Top 10 Challenges for PCI Pen Test Scoping in Cloud Environments

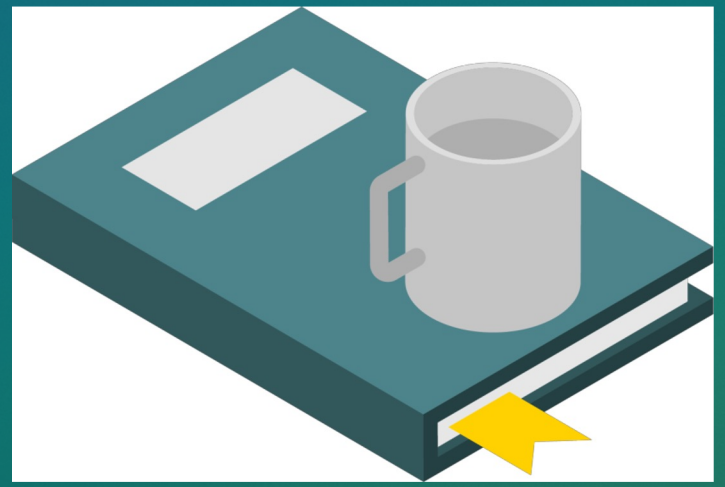
Sheryl Benedict, Principal Consultant, QSA
Carlos Marquez, Senior Penetration Tester, QSA

Agenda

Top 10 Penetration Testing Scoping Challenges in the Cloud

Scoping of cloud services involves accurate information, in-depth understanding of customer expectations, compliance requirements, technical deployments and specific technologies.

We will review the basics of penetration testing scoping; then with the help of real-world examples, discuss the top 10 challenges of scoping penetration tests in the cloud and how to face them.



Takeaways:

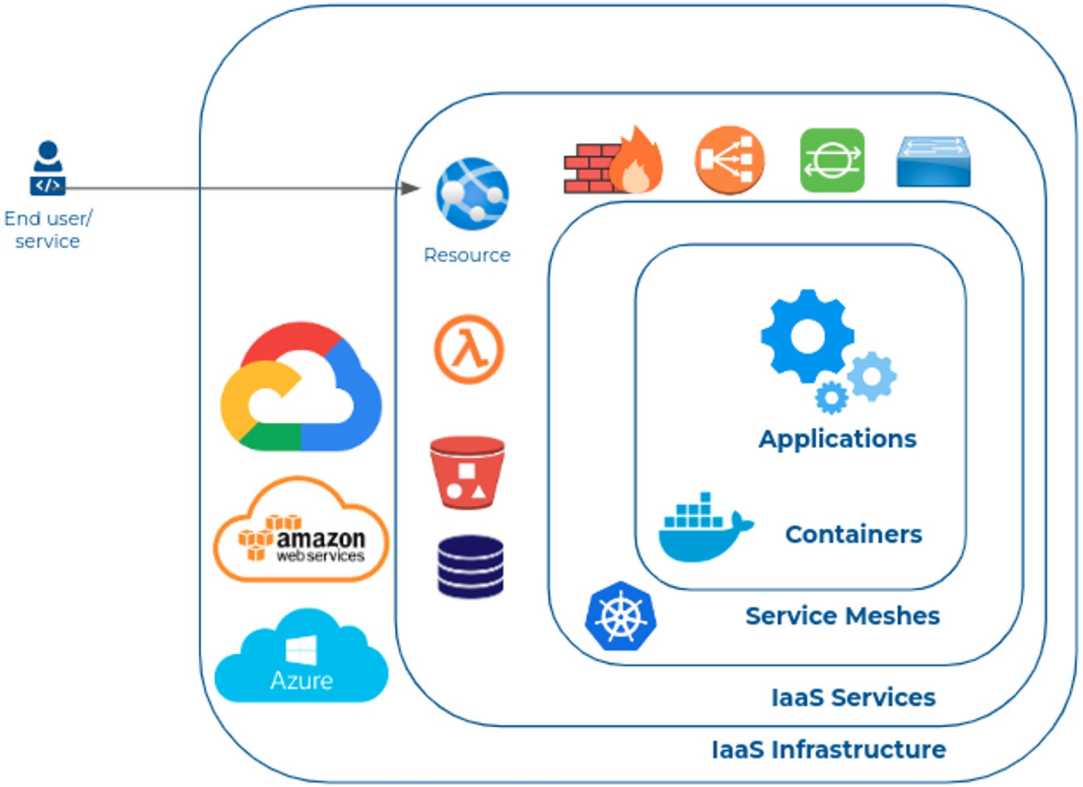
- Core Cloud Scoping Concepts
- Core Penetration Test Scoping Concepts
- Top 10 Challenges and Recommendations

PCI Security Standards Council®

Core Cloud Concepts
What's in the Cloud?

