A framework to study cyber expert's activities. First steps.

Alma Lelievre
EDF Lab Paris-Saclay, Conservation National des Arts et Métiers (CNAM)
alma.lelievre.auditeur@lecnam.net

Cecilia de la Garza
EDF Lab Paris-Saclay et Centre de recherche sur le travail et le développement (CRTD), Cnam
cecilia.de-la-garza@edf.fr

Tahar-Hakim Benchekroun
Centre de recherche sur le travail et le développement (CRTD), Cnam
tahar-hakim.benchekroun@lecnam.net

ABSTRACT

This paper presents the analytical framework of an ongoing study of the activity of cyber experts in French tradition ergonomics. It introduces the different professions involved in cybersecurity, defines the term "vulnerability" in this field, presents some of specific features of cyberattacks, and introduces the question on ongoing research and the methodology.

CCS CONCEPTS

• **Malware and its mitigation**; • **Management of computing and information systems**; • **Empirical studies in HCI**;

KEYWORDS

cybersecurity, ergonomics, vulnerability, SOC

ACM Reference Format:
Alma Lelievre, Cecilia de la Garza, and Tahar-Hakim Benchekroun. 2024. A framework to study cyber expert's activities. First steps.. In *European Conference on Cognitive Ergonomics (ECCE 2024), October 08–11, 2024, Paris, France*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3673805.3673839

1 INTRODUCTION

If, in the cybersecurity field, the first recorded virus in history is considered to be "Creeper", it is far from being the last. The development of connected objects over the last few decades in both, personal and professional areas, has increased the possible surfaces for cyber-attacks. Even though numerous regulations, measures and key actors have been implemented by states, institutions, companies or individuals, cyber-attacks continue to be recorded (and others remain hidden for fear of repercussions on an entity's image). Faced with these new and growing threats, the cybersecurity job market is growing, and studies in this field are emerging exponentially.

In this article, we use the NIST definition of cybersecurity as follows "measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer" [1]. While cybersecurity might once have been represented by a fortified castle (highly protected from the outside world), today it is more like an airport, with access zones restricted according to users' level of access, and a surveillance tower to monitor internal and external comings and goings [2]. The result is a controlled outward opening and incredible expansion and complexity of the areas to be monitored.

More area to monitor requires more technical and/or human resources. Even if the threat zone is larger, the perimeter of the attack entrance may not be. Cyber-attackers will target a small gateway and remain as discreet as possible. Cyber-defenders are therefore faced with cyber-attackers who can attack one system among many, at any time.

First of all, we'd like to mention the different types of cyber-defenders, as well as the other experts involved in information system protection. We will then present the "small gateways" that cyber-attackers can take, and some of the specific features of cyber-attacks and conclude with a presentation of the research question to which this paper relates, and the methodology followed.

2 VARIOUS CYBERSECURITY PROFESSIONALS

The cybersecurity field is not restricted to cyber operational agents. It involves a wide range of professionals at different stages in the life of an IS: development, implementation, upgrades, security, and repair.

Several specialties in the cyber domain may be carried out by the same operator, either through strategic choice, or through lack of human and financial resources. Others may be outsourced for the same reasons. The division of tasks between operators and the names given to these actors also depend on the organizations and countries involved. [3].

2.1 Operators involved in designing and maintaining a secure information system

Before a system can be used, it must be developed, then implemented in the network best suited to its use and kept operational.

Therefore, there are many professionals involved in the management side of cyber without being in charge of cyber's incident management: cybersecurity directors, Information Systems Security Managers, security coordinators, security program managers, security project managers...

Other experts may be called in at particular times: security architects, technical security specialists, cryptologists, security solution auditors...

2.2 Operators in charge of cybers' incidents and/or crises management

The operators in charge of managing a cyber-attack are separated into teams with different and complementary skills and expertise : the CERT team (Computer Emergency Response Team), the CSIRT

ECCE 2024, October 08–11, 2024, Paris, France

ACM ISBN 979-8-4007-1824-3/24/10
https://doi.org/10.1145/3673805.3673839

team (Computer Security Incident Response Team) and the SOC team (Security Operation Center). These teams include operators specialized in specific fields, such as SOC analysts in charge of detecting anomalies in information system activity [4], Cyber Threat Intelligence (CTI) operators in charge of studying the attackers' Techniques Tactics and Procedures, forensic analysts in charge of analyzing the cyber-attack, and so on.

