IRIS Advanced Threat Intelligence Orchestrator- A way to manage cybersecurity challenges of IoT ecosystems in Smart Cities.

Vasiliki-Georgia Bilali [0000-0002-7342-466X], Dimitrios Kosyvas [0000-0003-1330-0590],

Thodoris Theodoropoulos [0000-0002-4551-5804], Eleftherios Ouzounoglou [0000-0002-5078-3248], Lazaros Karagiannidis [0000-0002-9148-6258], Angelos Amditis[0000-0002-4089-1990]

[1] Institute of Communication & Computer Systems (ICCS), 9, Iroon Politechniou Str. Zografou, Athens, Greece, GR-15773

Abstract. The abstract should summarize the contents of the paper in short terms, i.e. 150-250 words.

This paper provides an overview of the Advanced Threat Intelligence Orchestrator in assisting organizations and society's first responders in managing, prioritizing, and sharing information related to cyber security incidents. In order to accomplish this, the capabilities and benefits of security, orchestration, automation, and response (SOAR) systems, on which Orchestrator is based, were promoted. The results of this survey conducted as part of the IRIS EU-funded project to protect Internet of Things (IoT) and Artificial Intelligence (AI)-driven ICT-enabled systems from cyber threats and attacks on their privacy facilitating SOC/CSIRTs/CERTs.
In this context, the tool is explored in methods of orchestrating and automating cyber security processes and routines. The open-source tool that was chosen for the creation of Advanced Threat Intelligence Orchestrator was SHUFFLE. SHUFFLE gives a wide variety of functionalities as it can be integrated with numerous tools and APIS. Furthermore, the provision of schematic workflows with action steps makes the stakeholders' interface more intuitive.

Keywords: Orchestration, SOAR, Information Management, Automation, CSIRTs, Threat Management, SHUFFLE

1 Introduction

Security operational centers (SoCs) and enterprise experts spend hours in security departments monitoring processes, waiting for alerts and searching for clues that something unusual is happening identified among massive amount of data. Many times, these alerts either do not reach security centers or misinterpreted by the system for immediate action, causing uncertainty and anxiety both within the organization and in a smart city. Even if the alerts are received, the process of sending the information to the appropriate

"place" is time-consuming, as well as managing a massive amount of data necessitates multiple decision-making processes. As a result, in many cases, implementing automation and orchestration is the answer when it comes to managing and, ultimately, combating cyber security threats.
Advanced Threat Intelligence Orchestrator can be provided as a drastic solution in a cyber-threat challenging world since it not only manages cyber-threat information and processes in IoT and AI-enabled infrastructures, but it also secures smart ecosystems by facilitating vulnerability management, security incident response, and security operations automation. This technical solution adheres to the capabilities of security, orchestration, automation, and response (SOAR). SOAR capabilities can benefit from relying on and leveraging security information and event management (SIEM) system information through automation and orchestration.

1.1 Data sources in smart cities

IoT implementation in urban areas improves citizens' daily lives and society's operations by providing safety and operational stability. These ecosystems consume static and real-time data from a wide range of sources, such as sensors, adaptors, actuators, IDs, SIEM alerts, CCTV cameras, and so on. Nonetheless, as IoT and AI smart ecosystems become more complex, their capabilities increase, making them more vulnerable to malicious actors.

1.2 State of the art of tools used into SOAR

As it is mentioned by Gartner Glossary[1] "SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies — where incident analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format".
SOAR platforms (SOARP) interact with several technologies such as threat detection technology tools, vulnerability detection tools, AI/ML-powered cyber defense systems etc. Indicatively some of them are **SIEM** is a piece of software that allows users to log, monitor, alert, anticipate, correlate, and display security-related events and data collected from networked devices [1]**. Unified Threat Management (UTMs),** contains a software or a hardware gathering security management information displaying security logs in a console. **Next-gen firewalls**, include traditional firewalls, combine them with filtering capabilities, network- and port-address translation (NAT), VPN support, and other features. According to [2], the threat detection technology tools mentioned above are unaware of an organization's entire IT ecosystem. **Vulnerability detection tools** is

[1]https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

a software tool that according to the bibliography, there are three major types of analysis tools and techniques for detecting software vulnerabilities: a) static analysis, which examines the system/software without executing it, including examining source code, bytecode, and/or binaries, b) dynamic analysis, which examines the system/software by executing it, giving it specific inputs, and examining results and/or outputs, c) hybrid analysis, combining a, b. [3]**. AI/ML-powered cyber defense systems** [2]**,** using deep learning and cutting-edge algorithms.

