TF-CSIRT

TRANSITS I

Operational Module

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

Version: 7.1

Session Plan

- Section 1 – Introduction to Incident Management
- Section 2 – Incident Handling – The ENISA Approach
- Section 3 – Real World Challenges
  - CSIRT vs SOC
  - Roles
  - Governance Issues
  - Preparation: Default rules, Resilience
  - On-Site and Off-Site Incident Handling
- Section 4 – Data Acquisition & Threat Intelligence
  - Detection, Monitoring, Reporting
- Section 5 – Secure communications (Messaging, PGP and TLP)
- Section 6 – Wrap-up

Exercise #1 – Fire Alarm

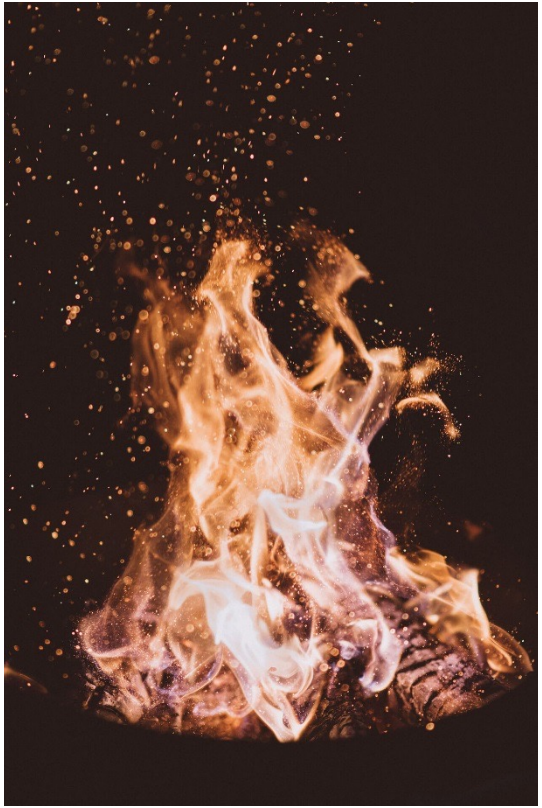


Photo by Joshua Newton on Unsplash

Exercise #1 – Fire Alarm

TF-CSIRT

Exercise #1 – Short Debrief

TF-CSIRT

- What worked?
- What failed?
- Next time, what would you do? What would you change?
- Other incident-oriented jobs?

- Fire-Fighting
  - The History of Fire Fighting
    → http://www.emergencydispatch.org/articles/historyoffirefighting.html
  - Fighting Fire with Organization: Summing it all Up
    → http://www.netage.com/pub/books/TeamNet/CHAPTERS%20PDF/CHAPTE~3.pdf

Photo by Hush Naidoo on Unsplash

Exercise #1 – Short Debrief

TF-CSIRT

- Fireman are NOT mighty lonesome gurus who can solve ANY fire, no matter its size, location and “combustible”
- Understand that it's a **TEAM** effort, each and everyone cooperating in reaching ”a” solution
  → **1 + 1 > 2**
- Follow the process rather than creating new ways to solve bleeding edge issues → preparation is key

- Message of the day:
  - **Don't reinvent the wheel**
  - **Follow the rules and operations will run smoother and far better**

TF-CSIRT

Section 1: Introduction to Incident Management

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

–

–

Section 1: Group Discussion

- What are your top 5 issues when it comes to handling incidents?

Photo by Mimi Thian on Unsplash

Section 1: Introduction to Incident Management
Basic Terminology

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

- 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

- 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

- **Passive defense**:
    - Firewalls
    - AV Solution
    - Blacklists
    - …

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

- **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

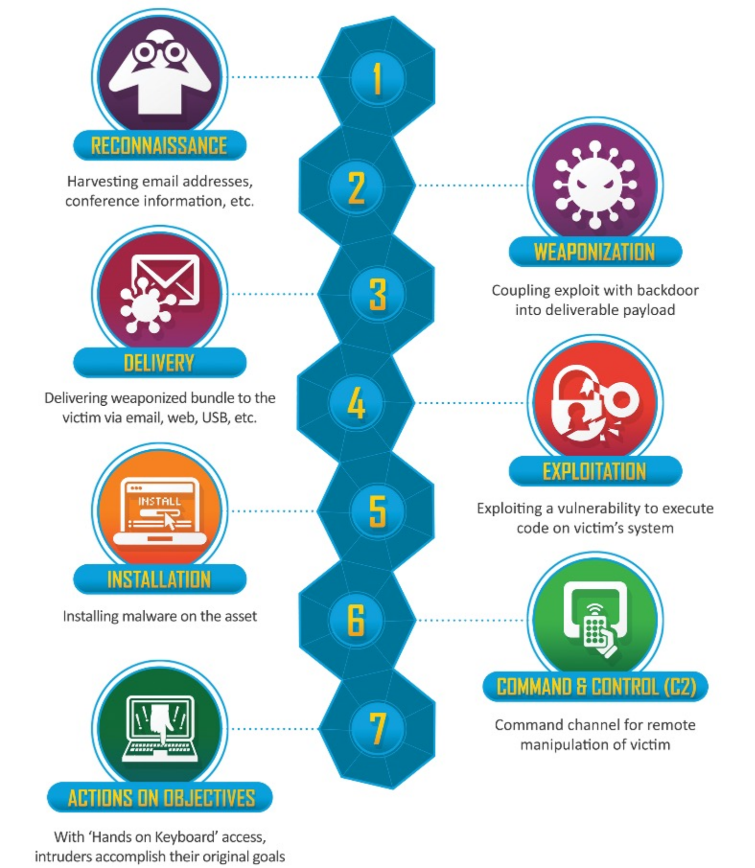
- Some incident handling teams are **as little as 2 people**
  - Simple tools for coordination and logging
  - No dimensioning issues
  - Excel spreadsheets, Wiki

- 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



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

© Lockheed Martin

Section 3 – Incident Management
Crisis Management

TF-CSIRT

- **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

Section 1: Introduction to Incident Management
Incident Management Models

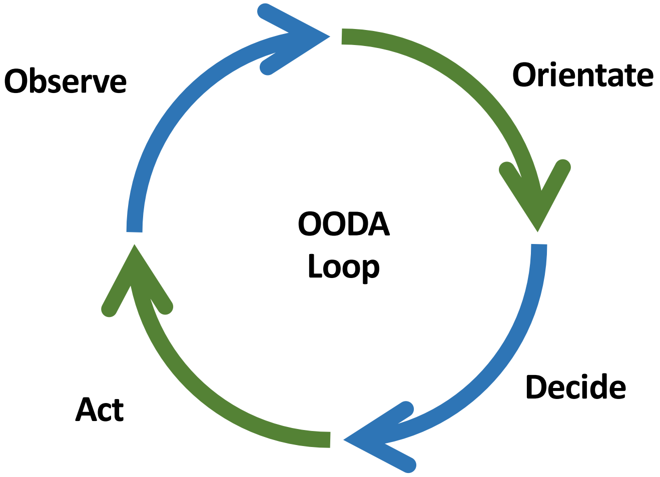
- Various flavors
  - Observe Orientate Decide Act (OODA loop) → June 1995, John R. Boyd
  - “Computer Incident Response Guidebook” → US Navy, August 1996

- 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

Section 1: Introduction to Incident Management
Incident Management Models – OODA Loop

TF-CSIRT

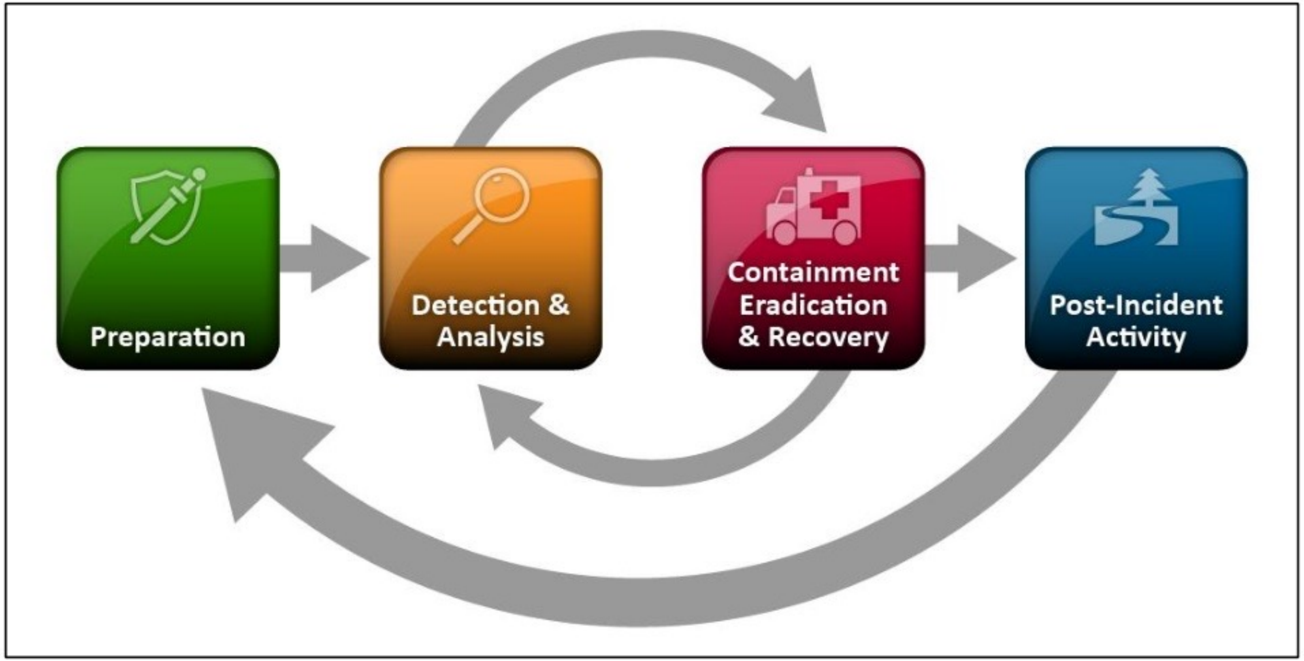
OODA Loop: Observe - Orientate - Decide - Act



