Observe-Orient-Decide-Act (OODA) for Cyber Security Education

By Muhammad Hasbi

WORD COUNT	5853	TIME SUBMITTED	03-APR-2023 02:18PM
		PAPER ID	98297567

Observe-Orient-Decide-Act (OODA) for Cyber Security Education

Dimas Febriyan Priambodo[1], Yogha Restu Pramadi[2]
Obrina Candra Briliyant[3], Muhammad Hasbi[4], Muhammad Adi Yahya[5]
Cyber Security Departement, Cyber and Crypto Politechnic, Bogor, Indonesia[1, 2, 3, 5]
Informatic Departement, STMIK Sinar Nusantara, Surakarta, Indonesia[4]

***Abstract*—A cyber range is a term to define an isolated simulation environment that can be used for cybersecurity training. As a training tool, the cyber range has a crucial role in improving the competence of its users. Isolated environmental conditions allow users to increase competence through cybersecurity training based on predetermined scenarios. There is no standard for scenario in training, most of them using common case. In this research, the cyber range is built based on the cyber range taxonomy and uses the observe-orient-decide-act (OODA) loop that has been proven for military education. The OODA loop is implemented and helps guiding each step of the attack and its handling in the built scenario. The scenario chosen is a case of data theft since data theft incidents have often occurred so that it is easier for user to understand. OODA loop for cyber range meets 16 of the 17 characteristics in the cyber range taxonomy. The final cyber range acceptance rate was 81.82%. The results of this acceptance give confidence that this new method can be used as an alternative to learning cybersecurity.**

***Keywords*—Cyber security; cybersecurity education; cyber range; OODA loop; play-role scenario**

I. Introduction

There are no renowned holistic Security Operating Center standards or industry specific guidelines [1]. It has deep impact for cyber range especially for education. Lack of standardization leads to the need for solutions.

In cyber security education, one of the factors that support the success of implementing a cybersecurity curriculum [2] is the availability of isolated laboratories for learning [2]. Most isolated laboratories that are specifically used for cybersecurity learning are scenario-based. Scenarios are prepared using field experience.

From this, a big problem arises, there is no standardization in real world of SOC, so how to transfer experience in education especially in scenario for cyber range.

Observe-Orient-Decide-Act (OODA) loop is a well-known analytical framework for decision-making developed by John Boyd [3]. The method has been used in the military world long time ago and has been proven to provide experience and improvement for military students. This is inspiring to be applied in cyber security learning as well as being a standard and measuring its suitability in meeting the need for cyber security learning tools. In bigger scenario SOC is giving many open problems described in Vielbert's paper [4]. The problem can be minimalized by proper cyber security laboratories.

Several methods of building cyber ranges have been carried out previously, as summarized in the research of [5], [6], and [7] to overcome similar problems. The data presented by [6] shows that the most commonly used experimental method is the simulation method due to its ease of use.

A cyber range with data exfiltration attack simulation is built in this research that simulates a real attack case. The built cyber range is expected to be used as a learning tool to understand cyber-attacks better and apply the framework of thinking according to the OODA loop in further learning. The final results of the research were then validated with the user acceptance test (UAT) to find out whether the system built could meet the needs of cyber security learning.

II. Related Works

A. ISMS Role in The Improvement of Digital Forensics Related Process in SOC's

This research [8] presents similar solution for better SOC with Plan, Do, Check, Act. The purpose of this research is to provide an Information Security Management System solution that complies with ISO 27001:2013. Focus in digital forensic and not for education purpose.

B. Design and Implementation of a Research and Education Cybersecurity Operations Center

This paper [9] show common SOC and tools inside it. This research also builds simulation with honeypot and dashboard and also implementing OODA loop in concept of SOC not in scenario build.

C. Design and Implementation of a Research and Education Cybersecurity Operations Center

This research [10] present Action Observe Hypothesis method to build SOC. Using Questionnaire for post task, same method with user acceptence test in this research. This research focus in recap many SOCs and implemented with multi honeypot for implementation.

Novelty in this paper is the use of multiple Intrution Detection System (IDS) with agent based and rule based also Elasticsearch, Logstash and Kibana (ELK) for dashboard. OODA loop implemented inside scenario build and detail

inside it to provide experience for student. This research is also suitable for Covid-19 learning situation which implement VPN for student and lecture for remote education and proofed with User Acceptance Test for validation with curriculum.

III. Research Methodology

The research design refers to knowledge embodied in development, techniques, methods, models, and theory development to map out how to produce artifacts or products that meet predetermined functional requirement [11]. In this study, the research design used was Design Science Research (DSR) as seen in Fig. 1. DSR was chosen since it has the principle of "learning through development (making artifacts)," which is appropriate when applied to this research. DSR is a method of determining and conducting research with the ultimate goal of an artifact of recommendations. DSR can also be defined as a method oriented to solving specific problems to get the right solution even though the solution is not optimal.

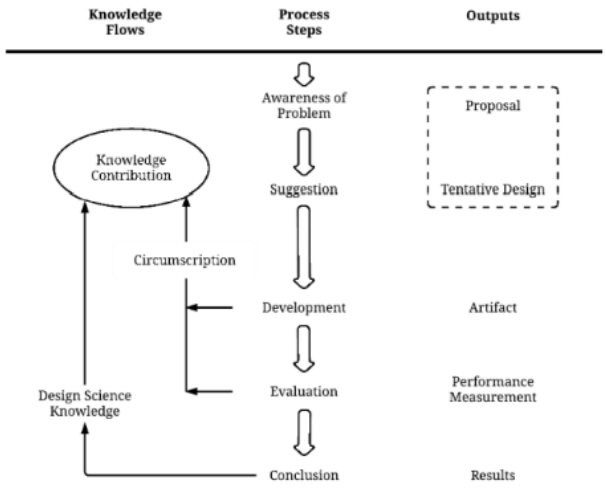

Fig. 1. DSR Process Model Cycle.

