INDUSTRY INTERNSHIP
SUMMARY REPORT

Cybersecurity Virtual Internship

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

Submitted by

VIKAS KUMAR(22SCSE1011141)

Vth Sem III Year

GALGOTIAS UNIVERSITY

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
GREATER NOIDA, UTTAR PRADESH
2024 – 2025

CERTIFICATE

I hereby certify that the work which is being presented in the Internship project report entitled “Cybersecurity Virtual Internship by Palo alto Networks “in partial fulfillment for the requirements for the award of the degree of Bachelor of Technology in the School of Computing Science and Engineering of Galgotias University, Greater Noida, is an authentic record of my own work carried out in the industry.

To the best of my knowledge, the matter embodied in the project report has not been submitted to any other University/Institute for the award of any Degree.

VIKAS KUMAR (22SCSE1011141)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Signature of Internship Reviewer **Signature of Dean (SCSE)**

TABLE OF CONTENTS

Abstract

The Palo Alto Cybersecurity Virtual Internship, facilitated by AICTE and supported by Palo Alto Networks, provided an in-depth, hands-on experience in foundational and advanced cybersecurity concepts. Conducted from July to September 2024, this 10-week internship emphasized practical learning across various domains of cybersecurity, earning an "Outstanding" (Grade O) for exceptional performance.

Key highlights and deliverables of the internship:

- **Modules Completed:**
  - **Fundamentals of SOC (Security Operations Center):** Gained expertise in incident detection, analysis, and response, along with understanding the core functions of a SOC.
  - **Fundamentals of Cloud Security:** Learned to secure cloud environments using policies, technologies, and controls to protect data and infrastructure.
  - **Cybersecurity Fundamentals:** Covered foundational concepts like risk management, threat landscapes, and defense mechanisms.
  - **Network Security Fundamentals:** Developed knowledge of network security, including firewalls, intrusion detection systems, and best practices.
- **Hands-on Experience:**
  - Applied theoretical knowledge to practical challenges in cybersecurity.
  - Explored real-world tools and methodologies for securing networks, data, and cloud environments.
- **Technical Tools Used:**
  - Hands-on exposure to tools and technologies relevant to SOC operations, network security, and cloud security management.
- **Skill Development:**
  - Strengthened analytical and problem-solving abilities by addressing cybersecurity challenges, such as identifying vulnerabilities and mitigating risks.
  - Enhanced technical understanding of modern cybersecurity practices and tools.
- **Key Outcomes:**
  - Comprehensive understanding of cybersecurity fundamentals and practices.
  - Practical experience with cybersecurity challenges, tools, and methodologies.
  - Preparedness for advanced roles in cybersecurity and related fields.

This internship provided a robust foundation in cybersecurity and a deeper understanding of industry standards and practices, equipping me for future endeavors in this domain

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Full Form
SOC	Security Operations Center
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
API	Application Programming Interface
OAuth	Open Authorization
ZAP	Zed Attack Proxy
PCCET	Palo Alto Networks Certified Cybersecurity Entry-Level Technician
GUI	Graphical User Interface
REST	Representational State Transfer
IDS	Intrusion Detection System
NGFW	Next-Generation Firewall
IOT	Internet of Things
SCSE	School of Computing Science and Engineering

CHAPTER 1

INTRODUCTION

1.1 Objective of the Internship Project

The primary objective of the Palo Alto Networks Cybersecurity Virtual Internship was to provide practical knowledge and hands-on experience in cybersecurity. This included learning to identify and mitigate cyber threats, understanding the core principles of network and endpoint security, and gaining expertise in using tools such as Prisma Cloud and the Cortex platform. Additionally, the internship aimed to enhance problem-solving skills by engaging in real-world scenarios and assessments, preparing participants to address modern security challenges effectively

1.2 Problem Statement and Research Objectives:

During this internship, the key challenge was to understand and address the evolving cybersecurity threats in various domains, including network, cloud, and endpoint security. The research objective was to explore innovative solutions for threat detection and prevention, enhance system resilience against potential attacks, and develop a comprehensive understanding of security operations to ensure robust and efficient protection for organizational infrastructure

1.3 Description of the Internship Domain and Organization:

The internship focused on the domain of cybersecurity, which is critical in safeguarding digital infrastructure from evolving threats and vulnerabilities. This domain encompasses various areas, including network security, cloud security, endpoint protection, and threat intelligence, all of which play a vital role in protecting organizational assets and data.

