SHORT-TERM INTERNSHIP
(Virtual)

Designed & Developed by

Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)

Internship report submitted in partial fulfilment of the requirements for the Award of

Bachelor of Computer Applications - Data Science

By

PAMPANA JAI KIRAN (2021-2222043)

Under the guidance of

Smt. U. Sahiti

Assistant Professor

Department of Computer Applications (PG)

Gayatri Vidya Parishad College for Degree and P.G. Courses (A)

Affiliated to Andhra University

Visakhapatnam

2023-24.

SHORT-TERM INTERNSHIP
(Virtual)

Name of the Student: PAMPANA JAI KIRAN

Name of the College: Gayatri Vidya Parishad College for Degree and P.G. Courses (A)

Registration Number: 2021-2222043

Period of Internship: From: September To: November

Name & Address of the Intern Organization Eduskills

ANDHRA UNIVERSITY

YEAR 2023-24

An Internship Report on

Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)

Submitted in accordance with the requirement for the degree of

BCA-Data Science

Under the Faculty Guideship of

Smt. U. Sahiti

Department of Computer Applications (PG)

Gayatri Vidya Parishad College for Degree and P.G. Courses (A)

Submitted by:

PAMPANA JAI KIRAN

Regd. No: 2021-2222043

Department of Computer Applications (UG)

Gayatri Vidya Parishad College for Degree and P.G. Courses (A)

Instructions to Students

Please read the detailed Guidelines on Internship hosted on the website of the AP State Council of Higher Education **https://apsche.ap.gov.in**

1. It is mandatory for all the students to complete 2 months (180 hours) of short- term internship either physically or virtually.
2. Every student should identify the organization for internship in consultation with the College Principal/the authorized person nominated by the Principal.
3. Report to the intern organization as per the schedule given by the College. You must make your own arrangements for transportation to reach the organization.
4. You should maintain punctuality in attending the internship. Daily attendance is compulsory.
5. You are expected to learn about the organization, policies, procedures, and processes by interacting with the people working in the organization and by consulting the supervisor attached to the interns.
6. While you are attending the internship, follow the rules and regulations of the intern organization.
7. While in the intern organization, always wear your College Identity Card.
8. If your College has a prescribed dress as uniform, wear the uniform daily, as you attend to your assigned duties.
9. You will be assigned a Faculty Guide from your College. He/She will be creating a WhatsApp group with your fellow interns. Post your daily activity done and/or any difficulty you encounter during the internship.
10. Identify five or more learning objectives in consultation with your Faculty Guide. These learning objectives can address:
    a. Data and Information you are expected to collect about the organization and/or industry.
    b. Job Skills you are expected to acquire.
    c. Development of professional competencies that lead to future career success.

11. Practice professional communication skills with team members, co-interns, and your supervisor. This includes expressing thoughts and ideas effectively through oral, written, and non-verbal communication, and utilizing listening skills.
12. Be aware of the communication culture in your work environment. Follow up and communicate regularly with your supervisor to provide updates on your progress with work assignments.
13. Never be hesitant to ask questions to make sure you fully understand what you need to do your work and to contribute to the organization.
14. Be regular in filling up your Program Book. It shall be filled up in your own handwriting. Add additional sheets wherever necessary.
15. At the end of internship, you shall be evaluated by your Supervisor of the intern organization.
16. There shall also be evaluation at the end of the internship by the Faculty Guide and the Principal.
17. Do not meddle with the instruments/equipment you work with.
18. Ensure that you do not cause any disturbance to the regular activities of the intern organization.
19. Be cordial but not too intimate with the employees of the intern organization and your fellow interns.
20. You should understand that during the internship programme, you are the ambassador of your College, and your behavior during the internship programme is of utmost importance.
21. If you are involved in any discipline related issues, you will be withdrawn from the internship programme immediately and disciplinary action shall be initiated.
22. Do not forget to keep up your family pride and prestige of your College.

Student's Declaration

I **PAMPANA JAI KIRAN** student of Under Graduate program, Regd.no **2021-2222043** of the department of **BCA-Data Science** of **Gayatri Vidya Parishad College for Degree and P.G. Courses (A)** do hereby declare that I have completed the mandatory internship from **September** to **November** in **Eduskills** under the faculty guideship of **Smt. U. Sahiti**.

Signature

Date

Certificate from Intern Organization

This is to certify that **PAMPANA JAI KIRAN** Regd.no **2021-2222043** of **Gayatri Vidya Parishad College for Degree and P.G. Courses (A)** underwent internship in Eduskills from **September** to **November**.

The overall performance of the intern during his/her internship is found to be _____(Satisfactory/Not Satisfactory).

Authorized Signatory with Date and Seal

Endorsements

Faculty Guide

Head of the Department

Principal

Acknowledgements

I am deeply indebted to Gayatri Vidya Parishad College for Degree and P.G. Courses (A),Visakhapatnam, affiliated to Andhra University for awarding Graduation in BCA-Data Science to pursue my short-term Internship on "**Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)"** acknowledged by APSCHE and supported by authorities concerned.

I am thankful to ***Prof. S. Rajani, Principal,*** Gayatri Vidya Parishad College for Degree and P.G Courses (A) for support and encouragement in the completion of the project work.

I am also thankful to ***Prof. I. S. Pallavi, Director of MCA,*** Gayatri Vidya Parishad College for Degree and P.G Courses (A), for extending support in the completion the of study.

I am also thankful to ***Sri. P. Venkata Rao, Associate Professor & HOD of BCA,*** Gayatri Vidya Parishad College for Degree and P.G Courses (A), for suggestions and encouragement.

Our sincere thanks to our project guide ***Smt. U. Sahiti, Assistant Professor,*** Gayatri Vidya Parishad College for Degree and P.G Courses (A), for her support and valuable suggestions for the completion of the internship.

I am also thankful to the college authorities, all the teaching staff and non-teaching staff of Gayatri Vidya Parishad College for Degree and P.G.Courses (A) who have been a constant source of support and encouragement during the study tenure.

I am thankful to the Eduskills Foundation and my college authority members for providing a virtual internship. I specially thank one and all who have directly and indirectly contributed to the completion of the short-term internship.

CONTENTS

CHAPTER 1: EXECUTIVE SUMMARY

The internship report shall have only a one-page executive summary. It shall include five or more Learning Objectives and Outcomes achieved, a brief description of the sector of business and intern organization and a summary of all the activities done by the intern during the period.

Learning objectives and outcomes:

Learning Objectives:

1. **Hands-On Experience:** Provide interns with practical, hands-on experience related to their field of study or career interests.
2. **Skill Development:** Enhance specific technical and soft skills relevant to the industry or profession.
3. **Networking Opportunities:** Facilitate connections between interns and professionals in the industry, promoting networking and relationship-building.
4. **Problem-Solving Skills:** Encourage interns to address real-world challenges and develop problem-solving skills.
5. **Teamwork and Collaboration:** Foster teamwork and collaboration skills by involving interns in group projects or collaborative tasks.

Outcomes:

1. **Resume Enhancement:** Strengthen the intern's resume with practical experience, making them more competitive in the job market.
2. **Improved Confidence:** Boost interns' confidence in their abilities through successful completion of tasks and projects.
3. **Career Clarity:** Help interns gain a clearer understanding of their career goals and preferences through exposure to different aspects of the industry.

CHAPTER 2: OVERVIEW OF THE ORGANIZATION

Suggestive contents

A. *Introduction of the Organization*
B. *Vision, Mission, and Values of the Organization*
C. *Policy of the Organization, in relation to the intern role*
D. *Organizational Structure*
E. *Roles and responsibilities of the employees in which the intern is placed.*
F. *Performance of the Organization in terms of turnover, profits, market reach and market value.*
G. *Future Plans of the Organization.*

A. Introduction of the Organization.

Palo Alto Networks, Inc. is an American multinational cybersecurity company with headquarters in Santa Clara, California. The core product is a platform that includes advanced firewalls and cloud-based offerings that extend those firewalls to cover other aspects of security. The company serves over 70,000 organizations in over 150 countries, including 85 of the Fortune 100. It is home to the Unit 42 threat research team and hosts the Ignite cybersecurity conference. It is a partner organization of the World Economic Forum.

In 2018, Palo Alto Networks was listed 8th in the Forbes Digital 100. In June 2018, former Google and SoftBank executive Nikesh Arora joined the company as Chairman and CEO.

B. Vision, Mission, and Values of the Organization.

Vision: "A world where each day is safer and more secure than the one before." This vision encapsulates their dedication to continuously improving the state of cybersecurity and protecting organizations from evolving threats.

MISSION: "To be the cybersecurity partner of choice, protecting our digital way of life." Let's unpack this statement to understand its implications:

Cybersecurity Partner of Choice: This signifies their desire to be the preferred provider of security solutions for organizations, building trust and exceeding expectations. It emphasizes their commitment to customer satisfaction and providing tailored solutions that fit specific needs.

Protecting Our Digital Way of Life: This broader focus extends beyond individual organizations. They recognize the integral role of cybersecurity in enabling safe and secure online activities for everyone, from businesses to individuals. Their mission reflects a societal responsibility to address evolving cyber threats and safeguard the digital world we rely on.

VALUES OF THE ORGANISATION: Palo Alto Networks emphasizes five core values that guide their culture and decision-making:

1. Disruption: They encourage innovative thinking and challenging the status quo in the cybersecurity landscape. They aim to disrupt traditional approaches and develop groundbreaking solutions that redefine security.

2. Execution: They prioritize efficiency and effectiveness in everything they do. They value clear goals, decisive action, and delivering results on time and within budget.

3. Collaboration: They foster a culture of teamwork and knowledge sharing across all levels of the organization. They believe that diverse perspectives and collaboration are essential for driving innovation and success.

4. Integrity: They prioritize ethical conduct and transparency in all their dealings. They value building trust with customers, partners, and employees through honesty and open communication.

