



Tales from a detection engineering in AWSLand

Rodrigo Montoro

Head of Threat & Detection Research

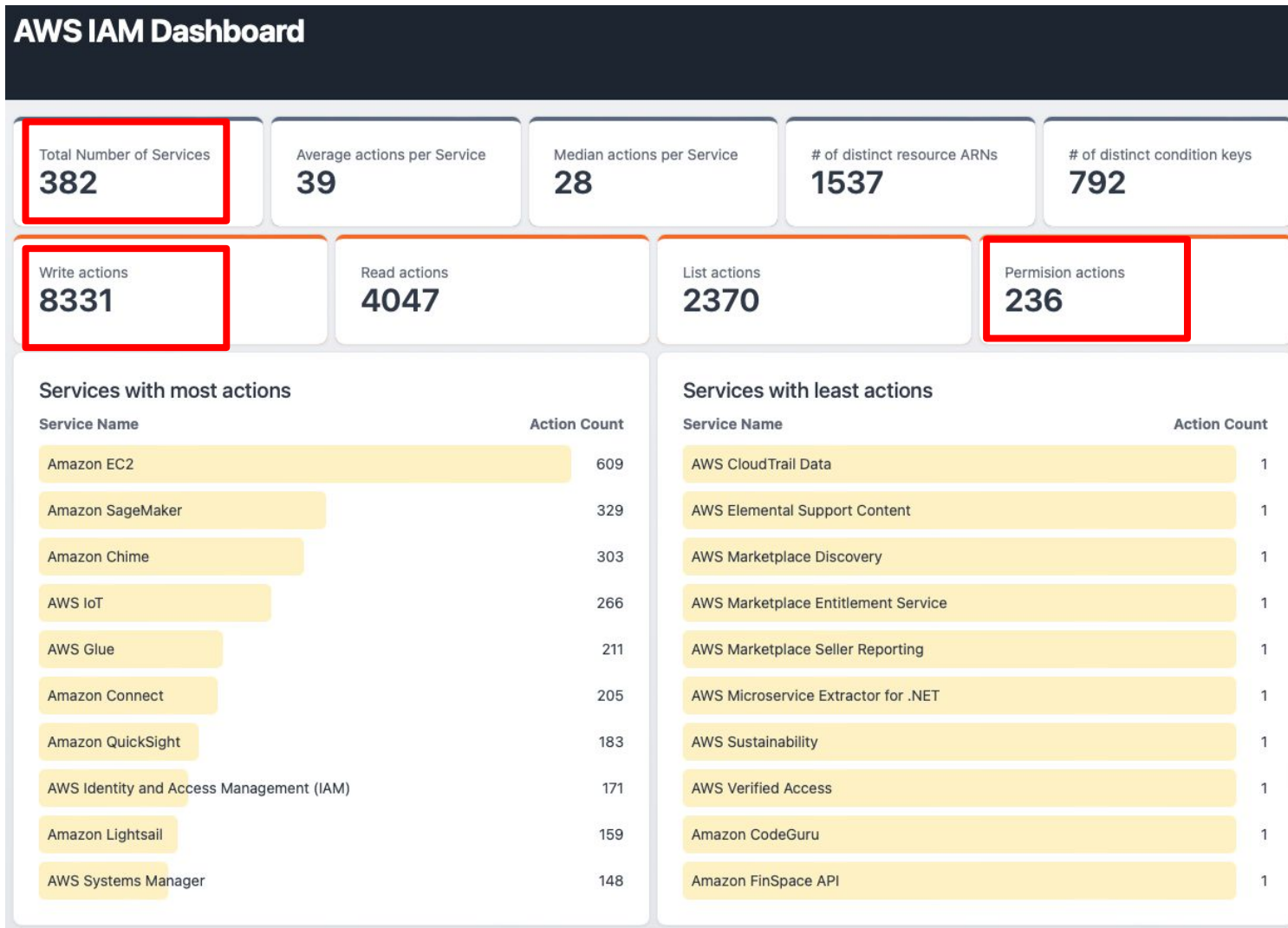
@spookerlabs

<https://linkedin.com/in/spooker>

\$ aws --profile **Rodrigo Montoro** sts get-caller-identity

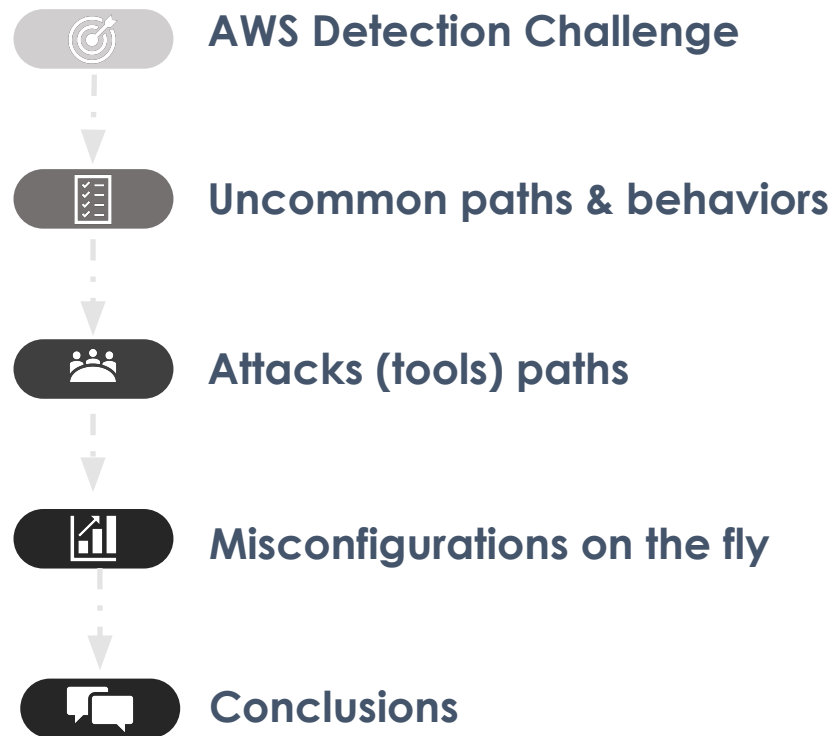
Clavis Segurança da Informação

- **Head of Threat & Detection Research** at Clavis Security
- Living in **Florianópolis** (Silicon Island)
- Author of **2 patented** technologies (US Patent Office)
- **Speaker** in different conferences (**Brazil,USA,Canada**)
- Proud **Dad** and **Husband**
- Full **Ironman** triathlon (**2x**)
- Crossfit and Powerlifting



