nviso

www.nviso.eu

Proposal to serve - Cloud Security Assessment

October 2021

Table of Contents

Introduction

Our Project Approach

Our References

Appendix A: About NVISO

Introduction

Your expectations and objectives

YOU EXPECT

You expect to understand whether **necessary security controls for their Azure resources and subscriptions** are in place and in accordance with cloud security best practices.

Furthermore, you want to understand the **areas of improvement** in their **design and architecture** of the cloud environment.

The current scope is estimated as the **main Azure environment and subscriptions**.

OUR RESPONSE

We will deliver the engagement using **industry best practices** and our **expertise**. The suggested option in this proposal is a **L2 Azure cloud security assessment**, which includes a design in-depth analysis.

Who is NVISO ?

NVISO is an independent European security consulting firm based in Brussels, Frankfurt and Munich. Security is our DNA and our sole focus. Our team consists of security experts that speak at conferences, research and publish on security, and have extensive experience in this field.

YOUR DELIVERABLE

A **detailed report** containing a non-technical summary, in-depth best practice evaluation descriptions (only L2), detailed descriptions of findings, **actionable recommendations** and references to additional sources of information, will be delivered.

At no extra charge, we can deliver a **management presentation** explaining the work we performed, the findings noted and the recommendations proposed.

We know cloud security

And actively stay on top of our game

Cloud environments are becoming increasingly complex, and complexity can introduce severe flaws with real consequences if they are not mitigated in time. Over the years, NVISO has built the right toolset and expertise to tackle a broad range of cloud features and cloud related technologies.

We break barriers – We research new technologies and share our findings with the community.

See Azure Automation, Detect ZeroLogon, Azure security logging

We build the tools – We created a PowerShell and python scripts to assess several cloud functionalities and collect evidence to look at misconfigured settings.

We help define the standards – We are recognized and contribute to the Microsoft Intelligent Security Association and are MS Gold Partner.

We share our expertise – Within the cyber security coalition we organized the cloud experience sharing day.

We are certified – Our team has several certificates such as GDAPT, AZ-500, MS-500 CSSP (Certified Cloud Security Professional).

NVISO also develops courseware related to SANS 401 which includes an introduction towards cloud security.

Cloud Security Services

An overview of our cloud services

In case you are thinking about **moving towards the cloud** or you are **already in the cloud** NVISO can assist you in both cases. Our cloud security services can range from an integrated security design in your new environment to reviewing your current infrastructure via our standardized security assessment.

Cloud Security Assessment

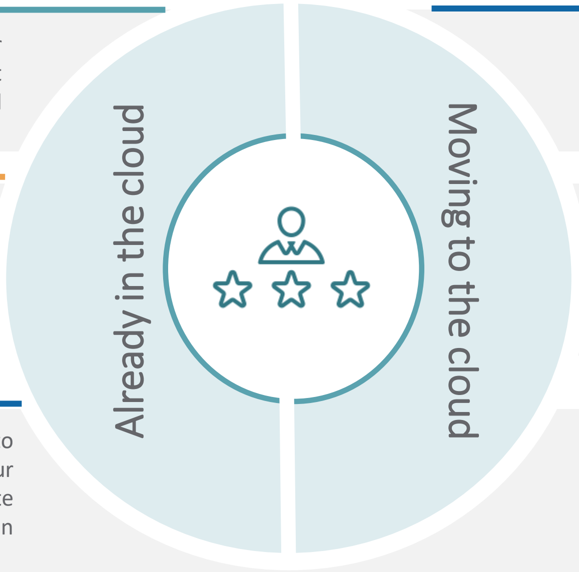
How secure your current environment is? Our assessment provides you an overview about your current exposure, missing security controls or typical misconfigurations within cloud environments.

Cloud security engineering

As your cloud environment is changing, you will need to review and adapt your security requirements continuously. After **an intake of the current setup** our security architects will **review changes and support your operational teams.**

Cloud security compliance

As new cloud resources are deployed, you will need to ensure that **compliance** of each cloud resource to your **corporate security standard**. NVISO can help you create automated compliance checks and reporting to gain visibility and additional compliance rules.



