Tempest

ACADEMY

Conference

2023

Tempest

ACADEMY

Conference

2023

A arte da segurança na nuvem

Detecção proativa de erros de configuração

Autor da apresentação: Lucídio Neto

Tempest

ACADEMY

Conference

01 Prolegômenos

02 Cenários Nefelibáticos

03 Detecção periódica e factual de atividade suspeita

04 “Filosofamento”

Tempest

:ACADEMY:

Conference

Facilitador

Lucídio Neto

Detecção proativa de erro de configuração

A.18

Cenário Nefelibático

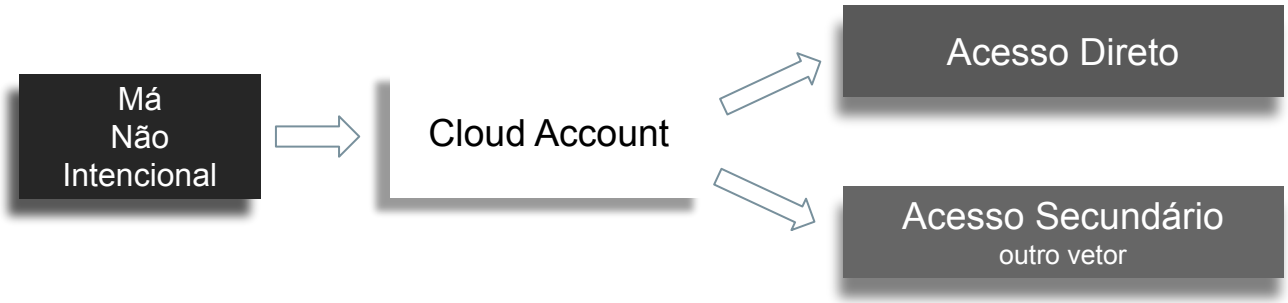
Ações exequíveis

Tempest
ACADEMY
Conference

Boa

Má
Não
Intencional

Má
Intencional



Redução de dano colateral

Tempest
[ACADEMY]
Conference

Mateus 26:41

O que queremos evitar?

Tempest
[ACADEMY]
Conference

Files	Amazon Web Services	Azure Blob Storage	Digital Ocean Spaces	Google Cloud Platform
11.2bn	312.0k	50.4k	7.0k	72.5k

Last Update
12 Nov 2023

GRAYHAT WARFARE
cause white is boring

O que queremos evitar?

Showing 1 - 20 out of 441856 results

Buckets Listing

#	Bucket	Files	Container
1	[redacted].windows.net	2896	private
2	[redacted].windows.net	13	files
3	[redacted].windows.net	1	grafenhausen
4	[redacted].windows.net	6	gourmet
5	[redacted].windows.net	1980	production
6	[redacted].windows.net	1983	development
7	[redacted].windows.net	2	customers
8	[redacted].windows.net	25	images

O que queremos evitar?

Tempest
[ACADEMY]
Conference

Bucket	Filename	Size	Last Modified
aws [redacted].s3.amazonaws.com	satlas/[redacted].zip	1.96TB	27-01-2023 20:19:36
[redacted].googleapis.com	mysql[redacted].sql	1.38TB	14-04-2021 09:42:13
aws [redacted].s3.amazonaws.com	resources/[redacted].zip	871.56GB	15-06-2023 09:56:58
aws [redacted].s3.amazonaws.com	resources/[redacted].zip	737.22GB	22-04-2022 20:52:12
aws [redacted].s3.amazonaws.com	[redacted].zip	716.26GB	09-08-2017 01:48:24
aws [redacted].s3.amazonaws.com	[redacted].zip	699.79GB	08-12-2022 20:16:23
aws [redacted].s3.amazonaws.com	[redacted].zip	661.27GB	13-01-2022 11:19:15
[redacted].googleapis.com	[redacted].zip	444.89GB	30-04-2020 03:12:03
aws [redacted].s3.amazonaws.com	resources/[redacted].zip	416.52GB	22-04-2022 16:26:31
aws [redacted].s3.amazonaws.com	[redacted].zip	358.29GB	16-04-2021 18:24:43

GRAYHAT WARFARE
cause white is boring

O que queremos evitar?

