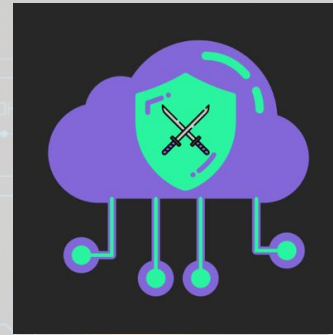


Insight into your Cloud Security



How to do Cloud Security assessments like a pro in only #4Steps

DEFCON 2022



About Secura

Secura is a digital security expert company since 2000 with the mission:


PROVIDING INSIGHT INTO YOUR DIGITAL SECURITY

Our approach is:

- To link security to (international) standards, metrics and certification
- Holistic: security is a matter of people, process and technology

Since Jan 2021 Secura is a Bureau Veritas company (BV is majority shareholder)

About Secura



ZeroLogon:
Unauthenticated domain controller compromise
by subverting Netlogon cryptography (CVE-2020-1472)

by Tom Tervoort, September 2020

Secura

ZeroLogon: CVE 2020-1472

Whitepaper
available now

[DOWNLOAD WHITEPAPER](#)

lder)



@Whoami?

Speaker



Ricardo Sanchez
Senior Security Specialist
(Mexican pentester)



- 
- 
1. Introduction
 2. Type of cloud assessments
 3. Conclusions
 4. Q&A



*Cloud is new infrastructure and multiple companies struggle to implement it correctly & securely
-> Set up a cloud webinar series to provide some insights from our side*



Poll



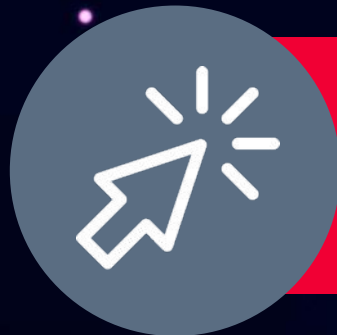
**Which cloud providers do you
(intend to) use?**

Introduction

1. Cloud is a **different way of thinking**
2. There are **challenges** on cloud environments (Technology, People and Processes)
3. There are **multiple strategies** for a cloud migration, each with their pros/cons.

Introduction

4. Can be more secure, but it may also provide a **false sense of security** (images, encryption, networking)
5. More to **configure, update and maintain**.
6. If the **risks are addressed** this can be great for the business.



Also check out our Cloud CTF
<https://www.brokenazure.cloud/>

What are the Biggest Security Threats in Cloud Environments?

