The Boulevard of Broken Buckets

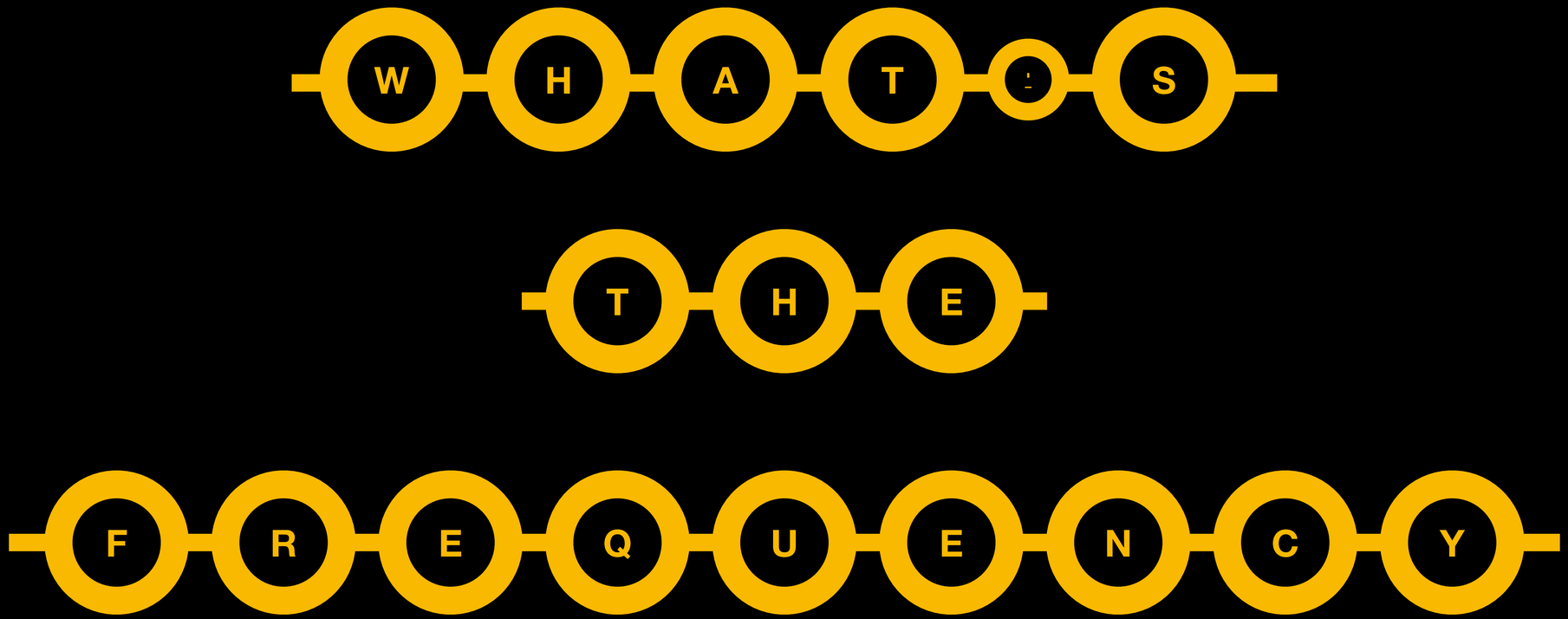
Misconfigured Cloud Storage & Wide Open Databases Hosted in Cloud Providers Errantly Exposed Billions of Records in 2020