- Detections from **Elastic rules**
 - **59** detections
 - **~22** services covered (around **5.8%** of services)
- Detections from **Sigma**
 - **31** detections
 - **~20** services covered (around **5.2%** of services)

AGENDA



Clavis Segurança da Informação

AWS Detection Challenge



By AWS itself

Clavis Segurança da Informação

Event pattern [Info](#)

Event source

AWS service or EventBridge partner as source

AWS services

AWS service

The name of the AWS service as the event source

IAM

Event type

The type of events as the source of the matching pattern

AWS API Call via CloudTrail

i All events that are delivered via CloudTrail have **AWS API Call via CloudTrail** as the value for **detail-type**. Events from API actions that start with the keywords List, Get, or Describe are not processed by EventBridge, with the exception of events from the following STS actions: GetFederationToken and GetSessionToken. Data events (for example, for Amazon S3 object level events, DynamoDB, and AWS Lambda) must have trails configured to receive those events. [Learn more.](#)

- ☒ Any operation
☐ Specific operation(s)

Event pattern

Event pattern, or filter to match the events

```
1 {
2   "source": ["aws.iam"],
3   "detail-type": ["AWS API Call via CloudTrail"],
4   "detail": {
5     "eventSource": ["iam.amazonaws.com"]
6   }
7 }
```

Copy

Test pattern

Edit pattern

Monitor changes to IAM

If you're interested only in changes to your IAM account, you can modify the event pattern inside EventBridge, the one you used to set up IAM notifications, with an `eventName` filter pattern, shown following.

```
"eventName": [
  "Add*",
  "Attach*",
  "Change*",
  "Create*",
  "Deactivate*",
  "Delete*",
  "Detach*",
  "Enable*",
  "Put*",
  "Remove*",
  "Set*",
  "Update*",
  "Upload*"
]
```

Customer 1
250 per month

Customer 2
200 per week

Customer 3 15k
in a day

Tactic	Stratus	Attack Technique
Initial Access	1	Console Login without MFA
Execution	2	Launch Unusual EC2 instances Execute Commands on EC2 Instance via User Data
Persistence	7	Backdoor an IAM Role Create an Access Key on an IAM User Create an administrative IAM User Create a Login Profile on an IAM User Backdoor Lambda Function Through Resource-Based Po Overwrite Lambda Function Code Create an IAM Roles Anywhere trust anchor
Privilege Escalation	5	Execute Commands on EC2 Instance via User Data Create an Access Key on an IAM User Create an administrative IAM User Create a Login Profile on an IAM User Create an IAM Roles Anywhere trust anchor
Defense Evasion	6	Delete CloudTrail Trail Disable CloudTrail Logging Through Event Selectors CloudTrail Logs Impairment Through S3 Lifecycle Rule Stop CloudTrail Trail Attempt to Leave the AWS Organization Remove VPC Flow Logs
Credential Access	4	Retrieve EC2 Password Data Steal EC2 Instance Credentials Retrieve a High Number of Secrets Manager secrets Retrieve And Decrypt SSM Parameters
Discovery	2	Execute Discovery Commands on an EC2 Instance Download EC2 Instance User Data
Lateral Movement	0	No Attack Techniques Defined
Collection	0	No Attack Techniques Defined
Exfiltration	5	Open Ingress Port 22 on a Security Group Exfiltrate an AMI by Sharing It Exfiltrate EBS Snapshot by Sharing It Exfiltrate RDS Snapshot by Sharing Backdoor an S3 Bucket via its Bucket Policy
Impact	0	No Attack Techniques Defined
Total	32	



CloudTrail EventName
ConsoleLogin
RunInstances
ModifyInstanceAttribute
UpdateAssumeRolePolicy
CreateAccessKey
CreateUser, AttachUserPolicy, CreateAccessKey
CreateLoginProfile
AddPermission20150331v2
UpdateFunctionCode20150331v2
CreateTrustAnchor
ModifyInstanceAttribute
CreateAccessKey
CreateUser, AttachUserPolicy, CreateAccessKey
CreateLoginProfile
CreateTrustAnchor
DeleteTrail
PutEventSelectors
PutBucketLifecycle
StopLogging
LeaveOrganization
DeleteFlowLogs
GetPasswordData
DescribeInstances
GetSecretValue
GetParameters
SendCommand
DescribeInstanceAttribute
-
-
AuthorizeSecurityGroupIngress
ModifyImageAttribute
ModifySnapshotAttribute
ModifyDBSnapshotAttribute
PutBucketPolicy
-

What about other services ?

Clavis Segurança da Informação

- Appstream 2.0 ?
- AWS Identity Center ?
- AWS Organizations ?
- AWS Clean Rooms ?
- Services with passrole actions ?

And it's not always about control plane

Clavis Segurança da Informação

- S3 buckets data events
- RDS Audit logs
- EKS (Kubernetes)
- VPC Flowlogs



Matt Fuller

Jan 3, 2021 · 16 min read · Member-only · Listen



How to Enable Logging on Every AWS Service in Existence (Circa 2021)



