SANS CLOUD SECURITY

https://www.sans.org/cloud-security

Secure Service Configuration in AWS, Azure, & GCP

Based on Content From
SEC510: Public Cloud Security:
AWS, Azure, and GCP
sans.org/SEC510

Onto the Introduction ›

Table of Contents

Introduction

Multiple clouds require multiple solutions. In an ideal world, you could learn the core concepts of cloud computing and apply them to whatever cloud provider your organization uses. Unfortunately, we live in a world where each of the top three most popular cloud platforms, Amazon Web Services (AWS), Microsoft Azure, and the Google Cloud Platform (GCP), radically differ from one another in both design and implementation. These differences affect how security professionals must operate in each environment.

This poster compares and contrasts the popular security services of each major cloud provider. By identifying insecure defaults and little-known security features, you can ensure the security of your organization's assets across each public cloud environment.

The contents of this poster are based on material from SEC510: Public Cloud Security: AWS, Azure, and GCP
For more information, visit sans.org/SEC510

Onto the Service Navigation

Table Of Contents ›

Service Navigation

Private Cloud Access

Identity and Access Management (IAM)

Network Assessment

Cryptographic Key Management

Instance Metadata Services (IMDS)

Network Flow Logging

Storage Assessment

Data Encryption

Serverless Assessment

Instance Metadata Service (IMDS)

Cloud Resource Hijacking
MITRE ATT&CK T1496: Consuming the victim's cloud resources to solve resource-intensive problems

- Cryptocurrency mining on cloud virtual machines
- Distributed denial-of-service (DDOS) attacks
- Password cracking on GPU virtual machines

Cloud Credential Management Assessment Criteria
Configure your Instance Metadata Service (IMDS) to be as inaccessible as possible

1. Turn off IMDS if the cloud infrastructure does not need to access cloud-managed resources
2. Remove access to legacy versions of the IMDS
3. Require metadata tokens for AWS
4. Turn off GCP's v0.1 and v1beta1 IMDS
5. Limit the IP hops token responses to 1 (AWS only)

	SSRF Protection	Token Timeout	Token Scope	Requires REST API	Prevents Extraction
AWS v1	NO	6 HOURS	NO	NO	NO
AWS v2	YES	6 HOURS	NO	NO	YES
Azure	YES	24 HOURS	YES	YES	NO
GCP v0.1 & v1beta1	NO	1 HOUR	NO	YES	NO
GCP v1	YES	1 HOUR	NO	YES	NO

Identity and Access Management (IAM)

AWS IAM Instance Role Assessment Criteria

Benchmark 1.19: Ensure that IAM instance roles are used for AWS resource access from instances

1. Note that instances without a managed profile role often contain hard-coded credentials
2. Create a least privilege IAM role with permissions scoped to the virtual machine's functional requirements
3. Verify each EC2 instance has an assigned "IAM Role" gateway or a private direct connection

AWS IAM Administrative Assessment Criteria

Benchmark 1.22: Ensure that IAM policies that allow full "*:*" administrative privileges are not created

1. List all IAM policies in each account
2. Get the latest version for each policy
3. Filter by policies with the Effect attribute set to Allow
4. Identify policies with the Action and Resource attributes set to a wildcard (*)

	Organization Policy	Principal Policy	Resource Policy	Conditional Policy	Default SA Policy
AWS	Default Feature	YES	YES	YES	No Permissions
Azure	Premium Only	YES	Limited	NO	No Permissions
GCP	Default Feature	YES	Limited	Partial	Editor Permissions

Network Assessment

AWS Default VPC Assessment Criteria

Benchmark 4.3: Ensure that the default security group of every VPC restricts all traffic

1. Remove the default VPC from each region
2. Modify the default VPC Network ACL
   - Remove the default ingress/egress rules
3. Modify the default security group in each region
   - Remove the default ingress/egress rules
4. Create custom VPC resources per service

Azure Network Assessment Criteria

Benchmark 6: Networking Security

6.1: Ensure that RDP access is restricted from the Internet
6.2: Ensure that SSH access is restricted from the Internet
6.3: Ensure that SQL databases do not allow ingress 0.0.0.0/0 (Any IP)

GCP Network Assessment Criteria

Benchmark 3: Networking

3.1: Ensure that the default network does not exist in a project
3.6: Ensure that SSH access is restricted from the Internet
3.7: Ensure that RDP access is restricted from the Internet