RAPID7
RESEARCH

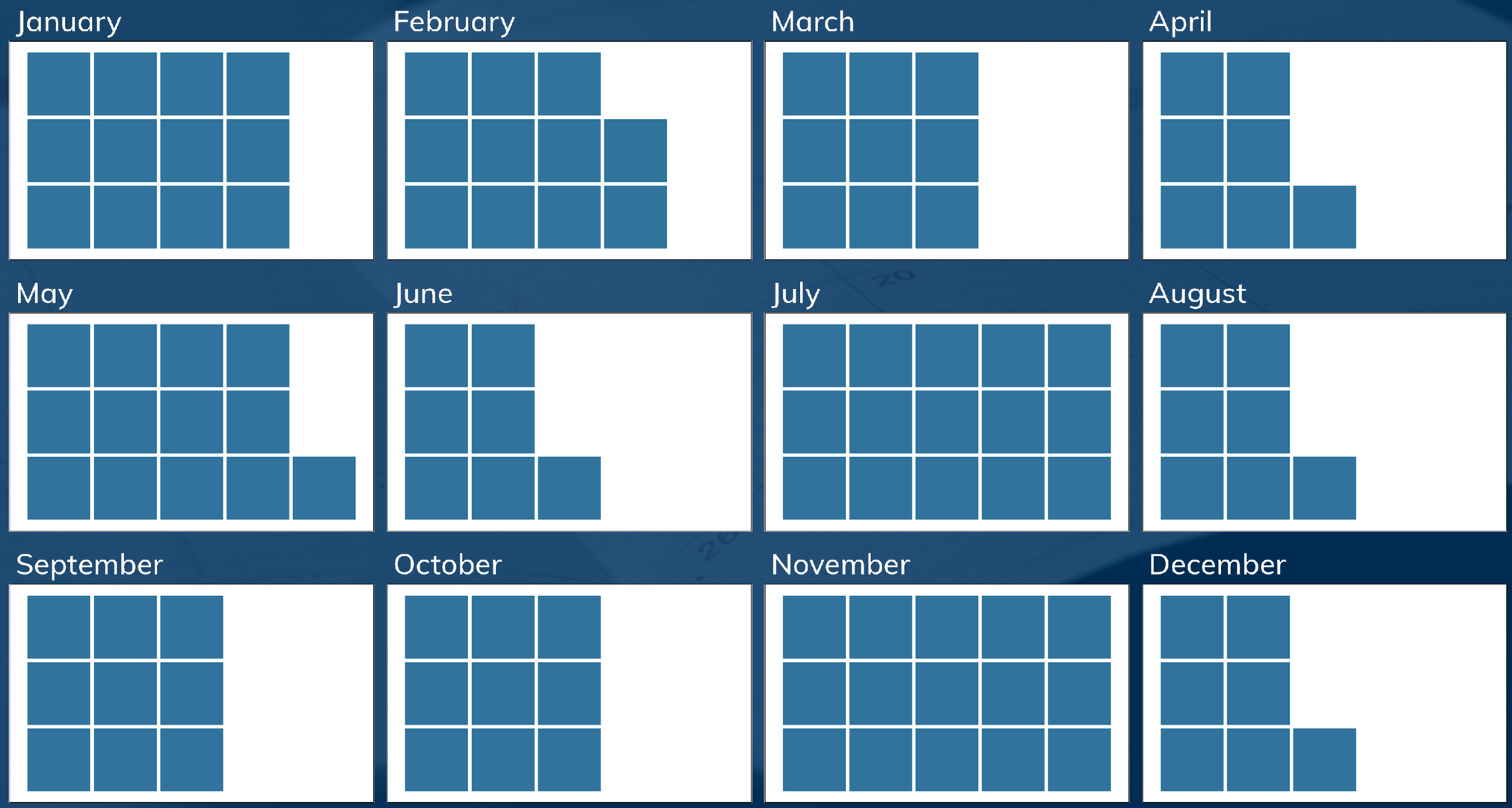
Photo by Varvara Grabova on Unsplash

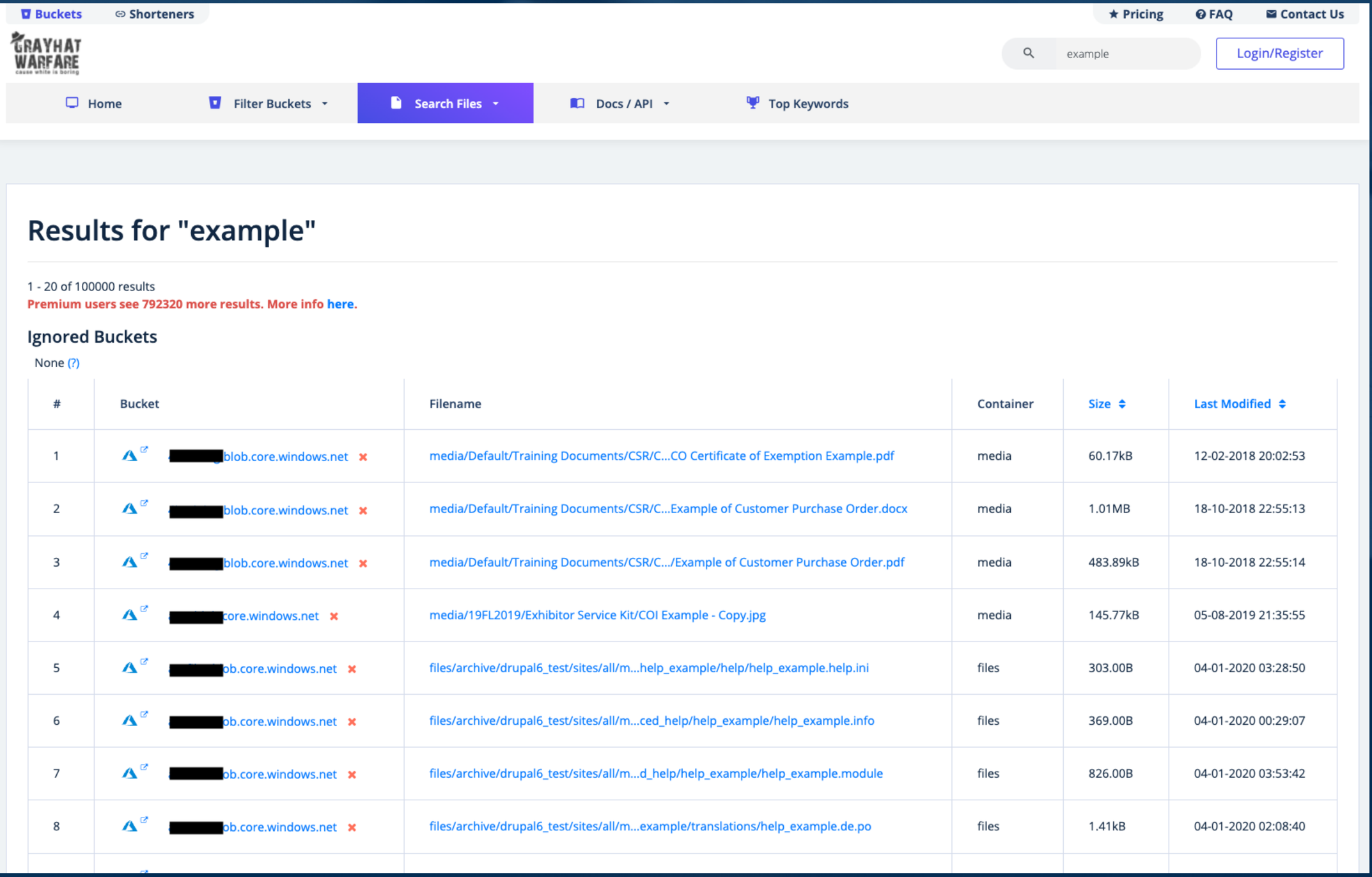
2021 Cloud Misconfigurations Report Redux

- 121 Publicly Reported Leaks & Breaches Disclosed in 2020
- Median exposure: *10 Million Records*
- No Industry or Record Type Left Unscathed


WHAT'S
THE
FREQUENCY

Misconfiguration Incident/Breach Cadence




Buckets
Shorteners
Pricing
FAQ
Contact Us
GRAYHAT WARFARE
example
Login/Register
Home
Filter Buckets
Search Files
Docs / API
Top Keywords
Results for "example"
1 - 20 of 100000 results
Premium users see 792320 more results. More info here.
Ignored Buckets
None (?)
Bucket Filename Container Size Last Modified
1 [redacted]blob.core.windows.net media/Default/Training Documents/CSR/C...CO Certificate of Exemption Example.pdf media 60.17kB 12-02-2018 20:02:53
2 [redacted]blob.core.windows.net media/Default/Training Documents/CSR/C...Example of Customer Purchase Order.docx media 1.01MB 18-10-2018 22:55:13
3 [redacted]blob.core.windows.net media/Default/Training Documents/CSR/C.../Example of Customer Purchase Order.pdf media 483.89kB 18-10-2018 22:55:14
4 [redacted]core.windows.net media/19FL2019/Exhibitor Service Kit/COI Example - Copy.jpg media 145.77kB 05-08-2019 21:35:55
5 [redacted]ob.core.windows.net files/archive/drupal6_test/sites/all/m...help_example/help/help_example.help.ini files 303.00B 04-01-2020 03:28:50
6 [redacted]ob.core.windows.net files/archive/drupal6_test/sites/all/m...ced_help/help_example/help_example.info files 369.00B 04-01-2020 00:29:07
7 [redacted]ob.core.windows.net files/archive/drupal6_test/sites/all/m...d_help/help_example/help_example.module files 826.00B 04-01-2020 03:53:42
8 [redacted]ob.core.windows.net files/archive/drupal6_test/sites/all/m...example/translations/help_example.de.po files 1.41kB 04-01-2020 02:08:40

Buckets (11) Info

Buckets are containers for data stored in S3. Learn more

Copy ARN | Empty | Delete | Create bucket

Find buckets by name

1

Name	AWS Region	Access	Creation date
a-very-super-secure-bucket	US East (N. Virginia) us-east-1	Bucket and objects not public	September 28, 2021, 15:01:12 (UTC-04:00)
ac[redacted]	US East (N. Virginia) us-east-1	Objects can be public	December 5, 2016, 22:42:03 (UTC-05:00)
av	US East (N. Virginia) us-east-1	Objects can be public	April 20, 2018, 21:41:22 (UTC-04:00)
cs	US East (N. Virginia) us-east-1	Objects can be public	March 10, 2019, 07:16:05 (UTC-04:00)
dc	US East (N. Virginia) us-east-1	Public	December 21, 2013, 22:55:59 (UTC-05:00)
hr	US East (N. Virginia) us-east-1	Objects can be public	June 26, 2020, 11:11:57 (UTC-04:00)
is.	US East (N. Virginia) us-east-1	Objects can be public	March 10, 2019, 06:39:02 (UTC-04:00)
is.	US East (N. Virginia) us-east-1	Objects can be public	July 13, 2018, 08:43:49 (UTC-04:00)
is.	US East (N. Virginia) us-east-1	Objects can be public	February 28, 2020, 15:48:25 (UTC-05:00)
podcast.datadrivensecurity.info	US East (N. Virginia) us-east-1	Public	December 22, 2013, 12:50:40 (UTC-05:00)
public-r-data	US East (N. Virginia) us-east-1	Public	July 10, 2016, 11:26:23 (UTC-04:00)

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

myawsbucket

Bucket name must be unique and must not contain spac

AWS Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration a

Choose bucket

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

- [x] **Block *all* public access**

  Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

  - [x] **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

    S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

  - [x] **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

    S3 will ignore all ACLs that grant public access to buckets and objects.