5. Inclusion: They strive to create a welcoming and diverse environment where everyone feels valued and empowered to contribute. They believe that inclusion leads to a richer and more productive work experience for everyone.

C. Policy of the Organization, in relation to the intern role.

- Corporate Governance: This outlines the framework for how Palo Alto Networks is managed and controlled, including the roles and responsibilities of the board of directors, management team, and shareholders.
- Code of Conduct: This defines the ethical standards expected of all Palo Alto Networks employees, contractors, and partners. It covers areas like conflicts of interest, insider trading, harassment, and discrimination.
- Sustainability Policy: This outlines Palo Alto Networks' commitment to environmental responsibility and social good. It may address energy efficiency, waste reduction, community engagement, and other sustainability initiatives.
- Diversity and Inclusion Policy: This affirms Palo Alto Networks' commitment to creating a diverse and inclusive workplace where everyone feels valued and respected. It may outline specific goals and initiatives for promoting diversity and inclusion across the company.
- Security Policy: This encompasses the company's overall approach to cybersecurity, including its internal security practices, data protection measures, and incident response procedures.

- Product Security Policy: This outlines the specific security measures taken to ensure the security and reliability of Palo Alto Networks' products and services.

D. Organizational Structure.

Leadership:

- Executive Team: Led by CEO Nikesh Arora, the executive team comprises leaders responsible for overall strategic direction and key functions like sales, marketing, product development, finance, and legal.
- Board of Directors: Oversees the company's performance and governance, ensuring adherence to regulations and stakeholder interests.

Business Units:

- Products: Responsible for product development, engineering, and lifecycle management of Palo Alto Networks' security solutions.
- Sales: Focuses on driving revenue growth through direct and channel sales partnerships.
- Services: Provides professional services like security consulting, deployment, and training.
- Marketing: Creates brand awareness, generates leads, and drives demand for Palo Alto Networks' solutions.
- Support: Offers technical support and customer service to ensure customer satisfaction.

Geographic Regions:

- Americas: Covers North and South America, with regional headquarters in Santa Clara, California.
- EMEA: Covers Europe, the Middle East, and Africa, with regional headquarters in Dublin, Ireland.
- APAC: Covers Asia Pacific, with regional headquarters in Singapore.

Other Important Units:

- Human Resources: Handles employee recruitment, development, and benefits.
- Finance: Manages financial operations, investments, and reporting.
- Legal: Provides legal counsel and ensures compliance with regulations.
- Research & Development: Focuses on cutting-edge security technologies and future innovations.

E. Roles and responsibilities of the employees in which the intern is placed.

Internship Placements:

Interns at Palo Alto Networks can be placed in various teams depending on their skills, interests, and the company's needs. Some common placements include:

- Product Development: Interns may work on software development, testing, user experience research, or technical writing.

- Sales & Marketing: Interns may assist with market research, lead generation, content creation, or event planning.
- Security Operations: Interns may gain experience in threat analysis, incident response, or security research.
- Finance & Legal: Interns may work on financial analysis, data visualization, or contract review.

Roles & Responsibilities around the Intern:

The specific roles and responsibilities of employees surrounding an intern will vary depending on the placement. However, here are some general examples:

- Mentors: Senior employees who guide and support the intern, providing them with training, feedback, and opportunities to learn new skills.
- Teammates: Other employees on the same team who collaborate with the intern on projects and tasks.
- Managers: Leaders who oversee the intern's work, provide performance feedback, and help them achieve their goals.

CHAPTER 3: INTERNSHIP PART

Description of the Activities/Responsibilities in the Intern Organization during Internship, which shall include - details of working conditions, weekly work schedule, equipment used, and tasks performed. This part could end by reflecting on what kind of skills the intern acquired.

Internships are a valuable way to gain newfound knowledge. I always maintain positive attitude and Read all the modules provided by them. Each module contains five articles. I used to do one thing that is I noted down the useful information from the articles. I always stayed focus and read all the topics very carefully. The equipment used while my Internship is going on is mobile, laptop, wi-fi , etc. I used to read all the topics and cleared all my doubts.

Benefits :

1. Learned new skills
2. Hands on experience
3. Skill development
4. Networking opportunities
5. Understanding compliance and regulations
6. Problem solving skills
7. Cyber security tools familiarity
8. Career guidance
9. Understanding corporate culture
10. Penetrated testing

A virtual internship was an opportunity to gain practical experience, develop skills, and expand one's professional network remotely.

ACTIVITY LOG FOR THE FIRST WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Received registration link from LMS Portal (To apply for internship through portal).	I applied and submitted my resume in my interested fields	
Day - 2	Enrolled at Eduskills site after applying at APSCHE LMS portal.	Enrolled at Eduskill site	
Day – 3	Received registration link to register for APSCHE-Eduskills virtual internship.	I registered for APSCHE Eduskills victual internship	
Day – 4	Received mail that I have been shortlisted for AICTE skills Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) virtual internship	I got to know that I have to complete the PCCET virtual internship	
Day – 5	Explained how to access LMS, How to complete my modules, How to do labs, How to accept badge, How to get certificate	I understood the process of completion of the course	
Day –6	What is Cyber security, Network security fundementals, Cyber security fundamentals, Cloud security fundamentals, Security operation fundamentals	Introduction to cyber security	

WEEKLY REPORT

WEEK – 1

Objective of the Activity Done:

Detailed Report:

Firstly, I received registration links for LMS Portal in our WhatsApp Group on September 28 2023 at 6:45 AM by our training and placement officer. I enrolled at Edu Skills site. I received a mail from Edu skills foundation providing the registration link to register for APSCHE Edu Skills virtual internship. I received an application mail from Edu skills foundation that I have been shortlisted for AICTE. Palo Alto cyber security virtual internship. through this mail they also inform me that the course has to be completed by October 31st.

They explained about why cyber security is used, it is all about protecting information systems and technology from unauthorized access, use, disclosure, disruption, modification, or destruction**.** It encompasses a broad range of activities and technologies aimed at safeguarding the systems and data we rely on every day.

I got to know about some tools which are used in cyber security, utilizing cyber security tools significantly enhances our ability to defend against cyber threats and safeguard our valuable digital assets. They boost efficiency, provide crucial insights, and empower security professionals to stay ahead of the ever-evolving threat landscape.

ACTIVITY LOG FOR THE SECOND WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Introduction to network security fundamentals The courses teach endpoint security prevention for threats like malware, viruses, ransomware, and phishing attacks.	Introduce IP addressing, subnetting, TCP/IP and OSI models, packet lifecycle, and encapsulation.	
Day - 2	The Connected Globe	This course will also provide details about connected devices, routing, area networks, and protocols.	
Day – 3	Networking and Addressing	The fundamentals of IP addressing, subnetting, TCP/IP and OSI models, packet lifecycle, and encapsulation.	
Day – 4	Endpoint Security	How to prevent various threats, including malware, viruses, ransomware, and phishing attacks.	
Day – 5	Network security	Including concepts recognize and potentially defend home networks and mission-critical infrastructure.	
Day –6	Palo Alto Networks Strata	This course introduces Palo Alto Networks network-security solutions.	

WEEKLY REPORT

WEEK – 2

Objective of the Activity Done:

Detailed Report:

This course introduces the fundamentals of the connected globe. This course will also provide details about connected devices, routing, area networks, and protocols.

Describes IP addressing, Describe subnetting, List the TCP/IP and OSI model layers, Detail the lifecycle of a packet, Detail how data is encapsulated.

It introduces the fundamentals of endpoint security on how to prevent various threats, including malware, viruses, ransomware, and phishing attacks. Explain how to explore endpoint and mobile device security using technology such as personal firewalls, host-based IPS, and management features

It introduces the fundamentals of network security including concepts you must understand to recognize and potentially defend home networks and mission-critical infrastructure. Network security technologies such as packet filtering, stateful inspection, application firewalls, and IDS and IPS and web content filters

Learn how to properly secure enterprise networks through PAN-OS deployment templates and migration options and DNS, URL Filtering, Threat Prevention, and WildFire® subscription services.

ACTIVITY LOG FOR THE THIRD WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Introduction to Cybersecurity fundamentals They provide insights into malware and ransomware types.	Discuss current attack methods, defense strategies, public Wi-Fi risks, and protection measures.	
Day - 2	Cybersecurity Landscape	It covers various security regulations and standards, identifies different cybersecurity threats and attacker profiles.	
Day – 3	Cyberthreats	In-depth understanding of malware and ransomware, their types, objectives, and properties.	
Day – 4	Attack Techniques	Covers current cyberattack methods, defense strategies, public Wi-Fi network risks, and protection measures.	
Day – 5	Security Models	In-depth understanding of security models, focusing on perimeter-based and Zero Trust security models.	
Day –6	Security Operating Platform	Describes the evolving landscape of cybercrime, the challenges faced by organizations	

WEEKLY REPORT

WEEK – 3

Objective of the Activity Done:

Detailed Report:

I learnt about the modern cybersecurity landscape, SaaS challenges, security regulations, standards, threats, attacker profiles, and cyberattack lifecycle steps. They provide insights into malware and ransomware types, objectives, properties, and the relationship between vulnerabilities and exploits.

It discuss current attack methods, defense strategies, public Wi-Fi risks, and protection measures. They delve into security models, focusing on perimeter-based and Zero Trust models, and explore the evolving landscape of cybercrime, organizational challenges, and employee roles in maintaining security. Lastly, the courses describe Palo Alto Networks' prevention architecture, its role in addressing cybersecurity challenges, and the key capabilities required for preventing successful cyberattacks.

It provides an in-depth understanding of security models, focusing on perimeter-based and zero-trust security models.

This course describes the evolving landscape of cybercrime, the challenges faced by organizations, and the importance of understanding the role of employees in maintaining security. It also describes the prevention architecture of the Palo Alto Networks portfolio, how it addresses cybersecurity challenges, and the key capabilities required to enable the prevention of successful cyberattacks.