Despite the fact that the implementation of SOAR capabilities into a variety of technical solutions is a relatively new phenomena, a literature study has begun to revolve around this subject [4], [5], [6], [7].

1.3 SOAR Solutions

There are many already existed market-oriented and Open-Source solutions. Gartner's 2020 SOAR market guide[2] entails a list of representative vendors and their products, including the following: Anomali ThreatStrecam, Cyware Virtual Cyber Fusion Center, D3 Security D3 SOAR, DFLabs IncMan SOAR, EclecticIQ Platform, FireEye Helix, Fortinet FortiSOAR, Honeycomb SOCAutomation, IBM Security Resilient, LogicHub SOAR+, Micro Focus ArcSight SOAR, Palo Alto Networks Cortex XSOAR [8], Rapid7 InsightConnect, ServiceNow Security Operations, Siemplify SOAR Platform, Splunk Phantom, Swimlane SOAR, ThreatConnect SOAR Platform, ThreatQuotient ThreatQ, Tines. The open source community is also providing solutions for the security Orchestration domain.

Some of the common elements of SOAR enabled tools include using machine learning algorithms, workflow automation, incident response playbooks, an open plugin framework, a case management visual environment, an intuitive user interface, a command line console, and so on. Some of the products, indicatively,

Cortex XSOAR [9] unifies security automation, case management, real-time collaboration and threat intelligence management, it also includes a registration fee.

DFLabs IncMac SOAR [4], [2] enable the planning and recovery phases through features such as knowledge bases, key performance indicators, and advanced reporting.

Anomali ThreatStream [10], converts raw data into actionable information by automating the collection and processing of data. This product is oriented to security teams' experts.

As a result, of cutting-edge research conducted through the IRIs project, SHUFLLE open source tool was the more interesting and mature since it facilitates to achieve project goals. More specifically, it supports thousands of premade integrations (see **Table 1**) using open frameworks such as OpenAPI to ease migration. Provides options for automating the digestion of trigger points. Possess a diverse set of cyber incident use cases (see **Table 1**), including MISP and HIVE cases that will be used in the project.

We also considered various user-oriented criteria, which resulted in the following benefits.

a. Maintains a well-organized GitHub repository and community

[2] https://www.splunk.com/en_us/form/gartner-soar-market-guide-2020.html

b. Contains useful documentation
c. Encourages creativity since the visual design allows you to personalize the dashboards.
d. It has the ability to integrate a wide range of tools from various categories
e. It is available in a free version.
f. It caters to the needs of both experts and non-experts.

1.4 SOAR Benefits

Automate critical use cases: The automatic definition of emergency cases, can be proved as savior in cases where the time is a valuable parameter for tackling an incident. In any case automating any kind of use cases indicates preparedness in operational and decision-making processes.

Streamlined Operations: Each element of SOAR contributes to the streamlining of security operations. Security orchestration aggregates data incoming from a variety of sources. Security automation, meanwhile, can easily handle low-priority alerts and incidents through the use of automated playbooks.

Immediate incident detection and automating response: This capability ensures that the system responds on time and without delay during the decision-making process of multiple data aggregation.

Faster response time: Security orchestration combines multiple alerts from different systems into a single incident. Security automation saves even more time by allowing the system to respond to alerts without the need for human intervention whenever possible. Adding context to textual data and automating the decision-making process allows for faster alert handling[3].

Elevating SIEM: A SOAR solution that integrates with a Security Information and Event Management (SIEM) is required to automate Security Operational Centers (SOCs). A SIEM with an integrated SOAR solution allows teams to respond to threats more quickly because all of the information they require is in one location. It also reduces the possibility of human error and the time analysts spend switching between tools because they can all be accessed through a unified interface.

