Using Splunk/ELK for Auditing AWS/GCP/Azure Security Posture

By Rod Soto and José Hernandez

$Whoami

José Hernandez
Principal Security Researcher at Splunk. He started his professional career at Prolexic Technologies (now Akamai), fighting DDOS attacks against Fortune 100 companies perpetrated by “anonymous” and “lulzsec.” As a engineering co-founder of Zenedge Inc. (acquired by Oracle Inc.), José helped build technologies to fight bots and web-application attacks. He has also built security operation centers and run a public threat-intelligence service.

Rod Soto
Principal Security Research Engineer at Splunk. Worked at Prolexic Technologies (now Akamai), and Caspida. Cofounder of Hackmiami and Pacific Hackers meetups and conferences. Creator of Kommand && KonTroll / NoQrtr-CTF.

Security in the Cloud...

- The cloud is prevalent and pervasive in all that we do.
- Cloud providers are not invulnerable and attacks against them affect our lives.
- As cloud adoption expands, there are an increasing number of new technologies and unknowns.
- Cloud security is not an exact translation of inside-the-perimeter security.
- Every provider has its own set of technologies, features, and security items.
- While there are several cloud-security initiatives, it is still an ongoing effort.
- There are a range of emerging tools designed to assess the cloud. We chose CS Suite because it helps analysts assess Azure, AWS, and GCP.

...Security in the Cloud

engadget

Login

Gear Gaming Entertainment Tomorrow Buyer's Guide Video Reviews

Microsoft and Amazon will fight for the Pentagon's $10B cloud contract

Project JEDI has attracted some of the biggest tech names in the world.

Rachel England, @rachel_england
04.11.19 in Business

28 Comments

1882 Shares

The Imaginary Line Between Provider And Customer

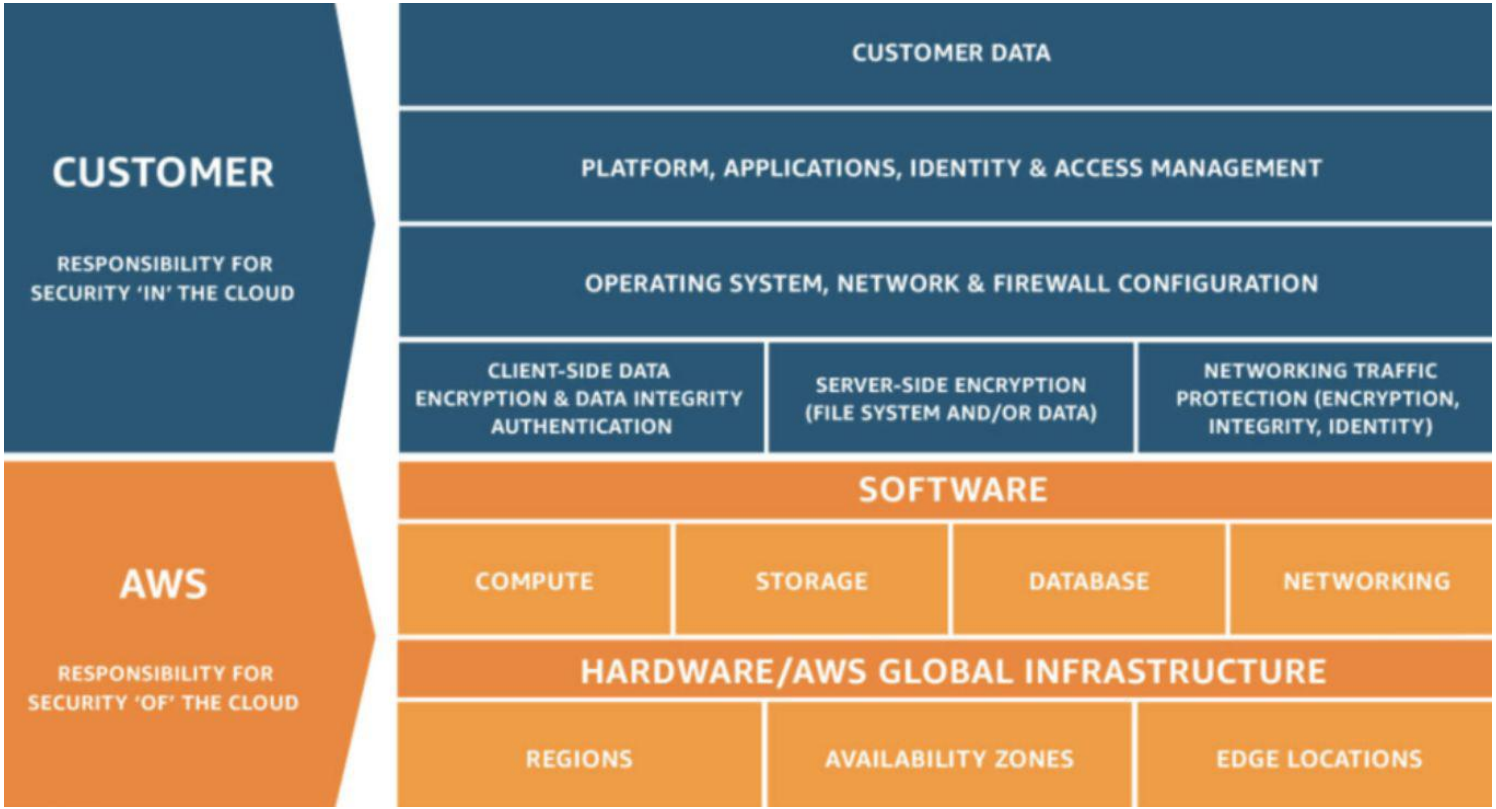
Responsibility per cloud service model	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
GRC (Security Governance, Risk & Compliance)			
Data Security			
Application Security			
Platform Security			
Infrastructure Security			
Physical Security			

Customer Responsibility

Shared Responsibility

Provider Responsibility

The Imaginary Line Is Not That Imaginary… AWS



Azure

Securing Azure resources is a shared responsibility between Microsoft and the customer

