2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems

Csaba Krasznay
Head of Institute
Institute of Cybersecurity
National University of Public Service
Budapest, Hungary
krasznay.csaba@uni-nke.hu

Gergő Gyebnár
Researcher
Black Cell Kft.
Budapest, Hungary
gergo.gyebnar@blackcell.hu

Abstract: The national energy system is the most critical of the critical infrastructures, and one which has become surprisingly vulnerable to cyberattacks in the last couple of years. Both unexpected technical design flaws and targeted attacks carried out by state-sponsored actors have raised challenges for the operators of essential services. Although this infrastructure is the subject of many regulations, and national security agencies pay special attention to such critical information infrastructures, gathering cyber threat intelligence is not straightforward for several reasons. First, special protocols in industrial control systems and operational technology (ICS/OT) systems are difficult to monitor. Second, information sharing does not really work, neither between states nor domestically. Third, due to the lack of thorough technical recommendations, there is no common understanding between responsible authorities and critical information infrastructure operators. In Hungary, key stakeholders of the national electricity system have realized that although some local and European legislation deals with the question of the cybersecurity of critical information infrastructure, many open questions remain in practice, both from policy and technology perspectives. In 2018, Hungarian manufacturers, energy service providers and responsible authorities started a discussion on what should be improved in legislation and technology, as well as in information sharing and how. This paper aims to describe the framework of this collaboration for information sharing and the initial results. Specifically, we present the current technical capabilities for gathering cyber threat intelligence in ICS/OT systems and propose some legislative actions that could support further technical solutions that are feasible in these special systems. We also present Tactics, Techniques, and Procedures (TTPs) and the goals of threat actors in energy systems that can be seen from the current data sets of our honeypots.

Moreover, we will also make some recommendations as to how the national and EU-wide legislation should be built up and what kinds of actions should be required from the key players in compliance with the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

Keywords: *ICS/OT security, energy cybersecurity, critical information infrastructure, NIS Directive, honeypot, ISAC*

1. INTRODUCTION

Energy is the most critical of the critical infrastructures. Without reliable energy services, our economy and society cannot operate. Related infrastructure has been attacked intensively from cyberspace since information technology became an inherent element of energy production and transmission. Most of the special systems were designed with safety in mind but not from a cybersecurity point of view, and therefore, as these industrial control systems and operational technology (ICS/OT) systems became interconnected, their built-in vulnerabilities were exposed to highly capable attackers who have sufficient knowledge to exploit them and who were state-sponsored. Moreover, due to the changing nature of energy consumption and the need for environment-friendly energy production, the whole industry has entered a paradigm shift, which involves currently unpredictable threats in the next decade.

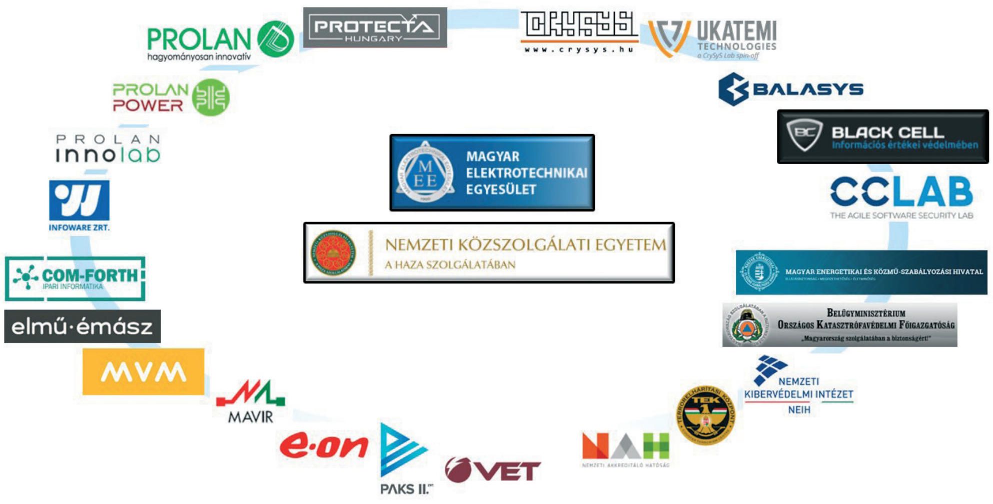
As a result of these developments, the protection of critical information infrastructures has become a key concern for legislators, diplomats, and military leaders. According to Healey and Jankins, a cyberattack against the electric grid falls into the "Destabilizing Presence" category, which might invoke a direct answer from a country. [1] The European Union expressed the need for a joint diplomatic response to malicious cyber activities under the Cyber Diplomacy Toolbox, as the Council "expressed concerns about the increased ability and willingness of State and non-State actors to pursue their objectives by undertaking malicious cyber activities," by defining that "Cyber-attacks constituting a threat to Member States include those affecting information systems relating to, inter alia: (…) services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas)." According to the Cyber Diplomacy Toolbox, "The Council stressed that clearly signalling the likely consequences of a joint Union diplomatic response to such malicious cyber activities influences the behavior of potential aggressors in cyberspace, thereby reinforcing the security of the Union and its Member States." [2]