The internship was conducted under the guidance of Palo Alto Networks, a global leader in cybersecurity solutions. Founded in 2005, Palo Alto Networks is renowned for its cutting-edge technologies and innovative products that address the ever-changing landscape of cybersecurity threats. The organization offers a comprehensive portfolio of solutions, including Next-Generation Firewalls, Prisma Cloud for cloud security, and Cortex for advanced threat intelligence and security automation. With a strong emphasis on innovation, Palo Alto Networks is committed to providing organizations with the tools and expertise needed to prevent cyberattacks and maintain operational resilience.

Through this internship, participants gained practical exposure to Palo Alto Networks' advanced security platforms and tools, enabling them to develop a deep understanding of cybersecurity principles and apply them effectively in real-world scenarios.

CHAPTER 2

INTERNSHIP ACTIVITIES

2.1 Tasks and Responsibilities:

During the internship, I was assigned several tasks aimed at enhancing my cybersecurity skills. These included:

- Configuring and managing network security using Palo Alto Networks Strata.
- Conducting threat analysis and prevention using Cortex and Prisma Cloud platforms.
- Completing hands-on assessments on advanced endpoint protection and infrastructure automation.
- Designing and implementing security models to identify and mitigate cyber threats.
- Performing real-time simulations to detect and respond to security incidents.
- Optimizing cloud security operations and ensuring secure data handling in cloud-native environments.

2.2 Daily/Weekly Progress:

Week 1: Introduction to Cybersecurity

- Learned the basics of cybersecurity, including threat prevention and endpoint protection.
- Explored Palo Alto Networks' platforms like Prisma Cloud and Cortex.
- Studied the core principles of cybersecurity operations and threat intelligence**.**

Week 2: Network Security Fundamentals

- Understood networking concepts such as addressing and security protocols.
- Completed assessments on Palo Alto Networks Strata and Network Security Fundamentals.
- Configured and managed firewall policies for network protection.

Week 3: Threat Prevention and Analysis

- Gained practical knowledge of advanced threat detection techniques.
- Conducted assessments on Attack Techniques and Cyberthreat Analysis.
- Utilized threat intelligence tools to identify and mitigate cyber threats.

Week 4: Cloud Security Essentials

- Studied cloud computing principles and security models.
- Learned to secure cloud-native environments using Prisma Cloud.
- Completed assessments on Cloud Security Fundamentals and Cloud Application Protection Platform.

Week 5: Hands-on with Security Operations

- Explored the Cortex platform for security automation and orchestration.
- Performed real-time simulations to detect and respond to security incidents.
- Conducted assessments on Elements of Security Operations and Infrastructure Automation.

Week 6: Advanced Endpoint Protection

- Learned to protect endpoint devices against advanced threats.
- Conducted assessments on Advanced Endpoint Protection and Threat Prevention.
- Optimized endpoint security strategies to minimize vulnerabilities.

Week 7: Vulnerability Testing and Optimization

- Performed vulnerability testing to identify security loopholes.
- Enhanced operational efficiency using security orchestration tools.
- Implemented caching mechanisms to optimize security response times.

Week 8: Data Security and Compliance

- Applied data encryption techniques for secure communication.
- Learned and implemented compliance measures as per industry standards.
- Completed assessments on Security Models and Cybersecurity Landscape.

Week 9: Finalizing the Cybersecurity Portfolio

- Reviewed all completed tasks and resolved any pending issues.
- Prepared a portfolio showcasing all cybersecurity projects and assessments.
- Conducted a presentation summarizing key learnings and challenges faced.

