CYBER SECURITY VIRTUAL INTERNSHIP

A Summer Internship report submitted in partial fulfilment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

(**Artificial Intelligence & Machine Learning**)

submitted by

CHIMMIRI SAI GANESH(208A1A4234)

Under the Guidance of

Mr. E.Akhil Babu

Asst. Professor

DEPARTMENT OF COMPUTER SCIENCE ANDENGINEERING

RISE KRISHNA SAI PRAKASAM GROUP OFINSTITUTIONS

(Approved by AICTE-NEW DELHI, Affiliated to JNTUK KAKINADA)

(An ISO Certified Institute, NBA accredited for B.Tech, in ECE,EEE,CE, ME and CSE, NAAC Accredited with 'A' Grade)

NH-16, Valluru, - 523272, Ongole, Prakasam District, A.P

2022-2023

RISE KRISHNA SAI PRAKASAM GROUP OF INSTITUTIONS

(Approved by AICTE-NEW DELHI, Affiliated to JNTUK KAKINADA)

(An ISO Certified Institute, NBA accredited for B.Tech, in ECE,EEE,CE, ME and CSE, NAAC Accredited with 'A' Grade)

NH-16, Valluru, - 523272, Ongole, Prakasam District, A.P

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the report entitled **"CYBERSECURITY VIRTUAL INTERNSHIP"**, that is being submitted by **CHIMMIRI SAI GANESH** of III Year I Semester bearing **208A1A4234**, in partial fulfillment for the award of the Degree of Bachelor of Technology in **Computer Science and Engineering** with specialization **ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING**, **RISE KRISHNA SAI PRAKASAM GROUP OF INSTUTIONS** is a record of bonafide work carried out by him.

Signature of Guide **Signature of Senior Faculty Member** **Signature of H.O.D**

Signature of External Examiner

Student's Declaration

I, **CHIMMIRI SAI GANESH** a student of **BACHELOR OF TECHNOLOGY** program, Reg.No: **208A1A4234** of the Department of **COMPUTER SCIENCE AND ENGINEERING** with specialization **ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING**, **RISE KRISHNA SAI PRAKASAM GROUP OF INSTITUTIONS** do hereby declare that I have completed the mandatory internship from JULY 2022 to SEPT 2022 in **CYBERSECURITY VIRTUAL INTERNSHIP** under the Faculty Guideship of **Mr.E.Akhil Babu , Asst. Professor**, Department of **COMPUTER SCIENCE AND ENGINEERING**, **RISE KRISHNA SAI PRAKASAM GROUP OF INSTITUTIONS**.

(Signature and Date)

Official Certification

This is to certify that **CHIMMIRI SAI GANESH** Reg. No: **208A1A4234** has completed his Internship in **CYBER SECURITY VIRTUAL INTERNSHIP** under my supervision as a part of partial fulfillment of the requirement for the degree of **BACHELOR OF TECHNOLOGY** in the department of **COMPUTER SCIENCE AND ENGINEERING** with specialization **ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING** in **RISE KRISHNA SAI PRAKASAM GROUP OF INSTITUTIONS.**

This is accepted for evaluation.

Endorsements

Faculty Guide:

E.Akhil Babu

Asst. Professor

Head of the Department:

Dr. D.V.V.S. PHANI KUMAR **M. Tech, Ph.D**

Asst. Professor

Copy of Certificate received from Intern Organisation:

N·E·A·T
प्रौद्योगिकी के लिए राष्ट्रीय शैक्षणिक सहयोग
National Educational Alliance for Technology

अखिल भारतीय तकनीकी शिक्षा परिषद्
All India Council for Technical Education

EduSkills®
Nation Building Through Skills

AICTE - EduSkills
2022
VIRTUAL INTERNSHIP

Virtual Internship Completion Certificate

This is to certify that

CHIMMIRI SAI GANESH

RISE Krishna Sai Prakasam Group of Institutions

has successfully completed 10 weeks

Cybersecurity Virtual Internship

during July - Sep 2022

Supported By paloalto Cybersecurity Academy

Saravanan Rajagopal
Training Partner Manager, APAC
Palo Alto Networks

Shri Buddha Chandrasekhar
Chief Coordinating Officer (CCO)
NEAT Cell, AICTE

Dr. Satya Ranjan Biswal
Chief Technology Officer (CTO)
EduSkills

Certificate ID :dcc2c7f7770908caa39de8d92c9b601a
Student ID :STU61cdb4e6495f91640871142

Acknowledgements

This internship opportunity I had with Cybersecurity was a great chance for learning and professional development. Therefore, I consider myself as a very lucky individual as I was provided with an opportunity to be a part of it. I am also grateful for having a chance to meet (Virtually) so many wonderful people and professionals who led me though this internship period.

Bearing in mind previous I am using this opportunity to express my deepest gratitude and special thanks to the Mentor(s) of Cybersecurity who in spite of being extraordinarily busy with her/his duties, took timeout to hear, guide and keep me on the correct path and allowing me to carry out my project at their esteemed organization and extending during the training.

I express my deepest thanks from the bottom of my heart sincerely to

E.Akhil Babu , Lecturer, RISE KRISHNA SAI PRAKASAM GROUP OF INSTITUTIONS, VALLURU. For taking part in useful decision & giving necessary advices and guidance and arranged all facilities to make our internship so successful. I choose this moment to acknowledge her contribution gratefully.

We would like to sincerely thank **Dr. D.V.V.S. Phani kumar**, Asst. Professor & HOD, Computer Science &Engineering, for providing all the necessary facilities that led to the successful completion of our report.

We would like to take this opportunity to thank our beloved Principal **Dr. A.V. BHASKAR RAO**, Ph.D, M. Tech, for providing a great support to us in completing our project and for giving us the opportunity of doing the internship report.

Finally, we would like to thank all of our friends and family members for their continuous help and encouragement.

It is my radiant sentiment to place on record my best regards, deepest sense of gratitude to the **All-India Council of Technical Education (AICTE)** and Edu Skills have launched the virtual internship program on cybersecurity supported by Palo Alto. The purpose of the internship is **to help students pursue a career in cybersecurity Mr. Nikesh Arora, CEO, Palo Alto Cybersecurity, Mr. NirZuk founder of Palo Alto Cybersecurity.**

I perceive as this opportunity as a big milestone in my career development. I will strive to use gained skills and knowledge in the best possible way, and I will continue to work on their improvement, in order to attain desired career objectives. Hope to continue cooperation with all of you in the future.

Sincerely,

Vision of the Institute	To be a premier institution in technical education by creating professionals of global standards with ethics and social responsibility for the development of the nation and the mankind.
Mission of the Institute	ImpartOutcomeBasedEducationthroughwellqualifiedanddedicatedfaculty.
	Provide state-of-the-art infrastructure and facilities for application-oriented research.
	Reinforce technical skills with life skills and entrepreneurship skills.
	Promotecutting-edgetechnologiestoproduceindustry-readyProfessionals.
	Facilitateinteractionwithallstakeholderstofosterideasandinnovation.
	In culcate moral values, professional ethics and social responsibility
Vision of the Department	To be a center of excellence in computer science and engineering for value-based education to serve humanity and contribute for socio-economic development..
Mission of the Department	Provide professional knowledge by student centric teaching-learning process to contribute software industry.
	Inculcate training on cutting edge technologies for industry needs.
	Create an academic ambiance leading to research.
	Promote industry institute interaction for real time problem solving.

Program Outcomes (POs):

PO1	**Engineering Knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering Problems
PO2	**Problem Analysis:** Identify, formulate, review research literature, and analyze complex Engineering problem searching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences
PO3	**Design/Development of Solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and Environmental considerations.
PO4	**Conduct Investigations of Complex Problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretationof data, and synthesis of the information provide valid conclusions
PO5	**Modern Tool Usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex Engineering activities with an understanding of the limitations
PO6	**The Engineer and Society:** Apply reasoning informed by the contextualknowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the Professional engineering practice.
PO7	**Environment and Sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the Knowledge of, and need for sustainable development.
PO8	**Ethics:** Applyethicalprinciplesandcommittoprofessionalethicsandresponsibilities and norms of the engineering practice
PO9	**Individual and Team Work:** Function effectively as an individual, and as amember or leader in diverse teams, and in multidisciplinary settings
PO10	**Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions
PO11	**Project Management and Finance:** Demonstrate knowledge and understandingof the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments
PO12	**Life-long Learning:** Recognize the need for, and have the preparation and abilityto engage in independent and life-long learning in the broadest context of technological change.