1	Source	Log Type	Destination(s)
2	ACM	Certificate Transparency Logs	Published Publicly
3	API Gateway	Access Logs	CloudWatch Logs
4	Amplify	Access Logs	Download as CSV
5	App Mesh	Access Logs	Sent to Envoy and K8s
6	AppSync	Debug Logs	CloudWatch Logs
7	Aurora	Detailed Activity Logs	Kinesis Data Stream
8	AutoScaling	ASG State Change Events	SNS
9	Audit Manager	Control Activity Logs	Via API or UI
10	Batch	Container Logs	CloudWatch Logs, Splunk, Syslog
11	Chime	SIP Message Logs	CloudWatch Logs
12	CloudFormation	Stack Events	Console
13	CloudFront	Standard Logs	S3
14	CloudFront	Real-Time Logs	Kinesis Data Stream
15	CloudHSM	Audit Logs	CloudWatch Logs
16	CloudTrail	AWS Account Audit Logs	S3, CloudWatch
17	CloudWatch Logs	CloudWatch Logs	ElasticSearch, Lambda, S3
18	CodeBuild	Build Logs	CloudWatch, S3
19	CodeDeploy	Deployment Logs	EC2 Instance
20	Config	Resource Change Events	SQS
21	Connect	Contact Flow Logs	CloudWatch Logs
22	DataPipeline	Pipeline Logs	S3
23	DataSync	Task Logging	CloudWatch Logs
24	DirectoryService	AWS Managed Microsoft AD Logs	CloudWatch Logs
25	DMS	Migration Logs	CloudWatch Logs
26	DocDB	Profiler Logs	CloudWatch Logs
27	DynamoDB	Stream of Table Changes	Kinesis Data Stream
28	EC2	Instance Logs	CloudWatch Logs
29	ECS	Container Logs	CloudWatch Logs, Splunk, Fluentd, Syslog, Firelens
30	EKS	Control Plane Logs	CloudWatch Logs

Clavis Segurança da Informação

Uncommon paths & behaviors



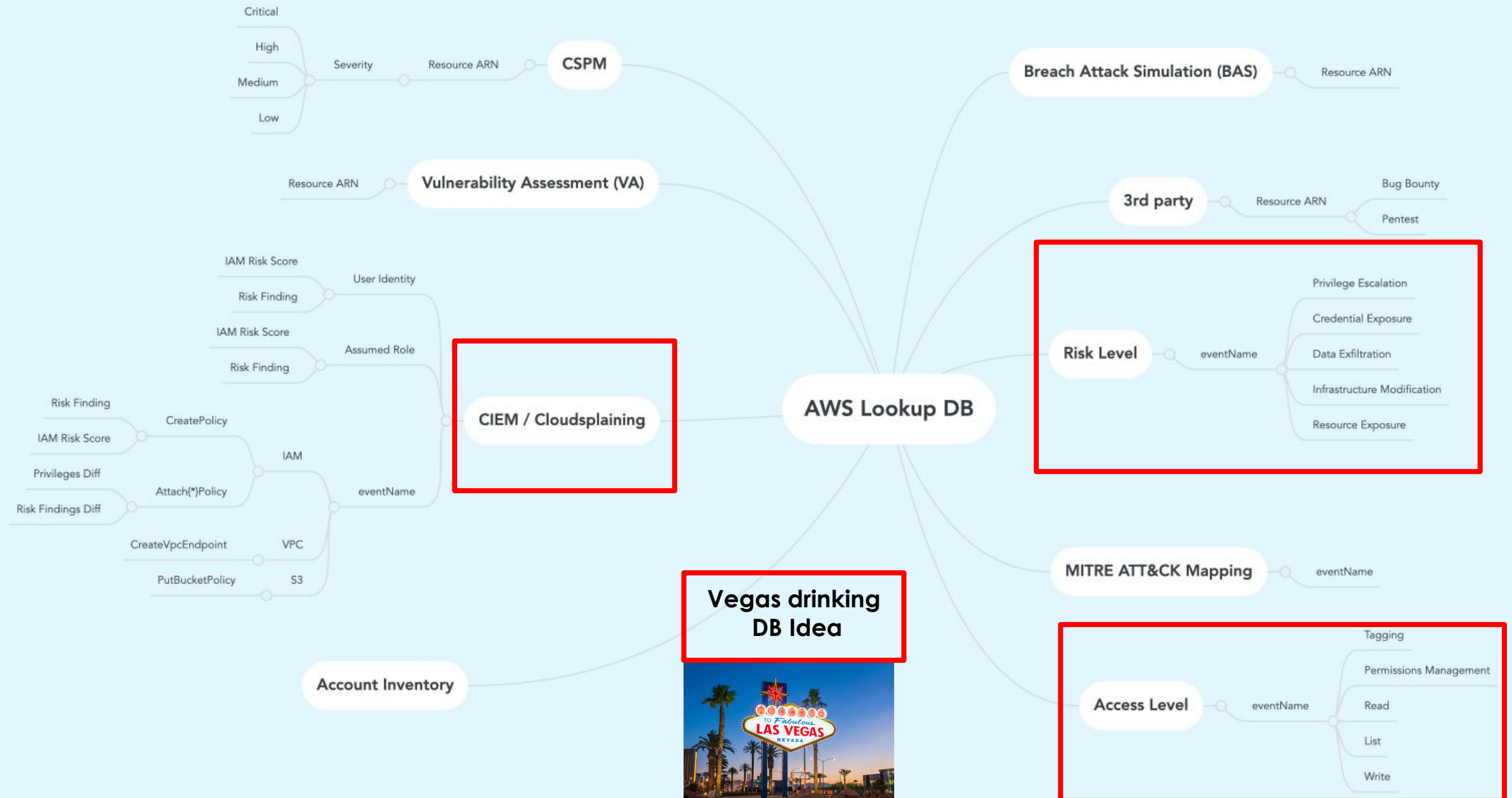
Clavis Segurança da Informação

```

1  {
2    "eventVersion": "1.08"
3    "userIdentity": {
4      "type": "IAMUser",
5      "principalId": "AIDAZXQAMD324RWODNQX",
6      "arn": "arn:aws:iam::668941950455:user/awslandadmin",
7      "accountId": "668941950455",
8      "accessKeyId": "ASIAZXQAMD3WVLYX5M4",
9      "userName": "awslandadmin",
10     "sessionContext": {
11       "sessionIssuer": {},
12       "webIdFederationData": {},
13       "attributes": {
14         "creationDate": "2023-08-04T05:17:38Z",
15         "mfaAuthenticated": "true"
16       }
17     }
18   },
19   "eventTime": "2023-08-04T05:19:41Z",
20   "eventSource": "iam.amazonaws.com",
21   "eventName": "CreatePolicy",
22   "awsRegion": "us-east-1",
23   "sourceIPAddress": "187.112.73.165",
24   "userAgent": "AWS Internal",
25   "requestParameters": {
26     "policyDocument": "{\n\t\t\"Version\": \"2012-10-17\",\n\t\t\"Statement\":\n\t\t[\n\t\t\t{\n\t\t\t\t\"Sid\": \"VisualEditor0\",\n\t\t\t\t\"Effect\": \"Allow\",\n\t\t\t\t\"Action\": [\n\t\t\t\t\t\"iam:PassRole\",\n\t\t\t\t\t\"ec2:*\"\n\t\t\t\t],\n\t\t\t\t\"Resource\": \"*\"\n\t\t\t}\n\t\t]\n\t\t}",
27     "tags": [],
28     "description": "",
29     "policyName": "awslandPolicy"
30   },
31 }