ACTIVITY LOG FOR THE FORTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Introduction to Cloud security fundamentals They explain how cloud-native application protection platforms (CNAPP).	Cover the core technologies used in cloud computing, such as virtual machines and containers, development operations teams, and the CI/CD pipeline.	
Day - 2	Fundamentals of Cloud Security: Cloud Native Technologies	This course describes the core technologies that are used in cloud computing, such as virtual machines and containers.	
Day – 3	Fundamentals of Cloud Security: Cloud Computing Overview	Overview of cloud computing including cloud computing models, shared responsibility, best practices, and hybrid cloud computing.	
Day – 4	Cloud Security Operations	Describes the models and processes by which organizations use cloud technologies.	
Day – 5	Cloud Application Protection Platform	How CNAPP provide comprehensive protection with integrated security and complince capabilities	
Day –6	Prisma Cloud	How the Prisma Cloud platform detects security risks using a cloud native application protection platform.	

WEEKLY REPORT

WEEK – 4

Objective of the Activity Done:

Detailed Report:

In this week I have learnt about the core technologies used in cloud computing, such as virtual machines and containers, development operations teams, and the CI/CD pipeline. They provide an overview of cloud computing models, shared responsibility, best practices, and hybrid cloud computing. The courses discuss the models and processes organizations use for cloud technologies, common software development models, and the supporting teams. They explain how cloud-native application protection platforms (CNAPP) offer comprehensive protection with integrated security and compliance capabilities for cloud-native applications in development and production. Lastly, the courses provide insights into how the Prisma Cloud platform prevents and detects security risks using a cloud-native application protection platform.

This course describes an overview of cloud computing including cloud computing models, shared responsibility, best practices, and hybrid cloud computing.

I learn how cloud-native application protection platforms (CNAPP) provide comprehensive protection with integrated security and compliance capabilities that protect cloud-native applications across development and production.

It provides an overview of how the Prisma Cloud platform prevents and detects security risks using a cloud-native application protection platform.

ACTIVITY LOG FOR THE FIFTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Introduction to Security operations fundamentals They introduce endpoint protection with the Cortex XDR agent, which combines behavioural protection and AI-based analysis.	Cover the daily life of a SecOps analyst, the six elements of security operations, and how SOAR technology simplifies cybersecurity response and prevention.	
Day - 2	Elements and Processes	Describes the daily life of a security operations (SecOps) analyst and the six elements of security operations.	
Day – 3	Infrastructure and Automation	Describes how the security orchestration, automation, and response (SOAR) technology.	
Day – 4	Advance Endpoint Protection	Introduces endpoint protection with the Cortex XDR agent combines industry-best behavioral protection and AI.	
Day – 5	Threat Prevention and Intelligence	Provides a high-level overview of Cortex XSOAR Threat Intelligence Management (TIM)	
Day –6	The Cortex platform	Cortex XSOAR, Cortex XDR, Cortex XSOAR TIM, and Cortex XSIAM.	

WEEKLY REPORT

WEEK – 5

Objective of the Activity

Done: Detailed Report:

In this week I have learnt about the daily life of a SecOps analyst, the six elements of security operations, and how SOAR technology simplifies cybersecurity response and prevention. They introduce endpoint protection with the Cortex XDR agent, which combines behavioural protection and AI-based analysis to stop advanced attacks. The courses provide a high-level overview of Cortex XSOAR Threat Intelligence Management (TIM), a security solution for automating and streamlining threat intelligence processes, including native threat intelligence, data sources, incident enrichment, and threat intel reports. Finally, the courses introduce the products in the Palo Alto Networks Cortex platform: Cortex XSOAR, Cortex XDR, Cortex XSOAR TIM, and Cortex XSIAM.

Every SecOps professional wants fewer alerts, more efficient tools, and faster containment. In today's security operations centers, alerts are overflowing as attackers deftly change their tactics.

Elements of Security Operations details the building blocks of simpler, more effective security operations, drawing from our experts' real-world experiences to help you build capabilities that deserve your confidence. You'll learn how you can:

- Simplify operations by integrating and consolidating tools
- Automate repetitive tasks to better use your analyst talent
- Consistently enforce policy across networks, clouds, and endpoints
- Rapidly respond to threats with deep visibility and contextual insight

CHAPTER 4: OUTCOMES DESCRIPTION

Describe the work environment you have experienced.

Work environments can vary significantly depending on the industry, company culture, and specific job roles. For individuals in the field of cybersecurity or those pursuing certifications in the Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET), the work environment may

1. Remote Access

- Many cybersecurity professionals, including entry-level technicians, work virtually. providing flexibility and eliminating the need for physical presence in an office.

2. Collaborative Spaces:

- Digital tools for collaboration, including video conferencing tools (Zoom, Microsoft Teams), messaging platforms (Slack, Microsoft Teams), and project management tools (Trello, Asana).

3. Technology Infrastructure:

- The work environment is likely to be equipped with advanced technology infrastructure, including computers, servers, and networking equipment. Security tools and software specific to cybersecurity tasks will also be prevalent.

4. Security Measures:

- Given the nature of the work, there will be a heightened focus on security within the workplace. This may include secure access controls, monitoring systems, and policies to safeguard sensitive information.

5. Online Communication Norms:

- Effective written communication skills are crucial. Interns need to communicate clearly and professionally through emails, messages, and other online platforms.

6. Digital Security Awareness:

- Interns must adhere to cybersecurity practices to ensure the security of the organization's data. This includes awareness of phishing risks and following digital security protocols.

7. Emphasis on Compliance:

- Depending on the industry, there may be a strong emphasis on compliance with regulatory standards and frameworks. This could shape the work environment to ensure that cybersecurity practices align with legal and industry requirements.

8. Professional Development Opportunities:

- Virtual interns may have access to online workshops, webinars, and training sessions to enhance their skills and knowledge in their respective fields.

A virtual internship work environment requires adaptability, effective digital communication, and the ability to navigate and utilize various online tools and platforms. It provides valuable experience in remote collaboration, which has become increasingly relevant in the modern workforce.

Describe the real time technical skills you have acquired.

Palo Alto Networks and the inferred focus areas of the Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET), here are some potential technological developments and trends that may be relevant to the subject area of training:

1. **Next-Generation Firewalls (NGFW):**
    - Ongoing advancements in NGFW technologies, including the integration of threat intelligence, behavior-based analysis, and advanced policy management.
2. **Cloud Security:**
    - Continued developments in cloud security solutions, especially those related to securing cloud-based applications and services.
3. **Endpoint Protection:**
    - Evolution of endpoint protection mechanisms, with a focus on behavior-based detection, response, and integration with threat intelligence.
4. **Threat Intelligence and Analysis:**
    - Advances in threat intelligence platforms and tools, emphasizing real-time analysis and proactive threat prevention.
5. **Security Orchestration and Automation:**
    - Growing importance of security orchestration and automation to streamline security workflows and respond to incidents more effectively.
6. **Zero Trust Architecture:**
    - Adoption and implementation of Zero Trust principles to enhance security by assuming zero trust even within the corporate network.

7. **Incident Response and Forensics:**
    - Continuous developments in incident response and digital forensics techniques, with an emphasis on rapid identification and mitigation of security incidents.
8. **Cloud-native Security Solutions:**
    - Integration of cloud-native security solutions, such as those offered by Palo Alto Networks' Prisma Cloud, to address security challenges in cloud environments.

These technological developments reflect the dynamic nature of the cybersecurity landscape and the need for cybersecurity professionals, including those pursuing the PCCET certification, to stay informed and adapt to emerging challenges and solutions.

Describe the managerial skills you have acquired.

Leadership skills :

Leadership skills are one of the soft skills that many employees look for in candidates and that can be helpful at all levels of our career. From managing a team to contributing to a project in a leadership role, leadership skills help us to motivate others and ensure tasks are completed promptly.

Teamwork skills :

Teamwork skills are important asset to any candidate who is a part of an organization or who works with other individual in their daily operations.

Behavioral skills :

Behavioral skills that allows you to interact with and work well with others. These skills enable you to build relationships, communicate effectively and handle situations.

Workmanship skills :

Workmanship skills are skills that enable you to learn new things and adapt to new situations within the workspace having good workmanship skills can setup us apart from other candidates and show employees your willingness to learn and change when necessary.

Time management skills :

Time management skills are that allows us to manage time and be productive as possible within the workplace. These skills ensures privilege tasks effectively focus on our professional growth and contribute to our organization as a whole.

Continuous Learning:

Willingness to learn and adapt to new technologies, industry trends, and management methodologies. Engaging in ongoing learning opportunities, courses, and certifications.

Describe how you could improve your communication skills.

Improving communication skills involves a multifaceted approach that addresses various aspects of both oral and written communication. Here are strategies to enhance different facets of communication:

Oral Communication:

1. **Practice Public Speaking:**
    - Engage in public speaking opportunities, such as joining a club or participating in events. Practice helps build confidence and fluency.
2. **Record and Evaluate Yourself:**
    - Record your speeches or presentations and review them to identify areas for improvement. Pay attention to tone, pace, and clarity.
3. **Join Toastmasters or Similar Groups:**
    - Toastmasters International offers a supportive environment for practicing and improving public speaking, leadership, and communication skills.
4. **Expand Vocabulary:**
    - Regularly read and learn new words to expand your vocabulary. This enhances your ability to articulate ideas effectively.
5. **Eye Contact and Body Language:**
    - Maintain eye contact to convey confidence and sincerity. Pay attention to your body language to ensure it aligns with your message.
6. **Receive Constructive Feedback:**
    - Seek feedback from peers or mentors. Constructive criticism helps identify areas for improvement.

Written Communication:

1. **Grammar and Punctuation:**
    - Brush up on grammar and punctuation rules. Clear and correct writing enhances your message's impact.

