Towards Smarter Security Orchestration and Automatic Response for CPS and IoT

Phu Nguyen, Rustem Dautov, Hui Song
SINTEF
Oslo, Norway
firstname.lastname@sintef.no

Angel Rego, Eider Iturbe, Erkuden Rios,
Diego Sagasti, Gonzalo Nicolas
TECNALIA
Bilbao, Spain
firstname.lastname@tecnalia.com

Valeria Valdes, Wissam Mallouli, Ana Rosa Cavalli
Montimage EURL
Paris, France
firstname.lastname@montimage.com

Nicolas Ferry
Université Côte d'Azur, I3S
Sophia Antipolis, France
nicolas.ferry@univ-cotedazur.fr

***Abstract*—Current security orchestration and response (SOAR) approaches have primarily focused on specific layers of systems, such as Intrusion Detection Systems, the network layer, or the application layer. We aim to find the gaps in the existing SOAR approaches for IoT/CPS-based systems, especially critical infrastructures, and propose some directions to fill in these gaps. This paper presents a literature survey and future research directions for advancing SOAR towards increased automation and more holistic operation, especially for the cyber-physical security of critical infrastructures. We have found 14 primary SOAR studies and discussed the gaps in general. There is a significant gap when it comes to a comprehensive and systematic approach to SOAR for multi-layered systems using IoT/CPS and considering the computing continuum perspective. To address the gap, we present our on-going work on a framework of multi-layer SOAR decision-making methods and orchestration tools that leverage Reinforcement Learning (RL)-based adaptation intelligence, virtual reality, avatar-human interaction and advanced Cyber Threat Intelligence (CTI) tools.**

***Index Terms*—Security Orchestration, CPS, IoT, Machine Learning, VR, CTI**

I. Introduction

The security of Critical Infrastructures (CIs) 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 CIs have become more intricate, vital, and interdependent than ever before. IoT/CPS-based CIs spanning across the computing continuum are increasingly becoming digitalized, connected, and distributed. 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. This vulnerability is evident in the rising number of cyber-security 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. Traditional static methods for IoT security can not handle this level of complexity [2], [3].

Security orchestration integrates tools and technologies to respond to incidents in a timely manner [4]. 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 set of activities performed by security experts and security tools to improve the response to a security event [5]. Security Orchestration Automation and Response (SOAR) mechanisms are security techniques to be employed on incident management. 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 from a certain user. Existing SOAR approaches such as [6], [5], [7] have mainly focused on specific layers of systems such as Intrusion Detection Systems (IDS), network layer, or application layer, or they are vendor-specific solutions as reviewed for the Smart Grid-Based SCADA Systems [4].

In this paper, we present a literature survey and our research directions for advancing SOAR towards increased automation and holistic operation, especially for the cyber-physical security of CIs. A systematic approach to SOAR at different layers of CIs is essential. This includes real-time SOAR, as well as continuous improvement and development of preventive security solutions while the systems and security threats are evolving. To this end, we are developing a framework of dynamic autonomous adaptation to improve resilience of interconnected CIs. Our framework is composed of multi-layer SOAR decision-making methods and orchestration tools that leverage Reinforcement Learning (RL)-based adaptation intelligence, virtual reality, avatar-human interaction and advanced Cyber Threat Intelligence (CTI) tools.

II. Literature Survey

In this section, we discuss the primary SOAR studies that we have found using the snowballing method [8]. First, we started with a set of eight papers that we have known of (see Table I, the first eight rows). This start set is not too small because of our strict selection criteria, i.e., must address the key SOAR aspects, such as having a good enough architecture of SOAR (orchestrator, infrastructure layer), orchestration/master control of security/resilience mechanisms, (directly/indirectly) targeting CPS/IoT. The start set covers different publishers, years, and authors. Based on this set, we snowballed recursively in both directions, i.e., backward and forward. This process allowed us to cover more than a thousand candidate papers. We first filtered the candidate papers based on their titles and abstracts. Only when we found the titles and abstracts of interest for SOAR, we continued to skim and scan through the contents of the candidate papers. For every paper kept until the skimming and scanning phases (16 in total), we consolidated the outcomes in group discussions among the authors to cross-check the selection decisions. Finally, we ended up with six more primary SOAR studies found during the snowballing process to make a total of 14 primary SOAR studies.

