Towards a Security Impact Analysis Framework: A Risk-based and MITRE Attack Approach

Abdelhadi Belfadel[1][0000−0002−8260−4638], Martin Boyer, Jérôme Letailleur, Yohann Petiot, and Reda Yaich

IRT SystemX,
2 Bd Thomas Gobert, 91120 Palaiseau, France
abdelhadi.belfadel@irt-systemx.fr

Abstract. Cyber security assessment aims at determining the cybersecurity state of an assessed asset to check how effectively the asset fulfills specific security objectives. We are confronted with a lack of an integrated framework coupling a top-down approach such as a risk-based analysis of information systems, with a bottom-up approach such as MITRE Attack to map and understand the details of the actions taken by the attackers to evaluate a defensive coverage throughout the development life cycle. We depict in this ongoing work the description of a Security Impact Analysis Framework (SAIF) to support cyber analysts, cyber administrators, and developers in their daily tasks of security impact analysis and provide project stakeholders with sufficient security proof and defense gaps. The goal is to avoid the use of a myriad of "tool islands" to automate the security impact assessment process providing sufficient safety evidence throughout the development cycle of a project. A case study of the development of an autonomous shuttle service is used to illustrate some selected assets from the MITRE Attack approach as practical usage of this framework.

Keywords: Security Impact Analysis · MITRE Attack · Risk-based Analysis · cybersecurity · Information Systems

1 Introduction

Security flaws represent significant risks to the reliable execution of business processes and can negatively affect business value, such as reputation or profits [1]. Consequently, organizations are continually investing more resources in protecting corporate assets [2].

Cyber security assessment aims at determining the cybersecurity state of an assessed asset in order to check how effectively the asset fulfils specific security objectives [3]. It is a process of challenging assets against their cybersecurity requirements, considering the potential risks, consequences of threats, and related costs [4]. With the protective measures set up in the system, the purpose of the cybersecurity assessment is to evaluate the correct implementation and

operation of controls and their adequacy and efficiency in meeting the security requirements of the system [5, 6].

In this context, the need to identify or discover analytic coverage and defense gaps during the development software or system engineering lifecycle is of high value, however, we were confronted with a lack of an integrated framework coupling a top-down approaches (risk-based analysis of information systems), with a bottom-up approach such as MITRE Attack to map and understand the details of the actions taken by the attackers to evaluate a defensive coverage to carry out these operations throughout the development life cycle. Information security standards such as ISO 27001 are stating only very abstract implementation suggestions for risk mitigation. Therefore, we aim in this work to define a comprehensive and sufficiently generic, and, thus, adaptable, framework that uses a risk-based and MITRE Attack approaches that adopts a specific process model for managing test validations and security impact assessment analysis.

2 Background and motivation

In this section, we present first the ISO 27001, EBIOS Risk Manager (EBIOS RM) and MITRE Attack approaches. Then we give the motivation of this work.

2.1 ISO 27001

The international standard ISO 27001 outlines a model for setting up, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System [7]. This standard follows the Plan-Do-Check-Act (PDCA) process model, which is used to structure all information security management system processes [8]. The activities to be carried out in each phase are as follows:

1. Plan: this activity is related to risk management and information security improvement that sets policy, objectives, procedures and processes to meet outcomes consistent with overall organizational policies and objectives.
2. Do: Implement and operate the information security management system policy, processes, controls and procedures.
3. Check: Evaluate and measure process performance against the established policy, practical experience, objectives and report the results to management for consideration.
4. Act: Undertake preventive and corrective actions, based on the outcome of the management review to improve the information security management system continuously.

2.2 EBIOS RM

A well known qualitative methods to manage the risks in information systems is called EBIOS (Expression of Needs and Identification of Security Objectives)

[9]. Modular and compliant with the international standards ISO/IEC 31000, ISO/IEC 27005, ISO/IEC 27001, the EBIOS method remains the essential toolbox used by many organizations in both public and private sectors to conduct information system security risk analyses. The EBIOS method provides a common vocabulary and concepts to achieve security objectives. It can be tailored to the context of each organization and then used as a basis for developing either a complete global study of the information system, or a more detailed study of a particular system according to the five EBIOS phases as depicted by [9] in Figure 1.

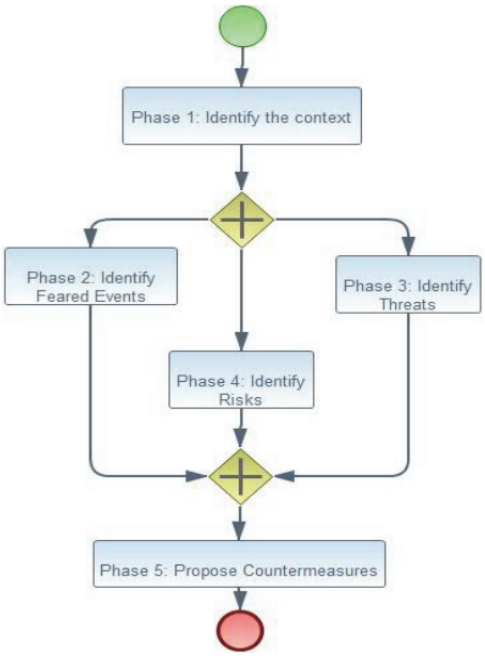

Fig. 1. EBIOS analysis method [9]