  - [x] **Block public access to buckets and objects granted through *new* public bucket or access point policies**

    S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

  - [x] **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

    S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | elasticsearch | Account

TOTAL RESULTS

7,413

TOP COUNTRIES

United States	2,051
Hong Kong	1,358
China	1,232
Germany	554
Netherlands	375

More...

TOP PORTS

9200	3,303
80	2,580
443	404
8081	283
8080	125

More...

TOP ORGANIZATIONS

Google LLC	578
Aliyun Computing Co., LTD	500
DXTL HK	476
Amazon Technologies Inc.	397
Microsoft Corporation	356

More...

View Report | Download Results | Browse Images | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted]

2021-08-31T15:43:52.741102

OOO 24 chasa TV

Russian Federation, Moscow

starttls | self-signed

SSL Certificate

Issued By:
|- Common Name:
elasticsearch-dev

Issued To:
|- Common Name:
elasticsearch-dev

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

```
220 elasticsearch-dev ESMTP Postfix (Ubuntu)
250-elasticsearch-dev
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
```

401 Authorization Required

2021-08-31T15:43:44.690464

[redacted]

EGIHosting

United States, San Jose

```
HTTP/1.1 401 Unauthorized
Server: nginx
Date: Tue, 31 Aug 2021 15:17:19 GMT
Content-Type: text/html
Content-Length: 590
Connection: keep-alive
WWW-Authenticate: Basic realm="Protected Elasticsearch"
```

2021-08-31T15:43:44.603486

African Oxygen Limited

United States, Los Angeles

database

```
HTTP/1.1 200 OK
Warning: 299 Elasticsearch-7.13.3-5d21bea28db1e89ecc1f66311ebdec9dc3aa7d64 "Elasticsearch built-in security features are not enabled. Without a
```

[redacted]

2021-08-31T15:40:14.459181

180-177-172-163.instances.scw.cloud

Dedicated Servers and cloud assignment, abuse reports : http://abuse.online.net

France, Paris

database

```
HTTP/1.1 200 OK
Warning: 299 Elasticsearch-7.13.2-4d960a0733be83dd2543ca018aa4ddc42e956800 "Elasticsearch built-in security features are not enabled. Without a
```

401 Authorization Required

2021-08-31T15:39:22.355024

[redacted]

es-cluster.hofmann1.rackspee...

SSL Certificate

```
HTTP/1.1 401 Unauthorized
```

RAPID7 RESEARCH

Networking

edit

Each Elasticsearch node has two different network interfaces. Clients send requests to Elasticsearch's REST APIs using its HTTP interface, but nodes communicate with other nodes using the transport interface. The transport interface is also used for communication with remote clusters.

You can configure both of these interfaces at the same time using the `network.*` settings. If you have a more complicated network, you might need to configure the interfaces independently using the `http.*` and `transport.*` settings. Where possible, use the `network.*` settings that apply to both interfaces to simplify your configuration and reduce duplication.

By default Elasticsearch binds only to `localhost` which means it cannot be accessed remotely. This configuration is sufficient for a local development cluster made of one or more nodes all running on the same host. To form a cluster across multiple hosts, or which is accessible to remote clients, you must adjust some network settings such as `network.host`.

WARNING

Be careful with the network configuration!

Never expose an unprotected node to the public internet. If you do, you are permitting anyone in the world to download, modify, or delete any of the data in your cluster.

Configuring Elasticsearch to bind to a non-local address will convert some warnings into fatal exceptions. If a node refuses to start after configuring its network settings then you must address the logged exceptions before proceeding.