```

How to enrich ?



- Over Permissive Policies
 - **Name** based / **Analysis** based
- Access Level or Risk Level Ratio
 - Console / Terraform / PACU / AWS Cli
- Spike of eventSource
 - Avg eventSource per identity arn (**hour, day, month**)
- First Time Seen (based on **user.identity**)
 - eventSource
 - eventSource + eventName
 - eventSource + access level
 - assume a role with permissive policy attached

Over permissive policies (pattern matching)

Clavis Segurança da Informação

JSON view

PolicyName	"ServicesAffected"	"Pri"
AdministratorAccess	201	
IAMFullAccess	1	
AdministratorAccess-Amplify	19	
AmazonDynamoDBFullAccesswithDataPipeline	8	
PolicyName		
AdministratorAccess		
IAMFullAccess		
AdministratorAccess-Amplify		
AmazonDynamoDBFullAccesswithDataPipeline		
AWSElasticBeanstalkFullAccess		
AmazonElasticMapReduceFullAccess		
PowerUserAccess		
AWSDataPipelineRole		
AWSGlueConsoleFullAccess		
AWSGlueConsoleSageMakerNotebookFullAccess		
AWSGlueServiceNotebookRole		
AWSGlueServiceRole		
AWSLambda_FullAccess		
AmazonElasticMapReduceRole		
DataScientist		
SystemAdministrator		
AWSAppMeshServiceRolePolicy	0	
AWSAppRunnerFullAccess	2	
AWSAppRunnerReadOnlyAccess	0	
AWSAppRunnerServicePolicyForECRAccess	4	
AWSAppSyncAdministrator	2	
AWSAppSyncInvokeFullAccess	1	

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAZXQAMD324RWODNQX",
    "arn": "arn:aws:iam::668941950455:user/awslandadmin",
    "accountId": "668941950455",
    "accessKeyId": "ASIAZXQAMD3WXSZL4US",
    "userName": "awslandadmin",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-08-04T17:23:55Z",
        "mfaAuthenticated": "true"
      }
    }
  },
  "eventTime": "2023-08-04T17:24:30Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "AttachUserPolicy",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "187.112.73.165",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "userName": "awslandpacu",
    "policyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
  },
  "responseElements": null
}
```

Over permissive policies (Analysis)

Clavis Segurança da Informação

```
1- {
2   "eventVersion": "1.08",
3   "userIdentity": {
4     "type": "IAMUser",
5     "principalId": "AIDAZXQAMD324RWODN9X",
6     "arn": "arn:aws:iam::668941950455:user/awslandadmin",
7     "accountId": "668941950455",
8     "accessKeyId": "ASIAZXQAMD3WVLYX5M4",
9     "userName": "awslandadmin",
10    "sessionContext": {
11      "sessionIssuer": {},
12      "webIdFederationData": {},
13      "attributes": {
14        "creationDate": "2023-08-04T05:17:38Z",
15        "mfaAuthenticated": "true"
16      }
17    }
18  }
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "ec2:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Potential Issue found: Policy is capable of Privilege Escalation

Method: CreateEC2WithExistingIP
Actions: iam:passrole, ec2:runinstances

Potential Issue found: Policy is capable of Resource Exposure

Actions: ec2:CreateNetworkInterfacePermission, ec2:DeleteNetworkInterfacePermission, ec2:ModifySnapshotAttribute, ec2:ModifyVpcEndpointServicePermissions, ec2:ResetSnapshotAttribute, iam:PassRole

Potential Issue found: Policy allows ALL Actions from a service (like service:*)

