INFORMATION SECURITY AND NETWORK SECURITY INTERN
Amicorp Management

AN INTERNSHIP REPORT

Submitted by,

SYED FAISAL EHSAN - 20211CCS0187

Under the guidance of,

Ms. AMREEN KHANUM D

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING, CYBER SECURITY

At

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Internship report **"Information Security and Network Security Intern"** being submitted by "SYED FAISAL EHSAN," bearing roll number "20211CCS0187" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a Bonafide work carried out under my supervision.

Ms. Amreen Khanum D
Assistant Professor
PSCS
Presidency University

Dr. ANANDARAJ SP
Professor & HoD
PSCS
Presidency University

Dr. MYDHILI NAIR
Associate Dean School
of CSE
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vc School of Engineering
Dean -PSCS / PSIS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

I hereby declare that the work which is being presented in the project report entitled **Information Security and Network Security using CISCO and ZOHO Solutions** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of our own investigations carried out under the guidance of **Ms. Amreen Khanum D, Assistant Professor, School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NUMBER	SIGNATURE
SYED FAISAL EHSAN	20211CCS0187	

AMICORP

Address
Amicorp Management India Private Limited
C/O Regus Eversun Business Centre
Ground Floor, E1 Block(Beech), Manyata
Embassy Business Park, Outer Ring Road
Bangalore 560 045
India

Telephone
+91 80 4005 4900
Facsimile
+91 80 4005 4906

E-mail
bangalore@amicorp.com
Web
www.amicorp.com

To Whom So Ever It May Concern,

This is to certify that **Syed Faisal Ehsan** has successfully completed a 3-month internship at Amicorp Management India Private Limited, serving in the capacity of an Information Security and Network Security Intern from 3rd February 2024 to 30th April 2024.

During the tenure of the internship, Faisal demonstrated excellent dedication and professionalism in all assigned responsibilities and actively contributed to various projects within the organization's cybersecurity environment.

Key Responsibilities and Technologies Worked on
The internship involved practical exposure to a wide array of cybersecurity technologies and tools, including but not limited to:

1. Cisco Firewall Management Center (FMC) – Implementing access control policies and firewall configurations
2. Cisco StealthWatch (Secure Network Analytics) – Network traffic monitoring and behavioral anomaly detection
3. Cisco Identity Services Engine (ISE) – Policy-based access control and endpoint compliance enforcement
4. Cisco Email Security Appliance (ESA) – Email threat filtering, anti-phishing, and DLP configurations
5. Splunk – Security Information and Event Management (SIEM) integration and log analytics
6. Nexpose (by Rapid7) – Vulnerability assessment and risk remediation
7. Wireshark & Snort – Packet analysis and network-based intrusion detection
8. Cisco Packet Tracer – Network simulation and topology planning

Faisal also actively participated in red-teaming and blue-teaming exercises, simulated incident response workflows, and applied cybersecurity frameworks including ISO 27001, NIST, and Zero Trust Architecture principles.

We appreciate Faisal's contributions and wish them continued success in future professional endeavors.

Signed by:
CC9489A6BE27417...

Asokan Kunnathully

Head of HR India

For Amicorp Management India Pvt. Ltd.

Authorised Signatory

AMICORP MANAGEMENT INDIA PVT. LTD. BANGALORE

ABSTRACT

This report outlines the key experiences and learnings from my internship, which focused on enterprise network security, with a particular emphasis on working with Cisco technologies, next-generation firewalls (NGFWs), and broader information security (InfoSec) practices. The internship took place in a mid-to-large-scale IT environment, where I had the opportunity to work directly with advanced security tools like Cisco Firepower NGFW, Cisco Identity Services Engine (ISE), and Cisco SecureX. This hands-on experience allowed me to understand how these solutions are applied in real-world scenarios to protect enterprise networks.

One of the core tasks during my internship was deploying and configuring next-generation firewalls. These firewalls are essential in today's security landscape because they go beyond traditional filtering by offering deep packet inspection, integration with threat intelligence, and application-level controls. I also worked on setting up secure network segmentation using Cisco TrustSec and dynamic VLANs to minimize the risk of lateral movement in case of a breach.

In addition to technical work, I gained exposure to some of the less visible—but equally important—aspects of cybersecurity: vendor management and contract governance. As organizations increasingly depend on third-party providers and cloud platforms, ensuring these partners meet security standards is critical. During my time there, I was involved in reviewing vendor compliance using standard security questionnaires (like VSQs), helping draft contract clauses related to data protection, and aligning these with industry standards like ISO 27001, SOC 2, and personal data regulations (PII).

Overall, this internship showed me that effective cybersecurity isn't just about using the right tools—it's also about having strong processes in place for managing risk, ensuring compliance, and holding vendors accountable. The experience gave me a clearer understanding of how technical security measures and governance work together to protect an organization's digital assets.

ACKNOWLEDGEMENT

First of all, we are indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Pro- VC, School of Engineering and Dean, School of Computer Science Engineering & Information Science, Presidency University, for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Deans **Dr. Mydhili Nair,** School of Computer Science Engineering & Information Science, Presidency University, and **Dr. Anandaraj SP**, Head of the Department, School of Computer Science Engineering & Information Science, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Ms. Amreen Khanum D,** Assistant Professor and Reviewer **Dr. Sharmasth Vali Y,** Associate Professor, School of Computer Science Engineering & Information Science, Presidency University for his inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the PIP2001 Capstone Internship Coordinators **Mr. Md Zia Ur Rahman and Dr. Sampath A K,** department Project Coordinator **Dr. Sharmasth Vali Y** and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us with in bringing out this project.

Syed Faisal Ehsan

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	iv
	ACKNOWLEDGMENT	v
	TABLE OF CONTENTS	vi
		vii
1.	**INTRODUCTION**	1
	1.1 Introduction to Network Security	8
	1.2 Cisco Network Security Solution and Impact	11
	1.3 Information Security – Vendor and Contract Management	14
	1.4 Hardware and Software Requirement for IDPS	17
	1.5 System Design and Implementation	18
	1.6 Data Management and Feature Extraction	19
	1.7 System Evaluation and Performance Metrics	23
	1.8 Model Building and Training	25
2.	**Proposed Methodology**	26
	2.1 Understanding SOC	26
	2.2 **Soc's** Role in Network Security	26
	2.3 Soc's role in server Security	27
	2.4 Threat Intelligence and Correlation	27
	2.5 Incidence Response and Recovery	28
	2.6 Compliance and Reporting	29
	2.7 Challenges in SOC	29
	2.8 Understanding GRC and Information Security	

2.9 ISO 27001 Implementation 30

2.10 SOC 2 Type 2 31

3. OBJECTIVES

3.1 Designing Small Enterprise networks using CISCO PT 34

3.2 Network Planning and Design Principles 34

3.3 Designing a Small Office Network in Packet Tracer

3.4 Security Considerations in Network Design 35

3.5 Monitoring and Troubleshooting 36

3.6 Scaling Up: Moving Beyond the Basics

3.7 Centralized Contract and Vendor Management with Zoho Contracts 37

4. SYSTEM DESIGN AND IMPLEMENTATION 40

5. TIMELINE OF THE INTERNSHIP 42

6. OUTCOMES

6.1 Vendor Management 43

6.2 Network Design using Cisco PT 44

6.3 Auding Finding Automation

6.4 Reduced Emergency Response Time

6.5 Seamless Communication and Coordination

6.6 Increased Accessibility 45

6.7 Enhanced Response 46

6.8 Resource Management

6.9 Real Time Alerts

6.10 Scalability and Adaptability

6.11 Contribution to SDGs

7. CONCLUSION & FUTURE SCOPE 47

APPENDIX – A 49
IMPLEMENTATION AND SCREENSHOTS
PLAGIARISM

APPENDIX - B 67

CHAPTER – 1
INTRODUCTION

1.1 Introduction of Network Security

In today's digitally driven world, computer networks play a vital role in how we communicate, share information, and keep systems running smoothly. At a basic level, a network is just a group of devices—like computers, servers, routers, and switches—that are connected to each other, either with cables (like Ethernet) or wirelessly (through Wi-Fi or mobile networks). These connections allow users and systems to access shared resources, collaborate more easily, and stay connected, whether it's in a small office, a large organization, or across the globe.

Depending on their size and purpose, networks can be grouped into different categories. A Local Area Network (LAN) is usually limited to a single location like a home or office. A Wide Area Network (WAN), on the other hand, connects multiple LANs over large distances—this is how the internet works. A Metropolitan Area Network (MAN) covers a wider area like a city or university campus, while a Personal Area Network (PAN) handles close-range communication, such as Bluetooth between a phone and headphones.
Networks are built using a mix of hardware and software. Hardware includes things like routers, switches, and firewalls, while the software side covers operating systems, network protocols, and monitoring tools. All of this is tied together using communication standards—most commonly the TCP/IP model—which ensures data is sent and received correctly between devices. The internet, being the biggest network of them all, relies on these same principles to connect billions of users and devices.

As businesses adopt cloud services, IoT devices, and support remote workforces, networks have grown more complex—and unfortunately, more vulnerable to cyber threats. Attacks like malware infections, ransomware, phishing, and denial-of-service (DoS) attempts are just a few examples of the risks organizations face. Because of this, network security has become a critical field within IT. It focuses on putting the right tools, policies, and practices in place to keep data safe, systems secure, and services up and running.
During my internship, I worked with Cisco technologies, a major name in networking and

security. Cisco provides not only core networking devices like routers and switches, but also powerful security solutions such as next-generation firewalls (NGFWs) and intrusion prevention systems (IPS). These tools help detect and block threats in real time. I also learned about techniques like network segmentation and 802.1X secure access, which are used to control how different users and devices connect to the network and limit potential attack points.

But network security isn't just about technology, it also involves making sure that external partners, cloud services, and vendors follow strict security standards. This means reviewing contracts carefully, managing risks with third-party services, and staying compliant with industry regulations. In short, networks are like the nervous system of any modern organization. Understanding how they work—and how to protect their key for any IT professional working in today's fast-paced, security-conscious environment.

A computer network is basically a group of connected devices—like computers, servers, or even smartphones—that can communicate with each other and share things like files, applications, or internet access. These networks can range from a simple setup in someone's home to large, complex systems that stretch across different countries. In today's tech-driven world, networks are at the heart of almost every information system, making it possible to transfer data quickly and keep operations running smoothly. But as networks grow in size and complexity, keeping them secure has become more challenging—and more important. That's why having a good understanding of how networks are structured and how communication protocols work is essential for building strong security defenses.

In the digital age, data is the lifeblood of modern life—flowing between individuals, businesses, and governments with every click, message, and transaction. As our reliance on interconnected systems grows, so does the importance of protecting the networks that carry this data. This is where network security becomes crucial.

Network security is the practice of protecting the integrity, confidentiality, and availability of data and systems as it moves across or resides within networks. It involves a broad range of technologies, processes, and protocols designed to defend against cyber threats, unauthorized access, data breaches, and service disruptions.

What makes network security especially important is not just the technology, but its human impact. A compromised network can lead to financial loss, identity theft, operational

shutdowns, and even risks to public safety. Whether it's safeguarding personal emails, securing business transactions, or protecting government infrastructure, network security plays a fundamental role in enabling trust in the digital world.

To better understand network security, it's helpful to look at its key domains, each addressing different layers and types of protection:

- Access Control

  This ensures that only authorized users or systems can access specific data or network resources. Techniques include multi-factor authentication, role-based access control, and identity verification.

- Network Segmentation

  By dividing the network into smaller zones, segmentation limits the spread of attacks. It creates boundaries within the network to isolate sensitive data or systems.

- Perimeter Security & Firewalls

  Firewalls are the gatekeepers of a network, filtering traffic between trusted internal systems and external networks. Perimeter security includes intrusion prevention systems and gateway defenses.

- Intrusion Detection and Prevention Systems (IDPS)

  These tools monitor network activity to detect suspicious behavior, unauthorized access attempts, or known attack signatures—and either alert administrators or actively block them.

- Endpoint Security

  Laptops, smartphones, and other devices connected to a network can serve as entry points for threats. Endpoint protection software ensures each device is secure and compliant with security standards.

- Virtual Private Network (VPN) and Remote Access Security

  With the rise of remote work, secure communication channels like VPNs ensure that data transferred from offsite locations remains encrypted and protected.

- Application Security

  Since many threats exploit vulnerabilities in software applications, this domain involves securing apps through code reviews, security testing, and patch management.

- Data Loss Prevention (DLP) DLP systems are designed to prevent unauthorized transmission of sensitive information—such as customer data, intellectual property, or

financial records—outside the network.

- Security Monitoring, Logging & Incident Response Even with strong defenses, incidents can occur. Monitoring tools track network activity in real time, while incident response teams investigate, contain, and recover from breaches.
- Security Policies & Compliance Beyond technology, effective network security relies on clear policies, user awareness, and adherence to standards (e.g., ISO 27001, GDPR, HIPAA). Human behavior, guided by policy, is often the first line of defense.

In summary, network security is not a single solution but a layered and dynamic strategy that requires constant vigilance, adaptation, and collaboration. For any organization, building and maintaining a secure network is as much about technology as it is about people—making it a vital aspect of the modern digital workplace.

1.2 Cisco Network Security Solutions and Its Impact.

1. Cisco Secure Firewall: The Digital Gatekeeper

In our interconnected world, safeguarding digital perimeters is paramount. Cisco Secure Firewall stands as a robust defense mechanism, offering:

- **Advanced Threat Protection**: Integrates with Cisco Talos for real-time threat intelligence, ensuring proactive defense against emerging threats.
- **Flexible Deployment**: Available as physical appliances, virtual instances, or cloud-native solutions, catering to diverse organizational needs.
- **Centralized Management**: Utilizes Cisco Defense Orchestrator for streamlined policy management across multiple firewalls.

By providing deep visibility and control over network traffic, Cisco Secure Firewall empowers organizations to enforce security policies effectively and respond swiftly to incidents.

2. Cisco Identity Services Engine (ISE): Intelligent Access Control

Ensuring that only authorized users and devices access network resources is critical. Cisco ISE offers:

- **Context-Aware Access**: Analyzes user roles, device types, and locations to enforce granular access policies.

- **Device Profiling**: Automatically identifies and classifies devices, enhancing visibility and control.

- **Guest Access Management**: Facilitates secure onboarding of guest users without compromising network integrity.

Cisco ISE serves as a centralized policy engine, enabling organizations to implement consistent access controls and maintain compliance with regulatory standards.

3. Cisco Umbrella: Cloud-Delivered Security

As organizations embrace cloud services, securing internet access becomes vital. Cisco Umbrella provides:

- **DNS-Layer Protection**: Blocks malicious domains before connections are established, preventing threats at the earliest stage
- **Secure Web Gateway**: Offers URL filtering and malware protection for web traffic.
- **Cloud Access Security Broker (CASB)**: Monitors and controls the use of cloud applications, mitigating shadow IT risks.

By delivering security from the cloud, Cisco Umbrella ensures consistent protection for users, regardless of their location.

4. Cisco SecureX: Unified Security Platform

Managing multiple security tools can be complex. Cisco SecureX simplifies this by:

- **Integrating Security Tools**: Connects Cisco and third-party solutions for cohesive threat detection and response.
- **Automating Workflows**: Streamlines routine tasks, allowing security teams to focus on critical issues.
- **Providing Unified Visibility**: Offers a centralized dashboard for monitoring security events across the organization.

SecureX enhances operational efficiency and accelerates incident response, strengthening an organization's security posture.

5. Cisco AnyConnect Secure Mobility Client: Secure Remote Access

With remote work becoming commonplace, secure connectivity is essential. Cisco AnyConnect offers:

- **VPN Services**: Ensures encrypted communication between remote users and corporate networks.
- **Endpoint Compliance**: Verifies device health before granting access, maintaining security standards.

- **Seamless User Experience**: Provides consistent access across various devices and platforms.

AnyConnect enables organizations to support a mobile workforce without compromising security.

6. Cisco Secure Workload (Tetration): Application-Centric Security

Protecting applications across hybrid environments is challenging. Cisco Secure Workload addresses this by:

- **Micro-Segmentation**: Implements fine-grained policies to isolate workloads and prevent lateral movement of threats.
- **Application Dependency Mapping**: Visualizes interactions between applications, aiding in risk assessment.
- **Compliance Monitoring**: Continuously assesses adherence to security policies and regulatory requirements.

By focusing on workload security, Cisco helps organizations safeguard critical applications in dynamic environments.

7. Cisco Duo Security: Strengthening Authentication

User credentials are often targeted by attackers. Cisco Duo enhances authentication through:

- **Multi-Factor Authentication (MFA)**: Requires additional verification methods beyond passwords
- **Device Trust**: Ensures that only secure, compliant devices can access resources.
- **Adaptive Policies**: Adjusts authentication requirements based on user behavior and risk levels.

Duo Security fortifies access controls, reducing the risk of unauthorized access.

8. Cisco's Transformative Impact on Networking

Beyond individual solutions, Cisco is reshaping the networking landscape through:

- **Secure Access Service Edge (SASE)**: Combines networking and security functions into a unified cloud service, supporting the modern workforce.
- **Zero Trust Architecture**: Adopts a "never trust, always verify" approach, ensuring continuous validation of users and devices.
- **Artificial Intelligence Integration**: Leverages AI to enhance threat detection, automate responses, and optimize network performance.

Cisco's holistic approach addresses the evolving challenges of digital transformation, enabling organizations to build resilient, secure networks.

Cisco's comprehensive suite of security solutions demonstrates its commitment to protecting the digital infrastructure of organizations worldwide. By integrating advanced technologies and adopting forward-thinking architecture, Cisco not only addresses current security challenges but also anticipates future needs, solidifying its role as a leader in the networking domain.

