

# SEC480 – AWS Secure Builder

Topics	#
<b>Book 1: Secure Development and Deployment Practices in AWS</b>	
Course Agenda .....	1-3
Introduction to SEC480 .....	1-4-8
Responsibility to, for, and of Security .....	1-9-34
Lab 1.1: Protecting Web Applications with the AWS Web Application Firewall .....	1-35
Identification, Authorization .....	1-36-56
Lab 1.2: Application Authentication using AWS Cognito .....	1-57
CICD .....	1-58-82
Lab 1.3: Shifting left with security controls in AWS CodePipeline .....	1-83
Workload & Service Hardening .....	1-84-105
Lab 1.4: Encryption at rest with the Relational Database Service (RDS) and Simple Storage Service (S3) .....	1-106
Contacts and Resources .....	1-107
<b>2FA</b>	
Non-Human Accounts .....	1-47
2FA (Two-Factor Authentication) .....	1-41
2FA on Non-Human Accounts .....	1-47
<b>Book 2: Securing AWS: Monitoring, Incident Response, and Trust</b>	
Security Monitoring .....	2-3-18
Lab 2.1: Security Monitoring using CloudTrail and Access Logs: Early Warning System .....	2-19
Exposure and Attack Vectors .....	2-20-41
Lab 2.2: AWS Inspector: Reducing Attack Surface .....	2-42
Incident Response .....	2-43-66
Lab 2.3: AWS GuardDuty and VPC Flow Logs: Incident Response in Action .....	2-67
Trust, Control, and Supply Chain .....	2-68-90
Lab 2.4: Self-Escalation with AWS Identity Access Management (IAM) .....	2-91
Contacts and Resources .....	2-92
<b>Workbook</b>	
Lab 1.1: Protecting web applications with the AWS Web Application Firewall .....	3-2-25
Lab 1.2: Application Authentication using AWS Cognito .....	3-26-39
Lab 1.3: Shifting left with security controls in AWS CodePipeline .....	3-40-56
Lab 1.4: Encryption at rest with the Relational Database Service (RDS) and Simple Storage Service (S3) .....	3-57-84
Lab 2.1: Security Monitoring using CloudTrail and Access Logs .....	3-85-103
Lab 2.2: AWS Inspector .....	3-104-117
Lab 2.3: AWS GuardDuty and VPC Flow Logs .....	3-118-130
<b>Lab 1.1</b>	
AWS Load Balancer	
Application Load Balancer .....	W-3
Load Balancer .....	W-3
<b>AWS WAF</b>	
IP Sets .....	W-19
Managed Rule Group .....	W-12
Managed Rule Group - Custom .....	W-21
Rule Group .....	W-12
SQLi .....	W-5
WAF & Shield .....	W-8
Web ACL .....	W-8
Web Application Firewall (WAF) .....	W-8
<b>Lab 1.2</b>	
AWS Cognito .....	W-28-39
AWS Load Balancer	
Cognito .....	W-27
<b>Lab 1.3</b>	
AWS CodeBuild .....	W-50
AWS CodePipeline .....	W-42-47
Release Change .....	W-52
AWS Load Balancer .....	W-40-41
BuildSpec .....	W-50
ECR	
Private Registry .....	W-48
Elastic Container Registry (ECR) .....	W-48
Repository .....	W-48
<b>Lab 1.4</b>	
AWS Key Management Service (KMS) ..	W-57-59
Encryption	
At Rest .....	W-57-59
Policy JSON Syntax .....	W-59
RDS	
Encryption .....	W-61
KMS Key .....	W-63
Restore DB .....	W-65-69
Relational Database Service (RDS) .....	W-60
S3 .....	W-69
AWS Managed Keys .....	W-69
Customer Managed Keys .....	W-69
Encryption .....	W-69
<b>Lab 2.1</b>	
Amazon Athena .....	W-96
AWS CloudTrail .....	W-98
AWS Secrets Manager .....	W-98
S3	
Access Logging .....	W-94
Bucket Policy .....	W-91
Public .....	W-89
Secure Bucket .....	W-85
<b>Lab 2.2</b>	
AWS Inspector .....	W-108
EC2 .....	W-104
<b>Lab 2.3</b>	
AWS GuardDuty .....	W-118
Findings .....	W-119
CloudWatch Log .....	W-125

# SEC480 – AWS Secure Builder

EC2	
Public IP	W-120
Security Groups	W-121-123
VPC Flow Logs	W-124
<b>Lab 2.4</b>	
Access Key	W-136
CloudShell	W-132, W-140
IAM	W-132
Policy	W-134
S3	W-131

## A

Access Key Rotation (IAM)	1-38
Access Key Rotation (Non-Human Accounts)	1-47
Access Keys (Service Accounts)	1-46
Account Takeover (Authentication Failures)	1-52
Adaptability (Authentication)	1-51
AI and Machine Learning Integration (Security)	1-42
Alert Fatigue	2-12
Alerting	
Amazon SNS	2-16
AWS CloudWatch Alarms	2-16
AWS EventBridge	2-16
Alerting (Cloud-Native)	2-16
Amazon Elastic Container Registry (ECR)	1-70
Amazon Inspector	
Definition	2-11
Amazon Machine Images (AMIs)	1-88
Amazon SNS (Simple Notification Service)	2-16
Anomaly Detection	2-17, 1-26
API Gateway	
RESTful APIs	1-86
Scalability	1-86
Security	1-86
Traffic Management	1-86
WebSocket APIs	1-86
API Keys (Secrets)	1-71-72
Application Identity	1-48
Cognito Identity Pools	1-48
IAM Roles	1-48
IAM Users with Access Keys	1-48
Application Logging	2-5
Application Migration Strategy	1-15
Rearchitect	1-15
Rehost	1-15
Relocate	1-15
Replatform	1-15
Repurchase	1-15
Retain	1-15
Retire	1-15
Application Owners (Security Context)	1-105
Application Security	
Bugs (Code Scanning)	1-77
OWASP Top Ten Web Applications	1-30
RASP (Runtime Application Self-Protection)	1-73
SAST (Static Application Security Testing)	1-77
Source Code Analysis	1-77

Artifacts (Build context)	1-68
Attack Patterns	1-26
Attack Surface	2-22
Entry Points	2-31
Supply-Chain	2-22
Attack Surface (Internal and External)	2-31
Attack Vectors (NIST context)	1-43
Attacks	
Brute Force	1-53
Credential Stuffing	1-54
CSRF (Cross-Site Request Forgery)	1-54
EC2	2-35
Password Spraying	1-53
Password-Based	1-54
Phishing	1-54
Session Hijacking	1-54
Social Engineering	1-54
SSRF	2-35
SSRF (Server-Side Request Forgery)	2-32-33
Supply-Chain	2-22, 2-34
Username Harvesting	1-54
Audit (Security Assurance)	1-21
Authentication	
2FA	1-51
Account Takeover	1-52
Adaptability	1-51
Applications	1-48
Attacks	
Brute Force	1-53
Password Spraying	1-53
Common Flaws	1-53
Compliance	1-51
Credential Stuffing	1-54
CSRF (Cross-Site Request Forgery)	1-54
Data Breaches	1-52
Demo: Common Flaws	1-56
Ease of Exploitation	1-54
Expectations of Modern Authentication	1-51
Failures	1-52
Frictionless User Experience	1-51
Impersonation	1-53
MFA	1-51
Lack of MFA	1-53
Multi-Factor Authentication (MFA)	1-55
OWASP Top Ten	
Identification and Authentication Failures (7)	1-52
Passwords	
Insufficient Recovery Mechanisms	1-53
Weak or Reused	1-53
Risk-Based Authentication	1-51
Services	1-48
Session Management	
Vulnerabilities	1-53
Session Management (Mitigation)	1-55
Sessions	
Hijacking	1-54
Username Harvesting	1-54

