OCTOBER 2023

INCIDENT RESPONSE MANAGEMENT

Barbara Krašovec

Thanks to Romain Wartel and Hannah Short

Security incidents happen
- It’s a matter of “when”, not “if”

John Chambers (former executive chairman and CEO of Cisco Systems) **famously said, “There are only two types of organisations: those that have been hacked and those that don’t know it yet.”**

TABLE
of contents

01. Approaches to cybersecurity incident response

02. Policies and procedures

03. IR Communication

04. IR process

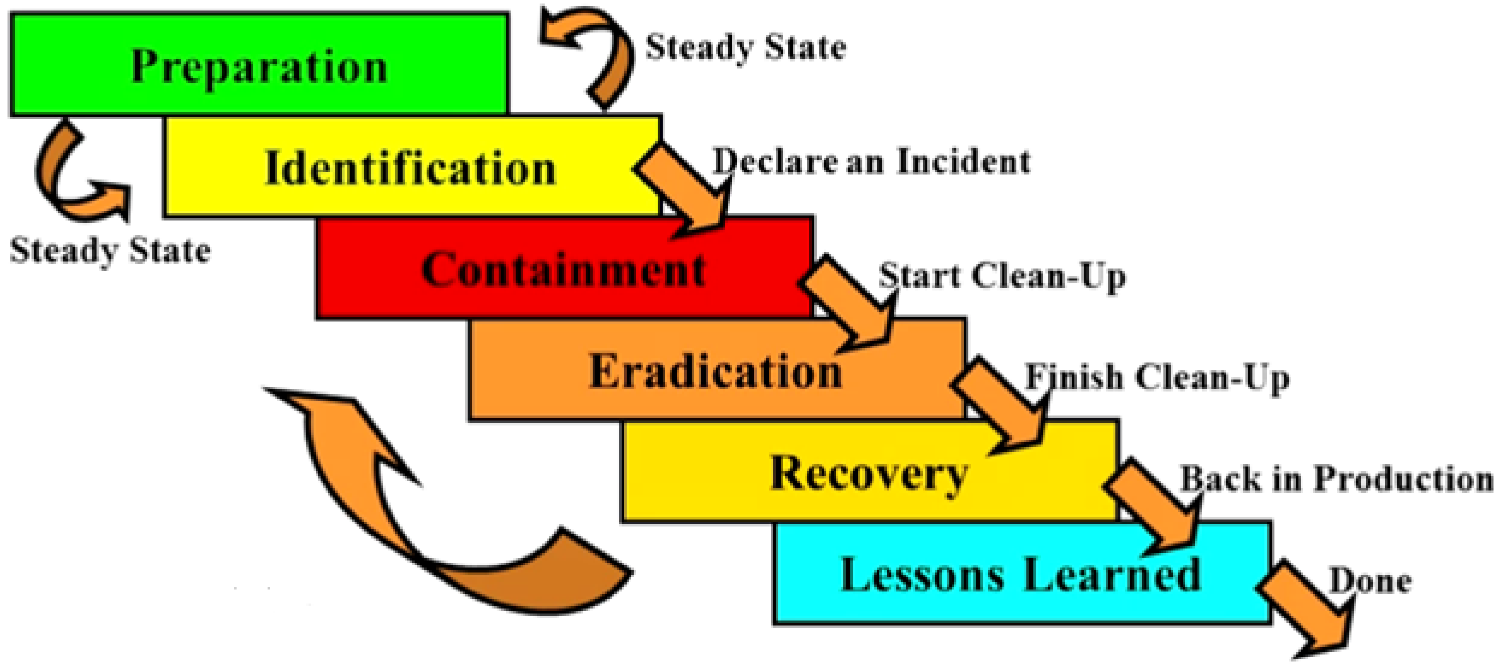
05. Examples

What is incident response?

Incident response (IR) is the process by which an organization handles a data breach or cyberattack. It is an effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.
(source: IBM)

Approaches to IR

The incident response model **PICERL** by SANS includes the following processes: **P**reparation, **I**dentification, **C**ontainment, **E**radication, **R**ecovery and **L**essons Learnt.

