A SOAR platform for standardizing, automating operational processes and a monitoring service facilitating auditing procedures among IoT trustworthy environments

A SOAR platform for standardizing, automating operational processes

Vasiliki G.Bilali*

Institute of Communication & Computer Systems (ICCS), giovana.bilali@iccs.gr

Eustratios Magklaris

Institute of Communication & Computer Systems (ICCS), stratos.magklaris@iccs.gr

Dimitrios Kosyvas

Institute of Communication & Computer Systems (ICCS), dimitris.kosyvas@iccs.gr

Lazaros Karagiannidis

Institute of Communication & Computer Systems (ICCS), l.karagiannidis@iccs.gr

Eleftherios Ouzounoglou

Institute of Communication & Computer Systems (ICCS), eleftherios.ouzounoglou@iccs.gr

Angelos Amditis

Institute of Communication & Computer Systems (ICCS), a.amditis@iccs.gr

Advanced Threat Intelligence Orchestrator (ATIO) is a sophisticated middleware solution designed to enhance unified threat management (UTM) monitoring processes by adhering Security Orchestration Automation Response (SOAR) capabilities. This paper provides a detailed overview of ATIO, highlighting its multitasking capabilities towards coordinating information from different types of tools, usually bringing with them different types of data. Also, it gives some details on the system implementation and some indicative operational workflows. Central to ATIO's functionality is its ability to concurrently or sequentially automate the execution and processing steps of multiple workflows, while adhering to cyber security standards, organization policies and regulations. The design of ATIO is flexible, accommodating various interconnected services and tools to meet specific requirements, as well as diverse infrastructure interfaces, accommodating different specifications seamlessly adhering standardized formats and Cyber Threat Information (CTI) languages, such as STIX2.1. This integration enhances interoperability and expands the scope of cyber-threat intelligence operations by enabling connectivity with various systems and diversified data types. Moreover, ATIO automation nature, boosting detection and acknowledge efficiency and

* Place the footnote text for the author (if applicable) here.

responsiveness in threat intelligence operations. It enables users to alter and filter workflow steps, preparing information for correlation and tracking cyber threat information (CTI) effectively. Additionally, ATIO includes robust mechanisms for monitoring user actions within the system, ensuring accountability and providing valuable insights into operational activities.

CCS CONCEPTS • Orchestration• Automated Standardized Processes • Workflow Execution

Additional Keywords and Phrases: SOAR, Workflow Monitoring application, Integrated infrastructure interfaces

ACM Reference Format:

First Author's Name, Initials, and Last Name, Second Author's Name, Initials, and Last Name, and Third Author's Name, Initials, and Last Name. 2018. The Title of the Paper: ACM Conference Proceedings Manuscript Submission Template: This is the subtitle of the paper, this document both explains and embodies the submission format for authors using Word. In Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY. ACM, New York, NY, USA, 10 pages. NOTE: This block will be automatically generated when manuscripts are processed after acceptance.

1 INTRODUCTION

In today's interconnected world, the integration of information technology (IT) and operational technology (OT) services, coupled with diverse communication levels and data types, presents a complex landscape across diversified environments. However, with this increasing sophistication comes the potential for processes and services to encounter disruptions. From industrial sites to incident security centres and healthcare facilities, the architecture of these environments continues to evolve, incorporating a mix of cloud and edge computing, traffic data, message-based data, and reports in various formats nested together with various log types.

When it comes to a cyber threat event the above data diversity makes the life of Security Analysts harder. Make difficult to recognize if the cyber event happened is either an attack or a system vulnerability confusing alerts with notifications. Taking on step further, the integration of IT and OT, along with the proliferation of communication levels and data types, introduces several challenges and hurdles in technical and decisional level that organizations must navigate. These hurdles include ensuring seamless interoperability between disparate systems, managing the security risks associated with interconnected networks, and maintaining operational efficiency through evolving technological landscapes. Moreover, the potential for process and service breakdowns underscores the critical need for robust solutions that can effectively manage and mitigate these risks.