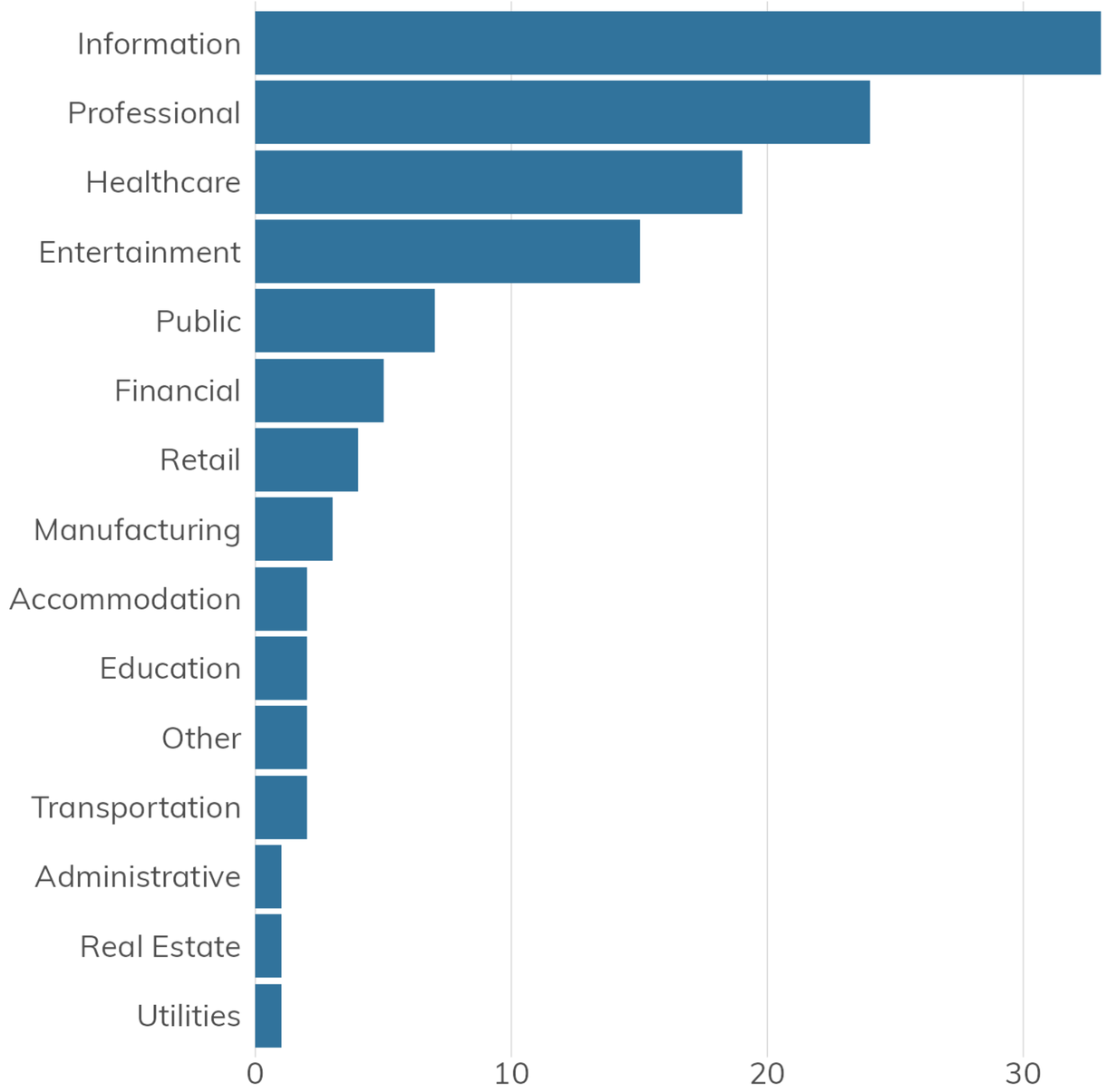
Record Loss by Type & Industry

	Other	Email	Name	Address	Identifier	Phone	Financial	Birthday	Credentials	Health	IP Address	Location	PII	Photo/Media
Information	23	16	10	7	6	9	6	3	8	5	5	8	1	7
Entertainment	13	12	10	8	4	6	3	6	7	1	4	2	2	
Professional	16	11	8	4	6	5	1	3	5	1	2	1	3	2
Healthcare	6	4	9	8	5	2	5	2	1	11	1	2		1
Public	1	3	4	4	4	2		3	1				2	
Retail	1	3	4	4	2	2	1	1		1	1			1
Financial	3	1	1	1	1		3	2					1	
Manufacturing	1	3	1	1		1		1	1		1	1		
Other	1	1	1	2	1		1				1		1	
Utilities			1	1	1	1	1	1		1				
Education	1	1	2		1	1		1						
Administrative	1	1	1	1		1	1							
Accommodation		1	2		2		1							
Transportation	1	1			1		1							
Real Estate					1								1	

Record L

	Other	Email	PII	Photo/Media
Information	23	16	1	7
Entertainment	13	12	2	
Professional	16	11	3	2
Healthcare	6	4		1
Public	1	3	2	
Retail	1	3		1
Financial	3	1	1	
Manufacturing	1	3		
Other	1	1	1	
Utilities				
Education	1	1		
Administrative	1	1		
Accommodation		1		
Transportation	1	1		
Real Estate			1	

Industry Breakdown



Record Loss by Type & Industry

	Other	Email	Name	Address	Identifier	Phone	Financial	Birthday	Credentials	Health	IP Address	Location	PII	Photo/Media
Information	23	16	10	7	6	9	6	3	8	5	5	8	1	7
Entertainment	13	12	10	8	4	6	3	6	7	1	4	2	2	
Professional	16	11	8	4	6	5	1	3	5	1	2	1	3	2
Healthcare	6	4	9	8	5	2	5	2	1	11	1	2		1
Public	1				4	2		3	1				2	
Retail	1	3	4	4	2	2	1	1		1	1			1
Financial	3	1	1	1	1		3	2					1	
Manufacturing	1	3	1	1		1		1	1		1	1		
Other	1	1	1	2	1		1				1		1	
Utilities			1	1	1	1	1	1		1				
Education	1	1	2		1	1		1						
Administrative	1	1	1	1		1	1							
Accommodation		1	2		2		1							
Transportation	1	1			1		1							
Real Estate					1								1	

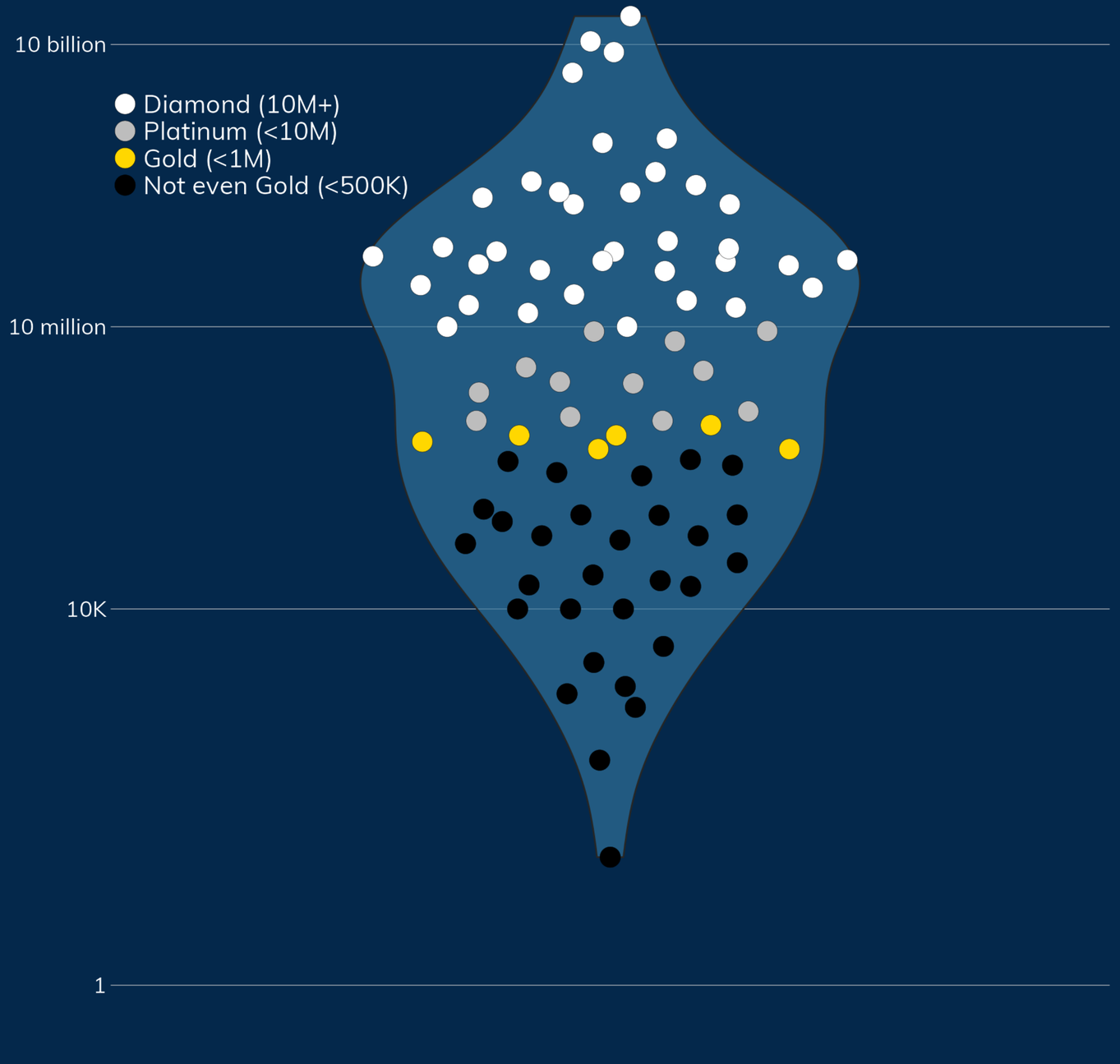
Record Loss by Type & Industry

	Other	Email	Name	Address	Identifier	Phone	Financial	Birthdate	Credentials	Health	IP Address	Location	Photo/Media	PII
Information	23	16	10	7	6	9	6	3	8	5	5	8	1	7
Entertainment	13	12	10	8	4	6	3	6	7	1	4	2	2	
Professional	16	11	8	4	6	5	1	3	5	1	2	1	3	2
Healthcare	6	4	9	8	5	2	5	2	1	11	1	2		1
Public	1	3	4	4	4	2		3	1				2	
Retail	1	3	4	4	2	2	1	1		1	1			1
Financial	3	1	1	1	1		3	2					1	
Manufacturing	1	3	1	1		1		1	1		1	1		
Other	1	1	1	2	1		1				1		1	
Utilities			1	1	1	1	1	1		1				
Education	1	1	2		1	1		1						
Administrative	1	1	1	1		1	1							
Accommodation		1	2		2		1							
Transportation	1	1			1		1							
Real Estate					1								1	

