Industry Project Report

On

Security Operations Center: An approach to various SIEM Tools

Developed By: -
Sarjan Patel (20162171019)

Guided By: -
Dr. Rohit Patel (Internal)
Mr. Akshat Suthar (External)

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

Year: 2024

CERTIFICATE

This is to certify that the **IBM/ Industry** Project work entitled **“Security Operations Center: An approach to various SIEM Tools”** by Sarjan Patel(Enrolment No. 20162171019) 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) Department at TechDefenceLabs Solutions Pvt. Ltd.. The results/findings contained in this Internship 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:

Acknowledgements

I am sincerely grateful to TechDefence Labs and Mr. Akshat Suthar for the enriching opportunity to working with their esteemed organization. Akshat sir's mentorship and guidance are invaluable, shaping my understanding of complex Cyber Security concepts and their real-world applications. His commitment to fostering a conducive learning environment greatly contributed to my professional growth. I extend my thanks to the entire TechDefence Labs team for their warm welcome and collaborative spirit. The exposure and hands-on experience gained during this internship have significantly enhanced my skills in the dynamic field of SOC. I am grateful for the encouragement, feedback, and growth opportunities provided by the TechDefence Labs team. This internship has deepened my technical knowledge and allowed me to apply theoretical concepts to practical scenarios. Thank you, TechDefence Labs, for providing a platform where I could contribute to meaningful projects, engage with cutting-edge technologies, and learn from industry experts. This experience has been pivotal in shaping my career aspirations and has laid a strong foundation for my future endeavors in Cyber Security. Sincerely,

Sarjan Patel(20162171019)
10/05/2024
ICT-Ganpat University

Abstract

This report delves into the immersive experience of an internship at TechDefence Labs Solutions Pvt. Ltd., offering a comprehensive overview of the cybersecurity landscape within a dynamic Security Operations Center (SOC) environment. The internship, under the guidance of seasoned professionals like Mr. Akshat Suthar, mentor at TechDefence Labs and Dr. Rohit Patel Principal, ICT and internal guide at Ganpat University, provided an enriching platform for practical learning and skill development. The abstract highlights the significant aspects covered in the report, encapsulating the essence of the internship journey. It sheds light on the core objectives, including skill enhancement, industry exposure, professional networking, and practical application of knowledge in cybersecurity operations. The scope of the internship encompasses diverse responsibilities such as monitoring, analysis, incident response, and collaboration with SOC teams. Key technologies and literature review elements underscore the importance of cutting-edge tools like Seceon, Securonix, Splunk, and Wazuh, alongside insights from cybersecurity literature. The abstract encapsulates the essence of the internship's contribution to skill development, industry insights, and preparation for a successful career in cybersecurity. Overall, the abstract provides a succinct overview of the internship's significance, setting the stage for a detailed exploration of the internship experience and its impact on professional growth and career aspirations in cybersecurity.

List of Figures

List of Tables

Table of Contents

CHAPTER 1 - OVERVIEW OF THE COMPANY

1.1 HISTORY

Founder: Sunny Waghela

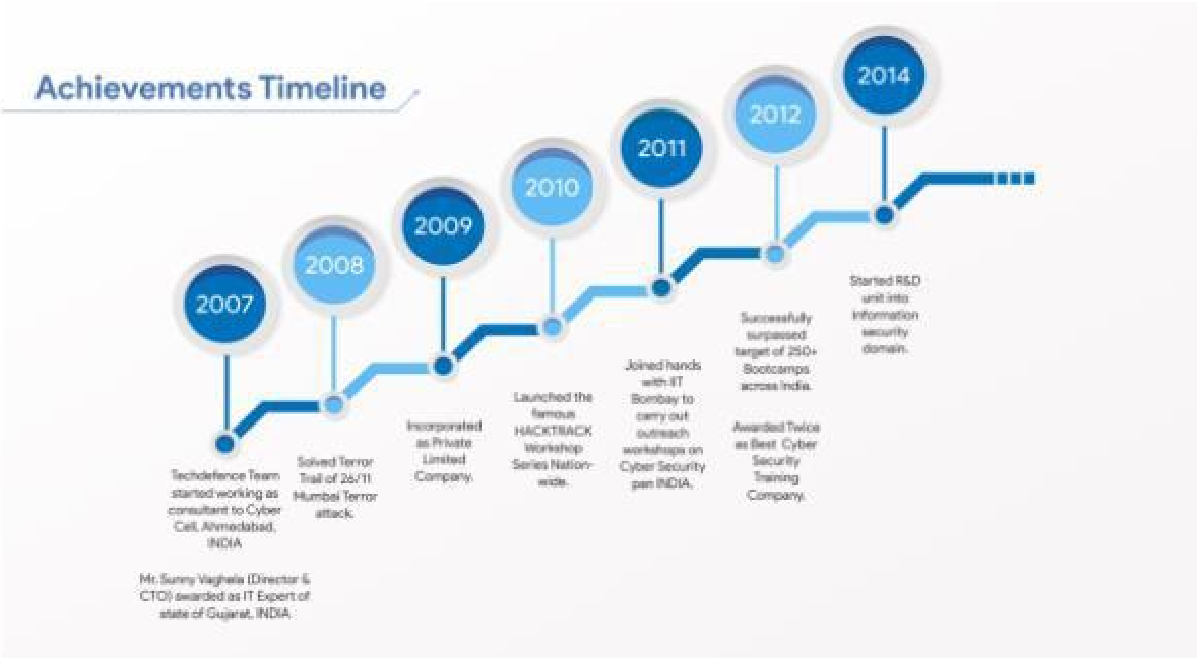
Founding Year: 2009

TechDefence Labs, launched in 2009 by Advanced TechDefence Pvt. Ltd., is a hub for information security expertise based in Ahmedabad, India. Starting with cyber security awareness programs, TechDefence has expanded its services to include training for corporations, educational institutions, and law enforcement agencies.

The company's growth led it to offer information security solutions and services. Recognizing the value of proactive security, TechDefence emphasizes manual security testing alongside its proprietary platforms. This multi-layered approach, combining manual expertise with automated tools, aims to deliver highly secure solutions with expert auditing.

Driven by a culture of creativity and passion, Tec Defence’s R&D team thrives on the philosophy of "seeing flaws where others see solutions." This innovative approach has resulted in groundbreaking solutions for satisfied clients like Cyberoam, Sulekha.com, Dealcloud, Logmeonce, HPCL, and Indian Oil.

TechDefence aspires to become the undisputed leader in cybersecurity, providing cutting-edge solutions and top-notch products that guarantee seamless business operations for clients. They achieve this through relentless innovation, delivering exceptional service and support, and fostering a culture of passion within the cybersecurity landscape, ultimately leading to a secure and protected digital space for all.



Achievements Timeline

2007

Techdefence Team started working as consultant to Cyber Cell, Ahmedabad, INDIA

Mr. Sunny Vaghela (Director & CTO) awarded as IT Expert of state of Gujarat, INDIA.

2008

Solved Terror Trail of 26/11 Mumbai Terror attack.

2009

Incorporated as Private Limited Company.

2010

Launched the famous HACKTRACK Workshop Series Nation-wide.

2011

Joined hands with IIT Bombay to carry out outreach workshops on Cyber Security pan INDIA.

2012

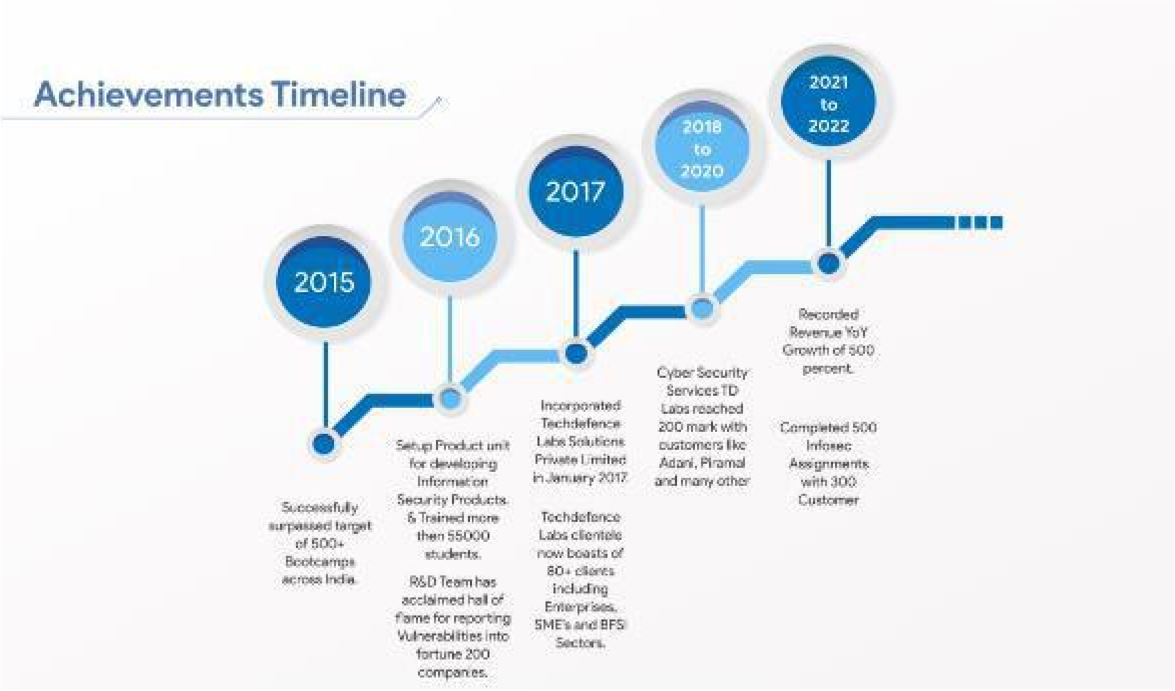
Successfully surpassed target of 250+ Bootcamps across India.

Awarded Twice as Best Cyber Security Training Company.

2014

Started R&D unit into information security domain.

Fig 1.1 Achievements Timeline 2007-2014



Achievements Timeline

2015

Successfully surpassed target of 500+ Bootcamps across India.

2016

Setup Product unit for developing Information Security Products. & Trained more then 55000 students.

R&D Team has acclaimed hall of fame for reporting Vulnerabilities into fortune 200 companies.

2017

Incorporated Techdefence Labs Solutions Private Limited in January 2017

Techdefence Labs clientele now boasts of 80+ clients including Enterprises, SME's and BFSI Sectors.

2018 to 2020

Cyber Security Services TD Labs reached 200 mark with customers like Adani, Piramal and many other

2021 to 2022

Recorded Revenue YoY Growth of 500 percent.