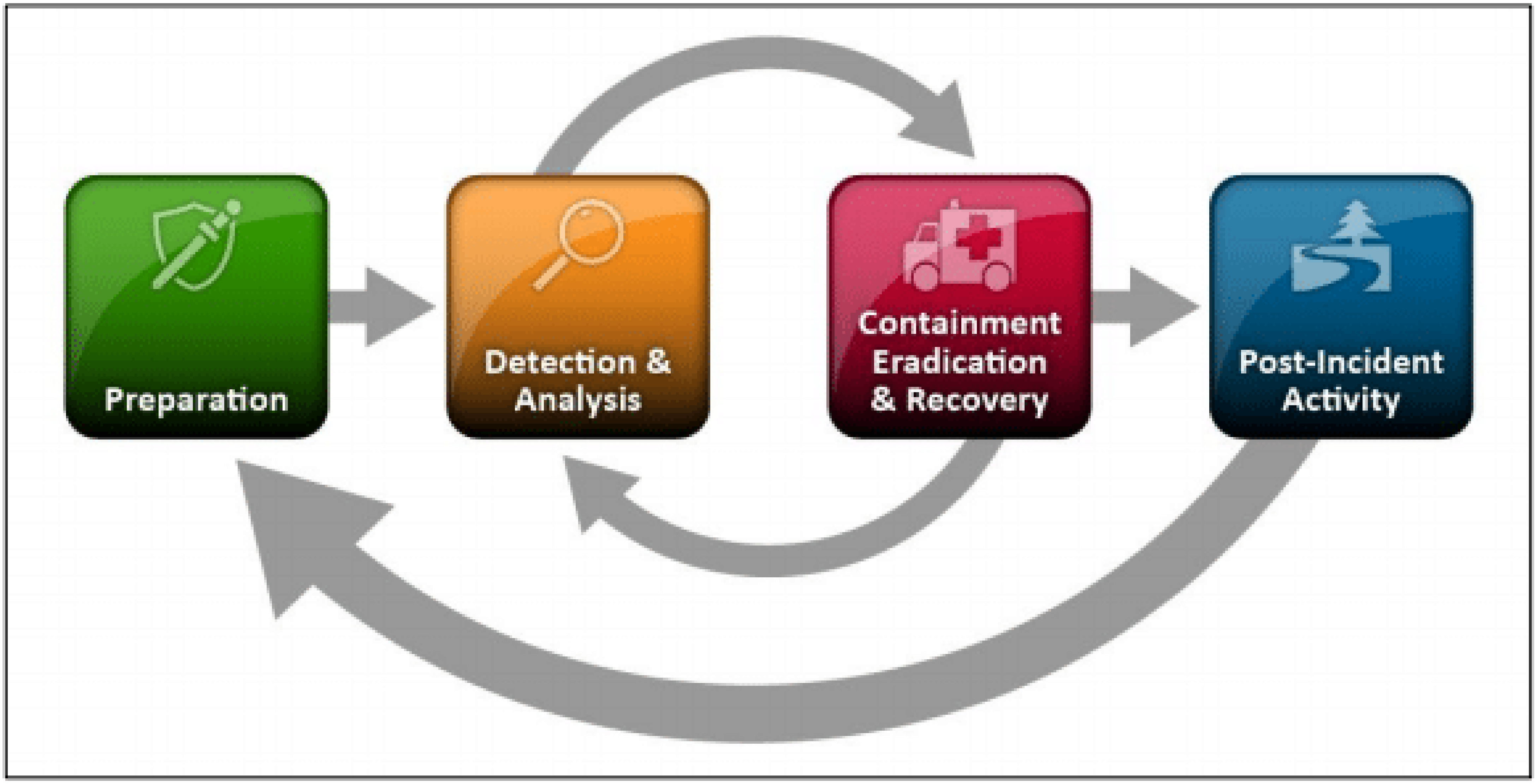


SOURCE: www.medium.com

SOAR - **S**ecurity **O**rchestration, **A**utomation and **R**esponse is a model that allows an organisation to respond automatically - it consists of compatible software that can provide automated responses to security events.

The incident response model **DAIR** - **D**ynamic **A**pproach to **I**ncident **R**esponse. It suggests thinking in terms of waypoints, outcomes, and activities. Waypoints are milestones in the incident response process, such as preparation, detection, verification, and triage. These milestones are not necessarily sequential, but rather occur in a cyclical, ongoing process.

Handling an incident



NIST incident response lifecycle
(source: NIST)

Incident response tasks

- develop IR policies and procedures,
- perform regular risk analysis and vulnerability assessments,
- monitor alerts and report suspicious cyber events,
- provide IR notifications, issue advisories,
- provide training and security exercises for personnel,
- debriefings (lessons learnt),
- run analysis/forensics,
- response coordination,
- provide expertise.

Most common threats

- Email is still the leading infection vector (phishing),
- theft of user credentials,
- (zero-day) software vulnerabilities,
- malware (trojan, ransomware, rootkits),
- DoS,
- brute force password attacks.

IR LIFECYCLE

Image by macrovector on Freepik

Preparation phase

The preparation phase includes key elements to help handle an incident.

- Follow organisation policy (set of rules, practices) and define procedures (with documentation and checklists on what needs to be done during response)
- Make an IR plan, where you prioritise the types of incidents based on organisational impact
- Make a communication plan, define communication tools and prepare contact lists
- Ensure proper access rights for the CSIRT team
- Define stakeholders
- Define forensics/analysis tools
- Define roles and responsibilities
- Provide training for responders

What is the objective of incident response?

- to quickly recover and resume operations
- to prevent reputation damage
- to understand what happened

Who has the main roles and is responsible?

- team leader
- lead investigator
- communication manager
- forensics coordinator

Adapt strategy, resources and goals according to the evolving threat landscape and organisation's goals

Policies, procedures

- When designing your procedures, avoid reinventing the wheel. Use templates:
  - AARC project: https://aarc-project.eu/policies/policy-development-kit/
  - WISE: https://wise-community.org

A policy describes high-level principles, it is a set of rules in an organisation (rarely changes)

A procedure is derived from the policy with all practical implementation details

- Start with **AUP for users**
- Define **IR procedure**, roles in IR and responsibilities of all stakeholders
- **Involve all key stakeholders** in the review of the policy and procedure
- Limit exceptions or custom processes: stick with the rest of the organisation's workflow
- **Document** and share your policy and procedure
- Transparency helps manage expectations, clarifies roles and responsibilities
- Test/update on a regular basis