Section 1: Introduction to Incident Management
Incident Management Models - NIST

TF-CSIRT

NIST SP 800-61 rev 2 (2012)

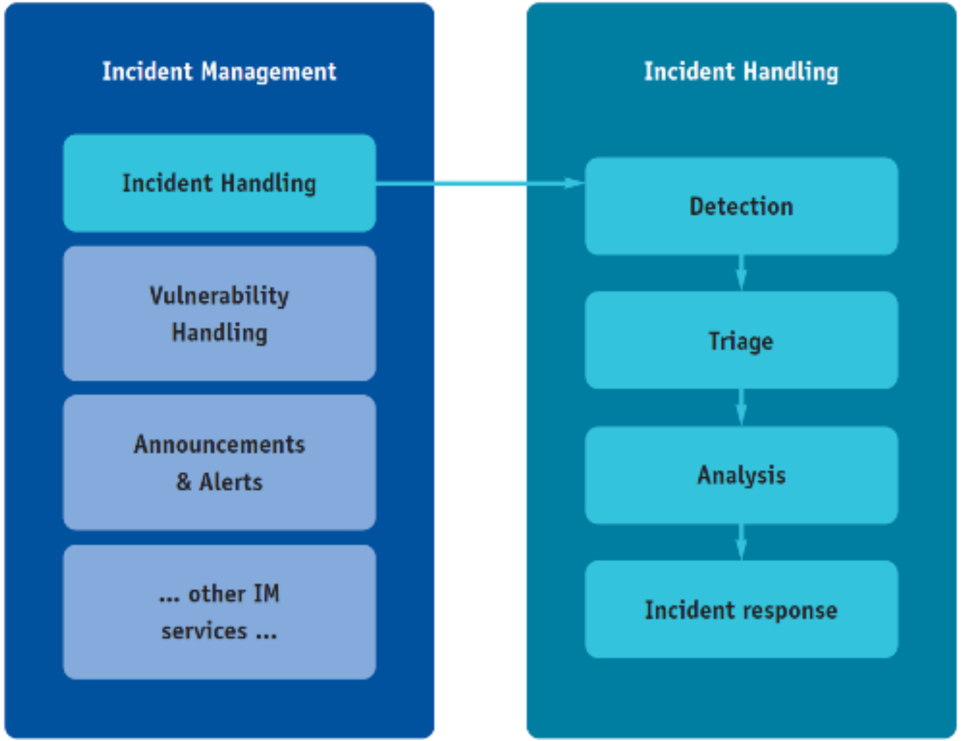


© NIST

Section 1 – Introduction to Incident Management
Incident Management models – ENISA Model

TF-CSIRT

ENISA Model for Incident Management

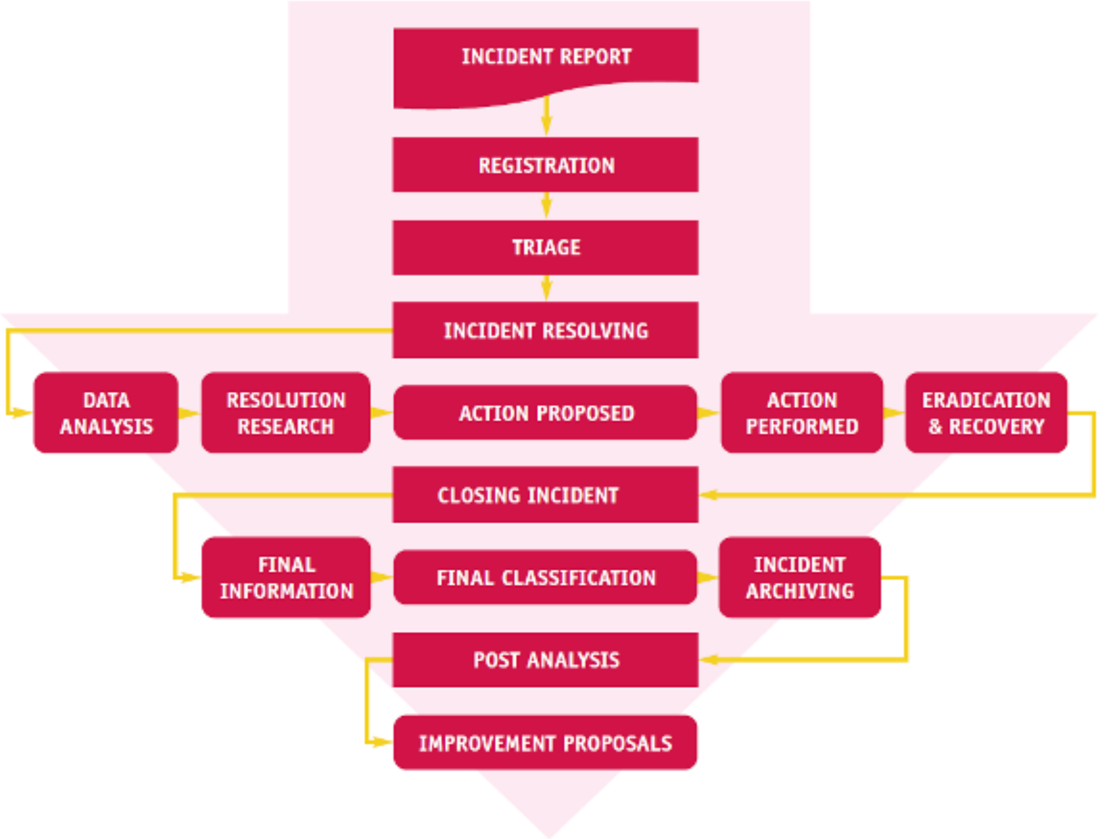


© ENISA

Section 1: Introduction to Incident Management
Incident Management Models – ENISA Good practice guide

TF-CSIRT

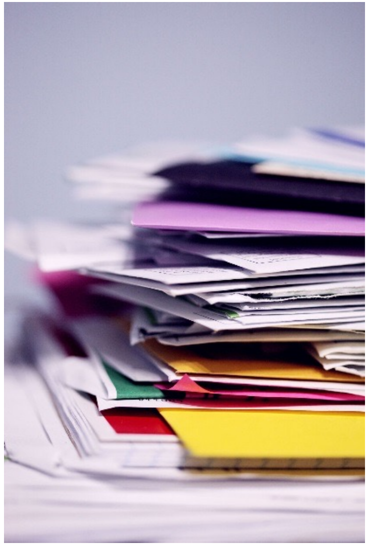
ENISA “Good Practice Guide for Incident Management” (p.34)



Content: Section 1 Summary

- 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

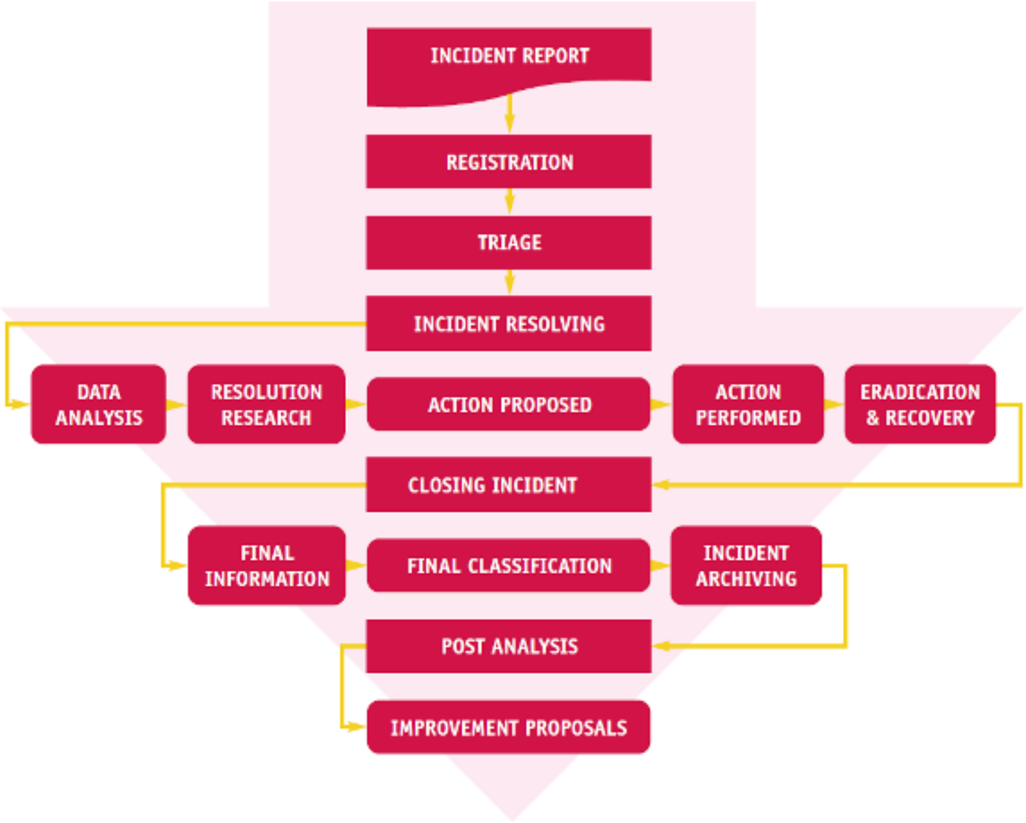
Olivier Caleff, Sven Gabriel, Przemyslaw Jaroszewski, Andreas Muehlemann, Roeland Reijers, Marius Urkis

