WM0824TU Deliverable 1

(Draft for the 21/9/2020)

Group 2
Luca Morgese **5434033/s2576120**
Fazia Ghuman **4364554**
Jeffrey Steen **4641426/s1193074**
Harvey van Veltom **4350073**
Casper Kroes **4433882**

1. Security issue and problem owner

Security problem. Small and mid-sized organizations are among the most targeted by cyber threats, as they usually do not have budget to dedicate to extensive security measures [1] and still interact with assets - or represent victims which may bear much value to cyber attackers []. As the paper by Bouwman e.a. shows [2] cyber threat environment awareness is a major focus in threat intelligence (TI) and while possessing security capabilities, small and mid-size companies can miss out important threat-environmental insights that could inform both a more efficient configuration of the security systems, and security policies, finally overall rendering them more prone to cyber attacks.

Why?. We want to understand how the OTI source of the OTX dataset can be used to provide a representation of a threat environment (TE) that may interest a given industry actor. By analysing specific features of IoCs in the OTX dataset, we believe that a model of attackers trends and directions, a TE, could be ascertained. By mapping companies' features and security profiles to a TE, we may be able to produce a metric on the "OTX-attacks-susceptibility", that is "given the security profile of your organization, you are susceptible 'by *N'* to the threat environment *A* (as observed in the OTX dataset)". By both consulting the metric and the TE itself, small and mid-sized companies would be able to take informed security decisions to better defend against attackers (as expressed in [9]), greedy for the low-hanging fruit that these companies may usually represent.

Problem owner. As mentioned, this study approach is mainly in regards to small and mid-sized companies that do not vastly budget their security infrastructure, and may lack further insights and threat intelligence (TI) to better tune their security posture. On a secondary level, if a similar metric would show to be particularly well descriptive and representative, it can be adopted by whoever actor to overall enrich TI.

As a last consideration, a framework for a similar metric could represent an instance of methodical use of OTI data, which is lacking in the current TI panorama, as research shows [2] .

2. Ideal metrics

- The proposed metrics follow the Observe and Orient phases of the OODA (Observe, Orient, Decide, Act) framework in [9], which also states the critical contribution of threat environment awareness for companies and organizations.

Ideal metrics for the security issue of improving TE awareness, strengthen the security posture by better tuning capabilities, and provide TI to inform security policies, could regard mainly the following aspects.

- Knowledgeability of TE, expressing “how well a company can define the threat environment to which it is subject to, according to all available TI”. An instance of such a metric could be given by indicators like
    - The number of TI sources it considers
    - The budget it dedicates to TI processing
    - Chief security officer qualitative assessment

If a company is capable of determining how well it knows the threats to which it is exposed, it can value this metric against its security performance, and decide whether it’s the case or not to put more resources towards understanding the threat context in which it may be located.

- Sectorial robustness of security posture, which would express “given a set of threat types, how well a company is prepared to counter each specific threat”, and could be extracted, for instance, by evaluating separately
    - Phishing: combine anti-phishing training results of personnel, and binary indicator on use/non use of secure email gateways;
    - DoS: number of DoS susceptible devices according to network scan, binary indicator on presence of NIDS
    - Malware: number of security alerts recorded, presence of backup management protocols, number of devices covered by AV over all company devices, number of critical (score > 5) CVS vulnerabilities individuated by network scan.
    - The above malware robustness metric can ideally be parameterized over malware type at least in the aspects of
        - Number of security alerts recorded related to malware type
        - Number of critical CVS vulnerabilities related to malware type individuated by network scan

Indicators on how well a company can defend against different threat sectors would help better define the risks for each sector, and in turn help determine the allocation of security budget towards specific capabilities.

- TE Susceptibility (TES), expressing “how much susceptible the company is to a specifically individuated TE”. A process to measure a similar metric may involve the steps of
    - Defining a threat environment for a specific business sector, over a specific period (frequency of attacks as individuated by TI, attack types, targeted locations, the provenance of threat)

- Quantitatively representing the security posture of a company with Knowledgeability of TE and Robustness to TE metrics
- Comparing how the security posture covers the threat surface of the specific threat environment.

An ideal TES metric could be a valuable tool to represent the security posture of a company against specific and dynamic threat trends. If provided timely, it would offer an important insight on whether further strengthening, tuning or revision of security capabilities is required, overall contributing to the security efficiency and performance - in our case of small and medium sized companies.