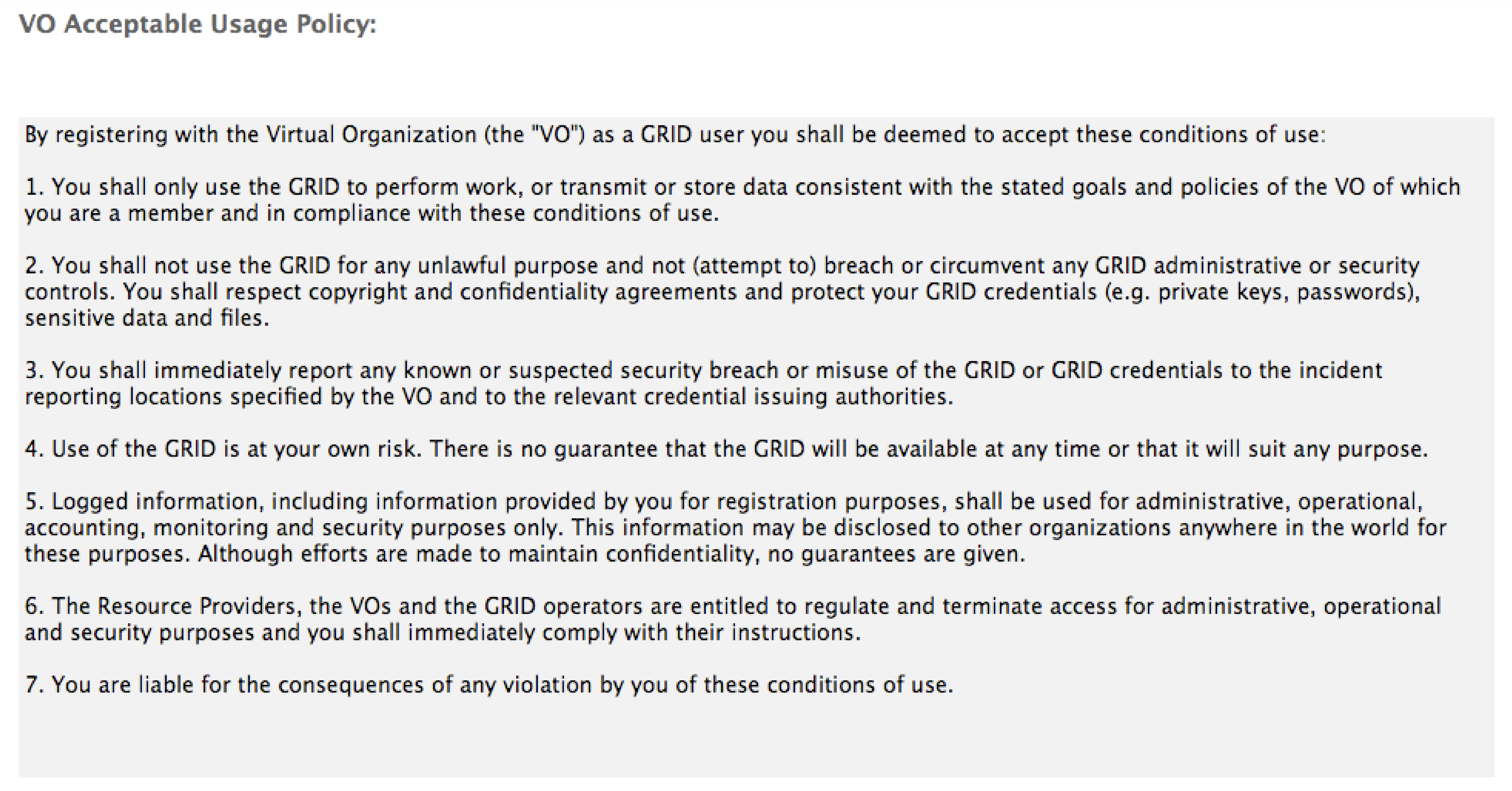
AUP = Acceptable use policy

It should include:

- defined acceptable and non-acceptable use,
- user registration,
- protection and use of authentication and authorisation credentials,
- data protection and privacy,
- disclaimers,
- liability ,
- sanctions.

See: https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

AUP = Acceptable use policy



VO Acceptable Usage Policy:

By registering with the Virtual Organization (the "VO") as a GRID user you shall be deemed to accept these conditions of use:

1. You shall only use the GRID to perform work, or transmit or store data consistent with the stated goals and policies of the VO of which you are a member and in compliance with these conditions of use.

2. You shall not use the GRID for any unlawful purpose and not (attempt to) breach or circumvent any GRID administrative or security controls. You shall respect copyright and confidentiality agreements and protect your GRID credentials (e.g. private keys, passwords), sensitive data and files.

3. You shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the VO and to the relevant credential issuing authorities.

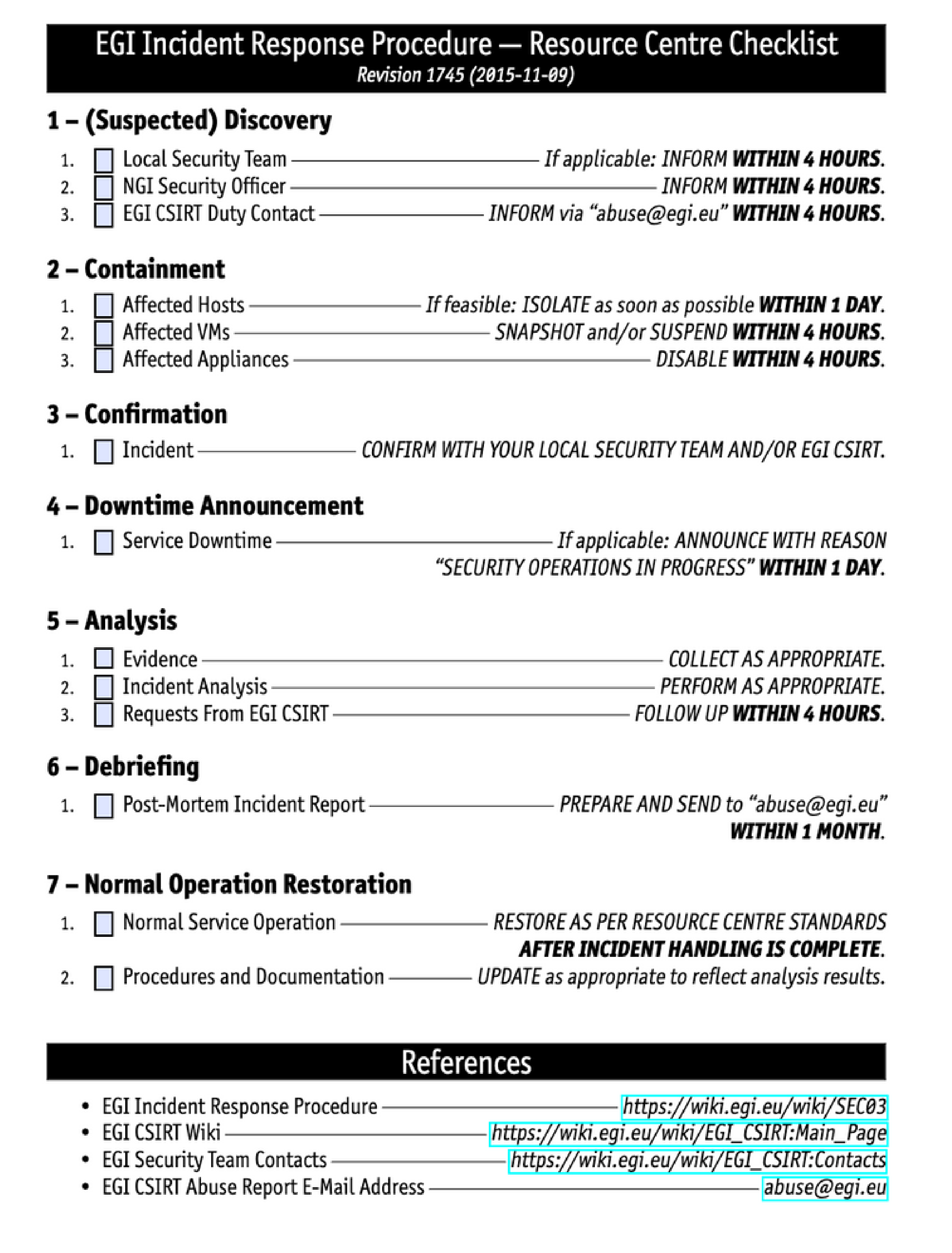
4. Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose.

5. Logged information, including information provided by you for registration purposes, shall be used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed to other organizations anywhere in the world for these purposes. Although efforts are made to maintain confidentiality, no guarantees are given.

