A report on

INTERNSHIP

CYBERSECURITY VIRTUAL INTERNSHIP

Submitted in partial fulfillment of the requirements

for the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

(DATA SCIENCE)

by

S.SAI VARSHITHA (224G1A3282)

DEPARTMENT OF COMPUTER SCEINCE AND ENGINEERING (DATA SCIENCE)

Srinivasa Ramanujan Institute of Technology

(AUTONOMOUS)

Rotarypuram Village, B K Samudram Mandal, Ananthapuramu - 515 701

2023-2024

Srinivasa Ramanujan Institute of Technology
(AUTONOMOUS)
Rotarypuram Village, B K Samudram Mandal, Ananthapuramu - 515 701

Department of Computer Science & Engineering
(Data Science)

Certificate

This is to certify that the internship report entitled CYBERSECURITY is the bonafide work carried out by **S. SAI VARSHITHA** bearing Roll Number 224G1A3282 in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering(Data Science)** for 10 weeks from May to July 2023.

Internship Coordinator **Head of the Department**

Dr. P. Chitralingappa, M.Tech.,Ph.D.,

Chitralingappa, M.Tech., Ph.D.,

Associate Professor

Associate Professor

Date: **EXTERNAL EXAMINER** Place: Ananthapuramu

PREFACE

Brief overview of the company's history:

- Who founded it
- What purpose and when

Company's Mission Statement:

Business Activities:

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible, whose constant guidance and encouragement crowned our efforts with success. It is a pleasant aspect that I have now the opportunity to express my gratitude for all of them.

It is with immense pleasure that I would like to express my indebted gratitude to my internship coordinator **Dr. P. Chitralingappa, Associate Professor, Department of Computer Science and Engineering (Data Science)**, who has supported me a lot and encouraged me in every step of the internship work. I thank him for the stimulating support, constant encouragement and constructive criticism which have made possible to bring out this internship work.

I am very much thankful to **Dr. P. Chitralingappa, Associate Professor, Department of Computer Science and Engineering (Data Science),** for his/her kind support and for providing necessary facilities to carry out the work.

I wish to convey my special thanks to **Dr G Balakrishna, Principal** of **Srinivasa Ramanujan Institute of Technology** for giving the required information in doing my internship. Not to forget, I thank all other faculty and non-teaching staff, and my friends who had directly or indirectly helped and supported me in completing my project in time.

I also express our sincere thanks to the Management for providing excellent facilities and support**.**

Finally, I wish to convey my gratitude to my family who fostered all the requirements and facilities that I need.

S. SAI VARSHITHA (224G1A3282)

Contents Page No

CHAPTER 1

INTRODUCTION

Palo Alto Networks Education Services provides a wide portfolio of role- based certifications aligning with Palo Alto Networks' cutting-edge cybersecurity technologies. Receiving a certification shows your peers, managers and the general public that you're committed to cybersecurity and that your work aligns to set standards.

The Cybersecurity Academy program from Palo Alto Networks is committed to ensuring secure experiences in the digital world for students, and inspiring them to pursue learning and careers in cybersecurity.

About PCCET

The PCCET certification is the first of its kind. It is

aligned with the NIST/NICE (National Institute of Standards and Technology/National Initiative for Cybersecurity Education) workforce framework, designed 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.

The PCCET certification is designed for students, the emergent workforce, skilled labour trying to transition into cybersecurity, hiring managers looking to hire entry-level technical help, technical professionals, educators, and any non-technical individuals interested in validating comprehensive knowledge on current cybersecurity tenets.

The technical curriculum developed and authorized by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise that prepare you to protect our digital way of life.

PCCET Exam Blueprint

Domain Weight (%)

• Fundamentals of Cybersecurity 30%

• Network Security Components 30%

• Cloud Technologies 20%

• Elements of Security Operations 20%

1.1 Modules

These are the modules which we learned during the self-paced learning period.

1.1.1 Introduction to Cyber Security

In this module we learned how 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. **1.1.2 Fundamentals of Network Security**

In this Module we learned how 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 Systems Interconnection (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.

1.1.3 **Fundamentals of Cloud Security**

In this module we learned how to

➢ Describe cloud computing models, virtualization, hypervisors, public cloud service provider options, and private deployment options.

➢ Explain the development operations (DevOps) strategy that unites teams to discover and remediate issues, automate deployment, and reduce time to market. ➢ Describe the evolution of data centers through mixed traditional and cloud computing technologies.