MICROSOFT'S COMMITMENT

Securing and managing the cloud foundation

- Physical assets
- Datacenter operations
- Cloud infrastructure

JOINT RESPONSIBILITY

Securing and managing your cloud resources

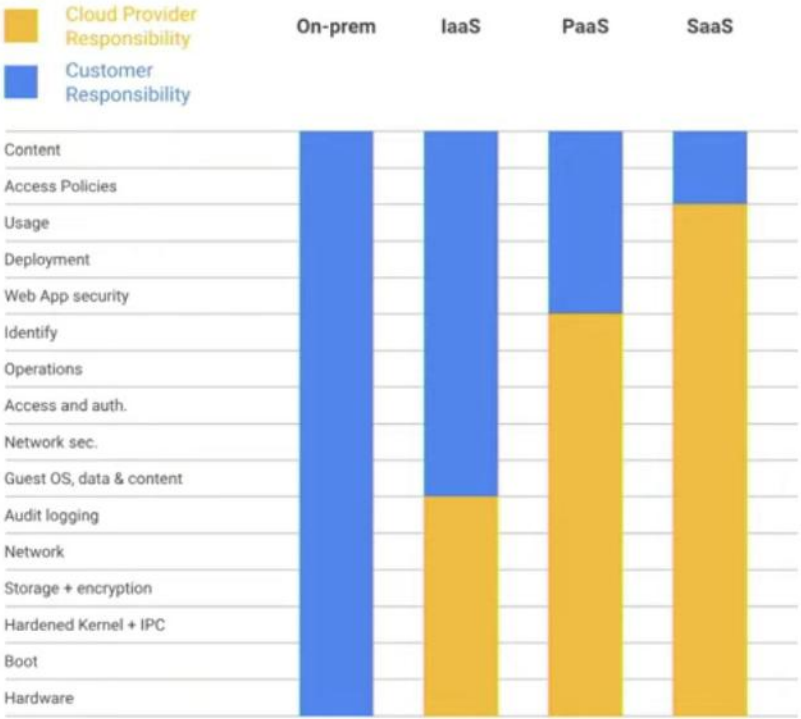
- Virtual machines
- Applications & workloads
- Data

GCP

Understanding shared responsibility

The **boundaries change** based on the services selected by the customer

Customers can use multiple classes of services **simultaneously**



Google Cloud

Cloud Attacks Highlights

- Sony (2011): 77M users
- ICloud (2014): The Fappening
- CloudHopper: (2014 - 2016 -)(IBM, Fujitsu, NTT Data, Tata, HP, DXC, Dimension, CSC)
- Ashley Madison: (2015) / AFF (2015/2016)
- Equifax (2017): 143M customers
- HBO (2017): 1.5 TB of data stolen, including unreleased GoT
- Marriott (2018): 327M accounts
- Kubernetes: CVE-2018-1002105 (PrivEsc)
- Yup…2019 Capital One: 100M accounts

Main Cloud Attack Vectors CSA: "Treacherous 12"

1. Data breaches
2. Insufficient identity, credential, and access management
3. Insecure interfaces and application-programming interfaces (APIs)
4. System vulnerabilities
5. Account hijacking
6. Malicious insiders

Main Cloud Attack Vectors CSA: Treacherous 12

7. Advanced persistent threats (APTs)
8. Data loss
9. Insufficient due diligence
10. Abuse and nefarious use of cloud services
11. Denial of Service (DoS)
12. Shared technology vulnerabilities

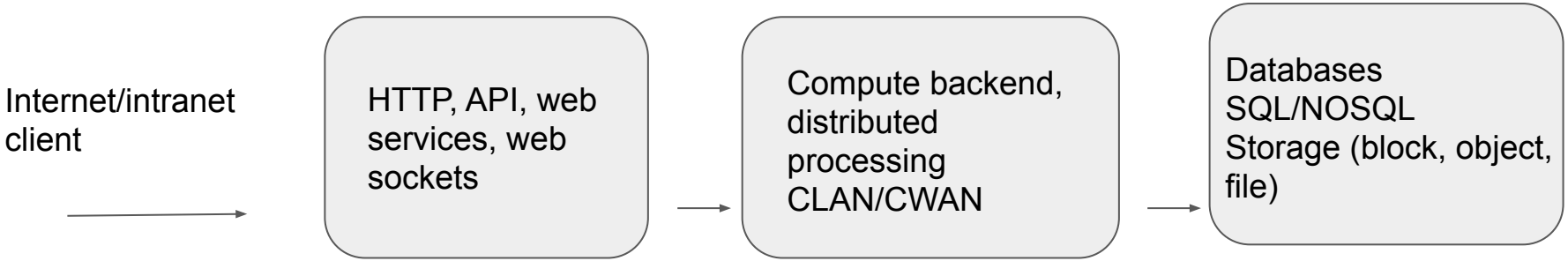
Main Targets of Cloud Attacks

- **Users:** ATO, key exfil, phishing
- **Providers:** AZ, AWS, GCP
- **Admins:** Like Domain Admin, they have access to all
- **Resources:** Cryptomining, DDoS for rent
- **Data:** Everyone's private life and work information
- **Third parties** Partner or co-tenant gets hacked, actor pivots to your cloud, attacks affecting IdP

DevOps Attack Surface (CI/CD Pipeline)

- **Source code repository:** Bitbucket, Beanstalk, Github, Gitlab, SVN, S3 buckets
- **CI/CD platform:** TravisCI, Jenkins, CircleCI, Gitlab
- **Container repository:** Docker, Vagrant
- **IaaS Provider:** Kubernetes flavor, OpenStack (this may also be local in some private, hybrid environments)
- **IaC** Ansible, Terraform, Chef, Cloudformation

Main Cloud Attack Surface Segments



Can We Create Common Criteria For Cloud Security?

