CYBER SECURITY INCIDENT RESPONSE

An EE-ISAC White Paper

EE-ISAC

Table of Contents

Document Control

Section	Name	Reviewed & Approved (date & name)
Foreword	Massimo Rocca	Alexander Harsch 30.03.2020
Context	Tania, Christina	Alexander Harsch 30.03.2020
1. Incident Response Phases	Dmytro	Alexander Harsch 30.03.2020
2. Preparation for Incidents	Dmytro, AleksanderW, Marcel, Jalal, Tania	Paul Smith 14.04.2020
3. Detection & Analysis	AleksanderW, Marius, Daniel, Marcel	Paul Smith 14.04.2020
4. Containment, Eradication & Recovery	Ivan, Jalal, Michael	Alexander Harsch 31.03.2020
5. Post-Incident Activity	Marius, AlexanderN	Alexander Harsch 14.04.2020
6. Incident Examples with best practices	Andreas	Alexander Harsch 03.04.2020
Conclusion	Tania, Paul	Alexander Harsch 03.04.2020
Appendix A	AleksanderW	Alexander Harsch 03.04.2020

Foreword

The mission of the European Energy ISAC (EE-ISAC) is to share knowledge among the network of trust, to increase the resilience of the European Energy system: this appears especially true when our community discusses incident response.

Many experts suggest that once security of infrastructure is compromised, especially in the electricity sector, it is already too late and the battle against the attacker is lost. From the point of view of the security analyst, it is strategical to move the attention from event management to set full priority on prevention and planning of countermeasures, but from the perspective of the operator, response is still a big issue and uncovers an entire world of procedures to design, organize and nurture.

Furthermore, this complex topic is out of the scope of the latest regulations and guidelines because, again, the prescriptions focus on risk analysis, risk mitigation and incident reporting.

EE-ISAC members had the urgency to meet and discuss together about best practices, starting from the basic of standards and sharing of our experiences; we discovered soon that available material was too generic and that our research would turn into an opportunity.

We could start a new journey with our contributors among the operators, the vendors and academics to create a live document where we could approach the problems and describe those solutions that we find feasible, scalable and sustainable for our organizations.

The following pages are the results of this experiment. We are confident that other suggestions will come in the next months and that other contributors could enrich our community.

Thank you for your interest in EE-ISAC.

Massimo Rocca

Chair of EE-ISAC

Context

EE-ISAC aims to help energy utilities improve their resilience against cyber-attacks by enabling information sharing and improving cyber security awareness across the energy sector. EE-ISAC has gathered a synthesis of experience from their membership to offer some useful guidance, especially to assist smaller businesses to prepare and respond adequately to cyber incidents.

In recent years several incidents have targeted critical infrastructures, including the energy sector, as Figure 1 demonstrates. As devices used in Operational Technology (OT) facilities trust each other and their users, one compromised device can allow a compromise to the whole system. Previous attacks have made use of that trust. A common preventive measure against this type of attack is the intentional isolation of OT systems using an air gap. While the idea is sound, the experience of recent attacks shows us air gapped systems are not secure and air gapped systems are very rare.

With an increasing likelihood of incidents, and both small and larger organisations being targeted, it is essential to prepare incident response capability in order to safeguard society's dependency on energy.

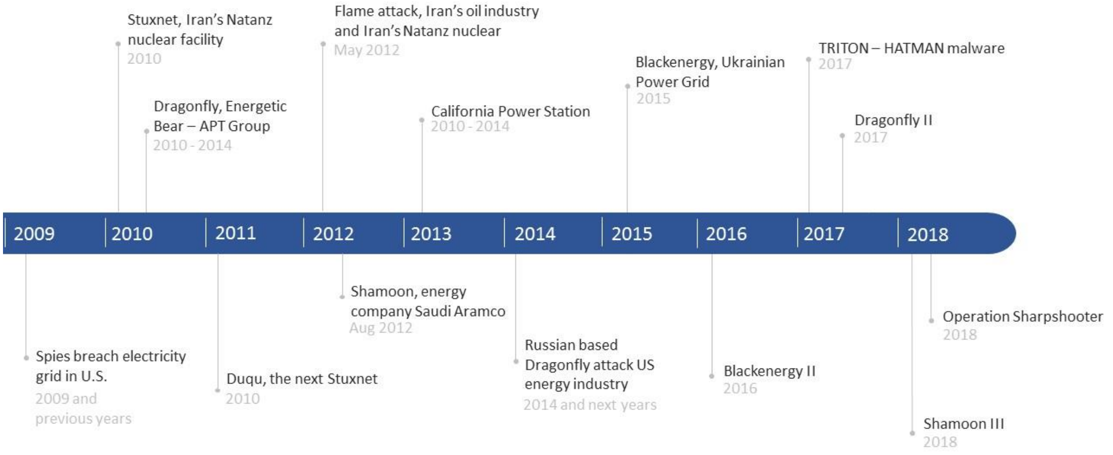
Stuxnet, Iran's Natanz nuclear facility 2010
Flame attack, Iran's oil industry and Iran's Natanz nuclear May 2012
Blackenergy, Ukrainian Power Grid 2015
TRITON – HATMAN malware 2017
Dragonfly, Energetic Bear – APT Group 2010 - 2014
California Power Station 2010 - 2014
Dragonfly II 2017
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Shamoon, energy company Saudi Aramco Aug 2012
Operation Sharpshooter 2018
Spies breach electricity grid in U.S. 2009 and previous years
Russian based Dragonfly attack US energy industry 2014 and next years
Duqu, the next Stuxnet 2010
Blackenergy II 2016
Shamoon III 2018

Figure 1 Incident Timeline [Ref ENISA]

Smaller utilities may have some way to go to implement adequate cyber security. Regulations such as the Network and Information Security (NIS) Directive are now enforcing the requirement for an Incident Response capability. This document aims to offer some assistance in building that capability.

1. Incident Response Phases

Incident Response requires thorough preparation as well as the ability to identify, contain and recover from cyber-attacks.

Several standards and guidelines on incident response exist. The most well-known are ISO 27035:2016 “Information security incident management”, SANS Incident Response Process and NIST 800-61 Rev. 2 “Computer Security Incident Handling Guide”. Here we briefly describe each of them and summarize the proposed approaches into defined stages of incident response.

The ISO 27035:2016, despite its title, concerns mainly IT systems and networks, something many users of ISO 27k series of standards could see as limited, since it does not address other forms of information, such as paperwork, intellectual property, patents, knowledge etc. The ISO 27035 Standard proposes five phases of incident management process:

1. Plan and prepare
2. Detection and reporting
3. Assessment and decision
4. Responses
5. Lessons learned

The SANS Incident Response Process is more focused on a typical malware-based event and was developed especially for computer-based incident response rather than information security incidents. The SANS IR Process consists of six stages:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

The NIST 800-61 Rev. 2 guideline is one of most detailed standards publicly available and more deeply describes the incident response process in computer security. According to the NIST document, there are four main stages of incident response handling:

1. Preparation
2. Detection and analysis
3. Containment, eradication and recovery
4. Post-incident activity

It should be clear that there is no such thing as a single gold standard to organize computer security incident response there and there is no industry-wide agreement on which is the best approach. This document uses terminology as described in the NIST 800-61 Rev.2 guideline [refer to NIST SP 800-61].

2. Preparation for Incidents

Preparedness for cyber security incidents requires a combination of preventive measures and organizational structures and planning to be put in place. In this section, key points regarding these issues are discussed.

Preventive Measures

The following offers some examples of preventative measures that we recommend that can be used to reduce the attack surface and the likelihood of incidents.

