297

Module Contents

Module 6 //

Cloud Security Operations

Maps to the following domains in the Security Guidance:

- **Domain 9 //** Incident Response
- **Domain 13 //** Security as a Service
- **Domain 14 //** Related Technologies

Covers the following subject areas:

- What to look for in a cloud provider
- Security as a Service
- Incident Response
- IoT
- Serverless
- Mobile
- Big Data

CSA cloud security alliance®

298

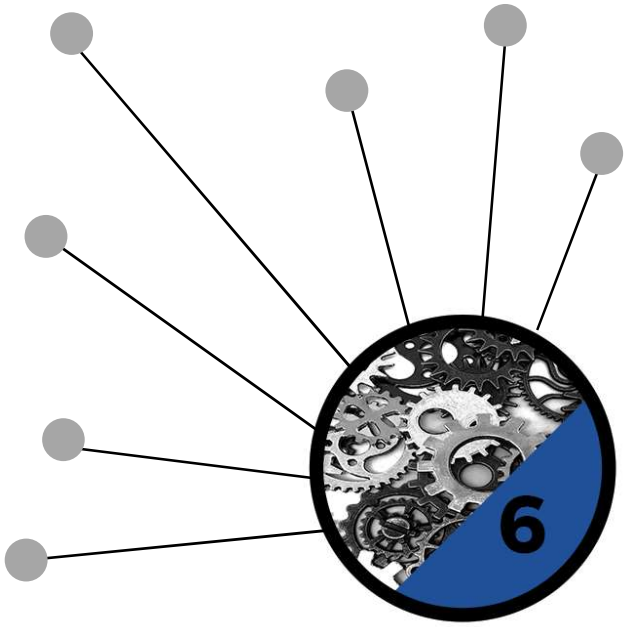
INSTRUCTOR LOGO HERE
Change img on all slide masters.

298

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Module Structure

- Unit 1 // Module Intro
- Unit 2 // Selecting A Cloud Provider
- Unit 3 // Incident Response
- Unit 4 // SECaaS Fundamentals
- Unit 5 // SECaaS Categories & Recommendations
- Unit 6 // Related Technologies
- Unit 7 // CCSK Exam Prep



cloud security alliance

299

INSTRUCTOR LOGO HERE
Change img on all slide masters.

299

Objectives

How to select cloud providers

The advantages & disadvantages of Security as a Service

The different major Security as a Service categories

How to respond to security incidents in the cloud

The security issues of technologies related to cloud computing: Big Data, mobile, serverless, IoT

Security as a Service (SECaaS) recommendations

cloud security alliance

300

INSTRUCTOR LOGO HERE
Change img on all slide masters.

300

Copyright 2019 Cloud Security Alliance and Securosis, LLC

301

302

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Or In Other Words…

What do you do?

What do I have to do?

cloud security alliance®

303

INSTRUCTOR LOGO HERE
Change img on all slide masters.

303

And…

Do you enable me to do what I need to do?

cloud security alliance®

304

INSTRUCTOR LOGO HERE
Change img on all slide masters.

304

Copyright 2019 Cloud Security Alliance and Securosis, LLC

THINGS TO LOOK FOR IN A CLOUD PROVIDER PART 1

- COMPARTMENTALIZATION OF JOB ROLES
- WELL-DEFINED SECURITY POLICIES
- REVIEWABLE AUDITS
- THE ABILITY TO INSPECT / AUDIT PROVIDER
- WELL-DEFINED CONTRACTUAL LANGUAGE (SECURITY / PRIVACY)
- WELL-DEFINED BC/DR POLICY / PROCESS

CSA cloud security alliance®

305

INSTRUCTOR LOGO HERE
Change img on all slide masters.

