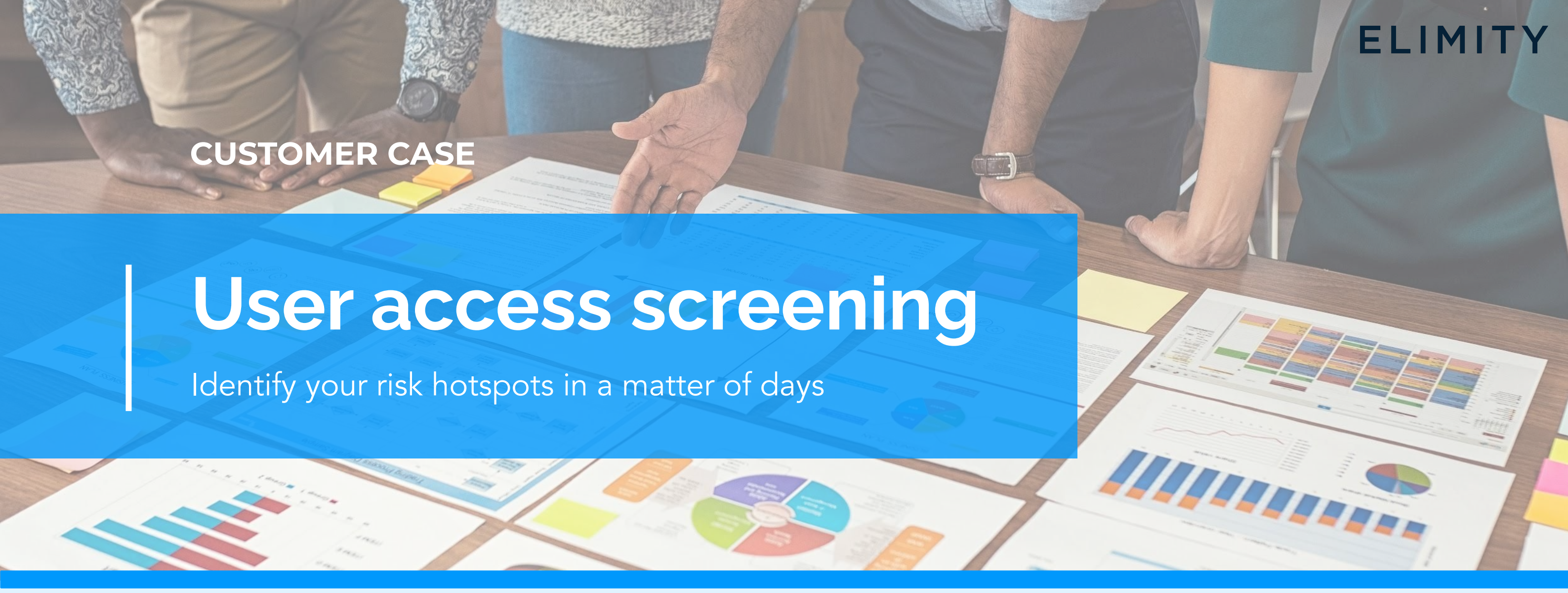


ELIMITY

CUSTOMER CASE

User access screening

Identify your risk hotspots in a matter of days

SUMMARY

As so many organizations, our client, active in the manufacturing industry, wanted insights in its current IT risk posture.

They knew they had too little control over the accounts and their accesses, but had no comprehensive overview of the situation. As a result, they didn't know exactly what the situation was and where the biggest risks were located. That, in turn, kept them from convincing management to free up resources in order to take action.

To help the client, we performed an in-depth analysis of the key access risks residing in and across their most important applications, and provided them with a report including our findings and recommendations. In just 3 days of work, this enabled them to understand their access risks and gave them objective numbers to support decision-making with regard to next steps.

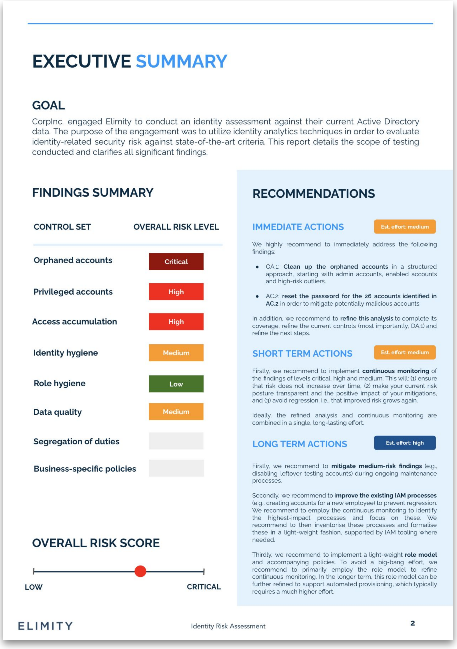
RESULT

We provided our client with a detailed report of the key access risks in **just a couple of days** and gave them access to our platform so they could dig a little deeper into the results themselves.

IMPACT

Using technology to perform an in-depth analysis gave our client the insights they needed to understand their access risks and enabled them to let others understand them as well.

They used these insights to support the development of the identity roadmap. First stop: clean-up to improve the IT risk posture.



EXECUTIVE SUMMARY

GOAL

CorpInc. engaged Elimity to conduct an identity assessment against their current Active Directory data. The purpose of the engagement was to utilize identity analytics techniques in order to evaluate identity-related security risk against state-of-the-art criteria. This report details the scope of testing conducted and clarifies all significant findings.