2. **Proofread:**
    - Always proofread your written communication before sending it. Correct spelling and grammatical errors to maintain professionalism.
3. **Clarity and Conciseness:**
    - Strive for clarity and conciseness in your writing. Clearly articulate your points without unnecessary complexity.
4. **Tailor Communication to the Audience:**
    - Adapt your writing style to suit the audience. Ensure that your message is accessible and relevant to the reader.
5. **Expand Writing Styles:**
    - Practice different writing styles, such as emails, reports, and proposals. Versatility in writing enhances your overall communication skills.

Conversational Abilities:

1. **Active Listening:**
    - Develop active listening skills. Show genuine interest in others' perspectives and respond thoughtfully.
2. **Ask Open-ended Questions:**
    - Encourage meaningful conversations by asking open-ended questions. This promotes dialogue and deeper understanding.
3. **Stay Informed:**
    - Stay updated on current events and industry trends. This provides conversational fodder and allows you to contribute meaningfully.

Confidence Levels and Anxiety Management:

1. **Visualization Techniques:**
    - Visualize successful communication scenarios to build confidence. Picture yourself speaking confidently and effectively.

2. **Breathing Exercises:**
    - Practice deep breathing exercises to manage anxiety. Controlled breathing helps calm nerves before speaking.
3. **Gradual Exposure:**
    - Gradually expose yourself to challenging communication situations. Incremental exposure helps build confidence over time.

Understanding Others and Being Understood:

1. **Empathy:**
    - Cultivate empathy to understand others' perspectives. This promotes effective communication and relationship-building.
2. **Clarification:**
    - If unsure, seek clarification during conversations. It's better to ensure understanding than to make assumptions.

Extempore Speech and Articulation:

1. **Regular Practice:**
    - Engage in regular extempore speaking practice. It sharpens your ability to think on your feet and articulate thoughts coherently.
2. **Thematic Preparation:**
    - Stay informed about current topics to be prepared for extempore speeches. This enhances your ability to speak confidently on a variety of subjects.

Closing Conversations, Maintaining Niceties, Greeting, Thanking, and Appreciating Others:

1. **Politeness and Gratitude:**
    - Cultivate a habit of expressing gratitude. Thank others genuinely, whether through a thank-you note, email, or in person.
2. **Closing with Purpose:**
    - Conclude conversations with clarity and purpose. Summarize key points, express appreciation, and provide next steps if applicable.

3. **Active Greetings:**
    - Practice active and warm greetings. A friendly demeanor sets a positive tone for communication.
4. **Acknowledgment:**
    - Acknowledge others' contributions and express appreciation. Recognizing others fosters positive relationships.

Remember that improvement is an ongoing process, and consistent effort in these areas will contribute significantly to enhancing your overall communication skills. Regular self-assessment and a willingness to learn from each experience are key components of continuous improvement.

Describe how you could enhance your abilities in group discussions, participation in teams, contribution as a team member, and leading a team/activity.

Enhancing your abilities in group discussions, participation in teams, contribution as a team member, and leading a team/activity requires a combination of communication skills, collaboration, and leadership qualities.

Group Discussions and Participation:

1. **Active Listening:**
    - Practice active listening by focusing on the speaker, maintaining eye contact, and avoiding distractions. This ensures you fully understand others' perspectives.
2. **Confidence:**
    - Build confidence in expressing your ideas. Start by contributing smaller points and gradually take on more prominent roles in discussions.
3. **Preparation:**
    - Before group discussions, research and gather information on the topic. Being well-prepared allows you to contribute more effectively.
4. **Constructive Feedback:**
    - Provide constructive feedback to others. Acknowledge their points, and if you disagree, do so respectfully, supporting your viewpoint with evidence.

Contribution as a Team Member:

1. **Teamwork Skills:**
    - Develop strong teamwork skills by understanding team dynamics, being supportive, and actively participating in collaborative efforts.

2. **Specialized Knowledge:**
    - Contribute your specialized knowledge or skills to complement the strengths of the team. This enhances your value as a team member.
3. **Flexibility:**
    - Be adaptable and open to different perspectives. Embrace change and be willing to modify your approach based on team decisions.
4. **Initiative:**
    - Take initiative by volunteering for tasks and demonstrating a proactive attitude. Show enthusiasm for the team's goals.
5. **Communication:**
    - Maintain clear and transparent communication within the team. Update team members on your progress and be receptive to their input.

Leading a Team/Activity:

1. **Vision and Goal Setting:**
    - Clearly articulate the team's vision and set achievable goals. Ensure that every team member understands their role in achieving these objectives.
2. **Effective Communication:**
    - Develop strong communication skills. Clearly convey expectations, provide feedback, and keep the team informed about project updates.
3. **Delegation:**
    - Learn effective delegation. Assign tasks based on team members' strengths and interests, and provide the necessary resources and support.
4. **Conflict Resolution:**
    - Develop skills in conflict resolution. Address conflicts promptly, promote open dialogue, and work towards solutions that benefit the entire team.

5. **Motivation:**
    - Motivate the team by recognizing and celebrating achievements. Encourage a positive and collaborative work environment.
6. **Decision-Making**:
    - Make informed decisions after considering input from team members. Foster a democratic decision-making process when appropriate.
7. **Continuous Improvement:**
    - Foster a culture of continuous improvement. Encourage feedback from the team, and be open to making adjustments based on lessons learned.
8. **Lead by Example:**
    - Demonstrate the qualities you expect from your team. Lead by example, exhibiting dedication, professionalism, and a strong work ethic.

Remember, improvement in these areas is an ongoing process. Regular self-reflection, feedback from peers, and a commitment to continuous learning will contribute significantly to your growth in group discussions, teamwork, and leadership roles.

Describe the technological developments you have observed and relevant to the subject area of training.

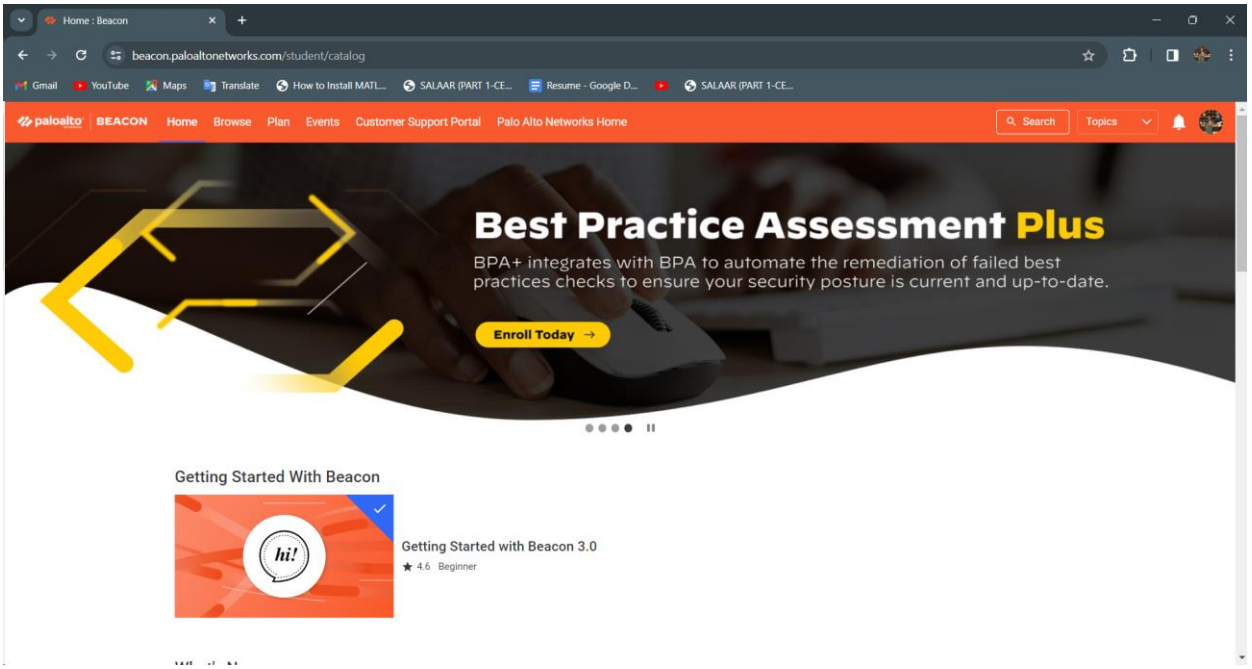
Palo Alto Networks and the inferred focus areas of the Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET), here are some potential technological developments and trends that may be relevant to the subject area of training:

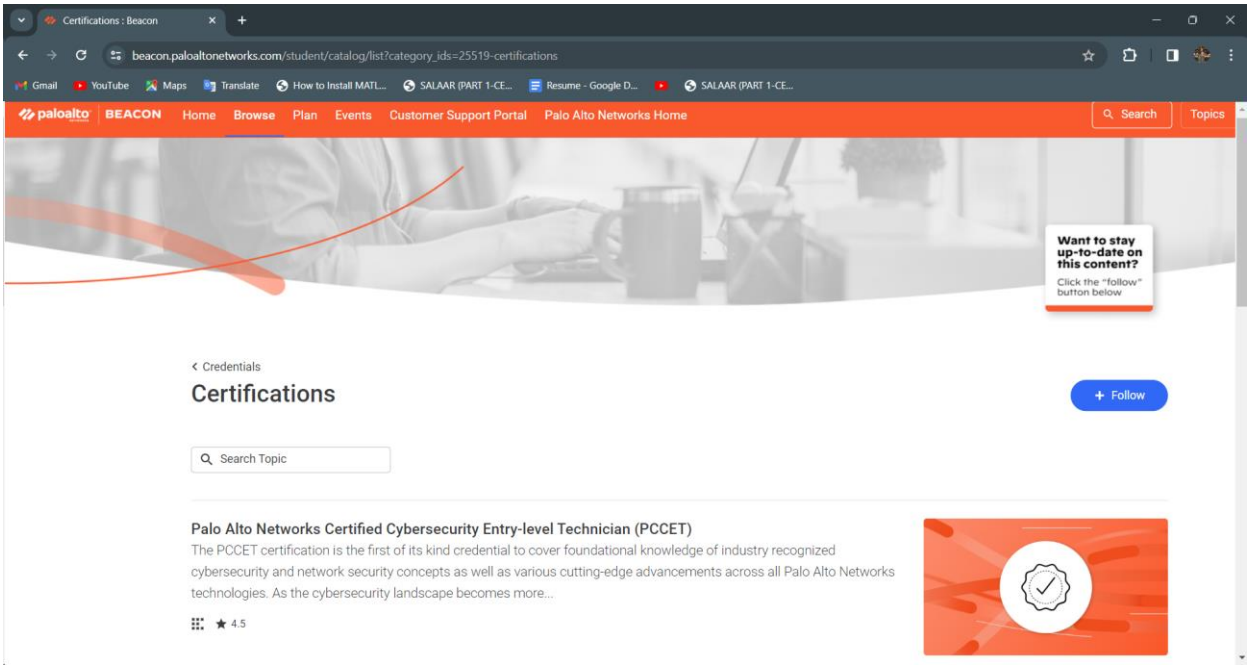
1. **Next-Generation Firewalls (NGFW):**
    - Ongoing advancements in NGFW technologies, including the integration of threat intelligence, behavior-based analysis, and advanced policy management.
2. **Cloud Security:**
    - Continued developments in cloud security solutions, especially those related to securing cloud-based applications and services.
3. **Endpoint Protection:**
    - Evolution of endpoint protection mechanisms, with a focus on behavior-based detection, response, and integration with threat intelligence.
4. **Threat Intelligence and Analysis:**
    - Advances in threat intelligence platforms and tools, emphasizing real-time analysis and proactive threat prevention.
5. **Security Orchestration and Automation:**
    - Growing importance of security orchestration and automation to streamline security workflows and respond to incidents more effectively.
6. **Zero Trust Architecture:**
    - Adoption and implementation of Zero Trust principles to enhance security by assuming zero trust even within the corporate network.

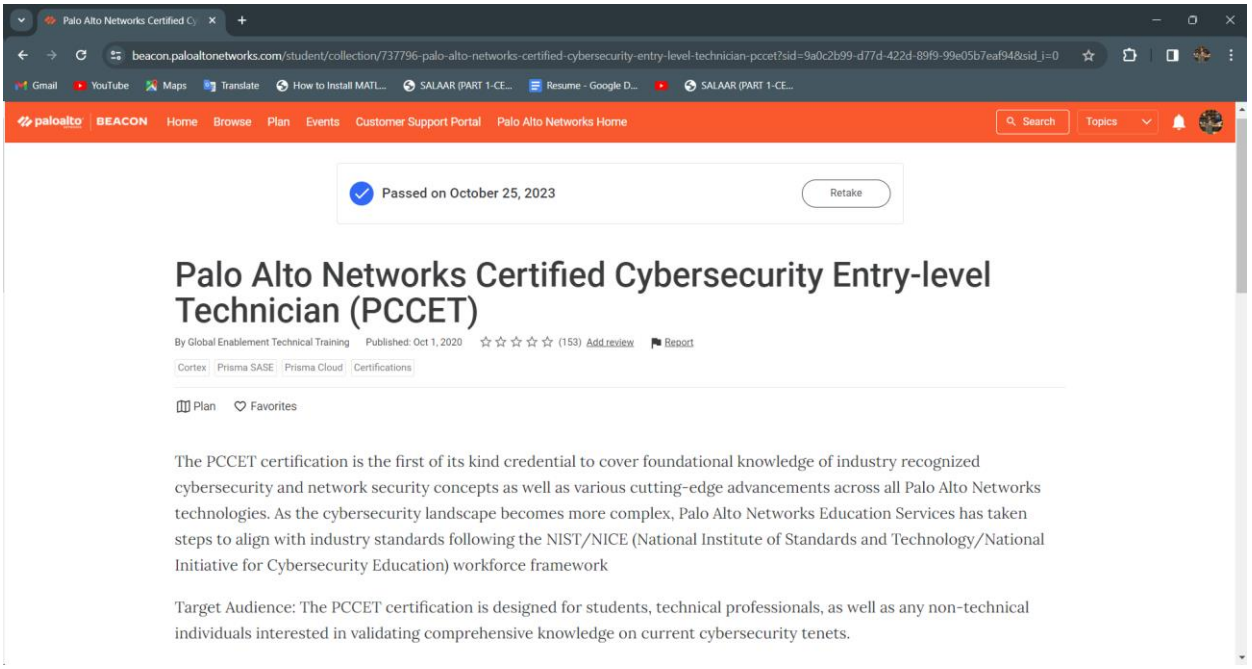
7. **Incident Response and Forensics:**
    - Continuous developments in incident response and digital forensics techniques, with an emphasis on rapid identification and mitigation of security incidents.
8. **Cloud-native Security Solutions:**
    - Integration of cloud-native security solutions, such as those offered by Palo Alto Networks' Prisma Cloud, to address security challenges in cloud environments.

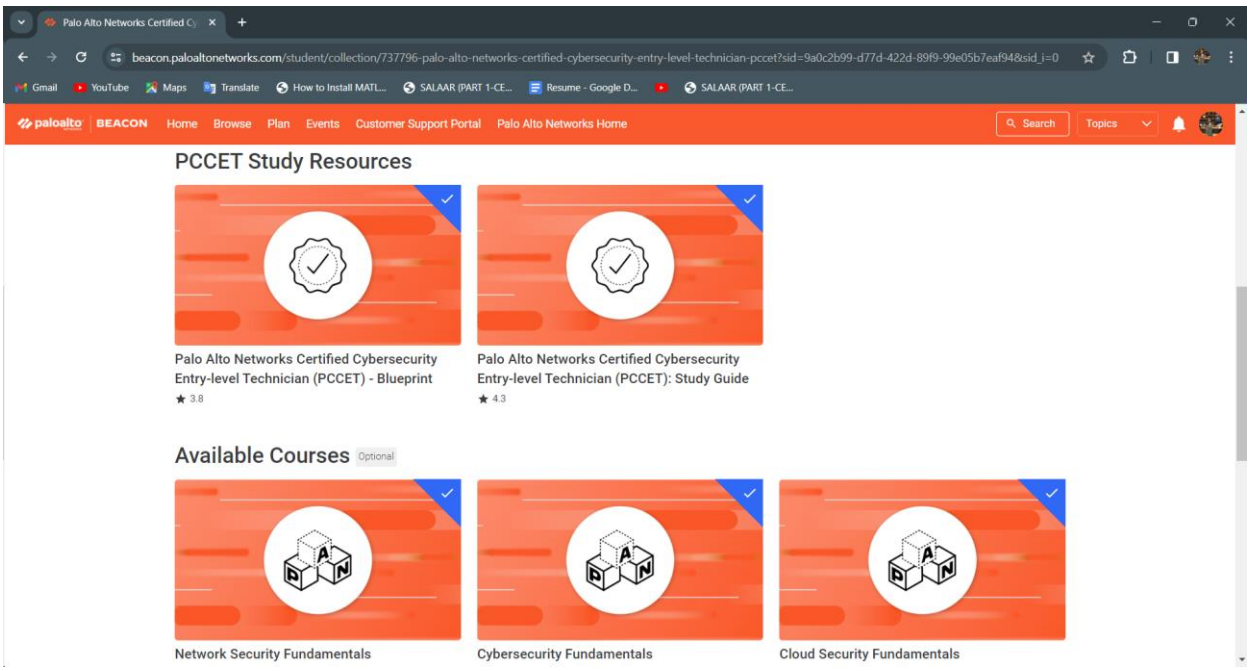
These technological developments reflect the dynamic nature of the cybersecurity landscape and the need for cybersecurity professionals, including those pursuing the PCCET certification, to stay informed and adapt to emerging challenges and solutions.