305

THINGS TO LOOK FOR IN A CLOUD PROVIDER PART 2

- CONFIGURATION MANAGEMENT PROCESS
- PATCH MANAGEMENT PROCESS
- ROBUST, WELL-DOCUMENTED API
- SECURITY IN THE DEVELOPMENT PROCESS
- SECURITY IN THE OPERATIONS PROCESS
- PRIORITIZATION OF SECURITY

CSA cloud security alliance®

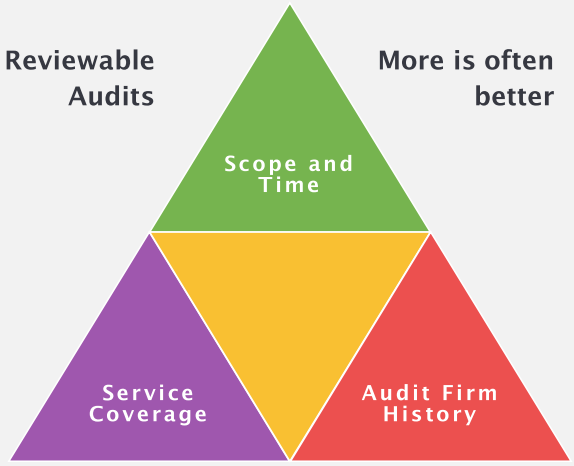
306

INSTRUCTOR LOGO HERE
Change img on all slide masters.

306

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Things To Look For In A Cloud Provider



307

307

IaaS (And Most PaaS) Provider Critical Security Capabilities

- API/admin activity logging
- Elasticity and autoscaling
- APIs for all security features
- Granular entitlements
- Good SAML support
- Multiple accounts per customer (or equivalent)
- Software Defined Networking
- Region/location control
- Infrastructure templating/automation

These are not directly stated in the Guidance

308

308

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SaaS Provider Critical Security Capabilities

- Robust external security and compliance assessments available for customers to review
- Granular IAM entitlements within the SaaS application
- SAML support
- Logging of administrator activity
- External log feeds or API access to logs
- Strong internal controls to limit admin access to customer data
  - These should be externally validated and clearly documented

These are not directly stated in the Guidance

CSA cloud security alliance®

309

INSTRUCTOR LOGO HERE
Change img on all slide masters.

309

CSA Tools To Help

CCM™

CAIQ™

CSA STAR

STAR WATCH
Assurance on Demand

AND MORE! https://cloudsecurityalliance.org/research/

CSA cloud security alliance®

310

INSTRUCTOR LOGO HERE
Change img on all slide masters.

310

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. The critical security capabilities for cloud providers are a list of features required in a cloud platform to fully enable customers to build a comprehensive cloud security program.
2. When evaluating cloud providers, consumers should also look at all available documentation, and pay particular attention to internal security controls that ensure a strong baseline level of security over time.
3. Individual security features are not as indicative as strong programmatic controls.
4. Cloud providers should also offer a wide array of reviewable third-party audits and assessments to validate their security program and control.
5. The Cloud Security Alliance provides the CAIQ. CCM, STAR, and STARWatch to help both cloud providers and consumers in communicating security posture.

cloud security alliance®

311

INSTRUCTOR LOGO HERE
Change img on all slide masters.

311

312

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Incidents Change

- Likelihood of some kinds of incidents goes up, others go down – it's a different environment
  - The metastructure is the biggest difference
- Consider attacks targeted at the Cloud Provider and how that affects your systems
- You and the provider will likely have different priorities
- Your processes will certainly change
  - Don't wait until the first incident to figure this all out

CSA cloud security alliance®

313

INSTRUCTOR LOGO HERE
Change img on all slide masters.

313

IR Lifecycle

CSA cloud security alliance®

314

INSTRUCTOR LOGO HERE
Change img on all slide masters.

314

Copyright 2019 Cloud Security Alliance and Securosis, LLC

PREPARATION | DETECTION & ANALYSIS | CONTAINMENT, ERADICATION, RECOVERY | POST-MORTEM

- Understand where data is and moves.
- Understand and clarify SLAs and contracts.
  - These become your primary communication and enforcement tool.
  - Look for things like:
    - Points of contact, communications channels.
    - Incident definition and notification criteria.
    - Testing, scoping, and roles and responsibilities.
- Build a cloud jump kit.
- Architect for faster detection, investigation, and remediation.
  - Immutable, infrastructure as code, isolation, instrumentation.
- Test the plan.
- Know who to call!