Systems Scalability: The scalability of the system is achieved by the Web based application of SHUFFLE solution.

2 Specifications of Advance Threat Intelligence Orchestrator

In IRIS context, Advanced Threat Intelligence Orchestrator will be a facilitator of the communication among the external data sources and stakeholders. The end-user categories are composed by SOC teams, CSIRTS/CERTS and AI infrastructure providers. In particular, Orchestrator will create workflows to respond to incident information

[3] https://www.siemplify.co/blog/security-orchestration-automation-response-benefits/

sent from infrastructures by implementing expert knowledge and processes. Each workflow's knowledge can be updated based on the most recent laws and processes.

2.1 Orchestrator's Subcomponents

The Advanced Threat Intelligence Orchestrator is made up of six sub-components, including two visual environments and four backend tools. The structure of the integrated tool is presented below:

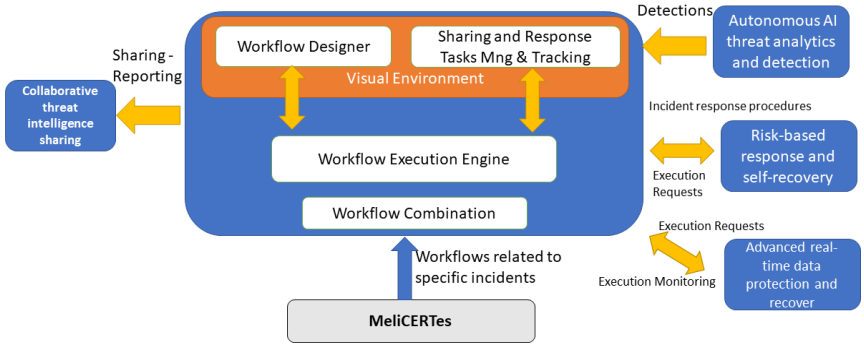

Fig. 1. The internal structure of the Orchestrator and its relationship to input and output information.

The visual environment consisting of a) the Workflow Designer as well as b) the Sharing, and Response Tasks Management & Tracking will be based on the Shuffle visual environment, while the backend tools will provide extra functionalities to imported and exported information.

Workflow Designer/Manager is a graphical environment that allows the creation of multiple scenario workflows. In particular, the definition of various incident response scenarios is the digitized form of the associated runbooks/playbooks that are executed. The runbooks are documents comprising proper background information and procedures to successfully execute security-related tasks, or address incidents, while the playbooks are documents comprising workflows, operating procedures, and cultural values required to approach and complete tasks in a consistent way. Finally, the Workflow Designer/Manager will include all the steps that should be automatically or manually executed based on the defined workflows.

Workflow Execution engine is the engine that implemented on the defined workflows, executes the data exchange steps and realizes the command execution requests to components.

Workflow combination engine will take the already existing workflow procedures connected to cyber-incidents and will automatically combined them with expert input from the MeliCERTes platform to enable proactiveness.

Threat Sharing and Response Tasks management and Tracking is a visual environment, which a part of this provides information on the tools related to threat sharing and response tools that have been automatically applied or should be manually/semi-automatically applied based on the risk levels.

Data exchange framework is a framework facilitating the data exchange among the orchestrator and intercorrelated components through APIs.

Command execution requests framework (based either on existing solutions of components or definition based on the OpenAPI specifications) is a framework facilitating the execution requests from the orchestrator to the components through APIs as well as the sharing of information for automatically applied/executed processes.

2.2 Technologies

SOAR tools combine Security, Orchestration and Automation capabilities (SOA), with Security Incident Response Platform (SIRP), and Threat Intelligence Platform (TIP) to seamlessly manage all the data received and created workflows in real time. A scenario workflow, referred to as a Failed ssh login Scenario, is presented in this section.

SHUFFLE

Within this section, SHUFFLE documentation is presented, to imprint potential SOAR capabilities that Orchestrator could perform in IRIS information sharing and awareness platform, as well as to perform a "language" for users' common understanding.