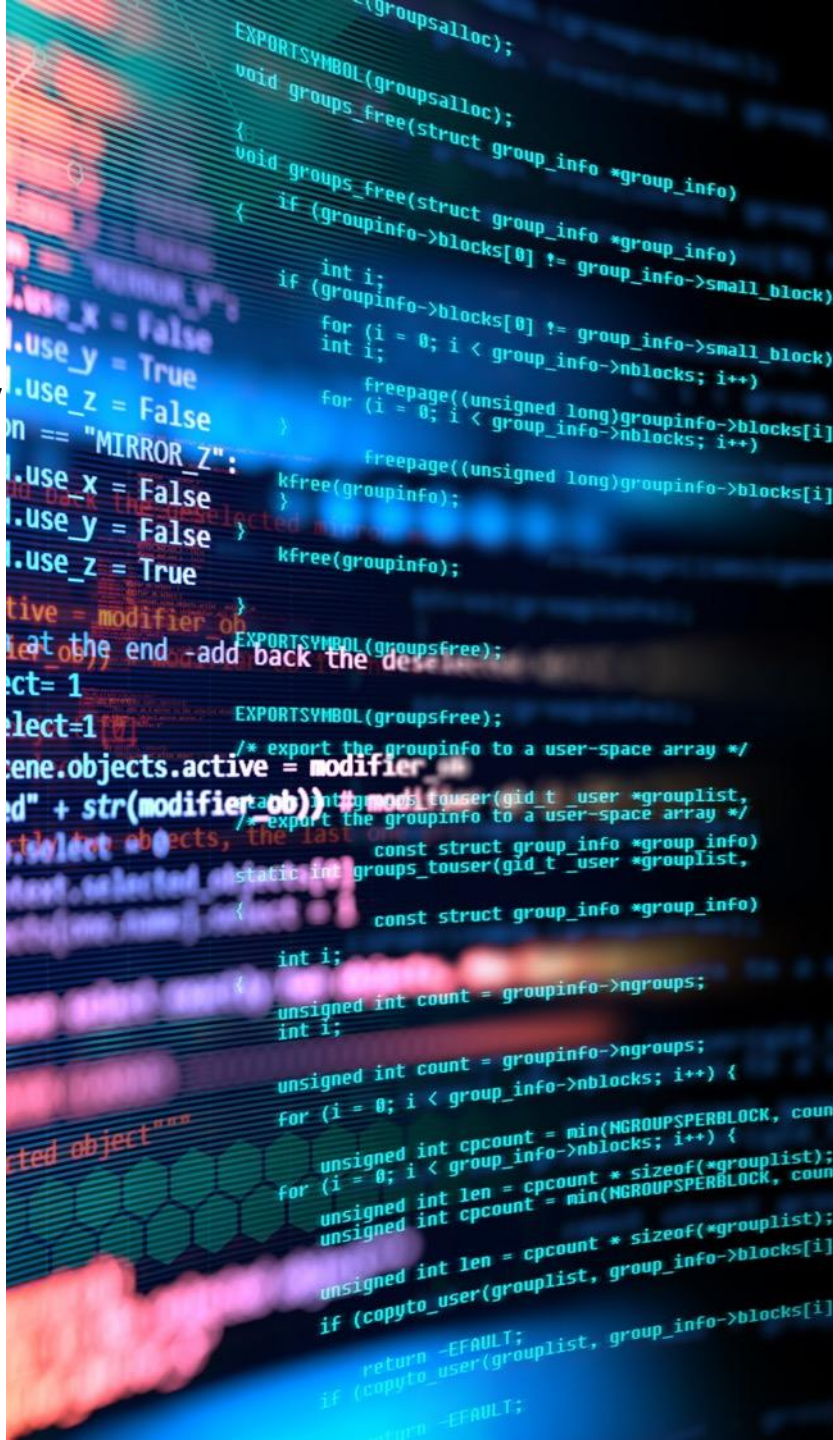
#1  **62%** Misconfiguration of the cloud platform/wrong set-up