# SEC480 – AWS Secure Builder

---

Authentication (IAM context) .....	1-37	Elastic Container Registry (ECR) .....	1-70
Authorization (IAM context) .....	1-37	EventBridge .....	2-16
Automating Security Processes .....	1-28	Automation .....	2-17
Automation .....		GuardDuty .....	2-6, 1-26
AWS EventBridge .....	2-17	IAM Identity Center .....	1-45
AWS Systems Manager Automation .....	2-17	Inspector (Container Security) .....	1-78-79
Build Processes .....	1-68	Lambda Functions (Machine Identity) .....	1-46
CloudWatch (Events) .....	2-17	Logging .....	2-4
Recovery Mechanisms .....	2-54	Aurora Logs .....	2-6
Runbooks .....	2-17	CloudTrail .....	2-4
Security Checks .....	1-68	CloudTrail Insights .....	2-6
Software Delivery Process .....	1-64	CloudWatch Alarms .....	2-8
Automation (CI/CD context) .....	1-59	CloudWatch Logs .....	2-4
Automation (DevOps) .....	1-27	CloudWatch Metrics .....	2-8
Automation (Security context) .....	1-28	GuardDuty .....	2-6
AWS .....		RDS Logs .....	2-6
API .....	1-85	S3 Data Events .....	2-6
API Gateway .....	1-86	WAF .....	2-6
Artifact .....	1-95	Monitoring in Practice .....	2-12
Aurora Logs .....	2-6	Monitoring Tools .....	2-11
Availability Zone (AZ) .....	1-89	X-Ray .....	2-12
Blueprint .....	1-25	Network ACLs .....	1-47
Cloud Development Kit (CDK) .....	1-22	Network ACLs (Access Control Lists) .....	1-47
CloudFront .....	1-90	Parameter Store .....	1-71-72
Cache .....	1-90	RDS (Relational Database Service) .....	1-89
Content Delivery Network (CDN) .....	1-90	RDS Logs .....	2-6
Edge Locations .....	1-90	Reference Architecture .....	1-25
CloudTrail .....	2-4, 1-33	S3 .....	
CloudTrail Insights .....	2-6	Definition .....	1-87
CloudWatch .....	1-33, 1-78-79	S3 (Simple Storage Service) .....	1-87
Alarms .....	2-16	S3 Buckets (misconfiguration) .....	1-31
Anomaly Detection .....	2-17	S3 Data Events .....	2-6
Automation (Events) .....	2-17	Secrets Manager .....	1-71-72
CloudWatch Alarms .....	2-8	Security Groups .....	1-47
CloudWatch Logs .....	2-4	Security Hub .....	1-26, 1-78-79
CloudWatch Metrics .....	2-8	Security Reference Architecture (SRA) .....	1-25
CodeBuild .....	1-62, 1-68	Example .....	1-26
Definition .....	1-64	Sign-in Process .....	1-40
Docker Integration .....	1-70	SNS (Simple Notification Service) .....	2-16
CodeBuild (SCA) .....	1-78-79	Systems Manager .....	2-17
CodeCommit .....	1-67	Automation .....	2-17
CodeDeploy .....	1-62	Systems Manager Patch Manager .....	1-33
Definition .....	1-64	WAF .....	1-26
CodeGuru .....	1-78-79	WAF Logging .....	2-6
CodePipeline .....	1-60	Workloads .....	1-92
Definition .....	1-64	X-Ray .....	2-12
CodeStar .....	1-65	AWS API .....	1-85
Cognito Identity Pools .....	1-48	AWS API Gateway .....	1-86
Common Services .....	1-85	Security and Compliance .....	1-91
Config Rules .....	1-33	AWS Artifact .....	1-95
Config Rules (IaC Scanning) .....	1-78-79	AWS Aurora Logs .....	2-6
Customer Incident Response Team (CIRT) ..	1-44	Definition .....	2-6
Deployment .....	1-64	AWS Availability Zone (AZ) .....	1-89
Docker Image .....	1-64	Definition .....	1-89
EC2 (Elastic Compute Cloud) .....	1-88	AWS CloudFront .....	1-90
EC2 Instances (Container Security) .....	1-78-79	AWS CloudTrail .....	2-4, 1-33
EC2 Instances (Machine Identity) .....	1-46	AWS CloudTrail Insights .....	2-6
ECS Cluster .....	1-70	Definition .....	2-6

# SEC480 – AWS Secure Builder

---

AWS CloudWatch .....	1-33, 1-78-79	AWS Lambda .....	
Alarms .....	2-16	Public Exposure .....	2-29
Anomaly Detection .....	2-17	AWS Macie .....	
AWS CloudWatch Alarms .....	2-8	Data Classification .....	2-28
AWS CloudWatch Logs .....	2-4	Definition .....	2-11
AWS CloudWatch Metrics .....	2-8	OSINT .....	2-28
AWS CodeBuild .....	1-62, 1-68	AWS Parameter Store .....	1-71-72
Artifacts .....	1-68	AWS RDS .....	
Build Processes .....	1-68	Amazon Aurora .....	1-89
Coding Standards .....	1-68	MySQL .....	1-89
Definition .....	1-64, 1-68	Non-Compliance (Misconfigurations) .....	1-96
Docker Integration .....	1-70	Oracle Database .....	1-89
Ephemeral Build Environments .....	1-68	PostgreSQL .....	1-89
Example (Docker) .....	1-70	Public Exposure .....	2-29
Scan for Vulnerabilities .....	1-68	Security and Compliance .....	1-91
Security Checks .....	1-68	AWS RDS (Relational Database Service) .....	1-89
AWS CodeCommit .....	1-67	AWS RDS Logs .....	2-6
AWS CodeDeploy .....	1-62	Definition .....	2-6
Definition .....	1-64	AWS Responsibilities .....	
AWS CodePipeline .....	1-60	Background checks .....	1-11
Definition .....	1-64	Core Services .....	1-11
IAM Integration .....	1-60	Hardware security .....	1-11
Key Features .....		Hypervisor .....	1-11
Automation .....	1-60	Networking and facilities security .....	1-11
Integration .....	1-60	Redundancy .....	1-11
Scalability .....	1-60	Software security .....	1-11
Security .....	1-60	AWS S3 .....	
Visualization .....	1-60	Compliance .....	1-87
AWS CodeStar .....	1-65	GDPR .....	1-87
Definition .....	1-65	HIPAA .....	1-87
Diagram .....	1-66	PCI DSS .....	1-87
AWS Common Services .....	1-85	SOC 2 .....	1-87
AWS Config .....		Default Settings .....	1-94
Definition .....	2-11	Example .....	
OSINT .....	2-28	Bucket Policy .....	1-97-98
AWS Config Rules .....	1-33	Non-Compliance (Misconfigurations) .....	1-96
AWS Customer Incident Response Team (CIRT) .....	1-44	Object Storage .....	1-87
AWS EC2 .....		Public Exposure .....	2-29
Amazon Machine Images (AMIs) .....	1-88	Security and Compliance .....	1-91
Attacks .....	2-35	Service Hardening .....	1-93
Instances .....	1-88	AWS S3 (Simple Storage Service) .....	1-87
Non-Compliance (Misconfigurations) .....	1-96	AWS S3 Data Events .....	2-6
Public Exposure .....	2-29	Definition .....	2-6
Security and Compliance .....	1-91	AWS Secrets Manager .....	1-71-72
Security Groups (Firewall) .....	1-88	AWS Security Blog .....	2-45
Service Hardening .....	1-93	AWS Security Bulletin .....	2-45
Virtual Machines .....	1-88	AWS Security Hub .....	1-26, 1-78-79
AWS EC2 (Elastic Compute Cloud) .....	1-88	Definition .....	2-11
AWS Elastic Beanstalk .....		AWS Security Reference Architecture (AWS SRA) .....	1-16, 1-25
Public Exposure .....	2-29	Example .....	1-26
AWS EventBridge .....	2-16	AWS Services .....	
AWS GuardDuty .....	2-6, 1-26	Security and Compliance .....	1-91
Definition .....	2-6, 2-11	AWS SRA Approach to Deploying AWS Security Services .....	1-25
Machine Learning .....	2-17	AWS Systems Manager .....	2-17
OSINT .....	2-28	Automation .....	2-17
AWS IAM .....		Runbooks .....	2-17
CodePipeline Integration .....	1-60		
AWS IAM Identity Center .....	1-45		

