Cloud Security

Michael J. Teske

Principal Author Evangelist-Pluralsight

Identify Cloud Computing Concepts

Cloud threats and attacks

Examine cloud attacks

- Tools
- Techniques

Examine countermeasures

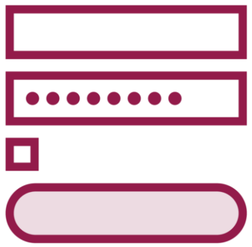
- Best practices
- Tools

Cloud Threats and Attacks

Cloud Provider Security

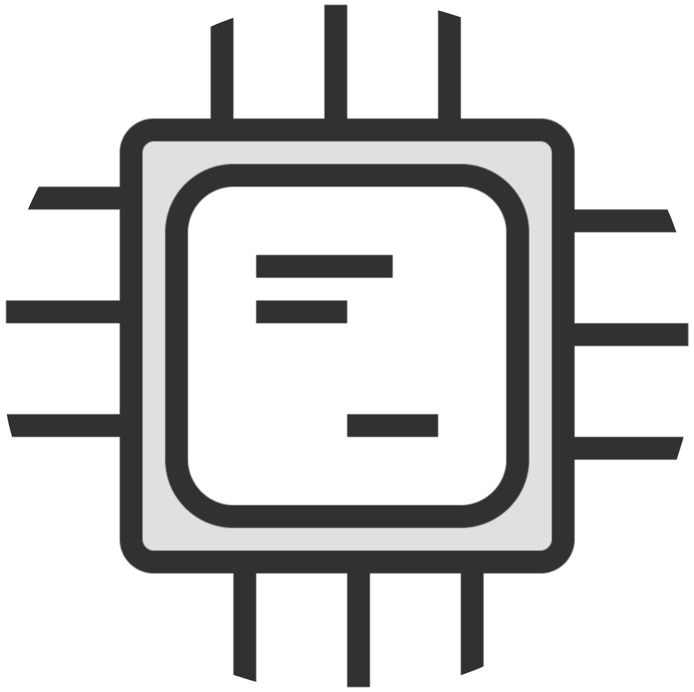
Limited access and access policies

Tracking via access logs



Requires protection against repudiation

Trusted Computing Model



Assists security problems through hardware enhancements

Roots of Trust (RoT)

