🧩 AWS DevOps Engineer (DOP-C02) — Detailed Summary with Security Mapping

---

1. Application Deployment

Purpose: Automate and manage application deployments across environments.
AWS Services:

- **AWS Elastic Beanstalk:** Simplifies deployment and scaling of web applications.
- **AWS CodeDeploy:** Automates application deployment to EC2, Lambda, and on-prem.
- **AWS App Runner:** Runs containerized web apps without managing servers.
- **AWS CloudFormation / CDK:** Infrastructure as Code (IaC).
- **AWS Systems Manager:** Operational automation, patching, configuration.

Security:

- Use **IAM roles** and **KMS encryption**.
- Ensure deployments run under least-privileged roles.
- Log every deployment via **CloudTrail**.

---

2. Application Integration

Purpose: Connect microservices, SaaS, and event-driven architectures.
AWS Services:

- **Amazon EventBridge:** Event bus for integrating services.
- **Amazon AppFlow:** Moves SaaS data into AWS securely.

- (Also implied: **SNS**, **SQS**, **Step Functions**).

Security:

- Integrates with **IAM**, **VPC endpoints**, and **KMS** for secure event flows.
- Encrypted message payloads.

---

3. Application Pipelines (CI/CD)

Purpose: Automate build, test, and deployment processes.
AWS Services:

- **AWS CodePipeline:** Orchestrates CI/CD stages.
- **CodeBuild:** Build and test automation.
- **CodeDeploy:** Deployment automation.
- **CodeArtifact:** Private dependency repository.
- **AWS CodeStar:** Unified project dashboard.
- **AWS FIS:** Chaos engineering for resilience.
- **AWS X-Ray:** Distributed tracing and debugging.

Security:

- Enforce **IAM-based access** to pipelines.
- Store secrets in **Secrets Manager** or **Parameter Store**.
- Encrypt build artifacts with **KMS**.
- Monitor with **CloudTrail** and **CloudWatch Logs**.

---

4. Automation

Purpose: Reduce manual intervention in infrastructure and operations.
AWS Services:

- **AWS Systems Manager (SSM):** Patch, command automation, and inventory.
- **AWS CloudFormation / CDK / Proton / OpsWorks:** Infrastructure automation.
- **AWS Lambda:** Serverless automation triggers.

Security:

- Controlled via **IAM roles** and **KMS-encrypted parameters**.
- Use **CloudTrail** for execution audits.

---

5. Code Repository Best Practices

Purpose: Maintain version control and security of codebases.
AWS Services:

- **AWS CodeCommit:** Git-based code repository.
- **CodeArtifact:** Manages dependencies and build packages.

Security:

- IAM permissions for repo access.
- **Encryption-at-rest** via KMS, **TLS-in-transit**.
- Audit repo activity with **CloudTrail**.

---

6. Cost Optimization

Purpose: Optimize cost across compute, storage, and networking.
AWS Services:

- **AWS Cost Explorer**, **Budgets**, **Trusted Advisor**, **Compute Optimizer**.

Security:

- Control billing access with **Organizations** and **IAM policies**.

---

7. Deployment Requirements & Hybrid Deployments

Purpose: Support mixed environments (on-prem + cloud).
AWS Services:

- **CodeDeploy (on-prem)**
- **AWS VPN**, **Transit Gateway**, **Direct Connect**, **PrivateLink**
- **AWS Directory Service** for identity federation.

Security:

- Use **VPC, NACLs, Security Groups** for secure network design.
- Identity federation via **IAM Identity Center** or **AD**.

---

8. IAM Policies

Purpose: Fine-grained access control.
AWS Services:

- **AWS IAM**, **IAM Identity Center**, **STS**, **RAM**.

Security:

- Defines **who can access what**.
- Combine **SCPs (Service Control Policies)** with **Organizations**.

---

9. Metrics, Monitoring, Alarms, Logging

Purpose: Operational visibility, auditing, and anomaly detection.
AWS Services:

- **Amazon CloudWatch:** Metrics and dashboards.
- **CloudWatch Logs & Alarms:** Log storage and alerts.
- **AWS CloudTrail:** API and user activity tracking.
- **AWS X-Ray:** Application tracing.
- **AWS Config:** Resource compliance tracking.
- **Managed Grafana / Prometheus:** Visualization and metrics.