# SEC480 – AWS Secure Builder

AWS Systems Manager Patch Manager	1-33
AWS WAF	1-26
Definition	2-11
Real World Attack	2-35
AWS WAF Logging	2-6
Definition	2-6
AWS Well-Architected Framework	1-16
Cost Optimization	1-16
Operational Excellence	1-16
Performance Efficiency	1-16
Reliability	1-16
Security	1-16
Sustainability	1-16
AWS Workloads	1-92
Definition	1-92
AWS X-Ray	2-12
Definition	2-12

## B

Benchmark	1-23
Best-Effort Logging	2-7
Blueprint	1-25
Blueprint (DPRA)	1-63
Blueprints	1-16
Branching (VCS context)	1-67
Breaches	1-24
Capital One	2-35
CrowdStrike	1-24
Equifax	2-51
FireEye	2-12
Marriott	1-102
Notifications	2-70
Real World Attacks	2-35
SSRF (Real World)	2-35
Target	1-24
Bugs (Code Scanning context)	1-77
Build (DevOps context)	1-27
Build Process	
Example (Real-World)	1-74-75
Business Owners (Security Context)	1-105

## C

Caching	
CloudFront	1-90
Canary Tokens	2-66
Capital One	
Breach	2-35
Center for Internet Security (CIS)	1-32
Centralized IAM Management	1-38
Centralized User Management	1-45
Change management	1-13
CI/CD	
Artifacts (Build context)	1-68
Automation	1-59
AWS CodeBuild	1-62, 1-68

AWS CodeCommit	1-67
AWS CodeDeploy	1-62
AWS CodePipeline	1-60
AWS CodeStar	1-65
AWS CodeStar Diagram	1-66
Build Processes (Automation)	1-68
Code Scanning	1-77
CodeBuild Definition	1-64
CodeBuild Docker Integration	1-70
CodeDeploy Definition	1-64
CodePipeline Definition	1-64
Compile Executable	1-64
Continuous Delivery (CD)	1-59
Continuous Delivery Service (AWS CodePipeline)	1-60
Continuous Integration (CI)	1-59
Dealing with Secrets	1-71-72
Demo: Code Scanning	1-82
Deployment	1-64
Deployment Pipeline Reference Architecture (DPRA)	1-63
DevOps Collaboration	1-59
DevSecOps	1-76
Docker	1-62
Docker Image	1-64
ECR (Elastic Container Registry)	1-70
ECS Cluster	1-70
Ephemeral Build Environments	1-68
Examples	
Code Scanning	1-82
CodeBuild Docker	1-70
Real-World Build Process	1-74-75
Release Automation: Pipeline Workflow	1-62
Repository	1-62
Secrets	1-71-72
Security Checks (Build)	1-68
Software Delivery Process	1-64
Stages (DPRA)	1-63
Version Control Systems (VCS)	1-67
CI/CD (Continuous Integration/Continuous Delivery)	1-59
CI/CD Pipeline	
Stages	
Build	1-73
Deploy	1-73
Source	1-73
Test	1-73
CIRT	
Customer Security	1-44
Isolating Impacted Systems	1-44
Revoke Access Keys	1-44
Rotate Credentials	1-44
Security Events	1-44
CIS	
Center for Internet Security	1-32
CIS (Center for Internet Security)	1-34
CIS Controls	1-23, 1-32
Roadmap	1-32