Top 10 Cloud Threats

Accountability and data risk

Misconfiguration and inadequate knowledge

Legal and regulatory compliance

Business continuity and resiliency

User privacy and secondary usage of data

Top 10 Cloud Threats

Service and data integration

Multi-tenancy and physical security

Incidence analysis and forensics

Infrastructure security

Non-production environment exposure

Hardware failure

Illegal access to the cloud

Shadow IT

Abusing cloud services

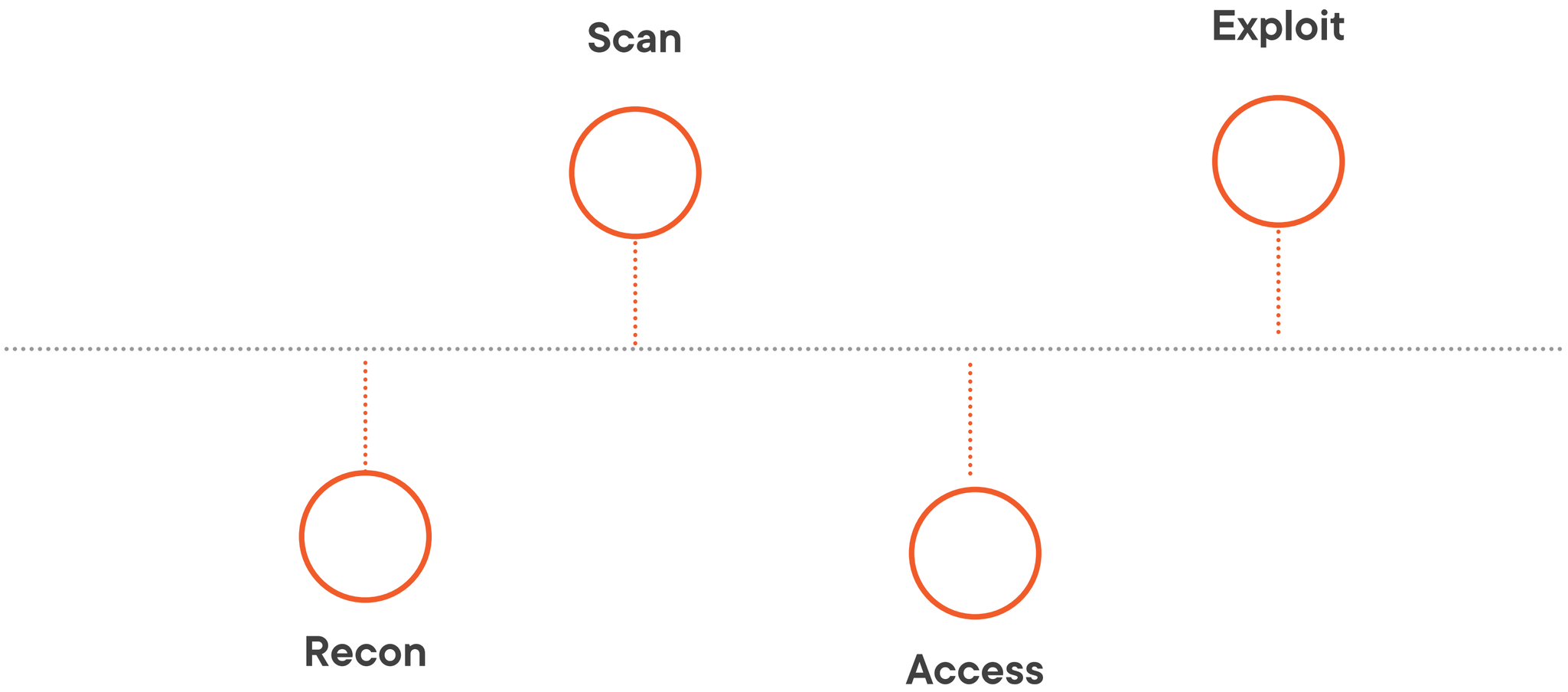
Unknow risk profile

Malicious Insiders

Weak authentication

Examine Cloud Attacks

Cloud Attacks

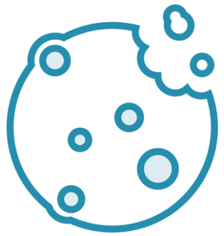


Cloud Computing Attacks

DNS attacks

SQL injection

Network sniffing



Session hijacking

Cryptanalysis attacks

Denial of Service

Common Cloud Attacks

Wrapping attack

Session riding

Side channel attack

Cloud hopper

MITC

Cloudbourne

Common Cloud Attack Tools

S3Scanner

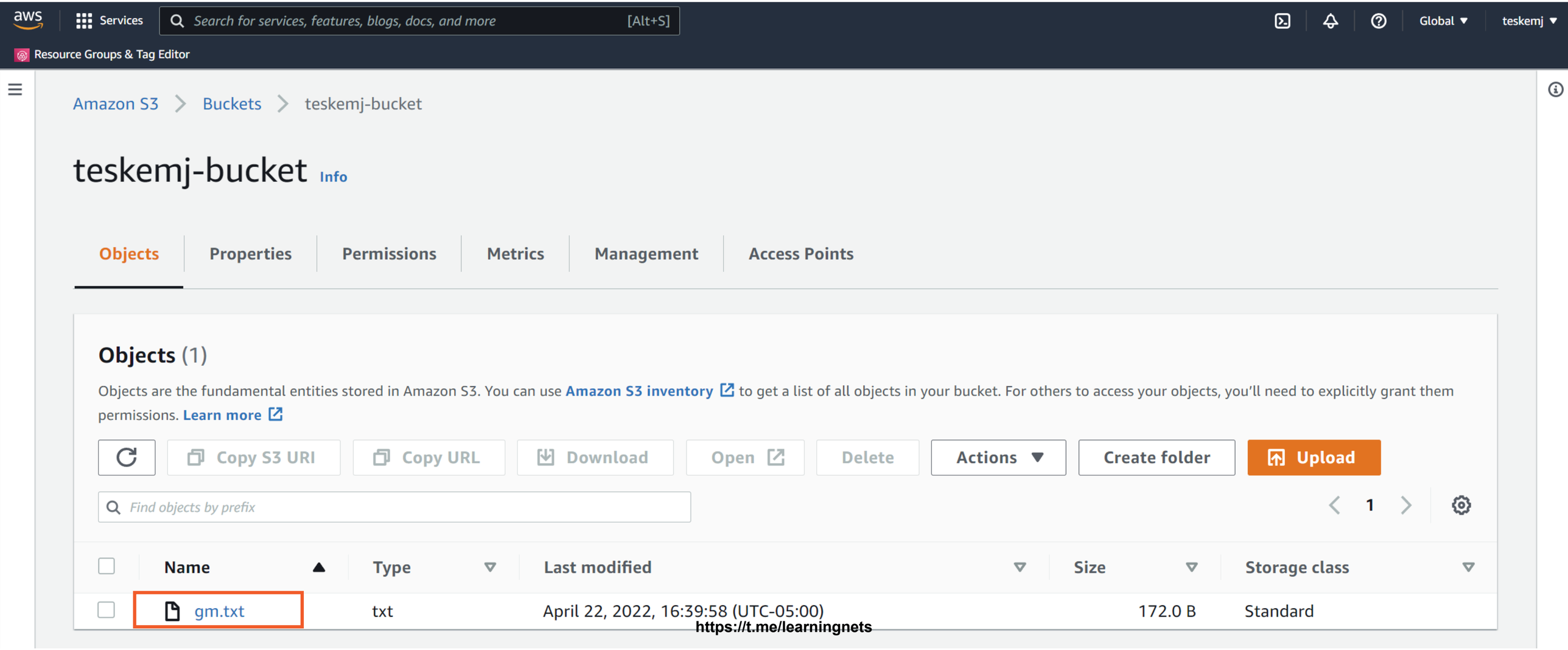
PACU

Dumpster Diver

CCAT

DockerScan

Tools



Tools

```
mj@mj: /mnt/d/repos/temp
mj@mj:/mnt/d/repos/temp$ s3scanner dump --bucket teskemj-bucket --dump-dir ./
/usr/local/lib/python3.6/dist-packages/boto3/compat.py:88: PythonDeprecationWarning: Boto3 will no longer support Python
 3.6 starting May 30, 2022. To continue receiving service updates, bug fixes, and security updates please upgrade to Pyt
hon 3.7 or later. More information can be found here: https://aws.amazon.com/blogs/developer/python-support-policy-updat
es-for-aws-sdks-and-tools/
  warnings.warn(warning, PythonDeprecationWarning)
teskemj-bucket | Enumerating bucket objects...
teskemj-bucket | Total Objects: 1, Total Size: 172.0B
teskemj-bucket | Dumping contents using 4 threads...
teskemj-bucket | Dumping completed
mj@mj:/mnt/d/repos/temp$ cat gm.txt
 --------------
< Good Morning >
 --------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
mj@mj:/mnt/d/repos/temp$
```

Examine Counter Measures

Cloud Security Alliance (CSA)