Automation emerges as a key strategy to address the complexities and challenges inherent in today's environments. Across various fields, automation technologies offer the promise of streamlining processes, enhancing operational efficiency, and improving overall system resilience. However, the landscape of automation is vast, with multiple technologies available to address specific needs and requirements.

Also log storage and retrieval is considered as a backup solution for organisations. More specifically, the daily processes stored securely to encrypted databases or to trust worthy environments and is ready to retrieved when recovery or self-recovery plan must be activated.

In this context, the Advanced Threat Intelligence Orchestrator (ATIO) [1] represents a full-stack comprehensive middleware solution designed to tackle the complexities of cyber threat intelligence management within diverse environments. By concurrently automating the execution of multiple workflows while adhering to industry regulations and standardized procedures and formats, ATIO offers organizations a powerful tool to enhance their cybersecurity posture and mitigate the risks associated with today's interconnected ecosystems.

The rest of this paper is structured as follows. Section 1 discusses the problem, Section 2 indicates the different technologies and data types that Advanced Threat Intelligence Orchestrator (ATIO) manages. Section 3 describes the service implementation elements. Finally, Section4, presents some indicative use case workflows along with their efficiency metrics resulting to some initial outcomes, Sections 5 concludes the paper.

2 ADVANCED THREAT INTELLIGENCE ORCHESTARTOR (ATIO) A SOAR MIDDLEWARE TO COMPOSE INFORMATION FROM SEVERAL TECHNOLOGIES AND DATA TYPES

The structure of an organization that consists a security center, separates its network to the organization segmentation encompassing organization assets and detection/protection tools and a SOC network segmentation includes defensive cybersecurity technologies and communication with the detection/ protection tools of the organization's network segmentation. Detection and Protection tools, as well as tools within SOC segmentation (e.g. response tools, cyber threat information correlation tools etc.) are called defensive cybersecurity tools.

In an environment where several tools are installed and connected through network, a central solution is established in order to manage the harvested cyber security information from tools installed in the infrastructure. Conclude to eliminate decision making time processes, facilitating information bottlenecks, monitoring users and processes status and access authorization, recording and storing the cyber threat information and user interaction logs. In Figure *1* is depicted the conceptual diagram of SOAR in an organization.

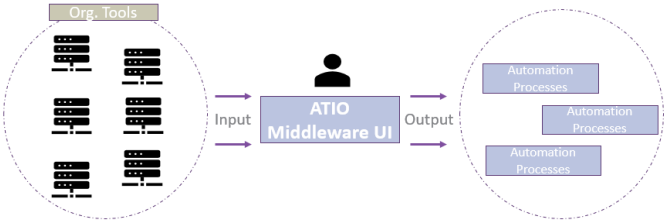

Figure 1: Advanced Threat Intelligence Orchestrator act as a SOAR executing automatically organizational processes. Information for the execution processes presented to the end-user on the ATIO middleware UI.

2.1 Data and platforms types, supported by SOAR

Cyber Threat Information travels through Security Orchestration Automation and Response (SOAR) services to Sharing Incident Response Platforms (SIRPs), Threat Incident Platforms (TIPs), and Security Orchestration Automation Platforms (SOAPs). Through its interoperability capabilities, SOAR seamlessly feeds multiple tools including Security Information and Event Management (SIEM) systems, recovery and analysis tools, as well as various databases.

In the context of SIRPs, SOAR enables the ingestion of diverse data formats ranging from human-readable JSON files to structured reports, facilitating efficient incident response workflows. Meanwhile, TIP data integrated with SOAR encompasses supplementary information regarding vulnerabilities or incidents connected with systems logs, enhancing threat intelligence analysis and response efforts.

Within SOAP environments, SOAR enriches organizational data by incorporating incident-related metadata, tags, and contextual information. This includes details about SOC analysts involved, tools utilized during incident handling, and pertinent incident attributes. Such integration enhances overall security orchestration, enabling streamlined incident management and response processes across the cybersecurity landscape.

The data transferred through ATIO are secondary information related to cyber threat information or incident.