Evaluating Risks and Operational Impact

Consider an impact assessment, to explore how your organisation could be affected by different attack scenarios, including advanced persistent threats. Look at the assets affected and how these risks could impact functions and services. The scale of impact will depend on the number of devices compromised or the number of customers if their service or data is affected.

The challenge of securing complex industrial environments from cyber security threats requires a multi-faceted approach that can be difficult to visualise and develop pragmatic controls for. To this end, the Bowtie model can be an effective tool for achieving this.

By plotting the specific threats leading up to an event and the resulting consequences, it becomes easier to plan and incorporate effective controls and isolation mechanisms to either prevent the event from taking place or limit the consequences in case it occurs.

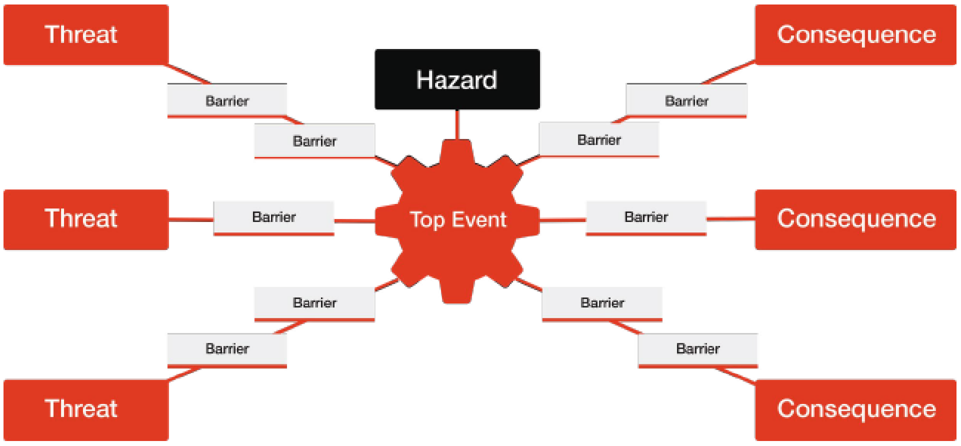

Figure 2 BowTie model [Ref Applied Risk]

Isolation mechanisms are intended as barriers to consume threat actors for a longer time or obstruct them to reach the top event. Targeted attacks against power utilities are planned a long time ahead and aim at generating the top event of disrupting the energy production, transmission and/or distribution. The final event (top event) can only be achieved by combining several events with pre-set timing. The ‘threat tree’ in Figure 3 shows the components needed to generate the top event.

The following show examples of events at each level in the threat tree:

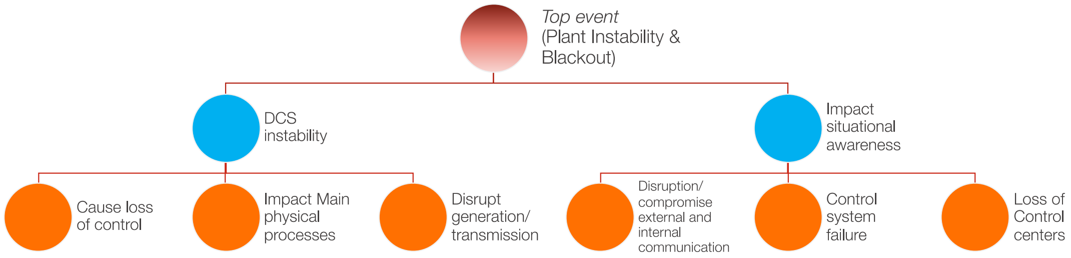
Top event
(Plant Instability & Blackout)
DCS instability
Impact situational awareness
Cause loss of control
Impact Main physical processes
Disrupt generation/ transmission
Disruption/ compromise external and internal communication
Control system failure
Loss of Control centers

Figure 3 Threat Tree [Ref Applied Risk]

Physical Security

Protecting computer and OT systems from unauthorized physical access should be one of the first measures taken. Minimizing entry points to server rooms, security measures on windows, ventilation ducts, fire exits etc., as well as strong organizational security measures to exclude unattended access to systems should be taken. This should be planned especially for legacy systems, which have limited or no authorization capabilities. Special attention should be given to substations and unstaffed facilities in the field.

Managing Vulnerabilities

A key activity to reduce the number of incidents is to reduce the attack surface. An activity to achieve this goal is to address known vulnerabilities in server and client software. From a standardization perspective, two ISO/IEC standards exist that address vulnerability management. While ISO/IEC 29147 addresses vulnerability disclosure, which is more important for vendors, the ISO/IEC 30111 addresses the handling process. It is useful in the context of this paper to use the key concepts outlined in these standards and from other organizations, such as ENISA and NIST, which are shown in the table below.

Term	Definition
Advisory	An announcement or bulletin that serves to inform, advise and warn about a vulnerability of a product or service.
Disclosure	The act of initially providing vulnerability information to a party that was not believed to be previously aware. The overall disclosure process typically includes multiple disclosure events.
Remediation	Patch, fix, upgrade, configuration or documentation change to either remove or mitigate a vulnerability, typically provided by vendors.

Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Zero-Day	A vulnerability for which no patch or fix has been publicly released.

While it is not possible to patch zero-day vulnerabilities, due to patches not being available, the process of identifying which vulnerabilities can be addressed with which patches and when, is the core of the vulnerability management process. The management of vulnerabilities therefore involves their prioritization. A good reference for prioritization are the Common Vulnerability Scoring System (CVSS) scores that are assigned to vulnerabilities, as well as the Common Vulnerability Enumeration (CVE) assignments for vulnerabilities by the vendors. To identify which vulnerability is exploitable, continuous scans, at appropriate intervals to keep track of new systems and applications being added, are an appropriate measure. By doing so, the occurred changes to systems and newly published vulnerabilities can be properly tracked. ENISA has published guidance on vulnerability disclosure and patch management[1].

Security Culture and Awareness

Developing a security culture through awareness raising and training can minimize the risk associated with the human factor in incidents. One of the most important preventative ways of protecting your organisation against cyber-attacks is raising cyber security awareness among employees. Educated personnel should be aware of risks related to:

1. Opening email attachments and links embedded in e-mail messages of unknown origin.
2. Running executables and documents (i.e. drivers, manuals) from an unknown source.
3. Using foreign, unidentified devices found in the office building.
4. Remote connections from untrusted networks.
5. Revealing internal, confidential information to external entities.
6. Other behaviours that include social engineering.

A company should have a well-established cyber security awareness plan. It can include:

1. An on-boarding training for new employees.
2. Regular basic cyber security meetings for all employees.
3. A series of short articles in internal newsletters or printed bulletins.
4. A phishing simulation – sending fake phishing e-mails to check how users react and educate them.
5. Rogue device simulations – leaving fake rogue devices, such as USB sticks or access points to check users' reactions.

[1] https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities
https://www.enisa.europa.eu/publications/info-notes/responsible-vulnerability-disclosure-and-response-matter
https://www.enisa.europa.eu/publications/vulnerability-disclosure
https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure
https://www.enisa.europa.eu/publications/info-notes/effective-patch-management

6. Quizzes with prizes.
7. Poster/video campaigns inside office building and facilities.
8. Direct training for management and key workers.

There are both, commercial and open-source tools that are available for simulations and training, as well as educational material. A good cyber security awareness plan should be supported by human resource departments and senior management.

Despite the quality of the education mentioned above, it may not be readily applicable to engineering and automation staff. Training for such employees should be planned, agreed and supported by grid operations management.