Program Educational Objectives (PEOs):

PEO1:	Develop software solutions for real world problems by applying Mathematics.
PEO2:	Function as members of multi-disciplinary teams and to communicate effectively using modern tools.
PEO3:	Pursue career in software industry or higher studies with continuous learning and apply Professional knowledge.
PEO4:	Practice the profession with ethics, integrity, leadership and social responsibility.

Program Specific Outcomes (PSOs):

PSO1	**Domain Knowledge:** Apply the Knowledge of Programming Languages, Networks and Databases for design and development of Software Applications.
PSO2	**Computing Paradigms:** Understand the evolutionary changes in computing possess knowledge of context aware applicability of paradigms and meet the challenges of the future.

ABSTRACT

Cyber security

Large companies are subject to millions of cyber attack each month. That's why tactical improvements aren't enough. Our Cyber security Maturity Assessment helps you develop a strategy to fend off most attacks and recover quickly from any that might succeed.

India is home to a population which is rooted in diverse socio-economic backgrounds. As per theliving standards of people, a wide range of devices are in use - from high-end secured electronic devices to low-cost mobile phones. This makes it difficult for authorities to set uniform legal andtechnical standards for regulating data-protection

That means going beyond today's typical approach, in which most companies simply allocate a set percentage of revenue or IT budget to security, without assessing their true needs. Effective cyber security requires a sustained effort that encompasses not only application security, penetration testing and incident management but also employee behaviour, third-party risks, and many other potential vulnerabilities.

Our Cyber security Maturity Assessment goes far beyond the scope of a typical security audit—itprovides a foundational analysis on which you can build a truly robust and resilient cyber security program. Our deep expertise in enterprise technology, cloud computing, digital operations, and other relevant areas ensures that we can help you not only develop a powerful cyber security strategy, but implement it effectively.

Organization Information

Palo Alto Cyber security Academy and Edu Skills have teamed up to create an outcome-driven skilling effort that will train 2000+ educators and 5000 students on Cyber security. This program has been recognized by APSCHE for delivery as a virtual internship program to all higher education students in India.

Index

CHAPTER 1

INTRODUCTION

Cyber Security is a process that's designed to protect networks and devices from external threats.Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

It is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services. The range of operations of cyber security involves protecting information and systems from major cyber threats.

These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in theirmost innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. The modern cybersecurity landscape is a rapidly evolving hostile environment with advanced threats and increasingly sophisticated threat actors. This lesson describes the current cybersecurity landscape, explains SaaS application challenges, describes various security and data protection regulations and standards, identify cybersecurity threats and attacker profiles, and explains the steps in the cyberattack lifecycle.

Modern cyberattack strategy has evolved from a direct attack against a high value server or asset("shock and awe") to a patient, multistep process that blends exploits, malware, stealth, and evasion in a coordinated network attack ("low and slow"). Attackers use a variety of techniques and attack types to achieve their objectives. Malware and exploits are integral to the modern cyberattack strategy. This lesson describes the different malware types and properties, the relationship between vulnerabilities and exploits, and how modern malware plays a central role ina coordinated attack against a target.

CHAPTER 2
DESCRIPTION OF INTERNSHIP

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-edgeadvancements 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.

TRAINING CURRICULUM

Introduction to Cyber Security

Fundamentals of Network Security

Fundamentals of Cloud Security

Fundamentals of SOC (Security Operation Centre)

PROGRAM SCHEDULE:

Virtual Internship Starts on: July 2022

Virtual Internship Ends on: September 2022

Certificate Distribution by: 26 October 2022

CHAPTER 3

WEEKLY ACTIVITIES

WEEKLY OVERVIEW OF INTERNSHIP ACTIVITIES

Week-1	Introduction to Cyber Security
Week-2	Introduction to Cyber Security
Week-3	Fundamentals of Network Security
Week-4	Fundamentals of Network Security
Week-5	Fundamentals of Network Security
Week-6	Fundamentals of Cloud Security
Week-7	Fundamentals of Cloud Security
Week-8	Fundamentals of Cloud Security
Week-9	Fundamentals of SOC (Security Operations)
Week-10	Fundamentals of SOC (Security Operations)

CHAPTER 4

MODULES

1. Introduction to Cyber Security

2. Fundamentals of Network Security

3.Fundamentals to Cloud Security

4.Fundamentals of SOC (Security Operation Centre)

5.Technology

6. Internship Reflection

7.Conclusion

4.1 Introduction to Cyber Security

This course introduces the fundamentals of cybersecurity, including the concepts needed to recognize and potentially mitigate attacks against home networks and mission-critical infrastructure.

After you complete this training, you should be able to:

- Describe the current cybersecurity landscape
- Identify cybersecurity threats
- Evaluate different malware types and cyberattack techniques
- Describe the relationship between vulnerabilities and exploits
- Identify how spamming and phishing attacks are performed
- Describe Wi-Fi vulnerabilities, attacks, and advanced persistent threats
- Explain perimeter-based Zero Trust security models
- Identify capabilities of the Palo Alto Networks prevention-first architecture

Topics:

- Cyber Security Landscape
- Cyberattack Types
- Cyberattack Techniques
- APTs and Wi-Fi Vulnerabilities
- Security Models

Cyber Security Landscape:

The modern cyber security landscape is a rapidly evolving hostile environment with advanced threats and increasingly sophisticated threat actors. This lesson describes the current cyber security landscape, explains SaaS application challenges, describes various security and data protection regulations and standards, identify cyber security threats and attacker profiles, andexplains the steps in the cyber attack lifecycle.

Modern Computing Trends:

The nature of enterprise computing has changed dramatically over the past decade.

Introduction to Web 2.0 and Web 2.0 Applications

Core business applications are now commonly installed alongside Web 2.0 apps on a variety of endpoints. Networks that were originally designed to share files and printers are now used to collect massive volumes of data, exchange real-time information, transact online business, and enable global collaboration. Many Web 2.0 apps are available as software-as-a service (SaaS), web-based, or mobile apps that can be easily installed by end users or that can be run without installing any local programs or services on the endpoint

Web 3.0

The vision of Web 3.0 is to return the power of the internet to individual users, in much the same way that the original Web 1.0 was envisioned. To some extent, Web 2.0 has become shaped and characterized, if not controlled, by governments and large corporations dictating the content that is made available to individuals and raising many concerns about individual security, privacy, andliberty. AI and Machine Learning

New Application Threat Vectors

Exploiting vulnerabilities in core business applications has long been a predominant attack vector, but threat actors are constantly developing new tactics, techniques, and procedures (TTPs).