2.1.1Variety of Data types

In this sub-section we will review some cyber security tools' categories harvesting either primary or secondary information from organisation's cyber security events. Heterogenous information should be processed and orchestrated in order to result as a cohesive information for the organisation.

Table 1: Data types communicated by different types of tools within cyber security protected organizational environments.

Data	**Threat Detection**	**Vulnerability Detection**	**TIP**	**SIRP**	**SIEM**
Logs					x
IP	x				
CAPEC		x			
TTPs		x	x		
CVEs		x	x		
CPEs		x	x		
Customized Reports	x	x	x	x	x
STIX2.1 Reports [2]	x	x	x	x	x
Customized Playbooks				x	
STIX-CACAO playbooks [3]				x	

2.1.2Variety of log types

Each event within a service is related with an event type. Each event type produces several event logs encompassing: a) security event log types, b) system event log types, c) application event log types and d) other event log types [4].

Security event log types including the Logon events, Logon validation events, Object access events Account management events, privilege use events, process tracking events.

System event log types including system start up and shutdown, services status, firewall status

Application event log types records events from any application that stores its logs in a Windows application log file, the application logs may include event logs created by applications such as antivirus or databases.

Other event log types: Powershell logs, Scheduled tasks logs, RDP logs, WMI logs.

2.1.3Results

In a nutshell, the tools which are used and the data which are transferred within an organization's infrastructure varies. A middleware is needed to bring together information from organization's network segmentation to the SOC network segmentation.

- A SOAR solution, in our case the Advance Threat Intelligence to transmit (ATIO) transfers data in the form of json reports, transforms and filters several types of data among different integrated tools in the whole system, while at the same executes automatically workflow processes.
- The creation of a monitoring app incorporates into ATIO to record ATIO workflows logs of user interaction.

More details will for both solutions will be found on Section 4.3.

3 ADVANCED THREAT INTELLIGENCE ORCHESTRATION (ATIO) AS A SERVICE SUPPORTING ELEMENTS

It is very common tactique, an organization to has installed two different kinds of detection systems in the same network. For example, let's assume the installation of an incident detection system a) based on payload signatures and b) based on anomaly behavior. Even if both solutions belong in the same tool category, however they support different capabilities, developed by different programming languages and paradigms. Finally, they have different system implementation requirements, support different use case needs and serve a different purpose. More specific, both tools detect threat events, nonetheless the former looks at the network traffic payload to identify them, while the other looks at the event logs of the network to identify them. The former produces constant output, that may not be always important, while the latter produces bursty output, that may not be always true positive.

In order to acknowledge the incident, SOC teams need to intervene and cross check the detection report, usually incorporating standard procedures and strategies, that are dictated by organization specific policies. Also, monitoring and threat detection tools integrated within the ATIO can produce alerts based on anomaly behavior, that need to be reviewed by security experts in order to get acknowledged and then receive a ticket for the response evaluation.

This section will guide you through the steps that occurred before to and during the ATIO installation and workflow execution.

3.1 Efficiency Metrics

For estimating organization efficiency as a mean of effectiveness it is very important to primarily have introduce metrics like, MTTD (mean time to Detect), MTTA (mean time to Acknowledge), MTTR (mean time to Respond) [5]. The average time for these metrics varies according to the organization management system. In some cases, identified as very high, ranging from several minutes to hours, or even days. Based on the studies conducted by [6]. Seven (7) days is a typical time frame for detecting and resolving various types and levels of events. However, according to the same report, the average period for threat discovery is three (3) days. By leveraging the use of an ATIO middleware, cybersecurity teams are able to reduce the metrics such as MTTD, MTTA and MTTR, to some fragments of a minute. Some indicative measures will be showcases in Section 4.4.

3.2 CLouD installation specifications

ATIO implementation and workflow design lied upon the open-source tool, namely Shuffle [7]. Shuffle enables their users to "draw" a standardized workflow procedure by indicating the a) end-points and b) designing the APIs that are going to connect the tools. We created a network of OPEN-APIs for data exchange.