6. The Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions.

7. You are liable for the consequences of any violation by you of these conditions of use.

Incident response procedure



EGI Incident Response Procedure — Resource Centre Checklist

Revision 1745 (2015-11-09)

1 – (Suspected) Discovery

1. □ Local Security Team — *If applicable: INFORM **WITHIN 4 HOURS**.*
2. □ NGI Security Officer — *INFORM **WITHIN 4 HOURS**.*
3. □ EGI CSIRT Duty Contact — *INFORM via "abuse@egi.eu" **WITHIN 4 HOURS**.*

2 – Containment

1. □ Affected Hosts — *If feasible: ISOLATE as soon as possible **WITHIN 1 DAY**.*
2. □ Affected VMs — *SNAPSHOT and/or SUSPEND **WITHIN 4 HOURS**.*
3. □ Affected Appliances — *DISABLE **WITHIN 4 HOURS**.*

3 – Confirmation

1. □ Incident — *CONFIRM WITH YOUR LOCAL SECURITY TEAM AND/OR EGI CSIRT.*

4 – Downtime Announcement

1. □ Service Downtime — *If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS" **WITHIN 1 DAY**.*

5 – Analysis

1. □ Evidence — *COLLECT AS APPROPRIATE.*
2. □ Incident Analysis — *PERFORM AS APPROPRIATE.*
3. □ Requests From EGI CSIRT — *FOLLOW UP **WITHIN 4 HOURS**.*

6 – Debriefing

1. □ Post-Mortem Incident Report — *PREPARE AND SEND to "abuse@egi.eu" **WITHIN 1 MONTH**.*

7 – Normal Operation Restoration

1. □ Normal Service Operation — *RESTORE AS PER RESOURCE CENTRE STANDARDS **AFTER INCIDENT HANDLING IS COMPLETE**.*
2. □ Procedures and Documentation — *UPDATE as appropriate to reflect analysis results.*

References

- EGI Incident Response Procedure — *https://wiki.egi.eu/wiki/SEC03*
- EGI CSIRT Wiki — *https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page*
- EGI Security Team Contacts — *https://wiki.egi.eu/wiki/EGI_CSIRT:Contacts*
- EGI CSIRT Abuse Report E-Mail Address — *abuse@egi.eu*

- IR procedure needs to exist for:
    - **Users** who report an incident
    - **Staff** who need to contain the incident, report or escalate
    - **Security teams**: detailed steps to coordinate the response
- Enforce procedures by using checklists.

Communication

- CSIRT needs to communicate with relevant stakeholders **during and after the incident**
- communications can be legally mandated or non-mandatory (sharing with the community, gaining information from other sources, including other technical teams, especially in case of federated access)
- The communication plan needs to include:
    - **how to communicate internally**
    - **how to communicate to external stakeholders**
    - **what are the roles and responsibilities (who communicates with whom)**
    - **identification of emergency contacts**
    - **contact list of all relevant stakeholders**
- the communication plan should be exercised in advance, staff should be trained

Communication

- Reporting about an incident often shows the maturity of the organisation
- Communication channels (tools) should be defined in advanced
- How to share sensitive data?

Importance of trusted/informal contacts

- they bring extra expertise, and knowledge in key moments
- helping others when dealing with an incident is beneficial for both parties. You can learn from there and build trust.

Who are the stakeholders?

- management
- IT
- HR (in case of insider attack)
- legal department
- regulator
- customers
- media

Communication with authorities? Obligatory when an attack is treated as cyber crime (eg. CSAM, trafficking with intellectual property, identity theft, frauds).

Communication with the press

- Communicate with the press when it is necessary or when you are obliged by law (e.g. nuclear sector and the matter of public safety)
- Only media-trained people should communicate with the media
- Define policy for media communication

The objective is to instill confidence that everything is under control, and proper actions are being taken.

- Avoid live communication and interaction.
- Explain only facts, don’t make suppositions.
- Assume what you say/write will be cut/paste.
- Don’t be too technical.

Sharing information

- Who needs to share information?
- With whom?
- What kind of information?
- When to share it?
- How? Using which tools? Phone, mail, portal, ticketing system?

Communication with authorities?

- criminalisation
- international incidents
- critical digital services that have an impact on public safety (eg. nuclear)

Training activities and SSC

- Periodic exercises are a must.
- Staff must be trained and should maintain security skills.
- Staff should be familiar with security procedures, policies, communication procedures etc.
- Also run communication challenges to verify that your contact list still contains valid contacts.

Detection and analysis

Can a deviation from normal operations be treated as an incident?

- **What are the IoCs?**
  - unusual network traffic
  - unusually high CPU usage
  - cleared log files
  - configuration changes
  - access to a server from an unusual IP address or user
  - sudden large quantities of transferred files
  - long-running sessions on a server
  - an employee finds an unknown USB drive somewhere
  - alert from IDS

Cyber event =! Incident

MTTI = mean time to identify

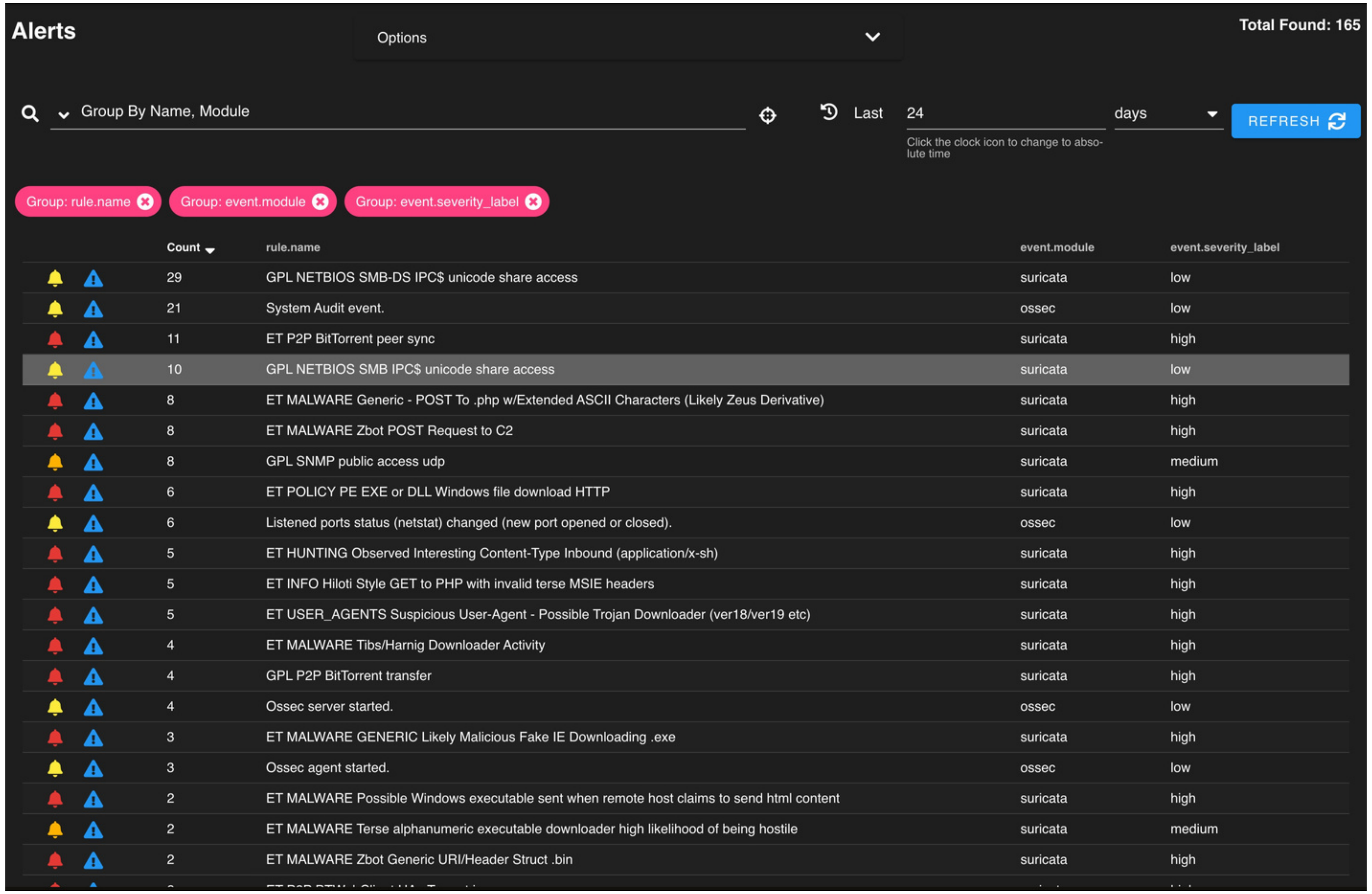
- usually very long (average around 200 days)
- efficient IR can significantly decrease the time