Actions: ec2

Potential Issue found: Policy allows actions that return credentials

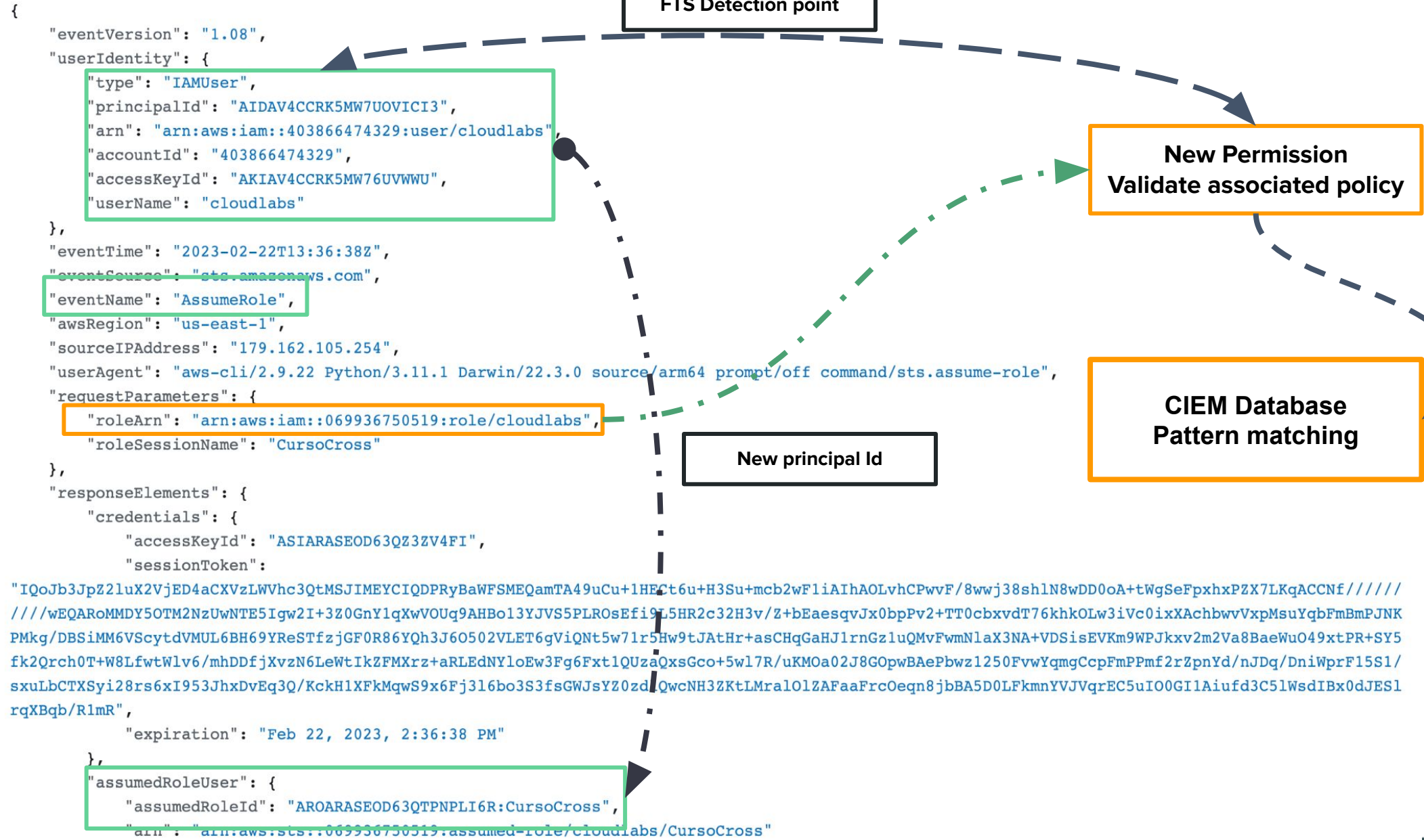
Actions: ec2:GetPasswordData

Potential Issue found: Policy is capable of Unrestricted Infrastructure Modification

Actions: ec2:AcceptTransitGatewayMulticastDomainAssociations, ec2:AcceptTransitGatewayPeeringAttachment, ec2:AcceptTransitGatewayVpcAttachment, ec2:AcceptVpcEndpointConnections, ec2:AcceptVpcPeeringConnection, ec2:AllocateAddress, ec2:AllocateHosts, ec2:AllocateIpamPoolCidr, ec2:ApplySecurityGroupsToClientVpnTargetNetwork, ec2:AssignIpv6Addresses, ec2:AssignPrivateIpAddresses, ec2:AssociateAddress, ec2:AssociateClientVpnTargetNetwork, ec2:AssociateDhcpOptions, ec2:AssociateEnclaveCertificateIamRole, ec2:AssociateIamInstanceProfile, ec2:AssociateInstanceEventWindow, ec2:AssociateRouteTable, ec2:

FTS (Assuming permissive role)

Clavis Segurança da Informação



IAM Access Analyzer policy generation

[PDF](#) | [RSS](#)

As an administrator or developer, you might grant permissions to IAM entities (users or roles) beyond what they require. IAM provides several options to help you refine the permissions that you grant. One option is to generate an IAM policy that is based on access activity for an entity. IAM Access Analyzer reviews your AWS CloudTrail logs and generates a policy template that contains the permissions that the entity used in your specified date range. You can use the template to create a policy with fine-grained permissions that grant only the permissions that are required to support your specific use case.

How policy generation works

IAM Access Analyzer analyzes your CloudTrail events to identify actions and services that have been used by an IAM entity (user or role). It then generates an IAM policy that is based on that activity. You can refine an entity's permissions when you replace a broad permissions policy attached to the entity with the generated policy. The following is a high-level overview of the policy generation process.

Vegas drinking DB idea (2/2)

