

# Industry Report

## Semester-8

## Internship

**Developed By: -**

Vishwarajsinh Rathod (CS) (20162171024)

**Guided By: -**

Prof. Prakruti Parmar (Internal)

Mr. Rahul Joshi (External)

**Submitted to**  
**Department of Computer Science & Engineering**  
**Institute of Computer Technology**



**Ganpat  
University**

॥ विद्यया समाजोत्कर्षः ॥

**Institute of  
Computer  
Technology**



**Year: 2024**



## CERTIFICATE

This is to certify that the **INDUSTRY** Work Vishwarajsinh Rathod (Enrolment No. 20162171024), of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by them in the CSE(CBA/BDA/CS). The results/findings contained in this Project have not been submitted in part or full to any other University / Institute for award of any other Degree/Diploma.

Name & Signature of Internal Guide

Name & Signature of Head

**Place: ICT - GUNI**

**Date: 12th May, 2024**

allianz cloud

803 Ocean, Sarabhai Main Road,  
Vadodara - 390023  
Tel: +91 9925200624  
CIN No.: U72900GJ2016PTC093690

On letter head of Allianz Cloud Pvt Ltd.



### Certificate of Internship Completion

This is to certify that Rathod Vishwarajsinh Shailendrasinh, a student of Institute of Computer Technology, Ganpat University, has successfully completed an internship in the field of Cyber Security at **Allianz Cloud Pvt, Ltd.** from January 01st, 2024, to April 30th, 2024, totaling 18 weeks.

During this internship, Vishwarajsinh was under the guidance of Mr. Rahul Joshi, our Chief Technology Officer. His internship activities primarily included Cyber Security - Vulnerability Assessment and Penetration Testing (VAPT) and Compliance.

Vishwarajsinh exhibited exceptional diligence, hard work, and a keen interest in learning throughout his tenure with us. He actively engaged in various processes and tasks assigned to him, demonstrating his adaptability and commitment to excellence.

We hereby acknowledge Vishwarajsinh's dedication and contribution to our organization and wish him continued success in his future endeavors.

Date: April 30th, 2024

For Allianz Cloud Pvt, Ltd.

  
Ashit Parekh

(HR Head)

M. 91- 9925200624



## **ACKNOWLEDGEMENT**

Industry Internship is a golden opportunity for learning and self-development. I consider myself very lucky and honored to have so many wonderful people lead me through in completion of this project. First and foremost, I would like to thank Dr. Rohit Patel, Principal, ICT, and Prof. Dharmesh Darji, Head, ICT who gave us an opportunity to undertake this project. My grateful thanks to Prof. Palwinder Singh for their guidance in project work, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where we would have been without his/her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

**Vishwarajsinh Rathod**

**(Enrollment No: 20162171024)**

## TABLE OF CONTENT

Title		Page Number
	<b>Title Page</b>	I
	<b>Certificate</b>	II
	<b>Acknowledge</b>	III
	<b>Table of Contents</b>	1-2
<b>1.</b>	<b>Overview of the Company</b>	3
	1.1 About Us	3
	1.2 Services	3
<b>2</b>	<b>Week-1 Progress</b>	4
	2.1 List of Task	4
	2.2 Tool/Technology/Approach to perform the task	4
	2.3 Screenshot	5
<b>3</b>	<b>Week-2 Progress</b>	6
	3.1 List of Task	6
	3.2 Tool/Technology/Approach to perform the task	6
	3.3 Screenshot	6
<b>4</b>	<b>Week-3 Progress</b>	7
	4.1 List of Task	7
	4.2 Tool/Technology/Approach to perform the task	7
	4.3 Screenshot	7
<b>5</b>	<b>Week-4 Progress</b>	8
	5.1 List of Task	8
	5.2 Tool/Technology/Approach to perform the task	8
	5.3 Screenshot	8
<b>6</b>	<b>Week-5 Progress</b>	9
	6.1 List of Task	9
	6.2 Tool/Technology/Approach to perform the task	9
	6.3 Screenshot	9
<b>7</b>	<b>Week-6 Progress</b>	10
	7.1 List of Task	10
	7.2 Tool/Technology/Approach to perform the task	10
	7.3 Screenshot	10
<b>8</b>	<b>Week-7 Progress</b>	11
	8.1 List of Task	11
	8.2 Tool/Technology/Approach to perform the task	11
	8.3 Screenshot	11

<b>9</b>	<b>Week-8 Progress</b>	12
	9.1 List of Task	12
	9.2 Tool/Technology/Approach to perform the task	12
	9.3 Screenshot	13
<b>10</b>	<b>Week-9 Progress</b>	14
	10.1 List of Task	14
	10.2 Tool/Technology/Approach to perform the task	14
	10.3 Screenshot	14
<b>11</b>	<b>Week-10 Progress</b>	15
	11.1 List of Task	15
	11.2 Tool/Technology/Approach to perform the task	15
	11.3 Screenshot	15
<b>12</b>	<b>Week-11 Progress</b>	16
	12.1 List of Task	16
	12.2 Tool/Technology/Approach to perform the task	16
	12.3 Screenshot	16
<b>13</b>	<b>Week-12 Progress</b>	17
	13.1 List of Task	17
	13.2 Tool/Technology/Approach to perform the task	17
	13.3 Screenshot	17
<b>14</b>	<b>Week-13 Progress</b>	18
	14.1 List of Task	18
	14.2 Tool/Technology/Approach to perform the task	18
<b>15</b>	<b>Week-14 Progress</b>	19
	15.1 List of Task	19
	15.2 Tool/Technology/Approach to perform the task	19
<b>16</b>	<b>Week-15 and Week 16 Progress</b>	20-21
	16.1 List of Task	20-21
	16.2 Tool/Technology/Approach to perform the task	20-21
	16.3 Screenshot	20-21
<b>17</b>	<b>Week-16 and Week 17 Progress</b>	20-21
	17.1 List of Task	20-21
	17.2 Tool/Technology/Approach to perform the task	20-21
<b>18</b>	<b>Conclusion</b>	22