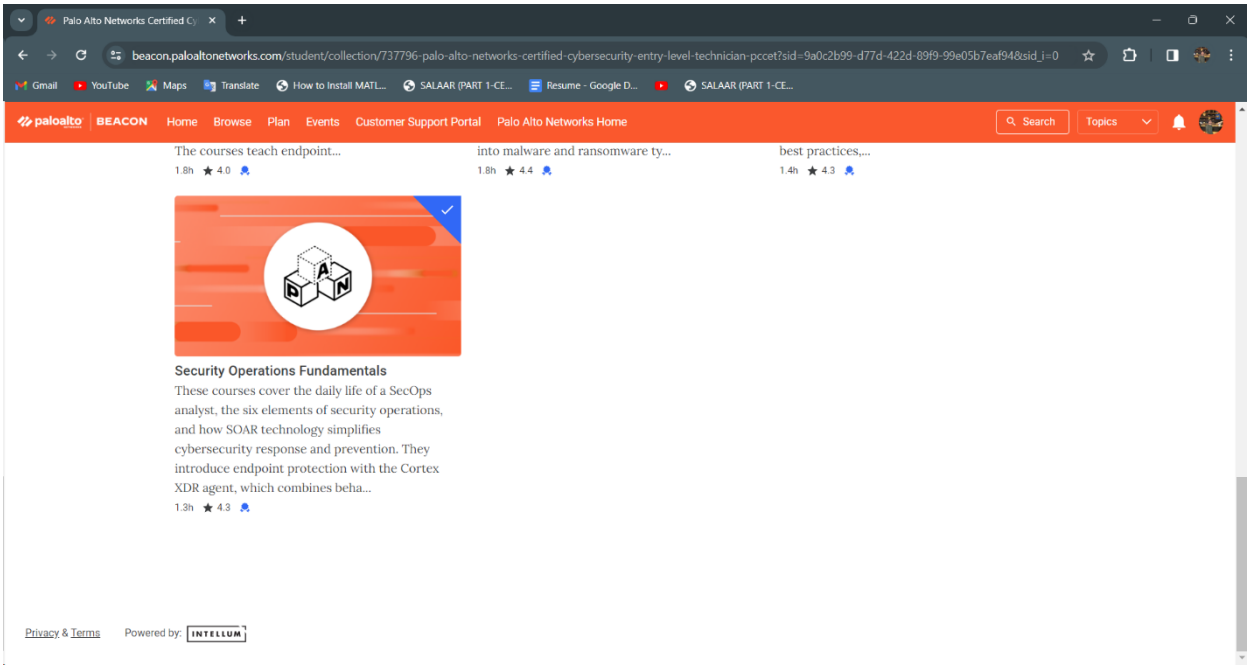
CHAPTER 5 - ANNEXURES

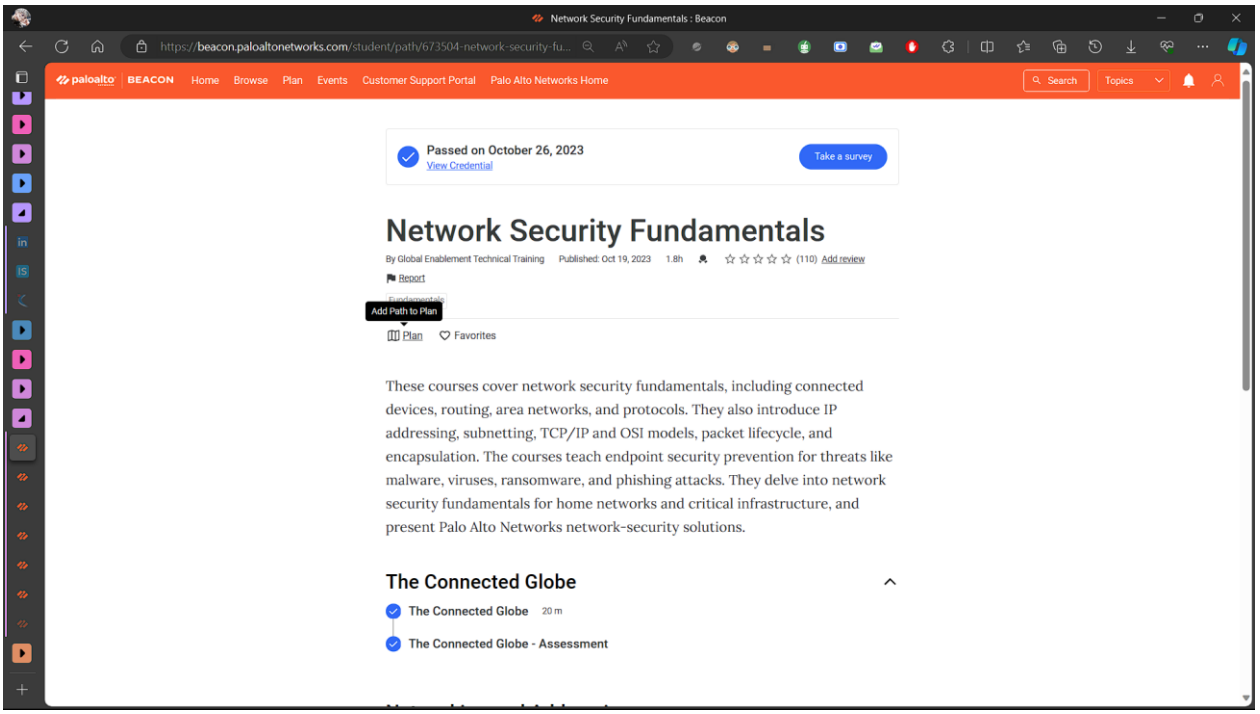


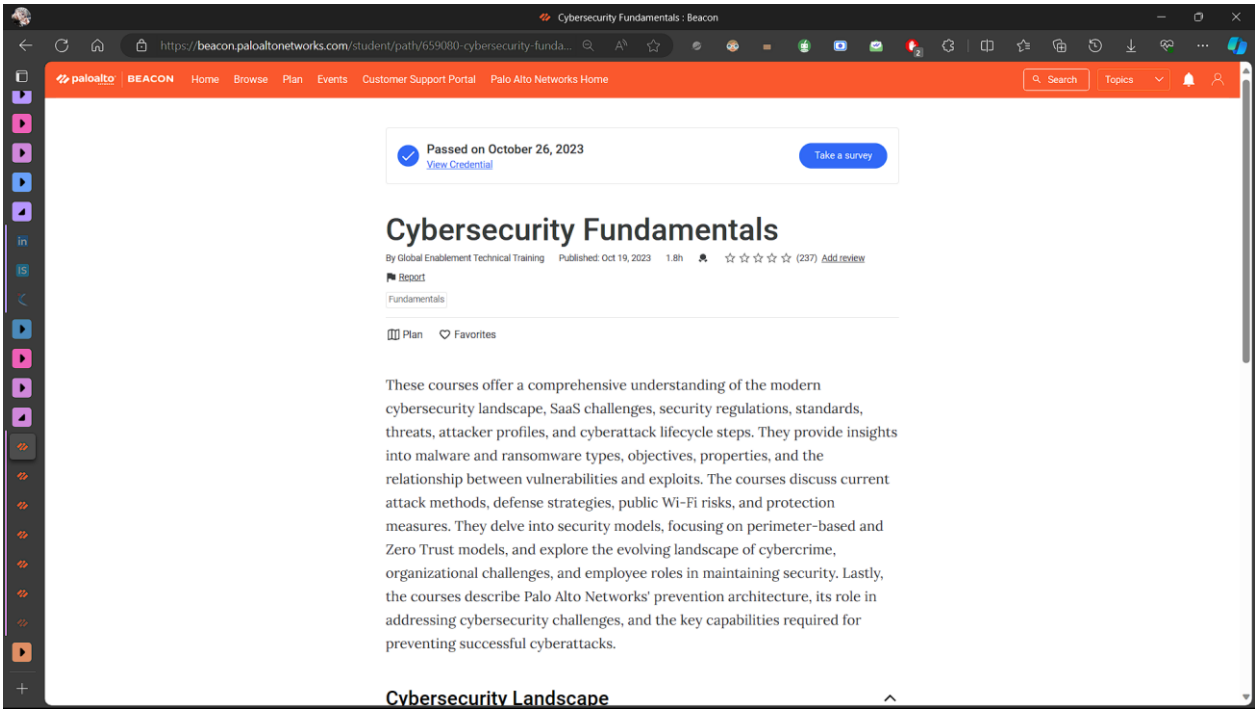


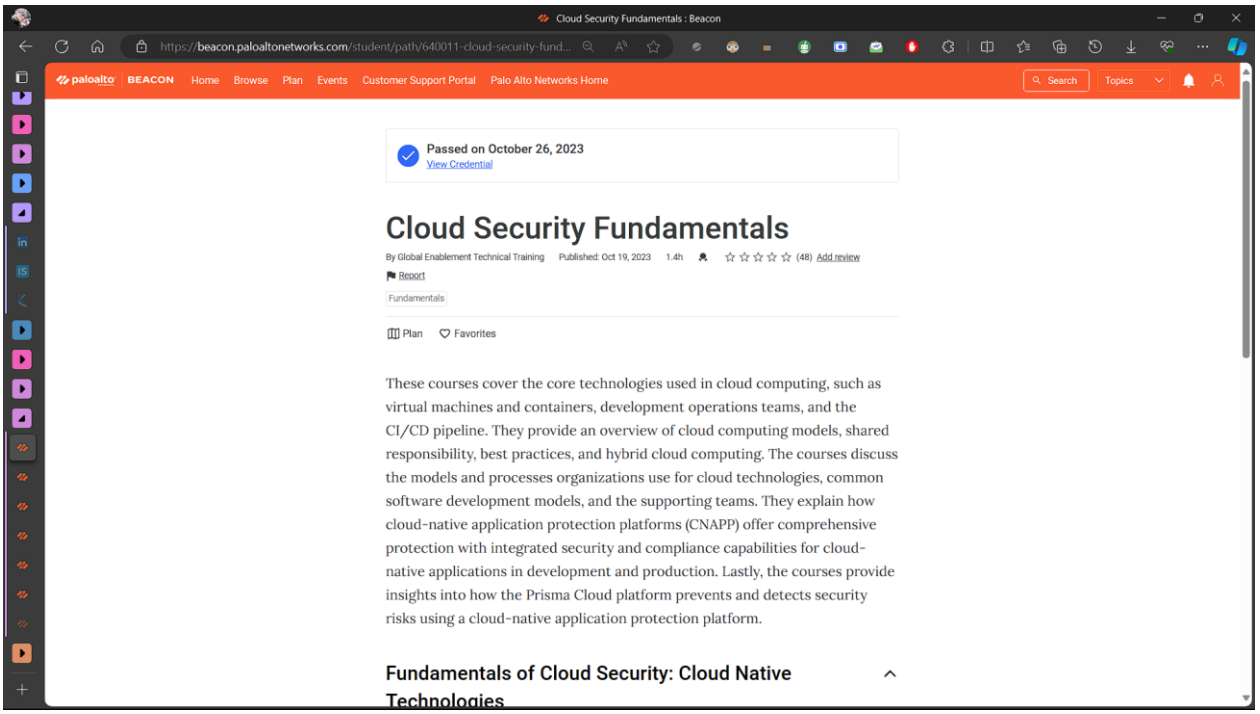

Palo Alto Networks Certified Cy
beacon.paloaltonetworks.com/student/collection/737796-palo-alto-networks-certified-cybersecurity-entry-level-technician-pccet?sid=9a0c2b99-d77d-422d-89f9-99e05b7eaf94&sid_i=0
Gmail
YouTube
Maps
Translate
How to Install MATL...
SALAAR (PART 1-CE...
Resume - Google D...
SALAAR (PART 1-CE...
paloalto
BEACON
Home
Browse
Plan
Events
Customer Support Portal
Palo Alto Networks Home
Search
Topics
Passed on October 25, 2023
Retake
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
By Global Enablement Technical Training
Published: Oct 1, 2020
(153)
Add review
Report
Cortex
Prisma SASE
Prisma Cloud
Certifications
Plan
Favorites
The PCCET certification is the first of its kind credential to cover foundational knowledge of industry recognized cybersecurity and network security concepts as well as various cutting-edge advancements across all Palo Alto Networks technologies. As the cybersecurity landscape becomes more complex, Palo Alto Networks Education Services has taken steps to align with industry standards following the NIST/NICE (National Institute of Standards and Technology/National Initiative for Cybersecurity Education) workforce framework
Target Audience: The PCCET certification is designed for students, technical professionals, as well as any non-technical individuals interested in validating comprehensive knowledge on current cybersecurity tenets.