Cyber Security Measures

The following cyber security measures are the foundation of an efficient incident response process:

- **Asset Inventory** – It is crucial to know what devices exist in a network, what are their software versions (including latest security patches), latest configuration changes and how they communicate with other devices in the network or outside of it. This asset inventory can be done manually (which is error-prone, not scalable and can delay the detection of rogue devices significantly) or with the help of passive or semi-active network monitoring tools. Knowing the inventory of assets interacting with OT gives a more thorough preparation to deal with unfolding events. It is also essential to keep track of changes to the inventory with a change management process to ensure asset information is always up to date.

- **System Hardening** – Reduces the attack surface of an asset. This can be achieved by disabling and removing unnecessary services and features at network, operating system and embedded (RTUs, PLCs and IEDs) levels. The Center for Internet Security (CIS) benchmark provides an extensive list of materials that can be used to support system hardening[2].

- **Network Access Control (NAC)** – Access of new devices to a network should be controlled via pre-admission and post-admission policies, including policy checks and remediation of issues. There are open-source solutions to NAC, such as openNAC[3] and PacketFence[4] Providing secure methods for remote access when necessary and ensuring least privilege, role-based user access is also an essential part of access management. The above items essentially work together, since the asset inventory is needed to implement and keep track of network segmentation, which is enforced via network access control.

- **Network Segmentation –** Assets with similar security requirement levels or/and similar functional requirements can be grouped into zones based on their criticality/functionality or the consequences of an incident. Segmenting a network in this way can prevent devices from different zones communicating with each other, therefore reducing the possibility of an attacker pivoting from one segment to another (e.g. from the IT network to a PLC). Segmentation can be implemented using conduits that provide a secure path for information to flow between zones, such as firewalls, data diodes and VLANs[5].

[2] https://www.cisecurity.org/cis-benchmarks/
[3] http://www.opennac.org/
[4] https://packetfence.org/
[5] [Refer to IEC 62443]

- **Identity and Access Management (IAM) –** Manage access and consider authorisation and account management by defining roles and an appropriate set of access rights to carry out each role. Critical devices should authenticate to each other with the use of certificates for verification.

- **Application Whitelisting –** Maintain whitelists of authorised applications on critical systems and OT components. The use of whitelisting rather than blacklisting can improve the capacity to detect intrusions.

Human Resources, Organization and Procedures

Incident response, in general, requires a holistic attitude towards situation analysis and mitigation of hostile actions taken against industrial asset and critical targets. Threat analysis and case studies teach us how important it is to keep constant dialog and cooperation among IT and OT departments, cyber and physical security experts, market units and auditors. Therefore, to foster proactive early warning acknowledgement and a timely response to critical events, it is recommended to establish a permanent and multidisciplinary taskforce in the organization, which must be able to select the right mitigation strategy whenever needed, with the aim to minimize the impact on service continuity and on the business.

To achieve this objective, the taskforce should include:

- Business line operation experts knowing the consequences of system and/or communication channel shutdown

- IT/TLC experts knowing business continuity specifications (Recovery Point Objective, Recovery Time Objective) of the infrastructure and able to interact with providers and partners during major incidents

- Incident Response managers, committed to take decisions regarding the actions to be taken and monitor the thresholds (i.e. extension of the event, severity) in case of events in progress

- Communication experts that should establish the communication strategy for internal, external and institutional exchanges

- Computer forensic analysts that can understand attack schemes and malware behaviours to suggest possible mitigations

The taskforce should be organized in shifts and must be in touch with the crisis management team or the board of directors, in case the event escalates to a crisis. The organization should provide means and opportunities to keep the taskforce motivated and trained also promoting simulations.

Security Operations Centre (SOC)

Companies may establish an in-house SOC. The biggest challenge with this is to find and employ properly trained staff. In addition, 24/7 duties require more operators and better funding and can prove to be expensive. The advantages of establishing an in-house SOC include no sensitive data are transferred outside the company; the operators are available ad-hoc and on-site, and they have better understanding of the network and company business. As an alternative there are a lot of SOC offerings on the market that offer some form of outsourcing; these might be interesting for smaller utilities that do not have in-house capabilities. Another model is a hybrid SOC, wherein during business hours an in-house team operates and there is afterhours support from contractors. The following questions should be asked before establishing a SOC:

- What are the different models available, including their pros and cons?

- What should be in the contract for an outsourced SOC?
- How do you ensure the quality of an outsourced SOC?
- Gather experiences from EE-ISAC members on tailoring SOC capability to the OT environment.

EPRI recommends the Integrated Security Operations Centre (ISOC) model for holistic monitoring and effective situational awareness. An ISOC extends SOC responsibilities and capabilities by integrating the operational technology, physical security, and information technology domains into a central monitoring centre to improve visibility and situational awareness, coordinate incident response efforts among the domains, and optimize resources. Figure 4 depicts a high-level, notional architecture for an ISOC, in which data (such as logs, alerts/alarms, and raw device data) from business IT systems, OT environments (including substations and control centres), and physical security are collected in a centralized location.

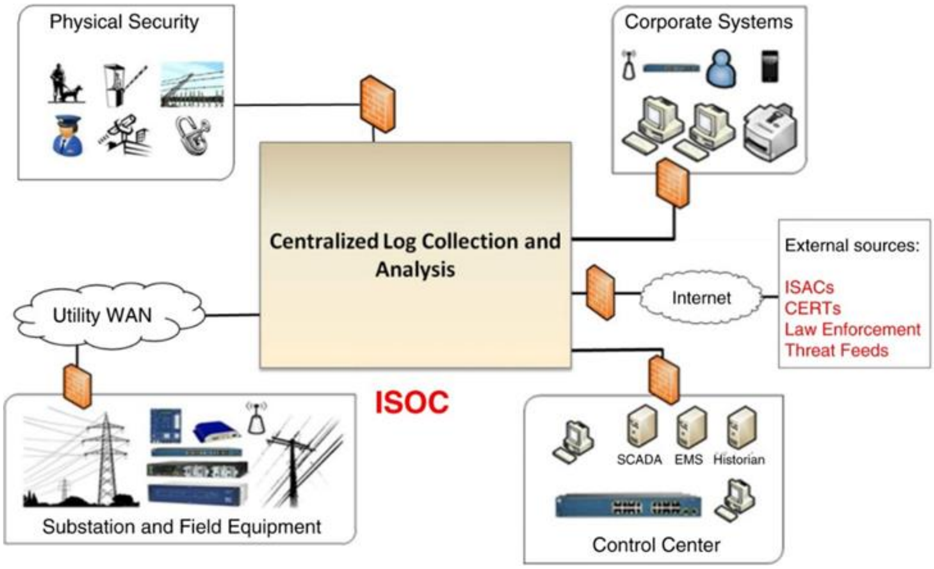

Figure 4 Integrated SOC [Ref EPRI]

Computer Security Incident Response Team

Similar to a SOC, a company may wish to establish a Computer Security Incident Response Team (CSIRT), either internal to the company or outsourced. Its functions are best described in Computer Security Incident Response Team Services Network, published by the Forum of Incident Response and Security Teams (FIRST)[6]. The difference between a SOC and CSIRT is that the latter operates on strategic and operational levels rather than the technical. It is focused mainly on threat analysis, impact of security incidents on the business, information sharing, cooperation and prevention. Additionally, whereas SOC staff consist of employees that are strictly assigned to this unit, a CSIRT may be an ad-hoc team that consists of employees from different units.