Fig. 1 shows the relationship of each process, the flow of knowledge, and the output of the DSR, which is called the DSR cycle.

A. Awareness of Problem

Researchers identify problems that will be raised for research or problem formulation [11]. Sources of problems can be obtained from various existing sources. The problem identification process can be carried out in various ways such as literature study, practice, and discussion or interview. Once identified, the problem must also be defined. The problem definition process be done through a literature study to state that the problem has not been resolved and the solutions offered will contribute academically. In addition, problem definition also includes determining the scope of the problem to be solved using available resources.

B. Suggestion

The suggestion stage contains suggestions or solutions offered by researchers to overcome the problems that have been defined at the awareness of problem stage. These solutions can be generated based on existing research or through the thoughts and creativity of researchers in solving problems using appropriate research methods. The solution can be a new idea or combine an existing solution with something different. The result of this stage is a tentative design that describes the solution to the problems in the previous stage.

The pattern chosen to be used in the suggestion stage is modeling existing solutions and combining partial solutions. The existing solution modeling pattern is a design used to model solutions that have been used to overcome similar problems [11]. The results of the solution modeling are then developed and adapted to be a solution to the current research problems. The pattern of combining partial solution is a pattern that is used to take some concepts, ideas, or solutions from related references that can support the construction of solutions from the research conducted [11].

C. Development

The development stage is the stage to implement or develop a tentative design that has been made at the suggestion stage. The pattern used in the development stage is the same as the suggestion stage, namely modeling existing solutions and combining partial solutions. The explanation of the two patterns is also the same as the one at the suggestion stage. In addition, the solutions developed at the development stage are also prepared based on the tentative designs that have been made at the suggestion stage. In the development stage of this research, the cyber range is built based on the cyber range taxonomy from the research of Yamin et al. [7], attack simulation laboratory of Mahardhika research [12], and the benefits of building cyber ranges from the research of Leitner et al. [13] through a pattern of combining partial solutions while still considering the tentative designs that have been made. The combined results of the research of Yamin et al. [7] and Mahardhika [12] is used to compile a needs analysis in the design and construction of cyber ranges. In addition, the research of Grant et al. [14] also Debatty dan Mees [15] is used to create solution modeling in the form of scenarios and topology of the cyber range environment through the existing solution modeling pattern.

D. Evaluation

The results of the artifact implementation at the development stage are then evaluated at this stage based on predetermined functional specifications. The process carried out at the evaluation stage is to determine how well the performance of the artifact is based on the empirical method used. This stage is an opportunity to make improvements to the artifact based on the experience gained during the previous stage. This is also called the circumscription of the DSR cycle. The pattern used in the evaluation stage is demonstration. After the development stage is complete, the cyber range will be demonstrated. For validation a number of Cyber and Crypto Politechnic cadets will be asked to run the scenario that has been built according to the steps stated in the user manual for the attack simulation laboratory. After running the scenario, cadets will be asked to fill out a UAT questionnaire. UAT is needed to find out whether the cadets are able to apply the OODA loops framework during running APT attack scenarios. In addition, UAT is also used to measure whether the attack

simulation laboratory built has met the learning needs of the Cyber and Crypto Politechnic and can increase cyber situation awareness among Cyber and Crypto Politechnic cadets. Validation is done with UAT. The results of filling out the UAT questionnaire were then analyzed using a Likert measurement scale.

E. Conclusion

This is the last stage of the research cycle in DSR. The result of this stage is the solutions delivering that answer the formulation of the problem in research. In addition, the results obtained at the evaluation stage will also be presented at the conclusion stage. The process carried out at the conclusion stage is symbolized by a small arrow outwards in the DSR cycle. The purpose of the arrow is that the results of the research must be communicated or published so that they can contribute to science in the related field [16].

IV. IMPLEMENTATION

A. Design of Cyber Range

Cyber range design is done through a literature study of solutions and related research. The literature study was conducted on the research of Grant et al.[14], Debatty and Mees [15] to produce a cyber range design in the form of a tentative network infrastructure design from the cyber range and analysis of cyber range needs.

B. Tentative Design

Based on the literature study conducted on the research of Grant et al.[14], the network security infrastructure in an organization generally consists of a firewall, DMZ, servers, and workstations located in the Intranet. In addition, there is also an IDS located in the DMZ. Placing the IDS on the DMZ allows the IDS to monitor network traffic between the Intranet to the Internet, between the DMZ to the Internet and between machines within the DMZ. Network security infrastructure in organizations from the research results of Grant et al. [14] is in Fig. 2.

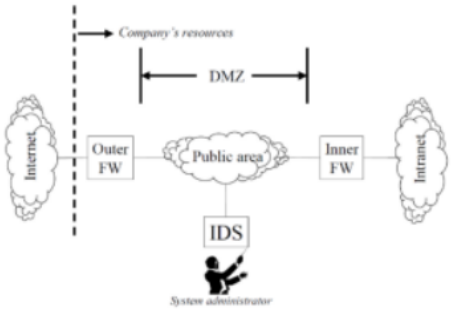

Fig. 2. Network Security Infrastructure in Organizations.