55%
Unauthorized access


52%
Insecure interfaces /APIs

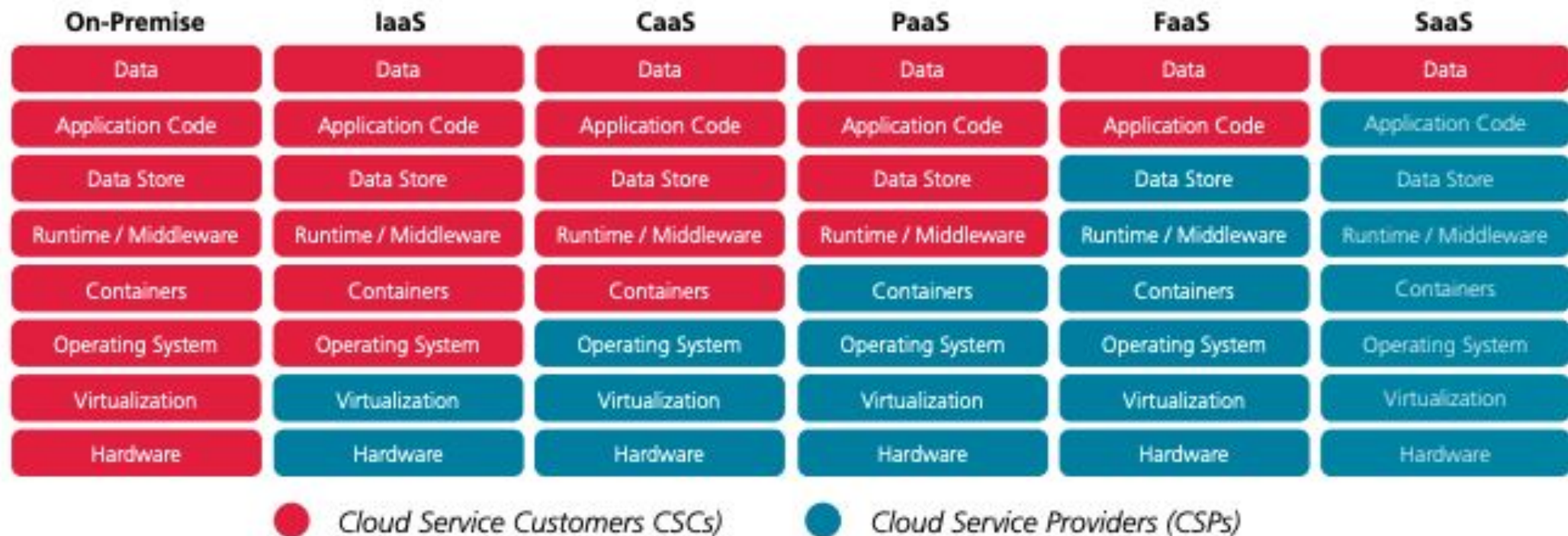

49%
Hijacking of accounts, services or traffic

019-2/



Cloud is a Different Way of Thinking

From On-Premise to SaaS

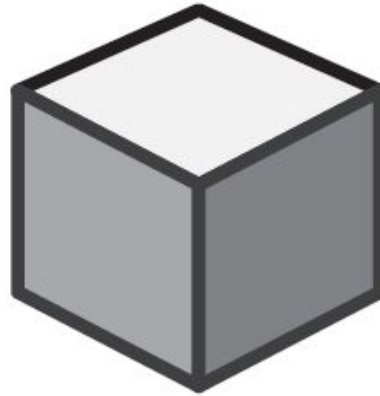


What is Crystal Box?



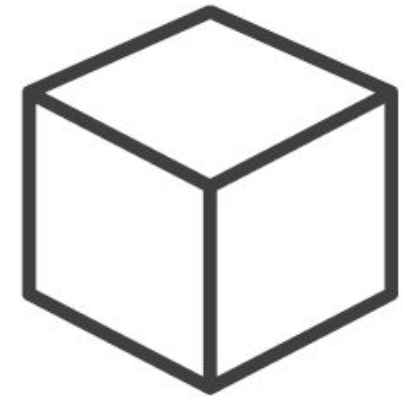
Black Box Testing

No information available,
except target addresses



Grey Box Testing

Some information available,
such as credentials to log in



Crystal Box Testing

Full information available,
including source code

Migration methodologies



1. Lift and Shift



2. Ad-Hoc



**3. SaaS /
Serverless**



**4. Future State
(Hybrid)**

Most of our clients work with a hybrid environment

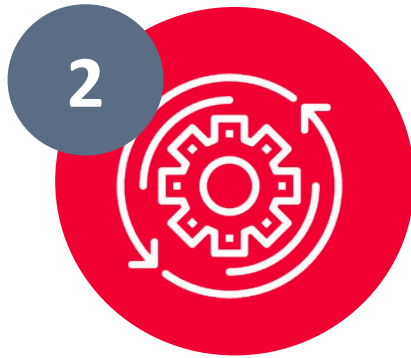
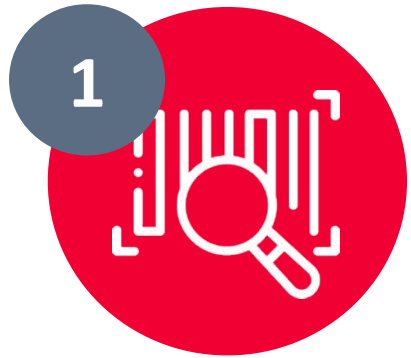
Risk Strategies



**Finding Vulnerabilities
& Addressing Them Is
Always Challenging!**



Type of Cloud Assessments



**Automatic
Compliance Scans**

**Automatic
Operational Scans**

**Non-Native Cloud
Elements Vulnerability
Assessment**

**Cloud Elements
Manual Configuration
Reviews**

**Identity & Access
Management
Review**

Easy >>>>>

Medium

>>>>>

Hard





Poll

**Which tests have you done in
your cloud environment?**

1. Automatic Compliance Test

CONCEPT

Best-practice cybersecurity standards for a range of IT systems and products. These baselines bring value and basic security to an environment, however you might still be at risk of an attack.