2.3 MITRE ATT&CK

The scientific community has focused on modeling patterns and techniques of cybersecurity attack from reported incidents in an attempt to anticipate adversary behavior, tactical approaches and systematic malicious actions [10, 11]. In this regard, one of the most identifiable adversary models is the one proposed by MITRE ATT&CK, which tackles the who, how, and why of cyberattacking a digital infrastructure [12]. MITRE ATT&CK is a comprehensive knowledge base of adversary tactics and techniques based on real world insights into cybersecurity related threats. It has received wide acceptance from the research

community and industry and has met with numerous applications such as behavioral analysis development or adversary emulation [12].

2.4 Motivation

We depict in Figure 2 the targeted security assessment activities throughout a system engineering lifecycle in our organization. This business process cooperation viewpoint is proposed due to the lack of a hybrid framework or tools that uses a risk-based approach coupled to MITRE Attack knowledge base to carry out all activities to discover the analytic coverage and defense gaps during an engineering process (modelization, development or CI/CD phases). To achieve this goal, we aim to model and develop a framework that manages these security assessment activities with different stakeholders of a project, namely a project manager, a cyber security administrator, cyber analysts, developers and CI/CD administrators.

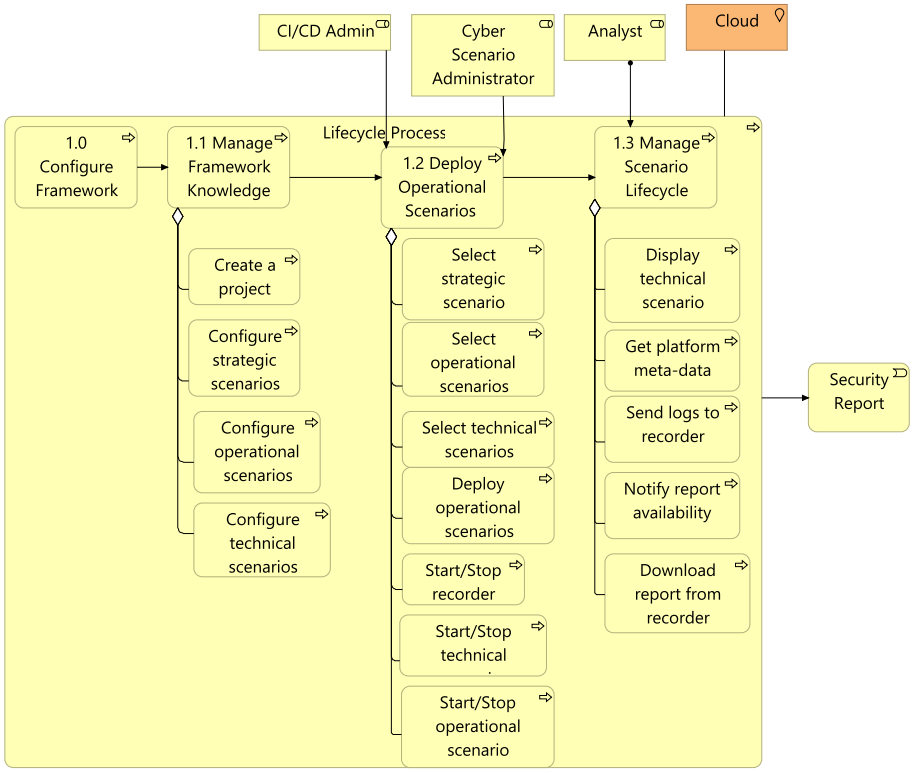

Fig. 2. Motivation - Business Process Cooperation Viewpoint. This diagram describes relationships with the targeted business processes and the Actors that perform the processes.

This targeted framework lifecycle starts with the configuration of the knowledge base by an analyst administrator (sub-process 1.1). This sub-process enables to create an instance of a project, and configure several levels of the framework's knowledge base such as the strategic level (paths of attack that a risk source could take to achieve its objective), operational level (the operating procedures likely to be used by the risk sources to carry out the strategic scenarios), technical scenarios (what compose an operational scenario), and technical attacks (refers to a technical implementation of a technical scenario). The latter is implemented as a technical attack that is reused from an existing knowledge base (such as MITRE Attack), or a technical custom attack that is a custom implementation. More details about these abstraction levels will be presented further in section 4.