# **CHAPTER - 1**

## **1.1 ABOUT US:**

Since its establishment in 2003, Allianz Cloud has fostered an entrepreneurial environment, driving continuous evolution and innovation to meet the dynamic needs of its clients and industry. Headquartered in Vadodara, India, Allianz Group operates globally, including regions like the US, Kenya, Hong Kong, and the Middle East. Allianz Cloud, a subsidiary of Allianz Group, specializes in cloud computing, telecommunications, and information security. Mission: Deliver innovative services by challenging norms, embracing innovation, and evolving to meet client and industry needs.

## **1.2 SERVICES:**

### **❖ Allianz Cloud operates with key departments:**

- IT Enabled Solutions
- Information Security
- Telecommunications
- Datacenter Services
- Cloud Infrastructure

### **❖ Departments play crucial roles:**

- IT Solutions tailored to client needs
- Safeguarding data and systems from cyber threats
- Managing telecommunications infrastructure
- Ensuring data center reliability, security, and performance
- Managing and maintaining cloud infrastructure

## **CHAPTER - 2**

### **2.1 LIST OF TASK:**

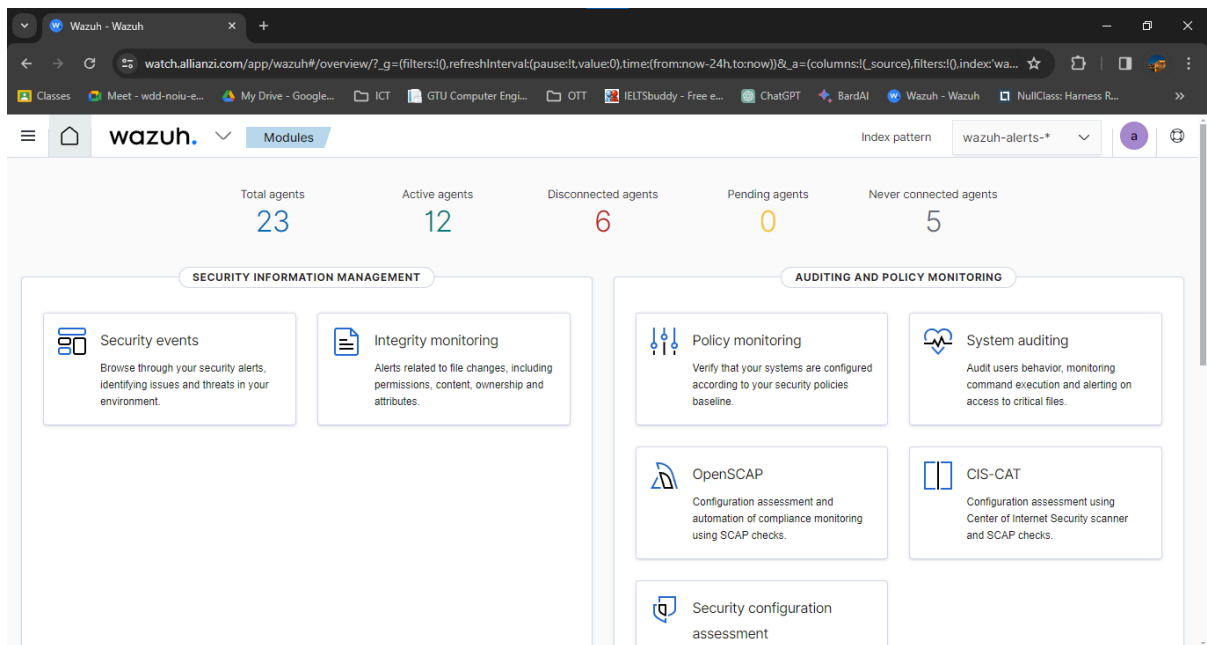
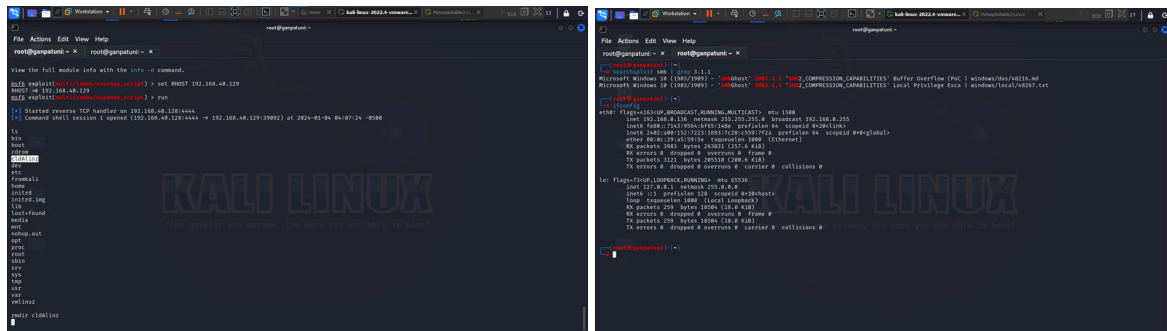
- ❖ Penetration Testing on Metasploitable (Linux) and Windows 10.
  - Conducting ethical hacking assessments on Metasploitable (Linux) and Windows 10 to identify vulnerabilities and weaknesses. Utilizing tools like Metasploit, the tests simulate real-world cyber threats, aiming to enhance the overall security posture of the systems. The results offer actionable insights for proactive defense measures.
- ❖ Practical exposure to utilizing Wazuh in real-world scenarios.
  - Obtaining real-world proficiency in deploying and using Wazuh for log analysis, intrusion detection, and vulnerability detection. This hands-on experience enhances understanding of Wazuh's capabilities in threat detection, incident response, and compliance management, contributing to effective cybersecurity practices.