Often **performed automatically** with little or no effort, for instance, by starting companies.



Is a good starting point, but is **not enough**.



Be careful with false positives and negatives.



How Secure is a CIS/AWS Compliant Cloud Environment?



<https://www.secura.com/blog/how-secure-is-a-compliant-cloud-environment>

Examples

- Levels
- Scored vs not scored
- A lot of different ones

Cloud Providers

Alibaba Cloud

Expand to see related content ↓

Cloud Providers

Amazon Web Services

Expand to see related content ↓

Cloud Providers

Google Cloud Computing Platform

Expand to see related content ↓

Cloud Providers

Google Workspace

Expand to see related content ↓

Cloud Providers

IBM Cloud Foundations

Expand to see related content ↓

Cloud Providers

Microsoft 365

Expand to see related content ↓

Cloud Providers

Microsoft Azure

Expand to see related content ↓

Examples

3 Storage Accounts	115
3.1 Ensure that 'Secure transfer required' is set to 'Enabled' (Scored)	115
3.2 Ensure that 'Storage service encryption' is set to Enabled for Blob Service (Scored)	117
3.3 Ensure that storage account access keys are periodically regenerated (Not Scored).....	119
3.4 Ensure that shared access signature tokens expire within an hour (Not Scored)	121
3.5 Ensure that shared access signature tokens are allowed only over https (Scored)	123
3.6 Ensure that 'Storage service encryption' is set to Enabled for File Service (Scored)	125
3.7 Ensure that 'Public access level' is set to Private for blob containers (Scored).	127

How Do We Fix Them?



Azure PowerShell

Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server, enable auditing.

```
Set-AzureRmSqlServerAuditingPolicy -ResourceGroupName <resource group name> -  
ServerName <server name> -AuditType <audit type> -StorageAccountName <storage  
account name>
```

2. Automatic Operational Scans

CONCEPT

Automatic or semi-automatic scans that try to interpret results for us. E.g. cloud-built scans, networking, infra as a code, bad practices, etc.



Once normal compliance scans are covered this is a good idea. Still not enough to be more secure, but the **combination gives more security**.



If the cloud built-in scans are used they can be **expensive** (but good).



Be careful with false positives and negatives.



Examples

Search (Ctrl+/) <<

GENERAL

- Overview
- Security policy
- Quickstart
- Events
- Onboarding to advanced sec...
- Search

PREVENTION

- Recommendations
- Security solutions
- Compute
- Networking
- Storage & data
- Applications
- Identity & Access

Subscriptions Log Integration

Overview

Recommendations 15 Total	Security solutions 1 Stopped reporting	New alerts & incidents 0 0	Events - last week 18,6K Total
---	---	--	---

Prevention

Compute 31 Total	Networking 20 Total	Storage & data 23 Total	Applications 7 Total
-----------------------------------	--------------------------------------	--	---------------------------------------

Detection

Security alerts

HIGH SEVERITY	22
MEDIUM SEVERITY	4
LOW SEVERITY	1

Most attacked resources

mujWebWAF	16 Alerts
40.68.244.46	11 Alerts
motajump	1 Alerts

Examples

- ❗ EBS Volume Not Encrypted
- ❗ Potential Secret in Instance User Data
- ❗ Security Group Opens All Ports to All
- ❗ Security Group Opens DNS Port to All
- ❗ Security Group Opens FTP Port
- ❗ Security Group Opens MongoDB Port to All

Problem 136

```
[GEN003][WARNING] Block 'module.redshift:aws_redshift_cluster.main' includes a potentially sensitive attribute 'master_password' in its definition. See the documentation for 'aws_redshift_cluster' for more details.
/home/kali/Downloads/sadcloud-master/modules/aws/redshift/main.tf:27
```

```
24 resource "aws_redshift_cluster" "main" {
25   cluster_identifier = var.name
26   master_username    = "foo"
27   master_password    = "Password1"
28   node_type          = "dc1.large"
29   cluster_type       = "single-node"
30   skip_final_snapshot = true
```

How Do We Fix Them?