Once the knowledge base is set by the *analyst administrator*, a *developer* or an *analyst* can use the framework to deploy operational scenarios based on their objectives and contextual information. In this context (sub-process 1.2), an *analyst* can choose/select an existing strategic scenario, then a related operational scenario and technical scenario to be deployed for security assessment and testing in a target cloud environment. Once the related technical configuration of the technical scenario is deployed to the targeted cloud platform, the *analyst* starts the recorder to be able to start the recording and the creation of the security report (logs and key performance indicators). The technical scenario can be started and the display of the scenario status is presented to the *analyst*. At the end of the technical scenario execution, the *analyst* stops the technical scenario, and the recorder notifies the *analyst* when the final report is ready to be downloaded for an extensive analysis for the identification for any security gaps.

To achieve this goal, we first analyze the state of the art and then present a newly proposed process model that allows us to use, in a hybrid approach, a risk-based approach coupled with MITRE Attack to organize all assets in this proposed Security Impact Analysis Framework (SIAF).

3 State of the Art

Several existing work have already proposed high-level conceptual or specific frameworks, techniques, security controls, solutions, processes or tools that are already known in the domains of information security management, software engineering and project management to address risk or cyber security assessment techniques implementation. However, there is a lack of a hybrid cyber security assessment methodology and tools that merges a risk-based and MITRE Attack approaches that might be used during the development lifecycle of a system. In addition, information security standards such as ISO 27001 only provide very abstract implementation suggestions for risk assessment.

In vulnerability identification and analysis, [13] proposed an integrated risk-security assessment method based on ISO 31000 and ISO/IEC/IEEE 29119 that

enables semi-automated evaluations that comprise graph-based system analysis and modelling, tests' preparation and execution.

In penetration testing category, [14] presented a risk-based approach to testing, in which the test preparation steps are driven by the results of independent risk assessments. This means focusing on the most critical system components and threats, with well-tailored testing scenarios and techniques. Authors in [15] assessed the security of 50 government agencies. The level of implementation of information security management systems and the compliance with the ISO 27001 standard and current regulations were evaluated. Based on this assessment, a number of recommendations were made to raise the level of information security in the public administration. In [16], authors proposed a generic cybersecurity management framework for the protection of business, government and society. The main objective of the authors' work is to enable managers to integrate counter-intelligence and place risk in a manageable context. [17] proposed a development methodology to implement cyber security strategies. This contribution is composed of several steps that includes requirement elicitation, security objectives, strategic moves and implementation framework repository.

In the context of check-list based evaluation, authors in [18] proposed a security assessment framework for internet banking services applied for 21 banks in Pakistan. The framework was employed by its authors to get a picture of the security of the banks analyzed and to draw guidelines for the banks, clients, and also for the State Bank of Pakistan. However, no guidance was given of other potential users of the framework. In [19], authors adopted standards and guidelines such as ISO/IEC 27001 to propose an assessment procedure that focuses on the elicitation phase of cybersecurity controls to get the set of checklist items that are most appropriate for the organizations' application domain and business context.

Some contributions [20, 21] have the aim to consider attackers' capabilities, and have proposed some solutions to bridge the gap and combine top-down and bottom-up approaches. Authors in [20] illustrate how attack-defense trees fit into an existing risk analysis based on risk mitigation factors. The authors combined ISO/IEC 27002 [22] to attack-defense trees to identify the security controls that an organization needs to implement. This to reduce the likely success of the attack, and thus the overall risk. In [21], authors proposed a lightweight framework for SMEs to assess and evaluate the risks facing their organization, and to effectively allocate their limited resources. This framework is first driven by domain experts by providing attack scenarios for a specific domain, then users focus on the specification of their security practices. This information is then related to attack paths and corresponding security impacts in order to assess the total risk.

4 Security Impact Analysis Framework

To attend the objective depicted in section 2.4, we propose a hybrid conceptual framework that adopts our new model based on the Know, Enter, Find and

Exploit (KEFE) process model. The later uses a risk-based approach based on EBIOS RM methodology which is compliant with ISO 27001, coupled to MITRE Attack knowledge base. This aims to support decision-making during a software or system development lifecycle for security impact assessment and enables asset reuse across projects. We describe hereafter the process model and the conceptual framework.

4.1 Know, Enter, Find, Exploit (KEFE) process model

This process model is designed following a hybrid approach. We perform risk-based analysis and management steps according to the five EBIOS method phases. First, we deal with context analysis. This step establishes the environment, purpose and operation and main assets of the target system. Second, we conduct the security needs analysis, by identifying feared events of the system and severity level to those events based on the harm it may induce. Third, we identify strategic scenarios and describe the threats affecting the system by studying attack methods or threats. Finally, we identify one or several operational scenarios that are aligned to the MITRE knowledge base using the Know, Enter, Find and Exploit process model which is applied to structure all the security impact assessment processes during the development, testing and CI/CD phases of an engineering process. The actions to be carried out in each phase of this process model is depicted below:

- *Know*: This phase aims to identify the vulnerabilities of the target system and gather techniques to aid in next phases of the process model. It involves information gathering (from MITRE category *Reconnaissance*) tactics that can be used during security test assessments. It also involves *Resource Development* tactics from MITRE to support targeting such as techniques stole resource that can be used to support targeting.
- *Enter*: This phase aims to gain a foot in the target system once the know phase has succeeded. It brings together techniques for stealing credentials (listed in MITRE as *Credential Access* category), gaining a foot in the target system (*Initial Access* MITRE category) or adversary-controlled code (*Execution* MITRE category).
- *Find*: This phase aims to gain knowledge about the system and observe the environment before deciding how to act. We bring several techniques to this phase from different MITRE categories as depicted in Table 1 such as *Discovery*, *Lateral Movement*, *Defense Evasion*, *Execution*, *Privilege Escalation*, *Credential Access* or *Persistence* category.
- *Exploit*: This last phase of the process model is the exploitation that aims to compromise integrity or disrupt availability by manipulating operational processes. As depicted in Table 1, several techniques might be used and are categorized in MITRE knowledge base as *Impact*, *Exfiltration* or *Command and Control* category.

An instance of the KEFE process model depicted in Table 1 combines different MITRE techniques to create an operational scenario to be implemented as

Operational Scenarios			
Know	**Enter**	**Find**	**Exploit**
Develop Capabilities	Exploit Public-Facing Application	Cloud Service Discovery	Data Destruction
Gather Victim Network Information	Valid Accounts	Exploitation of Remote Services	Data Encrypted for Impact
Active Scanning	Deploy Container	Internal Spearphishing	Endpoint Denial of Service
Vulnerability Scanning	Supply Chain Compromise	Modify System Image	Disk Wipe
Phishing for Information	Trusted Relationship	Software Deployment Tools	Exfiltration Over Alternative Protocol
Compromise Accounts	Brute Force	Cloud Infrastructure Discovery	Exfiltration Over C2 Channel
Compromise Infrastructure	Hardware Additions	Command and Scripting Interpreter	Exfiltration Over Web Service
Obtain Capabilities	Phishing	Remote Services	Resource Hijacking
Gather Victim Org Information	User Execution	File and Directory Discovery	Network Denial of Service
Gather Victim Identity Information		Cloud Service Dashboard	Remote Access Software
Search Closed Sources		Modify Cloud Compute Infrastructure	Service Stop
Valid Accounts		Exploitation for Privilege Escalation	Data Manipulation
		Pre-OS Boot	System Shutdown/Reboot
		Rootkit	Account Access Removal
		Data from Information Repositories	Weaken Encryption
		Man in the Browser	Inhibit System Recovery
		Network Sniffing	

Table 1. Usage of Risk-based and MITRE ATT&CK Approaches based on the Know, Enter, Find and Exploit process model - Use case applied during the development on an autonomous vehicle system

a technical scenario. The example below depicts some instances that are implemented further on as technical scenarios. A description of each level (strategic, operational, and technical scenario) is given hereafter and the hierarchy of levels are depicted in Figure 3.

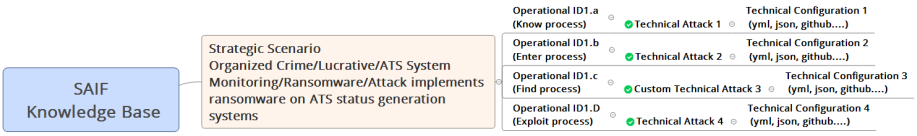

Fig. 3. KEFE model - Scenarios Hierarchisation

Strategic Scenario High-level scenarios, called strategic scenarios. This level gathers all paths of attack that a risk source could take to achieve its objective. This is linked to the strategic scenarios identified in the risk-based methodology. However, in our context, it might be linked to a technical scenario to simulate a desired state in a target system. This scenario has the following

value template that is a combination of several identified values after the realization of the risk-based method (in our context, EBIOS RM): *Source of risk/Targeted Objective/Business Values/Type of attack/method.* As an example, this value is considered as a strategic scenario instance in our framework: *Organized crime/Lucrative/Supervision of systems/Software asset*

Operational Scenario This represents operating procedures likely to be used by the sources of risk to carry out the strategic scenarios. In our context, all operational scenarios are linked to a strategic level, and an operational scenario should be linked to *only one* existing knowledge base at a time (in this context is MITRE knowledge base). The list of operational scenarios of a strategic one is based on the KEFE process model as mentioned in 4.1. Finally, an operational scenario is linked to *one or several* technical scenarios.

Technical Scenario This represents two kinds of technical attacks: A technical attack or a technical custom attack. Each one of them can be implemented by one technical configuration. A *technical attack* is what composes an operational scenario. It represents a way to perform an action on a system for an attacker and is implemented following the best practice defined in an existing knowledge base (in this context MITRE). *A technical custom attack* is an action on a system that is not covered by an existing knowledge base, for instance, the creation of malware. Finally, a *technical configuration* represents the implementation of the technical or a custom attack through a containerized solution such as a docker-like configuration file.

4.2 KEFE Model Example

We depict in this section a concrete example applied in the context of the development of an autonomous shuttle service to illustrate some selected assets from the MITRE Attack approach as practical usage of the proposed KEFE model.