Common Criteria For Cloud Security

1. **Network:** External access, VLAN/VWAN, VPN, routing
2. **Security:** CIA → heavy emphasis in IAM, encryption, and FWs
3. **Compute:** Artifacts such as virtual machines, containers, apps, microservices
4. **Database:** SQL, NOSQL
5. **Storage:** Basically buckets and file type storage (block, object, file)
6. **Management:** Kubernetes flavor, logging setup, Management access

Common Criteria for Cloud Security Audits

Compute

AWS: EC2, Lightsail, Lambda, Elastic Beanstalk, ECS, EKS, Batch, ECR, Kubernetes

Azure: Virtual machines (VMs), load balancers, app services, batch, Mesh, disks, Kubernetes

GCP: VM Instances, disks, snapshots, images, TPUs, metadata, zones, Kubernetes, "big data"

Common Criteria for Cloud Security Audits

Management

AWS: Console, CloudTrail, Config, OpsWorks, Systems Manager, CloudFormation, Kubernetes

Azure: Console, Monitor, Advisor, activity log, metrics, manage applications, solutions, Kubernetes

GCP: Console, StackDriver, audit logs, cloud tasks

Common Criteria for Cloud Security Audits

Storage

AWS: S3, EFS, FSx, S3 Glacier, storage gateway, AWS backup

Azure: Data Box, Storage explorer, StorSimple, Data Lake Storage

GCP: Bigtable**,** Buckets, DataStore, FireStore, Filestore, Spanner, Memorystore

Common Criteria for Cloud Security Audits

Security

AWS: IAM**,** Resource Access Manager, Secrets Manager, GuardDuty, AWS SSO, Certificate Manager, Key Management Service, Dir Service, WAF & Shield, Security Hub

Azure: Azure AD, Security Center (encryption, FW, WAF, etc.), Azure Vault

GCP: Security Command Center, Cloud Identity-Aware Proxy, Access Context Manager, VPC, Binary Authorization, Data Loss Prevention, cryptographic keys, Access Approval, Web Security Scanner

Common Criteria for Cloud Security Audits

Network

AWS: VPC, CloudFront, Route53, API Gateway, Direct Connect, AWS App Mesh, AWS Cloud Map, Global Accelerator

Azure: Virtual Networks, Load Balancers, DNS zones, CDN, Traffic Manager**,** ExpressRoutes, IPs, route tables/filters, Virtual WANS, Network Interfaces

GCP: Virtual Private Cloud network, Network Services, Hybrid Connectivity, Network Service Tiers, network security

Common Criteria for Cloud Security Audits

Database

AWS: RDS, DynamoDB, ElastiCache, Neptune, Amazon Redshift, Amazon QLDB, Amazon DocumentDB

Azure: SQL DB, Azure DB for PostGres/MariaDB, Redis, SQL Elastic pools, Cosmos DB

GCP: Datastore, BigQuery, MongoDB, PostgreSQL

Enter Cloud Security Suite

One-stop tool for auditing the security posture of AWS/GCP/Azure infrastructure

Gathers and presents unified information from the following tools:

- GScout
- Scout2
- Prowler
- Lynis
- Azure Audit template

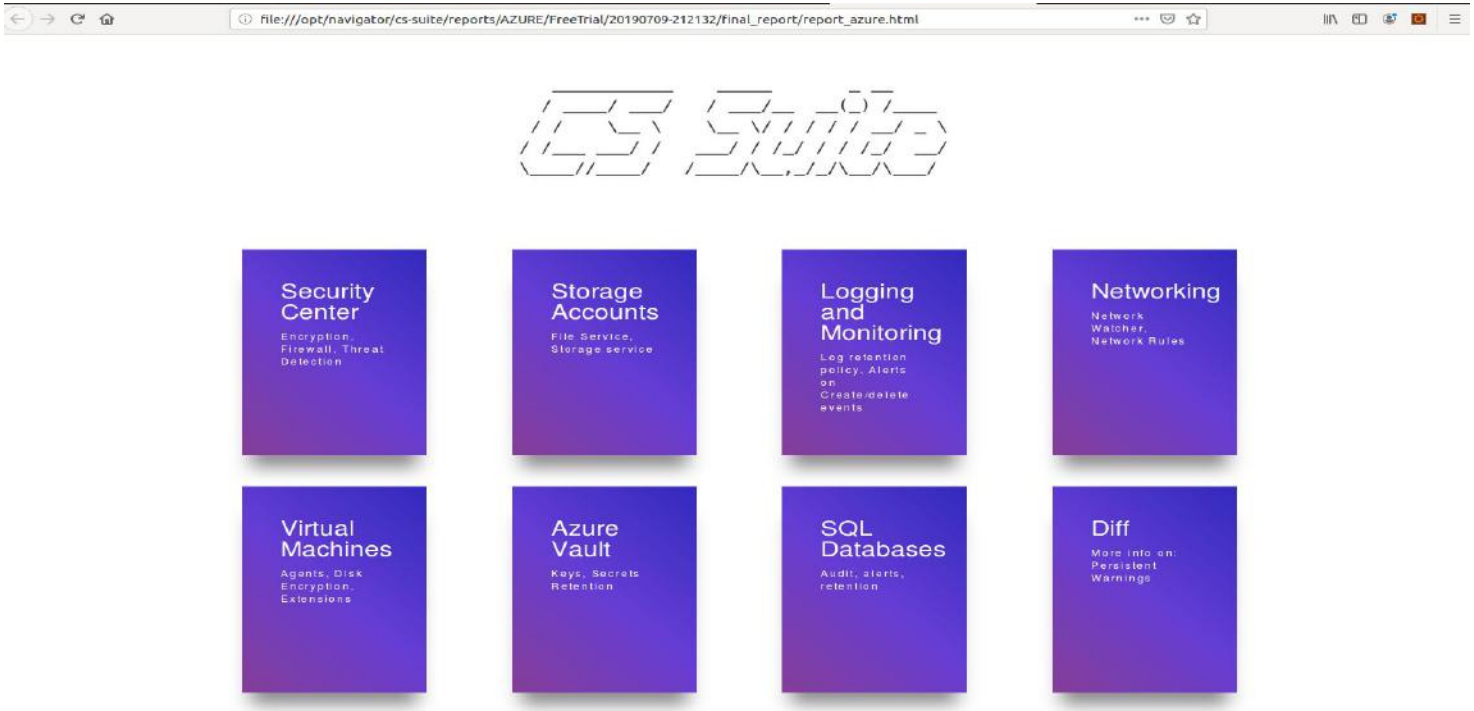
```
└── # python cs.py -h
usage: cs.py [-h] -env {aws,gcp,azure} [-aip AUDIT_IP] [-u USER_NAME]
             [-pem PEM_FILE] [-p] [-pId PROJECT_ID] [-az_u AZURE_USER]
             [-az_p AZURE_PASS] [-o OUTPUT] [-w]

this is to get IP address for lynis audit only

optional arguments:
  -h, --help            show this help message and exit
  -env {aws,gcp,azure}, --environment {aws,gcp,azure}
                        The cloud on which the test-suite is to be run
  -aip AUDIT_IP, --audit_ip AUDIT_IP
                        The IP for which lynis Audit needs to be done .... by
                        default tries root/Administrator if username not
                        provided
  -u USER_NAME, --user_name USER_NAME
                        The username of the user to be logged in,for a
                        specific user
  -pem PEM_FILE, --pem_file PEM_FILE
                        The pem file to access to AWS instance
  -p, --password        hidden password prompt
  -pId PROJECT_ID, --project_id PROJECT_ID
                        Project ID for which GCP Audit needs to be run. Can be
                        retrivied using `gcloud projects list`
  -az_u AZURE_USER, --azure_user AZURE_USER
                        username of azure account, optionally used if you want
                        to run the azure audit with no user interaction.
  -az_p AZURE_PASS, --azure_pass AZURE_PASS
                        username of azure password, optionally used if you
                        want to run the azure audit with no user interaction.
  -o OUTPUT, --output OUTPUT
                        writes a log in JSON of an audit, ideal for
                        consumptions into SIEMS like ELK and Splunk. Defaults
                        to cs-audit.log
  -w, --wipe            rm -rf reports/ folder before executing an audit
```

