Securing Cloud Applications & Users

Module 5

241

Module Content

Content in this module comes from the following domains in CSA's Security Guidance:

- Domain 10 // Application Security
- Domain 12 // Identity Entitlement and Access Management
- Domain 14 // Related Technologies

Covers the following subject areas:

- SSDLC
- Immutable
- DevOps
- IAM

242

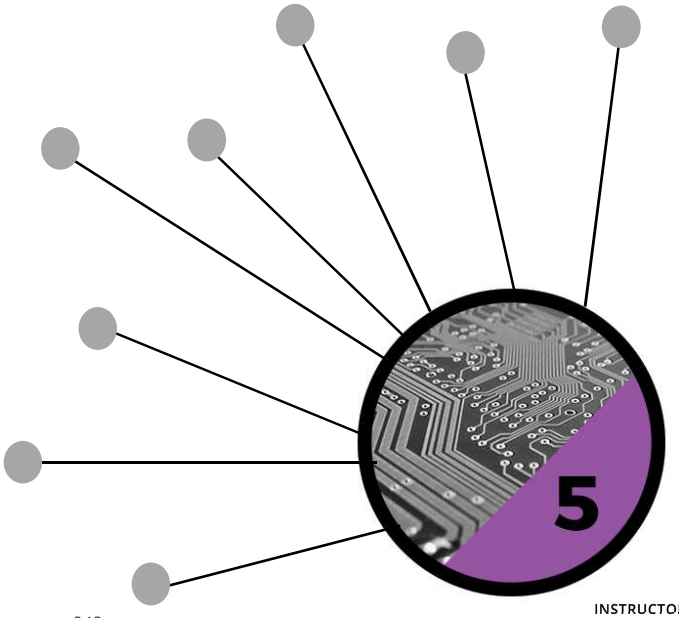
INSTRUCTOR LOGO HERE
Change img on all slide masters.

242

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Module Structure

Unit 1 // Module Intro
Unit 2 // SSDLC
Unit 3 // Testing and Assessment
Unit 4 // DevOps and Immutable
Unit 5 // Secure Operations and Architecture
Unit 6 // IAM definitions
Unit 7 // IAM Standards
Unit 8 // IAM in practice



cloud security alliance®

243

INSTRUCTOR LOGO HERE
Change img on all slide masters.

243

Objectives

Discover how application security differs in cloud computing.

Review secure software development basics and how those change in the cloud.

Leverage cloud capabilities for more secure cloud applications.

cloud security alliance®

244

INSTRUCTOR LOGO HERE
Change img on all slide masters.

244

Copyright 2019 Cloud Security Alliance and Securosis, LLC

How Cloud Changes AppSec

Opportunities

- Higher baseline security
- Responsiveness / agility
- Isolated environments
- Independent VMs for microservices
- Elasticity
- DevOps
- Unified interface

Challenges

- Limited visibility
- Increased application scope
- Changing threat models
- Reduced transparency

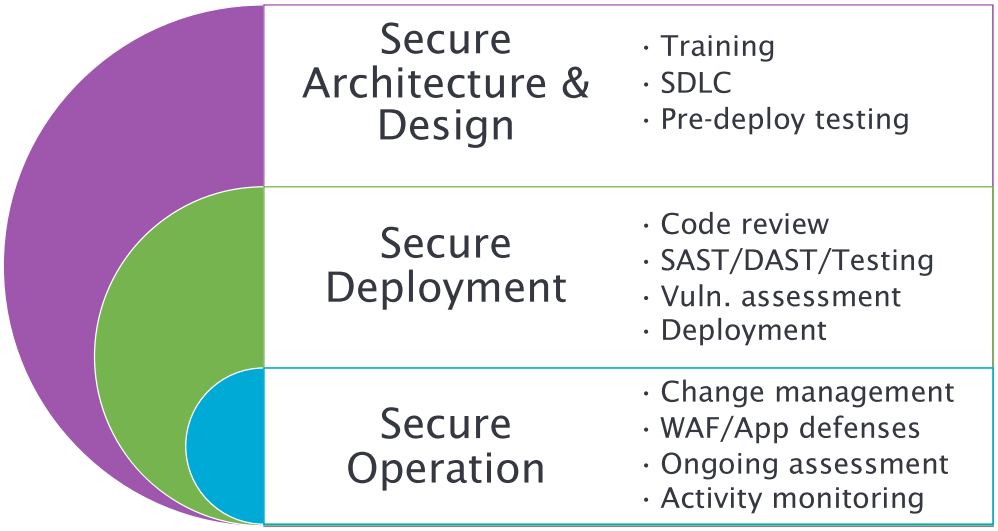
CSA cloud security alliance®

245

INSTRUCTOR LOGO HERE
Change img on all slide masters.

245

Application Security Phases



CSA cloud security alliance®

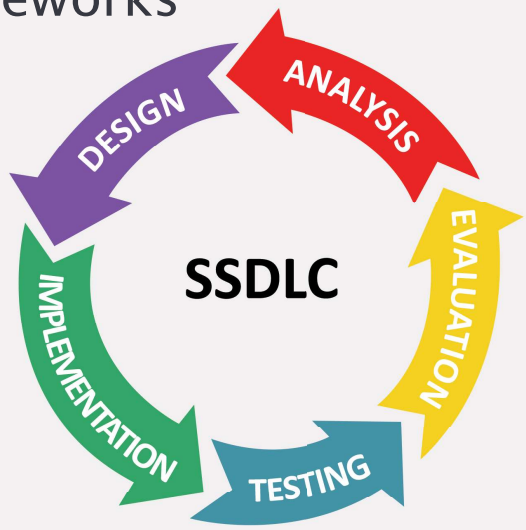
246

INSTRUCTOR LOGO HERE
Change img on all slide masters.