Completed 500 Infosec Assignments with 300 Customer

Fig 1.2 Achievements Timeline 2015-2022

1.2 DIFFERENT PRODUCT

Table 1.1 Security Assessment Services

Vulnerability Assessment and Penetration Testing	Red Team Assessments
Web Application Penetration Testing	Mobile App Penetration Testing
Network Security Penetration Testing	Wireless Network Assessment
Code Review	Configuration Review

Table 1.2 Security Consulting Services

ISO 27001:2013 Compliance	RBI Cyber Security Compliance
ISNP Compliance	Cyber Risk, Gap & Maturity Assessment
GDPR Implementation and Readiness	NABARD Cyber Security Framework
Cyber Insurance Consulting	SEBI Cyber Security Framework
SOC Compliance	PCI DSS Compliance

Table 1.3 Specialized Services

Social Engineering Services	Red Teaming Services
Incident Response and Malware Analysis	Managed Security Services
Cyber Crime Investigation	Forensics as a Service

Table 1.4 Digital Forensics Services

Disk Imaging and Analysis	Computer Mobile Device Forensics
eDiscovery	Ransomware Forensics
Data Breach Response	Compromise Assessment

Table 1.5 Training Services

Training & Workshops	Information Security Certifications
UG & PG Courses with Universities	-

1.3 ORGANIZATION CHART

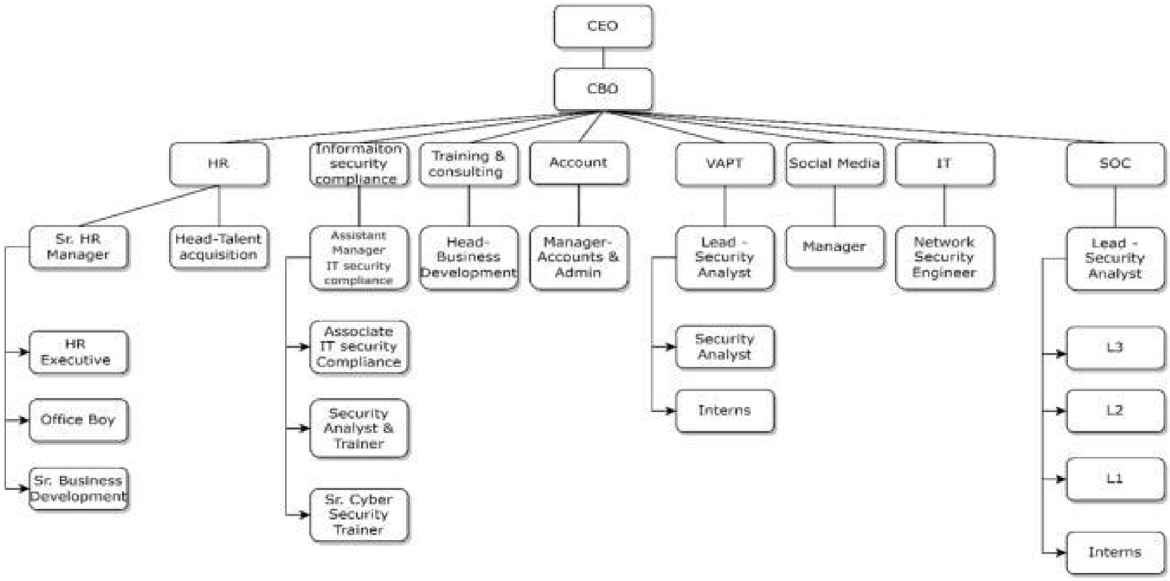


Fig 1.3 Organization chart

The organizational chart includes information about the different departments and positions of the Company. It contains information about every department such as HR, the Information Security Compliance Team, the Training Team, VAPT as well as SOC Team. The SOC Department, Where I work includes the following structure.

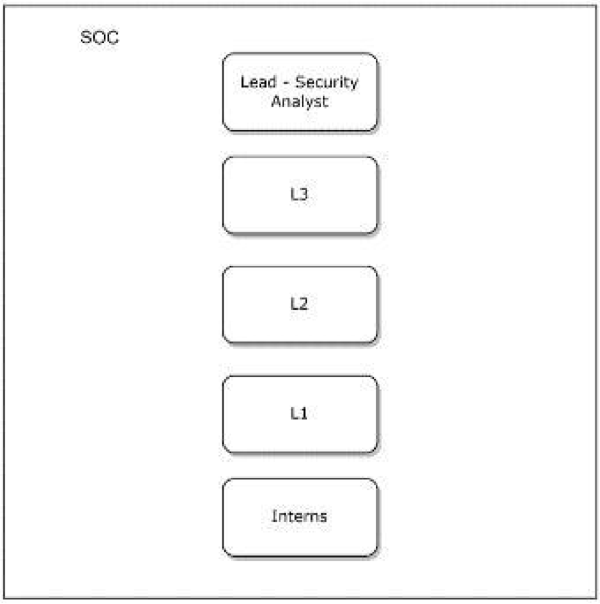


Fig 1.4 SOC Department Chart

CHAPTER 2 - OVERVIEW OF DIFFERENT DEPARTMENTS

2.1 THE DETAILS ABOUT THE WORK BEING CARRIED OUT IN EACH DEPARTMENT.

To go through the workflow, we have a total 6 departments

1. **SOC (Security Operations Centre):**

   - Purpose: To monitor and respond to security incidents in real time.
   - Goals: Ensure the organization's information systems and data are secure from cyber threats.

2. **VAPT (Vulnerability Assessment and Penetration Testing)**

   - Purpose: To identify and address vulnerabilities in the organization's systems.
   - Goals: Conduct regular testing to find and fix potential weaknesses before they can be exploited.

3. **Compliances:**

   - Purpose: To ensure the organization adheres to relevant industry regulations and standards.
   - Goals: Maintain compliance with legal and regulatory requirements to avoid penalties.

4. **Training:**

   - Purpose: To enhance the skills and knowledge of employees in various areas.
   - Goals: Improve the overall competence of the workforce, aligning with organizational needs

5. **HR (Human Resource):**

   - Purpose: To manage personnel-related aspects, including recruitment, and performance.
   - Goals: Attract, develop, and retain a qualified and positive workplace culture.

6. **Executive:**
    - Purpose: To provide strategic direction and decision-making for the organization.
    - Goals: Ensure the overall success and growth of the organization by making effective decisions.

2.2 TECHNICAL SPECIFICATIONS OF MAJOR EQUIPMENT

SOC (Security Operations Center):

- Seceon
- Securonix
- Wazuh
- Splunk
- Crowdstrike

VAPT (Vulnerability Assessment and Penetration Testing)

- Metasploit
- Burp Suite
- Nmap
- Wireshark

COMPLIANCES:

- Excel, Word, PPT (Microsoft Office Suite)
- NSE (National Stock Exchange) portal
- BSE (Bombay Stock Exchange) portal
- MXtoolbox

Training:

- Google Classroom
- Learning Management System (LMS)

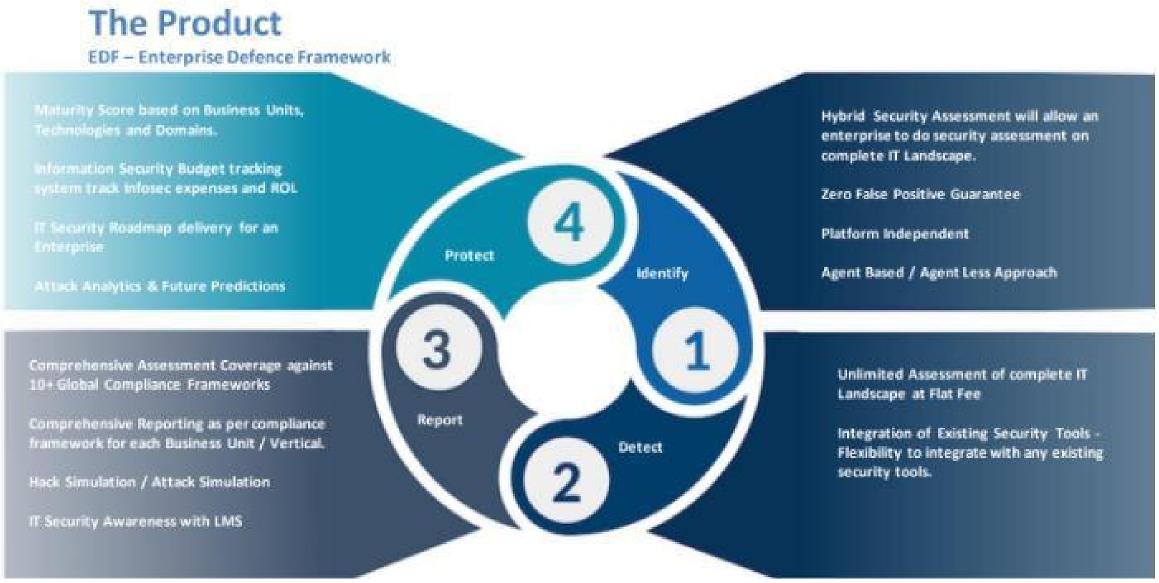
HR:

- KEKA

Executive:

- Microsoft Teams
- O-365 (Office 365)

2.3 SEQUENCE OF OPERATION FOR MANUFACTURING OF END PRODUCT



The Product

EDF – Enterprise Defence Framework

Maturity Score based on Business Units, Technologies and Domains.

Information Security Budget tracking system track Infosec expenses and ROI.

IT Security Roadmap delivery for an Enterprise

Attack Analytics & Future Predictions

Hybrid Security Assessment will allow an enterprise to do security assessment on complete IT Landscape.

Zero False Positive Guarantee

Platform Independent

Agent Based / Agent Less Approach

Comprehensive Assessment Coverage against 10+ Global Compliance Frameworks

Comprehensive Reporting as per compliance framework for each Business Unit / Vertical.

Hack Simulation / Attack Simulation

IT Security Awareness with LMS

Unlimited Assessment of complete IT Landscape at Flat Fee

Integration of Existing Security Tools - Flexibility to integrate with any existing security tools.

Fig 2.1 EDF

The company is service-based; hence no end product is generated. Instead, the company provides various services in domains like Security Operations Centre, Vulnerability Assessment and Penetration Testing, Compliance, and Training.

CHAPTER 3 - INTERNSHIP MANAGEMENT

3.1 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.
- Analysed 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.

3.2 PURPOSE

Skill Development:

- Gain hands-on experience in cybersecurity
- Develop proficiency is using SOC tools and technologies
- Enhance technical skills in threat detection, incident response and vulnerability management

Industry Exposure:

- Understand the 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.
- Analysed and responded to security incidents effectively.

Contribution to Security Operations:

- Actively monitor and analyse security alerts.
- 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.

Overall Objective:

- Provide a structured environment for interns to develop practical skills.
- Gain exposure to the cybersecurity industry.
- Contribute to the organization’s security objectives at TechDefenceLabs Solutions Pvt. Ltd.

3.3 OBJECTIVE

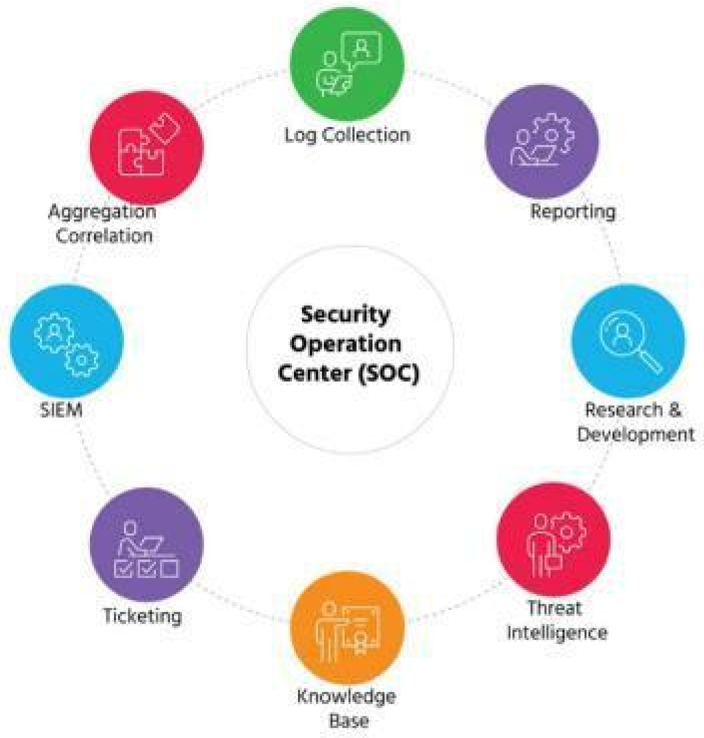


Fig 3.1 SOC

- 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.
- Explore your career interests: See if cybersecurity is the right field for you by getting firsthand experience of the daily tasks and challenges.

TechDefence Labs' Objectives:

- Train future talent: Invest in the future of the cybersecurity workforce by equipping interns with the necessary skills and knowledge.
- Get fresh perspectives: Gain new ideas and approaches from interns to improve products, services, and overall operations.
- Boost company morale: Create a more energetic and positive work environment with the infusion of young talent.

3.4 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.

Influencing Factors:

- SOC Size and Complexity:
- Larger SOCs may have more specialized roles.

SOC Team's Needs:

- Current projects, focus areas, and resource constraints can shape tasks.

Intern's Skills and Experience:

- Prior knowledge and experience in cybersecurity determine task assignments.