GRAYHAT WARFARE
cause white is boring

Tempest
[ACADEMY]
Conference

Showing 1 - 20 out of 11231455917 results

#	Bucket	Filename	Container	Size	Last Modified
1	[redacted].windows.net	[redacted].pdf	[redacted]	278.14kB	14-08-2020 10:03:43
2	[redacted].windows.net	[redacted].csv	[redacted]	2.82kB	06-07-2021 11:01:31
3	[redacted].windows.net	[redacted].csv	[redacted]	107.16kB	09-12-2020 10:04:00
4	[redacted].windows.net	[redacted].csv	[redacted]	178.97kB	05-08-2020 23:22:51
5	[redacted].windows.net	[redacted].csv	[redacted]	135.45kB	05-08-2020 22:31:53
6	[redacted].windows.net	[redacted].csv	[redacted]	593.61kB	13-08-2020 17:08:44
7	[redacted].windows.net	[redacted].csv	[redacted]	43.35kB	05-08-2020 22:31:53
8	[redacted].windows.net	[redacted].csv	[redacted]	62.00B	07-02-2022 10:21:11

O que queremos evitar?

Tempest
[ACADEMY]
Conference

Showing 1 - 20 out of 2308 results

#	Bucket	Filename	Size	Last Modified
1	[redacted].digitaloceanspaces.com	documentos/[redacted]Ferreira.pdf	188.55kB	12-01-2021 11:41:46
2	[redacted].digitaloceanspaces.com	documentos/[redacted]STRONG.jpg	93.10kB	12-01-2021 11:43:38
3	[redacted].digitaloceanspaces.com	documentos/[redacted]PF.pdf	117.89kB	14-07-2021 17:02:48
4	[redacted].digitaloceanspaces.com	documentos/[redacted]van.pdf	98.88kB	12-01-2021 11:33:08
5	[redacted].digitaloceanspaces.com	documentos/[redacted]osa.JPG	57.76kB	12-01-2021 11:30:42
6	[redacted].digitaloceanspaces.com	documentos/[redacted]OR.pdf	147.15kB	12-01-2021 11:34:59
7	[redacted].digitaloceanspaces.com	documentos/[redacted]PF.jpg	139.47kB	12-01-2021 11:30:27
8	[redacted].digitaloceanspaces.com	documentos/[redacted]F.jpg	1.76MB	15-07-2021 18:13:11
9	[redacted].digitaloceanspaces.com	documentos/[redacted]pf.pdf	138.53kB	28-09-2021 20:19:33
10	[redacted].digitaloceanspaces.com	documentos/[redacted]F.jpg	458.10kB	12-01-2021 11:32:02
11	[redacted].digitaloceanspaces.com	documentos/[redacted]F.png	484.68kB	12-01-2021 11:32:18