Installation

Github https://github.com/SecurityFTW/cs-suite

- We **modified** the original project to produce output logs that can be ingested by major SIEM frameworks.
- You will need **CLI** tools, accounts with **read** privileges, and an API **token** for authentication, in some cases.
- Your **vision** may vary, depending on **segmented** resources and organizational architecture.
- The tool, however, presents a **nice report** category interface.

Azure Security Benchmarks



GCP Security Benchmark

File | /Users/rsoto/Desktop/cs-suite/reports/GCP/splunk-research/20190710-105328/SSH%20Port%20Open%20to%...

Apps | Okta | Splunk | service portal | Pwny Portal | Reference Manual... | splunk-ext - Sign In | Phantom | Phantom Commun... | GitHub - phantom...

Network | Service Account | Firewall | Bucket | Role | SQL Instance | Compute Engine

The following entities were found to be in violation of this rule: SSH Port Open to All

default-allow-ssh

```
network: "https://www.googleapis.com/compute/v1/projects/splunk-research/global/networks/default"
```

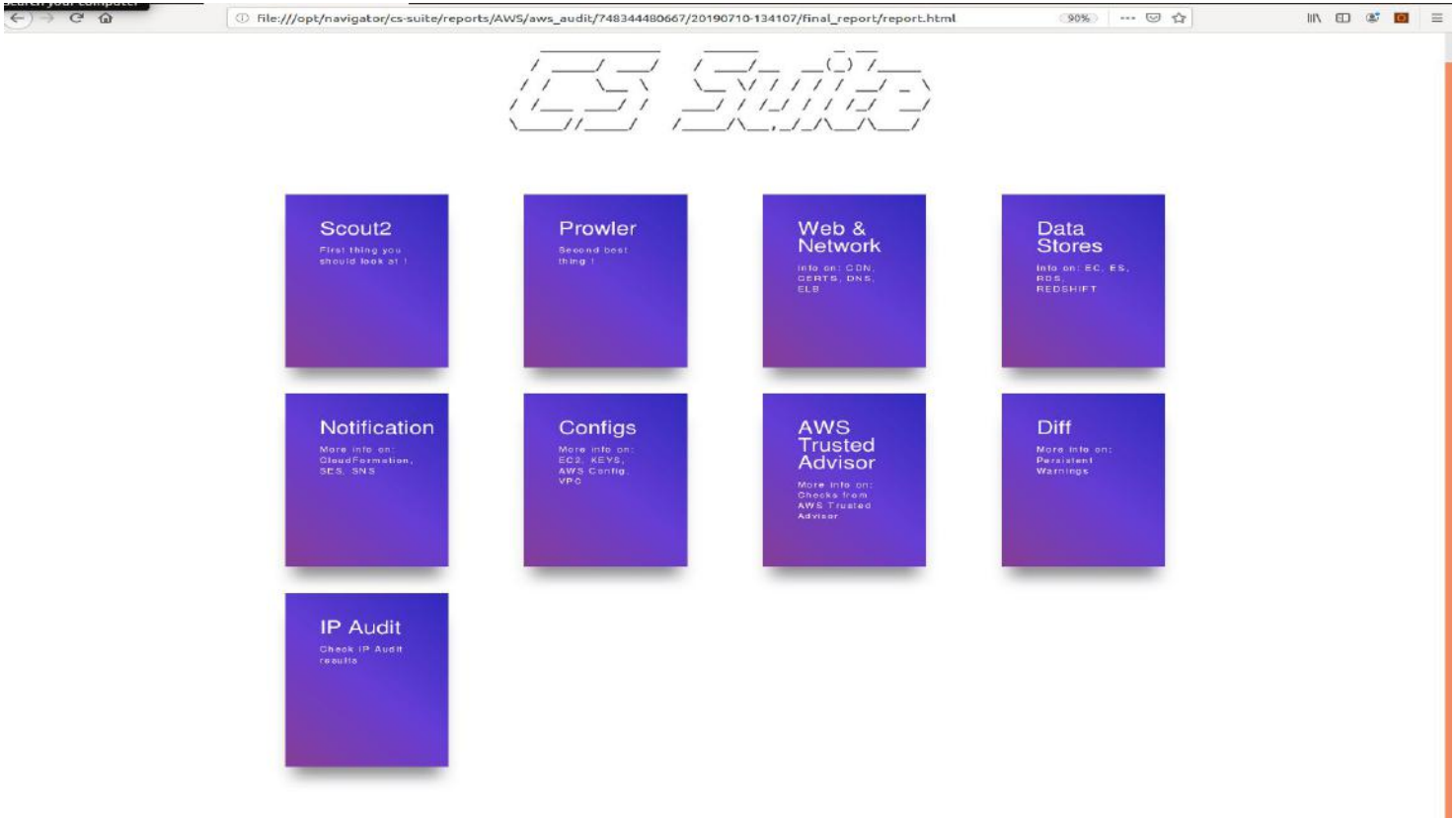
```
sourceRanges: [
    "0.0.0.0/0"
]
```

```
direction: "INGRESS"
```

```
destinationRanges:
```

```
allowed: [
    {
        "IPProtocol": "tcp",
        "ports": [
```