CSA cloud security alliance®

315

INSTRUCTOR LOGO HERE
Change img on all slide masters.

315

PREPARATION | DETECTION & ANALYSIS | CONTAINMENT, ERADICATION, RECOVERY | POST-MORTEM

- Detection depends on data availability.
  - Know your data sources- what the provider gives you, and what you collect yourself.
  - Pay particular attention to in-cloud monitoring and alerting capabilities.
- Analysis impacted by lack of transparency to provider's infrastructure.
- Data source issues:
  - What should be logged and what is logged?
  - Are logs consistent and complete?
  - Do logs reflect the dynamic nature of the cloud?
  - Do logs meet legal requirements, tamper resistance, and format requirements?
- Forensics likely limited to your virtual instances. Snapshots are useful.

CSA cloud security alliance®

316

INSTRUCTOR LOGO HERE
Change img on all slide masters.

316

Copyright 2019 Cloud Security Alliance and Securosis, LLC

PREPARATION | DETECTION & ANALYSIS | **CONTAINMENT, ERADICATION, RECOVERY** | POST-MORTEM

- The cloud provider's primary responsibility is to the entire customer base.
  - Containment may mean containing you. You will be sacrificed to maintain the stability of the service.
- You are responsible for your own containment, eradication, and recovery.
  - Start with the management plane/metastructure.
- Software defined infrastructure allows you to rebuild in a new area without having to immediately eradicate the active attack.

CSA cloud security alliance®

317

INSTRUCTOR LOGO HERE
Change img on all slide masters.

317

PREPARATION | DETECTION & ANALYSIS | CONTAINMENT, ERADICATION, RECOVERY | **POST-MORTEM**

- Mostly equivalent to how you handle for traditional infrastructure
- Pay particular attention to data sources, the metastructure/management plane response, and communications with the cloud provider.

CSA cloud security alliance®

318

INSTRUCTOR LOGO HERE
Change img on all slide masters.

318

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Incident Response Recommendations

- SLAs and setting expectations around what the customer does versus what the provider does are the most important aspect of incident response for cloud-based resources.
- Clear communication of roles/responsibilities and practicing the response and hand-offs are critical.
- Cloud customers must set up proper communication paths with the provider that can be utilized in the event of an incident. Existing open standards can facilitate incident communication.
- Cloud customers must understand the content and format of data that the cloud provider will supply for analysis purposes and evaluate whether the available forensics data satisfies legal chain of custody requirements.
- Cloud customers should also embrace continuous and serverless monitoring of cloud-based resources to detect potential issues earlier than in traditional data centers.
  - Data sources should be stored or copied into locations that maintain availability during incidents.
  - If needed and possible, they should also be handled to maintain a proper chain of custody.

cloud security alliance®

319

INSTRUCTOR LOGO HERE
Change img on all slide masters.

319

Incident Response Recommendations

- Cloud-based applications should leverage automation and orchestration to streamline and accelerate the response, including containment and recovery.
- For each cloud service provider used, the approach to detecting and handling incidents involving the resources hosted at that provider must be planned and described in the enterprise incident response plan.
- The SLA with each cloud service provider must guarantee support for the incident handling required for the effective execution of the enterprise incident response plan. This must cover each stage of the incident handling process: detection, analysis, containment, eradication, and recovery.
- Testing will be conducted at least annually or whenever there are significant changes to the application architecture. Customers should seek to integrate their testing procedures with that of their provider (and other partners) to the greatest extent possible.

cloud security alliance®

320

INSTRUCTOR LOGO HERE
Change img on all slide masters.

320

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. The fundamental nature of cloud changes the likelihood and nature of incidents. It is important to adjust your incident response process to account for these.
2. Cloud consumers and cloud providers will have different priorities in an incident. These may conflict when a provider needs to contain a consumer.
3. Focus on preparation, especially communications with cloud providers, adjusting IR plans, and building tool or "jump" kits to more-rapidly respond.
4. When available, infrastructure as code can allow isolation of a compromised environment while rebuilding a functional environment in parallel to reduce downtime.
5. But don't forget, this will carry over any active vulnerabilities and configuration errors in the templates.

cloud security alliance®

321

INSTRUCTOR LOGO HERE
Change img on all slide masters.