Clavis Segurança da Informação

Generated policy

1

2

3

Customize permissions

Review the following policy template. You must specify resources for actions that support resource-level permissions to continue creating the policy.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "access-analyzer:ValidatePolicy",  
8         "iam:GetAccountPasswordPolicy",  
9         "iam:GetAccountSummary",  
10        "iam:ListAccountAliases",  
11        "iam:ListGroups",  
12        "iam:ListPolicies",  
13        "iam:ListRoles",  
14        "iam:ListUsers"  
15      ],  
16      "Resource": "*"   
17    },  
18    {  
19      "Effect": "Allow",  
20      "Action": [  
21        "iam:GetRole",  
22        "iam:ListAttachedRolePolicies",  
23        "iam:ListInstanceProfilesForRole",  
24        "iam:ListRolePolicies",  
25        "iam:ListRoleTags"  
26      ],  
27      "Resource": "arn:aws:iam::${Account}:role/${RoleNameWithPath}"  
28    },  
29    {  
30      "Effect": "Allow",  
31      "Action": [  
32        "iam:GetUser",  
33        "iam:ListAccessKeys",  
34        "iam:ListAttachedUserPolicies",  
35        "iam:ListGroupsForUser",  
36        "iam:ListUserTags"  
37      ],  
38      "Resource": "arn:aws:iam::${Account}:user/${UserNameWithPath}"  
39    }  
40  ]  
41 }
```

**Principal
information**

Services

Actions

Access Level

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

Clavis Segurança da Informação

Misconfigurations everywhere



What are misconfigurations ?

Clavis Segurança da Informação

Cloud Misconfiguration – A Major Security Threat

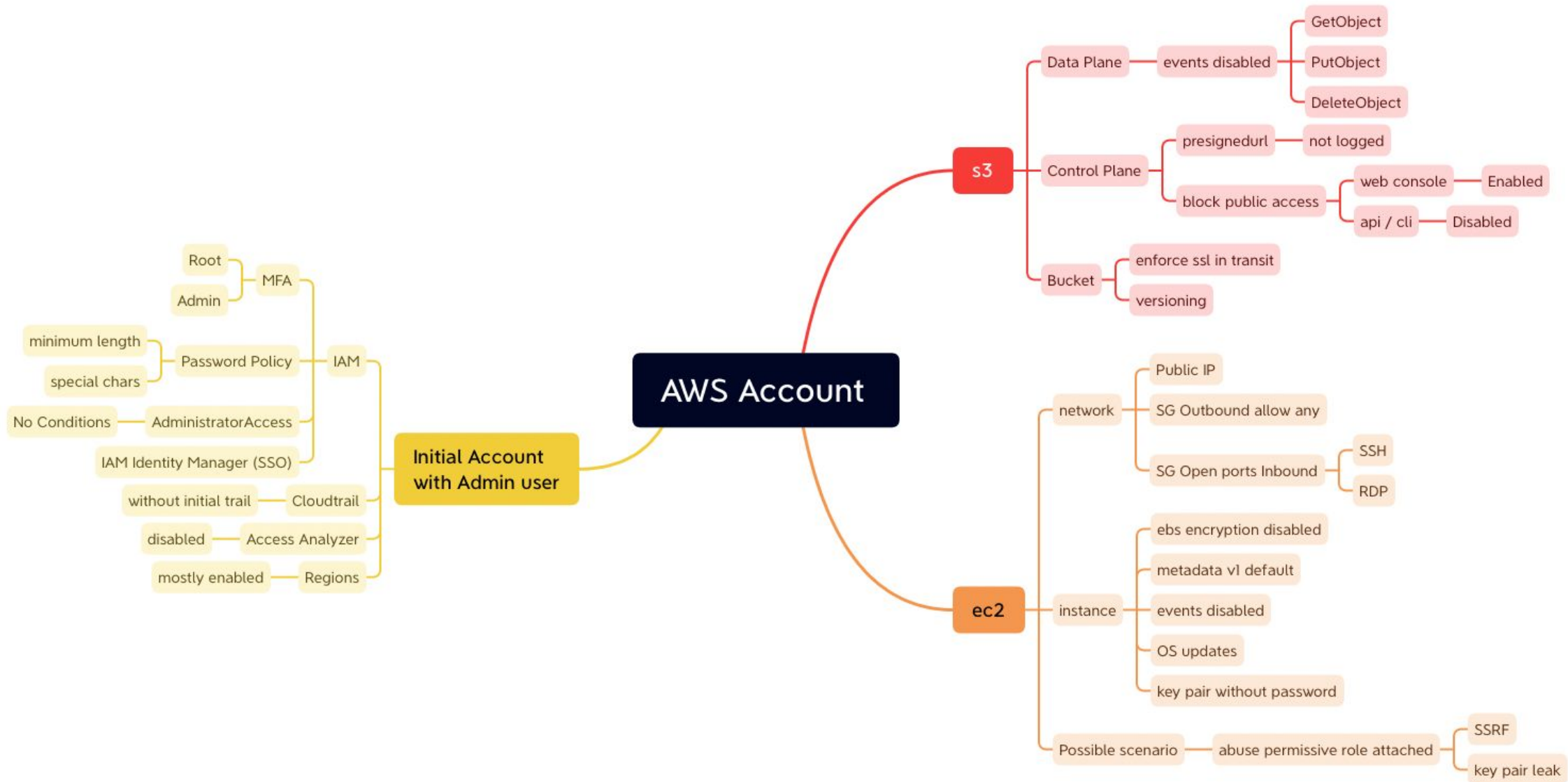
Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption. These [cyber threats](#) come in the form of security breaches, external hackers, [ransomware](#), [malware](#), or [insider threats](#) that use [vulnerabilities](#) to access your network.

The NSA considers cloud misconfiguration a leading vulnerability in a cloud environment. While these risks are often less sophisticated, the issues' prevalence is generally through the roof.

Misconfiguration is a cloud computing problem because multi-cloud environments can be quite complicated, and it can be tough to detect and manually remediate mistakes. According to a Gartner survey, these issues cause [80% of all data security breaches](#), and until 2025, up to [99% of cloud environment failures will be attributed to human errors](#).

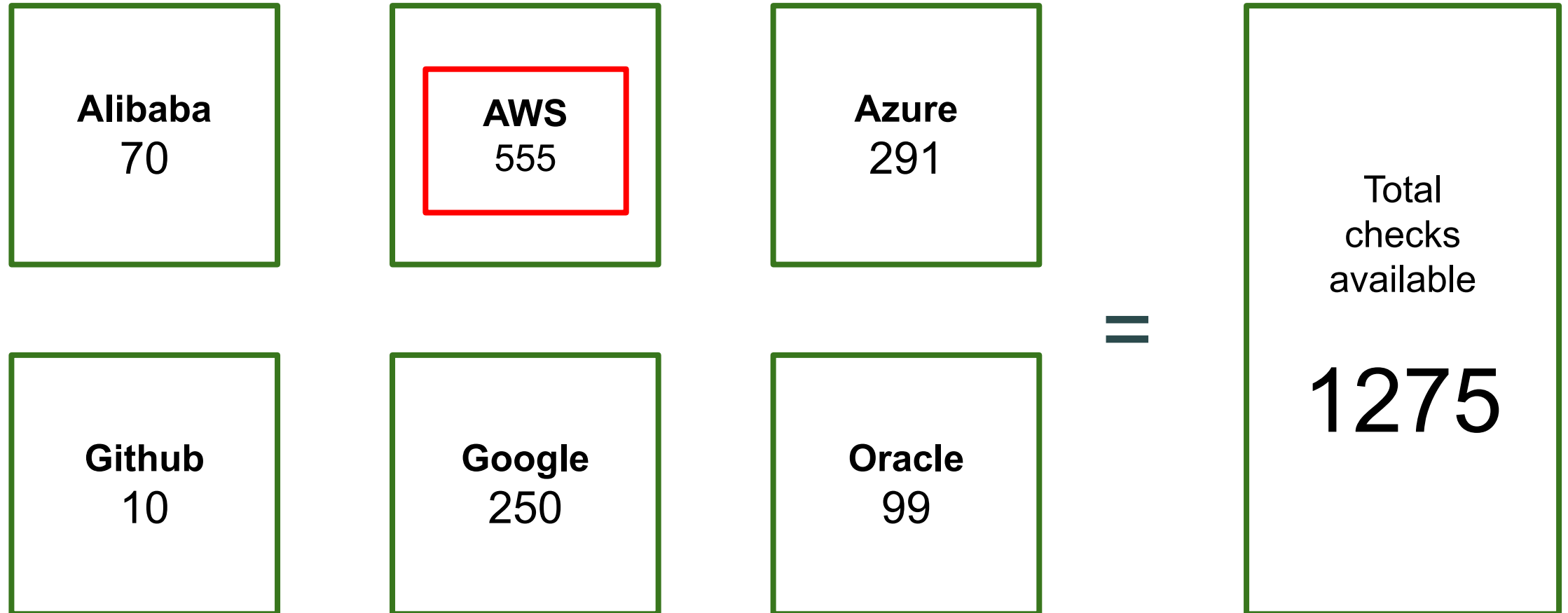
How a misconfiguration shows up? AWS deFAULTS

Clavis Segurança da Informação



Lot of possible opportunities (based on cloudsploit)

Clavis Segurança da Informação



Cloudsploit detection sample

Clavis Segurança da Informação