Record Loss by Type & Industry

	Other	Email	Name	Address	Identifier	Phone	Financial	Birthday	Credentials	Health	IP Addre	Location	PII	Photo/Media
Information	23	16	10	7	6	9	6	3	3	5	5	8	1	7
Entertainment	13	12	10	8	4	6	3	6		1	4	2	2	
Professional	16	11	8	4	6	5	1	3	2	1	2	1	3	2
Healthcare	6	4	9	8	5	2	5	2		11	1	2		1
Public	1	3	4	4	4	2		3					2	
Retail	1	3	4	4	2	2	1	1		1	1			1
Financial	3	1	1	1	1		3	2					1	
Manufacturing	1	3	1	1		1		1				1		
Other	1	1	1	2	1		1				1		1	
Utilities			1	1	1	1	1	1		1				
Education	1	1	2		1	1		1						
Administrative	1	1	1	1		1	1							
Accommodation		1	2		2		1							
Transportation	1	1			1		1							
Real Estate					1								1	

Chart Toppers



The Usual Suspects

AWS S3
30 (25%) Incidents

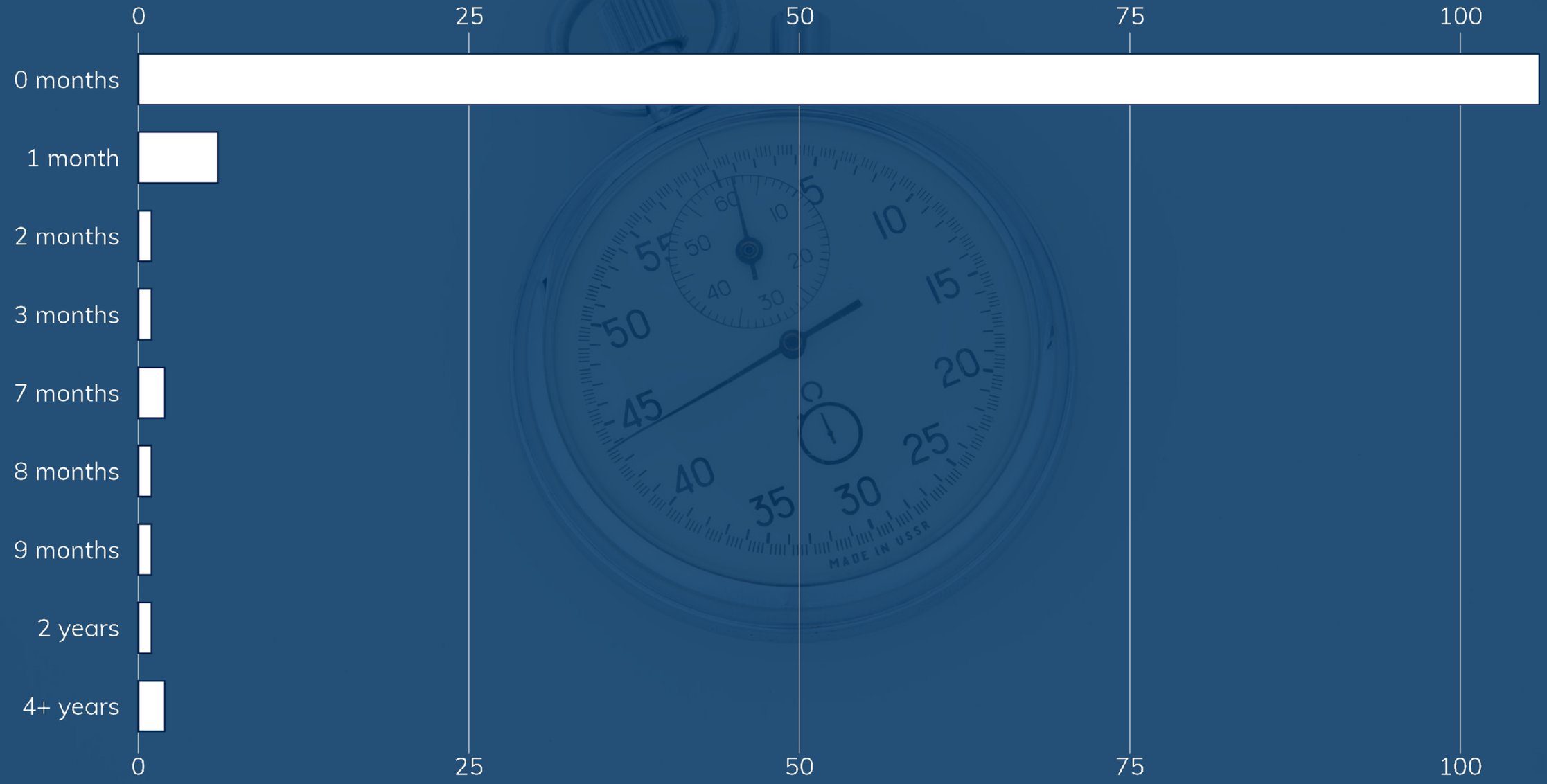
Elasticsearch
24 (20%) Incidents

Google Cloud
3 (~3%) Incidents

Azure Blob
2 (~2%) Incidents


HDS
STEVE MILLER BAND
1 FLY LIKE AN EAGLE
2 WILD MOUNTAIN HONEY
3 SERENADE
4 DANCE, DANCE, DANCE
5 MERCURY BLUES
6 TAKE THE MONEY AND RUN
7 ROCK 'N ME
8 YOU SEND ME
9 BLUE ODYSSEY
10 SWEET MAREE
11 THE WINDOW
Manufactured for Mobile Fidelity International, Incline Village, NV 89452-8359 to HDS Specifications
℗ 1996 EMI-Capitol Music Special Markets
All rights reserved. Unauthorized copying, reproduction, hiring, lending, public performance and broadcasting prohibited.
Made in U.S.A.
MFI-4406 (7243-8-19037-2-8)
EMI-Capitol Music
FLY LIKE AN EAGLE
Produced by Steve Miller
Executive Producer: John Palladino
A Haworth Enterprises Production
℗ © 1976 Haworth Enterprises
DIGITAL dts SURROUND
A dts DECODER IS REQUIRED
HIGH DEFINITION SURROUND™
miller nevada ltd., inc.

Record Time



Discovery Over Time In Breaches

Depending on the type of attack, defenders have gotten much better at detecting evidence of compromise since 2016.