The 14 existing SOAR approaches surveyed in Table I have mainly focused on a specific layer of systems such as IDS (papers #2, #9, #14), network layer (#2, #5, #10, #11, #14), or application layer (#1, #6, #8), or very specific mechanisms for resilience of CPS (#3, #4, #10). There is a lack of a systematic approach for SOAR for the multi-layered systems using IoT/CPS, computing continuum perspective. Furthermore, there is a need to address the cascading effects in cross-layer, cross-systems, cross-physical-cyber domain, and even cross-application domain scenarios. Recent approaches that leverage AI/ML (e.g., #1, #2, #13) have not addressed the cross-layer/system/domain aspects. It is also worth exploring the use of digital twin solutions, and DevSecOps (only #2 presenting policies as code enforcement) or SecDevOps as part of SOAR solutions to co-evolve with the systems being defended against continuously evolving threats.

III. Towards Dynamic Autonomous Adaptation for Resilience

To fill in the gaps discussed above, we are designing and developing a framework of dynamic autonomous adaptation to improve resilience of interconnected CIs as depicted in Fig. 1. The framework will be used by CI operators to automatically monitor, analyse, plan and deploy adaptation strategies during system operation. The framework includes the following main methods and tools:

- Intelligent decision-making methods supporting the CI adaptation in the face of business continuity risks incidents, including the escalation and de-escalation of responses. For every security alert, RL-based intelligence will be used to autonomously devise a response strategy, as well as improve in the long-term the adaptation strategies that combine automatic system level and manual responses (SOAR4BC).

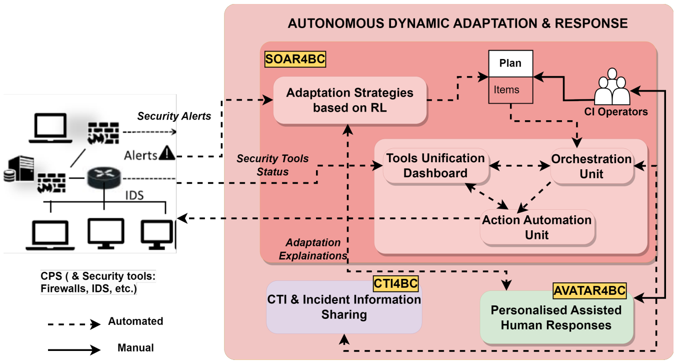
AUTONOMOUS DYNAMIC ADAPTATION & RESPONSE
SOAR4BC
Adaptation Strategies based on RL
Plan
Items
CI Operators
Security Alerts
Alerts
IDS
Security Tools Status
Tools Unification Dashboard
Orchestration Unit
Action Automation Unit
Adaptation Explainations
CTI4BC
CTI & Incident Information Sharing
AVATAR4BC
Personalised Assisted Human Responses
CPS (& Security tools: Firewalls, IDS, etc.)
Automated
Manual

Fig. 1: Dynamic Autonomous Adaptation for Resilience of Critical Infrastructures

- Multi-layer SOAR decision-making methods and orchestration tools (security tools unification, orchestrator and automation unit) to work as system level response, which leverage long-term adaption intelligence to address recovery (SOAR4BC).
- Avatar-shaped real-time personalised assistance and automatic generation of response recommendations for CI operators and Security Operations Center (SOC) operators (AVATAR4BC).
- Methods and tools to facilitate the compliance with cybersecurity information sharing policy requirements of NIS Directive 2.0 (CTI4BC).

A. Multi-layer Security Orchestration and Automatic Response-SOAR4BC

By offering strong event detection, situational awareness, and autonomous adaptation capabilities, we seek to equip CI operators in successfully countering growing threats. We are developing SOAR4BC, which is a state-of-the-art AI-based SOAR solution to enable self-healing across various CI system levels, improving recovery through continuous learning of system status and control effectiveness. It does so by utilizing multi-layer (digital twin-based) SOAR decision-making methodologies and orchestration tools. Our SOAR strategy provides seamless integration into CI operations by embracing SecDevOps practices.

The SOAR4BC service, which is equipped with deep RL-based adaptation intelligence, automatically organises a combination of automatic and human solutions in reaction to a newanomaly (e.g., a security alert) to reduce the estimated business continuity risks in real-time. In SOAR4BC, AI-based response adaptability and actionable security improve decision-making and orchestration processes by identifying the best security countermeasures depending on the current system state, risk information and detection information. It allows for generalization over unseen situations and devises instant responses and long-term solutions naturally for linked critical infrastructure assets. The SOAR4BC platform provides the optimisation of security strategies, tactics, and decision support (especially by explaining deep RL decisions to human

