SECURITY OPERATIONS CENTER AN APPROACH TO VARIOUS SIEM TOOLS

Presented By:
Sarjan Patel (20162171019)

Guided By:
Dr .Rohit Patel(ICT – Ganpat University)
Mr. Akshat Suthar(TechDefence)

Content

History of Organization

Departments

Internship Summary

Technology

Purpose

Objective

Scope

Security Operations Center

Seceon

Securonix

Wazuh

Roles and responsibilities

Group dependencies

History of TechDefenceLabs Solutions Pvt. Ltd.

- TechDefence Labs is an information security based innovation center developed by Techdefence Labs Solutions Private Limited. Starting from the small awareness programs on cyber security to conducting training sessions for the Corporates, Educational Institutions and Law Enforcement Agencies, TechDefence has encapsulated its growth in multiple fields of expertise. With multi-fold growth in training and consulting for information security solutions, TechDefence has now proudly marched into Information Security Solutions and Services.

Departments in organization

- SOC(Security Operations Center)
- VAPT(Vulnerability Assessment and Penetration Testing)
- Compliance
- Training
- HR(Human Resources)
- Executives

Organization chart

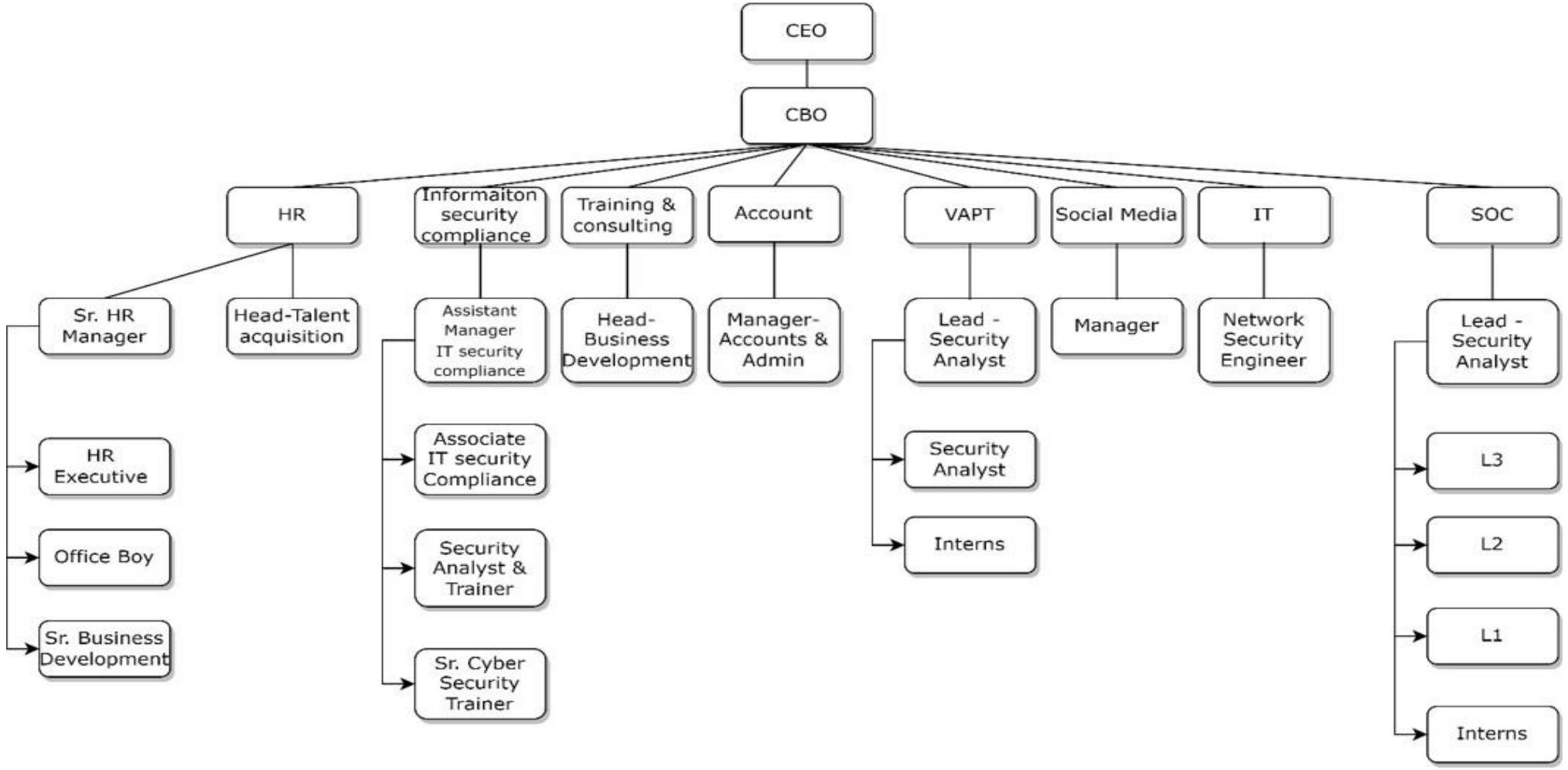


Fig 1.2-Organization Chart

Internship Summary

- Gained hands-on experience in security operations center (SOC) operations, working alongside seasoned analysts in a dynamic and fast-paced environment.
- Monitored security events from various sources, including network devices, logs, and endpoint security solutions, to identify potential threats and anomalies.
- Analyzed and investigated security incidents, following established procedures to assess their severity and potential impact.
- Escalated critical incidents to senior analysts and security experts for further investigation and response.
- Participated in training sessions and workshops, improving skills in SIEM tools, log analysis, and incident response.
- Developed strong communication and collaboration skills, working effectively with internal and external stakeholders.

Overall, this internship is providing invaluable experience in the field of security operations, solidifying my interest in pursuing a career in cyber security.

Technology

SIEM Tools

- Seceon
- Securonix
- Splunk
- Wazuh

TPD Tools

- IBM Xforce
- Virustotal
- AbuseIPDB
