A blueprint and proof-of-concept for a national cyber security sensor network[1]

Florian Skopik and **Stefan Filip**
AIT Austrian Institute of Technology. Austria

ABSTRACT

The timely exchange of information on new threats and vulnerabilities has become a cornerstone of effective cyber defence in recent years. Especially national authorities increasingly assume their role as information brokers through national cyber security centres and distribute warnings on new attack vectors and vital recommendations on how to mitigate them. Although many of these initiatives are effective to some degree, they also suffer from severe limitations. Many steps in the exchange process require extensive human involvement to manually review, vet, enrich, analyse and distribute security information. Some countries have therefore started to adopt distributed cyber security sensor networks to enable the automatic collection, analysis and preparation of security data and thus effectively overcome limiting scalability factors. The basic idea of IoC-centric cyber security sensor networks is that the national authorities distribute Indicators of Compromise (IoCs) to organizations and receive sightings in return. This effectively helps them to estimate the spreading of malware, anticipate further trends of spreading and derive vital findings for decision makers. While this application case seems quite simple, there are some tough questions to be answered in advance, which steer the further design decisions: How much can the monitored organization be trusted to be a partner in the search for malware? How much control of the scanning process should be delegated to the organization? What is the right level of search depth? How to deal with confidential indicators? What can be derived from encrypted traffic? How are new indicators distributed,

[1] This paper is an extended version of (Skopik & Filip, 2019).

Published online: 2nd December 2019

prioritized, and scan targets selected in a scalable manner? What is a good strategy to re-schedule scans to derive meaningful data on trends, such as rate of spreading? This paper suggests a blueprint for a sensor network and raises related questions, outlines design principles, and discusses lessons learned from small-scale pilots.

Keywords: *cyber security sensor networks, indicator of compromise, indicator distribution, design principles, proof-of-concept, national cyber security*

1 INTRODUCTION

Situational awareness is a cornerstone of every successful defence strategy (Franke & Brynielsson, 2014). Not knowing what is going on can be lethal. That’s not only a well-known wisdom, it’s certainly also true for the cyber space. Dedicated authorities in the form of cyber security centres, ISACs and (sector-specific) CERTs/CSIRTs create cyber common operational pictures (CCOPs) (Pahi et al., 2017) on a continuous basis to support decision makers with reliable information. The faster such CCOPs can be created and the more accurate they are, the better is the support of decision making. The timely notification of new malware waves, widely distributed vulnerabilities, and critical attack trends can be a game changer for the defenders.

In this work we introduce a small-scale demonstrator of a cyber security sensor network (CSSN). Our model employs the well-proven Malware Information Sharing Platform (MISP) (Wagner et al., 2016) to host and manage indicators of compromise (IoCs), and which allows sensor network nodes (SNNs), located within organizational networks, to access its database and download new IoCs. Each SNN forwards scanning tasks with encapsulated IoCs to its connected sensors, distributed within its associated network infrastructures (typically critical infrastructure providers). These sensors look up if said indicators are present on their monitored devices and report sightings back to the SNN, which aggregates them and pushes them back to the MISP instance. In a real application case, a national authority or sector-CERT operates this MISP server and create new IoC entries in a MISP feed. Then the synchronisation process with the SNNs is automatically kicked off, and eventually within a couple of minutes first reports on sightings (if the IoC can be validated instantaneously) can be expected to be reported back.

While this application case seems quite simple, there are numerous tough questions to be answered in advance, which steer the design and deployment of a cyber security sensor network. Some of these questions are centred on (i) its governance model, e.g., how much the monitored organization can be trusted as a partner or how much control of the scanning process should be delegated to the organization; (ii) its operational mode, e.g., how new indicators are distributed, prioritized, and scan targets selected in a scalable manner or what a reliable strategy is to re-schedule scans to derive meaningful data on trends; and (iii) implementation details, e.g., how to ensure the confidentiality of secret indicators, or the treatment of encrypted traffic.

We introduce a blueprint of a cyber security sensor network (CSSN) system, which comprises a MISP server, numerous SNNs and associated sensors. In this context, the contributions of this extended paper of (Skopik & Filip, 2019) are as follows:

- We discuss the stakeholder structure, actor roles and responsibilities to run the CSSN and take a look into the different tasks of national authorities, sector-CERTs, and industry organizations.
- We investigate in detail the vital processes to set up and operate a national cyber security sensor network.
- We provide an overview of sensor technologies capable of verifying indicators of different classes.
- We introduce shortly the design of our proof-of-concept and discuss some implementation aspect.
- We review lessons learned from a pilot and derive common design patterns and principles for cyber security sensor networks.

The remainder of the paper is organized as follows. Section 2 provides an overview of related work. Then, Sect. 3 elaborates in detail on the different stakeholders and their roles and responsibilities to run an IoC-based sensor network. Section 4 outlines the operational processes along an illustrative scenario. Some insights on indicator types are given in Sect. 5 while Sect. 6 shows briefly the design of a Proof-of-Concept, which can act as a blueprint for a scalable implementation. Instead of evaluating the actual PoC, we discuss the rationale behind the design and actual design patterns of cyber security sensor networks in Sect. 7. Finally, Sect. 8 concludes the paper.

2 BACKGROUND AND RELATED WORK

Indicators of compromise are a means to validate the exploitation of a vulnerability (Rid et al., 2015). They are used to look for traces that a system has been hacked, modified or exploited in some malicious way.

Therefore, vendors of malware scanning solutions distribute IoCs to their deployments so that customers can automatically verify infections. Eventually, this makes malware scanners the simplest form of sensor nodes which are supplied with new signatures on a regular basis. Signatures to identify malicious domains and IP addresses may also be developed by analysing DNS traffic (Passive DNS). These types of sensors are de-facto state of the art in more mature organizations and can be connected to security information and event management (SIEM) solutions (Blask et al., 2010) to evaluate their results and get an overview of the current threat situation. However, this knowledge resides mostly within organizations only and is just useful to them since only they know their specific processes and are capable of interpreting the results correctly.

National authorities may receive manual reports from organizations which may be based on automatically collected data. This reporting should tremendously increase the awareness of national cyber security centres and CERTs/CSIRTs as intended by the EU’s NIS directive (European Commission, 2016), US CISA (US Congress, 2015). Additionally, information sharing across organizations (Skopik et al., 2016) takes mostly place within industry sectors, which run similar services deployed on similar technologies, and thus, fighting with the same security issues. However, this information sharing processes are mostly initiated on demand and performed manually instead of automatically; e.g., manual exchange of indicators in MISP (Wagner et al., 2016). What is missing, is a means for a near real-time evaluation of the current situation in case of raging malware or serious and widely distributed vulnerabilities. Getting to know, who is affected and how serious the problem is, requires tremendous human effort. So, an automatic evaluation and forwarding would be desirable for the national authorities and considerably relax the situation in the beginning of a new attack wave. Cyber security sensor networks, as proposed by several national cyber security strategies (Luiijf et al., 2013) could be of great help, and some real-world examples are already deployed, e.g., in France, Finland (Rantapelkonen et al., 2013) and Switzerland (Cavelty, 2014) for exactly that purpose.

Eventually, collecting information about cyber-attacks, incidents and threats in a timely manner is essential to gather cyber situational awareness (Franke & Brynielsson, 2014), and a prerequisite of justified decision making (Stotz & Sudit, 2017).

3 ROLES, RESPONSIBILITIES AND INTERACTIONS

The envisioned cyber security sensor network (CSSN) comprises numerous types of stakeholders with individual roles and pre-modelled interaction patterns.

3.1 Overview of the Stakeholders of the Sensor Network

Figure 1 shows the stakeholder structure to support the information sharing process between organizations, sector-CERTs/CSIRTS and national authorities. The process starts at the top, where a national cyber security centre (CSC) maintains cyber situational awareness for high-level decision making (Franke & Brynielsson, 2014). To fulfil this task the CSC gains access to various non-public threat information sources, such as confidential repositories and lists from secret services and law enforcement. Carefully selected subsets of these threat information are then forwarded, preferably as indicators of compromise (IoCs) (Obrst et al., 2012). to the sector-CERTs, where they feed a MISP server (Wagner et al., 2016) with these (partly confidential) information. The sector-CERTs may additionally subscribe to various other useful public sources (e.g., vendor lists and the like).