- Determine if they are **false positives**
- Is there a business reason?



X. Non-Cloud Elements Vulnerability Assessment

CONCEPT

An analysis of the non-native cloud elements running in the cloud. For example, virtual machines, databases, software, code, etc.



Companies that **migrate their infra** without or with few re-architecture.



Be careful with the false sense of security.



Non-cloud elements in the cloud **can be the entry point** to your environment.





Examples

- Unpatched OS
- Insecure images OS
- Software with known vulnerabilities
- Insecure code

From here, an **attacker** may pivot further.

How Do We Fix Them?

Same as with on-premise:

- Update
- Limit the attack surface
- Secure code



3. Cloud Configuration Review

CONCEPT

Based on automatic and semi-automatic scans further **manual test** is performed to assess the real impact of the vulnerabilities.



Companies that **want to be sure the configuration is secure** and are experts in interpreting the results.



Business logic and operational flaws are discovered here.



The point of this type of test is to **trigger a conversation** in the company to determine if the configuration is appropriate.





Examples

- Domain Controller virtual machine running in the environment
- Networking misconfiguration
- High availability misconfiguration
- Key management

How Do We Fix Them?

- Having conversations
- Was that a conscious decision?



4. Identity & Access Management Review

CONCEPT

Determine if privilege escalation or pivoting is possible in the environment. E.g., can an attacker that compromises a developer role become admin? Or can a low privilege cloud user access on-premise assets?



Companies with a **good understanding of cloud security** that can go further in their checks.