➢ Detail how Secure Access Service Edge (SASE) solutions help organizations embrace the concepts of cloud and mobility.

➢ Describe how the Prisma Cloud security platform detects and prevents security risks.

1.1.4 The Fundamentals of SOC (Security Operations Center)

In this module we learned how to do ➢ Security operations framework.

➢ Purpose of Security Operations.

➢ Goals of Security Operations.

➢ Process and Procedures executed by Security Operations organization. ➢ Functions need to be involved to achieve stated goals.

➢ Information SecOps function needs.

➢ Security operations to complete its core mission.

➢ SOAR is the automation of the orchestration of all elements of security operations. Dept.

of CSD

CHAPTER 2

Technology

Technologies required for Cyber Security

There have been many cases of attack on critical infrastructures such as healthcare, water systems, and power grids. On a smaller scale, there has been a spurt in ransomware and malware attacks on enterprise networks.

Man creates technology, and it is the man who can get the better of this technology. Thus, no cyber security mechanism is fool proof and can ever be. The wise choice is to constantly identify and adopt emerging technologies to fortify cyber security. Here's a list of the top advanced cyber security technologies on the charts.

1. Artificial Intelligence & Deep Learning

Artificial intelligence (AI) and deep learning are two closely-related fields of technology that are revolutionizing the way computers interact with and respond to the world around them. AI is the broader concept of machines being able to carry out tasks in a way that mimics human behaviour .

Deep learning is a subset of AI that uses multi-layered artificial neural networks to learn from large amounts of data. Deep learning algorithms are able to identify patterns in the data that humans may not recognize, allowing them to make decisions and predictions with greater accuracy than traditional machine learning algorithms.

Deep learning is used in a wide range of applications, from facial recognition and natural language processing to autonomous vehicles and medical diagnosis.

2. Behavioural Analytics

Behavioral analytics is a process by which data is collected from user interactions with a website, application, or other digital product, and analysed to understand user behavior. This data can be used to inform design decisions, identify user needs, and improve the user experience.

Behavioral analytics can also be used to identify areas of opportunity, such as customer segmentation and personalization, as well as areas of risk, such as fraud detection.

3. Embedded Hardware Authentication

Embedded hardware authentication is a form of authentication that uses physical hardware devices to verify a user's identity. This type of authentication is used to protect access to sensitive information and systems. Common hardware authentication devices include USB

tokens, smart cards, and biometric readers.

This type of authentication is more secure than traditional methods such as username and password because it requires physical access to the device or token to gain access. Additionally, many hardware authentication devices are designed to be tamper-resistant, making them difficult to bypass or manipulate.

4. Zero-Trust Model

As the name itself states, this model of cyber security is based on a consideration that a network is already compromised. By believing that one cannot trust the network, one would obviously have to enhance both 'internal' and 'external' securities. The crux here is that both internal and external networks are susceptible to a compromise and need equal protection. It includes identifying business-critical data, mapping the flow of this data, logical and physical segmentation, and policy and control enforcement through automation and constant monitoring.

5. Block chain Cybersecurity

Blockchain cyber security is one of the latest cyber security technologies that's gaining momentum and recognition. The blockchain technology works on the basis of identification between the two transaction parties. Similarly, blockchain cyber security works on the basis of blockchain technology's peer-to-peer network fundamental.

Every member in a blockchain is responsible for verifying the authenticity of the data added. Moreover, blockchains create a near-impenetrable network for hackers and are our best bet at present to safeguard data from a compromise. The use of blockchain with Artificial Intelligence can establish a robust verification system to keep potential cyber threats at bay.

CHAPTER 3

Applications

Cybersecurity threats change over time, and it is important for organizations to counter these threats. Intruders adjust by creating new tools and tactics to undermine security when new protections are developed to counter more recent attacks. Your organization's cybersecurity is only as strong as its weakest link. To safeguard your data and systems, it's crucial to have a collection of cybersecurity tools and techniques at your disposal. Below are a few important applications of cybersecurity.

1. Network Security Surveillance

Continuous network monitoring is the practice of looking for indications of harmful or intrusive behaviour. It is often used in conjunction with other security tools like firewalls, antivirus software, and IDPs. Monitoring for network security may be done manually or automatically using the software.