Security:

- Encrypted logs via **KMS**.
- Enable **CloudTrail** and **GuardDuty** for full audit visibility.

---

10. Network ACL & Security Group Design

Purpose: Secure and control network-level traffic.
AWS Services:

- **Amazon VPC**, **Security Groups**, **NACLs**.
- **Network Firewall**, **AWS Shield**, **AWS WAF**, **PrivateLink**, **Route 53**.

Security:

- Security Groups: Instance-level control (stateful).
- NACLs: Subnet-level control (stateless).
- Network Firewall: Centralized traffic filtering.
- Shield/WAF: Application & DDoS protection.

---

11. Operational Best Practices

Purpose: Maintain reliability and compliance.
AWS Services:

- **Trusted Advisor**, **Systems Manager**, **Config**, **Resilience Hub**, **OpsWorks**.

Security:

- **Trusted Advisor** security checks (open ports, exposed keys).
- **Config Rules** for compliance enforcement.

---

12. Rollback Procedures

Purpose: Recover safely from deployment failures.
AWS Services:

- **CodeDeploy**, **CloudFormation**, **Elastic Beanstalk**, **Lambda versioning**.

Security:

- Protect rollback scripts via **IAM**.
- Ensure actions are logged via **CloudTrail**.

🛡️ SECURITY, IDENTITY, AND COMPLIANCE — DETAILED LAYER MAPPING

Service	Works At (Layer)	Purpose / Function
AWS IAM	Identity Layer	User, role, and policy management.
IAM Identity Center (SSO)	Federation Layer	Centralized single sign-on access.
AWS STS	Identity/Auth Layer	Temporary credentials for limited-time access.
AWS KMS	Data Protection	Manages encryption keys for AWS services.
AWS CloudHSM	Data Protection	Hardware-backed cryptographic operations.
AWS Secrets Manager	Application Layer	Secure storage and rotation of credentials.
AWS Shield	Network Layer	DDoS protection at L3/L4.
AWS WAF	Application Layer	Web traffic filtering (L7 protection).
AWS Network Firewall	Network Layer	Stateful firewall inside VPCs.
AWS Certificate Manager (ACM)	TLS Layer	Manages SSL/TLS certificates.
Amazon Cognito	Identity (App Layer)	User authentication and federation.
Amazon GuardDuty	Detection Layer	Threat detection using logs and network flow.
Amazon Inspector	Compute Layer	Vulnerability scanning for EC2/ECR/Lambda.
AWS Security Hub	Aggregation Layer	Centralized security findings dashboard.

Amazon Macie	Data Layer	Detects and protects sensitive data (PII).
Amazon Detective	Investigation Layer	Incident analysis and investigation.
AWS Directory Service	Identity Layer	AWS–Active Directory integration.
AWS RAM	Management Layer	Cross-account resource sharing securely.

🧱 SECURITY LAYER SUMMARY

Layer	Representative Services	Function
Identity & Access	IAM, Identity Center, STS, Cognito	Authentication & Authorization
Data Protection	KMS, CloudHSM, Secrets Manager, ACM, Macie	Encryption, Privacy, Key Management
Network Security	SGs, NACLs, Network Firewall, Shield, WAF	Traffic filtering, DDoS protection
Threat Detection & Compliance	GuardDuty, Inspector, Security Hub, Detective, Config	Detection, Compliance, Auditing
Application Security	WAF, Cognito, Secrets Manager	Protect app-level access and secrets

🔐 QUICK SECURITY RECOMMENDATIONS

- Enforce **least privilege** using IAM policies and SCPs.
- Encrypt **data at rest (KMS)** and **in transit (ACM)**.
- Centralize alerts with **Security Hub** and **GuardDuty**.
- Secure private connectivity with **VPC endpoints / PrivateLink**.
- Rotate secrets automatically using **Secrets Manager**.