	Connected to the Internet	Admin Ports Open	Ingress Filtering	Egress Filtering	Consistent Controls
AWS	YES	NO	YES	NO	YES
Azure	YES	NO	YES	NO	NO
GCP	YES	YES	Limited	Limited	YES

Network Flow Logging

AWS Network Logging Assessment Criteria
Benchmark 2.9: Ensure that VPC flow logging is enabled in all VPCs

1. Enable flow logging in every VPC
2. At a minimum, capture “Reject” packet data
3. Configure a 365-day minimum log retention period
4. Archive logs in long-term storage (e.g. S3 / Glacier)

Azure Network Logging Assessment Criteria
Benchmark 6.4 Network Security Group flow logs should be enabled, and the retention period should be set to greater than or equal to 90 days

1. Enable the flow logs option in the Network Security Group
2. Create a storage account for flow log data
3. Configure a 365-day log retention period (90 minimum)

GCP Network Logging Assessment Criteria
Benchmark 3.9: Ensure that VPC Flow logs is enabled for every subnet in VPC Network

1. View the VPC service and enumerate each subnet
2. Set each subnet’s flow log attribute to true
3. Be aware of the sampling rate

	Enabled by Default	Minimum Delay	Maximum Retention Period	Command Line Support	Log Blocked Ingress Traffic
AWS	NO	1-6 MINUTES	Indefinite	YES	YES
Azure	NO	10 MINUTES	Indefinite	Using Extension	YES
GCP	NO	5 SECONDS	3650 DAYS	YES	NO

Private Cloud Access

Advanced Remote Access Assessment Criteria

Require multiple factors of authentication for remote administrative access

1. Block all SSH/RDP access from the public Internet
2. Enable advanced remote access cloud services
3. Securely access cloud resources through a VPN gateway or a private direct connection

	Internal Service Routes	Custom Service Endpoints	Service Access Control	Endpoint Policy	Principal Restrictions
AWS	YES	YES	YES	YES	YES
Azure	YES	YES	YES	YES	NO
GCP	Limited	TBD	YES	TBD	NO

	Internal Shell Access	Site-to-Site VPN	Point-to-Site VPN
AWS	YES [1]	YES	YES
Azure	YES [2]	YES	YES
GCP	YES [3]	YES	NO

Cryptographic Key Management

Assessment Criteria

Limit and audit all cryptographic key usage

1. Prevent individuals from decrypting production data; only applications should have this permission
2. Record and audit all decryption events
3. Ensure that keys are rotated on a schedule
4. No one should be able to instantly delete a cryptographic key

	Flexible Access Policy	Audit Logging	Automatic Key Rotation	Deletion Schedule	Single-Tenant Option
AWS	YES	YES	YES (if turned on)	7-30 DAYS	YES
Azure	YES [4]	YES	No Policy Found	7-30 DAYS (if turned on)	YES
GCP	YES	YES	YES (if turned on)	24 HOURS	“Selected Customers”

Data Encryption

Data Encryption Assessment Criteria

All data should be encrypted at rest and in-transit (there are extremely few exceptions)

Azure Database Service Encryption Assessment Criteria

- Benchmark 4.9: Ensure that "Data encryption" is set to "On" on a SQL database
- Benchmark 4.10: Ensure that the SQL server's TDE protector is encrypted with BYOK (use your own key)
- Benchmark 4.11: Ensure that the "Enforce SSL connection" is set to "ENABLED" for MySQL database Server
- Benchmark 4.13: Ensure that the "Enforce SSL connection" is set to "ENABLED" for PostgreSQL database Server

AWS KMS Audit Logging with CloudTrail

Benchmark 2.7: Ensure that CloudTrail logs are encrypted at rest using KMS CMKs

```
1  resource "aws_s3_bucket" "cloudtrail" {
2      bucket = "cloudtrail"
3      force_destroy = true
4      policy = data.aws_iam_policy_document.cloudtrail_s3.json
5  }
6
7  resource "aws_cloudtrail" "aws_api_calls" {
8      name = "aws-api-calls"
9      s3_bucket_name = aws_s3_bucket.cloudtrail.id
10     include_global_service_events = true
11     kms_key_id = aws_kms_key.cloudtrail.arn
12 }
```

Storage Assessment

AWS S3 Assessment Criteria

Review S3 for the following security benchmarks:

1. Configure Block Public Access at the account level
2. Configure Block Public Access at the bucket level
3. Configure Server Access Logging for audit logging
4. Configure Object-level Logging into CloudTrail
5. Configure Default Encryption at the bucket level