[6] https://www.first.org/

Law Enforcement and Incident Response

Most European Union member states introduced regulations that oblige critical infrastructure operators to include law enforcement in incident response processes. There is no single, universal rule at which phase and from which level this should happen – it differs from country to country. However, managers must be properly prepared for such situations. Moreover, usually there should be a single point of contact (SPOC) established.

Another important topic is cooperation with governmental bodies, whose requirements differ between countries. However, most energy sector companies are obliged to report incidents at certain level to a national agency.

Incident Response Plans and Procedures

Each organization should have well-established procedures for incident handling. It is very important for energy sector companies to include grid operations units in the process of creating such procedures. They must include such steps as gaining access to substations and other facilities and be compliant with continuity plans.

A good incident handling procedure should specify:

- Roles and responsibilities (examples are shown below)
- A triage process (summarized below)
- Involvement of external parties (i.e. SOC, computer forensics)
- Cooperation with partners and national agencies
- An authorization to perform incident handling tasks (i.e. disconnect a device or acquire data from disks)
- Continuity plans (i.e. how information about an incident should be handed to the next shift)
- Communication processes

Fast and effective incident response requires a clear understanding of roles and responsibilities for each stakeholder. Decision making processes during incidents must be very clear, especially where response actions may have safety or asset consequences or a financial impact.

Roles and Responsibilities

Looking broadly on the preparation of an incident response plan, the composition of a CSIRT can include (but is not limited to) the following roles and responsibilities:

- **CSIRT Manager** – responsible for organizing and controlling all the team's activities and objectives accomplishment.
- **Site Manager** – responsible for the organization's main operational processes with authority to decide and delegate authority (for example, interruption of processes).
- **Chief Information Officer** - responsible for the organization's information and IT processes with similar a role to the Site Manager in terms of authorities.
- **Network Administrator –** responsible for computer network operations within the organization.
- **System Administrator –** responsible for the operation of servers, clients and other respective systems in the organization.

- **Security Experts** – responsible for performing the technical part of the incident response.
- **Legal Expert** – consulting the CSIRT about compliance issues and helping to resolve conflicts with other parties.
- **Public Relation Specialist** – responsible for information dissemination and messaging to the media.

Ideally, response actions need to be planned out in advance, integrated with safety plans and tested, practising the response with internal and outsourced teams. It is essential to know and practise responsibilities in advance.

The levels of support required from key suppliers must also be agreed in advance, and the procedures defined for engaging that support. The escalation process to the crisis management team must be defined and communicated. Engaging all necessary aspects of the organisation, not just IT and OT.

Incident Handling Tiers and Triage

Usually incident handling is organized into three tiers that characterize the sophistication of the incident handling activities that are undertaken at each tier:

1. **Tier 1 – Basic Incident Handling:** initial triage, solving simple incidents, closing false positives, incident escalation;
2. **Tier 2 – Intermediate Incident Handling:** deeper investigation and mitigation; and
3. **Tier 3 – Advanced Incident Handling:** threat intelligence, prevention, reverse engineering, forensic, information sharing and analysis.

The higher the tier, typically more qualified staff is required. Moreover, in terms of operational availability, Tier 1 and 2 resources might be organised into shifts, while Tier 3 could work during office hours, with on-call duties. Depending on an organisation’s capabilities and requirements, different tiers might be provided in-house or outsourced. They could be organised as part of the organization’s SOC, CSIRT, and a Computer Emergency Response Team (CERT).

Security events should be analysed, either automatically using SIEM correlation rules (see below) or manually. Internal procedures should describe the criteria for classifying events as an incident. Having classified an event(s) as an incident, it must be categorized based on its severity level and type of incident. This process is called triage. Example severity levels include low, moderate, high, and critical. Meanwhile, types of incidents include denial of service, malicious code, unauthorized access, inappropriate usage, or multiple component (a combination of other categories). This categorization should define how the incident is handled with defined procedures.

Training and Exercises

An essential component of incident response preparedness is training and exercises. Exercising incident response can improve the reactive capabilities of a utility significantly. It is also essential that incident responders know and practise their responsibilities in advance and are familiar with escalation processes to engage all necessary aspects of the organisation and crisis management teams. Planning and exercising scenarios in advance will aid a more rapid response. As a general rule, companies should run exercises at least once a year.

When planning trainings and exercises, Table Top Exercises (TTX) and Live Fire Exercises (LFX) should be considered:

- **Table Top Exercises** involve not only cyber security teams, but also C-level management, public relations and grid operations personnel. Scenarios concentrate on cooperation, communication and checking procedures. Activities include computer incident response management, crisis management, communication with the public, cooperation with public administration and law enforcement units, and power grid operations.
- **Live Fire Exercises** are more technically-oriented training and involve computer security teams, network administrators and automation engineers. LFX should be conducted in the real-world or a simulated environment, which resembles a company's computer network. The main goal of this type of exercise is to test your team to determine how they cope in stressful conditions. An intensive session should include activities such as: penetration, social engineering, exploiting, computer forensic, manipulation over SCADA/DCS/PLC and recovery. Participants should not concentrate on system hardening – rather on response, mitigation and reporting. An organization can hire external experts to conduct such exercises or organise them inside the company. It is recommended that participants should be off-duty and fully available during the exercise.

There is a list of established training courses, which have proven to significantly improve participants reactive capabilities, in Appendix 2 – Training.

3. Detection and Analysis

Detection Sources and Tools

It is essential to deploy passive monitoring tools to detect anomalies, which could indicate a cyberattack, and anticipate the latest risks. Establishing a baseline of normal communications within OT allows new and different communications to be more easily detected. Many data sources from different security deployments offer a stack of alerts that need to be analysed to find critical threats and link information that belongs to the same threat or incident. This allows a context to be built from the data to aid decisions and prioritise actions. Alerts can be categorized based on their detection source, such as network- or host-based intrusion detection systems, human reports, and other logs. Below, we detail each of these types of tools.

Intrusion Detection Systems (IDS)

Monitoring and intrusion detection tools tend to focus on specific threat vectors and analysis approaches. Therefore, implementing several distinct monitoring and detection techniques can offer a broader coverage of the situation. A useful resource is ENISA’s guidance on dependencies on communication networks for ICS/SCADA systems, specifically section “3.3.2 Security groups and tools for SCADA systems.”[7]

Intrusion detection systems include signature-based approaches, which detect known threats that have an associated signature, and anomaly-based approaches, which can learn a baseline of network communications or host behaviour and detect deviations. Although anomaly-based approaches sound ideal, they also increase the possibility of false positives, i.e. raising an alert for something that is not a real malicious action.

Host or endpoint security solutions, in general, are not applicable to many OT devices (e.g. PLCs, RTUs, IEDs) because of issues such as constrained resources and the diversity of operating systems. These solutions are important for IT devices (e.g. workstations) but do not provide complete detection capabilities; therefore, OT environments require network monitoring solutions. OT-focused network monitoring solutions are usually fully passive (i.e. they do not inject any traffic in the network) in order to not disrupt critical processes. There are also newer solutions that are selectively active, i.e. they can send specific queries that are fine-tuned to certain OT devices, which allow the tools to obtain more information from the devices (such as specific firmware versions and SNMP information) without interfering with their normal behaviour.

Besides the previously mentioned divisions (i.e. signature- vs anomaly-based, host- vs network-based, and active vs passive), network-based IDS can also be divided into the type of information they analyse from network packets. In this context, flow analysis refers to analysing metadata such as which devices communicate with other devices, what is the duration and length of these communication sessions, which protocols they use and so on. Deep Packet Inspection (DPI), on the other hand, refers to analysing the full content of each packet, which requires being able to fully parse the protocols used by the communicating devices. In general, DPI provides much better information than flow analysis, but it requires very specialized tools for OT. Moreover, DPI is becoming increasingly challenging to realize as communication protocols are encrypted.