246

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SSDLC Frameworks & Guidance



cloud security alliance®

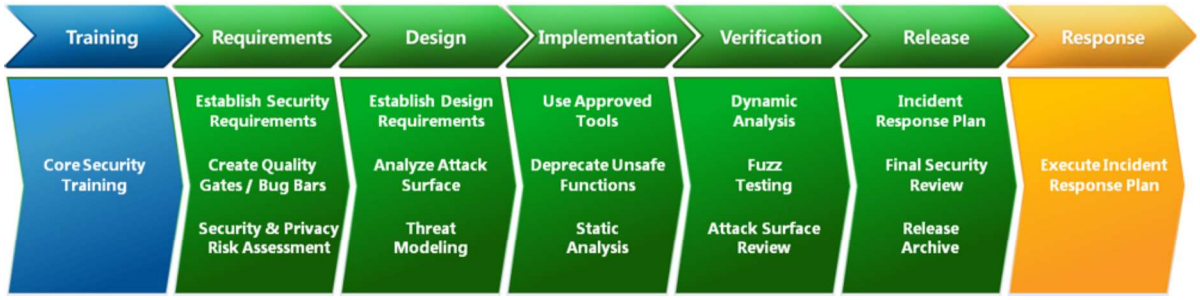
247

INSTRUCTOR LOGO HERE
Change img on all slide masters.

247

SSDLC Frameworks & Guidance

Microsoft's Security Development Lifecycle



cloud security alliance®

248

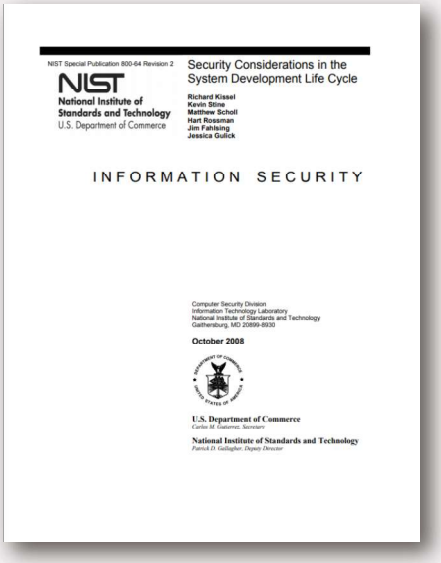
INSTRUCTOR LOGO HERE
Change img on all slide masters.

248

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SSDLC Frameworks & Guidance

NIST 800-64


NIST Special Publication 800-64 Revision 2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Security Considerations in the System Development Life Cycle

Richard Kissel
Kevin Stine
Matthew Scholl
Hart Rossman
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

cloud security alliance®

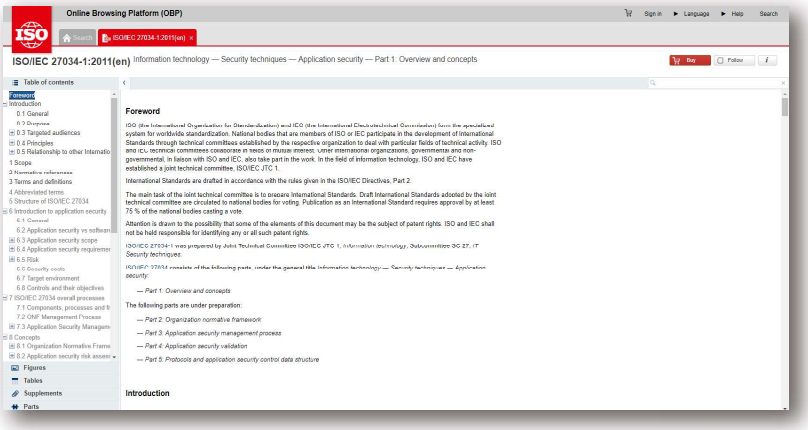
249

INSTRUCTOR LOGO HERE
Change img on all slide masters.

249

SSDLC Frameworks & Guidance

ISO/IEC 27034



cloud security alliance®

250

INSTRUCTOR LOGO HERE
Change img on all slide masters.

250

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SSDLC Frameworks & Guidance

- Other organizations, including OWASP and a variety of application security vendors, also publish their own lifecycle and security activities guidance.

CSA cloud security alliance®

251

INSTRUCTOR LOGO HERE
Change img on all slide masters.

