Knowledge Systematization for Security Orchestration in CPS and IoT Systems

Phu Nguyen, Hui Song, Rustem Dautov
SINTEF
Oslo, Norway

Nicolas Ferry
Université Côte d'Azur, I3S
Sophia Antipolis, France

Angel Rego, Erkuden Rios, Eider Iturbe
TECNALIA
Derio, Spain

Valeria Valdes, Ana Rosa Cavalli, Wissam Mallouli
Montimage
Paris, France

***Abstract*—Cyber-Physical Systems (CPS) and the Internet of Things (IoT) are crucial in a number of fields, including healthcare, energy, mobility, and communication. IDS, network, and application layers are among the system layers that are the primary focus of current Security Orchestration, Automation, and Response (SOAR) techniques. However, taking into account the computing continuum, there is a noticeable lack of complete SOAR techniques for multi-layered IoT/CPS systems. We aim to systematize the current SOAR approaches for IoT/CPS-based critical infrastructures. Three research topics served as the basis for our systematic review, which produced important findings: (i) IoT/CPS systems require a complete SOAR that addresses many architectural elements; (ii) AI/ML improves automation, but it is insufficient in addressing explainability and cross-layer/system/domain issues; and (iii) the incorporation of digital twin solutions into SOAR frameworks is still in its early stages. We highlight areas for further research to enhance SOAR solutions' efficacy, flexibility, and comprehensiveness in addressing evolving cybersecurity challenges.**

***Index Terms*—Systematic Review, Security Orchestration, SOAR, IoT, CPS, AI, ML, Digital Twin, SLR.**

I. Introduction

The secure functioning of critical infrastructures in key sectors such as finance, energy, healthcare, transport, communication, gas, and water are of paramount importance to a nation's security, economy, and the well-being of its citizens [1]. With the increasing interconnection between the digital and physical realms, these critical infrastructures have become more intricate, vital, and interdependent than ever before. IoT/CPS-based critical infrastructures spanning across the computing continuum are increasingly becoming digitalized, connected, and distributed [2]. As a result, the attack surfaces of these systems are expanding, making them vulnerable to cyber-security threats that are evolving and becoming more sophisticated [3]–[5]. This vulnerability is evident in the rising number of cybersecurity incidents, such as phishing and ransomware, as well as cyber-physical incidents that involve the physical violation of devices or facilities in conjunction with malicious cyber activities.

The increasing cybersecurity threats have become a matter of life and death, as time to respond is crucial in some critical infrastructures such as energy, mobility, healthcare. Additionally, the systems are getting more complex, integrating systems of systems, which makes it difficult to ensure security and recover in case of security attacks. Besides, security orchestration, automation and response (SOAR) solutions generally involve many techniques and tools that makes them complex to administrate leading to overwhelming burden for security operators. Traditional static methods for IoT security can not handle this level of complexity [6], [7]. A systematic approach to security orchestration and response at different layers of critical infrastructures is essential. This includes real-time security orchestration and response, as well as continuous improvement and development of preventive security solutions while the systems and security threats are evolving.

In this work, we have conducted a Systematic Literature Review (SLR) to analyze the research landscape of SOAR approaches applicable for IoT/CPS/computing continuum to identify gaps in the research for IoT/CPS-based multi-layered critical systems. The contributions of our SLR are our answers to the following research questions: ***RQ1:*** *What is the current research landscape of the SOAR methods for orchestrating multi-layer security and automated reaction in the systems across the computing continuum?* ***RQ2:*** *What are the specialized SOAR approaches for each system layer such as infrastructure, network, OS, application, business, also from computing continuum IoT devices, Edge/Fog, Cloud?* ***RQ3:*** *What are the current limitations and what are the open issues to be further investigated?* Some highlights of our findings: Existing SOAR approaches (e.g., [8]–[10] have mainly focused on specific layers of systems such as IDS, network layer, or application layer. There is a lack of a systematic approach for SOAR for the multi-layered systems using IoT/CPS, computing continuum ([11]) perspective. Furthermore, there is a need to address the cascading effects cross-layer, cross-systems, cross-physical-cyber domain, and even cross-application domain. Recent approaches that leverage AI/ML have not addressed the cross-layer aspects. It is also worth exploring the use of digital twin solutions and DevSecOps or SecDevOps as part of the SOAR solution to co-evolve with the systems being defended against continuously evolving security threats.