### **2.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:**

- ❖ Nmap
- ❖ Msfconsole
- ❖ Wazuh



## 2.3 SCREENSHOTS:



## CHAPTER - 3

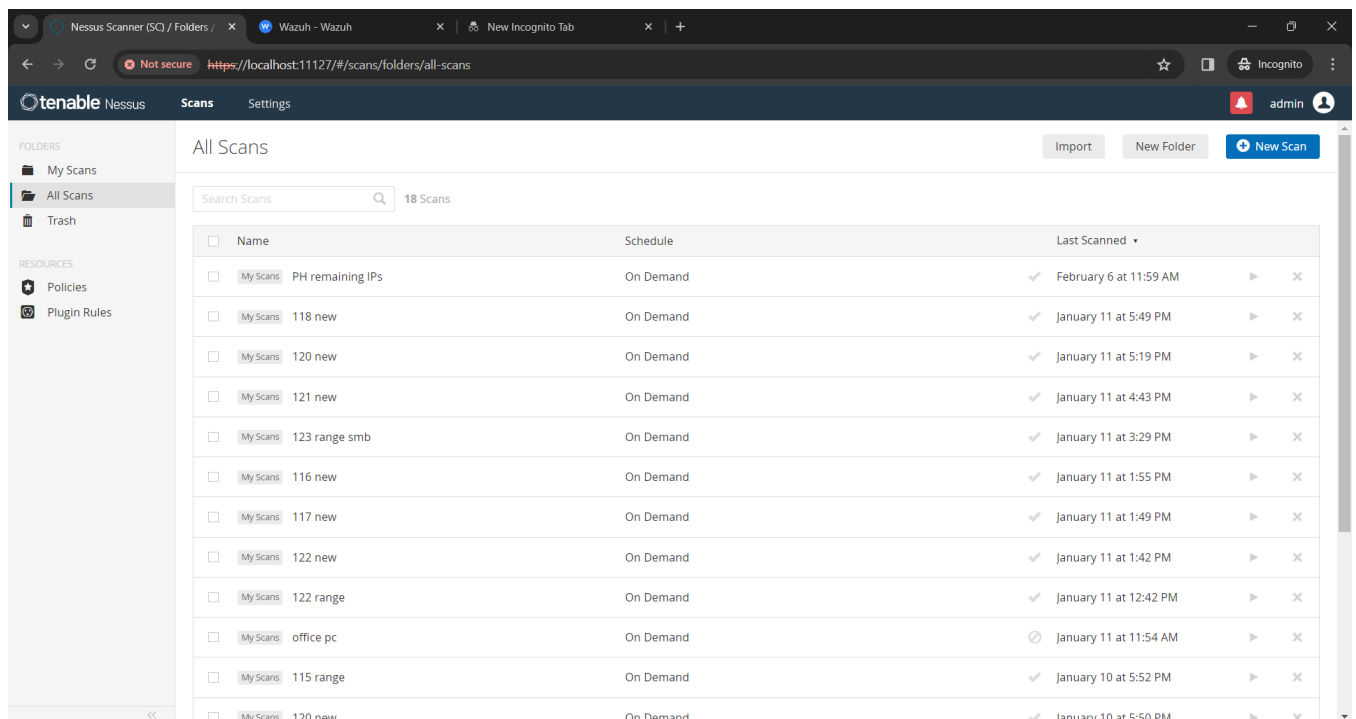
### 3.1 LIST OF TASK:

- ❖ Discovered diverse vulnerabilities using the Nessus Tool, subsequently addressing and remediating them through the application of necessary security updates. Conducted a comprehensive rescan on all systems to identify and rectify any potential issues that may exist, ensuring a thorough approach to cybersecurity.

### 3.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Nessus
- ❖ Angry IP
- ❖ Wazuh

### 3.3 SCREENSHOTS:



The screenshot displays the Tenable Nessus web interface. The left sidebar shows the navigation menu with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules). The main content area is titled 'All Scans' and shows a search bar with '18 Scans' results. A table lists the scans with columns for Name, Schedule, and Last Scanned. The scans are listed in descending order of last scanned time.

