Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators

Florian Skopik, Stefan Filip
Austrian Institute of Technology, Center for Digital Safety and Security
Giefinggasse 4, 1210 Vienna, Austria
firstname.lastname@ait.ac.at

***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, 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.**

***Index Terms*—cyber security sensor networks, indicator distribution, design principles, national cyber security**

I. Introduction

Situational awareness is a cornerstone of every successful defence strategy [1]. 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) [2] 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) [3] 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 the paper 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 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 II provides an overview of related work. Then, Sect. III elaborates in detail on the different stakeholders and their roles and responsibilities to run an IoC-based sensor network. Some insights on indicator types are given in Sect. IV, while Sect. V outlines 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 rational behind the design and actual design patterns of cyber security sensor networks in Sect. VI. Finally, Sect. VII concludes the paper.

II. Related Work

Indicators of compromise are a means to validate the exploitation of a vulnerability [4]. 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 [5] 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 [6], US CISA [7]. Additionally, information sharing across organizations [8] 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 [3]. 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 [9] could be of great help, and some real-world examples are already deployed, e.g., in France, Finland [10], and Switzerland [11] for exactly that purpose. Eventually, collecting information about cyber attacks, incidents and threats in a timely manner is essential to gather cyber situational awareness [1], and a prerequisite of justified decision making [12].

III. Roles, Responsibilities and Interactions

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

A. 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 [1]. 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) [13], to the sector-CERTs, where they feed a MISP server [3] with these (partly confidential) information. The sector-CERTs may additionally subscribe to various other useful public sources (e.g., vendor lists and the like). 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) [2] – 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.

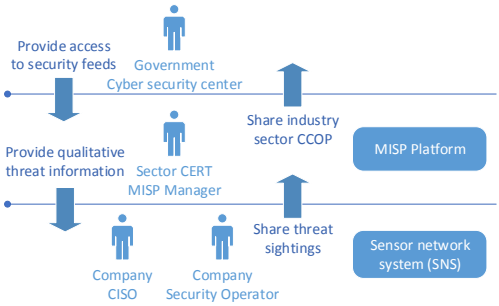

Figure 1. CSSN stakeholders and their interactions.

B. 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 [6]. 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.

In short, the tasks of the CSC are as follows (cf. Figure 2):

- **Provide access to non-public feeds:** The CSC exchanges threat information with vendors and institutions from other countries. Because of this tight cooperation and because the CSC is close to the government, it gets access to non-public threat information. The CSC revises and refines gathered information and provides it in an applicable data format to the sector-CERTs.
- **Receive CCOPs for each industry sector:** Each sector-CERT creates regularly a CCOP for its respective industry sector, which is passed on, combined with additional threat information to the CSC. This information is the basis for national decision making.
- **Derive ongoing attacks against specific sectors:** After one sector-CERT passed on a new CCOP or threat information to the CSC, the CSC assesses the collected information and compares it with gathered information from other industry sectors. The CSC can then derive if there is an attack especially targeted against an industry sector (or individual nation state).
- **Advise CERTs about attacks on other industry sectors:** Based on the evaluated threat level and based on the received CCOPs, the CSC informs sector-CERTs about emerging attacks in other domains. As a result, the CSC is the connecting link between multiple sector-CERTs and other involved organizations.
- **Create a CCOP for a national high-level overview:** With the collected information from all previous steps, the CSC creates an aggregated national CCOP for national decision making.
- **Evaluate threat level based on the high-level CCOPs:** In a final step the CSC rates the overall threat level and identifies vulnerable industry sectors, e.g., due to their above-average attack surface or commonly outdated hard- and software assets.

C. 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

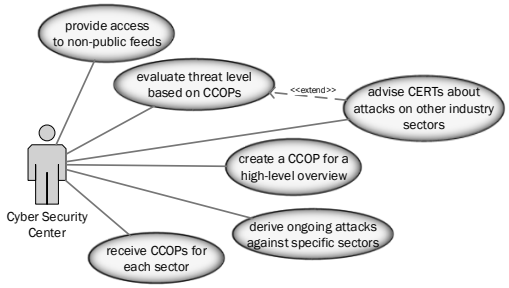

Figure 2. The tasks of the Cyber Security Center.