–

–

Section 2: Incident Handling
ENISA Workflow Overview

TF-CSIRT



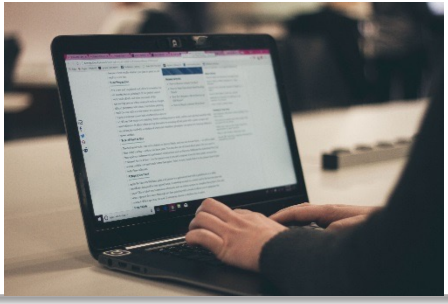
Section 2: Incident Management Models – ENISA
1 – Incident Report

TF-CSIRT

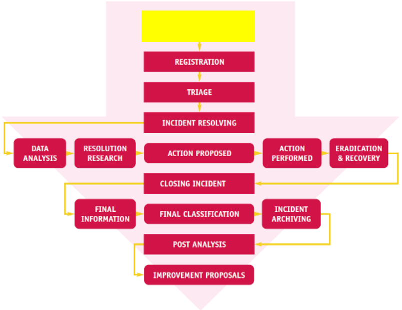
Group exercise:

- You arrive at the office and are responsible for the tickets. This is what you find …

1. What do you do?
2. What are your next steps?



INCIDENT REPORT



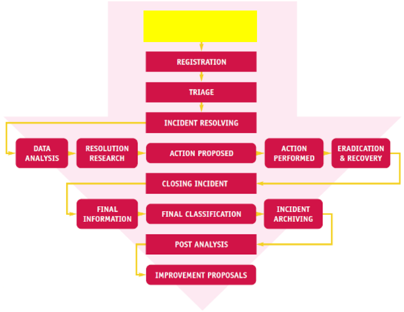
Photos by Nathan Dumlao and Neonbrand on Unsplash

Section 2: Incident Management Models – ENISA
1 – Incident Report

- 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



Section 2: Incident Management Models – ENISA
1 – Incident Report

TF-CSIRT

- Full automation to input of incident details looks like a dream… but

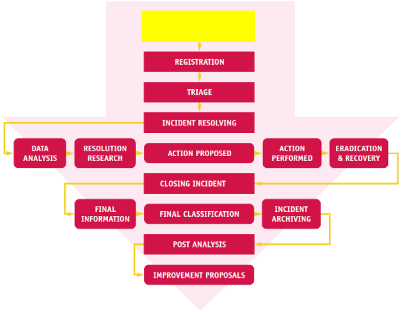
1. Needs to find a commonly agreed terminology that fits everyone, every case, every tool...

2. Needs to work on correlation and notification similarities

3. Let's evaluate the number of incidents reported on a standard day... and see if it's worth it

4. What about bursts in case of a wide outage/incident?

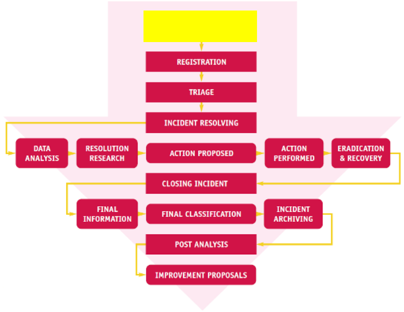
INCIDENT REPORT



Section 2: Incident Management Models – ENISA
1 – Incident Report

- Feeds from detection
- 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 emails) 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, …)

INCIDENT REPORT

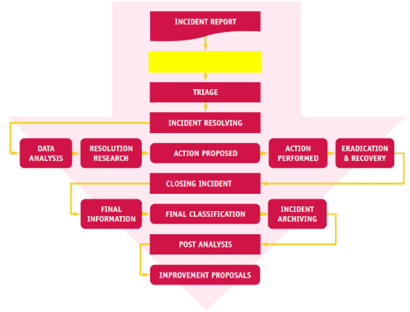


Section 2: Incident Management Models – ENISA
2 – Registration

TF-CSIRT

- Registration process easier with an incident report registration form
  - 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

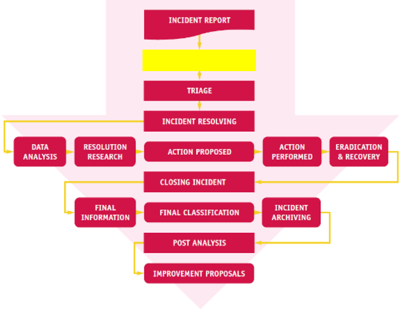
REGISTRATION



Section 2: Incident Management Models – ENISA
2 – Registration

- Attacks against a registration system:
  - Malicious input: as any input system, all input must be first evaluated
    - Flooding
    - Spamming
    - Leak
- Set up some anomaly detection mechanisms and initial filtering for tagging the registered incident
- Some tasks cannot be automated: takes time, and human resources

Registration

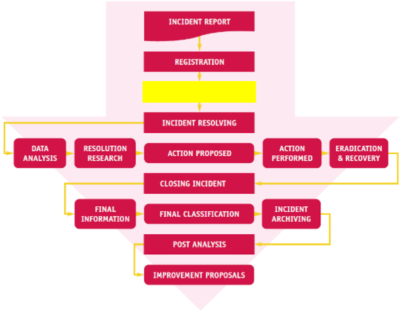


Section 2: Incident Management Models – ENISA 3 – Triage

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
- Solution:
  - Take into account, diagnose, cure
  - E.g. set priorities according to formal criteria such as severity of the wounds

TRIAGE



Section 2: Incident Management Models – ENISA 3 – Triage

- Incident Handling has 4 Steps
  - Verification
  - Initial Classification
  - Assign severity and priority
  - Assignment to an incident handler

TRIAGE

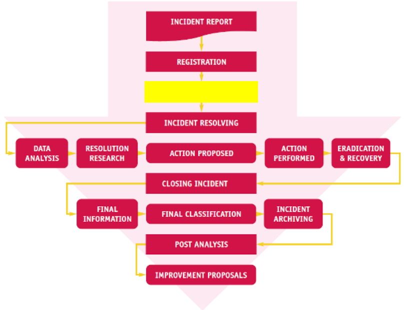


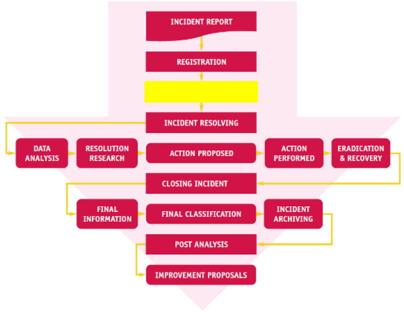
Photo by Erika Giraud on Unsplash

Section 2: Incident Management Models – ENISA 3 – Triage

TF-CSIRT

- Verification
  - Is it out of scope / out of perimeter
  - Usually many messages about scan complaints, virus attacks
  - Other uninteresting cases
    - 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?

TRIAGE



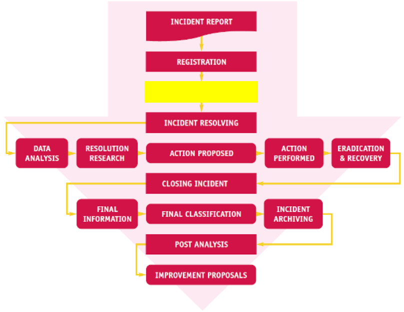
- **Are you ready to send an ACK?**
- **Do you need additional details?**

Section 2: Incident Management Models – ENISA
3 – Triage

TF-CSIRT

- Incident Initial Classification / Severity Assessment
  - Aim to fit into the CSIRT classification scheme with rating, based on the CSIRT role for its constituencies
  - The more details to help classify, the better
- 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

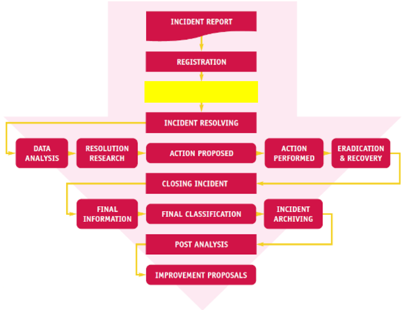
TRIAGE



Section 2: Incident Management Models – ENISA
3 – Triage

- 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 will decide on the amount of effort that will be allocated to the handling of the incident