In addition to this research, a literature study was also conducted on the research of [15]. From the research of [15], obtained infrastructure for simulation of a small organization network consisting of firewall, DMZ, honeypot, vulnerable web server, internal workstation, Security Onion server for monitoring, and traffic generator. Virtual workstations are also provided for users connected to the internal network. The design of the organization's network simulation infrastructure can be seen in Fig. 3.

From the results of a literature study conducted on [12], obtained information that the attack laboratory topology can be built on the CAN topology provided that it has two main components, network infrastructure as the target of attack and APT group [17] infrastructure. Topology design of attack simulation laboratory in [12] research can be seen in Fig. 4.

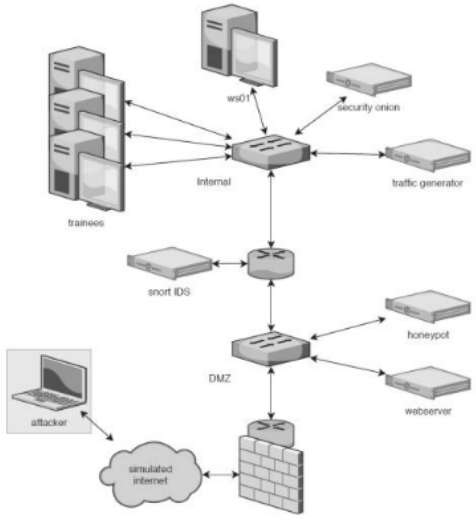

Fig. 3. Organizational Network Simulation Infrastructure.

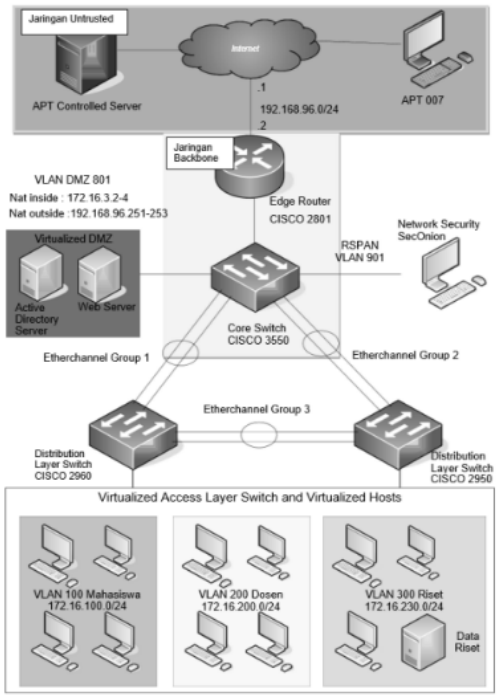

Fig. 4. Attack Simulation Laboratory Topology[12].

By utilizing the results of the literature study from previous research, a tentative design was designed as the final result of the suggestion stage in the DSR cycle as well as an initial design in the development of cyber range infrastructure. The design results of the cyber range design that have been made can be seen in Fig. 5.

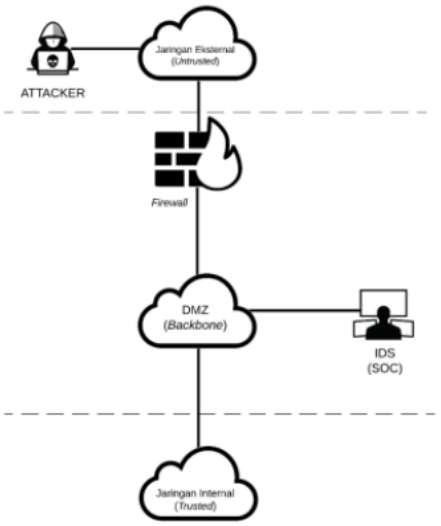

Fig. 5. Cyber Range Tentative Design.

The tentative design of cyber range divides the network into, external network (untrusted) in Table III, DMZ, backbone network, and internal network (trusted), all part was built in hardware listed in Table I and virtual machine listed in Table II. On the external network, there is an attacker's infrastructure consisting of various tools or virtual machines that aim to steal data from the internal (trusted) network seen in Table IV. Meanwhile, on the backbone and DMZ networks shown in Table V and Table VI, there is a main infrastructure to connect every device in the cyber range, firewalls, and IDSs that monitor activities in the internal network and the DMZ. On the internal network, there is an infrastructure of the target that is vulnerable to attacks from external networks seen in Fig. 6

TABLE I. CYBER RANGE HARDWARE

No	Hardware	Qty	role	Spesification
1	Cisco Catalyst 3650	1	Router and Switch	24X10/100/1000 Ethernet and 4X 1G uplink port
2	Supermicro Rackserver	1	pfsense	4X intel Xeon @2,13 GHz RAM 8GB HDD 1TB NIC 2 ethernet port
3	Server	1	Network Security Monitoring	6X intel Xeon @3,07 GHz RAM 32 GB HDD 1TB NIC 4 ethernet port
4	HPE Proliant DL20 Gen 10	2	Attacker VM, DMZ, Target VM	8X intel Xeon @3,5 GHz RAM 16 GB HDD 1TB NIC 2 ethernet port

TABLE II. CYBER RANGE VIRTUAL MACHINE

No	VM ID	role	Spesification
1	101	Attacker	OS Kali Linux CPU 2 Core RAM 4 GB HDD 100 GB
2	201	Domain Controler & Mail Server	OS Zentyal CPU 4 Core RAM 8 GB HDD 250 GB
3	301	Web Server	OS Ubuntu Server CPU 2 Core RAM 2 GB HDD 250 GB
4	410	Target	OS Windows 10 CPU 2 Core RAM 3 GB HDD 50 GB
5	510	Target	OS Windows 10 CPU 2 Core RAM 3 GB HDD 50 GB
6	610	Target	OS Windows 10 CPU 2 Core RAM 3 GB HDD 50 GB