[7] https://www.enisa.europa.eu/publications/ics-scada-dependencies

Section “Appendix 1 – Open Source Tools” describes some open source network intrusion detection tools. A combination of both signature-based and anomaly-based network intrusion detection will detect known signatures, as well as protect against many zero-day vulnerabilities.

Human Resources

Well-prepared (trained) employees are one of the best and most cost-effective sources of true positive detections. Both engineers and office workers can easily distinguish between normal behaviour and an anomaly. However, an organisation should establish well-known communication channels, such as an emergency phone number and a ticketing system, enabling employees to readily report suspicious activity.

Logs

Logs are the most common source of information to support the detection of attacks. They can come from a variety of devices and systems: operating systems, network devices and authentication services, and are collected by log servers. The communication protocol, which is typically used for such collection, is syslog. Though, other protocols can be used as well. Usually, logs contain information such as source, timestamp, short description and severity. A big challenge with log collection is that they produce a lot of overhead data, including true negatives and false positives. Thus, logs need to be aggregated and correlated – this is usually done using a SIEM tool (see below).

Security Incident and Event Management (SIEM)

A SIEM system is a software intended to aggregate and analyse information from both endpoints and from network monitoring tools. There are different approaches to setting up such platforms for energy utilities: one is to have completely separated installations for IT and OT networks, the second is to have one instance. SIEMs may also be connected to physical security systems and warn, for example, about intrusions.

Appendix 1 – Open Source Tools lists some open-source SIEM options.

Security Orchestration, Analysis and Response (SOAR) Platform

A SOAR platform is a software solution for incident handlers, which supports incident handling and analysis processes. Important features of these platforms include the ability to create and manage playbooks – mappings of internal procedures onto actionable steps, e.g. initial triage and malware analysis – and information enrichment. Regarding the latter, a SOAR platform should be able to gather Indicators of Compromise (IOCs) from an incident and compare them with available sources, such as MISP (see below) or commercial feeds. An example open-source SOAR platform is The Hive[8], which supports these features.

Threat Intelligence

The goal of threat intelligence is to make information available to analysts that helps them in the mitigation of potential incidents. There are several levels of threat intelligence that vary in their complexity, ability to be shared and the comprehensiveness of the information. This is depicted very well in the pyramid of pain in threat intelligence[9], which separates the various types of intelligence available. While Tactics, Techniques and Procedures (TTPs) are the most abstract type of information available, they need the most additional effort to be applied to actual incidents. On the other hand, IP addresses and hash values can be easily shared and applied but reveal little about how an adversary behaves.

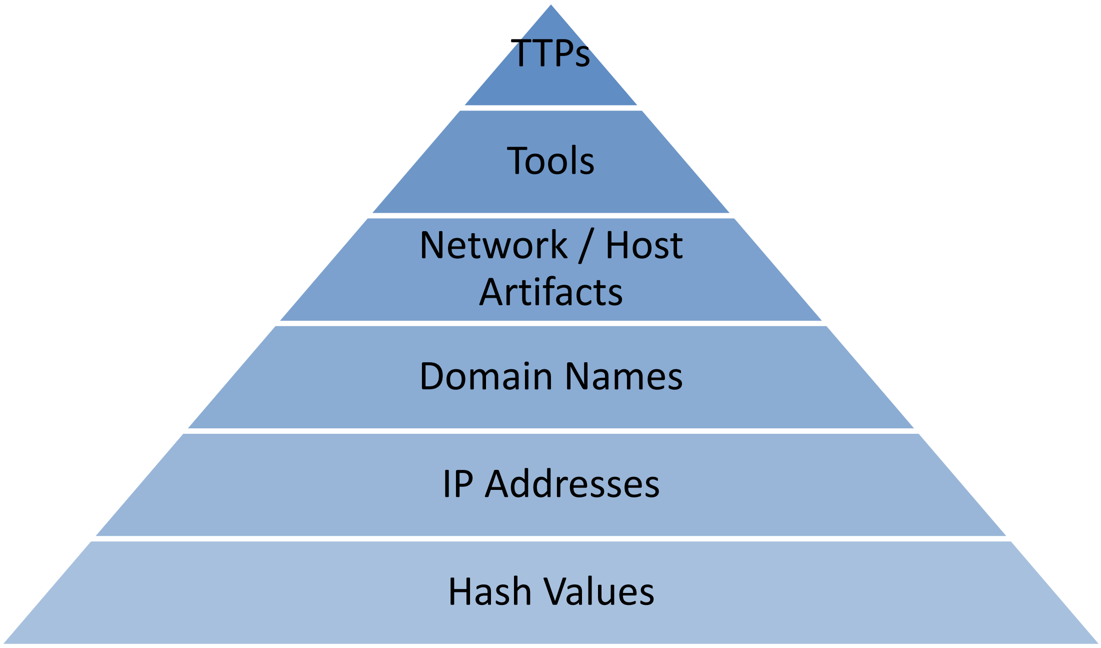

Figure 5: Pyramid of Pain in threat intelligence

To complement an effective incident response, the use of threat intelligence of every type is necessary, and the automation of its application is key for situational awareness and thus not only an effective, but a fast incident response.

The data available through threat intelligence can then be combined with the data available from the monitoring service for analysis and pattern identification. The quality

[8] https://thehive-project.org/

[9] http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

of the results of the analysis is, of course, dependant on the amount and quality of the data available. This leads directly to the point where sharing becomes a win-win-situation for every party involved. Whenever information about an attack is shared and that in a faster way than the attack is carried out, the defence of unaffected systems is greatly improved by the ability to identify formerly unknown threats. Since it is impossible for a participant in a threat intelligence exchange program to always evade an attack, the sharing becomes a security advantage.

Threat information can be sector specific, as much as the equipment used in the sector is specific to it. If sector specific equipment and protocols are common, there are surely threats that are targeting these as well, and a source sharing this tailored information is to be preferred over more general sources.

ENISA is responsible for developing an annual threat landscape in the context of the EE-ISAC on cyber security threats to the whole lifecycle of the power supply chain. This work aims to outline the main threats in the energy sector and depict the impact an incident can have on the energy power chain. This lays the ground for Information Sharing and Analysis Centres, such as the ICS-CERT and the EE-ISAC, in which sector relevant information is processed, analysed and shared to its members and participants.

EE-ISAC MISP

Sector-specific information sharing is a key objective for the EE-ISAC and to facilitate it on a technical level, an instance of the Malware Information Sharing Platform[10] (MISP) has been put into operation. MISP is an EU-supported open source project originating out of CIRCL, the Computer Incident Response Centre Luxembourg[11] and with more than 6.000 organisations running an instance of MISP, it became the de-facto standard for automated threat intelligence exchange.

The EE-ISAC is running its own instance of the MISP to bring together sources of threat intelligence information that is tailored to the energy sector. The functionality is provided to the members of the EE-ISAC who can use the available information and contribute information they consider relevant. The aim is to enrich the intelligence community with threat trends and attack patterns that could affect energy companies.

The EE-ISAC is vetting and integrating different sources of information to enable the distribution of threat intelligence relevant to the energy sector. Their MISP instance connects members and partners to protected information.