The operational scenario considered in this example is of an activist (or Hacktivist) attacker whose goal is to impact the availability of the service (see Figure 4) by using the denial of the service method. To carry out this attack, there are several ways. First, in the *Know* phase, the attacker will start by developing his toolkit, he will prepare for the attack by choosing his tools or by developing them himself. Then, he will retrieve information about the target system online. The final goal of this phase is to launch a vulnerability scan. In case the attacker detects a vulnerability, he will proceed to the *Enter* phase where he will exploit the vulnerability to get inside the system. Another way to proceed would be to launch a phishing attack to gain access to a valid account. This account will allow him to implant a malicious container image. Once the container has been implemented or the flaw exploited, the attacker will now start looking for his final goal. In our case, to impact the availability as depicted in the *Find* phase. In the first scenario, he will exploit a flaw to get into the cloud system. In the second scenario, it is his container image that will perform the

malicious actions. Finally, the only thing left to do is to damage the cloud VMs to make them inoperable, this is the *Exploit* phase.

This operational scenario is linked to several technical scenarios and are implemented following the best practice defined in this case on MITRE knowledge base. For instance the activity *Active scanning* of the *Know* phase is implemented according to several sub-techniques described in MITRE [1] (T1595.001 Scanning IP Blocks; T1595.002 Vulnerability Scanning and T1595.003 Wordlist Scanning). Each of these sub-techniques are implemented further as a technical configuration that is a script (such as a docker configuration file) deployed in the platform under security test assessment during a CI/CD phase (see Figure 4 for the list of selected technical tools that might be used in this example). Finally, each operational level is linked to mitigation techniques that can be used to prevent a technique or sub-technique from being successfully executed. In the given example, the *Active scanning* activity is linked to mitigation technique M1056 [2].

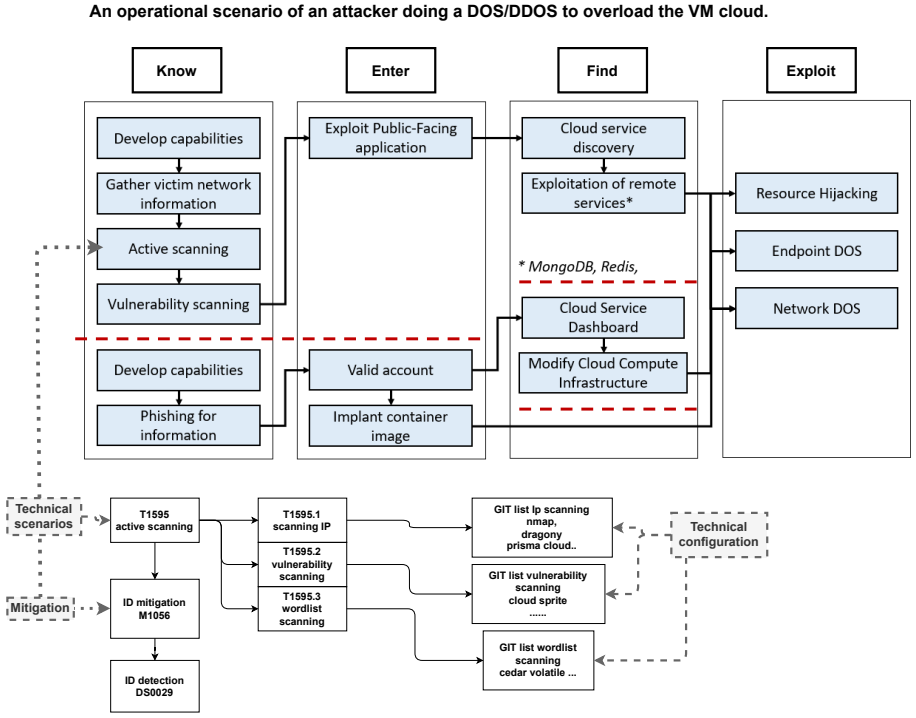

Fig. 4. KEFE model example

[1] https://attack.mitre.org/techniques/T1595/
[2] https://attack.mitre.org/mitigations/M1056/

4.3 Conceptual Framework

The proposed SAIF framework consists of several components, which are described in this sub-section enabling the realisation of the business process depicted in Figure 2. The connections or communications between different components will be performed through APIs or direct calls inside the same component. The technology foundations as a first and high-level analysis are described in this section, however, specific technology selections for the components are decided in later sections. As previously shown, the high-level architecture of the Framework is depicted in Figure 5, and is composed of the following main components (from top to down):