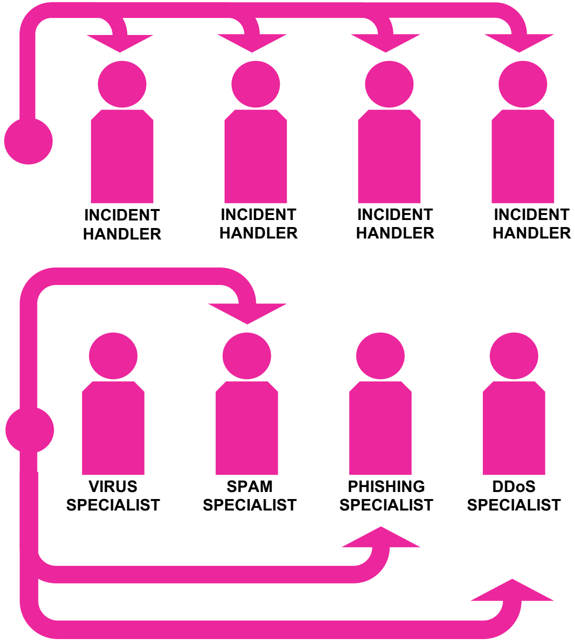
TRIAGE



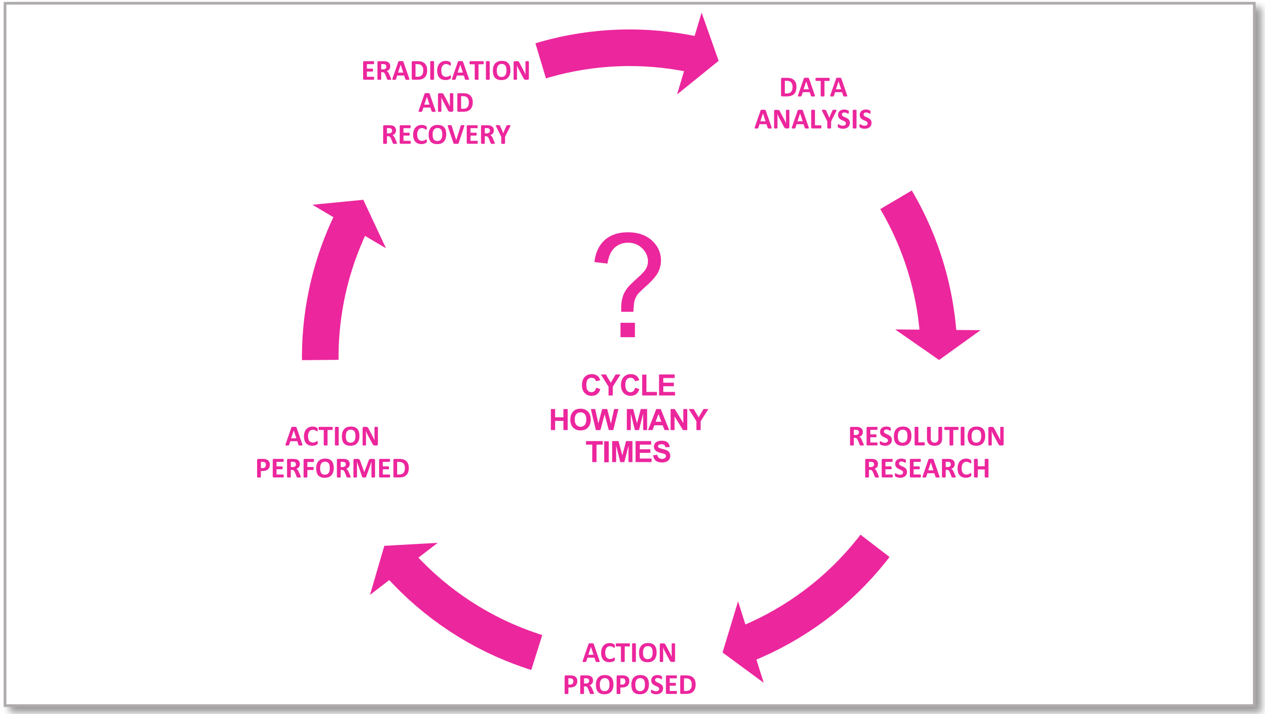
Section 2: Incident Management Models – ENISA
3 – Triage

TF-CSIRT

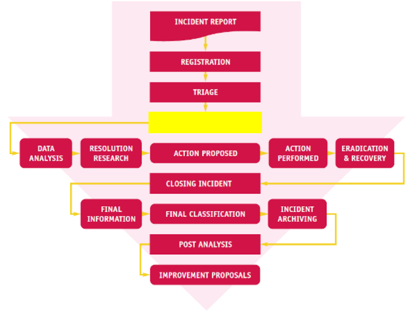
- Incident Assignment
  - Once the classification is done and the type of effort can be estimated …
  - The Ticket can be assigned to an Incident Handler
  - Criteria for assignment
    - Expertise or capabilities, Resource availability
    - Knowledge, Language
- Roles and tasks
  - Incident Handler / Manager
    - Communication / Organization
      (Incident reporter / Management / Peers)
  - Analyst(s)
  - Who decides if a system can be shut down and when?
  - Move to a 'war-room'?
- Checklists: Contact roster, Incident procedure(s)



Section 2: Incident Management Models – ENISA
4 – Incident Resolution



INCIDENT RESOLUTION



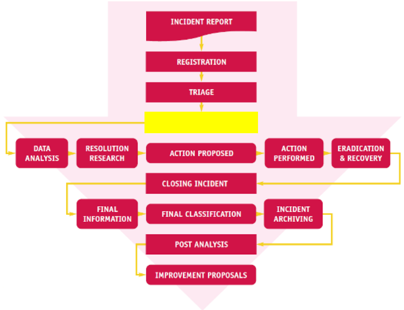
Section 2: Incident Management Models – ENISA
4 – Incident Resolution

TF-CSIRT

Analysis of competing hypothesis

Hypothesis	Evidence / details / comment	Likely / unlikely

Incident Resolution



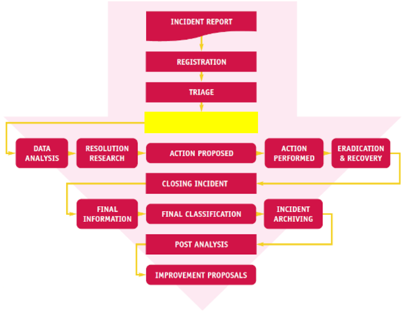
Section 2: Incident Management Models – ENISA
4 – Incident Resolution

TF-CSIRT

Analysis of competing hypothesis

Hypothesis	Evidence / details / comments	Likely / unlikely
Power outage due to storm		
Cyber attack	Unknown IP in the logs	
Squirrel triggered a local power outage		

Incident Resolution



Section 2: Incident Management Models – ENISA
4 – Incident Resolution

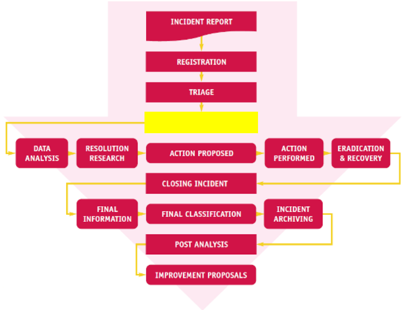
Analysis of competing hypothesis

Hypothesis	Evidence / details / comment	Likely / unlikely
Power outage due to storm	No info in media found	✗
Cyber attack	Unknown IP in the logs	✗
Squirrel triggered a local power outage	Local power outage, complete block was down	✓

- Inconsistency?
- Sensitivity? How would the hypothesis be impacted if certain key evidence were wrong?
- Look for simple information first! Phone call vs. IP Address

- **Conclusion and evaluation: determine the best hypothesis**

Incident Resolution



INCIDENT REPORT
REGISTRATION
TRIAGE
DATA ANALYSIS
RESOLUTION RESEARCH
ACTION PROPOSED
ACTION PERFORMED
ERADICATION & RECOVERY
CLOSING INCIDENT
FINAL INFORMATION
FINAL CLASSIFICATION
INCIDENT ARCHIVING
POST ANALYSIS
IMPROVEMENT PROPOSALS

Section 2: Incident Management Models – ENISA
4 – Incident Resolution

- May require to ask for resources outside of the CSIRT
- As time goes, additional details will be collected
  - Other incidents may be related
  - Additional victims may be discovered
  - …

Incident Resolution

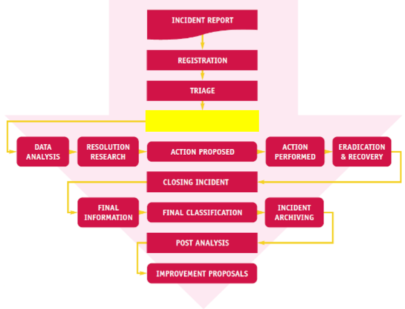


Photo by Markus Spiske on Unsplash

Section 2: Incident Management Models – ENISA
5 – Data Analysis

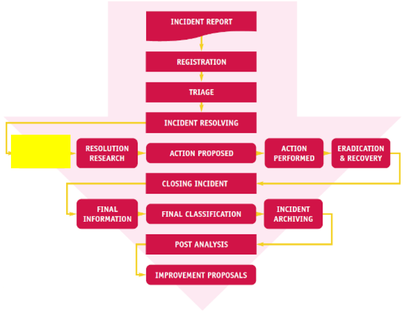
- Formal process
  - Needs to be documented
  - Best if it can be replayed
  - **Never work on real data, always on copies**

- Select the sources
  - People/staff, components, data, time range

- Build a team
  - Team manager
  - Split the work according to
    - Process steps, expertise, availability, workload
  - Teams' effort

- Proceed according to your plan

Incident Resolution
-
Data Analysis

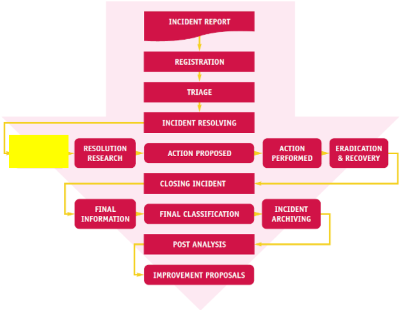


Section 2: Incident Management Models – ENISA
5 – Data Analysis

- Gather more data
- Look for details to support the effort of incident handling
- Involves data collection and support from the victims
    - 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