The Directive on the security of network and information systems (NIS Directive) identifies the key types of entities related to the energy sector, or more precisely, the electricity system as essential services, in its Annex II:

- Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council (1), which carry out the function of "supply" as defined in point (19) of Article 2 of that Directive;
- Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC;
- Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC. [3]

In practice, these declarations and legal texts could not achieve their goals without the extensive cooperation of the responsible national players as identified in the NIS Directive: the responsible national authorities, local ICS/OT and cybersecurity developers and service providers. In Hungary, the Security for Control Systems (SeConSys) initiative was established in 2018 to support the cooperation of these actors and facilitate the implementation of the NIS Directive, while increasing the competitiveness of Hungarian developers on the European market by providing leading cybersecurity technologies for the energy sector. Among others, the National Cyber Security Centre, which is designated as the National Single Point of Contact (SPOC) and acts as the national Computer Security Incident Response Team (CSIRT), as well as the sectoral authority – responsible for the designation of critical infrastructures in the energy subsector – are also part of this cooperation as can be seen in Figure 1. There are two working groups in SeConSys: one is responsible for regulatory questions, the other deals with technical challenges and both aim to provide an acceptable and feasible cybersecurity framework for the national electricity systems in compliance with the NIS Directive. As a result of this cooperation and with the support of the National Cyber Security Centre of Hungary, by the end of 2020, a Cyber Security Handbook for Electrical Industrial Control Systems was released and made publicly available.

FIGURE 1: MEMBERS OF SECURITY FOR CONTROL SYSTEMS (SECONSYS)


PROLAN hagyományosan innovatív
PROTECTA HUNGARY
www.crysys.hu
UKATEMI TECHNOLOGIES a CrySyS Lab spin-off
BALASYS
BLACK CELL Információs értékei védelmében
CCLAB THE AGILE SOFTWARE SECURITY LAB
PROLAN POWER
PROLAN innolab
INFOWARE ZRT.
MAGYAR ELEKTROTECHNIKAI EGYESÜLET
NEMZETI KÖZSZOLGÁLATI EGYETEM A HAZA SZOLGÁLATÁBAN
MAGYAR ENERGETIKAI ÉS KÖZMŰ-SZABÁLYOZÁSI HIVATAL
COM-FORTH IPARI INFORMATIKA
elmű·émász
BELÜGYMINISZTÉRIUM ORSZÁGOS KATASZTRÓFAVÉDELMI FŐIGAZGATÓSÁG
MVM
NEMZETI KIBERVÉDELMI INTÉZET NEIH
MAVIR
TEK
e·on
PAKS II.
VET
NAH NEMZETI AKKREDITÁLÓ HATÓSÁG

As the Handbook states in its chapter about the practical cyber defense of electricity systems,

> The operations management of the electricity system is a continuous, real-time process. The peculiarity of electricity is that the state of the system reacts very quickly to the control. The balance between consumption and production must be ensured under the right voltage conditions and the smooth running of business processes; all through the cooperation of many actors (across countries). Their feasibility today – and increasingly in the future – has made the operation of the electricity system dependent on ICS/SCADA components. The functionality of ICS/SCADA itself also depends on the power system. Although this chapter primarily makes recommendations for the IT/ICT sector, in line with the SeConSys approach, proper knowledge and consideration of OT specificities will also be provided. IT/ICT and OT security are valid together – the two areas need to be addressed together. In some cases, modifying an OT process makes the system as a whole less vulnerable from an ICT perspective, and special attention must be paid to ICT security for critical OT processes. In addition, due to the multi-stakeholder and geographically extensive connections, the system can be considered distributed and there is no complete control over it from any of the actors. [4]

The first recommendation of the Handbook stresses the importance of information sharing and gathering threat intelligence, in accordance with the feedback from the SeConSys members. The purpose of cyber threat intelligence is to provide background information to enable management personnel to make informed decisions. This puts cyber security incidents in an appropriate professional context and supports hypothesis generation as a source at the beginning of incident management. In addition, it provides an opportunity for developing appropriate reactive defensive capabilities in relation to a specific event or sequence of events. Industry-specific reporting is essential for strategic (security management, organizational management), tactical (security teams, network teams, incident management teams) and operational (threat hunters, incident management teams, security management) organizations. This approach is aligned with Hungary's National Energy Strategy 2030, with an Outlook until 2040. The Strategy's declaration on cybersecurity highlights four action points: the creation of a sectoral recommendation (which is embodied by the Handbook), sectoral cyber threat information sharing, setting up a rapid incident management team and capacity building with skilled experts. [5]