321

322

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Defining SECaaS

Security as a Service is defined as a security product or service, with cloud-based management. These services can secure systems and data in the cloud, in traditional on-premise networks, or hybridized environments.

CSA cloud security alliance®

323

INSTRUCTOR LOGO HERE
Change img on all slide masters.

323

SECaaS Characteristics

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

- Security products or services delivered as a cloud service
- Meets the NIST essential characteristics

CSA cloud security alliance®

324

INSTRUCTOR LOGO HERE
Change img on all slide masters.

324

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SECaaS Potential Benefits

- Cloud Computing Benefits
- Staffing And Expertise
- Intelligence Sharing
- Deployment Flexibility
- Insulation Of Clients
- Scaling And (Maybe) Costs

CSA cloud security alliance®

325

INSTRUCTOR LOGO HERE
Change img on all slide masters.

325

SECaas Potential Concerns

- Lack Of Visibility
- Regulation Differences
- Handling Of Regulated Data
- Data Leakage
- Changing Providers
- Migrating to SECaaS

CSA cloud security alliance®

326

INSTRUCTOR LOGO HERE
Change img on all slide masters.

326

Copyright 2019 Cloud Security Alliance and Securosis, LLC

ALWAYS KEEP IN MIND…

An organization cannot outsource accountability… Ever.

cloud security alliance®

327

INSTRUCTOR LOGO HERE
Change img on all slide masters.

327

Review

1. SECaaS looks from the other side to secure systems and data in the cloud as well as hybrid and traditional enterprise networks via cloud-based services. These systems may be in the cloud or more traditionally hosted within the customer's premises.
2. Security as a Service includes security products delivered as a cloud service, that also meet the NIST essential characteristics.
3. They offer the same benefits as the rest of cloud computing and may also offer benefits such as deeper expertise among their staff, as well as intelligence sharing across all the customers they protect.
4. Drawbacks can include regulatory differences, reduced visibility, and the potential for your data leaking through the provider.
5. The cloud consumer can never outsource their security accountability.

