WM0824TU Deliverable 1

Group 2

Luca Morgese	**5434033/s2576120**
Fazia Ghuman	**4364554**
Jeffrey Steen	**4641426/s1193074**
Harvey van Veltom	**4350073**
Casper Kroes	**4433882**

1. What security issue does the data speak to? Why? Who is the problem owner of the security issue and why?

Security Issue. As literature reports [1][2], it's fairly common for security professionals in defender companies to design security strategies against a mostly qualitative, experience-driven assessment of a threat environment (TE). Security professionals build an understanding of a TE following a threat intelligence (TI) strategy, which implies gathering threat information from a wide variety and range of sources . The security issue we define therefore is "**The *lack of knowledge (awareness) of a threat environment, to be used for improving security efficiency and posture - thus performance - of a defender party***".

The problem owner. We chose large companies in the **Energy Sector**, for two reasons: (1) they are increasingly at risk of cyber attacks due to developments in energy grids interconnectivity [3], and are thus an interesting case on which we can test our studies on integrating OTI (Open Threat Intelligence); (2) being "big players" in the cyber-landscape, we foresee a greater availability of OTI data in the OTX dataset, which would contribute to the overall accuracy and usefulness of our detections.

Relevance of the OTX AlienVault Dataset. The domain of TI sources is vast and inconsistent [1] and as mentioned, TI insights are usually gathered from a collection of such sources. The open OTX AlienVault dataset is one of these whose contribution is seldom - if ever - methodically integrated in a TI strategy [1][2]. We can thus use information of the indicators of compromise (IoCs) in the OTX dataset to export its ***partial*** representation of a threat landscape, from an OTI perspective. Energy companies can integrate and test the view represented by metrics on the OTX dataset with their TI strategy, and analyze whether and in which level a similar source is representative to their firm, for instance by comparing OTX insights with logs from their network monitoring capabilities.

2. What would be the ideal metrics for security decision-makers?

The Observe and Orient phases of the OODA framework [4] highlights the critical contribution of threat environment awareness for defenders to tune their security controls and systems. Decision-makers would find ideal metrics in those capable of capturing the threat environment (observation) and the defender's security posture (to orient further analysis). According to this framework, we propose the following ideal metrics in the aim of the stated security issue.

Threat Environment Knowledgeability (TEK): "*how well a company can define the threat environment to which it is subject to, according to all available TI, over a time span*". An instance of this metric could be elaborated upon considering indicators like

1. How many TI sources are processed to produce a model of the threat environment, upon an ideal set of all TI resources (hard to define and subject to bias), weighted on their quality.
2. A quantifiable assessment of the security experts on how much they are confident they know about the threat environment.

If a company *knows* how much of the TE it is capable of capturing, it can make decisions on putting more resources on TI or not, and has an indicator to value how much confidence can be put into security decisions.

A **Threat Category Robustness** (TCR): "*how well a company counters each specific threat category (from a set of threat categories)*". Each threat category would have a related TCR, computed considering different indicators. It would be comparable to a result of threat-category specific penetration tests. For instance:

- A Phishing-TCR, computed on the results of anti-phishing training, and how many employees took the training. Presence of secure email gateways and their configuration could also be considered.
- Ransom-TCR, assessed on the number of privilege-escalation/code-injection scanned vulnerabilities and their score, on the number of ransom-related NIDS alerts, and on the presence of post-controls.

And so on for other attack types. A similar indicator would give a direct insight into the security posture of the company, and greatly help in assessing risk, thus informing budget decisions.

3. Metrics in available in practice

Hughes and Cybenko [5] provide an outline of what elements a successful attack consists of and in that process also gives an overview of which metrics are relevant to track the threat environment. The three elements necessary for a successful attack are:

- System susceptibility: for a system to be susceptible there must be a vector by which an attacker can access a system. A suitable metric for this is the number of access points to critical services or functionalities, of which it is often better to have fewer. Threat Intelligence can provide additional information here because it can elaborate on what kinds of access points are frequently targeted and exploited by providing indicators on types of attacks and frequencies, as well as what companies are targeted.
- The second threat element introduced [5] is Threat Accessibility. Threat accessibility is related to the amount of input/output processes that can be probed by attackers,

where lower is better. These processes are normally used for legitimate user access but can sometimes be exploited by attackers. Again Threat Intelligence can give an overview of which types of attacks are often levied against what types of processes. Combining this with the specifics of a system in use could provide more insight in which processes are often targeted.

- The third metric is Threat Capability, which is related to how much insight an attacker can gain from observing the system. Useful metrics provided by Threat Intelligence here are the specific types of exploits being used.