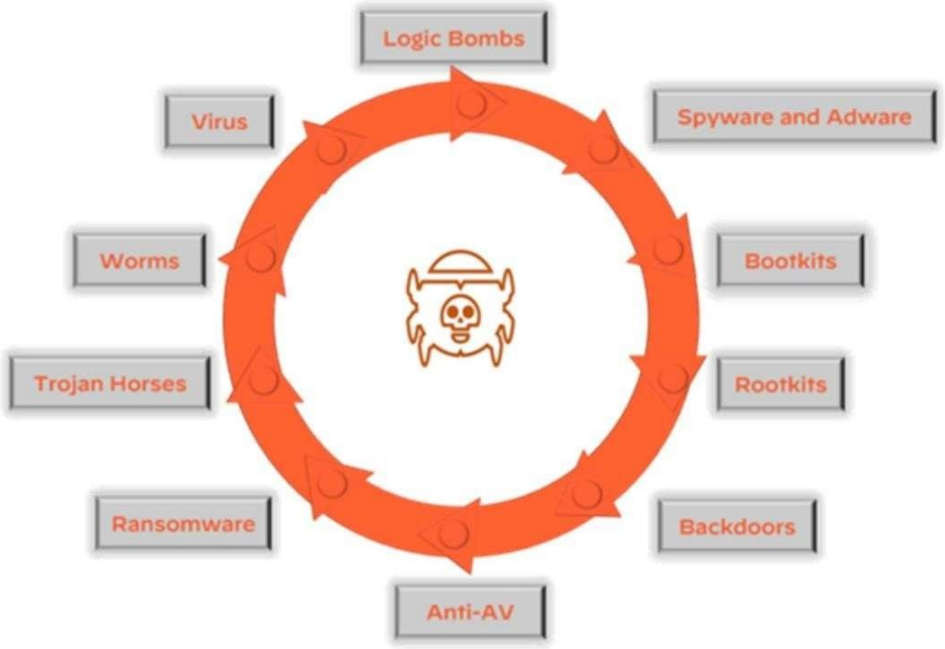
Protect Networks and Cloud Environments

To effectively protect their networks and cloud environments, enterprise security teams must manage the risks associated with a relatively limited, known set of core applications, as well as the risks associated with an ever-increasing number of known and unknown cloud-based applications. The cloud-based application consumption model has revolutionized the way organizations do business, and applications such as Microsoft Office 365 and Salesforce are being consumed and updated entirely in the cloud.

Cyberattack Types:

Attackers use a variety of techniques and attack types to achieve their objectives. Malwareand exploits are integral to the modern cyberattack strategy. This lesson describes the different malware types and properties, the relationship between vulnerabilities and exploits, and how modern malware plays a central role in a coordinated attack against a target. This lesson also explains the timeline of eliminating a vulnerability.

Malware Types:



Logic Bombs

A logic bomb is malware that is triggered by a specified condition, such as a given date or a particular user account being disabled.

Spyware and adware

Spyware and adware are types of malwares that collect information, such as internet surfing behaviour, login credentials, and financial account information, on an infected endpoint. Spywareoften changes browser and other software settings and slows computer and internet speeds on aninfected endpoint. Adware is spyware that displays annoying advertisements on an infected endpoint, often as pop-up banners.

Rootkits

A rootkit is malware that provides privileged (root-level) access to a computer. Rootkits are installed in the BIOS of a machine, which means operating system-level security tools cannot detect them. **Backdoors**

Trojan Horses

A Trojan horse is malware that is disguised as a harmless program but actually gives an attacker full control and elevated privileges of an endpoint when installed. Unlike other types of malware,Trojan horses are typically not self-replicating.

Worms

A worm is malware that typically targets a computer network by replicating itself to spread rapidly. Unlike viruses, worms do not need to infect other programs and do not need to be executed by a user or process.

Virus

A virus is malware that is self-replicating but must first infect a host program and be executed bya user or process

Ransomware Types:

Ransomware is malware that locks a computer or device (locker ransomware) or encrypts data (crypto ransomware) on an infected endpoint with an encryption key that only the attacker knows,thereby making the data unusable until the victim pays a ransom (usually in cryptocurrency suchas Bitcoin).

Cyberattack Techniques

Attackers use a variety of techniques and attack types to achieve their objectives. Spamming and phishing are commonly employed techniques to deliver malware and exploits to an endpoint via an email executable or a web link to a malicious website. Once an endpoint is compromised, an attacker typically installs back doors, remote access Trojans (RATs), and other malware to ensure persistence. This lesson describes spamming and phishing techniques, how bots and botnet's function, and the different types of botnets.

Business Email Compromise (BEC)

Business email compromise (BEC) is one of the most prevalent types of cyberattacks that organizations face today. The FBI Internet Crime Complaint Centre (IC3) estimates that "in aggregate" BEC attacks cost organizations three times more than any other cybercrime and BEC incidents represented nearly a third of the incidents investigated by Palo Alto Networks Unit 42 Incident Response Team in 2021. According to the Verizon 2021 Data Breach Investigations Report (DBIR), BEC is the second most common form of social engineering today

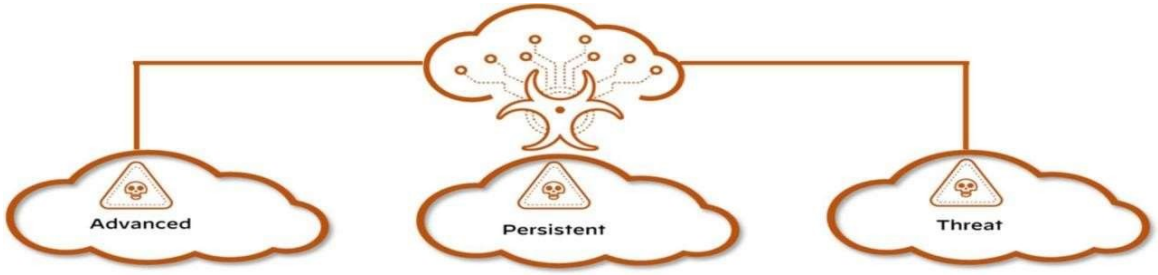
Phishing Attacks

We often think of spamming and phishing as the same thing, but they are actually separate processes, and they each require their own mitigations and defences. Phishing attacks, in contrastto spam, are becoming more sophisticated and difficult to identify and many more types of attacks

Advanced Persistent Threats and Wi-Fi Vulnerabilities

With the explosive growth in fixed and mobile devices over the past decade, wireless (Wi-Fi) networks are growing exponentially—and so is the attack surface for advanced persistent threats.

Advanced persistent threats, or APTs, are a class of threats that are far more deliberate and potentially devastating than other types of cyberattacks. APTs are generally coordinated events that are associated with cybercriminal groups.



Lazarus

Attacks against nation-states and corporations are common, and the group of cybercriminals that may have done the most damage is Lazarus. The Lazarus group is known as an APT. The Lazarus group has been known to operate under different names, including Benioff and Hidden Cobra. They were initially known for launching numerous attacks against government and financial institutions in South Korea and Asia. In more recent years, the Lazarus group has been targeting banks, casinos, financial investment software developers, and crypto-currency businesses. The malware attributed to this group recently has been found in 18 countries around the world.

Security Models

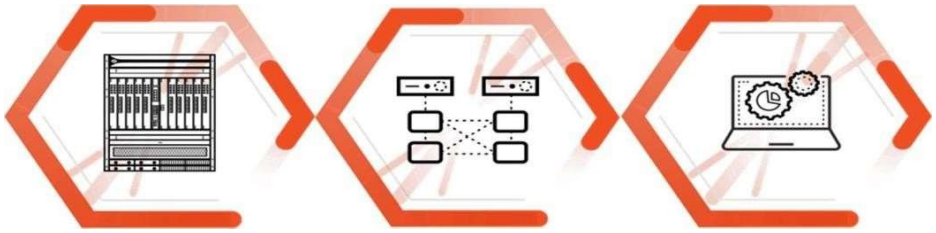
The goal of a security model is to provide measurable threat prevention through trusted and untrusted entities. This can be a complicated process, as every security model will have its own customizations and many variables need to be identified. This lesson describes the core concepts of a security model and why the model is important, the functions of a perimeter-based security model, the Zero Trust security model design principles, and how the principle of least privilege applies to the Zero Trust security model.

perimeter-Based Security Model

Perimeter-based network security models date back to the early mainframe era (circa late 1950s),when large mainframe computers were located in physically secure “machine rooms.” These rooms could be accessed by a limited number of remote job entry (RJE) terminals directly connected to the mainframe in physically secure areas.

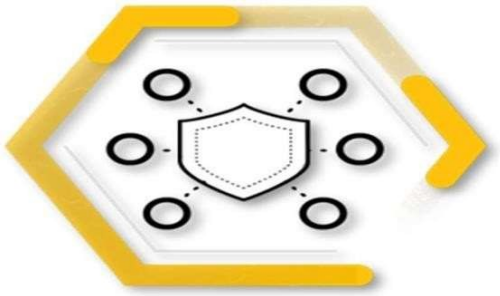
Relies on Physical Security

Today's data centres are the modern equivalent of machine rooms, but perimeter-based physical security is no longer sufficient. Click the arrows for more information about several obvious but important reasons for the security issues associated with perimeter-based security.