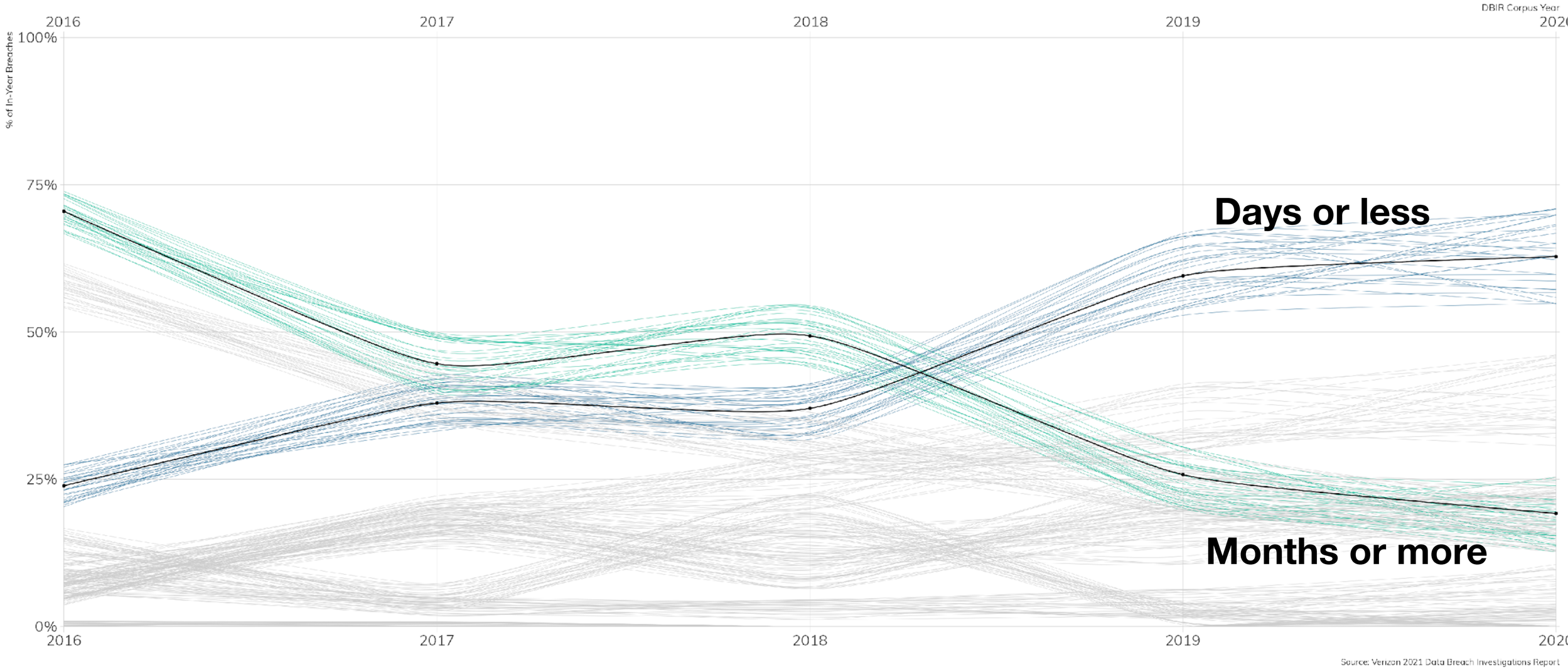
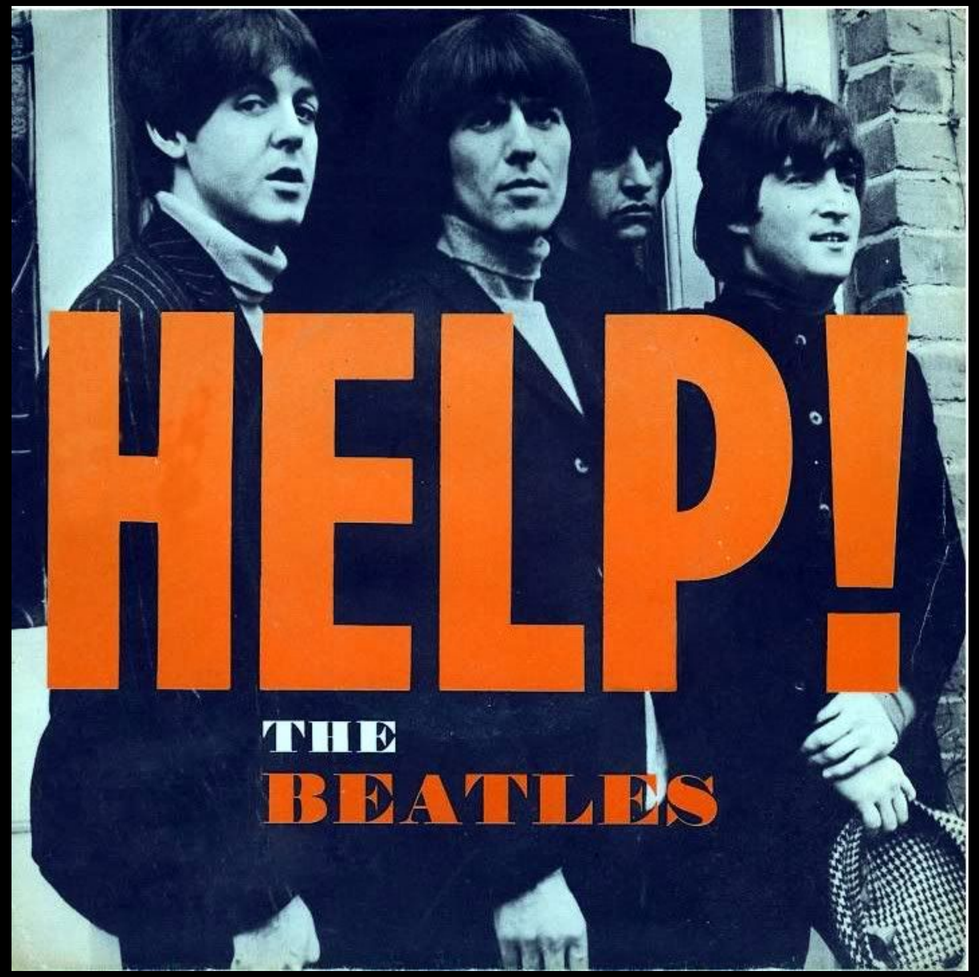