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. The tasks of a sector-CERT in our application scenario, also depicted in Figure 3, are:

- **Receive feeds from CSC:** The sector-CERT receives threat information and enters it in its MISP service.
- **Operate MISP service:** The MISP service holds IoCs to be scanned for with the cyber security sensor network and is maintained and operated by the sector-CERT. Within this platform, the threats combined with their indicators and the reported sightings from the organizations are stored.
- **Determine qualitative threat feeds for industry sectors:** One of the sector-CERT's core tasks is to find and subscribe to high-quality and applicable (mostly public non-commercial) threat information sources. Within the MISP service the threat information sources are also called feeds. After the subscription the MISP service starts to collect threat information from these feeds regularly.
- **Provide API access for the sensor network system:** The sector-CERT uses the MISP service to provide a REST interface, so that the organizations (more specifically sensor nodes deployed in their infrastructures) can access the collected threat information. However, access is limited, and organizations must register themselves to the threat sharing program first. Once registered, organizations share their public keys with the sector-CERT and get credentials, such as an API key to use the interface and to request threat information.
- **Retrieve sightings from organizations:** After an organization has requested threat indicators from the MISP service and has found one of these indicators in its infrastructure, it reports a sighting back to the MISP service. These sightings are then merged with their associated threat indicator and are stored in the MISP's database. In a following step the sector-CERT aggregates the received sightings to maintain overview about discovered

instances.

- **Identify wide-spread malicious activities and inform companies:** With the help of the collected sightings, the sector-CERT can re-evaluate a large-scale threat situation. Once it has identified a dangerous trend, it first informs the companies participating in the threat sharing program of the found threat and raises its threat level. Informed companies can then reassess the risk based on the warning and improve planned countermeasures if necessary.
- **Derive conclusions from sightings and create a sector CCOP:** Another task of the sector-CERT is to create a CCOP by aggregating sightings and feedback from the organizations that consumed IoCs.
- **Provide sector CCOPs to the CSC:** At regular intervals, on request and in the event of an immediate threat, the sector-CERT sends the current sector-specific CCOP to the CSC. In the event of a major attack, the CSC can use additional information channels to best support the CERT sector with additional information about the threat.

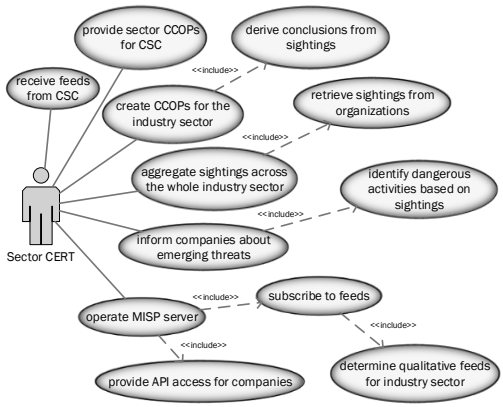

Figure 3. The tasks of a Sector-CERT.

D. 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. The associated tasks are depicted in Figure 4 and are as follows:

- **Manage the sensor network node (SNN):** The security operator's main task is to maintain the sensor network node and to keep it operational and secure. He is responsible for the correct positioning, implementation and configuration, as well as maintenance of the SNNs. He is in control of the prioritization of the scanning tasks and ensures the security of the communication channels between the SNNs and its sensors.
- **Manage sensors:** The security operator is responsible to registering all to be monitored devices at the SNN and equip them with appropriate sensors. Therefore, he has to either install a sensor software (agents/daemons) on the devices or gain access to the relevant data from external (e.g., via network taps), register them to the sensor network node and update their configurations accordingly. After this registration is completed, the security operator must determine which types of IoCs (see later) can be searched for on this device and the corresponding scanning tools have to be installed and configured. Once these two preliminary steps are done, the sensor is functional on its own and the SNN can send scan jobs to the sensor.
- **Evaluate sightings and create an organization's CCOP:** Based on the collected data of the SNN (which is transparently visible to the organization), the security operator can evaluate the current threat status. Based on his assessment of the situation, he prepares a CCOP and transmits it to the CISO, which s/he then accounts for in future risk analysis activities.
- **Receive action plan from CISO:** The security operator receives an action plan comprising upcoming tasks, based on anticipated strategic risks analysed by the CISO. These tasks are to be implemented by the security operator in order to implement the strategic security goals of an organization. Specifically, these strategic goals determine protection levels of assets, and therefore also scanning intervals, depths, and invested effort into discovering threats in certain network segments or categorized by assets. In our model, the organization therefore determines where to look for certain distributed IoCs.