Next, Section II gives the details of our SLR approach. We

This work has received funding from the European Union's Horizon Europe research and innovation programme under grant agreements No 101070455 (DYNABIC).

present in Section III a classification schema of the primary studies in our SLR. Then, we present the results of our SLR in Section IV, and compare our study with related work in Section V. We give our conclusions in Section VI.

II. Review Process

A. Research Questions

This paper aims to answer three RQs in Section I. RQ1 includes the following sub-RQs. **RQ1.1 -** *RQ1.1: What is the current trend of SOAR publications?* Answering this question allows us to see how SOAR is a topic of interest. **RQ1.2 -** *What are the architectures of the targeted systems being addressed by the SOAR methods?* Answering this question allows us to see which layers of the architectures of the systems being protected by SOAR. **RQ1.3 -** *What are the application domains of the systems supported by the SOAR methods?* As we are interested in identifying the domains, we are also interested in the different domains and their specific and common challenges to be supported by the existing SOAR.

RQ2 has three sub-questions. **RQ2.1 -** *Are there approaches combining different SOAR solutions for different layers (system of systems perspective)?* Answering this question would give an overview of how different system layers are addressed by what SOAR methods specifically and if there is any holistic approach existing. **RQ2.2 -** *What are security mechanisms used in the existing SOAR solutions?* In other words, we would want to extract how different single-purpose security solutions can be integrated to form the existing SOAR solutions. After identifying the SOAR solutions, we extract how different single-purpose solutions can be integrated. **RQ2.3 -** *What is the landscape of using AI, SecDevOps approaches, Digital Twin (DT) approaches for SOAR?* As the amount of data needed to be processed with minimum time delay, we examine how trending the automated SOAR support using AI is, as well as other approaches such as SecDevOps, DT.

RQ3 does not consist of any sub-RQs. However, this RQ helps to express the current issues and suggest possible directions for future research.

B. Selection Criteria

Because the search strategy produced a wide range of primary studies with diverse content and outcomes, it was necessary to establish a set of inclusion criteria that all primary papers had to meet. Our selection procedure was conducted in the most transparent and unbiased way possible, with all the primary studies having to meet the following Inclusion Criteria (IC). The selected primary studies must address the key SOAR aspects, such as having a good enough architecture of SOAR (orchestrator, infrastructure layer), orchestration/master control of security mechanisms, with enforcement. The must address across the Computing Continuum, e.g., CPS/IoT/Edge / Critical Infrastructures, Software defined systems.

C. Search and Selection Strategy

Using online inquiry features of popular publication databases is the most notable approach to scan for primary studies when directing supplemental studies [12]. We used the following popular publication databases, i.e., IEEE Xplore[1], ACM Digital Library[2] to search for potential primary studies.

Our selection process is based on the predefined selection criteria (Section II-B). We first filtered the candidate papers based on their titles and abstracts. When the titles and abstracts were not enough to decide whether to discard or keep the papers, we continued to skim and scan through the contents of these papers. When a candidate paper appeared in more than one database, we kept it, at first, in multiple search results. Then, we consolidated the outcomes in group discussions among the authors to cross-check the selection decisions and acquired the set of *twenty-four* (24) primary studies with no duplicates as shown in Table I.

III. A Classification Schema / Taxonomy

A. Unification

SOAR mechanisms are based on security techniques to be employed on incident management. Since a SOAR must react to a wide range of attacks or, in general, events, the available mechanisms or disparate security tools must be unified to make the incident-handling process efficient and effective. Some examples of mechanisms are firewalls, to prevent access or block networks instantly when an attack occurs, or certificate management to revoke/renew credentials when they have been stolen or when the system detects suspicious activity on a user.

Even if SOAR solutions thrive for more automation, it is still important to clearly define the endpoints for human-in-the-loop. This means that in addition to the unification of security tools, there must be unification with security experts in the decision makings, especially where automated responses are not possible. Security experts must still supervise every automated SOAR response and interfere if decisions it produces are inaccurate. This does not mean to correct every recommendation of SOAR, especially the trivial ones, but to spot and correct recommendations that contain a large error.

B. Orchestration

Security orchestration integrates tools and technologies both security and non-security specific to respond to incidents in a timely manner [13]. In this context, an orchestrator is in charge of coordinating and synchronising these tools to protect the system throughout its life cycle. The process of orchestration involves a previously defined set of activities performed by security experts and security tools to improve the response to a security event [14].

An orchestrator can help reasoning and choosing the appropriate and effective course of actions for handling a security incident. Triggered by an alert, an orchestrator can investigate and determine the proactive response to threats. While more automation is desirable, supporting human-in-the-loop is still crucial, either for the explainability of the automated decision making and response, or for the integration with security experts. In this sense, visualisation support is a must.