Photo by Stanislav Remnev on Unsplash


HELP!
THE
BEATLES

How To Avoid Being A Misconfiguration Headline

Know What You Are Exposing

How To Avoid Being A Misconfiguration Headline

Buckets (11) Info

Buckets are containers for data stored in S3. Learn more

Copy ARN | Empty | Delete | Create bucket

Find buckets by name

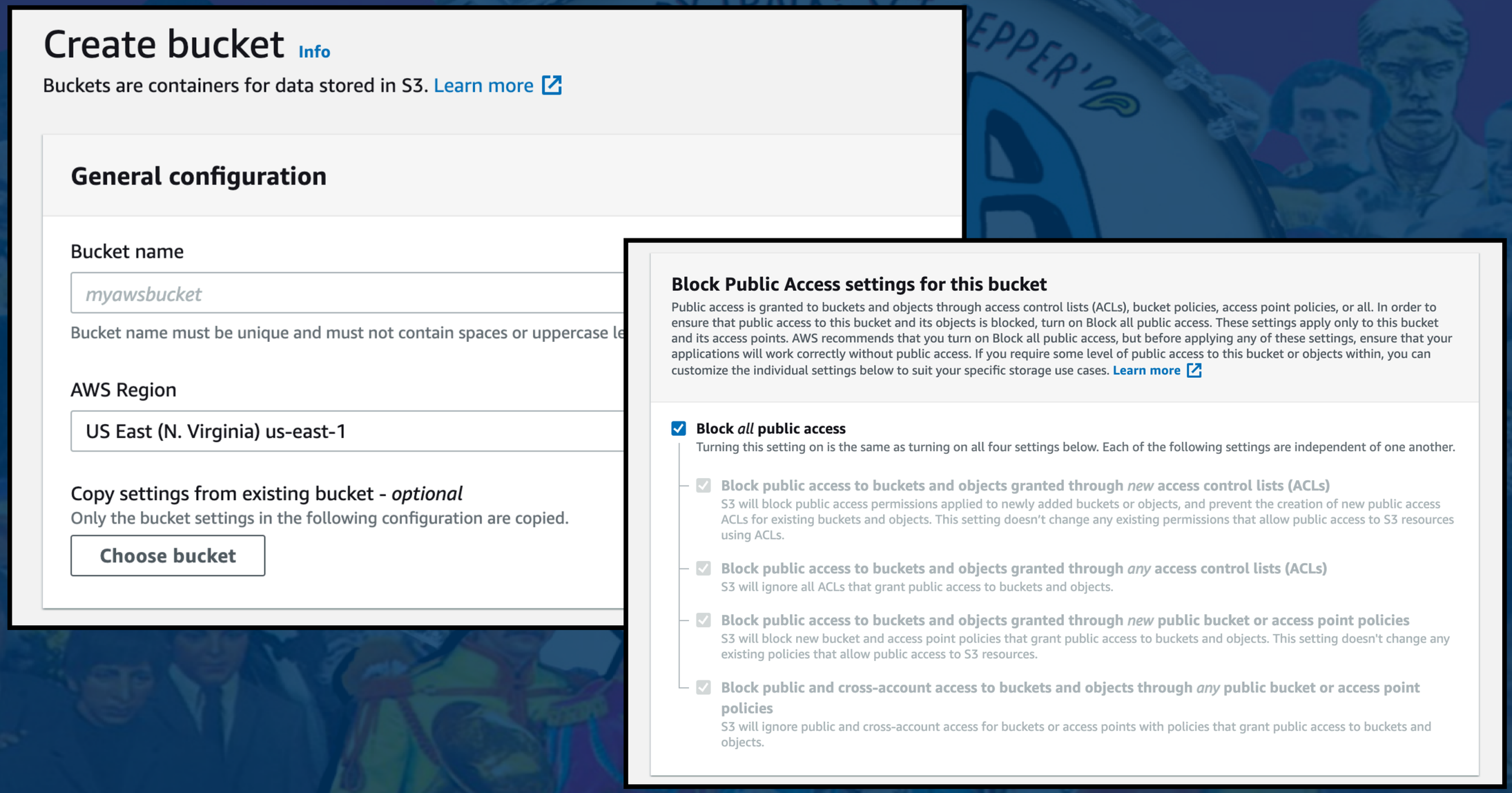
1

Name	AWS Region	Access	Creation date
a-very-super-secure-bucket	US East (N. Virginia) us-east-1	Bucket and objects not public	September 28, 2021, 15:01:12 (UTC-04:00)
ac[redacted]	US East (N. Virginia) us-east-1	Objects can be public	December 5, 2016, 22:42:03 (UTC-05:00)
av	US East (N. Virginia) us-east-1	Objects can be public	April 20, 2018, 21:41:22 (UTC-04:00)
cs	US East (N. Virginia) us-east-1	Objects can be public	March 10, 2019, 07:16:05 (UTC-04:00)
dc	US East (N. Virginia) us-east-1	Public	December 21, 2013, 22:55:59 (UTC-05:00)
hr	US East (N. Virginia) us-east-1	Objects can be public	June 26, 2020, 11:11:57 (UTC-04:00)
is.	US East (N. Virginia) us-east-1	Objects can be public	March 10, 2019, 06:39:02 (UTC-04:00)
is.	US East (N. Virginia) us-east-1	Objects can be public	July 13, 2018, 08:43:49 (UTC-04:00)
is.	US East (N. Virginia) us-east-1	Objects can be public	February 28, 2020, 15:48:25 (UTC-05:00)
podcast.datadrivensecurity.info	US East (N. Virginia) us-east-1	Public	December 22, 2013, 12:50:40 (UTC-05:00)
public-r-data	US East (N. Virginia) us-east-1	Public	July 10, 2016, 11:26:23 (UTC-04:00)

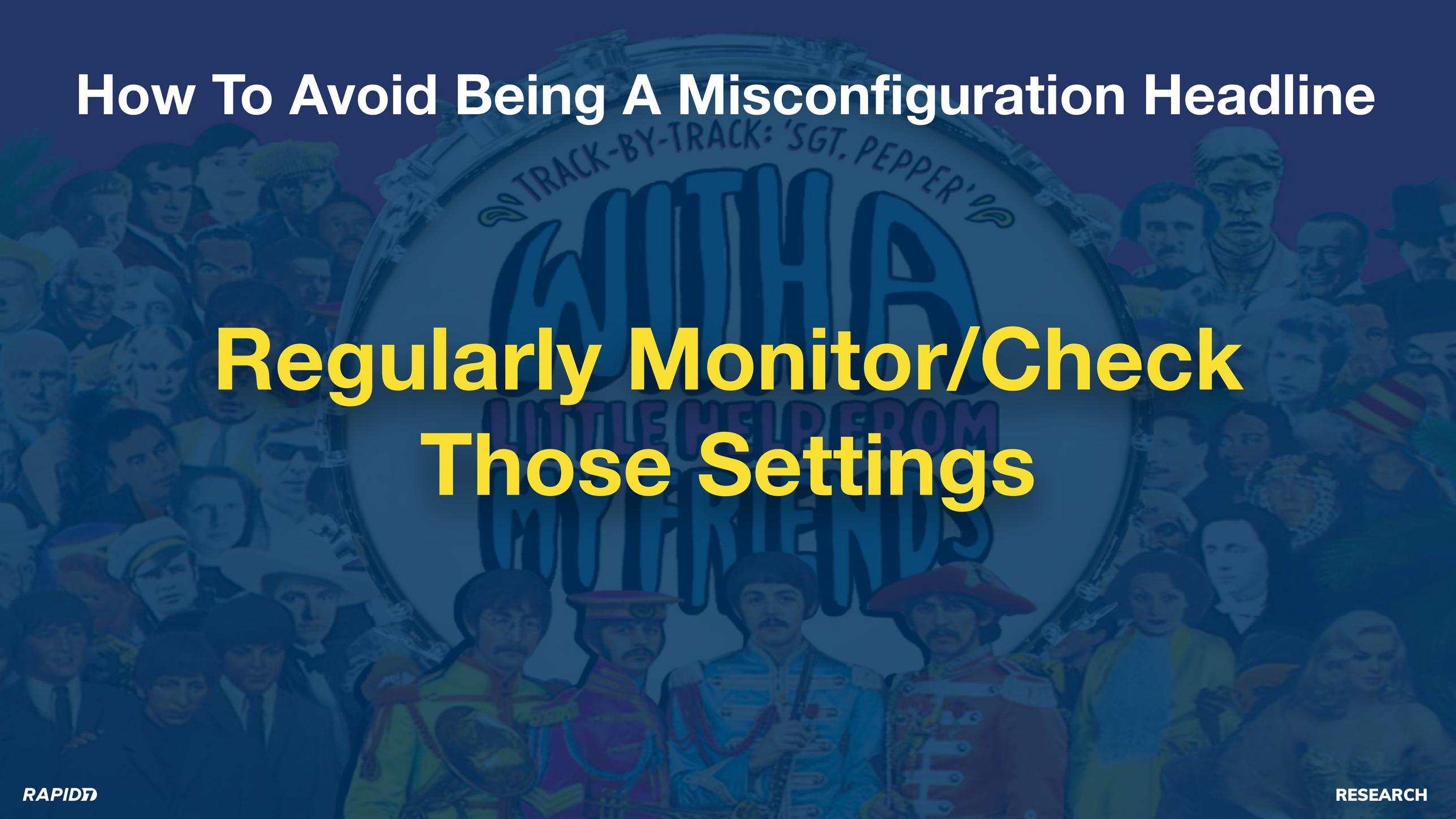
How To Avoid Being A Misconfiguration Headline