251

Cloud Impact On SSDLC

- More reliance on cloud provider under shared responsibilities model
- Large changes to visibility and control
- Highly variable differences between providers and platforms
- Management plane/metastructure now within scope of application security
- New architectural options, especially with PaaS
- DevOps // Not cloud-specific, but highly correlated

CSA cloud security alliance®

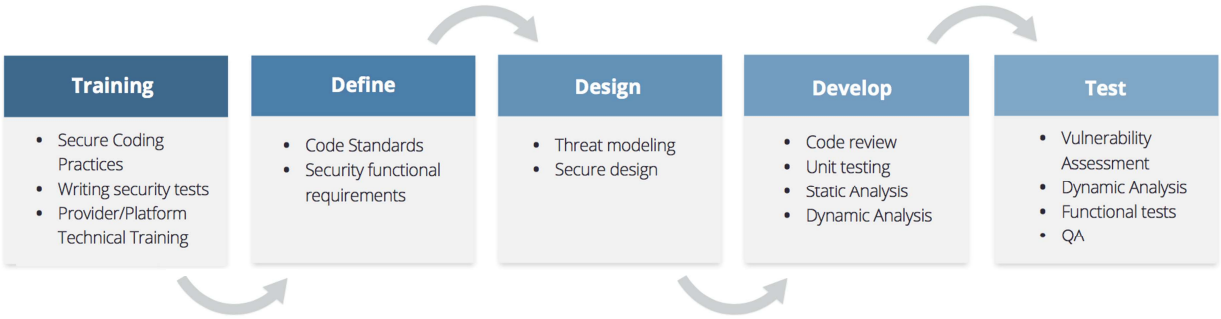
252

INSTRUCTOR LOGO HERE
Change img on all slide masters.

252

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Secure Design & Development



cloud security alliance

253

INSTRUCTOR LOGO HERE
Change img on all slide masters.

253

Threat Modeling Example

THREAT	DESCRIPTION	EXAMPLE
Spoofing	Assume identity of client, server or request/response	Phishing attack to fool user into sending credentials to fake site
Tampering	Alter contents of request of response	Message or data integrity compromised to change parameters or values
Repudiation	Dispute legitimate transaction	Illegitimately claiming a transaction was not completed
Information Disclosure	Unauthorized release of data	Unencrypted message sniffed off the network
Denial of Service	Service not available to authorized users	System flooded by requests until web server fails
Elevation of Privilege	Bypass authorization system	Attacker changes group membership

cloud security alliance

254

INSTRUCTOR LOGO HERE
Change img on all slide masters.

254

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Example Mapping Threat Model To Countermeasures

THREAT	SECURITY SERVICE
Spoofing	Authentication
Tampering	Digital signature, Hash
Repudiation	Audit logging
Information Disclosure	Encryption
Denial of Service	Availability
Elevation of Privilege	Authorization

CSA cloud security alliance®

255

INSTRUCTOR LOGO HERE
Change img on all slide masters.

255

Review

1. The secure software development lifecycle (SSDLC) is a structured process for ensuring security needs are met throughout application development processes.
2. There are multiple frameworks, such as those from Microsoft and OWASP.
3. Cloud will impact each phase of the lifecycle, from training all the way into operations. Changes in visibility and more reliance on the shared responsibilities model are constant threads.
4. When modeling application threats for cloud deployments, some risk will be greater and some less. Threat modeling is a great way to evaluate these differences.

CSA cloud security alliance®

256

INSTRUCTOR LOGO HERE
Change img on all slide masters.

256

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SSDLC Testing & Assessment

Module 5 // Unit 3

257

Note: Testing is not isolated to secure development or secure deployment, these phases overlap and there aren't walls between them.

We merely break them out as a way to structure the discussion

CSA cloud security alliance®

258

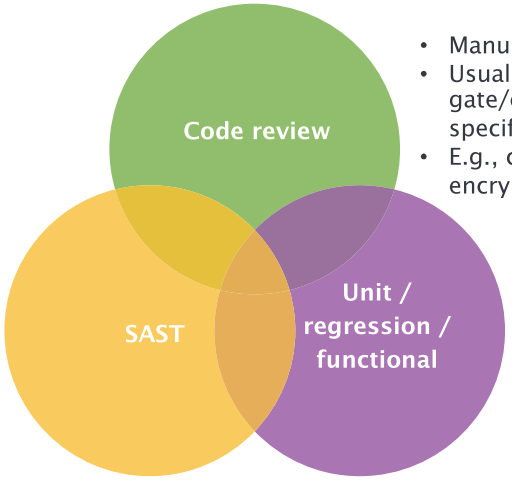
INSTRUCTOR LOGO HERE
Change img on all slide masters.

258

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Secure Development & Testing

- Cloud doesn't change the kind of testing, but does change some of what is tested
- E.g., need to account for cloud API calls, environment, PaaS integration



- Manual
- Usually implemented at gate/checkpoint for only specific functionality
- E.g., cloud auth and encryption

- Static Application Security Testing
- Add checks for cloud credentials and API calls

cloud security alliance®

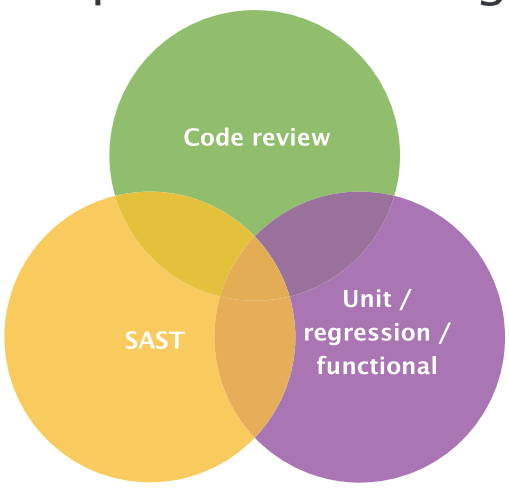
259

INSTRUCTOR LOGO HERE
Change img on all slide masters.

