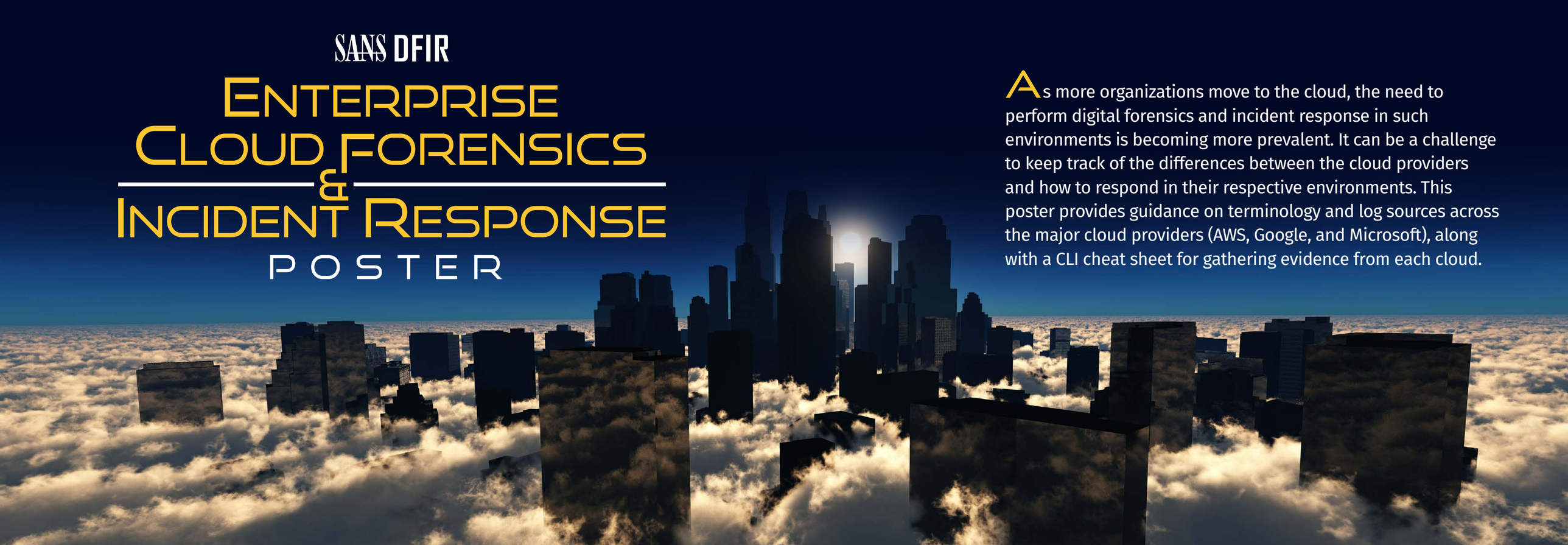
SANS DFIR

Enterprise Cloud Forensics & Incident Response Poster



As more organizations move to the cloud, the need to perform digital forensics and incident response in such environments is becoming more prevalent. It can be a challenge to keep track of the differences between the cloud providers and how to respond in their respective environments. This poster provides guidance on terminology and log sources across the major cloud providers (AWS, Google, and Microsoft), along with a CLI cheat sheet for gathering evidence from each cloud.

DFPS_FOR509_v1.1_07-22

Cloud Terminology

Service	AWS	Azure	GCP
Virtual Machine	EC2 Instance	Virtual Machine	Compute Engine
Serverless	Lambda	Functions	Cloud Functions
VM Disk Storage	EBS(Elastic Block Store)	Managed Disks	Persistent Disks
Object Storage	S3 (Simple Storage Service)	Blob Storage	Cloud Storage
Network File Storage	EFS (Elastic File System)	File Storage	File Store
Virtual Networking	VPC	VNet	Cloud Virtual Network
Logging	CloudWatch & CloudTrail	Log Analytics	Log Explorer
Message Queuing	SQS (Simple Queue Service)	Event Hub	Cloud Pub/Sub

Significant Log Sources

Microsoft 365

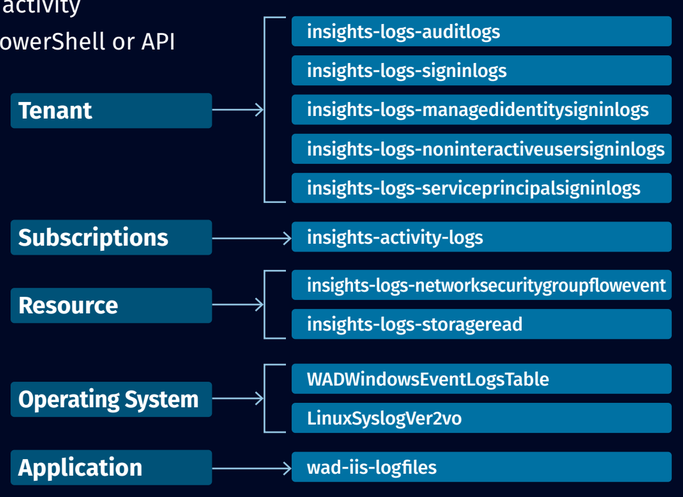
Unified Audit Log

- Every Microsoft workload, user and admin activity
- Accessed via Purview compliance portal, PowerShell or API