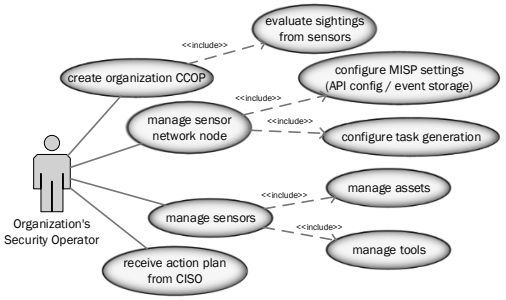

Figure 4. The tasks of security operators (in accordance with the organizations' CISOs).

IV. 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 [4]. 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.

A. Categorization by Complexity

A common categorization of indicators is based on their complexity [14]. 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).

B. 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 I). 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 (like an email, 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 I
INDICATOR CLASSES.

V. 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 5. Due to space limitations, we provide here a rough overview only, to convey an idea of the complexity of the system.

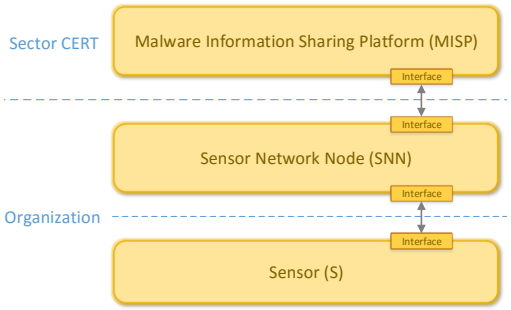

Figure 5. Overview of the sensor network structure.

A. 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. Fig. 6).

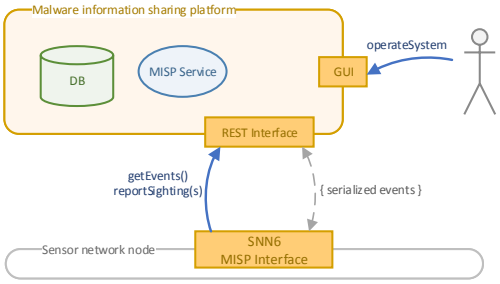

Figure 6. A MISP server provides IoCs and attches reported sightings to the same.

B. Tier 2: Sensor Network Node

The sensor network node (SNN) (Fig. 7) 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.

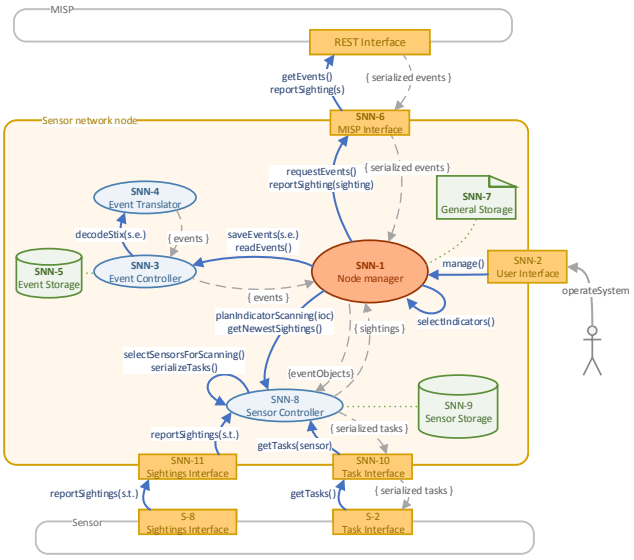

Figure 7. The sensor netwok node (SNN) queries the MISP server for new IoCs, creates scanning tasks, distributes them to specific sensors, and receives sightings back.

C. Tier 3: Sensing Tools

A sensor is a software component that is invoked by the SNN and that scans a technical device for IoCs. 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).

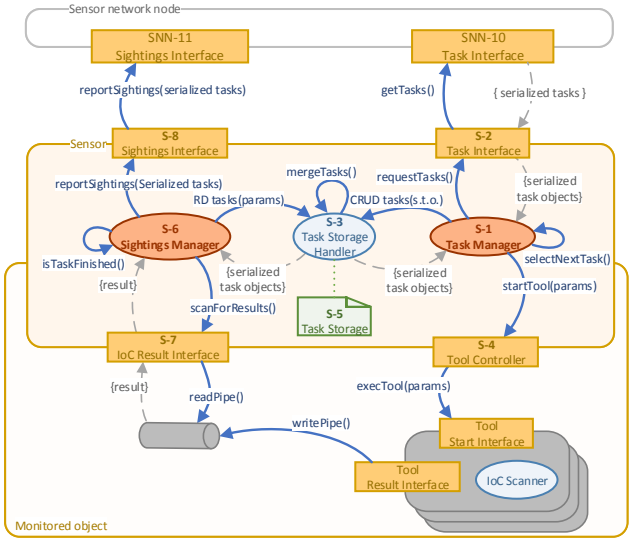

Figure 8. The Task Manager receive a scanning task from the SNN and invokes the appropriate tool, which in turn delivers a result back to the Sighting Manager, and eventually to the SNN which requested the scan activity in the first place.