During the development of the IRIS project, we have successfully deployed and integrated the ATIO system on many different environments. The easiest deployment scenario for the Orchestrator would be to run locally on a dedicated server using the provided Dockerfiles, by running a single `docker-compose up` command. The

Orchestrator is always using HTTP end-points for listening to incoming events, and thus the deployment state is independent of its operation.

The workflows running inside ATIO consist of applications [8] called "Actions", and some intermediate workflow processing steps that connects the App among them and at the same time manipulate the state of a JSON file. These actions are executed by workers running as containers in a jailed environment, and are managed by the Orborus worker scheduler. Every action result is expressed in JSON format, and the majority of the actions fall inside the categories of either REST-API clients or short, simple Python scripts.

Accordingly, we have also managed to deploy the ATIO's modules, namely Frontend, Backend, Orborus and OpenSearch, on a Kubernetes cluster as pods [9]. The usage of a cloud solution such as this is commonly preferred in the industry, as it offers both greater scalability of resources and faster deployment, but also more flexible management of expenses.

Shuffle incorporates the k8s.Core library to manage the creation and deletion of successful pods inside the Kubernetes cluster. The workers are usually separated into a dedicated network namespace that can be configured to dynamically allocate needed resources, monitor the utilization of the ATIO, establish a hardened security firewall policy or access restrictions.

For the setup the creation of a Kubernetes manifest file is required, that should describe the appropriate network addresses of each of the corresponding ATIO modules, along with a dedicated volume for permanent storage for the OpenSearch elastic database engine, and also an Ingress HTTPS service for the Frontend module. For the deployment of the main modules we used the `kubectl` application that requires an authentication token for access control.

3.3 Standardized Language format and Data model

The development of a shared data model in standardized format, in our case STIX2.1, ensures interoperability between the SOAR solution and the associated tools. The above method is frequently utilized in the defensive cyber security field, and it is a common manner of representing it, as evidenced by various studies [10], [11].

An "identification event report" data model, was structured within IRIS, to ensure interoperability in the IRIS system environment during the integration. The common data model originated by the composition of different and diversified tools inputs, that had modified their outputs from proprietary to STIX2.1. This gave us the opportunity to experiment with a realistic use case, since in organizations the tools and services used are not follow a standardize format. Furthermore, even when the data schema is standardized the interpretation of information to a common consensus most of time needs an additional effort by the organization. When the data schemas of the information have been stabilized then the ATIO can verify the information received by each separate tool and then automatically process it and forward it to the appropriate tool.

4 WORKFLOWS EXAMPLES

This section highlights some IRIS typical orchestration use case scenarios. The workflow and use cases described below are either launched by different types of defensive security solutions, namely vulnerability and threat detection tools and subsequently ATIO handles received files differently. In addition, a customized Monitoring Workflow application is offered, to monitor the state of each workflow. In **Error! Reference source not found.**, you will see an end to end workflow that is executed simultaneously and sequentially to several tools. Also, you can see the status of some indicative action steps at the right of the image.

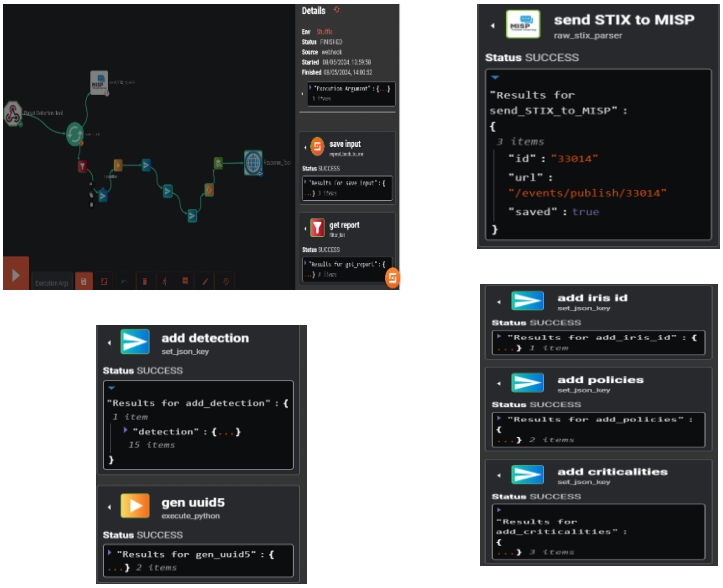

Figure 2: On the up left image corner an end-to end workflow in ATIO SOAR system initiated by a threat detection tool along with some indicative pre-processing and processing steps, on the upright image showing the status while the STIX2.1 report is published within MISP , on the down left image is showing the status while the detections are added in a proper format as well as a automatic unique UUID generated, on the downright image is presenting the addition of the iris_id, policies and criticalities.