CIRCLE EVENTS BLOG

cloud security alliance®

Membership ▾ STAR Program ▾ Certificates & Training ▾ Research ▾

Welcome to the Cloud Security Alliance

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

Earn your certificate in cloud security →

Read the latest cloud security research →

Improve your compliance with STAR →

Volunteer for a research working group →

Have a question about cloud security? Ask our community →

Latest News from CSA

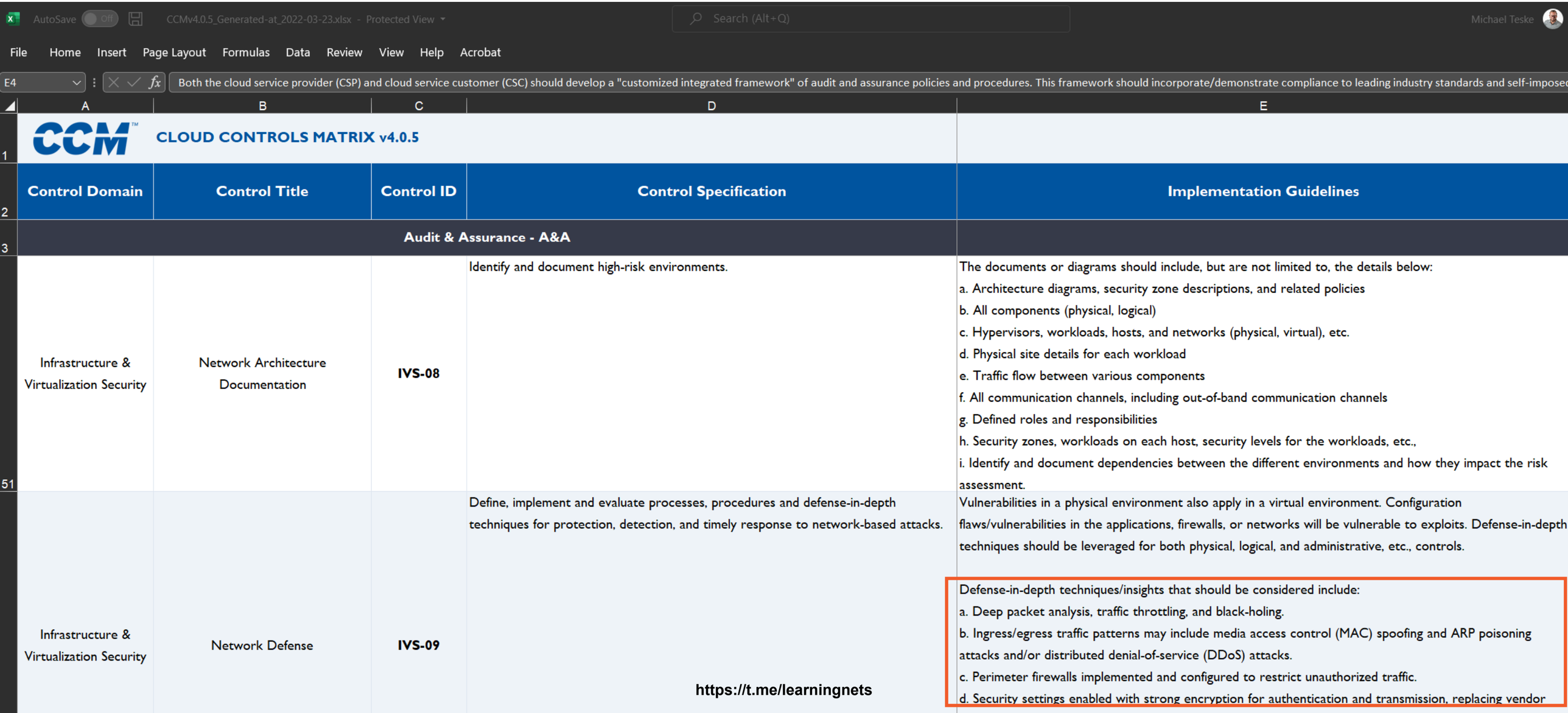
CCAK™

Certificate of Cloud Auditing Knowledge

ZERO TRUST Advancement Center

Collective knowledge guiding zero trust implementation

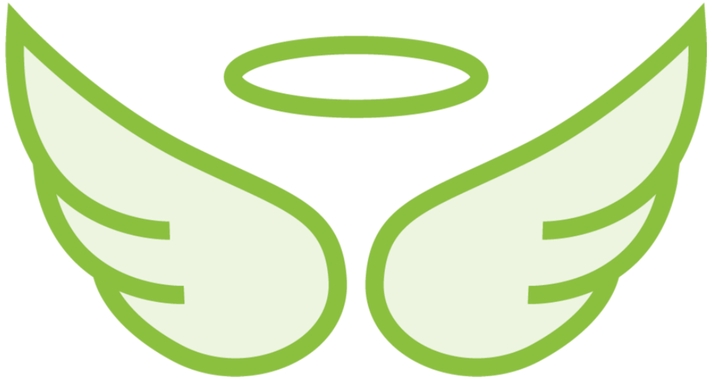
Cloud Controls Matrix



	A	B	C	D	E
1	CCM™ CLOUD CONTROLS MATRIX v4.0.5				
2	**Control Domain**	**Control Title**	**Control ID**	**Control Specification**	**Implementation Guidelines**
3	**Audit & Assurance - A&A**				
51	Infrastructure & Virtualization Security	Network Architecture Documentation	**IVS-08**	Identify and document high-risk environments.	The documents or diagrams should include, but are not limited to, the details below: a. Architecture diagrams, security zone descriptions, and related policies b. All components (physical, logical) c. Hypervisors, workloads, hosts, and networks (physical, virtual), etc. d. Physical site details for each workload e. Traffic flow between various components f. All communication channels, including out-of-band communication channels g. Defined roles and responsibilities h. Security zones, workloads on each host, security levels for the workloads, etc., i. Identify and document dependencies between the different environments and how they impact the risk assessment.
	Infrastructure & Virtualization Security	Network Defense	**IVS-09**	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Vulnerabilities in a physical environment also apply in a virtual environment. Configuration flaws/vulnerabilities in the applications, firewalls, or networks will be vulnerable to exploits. Defense-in-depth techniques should be leveraged for both physical, logical, and administrative, etc., controls. Defense-in-depth techniques/insights that should be considered include: a. Deep packet analysis, traffic throttling, and black-holing. b. Ingress/egress traffic patterns may include media access control (MAC) spoofing and ARP poisoning attacks and/or distributed denial-of-service (DDoS) attacks. c. Perimeter firewalls implemented and configured to restrict unauthorized traffic. d. Security settings enabled with strong encryption for authentication and transmission, replacing vendor