<input type="checkbox"/>	Name	Schedule	Last Scanned		
<input type="checkbox"/>	My Scans PH remaining IPs	On Demand	✓ February 6 at 11:59 AM	▶	✕
<input type="checkbox"/>	My Scans 118 new	On Demand	✓ January 11 at 5:49 PM	▶	✕
<input type="checkbox"/>	My Scans 120 new	On Demand	✓ January 11 at 5:19 PM	▶	✕
<input type="checkbox"/>	My Scans 121 new	On Demand	✓ January 11 at 4:43 PM	▶	✕
<input type="checkbox"/>	My Scans 123 range smb	On Demand	✓ January 11 at 3:29 PM	▶	✕
<input type="checkbox"/>	My Scans 116 new	On Demand	✓ January 11 at 1:55 PM	▶	✕
<input type="checkbox"/>	My Scans 117 new	On Demand	✓ January 11 at 1:49 PM	▶	✕
<input type="checkbox"/>	My Scans 122 new	On Demand	✓ January 11 at 1:42 PM	▶	✕
<input type="checkbox"/>	My Scans 122 range	On Demand	✓ January 11 at 12:42 PM	▶	✕
<input type="checkbox"/>	My Scans office pc	On Demand	⌚ January 11 at 11:54 AM	▶	✕
<input type="checkbox"/>	My Scans 115 range	On Demand	✓ January 10 at 5:52 PM	▶	✕
<input type="checkbox"/>	My Scans 120 new	On Demand	✓ January 10 at 5:50 PM	▶	✕

# CHAPTER - 4

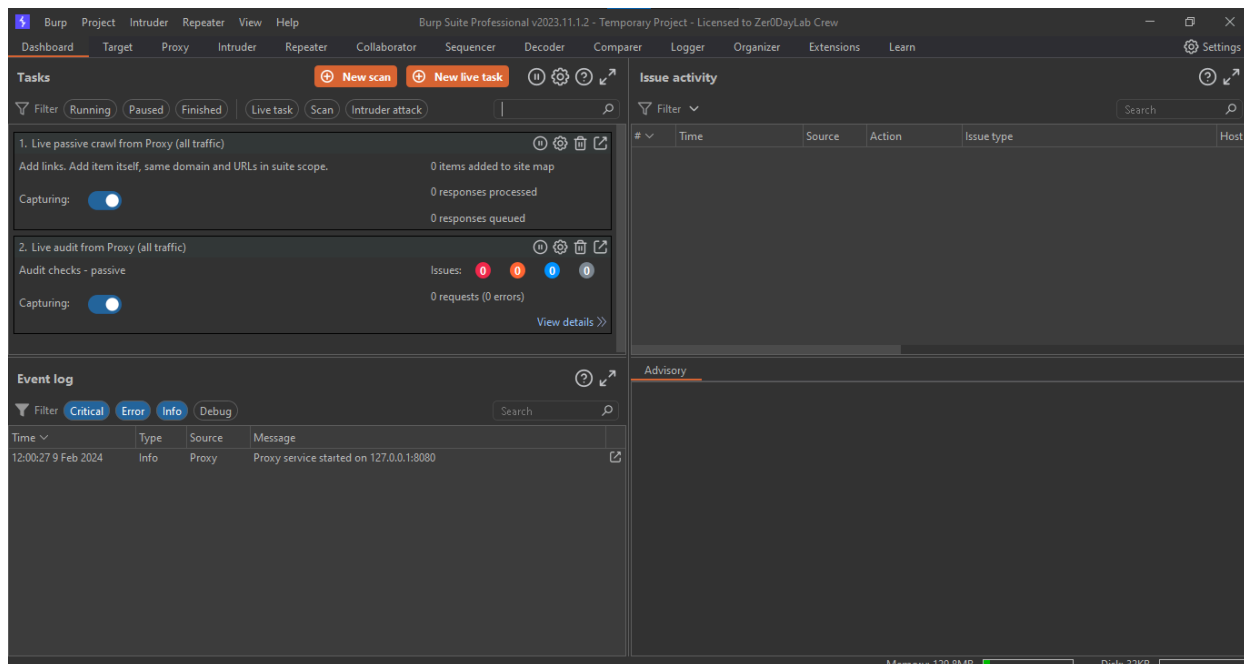
## 4.1 LIST OF TASK:

- ❖ Conducting web application security assessments with BurpSuite, scrutinizing the interaction between a web application and its users to identify and address potential security vulnerabilities. This process involves in-depth analysis of data exchanges, aiming to fortify the application's defenses against cyber threats.

## 4.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ BurpSuite
- ❖ SQLMAP
- ❖ DirSearch

## 4.3 SCREENSHOTS:



# CHAPTER - 5

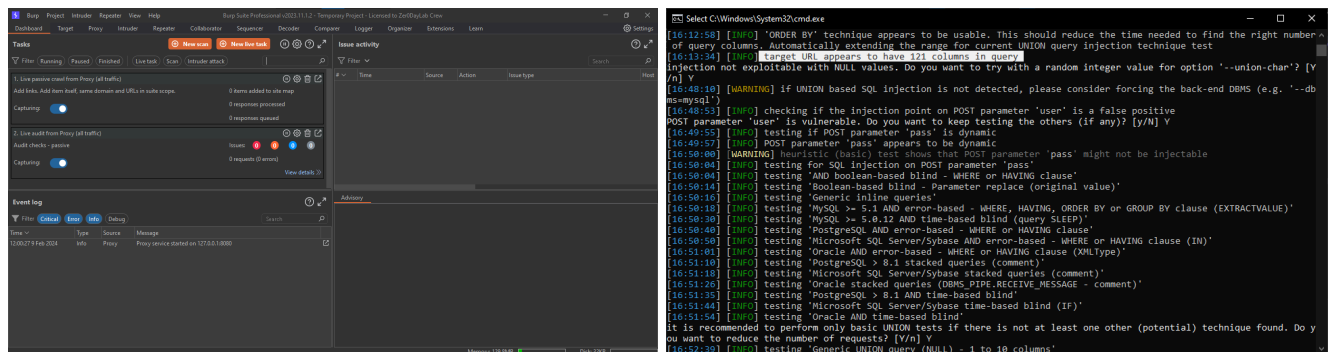
## 5.1 LIST OF TASK:

- ❖ Executed SQL Injection, accessing the Admin Panel, acquiring unrestricted customer data, including personal details and sensitive account credentials, posing significant security and privacy risks. Additionally, gained access to transactional data, amplifying the potential impact on security..