Azure

Log Types

- Tenant logs (on by default)
- Subscription logs (on by default)
- Resource logs (off by default) – NSG Flow logs included here
- Operating system logs (off by default)
- Application logs (off by default)



Access Methods

- View them directly on the Azure portal.
- Store them in a Log Analytics workspace.
- Send them to a storage account for archival or export.
- Send them to a SIEM by using an event hub or Graph API.

AWS

Log Types

- CloudTrail – Tenant audit logs
- CloudTrail Insights – API usage outside of baselines
- CloudWatch Logs – Forwarded logs from applications and endpoints
- GuardDuty – Anomaly detection within CloudTrail
- VPC flow logs – NetFlow logs from your VPCs
- S3 Server access – Logs from web-based storage access
- Route 53 – DNS Resolver Logs
- Load Balancer Logs

Access Methods

- View them in the AWS console
- Store them in S3 and search with Athena
- Analyze them with AWS Detective
- Ship them with Event Hub to your SIEM

GCP

Log Types

- Admin Activity Logs
- System Event Logs
- Enterprise Group Audit Logs
- Login Audit Logs
- Access Transparency Logs
- Policy Denied Audit Logs
- Bucket Logs

**You get 400 days of free logs under the _Required bucket*

GWS

Log Types

- Admin log events
- Drive log events
- Gmail log events
- OAuth log events
- Rules log events
- Takeout log events
- User log events

SANS Training

FOR509: Enterprise Cloud Forensics and Incident Response

The world is changing and so is the data we need to conduct our investigations. Cloud platforms change how data is stored and accessed. They remove the examiner's ability to directly access systems and use classical data extraction methods. Unfortunately, many examiners are still trying to force old methods for on-premise examination onto cloud-hosted platforms. Rather than resisting change, examiners must learn to embrace the new opportunities presented to them in the form of new evidence sources. FOR509: Enterprise Cloud Forensics and Incident Response addresses today's need to bring examiners up to speed with the rapidly changing world of enterprise cloud environments by uncovering the new evidence sources that only exist in the Cloud.

SOF-ELK for Cloud Logs

Microsoft 365

Unified audit log – either exported from the portal or PowerShell, must be CSV formatted

Parser: /usr/local/sof-elk/configfiles/6701-office365.conf

Logstash folder: /logstash/office365

Azure

Tenant, subscription and resource logs – exported from storage account in JSON format

Parser: /usr/local/sof-elk/configfiles/6801-azure.conf

Logstash folder: /logstash/azure

Preprocessing commands:

- Processing Azure PT1H files:

```
$ find . -type f -name PT1H.json -exec cat {} + | tee output.json
```

AWS

CloudTrail logs

Parser: /usr/local/sof-elk/configfiles/6901-aws.conf

Logstash folder: /logstash/aws

Preprocessing commands:

- `$ aws-cloudtrail2sof-elk.py -r ./path/to/log -w /logstash/aws/cloudtrail.json`

GCP

Google Logging exports

Parser: /usr/local/sof-elk/configfiles/6950-gcp.conf

Logstash folder: /logstash/gcp

Google Workspace

Google Workspace audit logs exported via API in JSON format – email tracking logs exported to CSV from the admin portal

Parser: /usr/local/sof-elk/configfiles/6951-gws.conf

Logstash folder: /logstash/gws

Flow Logs

VPC flow logs from AWS or GCP, NSG flow logs from Azure

Logstash folder: /logstash/nfarch

Preprocessing commands:

- AWS: `$ aws-vpcflow2sof-elk.sh -r /path/to/aws/flow/log -w /logstash/nfarch/aws_flow_log.txt`
- Azure: `$ azure-vpcflow2sof-elk.py -r /path/to/azure/flow/log -w /logstash/nfarch/azure_flow_log.txt`

Default Log Retention Configuration

	AWS	Azure	GCP
Authentication	30 days	90 days	400 days
User Accounts	30 days	90 days	400 days
Resources	30 days	90 days	400 days
Storage	Off by default	Off by default	Off by default
Flow Logs	Off by default	Off by default	Off by default
Firewall Logs	Off by default	Off by default	Off by default