[1]https://ieeexplore.ieee.org
[2]https://dlnext.acm.org

C. Automation and Enactment

SOAR solutions aim for more automation, especially in the routine tasks, e.g., extracting data from technical blogs, websites, finding correlation among different reported attacks, and updating incident severity based on threat intelligence feeds. While a fully automated SOAR can provide faster and more inexpensive responses, there is an acknowledgement that over-automation may produce negative effects, e.g.: treating false positives as valid and perform unnecessary protections on a system. On the other side, too little automation can lead to dangerous delays when analysing the attack and perform the protection manually or assigning more people dedicated to security tasks [15]. The best solution is usually a trade-off between automation of tasks like detection and reaction and expert analysis on the nature of the attack and final resolution [16]. Automated incident response aims at eliminating, or at least minimizing, human intervention during the process, including automatic proactive and reactive reactions.

Proactive strategies are used by companies to anticipate challenges, threats and attacks and prepare the system to handle these. **Reactive strategies** consist in triggering actions such as adaptations in response to security events without anticipating the need for subsequent reaction. These two strategies typically need to be used in combination to prevent, detect and react against security attacks. E.g., when reactions take time to produce their effects, they must be started head of time so their effect is complete in a timely fashion [17].

D. Cloud, Edge/Fog, IoT layers

Numerous IoT architectures have been proposed in existing literature, each decomposed into varying numbers of layers. Three layers make up a straightforward IoT design that has been widely used in the literature and spans the computing continuum: perception (IoT devices), network (Edge/Fog), and application (Fog/Cloud). In our work, we utilize the IoT World Forum Reference Model of the IoT architecture [18] as a basis for our taxonomy. This particular architecture offers a highly detailed breakdown of the different layers commonly found in IoT systems. The IoT World Forum Reference Model comprises of seven layers: Physical Devices and Controllers, Connectivity, Edge Computing, Data Accumulation, Data Abstraction, Application Layer, Collaboration and Processes.

IV. Results

Table I presents 24 selected primary studies. We conducted in-depth evaluations and analyses of these studies in order to answer the research questions as follows.

A. High-Level Details (RQ1)

Answering RQ1.1 - What is the current trend of publications in reporting SOAR methods? The 24 primary studies have been published since 2016. Nearly half of the primary studies (#9, #13, #14, #18, #19, #23, #24) focus on the security orchestration solutions at the network layer, especially leveraging software defined networking and network virtualization techniques. Two primary studies #11, #21 have specialised approaches for security solution based on honeypots. Security policies automation is also an important topic. This starts to be some AI/ML application to SOAR solutions, even though only a few approaches. Most existing SOAR approaches have not leveraged Digital Twin (DT) frameworks for SOAR. In [19], the authors present a review of SOAR approaches that classifies the main functionalities of SOAR into three main areas: Unification, orchestration, and automation. While more and more SOAR approaches aim at automation, only one study #3 has explicitly addressed the explainability of security orchestration.

TABLE I: The primary studies.

#	Year	PV	Title
1	2024	C	Digital Twin-Based Security Orchestration, Automation and Response for IoT and CPS
2	2024	C	AI4SOAR: A Security Intelligence Tool for Automated Incident Response
3	2024	C	Security Orchestration with Explainability for Digital Twins-based Smart Systems
4	2024	C	A SOAR platform for standardizing, automating operational processes and a monitoring service facilitating auditing procedures among IoT trustworthy environments
5	2023	C	Digital Twin-Enhanced Incident Response for Cyber-Physical Systems
6	2023	J	Generating ICS vulnerability playbooks with open standards
7	2023	C	Towards Smarter Security Orchestration and Automatic Response for CPS and IoT
8	2023	J	Digital-Twin-Based Security Analytics for the Internet of Things
9	2023	J	PALANTIR: An NFV-Based Security-as-a-Service Approach for Automating Threat Mitigation
10	2022	C	SOAR4IoT: Securing IoT Assets with Digital Twins
11	2022	C	Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots
12	2022	J	An automated closed-loop framework to enforce security policies from anomaly detection
13	2021	C	Efficient Incident Response System on Shared Cyber Threat Information Using SDN and STIX
14	2020	C	Security Orchestration and Enforcement in NFV/SDN-Aware UAV Deployments
15	2020	C	Switched-Based Resilient Control of Cyber-Physical Systems
16	2020	C	Architecture-Centric Support for Integrating Security Tools in a Security Orchestration Platform
17	2020	C	Cyber-Resilience Evaluation of Cyber-Physical Systems
18	2019	C	Towards a fully automated and optimized network security functions orchestration
19	2019	J	Adding Support for Automatic Enforcement of Security Policies in NFV Networks
20	2019	J	Automated Interpretation and Integration of Security Tools Using Semantic Knowledge
21	2019	J	HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design
22	2017	C	Testbed for security orchestration in a network function virtualization environment
23	2017	J	PSI: Precise Security Instrumentation for Enterprise Networks
24	2016	C	Orchestration of software-defined security services