## 5.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Acunetix
- ❖ BurpSuite
- ❖ SQLMAP

## 5.3 SCREENSHOTS:



## CHAPTER - 6

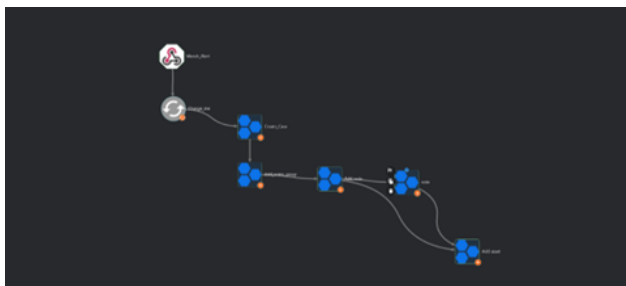
### 6.1 LIST OF TASK:

- ❖ The integration of Wazuh, Shuffle, and IRIS automates alert retrieval, case creation, and incident response, boosting security operations effectiveness. Shuffle expedites incident response by automating routine tasks, resulting in quicker reaction times to security threats. The automation of case creation in IRIS from alerts sourced from Wazuh and Shuffle enhances incident response by ensuring swift detection and resolution of security issues. Automated workflows in IRIS for managing notes, assets, and incident details contribute to a streamlined and efficient incident response process.

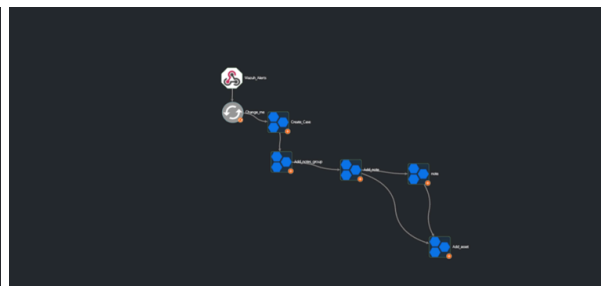
### 6.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris

### 6.3 SCREENSHOTS:



**Linux**



**Windows**

## CHAPTER - 7

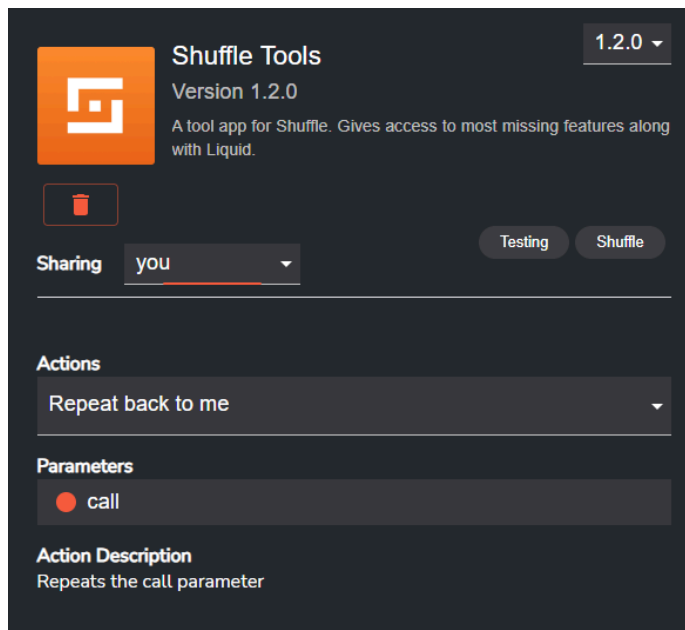
### 7.1 LIST OF TASK:

- ❖ Shuffle, with its apps and nodes, facilitates collaboration between tools via API keys, enhancing security event management. When integrated with Wazuh, it optimizes security event handling by automating processes like alert management and incident response, improving overall operational efficiency.

### 7.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris

### 7.3 SCREENSHOTS:



## CHAPTER - 8

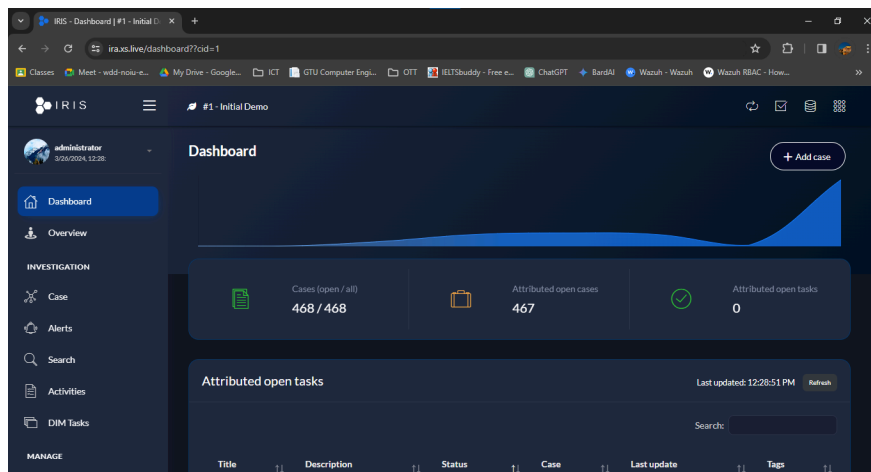
### 8.1 LIST OF TASK:

- ❖ DFIR-Iris is a comprehensive platform designed for digital forensics and incident response (DFIR) tasks. It offers a wide array of features such as case management, evidence collection, analysis tools, and reporting capabilities. DFIR-Iris streamlines the entire investigative process, from initial incident identification to evidence collection, analysis, and resolution, enabling security teams to effectively handle security incidents and mitigate risks.