Assessment of the event - > If the event is confirmed as an incident, it is reported and then handled by the CSIRT team

Detection and analysis

Logging and monitoring

- SOC monitors the network and examines logs from hosts, devices, firewalls and alerts from IDS.
- SOC performs analysis of suspicious events and identifies potential impacts.
- Proactive research and analysis of emerging threats.



Count	rule.name	event.module	event.severity_label
29	GPL NETBIOS SMB-DS IPC$ unicode share access	suricata	low
21	System Audit event.	ossec	low
11	ET P2P BitTorrent peer sync	suricata	high
10	GPL NETBIOS SMB IPC$ unicode share access	suricata	low
8	ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)	suricata	high
8	ET MALWARE Zbot POST Request to C2	suricata	high
8	GPL SNMP public access udp	suricata	medium
6	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
6	Listened ports status (netstat) changed (new port opened or closed).	ossec	low
5	ET HUNTING Observed Interesting Content-Type Inbound (application/x-sh)	suricata	high
5	ET INFO Hiloti Style GET to PHP with invalid terse MSIE headers	suricata	high
5	ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc)	suricata	high
4	ET MALWARE Tibs/Harnig Downloader Activity	suricata	high
4	GPL P2P BitTorrent transfer	suricata	high
4	Ossec server started.	ossec	low
3	ET MALWARE GENERIC Likely Malicious Fake IE Downloading .exe	suricata	high
3	Ossec agent started.	ossec	low
2	ET MALWARE Possible Windows executable sent when remote host claims to send html content	suricata	high
2	ET MALWARE Terse alphanumeric executable downloader high likelihood of being hostile	suricata	medium
2	ET MALWARE Zbot Generic URI/Header Struct .bin	suricata	high

Analysis methodology

- verify the incident
- **gather system description**, how it is connected to other systems, who has access to it, in which network segment is it placed, what is the impact of its compromise
- **collect information**: evidence of compromise, logs, reports, history files, traces on the system
- **find an entry point** and the security gap
- create **timeline**
- **record all activities** (e.g. by running script program on linux)
- **analyse** the gathered data and make a list of IoCs
- **recover** data

Timelines

- Keep **timelines of your findings** (what did you discover in the analysis, where and when) and **timings of the incidents** (which activities were found on the compromised host and when did they start)

- Document every action taken with timestamps
- Some innocuous details may become key later
- Document all your actions, these documents should answer the Who, What, Where, Why, and How questions.

- Use tools to write them, such as https://thehive-project.org/

What to look for?

- look for abnormalities (performance issues, changed files, long sessions, a lot of outbound connections etc.)
- look for changed files (new accounts, new cronjobs, file changes, changed binaries etc.)
- check if log files were deleted
- check the folders that are world-writable
- check for processes with unusual activity or name
- checking network and DNS logs give some answers
- check IDS alarms
- check open files (lsof -i), sockets, file descriptors etc.
- check for executables using linked libraries that are unknown (could indicate malicious code - check with ldd)

USEFUL COMMANDS:

```
lsof
vmstat
uname
uptime
date
netstat
who
ps
ip
last
tcpdump
```

Common mistakes

- do not save findings on local disk, use external media devices, network devices or save them in memory (/dev/shm)
- do not cause any changes on the system (changes to files, times)
- poor network monitoring (turn on DNS logging, add network sniffer, enable auditing, increase the size of log retention)

Software for analysis

Network Tools	Disk analysis	(Rootkit) scanners	Memory dump analysis
tcpdump nmap Wireshard TShark Zeek	parted Sleuth kit Scalpel Autopsy foremost	RKHunter Chkrootkit Malwarebytes	Volatility Varc

Malware analysis Reverse Engineering	Development tools	Other	Timelines
Remnux Ghidra	GCC Perl Python gdb strace	git hashcat docker veracrypt John the Ripper	Hive log2timeline

Containment

Reduce the impact: After a suspected incident is confirmed, it needs to be contained so as not to cause any more damage. The goal is to stabilise environment

MTTC = mean time to contain

- usually very long (average around 70 days)
- efficient IR can significantly decrease the time

Possible actions:

- isolate network segment (where the compromised server is located)
- power down a switch
- change password
- disable a service
- blacklist an IP
- replace the compromised system with the replica
- create a memory dump and backup of the system, before wiping it (make VM snapshot)
- collect all IoCs

Eradication

- Examples of eradication:
  - reinstallation of the system and restoration,
  - scanning the network for IoCs,
  - removing the malware and patching the security hole,
  - It can also be resetting all affected user accounts,
- It is crucial to collect the evidence before the eradication phase and understand what happened and why.
- The outcome of this phase should include additional security measures that will prevent the same compromise from happening again.

Eradication is the full removal of any malicious code or other threats that were introduced to the environment during the incident, minimising the risk of reoccurrence and restoring affected systems to their previous state, ideally while minimizing data loss.

