Or, how to continue working if the people can't anymore?
  - Look for signs of burned-out members
  - Plan for replacements
  - Prepare a hand-over process

- Sometimes resolving incidents takes time; hours, days, weeks.
  - Hours: Make sure to include breaks and provide food and drinks
  - Days: Think about replacing members; have replacement ready and up-to-date
  - Weeks: Set up a rotation schedule

- Be prepared you have to force members to stop working.

TF-CSIRT

- On-site
  - Local environment with full access to internet resources
  - If the incident is local or the teams are local
- Off-site
  - When handling incidents on call, working from home
  - Sometimes, staff must be sent to a remote site
  - Can be geographically far away, with different time-zones
    - **Need a logistical support**
  - Need standalone components
  - Need secured communications with the headquarters

Photo by Outside Co and Loic Mermilliod on Unsplash

TF-CSIRT

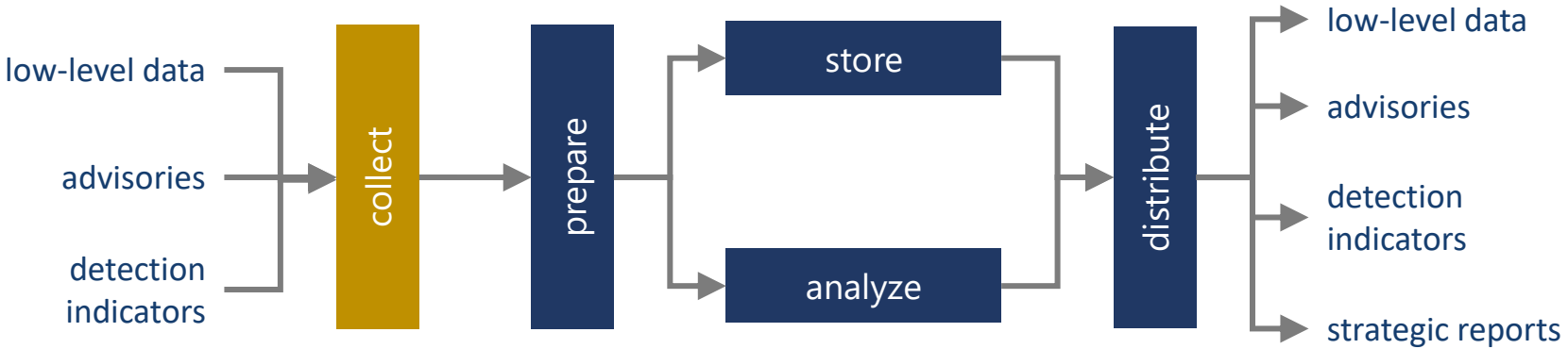
Section 4: Data Acquisition & Threat Intelligence

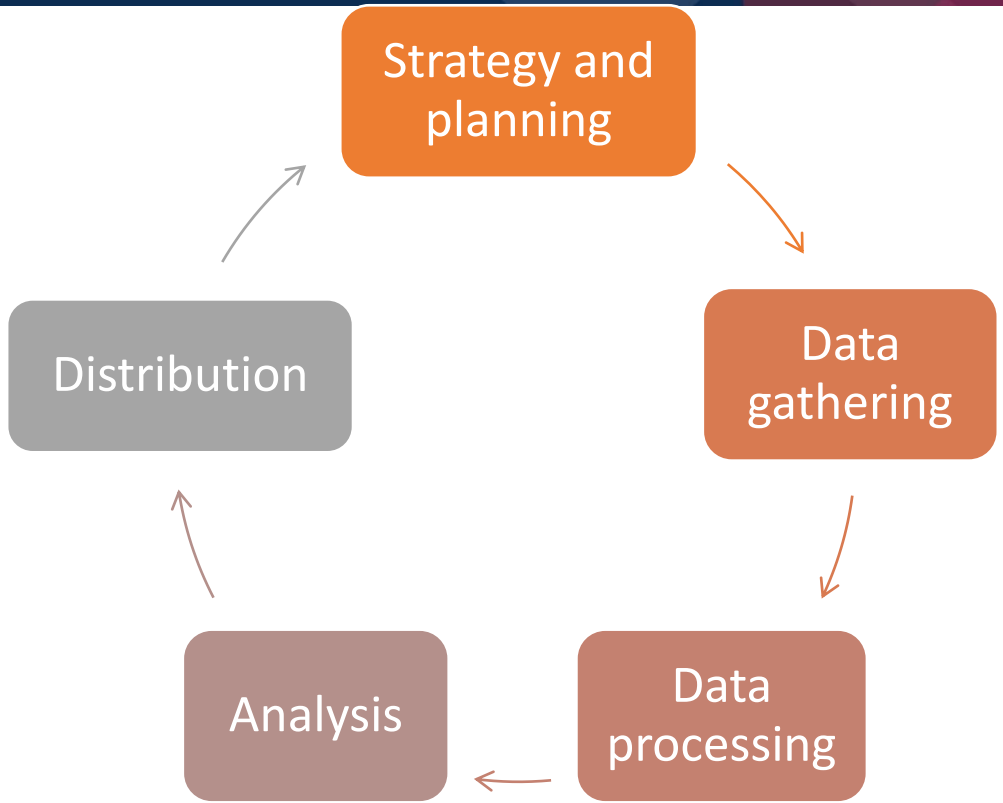
Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis

- **Threat intelligence** is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. (Gartner)
- Examples:
  - Feed of malicious URLs from a popular vendor
  - Analysis of *EvilStalker* malware
  - Report on *APT-1337* actor's TTPs (tactics, techniques, procedures)

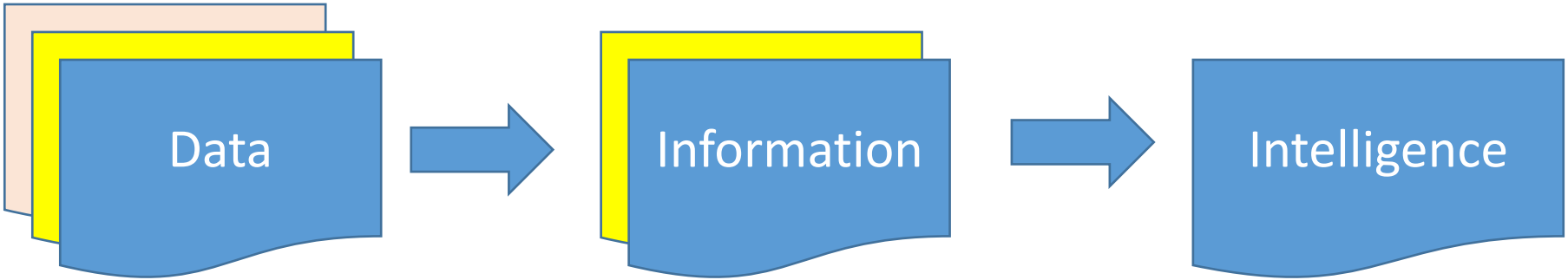
- **Actionable Information** is information that can be examined, expanded, and compared, leading to solid observations and conclusions. It should be ***relevant, timely, accurate, complete*** and ***ingestible***. (ENISA)
- Examples:
  - Vulnerability advisory for a product you are using
  - Need for a new security control which addresses malicious software or tool
  - List of IP addresses in your network that looked up a known malicious domain name

TF-CSIRT


low-level data
advisories
detection indicators
collect
prepare
store
analyze
distribute
low-level data
advisories
detection indicators
strategic reports