Week 10: Submission and Review

- Submitted the completed tasks and cybersecurity projects.
- Presented findings and solutions implemented during the internship to mentors.

- Received feedback on performance and documented overall learnings from the internship.

2.3 Skills or Tools Used:

During the Palo Alto Networks Cybersecurity Virtual Internship, the following skills and tools were utilized to enhance knowledge and practical expertise:

Cybersecurity Skills:

- Threat Intelligence and Prevention
- Advanced Endpoint Protection
- Network Security Configuration
- Cloud Security Operations
- Security Automation and Orchestration
- Vulnerability Assessment and Penetration Testing
- Incident Response and Remediation
- Data Encryption and Secure Communication
- Compliance with Security Standards (e.g., GDPR, ISO 27001)
- Security Model Design and Implementation

Tools and Platforms:

1. **Palo Alto Networks Tools:**
    - Prisma Cloud: For securing cloud-native applications and cloud infrastructure.
    - Cortex Platform: For security automation, threat detection, and response.
    - Palo Alto Networks Strata: For managing and configuring Next-Generation Firewalls.
2. **Security and Networking Tools:**
    - Wireshark: For packet analysis and network traffic monitoring.
    - Metasploit: For penetration testing and identifying vulnerabilities.
    - Nmap: For network scanning and mapping.
    - Snort: For intrusion detection and prevention.
3. **Cloud and API Tools:**
    - REST APIs: For secure integration and communication with cloud platforms.
    - Postman: For testing API requests and analyzing responses.
4. **Automation and Orchestration Tools:**
    - Terraform: For infrastructure automation.

- Demisto: For security orchestration and incident response workflows.

5. **Development and Analysis Tools:**
   - Python: For scripting and automating security tasks.
   - Bash: For managing and configuring Linux environments.
   - Android Studio (for mobile security testing): For app debugging and vulnerability analysis.
6. **Compliance and Vulnerability Testing Tools:**
   - OpenVAS: For vulnerability scanning and risk management.
   - Burp Suite: For testing web application security.
   - OWASP ZAP (Zed Attack Proxy): For identifying application vulnerabilities.
7. **Other Security Concepts and Libraries:**
   - OAuth 2.0: For secure API authentication.
   - SharedPreferences (Android Security): For managing user preferences securely.

These tools and skills provided a robust foundation for understanding and tackling complex cybersecurity challenges in real-world scenarios.

CHAPTER 3

LEARNING OUTCOMES

3.1 Skills Acquired:

Technical Skills:

- Proficiency in using Palo Alto Networks platforms such as Prisma Cloud, Cortex, and Strata.
- Expertise in configuring and managing network security policies.
- Advanced knowledge of threat intelligence, endpoint protection, and security automation.
- Hands-on experience with tools like Wireshark, Metasploit, Nmap, and Snort for network and vulnerability analysis.
- Understanding and implementation of OAuth 2.0 for secure API authentication.
- Skills in scripting and automation using Python and Bash.
- Proficiency in using Terraform and Demisto for security orchestration and infrastructure automation.
- Knowledge of cloud-native security solutions and secure data encryption techniques.

Soft Skills:

- Effective time management to complete tasks and assessments within deadlines.
- Problem-solving and analytical thinking to address complex cybersecurity challenges.
- Collaboration and teamwork during group discussions and mentorship sessions.
- Communication skills enhanced through presentations and reporting of key findings.
- Attention to detail while performing vulnerability testing and compliance checks.
- Adaptability to learn and apply new tools and technologies in cybersecurity.

3.2 Knowledge Gained:

- Gained a comprehensive understanding of cybersecurity principles, including threat intelligence, endpoint protection, and cloud security operations.
- Learned the importance of designing secure and scalable security architectures to protect organizational assets.
- Understood the need for proactive threat detection and automated response mechanisms to minimize risks.

- Acquired hands-on experience in configuring and managing advanced security tools for real-world applications.