# SEC480 – AWS Secure Builder

---

Safeguard .....	1-32	AWS S3 .....	1-87, 1-91
Clients/Customers (Variables) .....	1-55	Non-Compliance .....	1-96
Cloud		AWS Services .....	1-91
IAM .....	1-37	Benchmark .....	1-23
Responsibility .....	1-14	Center for Internet Security (CIS) .....	1-32
Security Practices .....	1-14	CIS (Center for Internet Security) .....	1-34
Cloud Computing		CIS Controls .....	1-23, 1-32
AWS Workloads .....	1-92	COBIT .....	1-23
Cloud Development Kit (CDK) .....	1-22	Compliant by Design .....	1-95
Cloud Infrastructure		Culture (Security Program) .....	1-34
Availability Zone (AZ) .....	1-89	Desired outcomes .....	1-19
Cloud Security Posture Management (CSPM) ....	2-41	Difference from Security .....	1-19
Cloud Services		Discussion on Importance of CIS and Maturity of	
IAM Integration .....	1-49	Security Program .....	1-34
Cloud-Native Alerting .....	2-16	Discussion on Security vs Compliance .....	1-24
CloudFront		Due Care .....	1-22
Cache .....	1-90	Due Diligence .....	1-22
Content Delivery Network (CDN) .....	1-90	Due Diligence and Best Practices .....	1-22
Edge Locations .....	1-90	Examples	
COBIT .....	1-23	Proper Configuration .....	1-97-98
Code Scanning .....	1-77	Zoom .....	1-103
Bugs .....	1-77	Forensic Readiness .....	2-13
Example .....	1-82	Frameworks .....	1-23, 2-38
SAST (Static Application Security Testing) .	1-77	Frameworks and Standards .....	1-23
Source Code Analysis .....	1-77	GDPR .....	1-20, 2-27
Codebase quality .....	1-13	GDPR (S3) .....	1-87
Codebase security .....	1-13	HIPAA .....	1-20, 2-27
Coding Standards (CI/CD Build) .....	1-68	HIPAA (S3) .....	1-87
Cognito Identity Pools .....	1-48	Implications .....	2-18
Collaboration (DevOps context) .....	1-27	Initiatives .....	2-38
Commit (VCS context) .....	1-67	ISO 27001 .....	1-23
Common Flaws (Authentication) .....	1-53	ISO Standards (Compliant by Design) .....	1-95
Brute Force Attacks .....	1-53	Logging .....	2-9-10
Impersonation .....	1-53	Mandates .....	2-38
Insufficient Recovery Mechanisms .....	1-53	Maturity .....	1-24
Lack of MFA .....	1-53	Maturity (Security Program) .....	1-34
Password Spraying .....	1-53	Misconfigurations .....	1-96
Session Management Vulnerabilities .....	1-53	Monitoring .....	2-13
Username Harvesting Example .....	1-56	Monitoring for Security and Compliance ....	2-13
Weak or Reused Passwords .....	1-53	NIST Cybersecurity Framework (CSF) .....	1-23, 2-39-40
Communication		NIST Digital Identity Guidelines (SP 800-63 se-	
Breach Notifications .....	2-70	ries) .....	1-43
Communications Lead (Incident Response) .....	2-52	NIST Guidance .....	1-43
Compile Executable (CI/CD) .....	1-64	Non-Compliance	
Complexity (Security Risk) .....	1-99	Due to Misconfigurations .....	1-96
Compliance .....	1-17	PCI DSS .....	1-17, 1-23, 2-27
Adherence to requirements .....	1-19	Breach .....	1-24
Assurance .....	1-21	PCI DSS (Compliant by Design) .....	1-95
Attestations (Compliant by Design) .....	1-95	PCI DSS (S3) .....	1-87
Audit .....	1-21, 2-38	PCI Report of Compliance (ROC) .....	1-21
AWS API Gateway .....	1-91	PII (Personally Identifiable Information) ...	2-18
AWS Artifact .....	1-95	Point in time assessment .....	1-19
AWS CloudTrail .....	1-33	Proactive .....	1-19
AWS Config Rules .....	1-33	Reactive .....	1-19
AWS EC2 .....	1-91	Regulations (Assurance) .....	1-21
Non-Compliance .....	1-96	Relevancy .....	2-27
AWS RDS .....	1-91	Reporting .....	2-13
Non-Compliance .....	1-96		

# SEC480 – AWS Secure Builder

Risk Management (NIST) .....	1-43
Risk Mitigation .....	1-20
Security (discussion) .....	1-24
Security Maturity Assessments .....	1-104
Shared Responsibility .....	1-17
Shared Responsibility Model .....	1-17
SOC (Service Organization Control) .....	1-95
SOC (System and Organization Controls) ...	1-21
SOC 2 (S3) .....	1-87
Standards .....	1-23
Standards (Assurance) .....	1-21
Violations	
Zoom .....	1-103
Vulnerability and Patch Management .....	1-33
Vulnerability Management .....	1-81
Compliance (Authentication) .....	1-51
Compliance as a Tool .....	2-38
Compliance Reporting .....	2-13
Compliant by Design .....	1-95
Attestations .....	1-95
AWS Artifact .....	1-95
ISO Standards .....	1-95
PCI DSS .....	1-95
SOC (Service Organization Control) .....	1-95
Confidence (Security Assurance) .....	1-21
Container Security Tools	
Amazon Inspector .....	1-78-79
Aqua Security .....	1-78-79
EC2 Instances .....	1-78-79
Trivy .....	1-78-79
Content Delivery Network (CDN)	
CloudFront .....	1-90
Content Security Policy (CSP) .....	2-89
Continuous Delivery (CD) .....	1-59
Continuous Delivery Service (AWS CodePipeline)	1-60
Continuous Integration (CI) .....	1-59
Continuous Verification (Zero-Trust) .....	1-42
Contract Details (Trust and Supply Chain) .....	2-69
Control	
Information .....	2-25
Responsibility .....	1-13
Core Functions (NIST CSF) .....	2-40
Coupa (Vendor Management) .....	2-75
Credential Stuffing .....	1-54
Cross-Site Request Forgery (CSRF) .....	1-54
Cryptographic Algorithms .....	1-100-101
Cryptographic Failures .....	1-100-101
Algorithms .....	1-100-101
Key Management	
Insecure .....	1-100-101
Culture (DevOps/DevSecOps) .....	1-27
Culture (Mitigation context) .....	1-55
Culture (Security Program) .....	1-34
Current and Emerging Trends .....	1-42
Customer Responsibilities	
Access controls .....	1-11
Applications and data .....	1-11
Configurations and management .....	1-11

Security settings .....	1-11
Customer Security	
CIRT .....	1-44
Rotate Credentials (CIRT) .....	1-44

## D

DAST (Dynamic Application Security Testing) ..	1-29, 2-41
DAST Tools	
Burp Suite .....	1-78-79
OWASP ZAP .....	1-78-79
Data Breaches (Authentication Failures) .....	1-52
Data Exfiltration Attempts .....	1-26
Data Integrity .....	2-86
Data Logging .....	2-6
Data Loss Prevention (DLP) .....	2-26
Database Credentials (Secrets) .....	1-71-72
Databases	
Amazon Aurora (RDS) .....	1-89
AWS RDS (Relational Database Service) ....	1-89
MySQL (RDS) .....	1-89
Oracle Database (RDS) .....	1-89
PostgreSQL (RDS) .....	1-89
Dealing with Secrets .....	1-71-72
Decision Trees	
Incident Response .....	2-53
Default Settings	
AWS S3 .....	1-94
Default Settings (Security Risks) .....	1-94
Defenses	
Dependency Management .....	2-88-89
Software Composition Analysis (SCA) ....	2-88-89
Defenses in Practice .....	2-88-89
Definition (2FA/MFA) .....	1-41
Delineation (Security Responsibilities) .....	1-18
Demo: Code Scanning .....	1-82
Demo: Common Flaws .....	1-56
Dependency Management .....	2-88-89
Deployed Workloads .....	2-30
Deployment (CI/CD) .....	1-64
Deployment (DevOps context) .....	1-27
Deployment Pipeline Reference Architecture (DPRA)	1-63
DevOps	
Automation .....	1-27, 1-59
Build .....	1-27
CI/CD (Continuous Integration/Continuous De-	
livery) .....	1-59
Collaboration .....	1-27, 1-59
Continuous Delivery (CD) .....	1-59
Continuous Integration (CI) .....	1-59
Culture .....	1-27
Deployment .....	1-27
DevSecOps .....	1-76
Infrastructure as Code (IaC) .....	1-27
Infrastructure Provisioning .....	1-27
Monitoring and Feedback .....	1-27