1.3 Information Security – Vendor, Contract and Change Management

Vendor and Contract Management in Information Security: Aligning with ISO 27001, NIST, and SOC 2 Introduction - In today's interconnected digital landscape, organizations increasingly rely on third-party vendors to deliver essential services, ranging from cloud storage to customer support. While this collaboration offers numerous benefits, it also introduces significant information security risks. A single vulnerability in a vendor's system can compromise an organization's data integrity, confidentiality, and availability.
Recognizing these challenges, frameworks like **ISO 27001**, **NIST**, and **SOC 2** emphasize the importance of robust vendor and contract management. These standards provide guidelines to ensure that third-party engagements do not become the weakest link in an organization's security posture.

This report delves into the intricacies of vendor and contract management within the realm of information security, offering insights into best practices and strategies to align with these prominent standards.

Understanding Vendor Management in Information Security
Vendor management refers to the systematic process of overseeing third-party service providers to ensure they meet an organization's expectations, particularly concerning information security. This includes:

- **Vendor Selection**: Evaluating potential vendors based on their security practices, compliance certifications, and overall risk profile

- **Risk Assessment**: Identifying and analyzing potential risks associated with vendor relationships.
- **Contractual Agreements**: Establishing clear terms that define security requirements, responsibilities, and consequences for non-compliance.
- **Ongoing Monitoring**: Regularly reviewing vendor performance and compliance to ensure continued alignment with security standards.

Contract Management: The Foundation of Secure Vendor Relationships

Effective **contract management** is pivotal in setting the tone for secure vendor engagements. Key components include:

- **Security Clauses**: Contracts should explicitly state the security measures vendors must implement, referencing relevant standards like ISO 27001 or SOC 2.
- **Compliance Requirements**: Vendors should be obligated to maintain specific certifications or undergo regular audits to verify compliance.
- **Data Protection Provisions**: Clearly define how data will be handled, stored, and protected, including protocols for breach notifications.
- **Termination Clauses**: Outline procedures for data retrieval and destruction upon contract termination to prevent unauthorized access.

Aligning with ISO 27001

ISO 27001 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). When it comes to vendor management, ISO 27001 emphasizes:

- **Annex A.15 – Supplier Relationships**: This section mandates organizations to ensure that security requirements are addressed in agreements with suppliers and that these requirements are met.
- **Risk-Based Approach**: Organizations should assess the risks associated with supplier access to organizational assets and implement appropriate controls.
- **Monitoring and Review**: Regularly monitor and review supplier services to ensure compliance with agreed-upon security requirements.

Aligning with NIST

The **National Institute of Standards and Technology (NIST)** provides a comprehensive framework for improving critical infrastructure cybersecurity. Key aspects related to vendor

management include:

- **Supply Chain Risk Management (SCRM)**: NIST emphasizes the importance of understanding and managing risks associated with the supply chain, including third-party vendors.
- **Security Controls (SP 800-53)**: This publication outlines specific controls for managing third-party risks, such as access restrictions, audit mechanisms, and incident response protocols.
- **Continuous Monitoring**: Organizations are encouraged to implement ongoing assessments of vendor security practices to detect and address vulnerabilities promptly.

Aligning with SOC 2

SOC 2 reports focus on a service organization's controls relevant to security, availability, processing integrity, confidentiality, and privacy. In the context of vendor management:

- **Third-Party Oversight**: Organizations must demonstrate that they have controls in place to manage third-party risks effectively.
- **Due Diligence**: Before engaging with vendors, organizations should assess their security posture, including reviewing SOC 2 reports or other relevant certifications.
- **Contractual Obligations**: Contracts should stipulate the security and compliance expectations from vendors, ensuring alignment with the organization's own SOC 2 requirements.

Best Practices for Effective Vendor and Contract Management

To ensure robust vendor and contract management aligned with ISO 27001, NIST, and SOC 2:

1. **Develop a Comprehensive Vendor Management Policy**: Document procedures for vendor selection, risk assessment, contract negotiation, and performance monitoring.I.S.
2. **Implement a Risk-Based Approach**: Prioritize vendors based on the sensitivity of the data they handle and the criticality of the services they provide.
3. **Conduct Regular Audits and Assessments**: Periodically evaluate vendor compliance through audits, questionnaires, and performance reviews
4. **Foster Open Communication**: Maintain transparent communication channels with vendors to address concerns and share updates on security requirements.
5. **Leverage Technology Solutions**: Utilize vendor risk management tools to streamline

assessments, monitor compliance, and manage documentation.

In an era where third-party collaborations are integral to business operations, ensuring that these relationships do not compromise information security is paramount. By adopting structured vendor and contract management practices aligned with standards like ISO 27001, NIST, and SOC 2, organizations can mitigate risks, ensure compliance, and build resilient partnerships. The strength of your organization's security is not only determined by internal measures but also by the security posture of your vendors.

1.4 Hardware and Software Requirements for IDPS

Implementing an effective Cyber Security Lab necessitates a robust combination of hardware and software components to ensure reliability, scalability, and real- time performance.

Hardware Requirements

1. **Processor:** A multi-core processor like Intel Core i7 or AMD Ryzen 7 to manage real-time data processing and communication tasks.
2. **Memory (RAM):** Minimum 16GB RAM to handle large datasets and simultaneous processing demands.
3. **Storage**: At least 512GB SSD for faster data retrieval and storage of cyber records and emergency logs.
4. **GPS Module**: Integrated GPS for accurate location tracking of s, ambulances, and hospitals.
5. **Wearable Devices**: Affordable smartwatches equipped with health sensors for continuous monitoring and emergency alerts.
6. **Network**: Stable and secure internet connectivity to facilitate real-time communication and data exchange.

Software Requirements

1. **Operating System**: Windows 10/11, Ubuntu 20.04, or Android/iOS for mobile applications.
2. **Programming Language:** Python for backend processing and Java/Kotlin for Android app development.

3. **Virtual Machines:** VM's for isolating test environments and creating sandboxes for testing
4. **API Integration:** Google Maps API for location tracking and routing services Version

1.5 System Design and Implementation

The Cyber Emergency Handling System comprises three core modules: data acquisition and preprocessing, real-time monitoring and response, and resource management.

1. **Data Acquisition and Preprocessing:** This module collects and processes data from Firewall Logs. It ensures data consistency and accuracy through validation and normalization techniques. A centralized database collects and aggregates data in real time. APIs are used to enable communication between applications, and the central system. The raw data is cleaned, standardized, and formatted to remove inconsistencies, handle missing values, and ensure compatibility across different platforms.
2. **Real-Time Monitoring and Response**: This component facilitates instant communication between users and emergency services. It includes features like real- time alerts, and automated emergency notifications. Automated triggers are set up to notify users, admins or first responders when certain thresholds are exceeded.
3. **Resource Management**: Leveraging predictive analytics, this module optimizes the allocation of cyber resources, staff deployment, and routing of emergency alerts to minimize response times. The system keeps track of available hospital beds, cyber equipment, ambulance locations, and blood bank stocks in real time. AI-driven models prioritize resource allocation based on proximity, severity, and resource availability. Cloud-based infrastructure ensures that resource data from multiple facilities can be updated and accessed without bottlenecks.

The implementation process involves iterative development, continuous testing, and integration of feedback to refine system functionalities. Cross-platform compatibility, secure
data handling, and user-friendly interfaces are prioritized to enhance system efficiency and user adoption.

1.6 Data Management and Feature Extraction

Data plays a pivotal role in the effectiveness of the Cyber IDPS lab. The system utilizes diverse datasets, including uptime metrics, network traffic capacity data, and blood bank inventories, to inform decision-making.

Data:

In today's highly digital and interconnected world, the threat landscape is expanding at an unprecedented rate. As a response, organizations are increasingly deploying Intrusion Detection and Prevention Systems (IDPS) to monitor, analyze, and defend against malicious activity. At the core of these systems are two essential processes: data management and feature extraction. These components form the building blocks of intelligent and responsive cybersecurity systems. Like the human nervous system collecting and interpreting signals to detect harm, IDPS relies on managing data effectively and extracting the right features from it to detect threats. This document aims to provide a comprehensive understanding of these two critical elements and their role in maintaining effective network security.

Data Management in IDPS

1. Data management within IDPS refers to the structured and efficient handling of the enormous volume of data generated in a digital environment. It encompasses the collection, preprocessing, storage, and governance of data in a way that becomes useful for analysis. Good data management ensures that the data fed into IDPS is relevant, clean, and timely, which directly impacts the system's ability to detect and prevent intrusions accurately. Without reliable data management, even the most sophisticated detection algorithms can falter, leading to false positives or undetected attacks.
2. Data Collection

   The first step in data management is data collection, which involves gathering information from various sources in the network infrastructure. These sources include network traffic (using packet sniffers), system and application logs, firewall data, and user activity logs. Data collection tools such as Wireshark, Bro/Zeek, NetFlow, and SNMP agents play a significant role in capturing these raw data points. This raw data forms the foundation upon which all subsequent analysis is based, so it must be comprehensive and representative of all relevant network activity.

3. Data Preprocessing

   Once data is collected, it often contains noise, redundancy, or incomplete records that can hinder analysis. Data preprocessing is the phase where these imperfections are addressed. This involves cleaning the data by removing irrelevant or duplicate entries, normalizing different data formats for consistency, aggregating events into meaningful summaries, and labeling data points for supervised learning scenarios. Preprocessing transforms raw data into a structured format that is ready for deeper analysis, significantly improving the accuracy and speed of intrusion detection.

4. Data Storage

   The storage of processed data is another crucial aspect of data management. Given the volume and velocity of data in large networks, storage solutions must be scalable, secure, and optimized for quick retrieval. Organizations often use data lakes, SIEM (Security Information and Event Management) systems, or time-series databases to store this information. Storage solutions must also support encryption, access control, and integrity verification to ensure the data remains untampered and confidential. Efficient storage is essential for supporting both real-time analysis and historical investigations.

5. Data Retention and Privacy

   Data retention policies dictate how long data is stored and when it should be deleted. These policies must strike a balance between the need for long-term analysis and compliance with privacy laws such as GDPR, HIPAA, or local data protection regulations. Organizations must ensure that data is anonymized where appropriate, access is restricted to authorized personnel, and data destruction is handled securely. Mismanagement in this area can lead to regulatory penalties and loss of customer trust.

6. Feature Extraction in IDPS

   Feature extraction is the process of identifying and isolating meaningful attributes from the collected data that can help distinguish between normal and malicious activities. It is similar to how forensic investigators look for specific clues at a crime scene. Good feature extraction allows IDPS to recognize subtle signs of intrusion that would otherwise be buried in the volume of data. This process is vital for enabling machine learning models or rule-based systems to make accurate predictions and decisions.

7. Basic Features

   Basic features are straightforward attributes that can be directly extracted from the raw data. These typically include IP addresses, port numbers, protocol types, and packet sizes. These features are often the first indicators of network behavior and are especially useful

in identifying anomalies like port scanning or IP spoofing. Because of their simplicity, basic features can be extracted quickly and used in real-time monitoring systems.

8. Time-Based Features

Time-based features consider how network behaviors change over specific intervals. These may include the number of connections initiated by an IP address in a two-second window, the duration of a session, or the rate of failed login attempts. These temporal metrics are useful for detecting Denial-of-Service (DoS) attacks, brute-force attempts, or bot activity. By analyzing time-based patterns, IDPS can identify deviations from normal usage that suggest malicious intent.

9. Content-Based Features

Content-based features delve into the payload or content of network packets or log files. These features include specific keywords, command execution patterns, or embedded scripts in data packets. Such features are crucial in identifying SQL injections, cross-site scripting (XSS), or malware signatures. Content-based analysis is more resource-intensive but offers deeper insight into what the data is actually doing, not just how it behaves.

10. Traffic Features

Traffic features provide insights into the volume and direction of data moving through a network. These features include the total bytes transmitted in a session, the number of requests from a particular host, or the ratio of incoming to outgoing data. Monitoring traffic features helps in detecting data exfiltration, bandwidth abuse, or unusual traffic spikes that might indicate a compromised system.

11. Statistical Features

Statistical features apply mathematical computations to summarize and quantify the behavior of network data. Examples include the entropy of a packet size distribution, the variance in inter-packet arrival times, or correlation coefficients between different traffic metrics. These features are particularly useful in machine learning models, where patterns and outliers can indicate potential security

12. Feature Selection vs. Feature Extraction

While feature extraction involves creating or identifying relevant attributes from raw data, feature selection is about choosing the most impactful ones. Not all extracted features contribute equally to intrusion detection. Feature selection uses methods such as mutual information, correlation analysis, or principal component analysis (PCA) to retain only the most valuable features. This helps reduce computational overhead, avoid overfitting in machine learning models, and enhance the overall performance of the IDPS.

13. Role in Machine Learning-Based IDPS

    In machine learning-driven IDPS, feature extraction becomes even more critical. Supervised learning models require labeled datasets where extracted features correspond to known attack types or normal behavior. Unsupervised models rely on clustering or anomaly detection, where features must effectively differentiate between benign and suspicious activities. Common algorithms include decision trees, random forests, support vector machines (SVM), and neural networks. High-quality features directly translate to higher detection accuracy and lower false positive rates.

14. Real-World Challenges and Considerations

    Implementing effective data management and feature extraction is not without its challenges. The sheer volume of data can overwhelm storage and analysis systems. Labeling data for supervised learning is labor-intensive and often incomplete. False positives and negatives can lead to alert fatigue or missed threats. Moreover, analyzing user behavior or deep packet content raises privacy concerns. Organizations must navigate these challenges by investing in scalable infrastructure, skilled personnel, and ethical data practices.

15. Best Practices for Implementation

    To optimize IDPS performance, organizations should adopt several best practices. First, domain knowledge should guide feature engineering, as cybersecurity professionals can identify threat indicators that automated systems might miss. Second, feature sets should be periodically reviewed and updated to adapt to evolving threats. Third, combining data from multiple sources—such as network traffic, host activity, and user behavior—can provide richer context for detection. Finally, automation tools should be used to streamline preprocessing and feature extraction, especially in environments requiring real-time threat detection.

Data management and feature extraction are foundational to the effectiveness of Intrusion Detection and Prevention Systems. These processes transform raw, chaotic data into structured, actionable intelligence, enabling IDPS to detect and respond to threats with speed and accuracy. As cyber threats continue to evolve, mastering these aspects becomes not just a technical necessity but a strategic imperative. With the right approach, organizations can build resilient security architectures capable of withstanding the complex and dynamic challenges of the digital age.

1.7 System Evaluation and Performance Metrics

The system's effectiveness is evaluated using key performance metrics:

1. **Response Time**: This metric measures the duration between alert generation and the initiation of an emergency response. A shorter response time is crucial in cyber emergencies to increase survival rates and minimize health complications. The system continuously optimizes algorithms and resource deployment to reduce response delays.
2. **Accuracy**: This assesses the precision of location tracking for devices and IP's ensures that the right cyber aid reaches the promptly, reducing the chances of misdirection and resource wastage.
3. **Reliability:** Reliability focuses on the system's uptime, fault tolerance, and error rates in data processing. A highly reliable system must operate seamlessly under high demand, ensuring uninterrupted service and consistent performance during emergencies. Regular system audits, maintenance, and redundancy mechanisms are implemented to maximize reliability.
4. **User Satisfaction:** User satisfaction is evaluated through feedback regarding system usability, interface design, response efficiency, and overall effectiveness. Surveys, user testing, and feedback loops help identify areas for improvement, ensuring the system meets user needs and expectations.

Continuous monitoring and performance assessments ensure that the system remains responsive, accurate, and efficient. Regular updates and maintenance enhance system reliability and adapt to evolving emergency scenarios.

1.8 Model Building and Training

Network Security involves building and training predictive models to enhance emergency response effectiveness. This process includes:

The development of the labs involves building and training predictive models to enhance emergency response effectiveness. This process includes:

1. Data Collection: Gathering diverse data from firewalls, logs, emergency alert logs, and forming a comprehensive dataset.

2. Data Preprocessing: Cleaning, normalizing, and encoding data to remove inconsistencies, handle missing values, and ensure quality input for models.
3. Feature Engineering: Designing relevant features such as vitals trends and emergency frequency to improve model predictions.
4. Model Selection: Testing algorithms like Random Forest, Gradient Boosting, and Neural Networks to determine the most effective for specific prediction tasks.
5. Training and Validation: Dividing datasets into training, validation, and testing subsets to evaluate model Hyperparameter Tuning: Fine-tuning learning rates, tree depths, and regularization techniques to optimize model accuracy and efficiency.
6. Model Evaluation: Measuring performance using accuracy, precision, recall, and F1-score to ensure reliability and safety.
7. Deployment and Monitoring: Deploying models into the live system with ongoing monitoring, updates, and performance tracking.
8. performance and prevent overfitting.

By addressing these challenges and incorporating advanced technologies, the system aims to set new standards in emergency management, Threat alerts ultimately saving lives and improving healthcare outcomes.

1.9 Supervised Models for Intrusion Detection and Prevention

Supervised machine learning models play a vital role in predicting and managing threats by learning from signatures and historical data with known outcomes. These models are trained on labelled datasets that include signature-based detection, firewall rules and emergency response records to identify patterns and predict future incidents.

Common supervised models used in cyber emergency handling include:

1. **Logistic Regression:** Ideal for binary classification tasks, such as predicting whether a is at risk of a heart attack based on vital signs. A statistical model used for binary or multiclass classification problems. It predicts probabilities using a sigmoid function.
2. **Decision Trees:** Used for making quick, rule-based decisions, like prioritizing ambulance dispatch based on condition and location. A tree-like model that splits data into branches based on feature thresholds, leading to a classification or regression output.

3. **Random Forest:** An ensemble model that improves prediction accuracy by combining multiple decision trees, useful for forecasting hospital resource needs. An ensemble learning method that combines multiple decision trees to improve prediction accuracy and reduce overfitting. Each tree is trained on a random subset of data and features.
4. **Gradient Boosting Machines (GBM):** Effective for handling complex patterns and imbalanced data, making it suitable for predicting rare but critical emergencies. An advanced ensemble method that builds trees sequentially, where each new tree focuses on correcting errors made by the previous ones. It uses gradient descent to optimize predictions.
5. **Support Vector Machines (SVM):** Utilized for classifying emergency severity levels by analyzing multidimensional data.