Use Safe & Resilient Configuration Settings

How To Avoid Being A Misconfiguration Headline



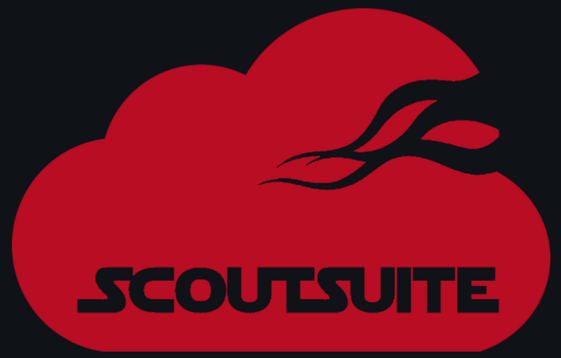
How To Avoid Being A Misconfiguration Headline



Regularly Monitor/Check Those Settings

How To Avoid Being A Misconfiguration Headline

README.md



CI Workflow passing codecov 24%

pypi package 5.10.2 downloads 3.6k/month Docker Hub rossja/ncc-scoutsuite docker pulls 77k

Description

Scout Suite is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments. Using the APIs exposed by cloud providers, Scout Suite gathers configuration data for manual inspection and highlights risk areas. Rather than going through dozens of pages on the web consoles, Scout Suite presents a clear view of the attack surface automatically.

Scout Suite was designed by security consultants/auditors. It is meant to provide a point-in-time security-oriented view of the cloud account it was run in. Once the data has been gathered, all usage may be performed offline.

The project team can be contacted at scoutsuite@nccgroup.com.

https://github.com/nccgroup/ScoutSuite

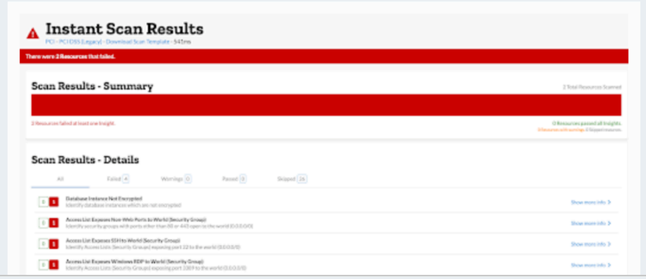
How To Avoid Being A Misconfiguration Headline

Use And Rely On Automation

How To Avoid Being A Misconfiguration Headline

Preventing Misconfigurations

Misconfiguration of cloud services is the number one reason for security and compliance risk. When using cloud services (IaaS, PaaS, Serverless, FaaS, and CaaS), security is a shared responsibility between you and the cloud service provider.



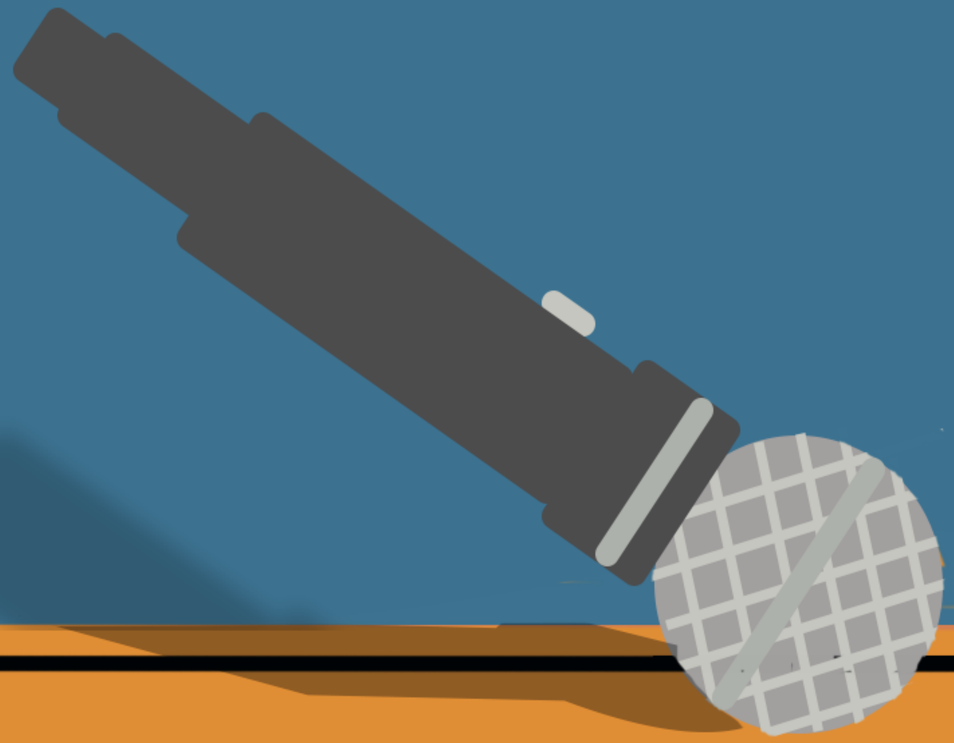
You, as the customer of the cloud service provider (CSP), are responsible for securing how you use cloud services, including properly configuring identity and access management (IAM), storage and compute settings, threat analysis and defense, and the security of the application and data processed and stored in the cloud.

Therefore, secure cloud configuration must be a dynamic and continuous process. At a base level, there is the configuration of the cloud infrastructure (e.g., blocking SSH ports, and IAM). Next, there is the configuration of the CSP security controls (e.g., enabling log monitoring and encryption). And, finally, SecOps teams must address changes to settings (e.g., detecting and acting on a threat actor turning off logging to cover their tracks).

With InsightCloudSec, all changes—no matter how they are implemented (via console, provisioning tools, or programmatically)—are detected through a two-tiered monitoring approach that includes API polling and event-driven harvesting for faster detection of changes and automation in real-time. This allows you to identify misconfigurations and resolve them with automated, real-time remediation.

With InsightCloudSec, you can accelerate innovation through the use of cloud and container services while minimizing the risk of misconfigurations.

research@rapid7.com



👀 https://www.rapid7.com/c/cloud-misconfigurations-2021/

https://github.com/rapid7/data/tree/master/2021-cloud-misconfigurations