Section 2: Incident Management Models – ENISA
5 – 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
- Level of positive support depends on good will without preparation
- Anticipation

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

Incident Resolution - Data Analysis

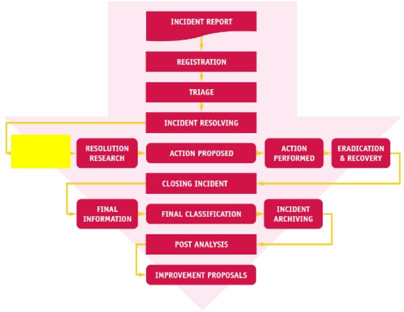


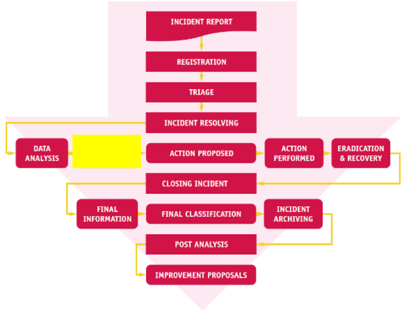
Photo by Sebastian Grochowicz on Unsplash

Section 2: Incident Management Models – ENISA
6 – Resolution Research

- Review data, analyze and see if it points to a resolution
- Recursive process with data analysis
- IRM: Information and Records Management
- SOPs: Standard Operations Procedures
- 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



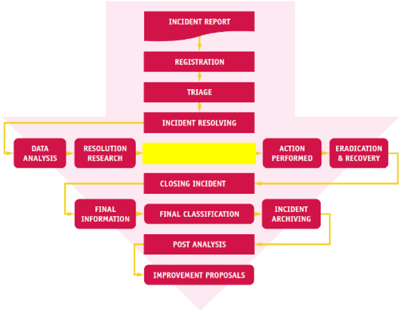
Section 2: Incident Management Models – ENISA
7 – Action Proposed

TF-CSIRT

- Based on the previous steps, proposal for new directions
  - Keeping on analyzing
  - Moving to other components
  - Aiming at going back in time up to the initial event
- 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

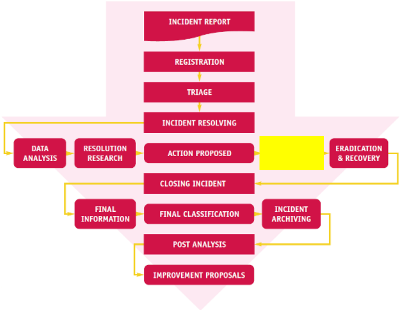
Incident Resolution - Actions Proposed



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

- Actions can be performed by incident team, responders 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

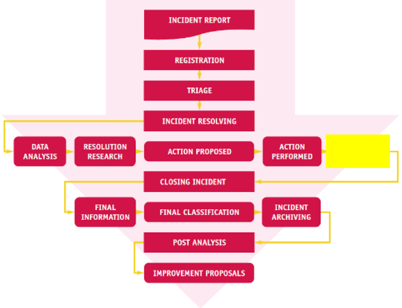
Incident Resolution - Actions Performed



Section 2: Incident Management Models – ENISA
9 – Eradication & Recovery

- Main goal: getting rid of the incident
  - Eradication
  - Recovery
  - Business restoration
- 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

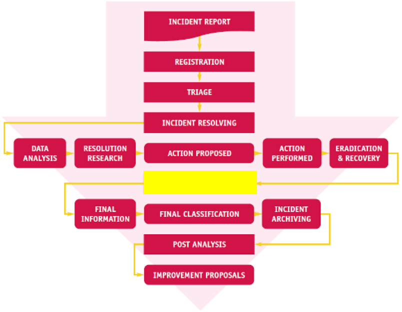


Section 2: Incident Management Models – ENISA
4 – Incident Resolution

TF-CSIRT

- Keep an eye on open tickets, updates might change the game
- 10 seconds for 10 minutes , a principle from the emergency room
  - Staff is under time pressure
  - Staff works so quickly that they make errors and compromise safety (or the result)
  - 10-for-10 tries to slow down just a little, take a deep breath and a formal time-out
    - What is the biggest problem right now?
    - What is the most dangerous aspect of the problem?
  - Encourage all team members to raise any further concerns or suggestions for improvement or refinement
  - Then dive back into work

Incident Resolution

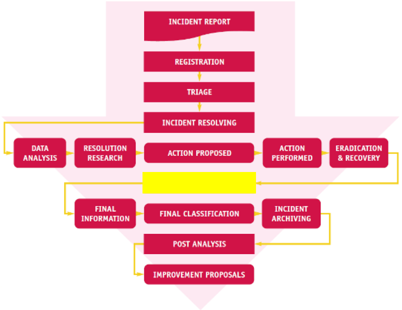


Spend 10 seconds more on data gathering, diagnosing and team planning and save time and improve safety for the next 10 minutes

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

- Last but not least, this is the end of the incident
- No longer an issue
- Who decides the incident is closed?
- What are the criteria to do so?
- 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

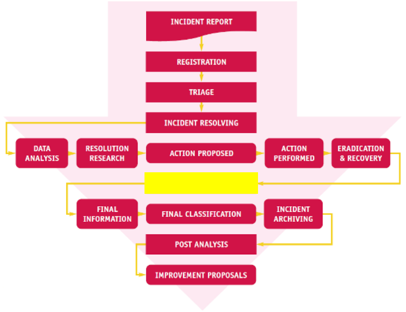


Section 2: Incident Management Models – ENISA
10 – Incident Closing

- 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

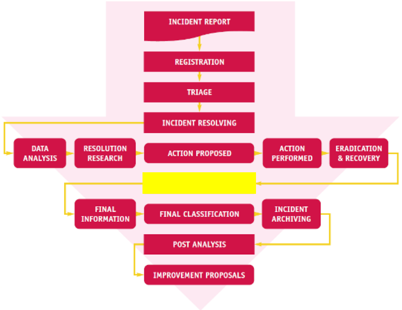


Section 2: Incident Management Models – ENISA 10 – Incident Closing

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



INCIDENT REPORT

REGISTRATION

TRIAGE

INCIDENT RESOLVING

DATA ANALYSIS

RESOLUTION RESEARCH

ACTION PROPOSED

ACTION PERFORMED

ERADICATION & RECOVERY

FINAL INFORMATION

FINAL CLASSIFICATION

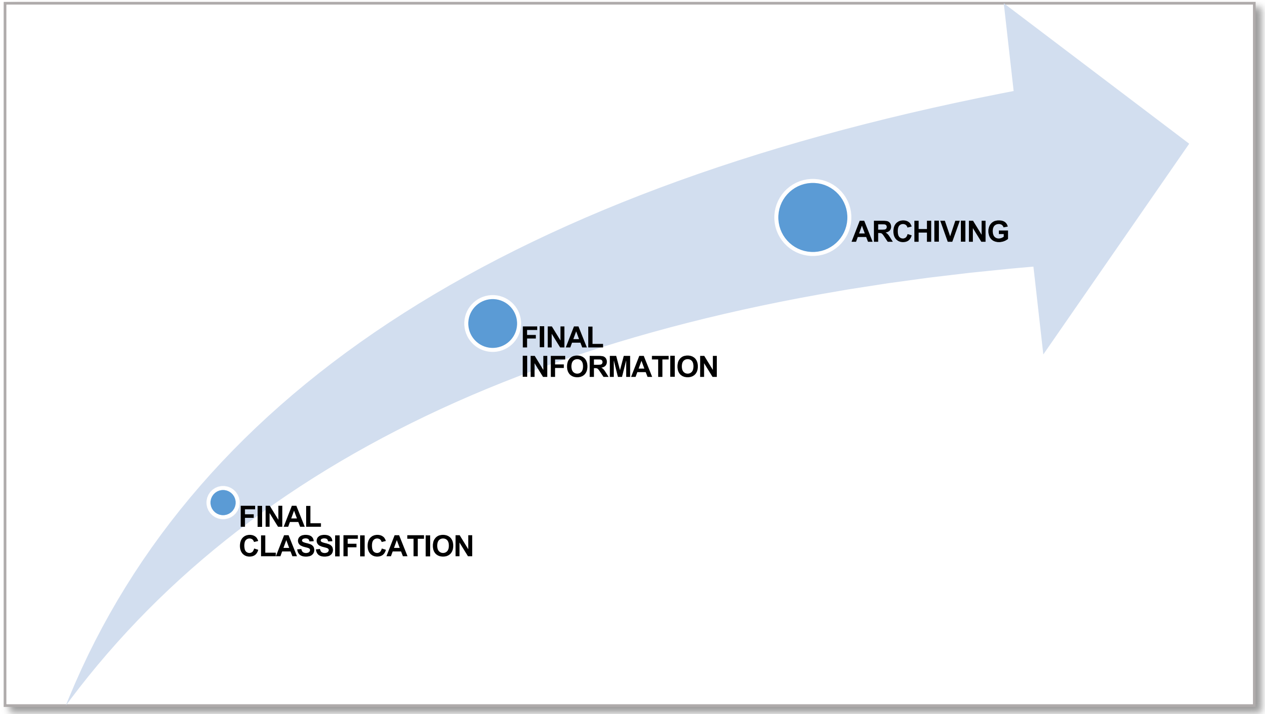
INCIDENT ARCHIVING

POST ANALYSIS

IMPROVEMENT PROPOSALS

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

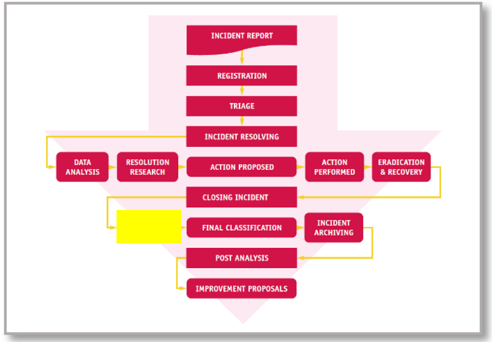
TF-CSIRT


FINAL CLASSIFICATION

FINAL INFORMATION

ARCHIVING

INCIDENT CLOSING

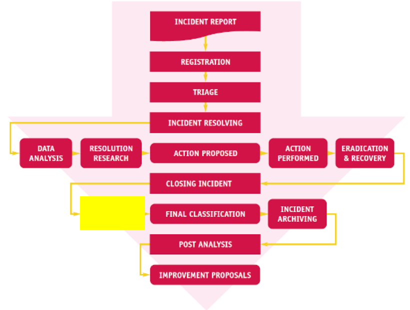


Section 2: Incident Management Models – ENISA
11 – Final Information

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
  - Need to adjust to both the audience understanding and to the incident's level of complexity
- 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