SHUFFLE is developing workflows for a variety of use case categories. SHUFLE has clustered these use cases into 8 groups, which namely are a) Communication, b) Case Management, c) SIEM, d) Assets, e) IAM, f) Intelligence, g) Network, h) Eradication cyber incident detection, prevention, remediation, case management, communication etc., more information on **Table 1** below. The below use case categorization has been depicted from GitHub repository. [4] Based on the case scenarios, specific SOC tools are involved.

SHUFFLE open source tools have a wide range of capabilities, including integration and communication with a plethora of tools, including (e.g. Hashdd, Elastic Search, the Hive, MISP, Keycloak IAM, etc.), managing cyber-security issues, related to threat and vulnerability management, authority management, security incident response and security operations automation.

[4] https://github.com/Shuffle/python-apps

Table 1. SHUFFLE use case categories correlated with capabilities and tools

Use Case Category	Use Case Capabilities	Tools
Communication	• Write text to someone • Read chats • List chats • Send actionable buttons • Send a file • Search through chat • Send a chat (comms) for every new email found (comms) every 5 minutes. Look for any IoC in it (SHUFFLE tools) and analyze it with Threat Intel.	Chat: • Discord • Slack • MS Teams • SMS Email: • Gmail • Outlook • AWS SES
Case Management	• Open ticket • Update ticket • Comment ticket (if not an update) • List Tickets • Merge ticket • Search for ticket(s) • Upload file(s) • Download file(s) • Add artifact / Indicator like IP and domain (security specific) • Syncronize tickets with another ticketing system (cases) every 5 minutes. When a new ticket comes, send a message to messaging app (communication)	• GitHub Notifications • TheHive • Service Now • Jira • Secureworks • HappyFox • PagerDuty • Zoho • ConnectWise
SIEM	• Search • Send event TO SIEM • Get Search results • Create Saved Search • Create Alert from Search (sends webhook / something else) • List Incidents • Get Incident • Update incident • Add comment	• Splunk • QRadar • Elasticsearch (ELK) • MDATP • Azure Sentinel • Logz.io • Security Onion
Assets	• Find hostname • Find Software by name • Find IP • Find hostname's owner • Search for CVE • List vulnerabilities by severity • List vulnerabilities by host • Get vulnerability • Edit vulnerability • Generate report	VMS systems: • Nessus • TenableVMS • Tenable Container Security • Snyk • Gitguardian Asset Management • McAfee CHS

Use Case Category	Use Case Capabilities	Tools
IAM	• Access Management • Active Directory • Single Sign-on	• Microsoft Identity and Access • Sailpoint IdentityQ • CISCO Identity Services Engine • Keycloak IAM • AWS IAM
Intelligence	• Search for IP • Search for Domain • Search for URL • Search for hash (md5, sha256...) • Add IP / domain / url / hash to have been seen (sighted MISP) • Search for CVE • Search for Threat actor • Get incidents	• MISP • Passivetotal • Recorded Future • Secureworks • Shoden • Virustotal • IBM xforce • IPInfo
Network	• Block IP • Block domain • Block URL • Sinkhole IP • Sinkhole domain • Unblock (all of the above) • Search for status with IP / domain.	• AWS WAF • Cisco • Check point • Palo Alto • Fortinet • AWS VPC FW
Eradication	• Ticketing system (list/create/edit alert) • Search • Find hostname • Ban hash/ip/url/domain • Isolate host • Execute script on host • Create rulE	• VMware Carbon Black • GoSecure • Cylances • InfoCyte • Waxuh • Windows Defender • Windows Defender ATP • CrowdStrike Falcon • Velociraptor • Qualys EDR • Trend MicroXDR

APIS Integration

The SHUFFLE platform makes third-party API integration straightforward by utilizing trigger-based communication techniques such as Webhook, which can be quickly activated by a POST request from the backend. Using this way, the synchronization of the workflow and the incoming input can be defined from the REST-API, and the necessary automated process can be simply configured in SHUFFLE.