GRAYHAT WARFARE
cause white is boring

Detecção Periódica

Sistemático e operacional

Detecção periódica

Tempest
[ACADEMY]
Conference


Tempest
ACADEMY
Conference
aqua
aws

https://github.com/aquasecurity/cloudsploit

Tempest

ACADEMY

Conference

NY

Adobe, Aqua Security

CloudQuery, **CloudSploit**,

Common Fate, Digraph,

SecureFrame, Stripe

https://matthewdfuller.com

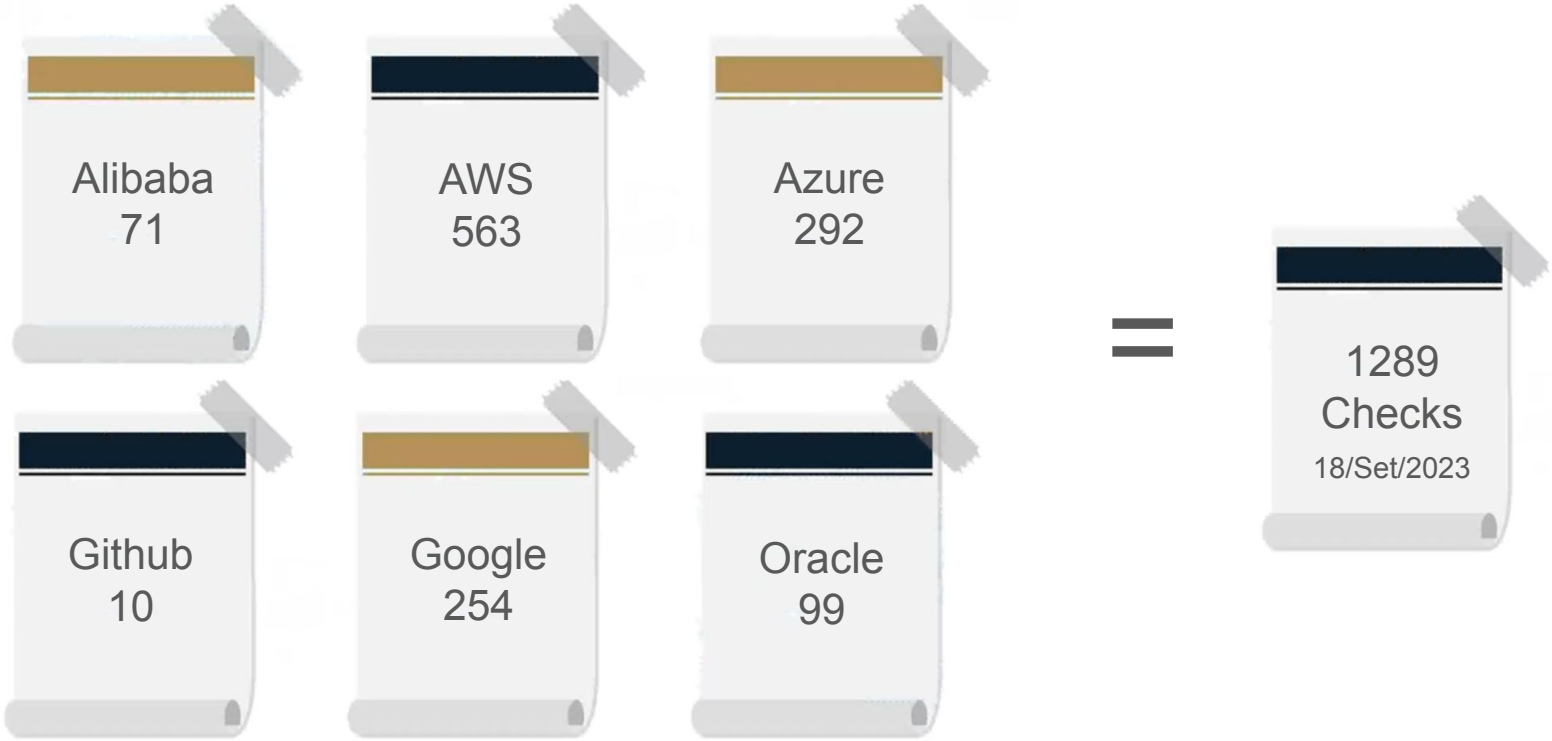
Matthew D. Fuller

Tempest

ACADEMY

Conference

Cloudsploit Checks



bucketPublicAccessBlock.js

Plugin

Tempest
[ACADEMY]
Conference

```
var helpers = require('../../../helpers/aws');

module.exports = {
    title: 'S3 Bucket Public Access Block',
    category: 'S3',
    domain: 'Storage',
    description: 'Ensures S3 public access block is enabled on all buckets or for AWS account',
    more_info: 'Blocking S3 public access at the account level or bucket-level ensures objects are not accidentally exposed.',
    recommended_action: 'Enable the S3 public access block on all S3 buckets or for AWS account.',
    link: 'https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-block-public-access.html',
    apis: ['S3:listBuckets', 'S3:getPublicAccessBlock', 'S3:getBucketLocation', 'S3Control:getPublicAccessBlock', 'STS:getCallerIdentity'],
    settings: {
        s3_public_access_block_allow_pattern: {
            name: 'S3 Public Access Block Allow Pattern',
            description: 'When set, whitelists buckets matching the given pattern. Useful for overriding buckets outside the account control.',
            regex: '^.{1,255}$',
            default: false
        },
        check_global_block: {
            name: 'Check Global Block',
            description: 'When set, check account level public access for S3 and override bucket level public access check.',
            regex: '^(true|false)$',
            default: 'false'
        }
    },
```