- Cyble
- Cisco Talos

EDR Tool

- CrowdStrike

Purpose

- Skill Development:
  - Gain hands-on experience in cybersecurity.
  - Develop proficiency in using SOC tools and technologies.
  - Enhance technical skills in threat detection, incident response, and vulnerability management.
- Industry Exposure:
  - Understand day-to-day operations of a SOC.
  - Familiarize with industry best practices and compliance requirements.
- Professional Networking:
  - Build relationships with SOC analysts and cybersecurity professionals.
  - Engage with the broader cybersecurity community through events and conferences.
- Practical Application of Knowledge:
  - Apply theoretical knowledge to real-world scenarios.
  - Analyze and respond to security incidents effectively.

- Contribution to Security Operations:
  - Actively monitor and analyze security alerts.
  - Escalating the analysis to the clients IT Department.
  - Contribute to improving security policies and procedures.
- Career Exploration:
  - Explore specific interests within the cybersecurity field.
  - Understand potential career paths, such as SOC analyst, incident responder, or security consultant.

Objective

- Gain hands-on experience:
  - Learn the ropes of security operations from experienced professionals in a real-world SOC environment..
- Build your skillset:
  - Master industry-standard SOC tools and technologies, and develop your analytical, problem- solving, communication, and collaboration skills.
- Get your foot in the door of the cybersecurity industry:
  - Gain valuable experience and connections to increase your chances of landing a full-time job after graduation.

Scope

- Monitoring and Analysis:
  - Continuous security event monitoring from various sources.
  - Analyzing logs to identify anomalies and indicators of compromise.
  - Researching and gathering threat intelligence from diverse sources.
- Incident Response:
  - Identifying and escalating potential security incidents.
  - Collecting and analyzing data during security incidents.
  - Assisting in mitigation, eradication, and recovery efforts.
- Other Responsibilities:
  - Reporting and documentation of findings and security incidents.
  - Participation in training sessions and workshops for skill development.
  - Collaboration with SOC team, security experts, and IT personnel.