# SEC480 – AWS Secure Builder

Operations Teams .....	1-27
SecDevOps .....	1-27
Test .....	1-27
DevOps Approach in Practice .....	1-27
DevOps Collaboration .....	1-59
DevSecOps .....	1-76
Cost Reduction .....	1-76
Culture .....	1-76
Security Expertise .....	1-76
Shift-Left .....	1-76
Differences (On-prem vs Cloud) .....	1-14
Discussion on IAM (AWS CIRT) .....	1-44
Discussion on Importance of CIS and Maturity of Security Program .....	1-34
Discussion on Security vs Compliance .....	1-24
Docker (CI/CD context) .....	1-62
Docker Image (CI/CD) .....	1-64
DPRA	
Blueprint .....	1-63
How it Works	
Environment Management .....	1-63
Monitoring and Feedback .....	1-63
Pipeline Actions .....	1-63
Pipeline Artifacts .....	1-63
Pipeline Stages .....	1-63
Security and Compliance .....	1-63
Stages .....	1-63
Drop-and-shop .....	1-15
Due Care .....	1-22
Due Diligence .....	1-22
Due Diligence (Vendor and Supply Chain) .....	2-71
Due Diligence and Best Practices .....	1-22
Dynamic Credential Provisioning .....	1-46
Dynamically Assign Permissions .....	1-47
IAM Roles .....	1-47

## E

Early Warning Indicators (Incident Response) ...	2-63
Ease of Exploitation .....	1-54
EC2 .....	1-13
Amazon Machine Images (AMIs) .....	1-88
Instances .....	1-88
Security Groups (Firewall) .....	1-88
Virtual Machines .....	1-88
EC2 Instances	
Machine-to-Machine Identity .....	1-88
EC2 Instances (Machine Identity) .....	1-46
ECS Cluster .....	1-70
Edge Locations (CloudFront) .....	1-90
EDR (Endpoint Detection and Response)	
Definition .....	2-61
Education	
User .....	1-55
Education (Security in SDLC) .....	1-29
Encryption (DLP context) .....	2-26
Encryption at rest .....	1-13
Encryption Keys (Secrets) .....	1-71-72

End-User Risk .....	2-87
Endpoint Detection and Response (EDR) .....	2-41
Enhanced Security with WebAuthn .....	1-42
Entry Points (Attack Surface) .....	2-31
Environmental Variables (Secrets) .....	1-71-72
Ephemeral Build Environments .....	1-68
Equifax	
Breach .....	2-51
Essential Security Tools .....	1-78-79
Example	
SRI .....	2-90
Examples	
AWS S3	
Bucket Policy .....	1-97-98
Code Scanning .....	1-82
CodeBuild Docker .....	1-70
Compliance	
Proper Configuration .....	1-97-98
IAM	
Role Policy .....	1-97-98
Real-World Build Process .....	1-74-75
Username Harvesting Vulnerability .....	1-56
Expectations of Modern Authentication .....	1-51
2FA/MFA .....	1-51
Adaptability .....	1-51
Compliance .....	1-51
Frictionless User Experience .....	1-51
Risk-Based Authentication .....	1-51
Exposed Services .....	2-29
Exposure	
Exposed Services .....	2-29
Information Leakage .....	2-24
OSINT (Open-Source Intelligence) .....	2-20
Reducing Sensitive Data Leakage .....	2-26
Risk .....	2-23

## F

Failures	
Authentication .....	1-52
Identification .....	1-52
File Integrity Monitoring (FIM) .....	2-8
FireEye	
Breach .....	2-12
Firewall rules .....	1-13
Forensic Readiness .....	2-13
Foundation (AWS Architecture) .....	1-16
Frameworks .....	1-23
NIST Cybersecurity Framework (CSF) ..	2-39-40, 1-104
NIST Incident Response (SP 800-61r2) .....	2-50
Frictionless User Experience (Authentication) ...	1-51
Fundamental differences: On-prem vs Cloud security practices .....	1-14

## G

GDPR
------



# SEC480 – AWS Secure Builder

---

Notification Timeline .....	2-70
Governance	
Control Over Information .....	2-25
Ownership .....	1-105
Groups (IAM context) .....	1-37

## I

IaC Scanning Tools	
AWS Config Rules .....	1-78-79
Checkov .....	1-78-79
TFLint .....	1-78-79
IAM	
2FA (Two-Factor Authentication) .....	1-41
2FA on Non-Human Accounts .....	1-47
Access Key Rotation .....	1-38
Access Key Rotation (Non-Human Accounts) ..	1-47
Access Keys (Service Accounts) .....	1-46
Application Identity .....	1-48
Audits .....	1-38
Authentication .....	1-37
Authorization .....	1-37
AWS CodePipeline Integration .....	1-60
AWS IAM Identity Center .....	1-45
AWS Sign-in Process .....	1-40
Best Practices .....	1-38
Centralized Management .....	1-38
Centralized User Management .....	1-45
Cloud Service Integration .....	1-49
Cognito Identity Pools .....	1-48
Definition .....	1-37
Definition (2FA/MFA) .....	1-41
Discussion (AWS CIRT) .....	1-44
Dynamic Credential Provisioning .....	1-46
Dynamically Assign Permissions .....	1-47
Example	
IAM Role Policy .....	1-97-98
Gatekeeper .....	1-37
Groups .....	1-37
Identity Lifecycle Management .....	1-43
Identity Provider (IdP) .....	1-45
Integration with Cloud Services .....	1-49
Machine-to-Machine Identity (Service Accounts)	
1-46	
Multi-Factor Authentication (MFA) ...	1-38, 1-41
Password Policy .....	1-38
Passwords .....	1-39
Permissions .....	1-37
Principle of Least Privilege .....	1-38, 1-50
RBAC (Role-Based Access Control) .....	1-50
Roles .....	1-37
Roles (Application Identity) .....	1-48
Roles (Best Practices) .....	1-38
Roles (Dynamic Assignment) .....	1-47
Service Accounts .....	1-46
Service Hardening .....	1-93
SSO (Single Sign-On) .....	1-39, 1-45

Strategy .....	1-49
Two-Factor Authentication (2FA) .....	1-41
Users .....	1-37
Users with Access Keys .....	1-48
Workforce Identity Management .....	1-45
IAM Best Practices .....	1-38
IAM in the Cloud .....	1-37
IAM Integration with Cloud Services .....	1-49
IAM Password Policy .....	1-38
IAM Roles (Application Identity) .....	1-48
IAM Roles (Best Practices) .....	1-38
IAM Users with Access Keys .....	1-48
IBM QRadar (SIEM) .....	2-60
Identification	
Failures .....	1-52
Identification and Authentication Failures .....	1-52
Account Takeover .....	1-52
Data Breaches .....	1-52
Identity	
Services .....	1-48
Identity Federation .....	1-42
Definition .....	1-42
Identity Governance and Administration (IGA) ..	1-42
Identity Lifecycle Management (NIST) .....	1-43
Identity Provider (IdP) .....	1-45
Impersonation (Authentication Flaw) .....	1-53
Incident	
Zoom .....	1-103
Incident Manager (Incident Response) .....	2-52
Incident Response .....	2-43
Canary Tokens .....	2-66
Containment (Demo) .....	2-56
Decision Trees .....	2-53
Early Warning Indicators .....	2-63
Eradication and Root Cause (Demo) .....	2-57
Identification (Demo) .....	2-55
Indicators of Attack (IoA) .....	2-64-65
Lessons Learned (Demo) .....	2-59
Monitoring .....	2-43
NIST IR Framework .....	2-50
People	
Communications Lead .....	2-52
Incident Manager .....	2-52
Security Analyst .....	2-52
Technical Lead .....	2-52
Plan .....	2-43
Playbooks .....	2-53
Demo .....	2-55-59
Preparation .....	2-43
Recovery and Education (Demo) .....	2-58
Security Incident Response Team (SIRT) ...	2-43
Steps	
Containment .....	2-46
Eradication .....	2-47
Identification .....	2-45
Lessons Learned .....	2-49
Preparation .....	2-44
Recovery .....	2-48