SANS DFIR Curriculum

SANSForensics @SANSForensics dfir.to/DFIRCast dfir.to/LinkedIn

Operating System & Device In-Depth

FOR308 Digital Forensics Essentials

FOR498 Battlefield Forensics & Data Acquisition — GBFA

FOR500 Windows Forensic Analysis — GCFE

FOR518 Mac and iOS Forensic Analysis & Incident Response

FOR585 Smartphone Forensic Analysis In-Depth — GASF

Incident Response & Threat Hunting

FOR508 Advanced Incident Response, Threat Hunting & Digital Forensics — GCFA

FOR509 Enterprise Cloud Forensics & Incident Response

FOR528 Ransomware for Incident Responders

FOR572 Advanced Network Forensics: Threat Hunting, Analysis & Incident Response — GNFA

FOR578 Cyber Threat Intelligence — GCTI

FOR608 Enterprise-Class Incident Response & Threat Hunting

FOR610 REM: Malware Analysis Tools & Techniques — GREM

FOR710 Reverse-Engineering Malware: Advanced Code Analysis

SEC504 Hacker Tools, Techniques & Incident Handling — GCIH

Threat Hunting in the Cloud

Events of Interest

Scenario	Log Source				
	AWS	Azure	GCP	GWS	M365
Impossible Travel	CloudTrail	Signin Logs	Login Audit Logs	Audit Report	UAL
Console Access via Service Accounts	CloudTrail	SPN Signin Logs	Policy Denied Logs	NA	UAL
Publicly Exposed Keys	CloudTrail	Activity Logs	System Event Logs	OAuth Log Events	UAL
Storage Canaries	CloudTrail/ Server Access Logs	Storage Logs	Storage Logs	Drive Log Events	UAL
Lateral Movement	CloudTrail	Activity Logs	System Event Logs	User Log Events	UAL
Password Sprays	CloudTrail	Signin Logs	Login Audit Logs	User Log Events	UAL
Cloud Tenant Enumeration	CloudTrail	Activity Logs (Limited)	System Event Logs	Service Logs	UAL

API Calls That Return Creds for AWS

- iam:CreateServiceSpecificCredential
- iam:ResetServiceSpecificCredential
- iam:UpdateAccessKey
- lightsail:GetInstanceAccessDetails
- lightsail:GetRelationalDatabaseMasterUserPassword
- rds-db:connect
- redshift:GetClusterCredentials
- sso:GetRoleCredentials
- mediapackage:RotateChannelCredentials
- mediapackage:RotateIngestEndpointCredentials
- sts:AssumeRole
- sts:AssumeRoleWithSaml
- sts:AssumeRoleWithWebIdentity
- sts:GetFederationToken
- sts:GetSessionToken
- chime:CreateApiKey
- codepipeline:PollForJobs
- cognito-identity:GetOpenIdToken
- cognito-identity: GetOpenIdTokenForDeveloperIdentity
- cognito-identity: GetCredentialsForIdentity
- connect:GetFederationToken
- connect:GetFederationTokens
- ecr:GetAuthorizationToken
- gamelift:RequestUploadCredentials
- iam:CreateAccessKey
- iam:CreateLoginProfile

CLI Cheat Sheet

PowerShell – Connecting to Microsoft 365

```
PS> Install-Module -Name ExchangeOnlineManagement
PS> Import-Module ExchangeOnlineManagement; Get-Module ExchangeOnlineManagement
PS> Connect-ExchangeOnline -UserPrincipalName <UPN> -ShowProgress $true
```

PowerShell – Connecting to Azure

```
PS> Install-Module -Name Az -AllowClobber
PS> Import-Module Az; Get-Module Az
PS> Connect-AzAccount
```

Download Cloudtrail Logs

```
$ aws s3 cp s3://<name of log bucket>/AWSLogs . --recursive
```

gcloud Log Collection

```
$ gcloud logging buckets list
$ gcloud logging read 'timestamp<="2021-02-28T00:00:00Z" AND timestamp>="2020-01-
25T00:00:00Z"' --format="json" > all_gcp_logs.json
```

Azure Snapshot Download

```
azcopy cp "<snapshot URL>" "c:\temp\snapshot.vhd" --check-md5 nocheck
```

AWS Snapshot Download via Coldsnap

```
coldsnap --region <region> download <snapshot id> image.dd
```

AWS Snapshot Creation and Mounting via AWS CLI

```
aws ec2 create-snapshot --volume-id <volumeid> --description "Making a snapshot"
aws ec2 create-volume --availability-zone <zone where your DFIR AMI is running>
--snapshot-id <snapshot-id>
aws ec2 attach-volume --volume-id <volume id returned from prior command>
--instance-id <your DFIR EC2 instance> --device </dev/sdX>
```

Resources

- **FOR509 GitHub:** https://for509.com/github
- **CrowdStrike CRT:** https://for509.com/crowdstrikecrt
- **Tesorion CERT UAL Extractor:** https://for509.com/tcert-ual
- **Invictus IR M365 Extractor:** https://for509.com/invictus-ual

Enterprise Cloud Forensics & Incident Response