**Day 3 - Network Security (12.6.)**

**1. Securing VPCs (AWS Focus)**

**Topics**

* NACLs (Network Access Control Lists) vs. Security Groups: Comparison and best use cases
* VPC Flow Logs: Capturing and analyzing network traffic
* Bastion Host: Secure access to private instances
* Threat modeling for network architecture (entry/exit points, segmentation)
* Network segmentation and isolation strategies

**Required Infrastructure & Components**

* Custom VPC with public/private subnets
* EC2 instances in both public and private subnets
* Bastion host in public subnet
* Security Groups and NACLs for each subnet
* VPC Flow Logs enabled and forwarded to CloudWatch Logs
* Optional: Systems Manager (SSM) for session management

**To-Dos & Steps**

1. Set up Security Groups:
   * Public instance: Allow SSH, HTTP/HTTPS
   * Private instance: Restrict to only Bastion or SSM
2. Configure NACLs to enforce subnet-level rules (e.g., block ports, CIDR restrictions)
3. Deploy a Bastion host (EC2) with limited inbound IP ranges
4. Access private instances via Bastion host or SSM Session Manager
5. Enable and review VPC Flow Logs for:
   * Rejected traffic
   * Unexpected access attempts
6. Demonstrate segmentation by restricting lateral movement between subnets

**Webinars:**

* AWS Virtual Private Cloud (VPC) Security Best Practices Webinar - <https://www.youtube.com/watch?v=fXUKEQPVcP0> 00:17
* [AWS – Best Practices for VPC Security](https://www.datadoghq.com/blog/vpc-components/)

**YouTube:**

* [AWS Security Groups vs Network ACLs (NACLs) explained](https://www.youtube.com/watch?v=ttc0b2NZTV0) – 00:04
* [AWS Bastion Host Tutorial](https://www.youtube.com/watch?v=pyoibaiZ2c8) – 00:04
* [AWS VPC Flow Logs Tutorial](https://www.youtube.com/watch?v=vxvsjfSUBSQ) – 00:10
* [AWS Systems Manager Session Manager Deep Dive](https://www.youtube.com/watch?v=xHNLNTa2xGU) – 00:50

**Reading Material:**

* [Security Best Practices for Amazon VPC](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-best-practices.html)
* [Amazon VPC Flow Logs User Guide](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html)
* [AWS Systems Manager Session Manager Guide](https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html)
* AWS Whitepaper: Security at Scale – Governance in AWS[ARCHIVED: Security at Scale: Governance in AWS](https://d1.awsstatic.com/whitepapers/compliance/AWS_Security_at_Scale_Governance_in_AWS_Whitepaper.pdf) – 16 pages
* [AWS Bastion Host: Secure Remote Access to Your Private Instances | by Tejas Mane | Medium](https://medium.com/@tejasmane485/aws-bastion-host-secure-remote-access-to-your-private-instances-7012a5a74fb3)

**2. SOC 2 Overview (Compliance Focus)**

**Topics**

* SOC 2 Trust Service Criteria: Security, Availability, Confidentiality, Processing Integrity, Privacy
* Control implementation strategies in AWS
* Logging and monitoring alignment (CloudTrail, Config, GuardDuty)
* SOC 2 vs. ISO 27001: Focus on service delivery and operations
* Documentation and evidence gathering for audit readiness

**Required Infrastructure & Components**

* AWS Config with conformance packs (SOC 2 template)
* AWS CloudTrail with multi-region enabled
* GuardDuty for threat detection
* Custom IAM roles with least privilege access
* Centralized logging to S3 or CloudWatch Logs
* AWS Artifact for SOC 2 reports

**To-Dos & Steps**

1. Map AWS services to SOC 2 criteria using AWS documentation
2. Enable AWS Config conformance packs and assess findings
3. Enable CloudTrail and GuardDuty across all regions
4. Simulate a SOC 2 control: Example – Logging and access review
5. Review IAM roles and access logs for security principles (least privilege, accountability)
6. Download SOC 2 audit reports via AWS Artifact

**Webinars:**

* AWS Compliance & Risk Management Webinar (SOC 2 Focus) - <https://www.youtube.com/watch?v=6qbBxwPZicw> – 00:15
* [AWS – Audit Readiness for SOC 2](https://www.ispartnersllc.com/blog/preparing-soc2-audit-aws/)

**YouTube:**

* [SOC 2 Compliance Explained](https://www.youtube.com/watch?v=mpxaZIUSOmc) – 00:12
* [AWS Artifact and Compliance Reports Walkthrough](https://www.youtube.com/watch?v=D__KkUv3Yxc) – 00:04

**Reading Material:**

* [AWS Artifact User Guide](https://docs.aws.amazon.com/artifact/latest/ug/what-is-aws-artifact.html)
* [AWS Config Conformance Packs Overview](https://docs.aws.amazon.com/config/latest/developerguide/conformance-packs.html)
* [AWS GuardDuty Documentation](https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html)
* [SOC 2 on AWS](https://aws.amazon.com/compliance/soc-faqs/)
* Mapping AWS Services to SOC 2 Trust Criteria[Mapping AWS Controls to SOC 2: A Comprehensive Guide](https://linfordco.com/blog/mapping-aws-controls-soc-2/)

**🎯 End-of-Day Goal / Outcomes**

**Participants should be able to:**

* Design and enforce secure VPC segmentation using Security Groups and NACLs
* Monitor and analyze network traffic with VPC Flow Logs
* Implement Bastion host or SSM access controls for private resources
* Understand SOC 2 criteria and apply relevant AWS services for compliance
* Map AWS infrastructure to SOC 2 control requirements and prepare for audit-readiness