### 8.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris

### 8.3 SCREENSHOTS:



## **CHAPTER - 9**

### **9.1 LIST OF TASK:**

- ❖ The procedure entails establishing user profiles, delineating their access privileges and responsibilities, and enrolling them into designated groups with constrained permissions. This systematic approach ensures that users are granted access tailored to their roles while maintaining stringent control over sensitive resources, bolstering overall security measures.

### **9.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:**

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris



9.3 SCREENSHOTS:

Users

Add user

Audit users

Refresh

Show 10 entries

Search:

#ID	Name	Login Name	Email	Active	Service Account
1	administrator			Active	✖
2	Darshak Solanki			Active	✖
3	Darshit Gorasiya			Active	✖
6	Jay Shah			Active	✖
7	Manager			Active	✖
8	Moin Shaikh			Active	✖
9	Office Beacon IND			Active	✖
10	Office Beacon PH			Active	✖
4	Shreyas Desai			Active	✖
11	Vaibhav Patel			Active	✖

Groups

Add group

Refresh

Show 10 entries

Search:

#ID	Name	Description	Permissions	#Members
1	Administrators	Administrators	standard_user, server_administrator, alerts_read, alerts_write, alerts_delete, search_across_cases, customers_read, customers_write, case_templates_read, case_templates_write, activities_read, all_activities_read	1
2	Analysts	Interns	standard_user, alerts_read, search_across_cases, customers_read, case_templates_read, activities_read	6
4	Office Beacon	Read Only		3
3	SOC-Manager	Manager	standard_user, alerts_read, alerts_write, alerts_delete, search_across_cases, customers_read, customers_write, case_templates_read, case_templates_write, activities_read	1
#ID	Name	Description	Permissions	#Members

Showing 1 to 4 of 4 entries

Previous

1

Next

## CHAPTER - 10

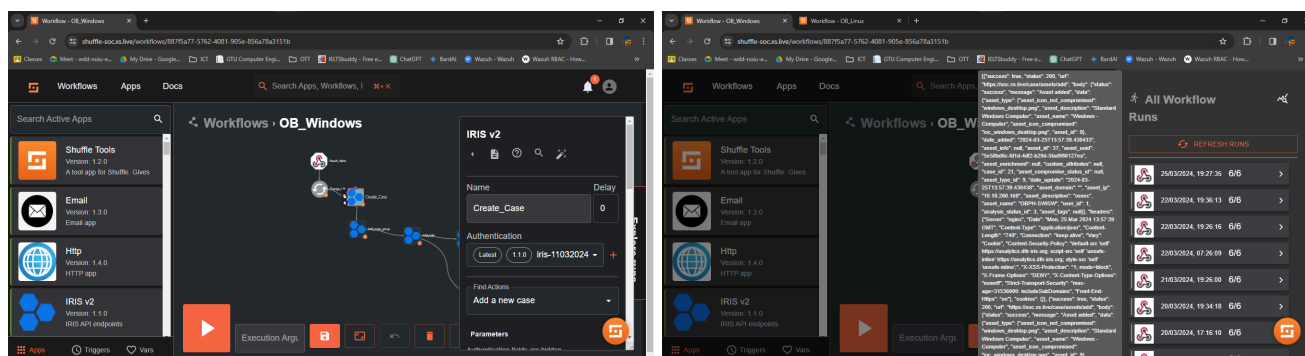
### 10.1 LIST OF TASK:

- ❖ Automating case creation in IRIS based on alerts retrieved from Wazuh and Shuffle, including those triggered by specific rule IDs defined in Wazuh configuration, amplifies incident response effectiveness. The automated workflows within Shuffle for managing notes, assets, and incident details further refine the incident response process, fostering organization and efficiency. This streamlined approach empowers security teams to swiftly address security incidents, thereby reducing potential impact and bolstering the overall security posture of the organization.

### 10.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris

### 10.3 SCREENSHOTS:



## CHAPTER - 11

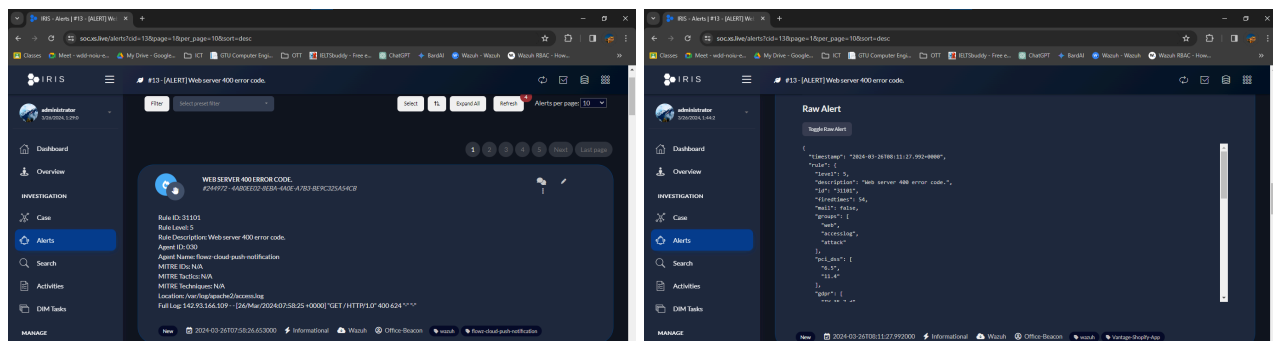
### 11.1 LIST OF TASK:

- ❖ Alerts in IRIS originating from Wazuh signify potential security issues detected by the Wazuh intrusion detection and monitoring system. These alerts provide insights into suspicious activities, anomalies, or potential threats identified across the organization's network and systems. By receiving alerts from Wazuh in IRIS, security teams can centrally manage and respond to security incidents, facilitating swift detection, investigation, and resolution of threats to the organization's infrastructure.

## 11.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris

### 11.3 SCREENSHOTS:



# CHAPTER - 12

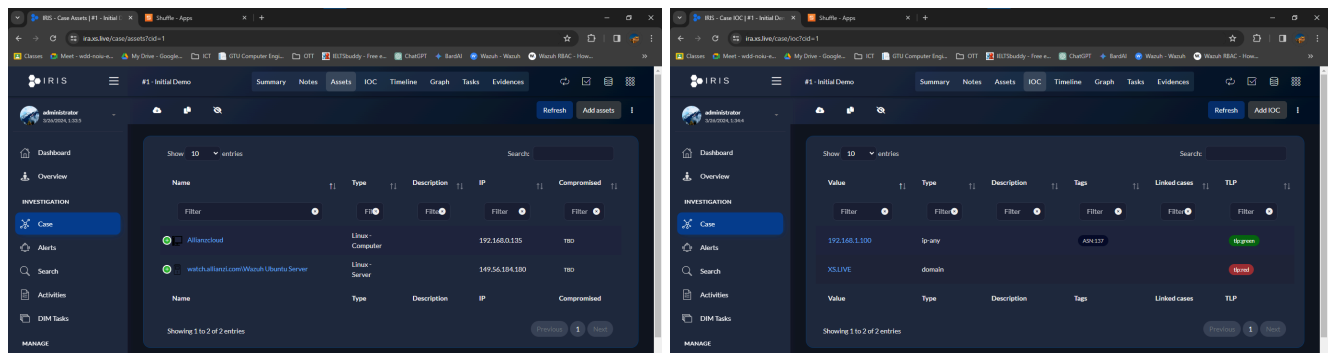
## 12.1 LIST OF TASK:

- ❖ The case description within IRIS entails thorough documentation of the security incident, incorporating relevant notes, assets, and indicators of compromise (IOCs). These components provide crucial context and insights into the incident's progression, aiding in effective incident response and future threat mitigation. By capturing comprehensive details, cybersecurity teams can collaborate efficiently and enhance the organization's overall security posture.

## 12.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris

## 12.3 SCREENSHOTS:



## **CHAPTER - 13**

### **13.1 LIST OF TASK:**

- ❖ Once the case solution is formulated, it is communicated to the client. This communication includes detailing the steps taken to address the security incident, providing insights into the remediation measures implemented, and offering recommendations to prevent similar incidents in the future. This transparent and proactive approach ensures the client is informed and reassured regarding the organization's security measures.

### **13.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:**

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris

## CHAPTER - 14

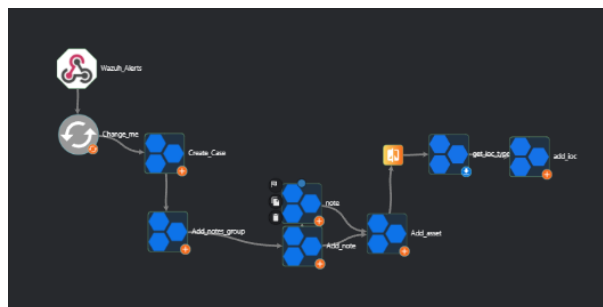
### 14.1 LIST OF TASK:

- ❖ The updated workflow incorporates automated IOC addition by parsing threat intelligence data. As new threat intelligence sources are ingested, the system automatically parses the incoming reports and extracts relevant IOCs, such as IP addresses, and domains. These IOCs are then seamlessly integrated into the system's threat intelligence database, enhancing its ability to detect and respond to emerging threats. By automating the process of IOC parsing and addition, the workflow becomes more efficient, enabling faster threat detection and response times.