Resultado da análise

.csv

Tempest [ACADEMY] Conference

Rule	Severity	URL Check Source (github)	Recomendation
Amazon EBS Public Snapshots	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/ec2/ebsSnapshotPublic.js	Modify the permissions of public snapshots to remove public access.
Certificate Expiry	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/iam/certificateExpiry.js	Update your certificates before the expiration date
EBS Volume Snapshot Public	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/ec2/ebsSnapshotPrivate.js	Ensure that each EBS snapshot has its permissions set to private.
EKS Kubernetes Version	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/eks/eksKubernetesVersion.js	Upgrade the version of Kubernetes on all EKS clusters to the latest available version.
ElasticSearch Exposed Domain	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/es/esExposedDomain.js	Update elasticsearch domain to set access control.
Environment Admin Privileges	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/mwaa/environmentAdminPrivileges.js	Modify IAM role attached with MWAA environment to provide the minimal amount of access required to perform it
Lambda Admin Privileges	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/lambda/lambdaAdminPrivileges.js	Modify IAM role attached with Lambda function to provide the minimal amount of access required to perform its ta
Lambda Public Access	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/lambda/lambdaPublicAccess.js	Update the Lambda policy to prevent access from the public.
Notebook Direct Internet Access	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/sagemaker/notebookDirectInternetAccess.js	Disable DirectInternetAccess for each SageMaker notebook.
Open All Ports Protocols	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/ec2/openAllPortsProtocols.js	Modify the security group to specify a specific port and protocol to allow.
Public AMI	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/ec2/publicAmi.js	Convert the public AMI a private image.
RDS Publicly Accessible	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/rds/rdsPubliclyAccessible.js	Remove the public endpoint from the RDS instance
Redshift Publicly Accessible	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/redshift/redshiftPubliclyAccessible.js	Remove the public endpoint from the Redshift cluster
Root Access Keys	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/iam/rootAccessKeys.js	Remove access keys for the root account and setup IAM users with limited permissions instead
Root Account Active Signing Certificates	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/iam/rootSigningCertificate.js	Delete the x509 certificates associated with the root account.
Root Account In Use	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/iam/rootAccountInUse.js	Create IAM users with appropriate group-level permissions for account access. Create an MFA token for the root
Root MFA Enabled	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/iam/rootMfaEnabled.js	Enable an MFA device for the root account and then use an IAM user for managing services
S3 Bucket All Users ACL	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/s3/bucketAllUsersAcl.js	Disable global all users policies on all S3 buckets and ensure both the bucket ACL is configured with least privile
S3 Bucket All Users Policy	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/s3/bucketAllUsersPolicy.js	Remove wildcard principals from the bucket policy statements.
Secrets Manager Secret Rotation Enabled	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/secretsmanager/secretRotationEnabled.js	Enable secret rotation for your secrets
SQS Public Access	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/sqs/sqsPublicAccess.js	Update the SQS queue policy to prevent public access.
Web Server Public Access	Critical	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/mwaa/webServerPublicAccess.js	Modify Amazon MWAA environments to set web server access mode to be private only
Access Keys Extra	High	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/iam/accessKeysExtra.js	Remove the extra access key for the specified user.
Access Keys Last Used	High	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/iam/accessKeysLastUsed.js	Log into the IAM portal and remove the offending access key.
Access Keys Rotated	High	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/iam/accessKeysRotated.js	To rotate an access key
ACM Certificate Expiry	High	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/acm/acmCertificateExpiry.js	Ensure AWS is able to renew the certificate via email or DNS validation of the domain.
Allowed Custom Ports	High	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/ec2/allowedCustomPorts.js	Modify the security group to ensure the ports are not exposed publicly
API Gateway Certificate Rotation	High	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/apigateway/apigatewayCertificateRotation.js	Rotate the certificate attached to API Gateway API
API Gateway Private Endpoints	High	https://github.com/aquasecurity/cloudsploit/tree/master/plugins/aws/apigateway/apigatewayPrivateEndpoints.js	Set API Gateway API endpoint configuration to private