Cloud secure design

NVISO can assist **you within the design process to integrate security in your design** based on your requirements, industry best practices and our technology expertise.

Cloud security architect

Continuously integrate our security expertise in your cloud environment. During the design phase we will **define and review the security controls**, in a later stage our security architects review **ongoing changes and support your operational teams.**

Cloud security roadmap

Define the security roadmap for the cloud services used withing your organization through workshops and setup cloud infrastructure for your organization defining **quick wins and structural recommendations**.

How and where we can help you

NVISO and Microsoft, a strong partnership

nviso

Whether you are already in the cloud, or you are planning to move, NVISO can guide you throughout your cloud migration journey.

Microsoft

Microsoft 365 CERTIFIED
SECURITY ADMINISTRATOR
ASSOCIATE
★★

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE
★★

Our expertise in Microsoft solutions includes a wide range of services on different MS products.

NVISO significantly invested in Microsoft certifications and today our people is widely certified in both AZ-500 and MS-500 exams.

Azure

- Azure Security Assurance
- Azure Security Review
- Azure Compliance Automation

Intune

- Secure Implementation
- Security Review

Microsoft 365

- Cloud Security Roadmap
- Windows Security Hardening

Office 365

- Security Roadmap
- Secure Engineering
- Security Review

Our Project Approach

How we will structure this project

Security Assessment Levels

What will we investigate in our assessments?

Within the cloud security assessment service, we have defined three levels for which our consultants will do an increasingly in-depth analysis of the security of your cloud environment. This is done against industry best practices and with known attack techniques and tools.

L1

CIS Benchmarks™

Cloud Baselines & Automated checks

Baseline Security Check

- Gap Analysis Report
- Risk Assessment
- Actionable Recommendations

4 MD*

<

L2

Cloud Best Practices & Controls

Manual In-depth Analysis

- Workshop to gain insights in application/infrastructure context
- In-depth architectural analysis
- External attack surface discovery, focused on getting initial access

L1 + 4 MD = **8 MD***

<

L3

ATT&CK™

Cloud ATT&CK Tactics & Techniques

TTP Validation

- MITRE ATT&CK cloud techniques validation
- Security posture against real attack vectors
- Detailed mapping on framework

L1 + L2 + 4 MD = **12 MD***

All assessment levels are enriched with our own cloud expertise.

Recommended Assessment Level for this environment:

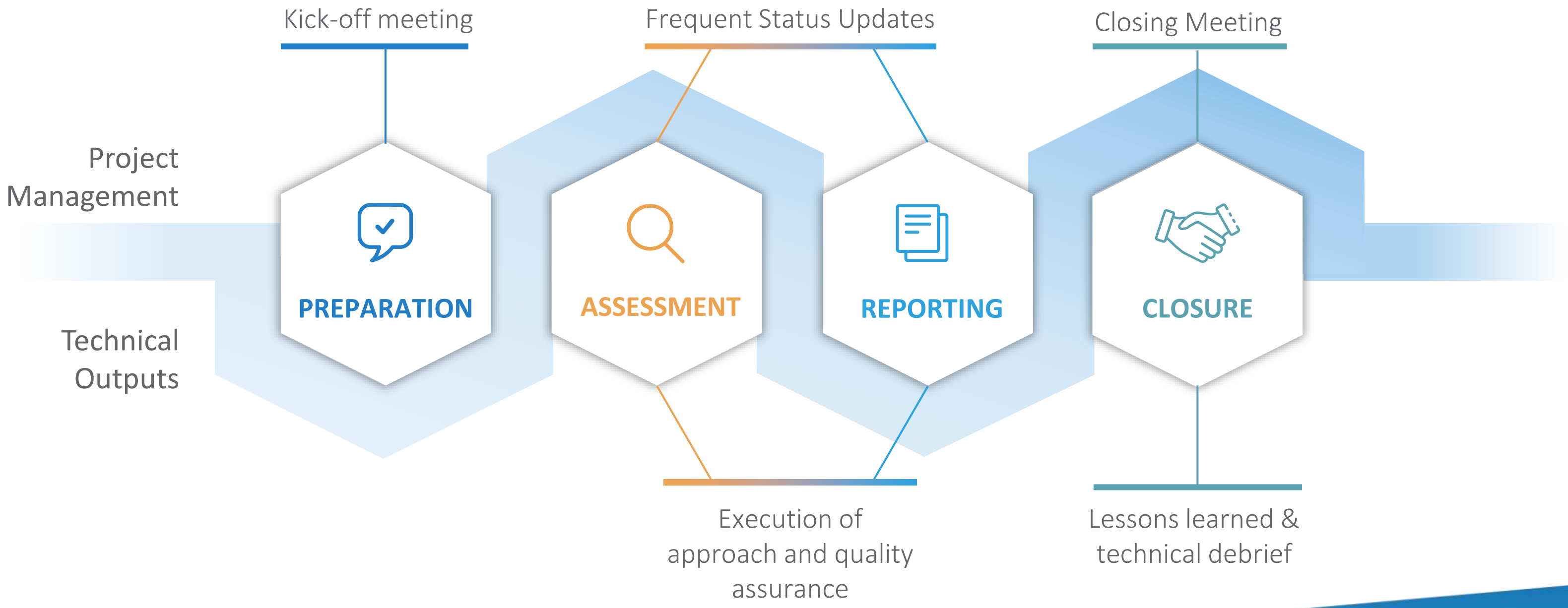
L2

* MD estimated for one average application/environment

Our Approach

An overview of our project method used

Our NVISO security assessment methodology can be summarized as:



Our Approach

An overview of our project method used

Based on widely accepted best practices and standards for cloud security and our experience with designing and implementing cloud environments, we will assess your cloud environment with the following approach:

Identify Requirements

During the first phase, we will together with you:

- Identify **security requirements** based on your organization and project
- Decide **security level** for the specific cloud infrastructure: fundamental, industry standard, and advanced

Validate Controls

Based on the information obtained in the first phase, we will execute:

- **Security baseline** checklist validation with automated tools, custom-built scripts and manual review steps
- L2 Architectural in-depth analysis compared to reference architecture
- L2 External attack surface discovery
- L3 TTP validation
- Definition of **key findings**

Recommend & Report

After the validation of the implemented controls, we will:

- Estimate impact, likelihood and **overall risk related to your business**
- Create **actionable recommendations**
- Define the **priority** of the recommendations
- L2 Suggest structural improvements to your cloud organization

Technologies

Microsoft Azure

Office 365

Preparation

Kick-off meeting and Objectives

Identify Requirements

During the **kickoff meeting**, we will discuss with you the exact project requirements for the engagement, the planning and we will aim to get **insights** in your environment and application.

Additionally, we will estimate together with you the desired **level of security** that we will use to benchmark your configuration.

Many organizations are looking into cloud solutions and many features exist to protect your environment. Based on what you want to protect, the risk appetite and budget, different controls can be implemented. Therefore, we built our security baseline on three levels of security: fundamental, industry standard, and advanced. We base our risk and priority ratings on these levels.

Desired level of security

Fundamental

●

The fundamental level of security is related to organizations requesting basic security features within their infrastructure. The organization wants to be **protected against generic, well-known attacks**. They will use the basic functionalities as provided by cloud providers like Azure or AWS.

Industry standard

● ●

The industry standard level of security is related to organizations requesting security controls that are in line with industry best practices and compliant with certain regulations. Recommendations are based on security controls that are implemented **within your specific industry** and your specific infrastructure.