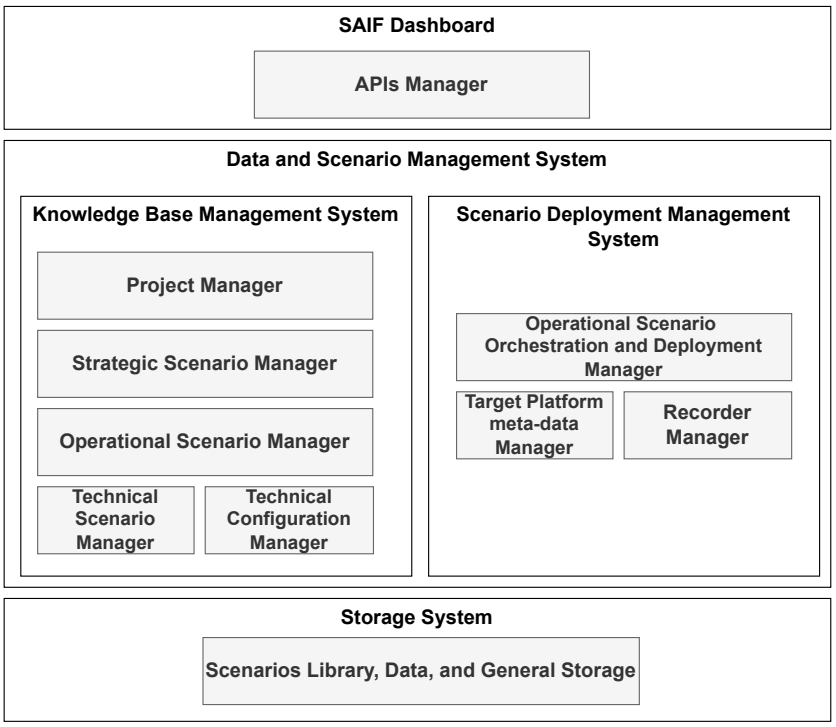

Fig. 5. Proposed Framework

– Framework Dashboard: A user-friendly dashboard and interface. It allows the users to create the required entities that will be managed during the configuration and the usage of the framework such as the creation of a project, a strategic, operational, and technical scenarios. This dashboard provides also functionalities to deploy the required technical configuration to a targeted cloud platform, with a dashboard that displays the KPIs and progress of the actual running technical scenarios.

- Knowledge Base Management System (KBMS): This component will offer the required APIs to the framework's stakeholders enabling the management of the required entities (project, scenarios, technical configuration. . .) during the development lifecycle of a project. It is connected to the Dashboard and to the Scenario Deployment Manager that retrieves and deploys the selected scenario to a targeted cloud platform.
- Scenario Deployment Management System (SDMS): This component manages the deployment lifecycle of the selected scenarios to a cloud platform. It aims to manage the recorder that captures the logs of each deployed container, as well as the generation of a report for each deployed scenario. This component serves to retrieve KPIs from the targeted cloud platform to display in the dashboard the scenario progressions, KPIs etc.
- Data and General Storage: This component stores the data managed in the framework. This latter has different needs of data storage, e.g., scenario library, configuration files, generated log files, report or structured data. Each of them has its own requirements and constraints in terms of velocity of storage and querying. This component will offer APIs to get access to the required type of storage depending on the requirements and constraints of each component.

5 Technical foundation

This section describes only technical insights to consider when analyzing in detail the technical requirements enabling the implementation of the targeted framework. The Cloud Computing side of the framework will be based on existing open source technology. Based on the initial design phase, the framework will follow a modern approach by combining containerization and virtualization techniques.

For the Dashboard (end user portal side) implementation, we aim to build this front-end with open source solution for creating customizable dashboards such as AngularJS [3] or VueJS [4] empowered with technologies such as Grafana [5] technology tools, that is widely used to compose observability dashboards with metrics, logs, and application data.

For the KBMS component, a python-based framework such as flask [6] might be employed to manage the configuration, retrieval and updates of the framework knowledge base. These choices are influenced by the data and general storage component that might be implemented by using document-oriented database such as MongoDB enabling the storage and querying of the data.

For the SDMS component, a job scheduler might be employed over Docker [7] /Kubernetes [8] APIs, with a solution to handle data ingestion such as Kafka

[3] https://angularjs.org/
[4] https://vuejs.org/
[5] https://grafana.com
[6] https://flask.palletsprojects.com/en/2.1.x/
[7] https://www.docker.com/
[8] https://kubernetes.io