4.2 Fundamentals of Network Security

This training introduces someone with no prior knowledge to the fundamentals of network security including concepts they must understand to recognize and potentially defend home networks andmission-critical infrastructure.



After completing this training, you should be able to:

- Describe basic operations of enterprise networks, common networking devices, routed and routing protocols, network types and topologies, and services such as DNS
- Explain IP addressing, subnetting, and packet encapsulation based on the Open SystemsInterconnection (OSI) model
- Describe network security technologies such as packet filtering, stateful inspection, application firewalls, and IDS and IPS and web content filters
- Explain how to explore endpoint and mobile device security using technology such as personal firewalls, host-based IPS, and management features
- Describe how to properly secure enterprise networks through PAN-OS deployment templates and migration options and DNS, URL Filtering, Threat Prevention, and Wildfires® subscription services

Topics

- The Connected Globe
- Addressing and Encapsulation
- Network Security Technologies
- Endpoint Security and Protection

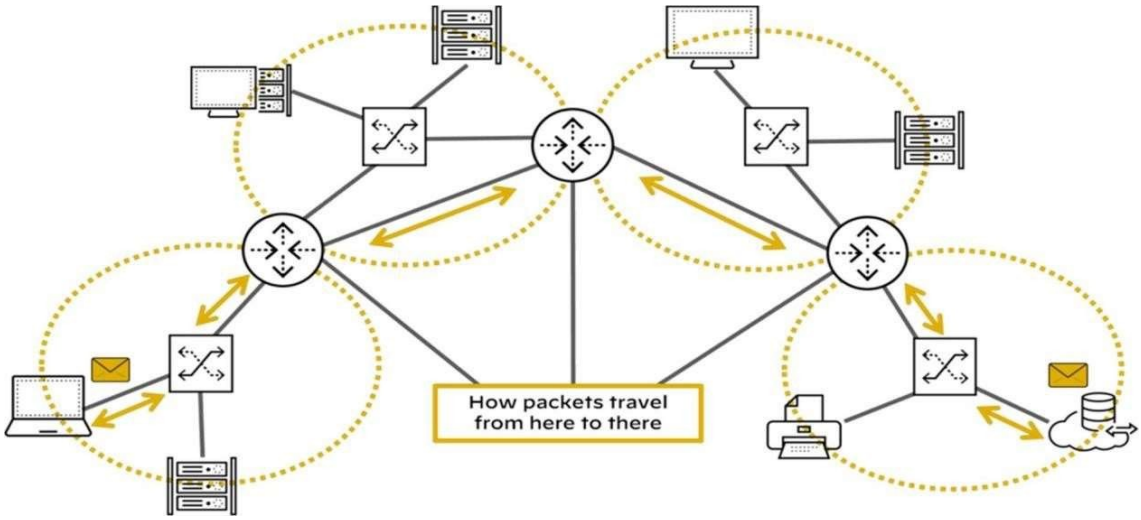
The Connected Globe

In this lesson, we will discuss how hundreds of millions of routers deliver Transmission Control Protocol/Internet Protocol (TCP/IP) packets using various routing protocols across local-area networks and wide-area networks. We also will discuss how the Domain Name System (DNS) enables internet addresses, such as www.paloaltonetworks.com, to be translated into routable IP addresses. **The Net**

In the 1960s, the U.S. defence Advanced Research Projects Agency (DARPA) created ARPANET, the precursor to the modern internet. ARPANET was the first packet-switched network. A packet-switched network breaks data into small blocks (packets), transmits each individual packet from node to node toward its destination, and then reassembles the individual packets in the correct order at the destination.

How Things Connect

The ARPANET evolved into the internet (often referred to as the network of networks) becausethe internet connects multiple local area networks (LAN) to a worldwide wide area network (WAN) backbone.



Today billions of devices worldwide are connected to the Internet and use the transport communications protocol/internet protocol (TCP/IP) to communicate with each over packets switched networks. Specialized devices and technologies such as routers, routing protocols, SDWAN, the domain name system (DNS) and the world wide web (WWW) facilitate communications between connected devices.

Addressing and Encapsulation

This lesson describes the functions of physical, logical, and virtual addressing in networking, IP addressing basics, subnetting fundamentals, OSI and the TCP/IP models, and the packet lifecycle.

TCP/IP Overview

In cybersecurity, you must understand that applications sending data from one host computer to another host computer will first segment the data into blocks and will then forward these data blocks to the TCP/IP stack for transmission.

TCP/IP Protocol Stack

The TCP stack places the block of data into an output buffer on the server and determines the maximum segment size of individual TCP blocks permitted by the server operating system. The TCP stack then divides the data blocks into appropriately sized segments, adds a TCP header, andsends the segment to the IP stack on the server.

The IP stack adds source and destination IP addresses to the TCP segment and notifies the server operating system that it has an outgoing message that is ready to be sent across the network. When the server operating system is ready, the IP packet is sent to the network adapter

Introduction to Subnetting

Subnetting is a technique used to divide a large network into smaller, multiple subnetworks by segmenting an IP address into two parts: the network portion of the address and the host portion of the address.

OSI Model and TCP/IP Protocol Layers

The OSI model is defined by the International Organization for Standardization and consists of seven layers. This model is a theoretical model used to logically describe networking processes

Network Security Technologies

In this lesson, we will discuss the basics of network security technologies such as firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), web content filters, virtual private networks (VPNs), data loss prevention (DLP), and unified threat management (UTM), which are deployed across the industry.

Legacy Firewalls

Firewalls have been central to network security since the early days of the internet. A firewall isa hardware platform or software platform or both that controls the flow of traffic between a trusted network (such as a corporate LAN) and an untrusted network (such as the internet).

Packet Filtering Firewalls

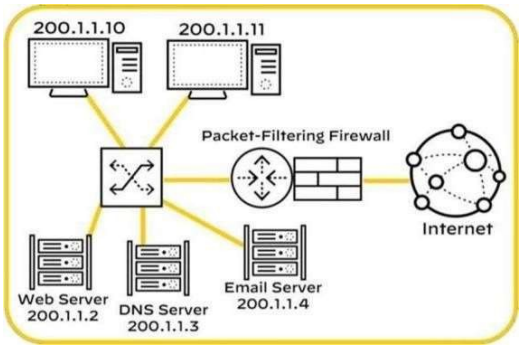
First-generation packet filtering (also known as port-based) firewalls have the following characteristics:

Operation

Packet filtering firewalls operate up to Layer 4 (Transport layer) of the OSI model and inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, ICMP), and port number.

Match

Packet filtering firewalls match source and destination IP address, protocol, and port number information contained within each packet header to a corresponding rule on the firewall that designates whether the packet should be allowed, blocked, or dropped. **Inspection** Packet filtering firewalls inspect and handle each packet individually, with no information about context or session.



Endpoint Security and Protection

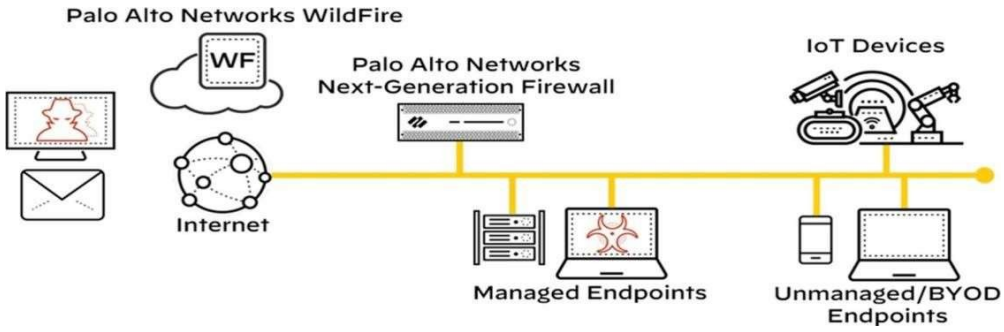
In this lesson, we will explore endpoint security challenges and solutions, including malware protection, anti-malware software, personal firewalls, host-based intrusion prevention systems (HIPSs), and mobile device management (MDM) software. We will also introduce network operations concepts, including server and systems administration, directory services, and structured host and network troubleshooting.

