Bringing Socio-Technical Security Capabilities to Cyber Range Programs

Bilal Al Sabbagh[1]

[1] Stockholm University, DSV, 164 07 Kista, Sweden
bilal@dsv.su.se

Keywords: Cyber Range, Security Skills, Socio-Technical Approach, Cybersecurity Incident Response.

1 Introduction and Background

The increasing challenge in cybersecurity has been often tied to the advancement in technology development and its wide availability to end users. This development resulted in increasing opportunities of cybersecurity attacks in order to achieve gains at personal, organizational and national levels. The traditional approach to combat cybersecurity threats has mostly relied on continuous investment in security technologies. This approach has not effectively solved the problem as cybersecurity continue to constitute an increasing challenge. In fact, research and industry reports now confirm that technical controls alone are not sufficient to control cybersecurity threats [1]. A new perspective to understand cybersecurity challenge comes from the critical shortage in cybersecurity talents and skills. The cybersecurity job report from Cyber Adventures estimates a 3.5 million unfilled cybersecurity positions by the year 2021 [2]. This shortage is predicted to cost the world about $6 Trillions annual loss by year 2021 due to the rise in Cybercrimes. The key findings from ISACA report on state of cybersecurity report for the year 2019 highlights the lack of cybersecurity professionals who have the right skills and that the skills gap in cybersecurity will continue to increase in the coming years [3].

2 Developing Holistic Cybersecurity Skills

The mindset and hands-on experience of cybersecurity practitioners are focal during their skills development. Traditional cybersecurity training programs can't alone develop the skills expected to deal with cybersecurity threats during real situations before first exposing practitioners to artificial but rather empirical attacks scenarios. Cyber range is a virtual environment used to simulate real-life cybersecurity attacks and response scenarios. This experience is used to develop the skills of cybersecurity practitioners. The cybersecurity range can also be customized to emulate an organization infrastructure and its security risks and priorities. This would deliver contextual experience about what it takes to manage cybersecurity threats.

However, one important capability we propose to bring to cyber range programs is the ability to develop a holistic security mindset for security practitioners so they are able to consider the socio-technical characteristics of cybersecurity incident response. This poster proposes deploying two artefacts developed recently during the author PhD research focusing on developing a socio-technical approach in cybersecurity incident response [1]. The two artefacts are named Hyper Interactive Intelligent Pedagogical Platform for Security Awareness, and Socio-Technical Security Information and Event Management System (ST-SIEM).

3 Hyper Interactive Intelligent Pedagogical Platform for Security Awareness

This platform is designed to improve individual security awareness and learned lessons from cybersecurity incidents. The platform consists of five different frames. Each frame contains a different medium for presenting information: Hypervideo, Wiki, Frequently Asked Questions (FAQ), PowerPoint Presentation and a Conversational Agent (Chat bot). The knowledge provided from a cyber range program can be presented in these different formats to take into consideration the different learning styles of cybersecurity practitioners when developing their cybersecurity skills [4]. The desired outcome is improving the learning experience of practitioners. Figure 1 visualizes how the five different mediums are presented to the user.