Azure Storage Assessment Criteria

Benchmark 3: Storage Accounts

1. Enable the secure transfer required attribute
2. Rotate storage account access keys periodically
3. Configure logging for read, write, and delete requests
4. Expire Shared Access Signatures (SAS) tokens in less than 60 minutes
5. Ensure that SAS tokens require HTTPS connections
6. Configure Blob containers access level to Private

GCP Storage Assessment Criteria

Benchmark 5: Cloud Storage

1. Ensure that cloud storage buckets are not anonymous or publicly accessible
2. Ensure there are no publicly accessible objects in storage buckets
3. Ensure that logging is enabled for cloud storage buckets

	Block Public Access Policy	Access Logging	Default Encryption
AWS	YES	YES	NO
Azure	NO	YES [5]	YES
GCP	NO	YES	YES

Serverless Assessment

Cloud Serverless Assessment Criteria

Review functions for the following security misconfigurations:

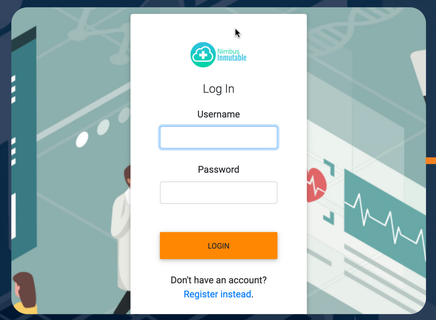
1. Scan functions for secrets management and persistence issues
2. Authenticate requests to publicly accessible functions
3. Use unique service accounts per function
4. Regularly audit function permissions for least privilege
5. Enable function audit and network controls (if available)

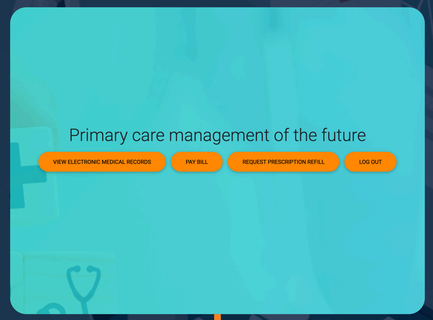
	Function	OS	Default Directory	User
AWS	Node.js 12	Amazon Linux 2	/var/task	sbx_user1051
Azure	.NET Core 3.1	Debian GNU/Linux 9	/	root
GCP	Go 1.11	Ubuntu 18.04.2 LTS	/srv/files	root

	Root User	Warm Environment	Credential Timeout	Read-Only File System	Default Network
AWS	NO	11 MINUTES	12 HOURS	YES [6]	YES
Azure	YES	6 MINUTES	8 HOURS	NO	YES
GCP	YES	3 MINUTES	30 MINUTES	NO	YES

	Default SA	Custom SA	HTTPS Access	VPC Integration
AWS	Least Privilege	YES	API Gateway	YES
Azure	Least Privilege	YES	Built-in [7]	YES [9]
GCP	Excessive	YES	Built-in [8]	YES [10]

Nimbus Inmutable



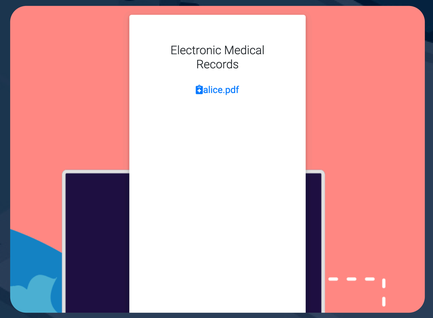


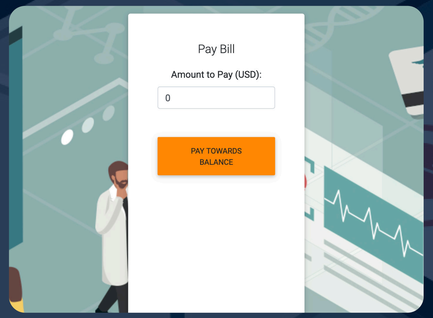
Google Cloud

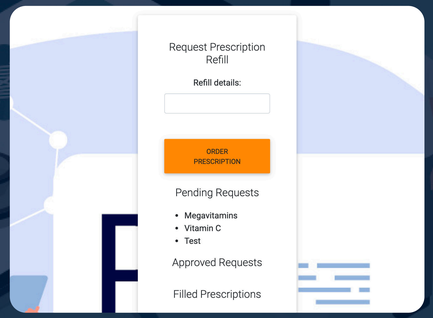
aws

Azure

Nimbus Inmutable is a fictional company featured in the labs for SEC510: Public Cloud Security: AWS, Azure, and GCP. Its corporate website runs on all three of the major clouds and leverages the cloud services available for the cloud on which it is deployed. It includes the ability to view your Electronic Medical Records (EMRs), pay your bill, and request prescription refills. Despite having fairly basic functionality, Nimbus uses all of the services detailed in the next slide. This illustrates how complex a modern app in the cloud can be.