These models enhance real-time decision-making, optimize resource allocation, and improve the accuracy of emergency predictions, ultimately saving lives and reducing response times.

1.10 Challenges and Future Enhancements

While the Cyber Emergency Handling System offers numerous advantages, it faces challenges such as data privacy concerns, integration complexities with existing healthcare infrastructures, and the need for continuous updates to handle new types of emergencies. Future enhancements may include:

1. **AI-Powered Predictive Analytics**: Utilizing machine learning algorithms to analyse historical health and emergency data, enabling the system to predict and prevent potential emergencies. This proactive approach can help in resource planning and early interventions, ultimately improving outcomes.
2. **Blockchain for Data Security:** Implementing blockchain technology to ensure secure, transparent, and tamper-proof handling of sensitive cyber data. This enhances data integrity, prevents unauthorized access, and builds trust among users and healthcare providers.
3. **Integration with Smart Cities:** Connecting the system with smart city infrastructure, such as IoT-enabled traffic management and surveillance systems, to streamline emergency responses. This integration allows for real-time traffic control for ambulances and better coordination with urban emergency services, ensuring quicker and more efficient responses.

CHAPTER – 2

PROPOSED METHODOLOGY

In a world where cyber threats are growing in frequency, sophistication, and impact, organizations require a robust and proactive approach to defending their digital environments. The Security Operations Center (SOC) has emerged as a cornerstone of modern cybersecurity strategy. A SOC acts as the central hub for monitoring, detecting, analyzing, and responding to cybersecurity incidents in real-time. It is designed to defend not only the network infrastructure but also individual endpoints and servers, which are common entry points for attackers. This report explores the structure, functions, and strategic value of SOCs, with a focus on their role in protecting networks, servers, and endpoint devices from cyber threats.

2.1 Understanding the Security Operations Center (SOC)

A Security Operations Center is a dedicated facility that houses a team of information security professionals responsible for continuously monitoring and improving an organization's security posture. The SOC functions around the clock, analyzing data from firewalls, intrusion detection systems (IDS), antivirus software, and endpoint detection and response (EDR) tools. The goal is to identify and respond to security incidents swiftly before they can escalate into significant breaches. The SOC team includes SOC analysts, incident responders, threat hunters, and SOC managers, each playing a vital role in ensuring effective security operations.

Modern SOCs often operate in a layered environment, integrating people, processes, and technologies. This integration enables the SOC to centralize threat intelligence, manage logs from diverse systems, and provide an organized response to incidents. By creating a unified view of an organization's cybersecurity status, SOCs enhance decision-making and promote resilience against attacks.

2.2 SOC's Role in Network Security

The SOC's primary responsibility in network security is to provide real-time monitoring and threat detection across all network layers. Through the use of tools such as Security Information and Event Management (SIEM) systems, Intrusion Detection and Prevention Systems (IDPS),

and Network Traffic Analysis (NTA) platforms, the SOC team maintains constant visibility into network activity. These tools aggregate logs and telemetry from routers, switches, firewalls, and cloud environments to detect suspicious behavior.

Anomalies such as abnormal data flows, repeated failed login attempts, or the presence of malware signatures trigger alerts in the SOC. SOC analysts then investigate these alerts to determine whether they represent legitimate threats or false positives. If a threat is confirmed, the SOC coordinates a response, which may include isolating affected systems, applying patches, or blocking malicious IP addresses. By monitoring network traffic continuously, the SOC ensures that attacks such as Distributed Denial-of-Service (DDoS), man-in-the-middle (MitM), and advanced persistent threats (APTs) are detected and mitigated in a timely manner.

2.3 SOC's Role in Server Security

Servers are critical assets that store and process sensitive information. As such, they are frequent targets of cyberattacks. The SOC plays a crucial role in protecting these servers by monitoring server logs, file integrity, user access, and system processes. Servers running databases, applications, or email services generate extensive logs that are analyzed for signs of exploitation, unauthorized access, or data exfiltration.

One of the key tools used by SOCs for server protection is Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solutions that provide real-time telemetry from server endpoints. These tools can identify suspicious behaviors such as privilege escalation, unusual process execution, or attempts to disable security controls. The SOC team correlates this data with threat intelligence feeds and known indicators of compromise (IOCs) to rapidly detect and respond to threats.

In addition, SOCs ensure that servers adhere to security configurations, conduct regular vulnerability assessments, and enforce patch management. This proactive stance minimizes the attack surface and ensures that servers remain resilient to known vulnerabilities. Moreover, in the event of a breach, the SOC coordinates forensic investigations to understand the root cause and improve defenses.

2.4 SOC's Role in Endpoint Security

Endpoints such as desktops, laptops, smartphones, and IoT devices represent the front lines of cybersecurity. They are the most exposed part of an organization's network and are often the first point of entry for attackers. The SOC ensures endpoint security by integrating advanced EDR solutions that monitor user behavior, application activity, and system health in real-time.

Through behavioral analytics, SOCs can detect deviations from normal usage patterns that might indicate a compromised device or insider threat. For example, if a user begins downloading large volumes of data at odd hours or accesses systems they typically do not use, the SOC is alerted. These alerts are investigated for potential signs of malware, phishing, ransomware, or insider attacks.

To further enhance endpoint security, SOCs enforce endpoint hardening policies, manage antivirus and anti-malware solutions, and ensure that only authorized software is installed. They may also use Mobile Device Management (MDM) systems to secure endpoints that operate outside the corporate firewall. By maintaining real-time oversight and rapid response capabilities, the SOC significantly reduces the likelihood of endpoint-based breaches.

2.5 Threat Intelligence and Correlation

A key advantage of SOCs is their ability to leverage threat intelligence for proactive defense. Threat intelligence refers to the collection and analysis of data about existing and emerging threats. SOCs utilize internal data, external feeds, and shared intelligence communities to gain insights into the tactics, techniques, and procedures (TTPs) used by attackers.

This intelligence is fed into correlation engines that help identify patterns across network, server, and endpoint data. For instance, a malware signature identified on an endpoint might correlate with network traffic to a known malicious domain, triggering an alert for a broader attack campaign. The SOC’s ability to correlate diverse datasets enables a holistic understanding of attacks and facilitates coordinated responses.

2.6 Incident Response and Recovery

When a security incident is detected, the SOC takes the lead in executing the organization’s incident response plan. This includes containment (isolating infected systems), eradication (removing malware or malicious users), recovery (restoring services), and post-incident analysis (understanding root causes and improving defenses). The SOC maintains playbooks and

workflows to ensure a structured and efficient response.

Timely incident response minimizes downtime, prevents data loss, and maintains business continuity. In critical scenarios such as ransomware attacks, the SOC works with legal and compliance teams to navigate regulatory obligations and communicate with stakeholders. Recovery efforts are guided by backup policies, disaster recovery plans, and coordinated efforts between IT and security teams.

2.7 Compliance and Reporting

SOCs also play a vital role in helping organizations comply with industry regulations and standards such as ISO 27001, NIST CSF, SOC 2, GDPR, and HIPAA. These frameworks require continuous monitoring, documented incident response, and evidence of risk management. The SOC provides the infrastructure to meet these requirements through automated logging, audit trails, and real-time reporting.

SOC dashboards and reports offer insights into threat landscapes, system vulnerabilities, incident trends, and remediation efforts. These reports are valuable for internal audits, executive briefings, and regulatory submissions. Through transparent reporting, the SOC helps build trust among stakeholders and demonstrates a mature cybersecurity posture.

2.8 Challenges in Operating a SOC

Operating a SOC comes with its own set of challenges. These include managing alert fatigue, recruiting skilled personnel, keeping up with evolving threats, and integrating diverse tools. False positives can overwhelm analysts, leading to delayed responses or missed attacks. Organizations must invest in automation, artificial intelligence, and training to enhance efficiency and reduce human error.

Furthermore, the cost of building and maintaining a 24/7 SOC can be high, prompting some organizations to opt for managed SOC services (MSSPs) or hybrid models. These models offer scalability and access to specialized expertise but require strong governance and integration with internal IT teams.

A Security Operations Center is an indispensable asset in today's cybersecurity ecosystem. It provides centralized visibility, rapid threat detection, and coordinated response across networks, servers, and endpoints. By continuously monitoring digital environments, leveraging threat intelligence, and enforcing security policies, the SOC acts as a guardian of organizational assets.

Its contributions are vital not only in preventing breaches but also in fostering resilience, compliance, and strategic risk management. As the threat landscape continues to evolve, the SOC will remain a foundational element of effective and proactive cybersecurity defense.

2.9 Understanding GRC and Information security

Information Security and the Implementation of ISO 27001, ISMS, SOC 2, and Related Standards In an increasingly digital and interconnected world, information has become one of the most valuable assets an organization possesses. Protecting this information from unauthorized access, alteration, theft, or destruction is not only a matter of operational necessity but also a critical requirement for maintaining stakeholder trust and regulatory compliance.

As cyber threats continue to grow in sophistication and scale, organizations can no longer rely on ad hoc or siloed defenses. Instead, they must adopt comprehensive, strategic, and structured approaches to information security. Frameworks such as ISO/IEC 27001, Information Security Management Systems (ISMS), SOC 2, and the NIST Cybersecurity Framework have emerged as essential tools for building, maintaining, and demonstrating robust security postures. These frameworks offer guidance not just on technological controls, but on governance, processes, and cultural alignment needed to protect critical assets and ensure business continuity.

2.10 ISO 27001 ISMS Implementation

ISO/IEC 27001, widely recognized across industries and geographies, provides a systematic approach to managing sensitive company information. It mandates the development and implementation of an Information Security Management System (ISMS), which encompasses policies, procedures, and controls that align with business needs and risk appetites. The implementation journey typically begins with defining the scope of the ISMS—deciding whether it applies to the entire organization or specific departments, geographies, or services. This is followed by a rigorous risk assessment process, identifying threats, vulnerabilities, potential impacts, and risk levels associated with key assets. Based on this analysis, risk treatment plans are devised, and controls are selected from Annex A of the ISO 27001 standard, which contains 114 controls across 14 domains such as access control, cryptography, supplier relationships, and information transfer.

What sets ISO 27001 apart is its emphasis on continual improvement and integration into the organization's strategic and operational framework. After controls are implemented, organizations conduct internal audits, management reviews, and corrective actions to assess performance and drive improvements. The culmination of this process is third-party certification, which validates the organization's commitment to information security and builds credibility with clients, partners, and regulators. ISO 27001 doesn't merely promote reactive defenses; it fosters a culture of proactive risk management, compliance, and information governance.

2.11 SOC 2 Type 2

Parallel to ISO 27001, SOC 2 has gained prominence, particularly among service-oriented and technology firms in North America. Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 assesses an organization's ability to manage data based on five Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. Unlike ISO 27001, which focuses on creating a comprehensive management system, SOC 2 concentrates on how specific systems and services handle customer data. There are two types of SOC 2 reports—Type I assesses design effectiveness at a point in time, while Type II evaluates the operational effectiveness of controls over a longer period.

The process of achieving SOC 2 compliance involves scoping the systems, identifying relevant trust principles, mapping existing controls, and implementing mechanisms to collect evidence of control effectiveness. Continuous monitoring is essential in demonstrating that controls are functioning as intended. For cloud service providers, SaaS platforms, and managed service vendors, a SOC 2 report is often a non-negotiable requirement for enterprise clients. It serves not just as a technical validation but as a strategic asset in vendor assessments and partnership discussions.

Though ISO 27001 and SOC 2 have different origins and emphases, they share several fundamental principles. Both require governance structures, risk assessments, incident response plans, monitoring systems, and regular reviews. Many organizations implement them concurrently or integrate their controls into a Unified Control Framework (UCF), which harmonizes requirements from multiple standards, including GDPR, HIPAA, and PCI-DSS. This integrated approach not only streamlines compliance but also reduces duplication of efforts and enhances operational efficiency.

In addition to ISO and SOC 2, the National Institute of Standards and Technology (NIST) offers another valuable framework, particularly in the United States. The NIST Cybersecurity Framework (CSF) is structured around five core functions: Identify, Protect, Detect, Respond, and Recover. These functions are designed to help organizations understand their current cybersecurity posture, set goals for improvement, and develop action plans. Unlike prescriptive standards, the NIST CSF is flexible and scalable, making it suitable for organizations of all sizes and maturity levels. It is particularly useful for aligning cybersecurity activities with business objectives and regulatory requirements.

The integration of these frameworks—ISO 27001 for holistic management systems, SOC 2 for customer data assurance, and NIST for operational alignment—provides a comprehensive foundation for information security governance. However, the journey to implementation is not without challenges. Many organizations face resource constraints, skill gaps, and resistance to change. Legacy systems may not support modern security requirements, and aligning diverse teams around new policies and processes can be difficult.

To overcome these obstacles, several best practices have emerged. Foremost among them is strong executive sponsorship. When leadership prioritizes security, allocates budget, and sets the tone from the top, the rest of the organization is more likely to follow suit. Cross-functional collaboration is also crucial; information security must be a shared responsibility among IT, HR, Legal, Compliance, and Operations. Automation and tooling can further ease the burden of implementation, especially when it comes to evidence collection, monitoring, and reporting. Security awareness training ensures that employees at all levels understand their roles in safeguarding information. Finally, regular assessments—be it internal audits, penetration tests, or external reviews—help organizations stay ahead of emerging threats and maintain compliance.

Ultimately, the value of implementing these frameworks goes beyond passing audits or obtaining certifications. They help organizations build resilience, earn stakeholder trust, and support sustainable growth. In today's risk-laden digital environment, clients, investors, and regulators are increasingly evaluating companies based on their security maturity. Adopting ISO 27001, SOC 2, and NIST not only protects critical data but also signals a commitment to ethical leadership and responsible governance.

In conclusion, information security is no longer a back-office IT function—it is a core business function with strategic implications. Implementing structured and internationally recognized frameworks like ISO/IEC 27001, ISMS, SOC 2, and NIST CSF enables organizations to move from reactive defense to proactive governance. These frameworks offer the guidance, tools, and structure needed to manage risks, enhance operational efficiency, and align cybersecurity initiatives with broader business objectives. In doing so, they turn security from a cost center into a value driver, helping organizations thrive securely in an era defined by digital innovation and persistent threats.

CHAPTER 3

OBJECTIVES

In today's digital-first environment, even small enterprises rely heavily on networks to carry out everyday operations—from sending emails and accessing cloud resources to hosting internal databases and managing customer interactions. A well-designed network acts as the backbone of a business, providing reliable, secure, and scalable connectivity across departments and locations. For aspiring network engineers, students, and IT professionals alike, the process of designing such networks may seem daunting at first. Thankfully, Cisco Packet Tracer—a simulation tool developed by Cisco Systems—makes it possible to model, test, and learn network configurations without requiring physical hardware. It gives users an immersive, risk-free space to explore, fail, and succeed while preparing them for real-world challenges.

3.1 Designing Small Enterprise Networks Using Cisco Packet Tracer

Cisco Packet Tracer is a multifaceted virtual lab that supports not only theoretical knowledge but hands-on learning. Through an intuitive drag-and-drop interface, users can simulate real networking hardware, such as routers, switches, servers, and end devices, as well as various cabling methods and wireless access points. One key strength of Packet Tracer lies in its ability to let learners visualize data flow and packet travel, providing immediate feedback on configurations. For example, a misconfigured IP address or subnet mask reveals its impact in real-time. The tool also supports scripting and automation, which makes it easier for students to understand emerging trends like intent-based networking and software-defined networking (SDN).

3.2 Network Planning and Design Principles

Before diving into a simulation, it is essential to understand the organization’s goals and networking needs. A small enterprise typically demands high availability, minimal latency, security, and the flexibility to scale operations without heavy investment. Good network design follows structured principles: hierarchical architecture (core, distribution, access layers), segmentation using VLANs for performance and security, and careful IP address planning to

avoid conflicts and inefficiencies. For instance, static IPs might be reserved for servers and printers, while DHCP dynamically assigns IPs to user devices. Planning also involves selecting the right routing protocols, defining failover paths, and setting quality of service (QoS) parameters where necessary to prioritize critical traffic like voice over IP (VoIP).

A practical small enterprise setup often consists of one or two routers to manage external connectivity, Layer 2 and Layer 3 switches for internal segmentation and efficient routing, and a variety of endpoints such as desktop computers, IP phones, wireless access points, and printers. Security appliances, either integrated or standalone, are introduced to enforce firewalls, VPNs, and content filtering.

3.3 Designing a Small Office Network in Packet Tracer

Consider a marketing firm with around 30 employees, divided into three departments—HR, Sales, and Administration. The network design begins with a core router that connects to the Internet Service Provider (ISP) and manages NAT (Network Address Translation) for outbound traffic. Behind the core router lies a Layer 3 switch that facilitates inter-VLAN routing.

Each department connects to its own access switch. VLAN10 is assigned to HR, VLAN20 to Sales, and VLAN30 to Admin. This segmentation ensures that broadcast domains are isolated and data privacy is upheld. DHCP is configured either on a central server or directly on the router to dynamically assign IP addresses within predefined subnets. A DNS server is also placed within the network for resolving internal and external domains, improving efficiency and reducing dependency on external name servers.

The wireless router offers limited access to guests by placing them in a separate VLAN (e.g., VLAN99), which is isolated from internal business traffic. Firewall rules, implemented either on the router or as ACLs on switches, further enhance security. These rules may block traffic between VLANs except for specific exceptions (e.g., allowing Admin to access HR records).

3.4 Security Considerations in Network Design

Security begins at the design stage. Within Packet Tracer, users can simulate essential security practices, such as configuring encrypted device management using SSH instead of Telnet, setting strong local authentication credentials, and deploying port security on switches to limit which

MAC addresses are allowed per port. ACLs (Access Control Lists) play a vital role in enforcing policy, for example, denying Sales VLAN users from accessing the HR file server or blocking incoming FTP traffic.