Overall Learning Experience:

- Valuable exposure to hands-on experience in a dynamic and fast-paced SOC environment.
- Skills development in security operations, incident response, and threat intelligence.
- Preparation for a successful career in cybersecurity

3.5 TECHNOLOGY AND LITERATURE REVIEW

Technology: SIEM TOOLS – Seceon, Securonix, Splunk, Wazuh

Literature review:

Working as a SOC Analyst intern at TechDefence Labs Solutions Pvt. Ltd. presents a unique opportunity to gain valuable hands-on experience, develop essential skills, and explore career possibilities in cybersecurity. While challenges exist, the potential benefits outweigh the risks, making this internship a valuable stepping stone for aspiring cybersecurity professionals. By carefully considering the benefits and challenges, leveraging relevant resources, and approaching the internship with dedication and a willingness to learn, you can maximize your experience and set yourself up for success in the cybersecurity field.

3.6 INTERNSHIP PLANNING

3.6.1 Internship Development Approach and Justification

Developing an effective internship program for a SOC (Security Operations Center) Analyst Intern involves careful planning to ensure that the intern gains valuable experiences and contributes meaningfully to the team. Here's an internship development approach and justification for a SOC Analyst Intern:

Internship Development Approach:

1. Structured Onboarding:

- Provide a comprehensive onboarding process to familiarize the intern with the organization's cybersecurity policies, tools, and procedures.
- Conduct orientation sessions to introduce the intern to the SOC team, organizational structure, and key stakeholders.

2. Learning Objectives:

- Define clear and achievable learning objectives for the intern, aligned with the overall goals of the SOC team.
- Outline specific skills and knowledge areas the intern is expected to develop during the internship.

3. Progressive Training:

- Implement a progressive training plan that starts with foundational concepts and gradually moves towards more advanced topics
- Utilize in-house training materials, online courses, and hands-on exercises to enhance the intern's skill set.

4. Mentorship Program:

- Assign a mentor from the SOC team to guide the intern throughout the internship.
- Facilitate regular one-on-one sessions for feedback, guidance, and discussions about the intern's progress.

5. Rotation Through SOC Levels:

- Structure the internship to include exposure to various SOC levels (L1, L2, and L3) to provide a holistic understanding of the SOC operations.
- Allow the intern to shadow and work alongside experienced analysts at different levels.

6. Real-world Simulation Exercises:

- Develop and conduct real-world simulation exercises to allow the intern to practice incident response and threat detection in a controlled environment.
- Provide feedback and debriefing sessions after each simulation to reinforce learning.

7. Project-Based Assignments:

- Assign the intern project-based tasks that contribute to the overall security posture of the organization.
- Examples include analysing historical incident data, contributing to the development of new detection rules, or researching emerging threats.

8. Continuous Feedback and Evaluation:

- Establish a feedback loop with regular performance evaluations to track the intern's progress.
- Provide constructive feedback and identify areas for improvement to guide the intern's development.

Justification for SOC Analyst Internship:

Skill Development:

- The internship provides an opportunity for the intern to develop practical skills in threat detection, incident response, and vulnerability management under the guidance of experienced professionals.

Knowledge Application:

- The intern can apply theoretical knowledge gained in academic settings to real-world scenarios, bridging the gap between classroom learning and practical application.

Talent Pipeline:

- The internship serves as a potential talent pipeline for the organization, allowing the SOC team to identify and nurture promising individuals who may later join as full-time SOC analysts.

Diversity and Inclusion:

- Internship programs contribute to diversity and inclusion initiatives by providing opportunities for individuals from different backgrounds to enter the cybersecurity field.

Knowledge Transfer:

- The internship facilitates knowledge transfer from experienced SOC analysts to the intern, ensuring the continuity of institutional knowledge within the organization.

Contribution to SOC Operations:

- The intern's contributions, even during the internship, can have a positive impact on the overall effectiveness of the SOC by assisting in incident response, analysis, and other operational tasks.

Professional Development:

- The internship offers a platform for the intern to build a professional network, collaborate with industry professionals, and attend relevant training sessions or conferences.

Organizational Reputation:

- Running a successful internship program enhances the organization’s reputation as a supporter of cybersecurity education and talent development.

By following this internship development approach, organizations can create a mutually beneficial experience for SOC Analyst Interns, fostering their growth while also strengthening the capabilities of the SOC team.

3.6.2 Internship Effort and Time

Topic	Level	Months
Network Security Fundamentals	Basic	0.5
Security Information and Event Management (SIEM)	Basic	1-2
Log Analysis	Basic	1-2
Threat Detection and Response	Intermediate	2-3
Incident Response	Intermediate	1-2
Security Automation	Intermediate	2-4
Vulnerability Management	Intermediate	3-4
Threat Hunting	Advance	3-4

Table 3.1: Internship Flow

3.6.3 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

3.6.4 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.

3.7 INTERNSHIP SCHEDULING (GANTT CHART)

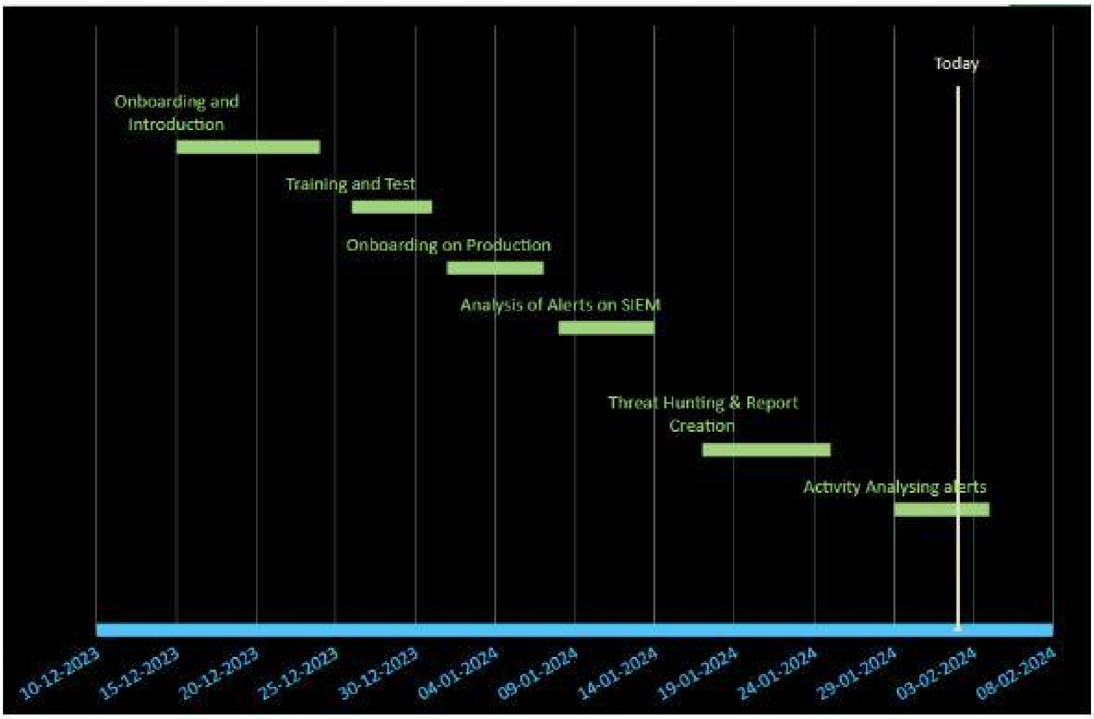


Fig 3.2: Gantt Chart for Internship Scheduling

The shown chart includes the timeline since the process of boarding started and training for the SOC Analyst began. Till now I have worked on some SIEM tools analysed logs and escalated alerts. While being involved in the process of Threat hunting, I also get the chance to create reports.

CHAPTER 4 - SYSTEM ANALYSIS

4.1 STUDY OF SECEON

Seceon’s powerful cybersecurity solution, aiSIEM combined with aiXDR, goes beyond standard threat detection. Imagine a central command centre where you can visualize your entire security landscape in real time.

This platform proactively detects and eliminates even sophisticated threats like ransomware, instantly neutralizing them to keep your business safe. But that’s not all. aiSIEM constantly analyzes your security posture, identifying vulnerabilities and suggesting improvements, ensuring you’re always ahead of the curve.Additionally, it ensures compliance with regulations through comprehensive monitoring and reporting, taking the burden off your shoulders.

Now, let’s explore the client dashboard, your personalized hub for managing all your clients (tenants). Each client has a dedicated space, ensuring complete data isolation and security. To streamline your workflow, the dashboard is divided into six key sections, each focusing on a specific security activity

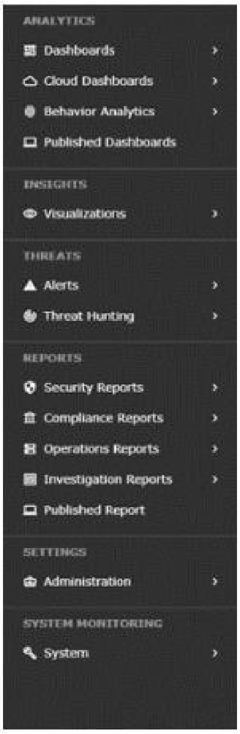
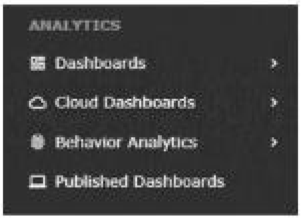


Fig: 4.1 Seceon Menu

Let’s understand each of the above-given sections:

- Analytics

  As the name suggests here, all the data will be presented for the purpose which is divided into four parts



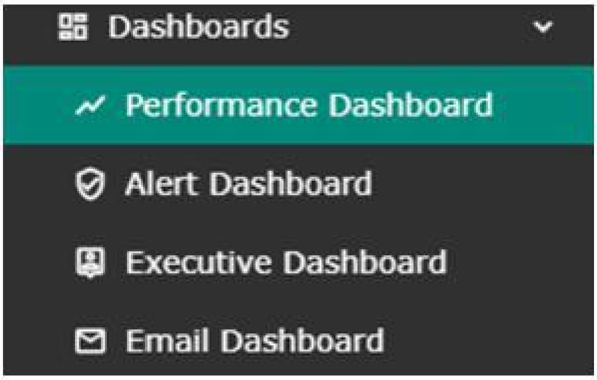
ANALYTICS

- Dashboards ›
- Cloud Dashboards ›
- Behavior Analytics ›
- Published Dashboards

Fig 4.2 Analytics Section

- Dashboard

  In the dashboard section, there are 3 types of dashboards



Dashboards

- Performance Dashboard
- Alert Dashboard
- Executive Dashboard
- Email Dashboard

Fig 4.3 Dashboards

- Performance Dashboard

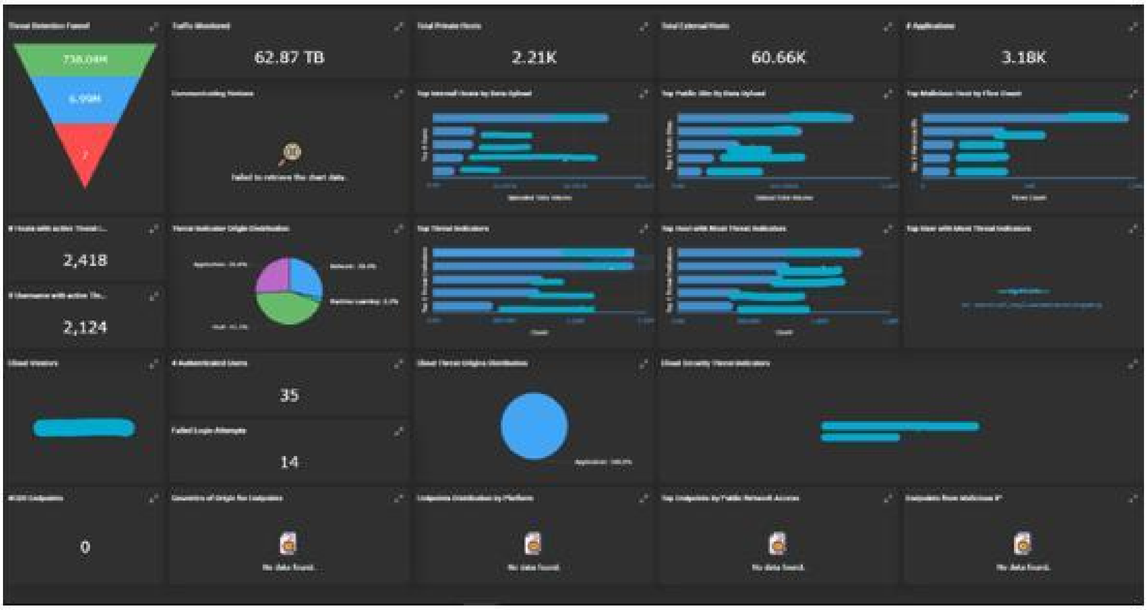


Fig 4.4 Performance Dashboard

In the performance dashboard, the data regarding the all overperformance of the organization in all the fields are taken into consideration as a security perspective such as:

- Top Threat Indicators
- Top Host with the Most Threat Indicators
- Top Public Site by Data Upload
- Top Internal Hosy by Data Upload

And many more fields are there which are seen in the performance.