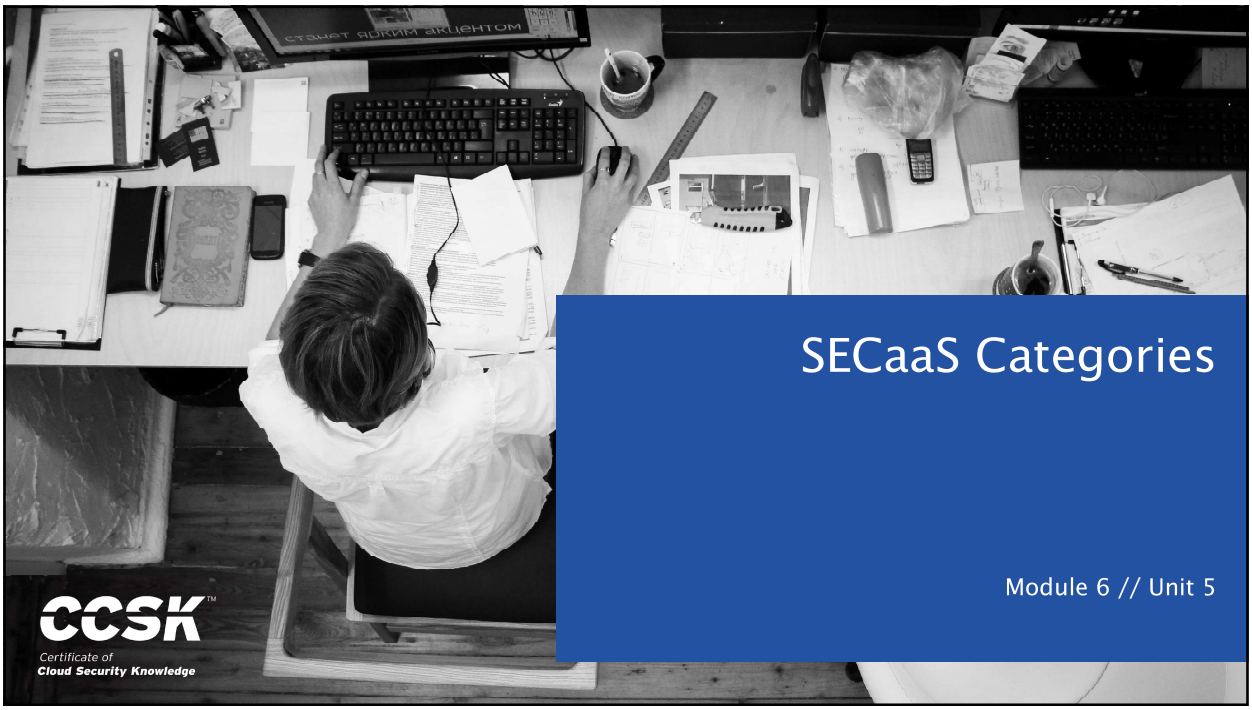
cloud security alliance®

328

INSTRUCTOR LOGO HERE
Change img on all slide masters.

328

Copyright 2019 Cloud Security Alliance and Securosis, LLC



SECaaS Categories

Module 6 // Unit 5

329

SECaaS // IAM Services

Identity, Entitlement And Access Management Services

- Federated Identity Brokers
- Strong Authentication
- Cloud-Based Directories
- Other emerging options

CSA cloud security alliance®

330

INSTRUCTOR LOGO HERE
Change img on all slide masters.

330

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SECaas // CASB

Cloud Access Security Brokers

- Discussed in the Data Security module
- Can be cloud-hosted
- Used to manage SaaS applications
- Poor name - the "access" was meant to refer to federated identity brokers but that market is separate

CSA cloud security alliance®

331

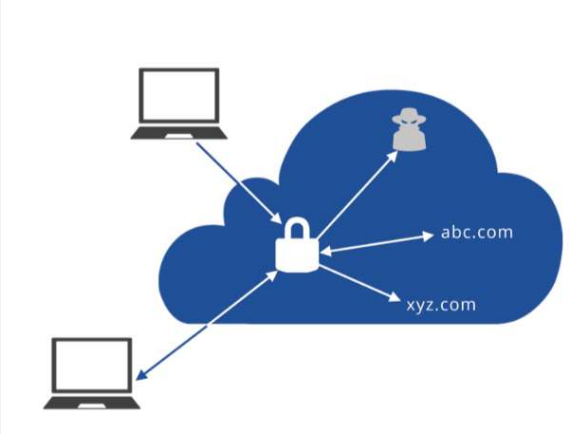
INSTRUCTOR LOGO HERE
Change img on all slide masters.

331

SECaas // Gateways

Web Security Gateways

- Web security delivered via the Cloud by proxying web traffic to the cloud provider.
- Policy rules for web access and allowed time frames also enforced.
- Protective, detective, and reactive technical control



CSA cloud security alliance®

332

INSTRUCTOR LOGO HERE
Change img on all slide masters.

332

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SECaas // Email

Email Security

- Filters inbound and outbound email to block spam, phishing, and malware.
- Protects users from email floods and provides business continuity.
- May include encryption.

CSA cloud security alliance®

333

INSTRUCTOR LOGO HERE
Change img on all slide masters.

333

SECaas // Assessment

Security Assessment

- Using cloud-based tools for assessment on either cloud services or on-premise resources.
- Main Types:
  - Traditional VA
  - Application Security
  - Cloud Platform Assessment