Packet Tracer allows for the simulation of these configurations so that learners can see the immediate effect of a security policy. For instance, misconfiguring an ACL might allow unauthorized access or block necessary traffic, and the simulator provides visual cues that help diagnose the issue. Additionally, features like SNMP (Simple Network Management Protocol) and Syslog servers can be used in more advanced simulations to replicate enterprise-level monitoring and alerting.

3.5 Monitoring and Troubleshooting Simulated Networks

Troubleshooting is where learners gain critical problem-solving skills. Packet Tracer provides tools to simulate both real-time and delayed packet movement, allowing users to trace issues step by step. For example, if a device isn't connected to the internet, users can check cable connections, interface statuses, IP settings, routing tables, and DNS resolutions. This process builds diagnostic intuition.

The simulation mode slows down packet movement so that users can view and analyze each protocol's packet structure—ICMP for pings, ARP for address resolution, or TCP for session establishment. This level of detail helps learners understand not only that something is wrong, but *why* it's wrong. Instructors can create troubleshooting labs that simulate real-life scenarios, such as DDoS attacks, broken routes, or DNS failures.

3.6 Scaling Up: Moving Beyond the Basics

Once learners master small enterprise design, they can gradually explore advanced topics such as MPLS, VPNs, and BGP configurations. While Cisco Packet Tracer has some limitations in replicating large-scale environments, the concepts practiced are directly applicable to real Cisco hardware and tools like Cisco DNA Center or Cisco SD-WAN.

Advanced Packet Tracer labs might include redundant links with HSRP (Hot Standby Router Protocol), multiple routing domains, inter-VLAN QoS policies, and IP SLA for measuring performance. These more complex labs allow learners to test high-availability configurations and prepare for real enterprise deployments. Packet Tracer also supports the use of IoT devices,

allowing simulations of smart offices with environmental controls, smart cameras, and security systems.

Designing small enterprise networks in Cisco Packet Tracer represents more than just passing a certification exam—it reflects the development of core engineering skills. By simulating real-world topologies, policies, and behaviors, users gain a deep understanding of how network components interact. This hands-on experience instills not just knowledge, but confidence.
As organizations continue their digital transformation journeys, the ability to build secure, efficient, and scalable networks becomes increasingly vital. Cisco Packet Tracer empowers learners and professionals to take the first steps toward that capability in a risk-free, educational environment. With a structured approach to design, a mindset for troubleshooting, and a strong grasp of security fundamentals, anyone can begin the journey toward becoming a network architect of tomorrow.

3.7 Centralized Contract and Vendor Management with Zoho Contracts

In today's complex and compliance-driven business environment, the importance of effective contract and vendor management cannot be overstated. Organizations frequently engage with multiple vendors, service providers, clients, and internal departments, all of which require precise, clear, and secure contractual arrangements. Managing these contracts manually or across disparate systems can lead to inefficiencies, missed deadlines, regulatory risks, and even data breaches. Zoho Contracts, a modern, cloud-based contract lifecycle management (CLM) platform, steps in to address these challenges by offering a centralized, secure, and intelligent system to streamline every phase of contract handling—from creation and negotiation to execution and renewal.

At the heart of Zoho Contracts is the idea of unifying the contract process under one secure umbrella. Businesses use it to digitize and automate routine contract-related tasks, ensuring standardized templates, controlled workflows, and easy collaboration among stakeholders. This significantly reduces the risks of non-compliance and contractual errors. Its integration with other Zoho services and third-party tools (like CRM and procurement platforms) enhances visibility and consistency across operations. What sets Zoho Contracts apart is its ability to monitor contract obligations, set automated alerts for renewals or expirations, and track historical changes with detailed version control, all while maintaining an auditable trail for governance purposes.

From a vendor management perspective, Zoho Contracts simplifies how organizations onboard and manage third-party providers. Contracts with vendors can be stored securely, tagged by category, and linked to specific procurement projects or business units. This central repository enables procurement and legal teams to quickly retrieve, evaluate, and review vendor performance metrics, SLAs, and compliance standards. The platform ensures that vendors operate under agreed-upon terms and are aligned with company goals and regulations. Moreover, the integration of approval workflows and e-signatures expedites the vendor onboarding and renewal cycles, minimizing delays and improving operational agility.

When it comes to information security, Zoho Contracts plays a vital role in safeguarding sensitive data. As businesses increasingly digitize their operations, ensuring data privacy and contractual confidentiality is paramount. Zoho Contracts is built with enterprise-grade security, including role-based access control, encrypted data transmission, secure audit trails, and compliance with industry standards like ISO/IEC 27001, GDPR, and SOC 2.

These features help ensure that contract-related data, especially those involving third parties, is not only protected from unauthorized access but also managed in compliance with legal and regulatory mandates. In the broader landscape of organizational governance, Zoho Contracts reinforces information security policies by ensuring that contract handling does not become a point of vulnerability. For example, it eliminates the use of unsecured email chains or local file transfers for contract exchange, thereby reducing the exposure to phishing or data leakage.

Instead, all contract interactions occur within a secure environment with detailed permissions and traceability. This is especially crucial in regulated industries like finance, healthcare, and technology, where contract mismanagement can result in fines, reputational damage, or litigation.

In conclusion, Zoho Contracts is more than just a digital paperwork tool—it is a strategic asset for businesses that want to manage contracts smartly, enhance vendor relationships, and maintain a high level of information security. Its centralized, automated, and compliance-oriented approach not only improves efficiency but also instills confidence among internal stakeholders, clients, and regulatory bodies. In an era where trust, speed, and compliance are key, platforms like Zoho Contracts are becoming indispensable to modern enterprise operations.

Chapter - 4

System Design and Implementation

In today's digital age, the threat landscape has become increasingly complex and dangerous. Organizations of all sizes face persistent risks from cybercriminals, insiders, and nation-state actors. To combat these threats, Intrusion Detection and Prevention Systems (IDPS) have emerged as essential components of enterprise cybersecurity architecture. IDPS technologies not only detect suspicious activity but also take action to block or prevent identified threats in real-time. However, the effectiveness of an IDPS depends largely on its design and implementation. A robust and well-integrated IDPS is the result of meticulous planning, architecture alignment, performance tuning, and continuous evaluation.

An Intrusion Detection and Prevention System combines two primary capabilities: detecting unauthorized access attempts (intrusion detection) and actively responding to them (intrusion prevention). There are several types of IDPSs, including network-based IDPS (NIDPS), host-based IDPS (HIDPS), wireless IDPS, network behavior analysis (NBA), and hybrid IDPS. Network-based IDPS monitors and analyzes traffic on a specific segment of the network, while host-based IDPS operates on individual hosts or devices to monitor system calls, file access, and process behavior. Wireless IDPS focuses on analyzing wireless network traffic for malicious behavior, and NBA identifies threats by examining network traffic to detect anomalies. Hybrid IDPS combines multiple approaches for a more comprehensive security posture. Each of these types contributes uniquely to the organization's defense strategy. A successful IDPS implementation often integrates multiple types for maximum coverage.

Designing an IDPS is not a one-size-fits-all endeavor. It involves understanding the organizational needs, existing infrastructure, threat profile, and regulatory environment. Requirement analysis is the first step, determining whether the IDPS should just monitor traffic or also block malicious activity, and whether it needs to support cloud, on-premises, or hybrid environments. Architecture design is another crucial factor, involving the choice between centralized versus decentralized architectures. Centralized systems simplify management but may introduce single points of failure, while decentralized systems offer resilience but can be complex to manage.

Sensor placement is a critical aspect of IDPS design. For network-based IDPS, sensors should be strategically placed at choke points such as gateways, DMZs, and internal segment boundaries to ensure maximum visibility. Integration with Security Information and Event Management (SIEM) platforms is equally important. The IDPS must be able to send alerts to a centralized SIEM for correlation, visualization, and response orchestration. This enhances situational awareness and streamlines incident response.

Scalability is another essential consideration. The system should be designed to accommodate future growth, whether through horizontal scaling (adding more nodes) or vertical scaling (adding capacity to existing nodes). High availability and redundancy are also vital. IDPS downtime can expose the organization to significant risks, so implementing failover mechanisms and redundant configurations ensures continuous protection.

In conclusion, the design and implementation of an IDPS require a thoughtful, strategic approach that aligns with organizational needs and threat landscapes. It is not merely about deploying tools, but about integrating them seamlessly into the broader cybersecurity ecosystem. By carefully considering architecture, scalability, integration, and redundancy, organizations can deploy an IDPS that not only defends against current threats but is also resilient and adaptable to future challenges.

CHAPTER – 5
Timeline for the Execution of Project

	Feb 03	Feb 27	Mar 23	Apr 16	May 10	June 03
Onboarding and Tools setup						
Infosec vendor KT						
Cisco Packet tracer network design						
Cisco Dcloud labs						
Vendor Contract migration to Zoho						
Vendor Due diligence for audit						
Audit external						
Audit Findings automation on JIRA						

The internship spanned from early February to early June, with structured activities and learning modules aligned across key weeks. The following is a breakdown of tasks and milestones based on the Gantt chart:

- Onboarding and Tools Setup (Week of Feb 03):
  The internship began with the standard onboarding process, which included setting up access to internal systems, tools, and communication platforms used by the organization.

- Infosec Vendor Knowledge Transfer (Feb 27 – Mar 23):
  During this period, I received in-depth knowledge about the organization's information security (Infosec) vendors. This included understanding their roles, services, and compliance responsibilities.
- Cisco Packet Tracer Network Design (Feb 27 – Mar 23):
  I worked on designing basic to intermediate network topologies using Cisco Packet Tracer. This helped in grasping core networking concepts and simulating real-world network scenarios.
- Cisco dCloud Labs (Feb 27 – Apr 16):
  Parallel to Packet Tracer, I engaged with Cisco dCloud labs—a cloud-based environment that provided practical, hands-on experience with enterprise-grade Cisco configurations and solutions.
- Vendor Contract Migration to Zoho (Mar 23 – Apr 16):
  I participated in the process of migrating vendor contract data into Zoho, a business automation tool. This task involved data organization, validation, and ensuring the correct tagging of vendor contracts.
- Vendor Due Diligence for Audit (Apr 16 – May 10):
  As part of the audit preparation, I assisted in performing due diligence checks on vendors. This included collecting and reviewing compliance documentation and assessing risk exposure.
- Audit Findings Automation on JIRA (Apr 16 – June 03):
  Toward the latter part of the internship, I contributed to automating audit findings and workflows using JIRA. This involved mapping audit issues to action items, setting up workflows, and ensuring proper tracking for follow-ups.

CHAPTER – 6

OUTCOMES

The onboarding and tools setup phase was crucial in familiarizing me with the internal IT ecosystem. I gained practical exposure to collaboration platforms, ticketing systems, VPN access, and basic administrative procedures. This foundation ensured I was equipped to effectively communicate and contribute within the company's workflow.

6.1 Vendor Management

Through the Infosec vendor knowledge transfer (KT) sessions, I developed a deeper understanding of third-party security providers, their roles in the cybersecurity landscape, and how vendor relationships are managed to ensure ongoing compliance and risk mitigation. I learned to interpret vendor security documentation and compliance reports such as ISO 27001 and SOC 2, which helped me appreciate the importance of aligning vendors with organizational security policies.

6.2 Network Design using CISCO PT

Working with Cisco Packet Tracer for network design was a hands-on technical exercise that sharpened my understanding of core networking concepts such as subnetting, VLAN configuration, routing, and device connectivity. I was able to simulate various network topologies, troubleshoot connectivity issues, and understand the practical application of theoretical network principles. This activity also served as a precursor to more advanced Cisco lab work.

Engaging with Cisco dCloud labs provided me with a cloud-based platform to explore real Cisco enterprise technologies in a sandbox environment. I experimented with advanced configurations such as next-generation firewalls, intrusion prevention systems (IPS), and identity-based access control using Cisco Identity Services Engine (ISE). These sessions allowed me to gain confidence in navigating enterprise-level tools and applying security principles in a safe, simulated environment.

My involvement in the vendor contract migration to Zoho deepened my appreciation for the administrative side of IT governance. I learned how to categorize and digitize vendor agreements, ensure metadata tagging for easier retrieval, and maintain version control. This experience reinforced the importance of accurate documentation and automation in managing large volumes of contractual data across departments.

The vendor due diligence task was particularly enlightening, as I actively participated in the preparation process for a compliance audit. I reviewed vendor responses to security questionnaires (e.g., VSQ), verified documentation against policy checklists, and collaborated with the compliance team to highlight any gaps. This enhanced my skills in risk assessment, critical thinking, and regulatory alignment.

6.3 Audit Finding automation

One of the most impactful parts of the internship was assisting with audit findings automation using JIRA. Here, I applied both technical and analytical skills to automate issue tracking and action items raised during audits. I created workflows, customized dashboards, and mapped responsibilities to relevant teams. This project demonstrated how agile practices and automation tools can streamline audit processes and improve organizational accountability.

Collectively, these tasks allowed me to bridge the gap between theoretical knowledge and practical implementation. I not only gained hands-on experience with industry-standard technologies like Cisco and Zoho, but also learned to appreciate the importance of security governance, audit preparedness, and effective vendor collaboration. These outcomes have strengthened my technical foundation and provided me with the skills, confidence, and perspective needed to contribute meaningfully to IT and cybersecurity teams in a professional setting.

The successful development and implementation of the **dcloud labs** have led to several significant outcomes that address critical challenges in emergency healthcare management. These outcomes contribute to enhancing response efficiency, improving care, and optimizing resource utilization.

6.4 Reduced Emergency Response Time

The integration of real-time GPS tracking for ambulances and resources has significantly reduced the response time during emergencies

6.5 Seamless Communication and Coordination

The unified platform ensures effective communication between hospitals, ambulances, blood banks, and emergency responders. Streamlined coordination has led to efficient resource allocation and improved handling of cyber emergencies.

6.6 Increased Accessibility for Vulnerable Populations

Affordable smartwatches and user-friendly mobile applications have made emergency services more accessible to and remote populations. Vulnerable groups now have timely access to cyber support, improving their safety and well-being.

6.7 Enhanced and Response

The mobile application provides step-by-step incident response instructions, empowering users to take immediate action during emergencies. Early intervention has increased the chances of stabilization before professional help arrives.

6.8 Efficient Resource Management During Large-Scale Emergencies

Predictive analytics and data-driven decision-making have optimized resource distribution during natural disasters and mass emergencies. This proactive approach has minimized resource shortages and ensured that critical areas receive prioritized support.

6.9 Real-Time Notifications and Alerts

Users receive real-time updates, and emergency protocols. Continuous updates keep users informed, enabling quick decision-making during emergencies.

6.10 Scalability and Adaptability of the System

The modular design allows the system to scale and adapt to various emergency scenarios, from individual incidents to large-scale disasters. Flexibility in deployment ensures the system remains effective across different emergency situations.

6.11 Contribution to Sustainable Development Goals (SDGs)

The project aligns with SDG 3: **Good Health and Well-being** and SDG 9: **Industry, Innovation, and Infrastructure.** The system promotes healthier lives and supports innovation in healthcare infrastructure.

CHAPTER 7

Conclusion and Future Scope

The internship experience has been transformative, bridging theoretical knowledge with practical skills in the domain of network security and cybersecurity systems. Over the course of this internship, I gained an in-depth understanding of how Intrusion Detection and Prevention Systems (IDPS) are conceptualized, designed, implemented, and monitored within real-world enterprise environments. From identifying network vulnerabilities to deploying sensor placements, configuring detection rules, and integrating IDPS with SIEM tools, each task contributed significantly to a holistic comprehension of modern cybersecurity challenges.

One of the most significant outcomes was the ability to appreciate the complexities involved in designing a scalable and adaptive IDPS. The process taught me the importance of planning architecture, ensuring compatibility with hybrid environments, maintaining regulatory compliance, and prioritizing incident response coordination. Furthermore, working on real datasets and understanding how data collection, preprocessing, and feature extraction shape detection models opened new perspectives on machine learning's role in cybersecurity.

The practical exposure to tools such as Cisco Packet Tracer, Wireshark, Snort, and Splunk enabled me to simulate enterprise-grade scenarios. I also understood how cyber threats evolve dynamically, and how real-time detection is not enough without prompt, accurate responses and policy enforcement. This realization reinforced the value of automation, correlation engines, and actionable intelligence in security operations.

- Moreover, I gained hands-on experience in aligning IDPS architecture with globally recognized frameworks like ISO 27001, NIST, and SOC 2.
- Understanding their principles and applying them to the system design ensured that security strategies were not only technically sound but also audit-compliant and business-ready. This alignment further highlighted the critical role of governance, documentation, and continuous risk assessment.
- Looking forward, the future scope for IDPS and security technologies is vast and evolving. With the emergence of AI-driven threats, quantum computing, and edge computing, security systems will need to become even more intelligent and decentralized.

IDPS solutions must evolve to incorporate behavioral analytics, threat intelligence feeds, and deep learning for anomaly detection. Zero Trust Architecture (ZTA) will become a standard expectation rather than a luxury, and IDPS will serve as one of its foundational components.

Additionally, cloud-native environments and microservices architectures demand agentless and scalable IDPS solutions that adapt quickly without degrading performance. Integrations with DevSecOps pipelines will allow security to be embedded from the development stage. Automation and orchestration through Security Orchestration, Automation, and Response (SOAR) platforms will revolutionize incident handling, reducing response time to seconds.