There are two main types of information that is available through the EE-ISAC instance:

1. Vetted information that has a high certainty of correctness
2. Trigger information that has a higher level of uncertainty but can be used to trigger an investigation

While a positive identification of a high-certainty threat intelligence IOC in a network should initiate an investigation, the lower certainty information is used for checks if certain undesired activities that could lead to an investigation took place, e.g. connections to TOR nodes from restricted networks.

The provision of comprehensive information is accomplished by the connections of the EE-ISAC instance with other, publicly and privately-run, instances of various

[10] MISP project: https://www.misp-project.org/
[11] CIRCL: https://www.circl.org/

organisations, e.g. like the sharing that is established between the private sector, the CERT community and the NCIRC, as depicted in Figure 3. The information that is shared is considered private at the beginning and must be cleared for usage within the group and external groups before these actions can take place.

The sharing of information between various and independently run instances of MISP is the intended goal of the platform and on par with the mission statement of the EE-ISAC.

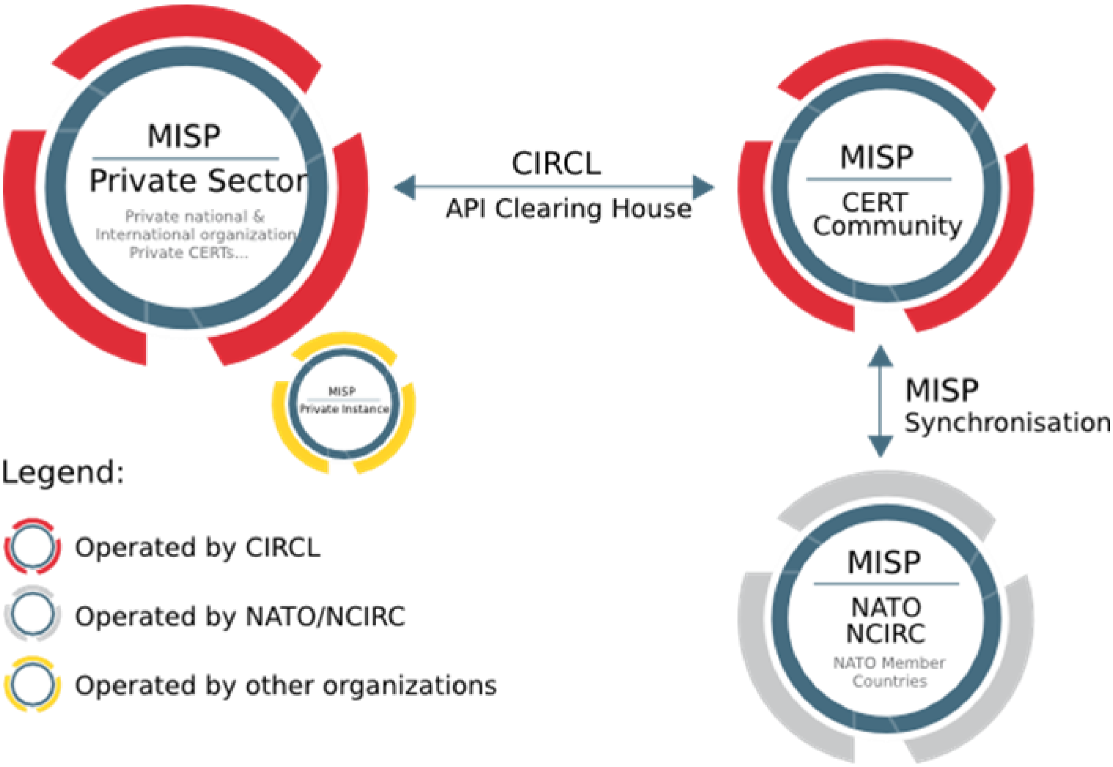

Figure 6: MISP sharing model. Source: MISP platform, https://www.misp-project.org/

Besides this core functionality, certain additional functions are provided in general and are subsequently cleared for usage within the EE-ISAC. Most notably are the API access that allows more flexibility for the data usage of its members and the extensibility via MISP-modules. Members can access the information either via the API or directly via the dashboard. If an integration into their own MISP instance takes place, the built-in features can also be used locally, which is facilitated by the exchange format and the object templates.

4. Containment, Eradication and Recovery

This phase involves containing an incident and restoring affected assets, data and processes. Pre-planning is essential to facilitate decisive actions during this phase. Procedures for containing different types of incident need to be in place.

Containment

After the incident response team has managed to gain a first understanding of the incident, actions need to be taken to instantly ensure that no further damage is being created by the adversary.

This can be achieved by

- Blocking communications to malicious IPs and domain lists and checking the SIEM for previous communications with these sites or IP addresses associated with the spread of malware.
- Blocking direct connections with suppliers may also be necessary until risk of malware propagation is reduced.
- Disconnecting VPN accesses and blocking access from IT to OT can be used as a first response to prevent spreading of malware.
- Disconnecting segments, e.g. from the DSO to the internet, Enterprise network to the OT segments, or central SCADA systems to the substations.

Cyber crisis simulations have shown, that most DSOs make use of the latter and terminate connections from IT and OT (see innogy's CyberRange-e). Whilst this is one of the most effective actions to defend against a remote attacker, it needs a diligent preparation to ensure staff is aware of the risk that comes with this measure and is aware of the acceptable downtime.

- Connections from IT to OT – what communication channels exist? how long can the DSO work without them? what is the maximum downtime? Who needs to be informed when taking the connection point down?
- Connections from the central SCADA system to the substations – How are substations being controlled? Do I have enough engineers to manually operate substations? What are the priority substations? What drivers exist regarding the acceptable downtime of the central SCADA systems (e.g. whether, road-works).

Eradication

At this phase, an impacted system should be cleaned up and secured to allow next steps to happen. If the original problem was not resolved or the eradication phase was performed partially, an incident could repeat again in a short time.

For critical systems, eradication should in general occur via a fresh build or via restores from trustable media. It should be put into consideration when eradicating central SCADA systems or other highly critical systems, to also replace hardware by new, uncompromised hardware.

Recovery

The main task during this phase is bringing the environment back online using a well-documented process for restoring from trustworthy ‘golden image’ backups. One of the challenges in this step is regularly testing this ability and the backups themselves. Stopping a production line for comprehensive drills is difficult, while maintaining a replica environment for testing is prohibitively expensive for most. Technologies like virtualisation can provide the required flexibility and assurance.

Risks need to be managed to make appropriate decisions during the recovery process. Knowledge of different attack methods can allow the best containment actions to be followed. Rapid containment may be necessary before an attacker can compromise other systems.

It is essential to consider the potential impact of any system recovery actions. For example, careful coordination with operations may be required especially where there is a potential safety or reliability impact from incident response actions. It is important to involve operations, safety and leadership teams in the decision process during incident response to ensure operational impact is understood.

Cyber Insurance

A cyber insurance policy may include assistance during a cyber incident. However, the levels of cover available may include only a reduced set of risks and limited coverage of the OT space.

Awareness of the risks and the potential for financial harm that a cyber security incident can cause has led to a sharp rise in demand for and provision of specialist cyber security insurance policies. Typically, these are designed to cover costs for responding to and investigating attacks, as well as damages incurred. Many policies are currently untested, however, and areas of coverage may be unclear.

5. Post-Incident Activity

Incident response is a continuous and dynamic process. Organizations need to adapt to changes in situation awareness and make sense of the latest threat information to decide and priorities actions.