TABLE III. UNTRUSTED NETWORK INFRASTRUCTURE

No	tools	Label	Subnet	IP (VPN)
1	Virtual Host (kali linux)	Caldera 101	192.168.41.0/24	192.168.170.2/24

TABLE IV. TRUSTED NETWORK INFRASTRUCTURE

No	tools	Label	VLAN	IP/Subnet
1	Virtual Switch	Keuangan & SDM	110	192.168.110.1/24
2	Virtual Switch	Produksi & Pemasaran	120	192.168.120.1/24
3	Virtual Switch	Operational Technology	130	192.168.130.1/24
4	Virtual Switch	Client 410	110	192.168.110.0/24
5	Virtual Switch	Client 510	120	192.168.120.0/24
6	Virtual Switch	Client 610	130	192.168.130.0/24
7	Virtual Switch	Security Onion	10	192.168.10.10/24

TABLE V. BACKBONE INFRASTUCTURE

Tools	Interface	IP	node
pfSense (firewall)	em0 (LAN)	192.168.2.1/24	Core switch
	em1 (WAN)	192.168.41.222/24	LAN PoltekSSN
	VLAN 10	192.168.10.1/24	
	VLAN 110	192.168.100.1/24	
	VLAN 120	192.168.120.1/24	
	VLAN 130	192.168.130.1/24	
	Gigabyte Ethernet 1/0/21		PVE1
	Gigabyte Ethernet 1/0/22		PVE2
	Gigabyte Ethernet 1/0/23	Monitor Interface	SOC
	Gigabyte Ethernet 1/0/24	192.168.2.2/24	pFsense (firewall)

TABLE VI. DEMILITARIZED ZONE (DMZ) INFRASTRUCTURE

No	Tools	VLAN	IP
1	Virtual Active Directory Server & Virtual Mail Server	800	192.168.3.2/29
2	Virtual Web Server		192..168.3.3/29

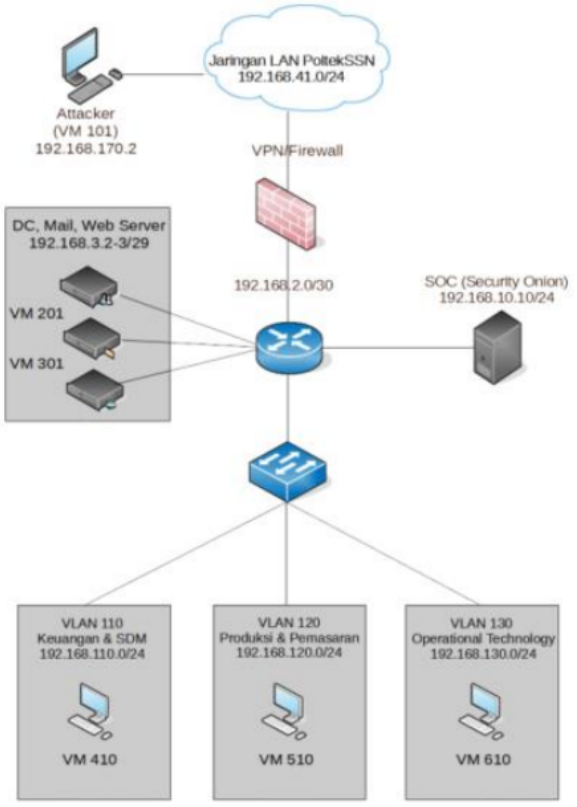

Fig. 6. Cyber Range Design.

C. Needs Analysis

Based on a survey conducted in the research of Yamin et al.[7], a system can be classified as a cyber range if it fulfills part or all of the components of the cyber range taxonomy. In the construction of cyber ranges in this study, the cyber range taxonomy is used as the basis for compiling a needs analysis of the built cyber ranges. The complete components of the cyber range taxonomy can be seen in Fig. 7.

D. Scenario

The scenario explains the objectives of the cyber range development, the environment in the form of the infrastructure used, the storyline behind the operation of the cyber range, the scenario application domain, and various tools used in the construction of the cyber range. Scenarios built-in cyber range is based on OODA loops. Every step taken by the attacker and the defender is arranged based on each stage in the OODA loop, which includes observing, orienting, deciding, and acting.

In the attack simulation scenario, initially cyber range users perform the task of the Red Team or Red APT group to attack with the aim of stealing data. After the attack was carried out, the students carried out the task of the blue team as SOC to monitor the attacks that occurred and take action against these attacks. The stages of the data exfiltration as resesarch by F Ullah [18] carried out by Red APT based on the OODA loop are as follows:

1) Observe: Red APT collects information through various sources related to target. From the results of the information collected, Red APT found several names of employees from target along with their email addresses. The names include Joko Nugroho (jnugroho@cybergym.local), Aurora Rahayu (arahayu@cybergym.local), and Caraka Kurniawan (ckurniawan@cybergym.local). This information is found on the website page of example target as shown in Fig. 8.

2) Orient: Red APT plans to exploit the weaknesses of the employee's nature to gain access to the target system. Red APT plans to make job offers with salaries and facilities that are more attractive than those offered by target to these employees via email.