Strategy and planning
Data gathering
Data processing
Analysis
Distribution

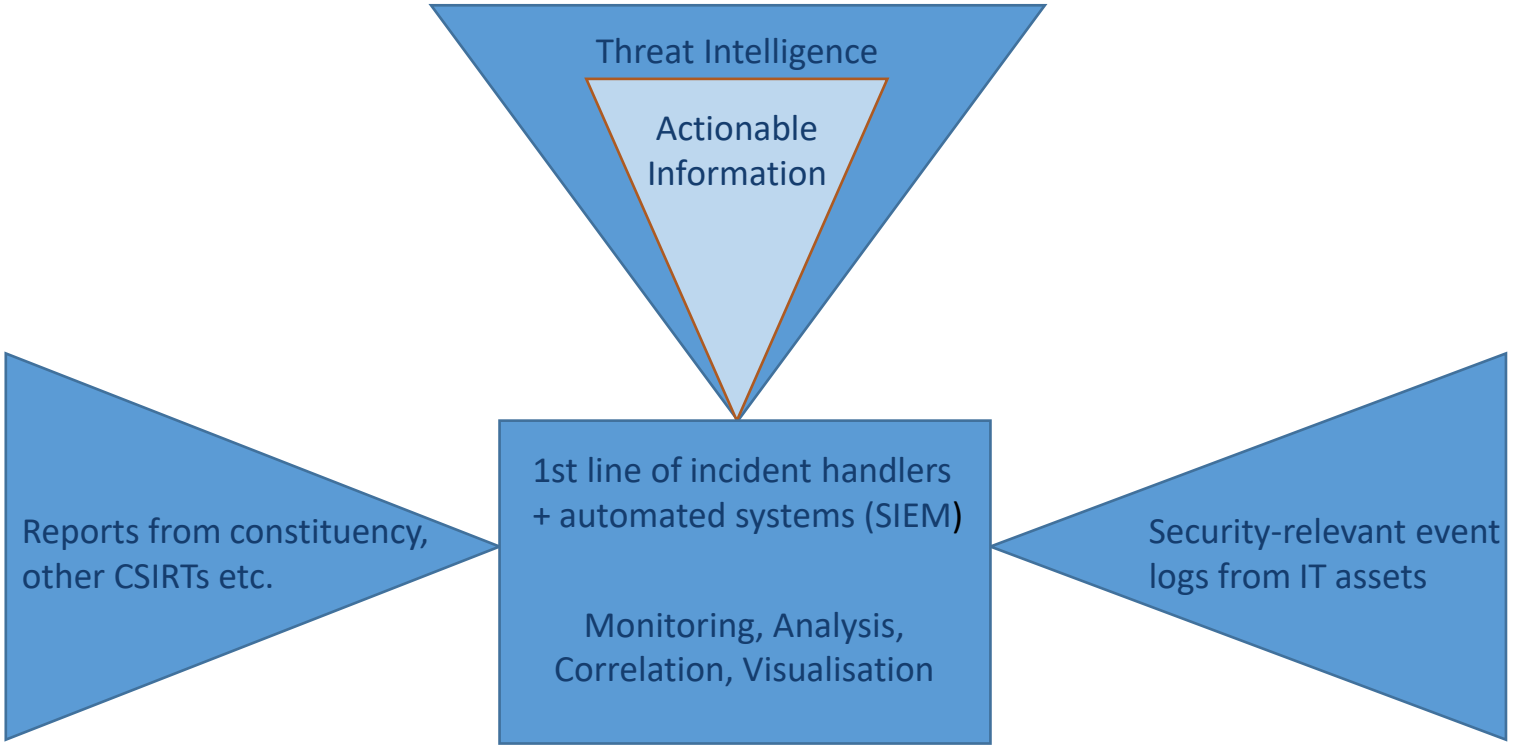
Data processing and intelligence



Malicious IPs from a CTI report

These IPs occured in our network

Need for additional analysi what exactly happened


Threat Intelligence
Actionable Information
Reports from constituency, other CSIRTs etc.
1st line of incident handlers + automated systems (SIEM)
Monitoring, Analysis, Correlation, Visualisation
Security-relevant event logs from IT assets

TF-CSIRT

- CTI Platforms
- Threat Intel Feeds
- IoCs mailing lists
- Bulletins, newsletters
- Reports and white papers
- Pastebin, Google Dorks etc.
- Own tooling and scripting

Photo by Thomas Charters on Unsplash

TF-CSIRT

- Sensors
  - Intrusion detection (network, host)
  - File integrity checking
  - Honeypots
  - Anomaly detection (behavior analytics)
    - User – Network – System/application
- Vulnerability detection (passive/active)
- EDR, XDR, SIEM.