259

Secure Development & Testing

- In IaaS, you have substantial restrictions to test the cloud infrastructure, but you are free to test the app, database, etc. In PaaS you are free to test your app code and all the rest is restricted. In SaaS you would need to rely on 3rd-party testing done on behalf of the providers
- In IaaS you are generally free to test without permission at the app level, but not in PaaS/SaaS



- Standards of dev testing
- Should be used to test for security capabilities / functions

cloud security alliance®

260

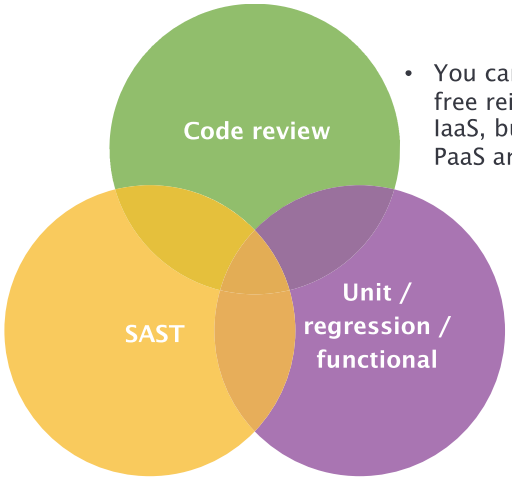
INSTRUCTOR LOGO HERE
Change img on all slide masters.

260

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Secure Deployment & Testing

- Use tools and companies with cloud-specific features and experience; tools and background don't translate from traditional to cloud as well in these areas



- You can expect mostly free reign to fuzz in IaaS, but not same level PaaS and SaaS

- Often requires close coordination with Cloud provider (depending on scope)

cloud security alliance®

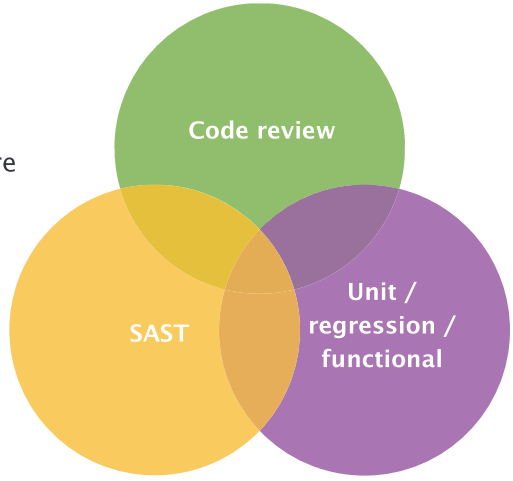
261

INSTRUCTOR LOGO HERE
Change img on all slide masters.

261

Secure Deployment & Testing

- Include developers and cloud admins within scope of penetration tests since they are often the weak link
- For multitenant apps, allow pen testers authorized access to try and break isolation



- Must define what level in the stack the scan targets
- External scans may require cloud provider permission

cloud security alliance®

262

INSTRUCTOR LOGO HERE
Change img on all slide masters.

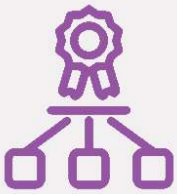
262

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Vulnerability Assessment In The Cloud

Test Images In The Pipeline

Use A Host-based Agent



Traditional Network Assessment (With Permission)

cloud security alliance®

263

INSTRUCTOR LOGO HERE
Change img on all slide masters.

263

Review

1. Secure software development involves a range of security testing. All of these are impacted by cloud computing.
2. With static analysis you should place a greater emphasis on looking for stored cloud credentials, as well as the proper configuration of API usage.
3. Dynamic analysis and vulnerability assessment may require permission from your cloud provider.
4. New vulnerability analysis options, such as scanning in a deployment pipeline or using host-based agents, are often better used for cloud.
5. Assessing the configuration of the cloud environment should now be within scope for an application security assessment.

cloud security alliance®

264

INSTRUCTOR LOGO HERE
Change img on all slide masters.

264

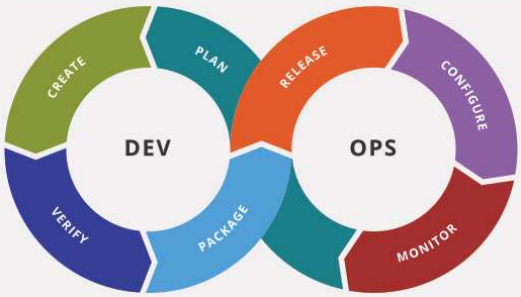
Copyright 2019 Cloud Security Alliance and Securosis, LLC

265

DevOps

Security Benefits:

- Greater standardization
- Automated testing
- Improved auditing
- Leverage automation techniques to improve security operations



No single definition, but typically refers to changing culture and process around continuous integration / delivery and automation.