2. Identification and Access Control (IAM)

The management has control over which individual can access which sections of the data. Usually, the management regulates who has access to data, networks, and computer systems. Here is where cybersecurity comes into the picture by identifying users and executing an access control. Various cyber security applications ensure IAM across an organization. IAM may be implemented in both software and hardware, and it often makes use of role-based access control (RBAC) to limit access to certain system components. Managers can manage who has access to what, when they can access it, and for how long, thanks to solution providers like Okta.

3. Software Security

Applications that are crucial to company operations are protected by application security. It contains controls like code signing and application whitelisting and may assist unify your security rules with things like file-sharing rights and multi-factor authentication. With the application of AI in cyber security, software security is bound to increase. 4. Risk Management Risk management, data integrity, security awareness training, and risk analysis are all covered by cyber security. The evaluation of risks and the control of the harm that may be done as a result of these risks are important components of risk management. The security of sensitive information is another issue covered by data security.

6. Physical Security

System locks, intrusion detection systems, alarms, surveillance systems, and data-destruction systems are a few examples of physical security measures. These allow organizations to secure their IT infrastructure.

7. Compliance and Investigations

Cybersecurity is helpful during the examination of suspicious situations. Additionally, it helps to upkeep and adhere to regulations.

8. Security during Software Development

The software aids in detecting software flaws when they are being developed and ensuring that regulations and standards are followed. Cybersecurity tools thoroughly test, scan, and analyse the software to identify any bugs, openings, or weaknesses that hackers or competing businesses might exploit.

CHAPTER 4 Modules Explanation

Module 1 Introduction to Cyber Security

Cyber Attack Lifecycle Modern cyberattack strategy has evolved from a direct attack against a highvalue 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”). The cyberattack lifecycle illustrates the sequence of events that an attacker goes through to infiltrate a network and exfiltrate (or steal) valuable data. Blocking just one step breaks the chain and can effectively defend an organization’s network and data against an attack.

Cyber Attack Techniques

- **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 contrast to spam, are becoming more sophisticated and difficult to identify.

• Whaling

Whaling is a type of spear phishing attack that is specifically directed at senior executives or other high-profile targets within an organization. A whaling email typically purports to be a legal subpoena, customer complaint, or other serious matter. **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.

• BootKits

A bootkit is malware that is a kernel-mode variant of a rootkit, commonly used to attack computers that are protected by full-disk encryption.

• 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

A backdoor is malware that allows an attacker to bypass authentication to gain access to a compromised system.

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 perimeterbased security model, the Zero Trust security model design principles, and how the principle of least privilege applies to the Zero Trust security model.

Module 2 Fundamentals of Network Security

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

Internet of Things

With almost five billion internet users worldwide in 2022, which represents well over half the world's population, the internet connects businesses, governments, and people across the globe. Our reliance on the internet will continue to grow, with nearly 30 billion devices and "things" – including autonomous vehicles, household appliances, wearable technology, and more – connecting to the internet of things (IoT) and nearly nine billion worldwide smartphone subscriptions that will use a total of 160 exabytes (EB) of monthly data by 2025.

Network Security Technologies

IDSs and IPSs can also be classified as knowledge-based (signaturebased) or behavior-based (statistical-anomaly-based) systems.

• Knowledge – Based Systems

A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. Knowledge-based systems have lower false-alarm rates than behavior-based systems. But to be effective, knowledge-based systems must be continually updated with new attack signatures.

• Behavior – Based Systems

A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that might indicate an intrusion attempt. Behavior-based systems are better at detecting new attacks against unknown vulnerabilities. But behaviorbased systems have a much higher false-positive rate than knowledge-based systems.

Module 3 Fundamentals of Cloud Security

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

Prioritizing Software Security in the Cloud

The customer is ultimately responsible for providing security for the data, hosts, containers, and server less instances in the cloud. Public cloud service providers have done a great job with the build, maintenance, and updating of computing hardware, virtual machines, data storage, and databases along with the minimum baseline security protection mechanisms. However, the customer is ultimately responsible for providing security for the data, hosts, containers, and serverless instances in the cloud.

Module 4 The Fundamentals of SOC (Security Operations Center)

Security Operations and Security Orchestration

Security Operations is a function that identifies, investigates, mitigates threats, and provides continuous improvement. Security orchestration automates processes within Security Operations.

Separate Groups and Processes Security Operations and security orchestration are two separate and different groups and processes, and most often are implemented and managed involving two different types of subject matter experts (SMEs). Both are required to work together to manage, identify, assess, and mitigate security issues and incidents in real time.

Automation Process

Security Operations engineers will use security orchestration to automate processes created by the Security Orchestration engineers.