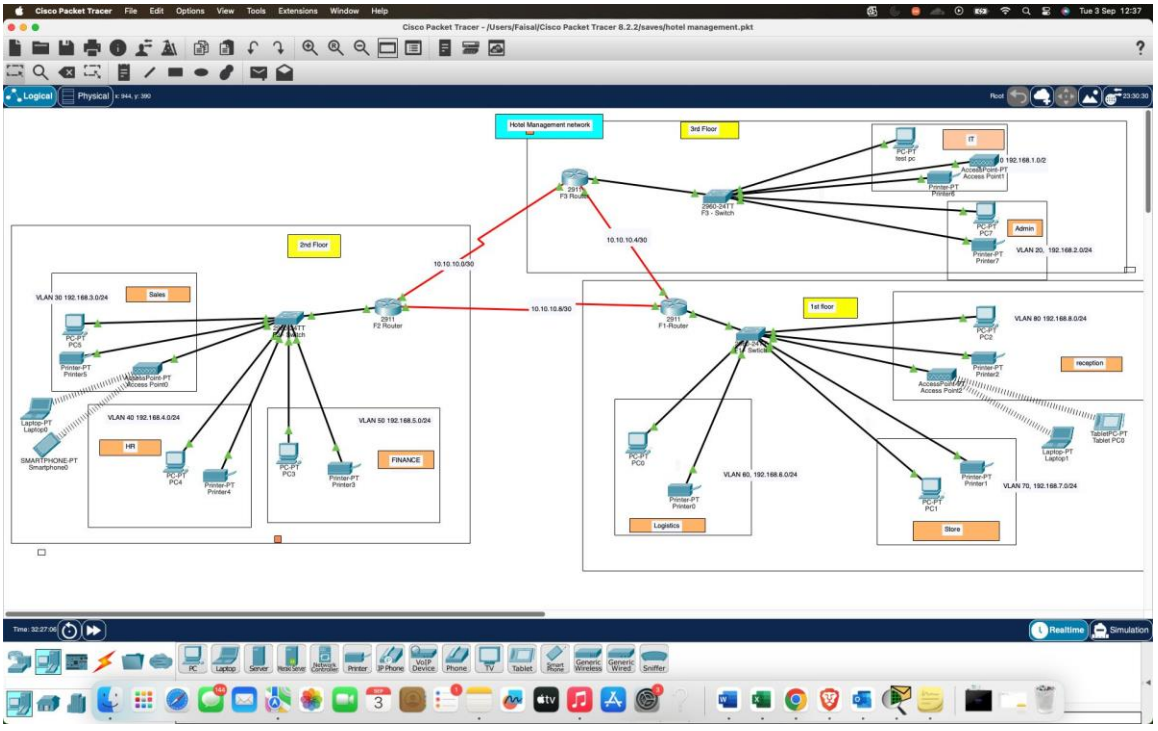
Internally, companies will invest in proactive threat hunting, red-teaming exercises, and blue-teaming simulations to strengthen their IDPS configurations and alerting logic. As cyber regulations become more stringent globally, IDPS deployments will need to cater not only to technical defenses but also to compliance reporting, forensic analysis, and legal evidence gathering.

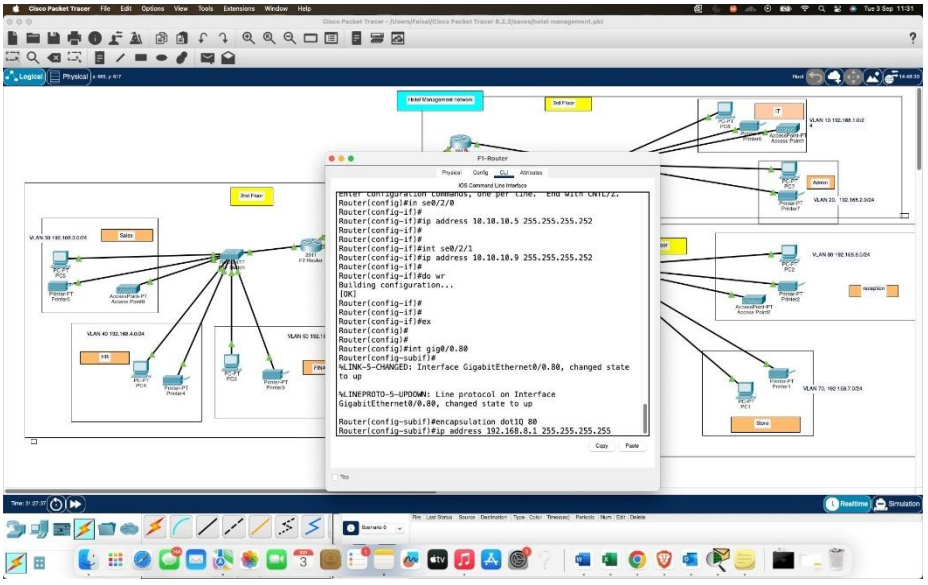
From a personal standpoint, this internship solidified my interest in pursuing a specialized career in cybersecurity architecture, with a focus on detection engineering and security automation. I now have a much clearer understanding of the roles and responsibilities within a Security Operations Center (SOC) and how each function contributes to maintaining a secure enterprise posture.

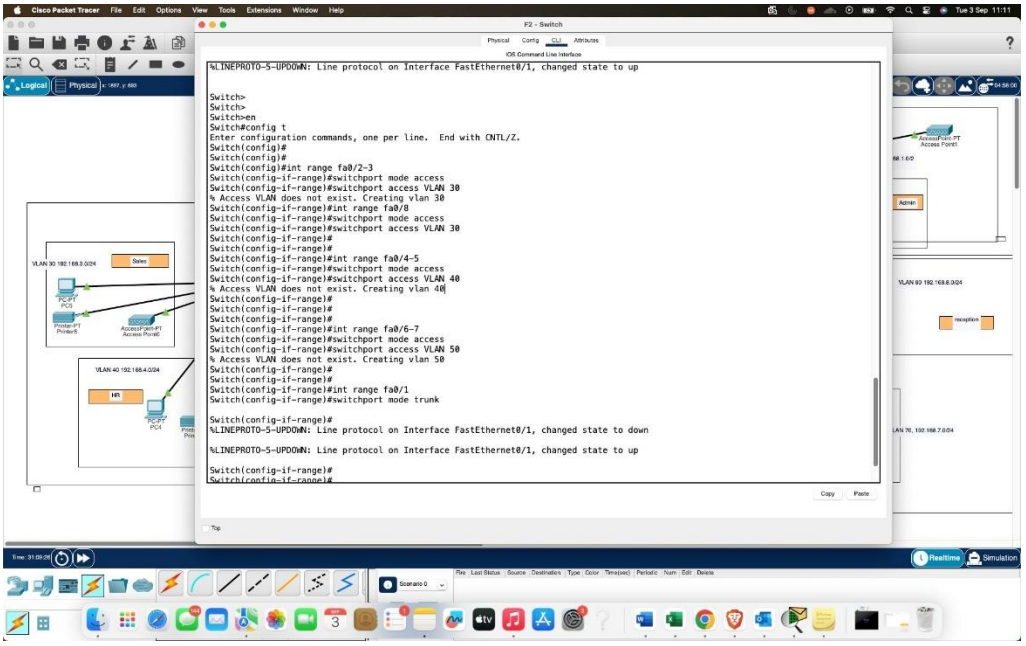
In summary, the internship was not just an academic requirement but a stepping stone into the dynamic world of cybersecurity. It fostered my technical acumen, strategic thinking, problem-solving ability, and collaborative mindset. With technology evolving rapidly, the insights and skills acquired will serve as a strong foundation for continuous learning and innovation in this critical field. I look forward to applying this knowledge in future professional opportunities, while staying updated with emerging trends, tools, and best practices that define the future of network and information security.

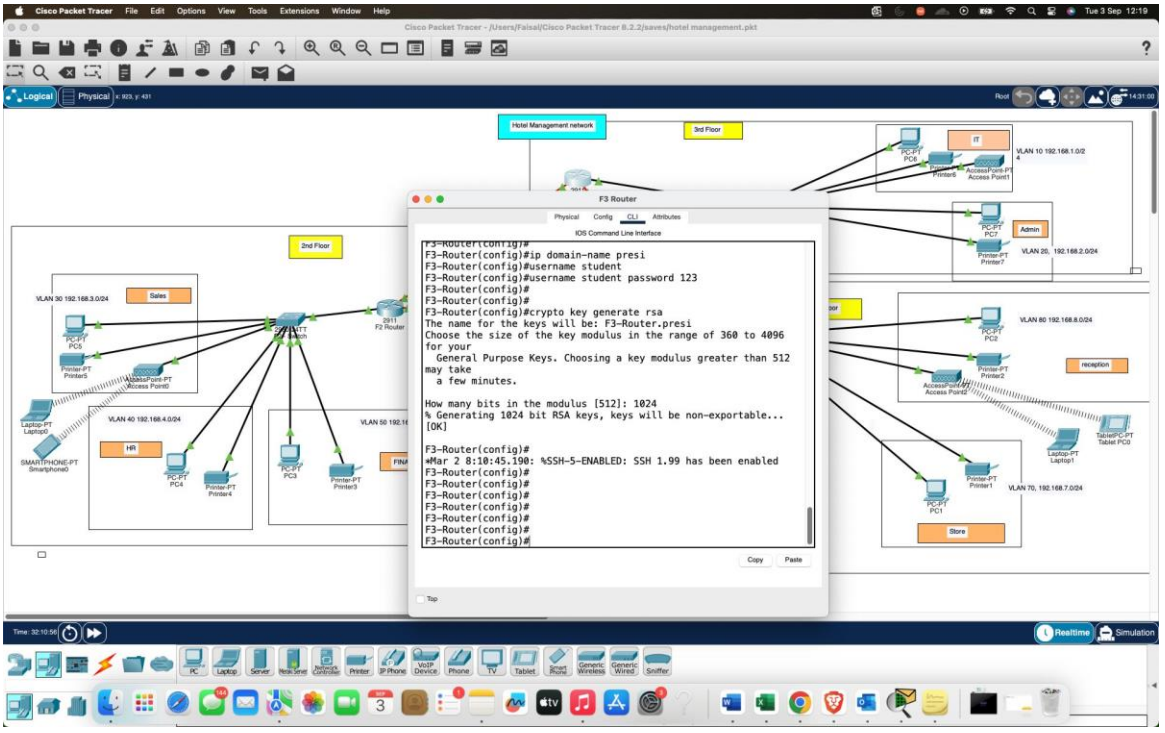
APPENDIX-A
IMPLEMENTATION AND SCREENSHOTS

1. Network Design using Cisco Packet Tracer









Step-by-Step Explanation of VLAN Configuration in Cisco Packet Tracer

1. Accessing the CLI of the Switch

The user is in the **CLI (Command Line Interface)** tab of a switch (labelled "F2 - Switch"). This is where all command-line based configurations are performed. It is the heart of Cisco device configuration, where users type Cisco IOS commands.

2. Entering Privileged EXEC Mode

Switch> en

The en command (short for enable) moves the user from **user EXEC mode** (indicated by Switch>) to **privileged EXEC mode** (Switch#), which allows access to more advanced commands.

3. Entering Global Configuration Mode

Switch# config t

This command switches to **global configuration mode**, where the administrator can make changes to the device configuration.

4. Configuring VLANs and Assigning Ports

Multiple VLANs are being created and assigned to interface ranges.

VLAN 30

Switch(config)# int range fa0/2-3

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 30

- **Interfaces FastEthernet 0/2 to 0/3** are selected.
- These interfaces are set to **access mode**, meaning they belong to a single VLAN.
- They are assigned to **VLAN 30**, which did not previously exist. The switch creates it dynamically.

VLAN 40

CopyEdit

Switch(config)# int range fa0/4-5

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 40

- Ports FastEthernet 0/4 and 0/5 are added to **VLAN 40**.
- Again, the VLAN is created automatically if it doesn't exist.

VLAN 50

Switch(config)# int range fa0/6-7

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 50

- Ports FastEthernet 0/6 and 0/7 are added to **VLAN 50** in access mode.

These steps create **logical separation** in the network. Each VLAN acts like an independent LAN, even though devices are physically connected to the same switch. This segmentation improves **security**, **performance**, and **network management**.

5. Configuring Trunk Port

Switch(config)# int range fa0/1

Switch(config-if-range) # switchport mode trunk

- **FastEthernet 0/1** is configured as a **trunk port**.
- A trunk port carries traffic from **multiple VLANs**, making it essential for inter-switch communication and connection to a router or Layer 3 device.

Trunk ports use protocols like **IEEE 802.1Q** to tag frames so that the receiving switch knows which VLAN the frame belongs to.

6. Interface Status Messages

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

This is a **system message** indicating that the interface status has changed. It typically appears after enabling or configuring a port.

7. Visual Topology

On the left, the Packet Tracer workspace shows the **network topology**. You can see:

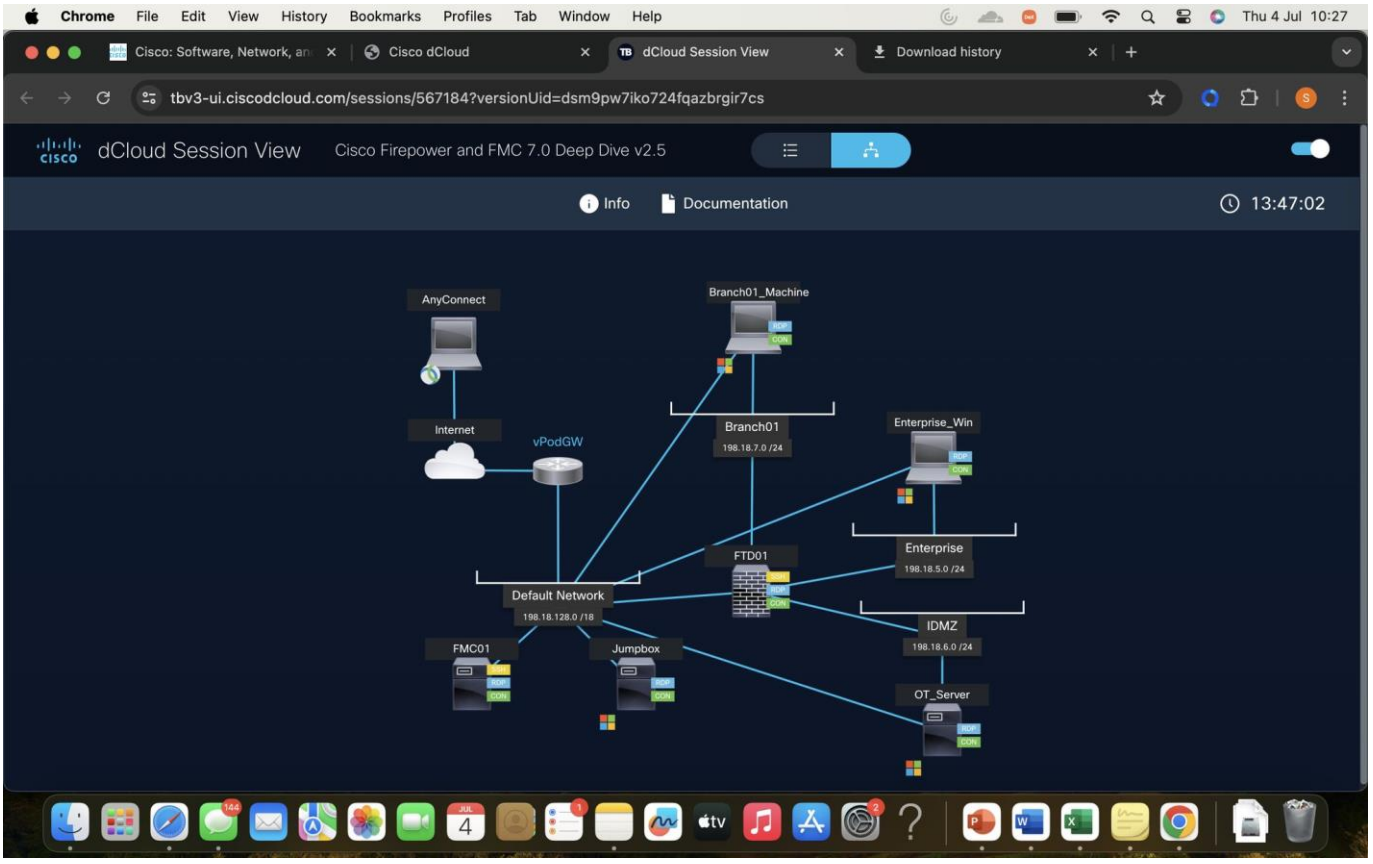
- PCs, printers, access points connected to different VLANs.
- VLANs are named and color-coded (e.g., VLAN 30 for Sales, VLAN 40 for HR).
- Each device is connected to specific switch ports (e.g., PC5 and Printer5 to VLAN 30).