PV: Publication venue; J: Journal; C: Conference;

Answering RQ1.2 - What are the architectures of the targeted systems being addressed by the SOAR methods? Under the scope of SOAR for CPS/IoT, the surveyed studies all target large distributed systems with many sensing and computation devices or virtual resources are connected by networks. However, we can also observe that the current studies are focusing specific parts or layers of the CPS/IoT systems. There is a need to have integrated and comprehensive approaches to SOAR that cover the entire CPS systems.

The 24 existing SOAR approaches in Table I have shown a clear focus on the following layers of CPS/IoT systems:

- The cyber-physical layer, targeting the threats towards low-end devices such as sensors and controllers, using specific mechanisms for resilience of CPS (#15, #17)
- The network layer, focusing on attacks to the networking devices and functions, using network security mechanisms. The majority of the studies in Table I are within this category, such as #11, #23, #9, #13, #21
- The application layer, handling the threats to the applications deployed in the local or public cloud, using security mechanisms on the general computing resources. The studies target the part of the systems that are deployed in public cloud or local cloud (#20)

Cross-layer approaches are still missing in the surveyed

studies. Some studies target the systems that span multiple layers. For example, the network security approach in #18 is based on software defined networks, and assume that the network functions are deployed in a cloud infrastructure. From this perspective, the target system is a mix of the network and the application layer. However, the orchestration is still focused on the network security, without the consideration of application-level security mechanisms. Comprehensive SOAR approaches that cover security concerns in multiple layers of the target architectures are still missing.

Virtualization is widely used in the target systems behind the surveyed studies, regardless of architectural focuses. When covering CPS and IoT devices, the studied SOAR approaches exploit the IoT platform or environment of the target system for monitoring and controlling the devices (#10). For general-purpose computation resources, all the approaches are based on a cloud infrastructure, so that they deal with virtual machines instead of the physical computers (#11). The studies towards on the network layer rely on SDN (#13#14) and NFV (#11#19) to virtualize the control of the network. As the virtualization technologies targeting different architecture layers are merging towards a integrated software-defined infrastructure, we would expect the future comprehensive SOAR approaches emerge from combining the use of multiple virtualization techniques.

Answering RQ1.3 - What are the application domains of the systems supported by the SOAR methods? Most primary studies are not domain-specific, except #9 that has the use cases related to e-commerce and e-health, and #14 is specialised for Unmanned Aerial Vehicles (UAVs). Recent approaches that leverage AI/ML (e.g., #12, #11, #20) have not addressed the cross-layer/system/domain aspects. It is also worth exploring the use of digital twin solutions, and DevSecOps (only #11 presenting policies as code enforcement) or SecDevOps as part of SOAR solutions to co-evolve with the systems being defended against continuously evolving threats.

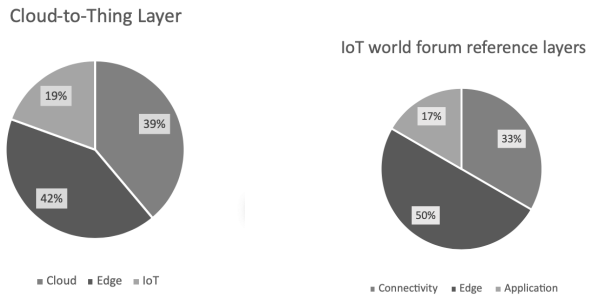
Nevertheless, some notable application domains include the telecom and networking sphere, where data transmission is paramount, SOAR ensures the integrity and confidentiality of communication channels. By automating incident response processes and orchestrating security measures, it mitigates risks associated with network breaches, ensuring uninterrupted connectivity and data flow (#22, #19).