Analysing and learning from closed incidents is vital to prevent repeated events and identify additional prevention actions. Closed incidents are a valuable source for organisational learning on how to improve the incident response process. Potential for improvements may exist in each process stage. As such, post-incident activities tightly relate to the continuous improvement process (CIP) of an organisation's security management capabilities required by established information security management standards including ISO/IEC 27001:2017 (see chapter 10.2 on continuous improvement). Planning their post-incident activities, organisations shall consider creating incident reports, structuring "lessons learned" from incidents, notifying internal and external parties and sharing information on incidents.

Creating incident reports

The incident report is the final report summarizing all observations, activities and results relating to the incident. The report is created upon the closing of the security incident. Incident reports are the for drawing conclusions and learning from past incidents. The incident manager composes the incident report from the documentation that has been collected during the treatment of the incident. The incident report consolidates information documented in the SOAR (Security Orchestration, Automation and Response) tool, in ticketing systems, in analysis reports and from other sources. Depending on the classification of the incidents it is recommended to distinguish ad-hoc incident reports and periodic incident reports:

- Ad-hoc incident reports: For major security incidents an own incident report dedicated to the particular incident is created.
- Periodic incident reports: Minor security incidents are reported as part of periodic incident reports (e.g., monthly or quarterly). Standard incidents may be aggregated depending on their criticality.

The incident report shall contain

- what happened,
- a timeline of events,
- classification and prioritisation of the incident,
- a list of affected assets in the OT and IT environments,
- impact of the incident on the organisation (occurred damage, etc.),
- steps for containment, analysis and eradication taken as well as immediate and interim measures implemented,
- the results of a root cause analysis of why the incident could have happened,
- and, for intentional incidents, available investigation results on the threat actor as well as threat actor success.

Structuring lessons learned

For enabling lessons learned from security incidents that have happened in the past organisations are recommended to give this important activity in the post-incident phase a structure. Lessons learned sessions are a follow-up to closed incidents to

- learn and improve the incident response process itself,
- identify control gaps and derive security measures to prevent similar incidents from happening in the future.

The following roles shall be considered to participate in lessons learned sessions:

- Incident manager
- Involved incident-response team
- Responsible information security manager for the affected business processes
- Business process managers or product managers of the business processes or products affected by the incident
- OT and IT service managers of the services affected by the incident
- Asset custodians of the assets affected by the incident

Particularly for major incidents, lessons-learned sessions shall be held as quickly as possible after closing the incidents to leverage the full experience of involved staff. OT-operations staff, though, is often busy and involved in multiple incidents at a time so that ad-hoc lessons learned sessions can be difficult to schedule in a timely manner. Pre-scheduled, periodic lessons learned sessions can avoid time-lag in the post-incident phase and the drain of knowledge connected to time delays.

. For example, learnings derived could be improving the detection stage to trigger preventive steps to be taken where these are compatible with OT processes. Also, correlating actual incidents to incident detection indicators may improve future analysis. What is more, feedback from lessons learned may help improving the speed of detection, thus reducing the amount of containment necessary.

Notifying internal and external parties

After closing the incident additional internal and external parties may need to be approached. Internally, it has to be ensured that the competent security officer is provided with an overview of the happened incidents. Closed incidents need to be well-captured within the organisation's information security management system (ISMS).

It is advisable to communicate the incident report to the business process owners affected by the incident as well as to the competent senior management of the affected business.

For security incidents with intent, management is in authority to decide whether an incident shall be prosecuted by civil or criminal law. For legal prosecution, most likely an additional in-depth forensic investigation preserving the chain of custody of evidence will be required. It is advisable to maintain a framework contract with a forensic services provider. Also, the legal department may need to be involved for preparing legal action. Moreover, if employees were affected by the incident, the internal communications department need to meaningfully and understandably communicate about the incident. Likewise, the external communications department will have to continue communication with the public in the post-incident phase for incidents that were affecting citizens, end consumers or had media coverage. For these departments not directly involved in incident treatment, the incident report is an important source for understanding what happened during incident response activities.

Lawmakers around the world are waking up to the danger posed by poor cyber security in ICS for energy, public health and safety. As part of the NIS EU Directive, Operators of Essential Services (OES) are obliged to report incidents that could affect essential services to competent authorities within defined thresholds. The NIS directive tool of the European Union Agency for Cybersecurity (ENISA) (https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool) supports organisations with identifying responsible authorities. If personal data has been breached by the incident, also the competent data protection authority (DPA) maybe needs to be provided with information.

Moreover, also the relevant sector-specific and national Computer Emergency Response Teams (CERTs) can be involved in post incident activities, particularly if it has been already involved during the incident response activities. In the post incident phase, CERTs can contribute information and expertise for creating the incident report, serve as a single point of contact (SPOC) for notifying authorities and communicating on incidents with national or international outreach as well as support the coordination of measures on an industry and national level.

Sharing information on incidents

Finally, reciprocal sharing of information on incidents with peer organisations can help preventing the same incident from happening again. Information Sharing and Analysis Centers (ISACs) provide an institutionalized frame for sharing information in a network of trust. Organisation shall share information on incidents with their ISAC. Among other information, particularly the following information on incidents may be useful for fellow ISAC members:

- Indicators of Compromise (IOCs) such as attacker source IP addresses, URLs, signatures and checksums
- Exploited vulnerabilities and to which technologies they relate
- Experience on executing the steps for containment, analysis and eradication suggested by vendors and service providers

6. Incident example with best practices

In this chapter, we look at an example use case to show specific measures within the incident response process to handle malware infections. Many of the described actions will vary depending on the specific type of malware and may require other measures for each incident response phase. Within the PDCA cycle, you can use this use case approach to improve the detection and incident response capabilities of your team.

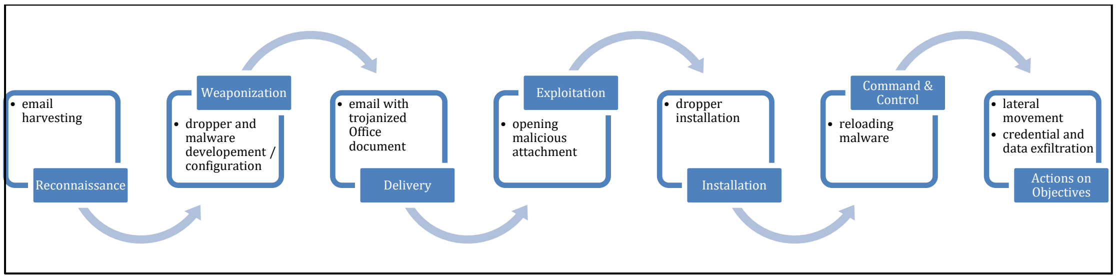

Figure 7 Example of Malware Infection Campaign based on the Cyber Kill Chain of the Emotet malware

Preparation: Train cyber security awareness, so employees will be able to identify potential malicious mails, files and system behaviour and know how they have to react (e.g. not clicking links or opening attachments and informing the security team about suspicious mails). Harden your environment to keep the attack surface for infections as small as possible (e.g. disable macros with Group Policy Objects on Windows systems).

Detection: Use IOCs to enable your tools (e.g. intrusion detections systems, network monitoring tools) to identify malicious files, new or manipulated registry keys and API function calls.

Analysis: Depending on your resources and expertise, you can do a basic analysis (new or altered files and processes on systems) or get third party help for malware analysis (disassembling, reverse engineering). The most important task at this stage is to identify the initial attack vector to be able to prevent reinfection. Use the analysis information for further detection and containment of infected systems.

Containment: Concerning containment there is the crucial decisions to make between ‘watch and learn’ vs ‘disconnect’. If there are indications for a targeted attack, then watch and learn will be the better approach. In case of automated malware, disconnection systems or subnetworks may prevent further damage.