There's a whole data center in there!

- Everything you'll find on premises (just virtual):
  - Firewalls, Servers, Switching and Routing
  - Security tools & appliances
  - Applications & Databases
  - User account directories
  - Disaster Recovery technologies
- The technology architecture is different, but PCI DSS control requirements apply just the same!



PCI Security Standards Council

Scoping and Assessing Cloud Services

- Master Accounts/Subscriptions
- Confirmation and validation of scope must be performed by the merchant/service provider prior to the PCI DSS assessment and the assessor will confirm the scope of the assessment and apply any applicable scope reduction

PCI Security Standards Council

Core Penetration Testing Scope Concepts

Shared Responsibility in Cloud Environments

- PCI DSS technical testing applies to most of the scenarios and are focused on Requirement 6 and 11
- The scope of a penetration test, includes the entire CDE perimeter and any critical systems from an internal and external facing perspective (PCI DSS Requirement 11.3)
- Penetration testing should be conducted as defined by the rules of engagement agreed upon by both parties

PCI DSS Requirement	Example Responsibility Assignment for Management of Controls		
	IaaS	PaaS	SaaS
1: Install and maintain a firewall configuration to protect cardholder data.	Shared	Shared	Provider
2: Do not use vendor-supplied defaults for system passwords and other security parameters.	Shared	Shared	Provider
3: Protect stored cardholder data.	Shared	Shared	Provider
4: Encrypt transmission of cardholder data across open, public networks.	Customer	Shared	Provider
5: Protect all systems against malware and regularly update anti-virus software or programs.	Customer	Shared	Provider
6: Develop and maintain secure systems and applications.	Shared	Shared	Shared
7: Restrict access to cardholder data by business need to know.	Shared	Shared	Shared
8: Identify and authenticate access to system components.	Shared	Shared	Shared
9: Restrict physical access to cardholder data.	Provider	Provider	Provider
10: Track and monitor all access to network resources and cardholder data.	Shared	Shared	Provider
11: Regularly test security systems and processes.	Shared	Shared	Provider
12: Maintain a policy that addresses information security for all personnel.	Shared	Shared	Shared
PCI DSS Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers	Provider	Provider	Provider

Source: PCI SSC Cloud Computing Guidelines; pg. 15

PCI Security Standards Council

Scope of Penetration Tests in the Cloud

Application, Data, Business Logic

application & design flaws
business logic flaws
data loss prevention
etc.

Service

VPC config
Sec Groups
S3 Bucket policies
EC2 Provisioning and API IAM access
cloudFormation risky templates

Account

IAM
hardening
Organization governance
Cross/sub account
trusts

Source: Cloud Security Alliance, Cloud Penetration Testing Playbook; pg. 8

Top 10 Challenges

1. Misunderstanding of penetration test scoping, cloud implementation model, and terminology	6. Virtual environments
2. Penetration Testing within Third Party Infrastructure	7. Undocumented Architecture/APIs or Services (APP)
3. Inaccurate inventory, network diagram, and data flow	8. Containers and Microservices
4. Inaccurate CDE boundaries	9. Serverless Infrastructure
5. Hidden Connections	10. Missing scenarios to be tested

PCI Security Standards Council®

Challenge 1: Misunderstanding of penetration test scoping, cloud implementation model, and terminology

Classic penetration test scoping questions and cloud environment do not always use the same terminology.