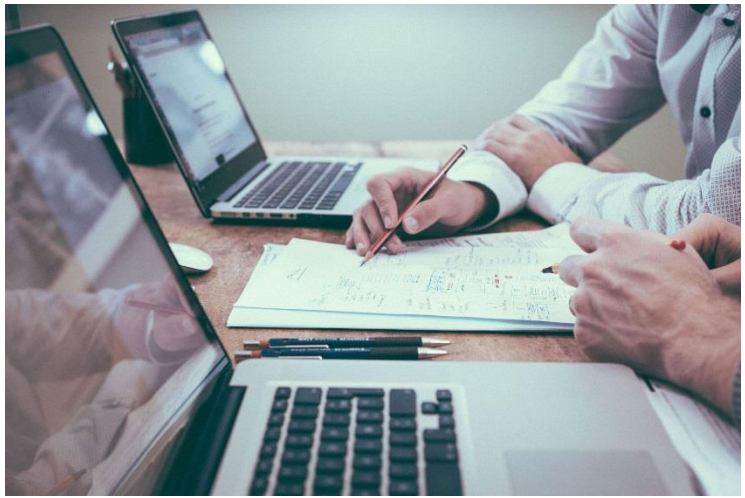
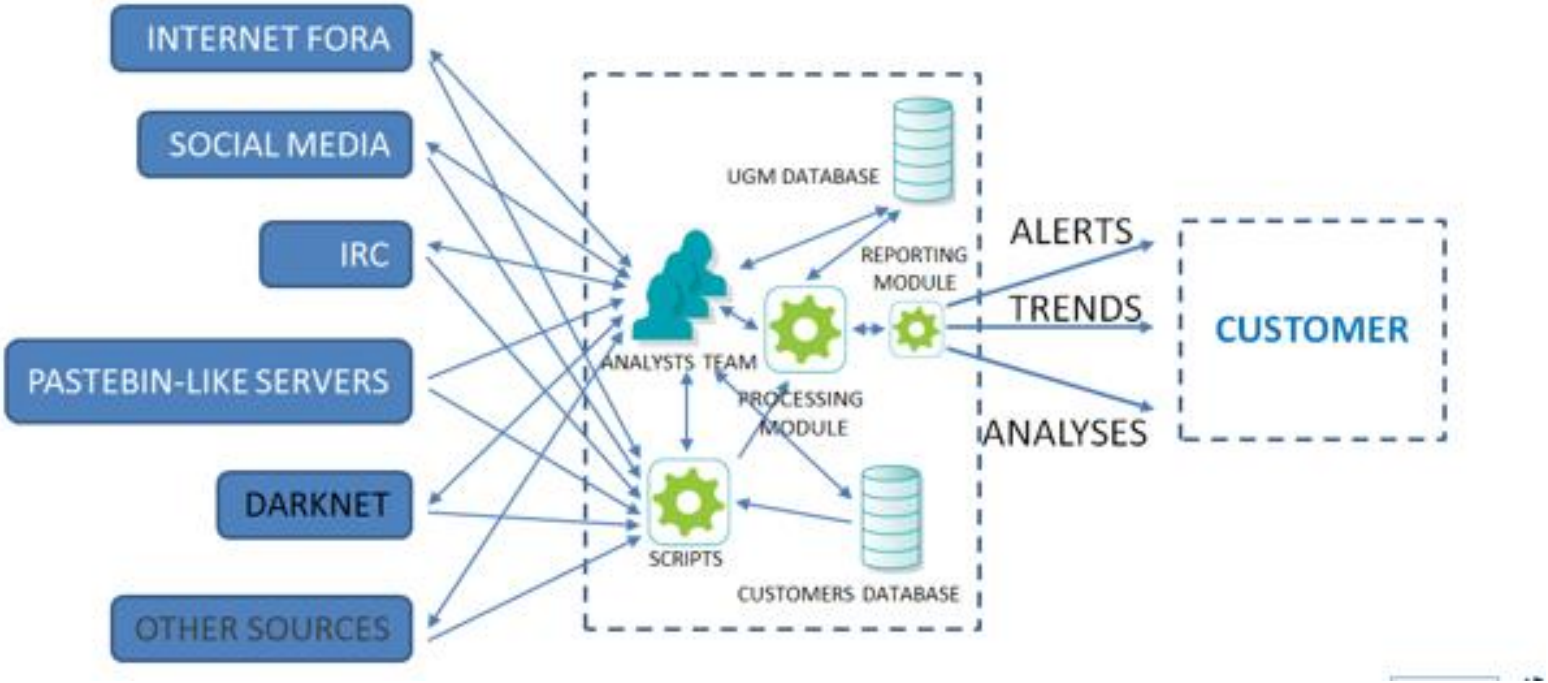