As a widely accepted solution for cyber threat information sharing, in accordance with the relevant Hungarian strategies and other related legislation, the Hungarian Energy and Public Utility Regulatory Authority decided to establish an Information Sharing and Analysis Centre (ISAC) for the sectoral stakeholders who are also members of SeConSys. This body, known as E-ISAC, began operating in 2018. Below, we present our technical experiences on the collection and sharing of sector-specific cyber threat information for key stakeholders.

2. EXPERIENCES WITH ICS/OT CYBER THREAT INTELLIGENCE

When we set our goals in 2018, we decided to build a proper industry-specific cyber threat intelligence (CTI) feed for ICS/OT networks with a special focus on electricity. The reason why we chose this area is that the concept of Industry 4.0 may bring automation and comfort via the internet, but it also entails a huge risk for these devices. A myriad of threat feeds is available, but if they are not used properly, they can generate large quantities of noise and a slew of false positives. Moreover, these feeds are either too generic or do not cover some geographic locations properly. To avoid inadequate feeds, we decided to build an energy sector-specific honeypot network with sufficient territorial coverage that emulates the relevant protocols used by the industry.

First of all, it was important to note that there are some existing software applications for emulating ICS/OT protocols. However, the information derived from these is limited and does not meet our predefined requirement for the threat feed. In our concept, the threat feed should consist of a narrow layer of indicators of compromise (IoCs) and other relevant repository-based rules that can be used for security operations (SecOps) in the field of threat hunting in ICS/OT infrastructures. We examined and tested the Conpot, GasPot, T-Pot, Dionaea, OpenPLC and MiniCPS frameworks. While all of these had advantages and disadvantages, we concluded that the best option for us was to develop our own software. First, we finalized the minimum viable product (MVP) protocol stack that represented the widely used protocols in the energy sector. These were Modbus, S7comm, IEC104 and generic IT protocols like telnet, ssh, http, and ftp. Other protocols, such as S7comm+, IEC101, IEC103 and IEC 61850 are to be included in a later phase as they were not identified as currently vital by the stakeholders. The second step was to define the level of interactivity. To leverage the power of CTI to effectively detect and respond to ICS related cyberattacks, it was clear that we needed to define the proper Tactics, Techniques, and Procedures (TTPs). Therefore, we used a map of TTPs based on the MITRE ICS ATT&CK framework, which "is a knowledge base useful for describing the actions an adversary may take while operating within an ICS network." [6] We plan to implement automatic support for the mapping of network data to MITRE ICS ATT&CK in the near future.

Initially, over 100 honeypots were virtually deployed in multiple cloud vendors. This was unsuccessful because it was not possible to simulate the real-life operation of such systems and adversaries could easily recognize that these are our honeypots. Subsequently, the number of our honeypots was reduced to 36 and then gradually increased to over 100. While carrying out this work, we realized that the design and implementation of honeypots for ICS is quite difficult on the infrastructure of cloud solution providers.

The major disadvantage of low-interaction honeypots is that they can easily be identified as decoys and thus cannot be used to examine the behavior of adversaries. However, the development and maintenance of high-interaction honeypots is challenging. To address these limitations, we decided to design a virtual, medium-interaction and server-side ICS honeypot that can be managed by a Software-Defined Network (SDN) controller using proxies. Our assumption was that such honeypots accessible over the internet are able to mimic a vulnerable interface that could determine the attackers' strategy. A broad spectrum of interactions is likely, including Denial-of-Service (DoS, flood the network), Man-in-the-Middle (MiTM) attacks, and device impersonation, which involves sending valid and malformed packets and the option of sabotage to trigger actions through malicious commands.

The following aspects were considered during the development of the infrastructure:

- Designing distributed and functionally separate elements;
- Using encrypted data connections between areas (e.g., VPS) and internal zones;

- Separating and protecting zones;
- High-speed data connections with minimal overheads;
- Simplifying the deployment of sensor devices;
- Minimizing maintenance needs for sensor devices (e.g., upgrades, configuration, new components);
- Monitoring and control of the condition of the sensors;
- Disconnecting sensor functions from actual VPSs, importing functions into the internal zone;
- Separating the processing zone from the zone containing the sensor functions;
- Creating a packet capture option;
- Grouping and virtualizing sensor functions (docker).