In e-commerce and banking sectors, where sensitive financial information flows incessantly, SOAR also can act as a reliable guardian mechanism. It automates fraud detection, orchestrates timely responses to security incidents, and fortifies transactional systems against malicious activities. Through rapid threat detection and response, it preserves the trust of consumers and the integrity of financial transactions (#20). In the realm of e-health, where the convergence of IoT and healthcare revolutionizes patient care, SOAR emerges as a critical safeguard. It ensures the confidentiality and availability of patient data, orchestrating security protocols to thwart unauthorized access and data breaches #9. By automating incident response in real-time, it secures medical devices and health records, bolstering patient safety and privacy. Across general IoT applications, spanning smart homes, industrial automation, and transportation, SOAR is indispensable. It defends against diverse threats targeting IoT devices, such as malware infections and unauthorized access attempts. By automating security workflows and orchestrating responses, it fortifies IoT ecosystems against cyber-attacks, ensuring the reliability and resilience of interconnected systems.

B. Low-Level Details (RQ2)

Answering RQ2.1 - What SOAR approaches combining different SOAR solutions for different layers (system of systems perspective)?

As discussed before, SOAR solutions typically involve and orchestrate multiple security components possibly deployed on multiple nodes across the whole computing continuum. Regarding the infrastructure layer at which the security components are deployed (see Fig. 1a), we found that most of them are located at the Cloud and Edge layers (e.g., #7, #18, #22). There is only very little support for the Things/IoT layer (#14, #21, #15, #17, #6, #8, #10). This remains a major limitation in existing SOAR solutions for the computing continuum as Things (i) can embed actuators, which can have a direct impact of the physical environment possibly raising safety concerns; and (ii) are typically largely broadening the exposure to threats of IoT/CPS systems. The latter is in particular due to the fact that IoT systems typically embed numerous Things, which can be geographically distributed and thereby operating in different cyber-physical contexts (i.e., with their own threats), often close to the users (i.e., devices can be accessible to human, making it possible to physically harm them).



(a) (b)

Fig. 1: SOAR solutions for different layers

We believe this limitation mainly applies to the reaction mechanisms and is largely due to the limited support at the IoT layer for software-defined approaches. This, by contrast with monitoring mechanisms that seldomly need to be adapted. Reaction, and in particular automatic reactions, requires being able to reach heterogeneous devices to adapt a parameter or the structure of the software they are operating. Software-defined approaches are key to enable such adaptation as they provide homogeneous abstraction for programmatically running parameter or structural adaptation at the network (SDN) or infrastructure (SDI) levels. Whilst these approaches

are now becoming widely used at the Cloud/Edge layers, with lightweight containerization for instance, they are mostly impractical at the IoT layer due to limited computing capabilities.

A key focus for several of our primary studies (e.g., #19, #22, #20) are the Connectivity and Edge layers of the IoT world forum reference model (Fig. 1b). This seems to be a natural first step for SOAR solutions as networking is making the glue between security solutions and reconfiguring network enables their orchestration. SDN and NFV are the preferred solutions as they enable dynamic reconfiguration of the network in an abstract layer which is independent from the technology used by the orchestrated security components.

Answering RQ2.2-What are security mechanisms used in the existing SOAR solutions?

On the subject on how to create a SOAR based on the integration of multiple security elements, there is a focus on using network mechanisms for detection and execution, policies for security application, and additionally, custom crafted solutions for orchestrating the tools. In many of the primary studies are a bias to create the SOAR from a central defense mechanism rather than merging different defense system into a fully orchestrated solution.

Regarding where the mechanisms are applied, there is a clear preference to control systems via their connections or acting on the network layer (#14,#13,#18,#22,#19,#11,#23,#17,#15,#12,#21) through Network Virtualization Functions (NFVs), Network Security Functions (NSFs), Software Defined Networks (SDNs) or Virtual LANs (VLANs). Other studies, as #22,#19, present solutions that act on network reconfiguration changes as primary mechanism, and some other studies use honeypots management as the starting point to create a SOAR solution (#22,#19,#11,#21). There is little research acting on controls into the host, like antivirus, kill processes or update vulnerable dependencies, explained partially because control of the host to isolate it (network) or deviate from the attacker (as honeypots do) are very successful techniques to prevent or detect attacks at an early phase instead of trying to recover the host after an attack to the normal situation.

When dealing on how controls are managed and enforced into the different elements of the system to be secured, policy-based techniques are the mainstream (#14,#20,#23,#17,#12,#9) approach compared to other dedicated rule-based only and custom-made techniques. In this case, policies bring several benefits. On one hand, they provide a simple structured way to enforce security mechanisms to keep a system safe or to be applied when an incident is detect. The policies can contain different information, and can be stored and transmitted as information instead of being a program with fixed rules. Reverting and applying new updated policies is also simpler in the target machines. On the other hand, policies allows for additional layer of abstraction to enforce security mechanisms on heterogeneous systems, thus allowing to apply the same security policies to servers with different operating systems, different web server implementations or different network devices.