Advanced

● ● ●

The advanced level of security is related to organizations embedding security into their business model. These organizations are risk-aware and want to invest into **more advanced security controls**. These type of security controls will help you to prevent and detect cyber attacks in an efficient manner within your infrastructure.

Assessment

How will we execute our assessment? (L1)

Validate Controls

The **security baseline checklist** with controls that NVISO defined based on authoritative sources, like the CIS Benchmarks and cloud provider documentation, will be validated with **automated tools**, custom-built scripts and manual checks. Nine different categories have been defined.

CIS Benchmarks™

Security Baseline Categories

Identity and Access Management
Ensure a secure configuration of IAM and prevent unauthorized access by applying strong authentication mechanisms and the least-privilege principle.

Configuration Management
Ensure that assets are managed, security assessments performed, and patches deployed.

Logging
Enable logging of cloud elements and make them available for monitoring and long-term retention. Make sure that access is restricted to logs.

Security Services
Enable security monitoring and threat detection by applying a fine-grained configuration of the security services and applying security policies.

Monitoring
Enable monitoring of suspicious activities and deviations from a security baseline and configure corresponding alerts and automated remediation.

Web Protection
Protect web applications and apply additional protection techniques with application gateways, API gateways and WAFs.

Networking
Verify if network security groups/firewalls are correctly configured and logged. Make sure that accesses from the Internet are restricted.

Business Continuity
Ensure that services and data remain available when operational issues occur.

Data Protection
Apply data encryption for data in rest and in transit, decent logging and restricted access to storage. Protect encryption keys.

Assessment

How will we execute our assessment? (L2)

Validate Controls

In a L2 cloud security assessment, NVISO dives deeper into the customer environment by performing a manual **in-depth analysis** of the main security components of the cloud environment and the business flows of the cloud application. We will actively sit together with your teams during a **workshop** to discuss the application, the cloud environment and the foreseen security controls.

Additionally, **structural improvements to the overall architecture** will be validated. The in-depth analysis is based on industry best practices, well-architected frameworks and our own expertise.

L2

Microsoft Azure amazon web services Google Cloud

In-depth architectural analysis

Identity and Access Management

We perform an in-depth analysis of the different identities, roles, and privileges of the different services and users within the cloud environment. Based on the business flows of the application, we evaluate the least-privilege principle and RBAC/ABAC models.

Networking

We consider the validation of the business data flows of the application and map them to the network flows in the cloud in order to detect excessive network openings. These could lead to undesired external exposure or ineffective network segregation.

Logging and Monitoring

We investigate the centralized logging and monitoring approach in order to get visibility across different cloud environments. Additionally, we evaluate secure configuration controls that ensure basic security is implemented and alert on misconfigurations.

Assessment

How will we execute our assessment? (L2)

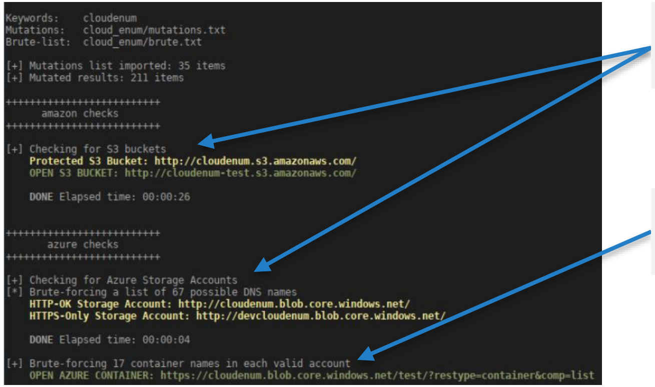
Validate Controls

NVISO will perform an **external attack surface discovery** exercise to determine if the cloud environment is vulnerable to the most common **initial attack vectors** as defined in the MITRE ATT&CK framework.

We simulate tools and techniques known to be used by adversaries against cloud resources. The goal of this exercise is to visualize the external exposure and to identify techniques to **gain initial access** to the cloud environment: public IP discovery; port and vulnerability scanning; exposed services detection, e.g. storage or databases; user/role enumeration.