- determine the cause
- remove backdoors
- improve security controls
- run vulnerability scan
- improve monitoring

Recovery

RECOVERY STEPS:

- Patch or reinstall the compromised system, remove malicious software, identify the attacker's entry point to the server, and remove the security gap.
- Update hardware firmware and BIOS if there are newer versions available, especially if they include security patches.
- Configure servers and services using automatic configuration management.
- Reset user accounts if they were exposed.
- Restore the data from the backup.
- Verify perimeter security (firewall rules, ACLs etc.)
- Configure remote logging for each server.
- After all previous steps, reconnect the rebuilt system to the network.
- Test services and security controls.
- Restore the system to its normal operations.
- Monitor the system for abnormal behaviour and for any suspicious activity.

Take appropriate measures to prevent the same attack from happening again

- **Update technical and organisation measures**
- **Update documentation**
- **Provide additional training and raise awareness**
- **Update monitoring**

Post-activities

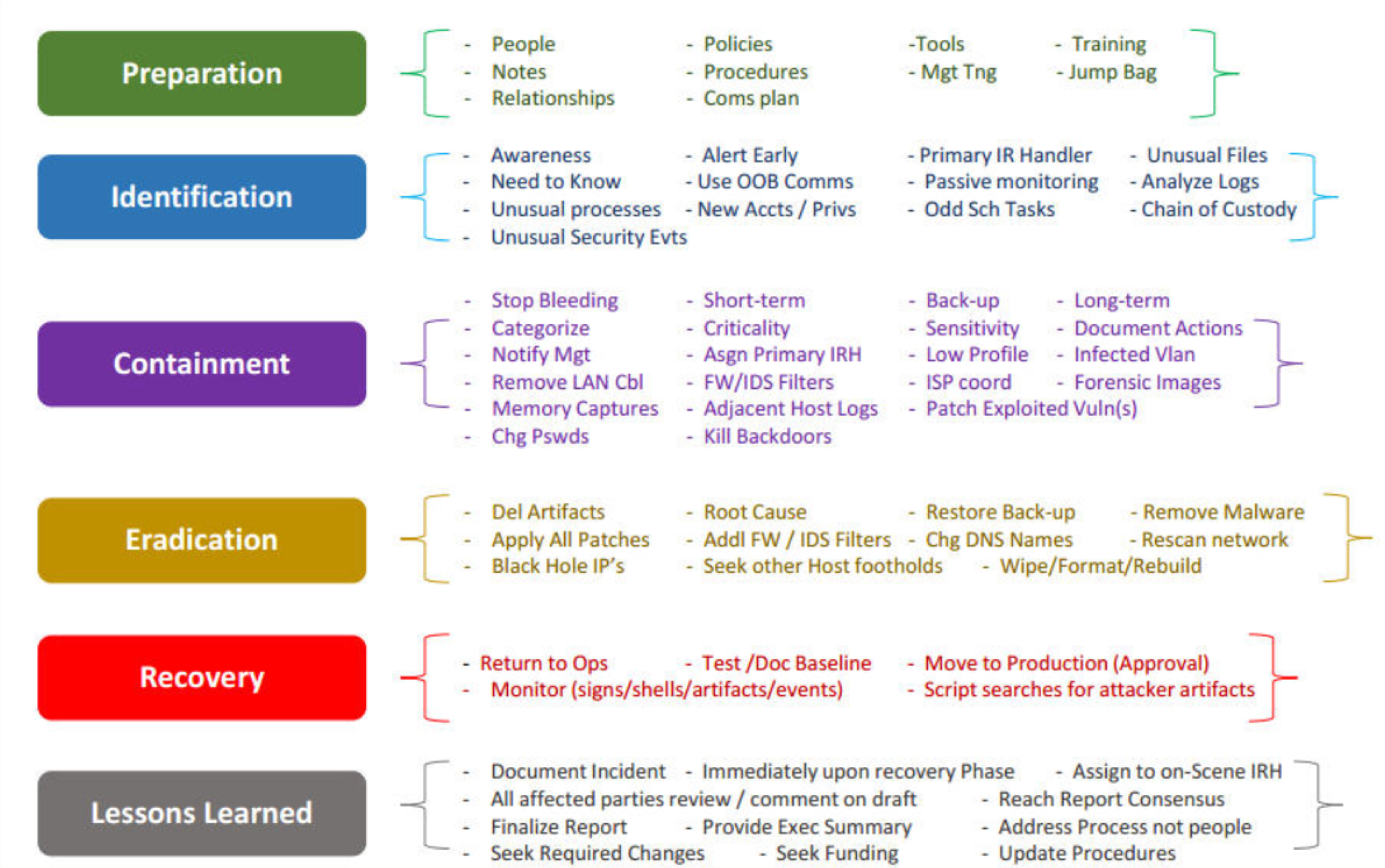
- **Lessons learnt** is the final process of IR, also called **debriefing**.
- documentation should be wrapped up,
- all steps of the incident response should be discussed and reviewed,
- final report should be sent to all stakeholders
- time to conduct a detailed post-incident review and identify areas of improvement (root cause analysis and corrective measures)
- Invite all stakeholders to a lessons learnt meeting and discuss these questions. The answers on how to improve the incident response process should be included in the documentation, policies and procedures right away.

- **The goal is to make the incident response process more effective and efficient.**
- **The lessons learnt phase should not be overlooked, as it may lead to repeating the same mistakes over and over again.**

QUESTIONS

- What happened, how and why?
- What was the scope?
- How was the incident contained and eradicated?
- How did we/the site deal with it?
- What were the problems and what can be done to eliminate them?
- What went well?
- What was missing (contact list or procedure etc.) or went badly?
- What needs to be changed?
- How did the recovery process go, what was done?