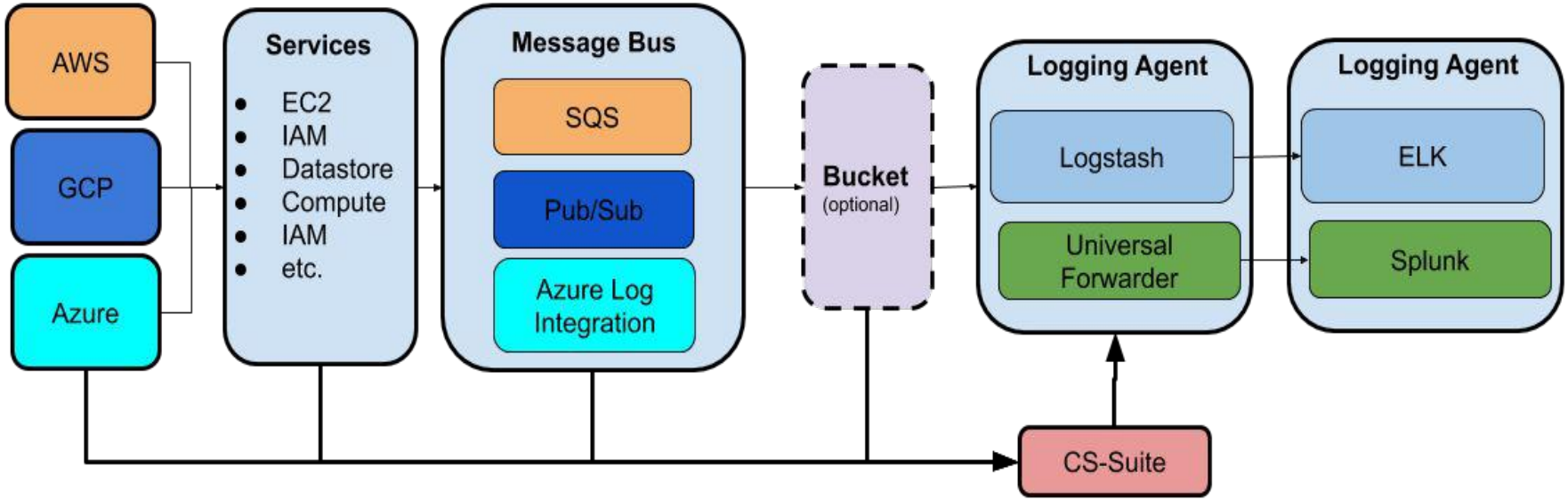
AWS Security Benchmarks



The Challenge Of Getting All These Sources Together...

- Logging in the cloud costs **$** and requires **time** for setup. It is not provided by default (CloudTrail, Stackdriver, Azure Monitor, GCP Stackdriver).
- A log **indexing** and **data streaming** pipeline infrastructure (Splunk/ELK) needs to be present.
- Architecture of **streaming** and **storage**
- A framework that allows **analysis** and further knowledge operation (basically SIEM).
- Most of the cloud providers have **JSON** output. Not all monitoring logs are in JSON file, but enough to get a first comprehensive approach.

Architectural Diagram



Integration with popular SIEMS Splunk/ELK

- Based on the common criteria items we can create **knowledge objects** that can allow the analyst have a better vision on cloud security resources
- Things such as **dashboards**, reports can help analysts make sense of the onslaught of logs coming from such disparate sources
- We can then create **alerts**, lookups and even SOAR **playbooks** that can help us **automate** from the onslaught of logs.

ELK

filebeat.yml+ buffers

```yaml
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /Users/jhernandez/workspace/cs-suite/cs-audit.log
  json.keys_under_root: true
  json.add_error_key: true
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: true
setup.template.settings:
  index.number_of_shards: 1
setup.kibana:
output.elasticsearch:
    hosts: ["http://xxxxxx:9200"]
processors:
  - add_host_metadata: ~
```

Discover

New Save Open Share Inspect

Filters 1 data.type:"WARNING" KQL Aug 4, 2019 @ 20:47:00.0 → Aug 4, 2019 @ 20:48:00.0 Refresh

filebeat-*

Selected fields

? _source

Available fields

@timestamp
t _id
t _index
_score
t _type
t agent.ephemeral_id
t agent.hostname
t agent.id
t agent.type
t agent.version

? **category**

Top 5 values in 35 / 35 records

management	62.9%
security	25.7%
network	11.4%

Aug 4, 2019 @ 20:47:00.000 - Aug 4, 2019 @ 20:48:00.000 — Auto

Time	_source
Aug 4, 2019 @ 20:47:10.799	@timestamp: Aug 4, 2019 @ 20:47:10.799 category: management data: { "region": "us-east-1", "value": "No CloudWatch group found for CloudTrail events", "score": "Scored", "type": "WARNING", "check_no": "3.2", "level": "Level 1" } timestamp: 2019-08-05T00:47:07.167563Z name: cs-audit log.file.path: /Users/jhernandez/workspace/cs-suite/cs-audit.log log.offset: 598,447 message: aws prowler report check: Ensure a log metric filter and alarm exist for Management Console sign-in without MFA (Scored) level: INFO input.type: log ecs.version: 1.0.1 host.architecture: x86_64