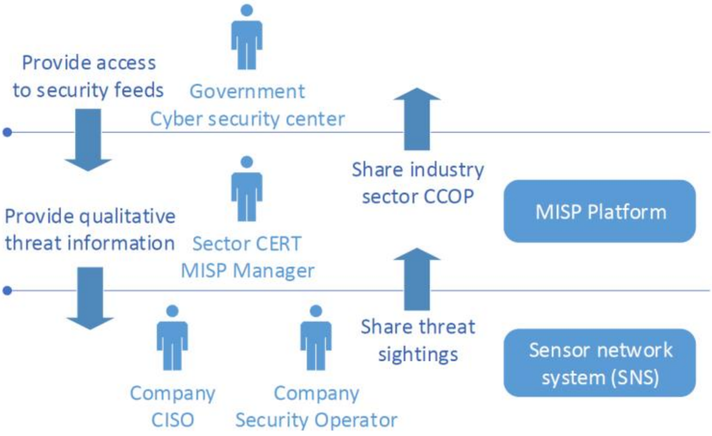
Provide access to security feeds
Government Cyber security center
Share industry sector CCOP
MISP Platform
Provide qualitative threat information
Sector CERT MISP Manager
Share threat sightings
Sensor network system (SNS)
Company CISO
Company Security Operator

Figure 1. CSSN stakeholders and their interactions.

This preselection process of relevant threat information sources reduces the work for the individual organizations and ensures the delivery of high-quality information shaped to the needs of an industrial sector (i.e., fitting to the commonly used assets in a certain domain).

The preselected events are then consumed by the sensor network nodes (SNNs), distributed throughout the organizations. An SNN searches for the received IoCs in its associated network and reports found sightings back to the sector-CERT's MISP server. The CERT aggregates received feedback on a continuous basis and creates common cyber operational pictures (CCOPs) (Pahi et al., 2017) – some of them for specific industry sectors. Expert circles and national decision makers use these CCOPs as the basis to assess the overall cyber security situation within an industry sector. This is an essential prerequisite to take timely counteractions in case of large-scale coordinated cyber attacks.

3.2 The governmental Cyber Security Center

A cyber security center (CSC) is a governmental institution which has the responsibility to periodically assess the overall cyber security situation of critical industry sectors (European Commission, 2016). For that purpose, the CSC collects information about the security status of critical infrastructures to gain knowledge whether an infrastructure is the victim of any serious attack. The distribution of IoCs to organizations and their validation, i.e., the discovery of IoCs in distributed networks, is an essential tool to assess the current situation and anticipate further trends. The CSC therefore asks specific sector-CERTs for support to send them CCOPs for their respective sectors and, eventually, generates an overall picture across all sectors.

3.3 Sector-CERTs

A sector-CERT is an independent organization of information technology specialists that advises in case of cyber security incidents in their industry sector. The sector-CERT collects information about recent cyber attacks and provides general recommendations, as well as advice to individual organizations, to help fend off attacks. A popular method for sharing threat information is a mailing list which is run by a CERT, but in order to collect large amounts of specific information ("IoC sighting") in very short time-frames (i.e., hours), an automated threat sharing mechanism offers numerous advantages. That is why the sector-CERT operates an automated threat sharing service, like a MISP server.

3.4 Organizations

An important stakeholder within each organization is the security operator (and the whole IT team respectively) who keeps (in accordance with the CISO) the organization's infrastructure secure. Note, this abstract role resides at a lower, more technical, level within the organization.

4 OPERATIONAL PROCESSES

The following scenario aims to provide a consistent application context of a national cyber security sensor network and gives insights into the threat information sharing processes. Within this scenario there are three major stakeholders (government, CERTs, organizations) which operate at three different levels. The stakeholders and their exemplary organizations are:

- The Cyber security center (CSC)
- The GreenPower GmbH (GPC)
- The Austrian Energy CERT (AEC)

The Cyber Security Center: In this scenario the government is worried about cyber attacks against critical infrastructures and establishes a Cyber security center, CSC. The *CSC* has the responsibility to relay on valuable information between the stakeholders. Therefore, it forwards valuable threat information to the sector CERTs and collects summary reports of the organizations' security status from them in return. The CSC then uses the collected reports to create a CCOP which can be accessed at any time by the government. In order to provide threat information to the CERTs, the CSC has access to international information sources from other countries and multiple threat information vendors.

The Austrian Energy CERT: In this example the sector CERT for energy, the Austrian Energy CERT, AEC is responsible to increase the cooperation between companies in the energy domain. The fundamental idea of the AEC is to strengthen the security competence in the energy sector and act as a neutral entity which defines general communication conditions between all organizations. Moreover, the AEC collects threat indicators, threat sightings and individual security reports and provides a summary report of the security status in the energy sector to the CSC. To perform this task the AEC operates a MISP service which helps to share and collect the mentioned information. The following list describes the relevant components operated by the sector CERT.

- *MISP service* - The Malware Information Sharing Platform (MISP) (Wagner et al., 2016) is a threat intelligence platform for sharing, storing and correlating indicators of compromise and sightings. The AEC accesses the stored data and uses it to derive CCOPs. In addition, the AEC provides access to other partners via the built-in API to share information.
- *Sensor network system* - From the AEC's point of view, the Sensor network System (SNS) is a logical combination of multiple sensor network nodes (SNNs). The AEC uses the SNS to collect threat sightings from partners and to evaluate the quality of IoCs.

The company GreenPower GmbH (GPC): GPC is a small energy producing company in the energy supply sector and has problems with recent cyber attacks against their enterprise infrastructure. These recent attacks were targeted attacks against hardware and software which is used especially in the energy supply industry sector. Other companies in this sector are affected as well, but were able to enforce countermeasures in time, due to their collaboration with the AEC. That is the reason why the GPC decides to participate in the threat sharing program of the AEC as well. To participate in this threat sharing program the GPC has to introduce the sensor network node and associated sensors which are provided by the AEC. The following list describes the relevant components for the organization.

- *Sensor network node (SNN)* - The sensor network node is a software component which is provided by the AEC and which has to be maintained and operated by the GPC. It is the communication interface between the MISP service and the sensors. The SNN performs most of its tasks (like request new threat indicators) automatically and manages a task-list for each individual sensor.
- *Sensor* - The sensor is a minimized software package which is installed on a supported electronic device. A sensor can perform scans for threat indicators and reports sightings back to the SNN. It is controlled by the SNN.

4.1 Threat information provisioning

To provide threat information to the sensor network system and hence also for the companies, the AEC searches for various threat information sources. Figure 2 provides an overview of the steps within this phase.

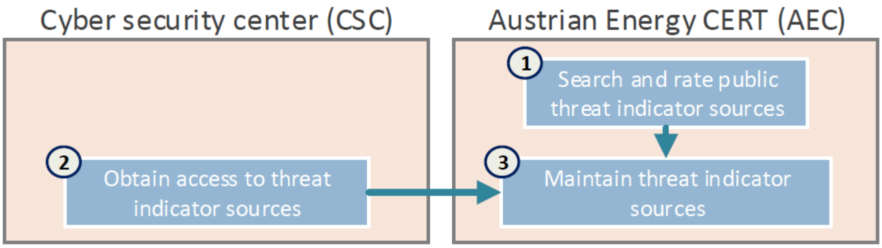
Cyber security center (CSC)
Austrian Energy CERT (AEC)
1
Search and rate public threat indicator sources
2
Obtain access to threat indicator sources
3
Maintain threat indicator sources

Figure 2. Information provisioning by the AEC

(1) **Search and rate public threat information sources:** The *AEC* operates a MISP service and searches for threat information feeds from public sources. Because of the huge amount of public sources the AEC needs to rate the quality and relevance. Following a careful evaluation, the *AEC* decides that the official *CIRCL OSINT Feed* and the *ZeuS IP blocklist* are perfect feeds for the energy supply sector and subscribes to them. After the subscription the MISP service collects threat events from these feeds at regular intervals automatically. Each received event describes a threat, for example a ransomware, and has multiple threat indicators attached to it. The event data is then stored permanently in the database of the MISP service for further processing.