Due to the sensitive nature of this operational environment, further technical details cannot be shared. However, it is worth noting that our findings are similar to what Dodson, Beresford and Vingaard published in their paper [7]. Our goal was to validate and extend their results, which is why this paper does not examine other relevant ICS honeypot-related research. We can confirm that ICS/OT honeypots should be dispersed geographically, should be hosted on realistic IP addresses and not on cloud providers, should be high-interaction, and should be systematic and continuous. In order to gain better results, we recommend cooperation and information sharing between such honeypot operators, at least inside the European Union, in accordance with the requirements of the planned NIS2 Directive.

3. RESULTS

Our honeypots have been up and running since 2018. In order to measure and evaluate the success of their operation, we will review the data from our system between 1 November 2019 and 4 December 2020. This data set represents not just the number of attacks but also the history of the honeypot development. In that sense “attack” represents all successful interactions with the honeypots. We filtered out all mass scans and typical opportunistic nmap scans. At this stage, we were not able to distinguish between human and automatic bot-like activities. The reason for fluctuation stems from the availability of cloud providers, and the difference between the number of IT and ICS attacks can be explained by our initial lack of experience regarding ICS/OT knowledge. Our results are described in Table I and are explained below.

TABLE I: NUMBER OF IT AND ICS ATTACKS IN A GIVEN TIMEFRAME, DETECTED BY THE HONEYPOT SYSTEM

Interval start	Interval end	Number of IT attacks	telnet	http	ftp	dos	Number of ICS attacks	Modbus	S7comm	IEC104
2019.11.01	2019.12.01	949 898	949 898	-	-	-	-	-	-	-
2019.12.01	2020.01.01	5 178 366	5 178 352	14	-	-	27 736	27 736	-	-
2020.01.01	2020.02.01	5 677 315	5 677 269	11	-	35	37 998	37 998	-	-
2020.02.01	2020.03.01	11 320 234	11 300 972	10	8	19 244	17 653	17 653	-	-
2020.03.01	2020.04.01	5 056 354	5 050 695	2	-	5 657	22 948	22 948	-	-
2020.04.01	2020.05.01	2 429 267	2 425 523	1	-	3 743	17 257	17 257	-	-
2020.05.01	2020.06.01	88 315	88 022	-	-	293	755	755	-	-
2020.06.01	2020.07.01	2 429 813	2 427 785	2	-	2 026	7 731	7 731	-	-
2020.07.01	2020.08.01	1 317 754	1 316 275	5	1	1 473	10 944	10 944	-	-
2020.08.01	2020.09.01	200 656	200 416	-	-	240	1 451	1 451	-	-
2020.09.01	2020.10.01	84 544	70 287	13 058	930	-	26 524	13 059	12 518	947
2020.10.01	2020.11.01	131 168	107 888	21 788	1 226	-	1 558	260	-	1 298
2020.11.01	2020.12.01	66 654	43 360	17 530	955	-	267	267	-	-
2020.12.01	2020.12.04	6 308	4 138	1 599	131	-	18	18	-	-
SUM		34 930 338	34 840 880	54 020	3 251	32 711	172 840	158 077	12 518	2 245

Interval start: The start date of the measured data.

Interval end: The end date of the measured data.

Number of IT attacks: The aggregated attacks against emulated generic IT protocols, proxies, and environments.

http: The emulated webpages impersonate the web admin and login pages of Siemens and Moxa devices. Typical attack types detected were flooding, brute forcing, as well as a very small number of crafted/malformed HTTP packets.

telnet: Most of the attacks came from this source in proportion. Using a simple telnet emulation, we collected over 3 million unique IP addresses that were not previously recognized as bots. Most adversaries tried to block serial COM, while the rest tried to determine what information is shared between connected devices, including the particular hardware or software model. In some cases, approximately 6% of the adversaries tried to exploit known vulnerabilities associated with the protocol. In most cases, however, we experienced brute-force attacks. It should be highlighted that in February 2020 we detected an enormous number of attacks, double in numbers compared to the previous and the following month. This trend was also reported by various industry sources. For example, Microsoft Digital Defense Report stated that "IoT threats are constantly expanding and evolving. The first half of 2020 saw an approximate 35% increase in total attack volume compared to the second half of 2019." [8]

ftp: We set up an ftp server, which was used for sandboxing, with a user/password that could be easily guessed; for example, by using rockyou.txt, which is widely used by the users of Kali Linux as a default password dictionary. We assumed that the typical attacker would use Kali in that scenario. Sandboxing was implemented by our own static malware lab. In this period, we created 67 new YARA rules based on the examined IoCs that we had found in the uploaded content and shared these with the community. YARA is a widely used tool by malware researchers to identify and classify malware samples.