2.3 Failed ssh login Scenario

The example of a failed remote authentication login was chosen to demonstrate a small portion of SHUFFLE 's capabilities and to familiarize the user with the platform's consensus and visual output. So, to establish an input data pipeline for the SHUFFLE procedure, Wazuh, an open-source platform for thread identification, security monitoring, and incident response, was used. As a result, a Wazuh manager was set up and agent in virtual machines and integrate SHUFFLE to monitor for failed ssh authentication. The Wazuh manager checks the security logs produced by the manager itself and the agent that controls and when it detects a password failure it sends a HTTP-POST request to the SHUFFLE Webhook.

This request is essentially a JSON message containing information about the authentication attempt and the configuration rules from Wazuh. By sending this message we trigger the SHUFFLE Webhook and kickstart the flow of our use case.

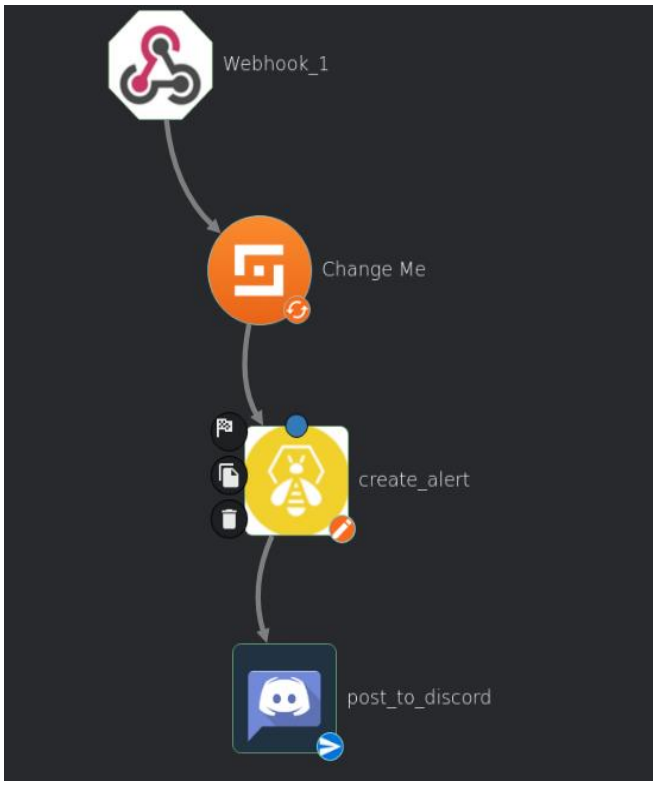

Fig 2. Orchestrator's Workflow Designer visual environment relying on SHUFFLE design environment

In **Fig *2*** the pointing arrow shows the direction of input data in SHUFFLE and all the blocks have access to that information.

In this example we have also used TheHive that is an incident response platform to create an alert regarding the failed connection by filtering some fields of the original message. At the end of the flow we post in a Discord channel some results like the IP and port used in the login attempt to notify the user.