SOC members can evaluate all information in one place and simply connect all accessible systems by leveraging intuitive, simple-to-use and configure middleware such as ATIO (Shuffle). The prerequisites for executing any processing step or type of workflow we should firstly define the standardized format used. As was mentioned in Section 3.3, we used STIX2.1 standardized format.

4.1 Different Type of Automation Workflows

4.1.1 Sequential, or concurrent execution workflows

Sequential or concurrent execution workflows may help the system by:

a) serving various systems and applications at the same time, b) making it easier to scale, suitable for the cloud, and c) simplifying architecture, removing complexity, and allowing for autonomous execution of parallel operations.

Contacting many cybersecurity systems at the same time enables the SOC team to respond quickly and notify others. From early detection to timely risk analysis and acknowledgement, incident detections can be enriched and delivered to IT teams faster, with fewer errors, and accompanied by prescribed actions. Automation is essential in today's cybersecurity operations, since the majority of jobs should follow regular protocols, with only a small portion of the entire process requiring human interaction and examination.

4.1.2Altering, filtering, preparing report workflows

Depending on the type of json report and file format, Orchestrator performs the required processing operations. These processing activities included filtering, removing, integrating STIX2.1 objective, converting to and from TAX-based language formats (such as STIX2.1, MISP, etc.), creating reports in a format that other integrated tools could digest, and so on. Also, the addition of internal ids, such as iris_id and misp_id, alongside the cyber threat information (CTI) makes it more useful to be acknowledge or correlated with internal or external threat/ vulnerability database. Within IRIS, we use the ATIO to manage the detection tools' input flows and convert them into a unified format that is fed into the response system.

Other systems that get notified about the detection event, like a cyber intelligence sharing platform or the end-user dashboard, may require different alteration on the original report, or even not require any change at all. Each of these cases can be handled automatically and error-free with the use of parallel workflows. Similarly, many other applications can get incorporated inside the workflow when the need for further operation on the detection report arises.

4.2 Use Case 1, 2- Vulnerability Identification and Threat Detection Response Workflows

Dive into IRIS use cases, we will investigate two (2) types, a) a threat detection and b) a vulnerability detection automated triggered workflow. Typically, their output is relatively distinct since are trying to investigate different incident type for different assets and in different time frequencies. For this reason, they transfer different fields within their individual json report.

More specific the output of

a) an OpenVAS based vulnerability scanner would produce an output including: target Asset's IP address, a list of the vulnerabilities found there, along with their respective CVE, CAPEC, etc. links, and maybe also a Severity score value for each vulnerability.
b) While the Suricata based intrusion detected system, described by a STIX2.1 Threat "Report", accompanied by an "Attack-Pattern", b) the "Actor's" IP address, c) the "Target" asset's IP address, d) and the Confidence level of the detection.

While, ATIO transforms the file to a form suitable for digestion by a response tool (Section 4.1), reassures that includes among other fields, also a) First seen/Last seen timestamps, b) the Confidence level of the detection, c) the Importance of the detected event, d) the Asset's risk evaluation score, e) and the organization's security Policies.

4.3 Use Case 3- Monitoring user actions and recording the changes, additions, deletions

The need of monitoring custom app arises from the need to a) Monitor crucial processes and user actions within an organisation, b) Keep track the changes within organization, c) Be aware to self-recover from a system shoot down or form a malicious cyber-attack.