Number of ICS attacks: The aggregated attacks against emulated ICS/OT protocols and environments.

Modbus: Adversaries tried to establish command and control capabilities over Modbus to read the contents of the packets. They were looking for the IP address of the building management system (BMS) interface and the IP address of the receiving Modbus device to see the Function Code of the request. With all this data, the Modbus device became easily identifiable, and its Modbus Register Map revealed its control and command options. As soon as they had identified the device and its control commands via Modbus, there was no limit to further actions apart from the sandbox boundaries because they could simply begin to issue commands as though they were the BMS.

S7comm: Attackers conducted information gathering using the S7ReadArea, which allowed them to accurately map variables on the PLC, and then attempt to modify the variables; for example, by setting the request time for the modification fairly low, mostly lower than 20 milliseconds, allowing themselves to continuously overwrite it with specific values. This may cause unexpected behavior on the PLC. We also experienced some MiTM attacks.

IEC104: This widely used protocol had just a few hits, mostly from DoS and MiTM attacks, but in a very few cases we experienced unauthorized access to the input modules, the processor and the output. The attacks on the DoS were IEC104 packet flooding attacks. This attack type is kind of a DoS which aims to flood the Master Terminal Unit (MTU) with specific IEC104 command packets in order to generate a possible malfunction by the MTU. It confuses the system operator or even disrupts its operation. In the MiTM IEC 60870-5-104 isolation attack, the attackers aimed to isolate and drop the IEC104 network traffic between PLC and MTU. They performed an ARP poisoning attack utilizing Ettercap software, where a specific filter is widely available which isolates and drops the IEC104 packets between the PLC and MTU.

In most cases, connections came from bots or Mass Scan-like tools (78%) from already known malicious IP addresses. ICS/OT specific search engines like Shodan and Censys were the source of 13% of the connections, while 9% of the attacks came from previously unknown IP addresses. Table II illustrates the number of initiated connections toward our honeypots between August and December 2020. Each row represents a different IP address with different decoys in different regions. The numbers are relatively consistent, meaning that if the IP address of a potentially vulnerable ICS/OT system is revealed, it will be attacked immediately and continuously. It is also notable that the number of ICS/OT targeting attacks is significantly lower than the number of IT attacks. We assume that ICS/OT knowledge is still owned by a minority of cyberattackers; therefore, companies operating special protocols should be prepared for highly skilled attackers as adversaries.

TABLE II: NUMBER OF DETECTED ATTACKS ON DIFFERENT IP ADDRESSES

Country	Number of connections
India	224 193
Singapore	179 132
India	177 674
Netherlands	175 710
Germany	171 926
Germany	171 659
Germany	171 000
Netherlands	170 941
Germany	170 330
Singapore	169 649
United Kingdom	169 621
Singapore	169 133
Germany	169 053
United Kingdom	168 131
Germany	167 219
Singapore	166 716
Singapore	166 275
Singapore	164 087
India	152 647

United Kingdom	151 726
Germany	150 122
Germany	129 184
Germany	123 769
United Kingdom	123 434
Germany	122 729
Netherlands	121 895
Netherlands	120 677
Netherlands	118 850
Germany	108 215
United Kingdom	99 042
United Kingdom	96 254
United Kingdom	95 098
Singapore	11 864
United Kingdom	9 130
Singapore	6 429

4. USING CYBER THREAT INTELLIGENCE IN PRACTICE

The latest Cyber threat intelligence overview prepared by the European Union Agency for Cyber Security (ENISA) summarizes the major requirements for CTI as follows:

- Cooperation and coordination of EU-wide CTI activities;
- Identification of CTI requirements;
- Facilitation of CTI's connection with geopolitical information and cyber-physical systems;
- Integrating CTI with security management processes;
- Development of a comprehensive CTI program by ENISA;
- Investment in some basic CTI concepts, in particular CTI maturity and threat hierarchies.