CSA cloud security alliance®

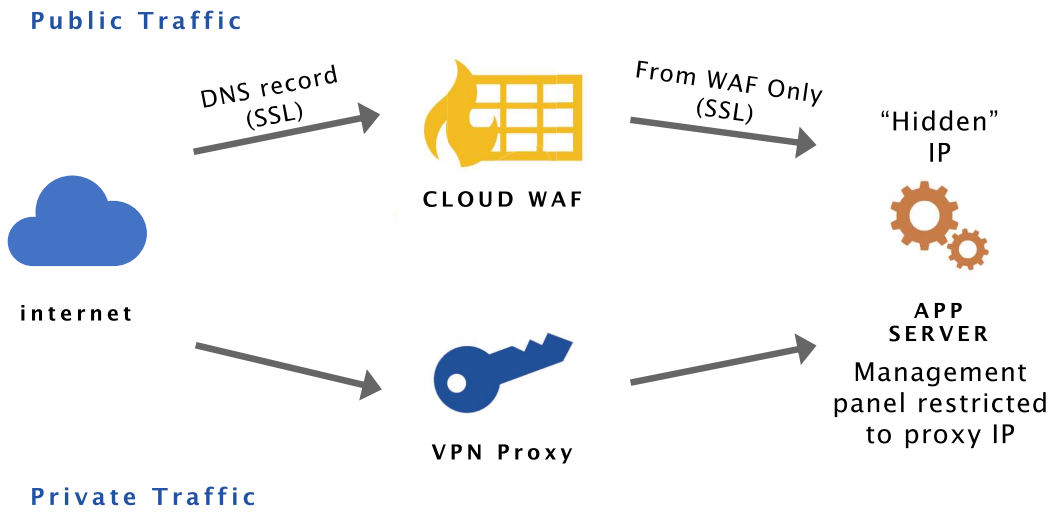
334

INSTRUCTOR LOGO HERE
Change img on all slide masters.

334

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Web Application Firewalls



CSA cloud security alliance®

335

INSTRUCTOR LOGO HERE
Change img on all slide masters.

335

SECaas // Encryption

Encryption & Key Management

- Cloud-based key management can protect cloud data and also on-premise data.
- Consistency with existing key management schemes is important.

CSA cloud security alliance®

336

INSTRUCTOR LOGO HERE
Change img on all slide masters.

336

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SECaas // SIEM

Security Information And Event Management (SIEM)

- Aggregate log and event data from virtual and real networks, applications, and systems.
- Correlate and provide alerts based on mutually agreed rule set.
- Ensure the hand-off between provider and internal ops group is clean.

CSA cloud security alliance®

337

INSTRUCTOR LOGO HERE
Change img on all slide masters.

337

SECaas // BC/DR

Business Continuity/ Disaster Recovery

- Involves using a cloud-service to back up internal controls.
- Requires synchronization and clear demarcation of accountability.

CSA cloud security alliance®

338

INSTRUCTOR LOGO HERE
Change img on all slide masters.

338

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SECaaS // Misc.

Additional Categories

- DDoS Protection
- Security Management
- Managed Network or Endpoint Security (e.g. IDS)

cloud security alliance®

339

INSTRUCTOR LOGO HERE
Change img on all slide masters.

339

SECaaS Recommendations

- Before engaging a SECaaS provider, be sure to understand any security-specific requirements for data-handling (and availability), investigative, and compliance support.
- Pay particular attention to handling of regulated data, like PII.
- Understand your data retention needs and select a provider that can support data feeds that don't create a lock-in situation.
- Ensure that the SECaaS service is compatible with your current and future plans, such as its supported cloud (and on-premises) platforms, the workstation and mobile operating systems it accommodates, and so on.

cloud security alliance®

340

INSTRUCTOR LOGO HERE
Change img on all slide masters.

340

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Security as a Service offerings include a wide range of categories that span most, if not all, major security domains.
2. The key is that the service meets the NIST essential characteristics, and this also includes hybrid offerings (e.g. the management is in the cloud with some on-premise components.
3. Common categories include everything from security assessment, to cloud-based defensive tools like WAF, email, and web filtering, to SIEM and logging.
4. When selecting a provider ensure you understand your data handling and compliance requirements and evaluate services that are compatible with your existing technology requirements, such as architectures and operating systems.

cloud security alliance®

341

INSTRUCTOR LOGO HERE
Change img on all slide masters.

341

342

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Related Technologies

Big Data

Internet of Things

Mobile

Serverless

Key technologies interrelated with cloud computing.

CSA cloud security alliance®

343

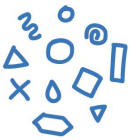
INSTRUCTOR LOGO HERE
Change img on all slide masters.