CSA cloud security alliance®

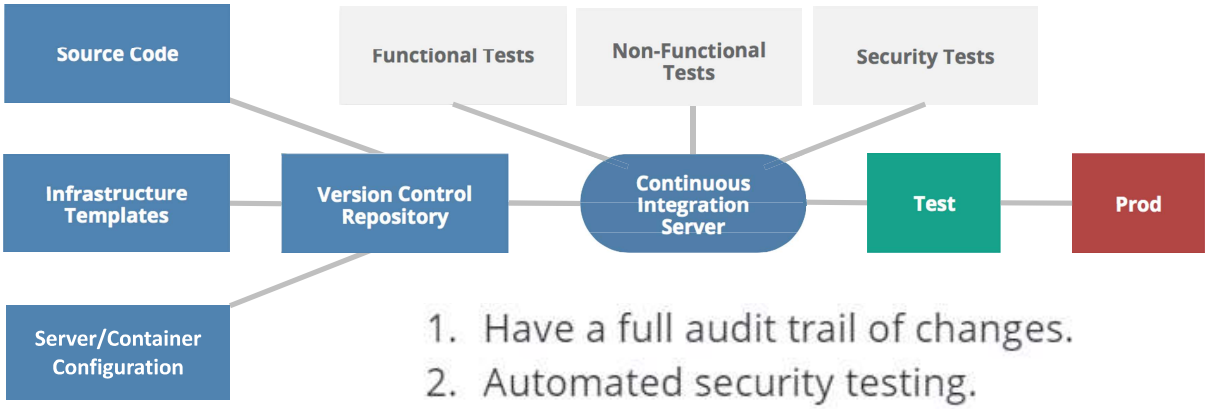
266

INSTRUCTOR LOGO HERE
Change img on all slide masters.

266

Copyright 2019 Cloud Security Alliance and Securosis, LLC

DevOps & Continuous Integration



1. Have a full audit trail of changes.
2. Automated security testing.

CSA cloud security alliance®

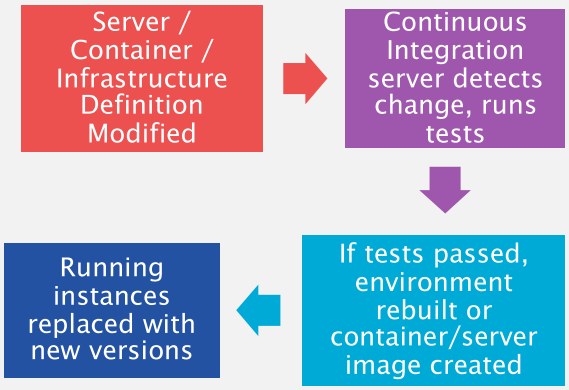
267

INSTRUCTOR LOGO HERE
Change img on all slide masters.

267

Immutable & Infrastructure As Code

- Infrastructure stack, virtual machines (instances), and containers all defined in templates in version control
- Environments and servers/containers rebuilt based on updated configurations
- Changes never made manually in production since the next approved change would overwrite
- Entire environment fully consistent, easy to rebuild / roll-back
- Can remove ability to log into production E.g., disable SSH on instances
- Massive security benefits- consistency, control, auditability



CSA cloud security alliance®

268

INSTRUCTOR LOGO HERE
Change img on all slide masters.

268

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. There are many definitions of DevOps, but a key defining characteristic is the use of continuous integration and/or continuous delivery (CI/CD).
2. Continuous integration pipelines support consistency and integrated security testing.
3. DevOps also supports immutable deployments, where instead of updating things or making manual changes we replaced them from a known good definition.
4. This supports security through consistency and allowing us to even remove the need to log into production assets.
5. There is a lot more to DevOps, but integrated security testing, consistency due to use of CI/CD, and immutable are some of the key security benefits.

cloud security alliance

269

INSTRUCTOR LOGO HERE
Change img on all slide masters.

269

270

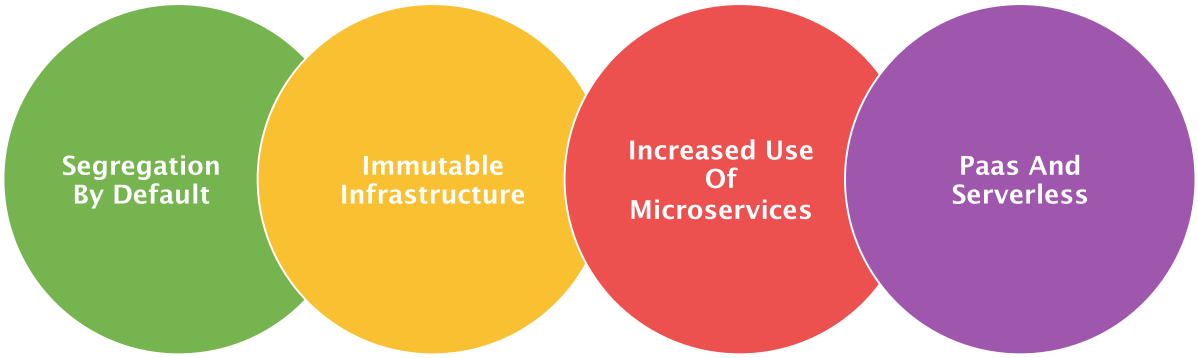
Copyright 2019 Cloud Security Alliance and Securosis, LLC

Secure Operations

- Lock down the management plane very tightly for production
- Actively monitor for changes at both cloud and app stack levels
- Don't neglect ongoing testing
- Cloud configuration is now within scope of change management
- WAF: Must auto scale, be embedded in the workload, or be cloud-hosted (filter traffic before it hits your application)
- RASP (Realtime Application Security Protection) an emerging option
  - RASP, one variant resembles a WAF inside the application