Depending on the organization, human and technical resources, those different teams are dispatched on the activities of monitoring, surveillance, detection, incident response and crisis management.

2.3 Service providers, trainers and partners.

While outsourcing services or calling on service provides is common in the field of entrepreneurship, it is particularly common in the field of cybersecurity or cyberattacks. This include security incident response service providers; security incident detection service providers; information system security support and consulting service providers; qualified information systems security audit service providers; and secure administration and maintenance service providers. The existence of these services providers means that companies can meet their cybersecurity needs without having to finance the necessary staff or services internally, which represents a significant human and financial cost. It also enables them to call on specific external skills not currently acquired, or too specific to be developed internally [3].

In addition to providing services, companies or institutions can be supported by specialist to develop Safety applications, but also for external trainers to train or sensitize their operators.

3 VULNERABILITIES : INHERENT SYSTEM BREACHES

3.1 Technical vulnerabilities

Vulnerabilities in the cybersecurity field are defined by NIST (National Institute of Standards and Technology) as « weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source »[5].

Vulnerabilities are inherent to an information system and represent flaws - more or less exploitable - in the system's security. Experts specializing in the search for vulnerabilities exist on both sides: cyber-defenders and cyber-attackers with different aims. There is a constant race to identify vulnerabilities, with cyber-defenders aiming to patch or monitor, and cyber-attackers to exploit them. On both sides, defenders and attackers, we're talking about cyber experts.

To illustrate our point, and without going into too much detail, the two categories of technical vulnerabilities are presented below.

3.1.1 «One-day »vulnerabilities. One-day vulnerabilities correspond to known vulnerabilities. Whenever possible, they may be accompanied by a patch, i.e., a corrective measure enabling the vulnerability to be eliminated.

For various reasons, patches may be communicated to the entities concerned, but they may not have integrated them into their systems (lack of time, resources, prioritization). Time windows may exist making opportunistic cyberattacks possible. Cyber-attacks can then occur between the communication of the vulnerability and its patching, and this can be a question of days or even hours.

There are also cases where there is no patch for a vulnerability, or where it cannot be transposed to the system in question. In such cases, it may be possible to implement protective measures other than patching, such as increased monitoring of the system to thwart or limit the spread of cyber-attacks, while waiting for a solution to be found.

3.1.2 «Zero-day »vulnerabilities. Unlike one-day vulnerabilities, zero-day vulnerabilities are unknown to their owners, but known to others. By definition, there is no patch for them.

If these are known only to malicious entities, they represent a real danger for the entities concerned, as they are not monitored as would have been in the case with a one-day vulnerability. This allows cyber-attackers to orchestrate a cyber-attack with the highest discretion.

3.1.3 Vulnerabilities score. Because vulnerabilities are inherent to a system, and the number of vulnerabilities could be great, there are different vulnerability scores to prioritize them and guide appropriate treatment (principally in prioritizing investment of human and technical resources).

In particular, there is a standardized international vulnerability assessment system: the Common Vulnerability Scoring System (CVSS). Ranging from 0 to 10, the CVSS calculates the criticality level of a vulnerability according to a basic, temporal, and environmental metric (10 corresponding to so-called critical vulnerabilities) [6]. The basic or innate metric assesses the vulnerability according to the complexity of its exploitation and its impact (in terms of data confidentiality, integrity, and availability). Environmental and temporal metrics are more concerned with the "life" of the vulnerability and its consequences, and the development of these exploits. CVSS is now in its 4th version. Unlike the 2nd version, with a grid of 3 total score levels (Low severity, Medium severity and High severity), the 3rd now has 5: None, Low, Medium, High, and Critical.

To complete the picture, there are also internal classifications for some companies.

3.2 Social engineering attacks: human vulnerability in question

Social engineering attacks are attacks that use human behavior to achieve their aims. The most common ones are phishing and spear phishing. These attacks enable users to carry out "malicious" actions on their own machines without their knowledge.