Cloud Services

Compute Services

Virtual Machines

Dedicated Virtual Machines on which cloud-based applications can be run.

Containers

Logically isolated compute service running on a single cloud virtual machine.

Serverless Functions

Provide code to the cloud to be executed on a random container when an event occurs.

IAM Service

Enforce access control to other services.

Cloud Flow Logging

Provides metadata about traffic internal to the cloud's private network.

Cloud Private Networks

Allows all services and infrastructure access to be controlled at the network level.

Cloud API Logging Services

Can track all activity within a cloud account and tie it to an IAM principal.

Key Management Services

Manages cryptographic keys. Nimbus's application uses custom code to encrypt its prescription data at the record level using these keys. Additionally, AWS KMS integrates with S3, the SSM Parameter Store, the Secrets Manager, RDS, and more to encrypt the data stored in these services at rest.

Storage Accounts

Capable of storing all kinds of data. Azure Storage is used as the backend for storing logs and the data for managed databases in Azure. Nimbus stores its assets, medical records, and corporate secrets in these services. The VM proxies its asset requests, while the medical records are cached on the VM's filesystem. Intermingling data of varying sensitivity levels can be dangerous as it is error-prone.

Cloud Private Endpoint Services

Keeps traffic within the private network and allows the organization to lock down access to managed services from outside that network.

Remote Access Services: Allows authorized personnel to access SSH and other network-protected services.

Logging Services

Used to store and view log data. Among other things, they can be used to audit flow logs and access to the cloud provider's APIs.

Cloud-Managed Relational Databases

Manages hosting for databases like MySQL, PostgreSQL, MSSQL, etc. Nimbus stores its user data and prescription refill requests in a cloud-managed MySQL database.

Remote Access Services

Allows authorized development and operations staff to administrate their private resources without poking holes in the cloud's firewall.

Secret Managers & Parameter Stores

Contain configuration and secrets used by the application. Nimbus uses these to store its database connection details and credentials, JSON Web Token (JWT) secret for user authentication, and more.

Resources

SANS staff, authors, and instructors produce thousands of free content-rich resources for the information security community annually. These resources aim to provide the latest in research and technology available to help support awareness and growth across a wide range of IT and OT security considerations. This next section provides a succinct list of cloud security resources, both inside and outside of SANS, as well as direct links to a number of general SANS free resources.

Cloud Security Resources

Posters, Cheat Sheets, and Tools
SANS Multicloud Cheat Sheet
SANS Cloud Security Free Tools
SANS Cloud Security and DevSecOps Best Practices

Whitepapers, Blogs, and Webcasts
Top 5 Considerations for Multicloud Security
SANS Cloud Security Blog
Rhino Security Blog
Top Threats to Cloud Computing - The Egregious 11
SANS Cloud Security Webcasts

Cloud Security Training Environments
CloudGoat
TerraGoat
ServerlessGoat
flAWS 2

AWS Resources
AWS Security Blog
Hands-On AWS Penetration Testing with Kali Linux by Karl Gilbert & Benjamin Caudill

Microsoft Azure Resources
Azure Security Podcast (@AzureSecPod)
Pen Testing Azure Applications by Matt Burrough

Google Cloud Resources
Google Cloud Security Resources
Google Cloud Security

Table Of Contents ›

SANS Free Resources

SANS Free
sans.org/free

SANS Blogs
sans.org/blog

SANS Newsletters
sans.org/newsletters

SANS Reading Room
sans.org/reading-room

SANS Webcasts
sans.org/webcasts

SANS Posters
sans.org/security-resources/posters

SANS Internet Storm Center
isc.sans.edu

Table Of Contents ›

About SANS Cloud Security

SANS Cloud Security focuses the deep resources of SANS on the growing threats to the cloud. SANS provides training, certification, research, and community initiatives to help security professionals build, deploy, and manage secure cloud infrastructure, platforms, and applications.

SANS Cloud Security curriculum provides intensive immersion training designed to help you and your staff master the practical steps necessary to defend systems and applications in the cloud against the most dangerous threats. The courses are full of important and immediately useful techniques that you can put to work as soon as you return to your office. The curriculum has been developed through a consensus process involving industry-leading engineers, architects, administrators, developers, security managers, and information security professionals. The courses address public cloud, multicloud, and hybrid-cloud scenarios for both established and developing organizations alike.