```
1  var async = require('async');
2  var helpers = require('../../../../helpers/aws');
3
4  module.exports = {
5    title: 'Open All Ports Protocols',
6    category: 'EC2',
7    domain: 'Compute',
8    description: 'Determine if security group has all ports or protocols open to the public',
9    more_info: 'Security groups should be created on a per-service basis and avoid allowing all ports or protocols.',
10   link: 'http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html',
11   recommended_action: 'Modify the security group to specify a specific port and protocol to allow.',
12   apis: ['EC2:describeSecurityGroups', 'EC2:describeNetworkInterfaces', 'Lambda:listFunctions'],
13   settings: {
14     ec2_skip_unused_groups: {
15       name: 'EC2 Skip Unused Groups',
16       description: 'When set to true, skip checking ports for unused security groups and produce a WARN result',
17       regex: '^(true|false)$',
18       default: 'false',
19     },
20   },
21   compliance: {
22     hipaa: 'HIPAA requires strict access controls to networks and services ' +
23       'processing sensitive data. Security groups are the built-in ' +
24       'method for restricting access to AWS services and should be ' +
25       'configured to allow least-privilege access.',
26     pci: 'PCI has explicit requirements around firewalled access to systems. ' +
27       'Security groups should be properly secured to prevent access to ' +
28       'backend services.'
29   },
30 }
```

Why not detecting in real time ?

Clavis Segurança da Informação

```
"responseElements": {
  "requestId": "216615fa-f838-4e82-a6b1-1f5129c325e2",
  "_return": true,
  "securityGroupRuleSet": {
    "items": [
      {
        "groupOwnerId": "668941950455",
        "groupId": "sg-078ad6f80316b9180",
        "securityGroupId": "sgr-0919ef51c88efd250",
        "description": "Open the sesame",
        "isEgress": false,
        "ipProtocol": "-1",
        "fromPort": -1,
        "toPort": -1,
        "cidrIpv4": "0.0.0.0/0"
      }
    ]
  }
},
"requestID": "216615fa-f838-4e82-a6b1-1f5129c325e2",
"eventID": "0746ca0a-4a80-413e-9935-542d65d6eb20",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "668941950455",
"eventCategory": "Management",
"sessionCredentialFromConsole": "true"
```