(2) Obtain access to threat indicator sources: In case that another country is targeted by a large-scale cyber attack it is most likely that other countries get hit as well as collateral damage. That is why the CSC communicates with other governmental institutions from other countries and exchanges threat information with them. The CSC then shares this non-public threat information with the AEC and populates the MISP service with these information. This cooperation ensures that widely relevant threats are detected as fast as possible which would not be possible with public threat information sources only.

(3) Maintain threat indicator sources: The AEC periodically searches for new threat sources, rates them based on their information quality and compares them with already subscribed sources. During this process the AEC detects, that the previously used ZeuS IP blocklist feed was of limited use within the last month and has raised some false positives as well. Compared to other sources, the ZeuS IP blocklist fell far behind in the quality rating and therefore the AEC decides to unsubscribe from this information source.

4.2 Registration to the threat information sharing program

The following processes are executed, when a new company wants to join the threat information sharing program. Figure 3 provides an overview of the steps within this phase.

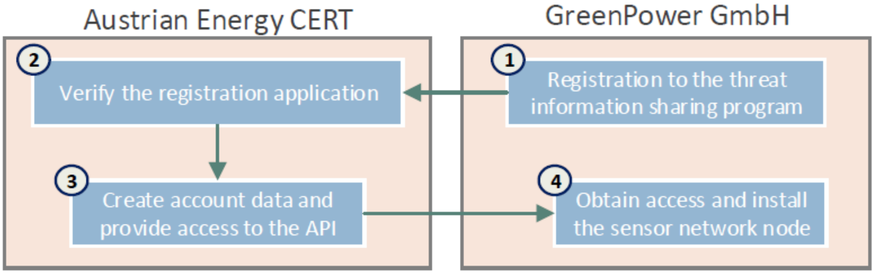
Austrian Energy CERT
GreenPower GmbH
1
Registration to the threat information sharing program
2
Verify the registration application
3
Create account data and provide access to the API
4
Obtain access and install the sensor network node

Figure 3. Registration process.

(1) Registration to the threat information sharing program: The GPC has realized that their standardized threat detection programs are not able to identify targeted attacks in time and asks for help at the AEC. That is the reason why the AEC offers the GPC to participate in their threat information sharing program to benefit from the faster threat detection. As a trade-off to be accommodated into their program, the GPC is willing to implement the required sensor network node within their company and will share their sightings with the AEC.

(2) **Verify the registration application:** The AEC verifies the registration by checking the validity of the application and whether the GPC is situated in the energy sector. After a successful inspection, agreements regarding the cooperation are signed by both sides.

(3) **Create account data and provide access to the API:** After the completion of the registration process the AEC grants the GPC access to the MISP service. In addition, the AEC provides further installation details for the sensor network node, which need to be implemented by the GPC.

(4) **Obtain access and install the sensor network node:** The organization GPC receives the information on how to install the sensor network node within its company's network. After the installation the parties share their public keys to setup a public key infrastructure. A public key infrastructure is meant to enable entities to securely communicate on an insecure public network and to authenticate themselves via a certificate (Housley et al., 1998). The security team of the GPC then installs sensors on all monitored devices and sets up the main SNN. This main component is then configured to operate as the communication device between the AECs MISP service and the company's sensors.

4.3 Indicator scanning and reporting

The following process, visualized in Figure 4, describes the indicator retrieval sequence followed by the scanning and reporting sequence. Most of these processes are performed automatically by the MISP service and the sensor network node.

(1) **Request newest threat information:** At periodic intervals, the sensor network node requests the newest threat information from the AEC's MISP service. This request includes information on when the latest request was issued and the maximum number of requested events.

(2) **Collect and send threat information:** The MISP service processes the incoming request and searches for the latest events in its database based on the request parameters. The service finds an event from a recent ransomware called "Petya" and an added indicator that this malware is creating a file named "BCA9D6.exe" in the user's home folder. The found event is then converted into the STIX format and sent back to the sensor network node.

(3) **Receive threat information and process it:** The sensor network node receives the requested events from the MISP service and extracts the

attached indicators of compromise. For the sensor network node only the indicators are relevant, the additional information, for example who has found a malware is not needed for an indicator scan and can therefore be removed to increase privacy. These minimized events are then stored in the sensor network node's database, to be able to merge sightings to events after the indicator scanning process.

(4) **Plan the threat scanning process:** The GPC's security operator rates the importance of event characteristics in advance, so that the sensor network node can plan the scanning process without any further human interaction. The security operator increases the importance of events found by the security company FireEye, because their latest threat information in the last 3 months had the lowest false alarm rate. At periodic intervals the sensor network node then iterates automatically over the stored events and selects them for the scanning process. In this selection process the events are ordered by their importance. When an event gets selected its indicators are extracted and the sensor network node examines which assets can be affected by the corresponding threat. The sensor network node then creates scanning jobs for the chosen sensors and stores them into a scanning queue.

(5) **Scan for indicators in the company's network:** Whenever a sensor has completed all of the past planned scanning jobs, new jobs are requested by the sensor from the node's scanning queue. Within this request a sensor, which is installed on a Windows machine in the HR department, receives the scanning job for the filename "BCA9D6.exe". The sensor then temporarily stores the new jobs locally and executes the file scanning tool. Before starting the scan the sensor takes into account the system's workload and tries to minimize any side-effects on performance of the scanning process.

(6) **Finish the threat scanning process:** If we assume that the sensor could not find the indicators for the Petya Malware, it finishes the scanning job and reports to the SNN that the indicator was searched for but could not be found. The sensor then deletes the scanning job from its temporary storage and continues the scanning process of further scanning jobs or requests a new list of jobs from the sensor network node.

(7) **Report sightings of indicators:** As soon as the sensor has found the suspicious file on the computer in the HR department it combines the sighting with the corresponding task and sends the information back to the sensor network node. The sensor network node then adds the current timestamp to the sighting, combines the sighting with the corresponding event, converts the event into the STIX format and sends the extended event back to the AEC's MISP service. The SNN performs the process

of reporting a sighting to the AEC's MISP service every time when a sensor could detect an IoC.

(8) **Receive sightings:** The MISP service listens permanently for sightings from the GPC found by its sensor network node. After the GPC's sensor network node merged the sighting of the suspicious filename with the event, it sends the finding to the AEC's MISP service. The MISP service receives the sighting information and stores it into its database. Since a message is sent to the MISP service for each individual sighting detected at the GPC, the MISP service can draw a diagram of the observed indicator and estimate its distribution speed.

(9) **Raise alert and inform responsible team:** In addition to the reporting of the sighting the sensor network node automatically informs the organization's security team as well. The security team of the GPC then examines the sighting and decides if it is a false positive or if further actions have to be performed. Since false positives cannot be detected automatically during a simple scanning process, they must be transmitted to the AEC via a separate communication channel. This is done via CCOPs which are created manually by employees of the GPC.