Endpoint Security

In 2022, there were more than 11.5 billion internet of things (IoT) devices worldwide, including machine-to-machine (M2M), wide-area IoT, short-range IoT, massive-and-critical IoT, and multi- access edge computing (MEC) devices. Traditional endpoint security encompasses numerous security tools

Endpoint Protection

Advanced malware and script-based attacks can bypass traditional antivirus solutions with ease and potentially wreak havoc on your business.



Secure the Enterprise

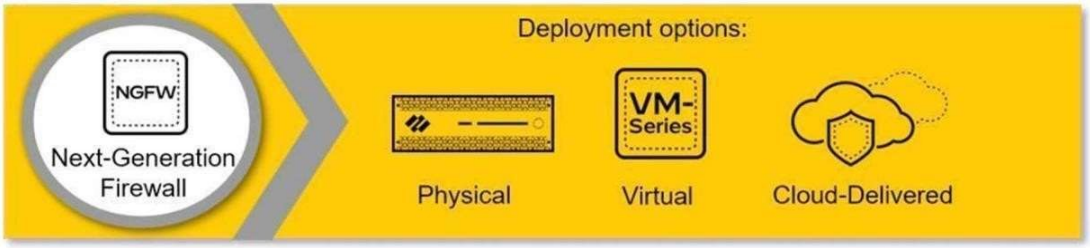
The networking infrastructure of an enterprise can be extraordinarily complex. The Palo AltoNetworks prevention-first security architecture secures enterprises' perimeter networks

Prevention-First' Architecture

Simplifying your security posture allows you to reduce operational costs and infrastructure whileincreasing your ability to prevent threats to your organization.

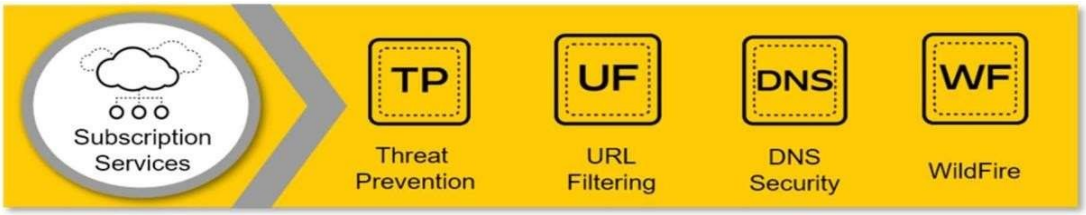
Next-Generation Firewall

The Palo Alto Networks Next-Generation Firewall is the foundation of our product portfolio. Thefirewall is available in physical, virtual, and cloud-delivered deployment options



Subscription Services

Subscription services add enhanced threat services and next-generation firewall capabilities, including DNS Security, URL Filtering, Threat Prevention, and wildfire malware prevention.



Panorama

Panorama provides centralized network security management. It simplifies administration while delivering comprehensive controls and deep visibility into network-wide traffic and security threats.

4.3 Fundamentals of Cloud Security

This training introduces the viewer to the fundamentals of cloud security, including concepts theymust understand to recognize threats and potentially defend data centres, public/private clouds, enterprise networks, and small office/home office (SOHO) networks from cloud-based attacks.

After you complete this training, you should be able to:

- Describe cloud computing models, virtualization, hypervisors, public cloud serviceprovider options, and private deployment options
- Explain the development operations (DevOps) strategy that unites teams to discover andremediate issues, automate deployment, and reduce time to market
- Describe the evolution of data centres through mixed traditional and cloud computingtechnologies
- Detail how Secure Access Service Edge (SASE) solutions help organizations embracethe concepts of cloud and mobility
- Describe how SaaS solutions provide data classification, sharing and permissionvisibility, and threat detection within the application
- Describe how the Prisma Cloud security platform detects and prevents security risks

Cloud Computing

The move toward cloud computing not only brings cost and operational benefits but also technology benefits. Data and applications are easily accessed by users no matter where they reside, projects can scale easily, and consumption can be tracked effectively. **Definition**

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner. Read the quote below for the definition of cloud computingaccording to the U.S. National Institute of Standards and Technology.

Cloud Computing Ecosystem

The cloud computing ecosystem consists of service models, deployment models, responsibilities,and security challenges.

Service Models, Deployment Models, and Responsibilities

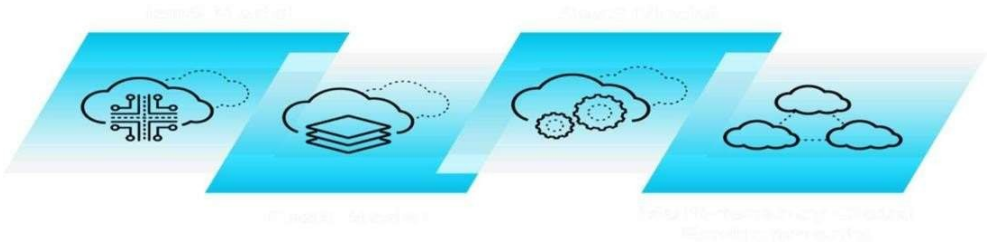
Virtualization is a critical component of a cloud computing architecture that, when combined withsoftware orchestration and management tools that are covered in this course, allows you to integrate disparate processes so that they can be automated, easily replicated, and offered on an as-needed basis.

Shared Responsibility Model

The security risks that threaten your network today do not change when you move from on-premises to the cloud. The shared responsibility model defines who (customer and/or provider) isresponsible for what (related to security) in the public cloud.

Cloud Security Responsibilities

In general terms, the cloud provider is responsible for security of the cloud, including the physicalsecurity of the cloud data centres, and foundational networking, storage, compute, and virtualization services.



Cloud Native Technologies

Like a new universe, the cloud native ecosystem has many technologies and projects quicklyspinning off and expanding from the initial core of containers.

A useful way to think of cloud native technologies is as a continuum spanning from virtualmachines (VMs) to containers to serverless. On one end are traditional VMs operated as stateful

entities, as we've done for over a decade now. On the other are completely stateless, serverless apps that are effectively just bundles of app code without any packaged accompanying operatingsystem (OS) dependencies. **Virtualization**

Virtualization is the foundation of cloud computing. You can use virtualization to create multiplevirtual machines to run on one physical host computer.

Overview

You can think of virtual machines as separate computers running various operating systems on a physical host computer. Virtual machines and their associated operating systems often are referredto as "virtual guest operating systems." These virtual guest operating systems all share the physicalcompute resources: processors, dynamic memory (RAM), and permanent storage media of a physical host machine.

Hypervisor

Hypervisor software allows multiple, virtual guest operating systems to run concurrently on a single physical host computer. The hypervisor functions between the computer operating systemand the hardware kernel.

Cloud Native Security

The speed and flexibility that are so desirable in today's business world have led companies to adopt cloud technologies that require not just more security but new security approaches. In the cloud, you can have hundreds or even thousands of instances of an application, presenting exponentially greater opportunities for attack and data theft.

The Four Cs of Cloud Native Security

The CNCF defines a container security model for Kubernetes in the context of cloud nativesecurity. Each layer provides a security foundation for the next layer.

Cloud

The cloud (and data centres) provide the trusted computing base for a Kubernetes cluster. If the cluster is built on a foundation that is inherently vulnerable or configured with poor security controls, then the other layers cannot be properly secured.

Clusters

Securing Kubernetes clusters requires securing both the configurable cluster components and theapplications that run in the cluster.

Containers

Securing the container layer includes container vulnerability scanning and OS dependency scanning, container image signing and enforcement, and implementing least privilege access.

Code

The application code itself must be secured. Security best practices for securing code include requiring TLS for access, limiting communication port ranges, scanning third-party libraries for known security vulnerabilities, and performing static and dynamic code analysis.

4.4 Fundamentals of SOC (Security Operation Centre)

The Fundamentals of Security Operations Centre training is a high-level introduction to the general concepts of SOC and SecOps. This lesson provides an overview of the Security Operations framework.