This overview also contains the results of a comprehensive CTI survey conducted by ENISA of interested stakeholders. The survey highlights current trends relating to the way in which CTI is managed from practical and technical perspectives – the following includes excerpts from the report:

- Semi-automation of CTI production is an important tool, but manual activities continue to comprise the core of CTI production;
- Information aggregation, analysis and dissemination activities are managed using widely available tools such as spreadsheets, mail and open-source management platforms, which is indicative of the efficiency of low-cost solutions;
- The importance of defining CTI requirements is understood by the CTI user-community – this is an indication that CTI is becoming part of decision-making at business and management levels;
- A combination of consumption and production of CTI is the prevailing method for building up an internal CTI knowledge base;
- Open-source information gathering is the most widely used ingestion method, followed by threat feeds from CTI vendors;
- Threat detection is assessed as the main use case for CTI; although indicators of compromise (IoCs) are still the most important elements of CTI in threat detection and threat response, threat behavior and adversary tactics (TTPs), seem to be responsible for the upwards trends in the use of CTI in organizations;
- Measuring the effectiveness of CTI is still a difficult task. An interesting finding regarding the level of satisfaction is the low rating given to the value of machine learning functions. [9]

In general, we can confirm these findings based on our experience. We wish to emphasize the importance of understanding TTPs from the list above. This allows us to understand the techniques and procedures and to link an attack, for example, to the MITRE ICS ATT&CK framework, which represents a useful knowledge base for describing the actions an adversary may take while operating within an ICS network. This kind of knowledge base can also be used to better characterize and describe post-compromise adversary behavior. In contrast to the results of ENISA's survey, we obtained promising preliminary results with machine learning-based predictions, and these may be the subject of a future paper. We assume that better and more extensive knowledge of machine learning, or artificial intelligence more generally could increase the efficiency of the everyday usage of such technologies in cyber threat intelligence.

To illustrate the importance of understanding TTPs, we will outline a cyber incident that has not yet been published. In this case, a financial investigation found that somebody had earned millions of dollars in a short transaction on an energy company. The investigation was successful and found that the attackers had downgraded and synchronized all the protection relays, stopping the relays from working at a given time. This resulted in a serious loss in both production and share value.

The adversary’s tactic was to inhibit the response function. It achieved this by modifying the control logic, using procedures very similar to Triton malware. This could be determined because the Human-Machine Interface (HMI) registry logs had been parsed to a Security Incident and Event Management (SIEM) system and there was a correlation rule with the proper ICS threat feed that contained Triton’s registry key modifications. Solely gathering IoCs would not have been enough. We needed to put these IoCs in context and had to have workflows, implemented and tuned use cases, threat hunting, triage, and other proactive workflows.

Besides the information security aspects of the above-mentioned cyberattack, such information would also be very valuable for the local authorities. As has been known since 2017, Triton is actively targeting ICS systems. One of the earliest warnings came from FireEye. Their threat research report clearly describes relevant IoCs, but their speculations on the intent of the attacks remain within the targeted organization. The research paper claims that, “We assess with moderate confidence that the attacker’s long-term objective was to develop the capability to cause a physical consequence. We base this on the fact that the attacker initially obtained a reliable foothold on the DCS and could have developed the capability to manipulate the process or shutdown the plant, but instead proceeded to compromise the SIS system. Compromising both the DCS and SIS system would enable the attacker to develop and carry out an attack that causes the maximum amount of damage allowed by the physical and mechanical safeguards in place.” [10] There is no mention of any financial intent. Moreover, in October 2020, the U.S. Department of Treasury announced sanctions against the State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), a Russian government-controlled research institution, which was attributed as a responsible party for building the customized tools that enabled the Triton attack. The reasoning is that “researchers who investigated the cyber-attack and the malware reported that Triton was designed to give the attackers complete control of infected systems and had the capability to cause significant physical damage and loss of life.” In this case, financial motivation was not mentioned either. [11]

Our major argument for cyber threat intelligence information sharing is that if local and European authorities had the relevant information on the “dual-use” of Triton (meaning to earn money and not “only” to prepare for physical destruction) and they shared this information with private companies who might be potential victims, a higher level of cyber preparedness would be achieved. We assume that potential financial loss is a higher motivation than a potential outage. Moreover, we assume that financial gain derived by the cyberattackers would finance other illicit operations in the future. If Western countries could cut off such illegal income streams from these allegedly state-sponsored groups, their operational capabilities would be lowered.

We believe that the capability of processing such CTI requires a higher level of cybersecurity maturity on the part of the organizations targeted. Therefore, we recommend that the organizations conduct self-assessments before the implementation of CTI. Predefined maturity frameworks of this type have been published by many organizations. We suggest using the Cybersecurity Maturity Model Certification (CMMC) developed by Carnegie Mellon University and Johns Hopkins University. According to CMMC, organizations at Level 3 are mature enough to "receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders." [12]

To describe an incident, we recommend using Structured Threat Information Expression (STIX), version 2.1, "that is a language and serialization format used to exchange cyber threat intelligence (CTI)." [13] We created our CTI feed using the standardized methods of STIX 2.1. We share this information via the Trusted Automated Exchange of Intelligence Information (TAXII), which is an application protocol for exchanging CTI over HTTPS. "TAXII defines a RESTful API (a set of services and message exchanges) and a set of requirements for TAXII Clients and Servers." [14] We not only collect IoCs but also correlate them into context using external feeds for better triage for SecOps.