L2

External attack surface discovery



```
Keywords:    cloudenum
Mutations:   cloud_enum/mutations.txt
Brute-list:  cloud_enum/brute.txt

[+] Mutations list imported: 35 items
[+] Mutated results: 211 items

++++++++++++++++++++++++++
      amazon checks
++++++++++++++++++++++++++

[+] Checking for S3 buckets
    Protected S3 Bucket: http://cloudenum.s3.amazonaws.com/
    OPEN S3 BUCKET: http://cloudenum-test.s3.amazonaws.com/

    DONE Elapsed time: 00:00:26


++++++++++++++++++++++++++
       azure checks
++++++++++++++++++++++++++

[+] Checking for Azure Storage Accounts
[*] Brute-forcing a list of 67 possible DNS names
    HTTP-OK Storage Account: http://cloudenum.blob.core.windows.net/
    HTTPS-Only Storage Account: http://devcloudenum.blob.core.windows.net/

    DONE Elapsed time: 00:00:04

[+] Brute-forcing 17 container names in each valid account
    OPEN AZURE CONTAINER: https://cloudenum.blob.core.windows.net/test/?restype=container&comp=list
```

Enumerate publicly accessible cloud resources

Brute-force publicly accessible cloud resources

Tools

MicroBurst TOOLS.NETSPI.COM

Pacu: The Open Source AWS Exploitation Framework

STORMSPOTTER

NMAP

ROADtools

Reporting

Presenting our findings and recommendations

nviso

Recommend & Report

Based on the outcome of the validation of security controls, we define a **finding** for each misconfiguration or weakness that has been identified. Per finding we will estimate the impact, likelihood and **overall risk** related to your **specific business and application needs**.

Actionable recommendations are formulated for each finding to improve the overall security posture of the cloud infrastructure. The **priority** for each finding is a result of the overall risk combined with the difficulty of implementation for that specific recommendation .

During the engagement you will be made immediately aware of critical risk findings, other findings will be raised during the reporting phase.

The **detailed report** will be made available to you in PDF format, together with supporting evidences that can be used for training or help in remediation steps.

Report structure

Executive Summary

Describes the business impact of the identified findings and general recommendations.

Project Information

Provides an overview of the scope, objectives, and approach.

L2 Cloud Security in-depth analysis

Describes in detail all the best practices that have been evaluated during the in-depth analysis, including the passed best practices.

L2 External Attack Surface Discovery

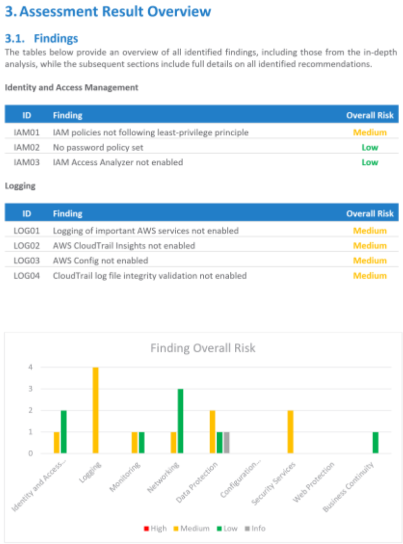
Describes the output of the different tools that have been used during the external attack surface discovery exercise and the interpretation of the results.

L2 + L3 MITRE ATT&CK Framework

Provides an evaluation of the mitigation and detection capabilities in place for MITRE ATT&CK techniques.

Cloud Security Assessment Findings

Covers all findings from the different security control validation steps, including a technical description, a risk estimation (business & technical), and recommendations with priority rating



3. Assessment Result Overview

3.1. Findings

The tables below provide an overview of all identified findings, including those from the in-depth analysis, while the subsequent sections include full details on all identified recommendations.