In order to build an orchestrated security response framework, the lack of standardized approaches compared to custom-made orchestrations is significant. While this seems a problem for future evolution of these SOAR solutions, this can be explained by the fact that many primary studies focus on a single security mechanism to protect a system, and then creates the rest of the infrastructure to handle the security in a coordinated way adding only additional mechanisms that are suitable as support tools for the main defense mechanism. In our primary studies selection custom orchestration is present in #14,#20,#23,#17,#12,#9 while workflow engine based or playbook based orchestration are usually named on primary studies when the objective is to provide an architecture reference #16 or when there is a focus on using standards #6 on the creation of SOAR solutions.

The type of mechanisms used or recommended in the different articles object of this study are not only the aforementioned ones for networking management and virtualization, honeypots, orchestration engines or polices, but also AI/ML (#22,#11,#23,#20,#6) , Information and Incident Sharing (IS) systems (#13,#16), resilience-based controls (#17,#15) or digital twins (#10,#8). An integral SOAR solution could use some mechanisms for network control, policy based enforcement and an engine to start and orchestrate the responses as minimal capabilities for simple and efficient response in most of the cases, while adding more mechanisms are beneficial as support tools, secondary layer of protection or when targeting specific requirements of the system to be secured.

Answering RQ2.3 - What is the landscape of using AI, SecDevOps approaches, Digital Twin approaches for SOAR?

The integration of AI, SecDevOps, and Digital Twin approaches within SOAR systems can be found in the literature by a diversity of applications and conceptual models. The literature surveyed describe Digital Twins as an emerging technology of critical importance, particularly in enhancing the security of IoT environments. Their utilization demonstrate a current trend in applying virtual models to simulate, predict, analyse, and respond to security scenarios #8.

Despite being less discussed in the literature, the role of AI within SOAR is present with a big importance. Its application is found within intent-based security policies, with Natural Language Processing (NLP) and generative AI models supporting the creation and classification of security policies #23. Additionally, AI's use is presented in decision tress to classify anomalies #12, which suggest a trend toward intelligent automation within the domain.

The SecDevOps methodology is not a dominant theme in the surveyed literature but is referenced in relation to abstracting security controls. These controls are envisioned as services designed to simplify cybersecurity operations, particularly within software-defined systems #20. Furthermore, the presence of SecDevOps within SOAR is implied through the automation of security policy generation #23, #12 and the development of metrics that enhance resilience of CPS #17.

However, it is important to note that a significant portion of the literature surveyed does not explicitly explore the intersec-

tion of AI, SecDevOps, and Digital Twins with SOAR, except #3, #7. This gap in the literature may indicate an emerging area of study that could benefit from further exploration. Overall, the current scenario suggests a growing interest in leveraging these technologies to enhance the efficacy and responsiveness of SOAR solutions, with Digital Twins showing a relatively more defined role compared to the integration of AI and SecDevOps methodologies.

C. Gaps and Limitations (RQ3)

Based on the studied literature, we summarize below the limitations and gaps related to the existing SOAR approaches:

- Comprehensive SOAR targeting multiple architectural aspects are missing, potentially based on interoperable virtualization of different system layers.
- AI/ML Integration: Recent approaches leveraging AI/ML have not sufficiently addressed cross-layer/system/domain aspects, and limited in the explainability. This limitation suggests a gap in integrating advanced technologies like AI/ML into SOAR solutions comprehensively.
- Digital Twin Solutions: While mentioned as a potential avenue for exploration, the actual integration of digital twin solutions into SOAR frameworks has only been touched upon recently. This represents a gap in utilizing emerging technologies like Digital Twins to enhance SOAR capabilities.
- DevSecOps/SecDevOps Integration: The adoption of DevSecOps or SecDevOps as part of SOAR solutions is mentioned, but only one study is presented with policies as code enforcement. This indicates a gap in incorporating DevSecOps/SecDevOps principles into SOAR methodologies.
- Limited Application Domains: While SOAR shows promise in various application domains such as telecom, banking, and e-health, there may be other sectors where its potential remains untapped. Exploring and addressing this limitation could broaden the scope of SOAR usage and build a generic SOAR solution customizable to fit the requirements of each sector.
- IoT Layer Support: Existing SOAR solutions primarily focus on Edge and Cloud layers, with limited support for the Things/IoT layer. This presents a significant gap, considering the increasing importance of IoT devices and their vulnerability to cyber threats.
- Software-defined approaches: The impracticality of software-defined approaches at the IoT layer due to limited computing capabilities of IoT devices poses a challenge. This limitation hampers the adaptability and effectiveness of SOAR solutions in IoT environments.
- Preference for Network Mechanisms: There is a clear preference for network mechanisms over host-based controls in SOAR implementations. This bias may overlook potential security enhancements that host-based controls could offer, indicating a gap in comprehensive security coverage.
- Lack of Standardized Orchestration Solutions: Custom-made orchestration is often employed due to the lack of standardized solutions for orchestrating responses in SOAR frameworks. This suggests a need for standardized approaches to streamline and enhance SOAR orchestration processes.
- Underexplored Intersection with AI, SecDevOps, and Digital Twins: While there are diverse applications of AI, SecDevOps, and Digital Twins within SOAR systems, the literature lacks comprehensive studies addressing the integration of these technologies. This gap highlights an opportunity for future research to explore the synergies and potential benefits of integrating these technologies into SOAR frameworks. Our review found a few recent studies addressing the integration of Digital Twins, AI, and SecDevOps in SOAR, highlighting a promising research direction.