5. RECOMMENDED STEPS TO DEVELOP, EXPAND AND ENHANCE ICS/OT THREAT INTELLIGENCE

Of key importance for gaining relevant feeds and context is the power of the sector-specific crowdsource. The best option is to give ISACs the ability to act as a threat intelligence platform (TIP). The importance of ISACs will increase with the rise of information technology, Industry 4.0 and 5.0. Their goal is to respond to the cybersecurity challenges generated within the industry by bringing the stakeholders together on a centralized platform. An ISAC must meet both human-to-human and machine-to-machine needs. Accordingly, traditionally accepted "human-readable intelligence" functions are no longer sufficient. Next-generation ISACs must harmonize knowledge that can be processed, shared, and distributed by both human and machine means, by hosting repository-based servers such as the Malware Information Sharing Platform (MISP) or TAXII. This ability is not tomorrow's technology, but yesterday's competition, with the advent of machine-to-machine AI-based attacks and defense, where manual human interaction is not enough. Therefore, these ISACs have to have two main scopes: human-readable intelligence and repository-based intelligence. We propose the structure below for information sharing on an ISAC platform. This structure was implemented on the Hungarian E-ISAC, and as such has been tested in a real-life environment.

Human Readable Intelligence

Our ISAC framework includes some basic ISAC functions that enable the whole sector or just one entity to use it as a "virtual war room" defense communication platform in case of a coordinated cyberattack. This functionality can support situational awareness. Human readable intelligence can be likened to a social media platform, such as Twitter, that informs the user about relevant cases in a predefined scope, which a stakeholder can "follow." Specific newsletters and vulnerability disclosures are also part of this threat intelligence feed. We provide the following sections for the stakeholders.

- *Report an incident*
    - *Anonymity:* The tab allows both anonymous and named incident reporting for authorized users. Anonymity is important because market competition within the sector can override information sharing, making the whole crowdsourcing project ineffective.
    - *Ticketing:* Incidents can be integrated with most ticketing tools (JIRA, SNOW, etc.), and the platform can also send email and SMS notifications directly.
- *Forum*
    - The forum serves to share upcoming tasks, sector-specific problems and solutions.
- *Documents*
    - Uploaded documents with descriptions of them are collected under Documents. Various categories, file visibility and permissions can be set individually.
- *News*
    - A classic news thread with many administrative and aggregation options.
- *Events*
    - Reminders and announced events can be published (Exercises, Expos, conferences, TTX, Range / Drill, etc.) The iCal function can be used to save the selected event to the user's calendar. Only the site administrator has permission to announce an event.

- *Site feed news*
  - Information about the collected resources (TTPs, Tools, Campaigns, Alerts, IoCs, etc.) as well as their distribution by type is found on this page.
- *Incident response*
  - If a dedicated CSIRT / CERT is available to the sector, then the entity's direct, dedicated contact details are displayed here.

Repository-based Threat Intelligence

One of the goals of these ISACs is to broadcast and spread the threat feed, which we achieve using integrated solutions such as MISP, STIX or TAXII. With the help of the technology, the organization and the entire sector can automate the detection of IoCs identified while hunting for threats. Furthermore, stakeholders can jointly perform malware analysis. Through this crowdsource power, the strength of the community can leverage the repository-based threat intelligence SecOps activity via tools like CybOx – integrated into STIX 2.0 – where the community can work together on malware analysis or even on a cyber kill chain. Such repository-based threat intelligence could also be used for other SecOps activities to feed SIEM, Security Orchestration, Automation and Response (SOAR), Intrusion Detection and Preventions Systems (IDPS) and threat hunting platforms, in the same way that antivirus or IDPS vendors do. The distribution of threat feeds is the privilege of the umbrella organization (for example the sectoral ISAC).

The platform should employ a sector-specific, deception-based intrusion detection infrastructure that enriches incoming data with relevant context (domain information, IP information, malware hash, botnet vulnerability database, etc.). We recommend the members of each ISAC produce sector-specific feeds. That requires a customized decoy and honeynet infrastructure, including DNS Honeypot, Honeytokens, ICS honeypots and honey personas.

6. CONCLUSION

In Hungary, the Hungarian Energy and Public Utility Regulatory Authority decided to set up an energy sector-specific ISAC, called E-ISAC, in accordance with Hungarian and local strategies and legislation. Its aim was to implement both human-readable intelligence and repository-based intelligence. However, during the implementation phase, we realized that there are no exact technical requirements or recommendations on how to implement the information sharing platform of E-ISAC. Neither the Authority nor the participants provided clear technical specifications. According to ENISA's report on NIS investments, this is a common problem in Europe:

> Irrespective of organizations’ current implementation state, the challenges that were most cited were the prioritization of other regulations, the existence of stronger local regulations and the lack of clarity of the NIS Directive expectations after transposition into national law. However, for organizations that do not have a dedicated NIS Directive implementation project, internal challenges such as the lack of resources (34.6% of such respondents), lack of skills (30.8%) and lack of collaboration (30.8%) appear to be most important. [15]

As the new EU Cybersecurity Strategy for the Digital Decade, released in December 2020, states,

> The Commission proposes to build a network of Security Operations Centres across the EU, and to support the improvement of existing centres and the establishment of new ones. (…) The centres would then be able to more efficiently share and correlate the signals detected and create high-quality threat intelligence to be shared with ISACs and national authorities, and thus enabling a fuller situational awareness. [16]

Based on our experience, we recommend the establishment of a European-wide, clear technical standard for cyber threat information sharing. We believe that the Strategy’s goal (“to connect, in phases, as many centres as possible across the EU to create collective knowledge and share best practices”) cannot be achieved without standardization. Therefore, we propose that ENISA and the European Telecommunications Standards Institute (ETSI) create a new European standard for cyber threat information sharing, based on the widely used STIX and TAXII protocols. We also recommend that the European Commission refer to this standard in the revised NIS Directive or “NIS 2” as a mandatory requirement for member states and organizations under the NIS Directive. Moreover, we recommend the creation of a threat intelligence feed with limited access for NIS obliged organizations at least on the national level. Such a feed could be financed by governments or by organizations through obligatory ISAC membership. CTI is the first step toward early warning and successful defense in cyberspace over the next decade. This is a basic requirement for SecOps and provides a unique opportunity for threat hunting for both private companies and national security authorities.

REFERENCES

[1] J. Healey and N. Jenkins, “Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing,” in *11th International Conference on Cyber Conflict: Silent Battle*, T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga and G. Visky, Eds., Tallinn, NATO CCD COE Publications, 2019, pp. 123–142.

[2] Council of the European Union, “COUNCIL DECISION concerning restrictive measures against cyber-attacks threatening the Union or its Member States,” 14 May 2019. [Online]. Available: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf. [Accessed 29 December 2020].

[3] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, 2016.

[4] P. Görgey and C. Krasznay, Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve, Budapest: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, 2020.

[5] *Nemzeti Energiastratégia 2030, kitekintéssel 2040-ig*, 2020.

[6] The MITRE Corporation, “ATT&CK® for Industrial Control Systems,” The MITRE Corporation, 3 June 2020. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page. [Accessed 29 December 2020].

[7] M. Dodson, A. R. Beresford and M. Vingaard, “Using Global Honeypot Networks to Detect Targeted ICS Attacks,” in *12th International Conference on Cyber Conflict - 20/20 Vision: The Next Decade*, T. Jančárková, L. Lindström, M. Signoretti, I. Tolga and G. Visky, Eds., Tallinn, NATO CCDCOE Publications, 2020, pp. 275–291.

[8] T. Burt, “Microsoft report shows increasing sophistication of cyber threats,” 29 September 2020. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/. [Accessed 2 January 2021].

[9] European Union Agency for Cybersecurity (ENISA), “Cyberthreat intelligence overview,” European Union Agency for Cybersecurity (ENISA), Attiki, Greece, 2020.

[10] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker and C. Glyer, “Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure,” 14 December 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html. [Accessed 27 December 2020].

[11] U.S. Department of the Treasury, “Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware,” 23 October 2020. [Online]. Available: https://home.treasury.gov/news/press-releases/sm1162. [Accessed 3 January 2021].

[12] Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC, “Cybersecurity Maturity Model Certification (CMMC),” 18 March 2020. [Online]. Available: https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf. [Accessed 28 December 2020].

[13] Cyber Threat Intelligence Technical Committee, “Introduction to STIX,” 29 November 2020. [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.html. [Accessed 2 January 2020].

[14] Cyber Threat Intelligence Technical Committee, “Introduction to TAXII,” 29 November 2020. [Online]. Available: https://oasis-open.github.io/cti-documentation/taxii/intro.html. [Accessed 3 January 2021].

[15] A. Drougkas, G. Bafoutsou and V. Paggio, “NIS Investments,” European Union Agency for Cybersecurity, Heraklion, Greece, 2020.

[16] European Commission, “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient,” 16 December 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391. [Accessed 27 December 2020].