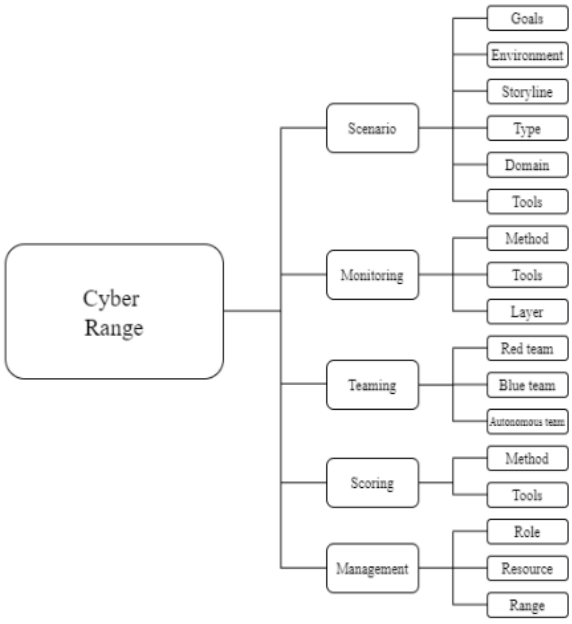

Fig. 7. Cyber Range Taxonomy


Pengalaman Kerja di PT TRINAKLIR

Joko Nugroho (jnugroho@cybergym.local), Aurora Rahayu (jnugroho@cybergym.local), Caraka Kurniawan (ckurniawan@cybergym.local)

We have created a fictional band website. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.We have created a fictional band website. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat

Fig. 8. Example Target Website for Observing

3) Decide: Red APT creates a payload in the form of an executable file that contains an access trojan command. The payload contains the command to execute the CALDERA agent. Payload is disguised by giving a file icon in the form of a job offer poster and providing a file name with the suffix.jpg. Windows operating system by default does not display the extension of a file, so naming a file with a .jpg ending will give the target the illusion that the received file is an image file.

4) Act: Red APT sends the payload accompanied by an attractive offer sentence using an email address with the name of the Company's HRD. The payload is sent to the email addresses of the three employees of target and hopes that there are employees who are interested and open the payload file. Fig. 9 shows the view of the email containing the payload received by the target.

Open the payload file and ignore the UAC notification on the computer gave an effect to automatically install trojan. After the payload installation process is complete, a backdoor is created so that Red APT has access to the victim's computer to steal database files on the target computer in SQL format. Agent implemented show in caldera dasboard seen in Fig. 10. The file theft was carried out using data exfiltration and data staging techniques using CALDERA. Fig. 11 shows the techniques used by Red APT to carry out data theft.

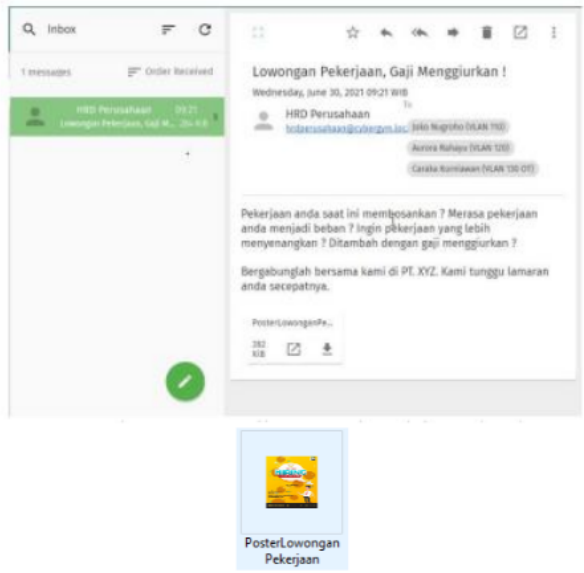

Fig. 9. Email Contains Payload.

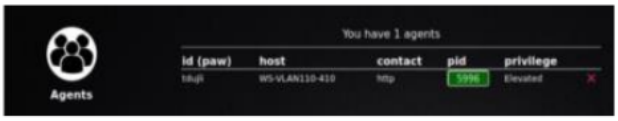

Fig. 10. Caldera Dashboard.

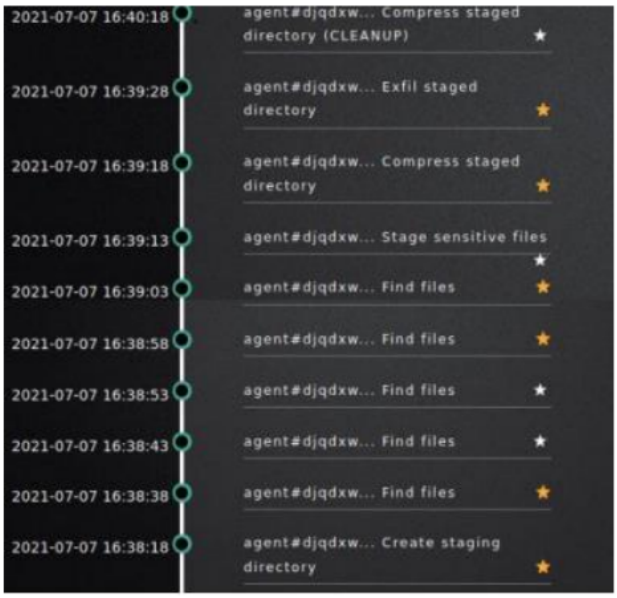

Fig. 11. Red APT Data Theft Techniques.

5) Observe: The OODA loop is an iteration, so after the goal of the attack, data theft is achieved, Red APT will return to the observe stage with the knowledge that has been obtained from the previous OODA iteration. In the next iteration, Red APT can explore the system to find data, information, or other vulnerabilities that can be exploited.