4. Metrics designed from the Alienvault OTX

We compute our metrics on all historic data available in OTX for the energy sector (i.e. pulses that have the “energy” string in *industries* label). In this way, we can ensure we have enough data for a meaningful analysis. Valuable metrics that we could define with OTX data, related to the overall Threat Landscape are:

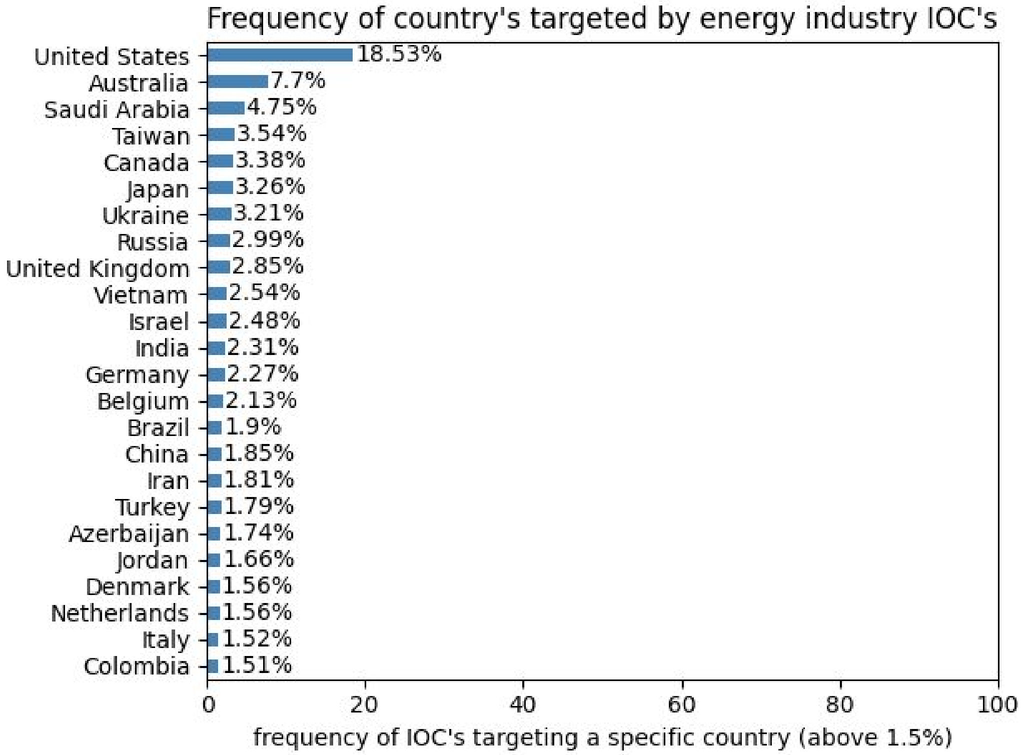
1. Frequency of IOCs for each country. For a company to decide where to invest, it is useful to know which countries are targeted the most by attackers. To construct such a metric one would take all the IOCs related to the energy sector and categorise them, by country, resulting in graph 1 below. The formula used for graph 1 is:
$$per\ country\ IoC\ frequency\ =\ \frac{\sum IoC_i^{country}}{\sum IoC_i}\ \times 100\%$$

2. To choose which types of controls to invest in it is necessary to have a clear overview of what types of threats target the energy sector. This can be visualised by plotting the frequency of the threat types associated with the IOCs as is done in graph 2. The formula for graph 2 is:
$$IoCs\ per\ threat\ =\ \frac{\sum IoC_i^{threatTag}}{\sum IoC_i}\ \times 100\%$$

3. And finally to have a complete overview of what IOCs are available it is also useful to provide some insight into the composition of the IOCs in the Alienvault OTX. This can be done by plotting the frequency of each type of IOCs, as is done in graph 3. The formula for graph 3 is:
$$IoCs\ per\ type\ =\ \frac{\sum IoC_i^{indicatorType}}{\sum IoC_i}\ \times 100\%$$