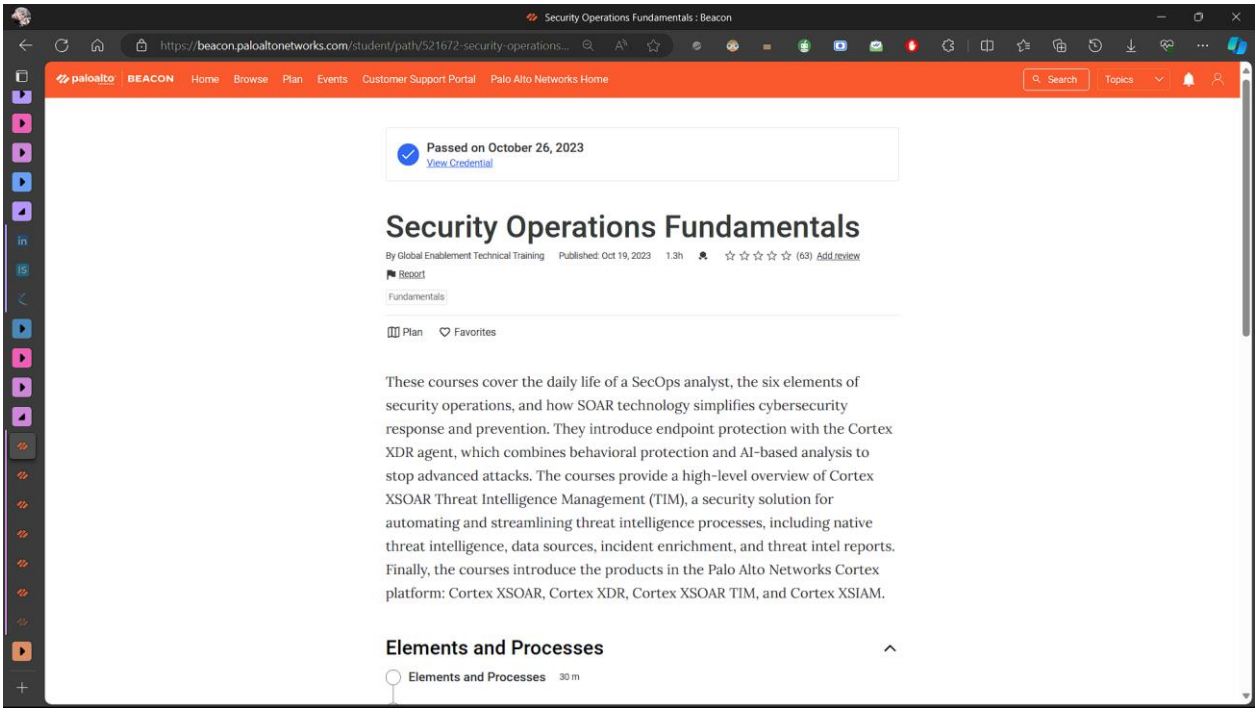

Palo Alto Networks Certified Cy
beacon.paloaltonetworks.com/student/collection/737796-palo-alto-networks-certified-cybersecurity-entry-level-technician-pccet?sid=9a0c2b99-d77d-422d-89f9-99e05b7eaf94&sid_i=0
Gmail
YouTube
Maps
Translate
How to Install MATL...
SALAAR (PART 1-CE...
Resume - Google D...
SALAAR (PART 1-CE...
paloalto
BEACON
Home
Browse
Plan
Events
Customer Support Portal
Palo Alto Networks Home
Search
Topics
PCCET Study Resources
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) - Blueprint
★ 3.8
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET): Study Guide
★ 4.3
Available Courses
Optional
Network Security Fundamentals
Cybersecurity Fundamentals
Cloud Security Fundamentals

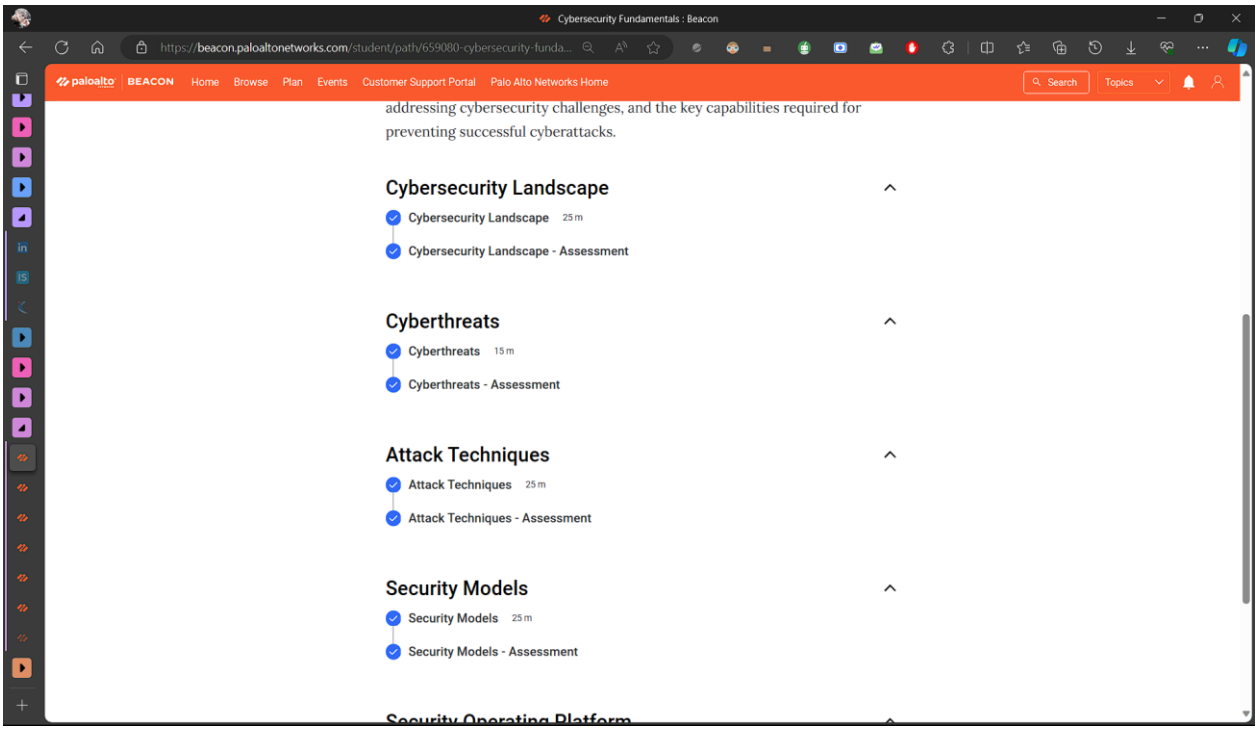

Palo Alto Networks Certified Cy
beacon.paloaltonetworks.com/student/collection/737796-palo-alto-networks-certified-cybersecurity-entry-level-technician-pccet?sid=9a0c2b99-d77d-422d-89f9-99e05b7eaf94&sid_i=0
Gmail
YouTube
Maps
Translate
How to Install MATL...
SALAAR (PART 1-CE...
Resume - Google D...
SALAAR (PART 1-CE...
paloalto BEACON
Home
Browse
Plan
Events
Customer Support Portal
Palo Alto Networks Home
Search
Topics
The courses teach endpoint...
1.8h ★ 4.0
into malware and ransomware ty...
1.8h ★ 4.4
best practices,...
1.4h ★ 4.3
Security Operations Fundamentals
These courses cover the daily life of a SecOps analyst, the six elements of security operations, and how SOAR technology simplifies cybersecurity response and prevention. They introduce endpoint protection with the Cortex XDR agent, which combines beha...
1.3h ★ 4.3
Privacy & Terms
Powered by: INTELLUM


Network Security Fundamentals : Beacon
https://beacon.paloaltonetworks.com/student/path/673504-network-security-fu...
paloalto BEACON
Home
Browse
Plan
Events
Customer Support Portal
Palo Alto Networks Home
Search
Topics
Passed on October 26, 2023
View Credential
Take a survey
Network Security Fundamentals
By Global Enablement Technical Training
Published: Oct 19, 2023
1.8h
(110) Add review
Report
Add Path to Plan
Plan
Favorites
These courses cover network security fundamentals, including connected devices, routing, area networks, and protocols. They also introduce IP addressing, subnetting, TCP/IP and OSI models, packet lifecycle, and encapsulation. The courses teach endpoint security prevention for threats like malware, viruses, ransomware, and phishing attacks. They delve into network security fundamentals for home networks and critical infrastructure, and present Palo Alto Networks network-security solutions.
The Connected Globe
The Connected Globe 20 m
The Connected Globe - Assessment