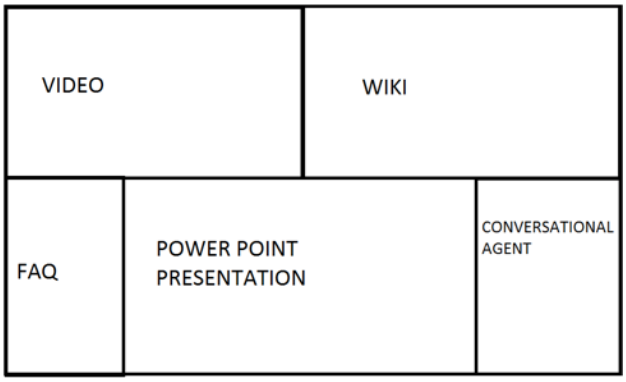

Fig. 1. Hyper Interactive Intelligent Pedagogical Platform with five frames

4 Socio-Technical Security Information and Event Management System (ST-SIEM)

ST-SIEM is an artefact designed to improve the context of actionable security information before they are processed by security analysts within an organization. The objective is to improve the efficacy of handling security incidents within an organization. A general existing limitation in actionable security information they are not customized to consider the security culture of the organization supposed to act on these incidents. ST-SIEM handles this limitation by tailoring security information context to consider the organization security spending mental model – how an organization prioritize security spending on different security controls: deter, detect, prevent, correct and recover. Moreover, ST-SIEM adapts the risk factor of security information based on the organization risk escalation maturity level measured and registered in the system. Finally, ST-SIEM associate social taxonomies with impact factor based on the business background (risks and priorities) of the organization. ST-SIEM was developed as a prototype and integrated with an open source SIEM tool. Figure 2 depicts the architecture of ST-SIEM including the socio-technical correlation engine which correlates the technical attributes of the security incident with the social attributes created based on the modeling of each organization security culture. Figure 3 depicts the defined roles to operate ST-SIEM artifact including the interaction between these different roles.

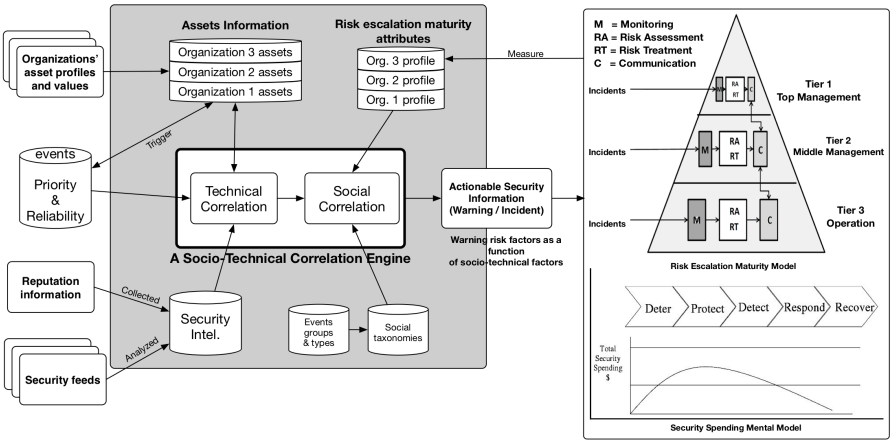

Fig. 2. Socio-Technical SIEM Architecture

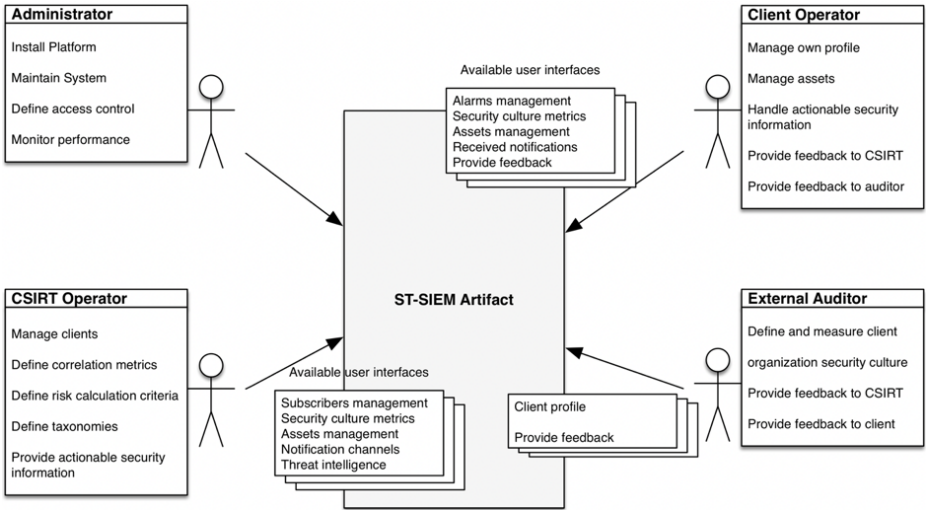

Fig. 3. Interactions between ST-SIEM Defined Roles

References

1. Al Sabbagh, B. 'Cybersecurity Incident Response : A Socio-Technical Approach', PhD dissertation, Department of Computer and Systems Sciences, Stockholm University, Stockholm, 2019.
2. Cybersecurity Jobs Report 2018-2021, https://cybersecurityventures.com/jobs/, last accessed 2019/05/22.
3. ISACA STATE OF CYBERSECURITY 2019, https://cybersecurity.isaca.org/state-of-cybersecurity, last accessed 2019/05/22.
4. Felder, M. R. and Silverman, K. L.: Learning and Teaching Styles in Engineering. Journal of Engineering Education 78(7), 674-681 (1988).