# SEC480 – AWS Secure Builder

---

Tabletop Exercise .....	2-43
Tabletop Exercises .....	2-62
Technical Controls .....	2-54
Tools and Implementation .....	2-60-61
Incident response .....	1-13
Incident Response Section .....	2-42
Indicators of Attack (IoA) .....	2-64-65
Indicators of Compromise (IOC) .....	2-45
Information	
Control .....	2-25
Information Leakage .....	2-24
Infrastructure as Code (IaC) .....	1-27, 2-41
Infrastructure Provisioning .....	1-27
Instances (EC2) .....	1-88
Insurance (Security Assurance) .....	1-21
Integrating Security into SDLC .....	1-29
Integrity Failures	
Software and Data .....	2-86
Intrusion Detection Systems (IDS) .....	2-8
ISO 27001 .....	1-23
Isolating Impacted Systems (CIRT context) .....	1-44
Ivalua (Vendor Management) .....	2-75

## K

Key Management	
Insecure .....	1-100-101

## L

Lambda Functions (Machine Identity) .....	1-46
Lessons Learned	
Zoom .....	1-103
Lift-and-shift .....	1-15
Logging	
Application Logging .....	2-5
AWS Aurora Logs .....	2-6
AWS CloudTrail .....	2-4
AWS CloudTrail Insights .....	2-6
AWS CloudWatch Alarms .....	2-8
AWS CloudWatch Logs .....	2-4
AWS CloudWatch Metrics .....	2-8
AWS GuardDuty .....	2-6
AWS RDS Logs .....	2-6
AWS S3 Data Events .....	2-6
AWS WAF Logging .....	2-6
Best-Effort Logging .....	2-7
CloudWatch Anomaly Detection .....	2-17
Compliance .....	2-9-10
Implications .....	2-18
Data Logging .....	2-6
Enhanced .....	2-17
Fix .....	2-14-15
Insufficient .....	2-14-15
Management Plane .....	2-4
Privacy	
Implications .....	2-18

SIEM .....	2-7
Logging in AWS .....	2-4
Logging Pitfalls .....	2-7-8
Logs (Security context) .....	1-26

## M

Machine Learning	
GuardDuty .....	2-17
Machine Learning (Security context) .....	1-26
Machine-to-Machine Identity	
EC2 Instances .....	1-88
Machine-to-Machine Identity (Service Accounts) .....	1-46
2FA on Non-Human Accounts .....	1-47
Access Key Rotation .....	1-47
Access Keys .....	1-46
Dynamic Credential Provisioning .....	1-46
Dynamically Assign Permissions .....	1-47
EC2 Instances .....	1-46
Lambda Functions .....	1-46
Monitoring and Logging .....	1-47
Network Security Controls .....	1-47
Service Accounts .....	1-46
Management Plane	
Logging .....	2-4
Marriott	
Breach .....	1-102
Maturity .....	1-24
Maturity (Security Program) .....	1-34
Mechanical Sympathy .....	1-16
Merging (VCS context) .....	1-67
MFA	
Lack of MFA .....	1-53
Non-Human Accounts .....	1-47
MFA (Multi-Factor Authentication) .....	1-51
Migration (On-prem to Cloud) .....	1-15
Misconfigurations (Compliance context) .....	1-96
Mitigation Strategies .....	1-55
Multi-Factor Authentication .....	1-55
Passwords	
Hashing .....	1-55
Salting .....	1-55
Regular Security Audits .....	1-55
Secure Password Storage .....	1-55
Session Management .....	1-55
Strong Password Policies .....	1-55
User Education .....	1-55
Monitoring	
Alert Fatigue .....	2-12
Alerting (Cloud-Native) .....	2-16
Anomaly Detection .....	2-17
Compliance .....	2-13
Compliance Reporting .....	2-13
File Integrity Monitoring (FIM) .....	2-8
Fix .....	2-14-15
Inadequate .....	2-14-15
Intrusion Detection Systems (IDS) .....	2-8
Security-Relevant Data .....	2-13

# SEC480 – AWS Secure Builder

Threat Hunting .....	2-13
Monitoring and Feedback (DevOps) .....	1-27
Monitoring and Logging (Machine Accounts) ....	1-47
Monitoring for Security and Compliance .....	2-13
Monitoring in Practice .....	2-12
Monitoring Tools .....	2-11
Multi-Factor Authentication (MFA) ..	1-38, 1-41, 1-55

## N

Network ACLs	
Network Security Controls .....	1-47
Network ACLs (Access Control Lists) .....	1-47
Network Security	
Service Hardening .....	1-93
Network Security Controls	
Network ACLs .....	1-47
Security Groups .....	1-47
Network Security Controls (Machine Accounts) ..	1-47
Network ACLs .....	1-47
Security Groups .....	1-47
Network Segmentation (Incident Response) .....	2-54
Network Traffic Analysis (NTA)	
Definition .....	2-61
Network-based Security Model .....	1-42
Networking	
AWS CloudFront .....	1-90
NIST	
Special Publication 800-61r2 (Incident Response)	
2-50	
NIST CSF	
Core Functions .....	2-40
Risk-Based Approach .....	2-39
NIST Cybersecurity Framework (CSF) .	1-23, 2-39-40,
1-104	
NIST Digital Identity Guidelines (SP 800-63 series)	
1-43	
NIST Guidance .....	1-43
NIST Incident Response Framework (SP 800-61r2) .	2-50
Non-Compliance	
AWS EC2 (Misconfigurations) .....	1-96
AWS RDS (Misconfigurations) .....	1-96
AWS S3 (Misconfigurations) .....	1-96
Due to Misconfigurations .....	1-96

## O

Object Storage (S3) .....	1-87
On-prem	
Responsibility .....	1-14
Security Practices .....	1-14
Open Worldwide Application Security Project	
(OWASP) .....	1-30
Open-Source Intelligence (OSINT) .....	2-20
Operations Teams .....	1-27
OSINT	

AWS Tools .....	2-28
Identification .....	2-28
Relevancy to Compliance .....	2-27
Workloads .....	2-30
OSINT (Open-Source Intelligence) .....	2-20
OWASP	
Top Ten Web Applications .....	1-30
OWASP Top Ten	
Broken Access Control .....	1-30
Cryptographic Failures .....	1-30
Cryptographic Failures (2) .....	1-100-101
Identification and Authentication Failures ...	1-30
Identification and Authentication Failures (7) ..	1-52
Injection .....	1-30
Insecure Design .....	1-30
Logging and Monitoring Failures (9) .....	2-14-15
Security Logging and Monitoring Failures ...	1-30
Security Misconfiguration .....	1-30
Security Misconfiguration (expanded) .....	1-31
Server-Side Request Forgery (SSRF) .....	1-30
Software and Data Integrity Failures .....	1-30
SSRF (Server-Side Request Forgery) .....	2-32-33
Vulnerable and Outdated Components .....	1-30
OWASP Top Ten Web Applications .....	1-30
Ownership	
Application Owners .....	1-105
Business Owners .....	1-105
System Owners .....	1-105
Ownership (Security Perspective) .....	1-105