- Change IP approach: Use FQDN + Services instead
- Identify cloud service implementation (SaaS, IaaS, PaaS, other)
- Provide cloud services “in use” to the penetration tester
- Terminology between vendors and service inventory

Resource:

https://cloud.google.com/free/docs/aws-azure-gcp-service-comparison

PCI Security Standards Council

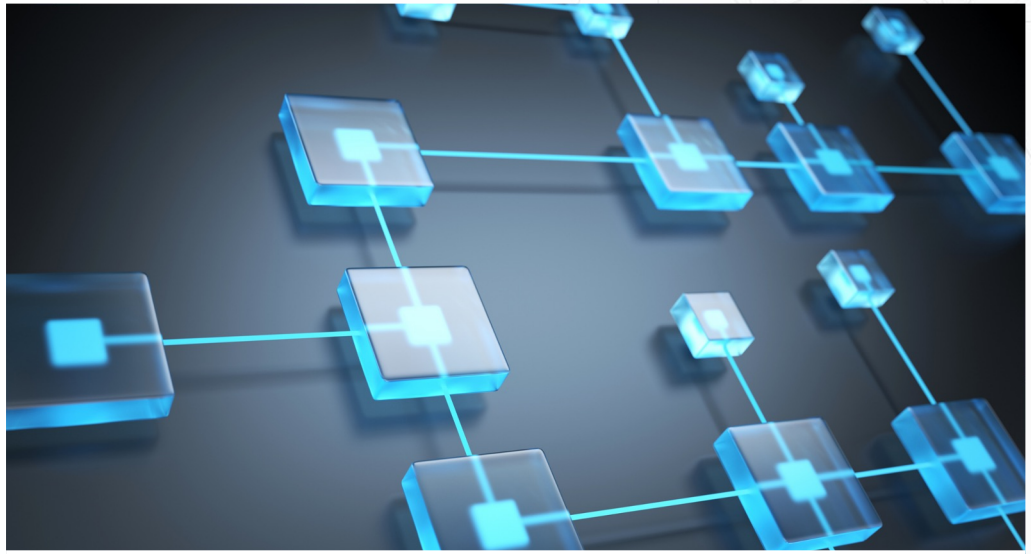
Challenge 2: Penetration Testing within Third Party Infrastructure

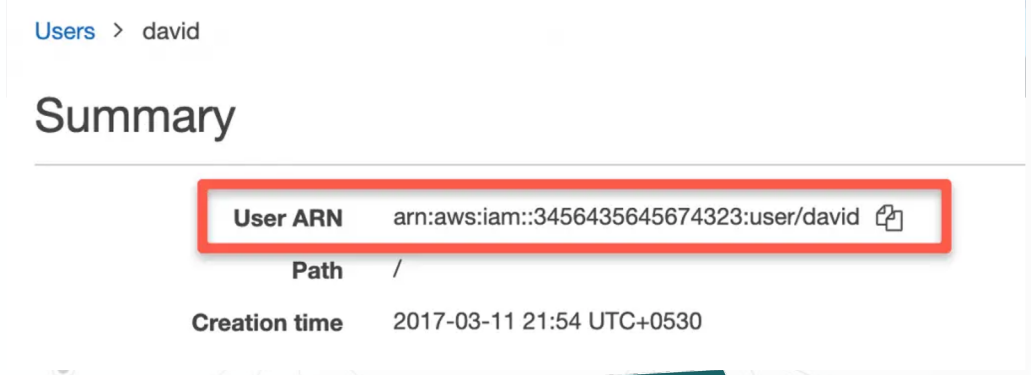
- Confirm cloud responsibilities and implementations
- Might want to consider having a test environment that is mirrored against production
- Determine if multi-tenancy is in use
- Check third party service providers terms and conditions and support policy for penetration testing
    - Some services can’t be pen tested. Such as, cloud infrastructure, social engineering of cloud provider

PCI Security Standards Council

Challenge 3: Inaccurate inventory, network diagram, and data flow

- Entities will need to ensure that system inventories are accurate and complete and align with documented network diagrams and data flow diagrams
- Confirm against responsibilities matrix and determine if the cloud provider is responsible for systems or if it is the customer's responsibility
- Confirm and validate scope with IPs/FQDNs against previous scans
- Generate automated inventory reports





