How to Detect Unauthorized Access

🛡️ **AWS CloudTrail**

- Tracks all actions (API calls) done in AWS.
- Helps find *who did what*, *when*, and *from where*.

👁️ **Amazon GuardDuty**

- Uses AI to detect suspicious behavior (like someone trying to hack).
- Sends **alerts** if something looks risky (like strange logins or port scans).

📊 **VPC Flow Logs**

- Shows all traffic in and out of your network.
- Helps detect unknown IPs or too much data transfer.

✅ **AWS Config**

- Tracks if anyone changes security settings.
- Helps check if something was misconfigured.

---

2. Real-Time Monitoring Tools

📈 **Amazon CloudWatch**

- Set **alerts** for strange behavior.
- Automatically **respond** using Lambda (e.g., block an IP).

🔒 **AWS Security Hub**

- Collects security alerts from all AWS services.
- Tells which alerts are **most important**.

Third-Party Tools (like Splunk or ELK)

- Advanced analysis.
- Helps in **investigation** and **response workflows**.

---

3. Prevent Unauthorized Access

🧱 **Security Groups & NACLs**

- **Security Groups**: Only allow required access to your EC2 (default allow-only).
- **NACLs**: Can block specific IPs or locations (default allow & deny rules).

🔐 **IAM (Identity & Access Management)**

- Use **MFA (2FA)** for extra security.
- Give **least privilege** – only what is required.

🌐 **AWS WAF**

- Protects websites from attacks like DDoS, bots, or malicious IPs.

- Limits repeated access or fake requests.

---

4. Network Security Practices

🔒 **Private Subnets**

- Keep sensitive servers hidden from internet.
- Use **Bastion Host** or **SSM Session Manager** for admin access.

🚦 **Route Control**

- Use **Transit Gateway** to monitor and control VPC-to-VPC traffic.
- Send traffic via security appliances for inspection.

---

5. Responding to Threats

⚙️ **Automated Response**

- Lambda can **block IPs** or **shut down instances**.
- Modify **security groups** in real-time if needed.

📝 **Manual Response**

- Follow **incident playbooks**.
- Take **snapshots/logs** for investigation.

---

6. Smart Detection Tools

🕵️ **AWS Detective**

- Visual tool to trace how an attack happened.
- Helps identify **root cause** and **attack path**.

🤖 **Amazon Macie & Machine Learning**

- Finds sensitive data and warns if accessed wrongly.
- Learns normal behavior and spots anything unusual.

✅ 7. Compliance & Best Practices

- Do **regular security checks** (vulnerability scan, penetration tests).
- Keep **logs and audit trails** for compliance (SOC 2, ISO 27001).
- Use **Infrastructure as Code (IaC)** for consistent security settings.
- Add security tests in **CI/CD pipelines**.

✅ Summary (Key Points to Remember)

Area	Tool/Service	Purpose
🔍 Detect	CloudTrail, GuardDuty	Watch logs, detect strange actions
👁️ Monitor	CloudWatch, Security Hub	Get alerts, central visibility
🔒 Prevent Access	IAM, NACLs, SGs	Block/allow traffic, least access
🚫 Stop Attacks Early	WAF, VPC Flow Logs	Block known threats, monitor traffic
🚨 Respond	Lambda, SSM	Take action automatically
🧠 Smart Analysis	Macie, Detective	Investigate and find patterns

Which AWS service helps detect suspicious login activity and port scanning in your VPC using machine learning?

A) AWS Config
B) AWS CloudTrail
C) Amazon GuardDuty
D) AWS WAF
Correct Answer: ✅ C) Amazon GuardDuty
Explanation:
Amazon GuardDuty uses AI/ML to detect threats like unusual logins, port scans, and data exfiltration in real time.