- Alert Dashboard

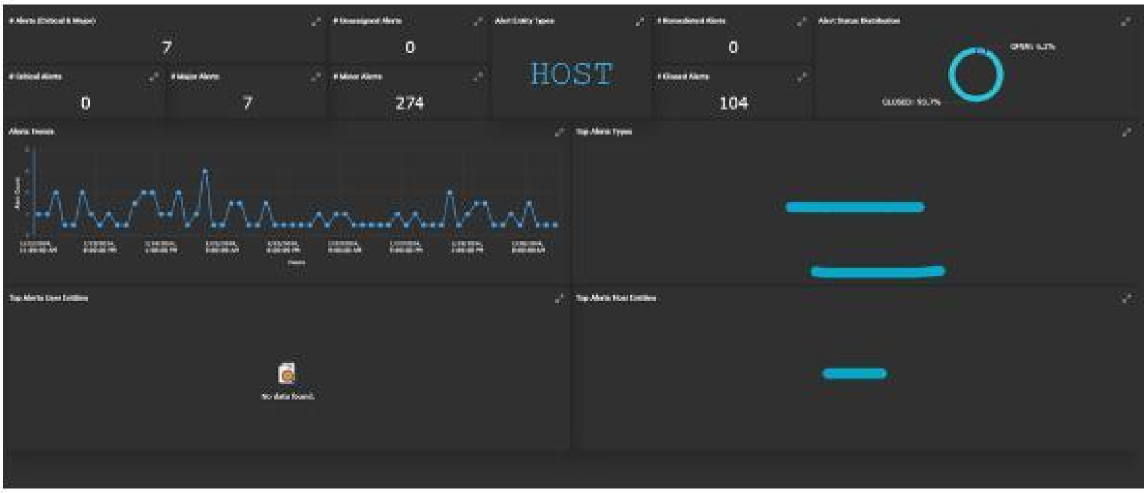


Fig 4.5 Alert Dashboard

Alert dashboard helps to show the major alerts that were triggered in large numbers with the alert count based on the time frame, It shows the data such as:

- Alerts Trends
- Top Alerts Types
- Top Alerts Host Entities
- Alert Entity Types

More in-depth detail is provided using the graphical representation

- Executive Dashboard

  This dashboard helps to get the current ongoing situation of the organization, including the EPS count also with most recent alert, and the device from which we are getting the high log flow

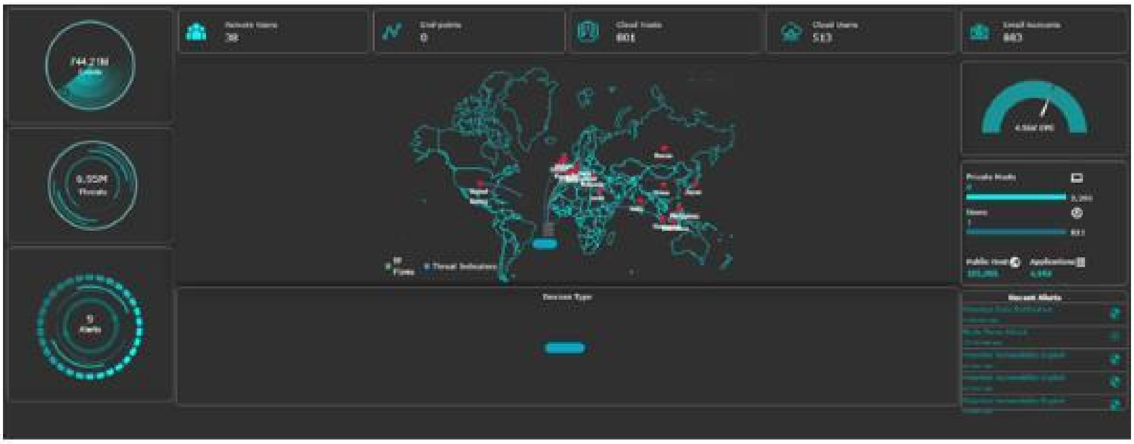


Fig 4.6 Executive Dashboard

- Email Dashboard

  As the name suggest, this dashboard will give the in-detail information about the all over email activity inside the organization domain. Which give the information like the Top Ten Email Sender By Domain, Top Ten Email Sender, Top Ten Communicator, Top Ten Email Receiver.

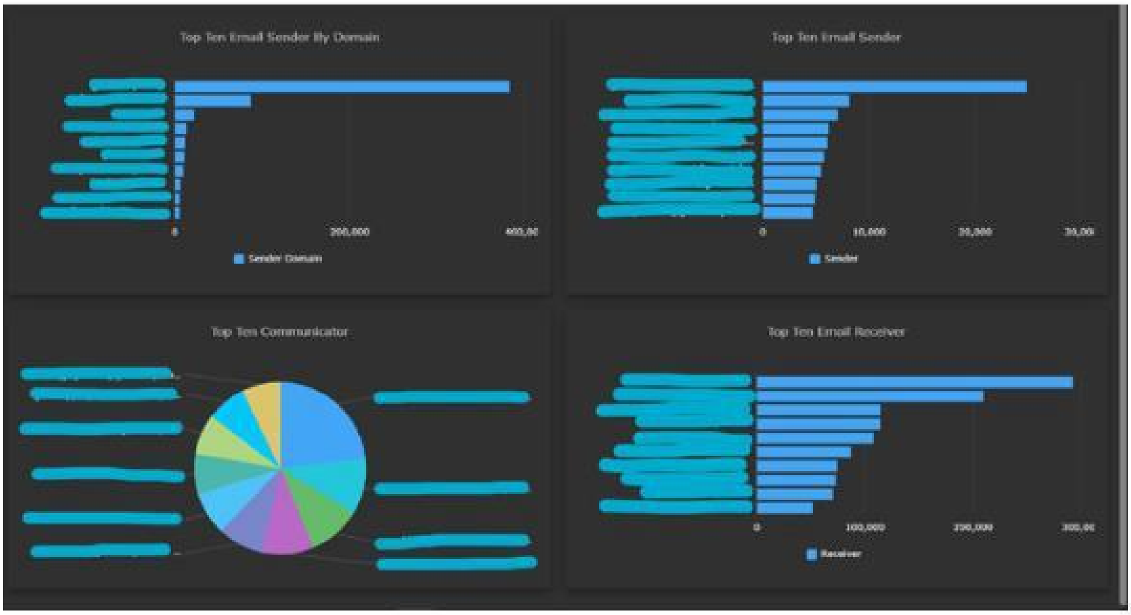


Fig 4.7 Email Dashboard

- Cloud Dashboard

Fig 4.8 Cloud Dashboard

- Microsoft Azure

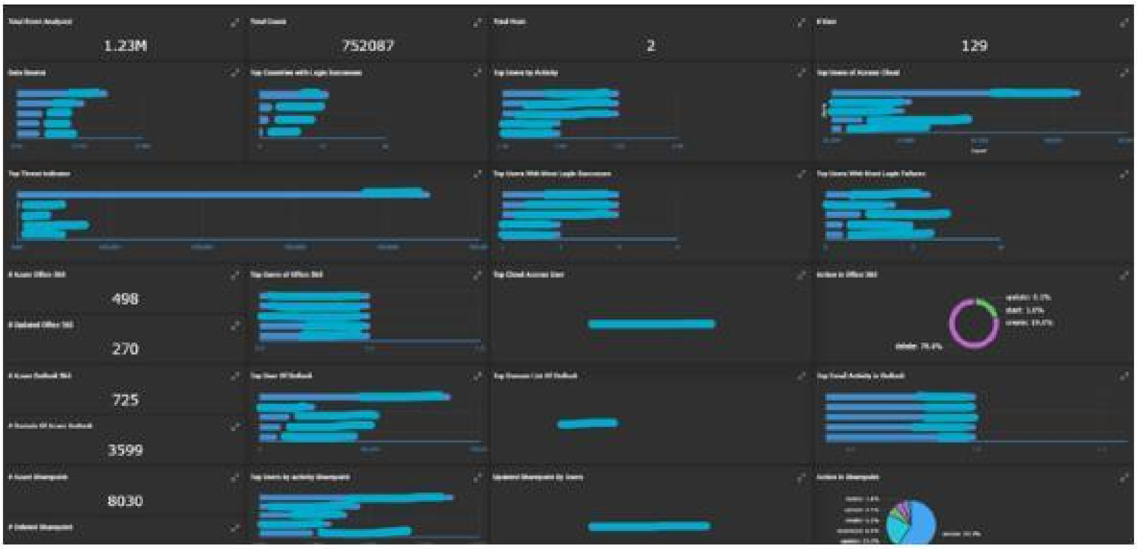


Fig 4.9 Azure Dashboard

List of detail that is provided from this dashboard:

- Data Source
- Top Countries with Login Successes
- Top Users by Activity
- Top Users by Activity
- Top Threat Indicator
- Top Users with Most Login Successes
- Top Users with Most Login Failures
- Top Cloud Access User
- Action in Office 365
- Top User of Outlook

- Top Domain List of Outlook
- Top Email Activity in Outlook
- Top Users by Activity SharePoint
- Updated SharePoint by Users
- Action in SharePoint

- Behavior Analytics

Fig 4.10 Behavior Analytics

In this section, we are going to get familiar to the UEBA, which is known as User Behavior Analysis

- User Behavior Analytics

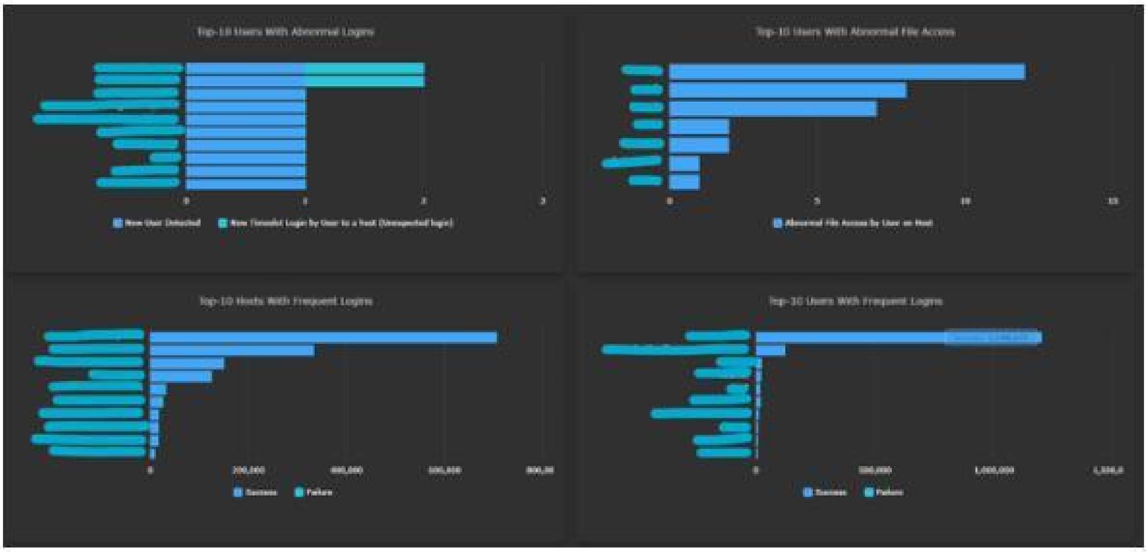


Fig 4.11: User Behavior Analytics Dashboard

Above shown is the analysis of the user is made using the machine learning a baseline created for each user and if any user cross that base line or the user behavior is slightly different than the base line then all that data is captured and presented over here with the user name and the category in which the user is according to base line.