The Fundamentals of Security Operations Centre training is a high-level introduction to thegeneral concepts of SOC and SecOps. It will introduce the Security Operations framework, people, processes, and technology aspects required to support the business, the visibility that is requiredto defend the business, and the interfaces needed with other organizations outside of the SOC. The training consists of nine lessons and will take approximately 3 hrs to complete. This trainingis intended for learners who want to enter the field of cybersecurity - whether a student entering the workforce or an established professional transitioning from another field - and will help themdemonstrate knowledge about SOC. It is recommended that the lessons be taken in order, but themenu below can be used to access any lesson, should you wish to determine your own learningpath.

Day in the Life of a SOC Analyst

a SOC analyst on the Security Operations team and it is his job to triage alerts to determine if there is a security threat. Before Erik starts his job, he will need to understand the general concepts of SOC and SecOps, and the business goals. Erik will need training and support from the people he interacts with on a daily basis. While mitigating threats, Erik will need to know the processes to follow, the teams he will be interacting with, and the technology he will be using to gain visibilityinto the network.

Business

Both Erik and the SOC team are responsible for protecting the business. The reason for Security Operations, for all of the equipment, for everything SOC does is ultimately to service one main goal, protect the business. Without the Business pillar, there would be no need for Erik or the SOCteam.

The Business pillar defines the purpose of the Security Operations team to the business and how it will be managed. The Business pillar helps to provide Erik and the rest of the SOC team with

answers to questions such as "Who do we need to help protect the business?"; "How will we protect the business?"; "Where are we going to do this from?"; and "How do we know if what wehave inplace is working effectively?"

People:

The People pillar defines who will be accomplishing the goals of the Security Operations team and how they will be managed. As a part of the People pillar, Erik received training necessary forhim to be able to triage the alerts in addition to the other processes and functions within the SOC. This training provides Erik with the skills necessary to become efficient at detecting & prioritizing alerts. As Erik's knowledge increases, he will have opportunities to grow on the SOC team. He will also have the skills to advance in his career to other areas.

Employee Utilization:

Methods should be developed to maximize the efficiency of a Security Operations team specific to the existing staff. Security Operations staff are prone to burnout due to console burn out and extreme workloads. To avoid this, team members should be assigned different tasks throughout the day. These tasks should be structured and may include: • Shift turnover stand up meeting (beginning of shift)

- Event triage
- Incident response
- Project work
- Training
- Reporting
- Shift turnover stand-up meeting (end of shift)

Training

Proper training of staff will create consistency within an organization. Consistency drives effectiveness and reduces risk. Use of a formal training program will also enable the organizationto bring on new staff quickly. Some organizations resort to on-the-job or shadow training for newhires, which is not recommended on its own. While shadowing other analysts during initial employment in the SOC is important, it should not be the only means of training.

Processes

While monitoring the ticketing queue, Erik notices a new set of alerts that has been sent to the SOC team by one of the network devices. Based on the alert messages, Erik needs to determine whether the alert message is a security incident, so he opens an incident ticket. Erik starts by doinghis initial research in the log files on the network device to determine if the threat is real. After reviewing the log files, Erik determines that the alert is a real threat. Based on the Severity Triangle, Erik has determined that the severity level for this alert is currently High. The Processespillar defines the step-by-step instructions and functions that are to be carried out by the SOC team for the necessary security policies to be followed. Processes are a series of actions or steps taken to achieve an end goal. As part of the Processes pillar, Erik will need to determine the other teamsthat should be involved, the scope of the work for each team, and what each team will be responsible for.

Interfaces

The alert generated by the network device; he partners with the Threat Intelligence Team to identify the potential risks this threat may pose to the organization. Erik also interfaces with the Help Desk, Network Security Team, and Endpoint Security Teams to determine the extent the threat has infiltrated the network.

Security operations is not a silo and needs to work with many other functions or teams. Each interaction with another team is described as an interface. The Interfaces pillar defines which functions need to take place to help achieve the stated goals, and how the SOC will interface with other teams within the organization by identifying the scope of each team's responsibilities and the separation of each team's duties.

Visibility

A detailed analysis of the threat, he will need to gather all of the necessary information to make a well-informed decision. Network visibility is needed for Erik to gather information about the network's status, the traffic passing through the network, and the conditions on which traffic is allowed to pass through. Without network visibility, Erik may miss important data that could leadto a real threat being treated as a false positive or missed altogether. The better visibility Erik has

into every aspect of the company's network, the better he and the SOC team can make an informed decision.

The Visibility pillar enables the SOC team to use tools and technology to capture network traffic, limit access to certain URL's determine which applications are being used by end users, and to detect and prevent the accidental or malicious release of proprietary or sensitive information.

Technology

The beginning of our scenario has been mitigated. Erik now needs to work with SOC team members and other teams to determine if the current network technology can be used to automate a process or response to automatically remediate this issue, or similar issues that may arise. TheTechnology pillar includes tools and technology to increase our capabilities to prevent or greatly minimize attempts to infiltrate your network. In the context of IT Security Operations, technology increases our capabilities to securely handle, transport, present, and process information beyondwhat we can do manually. By using technology, you amplify and extend your abilities to work with Information in a secure manner.

SOAR

Scale is one of the biggest challenges for SOCs. We stepped through each pillar to mitigate a threat, but while Erik was working on one threat, alerts and incidents continued to pour in. The number of incidents that each member of the SOC team must respond to is greater than what canbe managed through human intervention.

The only reasonable long-term solution is to empower existing resources with a combination of innovative orchestration, artificial intelligence, and machine learning technologies to automate many of the manual processes that a SOC team faces each data.

4.5 TECHNOLOGY

AI and Machine Learning

AI and machine learning are two related technologies that enable systems to understand and act on information in much the same way that a human might use information. AI acquires and applies knowledge to find the most optimal solution, decision, or course of action. Machine learning is a subset of AI that applies algorithms to large datasets to discover common patterns in the data thatcan then be used to improve the performance of the system.

Blockchain

Blockchain is essentially a data structure containing transactional records (stored as blocks) that ensures security and transparency through a vast, decentralized peer-to-peer network with no single controlling authority. Cryptocurrency, such as Bitcoin, is an example of a blockchain application.

Data Mining

Data mining enables patterns to be discovered in large datasets by using machine learning, statistical analysis, and database technologies.

Mixed Reality

Mixed reality includes technologies, such as virtual reality (VR), augmented reality (AR), and extended reality (XR), that deliver an immersive and interactive physical and digital sensory experience in real time.

Natural Language Search

Natural language search is the ability to understand human spoken language and context (rather than a Boolean search, for example) to find information.

4.6 INTERSHIP REFLECTION

I did complete the project related to the challenges in the cyber security. This is the period of technology, which is emerging heavily, and rapidly. The organizations are in the trend to acquire the modern technology and hence they utilize the information technology as their major requirements in the business. In the recent times, the organizations depended over the online channels for making promotion of their services and products towards their target customers. Using the online channel for organizational process is not safe as there are different methods thatcreate threat for the organization and its business.

Businesses require protection for their websites as well as for other online accounts from the attack of hackers, viruses and malwares. Making this specific project, I acquired knowledge on the challenges, which are faced by the organizations, which can conduct operations through the online mode and processes, they can implant for protecting their operations.

Experience by the learning is effective and my supervisors and mentors did help me a huge for constructing the project in the correct manner. I used the secondary sources for collecting data for the study. They helped me choosing the correct sources and collecting the useful information from them. In addition to this, the analysis of the data and establishing the conclusion was effective by the help received from them. hence the total experience was nice and I would use them during the future in developing my career and also during the pursuing the higher educations. Along with that, I learnt the methods for conducting the research.

This helped me to learn conducting different kinds of research. The research process has helped me lot which would allow me to conduct future research with more ease and reduce various challenges that I faced during this particular research. Through this research I did learn the processe4s of data collection, analysis of them and evaluating the chance, objectives and make conduct of the entire research.

By the learning process, this would help developing my career and other higher education. Underneath I am providing the discussion for the usefulness of the learning experience. For completing this course this is essential to have the learning experience. The experience does help me for gaining the knowledge on the business organizations, the cyber security system as well as methods to conduct the research. Hence, I have achieved huge knowledge by various aspect thatfacilitate to me for completing the course successfully.