TABLE I: Surveyed SOAR studies

#	Year	PV	Title (click to open the corresponding publication)
#1	2022	Elsevier (J)	An automated closed-loop framework to enforce security policies from anomaly detection
#2	2022	IEEE (C)	Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots
#3	2020	IEEE (J)	Switched-based Resilient Control of Cyber-Physical Systems
#4	2020	IEEE (C)	Cyber-Resilience Evaluation of Cyber-Physical Systems
#5	2017	NDSS (C)	Precise security instrumentation for enterprise networks
#6	2016	IEEE (W)	Orchestration of Software-Defined Security Services
#7	2011	IEEE (C)	System-Aware Cyber Security
#8	2009	IEEE (C)	Policy-based security configuration management, application to intrusion detection and prevention
#9	2023	MDPI (J)	PALANTIR: An NFV-Based Security-as-a-Service Approach for Automating Threat Mitigation
#10	2022	Scitepress (C)	Switched-based control testbed to assure cyber-physical resilience by design
#11	2022	IEEE (J)	Decentralized Resilient Output-Feedback Control Design for Networked Control Systems Under Denial-of-Service
#12	2020	Springer (C)	Architecture-centric support for integrating security tools in a security orchestration platform
#13	2019	Springer (C)	Automated Interpretation and Integration of Security Tools Using Semantic Knowledge
#14	2019	IEEE (J)	HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design

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

CI operators in natural language) by taking into account deployed safeguards and real-time risk levels.

Based on the optimal adaptation strategies, the SOAR4BC orchestrator (orchestration unit) can quickly supply, continually construct, deploy, and decommission security mechanisms (via tools unification) and system re-configurations (via action automation unit) to accommodate changing defence requirements and containment strategies. Following specified response methods, this module automates the synchronisation of multi-layer security procedures across many organisations, cloud services, and infrastructures. The self-healing techniques of SOAR4BC include isolating damages through Software-Defined Networking (SDN) capabilities and minimising cascade failures, e.g., in the case of energy operators of important services, to minimize wide-area blackouts or blackouts in regions that supply power to other vital infrastructures.

B. Real-time Personalised Assistance for CIs operators-AVATAR4BC

The objective of AVATAR4BC is offering human level responses to support CIs resilience. AVATAR4BC aims at augmenting informed human decision-making processes and clarifying the actions that CI operators and SOC operators should take in each case. In accordance with the human responses defined in the ”Plan” from SOAR4BC (Fig. 1), AVATAR4BC provides personalised technical assistance in real time, directed to the point of interest in each case. This customisation is delivered not only from a technical point of view, but also based on a psychological and behavioural point of view of the human operators. In addition, to ease the human-machine interaction, an avatar is developed for CI operators and SOC operators to guide them during the reaction and recovery processes, suggesting instructions, recommendations, and access to required digital evidences. Human operators are involved in the long-term recovery process, even if automation is important for short-term reactions. In this case, digital avatars help them by offering individualised advice on the steps to be performed.

AVATAR4BC is modelled as a realistic human 3D model, which is tailored to the operator's preferences in form and behaviour. This implies that, based on psychological information, AVATAR4BC adapts its appearance and responses to the operator's needs at any given moment. AVATAR4BC provides the operator with human-realistic responses to problems occurring in the CI, supplying guidance during the reaction and recovery processes, and offering easy-to-follow instructions, recommendations, and access to the necessary digital evidences, thus helping human-machine interaction. These interactions are based on responses generated by AVATAR4BC using an AI-based explanation system and translated into an audio-animation pair, allowing the 3D model to talk.

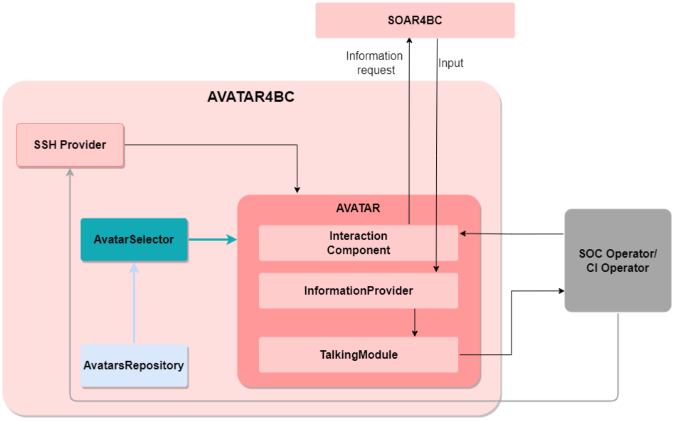

Fig. 2: AVATAR4BC architecture

This audio-animation response is generated using two different AI systems. One of them is an AI-driven text-to-speech system [9], which provides a realistic audio speech sample generated in real time. On the other hand, an AI-powered audio-to-face system [10], uses the audio speech sample to produce real-time facial animations. As the animations are produced, the human 3D model (avatar) receives and applies them to its own facial model, combining them with predefined animations emulating human behaviour. At the same time, the avatar plays the voice sample and synchronises it with the animations.