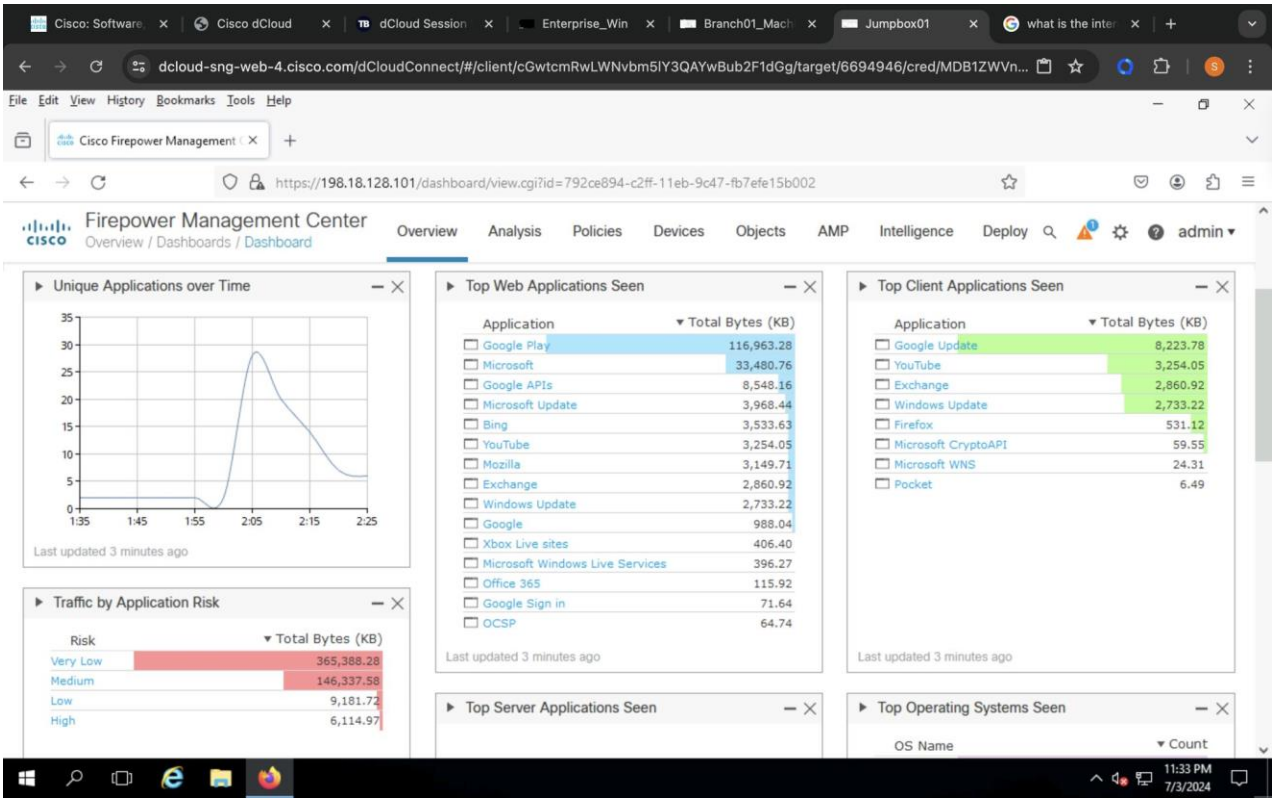
This confirms that the VLAN configuration in the CLI aligns with the **logical design** on the left.

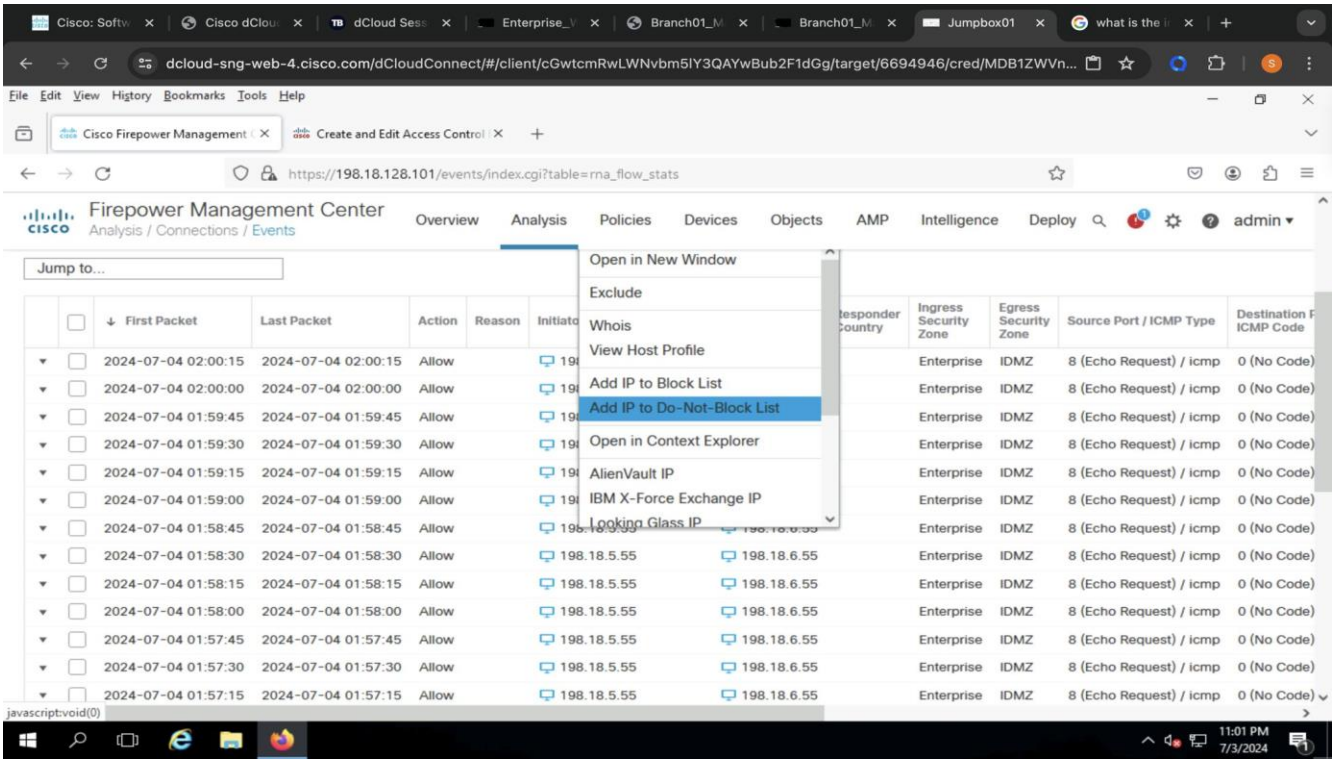
Conclusion

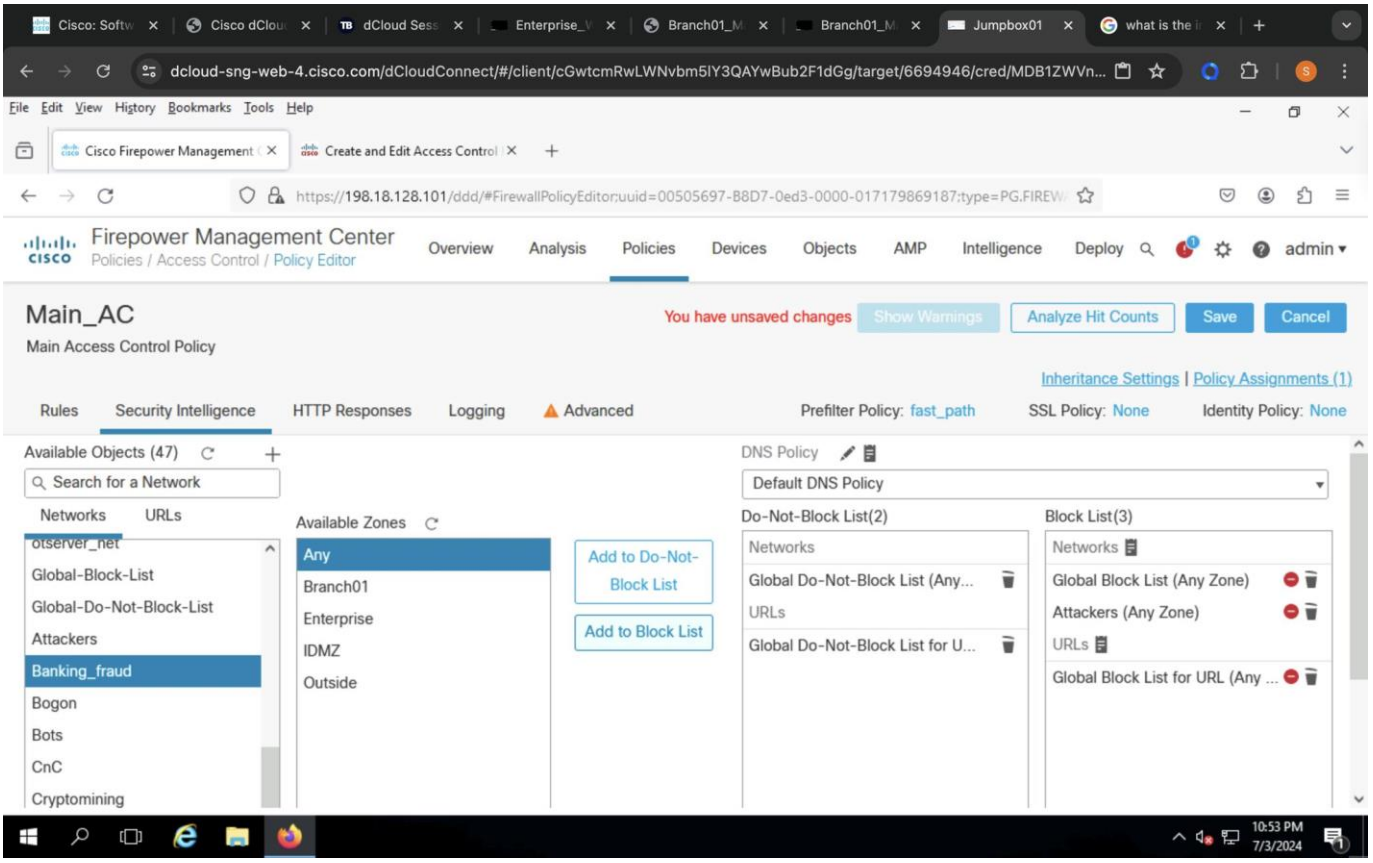
This configuration session demonstrates a foundational networking skill: **setting up VLANs and trunk links on a Cisco switch** using Packet Tracer. By isolating network segments (Sales, HR, Admin, etc.) into VLANs and connecting them via a trunk port, the administrator ensures secure, scalable, and organized traffic flow. It's a fundamental part of enterprise-grade network design, offering both **security** and **traffic management** benefits.

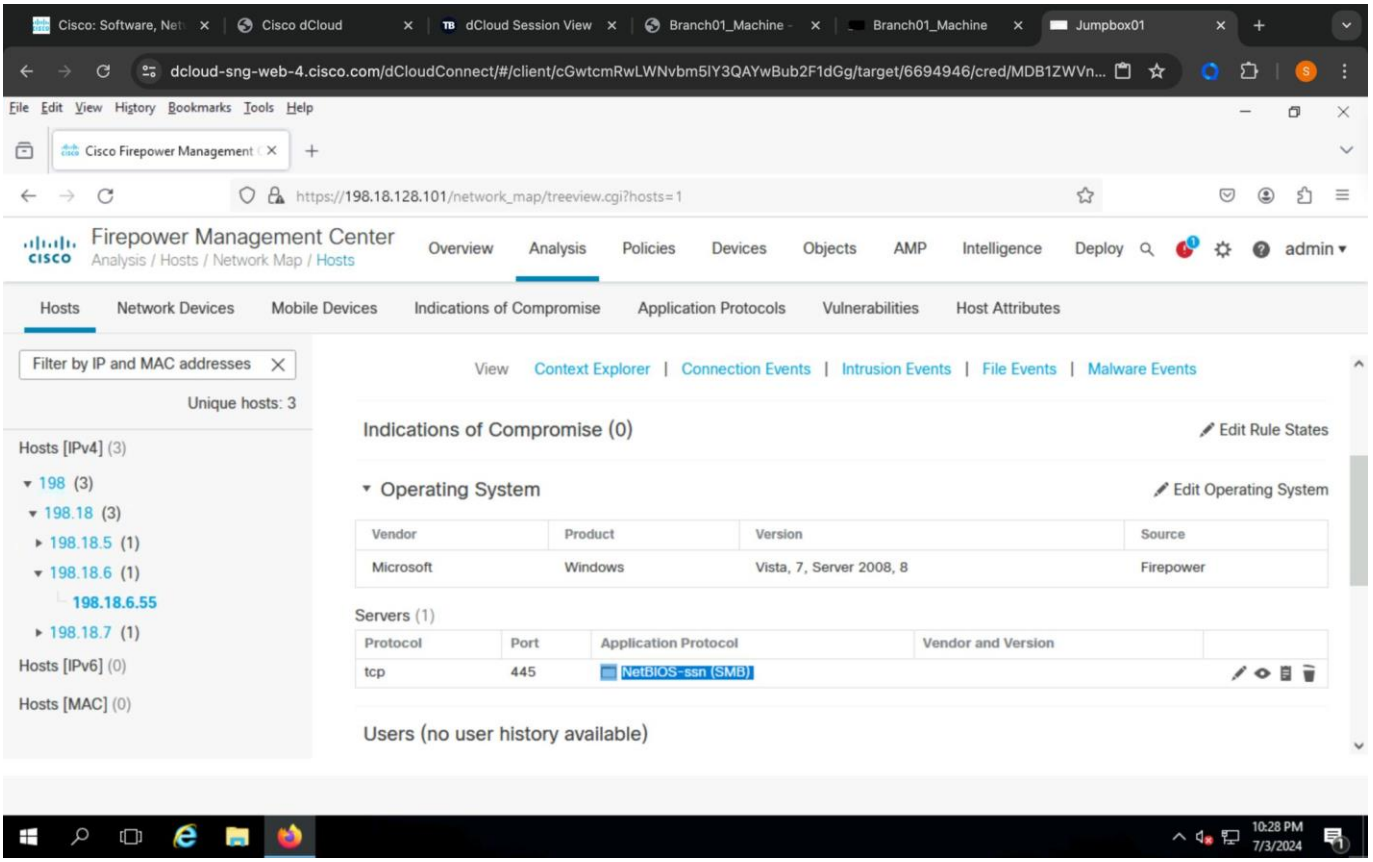
2. Cisco Firepower and FMC lab 7.0






Firepower Management Center
Analysis / Connections / Events
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
Jump to...
First Packet
Last Packet
Action
Reason
Ingress Security Zone
Egress Security Zone
Source Port / ICMP Type
Destination Port / ICMP Code
Open in New Window
Exclude
Whois
View Host Profile
Add IP to Block List
Add IP to Do-Not-Block List
Open in Context Explorer
AlienVault IP
IBM X-Force Exchange IP
Looking Glass IP
2024-07-04 02:00:15 2024-07-04 02:00:15 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 02:00:00 2024-07-04 02:00:00 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:59:45 2024-07-04 01:59:45 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:59:30 2024-07-04 01:59:30 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:59:15 2024-07-04 01:59:15 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:59:00 2024-07-04 01:59:00 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:58:45 2024-07-04 01:58:45 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:58:30 2024-07-04 01:58:30 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:58:15 2024-07-04 01:58:15 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:58:00 2024-07-04 01:58:00 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:57:45 2024-07-04 01:57:45 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:57:30 2024-07-04 01:57:30 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
2024-07-04 01:57:15 2024-07-04 01:57:15 Allow 198.18.5.55 198.18.6.55 Enterprise IDMZ 8 (Echo Request) / icmp 0 (No Code)
11:01 PM
7/3/2024


Firepower Management Center
Policies / Access Control / Policy Editor
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
Main_AC
Main Access Control Policy
You have unsaved changes
Show Warnings
Analyze Hit Counts
Save
Cancel
Inheritance Settings | Policy Assignments (1)
Rules
Security Intelligence
HTTP Responses
Logging
Advanced
Prefilter Policy: fast_path
SSL Policy: None
Identity Policy: None
Available Objects (47)
Search for a Network
Networks
URLs
Global-Block-List
Global-Do-Not-Block-List
Attackers
Banking_fraud
Bogon
Bots
CnC
Cryptomining
Available Zones
Any
Branch01
Enterprise
IDMZ
Outside
Add to Do-Not-Block List
Add to Block List
DNS Policy
Default DNS Policy
Do-Not-Block List(2)
Networks
Global Do-Not-Block List (Any...
URLs
Global Do-Not-Block List for U...
Block List(3)
Networks
Global Block List (Any Zone)
Attackers (Any Zone)
URLs
Global Block List for URL (Any ...
10:53 PM
7/3/2024



Core Functions of Cisco Firepower

1. Next-Generation Firewall (NGFW) Capabilities

Cisco Firepower delivers stateful inspection, application-layer filtering, deep packet inspection (DPI), and identity-based access control. It goes beyond traditional packet filtering by enabling granular control over applications, users, and web categories.

2. Intrusion Prevention System (IPS)

The integrated Snort-based Next-Gen IPS (NGIPS) provides signature-based and anomaly-based detection techniques to identify and block known and zero-day exploits. The IPS can be tuned with custom rules and policies to adapt to organizational needs.

3. Application Visibility and Control (AVC)

With AVC, Cisco Firepower provides insights into more than 4,000 applications, identifying their usage, risk levels, and bandwidth consumption. This is crucial for enforcing acceptable-use

policies and protecting sensitive data.

4. URL Filtering and Reputation-Based Blocking

Firepower integrates with Cisco Talos threat intelligence to classify and block URLs based on categories and risk reputation. It prevents access to malicious or policy-violating content in real-time.

5. Advanced Malware Protection (AMP)

Firepower 7.0 includes integration with Cisco AMP to detect and prevent file-based malware. It uses sandboxing and retrospective analysis to detect advanced threats and offers file trajectory visualization for forensic insights.

6. Threat Intelligence Integration

By leveraging Cisco Talos, Firepower gets real-time updates on threats, including zero-day attacks, command-and-control IPs, malware hashes, and URL categorization. This empowers proactive threat prevention.

Key Features in Version 7.0

1. Improved User Interface

FMC 7.0 introduces a more responsive and intuitive UI, improving user experience during policy configuration, event monitoring, and device management.

2. Faster Policy Deployment

Policy deployment in 7.0 is faster and more efficient. It allows parallel deployment to multiple devices and better error diagnostics.

3. Integration with SecureX

Firepower 7.0 natively integrates with Cisco SecureX, providing unified security operations, threat hunting, and case management across Cisco's security ecosystem.

4. Multitenancy Enhancements

Improved role-based access control and domain management features make it easier to manage

multi-tenant environments or large-scale enterprise networks.

5. Threat Response Enhancements

FMC 7.0 supports improved logging, automated remediation, and enhanced workflows for security analysts through integrations with tools like Cisco Threat Response.