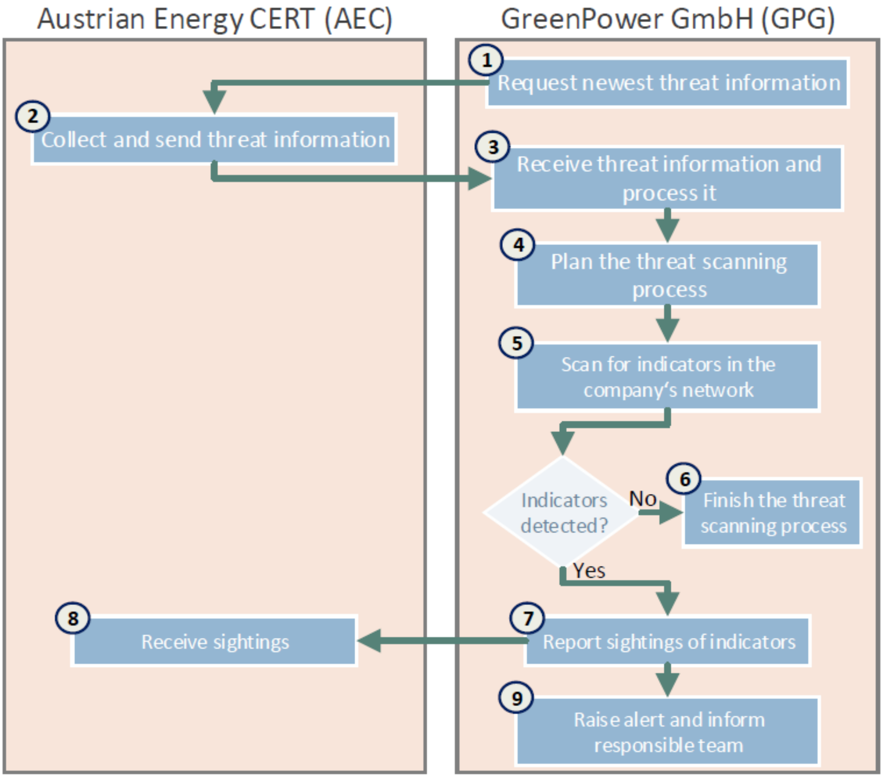
Austrian Energy CERT (AEC)
GreenPower GmbH (GPG)
1 Request newest threat information
2 Collect and send threat information
3 Receive threat information and process it
4 Plan the threat scanning process
5 Scan for indicators in the company's network
Indicators detected?
No
6 Finish the threat scanning process
Yes
7 Report sightings of indicators
8 Receive sightings
9 Raise alert and inform responsible team

Figure 4. Indicator scanning and sightings reporting.

4.4 Evaluation of the cyber security situation

The following process describes how the AEC uses the sightings to create a CCOP and how information derived from this CCOP is shared with the CSC. Figure 5 provides an overview of the steps within this phase.

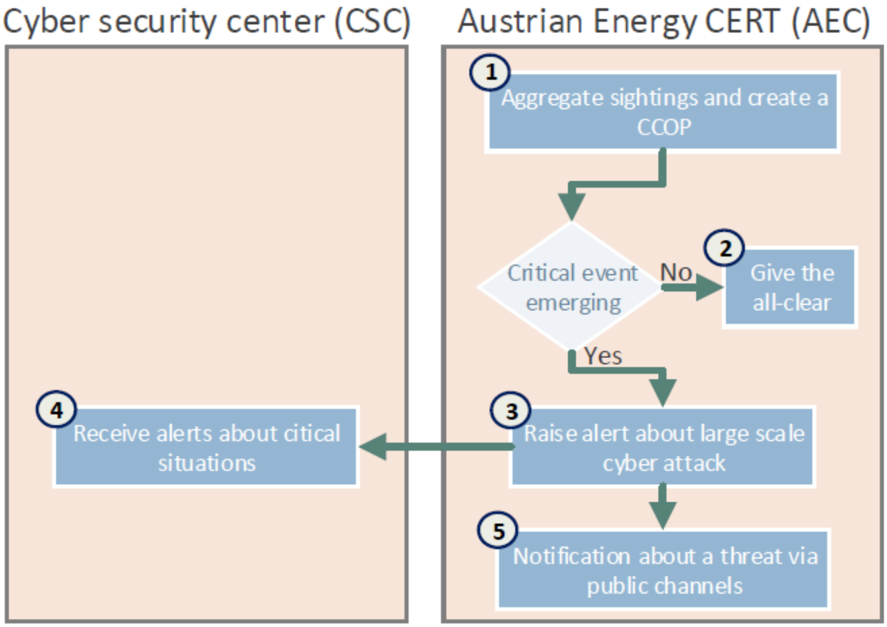
Cyber security center (CSC)
Austrian Energy CERT (AEC)
1
Aggregate sightings and create a CCOP
Critical event emerging
No
2
Give the all-clear
Yes
3
Raise alert about large scale cyber attack
4
Receive alerts about citical situations
5
Notification about a threat via public channels

Figure 5. Evaluation of the cyber security situation.

(1) Aggregate sightings and create a CCOP: The AEC collects information about sightings within the last 72 hours from the MISP service and creates a CCOP based on this information. This CCOP states that 5 out of 7 participating organizations in the energy sector are affected by the ransomware "Petya" and that the indicator of the suspicious file name has thus been confirmed. In addition, the CCOP indicates that 3 of the largest organizations in the energy sector have reported a 50% increase in sightings within the last 48 hours. It can be assumed that the organizations have recently been infected and that the malware has spread massively since the last 2 days. With the help of the threat sharing program, the malware was confirmed several times and the CCOP shows that the malware has already spread frequently. The AEC therefore concludes that the malware is an immediate threat and further steps are needed to get the malware under control.

(2) **Give the all-clear:** If we assume that the AEC cannot find any unusual behavior or any outliers in the CCOP, it will give the all-clear internally. No further information sharing with the CSC and the GPC will be done, and the event will be kept with very few sightings and many false-positives within the MISP's database.

(3) **Raise alert about large scale cyber attacks:** With the help of the CCOP the AEC can confirm the Ransomware as an emerging threat in the energy sector. Without any delay the AEC raises an alert about the emerging cyber attack and informs the CSC about it. Then the AEC collects more information about the malware and can identify that its main distribution is via targeted phishing e-mails to the HR departments of companies. After finding the used entry vector of the malware, the AEC informs organizations in the energy sector, how the malware gets access to an organization's computer and provides additional information for better risk mitigation.

(4) **Receive alerts about critical situations:** The CSC receives the alert about the apparent cyber attack and updates and assesses the overall cyber security situation based on the new information. Depending on the severity of the reported information, the CSC then decides if additional partners will be asked for help and which institutions outside of the threat sharing program need to be informed about this emerging threat as well. In addition to this, the CSC helps the AEC to collect information about the used exploits of the detected malware and shares information about the malware with the AEC until the threat has been contained. To keep each other up to date, the CSC and the AEC share as much information as possible about the identified threat and provide information to the organizations about possible countermeasures. The CSC and the AEC share this additional information over a side-channel. As soon as the GPC and all other organizations within the energy sector have eliminated the exploit by blocking the executable "BCA9D6.exe", the organizations will inform the AEC about it. The AEC can then give the all-clear to all participants within the threat sharing program via e-mail.

(5) **Notification about a threat via public channels:** In a last step the AEC informs all subscribers of its public mailing list about the found ransomware and the targeted phishing emails. Through this public information channel eventually all organizations and individuals will get informed, even when they do not participate in the threat sharing program.

5 INDICATOR TYPES AND SENSOR TECHNOLOGIES

An indicator of compromise, often abbreviated as IoC, is an information artefact which indicates with a high confidence an intrusion or malicious activity on a technical system like a computer (Rid et al., 2015). In addition to technically detectable unambiguous IoCs, a huge set of behavioural indicators, such as speed degradation, change of bandwidth utilization etc., exist that might point to underlying security issues. Technical Indicators can be identified by specialists when they analyse the modus operandi of cyber threats, forensically dissect malware samples, and are usually discovered through collaboration with specialized labs, national authorities and experts around the globe.

In order to search for IoCs automatically, they have to be classified and suitable sensors for specific indicator categories applied. Such a sensor is deployed directly on (or nearby) a technical device and examines if any of these known IoCs are present. In our model, a sensor must receive a scan job from the SNN that it is capable to execute. In other words, each type of indicator, such as a specific registry key in a Windows system, the name of a particular process or the hash sum of a system file, requires different technologies to discover them.