Security Operations Center

- During our internship till now, we gained valuable experience by exploring various SIEM tools used by the organization.

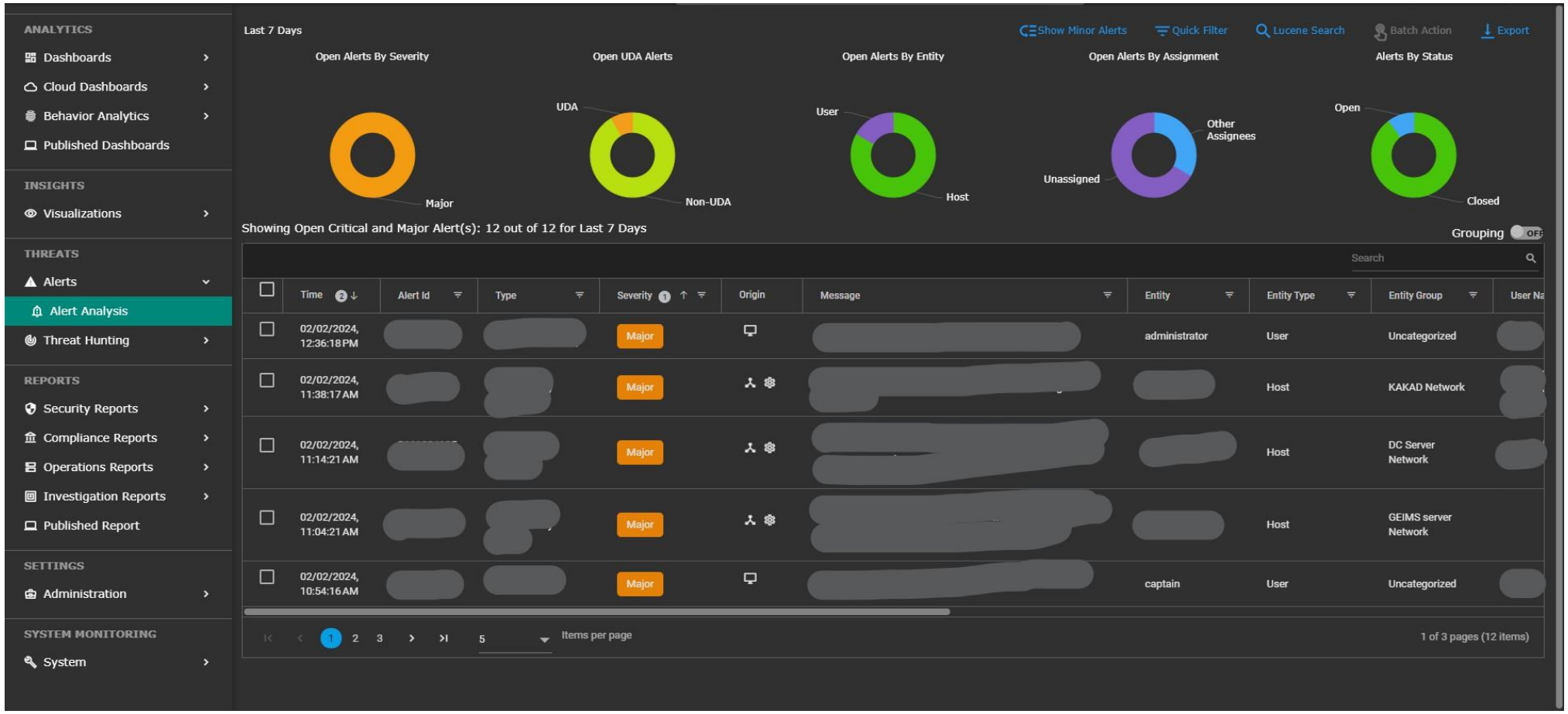
- These tools include Seceon, Securonix, Splunk and Wazuh , each offering unique features and capabilities.