SANS Cloud Security Blog

SANS Cloud Security Linkedin

SANS Cloud Security Twitter – @SANSCloudSec

SANS Cloud Security Youtube

Table Of Contents ›

SANS Cloud Security Courses

Long Courses

SEC488 Cloud Security Essentials
Learning the Language of Cloud Security.

SEC510 Public Cloud Security: AWS, Azure, and GCP
Multiple Clouds Require Multiple Solutions.

SEC522 Defending Web Applications Security Essentials | GWEB
Not a Matter of "if" but "When." Be Prepared for a Web App Attack. We'll Teach You How.

SEC540 Cloud Security and DevOps Automation | GCSA
The Cloud Moves Fast. Automate to Keep Up.

SEC545 Cloud Security Architecture and Operations
In the Cloud, No One Can Hear You Scream. Architect It Properly and You Won't Have to.

SEC588 Cloud Penetration Testing | GCPN
Aim Your Arrows to the Sky and Penetrate the Cloud.

SEC584 Cloud Native Security: Defending Containers and Kubernetes
Deliver Securely at the Speed of Cloud Native.

MGT516 Managing Security Vulnerabilities: Enterprise and Cloud
Stop Treating the Symptoms. Cure the Disease.

Short Courses

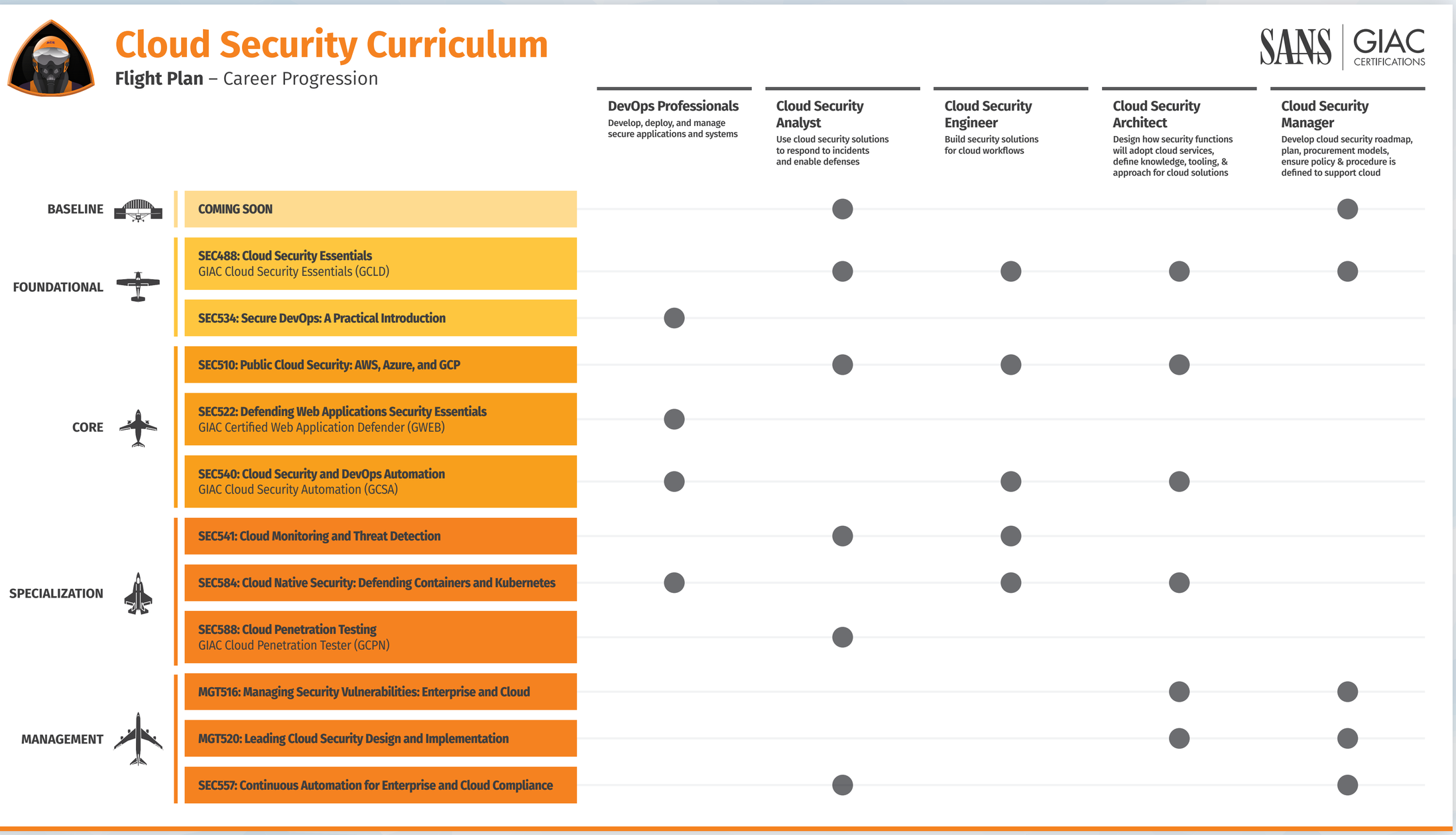
SEC534 Secure DevOps: A Practical Introduction
Principles! Practices! Tools! Oh My! Start Your Journey on the DevSecOps Road Here.