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 discussion 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.

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-occuring 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?

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.

Table II

IDENTIFIED DESIGN ISSUES OF THE PILOT AND DERIVED PRINCIPLES IN THE AREAS OF GOVERNANCE (G), OPERATIONS (O), AND IMPLEMENTATION (I).

VI. 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 [15] which can be identified by a mix of simple IoC classes given in Table I. 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 9 shows the overview of the PoC setup.

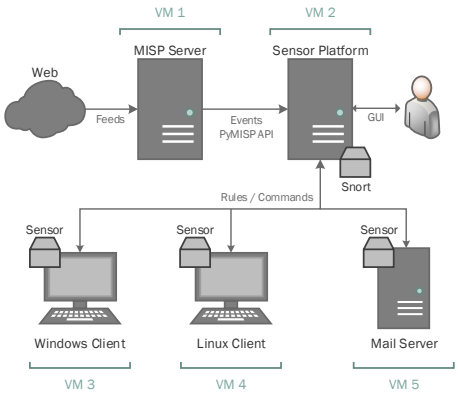

Figure 9. Simple proof-of-concept setup. In a further step machines VM2 to VM5 were replicated 10 times.

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. Table II 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 (cf. Table II), leads to the inference of general design principles for cyber security sensor networks.

VII. Conclusion and Future Work

In this paper, we extensively discussed an application case for cyber security sensor networks (CSSNs). We showed roles and responsibilities, 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. Our further work will pick up these issues and investigate design- and implementation alternatives. Eventually, we intend to extend the list of potential design issues, come up with more concrete design patterns, as well as evaluations of the different alternatives comprising discussions on their pros and cons. This should enable national stakeholders who are in charge of deploying national CSSNs to anticipate design- and operational issues and avoid conflicting implementations. A further research focus lies on the investigation of the effectiveness of such CSSNs. In other words, the question how much a CSSN of a particular shape could actually contribute to the discovery and handling of large-scale attacks is not fully answered yet. We plan to investigate previous large-scale cyber incidents and raise the question how much earlier and/or better decision making a national CSSN would have enabled.

Acknowledgment

This work was partly funded by the FFG project ACCSA (860649).

References

[1] U. Franke and J. Brynielsson, "Cyber situational awareness–a systematic review of the literature," *Computers & Security*, vol. 46, pp. 18–31, 2014.

[2] T. Pahi, M. Leitner, and F. Skopik, "Preparation, modelling, and visualisation of cyber common operating pictures for national cyber security centres," *Journal of Information Warfare*, vol. 16, no. 4, pp. 26–40, 2017.

[3] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "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, 2016, pp. 49–56.

[4] T. Rid and B. Buchanan, "Attributing cyber attacks," *Journal of Strategic Studies*, vol. 38, no. 1-2, pp. 4–37, 2015.

[5] C. H. Blask, S. Harper, A. Miller, and D. Van Dyke, "Security information and event management (siem) implementation," 2010.

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

[7] US Congress, "S.754 - to improve cybersecurity in the united states through enhanced sharing of information about cybersecurity threats, and for other purposes," 2015, https://www.congress.gov/bill/114th-congress/senate-bill/754.

[8] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Computers & Security*, vol. 60, pp. 154–176, 2016.

[9] E. Luiijf, K. Besseling, and P. De Graaf, "Nineteen national cyber security strategies," *International Journal of Critical Infrastructures 6*, vol. 9, no. 1-2, pp. 3–31, 2013.

[10] J. Rantapelkonen, M. Salminen *et al.*, "The fog of cyber defence," *Julkaisusarja 2. Artikkelikokoelma n: o 10*, 2013.

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

[12] A. Stotz and M. Sudit, "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, 2007, pp. 1–8.

[13] L. Obrst, P. Chase, and R. Markeloff, "Developing an ontology of the cyber security domain." in *STIDS*, 2012, pp. 49–56.

[14] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011.

[15] S. Mohurle and M. Patil, "A brief study of wannacry threat: Ransomware attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.