Public S3 Bucket

Tempest
[ACADEMY]
Conference

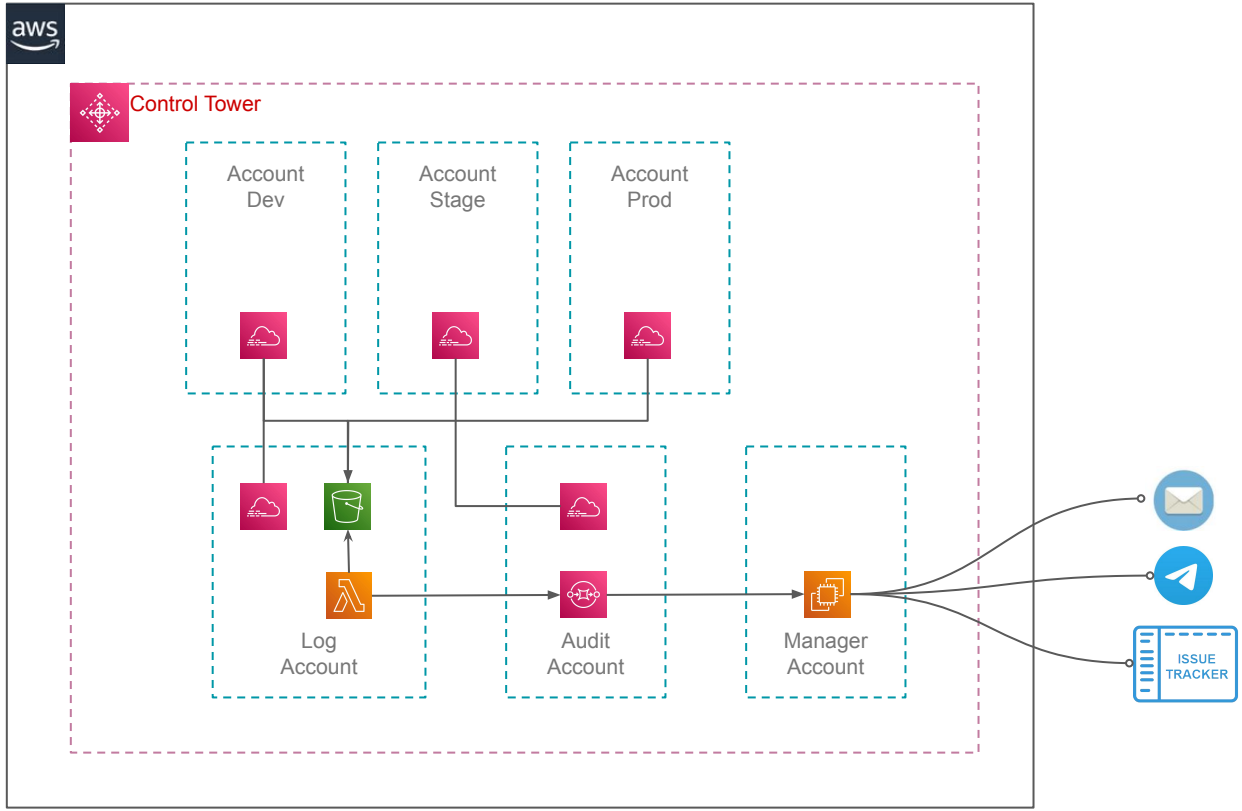
Rule	S3 Bucket All Users ACL / S3 Bucket All Users Policy
Severity	Critical
Impact	Data Leak
Recomendation	Disable global all users policies on all S3 buckets and ensure both the bucket ACL is configured with least privileges. Remove wildcard principals from the bucket policy statements.
AWS Documentation	http://docs.aws.amazon.com/AmazonS3/latest/UG/EditingBucketPermissions.html https://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html
CSPM2CT Splunk	**index=aws_cloudtrail eventName="PutBucketAcl" requestParameters.AccessControlPolicy.AccessControlList.Grant{}.Grantee.URI="http://acs.amazonaws.com/groups/global/AllUsers"** **index=aws_cloudtrail eventName=PutBucketPolicy requestParameters.bucketPolicy.Statement{}.Principal="*" requestParameters.bucketPolicy.Statement{}.Effect="Allow"**