## P

Passwordless Authentication .....	1-42
Passwords	
Attacks .....	1-54
Hashing .....	1-55
Insufficient Recovery Mechanisms .....	1-53
Salting .....	1-55
Secure Storage .....	1-55
Strong Policies .....	1-55
Weak or Reused .....	1-53
Passwords (Security Fatigue context) .....	1-39
Payment Card Data .....	2-27
PCI DSS .....	1-17, 1-23
Breach .....	1-24
Report of Compliance (ROC) .....	1-21
PCI Report of Compliance (ROC) .....	1-21
Penetration Testing (Security Assurance) .....	1-21
Perimeter (IAM context) .....	1-37
Permissions (IAM context) .....	1-37
Personally Identifiable Information (PII) .....	2-18
Phishing .....	1-54
Pillars (AWS Well-Architected) .....	1-16
Playbooks	
Demo (Incident Response) .....	2-55-59
Incident Response .....	2-53
Principle of Least Privilege .....	1-50

# SEC480 – AWS Secure Builder

RBAC (Role-Based Access Control)	1–50
Principle of Least Privilege (DLP context)	2–26
Principle of Least Privilege (IAM)	1–38
Privacy	
Implications	2–18
Personally Identifiable Information (PII)	2–18
PHI (Protected Health Information)	2–27
PII (Personally Identifiable Information)	2–27
Privilege Escalation	
Workloads	2–30
Process	
Threat Modeling	2–37
Process of shifting from On-premises to Cloud	1–15

## R

RBAC (Role-Based Access Control)	1–50
RDP (Remote Desktop Protocol)	
Exposure	2–29
RDS	
Amazon Aurora	1–89
MySQL	1–89
Oracle Database	1–89
PostgreSQL	1–89
Real World: Attacks in the Wild	2–35
Recovery Mechanisms	
Automation	2–54
Reducing Sensitive Data Leakage	2–26
Data Loss Prevention (DLP)	2–26
Encryption	2–26
Principle of Least Privilege	2–26
Security Awareness Training	2–26
Reference Architecture	1–16, 1–25
Regular IAM Audits	1–38
Regular Security Audits	1–55
Regulations (Security Assurance)	1–21
Release Automation: Pipeline Workflow	1–62
Repository (CI/CD)	1–62
Repository (VCS context)	1–67
Responsibility	
Cloud	1–14
Control	1–13
Delineation	1–18
for Security	1–10
of Security	1–10
On-prem	1–14
to Security	1–10
RESTful APIs (API Gateway)	1–86
Revoke Access Keys (CIRT context)	1–44
Risk	
End-User	2–87
Risk Factors	
Complexity	1–99
Risk Management	
Attack Surface	2–22
Attack Surface (Internal and External)	2–31
Exposure	2–23
Information Leakage	2–24

Security Maturity Assessments	1–104
Vulnerabilities and Attacks	2–34
Vulnerability Management	1–81
Risk Management (NIST context)	1–43
Risk of Exposure	2–23
Risk-Based Approach (NIST CSF)	2–39
Risk-Based Authentication	1–51
Roadmap (CIS context)	1–32
Roles (IAM context)	1–37
Rotate Credentials (CIRT context)	1–44
Runbooks (Systems Manager)	2–17
Runtime Application Self-Protection (RASP)	1–73
Runtime Protection	2–89
Content Security Policy (CSP)	2–89
Subresource Integrity (SRI)	2–89

## S

S3 Buckets (misconfiguration)	1–31
Safeguard (CIS context)	1–32
SAP Ariba (Vendor Management)	2–75
SAST (Static Application Security Testing)	1–29, 2–41, 1–77
SAST Tools	
AWS CodeGuru	1–78–79
Checkmarx	1–78–79
SonarQube	1–78–79
SCA Tools	
AWS CodeBuild	1–78–79
OWASP Dependency-Check	1–78–79
Snyk	1–78–79
Scan for Vulnerabilities (CI/CD Build)	1–68
Scripts (Indicators of Attack)	2–65
SDLC	
DAST	1–29
Education	1–29
Integrating Security	1–29
SAST	1–29
Secure Coding Standards and Guidelines	1–29
Security Awareness Training	1–29
Shift Left	1–29
Threat Modeling	1–29
SecDevOps	1–27
Secrets	
API Keys	1–71–72
AWS Parameter Store	1–71–72
AWS Secrets Manager	1–71–72
CI/CD Pipelines	1–71–72
Database Credentials	1–71–72
Encryption Keys	1–71–72
Environmental Variables	1–71–72
Secure Coding Standards and Guidelines	1–29
Secure Password Storage	1–55
Security & Compliance	
Adherence to requirements	1–19
Desired outcomes	1–19
GDPR	1–20
HIPAA	1–20

## SEC480 – AWS Secure Builder

Point in time assessment .....	1-19
Proactive .....	1-19
Reactive .....	1-19
Risk Mitigation .....	1-20
Security & Compliance: What is the difference? .	1-19
Security & Compliance: Why do we need both? .	1-20
Security Analyst (Incident Response) .....	2-52
Security and Compliance	
AWS API Gateway .....	1-91
AWS EC2 .....	1-91
AWS RDS .....	1-91
AWS S3 .....	1-91
Security Architecture	
Best Practices .....	1-16
Security Assurance .....	1-21
Security Awareness Training .....	1-29
Security Awareness Training (DLP context) .....	2-26
Security configurations .....	1-13
Security Events (CIRT context) .....	1-44
Security Fatigue .....	1-39
Security Frameworks and Standards .....	1-23
Security Groups .....	1-47
Network Security Controls .....	1-47
Security Groups (Firewall)	
EC2 .....	1-88
Security in the Cloud	
Security Architecture .....	1-16
Security Incident Response Team (SIRT) .....	2-43
Security Logging and Monitoring Failures ....	2-14-15
Security Maturity Assessments .....	1-104
NIST Cybersecurity Framework (CSF) ....	1-104
Security Misconfiguration .....	1-31
S3 Buckets .....	1-31
Security Model	
Network-based .....	1-42
Zero-Trust .....	1-42
Security-Relevant Data .....	2-13
Server-Side Request Forgery (SSRF) .....	2-32-33
Service Accounts .....	1-46
Service Hardening .....	1-93
AWS EC2 .....	1-93
AWS S3 .....	1-93
IAM .....	1-93
Network Security .....	1-93
Service Level Agreements (SLAs) .....	2-72-73
Services	
Identity .....	1-48
Public Exposure .....	2-29
Session Management	
Vulnerabilities .....	1-53
Session Management (Mitigation) .....	1-55
Sessions	
Hijacking .....	1-54
Shared Responsibility Model .....	1-11
AWS Responsibilities .....	1-11
Compliance .....	1-17
Compliance perspective .....	1-17
Customer Responsibilities .....	1-11
Security in the Cloud .....	1-12
Security of the Cloud .....	1-12
Shared Responsibility Model (overview) .....	1-18
Shift Left (Security in SDLC) .....	1-29
SIEM	
Definition .....	2-60
SIEM (Security Information and Event Management)	
2-7	
SOAR (Security Orchestration, Automation, and Re-	
sponse)	
Definition .....	2-61
SOC (System and Organization Controls) .....	1-21
Social Engineering .....	1-54
Phishing .....	1-54
Software	
Integrity Failures .....	2-86
Software and Data Integrity Failures .....	2-86
Software Composition Analysis (SCA) .....	2-88-89
Software Delivery Process .....	1-64
Compile Executable .....	1-64
Deployment .....	1-64
Solutions to Address Weaknesses .....	1-55
Culture .....	1-55
Mitigation Strategies .....	1-55
Variables .....	1-55
Source Code Analysis .....	1-77
Splunk (SIEM) .....	2-60
SSO (Single Sign-On) .....	1-39, 1-45
SSRF	
Attack .....	2-35
SSRF (Server-Side Request Forgery) ....	1-30, 2-32-33
Stages (DPRA) .....	1-63
Standards .....	1-23
Standards (Security Assurance) .....	1-21
Storage	
Object Storage (S3) .....	1-87
Strong Password Policies .....	1-55
Subresource Integrity (SRI) .....	2-89
Example .....	2-90
Supply-Chain (Attack Surface) .....	2-22
System Owners (Security Context) .....	1-105