A crucial drawback of massive sensor networks are the potential operational risks introduced by the sensors. A sensor itself must not be a security risk on its own by requiring privileged access rights and it should not require too much computational power to search for indicators. The actual business processes must not suffer from severe impact due to parallel scanning processes – which would effectively render the benefits of a cyber security sensor network null and void. Estimating potential side effects of search operations is a good reason to carefully categorize indicators according to the level of resources required to prove their presence. This categorization can then be utilized by a company’s CISO to decide which sensors are at an advantage compared to others, considering technical limitations.

5.1 Categorization by Complexity

A common categorization of indicators is based on their complexity (Hutchins et al., 2011). Here, indicators are distinguished based on how difficult it is to compute and confirm them. The three categories are (i) atomic indicators, (ii) computed indicators and (iii) behavioural indicators.

Atomic Indicators. This group of indicators is the simplest form and their presence alone on a technical device can identify a cyber threat. These indicators are for example a file name, an IP address, a folder name, a process name or an e-mail address. Compared to the other complexity categories, these indicators cannot be broken down into smaller parts without losing their forensic information value. When searching for such an indicator, it is sufficient to simply find it anywhere on a computer system and no calculations or additional data analysis are required. However, one problem associated with atomic indicators is that the false alarm rate is relatively high, and its sighting does not always have to pose a threat. An example of this can be an IP address which is used to launch a cyber attack. Finding this indicator on a company's network does not necessarily pose a threat, because the same IP address can also be used by a legitimate website. For this reason, it is important to perform further investigations into additional atomic indicators and possibly merge them with other indicators to identify a threat. A further drawback is that atomic indicators can quickly be changed by attackers. For example, the file name of a malware can change randomly with each wave, or the email address for sending a malware is changed after a certain time period.

Computed Indicators. Computed indicators, as the name implies, need some more or less complex calculations to confirm their presence. A good example is the hash sum of an infected file. In order to determine the hash sum of a file, the entire file content must be read and processed – and repeated for all files on a continuous basis. Another example is a certain communication patterns that needs to be monitored and validated with predefined rule sets (e.g., beaconing of bot members which can be detected with Snort). The important conclusion with respect to computed indicators is that a sensor needs to continuously perform calculations, so that when a scan request for a specific indicator comes in, only a simple lookup is needed. Therefore, although these indicators are much more reliable than atomic indicators, depending on the nature of the sensor, they can already be problematic for sensors (respectively devices) with low performance.

Behavioural Indicators. Behavioural indicators are those that combine several other (less complex) indicators and contain up to a whole attack profile. An example for a behavioural indicator is, if an attacker first sends someone an email and hides a malware within it (atomic indicator: e-mail address). This email is for example targeted to the HR department (computed indicator: letter of application with specific content) and contains a trojan horse (atomic indicator: filename, computed indicator: hashsum) to collect data from employees and send them to an external server (computed indicator: Snort).

Such a grouping of attacks is captured as tactics, techniques, and procedures (TTP) and represents the “modus operandi” of an adversary. Eventually, several simple indicators need to be merged at a higher level (the SNN) to prove the existence of a behavioural indicator. In order to keep the presented system fast and slim, we define behavioural indicators to be out of scope (however, still manageable with our proposed system if needed).

5.2 Technical Classification of IoCs

Once we have determined what categories of indicators (in terms of complexity) our system should be able to handle, we need to pick what indicators from a technical point of view are interesting to us (Table 1). While the complexity decision is mainly influenced by the to be monitored system (e.g., an enterprise backbone can handle other complexities than a low-bandwidth IoT network), the selection of appropriate indicator classes is mainly driven by the expected threats and malware implementations.

Indicator class	**Indicator examples**
Network indicator	attempted connections to an ip/domain; communication patterns (frequency), packet signatures, DNS requests; URL history; open ports / sockets; sessions
String indicators	Emails, sender contains pattern; executable contains string (such as email address, IP, domain name etc.)
File system indicators	presence of files/folders on the system; file hashes; content in a file / hosts file; Disk partitions / volumes
Process indicators	Running processes including their name, memory footprint etc., unscheduled restarts of processes
Operating system handling indicators	Windows registry; created user accounts, permission settings, other forms of OS-specific events

Table 1: Indicator classes

6 AN ARCHITECTURAL BLUEPRINT IN A NUTSHELL

Overall, we employ a 3-tier architecture, with a MISP server on top to fetch indicators from and report sightings to. One MISP instance serves numerous (up to several hundred) SNNs, which then drive concrete sensors (up to around 10 per SNN). An overview of this structure is depicted in Figure 6. Due to space limitations, we provide here a rough overview only, to convey an idea of the complexity of the system.

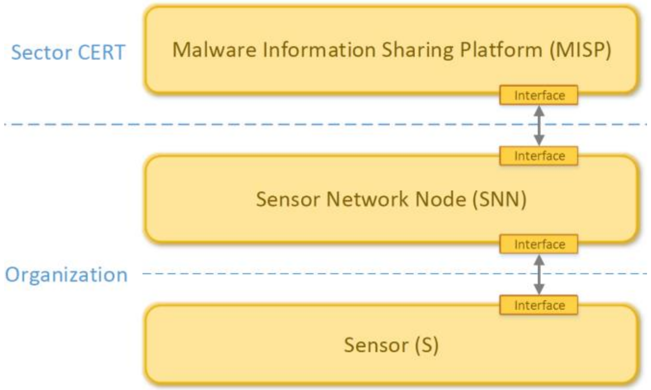

Figure 6. Overview of the sensor network structure.

Tier 1: MISP Server

The sector-CERT shares IoCs using a MISP server. For that purpose, it attaches new IoCs to sector-specific feeds (using an intuitive GUI) to which critical infrastructure operators are subscribed to. More specifically, the individual sensor network nodes (SNNs) deployed at company sites query the MISP server's feeds for new indicators and if new ones are recognized, download and apply them using a simple REST interface (cf. Figure 7).

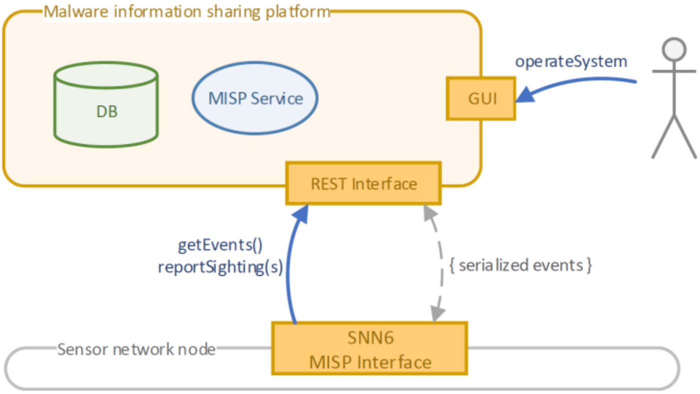

Figure 7. A MISP server provides IoCs and attaches reported sightings to the same.

Tier 2: Sensor Network Node

The sensor network node (SNN) (see Figure 8) is located within the infrastructures of critical organizations. Its main purpose is to query the MISP server for new IoCs, create scanning tasks for received IoCs and distribute these scanning tasks to the appropriate sensors. An operator can widely influence the operational mode of the SNN to configure, e.g., how often should be scanned, where should be looked for new IoCs, and what should be reported back to the MISP server as sightings.