- Below are the Interface’s of the each SEIM tool on which we have worked upon:

SIEM Tool : Seceon

- Seceon is an ai-SIEM, combined with ai-XDR, is a comprehensive cybersecurity management platform that visualizes, detects ransomware detection, and eliminates threats in real-time, with continuous security posture improvement, compliance monitoring and reporting, and policy management.
- Below are the Interface’s of the each SEIM tool on which we have worked upon:

SIEM Tool : Seceon



Seceon SIEM is an AI-powered cybersecurity management platform that detects and neutralizes threats across your IT environment, offering comprehensive visibility and automated responsecapabilities.

Case Flow of Seceon

Step 1: An alert triggers on the SIEM tool.

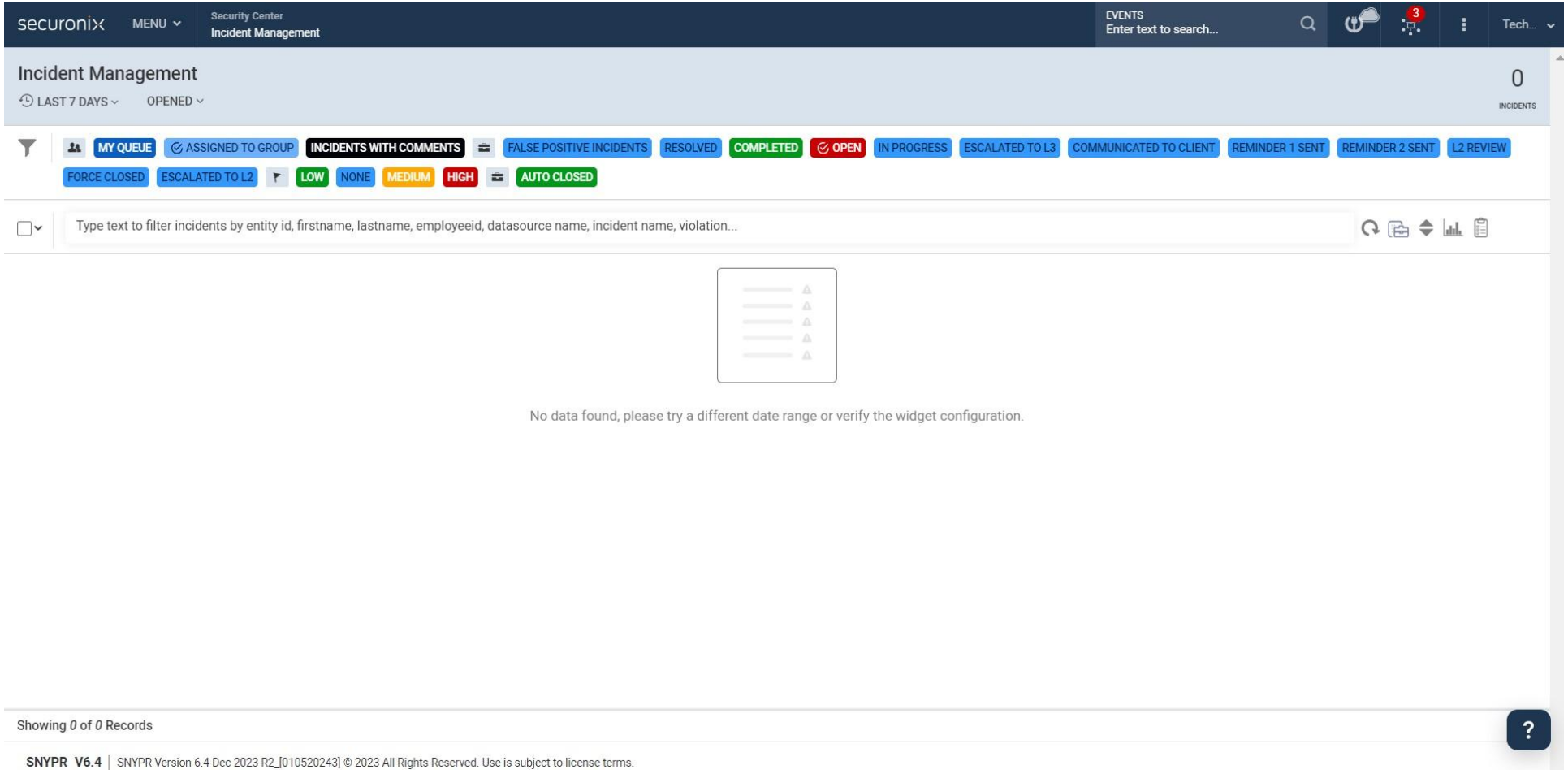
Step 2: Then we have to assigned the case to ourself.