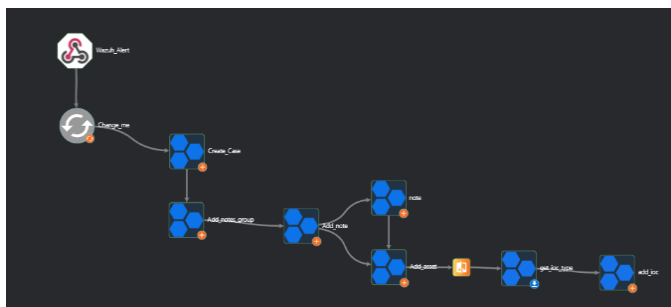
### 14.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Shuffle
- ❖ Iris

### 14.3 SCREENSHOTS:



Windows



Linux

## **CHAPTER - 15**

### **15.1 LIST OF TASK:**

- ❖ The MISP (Malware Information Sharing Platform) module integrated into Iris with the help of Cortex serves as a powerful tool for cybersecurity analysis and response, providing detailed insights into reports and threat intelligence data. This module enables users to access and analyze a wide range of threat intelligence feeds, reports, and indicators of compromise (IOCs) gathered from various sources. By leveraging the MISP module, organizations can gain valuable insights into emerging threats, trends, and attack patterns, empowering them to proactively defend against cyber threats and mitigate potential risks to their infrastructure. Additionally, the module facilitates collaboration and information sharing among security teams, enabling more effective threat detection and response efforts.

### **15.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:**

- ❖ Shuffle
- ❖ Iris
- ❖ Cortex

## CHAPTER - 16

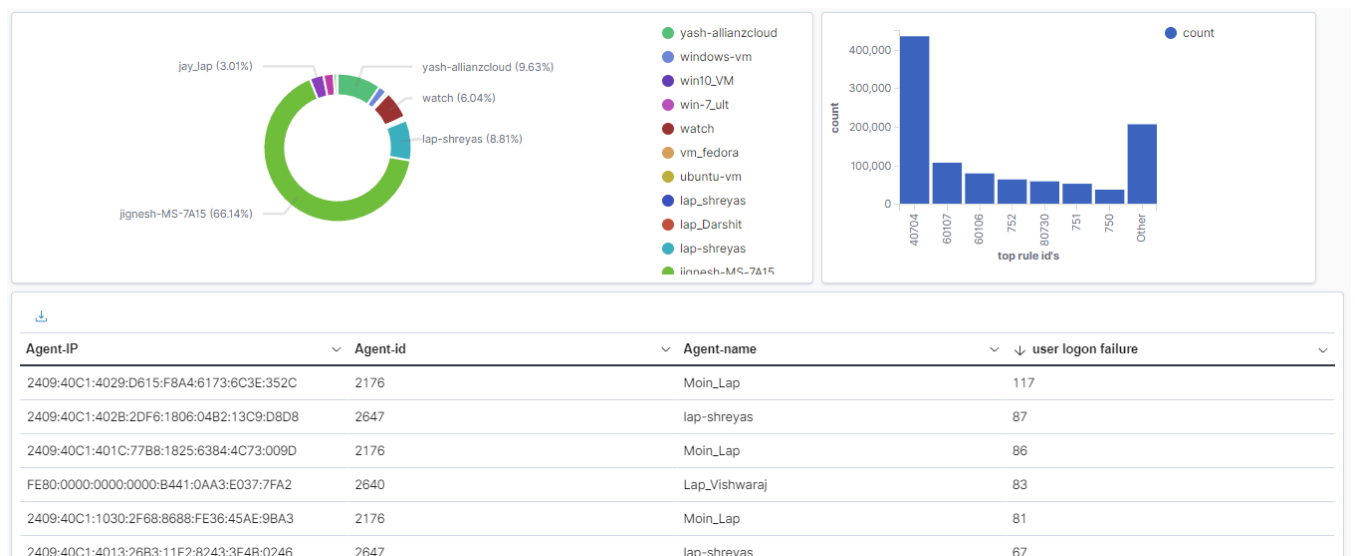
### 16.1 LIST OF TASK:

- ❖ Visualization in Wazuh for the top 5 rule-ID triggered events offers a concise overview of the most significant security incidents detected within the environment. This visualization typically presents a bar chart or table displaying the top 5 rule IDs that have triggered the highest number of events. Alongside each rule ID, relevant details such as the event count, agent IP, agent name, and agent ID are included. This visualization empowers security teams to quickly identify and prioritize the most critical security threats, enabling prompt investigation and response to mitigate potential risks effectively.

### 16.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:

- ❖ Wazuh

### 16.3 SCREENSHOTS:





## **CHAPTER - 17**

### **17.1 LIST OF TASK:**

- ❖ While simultaneously providing solutions or remediation for the cases generated in Iris, security analysts leverage their expertise to address identified security incidents effectively. By analyzing the nature of each case and its associated risks, analysts develop tailored remediation strategies to mitigate vulnerabilities and enhance the organization's security posture. This proactive approach ensures that security incidents are promptly addressed, minimizing potential impact and safeguarding the organization's assets and data against cyber threats. Additionally, monitoring security events in Wazuh allows analysts to detect and respond to ongoing threats, ensuring comprehensive protection across the organization's infrastructure.

### **17.2 TOOL/TECHNOLOGY/APPROACH TO PERFORM THE TASK:**

- ❖ Wazuh
- ❖ Shuffle
- ❖ Iris

## **CHAPTER - 18**

### **18.1 OVERALL ANALYSIS OF INTERNSHIP**

- ❖ During my internship in cybersecurity, I gained invaluable hands-on experience in diverse areas, including vulnerability assessments, penetration testing, web application security testing and . This opportunity allowed me to apply theoretical knowledge in real-world scenarios, enhancing my skills in identifying and mitigating security risks. The exposure to tools like Wazuh, Shuffle, IRIS and others enriched my understanding of security event monitoring and configuration assessment, preparing me for the role as a SOC analyst. Overall, this internship has been instrumental in shaping my cybersecurity expertise and providing a solid foundation for my future endeavors in the field.