```
"eventTime": "2023-08-05T05:14:37Z",
"eventSource": "ec2.amazonaws.com",
"eventName": "AuthorizeSecurityGroupIngress",
"awsRegion": "us-east-1",
"sourceIPAddress": "187.112.73.165",
"userAgent": "AWS Internal",
"requestParameters": {
  "groupId": "sg-078ad6f80316b9180",
  "ipPermissions": {
    "items": [
      {
        "ipProtocol": "-1",
        "groups": {},
        "ipRanges": {
          "items": [
            {
              "cidrIp": "0.0.0.0/0",
              "description": "Open the sesame"
            }
          ]
        }
      }
    ]
  },
  "ipv6Ranges": {},
  "prefixListIds": {}
}
},
}
```

Some good catches

Clavis Segurança da Informação

- Cross Account creation
- Public
 - snapshot
 - S3 bucket
 - AMI
 - EBS
- EC2 with Metadata v2 disabled
- VPC Endpoint

Clavis Segurança da Informação

Attacks (tools) paths/actions

AttachUserPolicy



AttachUserPolicy using aws cli

Clavis Segurança da Informação

Event name	Event time	User name	Event source
AttachUserPolicy	August 04, 2023, 14:11:45 (UTC-03:00)	awslandpacu	iam.amazonaws.com

AttachUserPolicy using Web Console

Clavis Segurança da Informação

Lookup attributes					
User name	ListMFADevices	Event name	ListMFADevices	Event time	August 04, 2023, 14:24:23 (UTC-03:00)
☐ ListResources	ListMFADevices	☐ ListAccessKeys	ListPolicies	☐ ListPolicies	awslandadmin
☐ ListResources	DescribeEventAggreg...	☐ ListAttachedUserPoli...	ListAttachedGroupPo...	☒ AttachUserPolicy	August 04, 2023, 14:24:30 (UTC-03:00)
☐ ListApplications	DescribeOrganization	☐ ListAccessKeys	GetGroup	☐ ListAccessKeys	August 04, 2023, 14:24:30 (UTC-03:00)
☐ DescribeRegions	ListNotificationHubs	☐ GetUser	GetAccessKeyLastUsed	☐ ListAttachedUserPoli...	August 04, 2023, 14:24:30 (UTC-03:00)
☐ ListNotificationHubs	ListPolicies	☐ ListAccessKeys	GetAccessKeyLastUsed	☐ ListUserTags	August 04, 2023, 14:24:30 (UTC-03:00)
☐ DescribeEventAggreg...	DescribeEventAggreg...	☐ ListAccessKeys	GetAccessKeyLastUsed	☐ GetPolicy	August 04, 2023, 14:24:24 (UTC-03:00)
☐ DescribeEventAggreg...	ListAccessKeys	☐ ListUserTags	GetAccessKeyLastUsed	☐ GetPolicy	August 04, 2023, 14:24:24 (UTC-03:00)
☐ DescribeEventAggreg...	ListUsers	☐ ListUserPolicies	GetAccessKeyLastUsed	☐ GetPolicy	August 04, 2023, 14:24:24 (UTC-03:00)
☐ GetCostForecast	ListGroups	☐ ListAccessKeys	ListAccessKeys	☐ GetPolicy	August 04, 2023, 14:24:24 (UTC-03:00)
☐ DescribeEventAggreg...	ListSAMLProviders	☐ GetLoginProfile	GetAccessKeyLastUsed	☐ GetPolicy	August 04, 2023, 14:24:24 (UTC-03:00)
☐ DescribeEventAggreg...	ListPolicies	☐ GetLoginProfile	GetAccessKeyLastUsed	☐ GetPolicy	August 04, 2023, 14:24:24 (UTC-03:00)
☐ DescribeEventAggreg...	GetAccountSummary	☐ GetLoginProfile	GetAccessKeyLastUsed	☐ GetPolicy	August 04, 2023, 14:24:23 (UTC-03:00)
☐ DescribeHub	ListRoles	☐ GetLoginProfile	GetAccessKeyLastUsed	☐ GetPolicy	August 04, 2023, 14:24:23 (UTC-03:00)
☐ DescribeEventAggreg...	ListMFADevices	☐ GetLoginProfile	GetLoginProfile	☐ GetPolicy	August 04, 2023, 14:24:23 (UTC-03:00)
☐ DescribeEventAggreg...	ListOpenIDConnectP...	☐ GetLoginProfile	GetAccessKeyLastUsed	☐ GetPolicy	August 04, 2023, 14:24:23 (UTC-03:00)
☐ DescribeEventAggreg...	ListAccountAliases	☐ GetLoginProfile	ListAccessKeys	☐ GetPolicy	August 04, 2023, 14:24:23 (UTC-03:00)
☐ GetCostAndUsage	DescribeEventAggreg...	☐ GetLoginProfile	ListPolicyGenerations		August 04, 2023, 14:24:15 (UTC-03:00)
	DescribeEventAggreg...	☐ ListGroupsForUser			August 04, 2023, 14:24:12 (UTC-03:00)

AttachUserPolicy using PACU

Clavis Segurança da Informação

Pacu (awslandpacu)

Running process

[iam__privileges]

Created

August 04, 2023, 01:49 (UTC-03:00)

Permissions

Group

Permissions policies

Permissions are defined by policies

Search

Policy name

iam__privileges

[iam__privileges]

Privileges

Event history (8) Info

Event history shows you the last 90 days of management events.

Lookup attributes

AWS access key

AKIAZXQAMDX35IYR3BHC

☐	Event name	Event time	User name
☐	AttachUserPolicy	August 04, 2023, 14:06:30 (UTC-03:00)	awslandpacu
☐	ListUserPolicies	August 04, 2023, 14:06:27 (UTC-03:00)	awslandpacu
☐	GetPolicyVersion	August 04, 2023, 14:06:27 (UTC-03:00)	awslandpacu
☐	GetUserPolicy	August 04, 2023, 14:06:27 (UTC-03:00)	awslandpacu
☐	ListAttachedUserPolicies	August 04, 2023, 14:06:27 (UTC-03:00)	awslandpacu
☐	GetPolicy	August 04, 2023, 14:06:27 (UTC-03:00)	awslandpacu
☐	ListGroupsForUser	August 04, 2023, 14:06:26 (UTC-03:00)	awslandpacu
☐	GetCallerIdentity	August 04, 2023, 14:06:25 (UTC-03:00)	awslandpacu

Attached via

Directly

Online

Directly

Comparison matrix

Clavis Segurança da Informação

Method	List / Read	Write / Perms Mgmt	Services	Total actions

Behavior works
as a trigger

Over permissive policies

Previous key use context (actions, services, timing, source)

Service / Attack	Cloudtrail event
ACM Private Certificate Authority (PCA)	acm-pca:PutPolicy
CloudWatch Logs Resource Policies	logs:PutResourcePolicy
EBS Snapshot Exposure	ec2:ModifySnapshotAttribute requestParameters.attributeType='CREATE_VOLUME_PERMISSION'
EC2 AMIs (Machine Images)	ec2:ModifyImageAttribute requestParameters.attributeType='launchPermission'
Elastic Container Registries (ECR)	ecr:SetRepositoryPolicy ecr:PutRegistryPolicy
Elastic File Systems (EFS)	elasticfilesystem:PutFileSystemPolicy
ElasticSearch Domains	es:UpdateElasticsearchDomainConfig
Glacier Vault	glacier:SetVaultAccessPolicy:
IAM Roles (via AssumeRole)	iam:UpdateAssumeRolePolicy
KMS Keys	kms:PutKeyPolicy
Lambda Function Cross-Account Access	lambda:AddPermission
Lambda Layers	lambda:AddLayerVersionPermission
RDS Snapshots	rds:ModifyDBSnapshotAttribute rds:ModifyDBClusterSnapshotAttribute requestParameters.attributeName='restore'
S3 Buckets	s3:PutBucketPolicy
Secrets Manager	secretsmanager:PutResourcePolicy
SES Sender Authorization Policies	ses:PutIdentityPolicy
SNS Topics	sns:AddPermission
SQS Queues	sqs:AddPermission

Clavis Segurança da Informação

Conclusions



Conclusions

Clavis Segurança da Informação

- **Know** what you have **running**
- **Understand** more **uncommon** services
- Make sure you have an **alert** for everything you have **sensitive** info
- Know your company **context**: same provider, different baselines
- Research and share



Thank you!

Rodrigo Montoro

<https://linkedin.com/in/spooker>

@spookerlabs

rodrigo.montoro@clavis.com.br