A phishing attack consists of sending a malicious e-mail with the look and feel of an "important" or enticing e-mail to users, asking them to provide personal data or to take urgent action. Users thinking they are reading legitimate mail, click on a link in the e-mail or an attachment, unwittingly planting malware and/or divulging personal information. [7].

Unlike phishing, spear phishing is sent to a specific group of users, or even a specific user. One example of spear phishing is the "President Fraud" technique, in which the attacker pretends to be the CEO, making the e-mail seems important or even urgent [2].

In both cases, phishing and spear phishing, the construction of the e-mail is crucial to the success of the attack, which therefore depends on the human reaction to the appearance of the e-mail and particularly the routine and emotional reaction.

3.3 Vulnerabilities market

To fight against the malicious exploitation of vulnerabilities, organizations rely on internal and external vulnerability researchers through - for example - bug bounty. These are events where developers reward the discovery of exploitable vulnerabilities if they can make a "Proof of concept".

People who discover vulnerabilities can either directly contact the developer outside bug bounty, use them for personal purposes, or sell them. In this way, a vulnerability market is created, in which vulnerabilities can be valued financially according to their novelty and the results of their exploitation. In addition, the price may vary according to whether the vulnerability is exclusive.

To conclude this section, we observe that the fields of cybersecurity are crossed by a great plurality of issues and a great complexity of challenges which impact directly the operationally level of cyber who have to continually develop new expertise in order to adapt to new technologies and to new tactics, techniques and procedures of cyber attackers. For our research we will focus on SOC cyber experts. First of all, to fully understand their activities, we need to understand the macro-organization of which they are a component and with which they work.

3.4 Cyber-attack market

As well as vulnerabilities, there is a real market of cyber-attack tools, mobilizing human, technical and organizational resources. For example, there are ransomware-as-a-service sales and denial-of-service (DoS) markets, where customers contact a cybercrime company and ask them to develop a tailor-made cyber-attack.

4 CYBERATTACKS : SOME KEY POINTS

As we saw in the previous section, vulnerabilities are intrinsic to information systems, and some of these can be exploited by cyber attackers. One of the key characteristics of cyber-attacks is the asymmetry of human and technical resources [2][4]. As Goodall, Lutters et Komlodi said: «defenders must continually identify and repair every vulnerability, while an attacker need only find a single unpatched vulnerability to exploit »[4]. These vulnerabilities can be exploited at any time on any type of information system. But why do cyber-attackers exploit these vulnerabilities ?

4.1 Cyber-attack objectives

Cyber-attacks can be divided into three categories: military, political and economic. In the case of cyber-attacks for military purposes, they are used as a cyberweapon to destabilize another power by destroying a military communications structure, for example. In the political arena, cyberattacks are orchestrated by foreign powers or hacktivist, who wish to make their position heard or cause destabilization. In the economic sphere, we could mention ransomware attacks or various phishing scams, for example.

Some cyberattacks can also be used in different fields, such as industrial spying attacks, which can be used in the economic field (stealing production plans or damaging infrastructures), the political field (spying on important people) and the military field (weapons innovation).

4.2 Being attacked without noticing

Being cyber-attacked doesn't necessarily mean being aware of it or understanding what's going on. While some cyberattacks have visible consequences (e.g. ransomware attacks), others are more discreet and are only discovered late and/or by chance (e.g. Stuxnet, which evolved in the information system for several years without being detected). As Hutchins, Clopperty and Amin point out: «The conventional incident response process initiates after our exploit phase, illustrating the self-fullling prophecy that defenders are inherently disadvantaged and inevitably too late»[8].

When a malicious intrusion is discovered, either through the detection of network anomalies or due to machine malfunctions, cyber experts need to understand as many elements of the attack as possible to contain it, stop it and gradually return to a nominal state, as far as possible. These experts must then be able to inform decision-makers of the entity, despite their (temporary or not) limited vision of the cyber-attack. [9].

4.3 Protecting these interests: a national and European obligation

Any entity with an information system can potentially be the victim of a cyber-attack. While a cyber-attack can have negative consequences for a company's image or economy, it can also have more serious consequences for certain entities. Faced with these risks, the French government has defined a list of critical infrastructures implying rigorous information system security constraints. The risk here is not necessarily in terms of the frequency of attacks, but in terms of their environmental or societal impact. This definition of high-risk points is also found at European level, with the European NIS directives defining Essential Service Operators (ESOs).