271

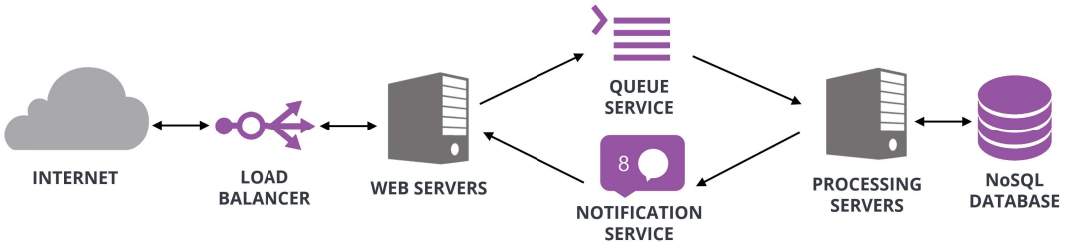
How Cloud Impacts Application Design & Architecture



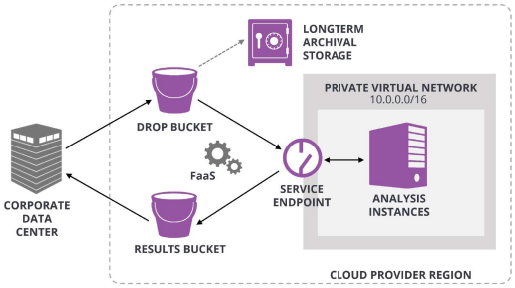
272

Copyright 2019 Cloud Security Alliance and Securosis, LLC

PAAS/Serverless & Security



- Provider takes on more security responsibilities
- Communicating via API on provider's platform reduces network attack paths
- Enables *software defined security* (security automated with APIs and code)
- May enable *event-driven security* (events in the cloud trigger execution of security code)



CSA cloud security alliance®

273

INSTRUCTOR LOGO HERE
Change Ing on all slide masters.

273

Application Security Recommendations

- Understand the security capabilities of your cloud providers. Not merely their baseline, but the various platforms and services.
- Build security into the initial design process. Cloud deployments are more often greenfield, creating new opportunities to engage security early.
- Even if you don't have a formal SDLC, consider moving to continuous deployment and automating security into the deployment pipeline.
- Threat modeling, SAST, and DAST (with fuzzing) should all be integrated. Testing should be configured to work in the cloud environment, but also to test for concerns specific to cloud platforms, such as stored API credentials.

CSA cloud security alliance®

274

INSTRUCTOR LOGO HERE
Change Ing on all slide masters.

274

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Application Security Recommendations

- Understand the new architectural options and requirements in the cloud. Update your security policies and standards to support them, and don't merely attempt to enforce existing standards on an entirely different computing model.
- Integrate security testing into the deployment process.
- Use software-defined security to automate security controls.
- Use event-driven security, when available, to automate detection and remediation of security issues.
- Use different cloud environments to better segregate management plane access and provide developers the freedom they need to configure development environments, while also locking down production environments.

CSA cloud security alliance®

275

INSTRUCTOR LOGO HERE
Change img on all slide masters.

275

Review

1. Secure operations is all about keeping your application secure once it is deployed into production.
2. When using cloud, the management plane is now a concern and the cloud configuration is now within scope for change management.
3. WAF will need to be adjusted to account for the different deployment options, like autoscaling, used in cloud.
4. New cloud architectural options, such as serverless and micro services may offer security benefits and are increasingly common.
5. Serverless puts more responsibility onto the cloud provider, leveraging the shared responsibilities model to reduce the customer's attack surface and scope of security operations.

CSA cloud security alliance®

276

INSTRUCTOR LOGO HERE
Change img on all slide masters.

276

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Identity & Access Management Definitions

Module 5 // Unit 6

277

Intro To CSA Identity Terms

ENTITY	• Discrete types that will have *Identity*; these are to Users, Devices, Code, Organizations and Agents
IDENTITY	• The unique expression of an entity within a given namespace.
IDENTIFIER	• The means by which an *Identity* can asserted, usually using crypto tokens for digital identities
ATTRIBUTES	• Facets of an *identity* (e.g., org. unit or IP address)
PERSONA	• Expression of an *identity* with attributes that indicates context. E.g., a developer logged into a given project

CSA cloud security alliance®

278

INSTRUCTOR LOGO HERE
Change img on all slide masters.

278

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Intro To CSA Identity Terms (Cont'd)

AUTHORITAT SOURCE	ROLE	• Has multiple meanings. Typically used to indicate a persona or subset. E.g., "developer" vs. "admin"
AUTHENTICA	AUTHENTICATION	• The process of confirming an identity. *Authn*
MULTIFACTO AUTHENTICA	MULTIFACTOR AUTHENTICATION	• Use of multiple factors in authentication (e.g., username + password + *token*)
AUTHORIZAT	ACCESS CONTROL	• Restricting access to a resource, Access management is the corresponding process
ENTITLEMENT	AUTHORITATIVE SOURCE	• The "root" source for an identity, such as a directory server

ch as a

ty.

ation

on

cloud security alliance®

279

INSTRUCTOR LOGO HERE
Change img on all slide masters.