In future research RED team can be improved [19] by implementing automated system as Applebaum's research. Meanwhile, the OODA loop carried out by SOC defender to detect anomalies and APT. APT has been studied in [20] and [21] research. OODA loop for blue team or defender in research scenario is as follows:

1) Observe: SOC target or defender team checks the results of network monitoring through Security Onion to find and collect network data. Security onion is agent based for cyber-attack defense [22]. The network monitor display on Security Onion can be seen in Fig. 12.

2) Orient: Filter and check for alerts detected by Security Onion. From these alerts, SOC performs an analysis to find suspicious activity. At this stage, the SOC can download the .pcap file to facilitate the analysis process. Based on the results of the analysis, it was found that there is HTTP access to an unknown IP address. Fig. 13 shows an HTTP access alert from a 192.168.110.2 (VM 410) to 192.168.170.2 (VM 101).

After further inspection with PCAP file, it was suspected that there was the theft of files from one computer because there was a file that was compressed in the .zip format as shown in Fig. 14. This allegation was also strengthened by evidence in the form of an email sent to several employees of PT TRINAKLIR containing a payload.

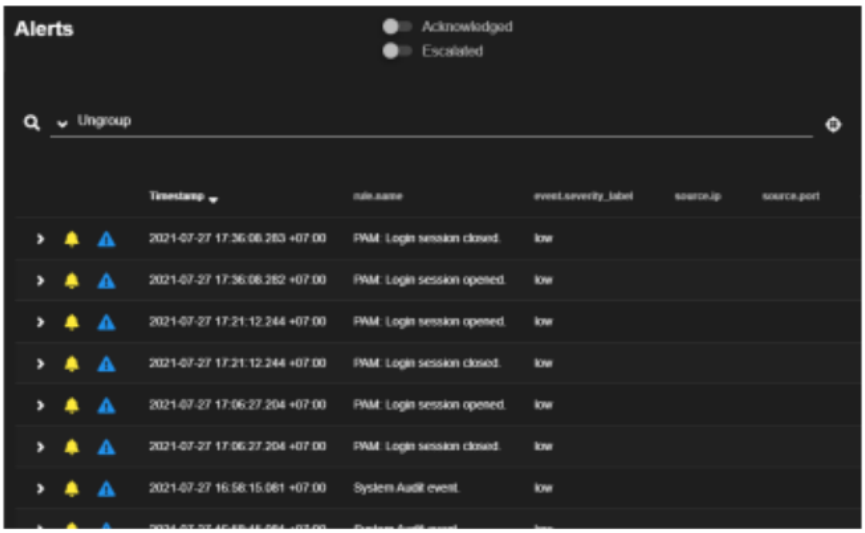

Fig. 12. Network Monitor Display on Security Onion.

Fig. 13. HTTP Access Alert Detail.

Fig. 14. Compressed File Delivery.

3) Decide: SOC determines solutions or steps that need to be taken to deal with attacks that occur and prevent similar incidents. These solutions can be in the form of creating incident tickets, forensic analysis of the victim's computer, blocking IP addresses from attackers, as well as cyber security awareness education to employees. However, in this scenario, the actions taken are limited to only generating tickets with TheHive escalated case from alert seen in Fig. 15 for the incidents that occur.

4) Act: Case from Fig. 15 can be more explored for detail. In simulating real SOC that has some tier, the case in TheHive is built for the task of assigning work to other SOC members as shown in Fig. 16.

5) Observe: The OODA loop is an iterative process, so that after the previous incident has been successfully handled, the SOC returns to monitor the network to maintain the security of target's network [23].

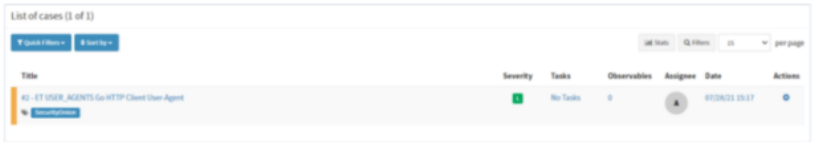

Fig. 15. Ticket Registered.

Fig. 16. Task Generated.

E. UAT Questionnaire

Evaluation of research results in the form of the cyber range is also carried out through UAT testing with respondent, 11 cybersecurity lecture (all population of cybersecurity engineering programme). Making instruments in the questionnaire aims to determine whether the features of the cyber range have met the cyber range taxonomy and can meet the needs of cyber security learning tools. The results of filling out the questionnaire were then analyzed using a Likert scale. The Likert scale is a measurement scale that aims to measure respondents' opinions on research results from very positive to very negative and in the form of words [24][25][26]. Table VII is list of questionnaire in this research.

TABLE VII. USER ACCEPTANCE TEST QUESTIONNAIRE

No	Statement	SS	S	R	TS	STS
1	The operation of the cyber range is easy for first-time users to learn					
2	The steps in the attack simulation scenario at the cyber range are in accordance with the OODA loop so that it is easy to understand and execute.					
3	Cyber range can meet cyber security learning					
4	Cyber range provides an isolated environment to execute simulated attack scenarios.					
5	All the tools in the cyber range work well.					
6	The monitoring system on the cyber range is running well.					
7	Cyber range can help cadets understand the role of the red team and blue team.					
8	The scoring method (assessment of attack simulation results) on the cyber range is running well.					
9	Cyber range management or management can be done easily					

F. UAT Questionnaire Analysis

The results of the UAT response data were then analyzed to measure the respondent's level of agreement with each statement in the UAT questionnaire using the following equation:

$$\frac{\sum(a \times b)}{c \times d} \quad (1)$$

a = total number of respondents who chose the b answer

b = score of the answer choices

c = respondent total

d = highest score

Furthermore, the results of the previous calculations are summed and recalculated to determine the level of acceptance of the cyber range that was built as a whole using the following equation:

$$\frac{\sum wx}{x \times y \times z} \times 100\% \quad (2)$$

w = total score of respondent's choice

x = total statement

y = total answer

z = highest score

Where w is score total of respondent's choice, x is total statement, y is total respondent, z is highest score.

