Palo Alto Networks Cybersecurity Academy - Cloud Security Fundamentals

Course Description:

In the Cloud Security Fundamentals course, students will learn basic principles associated with securing thecloud and SaaS-based applications through Secure Access Service Edge architecture and identify conceptsrequired to recognize and potentially mitigate attacks against traditional and hybrid datacenters as well as mission critical infrastructure. Students will also learn how to initially setup and configure containers on a docker bridge network and test the container security through the use of vulnerability scans and reports.

Course Objectives:

Upon completion of this course students will be able to perform the following:

- Define cloud computing service, deployment, and shared responsibility models.
- Describe cloud native technologies including virtual machines, containers and orchestration,and serverless computing.
- Identify cloud native security including Kubernetes security, DevOps, and DevSecOps, andvisibility, governance, and compliance challenges.
- Create and run docker bridge network containers in detached and interactive mode.
- Summarize hybrid data center security design concepts.
- Configure and test containers with vulnerability scanning.
- Review traditional data center security solution weaknesses.
- Investigate east-west and north-south traffic protection methods.
- Configure the NGFW to deny International Attackers.
- Recognize the four pillars of Prisma Cloud.
- Describe the layers and capabilities in a Secure Access Service Edge (SASE).
- Review the layers in a Prisma Access architecture solution.
- Demonstrate an understanding of unique SaaS-based security risks.
- Understand how Prisma SaaS protects SaaS-based applications and data.