The purpose of the monitoring app is to provide information in case of creation, deletion or modification of a workflow and keep the logs of each case. The monitoring application requires an authentication mechanism which contains the following parameters:

- Url: The address where shuffle is hosted.
- Api Key: The key of the admin user that is necessary in order to use the Shuffle API and get information about the workflows.

The workflows elements consisted by

- timer: Specifies the time interval between each execution of the workflow; a shorter duration enhances the system's responsiveness to changes.
- monitoring_app: Saves the previous state which contains information about the running workflows and compares it with the updated state to determine whether a workflow was created, deleted, or modified.

To showcase how the monitoring app works we will cover all the cases during the execution of the workflow. For example, at the picture below when there are no changes in all of the workflows. So, inside the notification field all the nested fields like CreationEvents, ModificationEvents and DeletionEvents are empty. The workflow_data holds the current saved state, which will serve as the previous state in the next execution.

4.3.1Monitoring Workflows Cases: Creation, Modification, Deletion

Moreover, the monitoring app can detect multiple cases of change simultaneously, so it can catch a combination of creation, modification and deletion of workflows. In Figure 3, are shown 2 out of three potential notifications of the current app.

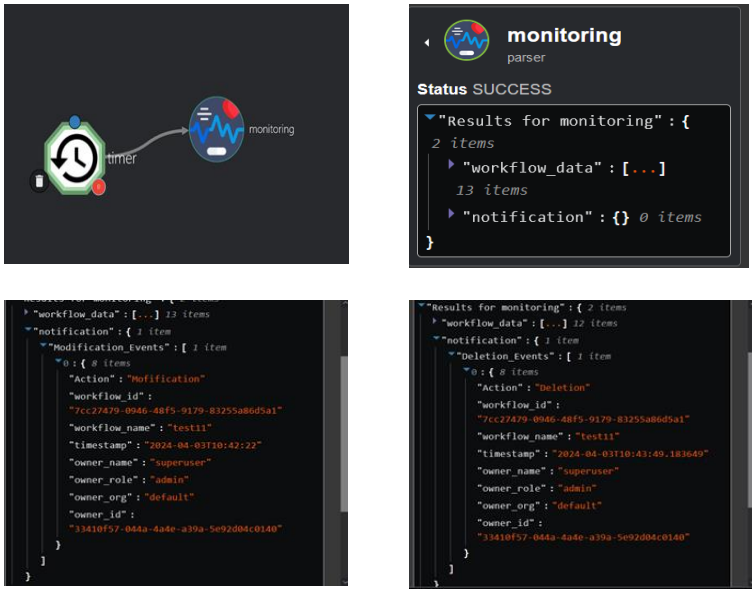

Figure 3: On the up left image corner the monitoring workflow, on the upright image corner the Idle State, on the down left image corner Modification notification, on the downright image Deletion notification are illustrated.

In Figure 4 is a detailed data diagram illustrating the flow of the monitoring mechanism within the backend system.

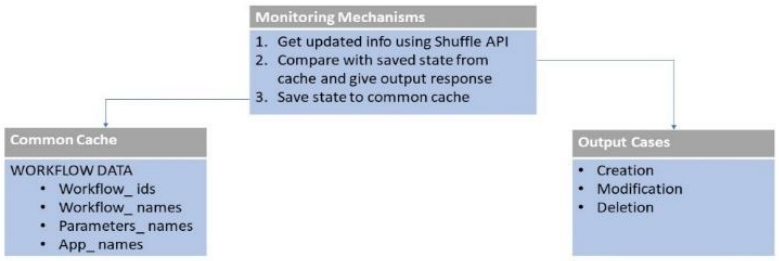

Figure 4: Monitoring Mechanism Flow

4.4 Results

The metrics established in Section 3 are measured and compared in three (3) separate cases: a) MTTD, b) MMTR, and c) MMTA.

Use Case 1: A network scanner inspects the network infrastructure. The detection is completed within 10 minutes and one or more vulnerabilities are identified. The found vulnerability report is pre-processed and properly prepared before being automatically delivered to tools responsible for acknowledgement and response.