Identity and Access Management

ID	Finding	Overall Risk
IAM01	IAM policies not following least-privilege principle	Medium
IAM02	No password policy set	Low
IAM03	IAM Access Analyzer not enabled	Low

Logging

ID	Finding	Overall Risk
LOG01	Logging of important AWS services not enabled	Medium
LOG02	AWS CloudTrail Insights not enabled	Medium
LOG03	AWS Config not enabled	Medium
LOG04	CloudTrail log file integrity validation not enabled	Medium

Closure

What will we provide after the execution of the project?

Technical Workshop

A **technical workshop** with your teams to ensure our methodology and used vulnerability chaining is technically captured to allow remediation. This session will be conducted based on the report, ensuring the details of all findings and recommendations is perfectly understood by all involved;

1

Management presentation

A **complimentary management presentation** to explain the work performed, the type of issues noted, their potential impact and highlight key improvement areas to further increase the security posture of the organization. We will focus on the higher risks and will ensure our explanations are easily understandable to a non-technical audience;

2

Feedback session

A **customer feedback** session to understand and capture the lessons learned from our end and your end, in order to further improve our collaboration in the future.

3

Our References

Some of our success stories

Some of our references

We have done this before – Cloud Security

Cloud Security Architect	Industry: **Utilities** Workload / Cost : **20 MD/ Year** Country: **Global**	NVISO has been elected as a service provider for all cloud security architecture on Azure and Office 365 for a global company that provides services to the utilities sector. This engagement include architecture reviews of the current setup, define and propose a blueprint that is NIST compliant and assisting future projects with the configuration and optimization of security features within Azure and O365.
Cloud Security Incident	Industry: **Financial services** Workload / Cost : **5 MD** Country: **Belgium**	Within NVISO we have a managed detect and respond team and several contracts with our clients to detect and respond on security incidents. NVISO involves cloud security experts in case a cloud security incident was detected. During the incident NVISO was able to provide insight into the O365 account compromise and the data that was exfiltrated during the attack. Based on the incident we provided actionable recommendation to improve the detect and respond capabilities within that organization.
Hybrid Monitoring model	Industry: **Pharmacy** Workload / Cost : **17MD** Country: **Belgium**	NVISO developed a SOC target operations model including a hybrid setup. The objective was to benefit from the cloud security toolset and integrate this with a centralized monitoring solution. Within this model we were able define the governance structure and processes within that organization. Technical use case implementation was done based on the MITTRE ATT&CK Framework.
Cloud Security Assessment	Industry: **Financial services** Workload / Cost : **7 MD** Country: **Belgium**	NVISO was requested to review an API based banking platform developed in the cloud, this projects was part of the PSD2 guidelines published by the European Central Bank. The application was hosted in AWS and we executed several compliancy checks against the CIS benchmarks to identify potential gaps and additionally a penetration test was performed on this environment.

For confidentiality reasons, we may not disclose our customers' names: upon request, however, we are happy to request our customers to be contacted by your team for reference.

Appendix A

About NVISO

About NVISO

Get to know us better

Our Company

NVISO is a pure play **Cyber Security consulting firm** since 2013 with 90+ specialized security experts.

Initially founded in **Belgium**, we opened offices in **Germany** (Frankfurt & Munich) in 2018!

Our mission is to **safeguard the foundations of European society from cyber attacks**.

Our DNA

Pride: We are proud of who we are and what we do.

We care: We care about our customers and people.

Break barriers: We challenge the status quo by continuous innovation.

No BS: We keep our promises and don't fool around.

Our Research

We invest 10% of our annual revenue in research of new security techniques and the development of new solutions.

Follow us on :

@NVISOsecurity and
@NVISO_Labs

blog.nviso.eu/

Our Services

We have a **strong track record** providing information and cyber security services to the **Financial Services**, **Government & Defense** and **Technology** sector.

NVISO can support you throughout the **entire cyber security incident lifecycle**.

HACKED?

CALL
+32 (0)2 588 43 80

NVISO • Security. Research. Risk.

www.nviso.eu

nviso