- Host Behavior Analytics

  A base line of an host behavior is created by the machine learning and the AI component of the tool from the past behavior of the host and if the host starts behaving different then it actual behavior or normal behavior,that all the data is captured by the SIEM and presented over this dashboard

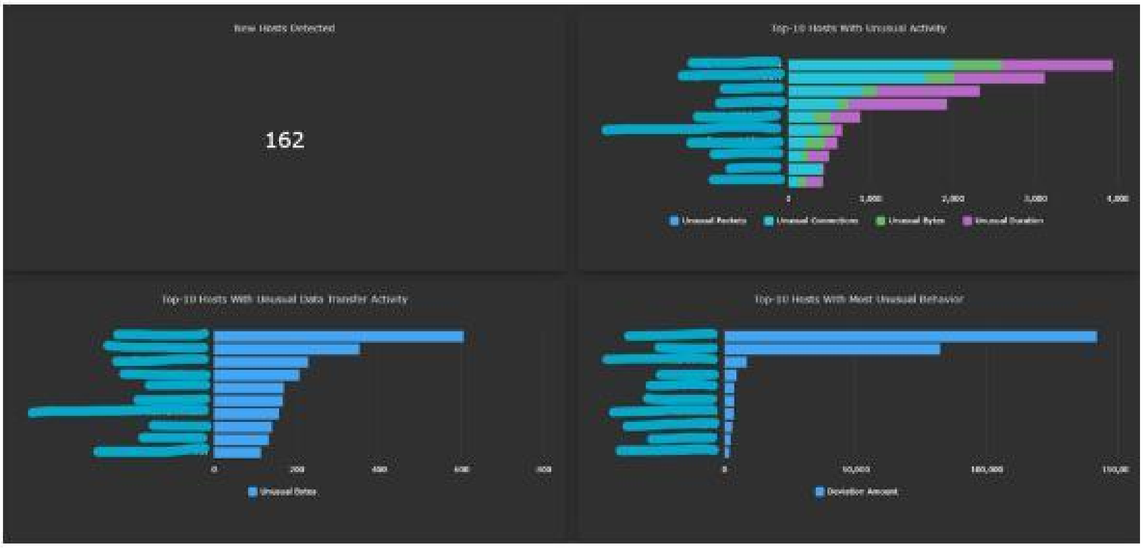


Fig 4.12: Host Behavior Analytics Dashboard

- Published Dashboard

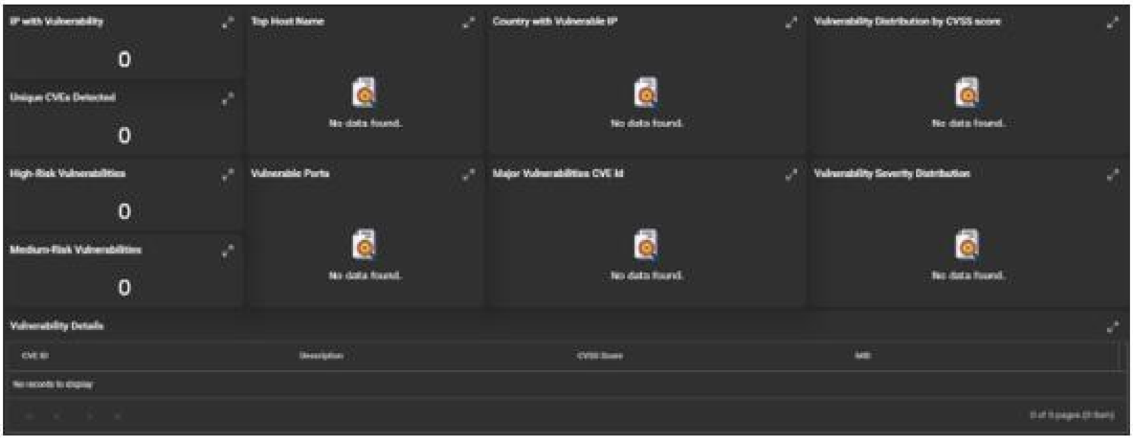
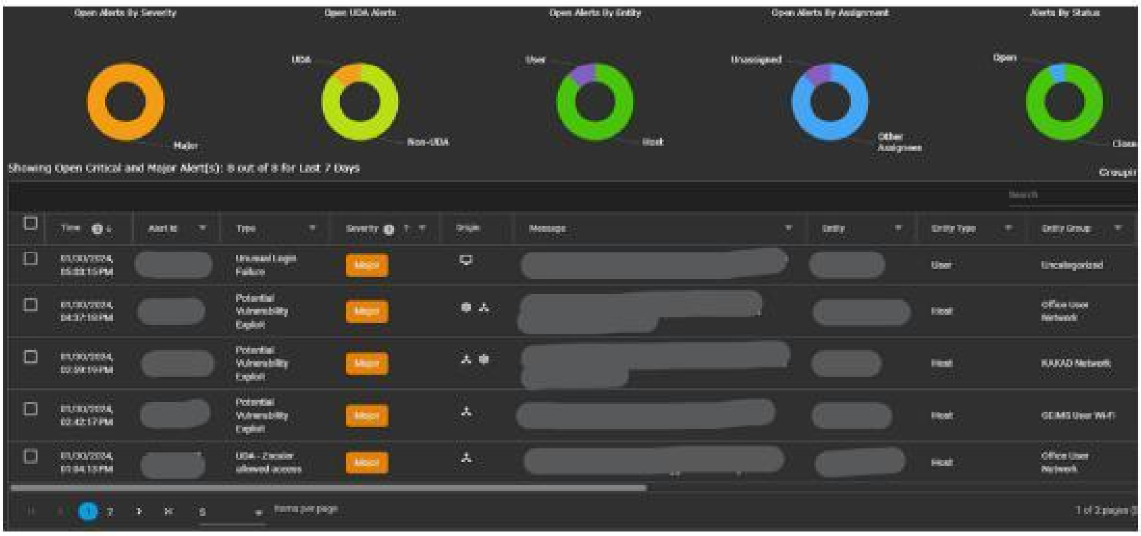


Fig 4.13 Published Dashboard

Over here all the data related to the Vulnerability assessment is presented here with the minute detail what vulnerability are there CVSS score for each vulnerability and many more.

- Threats

  The recent alert is shown over here in with its details such as Timestamp, Alert ID, Type of alert, and alert message.



Showing Open Critical and Major Alert(s): 8 out of 8 for Last 7 Days

□	Time	Alert Id	Type	Severity	Origin	Message	Entity	Entity Type	Entity Group
□	01/30/2024, 05:03:15 PM	[redacted]	Unusual Login Failure	Major		[redacted]	[redacted]	User	Uncategorized
□	01/30/2024, 04:37:10 PM	[redacted]	Potential Vulnerability Exploit	Major		[redacted]	[redacted]	Host	Office User Network
□	01/30/2024, 02:59:19 PM	[redacted]	Potential Vulnerability Exploit	Major		[redacted]	[redacted]	Host	KAKAD Network
□	01/30/2024, 02:42:17 PM	[redacted]	Potential Vulnerability Exploit	Major		[redacted]	[redacted]	Host	GEIMS User Wi-Fi
□	01/30/2024, 01:04:13 PM	[redacted]	UDA - Zscaler allowed access	Major		[redacted]	[redacted]	Host	Office User Network

Fig 4.14: Alert Dashboard

- Threat hunting

  The majority of this tab is used by the threat hunters and for the in-depth investigation of the activity of the particular entity. This tab helps to deep track the log and to run the query for the data which we want to retrieve from the logs and environment.

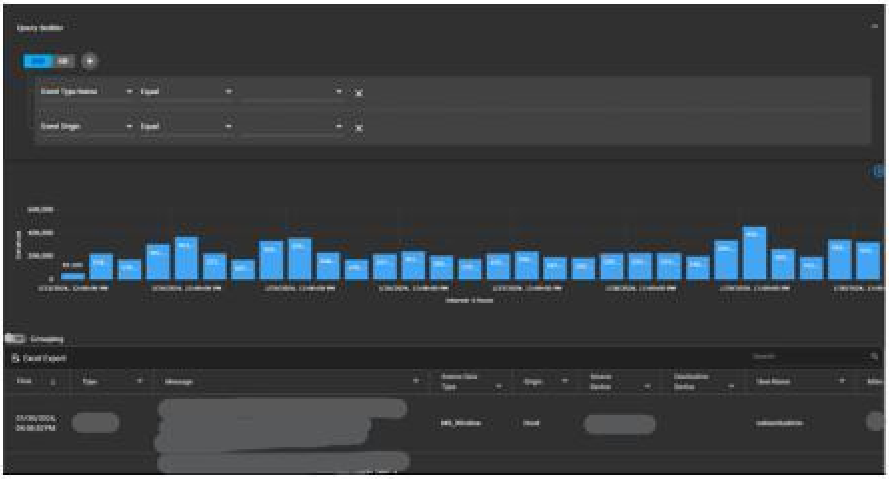
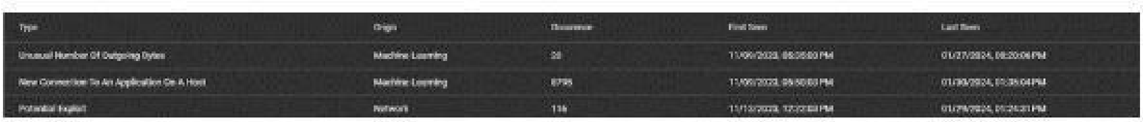


Fig 4.15: Deep Tracker

4.2 PROBLEM AND WEAKNESSES OF CURRENT SYSTEM

Seceon is an AI integrated tool, which take the help of the AI to make the analysis easy and simple but some time it works as weaknesses for the SIEM Let’s see the example



Type	Origin	Occurrence	First Seen	Last Seen
Unusual Number Of Outgoing Bytes	Machine Learning	20	11/09/2023, 08:35:03 PM	01/27/2024, 08:20:06 PM
New Connection To An Application On A Host	Machine Learning	8795	11/09/2023, 09:50:03 PM	01/30/2024, 01:35:04 PM
Potential Exploit	Network	116	11/13/2023, 12:22:03 PM	01/29/2024, 01:24:31 PM

Fig 4.16 Alert Details

As we can see the first scene of the incident is of 11/09/2023 and the last seen is 01/27/2024 due to AI it’s piled up the data with same incident on a day-by-day alert.

Which make tough for the analyst to investigate the incident because there is very big amount of the data to investigate and sometime which is too old and not of use for that case which is analyst is working on.

Now the weakness of the seceon is it own strength that is ML/AL, because the ML make the base line for all the host and the user for any threat for which the user/host is prone to so some time the normal behavior of the user is taken as the malicious activity and creates the alert which increases the false positive alert and the number of alerts.