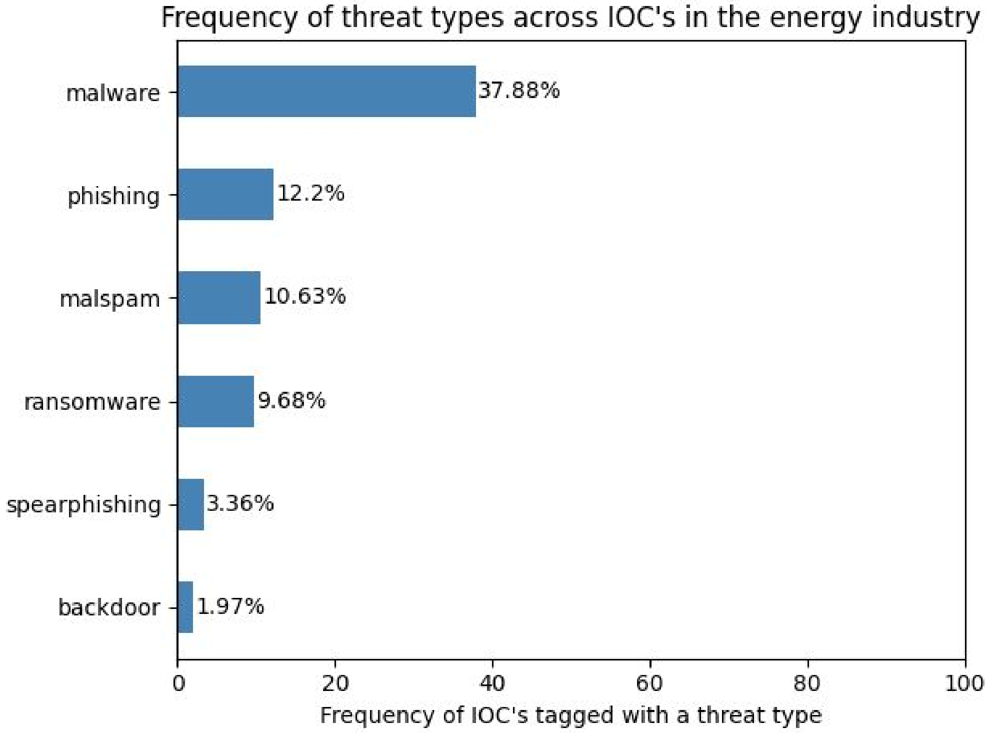
5. Visualisation designed metrics

The Alienvault OTX offers an API for python which allows for interacting with the OTX database to retrieve pulses based on search criteria. The information in these pulses can then be used to create the visualization of the metrics. To create these visualisations all pulses related to the energy industry are used (196 pulses in total) and these pulses provide a combined total of 12515 IOCs. The visualisations created are as follows:



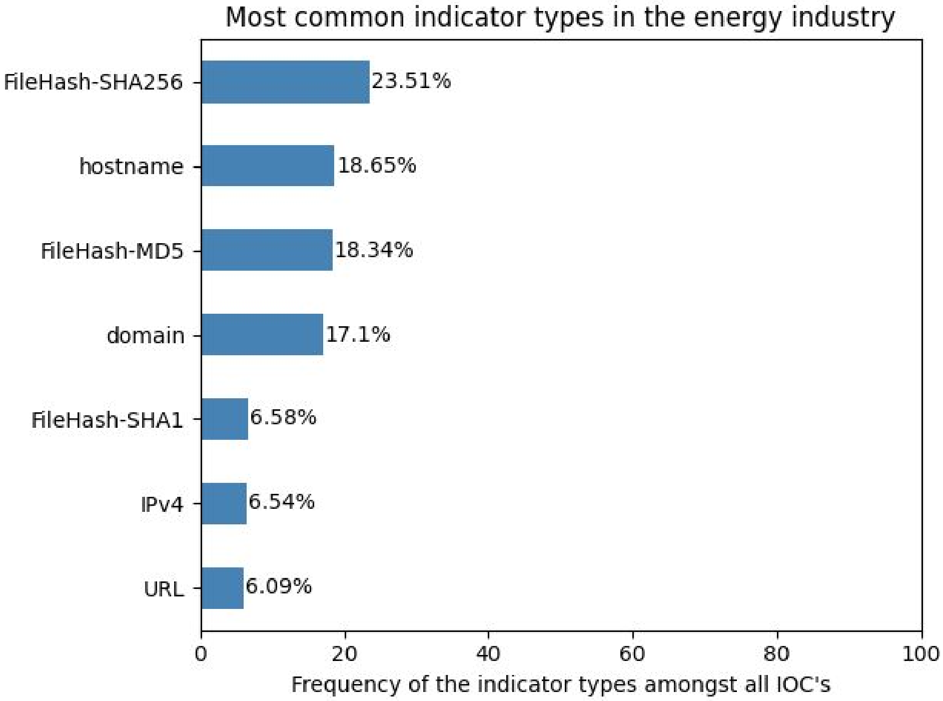
Graph 1

Graph 1 shows the frequency of countries targeted by IOCs related to the energy industry. Only countries with a total frequency of 1.5% or higher are shown to avoid information cluttering. It is important to note that it is possible and likely for an IOC to have more than one targeted country. What this metric shows, is that the largest part of IOCs in the energy industry targets the United States. This illustrates a bias in the OTX database.