6. SecureX Ribbon and Casebook

The SecureX Ribbon enables real-time investigation tools embedded directly in FMC, while the Casebook feature allows analysts to track and collaborate on specific threat incidents**.**

In Conclusion The modelling labs have proven to be incredibly powerful, aiding in a deeper understanding of implementation on production devices.
In exploration, I've come to appreciate the significance of FMC and FTD as exceptional Next-Generation Firewall and IDP Systems. These tools are indispensable for advanced threat protection and streamlined security management in today's digital landscape.

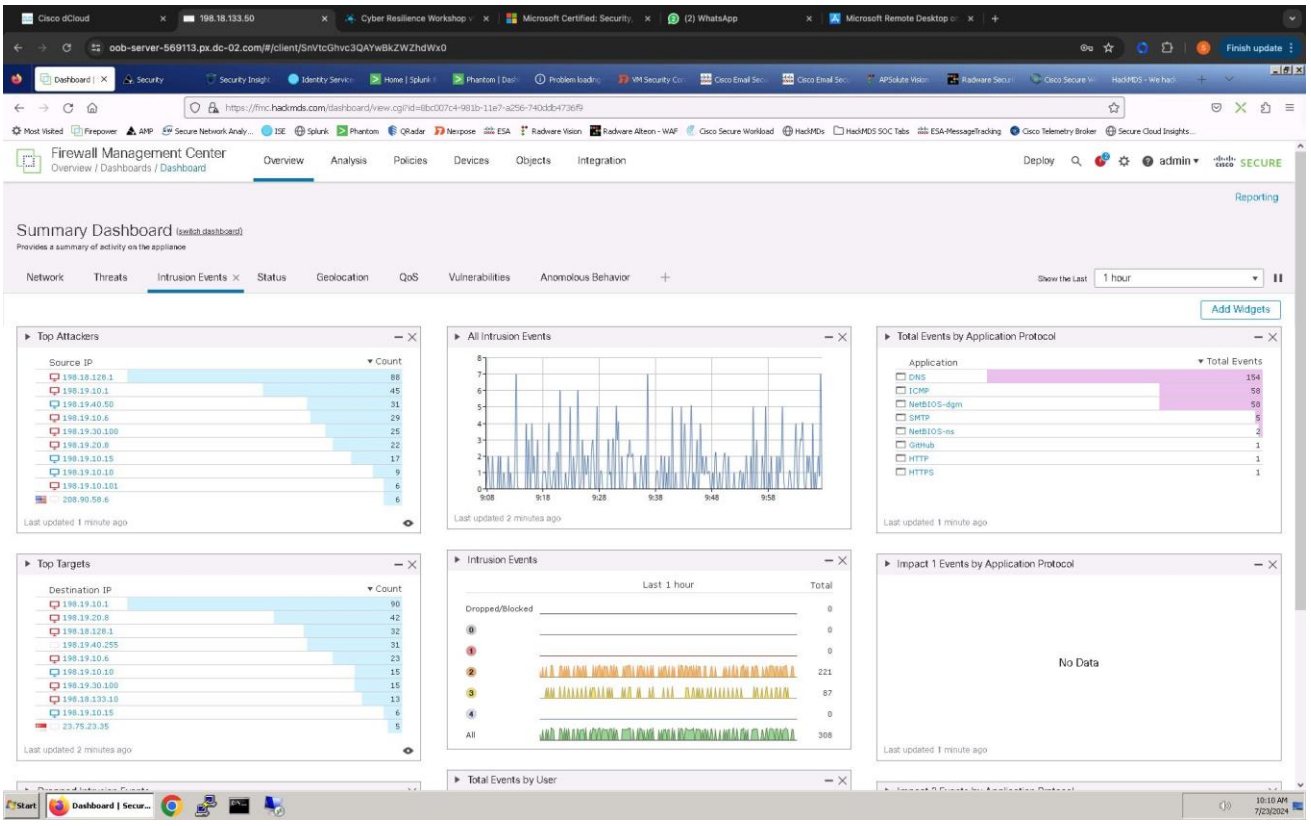
1. Network Discovery: Setting up Firepower involves initiating Network Discovery, a crucial step that helps in identifying the types of hosts communicating on your network.

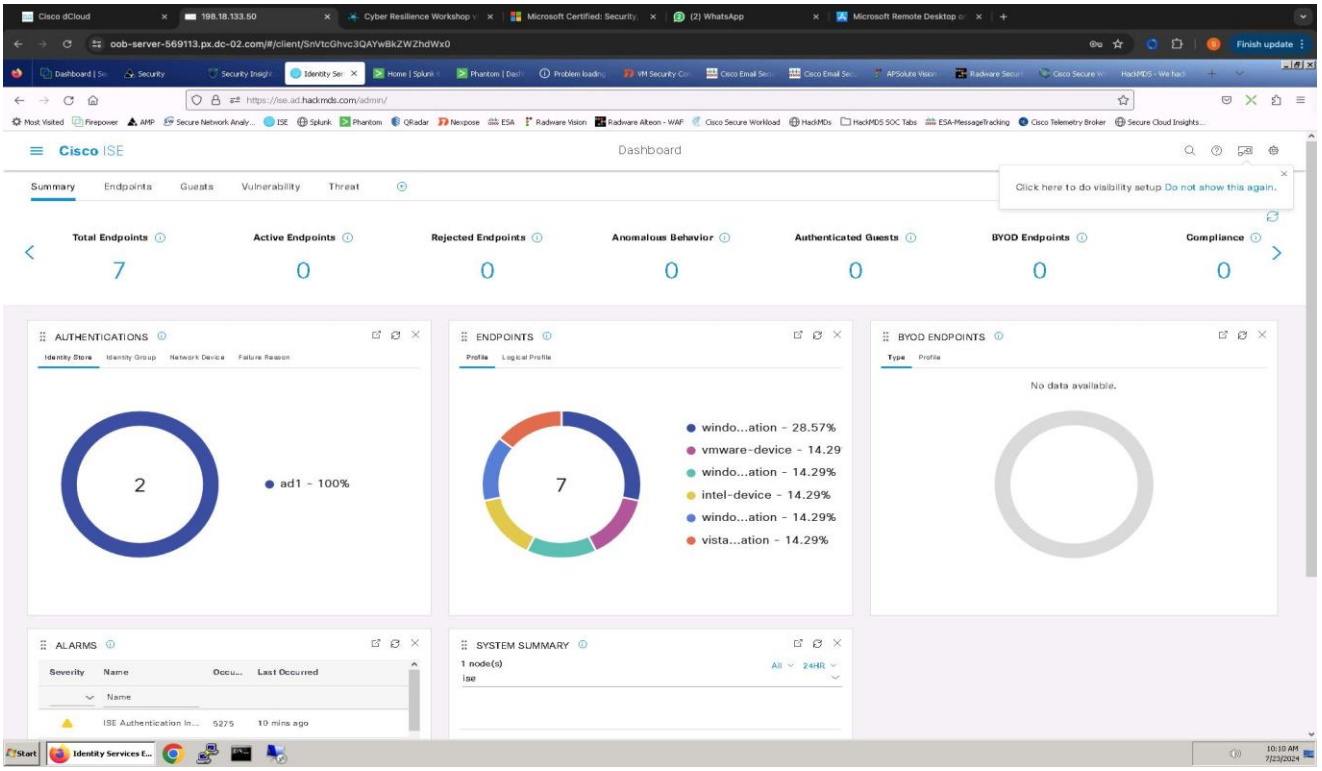
2. Access Control: Access Control Policies are akin to traditional firewall rules but are meticulously designed to filter traffic from specific zones, networks, and applications, allowing, denying, and logging traffic as needed.

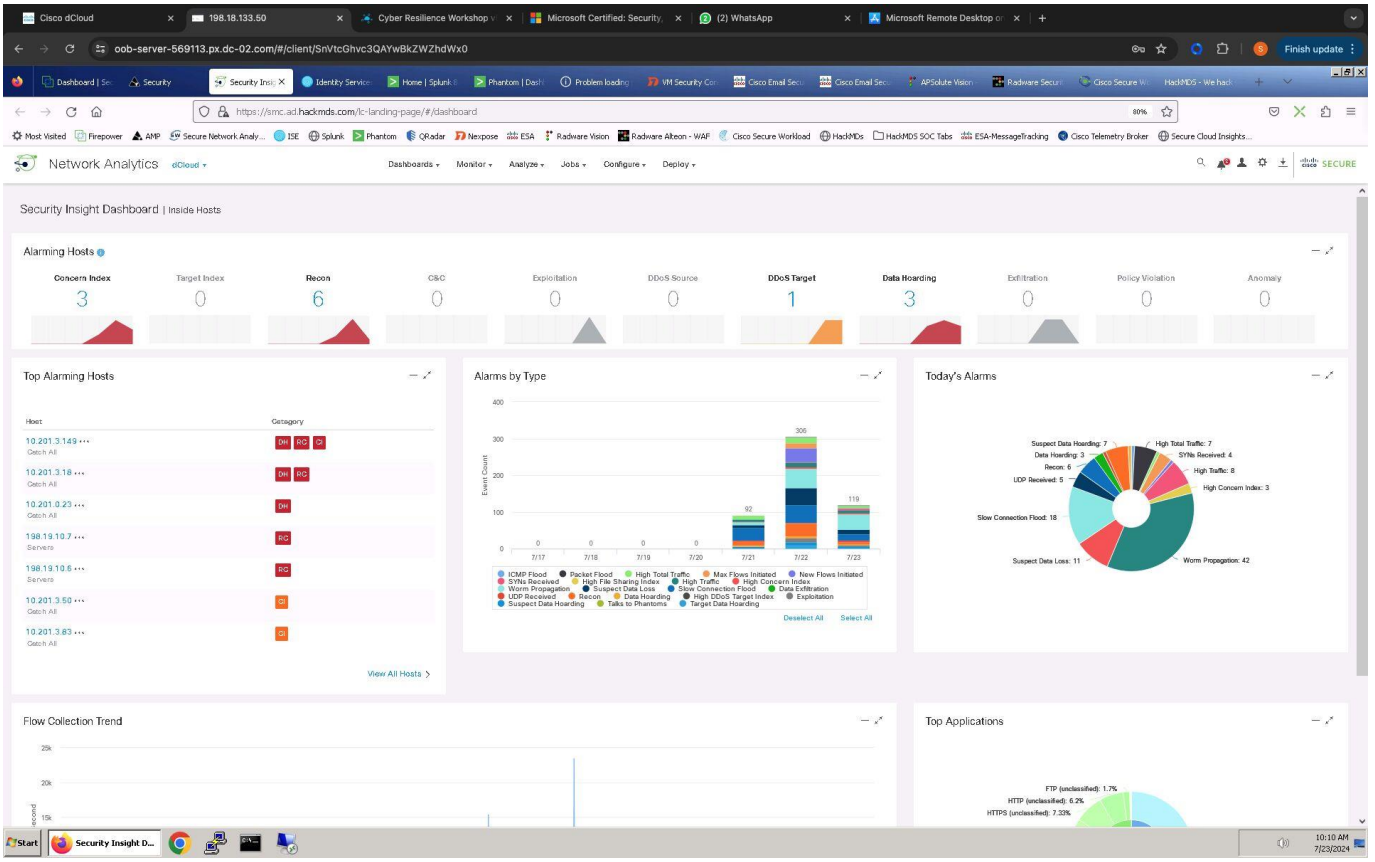
3. Security Intelligence: This advanced feature plays a pivotal role in blocking malicious content, leveraging block lists to eliminate unwanted traffic efficiently without draining processing power. It offers a comprehensive range of malicious threat categories that can be integrated into block lists.

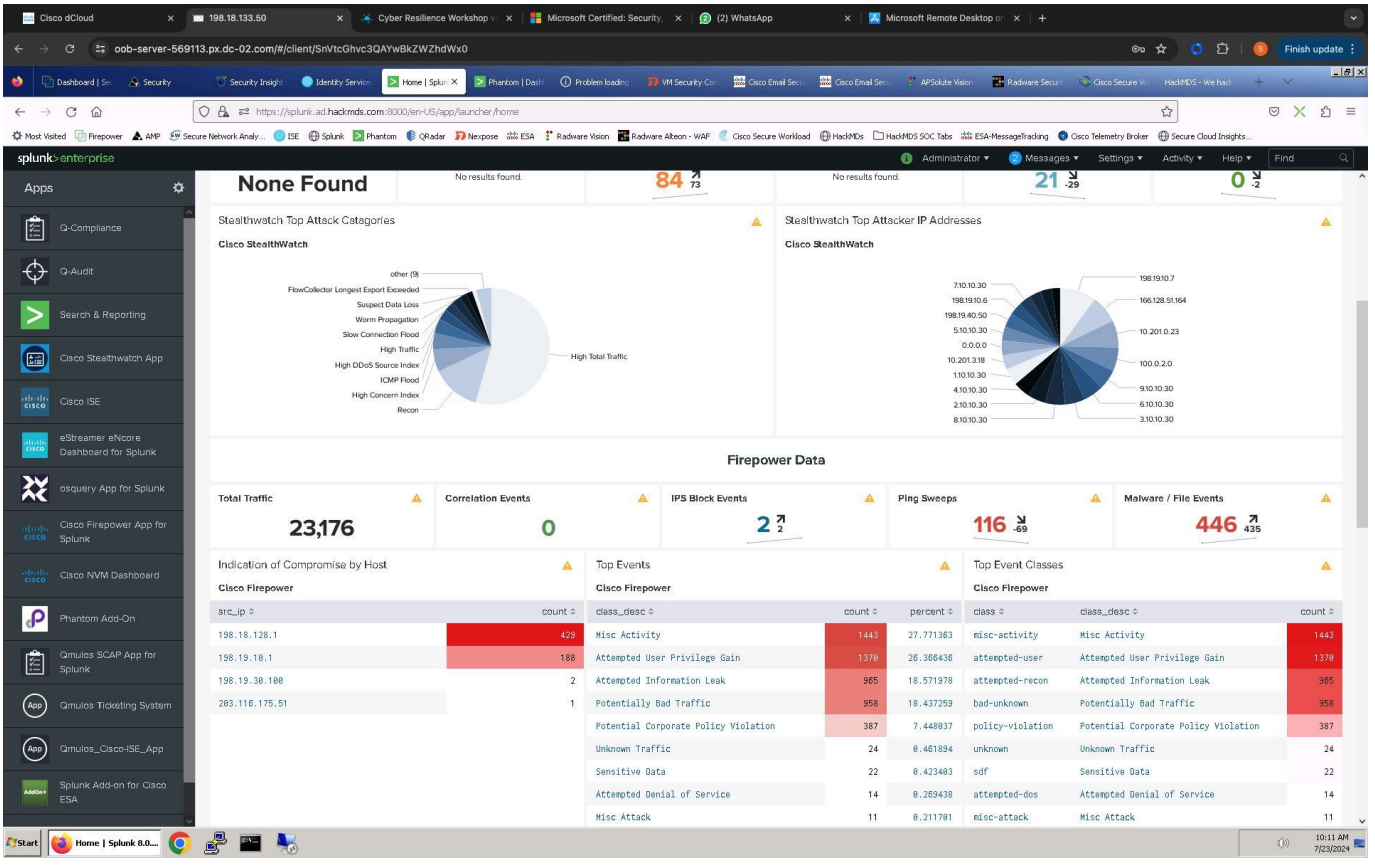
The FMC landscape is extensive, offering multiple features like URL filtering, Pre-filter policies, Intrusions, and Cisco AMP for malware in files, which I'm eager to explore further.

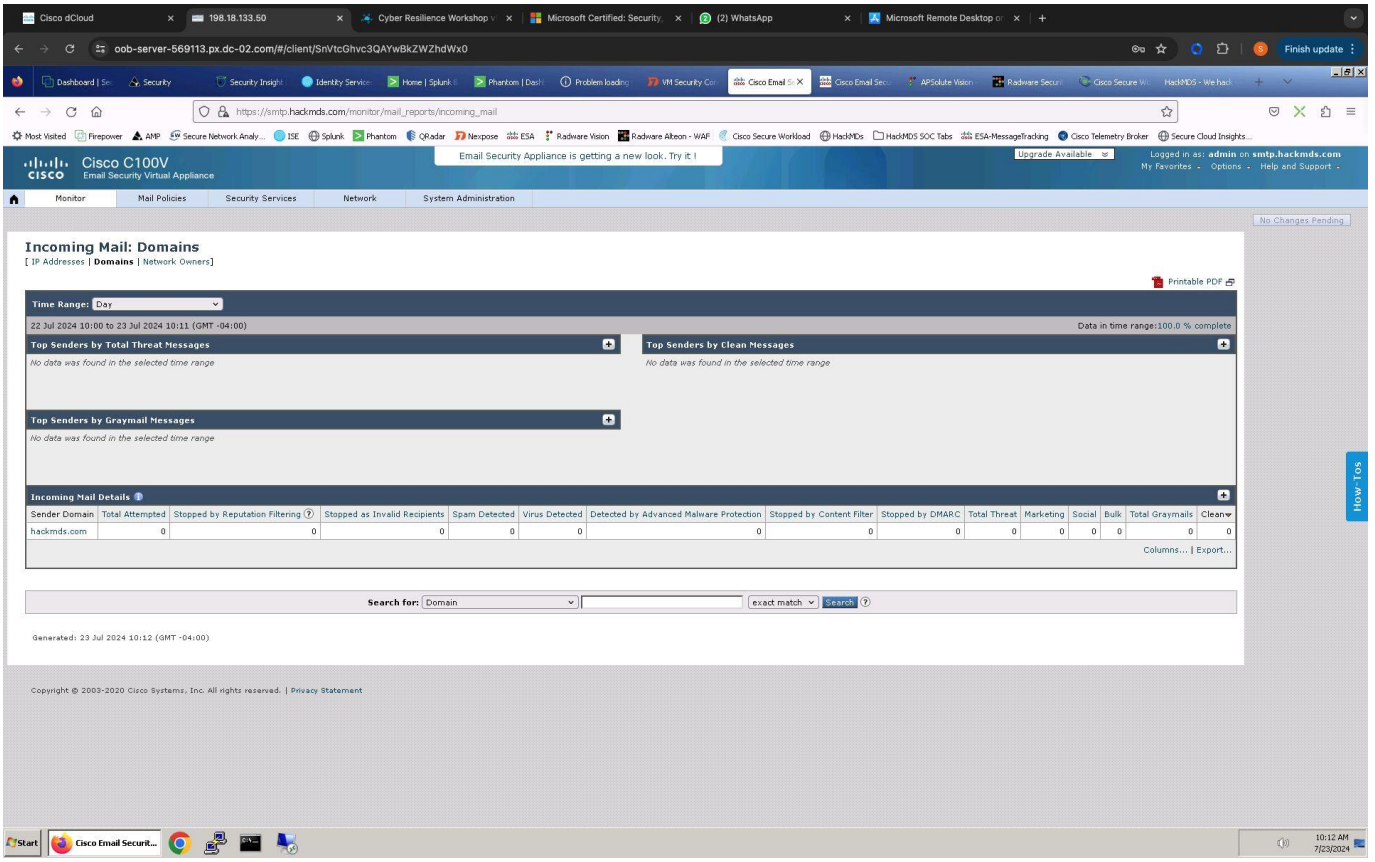
3. CISCO Cyber Resilience workshop






Network Analytics
Security Insight Dashboard | Inside Hosts
Alarming Hosts
Concern Index 3
Target Index 0
Recon 6
C&C 0
Exploitation 0
DDoS Source 0
DDoS Target 1
Data Hoarding 3
Exfiltration 0
Policy Violation 0
Anomaly 0
Top Alarming Hosts
Alarms by Type
Today's Alarms
Flow Collection Trend
Top Applications


splunk>enterprise
Apps
None Found
Stealthwatch Top Attack Catagories
Cisco StealthWatch
Stealthwatch Top Attacker IP Addresses
Cisco StealthWatch
Firepower Data
Total Traffic
23,176
Correlation Events
0
IPS Block Events
2
Ping Sweeps
116
Malware / File Events
446
Indication of Compromise by Host
Top Events
Top Event Classes



Design and implementation of a technical defense-in-depth model on production devices and enterprise environments, leveraging Cisco's security architecture. This initiative was inspired and supported by the **Cisco Cyber Resilience Workshop**, which provided practical insights into simulating both attacker and responder scenarios. Through this experience, I developed a deeper understanding of real-world threat mitigation, system hardening, and security orchestration.