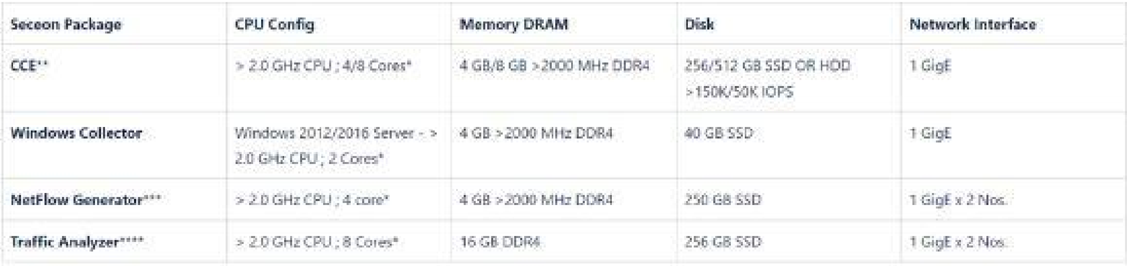
Also after some time it start fine tuning itself, due to the in-build AI/ML model and make the SIEM and alerts stable

4.3 REQUIREMENT OF NEW SYSTEM

The most basic thing which is required for the setup is the Rocky linux below are some step to follow:

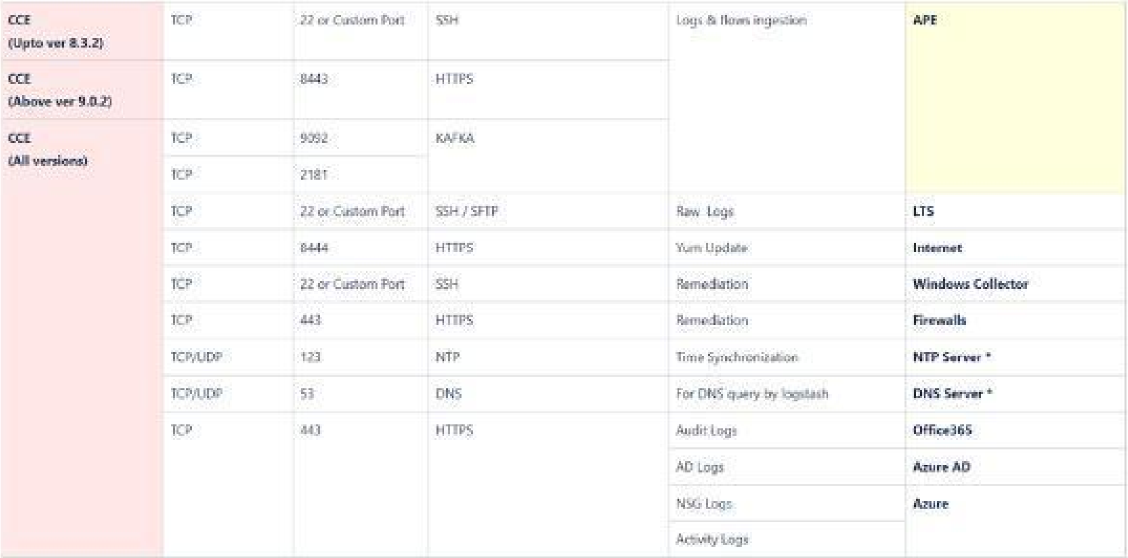
- Seceon server setup with Rocky Linux using Seceon repository
- Download ISO from Seceon Repository
- VM Creation: using downloaded ISO - Rocky-8.5-x86 64-minimal.is

Below are the specificaitons of the system which is required as the basic need



Seceon Package	CPU Config	Memory DRAM	Disk	Network Interface
CCE**	> 2.0 GHz CPU ; 4/8 Cores*	4 GB/8 GB >2000 MHz DDR4	256/512 GB SSD OR HDD >150K/50K IOPS	1 GigE
Windows Collector	Windows 2012/2016 Server - > 2.0 GHz CPU ; 2 Cores*	4 GB >2000 MHz DDR4	40 GB SSD	1 GigE
NetFlow Generator***	> 2.0 GHz CPU ; 4 core*	4 GB >2000 MHz DDR4	250 GB SSD	1 GigE x 2 Nos.
Traffic Analyzer****	> 2.0 GHz CPU ; 8 Cores*	16 GB DDR4	256 GB SSD	1 GigE x 2 Nos.

Fig 4.17: System Requirement



CCE (Upto ver 8.3.2)	TCP	22 or Custom Port	SSH	Logs & flows ingestion	APE
CCE (Above ver 9.0.2)	TCP	8443	HTTPS		
CCE (All versions)	TCP	9092	KAFKA		
	TCP	2181			
	TCP	22 or Custom Port	SSH / SFTP	Raw Logs	LTS
	TCP	8444	HTTPS	Yum Update	Internet
	TCP	22 or Custom Port	SSH	Remediation	Windows Collector
	TCP	443	HTTPS	Remediation	Firewalls
	TCP/UDP	123	NTP	Time Synchronization	NTP Server *
	TCP/UDP	53	DNS	For DNS query by logstash	DNS Server *
	TCP	443	HTTPS	Audit Logs	Office365
				AD Logs	Azure AD
				NSG Logs	Azure
				Activity Logs	

Fig 4.18: CCE Requirements

4.4 SYSTEM FEASIBILITY

4.4.1 Does The System Contribute To The Overall Objectives Of The Organization?

System fits very well with the overall objective of the organization, as it help with the automation tasks.

- It helps to maintain the compliance for the different types of organizations such as banking sectors where the compliance is the major objective for any organization.
- It helps to bring the different the multiple clients under one roof which is known as the multi tenancy, that is very easy to achieve in the Seceon.
- Seceon also help organization for the creating the security posture report of the client of every month as well as every year..

4.4.2 Can the System Be Implemented Using The Current Technology And Within The Given Cost And Schedule Constraints?

Yes, system is fully feasible with the current technology and within the given cost and also easy to implementation is done with the schedule constraints

4.4.3 Can the System Be Integrated With Other Systems Which Are Already In Place?

Yes, it is possible and very much easy to integrate the new system in to the existing environment. But there are some basic specification's that is required to fulfill the need of the current ongoing system.

4.5 PROCESS IN PROPOSED SYSTEM

What is Wazuh?

Wazuh is a unified XDR (Extended Detection and Response) platform that combines SIEM, endpoint detection and response (EDR), and log management capabilities. It collects and analyzes data from various sources, including

Endpoints: Servers, desktops, laptops, and mobile devices
Network devices: Firewalls, routers, switches, and intrusion detection/prevention systems (IDS/IPS)
Cloud workloads: Servers and applications hosted in public or private clouds
Applications: Web applications, databases, and other software systems

Benefits of Wazuh

- Improved security: Wazuh can help your client detect and respond to threats more quickly and effectively.
- Reduced costs: Wazuh is an open-source tool, so there are no licensing fees. It can also help your client reduce their security costs by consolidating multiple security tools into one platform.
- Increased visibility: Wazuh provides a centralized view of all security activity across your client's IT infrastructure.

- Scalability: Wazuh can be scaled to meet the needs of small businesses and large enterprises alike.
- Open source: Wazuh is an open-source project, which means that it is constantly being developed and improved by a community of developers.

How Wazuh can help industry:

Wazuh can be used by organizations in any industry, but it is particularly well-suited for organizations in the following industries:

- Finance: Wazuh can help financial institutions comply with security regulations and protect sensitive financial data.
- Healthcare: Wazuh can help healthcare organizations protect patient data and comply with HIPAA regulations.
- Retail: Wazuh can help retailers protect customer data and prevent fraud.
- Government: Wazuh can help government agencies protect critical infrastructure and sensitive data.

4.6 FEATURES OF PROPOSED SYSTEM

Wazuh offers a comprehensive set of techniques for threat detection, response, and prevention, making it a valuable tool for any organization's security posture. Here's a breakdown of its key functionalities:

Data Collection and Aggregation:

- Agents: Wazuh deploys lightweight agents on endpoints (servers, desktops, containers, etc.) to collect logs, system calls, file integrity changes, and other security-related data.
- Log Management: Wazuh centralizes and normalizes all collected data from various sources, including syslog, Windows Event Logs, and application logs.

Threat Detection and Analysis:

- Rule-based Engine: Wazuh uses a powerful rule-based engine to analyze collected data and identify suspicious activity based on pre-defined rules and indicators of compromise (IOCs).
- Machine Learning: Wazuh leverages machine learning algorithms to detect anomalies and emerging threats that might evade traditional rule-based detection.
- Threat Intelligence Integration: Wazuh integrates with threat intelligence feeds to stay updated on the latest vulnerabilities and attacker tactics, enhancing its detection capabilities.

Response and Remediation:

- Alerting and Escalation: Wazuh generates alerts for identified threats, notifying security teams through various channels like email, push notifications, and integration with ticketing systems.
- Automated Response: Wazuh can be configured to automatically take pre-defined actions upon detecting specific threats, such as blocking network connections, quarantining files, or stopping suspicious processes.
- Forensic Investigation: Wazuh provides detailed logs and reports for forensic analysis, helping security teams investigate incidents and understand attacker actions.

Additional Features:

- Vulnerability Management: Wazuh can identify vulnerabilities in systems and applications, helping prioritize patching efforts.
- Security Configuration Assessment: Wazuh can assess system configurations for compliance with security best practices.
- Compliance Reporting: Wazuh can generate reports to demonstrate compliance with various security regulations.

Overall, Wazuh offers a comprehensive and flexible approach to security by combining various techniques for data collection, analysis, response, and prevention.

4.7 SELECTION OF HARDWARE

Requirements

- Check the supported operating systems and the recommended hardware requirements for the Wazuh server installation. Make sure that your system environment meets all requirements and that you have root user privileges.

Recommended operating systems

- Wazuh server can be installed on a 64-bit Linux operating system. Wazuh supports the following operating system versions:

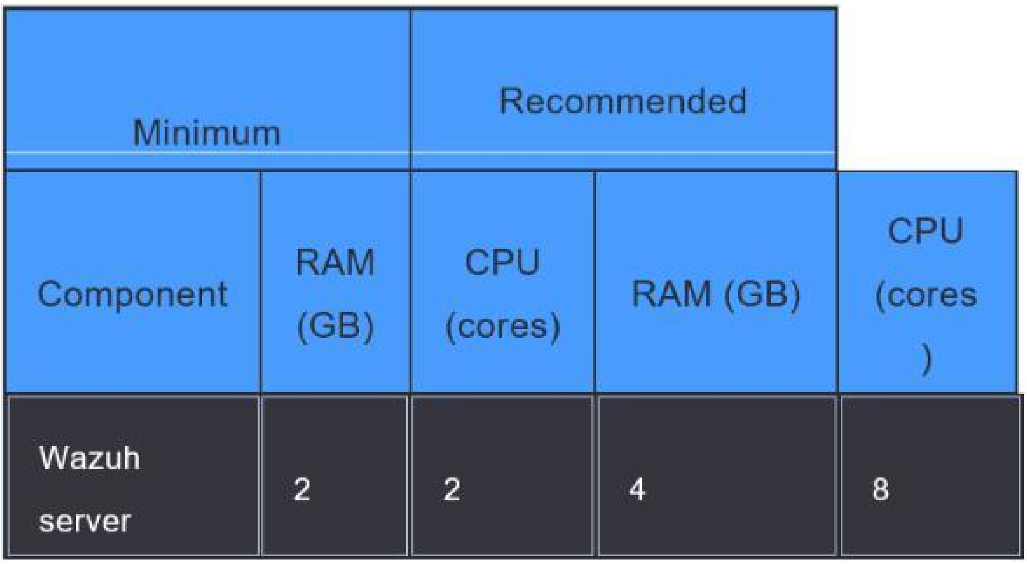
Amazon Linux 2	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04

Table 4.1 Wazuh System Requirements

Hardware requirements

The Wazuh server can be installed as a single-node or as a multi-node cluster.