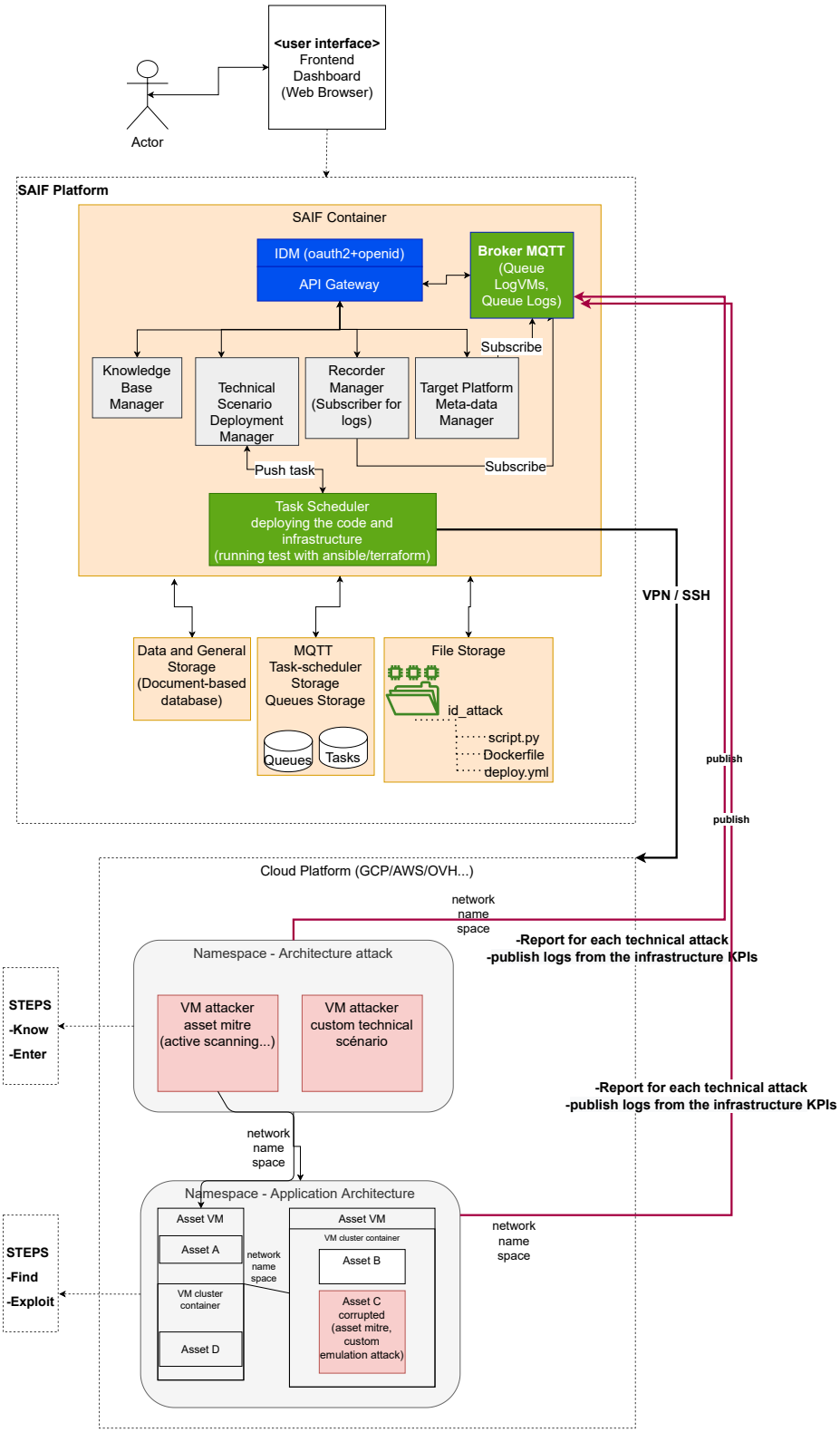

Fig. 6. SAIF Technical Architecture (Legend: Gray color refers to private components; Green color: refers to internal component with APIs for internal ones; Blue color: refers to a public accessible component with public APIs; White color: refers to a user interface component; Red color: refers to a technical attack deployed on a virtual machine or a container.

[9] backbone. Regarding the infrastructure, infrastructure as a service-based solutions for IT automation to configure systems, deploy technical configurations and orchestrate operational scenarios tasks will be considered such as Ansible [10] and Terraform[11].

Finally, the technical scenarios are containerised solution (Docker images or custom linux-based systems such as Yocto[12]), that might implement any technical tool used during a security test assessment. It should be deployed already in the target cloud environment as an image that can be invoked through the SDMS component.

6 Discussion

The Security Impact Assessment Framework is designed to assist cyber analysts, cyber administrators, and developers in their daily security impact analysis tasks. As mentioned in the opening sections, it aims to avoid the use of a myriad of "tool islands" to automate the security impact assessment process and the reuse of assets between projects by bringing together designed assessment techniques into a single repository. The goal is to provide project stakeholders with sufficient safety evidence throughout the development cycle of a project. However, there are some limitations that need to be highlighted. The proposed risk-based approach is implemented with the EBIOS framework. Thus, it requires the use of specialized skills for the determination and assessment of operating modes, in addition, it may need to use transformation models in case it is necessary to work with another approach to manage strategic and operational scenarios. With respect to the use case, the current framework implementation platform is intended to be used in a closed environment (pre-prod stage). Furthermore, the knowledge base of each project is specific and depends on the target system. Risk sources and objectives must be characterized and evaluated to select the most relevant ones, then a risk treatment solution must be identified for each risk through the design of the associated technical configuration, however, asset reuse is maximized with the possibility to reuse assets from one project to another.

7 Conclusion

Information security management is a complex and therefore time-consuming and expensive task. Organizations face changing threat landscapes and have to address them on multiple levels. Some efforts in research and industry already concentrate on increasing the automation of some aspects of information security.