Step 3: Each alert have the unique id, note that and respond to that ticket to the client.
Step 4: Case analysis is done and information is collected.

Step 5: Analysis report is sent to the client through mail.

Step 6: Further actions are taken based on the client response.

SIEM Tool : Securonix



Case flow of Securonix

Step 1: Violation or Threat is triggered.

Step 2: Case is created on that threat or violation.

Step 3: Case is analyzed by the analyst.

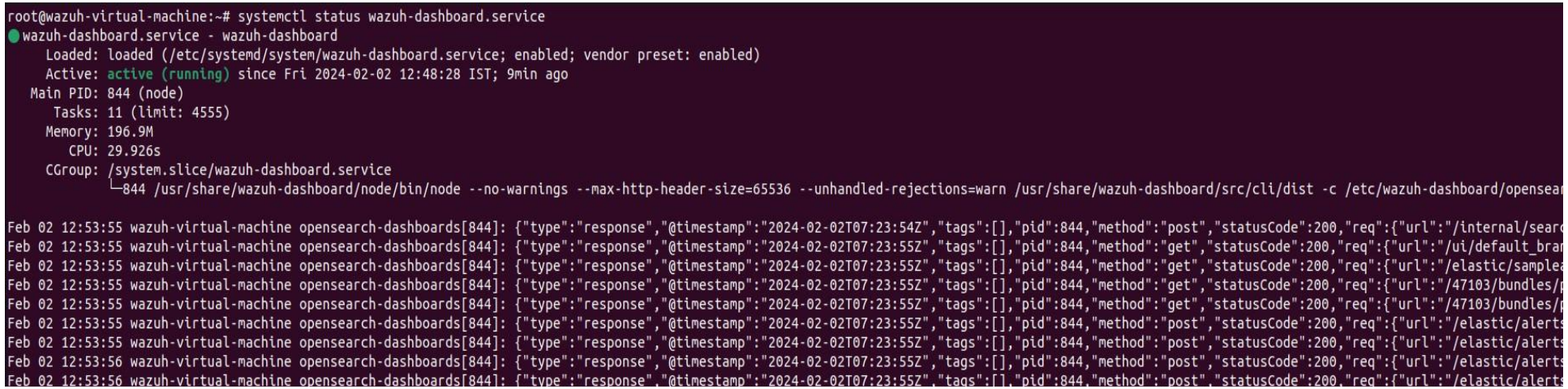
Step 4: If case is false positive then analyst close the case as false positive with the comment of analysis and the recommendation.

Step 5: If case if true positive then it is escalated to the client.

Step 6: State of the case is change to false positive or communicated to client, then it goes to the L2 bucket and further actions are taken by the L2.