PICERL cheat-sheet



Preparation

- People
- Notes
- Relationships
- Policies
- Procedures
- Coms plan
- Tools
- Mgt Tng
- Training
- Jump Bag

Identification

- Awareness
- Need to Know
- Unusual processes
- Unusual Security Evts
- Alert Early
- Use OOB Comms
- New Accts / Privs
- Primary IR Handler
- Passive monitoring
- Odd Sch Tasks
- Unusual Files
- Analyze Logs
- Chain of Custody

Containment

- Stop Bleeding
- Categorize
- Notify Mgt
- Remove LAN Cbl
- Memory Captures
- Chg Pswds
- Short-term
- Criticality
- Asgn Primary IRH
- FW/IDS Filters
- Adjacent Host Logs
- Kill Backdoors
- Back-up
- Sensitivity
- Low Profile
- ISP coord
- Patch Exploited Vuln(s)
- Long-term
- Document Actions
- Infected Vlan
- Forensic Images

Eradication

- Del Artifacts
- Apply All Patches
- Black Hole IP's
- Root Cause
- Addl FW / IDS Filters
- Seek other Host footholds
- Restore Back-up
- Chg DNS Names
- Wipe/Format/Rebuild
- Remove Malware
- Rescan network

Recovery

- Return to Ops
- Monitor (signs/shells/artifacts/events)
- Test /Doc Baseline
- Move to Production (Approval)
- Script searches for attacker artifacts

Lessons Learned

- Document Incident
- All affected parties review / comment on draft
- Finalize Report
- Seek Required Changes
- Immediately upon recovery Phase
- Provide Exec Summary
- Seek Funding
- Assign to on-Scene IRH
- Reach Report Consensus
- Address Process not people
- Update Procedures

Source: https://www.sans.org/media/score/504-incident-response-cycle.pdf

Common misakes

- No plan and no procedures in place
  - IR then takes much longer (longer time required for recovery
  - Often some traces are missed
  - Coordination between people takes a lot of time, a lot of confusion who does what, who is responsible
  - No tools available for forensics, means, longer time to investigate
- Damage the evidence
  - During an investigation (change access times on files)
  - Leaving traces in the logs/history files
- Blame culture
  - Don't blame an employee because it can have big consequences
- Poor communication
  - Caused either by poor language skills or done inconsistently and with partial data
  - It leads to confusion, misinformation, misunderstanding
- No logs available
- Compromised server or VM rebooted

ALSO:

- no backups
- destroying the evidence
- failure to container or eradicate
- failure to prevent the same incident from happening again
- failure to report or ask for help
- failure to handle IR all together

Recap

- The goals of IR: to quickly recover, prevent reputation damage, understand what happened and inform all the stakeholders.
- procedures need to be setup in advance: how to contain an incident, who to communicate with, via which channels, how to share data with the stakeholders, which tools will be used for forensics etc.
- Why did the incident happen? (status of security controls)
- Why wasn't it detected? (status of sensors, monitoring)
- How to prevent it from happening again?
- Well-defined procedures will help you keep the focus, you will stay in control and will not be led by the flow of events.
- Report an incident, even if it is unconfirmed.
- Sharing the IoCs with the community is priceless.

Lessons learnt from previous EGI-CSIRT incidents

- Never switch off a compromised system, valuable data will be lost. It will be difficult or impossible to establish a timeline of the events. Valuable data, even if deleted by the attacker, resides in the memory.

Lessons learnt from previous EGI-CSIRT incidents

- Keep a timeline of the incident (findings) and the timeline of the actions taken by the security team. It is crucial if someone else joins as a responder or takes over.

Lessons learnt from previous EGI-CSIRT incidents

- Major problem if no monitoring or logging service is in place.

Lessons learnt from previous EGI-CSIRT incidents

- Some incidents have not been detected for months - improving detection is a must in multiple organisations.

Lessons learnt from previous EGI-CSIRT incidents

- Sharing IoCs with other sites is priceless. It is a way to discover or prevent an incident at another site.

- SOC (MISP)
- email ?

Lessons learnt from previous EGI-CSIRT incidents

- Always verify the IoCs reported by sites, they may be false positives (site might make suppositions that turn out not to be valid)

Lessons learnt from previous EGI-CSIRT incidents

- When reporting, state only facts, don’t make any speculations
- all traces should be investigated.

Lessons learnt from previous EGI-CSIRT incidents

- Only allow media-trained people to communicate with the media, otherwise, more damage than good is done.

Lessons learnt from previous EGI-CSIRT incidents

- Do not forget to use the TLP designation when communicating with stakeholders.
- On which channels will this be communicated?

Lessons learnt from previous EGI-CSIRT incidents

- Private communication channels are very beneficial, usually you can get the information faster, but they should be clearly noted in the timeline and copied to the ticketing system and IR tools where you run the case.

Lessons learnt from previous EGI-CSIRT incidents

- IR is a team effort, not an effort of a security officer on duty - since teams work in shifts, it is important to document everything that is happening for the shift turnover

And as a community?

Attacks are becoming more and more complex and sophisticated, usually include multiple compromised machines or even sites. Individuals at the sites do not necessarily have enough expertise to deal with the incident.

As a community, we need to:

- build trust and collaborate,
- share threat intelligence,
- establish SOC (MISP + Zeek),
- provide joint security operations and incident response (as EGI CSIRT does for EGI community).

BUT as a community...

- Who will take care of central coordination? - a matter of everyone, but no one’s job
- How will the people involved communicate? Email is not the best option, messaging services are multiple, and people have different preferences.
- How to share data?
- Who can be trusted to join?
- What is the motivation of each individual?
- Who will provide tools to manage IR?