The learning experience helps to attend various research programs in the future. This may be thetype of education program or any other project and internship. This learning on the specific topichelps me to gain information on the business and the cyber security that helps me for pursuing further higher education over the similar topics. I can further elaborate the research project in thefuture and can managefilling the gaps to display this on the larger platform.

This learning experience will help in the future during establishing my career. This experience by the learning will help me to establish effective future and will reduce the challenges that are generally faced by obtaining any new topic for the research process. I have produced variety of knowledge on the business processes, using the cyber platform as well as the challenges from the using of cyber platform. This learning helped me to understand the research and the topic that has been provided during the course.

Apart from these benefits, I can utilize the learning experiences for exploring various other topics and achieve more information and knowledge. This helps be more effective for choosing my work field in the future.

Within the learning process, I did use the secondary information by various previous journals and articles. This has provided me with wide information on the cyber security and the challenges of the threats that can have over the business organizations. I require to make research proposal along with actual research project.

My supervisor had approved the research topic before my conduct on the specific research topic. For effective researching, I require proper information, many previous research works on the same topic. I also require to find the research scope as well as the research gaps that can help conducting future research on the same topic. The corresponding study suite proves effective and imperative for me in order to fulfil the underlying course successfully. This is because the moot intent of the corresponding suite shares a profound network with several other aspects of my curriculum. Furthermore, this research suite has endowed me with the requisite knowledge and understanding that appear imperative and indispensable regarding my curriculum.

4.7 CONCLUSION

After completion of my internship training, I could understand more about the company environment and helped to prepare myself to become skilled and more professional to fit in to professional field. At the beginning days of my internship, I was assigned to learn or gain knowledge about Linux and to study about company's atmosphere. Later the team was made and was assigned with the project throughout my internship, and was able to understand more about the real professional world. It was an industrial exposure for me which would work with a set of rules, and everything in the systematic manner. I sincerely and dedicatedly worked to gain more knowledge on the new things.

I studied about the projects assigned to us and initially we began with the working of basic applications to complex applications. To conclude with I learnt about different types of cyberattacks and the prevention ARY measures that are to be taken to avoid such attacks. Cyber security is the most important division of any company. Ethical hackers are helping the community from the cyber-crimes and protecting the private and valuable data

CHAPTER 5
OUTCOMES DESCRIPTION

5.1 DESCRIBE THE WORK ENVIRONMENT YOU HAVE EXPERIENCED

Palo Alto Cybersecurity Academy: -

4.7 I have experienced Palo Alto cybersecurity academy. PaloAlto cybersecurity academy is an organization which had provided free internship program for studentsto learn and understand and develop our knowledge and skills.

4.8 It is an organization which really provides and helps all the facilities and comforts to thestudents by which the students can be free to learn.

4.9 Palo Alto had conducted the orientation sessions andday wise classes anddiscussions.

4.10 This internship opportunity I had with Cybersecurity was a great chance for learning andprofessional development.

4.11 Therefore, I consider myself as a very lucky individual as Iwas provided with anopportunity to be a part of it.

4.12 I am also grateful for having a chance to meet (Virtually) so many wonderful people and professionals who led me though this internship period.

BEACON: -

4.13 I have experienced with Beacon. It is a platform which provided us to complete all the modules and course ofCybersecurity.

4.14 It is a platform which provided us all the material for each and every topic

4.15 There is also a source of YouTube to understand better about this internship and eachconcept of the whole course.

4.16 Through this virtual internship we gained the same amount of knowledge as if we had done

offline internship.

4.17 The timings of the day wise classes are arranged in a way that everyone can feel free to attend the classes and if we miss them there used to be a recording of the class, which is really nice.

4.18 A beacon, also known as a payload, is an executable or program that communicates back to a cyber attacked via some communication channel.

5.2 DESCRIBE THE REAL TIME TECHNICAL SKILL YOU HAVE ACQUIRED

Risk management: -

Your ability to think through what could possibly go wrong, assess the severity of threats ,and gauge the potential impact empowers you to focus your energy on the tasks whereyou'll havethe biggest impact.

Communication: -

Both written and verbal communication play a key role in cybersecurity. As an analyst, you mayneed to communicate technical concepts to individuals without a technical background, such as executives or legal teams. You may also be asked to write incident reports, where you'll have to document what you did in a concise and clear manner.

Collaboration: -

As a cybersecurity analyst, you'll likely work with a larger security team of other cybersecurity professionals. You may also need to collaborate with other teams with in your company (legal, IT, public relations) or share your findings with other organizationsof the greater cybersecurity community.

Adaptability: -

Cyber criminals are constantly adjusting and enhancing their attacks. Technology continues to advance, introducing new vulnerabilities. Adopting the mindset of a lifelong learner can helpyoukeep up with (or stay one step ahead of) these changes.

Critical thinking: -

Working in cybersecurity sometimes means making high-stakes decisions about yourorganization'ssecurity. Developing your critical thinking skills can help you to:

- Ask the right questions
- Evaluate and assess data
- Identify your assumptions
- Consider alternatives
- Understand context
- Draw data-driven conclusion

5.3 DESCRIBE THE MANAGERIAL SKILLS YOU HAVE ACQUIRED

Relationship Management: -

Relationship Management is fundamental to this role since Management is about people and utilizing them as resources. This is not just relationships with employees, bosses and peers, but also external stakeholders that can help or hindera department or organization's success.

Planning: -

Planning is the process of determining activities and tasks that need to be implemented – how, what, where and when – in order to meet an objective. Strategic Management deals heavily with this element. Planning is necessary as it identifies whatneeds tobe done within the constraints provided, such as time, money and resources.

Prioritisation: -

Managers need to not only be able to juggle their own workload, but also ensure that the workload of their employees is fairly distributed, while accounting for task and project deadlines. As with any team or organization, multiple projects are likely to be active at any given time.

Industry Knowledge: -

Industry knowledge is classified as a hard vs soft skill as it is less people and personal centric. Industry knowledge includes technical knowledge, such as programming languages, engineering skills, using complex software etc. It also covers other knowledge that isn't technically skewed. For example, patterns and trends within that context.

Many organizations prefer to hire senior managers who have prior experience in the same field. This is because it reduces the learning curve and time the new hire would need to adjustand adapt to their role.

5.4 DESCRIBE HOW YOU COULD IMPROVE YOUR COMMUNICATION SKILLS

Volunteer to give a presentation: -

As a fresh face within an organization you are in an ideal position to observe and learn. Suggest to your supervisor that at the mid-way point of your internship you would like to give a short presentation of the new skills you have learnt or projects you have worked on. Not only will this demonstrate your initiative and enthusiasm for the role but youwill have the ideal opportunity topractice your presentation skills.

Ask to host a team meeting: -

Most teams will have a weekly or monthly team meeting. Ask your supervisor if you can become more involved with the meeting, perhaps even asking to run the meeting. This will helpyou feel more confident speaking in front of other members of staff.

Keep on learning and practicing: -

The development of your communication skills needs to be an ongoing part of your professional learning and development. As you start your career you will be learning manynew technical skills which are incredibly important for your development.

However, effective communication skills will really help you go to the next level of your career. You might want to consider extra training or classes to perfect your business communication – raise this with your line manager as there might already be courses andtraining in place.

Practice your 'small talk' at informal times: -

The easiest and quickest way to improve your communication skills is to practice. And then practice some more! Use your internship as an ideal way to speak with your colleagues and learn from their experiences. Become involved with team and company events such as lunches, drinks and social activities. Make the effort to introduce yourself to people in your office. Ask them about their experience and engage them in conversation. This will help your language skills improve.

5.5 DESCRIBE HOW COULD YOU ENHANCE YOUR ABILITIES IN GROUPDISCUSSIONS, PARTICIPATION TEAM, CONTRIBUTION AS A TEAM MEMBER, LEADING A TEAM/ACTIVITY

I Joined Cybersecurity in Beacon: -

Along with joining Cybersecurity Certification Course you should also try to form questions and get answers through experts. One of the easiest sources for getting expert answers to your cybersecurity queries is cybersecurity group in telegram app. Along with asking your specific queries, you can also search for similar queries to further widen your scope of knowledge on that particular aspect. The platform is populated with several highly valuable queries and detailed answers that can directlyhelp you to improve your professional capabilities.