Expanded document View surrounding documents View single document

Table JSON

⏲	@timestamp	Aug 4, 2019 @ 20:47:10.799
t	_id	H0E-X2wBmXST5oAxlaOe
t	_index	filebeat-7.3.0-2019.08.04-000001
#	_score	-
t	_type	_doc

Visualize / Create

Save Share Inspect Refresh

Filters data.type:"WARNING" KQL Aug 4, 2019 @ 20:47:10.79 → Aug 4, 2019 @ 20:47:10.80 Refresh

+ Add filter

filebeat-*

Data Metrics & Axes Panel Settings

Metrics

Y-axis Count

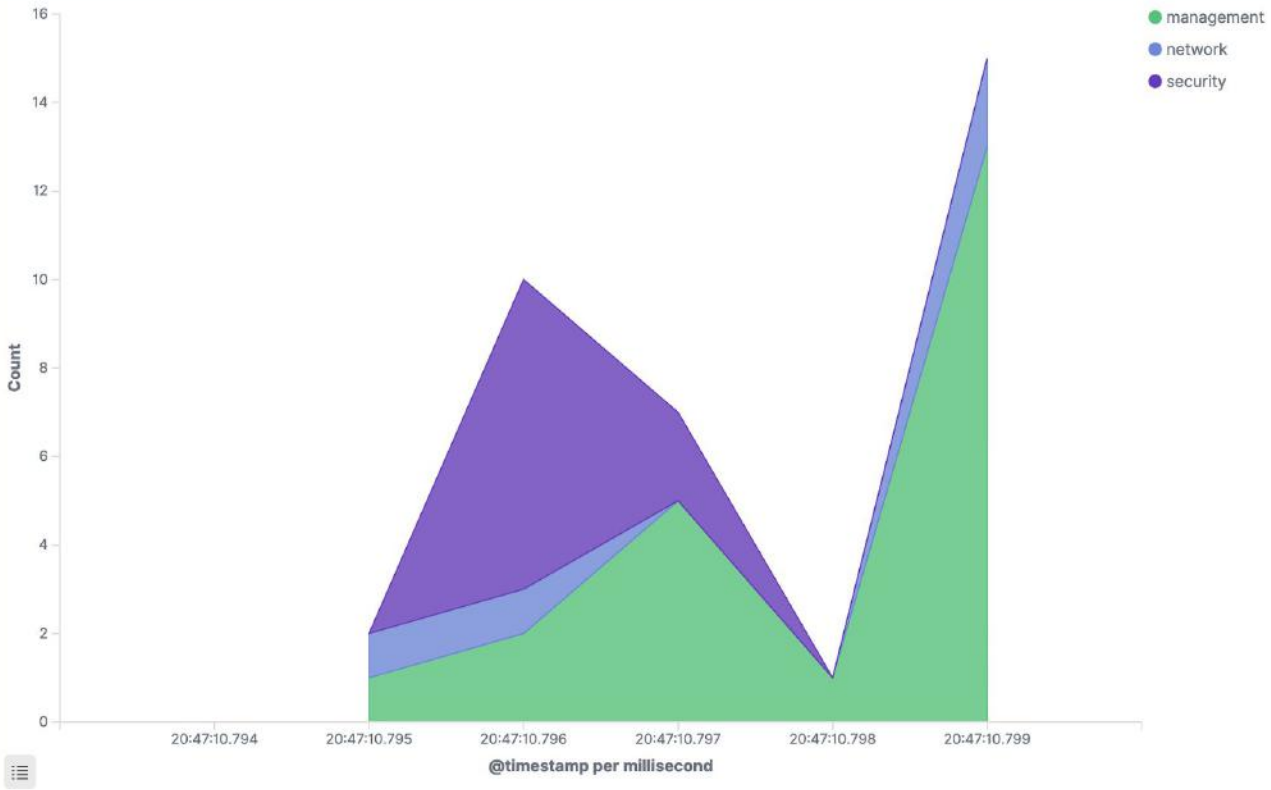
Add

Buckets

X-axis @timestamp per mil...

Split series category: Desc...

Add



Splunk

splunk>enterprise App: Search & Reporting ▾ jhernandez ▾ 4 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As ▾ Close

```
sourcetype="cs-suite" type="WARNING" OR data{}.type="WARNING" | replace "Compute Engine" WITH compute IN category | replace "Firewall" WITH network IN category | replace "Network" WITH network IN
    category | replace "Role" WITH security IN category | replace "Subnet" WITH network IN category | eval service=case(message LIKE "aws%", "AWS", message LIKE "gcp%", "GCP", message LIKE "azure%",
    "AZURE") | search service=AWS | rename data{}.value as value
```

Last 1 day ▾

✓ 315 events (7/31/19 3:21:16.000 PM to 8/1/19 3:21:16.000 PM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events (315) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 20 Per Page ▾ ‹ Prev 1 2 3 4 5 6 7 8 ... Next ›

‹ Hide Fields ☰ All Fields

SELECTED FIELDS
a category 3
a check 35
a host 1
a service 1
a source 1
a sourcetype 1
a value 100+

INTERESTING FIELDS
data{}.check_no 31
a data{}.level 3
a data{}.region 16
a data{}.score 1
a data{}.type 3
date_hour 7
date_mday 2
date_minute 4
a date_month 2
date_second 9

i	Time	Event
>	8/1/19 3:02:01.446 PM	


```
{ [-]
  category: management
  check: Ensure CloudTrail is enabled in all regions (Scored)
  data: [ [-]
    { [-]
      check_no: 2.1
      level: Level 1
      region: us-east-1
      score: Scored
      type: WARNING
      value: AWSMacieTrail-DO-NOT-EDIT trail in us-east-1 is not enabled in multi region mode
    }
    { [-]
      check_no: 2.1
      level: Level 1
      region: us-east-1
      score: Scored
      type: PASS
      value: honeypot-s3 trail in us-east-1 is enabled for all regions
    }
```

Cloud Security

Edit Export ...