Photo by Helloquence on Unsplash


INTERNET FORA
SOCIAL MEDIA
IRC
PASTEBIN-LIKE SERVERS
DARKNET
OTHER SOURCES
UGM DATABASE
REPORTING MODULE
ANALYSTS TEAM
PROCESSING MODULE
SCRIPTS
CUSTOMERS DATABASE
ALERTS
TRENDS
ANALYSES
CUSTOMER

TF-CSIRT

- Proactive gathering of information
  - Open-source intelligence (OSINT)
  - Third parties, service providers
  - Media
  - Blogs, Twitter, …
- Outcome from other incidents
  - Output from forensics analysis
  - Incident tracking system

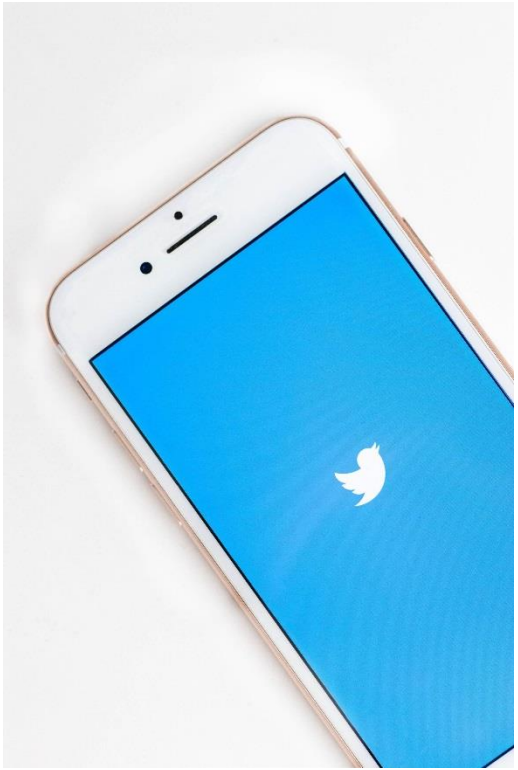


Photo by Sara Kurfess on Unsplash

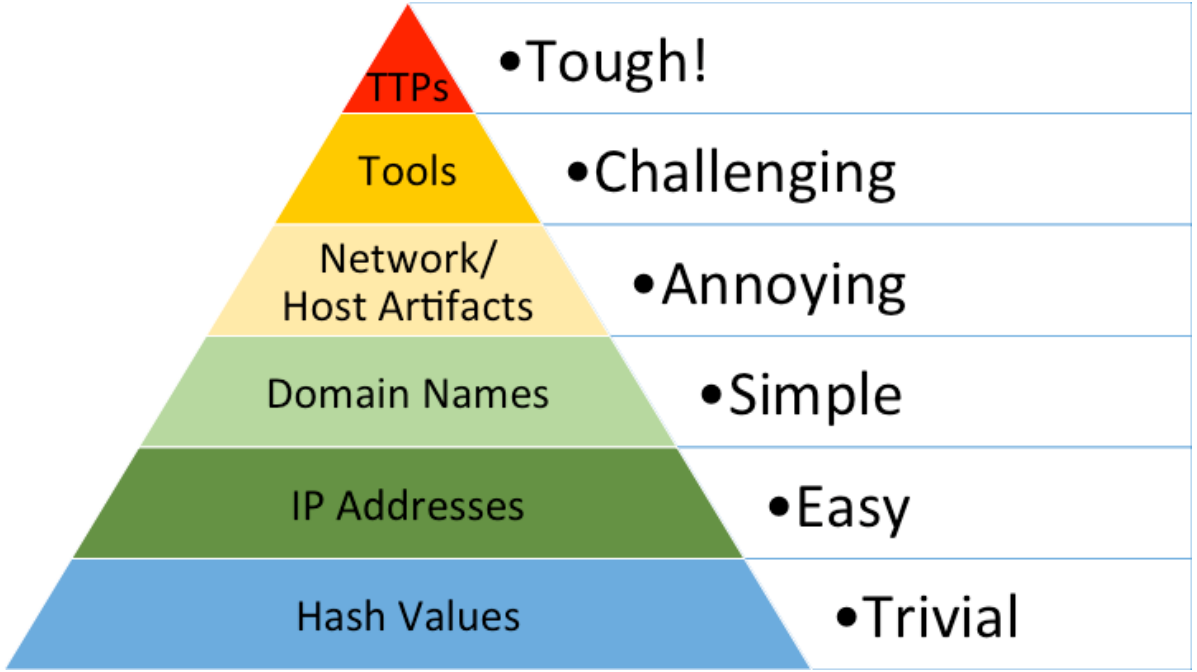


Photo by Sara Kurfess on Unsplash

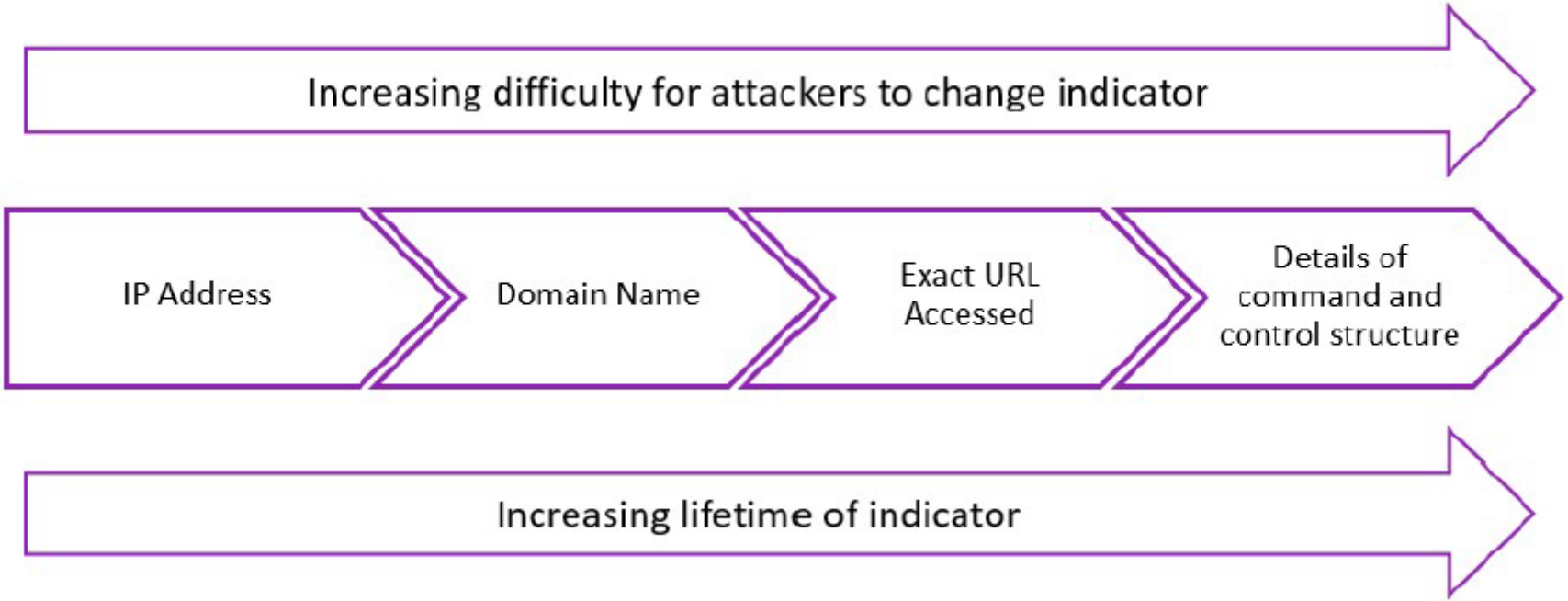
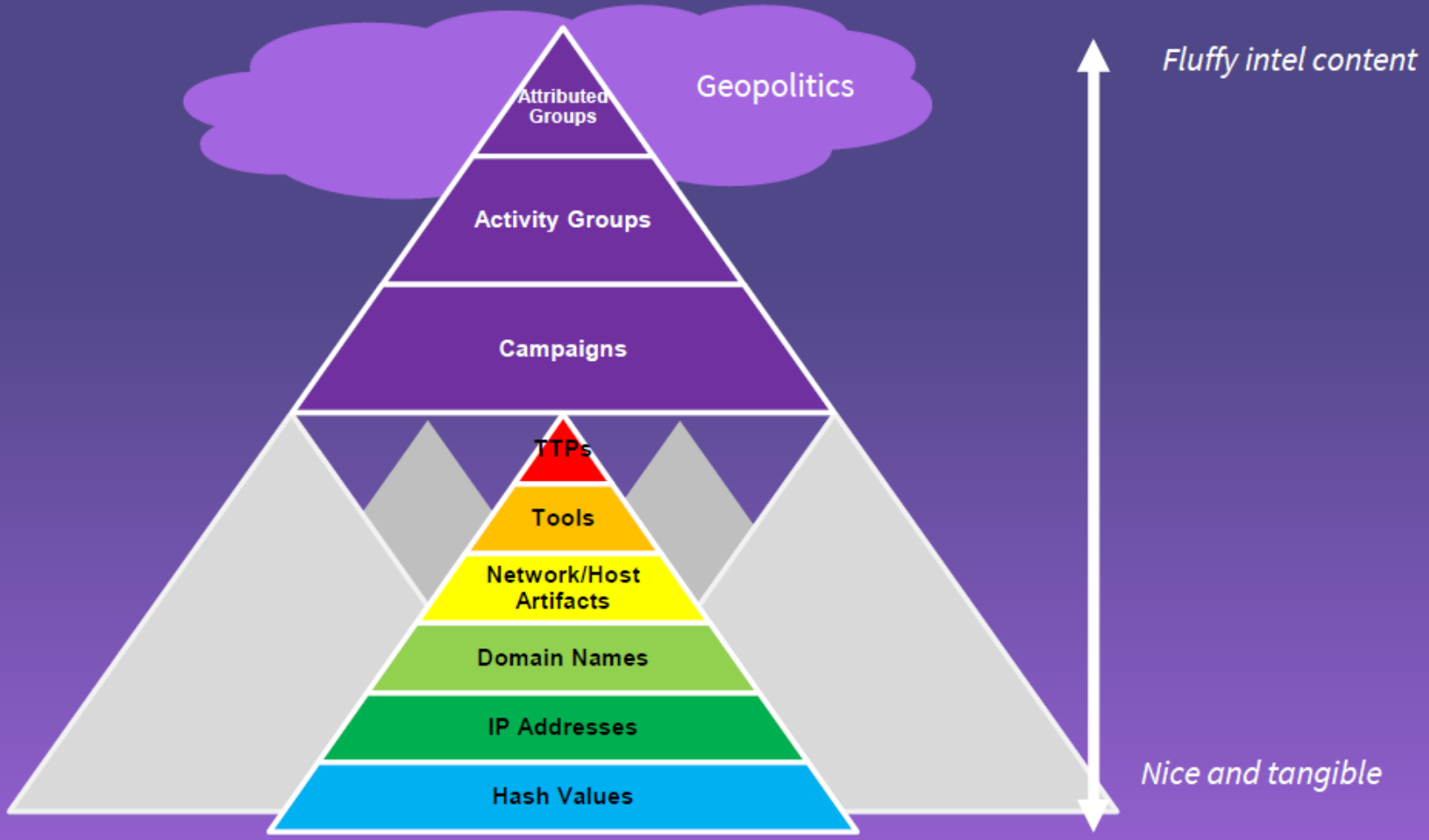