C. Information Sharing with other CIs and CERTs-CTI4BC

CTI4BC, the component for incident information sharing, is essential in automatically producing customised incident and Indicators of Compromise (IOCs) information for various stakeholders. In accordance with NIS Directive 2.0, CTI4BC smoothly integrates with SOAR4BC to enable dynamic extraction and distribution of digital evidence (traces) across multiple actors. The component connects with open CTI systems like MISP[1], providing extra information, to improve automation in CTI sharing and issue notification. CTI4BC serves as a common conduit or CTI Community Feed for voluntary exchange, offering rationalised data on cutting-edge threats and viable countermeasures to improve CTI for more effective detection.

To ensure confidentiality, the shared information undergoes anonymization processes to protect the identity of sharing organizations and maintain privacy regarding any personally identifiable information contained in the digital evidences. In terms of incident reporting, CTI4BC facilitates notifications to relevant stakeholders, including Computer Security Incident Response Teams (CSIRTs), aiming to streamline incident handling. It enables incident reports to include insights on disruption risk levels and potential cascading effects on other organizations and critical infrastructures, enabling CSIRTs to proactively respond and notify them accordingly.

The CTI process involves the consideration of both source and product of CTI. The source refers to the input data received by the CTI4BC component, which provides security-related information to the component to understand and process the event, while the product represents the end result of the threat intelligence process. Both source and product of CTI4BC contribute to the availability of security-related data about an event. The sharing of information within CTI4BC encompasses both vertical and horizontal sharing. Vertical sharing involves the exchange of information among components within the same CI, while horizontal sharing entails sharing information between CTI4BC instances designed for different CIs. This multi-dimensional sharing approach promotes collaboration and enhances the overall effectiveness of CTI4BC in addressing cyber threats and safeguarding critical infrastructures.

Furthermore, the sharing of information through CTI4BC and the utilization of simulation capabilities play a crucial role in managing cascading effects. By exchanging relevant data on incidents and threats, CTI4BC enables organizations and stakeholders to gain a better understanding of the potential effects of an incident across interconnected systems and CIs. Subsequently, simulation and modelling tools can analyse potential impacts and cascading effects of cyber incidents on the CI. This simulation process provides valuable insights into critical points of failures and vulnerabilities within the system enabling proactive identification and mitigation of potential risks.

IV. Conclusion

This paper presents a literature survey and our research directions for advancing SOAR approaches towards increased automation and more holistic functionality. More specifically, we have identified and discussed the gaps across 14 primary SOAR studies, such as the lack of adaptation for multi-layered systems or the sparse use of AI-based auto- matic response. To address the gaps, we show our on-going work on a framework that is equipped with intelligent orchestration capabilities, enabling the security management across the different computing continuum layers in a unified way. The solution includes enhanced virtual reality, by using interactive avatars, to help security operators in the decision making. Additionally, a Cyber Threat Intelligence tool, integrating automatic enrichment data processes and privacy and anonymization services to control information visibility, provides a comprehensive picture of incident causes, related information, and sharing of information in a protected way.

Acknowledgment

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

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] 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), pp. 409–426, Springer International Publishing, 2023.

[3] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliability Engineering & System Safety*, vol. 152, pp. 137–150, 2016.

[4] 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), pp. 157–169, Springer Singapore, 2021.

[5] 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), pp. 165–181, Springer, 2020.

[6] 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)*, pp. 1–8, 2022.

[7] S. Luo and M. Ben Salem, "Orchestration of software-defined security services," in *2016 IEEE International Conference on Communications Workshops (ICC)*, pp. 436–441, 2016.

[8] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, pp. 1–10, 2014.

[9] E. Casanova, J. Weber, C. D. Shulby, A. C. Junior, E. Gölge, and M. A. Ponti, "Yourtts: Towards zero-shot multi-speaker tts and zero-shot voice conversion for everyone," in *International Conference on Machine Learning*, pp. 2709–2720, PMLR, 2022.

[10] G. Tian, Y. Yuan, and Y. Liu, "Audio2face: Generating speech/face animation from single audio with attention-based bidirectional lstm networks," in *2019 IEEE international conference on Multimedia & Expo Workshops (ICMEW)*, pp. 366–371, IEEE, 2019.

[1] https://www.misp-project.org/