5 RESEARCH QUESTION

Faced with these latent threats, security measures are as much primary - to limit attacks - as secondary - to limit their propagation - and tertiary - to limit damage. The cybersecurity field is more concerned with system resilience than with complete system protection (an unattainable goal).Thus, to identify protective measures and characterize the properties of resilient organizations of information systems, it is necessary to analyze its different components, and more particularly the human activities mobilized through individual and collective knowledge and know-how.

5.1 The choice of SOC operators

After an initial exploration of the various cyber experts, the focus of this research was on SOC analysts (Security Operation Center analysts). Analysts are responsible for monitoring and detecting system intrusions. The ability to detect an anomaly in a complex, unstable system as early as possible, to avoid the installation or activation of a cyber-attack, is crucial to information system security. The sooner an intrusion is detected, the better the organization's chances of limiting the spread of the attack and/or limiting the damage.

During SOC analysts' activities, different sub-activities are mediated by different tools (at different levels of automation) with various cognitive requirements. For example, to detect an intrusion, analysts must implement detection rules based on their own knowledge in an automated system which analyzes the data sent to it according to the implemented rules [10]. As a result, the system sends an alert to the analyst, who must analyze it to determine whether it indicates an intrusion or not.

It's through the analysis of their activities that it will be possible to understand the issues of their work, their personal or collective organization strategies, and thus better equip them in their everyday work to allow the resilience of the entire IS.

5.2 Testing tools to characterize SOC analyst activity

Using an analysis tool used in the ergonomics of the activity, research is conducted on the surveillance, monitoring, detection, and response activities of SOC analysts. This research will help to better understand the technical resources available to SOC analysts and their use. It will also allow to analyze the distribution of work tasks in the SOC collective and the personal organization of each analyst to meet the monitoring needs but also for the performance of ancillary tasks. This will also lead us to identify the collaboration between the SOC team and other cyber experts, and their interactions with information system users [11].

Thus, we assume that surveillance activities in this specific area will require a specific definition on the one hand and refer to skills that are probably less studied on the other. Indeed, as described above, SOC experts have the activity of detecting anomalies from outside, caused by unwanted interaction, and not resulting from internal production processes. Furthermore, cyber-attackers either implement strategies to remain discreet, or have decided to attack. In the first case, it's difficult for SOC experts to detect anomalies, in the second case, it's too late and other strategies must be implemented to counter the effects of attack. Moreover, anomalies are commonplace which introduces another difficulty for SOC experts because it's necessary to be able to prioritize and decide quickly if an anomaly is related to a usual use, a failure or if it's a potential attack.

From a cognitive point of view, we will be led to question current models on monitoring, diagnosis and decision-making in complex dynamic environments developed in cognitive psychology and ergonomics to see how they can help to understand these activities in an environment of hostile attacks, and if necessary, adapt them if possible or seek to develop new ones.

6 METHODOLOGY AND PERSPECTIVE

A combination of qualitative research tools has been used and will continue to be mobilized as part of this research work. Exploratory interviews were conducted as part of an initial analysis which allowed us to better understand, for example the organization of the different cyber experts within the entity studied. In a second phase, focused on the analysis of the activity of SOC analysts, exploratory and systematic observations as well as explanatory interviews within the framework of self-confrontation will be organized. This work is completed by a literature review and critical analysis of internal documents.

6.1 Interviews and observations

To help us understand the entity's overall cybersecurity organization, we interviewed eleven operators involved in cybersecurity. They were chosen either based on their position in the functional organization structure (group leader, information systems security manager, etc.), or by opportunity during meetings at thematic events. This gave us a panel operator from each of the categories mentioned in part 1. This first phase enabled us to choose a study population (SOC analysts) according to the characteristics of their activities (cited in part 5) and for methodological practicality reasons. It also enabled us to build a cartography of the various expert collectives.

In the second phase, interviews and observation will be carried out with SOC operators to characterize their monitoring, surveillance, and detection activities. Two interview techniques will be used in this research: exploratory interviews and explicitation interviews [12].