Cloud security alert reports

Azure Audit

Azure Warnings

message	value	type
azure report	Please manually check for approval for these extensions ['LinuxDiagnostic', 'AADLoginForLinux']	WARNING
azure report	The VM test27MS does not have DATA DISK ENCRYPTION enabled	WARNING
azure report	The VM test27MS does not have OS DISK ENCRYPTION enabled	WARNING
azure report	Network Watcher is not enabled for your account	WARNING
azure report	There is currently no RETENTION policy applied to the LOG PROFILE	WARNING
azure report	There is currently no LOG PROFILE enabled	WARNING
azure report	Security Phone Contact is NOT SET	WARNING
azure report	Please manually check for approval for these extensions ['LinuxDiagnostic', 'AADLoginForLinux']	WARNING
azure report	The VM test27MS does not have DATA DISK ENCRYPTION enabled	WARNING
azure report	The VM test27MS does not have OS DISK ENCRYPTION enabled	WARNING
azure report	Network Watcher is not enabled for your account	WARNING
azure report	There is currently no RETENTION policy applied to the LOG PROFILE	WARNING
azure report	There is currently no LOG PROFILE enabled	WARNING
azure report	Security Phone Contact is NOT SET	WARNING
azure report	Please manually check for approval for these extensions ['LinuxDiagnostic', 'AADLoginForLinux']	WARNING
azure report	The VM test27MS does not have DATA DISK ENCRYPTION enabled	WARNING
azure report	The VM test27MS does not have OS DISK ENCRYPTION enabled	WARNING
azure report	Network Watcher is not enabled for your account	WARNING
azure report	There is currently no RETENTION policy applied to the LOG PROFILE	WARNING
azure report	There is currently no LOG PROFILE enabled	WARNING

Cloud Security Overview

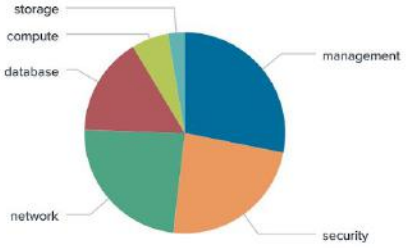
Edit Export ...

Overview of ALL Cloud Providers security posture

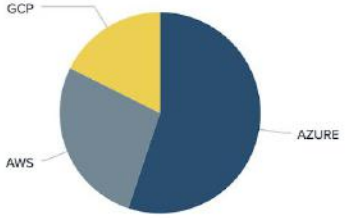
GCP checks	GCP checks	AWS checks	AWS check	Azure Check	AZURE Check
PASSED	**FAILED**	**PASSED**	**FAILED**	**PASSED**	**FAILED**
224	49	144	280	504	126