Photo by Sara Kurfess on Unsplash



Extending the 'Pyramid of pain'

Usable CTI – 4 dimensions

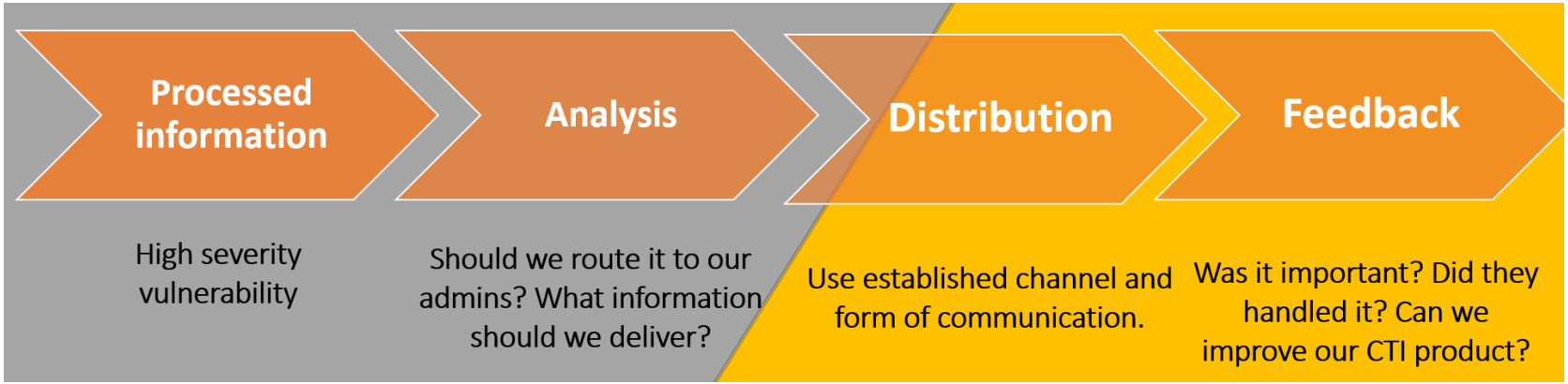
- Once a data is gathered and processed, its time for analysis.
  - How the contextual data and information can be used?
  - Who needs it?
  - How this contribute to our situational awareness?
- CTI products can be:
  - Strategic
  - Operational
  - Tactical / technical

Strategic • Actionable trends • Threat summary report • Contribution to the risk profile	**Operational** • Phishing campaign notification • Vulnerability advisory • Low level security control recommendation
Tactical • TTPs • Malicious tools and services • Modus operandi.	**Technical** • Actionable IoCs (those that we can find context for)


Strategic Cyber Threat Intelligence
Audience
Board of Directors C-Suite CEO, CIO, etc.
Analytical Tools
Analysis Competitive Hypotheses (ACH)
Analytical Focus
Global Threat Landscape, Attribution
Deliverables
Strategic CTI report, Mitigation Scorecard
Reporting Regularity
Quarterly, Semi-Annual, Annual
Operational Cyber Threat Intelligence
Audience
Security Admins, Security Analysts, SOC
Analytical Tools
OpenIOC, YARA, SNORT, SIGMA
Analytical Focus
Technical, Collecting, Analyzing IOC's
Deliverables
Weekly CTI Report, IOC Feed population
Reporting Regularity
Daily, Weekly, BI-Weekly
Cyber Threat Intelligence Program
Threat Intelligence Platform (TIP)
Strategic Cyber Threat Intelligence
Tactical Cyber Threat Intelligence
Operational Cyber Threat Intelligence
Cyber Threat Intelligence Sharing
Tactical Cyber Threat Intelligence
Audience
IT and Cyber Security Management
Analytical Tools
Killchain, Mitre ATT&CK, Diamond Model
Analytical Focus
TTP's, Cyber Attack Threat Modelling
Deliverables
Tactical CTI Report, Campaign Heatmap
Reporting Regularity
BI-Weekly, Monthly, Quarterly
Cyber Threat Intelligence Sharing
Audience
CTI Producers and Consumers
Analytical Tools
STIXX, TAXII, Mitre ATT&CK
Analytical Focus
TLP's, Standardization, Sanitation
Deliverables
Established Sharing Relationships
Reporting Regularity
Real-time Threat Intelligence Feeds

TF-CSIRT

- Analysis and distribution phase of CTI cycle – example.



TF-CSIRT

Section 5: Secure Communications (Messaging, PGP & TLP)

Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis

- **TLP CLEAR**
  Unlimited – no restrictions
- **TLP GREEN**
  Community-wide, not public
- **TLP AMBER**
  In-house (organization + clients), need-to-know distribution
- **TLP AMBER+STRICT**
  In-house (organization ONLY), need-to-know distribution
- **TLP RED**
  Personal, for named! recipients! only!

More information: https://www.first.org/tlp

When a meeting, or part thereof, is held under the Chatham House Rule, participants are **free to use the information** received,

but (!)

neither the **identity** nor the **affiliation** of the speaker(s), nor that of any other **participant**, may be revealed.

TF-CSIRT

Section 6: Wrap-up

Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis

TF-CSIRT

Operational Module

TRANSITS1 Materials

Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis

_
-