We presented an ongoing work about the design of a Security Impact Assessment Framework that uses a hybrid approach aligning a risk-based and MITRE

[9] https://kafka.apache.org/
[10] https://docs.ansible.com/ansible/latest/index.html
[11] https://www.terraform.io/
[12] https://www.yoctoproject.org/

approach that adopts the Know, Enter, Find, Exploit (KEFE) model for security impact analysis. This is to assist cyber analysts, cyber administrators, and developers in their daily security impact analysis tasks and discover analytic coverage and defense gaps during the whole software or system development lifecycle. The goal is to avoid the use of a myriad of "tool islands" to automate the security impact assessment process and provide project stakeholders with sufficient safety evidence throughout the development cycle of a project.

With our detailed perspective on the numerous components that are necessary to define a comprehensive and sufficiently generic, and, thus, adaptable, framework for security impact assessment we aim to foster a discussion on the architectural design of such a software package. While today, merely academic and very individualized solutions exist, it is likely that a more standardized and formalized framework will contribute to the practical implementation of such a security impact assessment system.

8 Acknowledgement

This research work has been carried out in the framework of IRT SystemX, Paris-Saclay, France, and therefore granted with public funds within the scope of the French Program "Investissements d'Avenir".

References

1. H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, pp. 70–104, 2004.
2. A. Ekelhart, S. Fenz, and T. Neubauer, "Aurum: A framework for information security risk management," in *2009 42nd Hawaii International Conference on System Sciences*. IEEE, 2009, pp. 1–10.
3. K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment," *NIST Special Publication*, vol. 800, no. 115, pp. 2–25, 2008.
4. T. IEC, "62351-1," *Power Systems Management and Associated Information Exchange-Data and Communications Security-Part 1: Communication Network and System Security-Introduction to Security Issues*, 2007.
5. M. Chapple, J. M. Stewart, and D. Gibson, *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons, 2018.
6. R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Computers & Security*, vol. 108, p. 102376, 2021.
7. I. Iso, "Iec 27001 (2005) information technology, security techniques, information security management systems requirements," *ISO, Geneva*, 2005.
8. R. Montesino and S. Fenz, "Automation possibilities in information security management," in *2011 European Intelligence and Security Informatics Conference*. IEEE, 2011, pp. 259–262.

9. R. Abdallah, N. Yakymets, and A. Lanusse, "Towards a model-driven based security framework," in *2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*. IEEE, 2015, pp. 639–645.
10. J. Straub, "Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks," in *2020 IEEE International Conference on Smart Cloud (SmartCloud)*. IEEE, 2020, pp. 148–153.
11. M. S. Khan, S. Siddiqui, and K. Ferens, "A cognitive and concurrent cyber kill chain model," in *Computer and Network Security Essentials*. Springer, 2018, pp. 585–602.
12. A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing mitre att&ck risk using a cyber-security culture framework," *Sensors*, vol. 21, no. 9, p. 3267, 2021.
13. J. Großmann and F. Seehusen, "Combining security risk assessment and security testing based on standards," in *International Workshop on Risk Assessment and Risk-driven Testing*. Springer, 2015, pp. 18–33.
14. A. Rennoch, I. Schieferdecker, and J. Großmann, "Security testing approaches–for research, industry and standardization," in *International Conference on Trustworthy Computing and Services*. Springer, 2013, pp. 397–406.
15. E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," *Computers & Security*, vol. 90, p. 101709, 2020.
16. P. R. Trim and Y.-I. Lee, "A security framework for protecting business, government and society from cyber attacks," in *2010 5th International Conference on System of Systems Engineering*. IEEE, 2010, pp. 1–6.
17. I. Atoum, A. Otoom, and A. A. Ali, "Holistic cyber security implementation frameworks: A case study of jordan," *International Journal of Information, Business and Management*, vol. 9, no. 1, p. 108, 2017.
18. S. Khattak, S. Jan, I. Ahmad, Z. Wadud, and F. Q. Khan, "An effective security assessment approach for internet banking services via deep analysis of multimedia data," *Multimedia Systems*, vol. 27, no. 4, pp. 733–751, 2021.
19. Y. You, I. Cho, and K. Lee, "An advanced approach to security measurement system," *The Journal of Supercomputing*, vol. 72, no. 9, pp. 3443–3454, 2016.
20. O. Gadyatskaya, C. Harpes, S. Mauw, C. Muller, and S. Muller, "Bridging two worlds: reconciling practical risk assessment methodologies with theory of attack trees," in *International Workshop on Graphical Models for Security*. Springer, 2016, pp. 80–93.
21. C. Schmitz and S. Pape, "Lisra: Lightweight security risk assessment for decision support in information security," *Computers & Security*, vol. 90, p. 101656, 2020.
22. I. ISO27002, "Iec 27002: 2005 information technology—security techniques—code of practice for information security management," 2005.