279

Intro To CSA Identity Terms (Cont'd)

ACCESS CO	AUTHORIZATION	• Allowing an identity access. *Authz*
FEDERATED MANAGEME	ENTITLEMENT	• Mapping an identity to an authorization
IDENTITY P	FEDERATED IDENTITY MANAGEMENT	• The process of asserting an identity across different systems
RELYING PA	IDENTITY PROVIDER	• The trusted source of the identity in federation
ROLE	RELYING PARTY	• The system that relies on an identity assertion from an identity provider

ss
cess

ross

d to

cloud security alliance®

280

INSTRUCTOR LOGO HERE
Change img on all slide masters.

280

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. It is important to understand the foundational terminology for identity and access management (IAM).
2. At the heart is an entity, which is a person, device, or other "thing" that will be given access.
3. An identity is the expression of that entity within a namespace, such as an email address or username for a given system.
4. Entities prove their identity by providing identifiers during authentication.
5. After being authenticated, users may be granted access to objects or actions. This is called an authorization, and an entitlement is a specific approval.
6. Federated identity is critical for cloud computing because it allows us to manage identities across different systems.

CSA cloud security alliance®

281

INSTRUCTOR LOGO HERE
Change img on all slide masters.

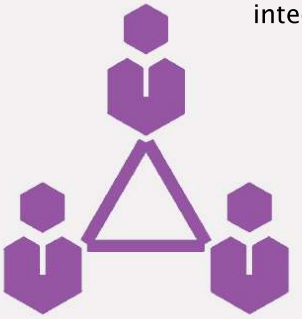
281

282

Copyright 2019 Cloud Security Alliance and Securosis, LLC

How IAM Is Different For Cloud

Management plane/metastructure integration



IAM now always spans organizational boundaries

Greater use of Federation to manage

CSA cloud security alliance®

283

INSTRUCTOR LOGO HERE
Change img on all slide masters.

283

IAM Standards For Cloud

Most Common			Less Common	
SAML	OAUTH	OPENID	XACML	SCIM

CSA cloud security alliance®

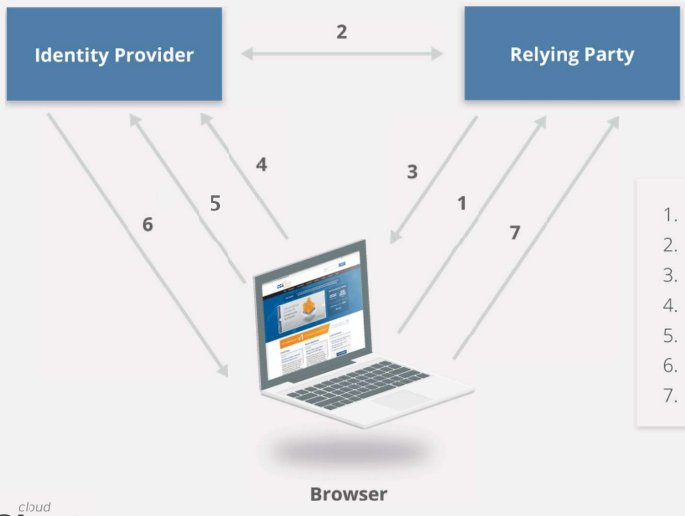
284

INSTRUCTOR LOGO HERE
Change img on all slide masters.

284

Copyright 2019 Cloud Security Alliance and Securosis, LLC

OPENID EXAMPLE



1. User sends their OpenID URL
2. IP and RP set shared secret
3. Browser redirected to get token from provider
4. Request to IP for token for site
5. Login if needed
6. Token returned to browser
7. Token handed to requesting site

CSA cloud security alliance®

285

INSTRUCTOR LOGO HERE
Change img on all slide masters.

285

Review

1. IAM for cloud computing relies on federated identity due to the requirement to manage authentication and authorization between the cloud consumer and the cloud provider.
2. The most widely supported and used federation standard for connecting enterprises with their cloud providers SAML.
3. Oauth and OpenID are web-centric federation standards often used by both consumers and organizations.
4. Federation involves multi-step cryptographically supported processes to connect an Identity Provider (the source for the identity) and the Relying Party (most often the cloud provider, where authorizations occur).
5. Typically the identity provider handles authentication, then the relying party handles authorization (enforcing what someone can actually do).

CSA cloud security alliance®

286

INSTRUCTOR LOGO HERE
Change img on all slide masters.

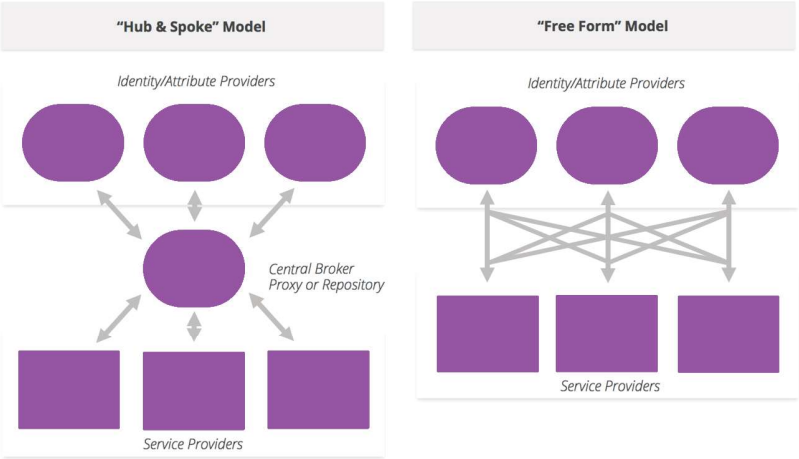
286

Copyright 2019 Cloud Security Alliance and Securosis, LLC

287

Managing Users & Identities For Cloud

- Cloud providers need to support internal identities and federation
- Cloud consumers need to determine where to manage identities and how to integrate with providers
- Generally, consumers should own the identity and federate to the provider (as much as possible)



CSA cloud security alliance®

288

INSTRUCTOR LOGO HERE
Change img on all slide masters.

288

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Additional Identity Decisions

- How to manage identities for systems/code/devices/services
  - Defining the identity provisioning process and how to integrate with cloud.
  - Often a good time to review and update your process
- Provisioning and supporting various cloud providers/platforms
  - Mapping attributes
  - Enabling monitoring/logging
  - Building entitlement matrices
  - Documenting break/fix for federation outages
  - IR for account takeovers and other IAM incidents
- Deprovisioning

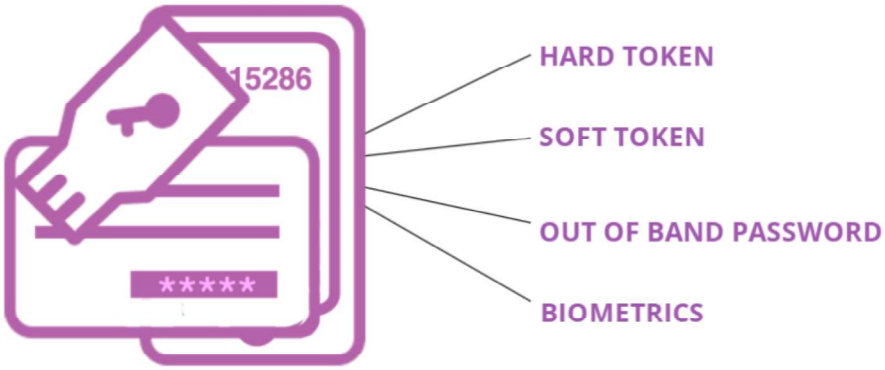
CSA cloud security alliance®

289

INSTRUCTOR LOGO HERE
Change img on all slide masters.

289

Authentication: MFA Is Mandatory



CSA cloud security alliance®

290

INSTRUCTOR LOGO HERE
Change img on all slide masters.

290

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Moving From RBAC To ABAC

RBAC
- Role Based Access Controls
- Very familiar
- Decisions based on assigned role in that context

ABAC
- Attribute Based Access Controls
- Decision based on more attributes than just role
- Far more granular and flexible
- Best model for cloud

CSA cloud security alliance®

291

INSTRUCTOR LOGO HERE
Change img on all slide masters.

291

Sample Cloud Entitlement Matrix

Entitlement	Super-Admin	Service-1 Admin	Service-2 Admin	Dev	Security-Audit	Security-Admin
Service 1 List	X	X		X	X	X
Service 2 List	X		X	X	X	X
Service 1 Modify Network	X	X		X		X
Service 2 Modify Security Rule	X	X				X
Read Audit Logs	X				X	X

CSA cloud security alliance®

292

INSTRUCTOR LOGO HERE
Change img on all slide masters.

292

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Identity Management Recommendations

- Organizations should develop a comprehensive and formalized plan and processes for managing identities and authorizations with cloud services.
- When connecting to external cloud providers, use federation, if possible, to extend existing identity management. Try to minimize silos of identities in cloud providers that are not tied to internal identities.
- Consider the use of identity brokers where appropriate.
- Cloud consumers are responsible for maintaining the identity provider and defining identities and attributes.
- These should be based on an authoritative source.
- Distributed organizations should consider using cloud-hosted directory servers when on-premises options either aren't available or do not meet requirements.

CSA cloud security alliance®

293

INSTRUCTOR LOGO HERE
Change img on all slide masters.

293

Identity Management Recommendations

- Cloud consumers should prefer MFA for all external cloud accounts and send MFA status as an attribute when using federated authentication.
- Privileged identities should always use MFA.
- Develop an entitlement matrix for each cloud provider and project, with an emphasis on access to the metastructure and/or management plane.
- Translate entitlement matrices into technical policies when supported by the cloud provider or platform.
- Prefer ABAC over RBAC for cloud computing.
- Cloud providers should offer both hosted identities and federation using open standards.
- There are no magic protocols: pick your use cases and constraints first and find the right protocol second.

CSA cloud security alliance®

294

INSTRUCTOR LOGO HERE
Change img on all slide masters.

294

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Due to the complexity of managing multiple directory servers and cloud providers, a hub and spoke model using a federated identity broker is often preferred.
2. Because of the broad network access supported by cloud providers, multi factor authentication is critical to help reduce the chances of account takeovers.
3. Many cloud providers are now supporting attribute based access controls, which support greater granularity in entitlements than traditional role-based access controls.
4. Building an entitlement matrix can help document authorizations for your cloud providers different services and help with assessments and audits.

cloud security alliance

295

INSTRUCTOR LOGO HERE
Change img on all slide masters.

295

296

Copyright 2019 Cloud Security Alliance and Securosis, LLC