PCI Security Standards Council

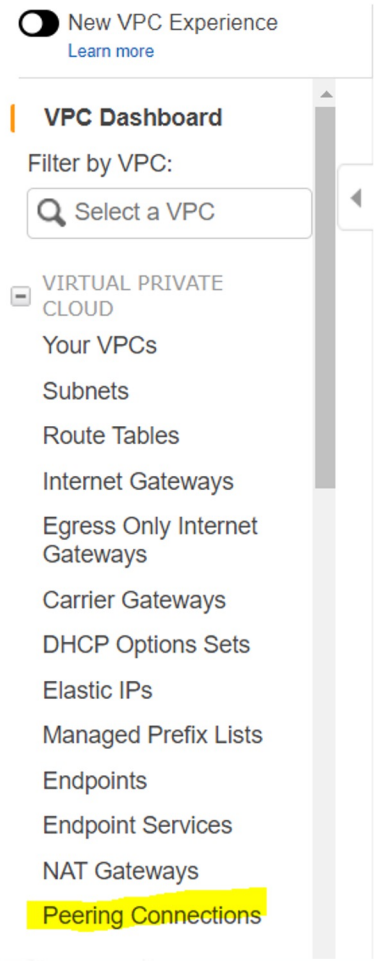
Challenge 4: Inaccurate CDE boundaries

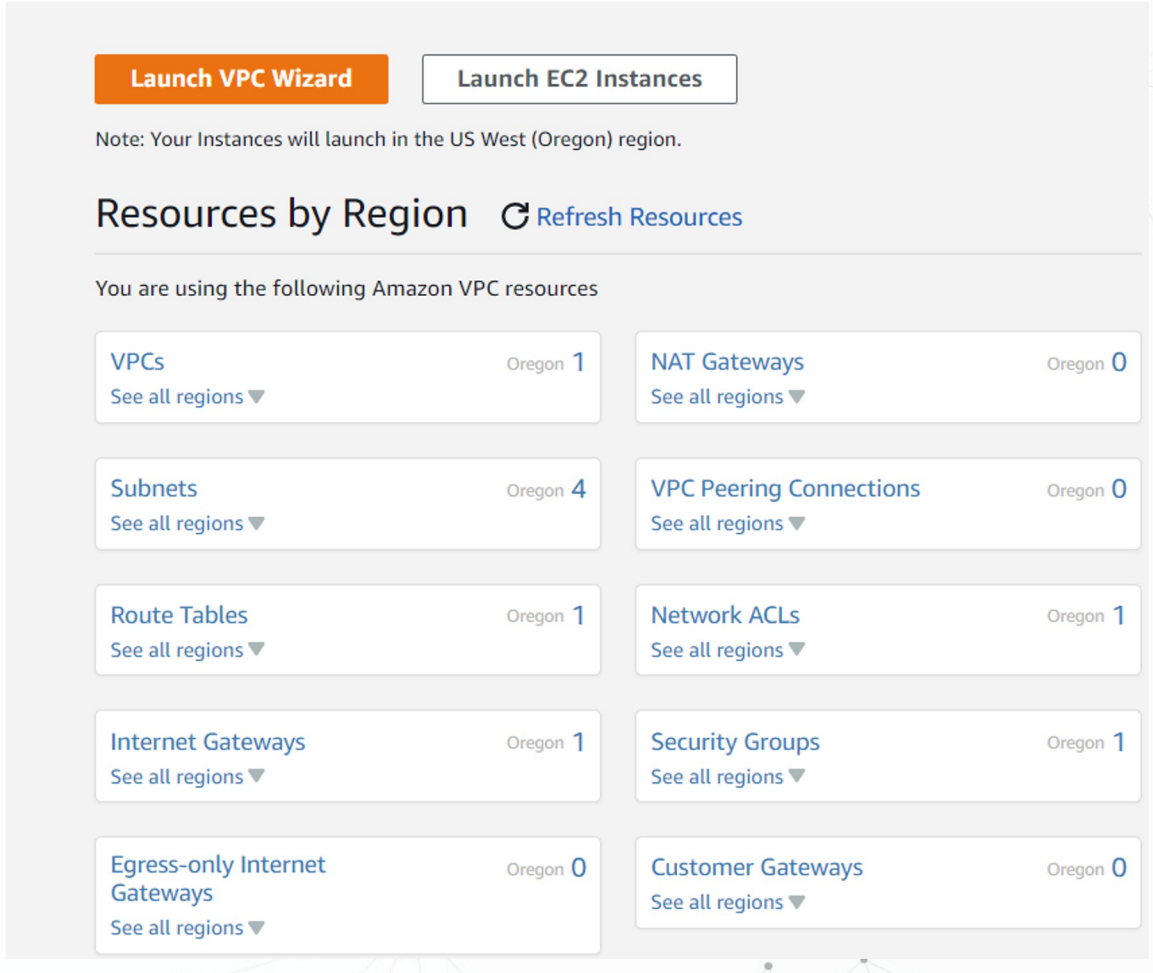
- Confirm segmentation controls in use
  - How does it work? RBAC, ACLs, etc.
  - In which OSI layer?
- Identify effective testing strategies
- Identify common layer between services/devices.
  - Shared resources: Load Balancers, Backup Agents
- Containers based isolation - Architecture review
  - Process, Sandbox, Hypervisor
  - TIP: Process based container isolation doesn't provide adequate segmentation for high security environments