Cloud Security Tools

Core Cloud Inspect



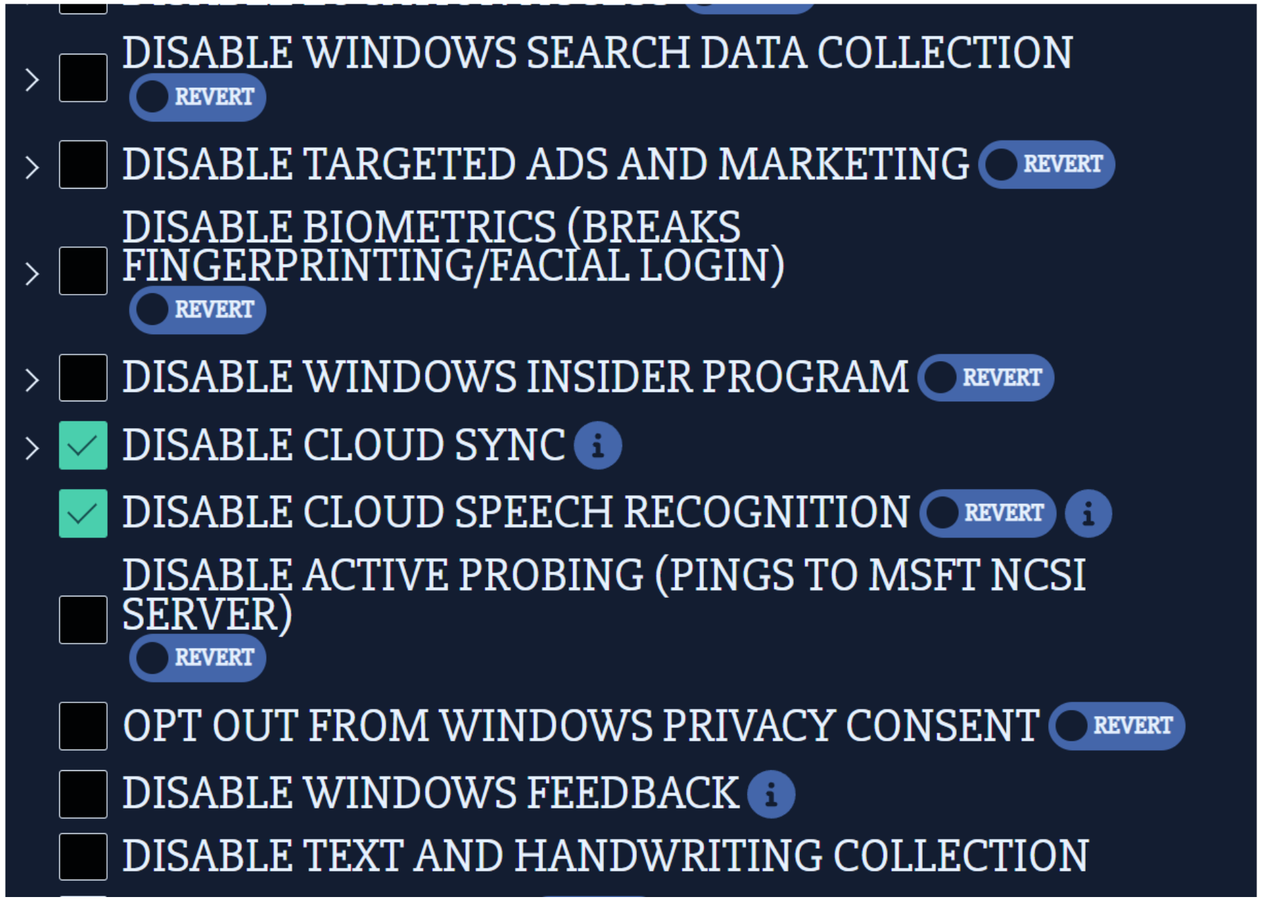
CloudPassage Halo

Privacy.Sexy

Enforce privacy & security on Windows and macOS

Search in 627 scripts

Select: None | Standard | Strict | All Windows | macOS View: Cards | Tree




```
233 :: ------------------------------------------------------------
234 echo --- Disable Web Browser Setting Sync
235 reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\SettingSync" /v
        "DisableWebBrowserSettingSync" /t REG_DWORD /d 2 /f
236 reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\SettingSync" /v
        "DisableWebBrowserSettingSyncUserOverride" /t REG_DWORD /d 1 /f
237 :: ------------------------------------------------------------
238
239
240 :: ------------------------------------------------------------
241 :: --------------Disable Windows Setting Sync---------------
242 :: ------------------------------------------------------------
243 echo --- Disable Windows Setting Sync
244 reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\SettingSync" /v
        "DisableWindowsSettingSync" /t REG_DWORD /d 2 /f
245 reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\SettingSync" /v
        "DisableWindowsSettingSyncUserOverride" /t REG_DWORD /d 1 /f
246 :: ------------------------------------------------------------
247
248
249 :: ------------------------------------------------------------
250 :: --------------Disable Language Setting Sync---------------
251 :: ------------------------------------------------------------
252 echo --- Disable Language Setting Sync
253 reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\SettingSync\Groups\Language"
        /t REG_DWORD /v "Enabled" /d 0 /f
254 :: ------------------------------------------------------------
255
256
257 :: ------------------------------------------------------------
258 :: -------------Disable cloud speech recognition-------------
259 :: ------------------------------------------------------------
260 echo --- Disable cloud speech recognition
261 reg add "HKCU\Software\Microsoft\Speech_OneCore\Settings\OnlineSpeechPrivacy" /v
        "HasAccepted" /t "REG_DWORD" /d 0 /f
262 :: ------------------------------------------------------------
263
264
265 pause
```

Securing Containers

Run containers as a non-root user

Use your own private registry

Verify image integrity, ie Docker Content Trust

Use Docker Bench Security

Learning Check

Learning Check

- Trusted Computing Model
- Mis-configuration and inadequate knowledge
- Wrapping attack
- Cloud Passage Inspect

Module Review

Key Learnings

Cloud threats and attacks

Examine cloud techniques

Examine countermeasures

Up Next:
Course Summary