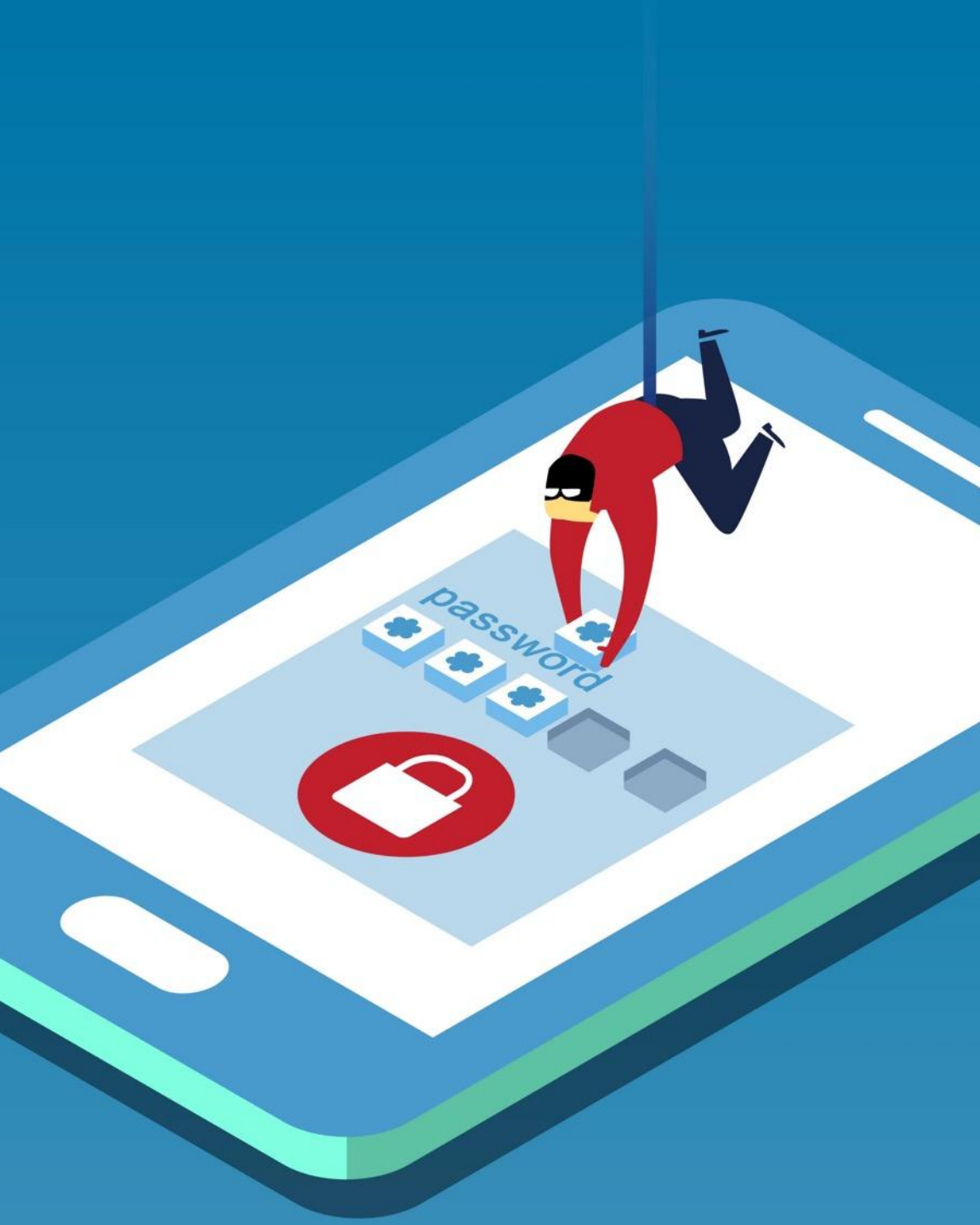


Difficult to perform correctly since a small configuration can have a big impact.



It often **involves other cloud components** (o365, github, etc).





Examples

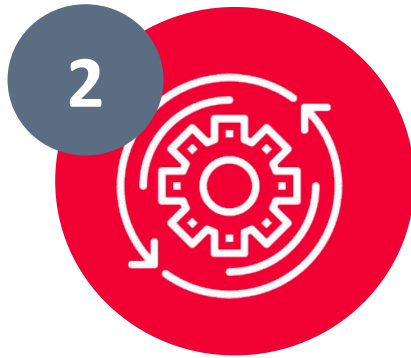
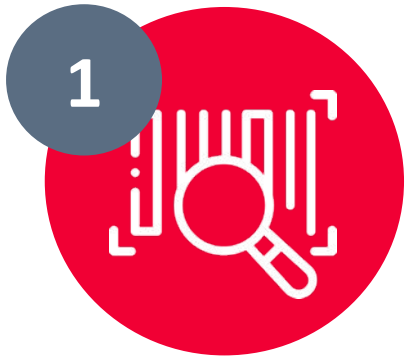
- Credentials saved in runbooks
- Information in environment variables
- Managed identities impersonation (abuse)
- Token extraction
- Conditional access and multifactor authentication bypass

How Do We Fix Them?

- Least privilege
- Compartmentalization
- Conditional Access
- Zero trust



Recap - Type of Cloud Assessments



Automatic Compliance Scans

Automatic Operational Scans

Non-Native Cloud Elements Vulnerability Assessment

Cloud Elements Manual Configuration Reviews

Identity & Access Management Review

Easy >>>>>

Medium

>>>>>

Hard



BrokenbyDesign: Azure

What can I do with this app?

This app will test your hacking skills in the Azure cloud space.

How do I submit flags?

All flags look have the format `SECURA{THIS_IS_4_FL4G}`.