3.3 Problem-Solving or Challenges Faced:

- **Challenge 1:** Addressing advanced threats across network and cloud environments.
  Solution: Utilized Palo Alto Networks' tools like Prisma Cloud and Cortex to analyze and mitigate threats effectively.
- **Challenge 2:** Optimizing performance in security automation workflows.
  Solution: Leveraged security orchestration tools such as Demisto to streamline and enhance workflow efficiency.

CHAPTER 4

PROJECT/WORK DELIVERABLES

4.1 Main Project/Tasks Completed

Cybersecurity Operations Enhancement:

- **Objective:**
  The primary goal was to enhance organizational security operations by utilizing advanced tools and implementing modern cybersecurity solutions.
- **Key Features:**
  - Real-time threat detection and prevention: Configured and managed Palo Alto Networks' Cortex platform for monitoring and addressing threats.
  - Cloud security integration: Secured cloud environments using Prisma Cloud for risk assessment and policy enforcement.
  - Security automation: Implemented automated workflows with Demisto to streamline incident response and log analysis.
  - Compliance and risk management: Conducted vulnerability assessments and ensured adherence to industry standards for data security.
- **Process:**
  - Utilized Prisma Cloud to identify vulnerabilities in cloud-native environments and applied remediation strategies.
  - Analyzed network traffic and detected attack vectors using the Cortex platform.
  - Conducted penetration tests with tools like Metasploit and Wireshark to simulate and mitigate real-world attacks.
  - Automated routine security tasks using Demisto to enhance workflow efficiency and reduce manual efforts.

4.2 Outcomes of Work

- **Technical Outcomes:**
  - Gained proficiency in Palo Alto Networks' tools for cybersecurity operations.
  - Successfully identified and mitigated vulnerabilities across network, endpoint, and cloud environments.
- **Performance Improvements:**
  - Reduced threat response times through automation and streamlined incident handling.

    - Strengthened organizational security by implementing robust threat prevention measures.
- **User-Centric Design:**
    - Simplified security workflows to ensure accessibility for team members with varying technical expertise.
    - Developed clear, detailed reports and dashboards for visibility into security operations.

4.3 Links or Attachments

1. **Presentation Slides:**
    - Summarizes the project's objectives, tools used, challenges faced, and key outcomes.
2. **Screenshots and Reports:**
    - Includes visuals of Cortex dashboards, Prisma Cloud analysis reports, and automation workflows implemented with Demisto.
3. **History Of Report**

Activity Name	Status	Duration	Completed On	Award
Security Operations Fundamentals	**Passed**	**1 h 20 m**	**8/29/2024**	**Yes**
Cloud Security Fundamentals	**Passed**	**1 h 25 m**	**8/29/2024**	**Yes**
Cybersecurity Fundamentals	**Passed**	**1 h 45 m**	**8/29/2024**	**Yes**
Network Security Fundamentals	**Passed**	**1h 50 m**	**8/28/2024**	**Yes**

CHAPTER 5

CONCLUSION

5.1 Reflections

The Palo Alto Networks Cybersecurity Virtual Internship was an invaluable experience that provided comprehensive knowledge and hands-on expertise in modern cybersecurity practices. Through engaging with advanced tools such as Prisma Cloud, Cortex, and Demisto, I developed a solid foundation in key areas like network security, cloud protection, and threat intelligence. These tools allowed me to address complex security challenges while learning to implement scalable and effective solutions.

The internship emphasized practical learning, including configuring security policies, automating workflows, and conducting vulnerability assessments. These tasks improved my technical skills and prepared me for real-world scenarios. Additionally, the focus on automation and orchestration expanded my understanding of optimizing security operations to enhance efficiency and response times.

Alongside technical expertise, the program helped me cultivate essential soft skills such as problem-solving, communication, and time management. Regular interactions with mentors and team discussions enabled me to refine my ability to analyze challenges, present solutions, and adapt to feedback.

This internship has equipped me with the tools and confidence to tackle cybersecurity challenges while fostering a commitment to continuous learning. It was a transformative journey that has prepared me to contribute effectively to securing digital infrastructures and protecting organizational assets in a dynamic cybersecurity landscape.