Detecção factual

Tempo real

Arquitetura de coleta de logs e alerta

Tempest
ACADEMY
Conference



CloudTrail
EC2 SIEM
Lambda
S3
SQS

CloudTrail Event

Tempest
:ACADEMY:
Conference

Quem

Quando

O que

Origem

Parâmetros


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAYXXXXXXXXXXXXXXX",
        "arn": "arn:aws:sts::012345678910:assumed-role/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
        "accountId": "012345678910",
        "accessKeyId": "ASIAYXXXXXXXXXXXXXXX",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAYXXXXXXXXXXXXXXX",
                "arn": "arn:aws:iam::012345678910:role/XXXXXXXXXXXX/XXXXXXXXXXXXXXXXXXXXXXX",
                "accountId": "012345678910",
                "userName": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
            },
            "attributes": {
                "creationDate": "2023-11-06T21:04:59Z",
                "mfaAuthenticated": "true"
            }
        }
    },
    "eventTime": "2023-11-06T21:12:19Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetAccountPublicAccessBlock",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.28.143.122",
    "userAgent": "[S3Console/0.4, aws-internal/3 aws-sdk-java/1.12.488 Linux/5.1xxstandard]",
    "errorCode": "NoSuchPublicAccessBlockConfiguration",
    "errorMessage": "The public access block configuration was not found",
    "requestParameters": {
        "Host": "012345678910.s3-control.us-west-2.amazonaws.com"
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "x-amz-id-2": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
```

Alerta de detecção factual

Tempest ACADEMY

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Search & Reporting

New Search

Save As | Create Table View | Close