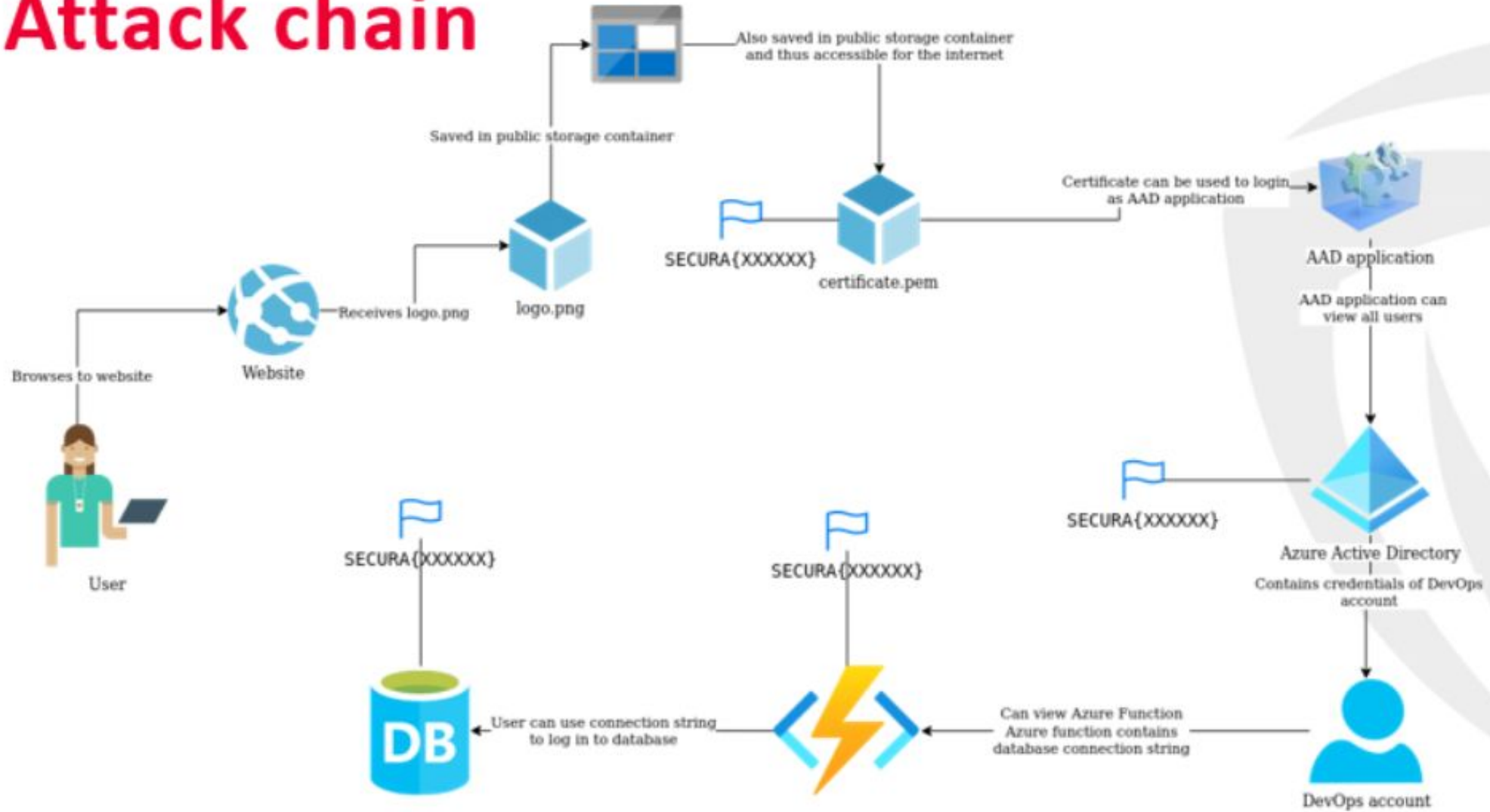
The Story

The company named SuperCompany B.V. has been working with IT systems for a while now and have an IT team of a whoppin' 2 people. Because the CEO of the company has heard that 'Cloud' is the new way of working, the CEO has asked the IT team to migrate all IT systems to the Azure cloud platform. Sadly, management does not allow the IT team to take courses or trainings to learn more about Azure cloud and so they have to learn as-they-go.

Get started!

Need a hint? Click [here!](#)

Attack chain



Conclusions

1. Cloud is a **different way of thinking**
2. Cloud **can provide a false sense of security**
3. It is possible to **pivot and privilege escalate**
4. If the **risks are addressed** this can be great for the business.
 - Accept, avoid, reduce and transfer
5. There are **multiple “levels” to address** cloud security
6. The **methods are complementary**
7. Some checks should trigger conversations within the company to **determine the proper risk level**



Thank you for your time and attention!



Ricardo Sanchez

Senior Security Specialist

Ricardo.Sanchez@secura.com

Follow us on:

