Integrating Security Behavior into Attack Simulations

Simon Hacks
Ismail Butun
Robert Lagerström
{shacks|butun|robertl}@kth.se
Division of Network and Systems Engineering
KTH Royal Institute of Technology
Stockholm, Sweden

Andrei Buhaiu
andrei.buhaiu@student.fhs.se
Swedish Defence University
Stockholm, Sweden

Anna Georgiadou
Ariadni Michalitsi - Psarrou
{ageorgiadou|amichal}@epu.ntua.gr
Decision Support Systems Laboratory
National Technical University of Athens
Athens, Greece

Abstract

The increase of cyber-attacks raised security concerns for critical assets worldwide in the last decade. Leading to more efforts spent towards increasing the cyber security among companies and countries. For the sake of enhancing cyber security, representation and testing of attacks have prime importance in understanding system vulnerabilities. One of the available tools for simulating attacks on systems is the Meta Attack Language (MAL), which allows representing the effects of certain cyber-attacks. However, only understanding the component vulnerabilities is not enough in securing enterprise systems. Another important factor is the 'human', which constitutes the biggest 'insider threat'. For this, Security Behavior Analysis (SBA) helps understanding which system components that might be directly affected by the 'human'. As such, in this work, the authors present an approach for integrating user actions, so called "security behavior", by mapping SBA to a MAL-based language through MITRE ATT&CK techniques.

CCS Concepts: • **Security and privacy → Domain-specific security and privacy architectures**.

Keywords: Security Behavior, Attack Simulations, Integration

ACM Reference Format:
Simon Hacks, Ismail Butun, Robert Lagerström, Andrei Buhaiu, Anna Georgiadou, and Ariadni Michalitsi - Psarrou. 2021. Integrating Security Behavior into Attack Simulations. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3465481.3470475

1 Introduction

Our modern society relies more and more on the continuous provision of electrical power. Most of the critical infrastructure that keeps our lives running depends on it [38]. At the same time, deliberate disruptions of electrical power and energy systems [10, 55] by attackers exploiting the controls of power grids, energy providers, and other critical infrastructure happens [42, 64]. These attacks can result in real-world catastrophic physical damage, like major power outages or city-wide disruptions of critical infrastructure [10, 55, 58]. One counter measure to address these threats are assessments of the power domain's cyber security.

To assess the cyber security of a domain and its single entities, one has to identify vulnerabilities, security-relevant parts must be understood, and potential attacks should be identified [47]. Hence, the use of attack simulations based on system architecture models have been proposed (e.g., [11, 28]). These approaches use a model of a system and simulate cyber-attacks to identify possible penetration points and attack paths. Consequently, the security assessor can focus on the collection of the information about the system and does not need to have specific security knowledge.

These previously presented approaches have all the same shortcoming that they rely on a static implementation of the model used. Therefore, the use of MAL (the Meta Attack Language) [34] was proposed. This framework for DSLs defines which information about a system is required and specifies the generic attack logic. Then, MAL is used to define concrete DSLs, such as coreLang [35] or powerLang [25], which represent general domain concepts. Organization specific aspects like the security behavior of the employees will have influence on the simulation results, but this is not reflected on the domain level. Classically, this kind of information is collected by means of surveys. This raises our research question on:

RQ: *How can the results of security behavior assessments be integrated into attack simulations?*

To answer this question, we explain the context of this research in Section 2.1. Following, we introduce the tool

ARES 2021, August 17–20, 2021, Vienna, Austria

ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3470475

to gather information on the security behavior of organization's employees (Section 2.2), which is then imported into a tool which performs attack simulations (Section 2.3). Subsequently, we present the mapping to transform the information from one tool to the other by means of the MITRE ATT&CK matrix (Section 3). Then, we illustrate the influence of security behavior in Section 4 and discuss our findings (Section 5), before we present related work (Section 6) and conclude our work in Section 7.

2 Background

Following, we illustrate the background of our research. First, we introduce the EnergyShield project, in which our research takes place and, thus, frames the objectives towards our solution. Then, we present the Security Behavior Analysis (SBA) tool that is used in our project to assess the security behavior of organization's employees. Finally, we explain the Vulnerability Assessment (VA) tool that takes the information of the SBA and performs attack simulations to determine choke points in the organization's system architecture.

2.1 EnergyShield

The EnergyShield project[1] [13] is funded within Horizon 2020 and aims to develop an integrated toolkit covering the complete Electrical Power and Energy Systems (EPES) value chain ranging from generation, over transmission service operators (TSO) and distribution service operators (DSO), to the consumer. The toolkit combines novel security tools from leading European technology vendors and is composed of the latest technologies for vulnerability assessment (automated threat modeling), monitoring & protection (anomaly detection and DDoS mitigation), and learning & sharing (security information and event management).

One of the objectives of the project, which we address in this research, demands the integration of the different tools with each other [13]. Accordingly, an overarching architecture has been designed [14] that technically connects the different tools to each other. Therefore, the different tools can announce if they have created new insights and the other tools can react. For example, SBA could announce that new results on the security behavior are available, which will trigger VA to get this information and perform updated attack simulations.

However, this overarching architecture does not determine how the concrete exchange of data between the tools can be achieved. Therefore, we suggest a conceptual mapping of the information collected by SBA to the information used in VA.

2.2 Security Behavior Analysis

The Security Behavior Analysis (**SBA**) Tool has its foundations in the **cyber-security culture framework**, presented in 2020, suggesting a multi-dimensional approach towards evaluating the security culture readiness of an organization [20]. Its model bridges the scientific, humanitarian approach [2, 9, 30, 40, 41, 46, 48, 53, 57, 61, 62, 65] with the security professional, technological approach [1, 12, 31–33, 56] towards information security. Using two distinct **levels**, *organizational* and *individual*, it co-examines the security factors formulating the external and internal conditions under which individuals perform within a working reality. Levels are analyzed into **dimensions**, as presented in Figure 1, which are further organized into **domains** reaching down to a measurable level of analysis.

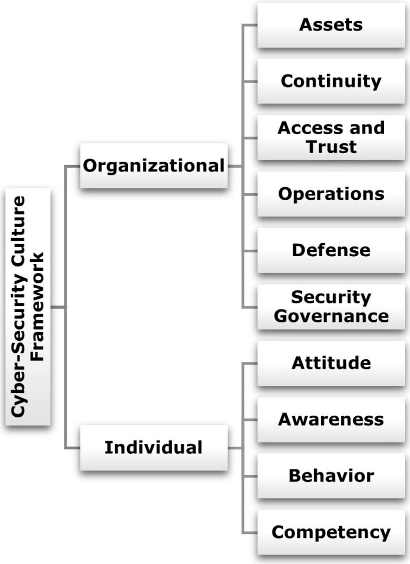


Figure 1. Cyber-Security Culture Framework - Levels and Dimensions

The cyber-security culture framework introduces an evaluation methodology based on assessment iterations called *campaigns*. Following the 4W1H methodology [4], campaigns are meant to address the following questions:

- *What* dimensions and domains, in other words, what security facets shall be evaluated?
- *Who* shall the campaign be targeting and assessing? Which individuals shall participate in the iteration?
- *When* shall it take place?
- *Where* shall the campaign be focusing on? The primary goal of the assessment iteration.
- *How* shall the security indicators be assessed? Using what kind of methods and techniques?

Depending on the application business domain, various scoring algorithms were also recommended starting from simple weighted average/sum approaches and leveraging to more sophisticated multi-criteria methodologies [3, 6, 52, 59].

The Security Behavior Analysis Tool, using a variety of assessment techniques, such as surveys, tests, serious games

[1] https://energy-shield.eu/

and simulations, empowers users to evaluate the cyber-security culture readiness of their organizations while underlying underestimated security facets. Identified weaknesses are further elaborated and correlated with possible cyber-threats. As a final step, the tool offers indicative mitigation and training program suggestions actively contributing to the overall security status improvement.

A number of targeted applications of the framework have already been realized during the COVID-19 pandemic [16, 19] demonstrating both the evaluation methodology and the significance of its findings.

2.3 Vulnerability Assessment

The VA tool depends on two components: on the one hand, the tool securiCAD that facilitates modeling of concrete architectures and perform attack simulations on them. On the other hand, icsLang based on the MAL framework, which codifies the meta model used in securiCAD. To bring the information of the SBA and VA together, a mapping from SBA's levels and dimensions (cf. figure 1) to icsLang is necessary. This mapping focuses on the general relation between these two concepts. However, for each organization there are concrete values and a concrete threat model that are used for the attack simulations. Obviously, these are different for every organization. Consequently, we focus on the mapping between SBA and icsLang.

2.3.1 securiCAD. securiCAD [11] by foreseeti[2] is a commercial threat modeling and attack simulation tool. foreseeti is a spin-off company from the Software Systems Architecture & Security group at KTH Royal Institute of Technology, Stockholm Sweden and thus the securiCAD tool is developed based on many years of scientific achievements.

The unique idea behind the tool is to combine traditional system modeling with security analysis by merging threat modeling and attack simulations. The models are similar to UML models and the simulations are based on Bayesian networks and Monte-Carlo simulations. The tool is non-intrusive, but the models can be automatically populated using data sources like vulnerability or network scanners.

In the tool, users can both assess the current security posture of a system and test what-if scenarios by creating new models or making changes to an existing model. There are several reports and metrics produced as output from securiCAD e.g., scores related to confidentiality, integrity, availability, or time-to-compromise.

There are currently three versions of the tool; 1) securiCAD Professional – for single users, 2) securiCAD Enterprise – a multi-user environment with automatic modeling capabilities for continuous risk assessment, and 3) securiCAD Vanguard – a fully automatic tool for cloud environments. The VA tool is based on the securiCAD Enterprise platform with specific MAL-support capabilities.

2.3.2 icsLang. securiCAD relies on MAL as underlying meta model, which is a language framework that combines probabilistic attack and defense graphs with object-oriented modeling. Based on MAL different Domain-Specific Languages (DSLs) can be designed that define the generic attack logic needed for threat models in a certain domain.

To create a MAL-based language, one needs to identify all relevant assets and their associations. An asset is comprised of multiple attack steps, representing real threats, which can lead to (represented by "−>") another attack step. An attack step is either of the type OR (represented by "|") or AND (represented by "&"). For OR attack steps, an attacker needs to compromise at least one parent, while all its parent attack steps must be compromised for an AND attack step. Additionally, there are defenses (represented by "#") that might hinder an attacker from compromising related attack steps. Finally, the object oriented concept of inheritance between assets is implemented in MAL.

In Appendix A Listing 1, we present an example of a MAL-based language. It contains four assets with their corresponding attack steps. The `Host` asset contains a *connect* attack step, which is an OR attack step, while *access* is an AND attack step. The -> symbol denotes the connected next attack steps. For example, if an attacker performs *phish* on the `User`, it is possible to reach *obtain* on the associated `Password` and as a result finally perform *authenticate* on the associated `Host`. In the last lines of the example the `associations` between the assets are defined. For more details, we refer to the original paper [34].

Based on MAL, we proposed icsLang initially in the context of powerLang [25], a language that composes different existing languages to cover all demands of the power domain. icsLang[3] is inspired by the ATT&CK Matrix for ICS[4] and based on coreLang [35]. The main asset is the `IcsAsset`, which represents common behavior. To enable all assets to communicate with each other, we created a connection to `IcsNetwork`. The rest of the language is structured along the MITRE ATT&CK categories level 2 (supervisory control), and level 1 (control network).

Level 2 includes the functions involved in monitoring and controlling physical processes and the general deployment of systems. The central asset on this layer is the `ControlServer` which operates the `Controller` on level 1 and also computes their output [63]. Level 1 includes the functions involved in sensing and manipulating physical processes. This is usually done by `Controller`, which communicates through an `IOServer` with LAN applications and the field equipment monitored and controlled by the control system applications. An overview of the entire language can be found in Figure 2.

[2] https://foreseeti.com/

[3] https://github.com/mal-lang/icsLang

[4] https://collaborate.mitre.org/attackics/

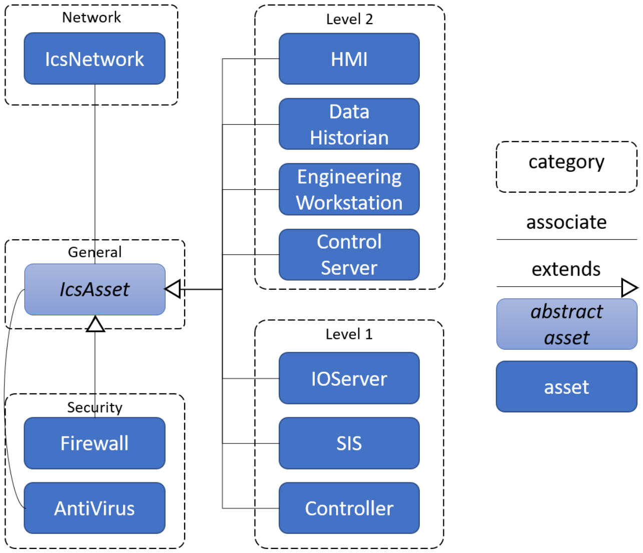


Figure 2. Overview of icsLang [25].

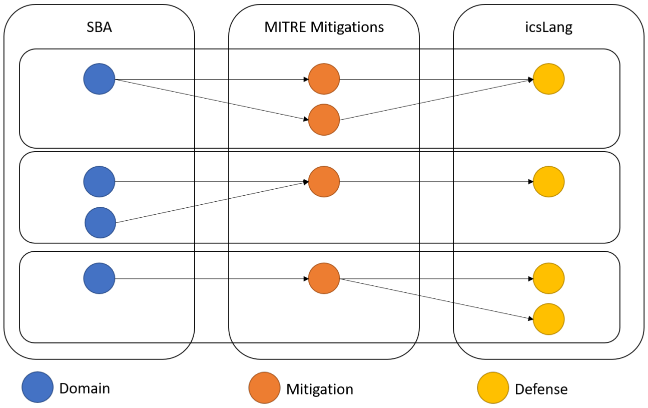


Figure 3. Exemplary mappings from SBA over MITRE ATT&CK to icsLang.

3 Mapping

Hitherto, we illustrated why adding security behavior information to attack simulations is beneficial, presented details about the SBA tool providing this information, and the VA tool performing the attack simulations. Next, we will illustrate the mapping from SBA to VA. Therefore, we will rely on the MITRE ATT&CK matrix.

Accordingly, the mapping follows a two-step process (cf. Figure 3), while formally both steps are equivalent. Firstly, we map certain SBA values to mitigations in MITRE ATT&CK. Here, we differentiate three different strategies for the mapping:

- **One-to-one:** There is one value in SBA that can be mapped to one mitigation in ATT&CK. In this case, the value will be taken unchanged.
- **One-to-many:** There is one value in SBA that can be mapped to many mitigations in ATT&CK. In this case, the value will be taken unchanged for all mitigations.
- **Many-to-one:** There are multiple values in SBA that are mapped to one mitigation in ATT&CK. In this case, we consider the worst-case scenario and choose the minimal value that the mitigation will be successful.

Secondly, we map the derived values of the mitigations to certain mitigations in icsLang. Therefore, we apply the same strategies as stated before. Next, we detail the mapping from and to MITRE ATT&CK for SBA and icsLang respectively.

3.1 Security Behavior Analysis to MITRE ATT&CK

The SBA results offer an overall understanding of an enterprise's cyber-security culture status, analyzing it into *individual* and *organizational* metrics. The next logical step of such an assessment was to identify and highlight the **cyber-threats** the organization is vulnerable against.

In accordance with the security factors, cyber-threats are also divided into *individual* oriented and *organizational* facilitated. The Management and Education of the Risk of Insider Threat (**MERIT**) model has been embraced by the vast majority of the scientific community [22, 23, 36, 43, 50, 51] attempting to comprehend and prevent the insider threat directly related to the first cyber-threat category. The second category refers to the external adversary tactics and techniques presented in detail in the **MITRE ATT&CK** framework. The latter has served numerous research attempts aiming to understand, detect, and defend against the external organizational perils [15, 26, 29, 37, 45, 49, 54].

A transition from the cyber-security culture framework domains to the MERIT model has already been documented [18]. Similarly, another effort to bridge the cyber-security culture model with the hybrid MITRE ATT&CK for Enterprise and Industrial Control Systems (ICS) matrix has recently been published [17]. The hybrid model was selected due to its suitability and applicability to the EPES sector, the primary application domain of SBA.

Figure 4 provides a high-level overview of the relation of the cyber-security culture framework to the hybrid MITRE ATT&CK model. In particular, it demonstrates how starting from the assessment of specific security dimensions and domains of the cyber-security culture framework, one may identify partially implemented or not fulfilled MITRE ATT&CK mitigations. Then, moving along the MITRE ATT&CK model, one may identify possible techniques and tactics that adversaries may use to take advantage of the organization's deficiencies. By analyzing the results of the assessment campaigns conducted to evaluate the organization's security culture, the organization can end up being fully aware of the cyber-threats it is vulnerable to and their mitigations.

Since there is a many-to-many relationship between the cyber-security culture framework domains and the MITRE

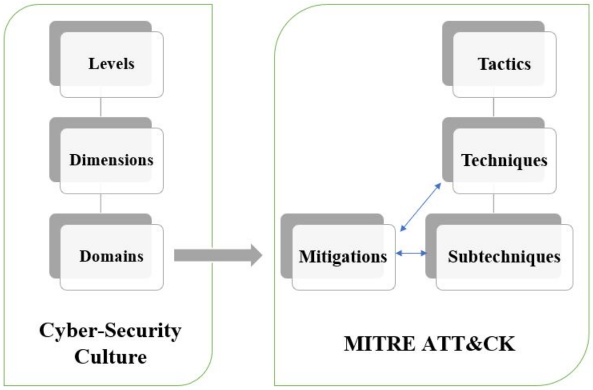


Figure 4. Cyber-Security Culture Framework related to MITRE ATT&CK Model

ATT&CK mitigations, a low-rated SBA security domain may indicate more than one affected mitigation. On the other hand, one mitigation may be connected to more than one domain, so failing in one domain does not necessarily mean underdeveloped mitigation techniques towards specific cyber-threats. To evaluate the cyber-risks an organization is up against and the successful implementation of a number of suggested mitigations, the joint evaluation of several security domains of the framework should be considered.

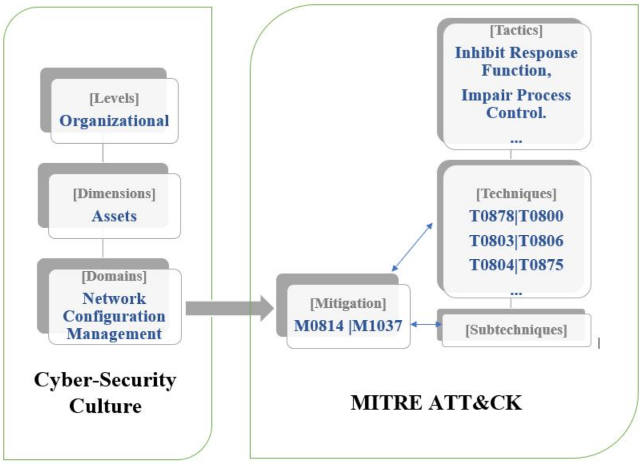


Figure 5. Example demonstrating relation of the Cyber-Security Culture Framework and the MITRE ATT&CK Model

To make it more explicit, Figure 5 depicts an example on top of Figure 4, on how the evaluation of a specific security domain can unravel the attackers' techniques to which the organization is potentially exposed, as well as the countermeasures, i.e. mitigations, that should be implemented to be protected against these perils. According to this example, the organization in question has assessed the *"Assets"* dimension of the organizational level. Precisely, low assessment results have been deduced for the *"Network Configuration Management"* domain. Based on the mapping with the hybrid MITRE ATT&CK matrix, the mitigations *M0814* - *"Static Network Configuration"* and *M1037* -*"Filter Network Traffic"* are possibly not adequately fulfilled, revealing alongside the techniques that need to be suppressed by these mitigations.

The mapping presented in Figure 5 additionally indicates that *M1037* is linked to the *"Network Infrastructure Management"* domain as well. Based on that, the organization now knows that a new campaign should be designed using the SBA tool to further assess this domain and size up the organization's exposure concerning mitigation *M1037.*

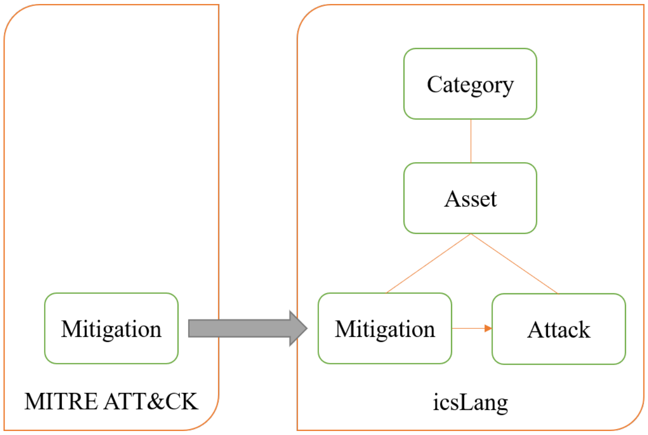


Figure 6. icsLang related to MITRE ATT&CK Model

3.2 MITRE ATT&CK to Attack Simulations

As indicated before, icsLang enables the modeling of organizations' operational technology (OT) environments. To validate these capabilities, we are continuously ensuring that the techniques found in MITRE ATT&CK ICS can be modeled with icsLang. Consequently, we prepared a set of models that illustrate those techniques and respective mitigations.

In MAL-based languages, assets include two fundamental building blocks: attacks and mitigations. Attacks represent the steps that an attacker performs on the asset, while mitigations represent efforts taken by the targeted organization to hinder the attacker to perform certain attacks. As SBA assesses the security behavior of an organization under attack and provides no information on the attacker, we solely map SBA's findings to mitigations in icsLang (cf. Figure 6).

Actually, we identified eleven different defenses in icsLang that can benefit from the SBA (cf. Appendix B). Additionally, we found eight domains that currently are not reflected in icsLang. For some of them, we plan to implement them in future (i.e., on the "individual" level). However, we are not going to implement each missing aspect. For example, "Risk assessment" does not reflect on aspects that we classically relate to the concept of attack simulations as it does not have any influence on the effectiveness of mitigations.

Hitherto, we have discussed the information flow from SBA to icsLang. However, we have not discussed how this information relates to existing information persisted in the language. Consider that a mitigation has a probability of $0 \leq X \leq 1$ to be effective, as determined for example following the method of Xiong et al. [67]. Now, the assessment of SBA has revealed that in a certain domain, that can be mapped to the mitigation according to the description at the beginning of this section, the behavior is valued with $0 \leq Y \leq 1$. As a value of 1 means that the effectiveness of mitigations is not negatively influenced and a value of 0 means that all related mitigations are completely corrupted. Consequently, we calculate the new effectiveness, $0 \leq X' \leq 1$, of the mitigation by simply multiplying these two values:

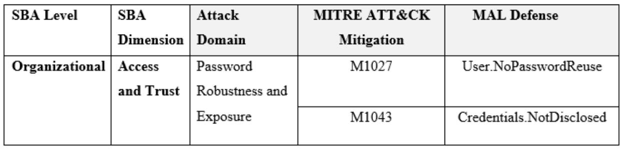
$$X' = X \times Y. \qquad (1)$$

4 Demonstration

In this section, we demonstrate one iterative simulation of the SBA and VA tools in order to present how positive changes in the social behavior of the employees in a company are reflected in the overall vulnerability of that company's assets.

The assessment of vulnerabilities prior to certain serious cyber attacks has prime importance not only for keeping the provided services running but also for the overall safety and integrity of the infrastructure being used [7, 8]. As such, demonstrating the vulnerabilities of the system under investigation via real-world like simulation is always beneficial for the security experts.

We are implementing a *1:n:n* (SBA-Domain:MITRE ATT&CK mitigation:VA-defense) case of “Password Robustness and Exposure” attack in which *n* is ‘2’ here as shown in Fig 7.



SBA Level	SBA Dimension	Attack Domain	MITRE ATT&CK Mitigation	MAL Defense
Organizational	Access and Trust	Password Robustness and Exposure	M1027	User.NoPasswordReuse
			M1043	Credentials.NotDisclosed

Figure 7. Mapping of the “Password Robustness and Exposure” attack.

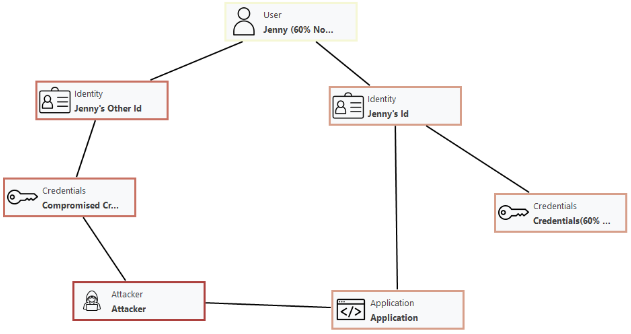


Figure 8. securiCAD model for the “Password Robustness and Exposure” attack.

Fig 8 represents the securiCAD model for the “Password Robustness and Exposure” attack. As shown, user Jenny's credentials and therefore the information available via the application are at stake.

Fig. 9 demonstrates the path of an attacker taken during the “Password Robustness and Exposure” attack. It also includes various defenses at the exact location on the path of the attack where they hinder the attacker's efforts. Here, by using the compromised credentials (via credential theft), the attacker accesses the application of interest via Jenny's ID and password with 36% probability (see Fig 10). Prevention mechanisms have been shown to be somewhat effective, depending on the user's ‘good’ social behavior: no password reuse and not disclosing the password.

In the first iteration, we considered the result of the SBA tool to be 60%, meaning that the employees are 60% knowledgeable on this specific cyber-security asset. This is reflected in the 60% chance on each defense associated with the MITRE ATT&CK mitigations (M1027-Password Policies and M1043-Credential Access Protection) and their corresponding defenses in MAL (‘User.NoPasswordReuse’ and ‘Credentials.NotDisclosed’).

As shown in Fig. 10, combined probabilities of the 60% defenses give a 36% chance of defending ($0.6 * 0.6 = 0.36$), which is reflected as 64% ($1.0 - 0.36 = 0.64$) chance of an attack to be successful.

Within this demonstration, we will investigate the effect of a positive change (0.2 which is equivalent to 20% enhancement considering the scoring margins: [0.0 - 1.0]) in the associated domain (level/dimension/domain) of the SBA tool on the vulnerability of the network/system being investigated. This positive change is assumed to be acquired by the SBA tool implementer/vendor at the pilot location by executing social-behavior related campaigns and training to improve the overall cyber-security knowledge of the employees on the specific domain that is being considered.

In the second iteration, after a successful training of the employees, we have considered the result of the SBA tool on the asset of interest to be enhanced to 80%, meaning that the employees of interest are now 80% knowledgeable on this specific cyber-security asset. This is now reflected as a 80% chance on each defense associated with the MITRE ATT&CK mitigations (M1027-Password Policies and M1043-Credential Access Protection) and their corresponding defenses in MAL (‘User.NoPasswordReuse’ and ‘Credentials.NotDisclosed’).

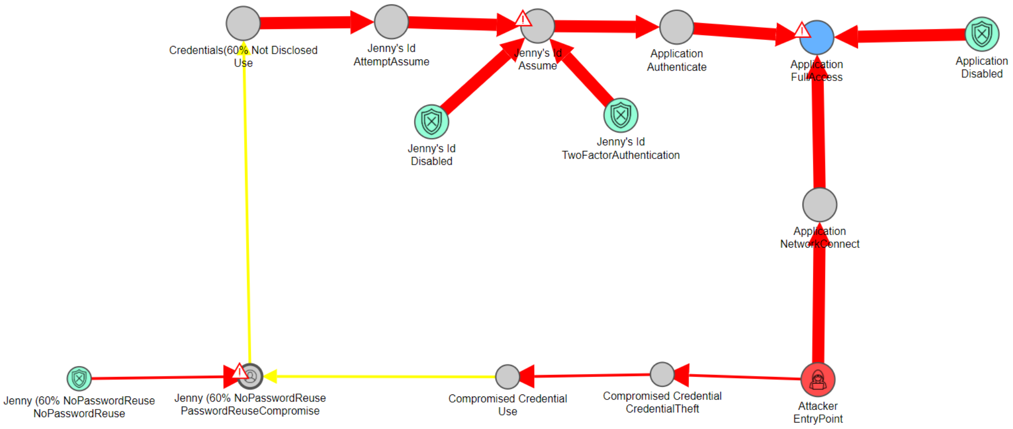


Figure 9. Path of an attacker during the "Password Robustness and Exposure" attack.

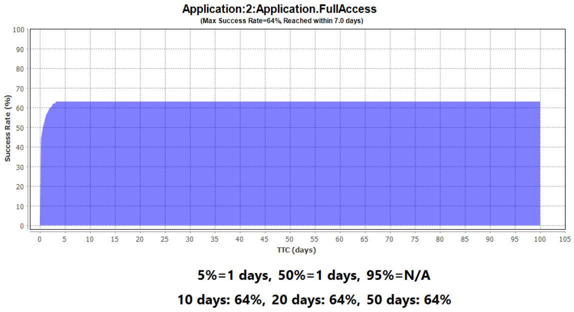


Figure 10. Result of Iteration #1.

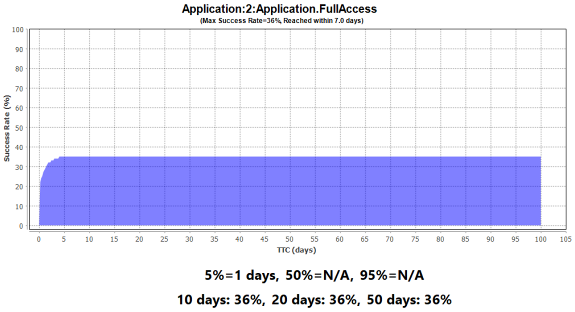


Figure 11. Result of Iteration #2.

As shown in Fig 11, combined probabilities of the 80% defenses give a 64% chance of defending ($0.8 * 0.8 = 0.64$), which is reflected as 36% ($1.0 - 0.64 = 0.36$) chance of an attack to be successful.

We have shown that positive changes in the outputs of the SBA tool are considered to have a positive impact on the overall protection of the system being investigated, which is proven by simple yet effective simulations.

5 Discussion

Before, we have presented how we include the outcomes of SBA into VA. However, our research includes several threats to validity that we discuss following:

Firstly, we rely in our mapping on the relation of two different artefacts (SBA and icsLang) to MITRE ATT&CK. This is problematic twice: On the one hand, the mapping includes two subjective decisions (from SBA to MITRE ATT&CK and from MITRE ATT&CK to icsLang) and other researchers might have decided differently. To overcome this shortcoming, in each decision several researchers were involved, and the results were discussed with practitioners in regular meetings. On the other hand, the choice of MITRE ATT&CK can be criticized. As MITRE ATT&CK is very popular among security professionals, it develops more and more into a de facto standard. Furthermore, it is already used by both research teams involved, which makes it a suitable approach. Another point of critique could be to use not an additional mapping between SBA and icsLang at all. Clearly, mapping SBA to icsLang would reduce the bias introduced by two subjective mappings, but SBA and icsLang need to be completely understood by both research teams involved at the same time. As indicated before, both teams have already related their artefacts to MITRE. Thus, we take the trade-off for less effort.

Secondly, we follow a very simplistic approach to determine the final values considered for our computations in the attack simulations. Basically, we always opt for the worst value by arguing that in security aspects the weakest link in the chain should determine the overall security. Additionally, this is also in line with the principle of Occam's razor [60], which recommends to stick to the simple instead of the complicated. However, if future applications of our research reveal the demand for more advanced determination of the values, our approach can be extended as desired.

Thirdly, we did not conduct efforts to generalize our findings beyond the presented application. This can be explained by the concrete demands formulated by the EnergyShield project as our research has to serve these. Moreover, the underlying SBA and attack simulations are very concrete concepts and generalization is challenging. Nonetheless for the mapping to icsLang, a certain degree of generalization is built in as icsLang is built upon coreLang that represents a broader domain than OT. Additionally, many of the MITRE ATT&CK mitigations are applicable to the enterprise and the ICS domain. Consequently, the SBA results could be used in other settings based on coreLang as well.

Fourthly, we solely demonstrated our approach. Our bigger evaluation in a real-world environment has not been conducted yet. However, the evaluation in a bigger setting is scheduled. In that evaluation, SBA and VA will be applied in EPES organizations, where employees will answer the questionnaire of SBA, the gathered information will be transmitted to VA, and finally attack simulations will be conducted based on a model of their IT architecture.

6 Related Work

To the best of our knowledge, there exists no approach to combine security behavior analysis with attack simulations. However, different efforts have been taken to unite security assessments with enterprise modeling. E.g., Grandry et al. [21] propose a mapping for information system security risk management to ArchiMate an enterprise architecture modeling language. Band et al. [5] extend this work by demonstrating the linkage between ArchiMate and other risk concepts.

Generally, EA models are a popular input for security assessments. Exemplary, Mathew et al. [44] propose a mapping from ArchiMate to the German BSI Grundschutz an implementation of ISO 27001. Then, they apply their approach to real-world data of an insurance company. Similarly, Xiong et al. [66] use EA repositories to foresee the effects of failing components on the entire architecture. They propose to use Design Structure Matrix to also assess hidden structures in agile contexts. A step further is taken by Hacks et al. [24], who propose a method to automatically create a MAL language based on an EA model. Then, they use the language to perform the attack simulation for power plants and substations and demonstrate the method with remodeling the attack on the Ukraine power grid from 2015.

Other than that, Holm et al. [27] created a mapping of the NeXpose Scanner to ArchiMate to generate EA models using the data collected by the scanner. Later on, these models are used as foundation for attack simulations used in securiCAD [28]. König et al. [39] conducted a mapping of the Substation Configuration Language (SCL) to ArchiMate to better enable the stakeholders to understand the Substation Automation (SA) system and its architecture.

All these approaches have in common that they focus on technical aspects as those are easier to grasp automatically. In this article, we do the next step by also considering the human aspects. Consequently, the attack simulations for each organization become more accurate and provide better insights how to improve security.

7 Conclusion

With this work, we wanted to provide an answer to the question how security behavior findings can be integrated into attack simulations. Therefore, we proposed a two-stepped mapping. First, we suggest a mapping from SBA, that provides organization specific knowledge about security behavior, to MITRE ATT&CK. This is followed by a mapping from MITRE ATT&CK to icsLang, the meta language used in securiCAD. Finally, we demonstrate the applied mapping on an exemplary case.

These mappings enable practitioners to incorporate knowledge about the security behavior within their organization into their attack simulations. Doing so, the attack simulations will produce more accurate results that are closer to the reality in the organization. Thus, countermeasures can be determined that are suited to the demands of the organization. Theoreticians benefit from our mapping, as we rely on MITRE ATT&CK. If they want to integrate their concepts with ours, they do not need to understand our concepts completely, but can rely on an established and popular concept.

Beyond the presented approach, there is still room for improvement. As for the Security Behavior Analysis Tool, cyber-threat identification using the MITRE ATT&CK hybrid matrix shall be applied, validated, and verified on the ongoing pilot applications. Based on the results, findings and user feedback, further correlation of the cyber-security culture framework with other widely recognized cyber-threat models shall be examined. Furthermore, expansion of the current MITRE ATT&CK relation using the rest of its versions might also be investigated and evaluated to enrich the application of the cyber-security culture framework to other business domains.

For securiCAD and icsLang, a further integration with the other tools in the EnergyShield project is planned as well as the evaluation in the pilots. With regards to the mapping itself, more advanced aggregation methods could be researched if the evaluation will show that the practitioners desire them. Finally, we concentrated on the behavior of the defenders. However, it might be possible to consider also different attackers based on the profile of the organization under attack. Hence, we plan to integrate this aspect in future.

Acknowledgments

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907.

References

[1] Information Systems Audit and Control Association (isaca). 2012. COBIT5: A Business Framework for the Governance and Management of Enterprise IT. (2012).

[2] S. Aurigemma and R. Panko. 2012. A Composite Framework for Behavioral Compliance with Information Security Policies. In *45th Hawaii International Conference on Systems Sciences*. Maui, Hawaii.

[3] M. Présent and B. Roy. 1986. and D. *ilhol, "A programming method for determining which Paris metro stations should be renovated," European Journal of Operational Research* 24, 2 (1986), 318–334.

[4] G. Bajaj, R. Agarwal, P. Singh, N. Georgantas, and V. Issarny. 2018. 4W1H in IoT Semantics. *IEEE Access* 6 (2018), 65488–65506. https://doi.org/10.1109/ACCESS.2018.2878100

[5] Iver Band, Wilco Engelsman, C Feltus, Sonia González Paredes, and Dux Diligens. 2015. Modeling Enterprise Risk Management and Security with the ArchiMate®. *Language, The Open Group* (2015).

[6] J.-P. Brans, P. Vincke, and B. Mareschal. 1986. How to select and how to rank projects: The PROMETHEE method. *European Journal of Operational Research* 24, 2 (1986), 228–238.

[7] Ismail Butun, Magnus Almgren, Vincenzo Gulisano, and Marina Papatriantafilou. 2020. Intrusion Detection in Industrial Networks via Data Streaming. In *Industrial IoT*. Springer, 213–238.

[8] Ismail Butun, Alexios Lekidis, and Daniel Ricardo dos Santos. 2020. Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities.. In *The International Conference on Information Systems Security and Privacy (ICISSP)*. INSTICC.

[9] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. 2013. Future directions for behavioral information security research. *Computers & Security* 32 (2013), 90–101. https://doi.org/10.1016/j.cose.2012.09.010

[10] Defense Use Case. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* (2016).

[11] Mathias Ekstedt, Pontus Johnson, Robert Lagerström, Dan Gorton, Joakim Nydrén, and Khurram Shahzad. 2015. securiCAD by foreseeti: A CAD tool for enterprise cyber security management. In *Enterprise Distributed Object Computing Workshop (EDOCW), 2015 IEEE 19th International*. IEEE, 152–155.

[12] J. H. Eloff and M. Eloff. 2005. Information Security Architecture. *Computer Fraud* 2005, 11 (2005), 10–16.

[13] EnergyShield. 2019. *Description of Action Part B.* Technical Report.

[14] EnergyShield. 2021. *Deliverable 1.5 – System architecture.* Technical Report.

[15] H. M. Farooq and N. M. Otaibi. 2018. Optimal Machine Learning Algorithms for Cyber Threat Detection. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim*. https://doi.org/10.1109/UKSim.2018.00018

[16] A. Georgiadou, S. Mouzakitis, and D. Askounis. 2020. Designing a Cyber-security Culture Assessment Survey Targeting Critical Infrastructures During Covid-19 Crisis. *International Journal of Network Security & Its Applications (IJNSA)* 13, 1 (2020), 33–50. https://doi.org/10.5121/ijnsa.2021.13103

[17] Anna Georgiadou, Spiros Mouzakitis, and Dimitris Askounis. 2021. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors* 21, 9 (2021). https://doi.org/10.3390/s21093267

[18] A. Georgiadou, S. Mouzakitis, and D. Askounis. 2021. Detecting Insider Threat via a Cyber-Security Culture Framework. *Journal of Computer Information Systems* (2021). https://doi.org/10.1080/08874417.2021.1903367

[19] Anna Georgiadou, Spiros Mouzakitis, and Dimitris Askounis. 2021. Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal* (26 Feb 2021). https://doi.org/10.1057/s41284-021-00286-2

[20] Anna Georgiadou, Spiros Mouzakitis, Kanaris Bounas, and Dimitrios Askounis. 2020. A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems* 0, 0 (2020), 1–11. https://doi.org/10.1080/08874417.2020.1845583 arXiv:https://doi.org/10.1080/08874417.2020.1845583

[21] E. Grandry, C. Feltus, and E. Dubois. 2013. Conceptual Integration of Enterprise Architecture Management and Security Risk Management. In *2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops*. 114–123. https://doi.org/10.1109/EDOCW.2013.19

[22] F. L. Greitzer. 2019. Insider Threats: It's the HUMAN, Stupid!. In *Proceedings of the Northwest Cybersecurity Symposium*. Richland WA USA. https://doi.org/10.1145/3332448.3332458

[23] F. L. Greitzer and D. A. Frincke. 2010. Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In *Insider Threats in Cyber Security, vol. 49*. Springer, Boston, 85–113. https://doi.org/10.1007/978-1-4419-7133-3_5

[24] Simon Hacks, Alexander Hacks, Sotirios Katsikeas, Benedikt Klaer, and Robert Lagerström. 2019. Creating Meta Attack Language Instances using ArchiMate: Applied to Electric Power and Energy System Cases. In *2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC)*. 88–97. https://doi.org/10.1109/EDOC.2019.00020

[25] Simon Hacks, Sotirios Katsikeas, Engla Ling, Robert Lagerström, and Mathias Ekstedt. 2020. powerLang: a probabilistic attack simulation language for the power domain. *Energy Informatics* 3, 1 (2020).

[26] K. Hasan, S. Shetty, and S. Ullah. 2019. Artificial Intelligence Empowered Cyber Threat Detection and Protection for Power Utilities. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, Los Angeles (Ed.). https://doi.org/10.1109/CIC48465.2019.00049

[27] Hannes Holm, Markus Buschle, Robert Lagerström, and Mathias Ekstedt. 2014. Automatic data collection for enterprise architecture models. *Software & Systems Modeling* 13, 2 (2014), 825–841.

[28] H. Holm, K. Shahzad, M. Buschle, and M. Ekstedt. 2015. P^{2}CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language. *IEEE Transactions on Dependable and Secure Computing* 12, 6 (2015), 626–639. https://doi.org/10.1109/TDSC.2014.2382574

[29] S. Hong, K. Kim, and T. Kim. 2019. The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training. *Journal of the Korea Institute of Military Science and Technology* 22, 6 (2019), 797–805. https://doi.org/10.9766/KIMST.2019.22.6.797

[30] Q. Hu, T. Dinev, P. Hart, and D. Cooke. 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences* 43 (August 2012), 4. https://doi.org/10.1111/j.1540-5915.2012.00361.x

[31] Joint Task Force Transformation Initiative. 2013. *SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations.* National Institute of Standards and Technology.

[32] ISO Central Secretary. 2013. *Information technology — Security techniques — Code of practice for information security controls.* Standard ISO/IEC 27002:2013. International Organization for Standardization. https://www.iso.org/standard/54533.html

[33] ISO Central Secretary. 2015. *Information security management.* Standard ISO/IEC 27001:2015. International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

[34] Pontus Johnson, Robert Lagerström, and Mathias Ekstedt. 2018. A Meta Language for Threat Modeling and Attack Simulations. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM, 38.

[35] Sotirios Katsikeas, Simon Hacks, Pontus Johnson, Mathias Ekstedt, Robert Lagerström, Joar Jacobsson, Max Wällstedt, and Per Eliasson. 2020. An Attack Simulation Language for the IT Domain. In *Graphical*

Models for Security. Springer, Cham, 67–86.

[36] A. Kim, J. Oh, J. Ryu, and K. Lee. 2020. A Review of Insider Threat Detection Approaches. *IEEE Access* 8 (2020), 78847–78867. https://doi.org/10.1109/ACCESS.2020.2990195

[37] D. Kim, Y. Kim, M.-K. Ahn, and H. Lee. 2020. Automated Cyber Threat Emulation Based on ATT&CK for Cyber Security Training. *Journal of the Korea Society of Computer and Information* 25, 9 (2020), 71–80. https://doi.org/10.9708/jksci.2020.25.09.071

[38] G.H. Kjølle, I.B. Utne, and O. Gjerde. 2012. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering & System Safety* 105 (2012), 80–89. https://doi.org/10.1016/j.ress.2012.02.006 ESREL 2010.

[39] Johan König, Kun Zhu, Lars Nordström, Mathias Ekstedt, and Robert Lagerstrom. 2010. Mapping the Substation Configuration Language of IEC 61850 to ArchiMate. In *2010 14th IEEEö International Enterprise Distributed Object Computing Conference Workshops*. 60–68. https://doi.org/10.1109/EDOCW.2010.35

[40] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner. 2014. Information security awareness and behavior: a theory-based literature review. *Management Research Review* 37, 12 (2014), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

[41] M. Limayem and S. G. Hirt. 2003. Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems* 4 (2003), 65–97. https://doi.org/10.17705/1JAIS.00030

[42] Yao Liu, Peng Ning, and Michael K Reiter. 2011. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)* 14, 1 (2011), 13.

[43] M. Maasberg and N. L. Beebe. 2014. The Enemy Within the Insider: Detecting the Insider Threat. *Journal of Information Privacy and Security* 10, 2 (2014), 59–70. https://doi.org/10.1080/15536548.2014.924807

[44] Delin Mathew, Simon Hacks, and Horst Lichter. 2018. Developing a Semantic Mapping betwen TOGAF and BSI-IT-Grundschutz. In *Multikonferenz Wirtschaftsinformatik (MKWI) 2018*, Paul Drews, Burkhardt Funk, Peter Niemeyer, and Lie Xie (Eds.), Vol. 5. 1971–1982.

[45] F. Maymí, R. Bixler, R. Jones, and S. Lathrop. 2017. Towards a definition of cyberspace tactics, techniques and procedures. In *2017 IEEE International Conference on Big Data (Big Data*. https://doi.org/10.1109/BigData.2017.8258514

[46] K. F. McCrohan, K. Engel, and J. W. Harvey. 2010. Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce* 9, 1 (2010), 23–41. https://doi.org/10.1080/15332861.2010.487415

[47] I. Morikawa and Y. Yamaoka. 2011. Threat Tree Templates to Ease Difficulties in Threat Modeling. In *2011 14th International Conference on Network-Based Information Systems*. 673–678. https://doi.org/10.1109/NBiS.2011.113

[48] Boon-Yuen Ng, Atreyi Kankanhalli, and Yunjie (Calvin) Xu. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems* 46, 4 (2009), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

[49] U. Noor, Z. Anwar, T. Amjad, and K.-K. R. Choo. 2019. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems* 96 (2019), 227–242. https://doi.org/10.1016/j.future.2019.02.013

[50] T. O. Oladimeji, C. K. Ayo, and S. Adewumi. 2019. Review on Insider Threat Detection Techniques. *Journal of Physics: Conference Series* 1299 (2019). https://doi.org/10.1088/1742-6596/1299/1/012046

[51] J. Ophoff, A. Jensen, J. Sanderson-Smith, M. Porter, and K. Johnston. 2014. A Descriptive Literature Review and Classification of Insider Threat Research. In *Proceedings of Informing Science & IT Education Conference (InSITE) 2014*. Wollongong.

[52] S. Opricovic and G.-H. Tzeng. 2004. Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. *European Journal of Operational Research* 156, 2 (2004), 445–455.

[53] S. Pahnila, M. Siponen, and A. Mahmood. 2007. Employees' Behavior towards IS Security Policy Compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. Waikoloa.

[54] M. Parmar and A. Domingo. 2019. On the Use of Cyber Threat Intelligence (CTI) in Support of Developing the Commander's Understanding of the Adversary. *in MILCOM* (2019), 2019–2019. https://doi.org/10.1109/MILCOM47813.2019.9020852

[55] Thomas Petermann, Harald Bradke, Arne Lüllmann, Maik Poetzsch, and Ulrich Riehm. 2011. *Was bei einem Blackout geschieht: Folgen eines langandauernden und großflächigen Stromausfalls*. Vol. 662. Büro für Technikfolgen-Abschätzung.

[56] G. Petric and K. Roer. 2018. *To measure security culture: A scientific approach*. CLTRe North America, Inc.

[57] Hyeun-Suk Rhee, Cheong-Tag Kim, and Young U. Ryu. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security* 28, 8 (2009), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

[58] Marti Rosas-Casals, Sergi Valverde, and Ricard V Solé. 2007. Topological vulnerability of the European power grid under errors and attacks. *International Journal of Bifurcation and Chaos* 17, 07 (2007), 2465–2475.

[59] T. L. Saaty. 1990. How to make a decision: The analytic hierarchy process. *European Journal of Operational Research* 48, 1 (1990), 9–26.

[60] Jonathan Schaffer. 2015. What Not to Multiply Without Necessity. *Australasian Journal of Philosophy* 93, 4 (2015), 644–664. https://doi.org/10.1080/00048402.2014.992447

[61] M. Siponen, S. Pahnila, and A. Mahmood. 2007. Employees' Adherence to Information Security Policies: An Empirical Study. *Privacy and Trust in Complex Environments* 232 (2007), 133–144.

[62] Z. A. Soomro, M. H. Shah, and J. Ahmed. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36, 2 (2016), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[63] Keith Stouffer, Joe Falco, and Karen Scarfone. 2011. Guide to industrial control systems (ICS) security. *NIST special publication* 800, 82 (2011), 16–16.

[64] Jian-Wei Wang and Li-Li Rong. 2009. Cascade-based attack vulnerability on the US power grid. *Safety science* 47, 10 (2009), 1332–1336.

[65] Michael Workman, William H. Bommer, and Detmar Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior* 24, 6 (2008), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005 Including the Special Issue: Electronic Games and Personalized eLearning Processes.

[66] Wenjun Xiong, Per Carlsson, and Robert Lagerström. 2019. Re-using Enterprise Architecture Repositories for Agile Threat Modeling. In *2019 IEEE 23rd International Enterprise Distributed Object Computing Workshop (EDOCW)*. 118–127. https://doi.org/10.1109/EDOCW.2019.00031

[67] Wenjun Xiong, Simon Hacks, and Robert Lagerström. 2021. A Method for Assigning Probability Distributions in Attack Simulation Languages. *Complex Systems Informatics and Modeling Quarterly* 26 (2021), 55–77.

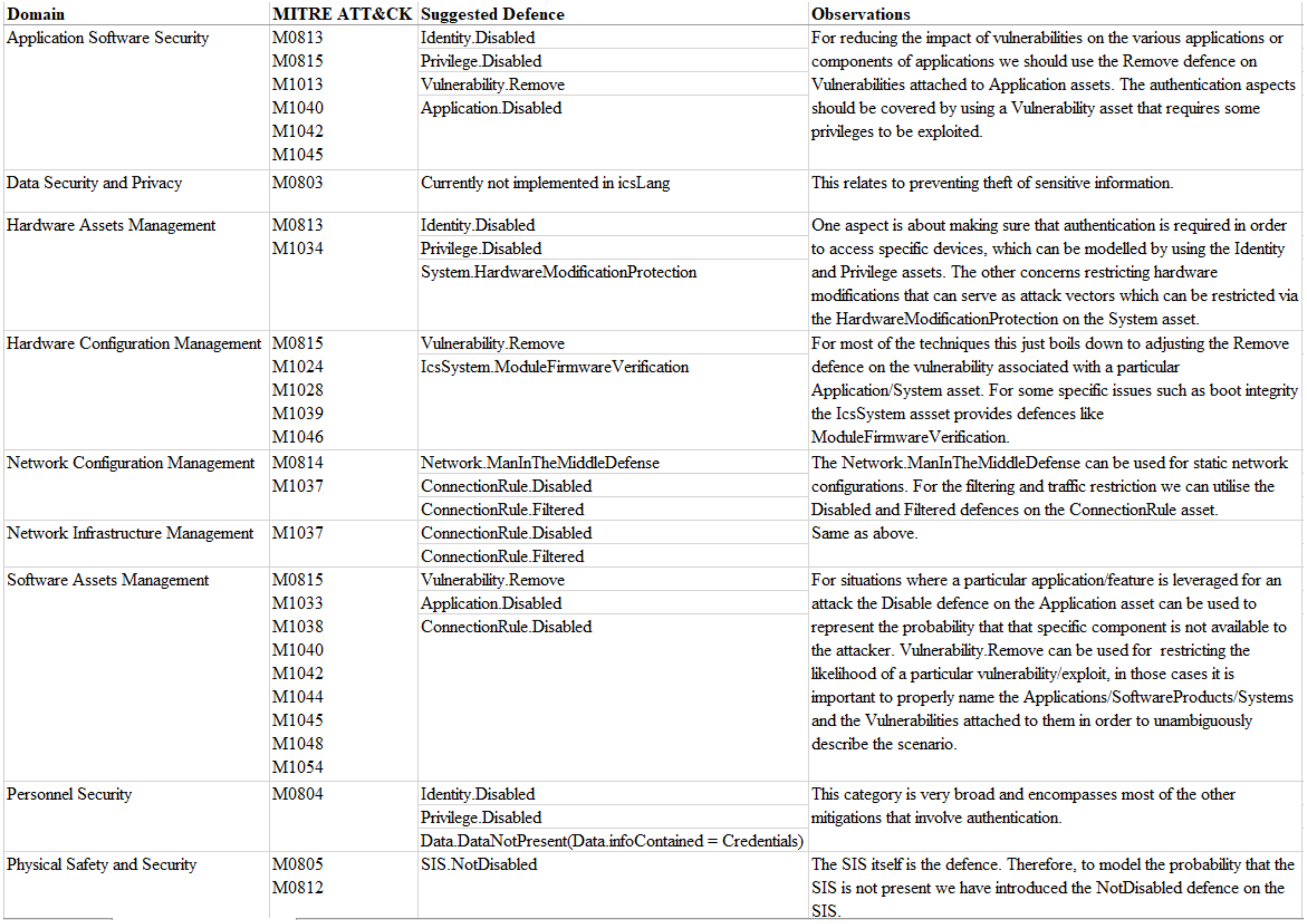
A Exemplary MAL Language

```
  asset Network {
    | access
      -> hosts.connect
  }

  asset Host {
    | connect
      -> access
    | authenticate
      -> access
    | guessPassword
      -> guessedPassword
    | guessedPassword [Exp(0.02)]
      -> authenticate
    & access
  }

  asset User {
    | attemptPhishing
      -> phish
    | phish [Exp(0.1)]
      -> pwds.obtain
  }

  asset Password extends Data {
    | obtain
      -> host.authenticate
  }
}

associations {
  Network [networks] *
    <-- NetworkAccess --> * [hosts] Host
  Host [host] 1
    <-- Credentials --> * [pwds] Password
  User [user] 1
    <-- Credentials --> * [pwds] Password
}
```

Listing 1. Exemplary MAL Code

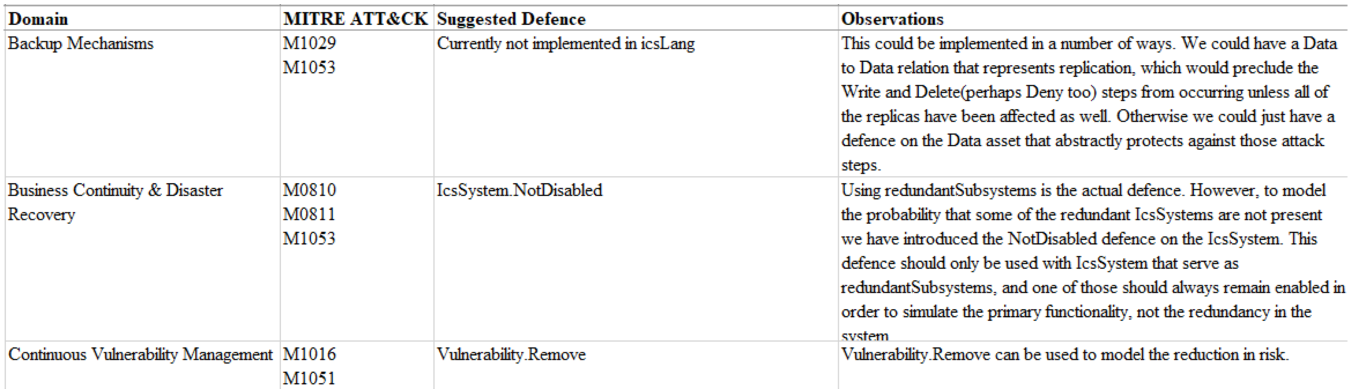
B Mapping SBA to icsLang

Table 1. Mapping SBA to icsLang – Level: Organizational; Dimension: Asset



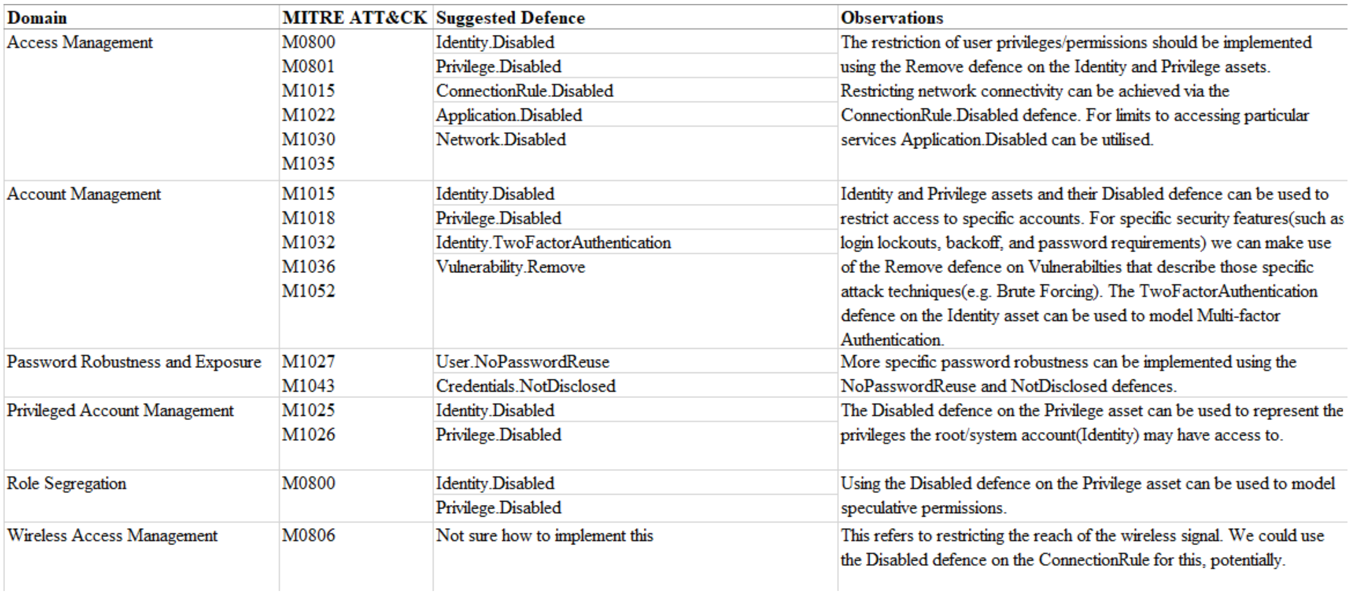
Domain	MITRE ATT&CK	Suggested Defence	Observations
Application Software Security	M0813 M0815 M1013 M1040 M1042 M1045	Identity.Disabled Privilege.Disabled Vulnerability.Remove Application.Disabled	For reducing the impact of vulnerabilities on the various applications or components of applications we should use the Remove defence on Vulnerabilities attached to Application assets. The authentication aspects should be covered by using a Vulnerability asset that requires some privileges to be exploited.
Data Security and Privacy	M0803	Currently not implemented in icsLang	This relates to preventing theft of sensitive information.
Hardware Assets Management	M0813 M1034	Identity.Disabled Privilege.Disabled System.HardwareModificationProtection	One aspect is about making sure that authentication is required in order to access specific devices, which can be modelled by using the Identity and Privilege assets. The other concerns restricting hardware modifications that can serve as attack vectors which can be restricted via the HardwareModificationProtection on the System asset.
Hardware Configuration Management	M0815 M1024 M1028 M1039 M1046	Vulnerability.Remove IcsSystem.ModuleFirmwareVerification	For most of the techniques this just boils down to adjusting the Remove defence on the vulnerability associated with a particular Application/System asset. For some specific issues such as boot integrity the IcsSystem assset provides defences like ModuleFirmwareVerification.
Network Configuration Management	M0814 M1037	Network.ManInTheMiddleDefense ConnectionRule.Disabled ConnectionRule.Filtered	The Network.ManInTheMiddleDefense can be used for static network configurations. For the filtering and traffic restriction we can utilise the Disabled and Filtered defences on the ConnectionRule asset.
Network Infrastructure Management	M1037	ConnectionRule.Disabled ConnectionRule.Filtered	Same as above.
Software Assets Management	M0815 M1033 M1038 M1040 M1042 M1044 M1045 M1048 M1054	Vulnerability.Remove Application.Disabled ConnectionRule.Disabled	For situations where a particular application/feature is leveraged for an attack the Disable defence on the Application asset can be used to represent the probability that that specific component is not available to the attacker. Vulnerability.Remove can be used for restricting the likelihood of a particular vulnerability/exploit, in those cases it is important to properly name the Applications/SoftwareProducts/Systems and the Vulnerabilities attached to them in order to unambiguously describe the scenario.
Personnel Security	M0804	Identity.Disabled Privilege.Disabled Data.DataNotPresent(Data.infoContained = Credentials)	This category is very broad and encompasses most of the other mitigations that involve authentication.
Physical Safety and Security	M0805 M0812	SIS.NotDisabled	The SIS itself is the defence. Therefore, to model the probability that the SIS is not present we have introduced the NotDisabled defence on the SIS.