T

Tabletop Exercise .....	2-43
Tabletop Exercises (Incident Response) .....	2-62
Technical Controls	
Network Segmentation .....	2-54
Technical Lead (Incident Response) .....	2-52
Technical settings .....	1-13
Test (DevOps context) .....	1-27
Third-Party Risk Assessments .....	1-21
Threat Hunting .....	2-13
Threat Intelligence Platforms (TIP)	
Definition .....	2-61
Threat Modeling .....	1-29, 2-36-37
Process .....	2-37

T

Tabletop Exercise .....	2-43
Tabletop Exercises (Incident Response) .....	2-62
Technical Controls	
Network Segmentation .....	2-54
Technical Lead (Incident Response) .....	2-52
Technical settings .....	1-13
Test (DevOps context) .....	1-27
Third-Party Risk Assessments .....	1-21
Threat Hunting .....	2-13
Threat Intelligence Platforms (TIP)	
Definition .....	2-61
Threat Modeling .....	1-29, 2-36-37
Process .....	2-37
Tool resistance (TL) .....	1-14

# SEC480 – AWS Secure Builder

## Tools

AWS CloudWatch .....	1-78-79
AWS Security Hub .....	1-78-79
Cloud Security Posture Management (CSPM) ..	2-41
Container Security	
Amazon Inspector .....	1-78-79
Aqua Security .....	1-78-79
EC2 Instances .....	1-78-79
Trivy .....	1-78-79
DAST (Dynamic Application Security Testing)	2-41
Dynamic Application Security Testing (DAST)	
Burp Suite .....	1-78-79
OWASP ZAP .....	1-78-79
EDR .....	2-61
Endpoint Detection and Response (EDR) ...	2-41
Infrastructure as Code (IaC) .....	2-41
Infrastructure as Code (IaC) Scanning	
AWS Config Rules .....	1-78-79
Checkov .....	1-78-79
TFLint .....	1-78-79
Network Traffic Analysis (NTA) .....	2-61
OSINT	
AWS Tools .....	2-28
Espial .....	2-27
Shodan .....	2-27
SpiderFoot .....	2-27
SAST (Static Application Security Testing) ..	2-41
SIEM	
IBM QRadar .....	2-60
Splunk .....	2-60
SOAR (Security Orchestration, Automation, and Response) .....	2-61
Software Composition Analysis (SCA) ....	2-88-89
AWS CodeBuild .....	1-78-79
OWASP Dependency-Check .....	1-78-79
Snyk .....	1-78-79
Static Application Security Testing (SAST)	
AWS CodeGuru .....	1-78-79
Checkmarx .....	1-78-79
SonarQube .....	1-78-79
Threat Intelligence Platforms (TIP) .....	2-61
Zscaler for Zero Trust Network Access (ZTNA)	2-41
Tools (Security)	
Essential Security Tools .....	1-78-79
Tools Demo .....	2-41
Transition (On-prem to Cloud) .....	1-15
Tripwires (Canary Tokens) .....	2-66
Trust, Control, and Supply Chain	
Breach Notifications .....	2-70
Contract Details .....	2-69
Due Diligence .....	2-71
Vendor Onboarding .....	2-72-73
Vendor Onboarding Policy and Process ....	2-74
Two-Factor Authentication (2FA) .....	1-41, 1-51
Typical AWS Sign-in Process .....	1-40

## U

Unauthorized Access .....	1-26
Unusual API Calls .....	1-26
User Education (Mitigation) .....	1-55
Username Harvesting .....	1-54
Example (Vulnerability) .....	1-56
Users (IAM context) .....	1-37
Users/Employees (Variables) .....	1-55

## V

Variables	
Clients/Customers .....	1-55
Users/Employees .....	1-55
Variables (Mitigation context) .....	1-55
VCS	
AWS CodeCommit .....	1-67
Definition .....	1-67
How it Works	
Branching .....	1-67
Commit .....	1-67
Merging .....	1-67
Repository .....	1-67
Understanding .....	1-67
Vendor Vetting (Defenses) .....	2-88-89
Vendors	
Frameworks	
NIST Cybersecurity Framework (CSF) ....	2-75
Shared Assessments SIG Questionnaire ...	2-75
Vendor Management Systems (VMS) ....	2-75
Vendor Risk Management Maturity Model (VR- MMM) .....	2-75
Onboarding .....	2-72-73
Policy and Process .....	2-74
Service Level Agreements (SLAs) .....	2-72-73
Vetting .....	2-88-89
Verification of Controls .....	1-21
Version Control Systems (VCS) .....	1-67
Virtual Machines (EC2) .....	1-88
Vulnerabilities	
Misconfigurations .....	2-34
SSRF (Server-Side Request Forgery) ....	2-32-33
Weak Credentials .....	2-34
Vulnerabilities and Attacks .....	2-34
Vulnerability and Patch Management .....	1-33
Vulnerability Management .....	1-81

## W

WAF	
Real World Attack .....	2-35
Web Bugs (Indicators of Attack) .....	2-64
Web Security	
CSP .....	1-13
HSTS .....	1-13
HTTP security headers .....	1-13
TLS certificate renewal .....	1-13

# SEC480 – AWS Secure Builder

---

WebSocket APIs (API Gateway) .....	1–86
Why do we Care & Why is it Important .....	1–18
Workforce Identity Management .....	1–45
Workloads	
Deployed .....	2–30
OSINT .....	2–30
Privilege Escalation .....	2–30

## Z

Zero Trust	
Zscaler (ZTNA) .....	2–41
Zero-Trust Security Model .....	1–42
Never trust, always verify .....	1–42
Zoom (Lessons Learned) .....	1–103
Zscaler for Zero Trust Network Access (ZTNA) ..	2–41