343

Big Data // Distributed data collection, storage, and processing

High Volume

High Velocity



High Variety

Distributed Data

Distributed Storage

Distributed Processing

CSA cloud security alliance®

344

INSTRUCTOR LOGO HERE
Change img on all slide masters.

344

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Big Data Cloud Security

Securing All The Storage
- Including Intermediary Storage Like Containers Or Storage Volumes For VMS Performing Processing

Encryption Key Management
- No Change To The Fundamentals, But BYOK Most Likely Required If PaaS Involved.

Secure The Platform
- Big Data Platforms Still Have Relatively Low Inherent Security.
- Look To PaaS And Isolated Virtual Networks

Know Your Platform
- Capabilities Vary Greatly Between Both Providers And Platforms
- If You Use Machine Learning/AI, Understand The Security And Privacy Model.

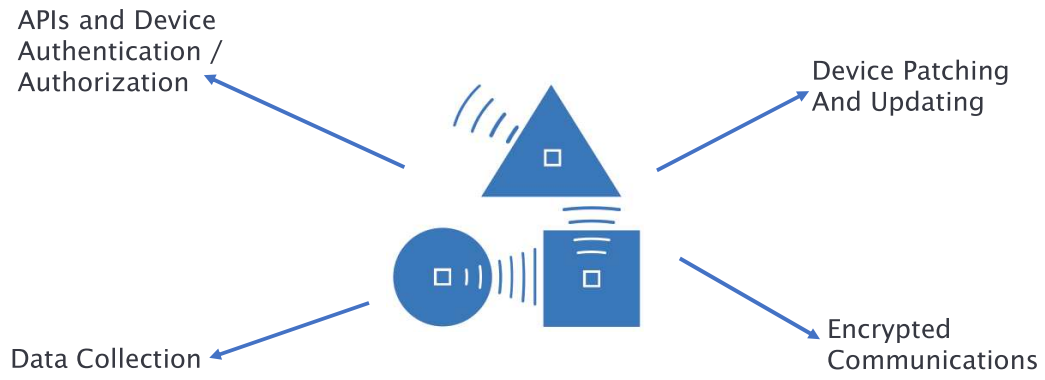
CSA cloud security alliance®

345

INSTRUCTOR LOGO HERE
Change img on all slide masters.

345

Internet Of Things Security Priorities



CSA cloud security alliance®

346

INSTRUCTOR LOGO HERE
Change img on all slide masters.

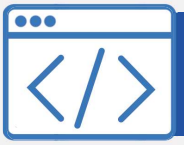
346

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Mobile & Cloud

Most mobile apps connect back to cloud.

Device Registration, Authentication, & Authorization
- Stored credentials are a risk.
- Including federation tokens with long refreshes.



Application APIs can expose the cloud deployment
- If not secured properly.

CSA cloud security alliance®

347

INSTRUCTOR LOGO HERE
Change img on all slide masters.

347

Serverless

- Includes PaaS and Function as a Service
- New frameworks being released at a rapid pace
- IAM and logging are key security issues for serverless apps
- Often provides more security benefits than downside due to pushing more security responsibility onto the cloud provider (in the shared responsibilities model)

CSA cloud security alliance®

348

INSTRUCTOR LOGO HERE
Change img on all slide masters.

348

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Related technologies are key technologies often seen with, and used by, cloud deployments. They include Big Data, the Internet of Things, mobile computing, and serverless computing.
2. Big Data platforms tend to have low inherent security, so using the cloud for isolation is important. It's also critical to understand where and how data is stored and, often, to protect it with distributed encryption.
3. The Internet of Things often uses cloud computing for back end processing, application logic, and data storage. Security concerns tend to focus on device and user authentication and authorization, secure communications, and data storage.
4. Mobile issues are often very similar to those of IoT when it comes to cloud as the cloud becomes the back-end for many mobile apps.
5. Serverless is a cloud-native technology and used in most modern deployments to some degree. IAM and logging tend to be a security focus since they are so different compared to on-premise or even virtualized workloads.

349

INSTRUCTOR LOGO HERE
Change img on all slide masters.