I Became a member of cybersecurity course group: -

A good Cybersecurity Training Course will help you crack the exams and gain professional skills but you also need to make the right connections in the industry. It is a valuable group of Cybersecurity professionals who openly share the knowledge to build connections and help each other grow. You can start attending community group to make friends with Cybersecurity professionals and experts. You can find a variety of people related to the Cybersecurity community- new learners, professionals, experts, trainers, and even recruiters. The group meet-ups will help you enhance your knowledge, seekand share the latest industry information, make new friends in the industry and even get a nice job with a good pay scale.

5.6 DESCRIBE THE TECHNOLOGICAL DEVELOPMENTS YOU HAVEOBSERVED AND RELEVANT TO THE SUBJECT AREA OF TRAINING

Customer relationship management (CRM) platform: -

I have observed Customer relationship management (CRM) is a technology for managing all your company's relationships and interactions with customers and potential customers. The goal is simple: Improve business relationships. A CRM system helps companies stay connected to customers, streamline processes, and improve profitability. The three types of CRM systems are operational, analyticaland collaborative.

Apex: -

I have observed Apex Technology is North Carolina's leading Managed

IT Service Provider. Our Full-Service, Flat-Rate Managed IT Services are designed to reduce costs, increase productivity, and mitigate business risk. If you are looking for stocks with good return, Apex Technology Acquisition Corp can be a profitable investment option.

Cloud Computing: -

I have observed cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

Cloud computing technology gives users access to storage, files, software, and servers through their internet-connected devices: computers, smartphones, tablets, and wearables. Cloud computing providers store and process data in a location that's separate from end users.

PHOTOS & VIDEO LINKS

- https://event.webinarjam.com/go/replay/99/6o231c97u50h31f6
- https://event.webinarjam.com/go/replay/101/504xrfylixphoyuv
- https://event.webinarjam.com/go/replay/101/8q40xip2i84b9zco
- https://event.webinarjam.com/register/99/yglm7uw5
- https://tinyurl.com/3n4w9r7m
- https://t.me/+xTOhjnCMuLNjNTg1
- https://event.webinarjam.com/go/replay/101/8q40xip2i84b9zco
- https://event.webinarjam.com/go/replay/101/8q40xip2i84b9zco
- https://beacon.paloaltonetworks.com/assessment_responses/take?enrollment_id= 228529340&survey=true
- https://event.webinarjam.com/go/replay/101/g2m9xu25u9yfrlf6
- https://event.webinarjam.com/go/replay/99/nyopwa81c49c3pc1
- https://event.webinarjam.com/register/99/yglm7uw5
- https://tinyurl.com/3n4w9r7m
- https://t.me/+g6_9Ez07hTFhNTFl
- https://apsche-internship.eduskillsfoundation.org/

EduSkills | paloalto NETWORKS

paloalto NETWORKS

Cybersecurity Academy

Palo Alto Networks Assessment-Based Certificate

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

SAI GANESH CHIMMIRI

has successfully demonstrated the knowledge to complete the Assessment-Based Certificate in

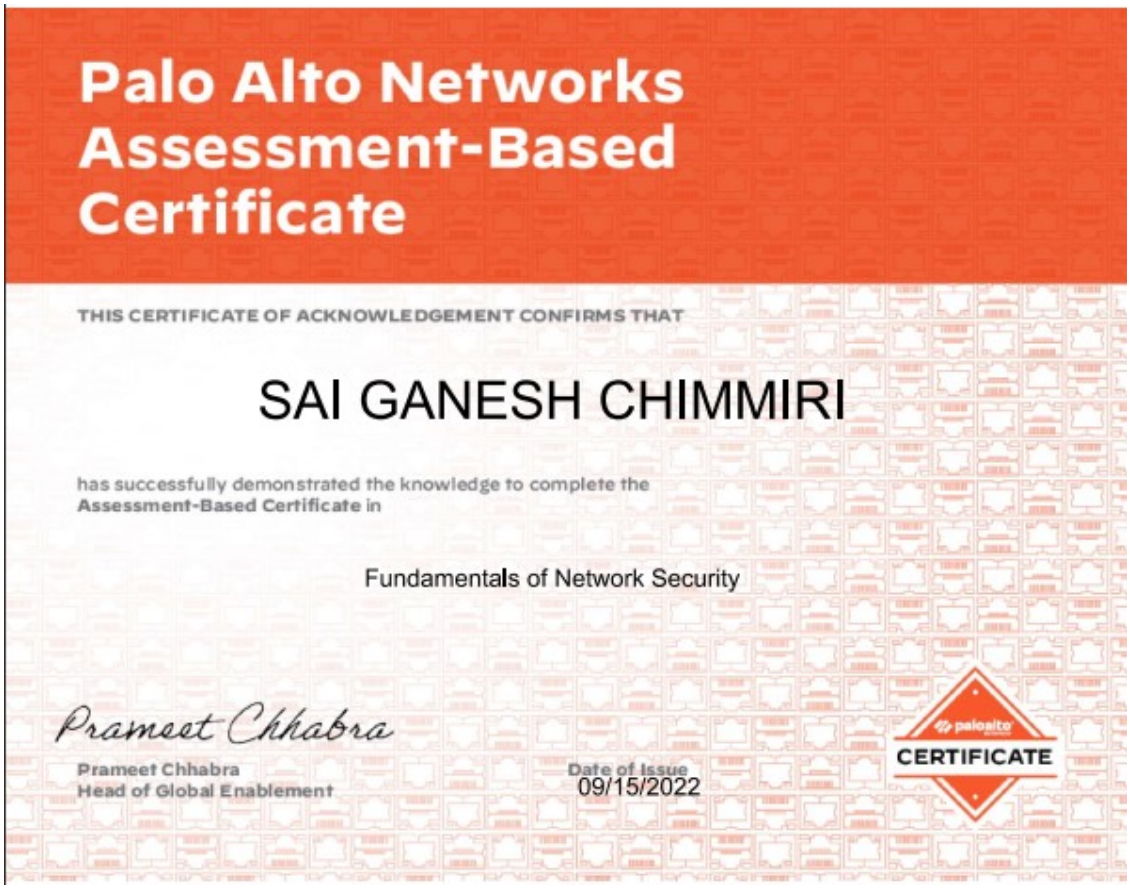
Introduction to Cybersecurity

Prameet Chhabra

Prameet Chhabra
Head of Global Enablement

Date of Issue
09/15/2022

paloalto CERTIFICATE



Palo Alto Networks Assessment-Based Certificate

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

SAI GANESH CHIMMIRI

has successfully demonstrated the knowledge to complete the **Assessment-Based Certificate** in

Fundamentals of Network Security

Prameet Chhabra

Prameet Chhabra
Head of Global Enablement

Date of Issue
09/15/2022

paloalto
CERTIFICATE

Palo Alto Networks Assessment-Based Certificate

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

SAI GANESH CHIMMIRI

has successfully demonstrated the knowledge to complete the **Assessment-Based Certificate** in

Fundamentals of Cloud Security

Prameet Chhabra

Prameet Chhabra
Head of Global Enablement

Date of Issue
09/26/2022

paloalto
CERTIFICATE

Certificate of Completion

The Fundamentals of SOC - Assessment

Completed by SAI GANESH CHIMMIRI on October 11, 2022

You earned 2000 Gold for completing The Fundamentals of SOC Knowledge Check!

Score: 94 Completion ID: 228778284

Student Self Evaluation of the Short-TermInternship

Student Name: CHIMMIRI SAI GANESH
Registration No: 208A1A4234

Term of Internship: 2 months

From: July 2022 To : Sept 2022

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**

MARKS STATEMENT
(To be used by the Examiners)

INTERNAL ASSESSMENTSTATEMENT

Name of the Student : CHIMMIRI SAI GANESH

Program of Study : B-TECH

Group : CSE(AI&ML)

Roll Number : 208A1A4234

College Name : Rise Krishna Sai Prakasam Group Of Institution

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**