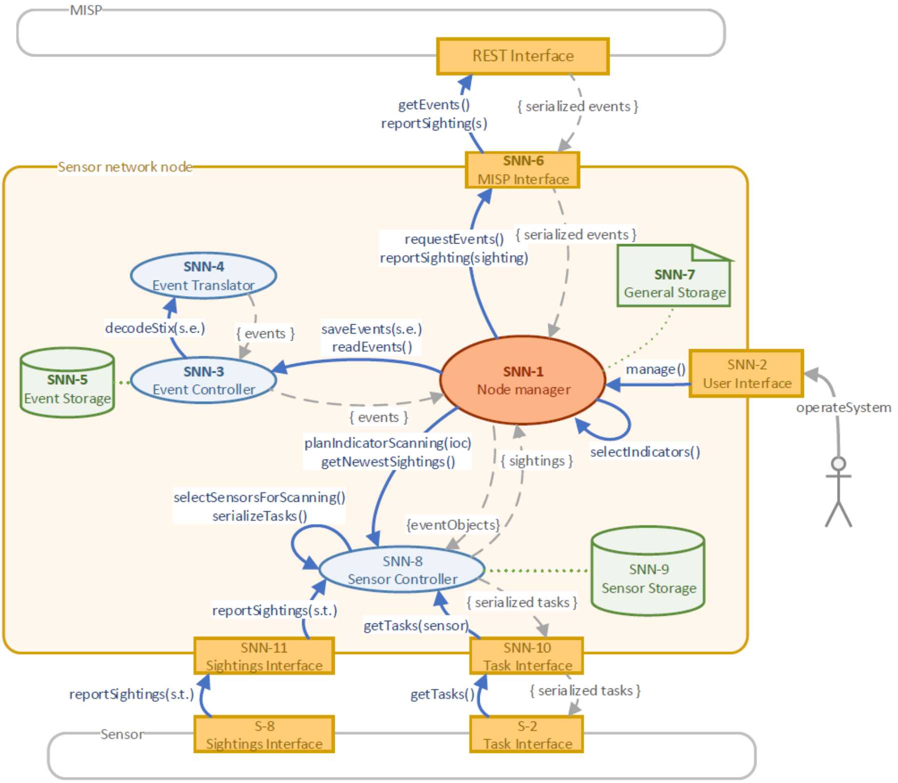

Figure 8. The sensor netwok node (SNN) queries the MISP server for new IoCs, creates scanning tasks, distributes them to specific sensors, and receives sightings back.

Tier 3: Sensing Tools

A sensor is a software component that is invoked by the SNN and that scans a technical device for IoCs (cf. Figure 9). A sensor can be installed directly on the monitored device or deployed within the network and evaluate the network communication. There are different sensor types depending on what (file system, memory, network etc.) is to be monitored. In principle, sensors can be distinguished as host-based sensors (i.e., agents that run on the monitored device and collect data directly) and network-based sensors (i.e., separate devices that are connected to the network via a tap).

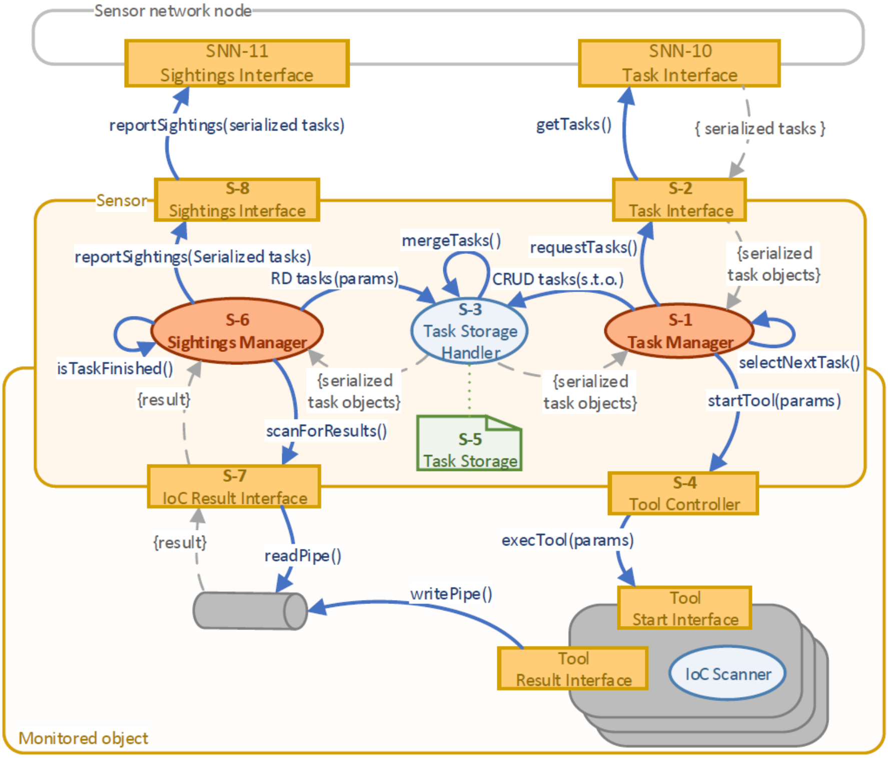

Figure 9. The Task Manager receive a scanning task from the SNN and invokes the appropriate tool, which in turn delivers a result back to the Sighting Manager, and eventually to the SNN which requested the scan activity in the first place.

7 SMALL-SCALE PILOT AND REVIEW OF A DOZEN LESSONS LEARNED

In order to validate the applicability of the introduced concept and evaluate its usability, we implemented and instantiated the architecture in course of a proof of concept (PoC) demonstrator. In this PoC, we simulated the spreading crypto trojan WannaCry (Mohurle, 2017) which can be identified by a mix of simple IoC classes given in Table 1. A list of predefined IoCs were created and published manually into a MISP instance through its web interface (in a real-life case this would be realized through feeds). This information was then retrieved by the SNNs, which propagate the IoCs to multiple sensors and await their scanning results. In a first phase, multiple virtual machines deployed to test the basic setup. In order to ease the test, all machines were connected to the same IP network. Figure 10 shows the overview of the PoC setup.

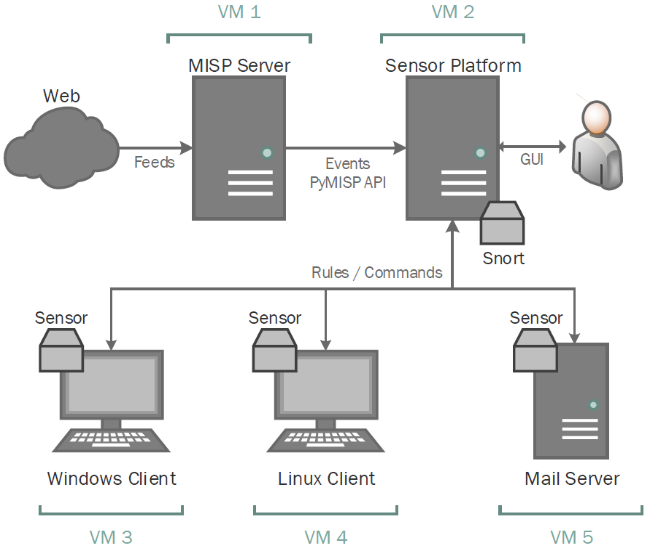

Figure 10. Simple proof-of-concept setup. In a further step machines VM2 to VM5 were replicated 10 times.

In course of this small-scale pilot study with one central MISP server, 10 SNNs and five sensors per SNN (to check different IoCs in files, processes, netflows, and the Windows registry), we identified numerous critical design issues. The list below touches on these issues, explains their relevancy and highlights different manifestations, typically at opposing ends on the same scale. The careful consideration and investigation of these issues in the areas of governance, operations, and implementation, leads to the inference of general design principles for cyber security sensor networks.

7.1 Governance Issues

G-1: Application case – high-level CCOPs v.s. detailed response planning.

It is of paramount importance to determine the application case clearly and well in advance. If the goal of the sensor network is to create high level CCOPs, different indicators will be captured and at another level of detail, frequency and intensity than in case detailed response planning relies on the sensor network's output.

Recommendation: The overall design of the sensor network, including number, type and positioning of sensors is driven by its application case.