These limitations and gaps suggest areas where further research and development efforts could enhance the effectiveness, adaptability, and comprehensiveness of SOAR solutions in addressing evolving cybersecurity challenges.

V. Related Work

Islam et al. [19] report a review on the security orchestration approaches including the execution of incident response strategy against a threat, the integration of several security systems, and cooperative security solutions. This paper gives a taxonomy of the various aspects of security orchestration approaches such as key functionalities, quality requirements, key components. The authors also present their findings in terms of the open research problems and difficulties in the area of security orchestration. The paper does not specifically analyse or include primary studies from the perspectives of computing continuum or IoT/Fog/Edge aspects. There are little details about the life-cycle management of a security orchestration/workflow. For example, it is not clear what languages or concepts that the primary studies specify security orchestrations, how security orchestrations are designed, how interoperability is handled, and how far orchestration goes from an infrastructure perspective (coverage of the IoT/Edge end). Moreover, for modern systems spanning the whole computing continuum, i.e., IoT/Fog/Edge/Cloud, it is challenging to evolve/maintain the security orchestrations as well as dynamically adapt them, e.g., how probes/agents are placed and deployed, how data are aggregated from different layers.

The review paper by Kinyua and Awuah [20] overviews the use of Machine Learning (ML) techniques in SOAR systems to support one or several activities of the so-called PICERL (Planning–Identification–Containment–Eradication–Recovery–Lessons learnt) framework. The authors conclude that to date there was no ML-driven SOAR solution fully supporting all of these steps (mainly focusing on ICER), but still highlight the growing importance of ML in SOAR. The increased use of ML is motivated by the amount of data needed to be processed with minimum time delay in order to generate adequate and timely response, which goes beyond the manual

capabilities of SOC human personnel. Examples of such data-intensive and time-critical tasks include network intrusion detection, anti-virus defence, detection and classification of malware emails, etc. To achieve these conclusions, the paper reviewed 11 commercially available SOAR frameworks, as well as the state-of-the-art research efforts.

Regarding practical usage, [15] describes the evaluation of six commercial SOAR tools from the human operator perspective, with respect to diverse characteristics ranging from usability, to speed to resolve incidences and to usefulness of the information provided by the SOARs. This analysis is based on results of performing real-life testing scenarios like network intrusion detection or suspicious activity from an insider IP address. Differences in experience level of the operators are also taken into account. The main insights of the evaluation are that the configuration phase of each SOAR tool is critical to get sound results, and that the operators' actually perceived increased efficiency in incident resolution by the SOAR. Other major results were that there were some negative correlations between operator tool preference and tool performance, and that a wide variability exists among these SOARs in resilience to resolve incidents under degraded internet connections.

VI. Conclusions

This paper has provided a systematization of knowledge in security orchestration, which is important in the protection of critical infrastructures across sectors. The escalating integration of digital and physical realms, particularly through IoT/CPS technologies, has intensified the complexity and interdependence of these infrastructures, rendering them more susceptible to evolving cyber threats. To address these challenges, a systematic approach to security orchestration and response (SOAR) is paramount. While current SOAR solutions have primarily focused on individual layers of critical systems, there exists a critical gap in developing holistic strategies that span the diverse layers of IoT/CPS-based infrastructures. Integrating advanced technologies like AI/ML, digital twin solutions, and DevSecOps into SOAR frameworks holds promise for bolstering resilience and adaptability in the face of ever-evolving threats. Through our study, we have illuminated these gaps and underscored the imperative for tailored SOAR approaches to safeguard critical infrastructures, paving the way for future research and development in this crucial domain.