```
index=[redacted] "GetAccountPublicAccessBlock"
| spath input=Body
| search errorCode="NoSuchPublicAccessBlockConfiguration" sourceIPAddress="[redacted]"
| convert ctime(_time) AS timestamp
| stats count values(userIdentity.accountId) as aws_account values(timestamp) as timestamp min(_time) as it, max(_time) as
    et values(errorCode) as errorCode by sourceIPAddress
| rename sourceIPAddress as src
| eval initial_time=strftime(it, "%Y-%m-%d %H:%M:%S"), end_time=strftime(et, "%Y-%m-%d %H:%M:%S"), et=et+1
| fields src count aws_account errorCode initial_time end_time
```

Yesterday

✓ **36 events** (11/6/23 12:00:00.000 AM to 11/7/23 12:00:00.000 AM) | No Event Sampling | Job | Smart Mode

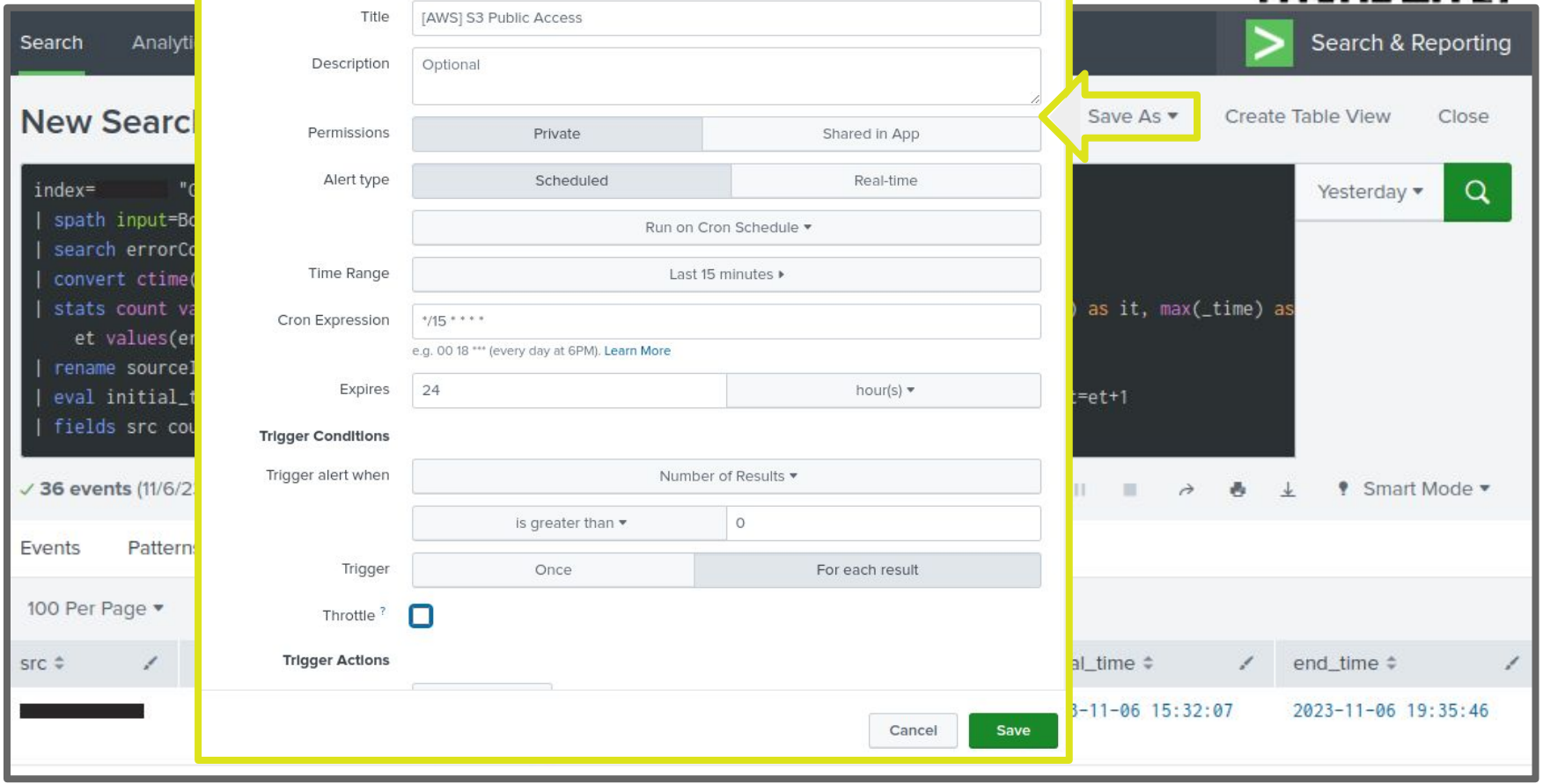
Events | Patterns | **Statistics (1)** | Visualization

100 Per Page | Format | Preview

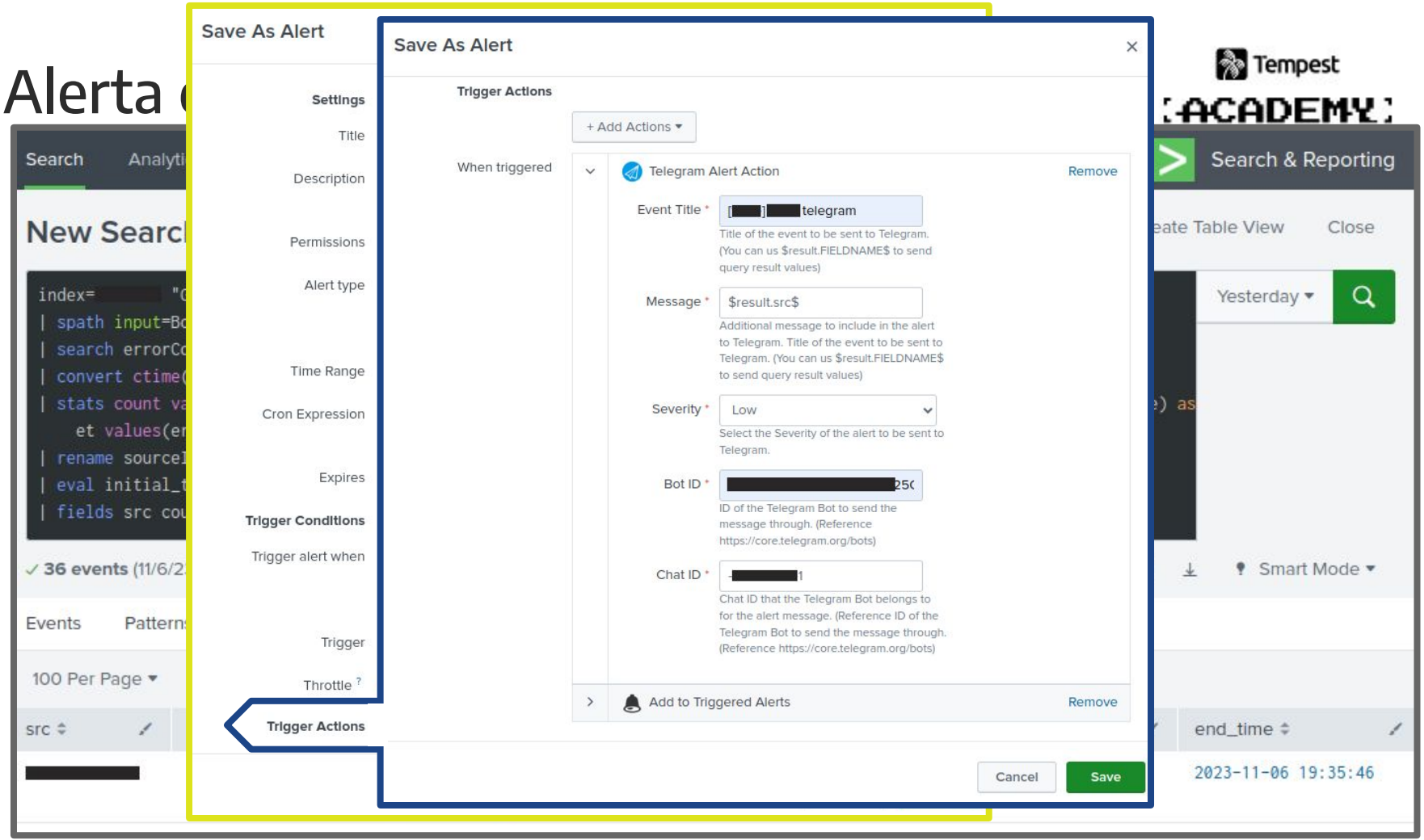
src	count	aws_account	errorCode	initial_time	end_time
[redacted]	36	[redacted]	NoSuchPublicAccessBlockConfiguration	2023-11-06 15:32:07	2023-11-06 19:35:46

Alerta

Tempest ACADEMY



Alerta


Save As Alert
Settings
Title
Description
Permissions
Alert type
Time Range
Cron Expression
Expires
Trigger Conditions
Trigger alert when
Trigger
Throttle
Trigger Actions
Save As Alert
Trigger Actions