Graph 2

Graph 2 shows the frequency of different types of threat in the energy industry. We selected the six most useful ones, which specify broad types of cyber-attacks. It is important to note that there is overlap between the different threat types. Ransomware for example is a form of malware. So if an IOC is tagged as ransomware it would also be tagged as malware. The problem owner can use this graph to determine that malware is the most common type of threat with malspam (malware delivered via email) and ransomware being common types of malware used. The problem owner can also see that IOCs targeting industry backdoors are much less common.



Graph 3

Graph 3 shows the most common indicator types of IOCs in the energy industry. It illustrates that problem owners should focus their cybersecurity on FileHash-SHA256 and FileHash-MD5 files as well as hostnames and domains. In turn, they can focus less on URLs and IPv4 indicators because they are less common compared to other indicator types.

6. Relevant differences/measuring security performance

For our security issue, security performance can be defined as “how well companies use their knowledge of the TE”. In the ideal scenario for this security problem, these companies’ awareness can be interpreted as (1) the capability to sketch their own threat environment (TEK) and (2) the performance regarding the combat of threat categories (TCR). Differences between companies on this would reflect the relative maturity of the cybersecurity operations compared to other companies in the energy sector.

The designed metrics to fulfil the objective are (1) frequency of IOCs per country, (2) frequency of threat types and (3) frequency of IOC types. By getting data on the frequency with which each type of attack is getting added to the OTX, an inference can be made about the frequency of attack types that are happening currently. The metric of IOCs targeting a specific country give some indication about the likelihood of an attack targeting a specific company. This information can be combined with other sources that give insight into the TE, such as other TI's, as well as data from the IDS of energy companies. This will move these companies closer to the ideal metric TEK.

7. Risk strategies for the problem owner

The visualisations show that as far as can be concluded from the Alienvault OTX, most threats in the energy sector target US companies and the most frequently occurring threat types are malware, (spear)phishing and ransomware. Graph 3 also shows that these indicators mostly come in the form of file-hashes, hostnames or domains. It must be noted that the Alienvault OTX likely has a bias in which countries are most represented in it. Additionally, we could not correct the numbers for the number of targets in each country. Nevertheless, it still could provide insight into which countries are more likely to be targeted.

As reported in point 1, the threat metrics we individuate can be tested by companies against pre-existing TI strategies, assert whether they contribute or not to the overall security posture.

If this data is representative of the overall threat landscape companies in the energy sector should prioritise controls for these types of threats because they are most frequently in touch with them. By tracking how these indicators change over time companies can also quickly catch on to changing trends within the threat landscape and change their priorities if necessary.

[1] X. Bouwman, H. Griffioen, J. Egbers, C. Doerr, B. Klievink, and M. van Eeten, ‘A different cup of TI? The added value of commercial threat intelligence’, 2020, pp. 433–450, Accessed: Sep. 17, 2020. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman.

[2] T. Moore, Tandy, S. Dynes, and F. Chang, ‘Identifying How Firms Manage Cybersecurity Investment’, 2015. https://www.semanticscholar.org/paper/Identifying-How-Firms-Manage-Cybersecurity-Moore-Tandy/7d81b3ecc520f8cb9d3980cf40fd3eb5aa17ce92 (accessed Sep. 24, 2020).

[3] P. D. Klerck, ‘The State of the station: A report on attackers in the energy industry’, *Deltalink*, May 27, 2019. https://www.deltalink.be/f-secure-white-paper/ (accessed Sep. 24, 2020).

[4] V. Lenders, A. Tanner, and A. Blarer, ‘Gaining an Edge in Cyberspace with Advanced Situational Awareness’, *IEEE Secur. Priv.*, vol. 13, no. 2, pp. 65–74, Mar. 2015, doi: 10.1109/MSP.2015.30.

[5] J. Hughes and G. Cybenko, ‘Three tenets for secure cyber-physical system design and assessment’, in *Cyber Sensing 2014*, Jun. 2014, vol. 9097, p. 90970A, doi: 10.1117/12.2053933.

Task division:

Luca: Defined, wrote and contributed to points 1, 2 and 4; general related literature research.

Fazia: Contributed to 3 & 6, proofreading draft, conducted general literature research regarding this topic.

Jeffrey: Contributed to 6 and 7, proofreading draft, general literature research.

Harvey: Contributed to 5 which includes setting up the python code for interacting with the OTX API, creating the graphs and writing the text. Proofread draft.

Casper: Contributed to 3, 4 and 7, proofread 1 & 2 and added additional literature; general literature research.