G-2: Degree of trust – full trust in clients v.s. zero trust environments.
The degree of trust the sensor network operator, e.g., a national cyber security center, has into the monitored organizations (i.e., their “clients”) determines which responsibilities are to be delegated to them. These clients can be powerful partners if they can themselves schedule scans, validate results, sort out false positives and the like; and at the same time, they can render the whole system useless, if they manipulate or suppress sightings -– either intentionally or unintentionally. A big issue related to that is also the question of who maintains the sensors, i.e., installs, updates and configures them.

Recommendation: Trust between the CSC/CERT and organizations at least to some degree is required to operate the whole system effectively. A sort of reputation system that rewards cooperative behavior can support the emergence of trust. Furthermore, managing nodes from outside does not seem to be in favor of the majority of organizations. (Further studies on this topic are however required to validate this rather subjective view).

G-3: Cost sharing – fair distribution of operational costs v.s. the government pays for everything.
It is obvious that running such a sensor network costs a considerable amount of money, especially the more staff is required to not only run, but also maintain the network, i.e., keep its components up to date and also ensure its security (I-12). In accordance with the application case (G-1), it is important to decide early who owns which parts of the sensor network, e.g., are the SNNs in control of the government, or of the monitored organization. Coupled to this question are further concerns regarding responsibility and accountability in case of failures or security breaches.

Recommendation: See the organizations as partners who maintain their own equipment. This allows them to utilize the advanced detection capabilities in their own environments (e.g., connect the SNN to their internal SIEM); in return, they deliver timely sightings. However, the maturity level of their security teams should be verified in advance.

G-4: Control over scanning processes – local v.s. global control.
The question of who controls the scanning process is a disputable one and not easy to answer. On the one side, the operator of the sensor network has an interest to carry out scanning operations consistently across all organizations; on the other side, operators of critical infrastructures typically refrain from having external parties “sniffing” in their networks. After numerous discussions with potentially affected organizations, our advice is

to keep control locally, but transparency globally. In other words, organizations decide what type of scanning operations they allow and what results they deliver, the sensor network operator (i.e., the CSC or CERT) however may define SLAs and needs to keep track of the search tasks' status on all tiers.

Recommendation: See organizations as partners, who run their SNNs themselves, but enforced via some sort of SLAs. Eventually, local expertise is needed to validate alarms and sort out false positives in an early stage.

7.2 Operations Issues

O-5: Verbosity of reports – reporting of sightings only v.s. frequent full status updates.

The verbosity and frequency of delivered reports highly depend on the application case. There are a couple of pitfalls to consider: (i) Should an organization also actively report if no IoC was sighted, after scanning all their systems? (ii) And if so, what if an IoC is spotted after "no sighting" was already reported? Both questions are highly related to the frequency of scanning operations (G-3, O-7), as well as scope (O-5) and depth of scanning operations (I-10).

Recommendation: Active keep-alive signals are beneficial, otherwise "no response" to newly published IoCs might mean nothing was found, or scanning was not performed at all.

O-6: Scanning scope – network-level v.s. host-level scans.

The scanning scope needs to be carefully selected in advance and in accordance with the application case (G-1). The far ends of the same scale are, on the bottom side, simple network based IoCs in unencrypted traffic on the perimeter versus in-depth scanning of hosts deep within the infrastructure of monitored organizations. While scans on the outside interfaces of the perimeter seem attractive for the monitored organizations, their use is limited behind the NAT mechanisms of the border firewall. Only the simple presence of an IoC somewhere within an organization could be detected, but not the degree and severity of compromise.

Recommendation: It might be advisable to scan within organizations but let them review and vet the results before they are delivered back to the MISP server.

O-7: Complexity of operations – simple IoC validation v.s. complex behavior analysis.

The complexity and difficulty of scanning processes drive costs and will of cooperation. While the simple validation of pre-modeled IoCs can be performed largely automatically, complex and collaborative behavior analysis is a different league. The latter would be able to find unknown deviations on a grand scale, e.g., bandwidth consumption anomalies across numerous organizations in an industry sector. However, this requires extensive deployments of network probes, costly human support for analysis and interpretation and is prone to false positives. Performing In contrast to that, IoC sighting is pricy, more accurate – but can only detect what is known in advance (“know what to look for”).

Recommendation: Start with simple IoC validation. It is already complex enough to enforce and can be extended later to more advanced forms of threat detection.

O-8: Re-occurrence of scanning – single specific-purpose search v.s. continuous trend analysis.

The search for newly added IoCs should not only be performed once, but on a reoccurring basis. This allows the discovery of new infections of spreading malware (cf. G-1). An advanced mechanism to balance how long for specific IoCs should be actively scanned for needs to be employed, and popular (i.e., widely recognized) IoCs, or these that point to highly threatening activities should remain longer in the database and/or should be looked for more frequently.

Recommendation: Be careful when scheduling re-occurring scans, since every scan binds resources, which are not available for other search activities. The main question is: What search interval delivers added value compared to the required effort?

7.3 Implementation Issues

I-9: Control flow – top-down distribution v.s. bottom up subscription.

A question of effective implementation is if new IoCs should rather be pushed down, i.e., the MISP server (or any other IoC repository) notifies the SNNs about new indicators, or rather be pulled from the underlying layers (i.e., queries in certain intervals). Similarly, sightings can be pushed back to the top tiers, or stored locally and polled from time to time. Both models have their advantages and disadvantage in terms of scalability, manageability and timeliness, and their selection depends mainly on the application case (G-1)

Recommendation: Consciously pick a model that suits the application case, consider future growth of the network and carefully define requirements in terms of timeliness.

I-10: Confidentiality of IoCs – confidential IoCs v.s. common open source knowledge.

Participating organizations may or may not be able to see the actual IoCs which are distributed through the sensor network and applied within organizations. It’s a matter of priorities, whether keeping IoCs confidential or letting organizations sort out false positives is of more importance. Literally, this is a matter of trust whether the one or the other model is preferred. The CSC may not trust organizations to keep IoCs confidential, which can interfere with law enforcement (e.g., if certain characteristics of malware leak to early and hinder prosecution); on the other side organizations may or may not trust that the capabilities of the sensor network are not misused – both, either intentionally to spy on organizations, or unintentionally.

Recommendation: Non-public IoCs are an important source and can increase the detection quality significantly. However, they must be carefully secured from distribution and (un)intentional publication. Multiple trust circles are recommended, where – depending on earned trust – the sharing level can be individually adjusted for different recipients.

I-11: Scanning depth – meta-data consumption v.s. DPI on encrypted data flows.

Besides the question where should be scanned for IoCs (host or network; see O-6), another one closely related to this is what kind of data streams should be scanned for. The simplest form is to look into the meta data of unencrypted streams on the perimeter to learn about with which outside servers communication takes place and in what interval. No actual payload is touched (deep packet inspection). On the other end of the scale is to even look into encrypted streams, whereas encryption can either take place on the application layer (e.g., HTTPS), or beneath that, e.g., encrypted VPN tunnels. These can also be broken with the consent of the operators/users but is not common practice and a clear weakness in the whole design. However, this way, it could be truly evaluated what data enters and leaves organizational boundaries.

Recommendation: It is not of relevance what is technically possible, but rather what is feasible. Careful consideration of the application case will answer the question what shall be detected and what data streams need to be investigated to achieve the goals.

I-12: Security of the sensor network – open platform v.s. locked-down invite-only participation.
It is obvious that the sensor network itself will quickly become an attractive target for cyber attackers; not only to bring it down before larger operations are carried out, but also to quickly learn what actions the defenders plan to fend off an ongoing attack. It is therefore of paramount importance to secure the network appropriately. This also includes proper on-boarding/off-boarding processes of organizations. Clearly, this will not only make it harder for cyber criminals to sneak in, but also make the participation at the network less flexible and more cumbersome for legitimate participants. Eventually, a main question with respect to this issue is how much such a platform should be open for occasional and flexible participation.

Recommendation: Foresee different trust circles. While the inner circle exchanges highly-critical information (and require an extended vetting process to get in), there should still be the possibility for “occasional contributors” to participate. Otherwise chances are high, that the network becomes too exclusive and will not be able to attract a critical mass of participants.