- **Hardware recommendations**

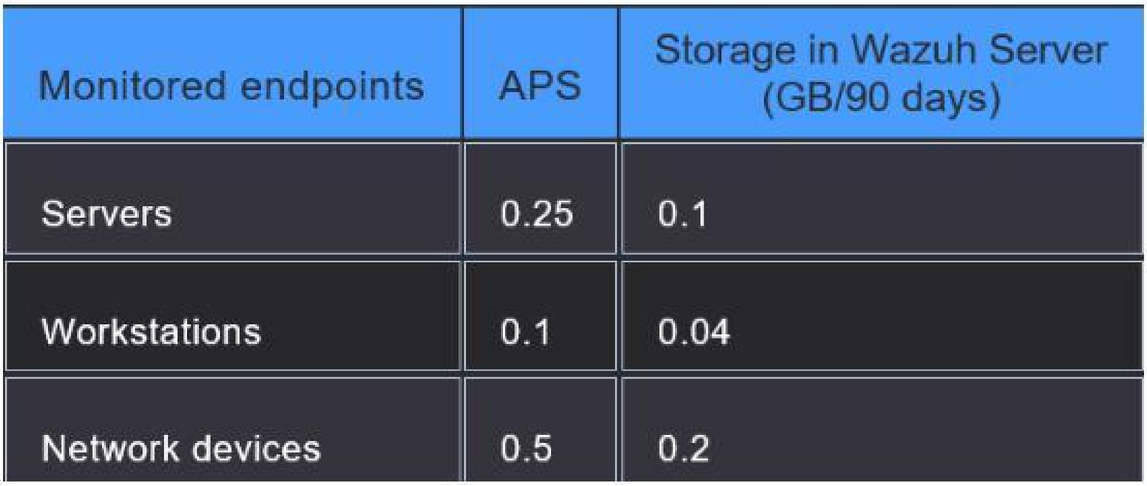


Minimum		Recommended		
Component	RAM (GB)	CPU (cores)	RAM (GB)	CPU (cores)
Wazuh server	2	2	4	8

Fig 4.19: Wazuh Server requirements

Disk space requirements

- The amount of data depends on the generated alerts per second (APS). This table details the estimated disk space needed per agent to store 90 days of alerts on a Wazuh server, depending on the type of monitored endpoints



Monitored endpoints	APS	Storage in Wazuh Server (GB/90 days)
Servers	0.25	0.1
Workstations	0.1	0.04
Network devices	0.5	0.2

Fig 4.20: Wazuh requirements

For example, for an environment with 80 workstations, 10 servers, and 10 network devices, the storage needed on the Wazuh server for 90 days of alerts is 6 GB.

CHAPTER 5 - SYSTEM DESIGN

At Techdefence Labs, as a Security Operations Center (SOC) Analyst, my internship involved intensive engagement with various system designs and methodologies crucial for efficient threat detection and incident response. This report outlines the system design aspects encompassing database design, data structure design, process design, and security mechanisms deployed during my tenure.

5.1 SYSTEM DESIGN & METHODOLOGY

The system design and methodology at Techdefence Labs revolve around establishing a robust framework for threat detection and incident response. This framework encompasses several key components:

- **Log Analysis Infrastructure:** The core of our system design lies in the effective analysis of logs generated by diverse network devices, servers, and applications. We utilize tools like Seceon, Securonix, and Splunk SIEM to collect, normalize, and correlate log data in real-time.

- **Incident Escalation Protocol:** A well-defined methodology governs the escalation of identified incidents to clients. Incidents are categorized based on severity and impact, ensuring a streamlined communication channel for prompt resolution.

- **Threat Hunting Strategies:** Beyond reactive incident response, our system design emphasizes proactive threat hunting. This involves the systematic search for potential threats within the network environment, leveraging both manual investigation techniques and automated threat intelligence feeds

5.2 PROCESS DESIGN

In the context of SOC operations, database design and data structure play a critical role in storing and organizing vast amounts of security-related data. Key considerations in our database design include:

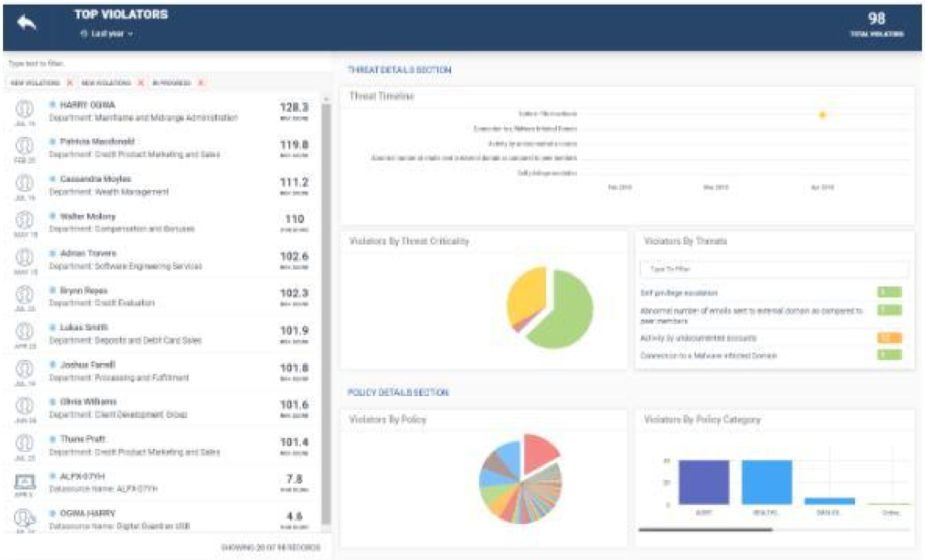
- Normalization: To minimize data redundancy and ensure data integrity, we employ normalization techniques to organize data into logical tables.
- Schema Design: Our database schema is tailored to accommodate various types of security-related data, including log entries, incident reports, threat intelligence feeds, and client information.

5.3 Output and Interface Design

While much of our work as SOC analysts revolves around back-end operations, interface design remains crucial for facilitating interaction with the underlying systems.

Key aspects of our interface design include:

- **Dashboard Visualization:** Dashboards provide a comprehensive view of the security posture, displaying metrics such as the number of incidents detected, their severity levels, and ongoing threat campaigns.



HARRY OGWA — Department: Mainframe and Midrange Administration — 128.3
Patricia Macdonald — Department: Credit Product Marketing and Sales — 119.8
Cassandra Moyles — Department: Wealth Management — 111.2
Walter Molony — Department: Compensation and Benefits — 110
Adrian Travers — Department: Software Engineering Services — 102.6
Brynn Repas — Department: Credit Evaluation — 102.3
Lukas Smith — Department: Deposits and Debit Card Sales — 101.9
Joshua Farrell — Department: Processing and Fulfillment — 101.8
Olivia Williams — Department: Client Development Group — 101.6
Thane Pratt — Department: Credit Product Marketing and Sales — 101.4
ALFX07YH — Datasource Name: ALFX07YH — 7.8
OGWA HARRY — Datasource Name: Digital Guardian USB — 4.6

SHOWING 20 OF 98 RECORDS

Self privilege escalation
Abnormal number of emails sent to external domain as compared to peer members
Activity by undocumented accounts
Connection to a Malware infected Domain

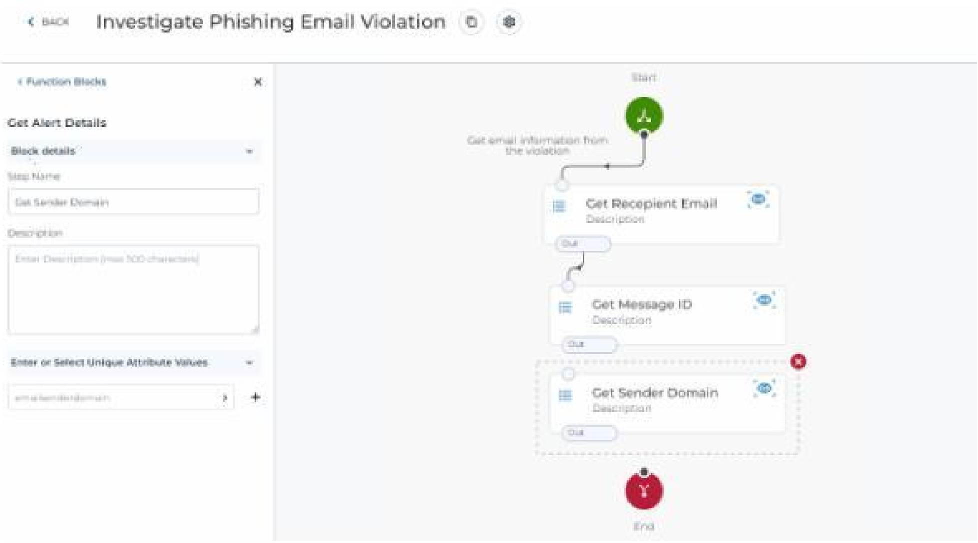
Fig 5.1: Securonix Dashboard

- **Custom Reports**: We design custom reports tailored to the specific requirements of clients, providing insights into security incidents, trends, and compliance metrics.
- **Playbook Repository:** A centralized repository is maintained to store and manage the collection of playbooks. This repository provides SOC analysts with easy access to the latest version of playbooks and ensures consistency in response procedures

5.3.1 Playbook Creation and its Usefulness in SOC

Standardization: Playbooks standardize the response procedures for common security incidents, ensuring consistency and efficiency in incident handling.

- Efficiency: By providing step-by-step instructions, playbooks enable SOC analysts to respond to incidents promptly and effectively, minimizing the time required to mitigate threats.
- Knowledge Transfer: Playbooks serve as a repository of institutional knowledge, allowing new SOC analysts to quickly familiarize themselves with established response procedures and best practices.
- Continuous Improvement: Playbooks are continuously updated and refined based on feedback and lessons learned from real-world incidents, enabling the SOC to adapt and improve its response capabilities over time.



Investigate Phishing Email Violation

Get Alert Details

Block details

Step Name: Get Sender Domain

Description: Enter Description (max 500 characters)

Enter or Select Unique Attribute Values: emailsenderdomain

Fig 5.2: Investing Phishing Email Playbook Flow

5.3.2 Access Control / Mechanism / Security

Security is paramount in SOC operations, and our system design incorporates robust access control mechanisms to safeguard sensitive data and infrastructure. Key security measures include:

- Role-Based Access Control (RBAC): Access privileges are assigned based on predefined roles, ensuring that individuals have access only to the data and functionalities necessary for their responsibilities.

- Encryption: Sensitive data, both in transit and at rest, is encrypted using industry-standard encryption algorithms, mitigating the risk of data breaches.

- Audit Trails: Comprehensive audit trails are maintained, logging all user activities within the system. This not only aids in forensic investigations but also ensures accountability and compliance with regulatory requirements.

In conclusion, my internship at Techdefence Labs provided invaluable insights into the intricate system design aspects underpinning SOC operations. From database architecture to interface design and security mechanisms, the experience enhanced my understanding of the holistic approach required for effective cybersecurity management.

CHAPTER 6 - IMPLEMENTATION OF THREAT HUNTING

6.1 INCORPORATING THREAT HUNTING INTO SOC OPERATIONS WORKFLOW

- **Seamless Integration:** Threat hunting is seamlessly integrated into the daily workflow of our SOC analysts. It's not treated as a separate task but rather as an integral part of our overall cybersecurity strategy.

- **Dedicated Time Slots:** Specific time slots are allocated within the workday for proactive threat hunting activities. This ensures that analysts have dedicated time to focus on hunting for potential threats rather than solely reacting to incidents.

- **Inclusion in Incident Response Procedures:** Threat hunting tasks are included within our incident response procedures. This means that whenever an incident is detected and responded to, analysts also consider if any related threats could be proactively hunted down.

6.2 ROLE OF THREAT INTELLIGENCE IN INFORMING THREAT HUNTING ACTIVITIES

- Utilization of Sources: We leverage a variety of sources for threat intelligence, including internal sources such as historical incident data and external sources such as threat intelligence feeds, open-source intelligence (OSINT), and information-sharing

- Prioritization: The gathered threat intelligence is analyzed to prioritize threat hunting efforts. By understanding the current threat landscape and the tactics, techniques, and procedures (TTPs) used by threat actors, we can focus our hunting activities on areas with the highest risk or potential impact.