The explicitation interviews will be semi-directive, guided by a characterization of the activities observed beforehand and seeking to have them explained by the operators concerned with a view to analyzing or even modeling individual and collective mechanisms of diagnosis, decision-making and action planning.

Different situations will be considered to analyze SOC activities, especially those considered crucial or difficult for cybersecurity. In an iterative manner, these observations in different situations of variability and criticality will participate in developing a systematic observation protocol capable of generalization and reproducibility [13].

6.2 Expected results

By the end of this first phase of research, we will seek to have a clearer picture of the activities of SOC analysts. This will involve: a description of the activities left to more or less automated digital tools; identification of the distribution of human resources; and a characterization of their monitoring and surveillance activities based on empirical findings.

7 CONCLUDING REMARKS

Despite the best efforts of cybersecurity experts, the system will always present flaws that cyber-attackers can exploit-if they can, either through design latent errors or misuse. [14]. Cybersecurity experts can, through monitoring, surveillance, and technical measures, limit the attack surface or its propagation. Moreover, a defensive strategy will force cyber-attackers to perfect their attacks more and more, requiring more resources to succeed [12], which will reduce the number of attacks, or at least the types of attackers.

Cyberdefense is therefore not just a matter of implementing measures to eliminate risk, but also of controlling it, in particular by detecting it early and implementing measures to limit its consequences. So, it's worth taking a closer look at the operators responsible for monitoring the network, who play a crucial role in defending information systems and in ensuring system resilience.

ACKNOWLEDGMENTS

This work is part of a research program focusing on cybersecurity in the Crisis Management and Human and Organizational Factors at EDF R&D

REFERENCES

[1] NIST. 2024. Cybersecurity. Glossary. Computer security resource center. https://csrc.nist.gov/glossary/term/cybersecurity

[2] Billois, G., Cougot, N., & Garnier, P. 2022. Cyberattaques: Les dessous d'une menace mondiale. Hachette.

[3] McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. 2015. Human Performance Factors in Cyber Security Forensic Analysis. Procedia Manufacturing, 3, 5301-5307.

[4] Goodall J. R., Lutters, G., W. & Komlodi, A. 2009. Developing Expertise for Network Intrusion Detection. Information Technology & People 22(2), Emerald Group Publishing Limited. p. 92-108

[5] NIST. 2024. Vulnerability. Glossary. Computer security resource center. https://csrc.nist.gov/glossary/term/vulnerability

[6] NIST (2023, November 6) *Vulnerability Metrics*. National vulnerability database. Information technologie Laboratory. NIST.

[7] Zhou, Y., Cui, X., Qu, W., & Ge, Y. 2022. The effect of automation trust tendency, system reliability and feedback on users' phishing detection. *Applied Ergonomics*, *102*, 103754. https://doi.org/10.1016/j.apergo.2022.103754

[8] Hutchins, E. M., Clopperty, M. J., Amin, M. R. 2011. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Proceedings of the 6th International Conference on Information Warfare and Security.

[9] Hettema, H. 2021.Rationality constraints in cyber defense : Incident handling, attribution and cyber threat intelligence. Computeur & Security, 109. p.1-1

[10] Thompson, R. S., Rantanen, E. M., & Yurcik, W. (2006). Network Intrusion Detection Cognitive Task Analysis : Textual and Visual Tool Usage and Recommendations. *Proceedings Of The Human Factors And Ergonomics Society Annual Meeting/Proceedings Of The Human Factors And Ergonomics Society Annual Meeting* , 50(5), 669-673.

[11] Forsythe, C., Silva, A., Stevens-Adams, S., & Bradshaw, J. (2013). Human Dimension in Cyber Operations Research and Development Priorities. In D. D. Schmorrow & C. M. Fidopiastis (Éds.), _Foundations of Augmented Cognition_ (Vol. 8027, p. 418-422). Springer Berlin Heidelberg

[12] Light, A. (1999). Vermersch's 'explicitation' interviewing technique used in analysing human-computer interaction.

[13] Norimatsu, H. 2008. *Les techniques d'observation en sciences humaines*. Paris: Armand Colin.

[14] Goodall, R., J., Lutters, G., W. & Komlodi, A. 2004. I Know My Network - Collaboration and Expertise in Intrusion Detection. p. 342-345. DOI: 10.1145/1031607.1031663