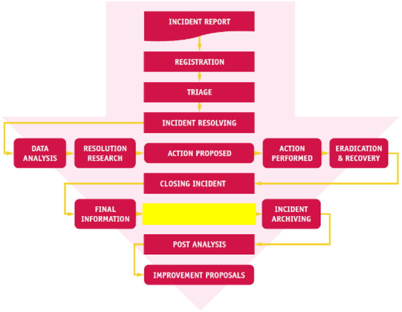
Section 2: Incident Management Models – ENISA
12 – Final Classification

- 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

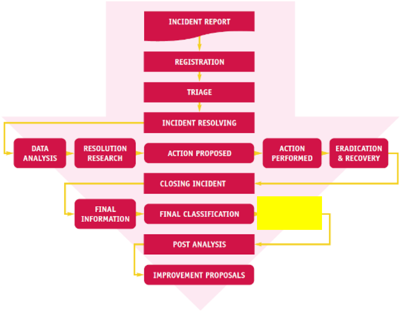
INCIDENT CLOSING
-
FINAL CLASSIFICATION



Section 2: Incident Management Models – ENISA
13 – Incident Archiving

- Archives
  - Must be easily accessible
  - If an incident occurs again, easier to follow a path that worked
  - Access must be secured and confidentiality must be enforced
  - Archive contain all steps to solve the incident
  - Any security breach of the archives is an incident it itself!
- Built-in function
  vs. CSIRT dedicated solution
  vs. Organization-wide solution

Incident Closing - Archiving

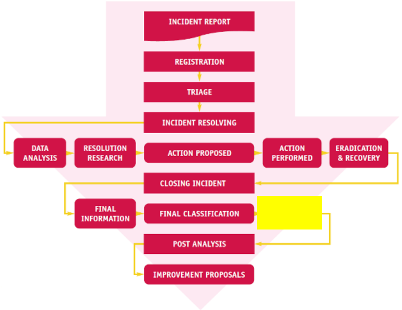


Section 2: Incident Management Models – ENISA
13 – Incident Archiving

TF-CSIRT

- Laws apply to data in most countries
  - Privacy regulations and data processing
  - Data retention requirement and data processing
- Depending on the country, laws might have different flavors
- After some times, the data are supposed to be deleted
  - What is the legal data archiving period?
- What if you trace back an APT incident that started **years ago**?

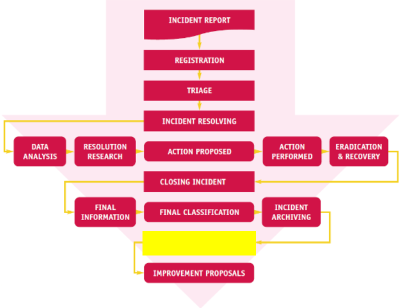
INCIDENT CLOSING
-
ARCHIVING



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

TF-CSIRT

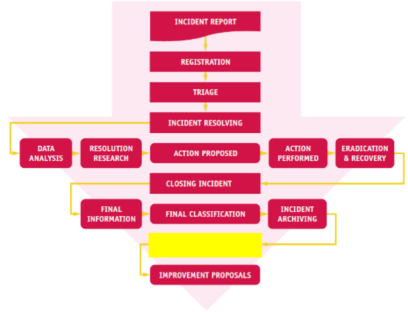
Post Analysis



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

- 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
- Either wait for some weeks before starting post-analysis
  - Or have dedicated people follow the incident handling from its start
  - Or organize regular post-incident analysis and feedback sessions
- Post analysis should be performed for all incidents
- Should deal with what worked well and what didn't?
- What are the lessons learned?

POST ANALYSIS

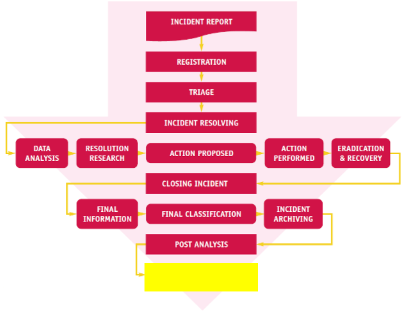


Section 2: Incident Management Models – ENISA 15 – Final Recommendations

- 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 directly
    - Internal team indirectly
    - External stakeholders

- Benefits
  - Better incident handling process
  - Easier relationships with CSIRTs and other stakeholders

Final Recommendations



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

–

–

Section 3: Real world challenges
CSIRT vs SOC

TF-CSIRT

CSIRT services (FIRST.org CSIRT service framework)

Information Security Event Management

- Monitoring and Detection
- Analyzing

Information Security Incident Management

- Accepting Reports
- Analyzing Incidents
- Analyzing Artefacts and Forensic Evidence
- Mitigation and Recovery
- Coordination

Vulnerability Management

- Vulnerability Discovery
- Report Intake
- Analysis
- Coordination
- Disclosure
- Response