Threat Hunting

Threat hunting is often thought of as a function of the Security Operations team. However, because it is separate from identify, investigate, and mitigate, it is distinct from the analyst activities and is included as an interface. Hunting allows you to dig into the data to find situations that the machines and automation may have missed. Threat hunting can be structured or unstructured. Structured hunts begin with a single piece of intelligence. Then a hypothesis is formed, and then the hunt to find the threat in the network begins. Formalized structured hunts tend to be more useful to an organization than unstructured efforts.

Content Engineering

Content engineering is the function that builds alerting profiles that identify the alerts that will be forwarded for investigation. The content engineer and the Security Operations team need to be tightly interfaced and feedback needs to continuously flow. An interface agreement between the teams needs to be created to identify how often content updates will be made, how they will be vetted, and the feedback process. It should identify how the Security Operations team and threat hunting team make requests for new alerts or modifications to existing alerts. Properly configured alerts will allow the Security Operations team to focus on important alerts that require further investigation.

CHAPTER 5

Real Time Example

Solar Winds Supply Chain Attack This was a massive, highly innovative supply chain attack detected in December 2020, and named after its victim, Austin-based IT management company Solar Winds. It was conducted by APT 29, an organized cybercrime group

connected to the Russian government. The attack compromised an update meant for Solar Winds' software platform, Orion.

During the attack, threat actors injected malware, which came to be known as the Sunburst or Solorigate malware—into Orion's updates. The updates were then distributed to Solar Winds customers.

The Solar Winds attack is considered one of the most serious cyber espionage attacks on the United States, because it successfully breached the US military, many US-based federal agencies, including agencies responsible for nuclear weapons, critical infrastructure services, and a majority of Fortune 500 organizations.

CHAPTER 6

Learning Outcomes

➢ 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

➢ Explain IP addressing, subnetting, and packet encapsulation based on the Open Systems Interconnection (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 cloud computing models, virtualization, hypervisors, public cloud service provider options, and private deployment options

➢ Explain the development operations (DevOps) strategy that unites teams to discover and remediate issues, automate deployment, and reduce time to market

➢ Describe the evolution of data centers through mixed traditional and cloud computing technologies

➢ Detail how Secure Access Service Edge (SASE) solutions help organizations embrace the concepts of cloud and mobility

➢ Describe how SaaS solutions provide data classification, sharing and permission visibility, and threat detection within the application

➢ Describe how the Prisma Cloud security platform detects and prevents security risks. ➢

Purpose of Security Operations ➢ Goals of Security Operations

➢ Process and Procedures executed by Security Operations organization. ➢ Functions need to be involved to achieve stated goals.

➢ Information SecOps function needs.

➢ Security operations to complete its core mission

Conclusion

By completing this internship, we learnt

• The importance of Cyber Security in day-to-day life. • Technologies required for Cyber Security. • Applications and advantages.

• Identify cybersecurity threats

• Cloud computing ecosystem

• Security operations framework

• Purpose of Security Operations

• Goals of Security Operations

• About the Security Models.

• About Network Security.

• About Cloud Security.

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 2024 VIRTUAL INTERNSHIP

Certificate of Virtual Internship

This is to certify that

Sai Varshitha Surasura

Srinivasa Ramanujan Institute of Technology

has successfully completed 10 weeks

Cybersecurity Virtual Internship

During April - June 2024

Supported By paloalto® NETWORKS

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 :1d43b26932487fbe1c62262f8a5a3b0d
Student ID :STU642179167a4571679915286

INTERNSHIP GRADE B

GRADE- O (Outstanding):90-100 | E (Excellent):80-89 | A (Very Good):70-79 | B (Good): 60-69 | C (Fair): 50-59 | D (Average): 40-49 | P (Pass): 30-39 | F (Fail): Below 30

References

[1] Technologies

https://ifflab.org/the-5-latest-cyber-security-technologies-foryour-business/ [2] Applications

https://www.geeksforgeeks.org/applications-of-cybersecurity/

[3] Introduction to cyber-security

https://beacon.paloaltonetworks.com/student/collection/737796/path/831804

[4] Fundamentals of Network Security
https://beacon.paloaltonetworks.com/student/collection/737796/path/831805

[5] Fundamentals of Cloud Security
https://beacon.paloaltonetworks.com/student/collection/737796/path/831806 [6] The

Fundamentals of SOC (Security Operations Center)

https://beacon.paloaltonetworks.com/student/collection/737796/path/831807\Dept. of CSD