V. RESULT AND DISCUSSION

A. Result of Reaching the Needs

The cyber range that has been built is then evaluated to find out the results of meeting the needs of the cyber range against the needs analysis that has been compiled based on the cyber range taxonomy. Based on the results of fulfilling the needs, cyber range meets 16 of 17 seen in Table VIII. Characteristics that are not fulfilled is special tools for scoring. In this cyber range, scoring is done by checking the success of the attack stages as well as ticketing with the help of Security Onion

monitoring tools, CALDERA attack automation tools and TheHive ticketing tools. The overall cyber range acceptance rate with formula 2 is 81.82%.

TABLE VIII. FULFILLMENT NEEDS RESULT

No	Req	Characteristics of Taxonomy	Fulfilled
1	Cyber range has a clear scenario development goal, namely simulating data theft attacks.	Scenario (Goals)	Yes
2	Cyber range provides an isolated environment to execute simulated attack scenarios in physical, virtual, or hybrid forms consisting of the target and attacker infrastructure.	Scenario (Environment)	Yes
3	Cyber range provides the storyline of the scenario to provide an overview of how the scenario execution process.	Scenario (Storyline)	Yes
4	Cyber range provides a static or dynamic scenario.	Scenario (Type)	Yes
5	The scenario in the cyber range is applied to a particular domain.	Scenario (Domain)	Yes
6	Cyber range can use a variety of tools to build or run a scenario.	Scenario (Tools)	Yes
7	Cyber range provides a particular method for monitoring the simulation of attacks carried out.	Monitoring (Method)	Yes
8	Cyber range provides special tools for monitoring systems.	Monitoring (Tools)	Yes
9	The monitoring system in cyber range works at the TCP/IP layer.	Monitoring (Layer)	Yes
10	Cyber range provides a red team role.	Teaming (Red team)	Yes
11	Cyber range provides a blue team role.	Teaming (Blue team)	Yes
12	Cyber range provides the role of an autonomous team.	Teaming (Autonomous team)	Yes
13	Cyber range provides a specific scoring method.	Scoring (Method)	Yes
14	Cyber range provides special tools for scoring.	Scoring (Tools)	No
15	Cyber range provides role management features.	Management (Role)	Yes
16	Cyber range provides computing resource management features	Management (Resource)	Yes
17	Cyber range provides range management features.	Management (Range)	Yes

B. UAT Questionnaire

Table IX is compilation of UAT result. Analysis results of the UAT response data with formula 1 is 405 in the Agree area seen in Fig. 17.

Fig. 17. Questionnaire Result.

TABLE IX. USER ACCEPTANNCE TEST RESULT

respondent	P1	P2	P3	P4	P5	P6	P7	P8	P9
1	3	4	5	4	4	4	5	3	4
2	4	4	5	5	4	4	5	4	4
3	2	4	5	5	4	4	5	2	4
4	4	4	5	5	4	5	5	5	4
5	3	4	5	4	4	4	4	3	3
6	2	4	5	5	3	3	4	4	3
7	4	4	5	5	4	4	5	4	4
8	4	4	4	4	4	4	4	4	2
9	4	4	4	4	4	4	4	4	3
10	4	5	5	5	5	4	5	4	4
11	4	4	4	5	4	4	5	4	4
Total	38	45	52	51	44	44	51	41	39
Precentage	69,09	81,81	94,55	92,73	80	80	92,73	74,55	70,91

VI. CONCLUSION

Based on meeting the needs, the cyber range meets 16 of the 17 characteristics in the cyber range taxonomy. Based on the results of the UAT questionnaire, a score of 405 was obtained in the Agree area, and the overall cyber range acceptance rate was 81.82%. This result also states that Observe-Orient-Decide-Act (OODA) for Cyber Security Education can be implemented globally.

VII. FUTURE WORKS

The scenario contained in the cyber range is only a simulation of data theft attacks. It is necessary to build a simulation with other cases to meet the learning needs of a more complete range of cybersecurity. The CALDERA agent tool can only run on Windows operating systems. It is necessary to add other similar tools so that attack simulations can be carried out on other operating systems. System performance from cyber reach has not been tested through stress tests or measured by certain methods. Cyber range performance testing and scenario and tool enhancement can be used as further research.

REFERENCES

[1] I. Bica and R. Reyhanitabar, "Preface," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10006 LNCS, p. V, 2016, doi: 10.1007/978-3-319-47238-6.

[2] S. Azadegan and M. O'Leary, "An undergraduate Cyber Operations curriculum in the making: A 10+ year report," IEEE Int. Conf. Intell. Secur. Informatics Cybersecurity Big Data, ISI, pp. 251–254, doi: 10.1109/ISI.2016.7745484.

[3] F. P. B. Osinga, Science, Strategy and War, 1st ed. Ney York: Routledge, 2007.

[4] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," IEEE Access, vol. 8, doi: 10.1109/ACCESS.2020.3045514.