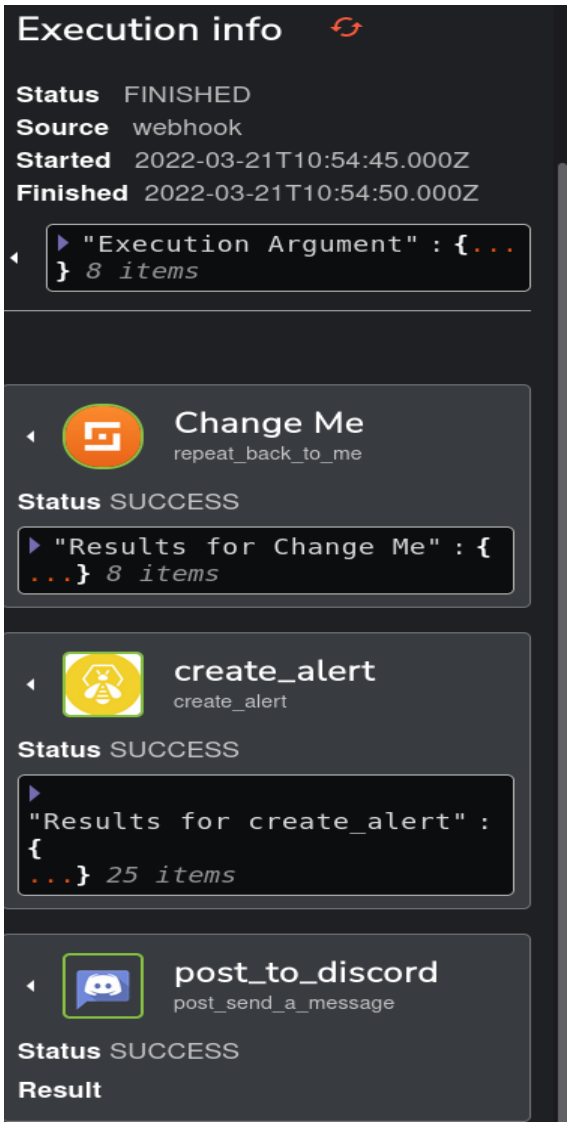

Fig 3. Orchestrator's Sharing and Response Track Management and Tracking visual environment relying on SHUFFLE design environment.

The results of the execution workflow are indicated to the figure above (**Fig 3**). These outcomes can be viewed in either the related tools or in this visual environment. As a

result of the scenario, users reported that the Orchestrator processes flowed smoothly and that it was user-friendly.

2.4 Stakeholders Communication through Orchestrator

The Advanced Threat Intelligence Orchestrator will be accessible to stakeholders via a user management interface. Begin by deciding whether to use a predefined or custom workflow. End users are thus able to seek and execute an already existed workflow or create a sequence of steps implementing tools based on use case categories (see **Table 1**), based on the triggering information received (e.g. alerts and events etc.). Orchestrator will be able to interface with the MeliCERTes platform and seek expert knowledge for response, improving default workflows and recommended response actions. The combination of multiple data sources gathered from other tools and MeliCERTes platform will improve the ability to compute efficient proactive response steps. As a result of the foregoing, security operations teams will benefit from automating iterative response processes, saving time for higher priority sorting tasks, and providing a standardized, easy-to-follow response.

3 Conclusions

In a nutshell, the numerous threats of security operational centers business face on a daily basis are draining resources and slowing incident response time, whether it is called alert fatigue or information overload. Here it comes SOAR platforms to give the solution by relieving SOC analysts of remedial and low-priority tasks, allowing them to focus on improving the overall effectiveness of SOC in responding to incidents. IRIS will take a step forward in this direction by implementing Orchestrator, which will assist stakeholders in lowering smart city risks while automatically managing, prioritizing, and sharing information related to cyber security incidents.

4 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.

References

[1] Redlegg Managed Security Services, "What is SIEM?".

[2] L. A. Johnson Kinyua, "AI/ML in Security Orchestration, Automation and Response: Future Research Directions," *Tech Science Press*, vol. 28, no. 2, p. 19, 2021.

[3] D. A. W. A. E. H. E. Kenneth Hong Fong, "State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation 2016," 2016.

[4] DFLABS- Cyber Incidents under control, "The most Comprehensive eBook on SOAR Use Cases," [Online]. Available: https://dflabs.com/wp-content/uploads/2020/12/The-Most-Comprehensive-eBook-on-SOAR-Use-Cases..pdf.

[5] LogRhythm, "Practical Use Cases for SOAR," [Online]. Available: https://logrhythm.com/practical-use-cases-for-soar-white-paper-2019/. [Accessed 2 2022].

[6] Palo Alto, "Top Security Orchestration Use Cases".

[7] Logsign, "Security Orchestration, Automation and Response (SOAR) Buyer's Guide- An Ultimate Guide for SOAR".

[8] Cortex, "The State of SOAR 2020- The fourth annual survey report on incident response," 2020.

[9] CORTEX, "Security Automation for Everyone," [Online]. Available: https://www.paloaltonetworks.com/cortex/cortex-xsoar.

[10] ANOMALI, "BIG DATA SECURITY. ACTIONABLE INTELLIGENCE. RELEVANT INSIGHTS".