Situational Awareness

- Data Acquisition
- Analysis and Synthesis
- Communication

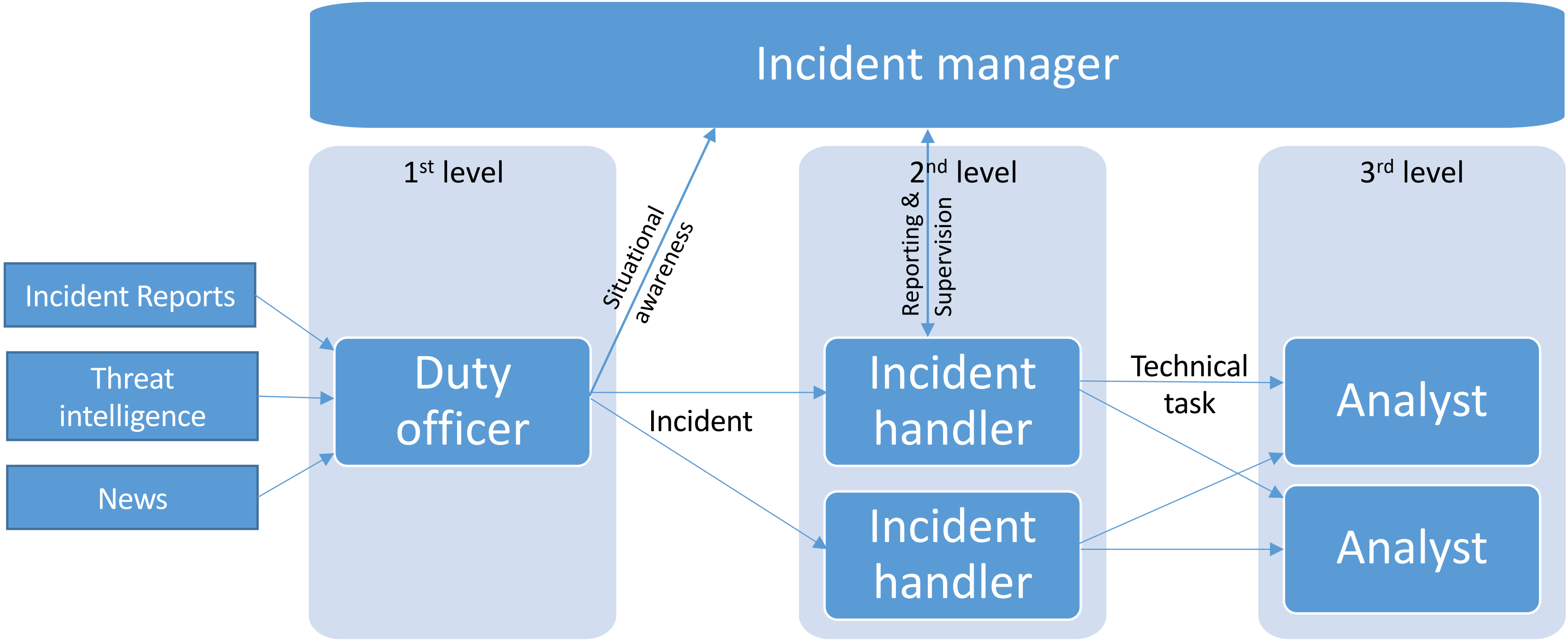
Knowledge Transfer

- 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
Roles



Section 3: Real world challenges
Possible additional roles

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

Section 3: Real world challenges
Roles – key takeaways

TF-CSIRT

- 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
Governance issues

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

Section 3: Real world challenges
Governance issues

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

Section 3: Real world challenges
Governance issues

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

Section 3: Real world challenges
Governance issues

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

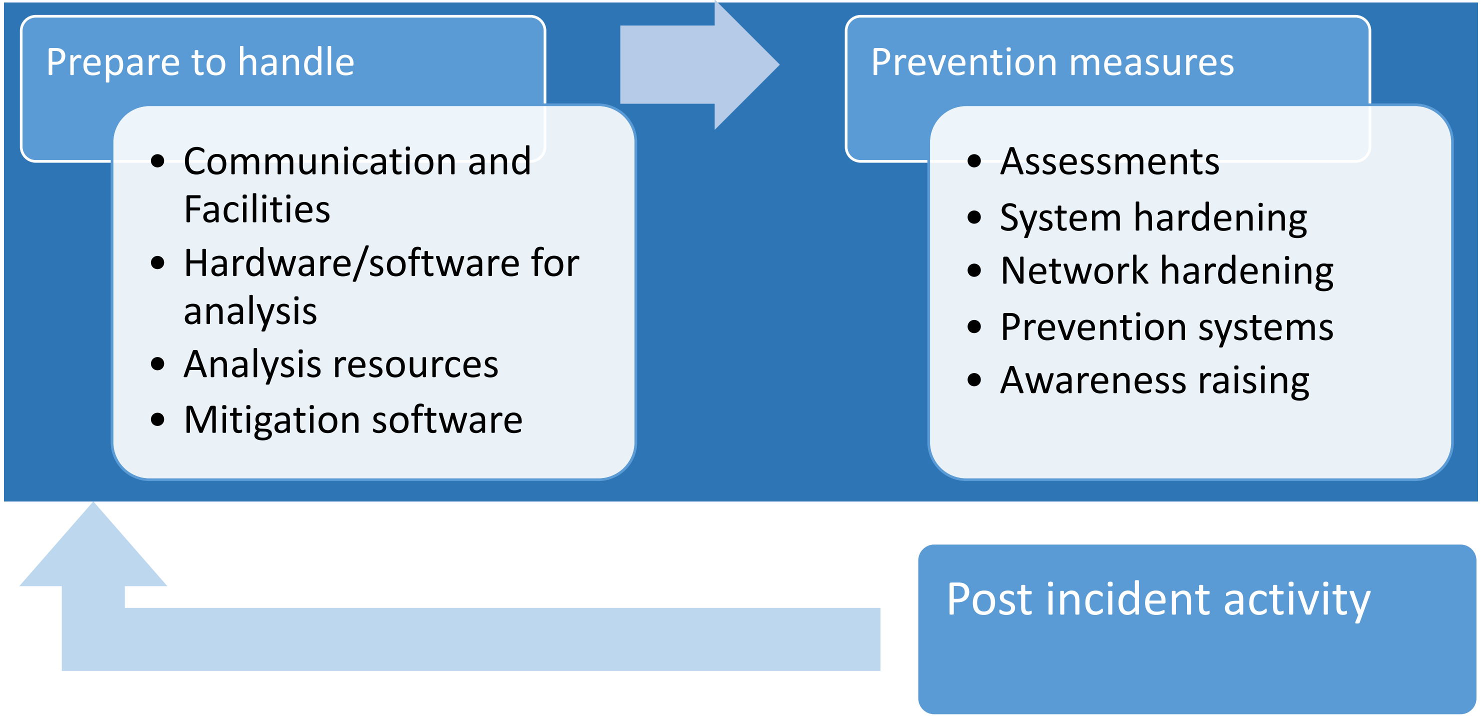
Section 3: Real world challenges
Governance issues

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

Section 3: Real world challenges
Preparation: NIST approach



Prepare to handle

- Communication and Facilities
- Hardware/software for analysis
- Analysis resources
- Mitigation software

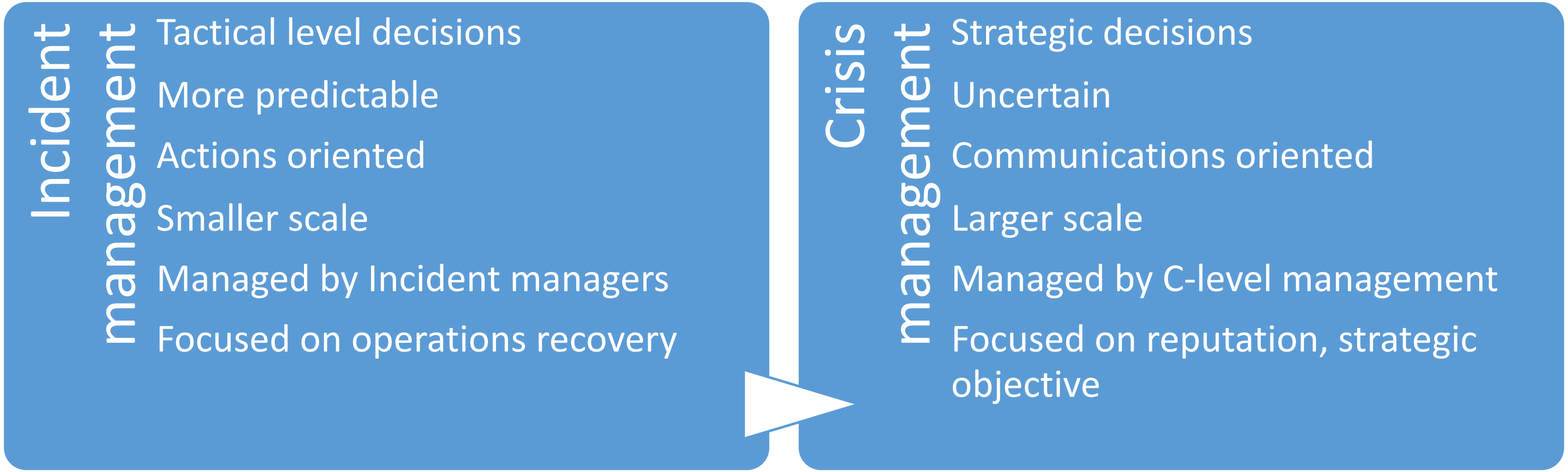
Prevention measures

- Assessments
- System hardening
- Network hardening
- Prevention systems
- Awareness raising

Post incident activity

Section 3: Real world challenges
Crisis management

- Security incident can grow into major incident or crisis, a situation which poses a threat to the organization's existence
- Differences between Incident and Crisis management:



Incident management

Tactical level decisions

More predictable

Actions oriented

Smaller scale

Managed by Incident managers

Focused on operations recovery

Crisis management

Strategic decisions

Uncertain

Communications oriented

Larger scale

Managed by C-level management

Focused on reputation, strategic objective

Section 3: Real world challenges
CSIRT role in crisis management

- FIRST.org CSIRT Services Framework

Service “Supporting crisis management” Functions:
• Distributing information to constituents • Reporting on cyber security status • Communicating strategic decisions

Section 3: Real world challenges
Preparation: Set some default rules

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

Photo by Joshua Rodriguez on Unsplash

Section 3: Real world challenges
Resilience

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

Photo by Nadine Shaabana on Unsplash

Section 3: Real world challenges
Resilience - How to keep working when everything falls apart

- 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?

Section 3: Real world challenges
Resilience - How to keep working when everything falls apart

- RFC 1149: A standard for the transmission of IP datagrams on avian carriers
- RFC 2549: RFC 1149 with Quality of Service
- RFC 6214: RFC 1149 adapted for IPv6

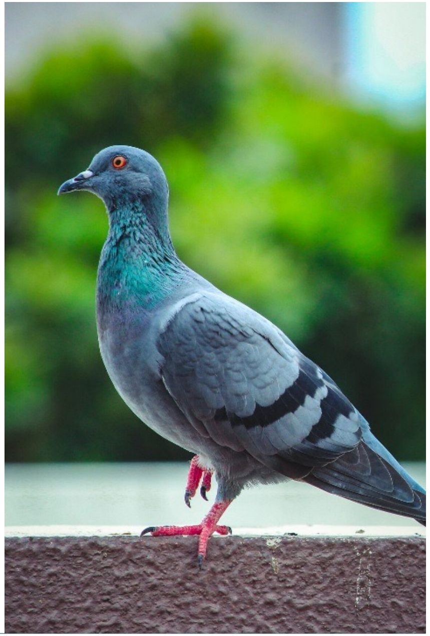


Photo by Kalpesh Patel on Unsplash

Section 3: Real world challenges
Resilience - When not to keep working

- 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.