The core principle of the **defense-in-depth model** is to provide multiple layers of security controls across the IT environment to delay, detect, and respond to cyber threats effectively. Below are the key Cisco and third-party technologies I employed, along with their respective roles in building a robust security posture.

1. Cisco Firewall Management Center (FMC)

At the core of the network perimeter defense, I configured and managed Cisco Firepower devices through **Firewall Management Center (FMC)**. This involved:

- Creating and applying **Access Control Policies (ACPs)** for precise traffic filtering.
- Implementing **stateful inspection** and **intrusion prevention rules** to block malicious activity.

- Monitoring event data and enforcing geo-location and application-based controls. This layer significantly enhances the organization's ability to enforce granular policies, reducing the attack surface and preventing unauthorized access to internal resources.

2. Cisco StealthWatch (Secure Network Analytics)

To ensure advanced threat detection and network visibility, I integrated **Cisco StealthWatch** for real-time behavioral analytics. Key activities included:

- Collecting NetFlow telemetry from routers and switches.
- Analyzing traffic patterns to detect anomalies such as data exfiltration or lateral movement.
- Generating alerts based on deviations from normal network behavior. StealthWatch's ability to provide **east-west traffic visibility** and **encrypted traffic analytics** proved essential for identifying stealthy threats and policy violations that evade perimeter defenses.

3. Cisco Identity Services Engine (ISE)

I deployed **Cisco ISE** to enable **policy-based access control** across wired, wireless, and VPN-connected devices. It played a pivotal role in:

- Enforcing **role-based access controls (RBAC)** tied to Active Directory identities.
- Applying **Network Access Control (NAC)** policies for posture assessment and device compliance.
- Automating quarantining or limiting access for non-compliant endpoints. Cisco ISE acts as the trust anchor, ensuring that only authenticated and authorized users/devices can access specific network segments, thus minimizing insider threats.

4. Splunk Integration with Cisco Ecosystem

Splunk was utilized as the **centralized SIEM platform** to correlate logs and events generated by Cisco security tools. My activities included:

- Ingesting logs from Cisco FMC, StealthWatch, and ISE.
- Building dashboards to visualize key indicators of compromise (IoCs).
- Creating alerts and workflows for **automated incident response**. This integration empowered security teams with **real-time situational awareness**, enabling faster detection, investigation, and response to security incidents.

5. Nexpose (by Rapid7) – Vulnerability Management

For continuous security assessment, I used **Nexpose** to identify and prioritize vulnerabilities across servers, endpoints, and networking devices. Tasks included:

- Performing authenticated and unauthenticated scans.
- Mapping discovered vulnerabilities to CVEs and CIS benchmarks.
- Generating remediation plans and collaborating with IT teams for patch management. This proactive approach to vulnerability management helped in **reducing the attack surface** and ensuring that exploitable weaknesses were addressed in a timely manner.

6. Cisco Email Security Appliance (ESA)

Recognizing email as a primary vector for malware and phishing, I implemented **Cisco ESA** to secure the organization's email infrastructure. Key configurations included:

- Enabling anti-spam, anti-malware, and anti-phishing filters.
- Applying **outbound data loss prevention (DLP)** and **encryption policies**.
- Analyzing message headers and attachments for malicious payloads. The ESA played a vital role in **preventing credential theft, ransomware spread, and data leaks**, ensuring secure communication within and outside the organization.

Beyond technical controls, the project emphasized the importance of:

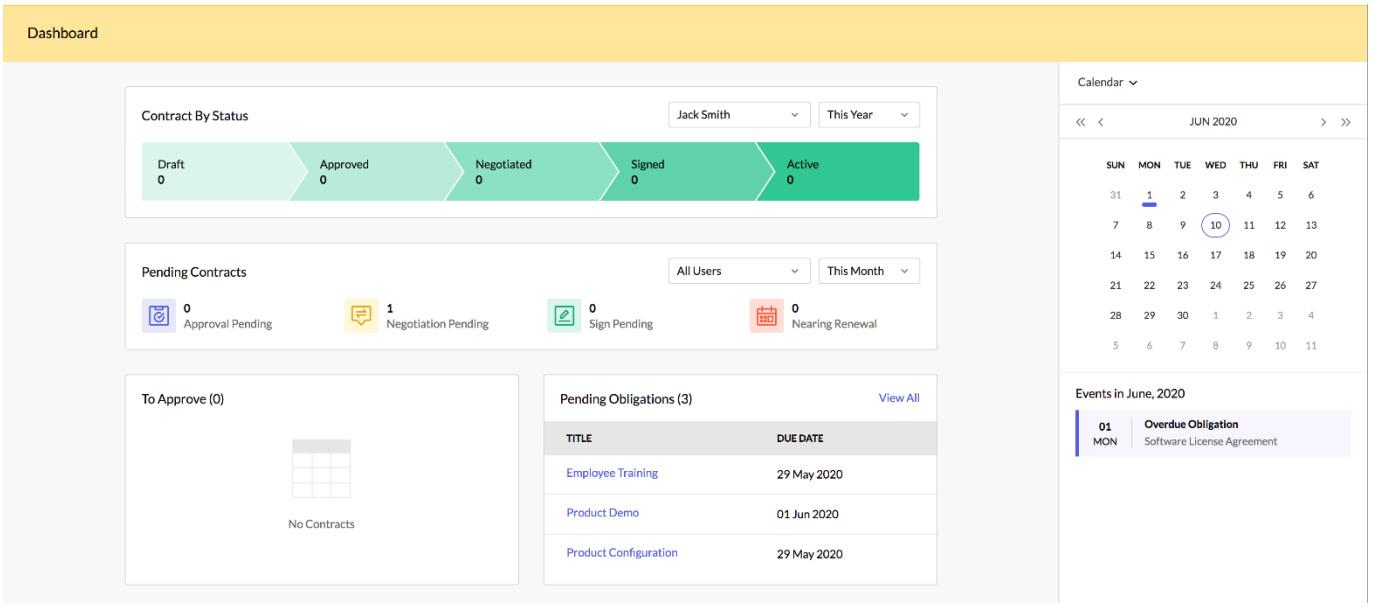
- **Security awareness training** for end-users to reduce human error.
- Implementing **physical security measures** to protect critical infrastructure.
- Conducting **simulated red vs. blue team exercises** to test the effectiveness of the controls.
- Following **Zero Trust principles**, assuming breach and continuously verifying access.
-

Through this layered security architecture, I gained first-hand experience in deploying a **resilient, adaptive, and scalable cybersecurity framework**. I learned that while no security model is flawless, consistent evaluation, automation, and strategic layering of controls can drastically reduce organizational risk.

This experience has significantly contributed to my understanding of enterprise-grade cybersecurity solutions and operational defense strategies. By working with a diverse set of tools—both Cisco-native and third-party—I was able to see how integrated solutions can work in tandem to form a cohesive security architecture. Moving forward, I intend to deepen my expertise in

security automation, Zero Trust frameworks, and threat intelligence-driven defense.

4.Migration to Zoho Contracts



1. Requirement Gathering and Initial Assessment

Before starting the migration, it's important to understand the full scope of the project.

Objective Clarification:

Define the goal of the migration—e.g., centralizing all existing vendor contracts in Zoho Contracts to improve visibility, tracking, and compliance.

Source System Review:

Identify where current contracts are stored—this could be a shared drive, Google Workspace, Excel trackers, or another contract management tool.

Contract Type Categorization:

Classify contracts by type (e.g., NDAs, SLAs, MSAs, licensing agreements). This helps during template mapping in Zoho.

Stakeholder Input:

Coordinate with legal, procurement, and IT teams to confirm data ownership, confidentiality concerns, and metadata requirements.

2. Zoho Contracts Environment Setup

Before uploading anything, the Zoho Contracts platform needs to be properly configured.

Account Creation and Access Setup:

Ensure that all relevant team members have user accounts with the correct roles (e.g., Admin, Reviewer, Viewer).

Template Configuration:

Set up reusable contract templates using Zoho's editor for common contract types. Include pre-approved clauses and fields like vendor name, start/end date, renewal terms, etc.

Custom Fields Definition:

Create custom metadata fields in Zoho (e.g., contract owner, department, value, renewal frequency) to allow better tagging and filtering post-migration.

Approval Workflow Configuration:

Establish internal workflows for contract reviews and approvals to ensure post-migration documents follow company policy.

3. Data Preparation and Cleaning

Clean, verify, and structure contract data before importing.

Contract Inventory Creation:

Build a master list of all contracts to be migrated, including key details like vendor name, contract start and end dates, renewal clauses, contact person, and associated documents.

File Naming and Format Standardization:

Rename files consistently (e.g., VendorName_ContractType_YYYY-MM-DD.pdf) and convert all documents to a supported format (PDF, DOCX).

Data Validation:

Ensure all critical information is complete. Fill in missing fields where possible, and flag incomplete or outdated contracts for review.

Redundancy Check:

Identify and remove duplicate or expired contracts that are no longer in use.

4. Importing Contracts into Zoho Contracts

Once the system is ready and data is clean, begin the import process.

Bulk Upload of Documents:

Use Zoho's bulk import tool or manually upload documents one by one. Map each contract to its appropriate metadata fields (vendor, contract type, duration, etc.).

Assign Ownership and Permissions:

Allocate each contract to its relevant contract owner or department and set user-level access restrictions to maintain confidentiality.

Tag Contracts for Easy Retrieval:

Use Zoho's tagging system to label contracts by department, criticality, or renewal frequency for improved searchability.

5. Testing and Quality Check

Verify that the migration was successful and data integrity is maintained. Random Sampling for Review: Manually check a sample of migrated contracts to verify that metadata, attachments, and ownership were correctly imported.

Approval Workflow Simulation: Run a few dummy approval workflows to ensure the system operates as expected post-migration.

Search and Filter Functionality Testing: Use filters to test whether users can easily find contracts based on custom fields like department or expiry date.

Reporting Dashboard Verification:

Ensure the analytics and reporting features reflect correct data from migrated contracts.

6. Stakeholder Training and Handover

Train end users and finalize handover.

Training Sessions:

Conduct walkthroughs for legal, procurement, and business users to explain how to search, review, and manage contracts in Zoho.

Documentation and SOPs:

Prepare user guides or standard operating procedures (SOPs) that explain key workflows (e.g., contract renewal, approval, archival).

Final Handover:

Submit the final report and migration summary to stakeholders. Include a list of contracts imported, custom fields used, and any issues encountered/resolved.

7. Post-Migration Monitoring and Optimization

After the migration, continue refining and improving usage.

Usage Monitoring:

Use Zoho's logs and dashboards to track user activity and contract engagement.

Automated Reminders:

Set up automated alerts for contract renewals, expirations, or review milestones.

Feedback Collection:

Gather feedback from users to identify any issues with usability or workflows and implement improvements where possible.

Conclusion

Migrating contracts to Zoho Contracts not only centralized and streamlined the organization's contract management but also laid the groundwork for better compliance, audit readiness, and vendor transparency. The structured process ensured data integrity, improved accessibility, and enabled the automation of critical contract lifecycle events.

10% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography

Match Groups

- 135 Not Cited or Quoted 10%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 8 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

7% Internet sources
7% Publications
4% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

ENCLOSURES

The cybersecurity internship carried out here aligns with **SDG-9: Industry, Innovation, and Infrastructure**, contributing to the advancement of secure digital ecosystems. This internship supports the well-being of society by enhancing the security of both industrial systems and personal internet usage. It emphasizes the critical role of cybersecurity practices such as vulnerability assessment, threat intelligence, and penetration testing in safeguarding infrastructure against evolving cyber threats.

INFORMATION SECURITY AND NETWORK SECURITY INTERN
Amicorp Management

AN INTERNSHIP REPORT

Submitted by,

SYED FAISAL EHSAN - 20211CCS0187

Under the guidance of,

Ms. AMREEN KHANUM D

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING, CYBER SECURITY

At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Internship report **"Information Security and Network Security Intern"** being submitted by "SYED FAISAL EHSAN," bearing roll number "20211CCS0187" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a Bonafide work carried out under my supervision.

Ms. Amreen Khanum D
Assistant Professor
PSCS
Presidency University

Dr. ANANDARAJ SP
Professor & HoD
PSCS
Presidency University

Dr. MYDHILI NAIR
Associate Dean School
of CSE
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vc School of Engineering
Dean -PSCS / PSIS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

I hereby declare that the work which is being presented in the project report entitled **Information Security and Network Security using CISCO and ZOHO Solutions** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of our own investigations carried out under the guidance of **Ms. Amreen Khanum D, Assistant Professor, School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NUMBER	SIGNATURE
SYED FAISAL EHSAN	20211CCS0187	

AMICORP

Address
Amicorp Management India Private Limited
C/O Regus Eversun Business Centre
Ground Floor, E1 Block(Beech), Manyata
Embassy Business Park, Outer Ring Road
Bangalore 560 045
India

Telephone
+91 80 4005 4900
Facsimile
+91 80 4005 4906

E-mail
bangalore@amicorp.com
Web
www.amicorp.com

To Whom So Ever It May Concern,

This is to certify that **Syed Faisal Ehsan** has successfully completed a 3-month internship at Amicorp Management India Private Limited, serving in the capacity of an Information Security and Network Security Intern from 3rd February 2024 to 30th April 2024.

During the tenure of the internship, Faisal demonstrated excellent dedication and professionalism in all assigned responsibilities and actively contributed to various projects within the organization's cybersecurity environment.

Key Responsibilities and Technologies Worked on
The internship involved practical exposure to a wide array of cybersecurity technologies and tools, including but not limited to:

1. Cisco Firewall Management Center (FMC) – Implementing access control policies and firewall configurations
2. Cisco StealthWatch (Secure Network Analytics) – Network traffic monitoring and behavioral anomaly detection
3. Cisco Identity Services Engine (ISE) – Policy-based access control and endpoint compliance enforcement
4. Cisco Email Security Appliance (ESA) – Email threat filtering, anti-phishing, and DLP configurations
5. Splunk – Security Information and Event Management (SIEM) integration and log analytics
6. Nexpose (by Rapid7) – Vulnerability assessment and risk remediation
7. Wireshark & Snort – Packet analysis and network-based intrusion detection
8. Cisco Packet Tracer – Network simulation and topology planning

Faisal also actively participated in red-teaming and blue-teaming exercises, simulated incident response workflows, and applied cybersecurity frameworks including ISO 27001, NIST, and Zero Trust Architecture principles.

We appreciate Faisal's contributions and wish them continued success in future professional endeavors.

Signed by:
[redacted]

For Amicorp Management India Pvt. Ltd.

Asokan Kunnathully

Authorised Signatory

Head of HR India

AMICORP MANAGEMENT INDIA PVT LTD BANGALORE

ACKNOWLEDGEMENT

First of all, we are indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Pro- VC, School of Engineering and Dean, School of Computer Science Engineering & Information Science, Presidency University, for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Deans **Dr. Mydhili Nair,** School of Computer Science Engineering & Information Science, Presidency University, and **Dr. Anandaraj SP**, Head of the Department, School of Computer Science Engineering & Information Science, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Ms. Amreen Khanum D,** Assistant Professor and Reviewer **Dr. Sharmasth Vali Y,** Associate Professor, School of Computer Science Engineering & Information Science, Presidency University for his inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the PIP2001 Capstone Internship Coordinators **Mr. Md Zia Ur Rahman and Dr. Sampath A K,** department Project Coordinator **Dr. Sharmasth Vali Y** and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us with in bringing out this project.

Syed Faisal Ehsan