References

[1] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, 2010.

[2] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial internet of things security: Requirements and fog computing opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020.

[3] F. Martinelli and O. Osliak, *Access Control for Cyber-Physical Systems*. Cham: Springer Nature Switzerland, 2025, pp. 4–9. [Online]. Available: https://doi.org/10.1007/978-3-030-71522-9_1718

[4] T. Dimitrakos, J. Lopez, and F. Martinelli, *Collaborative Approaches for Cyber Security in Cyber-Physical Systems*. Springer, 2023.

[5] P. Ferreira and E. Bellini, "Managing interdependencies in critical infrastructures—a cornerstone for system resilience," in *Safety and Reliability–Safe Societies in a Changing World*. CRC Press, 2018, pp. 2687–2692.

[6] F. Spegni, A. Sabatelli, A. Merlo, L. Pepa, L. Spalazzi, and L. Verderame, "A precision cybersecurity workflow for cyber-physical systems: The iot healthcare use case," in *Computer Security. ESORICS 2022 International Workshops*, S. Katsikas, F. Cuppens, C. Kalloniatis, J. Mylopoulos, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, M. A. Sotelo Monge, M. Albanese, B. Katt, S. Pirbhulal, and A. Shukla, Eds. Cham: Springer International Publishing, 2023, pp. 409–426.

[7] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliability Engineering & System Safety*, vol. 152, pp. 137–150, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832016000508

[8] U. Bartwal, S. Mukhopadhyay, R. Negi, and S. Shukla, "Security orchestration, automation, and response engine for deployment of behavioural honeypots," in *2022 IEEE Conference on Dependable and Secure Computing (DSC)*, 2022, pp. 1–8.

[9] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernández, "Honeydoc: An efficient honeypot architecture enabling all-round design," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 683–697, 2019.

[10] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, and J. Yusupov, "Towards a fully automated and optimized network security functions orchestration," in *2019 4th International Conference on Computing, Communications and Security (ICCCS)*, 2019, pp. 1–7.

[11] M. De Donno, K. Tange, and N. Dragoni, "Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog," *IEEE Access*, vol. 7, pp. 150 936–150 948, 2019.

[12] B. Kitchenham, S. Charters *et al.*, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[13] A. W. Mir and R. K. Ramachandran, "Implementation of security orchestration, automation and response (soar) in smart grid-based scada systems," in *Sixth International Conference on Intelligent Computing and Applications*, S. S. Dash, B. K. Panigrahi, and S. Das, Eds. Singapore: Springer Singapore, 2021, pp. 157–169.

[14] C. Islam, M. A. Babar, and S. Nepal, "Architecture-centric support for integrating security tools in a security orchestration platform," in *Software Architecture*, A. Jansen, I. Malavolta, H. Muccini, I. Ozkaya, and O. Zimmermann, Eds. Cham: Springer International Publishing, 2020, pp. 165–181.

[15] R. A. Bridges, A. E. Rice, S. Oesch, J. A. Nichols, C. Watson, K. Spakes, S. Norem, M. Huettel, B. Jewell, B. Weber *et al.*, "Testing soar tools in use," *Computers & Security*, vol. 129, p. 103201, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823001116

[16] M. Nyre-Yu, "Identifying expertise gaps in cyber incident response: Cyber defender needs vs. technological development," *scholarspace*, 2021. [Online]. Available: https://scholarspace.manoa.hawaii.edu/items/c70197b1-4bd5-4273-9528-72dbff298d92

[17] G. A. Moreno, J. Cámara, D. Garlan, and B. Schmerl, "Proactive self-adaptation under uncertainty: a probabilistic model checking approach," in *Proceedings of the 2015 10th joint meeting on foundations of software engineering*, 2015, pp. 1–12.

[18] Juxtology, "IoT: Architecture," Juxtology, 2018. [Online]. Available: https://www.m2mology.com/iot-transformation/iot-world-forum/

[19] C. Islam, M. A. Babar, and S. Nepal, "A multi-vocal review of security orchestration," *ACM Comput. Surv.*, vol. 52, no. 2, apr 2019. [Online]. Available: https://doi.org/10.1145/3305268

[20] J. Kinyua and L. Awuah, "Ai/ml in security orchestration, automation and response: Future research directions." *Intelligent Automation & Soft Computing*, vol. 28, no. 2, 2021.