SEC541 Cloud Monitoring and Threat Hunting
You Can Run, But You Can't Hide! You're on Our Radar.

MGT520 Leading Cloud Security Design & Implementation
Building and Leading a Cloud Security Program.

Table Of Contents ›

SANS Cloud Security Flight Plan



About the Authors

Brandon Evans | bevans@sans.org | @brandonmaxevans

Brandon is a Senior Application Security Engineer at Asurion, where he provides security services for thousands of his coworkers in product development across several global sites responsible for hundreds of web applications. As an application developer for most of his professional career, he moved into security full-time largely because of his many formal training sessions through SANS. Brandon[11] is lead author for the new SEC510: Public Cloud Security: AWS, Azure, and GCP course and a contributor and instructor for SEC540: Cloud Security and DevOps Automation. He is also a Co-Leader for the Nashville Chapter of OWASP.

Eric Johnson | ejohnson@sans.org | @emjohn20

Eric is a Co-founder and Principal Security Engineer at Puma Security and a Senior Instructor with the SANS Institute. His experience includes cloud security assessments, cloud infrastructure automation, static source code analysis, web and mobile application penetration testing, secure development lifecycle consulting, and secure code review assessments. Eric is the lead author and an instructor for SEC540: Cloud Security and DevOps Automation, and a co-author and instructor for both the new SEC510: Public Cloud Security: AWS, Azure, and GCP course and the upcoming SEC584: Defending Cloud Native Infrastructure course. Additionally, Eric is a SANS Security Awareness Developer Training Advisory Board Member and SANS Analyst for Application Security and DevSecOps Surveys.

Wes Braga | wesbragagt@gmail.com | @wesbragagt

Wes is a musician turned web application developer. He enjoys coffee, loud music, and developing user interfaces from design to development. Wes designed Nimbus Inmutable, the website featured on this poster and used in SEC510: Public Cloud Security: AWS, Azure, and GCP. After starting his career through a coding bootcamp and freelance work, Wes joined XSOLIS, a Nashville-based healthcare company, as a Software Engineer.

Footnotes

1. AWS's SSM Session Manager only works with IMDSv2 using non-stable versions of the SSM agent.
2. Azure's serial console requires that the VM supports password-based authentication for SSH.
3. GCP's "SSH from the browser" requires customers to manage their own firewall rule containing Google's entire public IP address range.
4. Multiple Key Vaults are necessary to grant a principal different permissions for different keys.
5. The Azure Terraform provider seems to be missing this capability.
6. AWS Lambda allows write access to the /tmp directory for temporary storage and processing.
7. The Azure Function's App Service plan provides a configuration option for redirecting all HTTP requests to HTTPS.
8. Google Functions do not natively offer a way to enable HTTPS connections without also enabling HTTP.
9. Only available with a Premium App Service plan.
10. Only available with a GCP Organization and VPC Service Controls enabled.
11. 01:23:45.678901 IP source-hostname.12345 > dest-hostname.9999: UDP, length 81
    E..m..@.@..C
    ...#....i'..Y+.....?j5sw4ylrmjqsamjoebzdiidsguqdelraifztgicboa3camzoebhxanbaj5ydkib.....
    01:23:45.678901 IP source-hostname.12345 > dest-hostname.9999: UDP, length 27
    E..7..@.@..x
    ...#....i'..#+..... ufyqg6na=.....

Table Of Contents ›

SANS The most trusted source for cybersecurity training, certifications, degrees, and research