8 CONCLUSION

In this paper, we extensively discussed an application case for cyber security sensor networks (CSSNs). We showed roles and responsibilities, defined operational processes, outlined the different types of indicators to look for, and briefly introduced an architecture for a supporting technical infrastructure. We consider the lessons learned and derived design principles as one of the main conclusions of our work, which may deliver important stimulus to the deployment of future sensor networks. We identified governance, operational and implementation issues, which all heavily impact the structure and dynamics of future CSSNs.

Future work will need to reduce the amount of human involvement to become scalable, especially to determine ways to relieve the human from reoccurring tasks and allow her/him to focus scarce and valuable resources on other tasks. Future research therefore needs to focus on:

- **Data retrieval:** Automatizing data retrieval from sources that emit data in a wide range of different formats is a key to increase the scalability. Besides getting along with numerous interface styles and protocols, the automatic generation of parsers to transform data in any format (STIX, OpenIoC, logs etc.) into one consistent format for later reasoning is particularly of interest here.

- **Natural language processing:** Besides the challenges of harmonizing different syntaxes, the much bigger challenge is to automatically process and understand free text messages, e.g., incident reports, threat assessment reports, whitepapers, blog entries, Internet forums and the like. Many valuable sources are available only in an unstructured text format, which is hard to digest automatically. However, accounting for high-level TTPs described in these sources is much more effective than an analysis based on technical indicators, such as logs, hash sums, urls and ip/mail addresses only. Either a machine-readable representation of these high-level TTPs or some smart algorithms to process this natural language texts directly are of particular importance.
- **Autonomous security database management and lookup:** Maintaining, querying and even cross-connecting (public) databases for targeted lookups when investigating incidents or assessing threat levels, e.g., when a suspicious ip address, url name or file is found in a company network, is a key requirement for automated threat assessment. Particular examples for such lookup databases are VirusTotal[2], ThreatMiner[3], ThreatCrowd[4] and DNSDumpster[5].
- **Information fusion and semantic reasoning:** Cross-connecting aforementioned sources, such as malware domains with file hashes, or CVE entries with information on exploits, is key to avoid tedious manual search activities and free the analyst's time for actual analysis instead of data collection activities. This will however require at least some semantic understanding of the information delivered by the sources. Semantic reasoning is a particularly interesting research area for future works in this field.
- **Decision making support systems:** Once the analysis is largely performed automatically, a human decision maker would only need to review the results and make a decision appropriate for a given situation. Re-occurring decisions, e.g., the triage in incident response, may, however, be automatized by using self-learning systems which monitor human decisions and comprehend which factors lead to certain decisions.

[2] https://www.virustotal.com

[3] https://www.threatminer.org

[4] https://www.threatcrowd.org

[5] https://dnsdumpster.com

Eventually, nation states need to ensure transparency regarding the application of cyber security sensor networks. If organizations do not know what the authorities are looking for, if there is no clear benefit for the monitored organizations and no reasons for collecting specific types of data, the acceptance of this technology will be extremely limited and thus its effectiveness suffer. In the best case, organizations and the nation state build a public-private-partnership were both sides benefit equally.

REFERENCES

Blask, C. H., Harper, S., Miller, A. & Van Dyke, D. (2010), ‘Security information and event management (siem) implementation’.

Cavelty, M. D. (2014), Reporting and analysis center for information assurance (melani) (phase 2: 2004–2010), in ‘Cybersecurity in Switzerland’, Springer, pp. 39–55.

European Commission (2016), ‘The directive on security of network and information systems (nis directive)’. https://ec.europa.eu/digital-single-market/en/network-andinformation-security-nis-directive.

Franke, U. & Brynielsson, J. (2014), ‘Cyber situational awareness–a systematic review of the literature’, Computers & Security 46, 18–31.

Housley, R. Ford, W., Polk, W. and Solo, D.. Internet x.509 public key infrastructure certificate and crl profile. Technical report, 1998.

Hutchins, E. M., Cloppert, M. J. & Amin, R. M. (2011), ‘Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains’, Leading Issues in Information Warfare & Security Research 1(1), 80.

Luiijf, E., Besseling, K. & De Graaf, P. (2013), ‘Nineteen national cyber security strategies’, International Journal of Critical Infrastructures 6 9(1-2), 3–31.

Mohurle, S. & Patil, M. (2017), ‘A brief study of wannacry threat: Ransomware attack 2017’, International Journal of Advanced Research in Computer Science 8(5).

Obrst, L., Chase, P. & Markeloff, R. (2012), Developing an ontology of the cyber security domain., in ‘STIDS’, pp. 49–56.

Pahi, T., Leitner, M. & Skopik, F. (2017), ‘Preparation, modelling, and visualisation of cyber common operating pictures for national cyber security centres’, Journal of Information Warfare 16(4), 26–40.

Rantapelkonen, J., Salminen, M. et al. (2013), ‘The fog of cyber defence’, Julkaisusarja 2. Artikkelikokoelma n: o 10.

Rid, T. & Buchanan, B. (2015), ‘Attributing cyber attacks’, Journal of Strategic Studies 38(1-2), 4–37.

Skopik, F. & Filip, S. “Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators.” International Conference on Cyber Situational Awareness, Data Analytics and Assessment, 2019. IEEE.

Skopik, F., Settanni, G. & Fiedler, R. (2016), ‘A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing’, Computers & Security 60, 154–176.

Stotz, A. & Sudit, M. (2007), Information fusion engine for real-time decision-making (inferd): A perceptual system for cyber-attack tracking, in ‘Information Fusion, 2007 10th International Conference on’, IEEE, pp. 1–8.

US Congress (2015), 'S.754 - to improve cybersecurity in the united states through enhanced sharing of information about cybersecurity threats, and for other purposes'. https://www.congress.gov/bill/114thcongress/senate-bill/754.

Wagner, C., Dulaunoy, A., Wagener, G. & Iklody, A. (2016), Misp: The design and implementation of a collaborative threat intelligence sharing platform, in 'Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security', ACM, pp. 49–56.

KEY TERMS

sensor network (565), sensor network node (459), cyber security (358), security sensor network (316), cyber security sensor (253), threat information (210), national cyber security (179), misp server (160), misp service (160), sector cert (140), scanning process (120), national cyber security sensor (100), cyber attack (100), information sharing (98), cyber situational awareness (95), cyber security center (95), threat sharing program (95), national authority (80), atomic indicator (80), energy sector (80), national cyber security centre (80), threat information sharing (79), aec misp service (79), critical infrastructure (70), computed indicator (70), industry sector (70), monitored organization (70), behavioural indicator (70), information sharing program (63), public threat information source (60)

BIOGRAPHICAL NOTES

Florian Skopik is Senior Scientist and Team Lead of the ICT Security Research Group at the Austrian Institute of Technology (AIT). His main topics are centred on critical infrastructure protection, smart grid security and national cyber security and defence. He published more than 100 scientific conference papers and journal articles and holds some 30 industry-recognized security certifications. Florian is member of various conference program committees and editorial boards, as well as standardization groups, such as ETSI TC Cyber and OASIS CTI. He frequently serves as reviewer for numerous high-profile journals, including Elsevier's Computers & Security. He is registered subject matter expert of ENISA (ENISA M-CEI-17-T01) in the areas of new ICTs and emerging application areas as well as Critical Information Infrastructure Protection (CIIP) and CSIRTs cooperation. As invited reviewer he evaluates research project proposals for numerous national research funding agencies, including the European Science Foundation (ESF), as well as the EC's Horizon 2020 programme.

Stefan Filip is freelancer of the AIT Austrian Institute of Technology and computer science student of the Vienna University of Technology. He pursues his master thesis focusing on cyber security sensor networks.

REFERENCE

Reference to this paper should be made as follows: Skopik, F. & Filip, S. (2019). A blueprint and proof-of-concept for a national cyber security sensor network. *International Journal on Cyber Situational Awareness*, Vol. 4, No. 1, pp155-184.