PCI Security Standards Council

Challenge 5: Hidden Connections

- Check redundancy systems
- Jump Boxes
- Examine cloud infrastructure configurations
  - Additional services WAF, IDS/IPS, LB, Gateways.
  - CI/CD pipeline components
  - Peering connections





Name	Peering Connecti	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
TestPeering	pcx-04942f02c02d...	Pending Acce...	vpc-27481a5f	vpc-01fe46b84107...	172.31.0.0/16	-	076003672620	076003672620

Challenge 6: Virtual environments

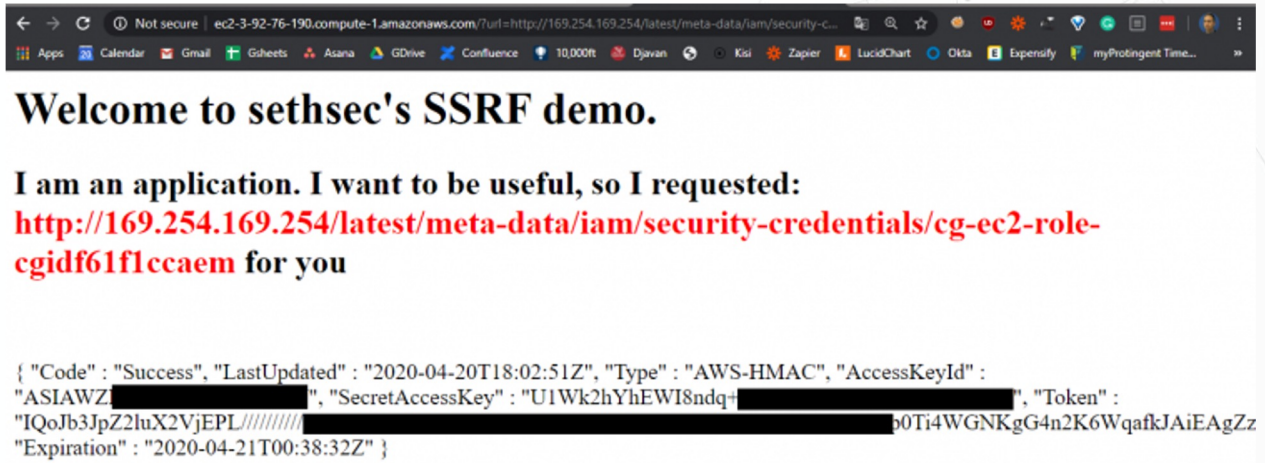
- Internal pentest and segmentation tests may require deploying an internal VPC and remote access
- Consider scenarios assuming low privilege internal compromise in the cloud
- Some vulnerabilities can only be found if you are already in the environment.

  E.g. Privilege escalation or attack vectors using metadata in AWS/GCP/Azure

PCI Security Standards Council

Challenge 7: Undocumented Architecture/APIs or Services (APP)

- Black box testing may not be the best approach. Providing API/WS documentation and business context is recommended
- Provide Postman collection, Swagger Open API, example requests, SDK, accurate API endpoint list
- Classic web attack vectors are still valid: E.g. Injections, IDoR, SSRF (e.g. Capital One 2019)



Source: https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-scenario-ec2_ssrf/

http://EC2_public_ip/?url=http://169.254.169.254/latest/meta-data/<instance-id>

PCI Security Standards Council

Challenge 8: Containers and Microservices

- Identify how orchestration is managed
- Identify if orchestration APIs/IU are exposed and ensure that authentication is tested
- Application architecture and a list of entry points may indicate services to be tested
- Pentesters should check for secrets and sensitive data in any container/orchestration configuration file.