3. Metrics in practice (metrics related to the security problem individuated that are currently in place - literature review)

- Hughes and Cybenko [3] present a Three Tenets Model that aims to capture the Threat Environment Susceptibility in cyber security in more general terms the model identifies three different elements that are necessary for a successful attack. These elements are: System susceptibility, Threat Accessibility and Threat capability. Metrics used in practice can be classified among these three metrics. The first metrics named are from the paper by hughes and cybenko [3], the additional metrics come from other sources.:
    - System susceptibility: the number of access points to critical functions in terms of functionalities or services (where lower is better).
        - Metrics for measuring Phishing susceptibility: Existing metrics of measuring the phishing susceptibility are for example false positives or false negatives [7]
        - Metrics for measuring Malware susceptibility: Malware susceptibility is associated to user behaviour. More precisely, the probability of malware infection increases as users install more applications [8]
        - Employee awareness also affects how susceptible a system is to threats [4]
        - Number of incidents within a sector, which are available via Open Source Threat Intelligence [4].
    - Threat Accessibility: The number of input/output processes that are visible to the attacker (where lower is better).
    - Threat capability: how much insight an attacker can get from observing the system. This can be lowered through “evidence variability” which ensures that data collected at one point in time can not meaningfully be compared with data collected at another moment.

4. Designed metrics (created from combining data from the dataset)

Our approach would approximate the ideal TES metric on the data from the OTX dataset. We could call a similar metric OTXES (o ti ex es), indicating that it is formed upon OTX data. Here follow the steps through which the metric might be built:

1. Filter OTX pulses over a time span and related to a specific industry. This can be done either via selecting pulses which have a specific industry listed in the `industries` property of a pulse, or via selecting all pulses from a specific, industry-related OTX group.
2. Extract features from items of compromise:
    a. Geographical origin of an attack
    b. Geographical location of the target of attack
    c. Threat type (ransomware, worm, phishing, drive-by, …)
    d. Overall quantity of IoC over a time span
    e. ...
3. Create a data structure representing the threat environment for the specific company, over a given time span, collecting relevant insights that were possible to discern
4. Profile the security posture of a given company on what capabilities are in place against specific threats (must be better defined, possibly find “easy to have” indicators on protection against phishing, ransom, their threat models, etc. try to find existing indicators on “how much effective is system X against attacks of type Y), include company location.
5. Evaluate TE-specific security posture against the TE data structure, matching respective indicators.

5. Visualisation designed metrics

The visualization will be done in Python. 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. Some examples of these visualizations can be:

1. Searching for pulses after a given timestamp and count the different affected industries within said pulses. This can be used to create a bar chart to visualize which industries are targeted more in the pulses and which are not targeted as often.
2. Looking at a specific industry and analyzing the different types of indicators. This can be graphically represented in a radar chart to visualize which type of indicators are most commonly affecting a certain type of industry.
3. Analyze the pulses based on targeted countries and malware families. These two types of data can be combined to create a histogram for a specific country that visualizes which malware family occurs more frequently in that specific country.

6. Relevant differences/measuring security performance (criteria)

Security performance for these metrics is how well the strengths and weaknesses of the problem owner are balanced for the current TI. 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. This information can be collaborated with other sources that give insight into the TI, such as other TI’s, as well as data from the

IDS of the problem owner. This will move the problem owner closer to the ideal metric; knowledgeability of the TI.

This information can be used in conjunction with other metrics, such as the cost of a breach of a specific defense, to guide the problem owner in choosing the optimal distribution of resources between all the defensive options.

By comparing the perceived threat environment to the strengths of the defenses the problem owner has in place, an improved evaluation can be made about the susceptibility of the problem owner to the threat environment. This will improve the problem owner's approximation of another ideal metric; TE susceptibility..

7. Risk strategies for the problem owner

The problem owner can use the metrics to determine aspects of the defense that need to be improved, as well as aspects that are being supported beyond what the threat calls for. By understanding the threat environment, the problem owner can redistribute its resources to the defenses more likely to be attacked.

The metric can also be used to find current attacks of which the problem owner was not yet aware, and those holes in the defence can be closed.

[1] J. Hayes and A. Bodhani, 'Cyber security: small firms under fire [InformatIon Technology Professionalism]', *Eng. Technol.*, vol. 8, no. 6, pp. 80–83, Jul. 2013, doi: 10.1049/et.2013.0614.

[2] 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.

[3] 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.

[4] E. Zhang, 'Security and Analytics Experts Share the Most Important Cybersecurity Metrics and KPIs', *Digital Guardian*, Dec. 05, 2017. https://digitalguardian.com/blog/what-are-the-most-important-cybersecurity-metrics-kpis (accessed Sep. 17, 2020).

[7] Sheng, Steve, et al. "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2010.

[8] Lalonde Levesque, Fanny, et al. "A clinical study of risk factors related to malware infections." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013.

[9] V. Lenders, A. Tanner, and A. Blarer, "Gaining an Edge in Cyberspace with Advanced Situational Awareness," *IEEE Security Privacy, vol. 13, no. 2, pp. 65–74, Mar. 2015, doi:*

10.1109/MSP.2015.30.

Task division:

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

Fazia: Contributed to 3, proofreading draft, conducted general literature research regarding this topic.
Jeffrey: 6 and 7
Harvey: 5 which includes setting up the python code for interacting with the OTX API.
Casper: Contributed to 3, proofread 1,2 and added additional literature; general literature research.