349

350

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Preparing For The CCSK Exam

Study The Guidance And ENISA Documents

- CSA Guidance: https://cloudsecurityalliance.org/download/security-guidance-v4/
- ENISA: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport
- CAIQ: https://cloudsecurityalliance.org/group/consensus-assessments/#_overview
- CCM: https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

Review The CCSK Prep Kit At:

- https://cloudsecurityalliance.org/education/ccsk/#_prepare

351

Preparing For The CCSK Exam

You Will Be Issued A Token After Completion Of This Class Via Email

- You will use the token and the email we have from your registration to start the exam.

You will have two attempts to pass the exam.

The exam is timed (90 minutes), but open book.

352

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Hints

- Read the Guidance 3-4 times and have it with you.
- As with any test, the wording is weird, but if you are familiar with the material and know where to check in the Guidance, you should be fine.
- Don't wait too long after taking this class… your tokens may take a week or two to arrive, which is a good time to take the test.
- If you have technical issues, email:

ccsk-admin@cloudsecurityalliance.org

CSA cloud security alliance®

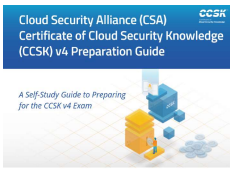
353

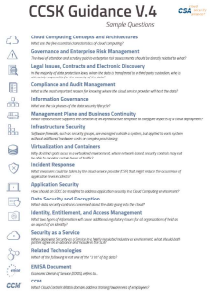
INSTRUCTOR LOGO HERE
Change img on all slide masters.

353

CCSK Prep Kit

- Complete Preparation Package
- Common Body of Knowledge (CBK)
- 16 Sample Questions
- Links for all other resources
- Testing Details
- https://cloudsecurityalliance.org/education/ccsk/#_prepare





CSA cloud security alliance®

354

INSTRUCTOR LOGO HERE
Change img on all slide masters.

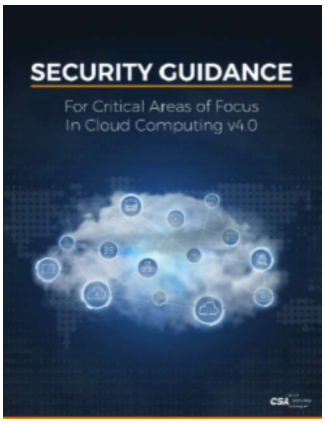
354

Copyright 2019 Cloud Security Alliance and Securosis, LLC

CSA Guidance

Security Guidance

- 87% of test
- Majority of the class
- Domain mappings at beginning of module 1
- Vendor agnostic
- Concepts reinforced by labs
- *https://cloudsecurityalliance.org/download/security-guidance-v4/*



ENISA Risk Report

European Version of NIST

- 6% max of test
- Benefits, Risks & Recommendations for Cloud InfoSec
- *https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport*

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Consensus Assessment Initiative Questionnaire

CAIQ

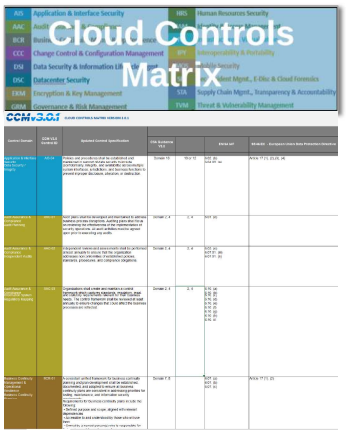
- 7% of test
- 295 Questions
- Direct alignment to CCM
- STARwatch input
- STAR Registry
- https://cloudsecurityalliance.org/group/consensus-assessments/#_overview

357

Cloud Controls Matrix

CCM

- 16 domains
- 133 controls
- Cross Mappings
- Architectural Relevance
- SPI applicability
- https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview



358

Copyright 2019 Cloud Security Alliance and Securosis, LLC

HOORAY!

YOU'RE ALL DONE!

Thank you for participating in this course. If you have questions, comments or concerns, please email *training@cloudsecurityalliance.org*

cloud security alliance®

359

INSTRUCTOR LOGO HERE

Change img on all slide masters.

359

Copyright 2019 Cloud Security Alliance and Securosis, LLC