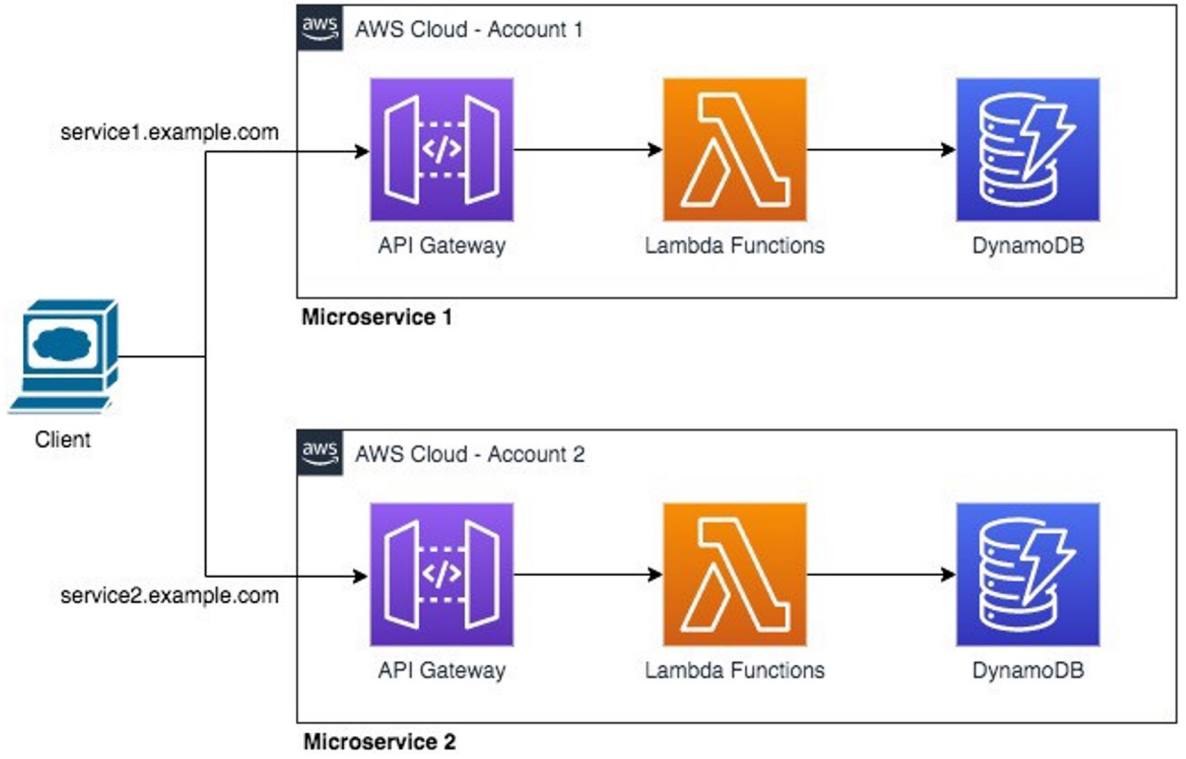
PCI Security Standards Council

Challenge 9: Serverless Infrastructure

- Provide scripts/events (and RBAC capability) that trigger key functions that may impact the security of the CDE or application

AWS Lambda invoke --function <value> <file>

- Identify effective testing strategies
- Distinguish between cloud infrastructure and application components
- Check responsibility matrix



Source: amazon.com

PCI Security Standards Council

Challenge 10: Missing scenarios to be tested

- Enumerate cloud services using OSINT resources (name resolution, brute force, S3/blob indexer, software repositories, coding forums, etc.)
- Explore attack surface
- Identify exposed authentication and entry points
- Privilege escalation vectors in the cloud
- Identify software repositories and audit them for sensitive information. E.g. AWS credentials in a private GitHub repository (Uber 2016)

In Summary

- It is important to ensure that your PCI DSS internal, external, and segmentation penetration testing scope is accurately defined and reflects the assets that are also considered in-scope for the PCI DSS assessment validation
- Confirmation and validation of scope must be performed by the merchant/service provider prior to the PCI DSS assessment and the QSA assessor will confirm the scope and apply any applicable scope reduction
- Understand what cloud provider service model is utilised and examine responsibility matrices
- You can't test what is not visible: Blackbox testing does not fits all architectures
- Cloud pentesting involves additional tests, many based on the technology used

PCI Security Standards Council®

Connect With Us

Sheryl Benedict, Principal Consultant
QSA, PCIP, CISA, CCSK, CDPSE, ISO 27001 Sr. Lead Implementer
+1 (714) 726-6971
sbenedict@foregenix.com

Carlos Marquez, Senior Penetration Tester
QSA, PFI, CISSP, CISM, CHFI, CEH, GPEN, CPTIA, CPSA, ISO 27001 Lead Auditor
cmarquez@foregenix.com