[5] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "Cyber ranges and testbeds for education, training, and research," Appl. Sci, vol. 11, no. 4, pp. 1–23, doi: 10.3390/app11041809.

[6] E. Ukwandu et al., "A review of cyber-ranges and test-beds: Current and future trends," Sensors (Switzerland), vol. 20, no. 24, pp. 1–36, 2020, doi: 10.3390/s20247148.

[7] M. M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," Comput. Secur., vol. 88, p. 101636, 2020, doi: 10.1016/j.cose.2019.101636.

[8] M. H. Khyavi, "ISMS role in the improvement of digital forensics related process in SOC's," Cryptogr. Secur., 2020.

[9] C. DeCusatis, R. Cannistra, A. Labouseur, and M. Johnson, Design and implementation of a research and education cybersecurity operations center. Springer International Publishing, 2019.

[10] C. Zhong, A. Alnusair, B. Sayger, A. Troxell, and J. Yao, "AOH-Map: A Mind Mapping System for Supporting Collaborative Cyber Security Analysis," Proc. - 2019 IEEE Conf. Cogn. Comput. Asp. Situat. Manag. CogSIMA 2019, pp. 74–80, 2019, doi: 10.1109/COGSIMA.2019.8724159.

[11] V. K. R. Baskerville "Foreword From Vaishnavi and (W. K., Design Science Research Methods and Patterns : Innovating Information and Communication Technology, 2nd ed. New York: CRC Press.

[12] S. Mahardhika, "Analisis Pemodelan Serangan Advanced Persistent Threat dengan Menggunakan Diamond Model of Intrusion Analysis dan Kill Chain." Sekolah Tinggi Sandi Negara.

[13] M. Leitner, "AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research," ACM Int. Conf. Proceeding Ser, doi: 10.1145/3424954.3424959.

[14] T. J. Grant, H. S. Venter, and J. H. P. Eloff, "Simulating adversarial interactions between intruders and system administrators using OODA-RR," ACM Int. Conf. Proceeding Ser., vol. 226, pp. 46–55, 2007, doi: 10.1145/1292491.1292497.

[15] T. Debatty and W. Mees, "Building a Cyber Range for training CyberDefense Situation Awareness," 2019 Int. Conf. Mil. Commun. Inf. Syst. ICMCIS 2019, pp. 1–6, 2019, doi: 10.1109/ICMCIS.2019.8842802.

[16] V. K. R. B. "Foreword F. Vaishnavi and (W K., Design Science Research Methods and Patterns : Innovating Information and Communication Technology, 2nd ed. New York: CRC Press.

[17] F. Extension and P. R. Brandao, "Advanced Persistent Threats (APT)-Attribution-MICTIC," J. Comput. Sci., vol. 17, no. 5, pp. 470–479, 2021, doi: 10.3844/jcssp.2021.470.479.

[18] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," J. Netw. Comput. Appl, vol. 101, pp. 18–54, doi: 10.1016/j.jnca.2017.10.016.

[19] A. Applebaum, D. Miller, B. Strom, C. Korban, and R. Wolf, "Intelligent, automated red team emulation," ACM Int. Conf. Proceeding Ser, vol. 5-9-Decemb, pp. 363–373, doi: 10.1145/2991079.2991111.

[20] M. B. Khan, "Advanced Persistent Threat: Detection and Defence," arXiv, 2020.

[21] J. H. Joloudari, M. Haderbadi, A. Mashmool, M. Ghasemigol, S. S. Band, and A. Mosavi, "Early detection of the advanced persistent threat attack using performance analysis of deep learning," IEEE Access, vol. 8, pp. 186125–186137, 2020, doi: 10.1109/ACCESS.2020.3029202.

[22] J. D. Yoo, "Cyber attack and defense emulation agents," Appl. Sci, vol. 10, no. 6, pp. 1–20, doi: 10.3390/app10062140.

[23] J. Silvander and L. Angelin, "Introducing intents to the OODA-loop," Procedia Comput. Sci, vol. 159, pp. 878–883, doi: 10.1016/j.procs.2019.09.247.

[24] A. Joshi, S. Kale, S. Chandel, and D. Pal, "Likert Scale: Explored and Explained," Br. J. Appl. Sci. Technol., vol. 7, no. 4, pp. 396–403, 2015, doi: 10.9734/bjast/2015/14975.

[25] B. P. Subedi, "Using Likert Type Data in Social Science Research: Confusion, Issues and Challenges," Int. J. Contemp. Appl. Sci., vol. 3, no. 2, pp. 2308–1365, 2016.

[26] James T Croasmun and Lee Ostrom, "Using Likert-type scales in the social sciences," J. Adult Educ., vol. 40, no. 1, pp. 19–22, 2011.

Observe-Orient-Decide-Act (OODA) for Cyber Security Education

ORIGINALITY REPORT

3%
SIMILARITY INDEX

PRIMARY SOURCES

1	papers.academic-conferences.org Internet	153 words — 3%
2	Bo Liu, Jiawei Li, Weiwei Lin, Weihua Bai, Pengfei Li, Qian Gao. "K‐PSO: An improved PSO‐based container scheduling algorithm for big data applications", International Journal of Network Management, 2020 Crossref	18 words — < 1%
3	Liuyue Jiang, Asangi Jayatilaka, Mehwish Nasim, Marthie Grobler, Mansooreh Zahedi, M. Ali Babar. "Systematic Literature Review on Cyber Situational Awareness Visualizations", IEEE Access, 2022 Crossref	11 words — < 1%
4	docplayer.com.br Internet	11 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	OFF	EXCLUDE MATCHES	OFF