13m ago

Category

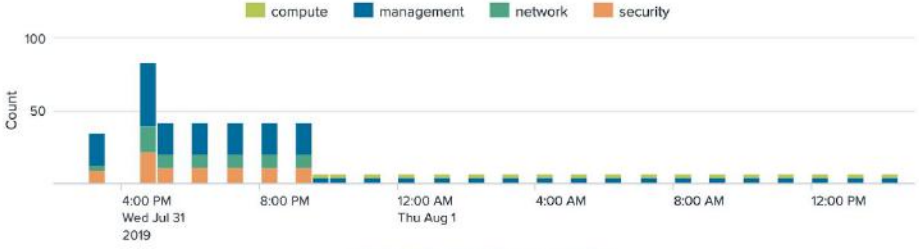


Cloud Providers



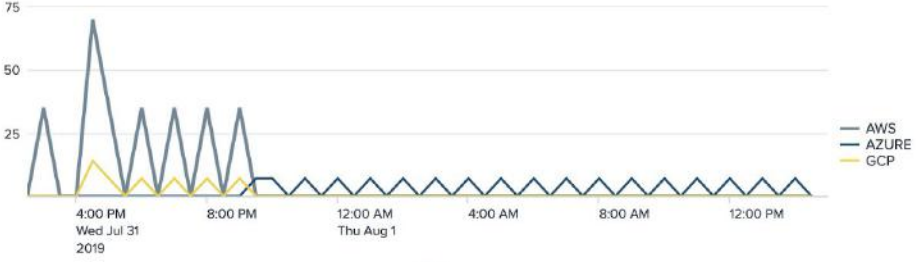
Security Category Across Providers

Failed checks over Time



Cloud Providers

Failed checks over Time



service	category	check	value	failed
AWS	management	VPC_AUDIT	VPC peering is not being used	126
AWS	network	DNS_AUDIT	Zone Z369YJTWBABSRQ does not have SPF records	126
AWS	management	EC2_AUDIT	List of servers which are not associated with IamInstanceProfile i-0214f3461d8233f89 i-0d215b965a3da9349	9
AWS	management	EC2_AUDIT	List of servers which are not associated with IamInstanceProfile i-032cca8fb4ba4edec i-04a190e3ce4d25077 i-0362d95285997f26c i-06cb4ed0d3c243625	9
AWS	management	EC2_AUDIT	List of servers which are not associated with IamInstanceProfile i-076b66a3c694f1bf2 i-0768634fa406c35ad i-0801bc23165219b23 i-09c953058ea2501d7 i-0e0beab03e9ce2c2f i-0c0545b0d2b9b995f i-01a61f61060427e93 i-091112a9022161fbd i-00200b0477e69a139 i-04f99731a2635615d i-0534f6e8c378dcab1 i-068d2e41aa2b45ee9 i-0f665f1db22bbf7eb i-049c0d64f4a3d34bb i-06e8c38d461a684c3 i-01b639c78f143cb8d i-0505cc5242663581d i-0a198803ab7bd7f21 i-0c8c413484cb4ab22 i-04367818f89def447 i-096990e79cb4f3e25 i-07f3e91c3e0a84afb i-0f797df509aef05fe i-05ef1782c9d6f4d59 i-0ba82e44961b83292 i-0369d190c6819e3f2 i-09214304072cacaef i-0e3a9c9b0680b256e i-0a85179f5b3db3399 i-0e21214b62e2f2d42 i-03ad46b3614f69c2a i-086d3c84d5f9871f0 i-08da33d259d0f43ed i-09c2f5bb0428fbfe8	9
AWS	management	EC2_AUDIT	List of servers which are not associated with IamInstanceProfile i-0fd9536bc75008fc4 i-09bb0f85f79d3fdb1 i-0c45edae77d43a24f i-0d16f5a7a6d0b3baa i-05a3d61c41b19fafd i-096be2a451c0d4550 i-0bdd4301683739fc9 i-0e68687f113028ac3 i-07ca362e67af6c40d i-04251639cd0fa73ec i-05173c29d334c3024 i-069ebb62ac2293b8b	9
AWS	management	EC2_AUDIT	List of volumes which are not encrypted vol-08c6e0830e7624644 vol-09080ad8588dbae45 vol-08be57dcb9942835a vol-06e6245e5587c143e vol-0db0f4403130d49a9 vol-0787760cbcda96b84 vol-012e0a28becf29788 vol-0cd5f8f6f7831ae10 vol-02223daad40f136a4 vol-0c9da8dd870f0448f vol-03aa7ad25c6490503 vol-00544cbefaa324a3e vol-0ed5c00b95bdd0f25 vol-0ea3acd44562bc6cb vol-0adfcdf2c7873460c vol-00c24c617577a8ada vol-0c4023fb87b7c838e vol-034b976fd831adf0e vol-0566bad152bc4a7b0 vol-02db2830d8255e49b vol-02891fff6db2dcaa7 vol-071d738e79284035c vol-0d95f64ba07048b38 vol-01e6bc3c9624ecfda vol-00b1ad660557f37c4 vol-07d6f6906a4088a0e vol-05ccd5a5538ede24a vol-0b106021be382a72b vol-049332d21ec5e78e5 vol-052793cf160314b61 vol-07b1f2657da5eb0d1 vol-07d4c08abc45c3be8 vol-096532deb3cd9241a vol-0cfc3400ed9e5e91d vol-08c9432fa9dc17119 vol-0d0bb967b80cb0efd vol-0eabc7695867e5baa vol-0308689ca1af13500 vol-07cd109db48d8f0f5 vol-041192a8b728cb6c6 vol-07b10fba6b1df9409	9
AWS	management	EC2_AUDIT	List of volumes which are not encrypted vol-0bd8911a48a007884 vol-0aa9cf2d9cc666dd0 vol-0c16e1b50c7555cfb vol-07b89099e4c500722 vol-07ea1ba7c476226bc vol-0a9d2163a5e96bf76 vol-0e460f22d90b98431 vol-03af1cdec0329b8a2 vol-0d593cc46250d66ad vol-028bdd12cef67a811 vol-0c6e5f343863f86a7 vol-0b9171a891a77fb42 vol-0e1a07b90efb0ef90 vol-08510f368b89700e3 vol-0dcd7f5ebf4affb8f vol-03117163bb5a482cb vol-0d7e50dbde4da7bdd vol-070db88e0ab4b5c43 vol-0482e07faac36e980 vol-0af9463c2b8b6791a vol-01942c970916702df vol-01d2e55a5353a5b2b vol-07b374ba17dea5ea7 vol-0615dd99efecb5de9 vol-0d0e90bd5a4619632 vol-00c48720f785d79c6 vol-062f5c66c6d5ec163 vol-06477a662e2865afa	9
AWS	management	EC2_AUDIT	List of volumes which are not encrypted vol-0c903b77ef617073b vol-010c21cf5f91c6450 vol-080d70f5aff00d312 vol-0c3903c9822fd2804 vol-0b3add6a971486e2f vol-0b30b4bbbacb4745e vol-07b302087473d3104 vol-0914aa308684780dd vol-07a9eae44ed0d1a9d vol-06fa08da0faf888d6 vol-07f07cf73317fcf83 vol-08dad905b503cbb0d vol-0e9dbbf36f4cb3968 vol-018f7fd7d77da58b5 vol-0e35c221f63ba439e vol-00dd0a938ad6a90e6 vol-0747c83283a6842e9	9
AWS	management	EC2_AUDIT	List of volumes which are not encrypted vol-0e305cfe902905726 vol-0e6959f2b0cb30304	9
AWS	management	EC2_AUDIT	List of volumes which are not encrypted with KMS key are vol-08c6e0830e7624644 vol-09080ad8588dbae45 vol-08be57dcb9942835a vol-06e6245e5587c143e vol-0db0f4403130d49a9 vol-0787760cbcda96b84 vol-012e0a28becf29788 vol-0cd5f8f6f7831ae10 vol-02223daad40f136a4 vol-0c9da8dd870f0448f vol-03aa7ad25c6490503 vol-00544cbefaa324a3e vol-0ed5c00b95bdd0f25 vol-0ea3acd44562bc6cb vol-0adfcdf2c7873460c vol-00c24c617577a8ada vol-0c4023fb87b7c838e vol-034b976fd831adf0e vol-0566bad152bc4a7b0 vol-02db2830d8255e49b vol-02891fff6db2dcaa7 vol-071d738e79284035c vol-0d95f64ba07048b38 vol-01e6bc3c9624ecfda vol-00b1ad660557f37c4 vol-07d6f6906a4088a0e vol-05ccd5a5538ede24a vol-0b106021be382a72b vol-049332d21ec5e78e5 vol-052793cf160314b61 vol-07b1f2657da5eb0d1 vol-07d4c08abc45c3be8 vol-096532deb3cd9241a vol-0cfc3400ed9e5e91d vol-08c9432fa9dc17119 vol-0d0bb967b80cb0efd vol-0eabc7695867e5baa vol-0308689ca1af13500 vol-07cd109db48d8f0f5	9

Save As Alert

Settings

Title: Failed Management Check

Description: $service$ has $count$ failed management checks in the last 1 hour

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

Trigg

r of Results

0

For each result

- **Risk Analysis** — Creates risk modifier events in the risk index
- **Run Playbook in Phantom** — Run a Phantom playbook on this event.
- **Run a script** — Invoke a custom script
- **Searching Domains** — Filter and search specific records using this endpoint. Using simple filter composition, any type of data fetching is possible
- **Send To UBA** — Forwards search results from Splunk Enteprise to UBA

+ Add Actions

Cancel | Save

Q&A

Thank You!

Rod Soto @rodsoto rod@rodsoto.net

Jose Hernandez @d1vious josehelps.com