SIEM Tool : Wazuh

- During the journey of the SIEM analysis, We also learnt about the SIEM deployment in the environment .
- Below are the some glimpses of the Wazuh deployment on our a system.
- We have installed Wazuh all in one where the indexer, manager and dashboard work on the same system.
- There is no dedicated system for each of them.
- **Wazuh Dashboard :**



- **Wazuh manager:**

```
root@wazuh-virtual-machine:~# systemctl status wazuh-manager.service
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2024-02-02 12:49:07 IST; 9min ago
    Process: 1037 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 122 (limit: 4555)
     Memory: 479.8M
        CPU: 2min 1.618s
     CGroup: /system.slice/wazuh-manager.service
             ├─1808 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─1809 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─1812 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─1815 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─1856 /var/ossec/bin/wazuh-authd
             ├─1869 /var/ossec/bin/wazuh-db
             ├─1890 /var/ossec/bin/wazuh-execd
             ├─1902 /var/ossec/bin/wazuh-analysisd
             ├─1914 /var/ossec/bin/wazuh-syscheckd
             ├─1930 /var/ossec/bin/wazuh-remoted
             ├─1931 /var/ossec/bin/wazuh-remoted
             ├─1963 /var/ossec/bin/wazuh-logcollector
             ├─1981 /var/ossec/bin/wazuh-monitord
             └─2022 /var/ossec/bin/wazuh-modulesd

Feb 02 12:49:00 wazuh-virtual-machine env[1037]: Started wazuh-db...
Feb 02 12:49:00 wazuh-virtual-machine env[1037]: Started wazuh-execd...
Feb 02 12:49:01 wazuh-virtual-machine env[1037]: Started wazuh-analysisd...
Feb 02 12:49:03 wazuh-virtual-machine env[1037]: Started wazuh-syscheckd...
Feb 02 12:49:04 wazuh-virtual-machine env[1037]: Started wazuh-remoted...
Feb 02 12:49:04 wazuh-virtual-machine env[1037]: Started wazuh-logcollector...
Feb 02 12:49:05 wazuh-virtual-machine env[1037]: Started wazuh-monitord...
Feb 02 12:49:05 wazuh-virtual-machine env[1037]: Started wazuh-modulesd...
Feb 02 12:49:07 wazuh-virtual-machine env[1037]: Completed.
Feb 02 12:49:07 wazuh-virtual-machine systemd[1]: Started Wazuh manager.
```

- **Wazuh indexer :**

```
root@wazuh-virtual-machine:~# systemctl status wazuh-indexer
● wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2024-02-02 12:50:22 IST; 9min ago
       Docs: https://documentation.wazuh.com
   Main PID: 1035 (java)
      Tasks: 80 (limit: 4555)
     Memory: 1.2G
        CPU: 2min 8.348s
     CGroup: /system.slice/wazuh-indexer.service
             └─1035 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.hea>
```

- **Wazuh – syslog forwarder:**

In this segment we learnt about the agentless onboarding of the device. Where we have used a Pfsence firewall as an endpoint and taken it log’s in to the wazuh.

Roles and responsibilities

INTERN – incident analysis , documentation and reporting , learning and development

SOC L1 – Monitoring, triage and initial analysis, incident response support

SOC L2 – in-depth analysis, incident mitigation, knowledge base development

SOC L3 – advanced analysis, tool and technology expertise, mentorship and training

SIEM ENGINEER – SIEM infrastructure management, rule and correlation configuration, integration with security tools

SIEM Manager – strategic planning, policy and compliance, incident response coordination, team leadership

Group Dependencies

Group 1: SOC Analysts (L1, L2, L3) and SOC Intern – information sharing, incident triage.

Group 2: SOC Analysts (L2, L3) and SIEM Engineer – advanced analysis, tool optimization.

Group 3: SOC Analysts (L1, L2, L3) and SIEM Manager – strategic planning, incident response coordination.

Group 4: SOC Intern and Entire SOC Team – mentorship and learning

Group 5: SIEM Engineer and SIEM Manager – strategic planning and implementation , policy and compliance.

THANK YOU !!