Eradication: Delete the mails on the mail server. Because malware becomes increasingly modular and samples within a malware family may vary in used infection vectors and spreading techniques, a complete reinstallation of systems is the safest eradication measure.

Recovery: Reinstall and restore systems from backups.

Investigation: Identify the root cause of the infection and come up with countermeasures.

Post-incident activities: Document lessons learned and incorporate new IOCs and response capabilities into your incident response process.

Conclusion

This paper highlights some essential activities for adequate preparation and response to cyber security incidents. Knowing the potential attack surface and the likely impact of incidents can indicate the required preventative activities. An understanding of the latest threat landscape and deployment of detection capability on networks and devices is essential to keep on top of preparations. Integrating several different monitoring techniques can provide more thorough situation awareness.

The full response and recovery process requires detailed coordination and careful management, especially for an operational environment where safety and reliability conditions need to be assured. Agreements with suppliers and escalation procedures must also be ready to bring the required support for incidents.

Where possible, collaborations to share threat information and response experience can help to improve preparations by developing a wider perspective on the issues. EE-ISAC aims to improve information sharing across the sector and give outlooks on the threat trends and attack schemes affecting the energy sector.

By involving multiple industry partners, EE-ISAC aims to achieve a combined effort and consistent support for the sector, particularly for smaller organizations with fewer resources for cyber security.

Appendix 1 – Open Source Tools

Preparation

OpenVAS	A fork of original Nessus project, designed for vulnerability identification and management
Nikto	A web server vulnerability scanner

Table 1 Open Source vulnerability assessment tools

Detection

Snort	• Monitors network traffic and connection requests. • Identifies malformed packets before they reach a host. • Analyses specifics through filtering or pattern matching. • Rules that define what is detected can be customised and need regular updates for new threats.
Suricata	• Detection for the application layer • Detects threats that are split over several packets. • Monitors protocols at the lower layers of the OSI model. • Detects intrusion attempts hidden in otherwise normal requests. • Distributed architecture to spread its load over several processors.
Zeek	(Formerly Bro) another alternative for network intrusion detection. Overview of differences between Snort, Suricata and Zeek tools: https://bricata.com/blog/snort-suricata-bro-ids/

Table 2 Open Source Network Intrusion Detection tools

ELK	Three layer functionality: 1. Elasticsearch - storage engine 2. Logstash - filters, processes and correlates log data 3. Kibana - visualisation capability. Accepts feeds from OSSEC & Snort. Logz.io – a cloud version of ELK
OSSIM	Includes detection and correlation capabilities. Assess vulnerabilities – correlates intrusion detection logs with vulnerability scanning results.

Table 3 Open Source SIEM tools

OSSEC	Provides host intrusion detection and is installed directly onto the server or device it is protecting

Table 4 Open Source Host Intrusion Detection tools

SecurityOnion (https://securityonion.net/) is an open-source distribution that contains most of the above tools (or similar alternatives) and can be used (almost) out-of-the-box.

Analysis

TheHive	A Security Incident Response platform aimed at collaboration between security teams, building tasks with metrics, triage and investigation. Works best in pair with Cortex or MISP.

Table 5 Open Source SOAR tools

Eradication

SIFT	A group of open-source tools for digital forensics
Volatility	A tool for memory forensics

Table 6 Open Source forensic tools

Appendix 2 – Training

EPRI Cyber Security IR and Recovery Tabletop Exercise

It is critical for utilities to continually evaluate and exercise their capabilities to effectively respond to events in their operational environments to determine if their processes satisfy operational requirements. With the increased inclusion of and dependence on processor-based operational and communications infrastructure, the potential for operational events to occur or be influenced by malevolent cyber agents also increases.

A tabletop exercise (TTX) is a facilitated, scenario-based discussion that tests an organization’s ability to respond to a potential scenario in a practice environment. It enables participants to review and discuss in detail the actions they would take to validate operational processes, procedures, and reporting structures. The key outputs of the TTX are an identification of people, process, or technology gaps and recommendations for addressing them.

This project provides the ability for the funding utilities to exercise their Incident Response and Recovery plan in a workshop environment that is facilitated by an independent party. The exercise or test of the plan is a requirement of the North American Electric Reliability Corporation critical infrastructure protection regulations CIP-008 and CIP-009. In addition to support for the utility’s regulatory compliance, the project will identify ways the utility can refine the processes and procedures that personnel in different roles within the organization must follow in a cyber event.

The table top exercise will also aid the utility in validating the roles, responsibilities, and authorities for cyber incident response and recovery, including:

- Who is the primary authority to orchestrate action in the response and recovery phases.
- Who performs cyber-related analysis of the operational environment?
- Who are the stakeholders?
- How is information shared?

How is mandatory reporting accomplished?

innogy’s CyberRange-e

The central training objective of the CyberRange-e is the active transfer of know-how and techniques for the detection and defence of cyber-attacks. Through your participation in the CyberRange-e, trainees will be able to assess the maturity level of their Incident Response capabilities with regards to operational and security Trainees learn to react adequately to a potential threat and initiate the escalation process in good time in case of an emergency.

innogy’s CyberRange-e is an arena, where realistic cyber war-gaming scenarios are trained for electric grid operators and utilities in general. The arena comprises all technology being used by electric utilities, including SCADA systems, substations, etc. Next to the War-Gaming part, experts give classes to explain current attack scenarios and vectors that pose threats to Utilities.

ENISA Training Materials

ENISA’s Cyber security Trainings provide essential material to develop skills in the Incident Responders community and in the field of Operational Security. The ENISA CSIRT training material covers four main areas: Technical, Operational, Setting up a CSIRT and Legal and Cooperation.

Information regarding the trainings offered can be found at:

https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/training-courses

During the Autumn2019 plenary, ENISA offered a training on setting up security monitoring for an ICS environment. The training was for EE-ISAC members only but its material can be found at:

https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-training-course-material-on-network-forensics-for-cybersecurity-specialists

https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf

Acknowledgements and Contact Details

This whitepaper has been produced, with the support of EE-ISAC members and partners:

EE-ISAC
Dr Paul Smith
AIT Austrian Institute of Technology
Paul.Smith@ait.ac.at

EE-ISAC
Christina Skouloudi
Konstantinos Moulinos
ENISA
Konstantinos.Moulinos@enisa.europa.eu
Christina.Skouloudi@enisa.europa.eu

EE-ISAC
Massimo Rocca
ENEL
massimo.rocca@enel.com

EE-ISAC
Jalal Bouhdada
Applied Risk
Jalal@applied-risk.com

EE-ISAC
Aleksander Wiśniewski
PSE
Aleksander.wisniewski@pse.pl

EE-ISAC
Michael Knuchel
Swiss Grid
Michael.Knuchel@swissgrid.ch

EE-ISAC
Ivan Dragnev
Electric Power Research Institute
Idragnev@epri.com

EE-ISAC
Tania Wallis
University of Strathclyde
Tania.Wallis@strath.ac.uk

EE-ISAC
Alexander Harsch
Marius Staggenborg
Innogy
alexander.harsch@innogy.com
marius.staggenborg@innogy.com

EE-ISAC
Daniel dos Santos
Forescout
daniel.dossantos@forescout.com

EE-ISAC
Marcel Kulicke
Siemens
marcel.kulicke@siemens.com

EE-ISAC
Alexander Novotny
EVN
alexander.novotny@evn.at

EE-ISAC
Dmytro Cherkashyn
Brandenburg University
d.cherkashyn@uniss.org

Andreas Seiler
LEW
andreas.seiler@lew.de