Table 2. Mapping SBA to icsLang – Level: Organizational; Dimension: Continuity



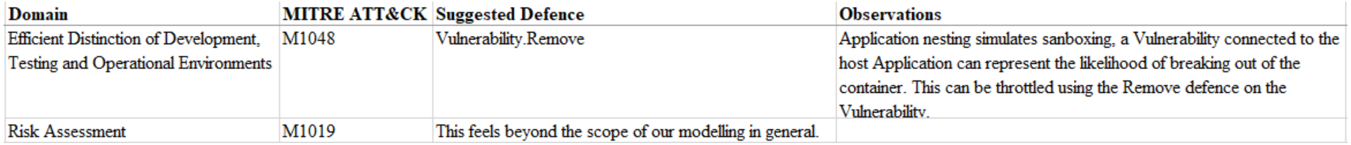
Domain	MITRE ATT&CK	Suggested Defence	Observations
Backup Mechanisms	M1029 M1053	Currently not implemented in icsLang	This could be implemented in a number of ways. We could have a Data to Data relation that represents replication, which would preclude the Write and Delete(perhaps Deny too) steps from occurring unless all of the replicas have been affected as well. Otherwise we could just have a defence on the Data asset that abstractly protects against those attack steps.
Business Continuity & Disaster Recovery	M0810 M0811 M1053	IcsSystem.NotDisabled	Using redundantSubsystems is the actual defence. However, to model the probability that some of the redundant IcsSystems are not present we have introduced the NotDisabled defence on the IcsSystem. This defence should only be used with IcsSystem that serve as redundantSubsystems, and one of those should always remain enabled in order to simulate the primary functionality, not the redundancy in the system
Continuous Vulnerability Management	M1016 M1051	Vulnerability.Remove	Vulnerability.Remove can be used to model the reduction in risk.

Table 3. Mapping SBA to icsLang – Level: Organizational; Dimension: Access and Trust



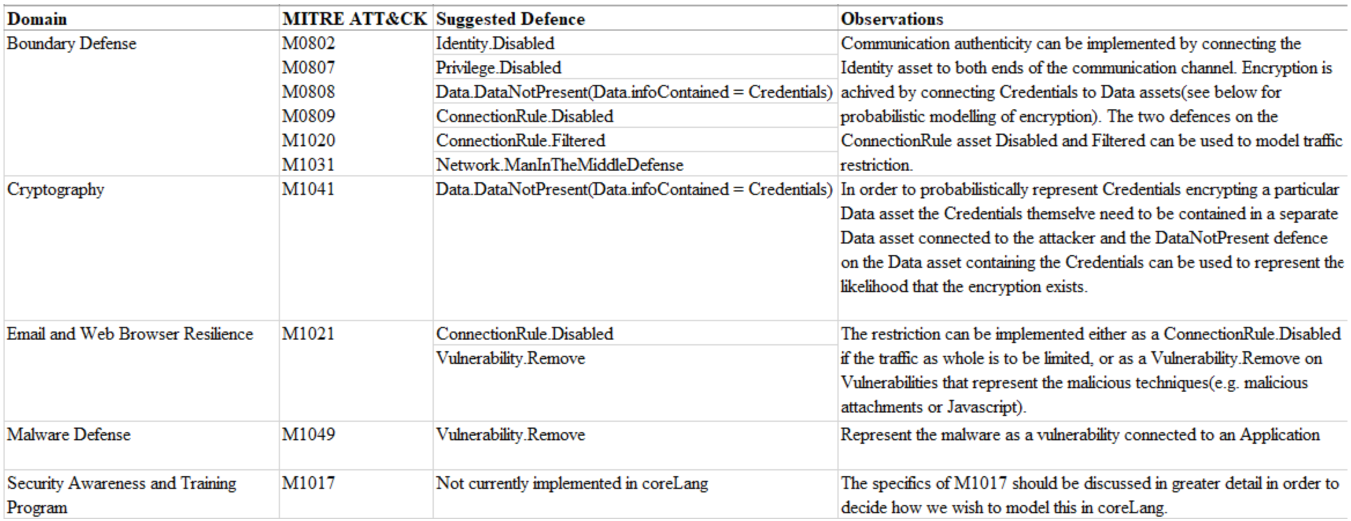
Domain	MITRE ATT&CK	Suggested Defence	Observations
Access Management	M0800 M0801 M1015 M1022 M1030 M1035	Identity.Disabled Privilege.Disabled ConnectionRule.Disabled Application.Disabled Network.Disabled	The restriction of user privileges/permissions should be implemented using the Remove defence on the Identity and Privilege assets. Restricting network connectivity can be achieved via the ConnectionRule.Disabled defence. For limits to accessing particular services Application.Disabled can be utilised.
Account Management	M1015 M1018 M1032 M1036 M1052	Identity.Disabled Privilege.Disabled Identity.TwoFactorAuthentication Vulnerability.Remove	Identity and Privilege assets and their Disabled defence can be used to restrict access to specific accounts. For specific security features(such as login lockouts, backoff, and password requirements) we can make use of the Remove defence on Vulnerabilties that describe those specific attack techniques(e.g. Brute Forcing). The TwoFactorAuthentication defence on the Identity asset can be used to model Multi-factor Authentication.
Password Robustness and Exposure	M1027 M1043	User.NoPasswordReuse Credentials.NotDisclosed	More specific password robustness can be implemented using the NoPasswordReuse and NotDisclosed defences.
Privileged Account Management	M1025 M1026	Identity.Disabled Privilege.Disabled	The Disabled defence on the Privilege asset can be used to represent the privileges the root/system account(Identity) may have access to.
Role Segregation	M0800	Identity.Disabled Privilege.Disabled	Using the Disabled defence on the Privilege asset can be used to model speculative permissions.
Wireless Access Management	M0806	Not sure how to implement this	This refers to restricting the reach of the wireless signal. We could use the Disabled defence on the ConnectionRule for this, potentially.

Table 4. Mapping SBA to icsLang – Level: Organizational; Dimension: Operations



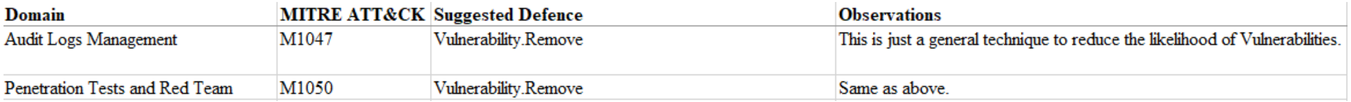
Domain	MITRE ATT&CK	Suggested Defence	Observations
Efficient Distinction of Development, Testing and Operational Environments	M1048	Vulnerability.Remove	Application nesting simulates sanboxing, a Vulnerability connected to the host Application can represent the likelihood of breaking out of the container. This can be throttled using the Remove defence on the Vulnerability.
Risk Assessment	M1019	This feels beyond the scope of our modelling in general.	

Table 5. Mapping SBA to icsLang – Level: Organizational; Dimension: Defense



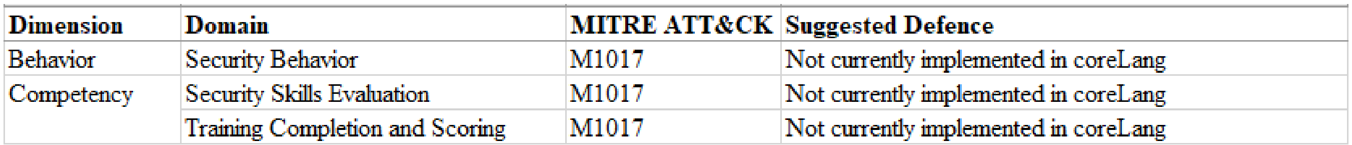
Domain	MITRE ATT&CK	Suggested Defence	Observations
Boundary Defense	M0802 M0807 M0808 M0809 M1020 M1031	Identity.Disabled Privilege.Disabled Data.DataNotPresent(Data.infoContained = Credentials) ConnectionRule.Disabled ConnectionRule.Filtered Network.ManInTheMiddleDefense	Communication authenticity can be implemented by connecting the Identity asset to both ends of the communication channel. Encryption is achived by connecting Credentials to Data assets(see below for probabilistic modelling of encryption). The two defences on the ConnectionRule asset Disabled and Filtered can be used to model traffic restriction.
Cryptography	M1041	Data.DataNotPresent(Data.infoContained = Credentials)	In order to probabilistically represent Credentials encrypting a particular Data asset the Credentials themselve need to be contained in a separate Data asset connected to the attacker and the DataNotPresent defence on the Data asset containing the Credentials can be used to represent the likelihood that the encryption exists.
Email and Web Browser Resilience	M1021	ConnectionRule.Disabled Vulnerability.Remove	The restriction can be implemented either as a ConnectionRule.Disabled if the traffic as whole is to be limited, or as a Vulnerability.Remove on Vulnerabilities that represent the malicious techniques(e.g. malicious attachments or Javascript).
Malware Defense	M1049	Vulnerability.Remove	Represent the malware as a vulnerability connected to an Application
Security Awareness and Training Program	M1017	Not currently implemented in coreLang	The specifics of M1017 should be discussed in greater detail in order to decide how we wish to model this in coreLang.

Table 6. Mapping SBA to icsLang – Level: Organizational; Dimension: Security Governance



Domain	MITRE ATT&CK	Suggested Defence	Observations
Audit Logs Management	M1047	Vulnerability.Remove	This is just a general technique to reduce the likelihood of Vulnerabilities.
Penetration Tests and Red Team	M1050	Vulnerability.Remove	Same as above.

Table 7. Mapping SBA to icsLang – Level: Individual



Dimension	Domain	MITRE ATT&CK	Suggested Defence
Behavior	Security Behavior	M1017	Not currently implemented in coreLang
Competency	Security Skills Evaluation	M1017	Not currently implemented in coreLang
	Training Completion and Scoring	M1017	Not currently implemented in coreLang