EduGAIN

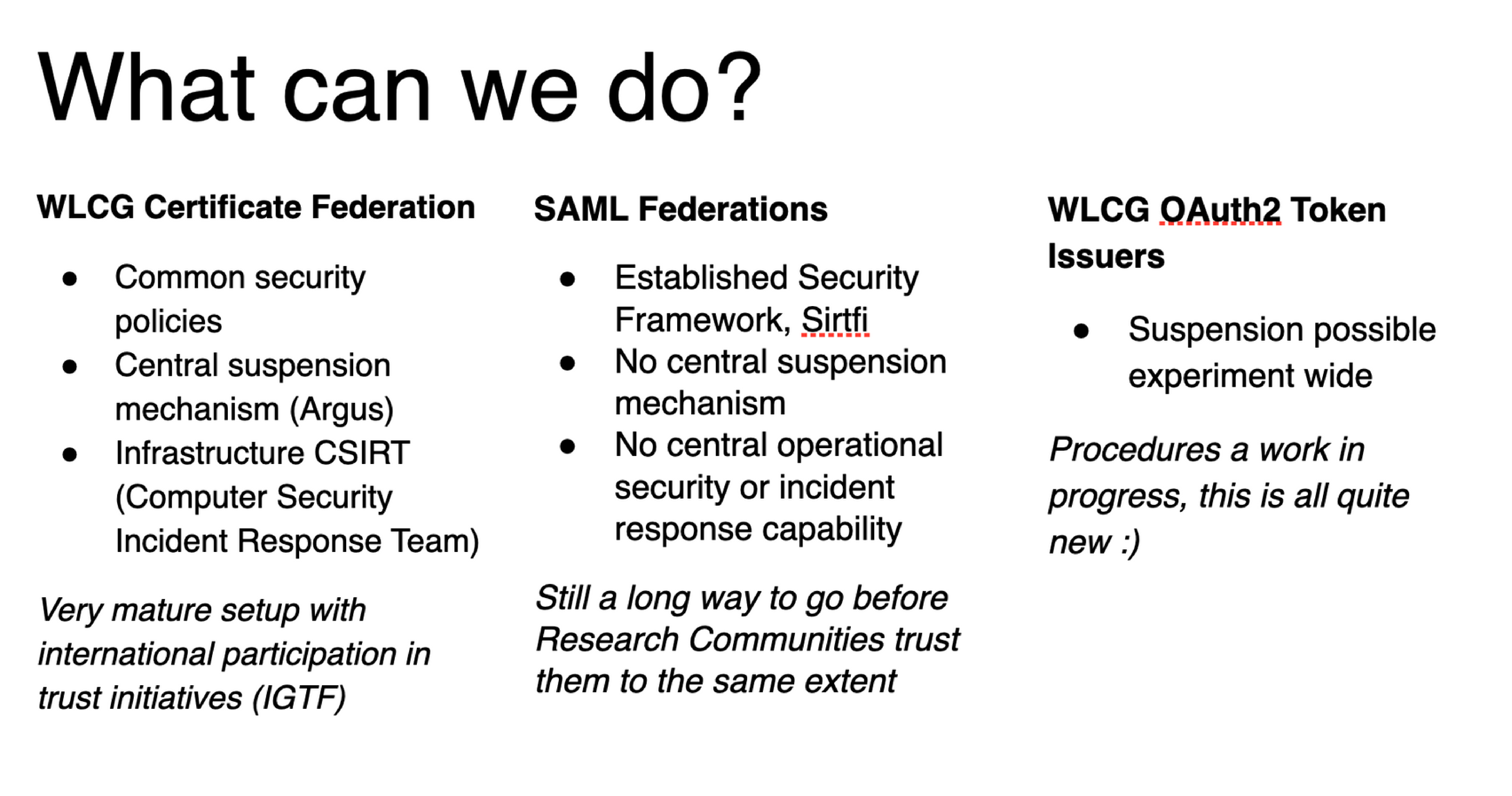
- large community, more than 4000 organisations
- organisations don’t necessarily know or trust each other
- can evidence be shared?
- who can/has to store it?
- are contact points provided?
- how to share data without breaking the rule of confidentiality

SUSPENSION

- Each service could suspend the account
    - How can they share the information between each other?
    - How do they know when the compromise has been resolved?
    - Won’t this take a long time anyway?
- The identity provider could suspend the account
    - What if they don’t react quickly?
    - How do we contact them?
    - What if they refuse?

Slide by Hannah Short

EduGAIN



What can we do?

WLCG Certificate Federation

- Common security policies
- Central suspension mechanism (Argus)
- Infrastructure CSIRT (Computer Security Incident Response Team)

Very mature setup with international participation in trust initiatives (IGTF)

SAML Federations

- Established Security Framework, Sirtfi
- No central suspension mechanism
- No central operational security or incident response capability

Still a long way to go before Research Communities trust them to the same extent

WLCG OAuth2 Token Issuers

- Suspension possible experiment wide

Procedures a work in progress, this is all quite new :)

Slide by Hannah Short

How do attackers hack highly secure systems?

The maturity concerning security varies. However, organisations with a respected and long tradition in security still get hacked, even if they have zero trust and defence-in-depth protection. How is this possible?

- phishing is still the most common attack vector (security is a matter of all, not of an IT department, education is crucial)
- human error (e.g. misconfiguration, wrong order of ACL rules etc)
- service bug
- crash of prevention system
- malicious insider (grumbled employee)

Some examples

Zero day vulnerabilities

A zero-day vulnerability is an undiscovered flaw in an application or operating system, a gap in security for which there is no defence or patch because the software maker does not know it exists (HPE)

- it is like a hidden backdoor that no one knows about
- one of the “famous” examples was log4j

Phishing

- **SPEAR PHISHING**: a phishing attack that targets a specific person in organisation
- **WHALING**: phishing that targets managers - impersonating high-ranking personnel to convince someone to disclose data, transfer money, grant access…
- **BARREL PHISHING:** fools victims in two different emails, the first one is to establish trust and doesn't contain malware, the second contains malware

Insider threats

Insider threats are cybersecurity threats that originate with authorized users—employees, contractors, business partners—who intentionally or accidentally misuse their legitimate access, or have their accounts hijacked by cybercriminals. (IBM)

- especially problematic as the attacker is within the organisation, with certain access rights and knowledge
- this type of attack is often underestimated
- can be unintentional or malicious
- what triggers them? life/work event, dispute, money
- malicious threat:
    - corporate espionage
    - data destruction.
    - data theft
    - impact on performance
    - lost confidence among colleagues

Insider threats

Malicious Insider Threat Indicators:

- unusual logins
- repeated attempted use of unauthorized applications
- an increase in escalated privileges
- excessive downloading of data
- unusual employee behaviour

Always inform HR and management. And remember that making accusations against a colleague has serious consequences on his/her work and/or life.

Advanced persistent threats

An advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time. APT attacks are initiated to steal data rather than cause damage to the target organization's network. (TechTarget)

- it is like someone is spying on you, watching every move you make,
- they use multiple tactics, every move is well calculated (like in a chess game)
- to gather intelligence about the target: reconnaissance (exploit by social engineering)
- when they enter the organisation’s internal network, they install malware, usually coded especially for the target
- code is obfuscated, they use rootkits - difficult to detect
- they can collect data for months
- famous examples: Stuxnet (Iranian nuclear plant), Aurora (stealing intellectual property, Cosy/Fancy Bear (high-profile espionage against political institutions by Russian APT group)

Side-channel attacks

An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions. (NIST)

- it is like a spy eavesdropping - not decrypting the information, but exploiting leaks in the communication process
- attacks usually not expected
- One such example is Wim van Eck’s attack, which is also known as a Transient Electromagnetic Pulse Emanation Standard (TEMPEST). This attack monitors the electromagnetic field (EMF) radiation emitted by a computer screen to view information before it is encrypted.
- Spectre and Meltdown

Quiz

1. What are the main phases of incident response?
2. Which of the following should be included in the preparation phase of the incident response?
    - ○ write procedures
    - ○ prepare communication plan
    - ○ choose forensics tools
    - ○ lessons learnt
3. When is it necessary to communicate with the media?
4. One of the goals of information sharing is:
    - ○ to help management understand the attack better
    - ○ to provide interested stakeholders with threat information
    - ○ to improve security based on the threat information
5. When is it necessary to communicate with HR?
6. Name three common mistakes in running incident response.
7. What is the name of the vulnerability that has no patch available?
8. What should an AUP consist of?