Section 3: Real world challenges
On-site and off-site Incident Handling

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

Section 3: Real world challenges
On-site and off-site Incident Handling

TF-CSIRT

- Being able to communicate between team members
  - Standard case: set-up some VPNs to enter the CSIRT infrastructure
  - Crisis case: use a dedicated shadow environment
    - Handle with great care! Not a word about that environment

- Preparation
  - Stand-by environment
  - Strict rules of usage
  - Dedicated means of communication
  - Personal belongings

Photo by Oscar Nilsson on Unsplash

Section 3: Real world challenges
On-site and off-site Incident Handling

TF-CSIRT

- Use of standalone resources
  - Internet may not be easily accessible
  - Local databases and local documentation
  - Spare disk drives, USB keys, …
  - Protection of all resources

- Time zone issues
  - Local CSIRT team members must adapt to business hours of the remote team
  - Reporting to the management must be addressed and adapted

- Preparation
  - Pre-loaded toolkits must be ready
  - Reusable components
  - Portable or virtualized environments

Section 3: Real world challenges
On-site and off-site Incident Handling

- Short-cut and by-pass
  - Money solve many logistical issues
  - Power plugs, HW/SW, Internet access
- Neither jet-lag nor exhaustion can be solved by money
  - Second team must be ready to support
  - Organize work shifts as soon as possible
  - Spare some time for the staff members' personal life
- Prevent from having additional issues
  - Protect the team and its resources while at rest

Photo by Katie Moum on Unsplash

TF-CSIRT

Section 4: Data Acquisition & Threat Intelligence

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

–

–

Threat Intelligence

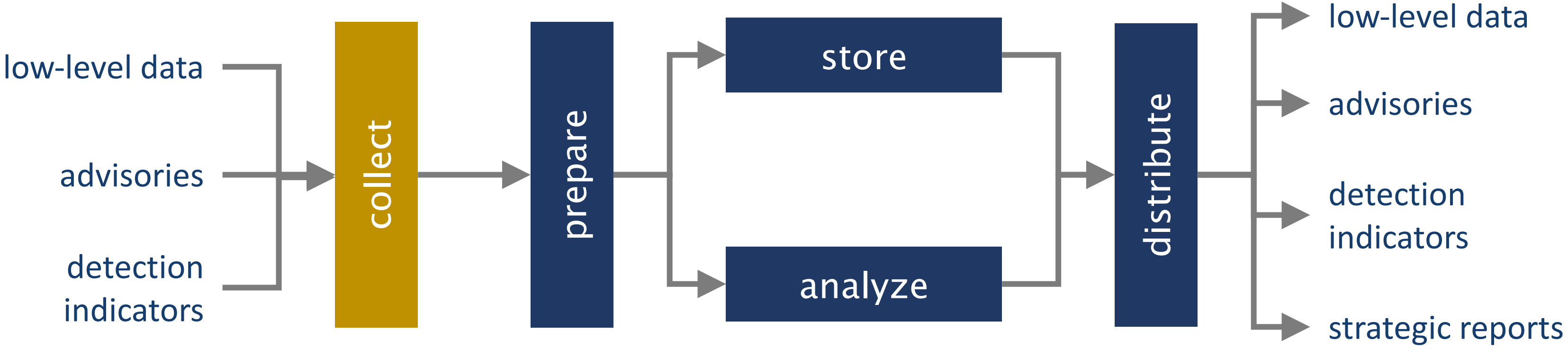
- **Threat intelligence** is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. (Gartner)
- Examples: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

Section 4 – Data Acquisition & Threat Intelligence
Actionable Information

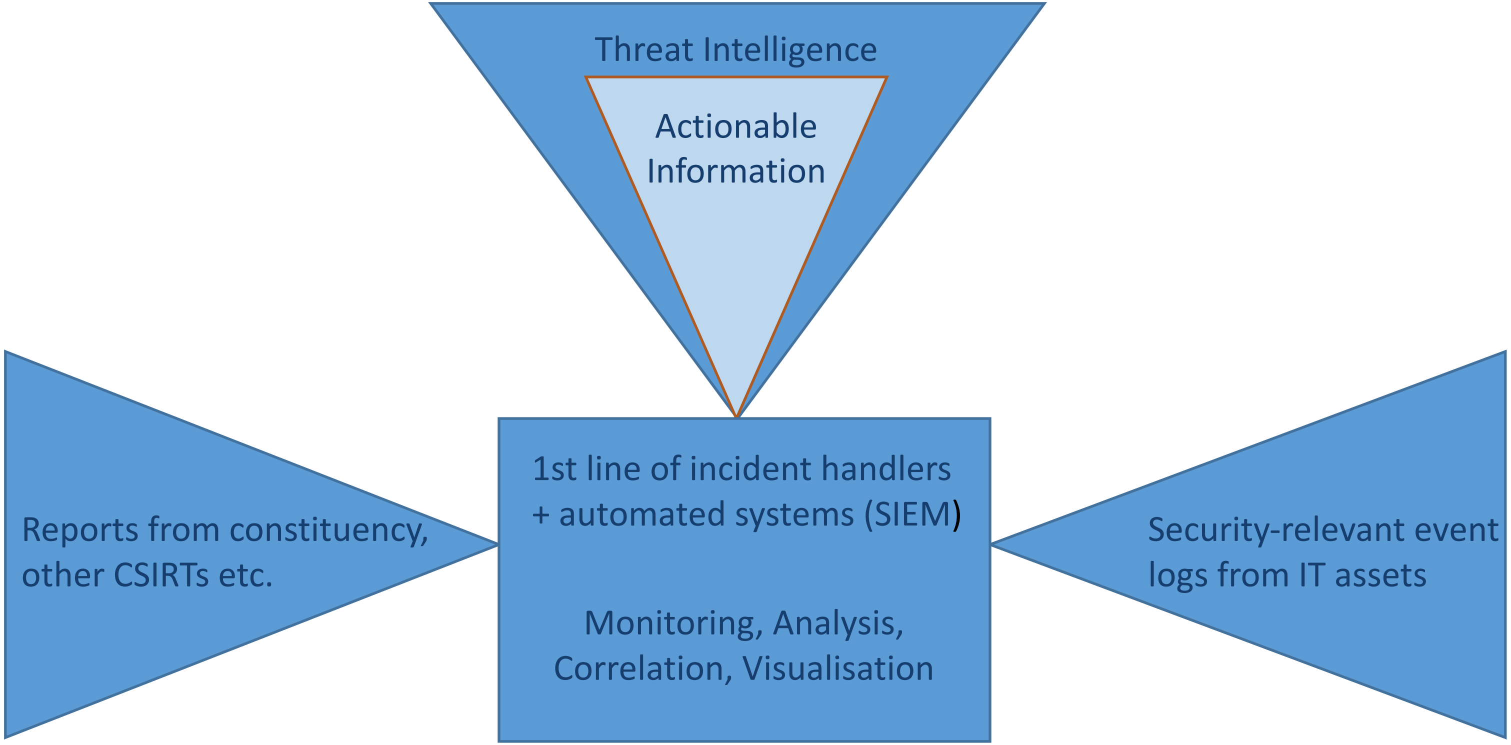
- **Actionable Information** is information that can be examined, expanded, and compared, leading to solid observations and conclusions. It should be ***relevant, timely, accurate, complete*** and ***ingestible***. (ENISA)
- Examples:
  - Vulnerability advisory for a product you are using
  - Anomaly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

Section 4 – Data Acquisition & Threat Intelligence
Data processing model

TF-CSIRT



Section 4 – Data Acquisition & Threat Intelligence
From acquisition of data to detection of incidents



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

Section 4 – Data Acquisition & Threat Intelligence Detection

- Detecting whether incident happened by:
  - Manual reporting
  - Monitoring infrastructure
  - Proactive gathering of information
  - Using outcome from other incident analysis

Photo by Nathan Bingle on Unsplash

Section 4 – Data Acquisition & Threat Intelligence
Detection - Monitoring infrastructure

- Logs
  - System
  - Application
  - Network (netflows, pcaps)
- System/network monitoring
- Security Infrastructure
  - Antivirus, DLP, firewalls, WAFs
- Any others?

Photo by Thomas Charters on Unsplash

Section 4 – Data Acquisition & Threat Intelligence
Detection - Monitoring infrastructure

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

Photo by Helloquence on Unsplash

Detection – Other sources of information

TF-CSIRT

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

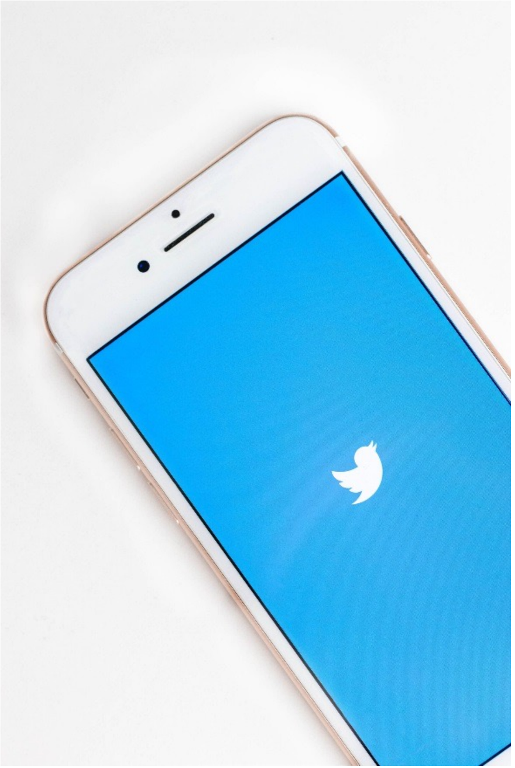


Photo by Sara Kurfess on Unsplash

Section 4 – Data Acquisition & Threat Intelligence Summary

- Fireman are NOT mighty lonesome gurus who can solve ANY fire, no matter its size, location and “combustible”
- Understand that it's a **TEAM** effort, each and everyone cooperating in reaching ”a” solution → **1 + 1 > 2**
- Follow the process rather than creating new ways to solve bleeding edge issues → preparation is key
- Message of the day:
  - **Don't reinvent the wheel**
  - **Follow the rules and operations will run smoother and far better**

Photo by Naassom Azevedo on Unsplash

TF-CSIRT

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

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

–

–

Section 5 – TLP Traffic Light Protocol

- **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

Section 5 – Chatham House Rule

TF-CSIRT

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

–

-