Use Case 2: A threat detector detects an incident within the organization by monitoring the system once every 1,5 min. After the detection the report is prepared and send to tools for acknowledgement and response.

Use Case 3: A malicious insider threat gains access to an organization's Unified Threat Management (UTM) system and deletes a crucial workflow procedure from the Advanced Threat Intelligence Orchestrator.

Table 2: Data types communicated by different types of tools within cyber security protected organizational environments.

Metrics	**Use Case 1**	**Use Case 2**	**Use Case 3**
MMTD	10 min	1,5 min	15 secs
MMTR	<2 sec	<2 sec	N/A
MMTA	<1 min	<1 min	9 secs
Total time	**<12 min**	**<3 min**	**22 secs**

As stated in Section 3.1, the complete detection, response, and information of an event can take between 3 and 7 days (mean time) if response implementation is performed alongside with the other activities. As we can see from the table above the IRIS mean time is significantly shorter. Even if we cannot compare mean times when the use cases, the deployment specification and the tools differ, we may recognize the progress that the ATIO may contribute to defensive cyber security. In that end we can escalate in the future to even more complex scenarios, with more integrated tools and processing steps.

5 CONCLUSIONS

Finally, ATIO provides a full middleware solution for enterprises looking to automate and enhance their threat intelligence management processes. Its concurrent automation, standard adherence, customized workflows, user

monitoring, and seamless integration features make it a valuable asset in today's ever-changing cybersecurity scene. Throughout the IRIS project, ATIO experimented with threat detection and vulnerability identification use cases, as well as constant workflow monitoring. To elaborate, inside the IRIS project, a bespoke app has been developed for this specific purpose. Also, the efficiency measures (MTTR, MTTD, and MTTA) of the above three (3) use case measured. The results laid the framework for ATIO SOAR, encouraged us to look into it further for other use cases, and demonstrated the future of organisation and automation procedures in SOC teams.

6 ACKNOWLEDGEMENT

This work is a part of the IRIS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021727. This content reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information this publication contains.

Bibliography

[1] D. T. E. L. A. V-G Bilali, "IRIS Advanced Threat Intelligence Orchestrator- A Way to Manage Cybersecurity Challenges of IoT Ecosystems in Smart Cities," in *Internet of Things: 5th The Global IoT Summit, GIoTS*, Ireland, 2022.

[2] OASIS Committee Specification 01, "STIX™ Version 2.1," Edited by Bret Jordan, Rich Piazza, and Trey Darley. 20 March 2020, [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html. Latest stage: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.

[3] OASISS OPEN, "CACAO Security Playbooks Version 2.0," 2023. [Online]. Available: https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd01/security-playbooks-v2.0-csd01.html.

[4] M. Yahia, Efective Threat Investigation for SOC Analysts, Birmingham: Packt Publishing Ltd., 2023.

[5] B. Kovacevic, Security Orchestartion, Automation, and Response for Security Analysts, Birmingham: Packt Publishing Ltd., 2023.

[6] P. d. G. M. S. F. H. R. R. D. V. A. S. Sean Kinser, "Scoring Trust Across Hybrid-Space: A Quantitative Framework Designed to Calculate Cybersecurity Ratings, Measures, and Metrics to Inform a Trust Score," in *34th Annual Small Satellite Conference*, 2020.

[7] SHUFFLE, "Shuffle Automating Security Industry," [Online]. Available: https://shuffler.io/.

[8] SHUFFLE, "Shuffle Apps," [Online]. Available: https://shuffler.io/docs/apps.

[9] SHUFFLE, "Configure Shuffle," [Online]. Available: https://shuffler.io/docs/configuration.

[10] R. M. a. C. M. Ricardo M. Czekster, "Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings," *Applied Sciences- Statae of the AAart of CyberSecurity,* p. 5005, May 2022.

[11] Z. S. J. C. Y. Z. T. Y. H. Y. J. L. Zhengjun Liu, "STIX-based Network Security Knowledge Graph Ontology Modeling Method," in *CGDA 2020: 2020 3rd International Conference on Geoinformatics and Data Analysis* , Marseille France , 2020.