- Guidance for Hunt Teams: Threat intelligence provides guidance for our hunt teams, helping them to refine their search parameters and identify relevant indicators of compromise (IOCs) or patterns of suspicious behavior

6.3 UTILIZATION OF DATA ANALYTICS AND MACHINE LEARNING FOR THREAT DETECTION

- Big Data Analytics: We harness the power of big data analytics to process and analyze large volumes of security telemetry generated by various sources within our network environment. This allows us to identify anomalous patterns or deviations from normal behavior that may indicate a potential threat.
- Machine Learning Algorithms: Machine learning algorithms are employed to automate the detection of suspicious behavior. These algorithms are trained on historical data to recognize patterns associated with known threats and can adapt over time to identify emerging threats or novel attack techniques.
- Rapid Identification: By combining data analytics with machine learning, we can rapidly identify potential threats amidst the operational noise of everyday network activity. This enables us to detect and respond to threats more effectively, reducing the time to detect and mitigate cyber incidents.

6.4 AUTOMATION AND ORCHESTRATION OF THREAT HUNTING PROCESSES

- Custom Scripts and Workflows: We have developed custom scripts and workflows to automate repetitive tasks involved in the threat hunting process, such as data collection, enrichment, and correlation. These scripts streamline the hunting process and free up analysts’ time for more strategic activities.
- Orchestration Platforms: Orchestration platforms are used to coordinate and automate the execution of complex threat hunting playbooks. These platforms allow us to integrate and orchestrate the interaction between various security tools
- Unified Defense Posture: By automating and orchestrating threat hunting processes, we can achieve a unified defense posture that leverages the collective capabilities of our security tools and systems. This enables us to respond more effectively to threats and reduce the risk of successful cyber attacks

6.5 CONTINUOUS IMPROVEMENT AND ITERATION OF THREAT HUNTING STRATEGIES

- Lessons Learned: Lessons learned from past hunts are used to refine and enhance our threat hunting strategies. By analyzing the outcomes of previous hunts, we can identify patterns, trends, and emerging threats that inform our future hunting efforts.

- Development of New Methodologies: Based on our analysis of past hunts and emerging threats, we develop new hunting methodologies and techniques to stay ahead of evolving threats. These methodologies are continuously refined and updated based on feedback and lessons learned from ongoing hunting activities.

- Culture of Continuous Learning: We foster a culture of continuous learning and adaptation within our SOC team. Analysts are encouraged to stay up-to-date on the latest threat trends, tools, and techniques through training, certifications, and knowledge sharing sessions. This ensures that our threat hunting capabilities remain at the forefront of cybersecurity innovation.

In summary, the implementation of threat hunting involves seamlessly integrating threat hunting into SOC operations, leveraging diverse sources of threat intelligence, harnessing data analytics and machine learning, automating and orchestrating threat hunting processes, and fostering a culture of continuous improvement and innovation. This multifaceted approach enables us to proactively detect and respond to threats, reducing the risk of successful cyber-attacks and enhancing our overall cybersecurity posture.

CHAPTER 7 - TESTING

7.1 TESTING PLAN

A robust SOC testing plan includes:

1. Testing Objectives: Assess detection capabilities, measure analyst response, test incident response process, and identify gaps and vulnerabilities.

2. Testing Scope: Evaluate network security controls, SIEM functionality, and analyst procedures, and communication channels.

3. Testing Methodology: Utilize penetration testing, scenario-based testing, log injection, and misconfiguration testing.

4. Testing Tools: Employ penetration testing frameworks, SOAR platforms, vulnerability scanners, and log generators.

5. Reporting and Remediation: Document findings, prioritize remediation and update procedures and playbooks based on outcomes.

6. Continuous Improvement: Maintain a regular testing cadence, and adapt scenarios to reflect evolving threats, and integrate lessons learned in training programs.

By implementing such a plan, organizations can ensure their SOC is well prepared to defend against cyber threats effectively.

7.2 TEST CASES

SOC Testing Breakdown:

1. SIEM Testing:

- Log Source Connectivity
- Log Parsing and Normalization
- Alert Generation
- Threat Intelligence Integration
- Reporting and Dashboarding

2. SOAR Testing:

- Playbook Execution
- Integration with SIEM and Security Tools
- Scalability and Performance

3. Detection and Response Capabilities:

- Scenario-Based Testing
- Vulnerability Scanning and Exploitation
- Endpoint Security Testing

4. Investigation and Analysis Tools:

- Forensic Artifact Collection
- Log Analysis Tools

5. Business Continuity and Disaster Recovery (BCDR) Testing:

- Incident Response Procedure
- Backup and Restore Functiaity

By conducting tests across these areas, SOC analysts can ensure their tools and processes are optimized for efficient threat detection, response, and recover

CHAPTER 8 - CONCLUSION AND DISCUSSION

8.1 OVERALL ANALYSIS OF INTERNSHIP

During the internship at Techdefence Labs, the viability and effectiveness of the project were thoroughly assessed. The integration of threat hunting into SOC operations proved to be a valuable addition to the cybersecurity strategy. The proactive approach facilitated by threat hunting complemented traditional reactive measures, resulting in improved threat detection and response capabilities. The implementation of threat intelligence, data analytics, and automation enhanced the efficiency and efficacy of threat-hunting activities, contributing to a more robust defence posture.

8.2 PROBLEMS ENCOUNTERED AND POSSIBLE SOLUTIONS

Throughout the internship, several challenges were encountered in the implementation of threat-hunting practices. These challenges included:

- Resource Constraints: Limited resources, such as time and manpower, posed challenges in conducting comprehensive threat-hunting activities.
- Complexity of Threat Landscape: The evolving and complex nature of the threat landscape made it challenging to stay ahead of emerging threats.
- Tool Integration Issues: Integration issues between different security tools and platforms hindered the seamless execution of threat-hunting processes.

Possible solutions to these challenges include:

- Resource Allocation: Prioritizing threat hunting activities and allocating dedicated resources to ensure consistent and proactive threat detection.
- Continuous Training and Education: Providing ongoing training and education to SOC analysts to enhance their skills and knowledge of emerging threats and hunting techniques.
- Enhanced Tool Integration: Implementing robust integration frameworks and protocols to streamline the interaction between security tools and platforms.

8.3 SUMMARY INTERNSHIP

My internship at Techdefence Labs provided invaluable hands-on experience in SOC analysis and threat hunting. Through the integration of threat hunting into SOC operations, significant progress was made in enhancing the organization's cybersecurity posture. The implementation of threat intelligence, data analytics, and automation facilitated proactive threat detection and response, mitigating potential risks and vulnerabilities

8.4 LIMITATIONS AND FUTURE ENHANCEMENTS

Despite the successes achieved during the internship, certain limitations were identified, including:

- Scalability: The scalability of threat-hunting processes may be limited by resource constraints and tool capabilities.
- Accuracy: The accuracy of threat detection may be affected by false positives or incomplete data.
- Adaptability: The ability to adapt to rapidly evolving threats and techniques may pose challenges in maintaining effectiveness over time.

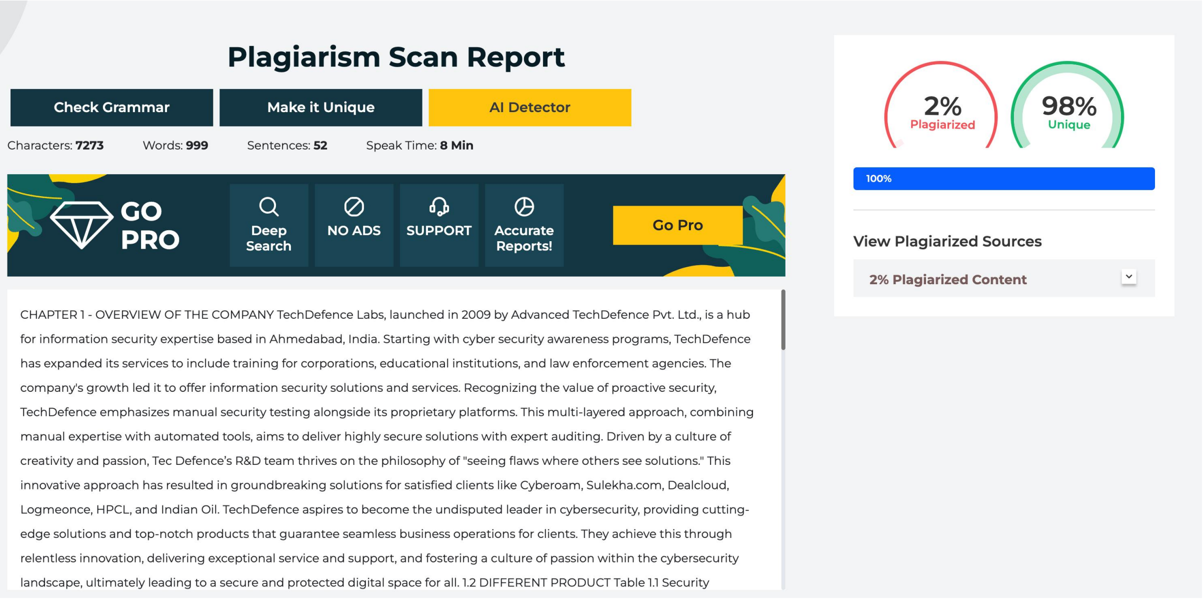
To address these limitations and further enhance the effectiveness of threat-hunting practices, future enhancements may include:

- Investment in Resources: Increasing investment in resources, such as personnel, training, and technology, to support scalable and efficient threat-hunting operations.
- Refinement of Processes: Continuously refining and optimizing threat hunting processes based on lessons learned and emerging best practices.
- Integration of Advanced Technologies: Leveraging emerging technologies such as artificial intelligence (AI) and machine learning (ML) to improve the accuracy and effectiveness of threat detection and response.

REFERENCES

1. M. Vielberth, F. Böhm, I. Fichtinger and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," in *IEEE Access*, vol. 8, pp. 227756-227779
2. N. Akshai Sankar and K. A. Fasila, "Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring," *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, Kochi, Kerala, India, 2023, pp. 350-354
3. Reddy Pulyala, S. ., Gupta Desetty, A. ., & Dutt Jangampet, V. . (2019). The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 10(3), pp. 1545–1549.
4. Stanković, S., Gajin, S., & Petrović, R. (2022). A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. No Nama Agent Integrity File Added Delete Modified, 1.
5. The SANS Internet Storm Center (ISC) provides daily diaries and analysis of security events and trends.
6. The Recorded Future blog offers insights into threat intelligence and emerging cyber threats.
7. The Krebs on Security blog by Brian Krebs provides in-depth analysis of cybersecurity incidents and trends.
8. CrowdStrike's white papers and case studies on incident response and threat hunting strategies.
9. IBM Security's white papers on SOC optimization, threat intelligence, and incident response best practices
10. "Security Operations Center – Building, Operating, and Maintaining your SOC" by Joseph Muniz, Gary McIntyre, and Nadhem AlFardan.
11. https://techdefencelabs.com/

PLAGIARISM SCAN REPORT



Characters: **7273** Words: **999** Sentences: **52** Speak Time: **8 Min**

CHAPTER 1 - OVERVIEW OF THE COMPANY TechDefence Labs, launched in 2009 by Advanced TechDefence Pvt. Ltd., is a hub for information security expertise based in Ahmedabad, India. Starting with cyber security awareness programs, TechDefence has expanded its services to include training for corporations, educational institutions, and law enforcement agencies. The company's growth led it to offer information security solutions and services. Recognizing the value of proactive security, TechDefence emphasizes manual security testing alongside its proprietary platforms. This multi-layered approach, combining manual expertise with automated tools, aims to deliver highly secure solutions with expert auditing. Driven by a culture of creativity and passion, Tec Defence's R&D team thrives on the philosophy of "seeing flaws where others see solutions." This innovative approach has resulted in groundbreaking solutions for satisfied clients like Cyberoam, Sulekha.com, Dealcloud, Logmeonce, HPCL, and Indian Oil. TechDefence aspires to become the undisputed leader in cybersecurity, providing cutting-edge solutions and top-notch products that guarantee seamless business operations for clients. They achieve this through relentless innovation, delivering exceptional service and support, and fostering a culture of passion within the cybersecurity landscape, ultimately leading to a secure and protected digital space for all. 1.2 DIFFERENT PRODUCT Table 1.1 Security