Cybersecurity Fundamentals : Beacon
https://beacon.paloaltonetworks.com/student/path/659080-cybersecurity-funda...
paloalto BEACON Home Browse Plan Events Customer Support Portal Palo Alto Networks Home
Search
Topics
Passed on October 26, 2023
View Credential
Take a survey
Cybersecurity Fundamentals
By Global Enablement Technical Training Published: Oct 19, 2023 1.8h (237) Add review
Report
Fundamentals
Plan
Favorites
These courses offer a comprehensive understanding of the modern cybersecurity landscape, SaaS challenges, security regulations, standards, threats, attacker profiles, and cyberattack lifecycle steps. They provide insights into malware and ransomware types, objectives, properties, and the relationship between vulnerabilities and exploits. The courses discuss current attack methods, defense strategies, public Wi-Fi risks, and protection measures. They delve into security models, focusing on perimeter-based and Zero Trust models, and explore the evolving landscape of cybercrime, organizational challenges, and employee roles in maintaining security. Lastly, the courses describe Palo Alto Networks' prevention architecture, its role in addressing cybersecurity challenges, and the key capabilities required for preventing successful cyberattacks.
Cybersecurity Landscape


Cloud Security Fundamentals : Beacon
https://beacon.paloaltonetworks.com/student/path/640011-cloud-security-fund...
paloalto BEACON Home Browse Plan Events Customer Support Portal Palo Alto Networks Home
Search
Topics
Passed on October 26, 2023
View Credential
Cloud Security Fundamentals
By Global Enablement Technical Training Published: Oct 19, 2023 1.4h (48) Add review
Report
Fundamentals
Plan
Favorites
These courses cover the core technologies used in cloud computing, such as virtual machines and containers, development operations teams, and the CI/CD pipeline. They provide an overview of cloud computing models, shared responsibility, best practices, and hybrid cloud computing. The courses discuss the models and processes organizations use for cloud technologies, common software development models, and the supporting teams. They explain how cloud-native application protection platforms (CNAPP) offer comprehensive protection with integrated security and compliance capabilities for cloud-native applications in development and production. Lastly, the courses provide insights into how the Prisma Cloud platform prevents and detects security risks using a cloud-native application protection platform.
Fundamentals of Cloud Security: Cloud Native Technologies


Security Operations Fundamentals : Beacon
https://beacon.paloaltonetworks.com/student/path/521672-security-operations...
paloalto BEACON Home Browse Plan Events Customer Support Portal Palo Alto Networks Home
Search
Topics
Passed on October 26, 2023
View Credential
Security Operations Fundamentals
By Global Enablement Technical Training Published: Oct 19, 2023 1.3h (63) Add review
Report
Fundamentals
Plan
Favorites
These courses cover the daily life of a SecOps analyst, the six elements of security operations, and how SOAR technology simplifies cybersecurity response and prevention. They introduce endpoint protection with the Cortex XDR agent, which combines behavioral protection and AI-based analysis to stop advanced attacks. The courses provide a high-level overview of Cortex XSOAR Threat Intelligence Management (TIM), a security solution for automating and streamlining threat intelligence processes, including native threat intelligence, data sources, incident enrichment, and threat intel reports. Finally, the courses introduce the products in the Palo Alto Networks Cortex platform: Cortex XSOAR, Cortex XDR, Cortex XSOAR TIM, and Cortex XSIAM.
Elements and Processes
Elements and Processes 30 m


Cybersecurity Fundamentals : Beacon
https://beacon.paloaltonetworks.com/student/path/659080-cybersecurity-funda...
paloalto BEACON Home Browse Plan Events Customer Support Portal Palo Alto Networks Home
Search
Topics
addressing cybersecurity challenges, and the key capabilities required for preventing successful cyberattacks.
Cybersecurity Landscape
Cybersecurity Landscape 25 m
Cybersecurity Landscape - Assessment
Cyberthreats
Cyberthreats 15 m
Cyberthreats - Assessment
Attack Techniques
Attack Techniques 25 m
Attack Techniques - Assessment
Security Models
Security Models 25 m
Security Models - Assessment

EVALUATION

Student Self Evaluation of the Short-Term Internship

Student Name: **Registration No:**

Term of Internship: **From:** **To :**

Date of Evaluation:

Organization Name & Address:

Please rate your performance in the following areas:

Rating Scale: **Letter grade of CGPA calculation to be provided**

1	Oral communication	1	2	3	4	5
2	Written communication	1	2	3	4	5
3	Proactiveness	1	2	3	4	5
4	Interaction ability with community	1	2	3	4	5
5	Positive Attitude	1	2	3	4	5
6	Self-confidence	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Work Plan and organization	1	2	3	4	5
9	Professionalism	1	2	3	4	5
10	Creativity	1	2	3	4	5
11	Quality of work done	1	2	3	4	5
12	Time Management	1	2	3	4	5
13	Understanding the Community	1	2	3	4	5
14	Achievement of Desired Outcomes	1	2	3	4	5
15	**OVERALL PERFORMANCE**	**1**	**2**	**3**	**4**	**5**

Date: **Signature of the Student**

Evaluation by the Supervisor of the Intern Organization

Student Name: **Registration No:**

Term of Internship: **From:** **To :**

Date of Evaluation:

Organization Name & Address:

Name & Address of the Supervisor with Mobile Number

Please rate the student's performance in the following areas:

Please note that your evaluation shall be done independent of the Student's self-evaluation

Rating Scale: 1 is lowest and 5 is highest rank

1	Oral communication	1	2	3	4	5
2	Written communication	1	2	3	4	5
3	Proactiveness	1	2	3	4	5
4	Interaction ability with community	1	2	3	4	5
5	Positive Attitude	1	2	3	4	5
6	Self-confidence	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Work Plan and organization	1	2	3	4	5
9	Professionalism	1	2	3	4	5
10	Creativity	1	2	3	4	5
11	Quality of work done	1	2	3	4	5
12	Time Management	1	2	3	4	5
13	Understanding the Community	1	2	3	4	5
14	Achievement of Desired Outcomes	1	2	3	4	5
15	**OVERALL PERFORMANCE**	**1**	**2**	**3**	**4**	**5**

Date: **Signature of the Supervisor**

Internal Evaluation for Short Term Internship
(Virtual)

Objectives:

- To integrate theory and practice.
- To learn to appreciate work and its function towards the future.
- To develop work habits and attitudes necessary for job success.
- To develop communication, interpersonal and other critical skills in the future job.
- To acquire additional skills required for the world of work.

Assessment Model:

- There shall only be internal evaluation.
- The Faculty Guide assigned is in-charge of the learning activities of the students and for the comprehensive and continuous assessment of the students.
- The assessment is to be conducted for 100 marks.
- The number of credits assigned is 4. Later the marks shall be converted into grades and grade points to include finally in the SGPA and CGPA.
- The weightings shall be:
    - Activity Log 25 marks
    - Internship Evaluation 50marks
    - Oral Presentation 25 marks
- Activity Log is the record of the day-to-day activities. The Activity Log is assessed on an individual basis, thus allowing for individual members within groups to be assessed this way. The assessment will take into consideration the individual student's involvement in the assigned work.
- While evaluating the student's Activity Log, the following shall be considered –

  a. The individual student's effort and commitment.

  b. The originality and quality of the work produced by the individual student.

  c. The student's integration and co-operation with the work assigned.

  d. The completeness of the Activity Log.

- The Internship Evaluation shall include the following components and based on Weekly Reports and Outcomes Description

    a. Description of the Work Environment.
    b. Real Time Technical Skills acquired.
    c. Managerial Skills acquired.
    d. Improvement of Communication Skills.
    e. Team Dynamics
    f. Technological Developments recorded.

MARKS STATEMENT

INTERNAL ASSESSMENT STATEMENT

Name Of the Student:
Programme of Study:
Year of Study:
Group:
Register No/H.T. No:
Name of the College:
University:

Sl.No	*Evaluation Criterion*	*Maximum Marks*	*Marks Awarded*
1.	Activity Log	25	
2.	Internship Evaluation	50	
3.	Oral Presentation	25	
	GRAND TOTAL	100	

Date:

Signature of the Faculty Guide

Certified by

Date:
Seal:

Signature of the
Head of the Department/Principal

Certificate of Completion

Jai Kiran Pampana

Has Successfully Completed

Cybersecurity Fundamentals

Date

10/26/2023

Michael Kelley
SVP, Worldwide Shared Services

paloalto NETWORKS

Cybersecurity Fundamentals

Completed by Jai Kiran Pampana on October 26, 2023

Certificate of Completion

Jai Kiran Pampana

Has Successfully Completed

Network Security Fundamentals

Date

10/26/2023

Michael Kelley
SVP, Worldwide Shared Services

paloalto NETWORKS

Network Security Fundamentals

Completed by Jai Kiran Pampana on October 26, 2023

Completion ID: 282668008

Certificate of Completion

Jai Kiran Pampana

Has Successfully Completed

Security Operations Fundamentals

Date

10/26/2023

Michael Kelley
SVP, Worldwide Shared Services

paloalto NETWORKS

Fundamentals of SOC (Security Operations Center)

Completed by Jai Kiran Pampana on October 26, 2023

Score: 95 Completion ID: 282678666

Certificate of Completion

Jai Kiran Pampana

Has Successfully Completed

Cloud Security Fundamentals

Date

10/26/2023

Michael Kelley
SVP, Worldwide Shared Services

paloalto NETWORKS

Fundamentals of Cloud Security

Completed by Jai Kiran Pampana on October 26, 2023

Score: 81 Completion ID: 282675088

ANDHRA PRADESH
STATE COUNCIL OF HIGHER EDUCATION

(A Statuory Body of the Government of Andhra Pradesh)

2nd, 3rd, 4th and 5th floors, Neeladri Towers, Sri Ram Nagar, 6th Battalion Road
Atmakur (V)Mangalagiri (M), Guntur, Andhra Pradesh, Pin - 522 503
www.apsche.ap.gov.in