+ Add Actions
When triggered
Telegram Alert Action
Remove
Event Title *
[redacted]telegram
Title of the event to be sent to Telegram. (You can us $result.FIELDNAME$ to send query result values)
Message *
$result.src$
Additional message to include in the alert to Telegram. Title of the event to be sent to Telegram. (You can us $result.FIELDNAME$ to send query result values)
Severity *
Low
Select the Severity of the alert to be sent to Telegram.
Bot ID *
[redacted]25(
ID of the Telegram Bot to send the message through. (Reference https://core.telegram.org/bots)
Chat ID *
-[redacted]1
Chat ID that the Telegram Bot belongs to for the alert message. (Reference ID of the Telegram Bot to send the message through. (Reference https://core.telegram.org/bots)
Add to Triggered Alerts
Remove
Cancel
Save
Search
Analyti
New Searc
index=
| spath input=Bo
| search errorCo
| convert ctime(
| stats count va
et values(er
| rename sourcel
| eval initial_t
| fields src cou
36 events (11/6/2
Events
Pattern
100 Per Page
src
Tempest
ACADEMY
Search & Reporting
eate Table View
Close
Yesterday
e) as
Smart Mode
end_time
2023-11-06 19:35:46

“Filosofamento”

Tempest
[ACADEMY]
Conference

Merci!

Lucídio Neto “Netux”

lucidio.neto@tempest.com.br

Tempest ACADEMY Conference