FINDINGS SUMMARY

CONTROL SET	OVERALL RISK LEVEL
Orphaned accounts	Critical
Privileged accounts	High
Access accumulation	High
Identity hygiene	Medium
Role hygiene	Low
Data quality	Medium
Segregation of duties	
Business-specific policies	

OVERALL RISK SCORE

LOW CRITICAL

RECOMMENDATIONS

IMMEDIATE ACTIONS Est. effort: medium

We highly recommend to immediately address the following findings:

- OA.1: **Clean up the orphaned accounts** in a structured approach, starting with admin accounts, enabled accounts and high-risk outliers.
- AC.2: **reset the password for the 26 accounts identified in AC.2** in order to mitigate potentially malicious accounts.

In addition, we recommend to **refine this analysis** to complete its coverage, refine the current controls (most importantly, DA.1) and refine the next steps.

SHORT TERM ACTIONS Est. effort: medium

Firstly, we recommend to implement **continuous monitoring** of the findings of levels critical, high and medium. This will: (1) ensure that risk does not increase over time, (2) make your current risk posture transparent and the positive impact of your mitigations, and (3) avoid regression, i.e., that improved risk grows again.

Ideally, the refined analysis and continuous monitoring are combined in a single, long-lasting effort.

LONG TERM ACTIONS Est. effort: high

Firstly, we recommend to **mitigate medium-risk findings** (e.g., disabling leftover testing accounts) during ongoing maintenance processes.

Secondly, we recommend to i**mprove the existing IAM processes** (e.g., creating accounts for a new employee) to prevent regression. We recommend to employ the continuous monitoring to identify the highest-impact processes and focus on these. We recommend to then inventorise these processes and formalise these in a light-weight fashion, supported by IAM tooling where needed.

Thirdly, we recommend to implement a light-weight **role model** and accompanying policies. To avoid a big-bang effort, we recommend to primarily employ the role model to refine continuous monitoring. In the longer term, this role model can be further refined to support automated provisioning, which typically requires a much higher effort.

ELIMITY Identity Risk Assessment 2

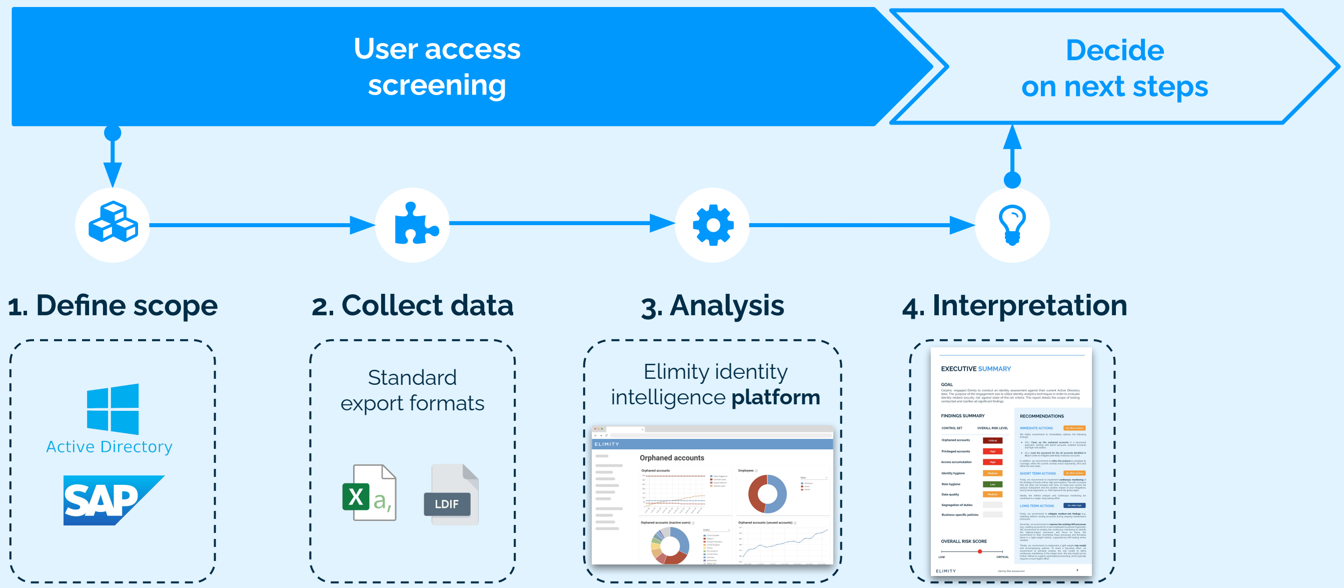
APPROACH

We provided our client with a detailed report of the key access risks in **just a couple of days** and gave them access to our platform so they could dig a little deeper into the results themselves.

- **Focus on actual risk**
  As opposed to typical IAM assessments, we don't focus on the presence of governance processes, but on the actual IT risk present in the existing accounts and their accesses. This allows the customer to prioritize clean-up efforts for maximal risk reduction and efficiently introduce governance processes later on.

- **Data-driven**
  We put identity and access data to work with our dedicated technology allowing for a more cost-efficient but also more in-depth analysis of the IT risk posture.

- **Non-invasive**
  We conduct the screening without impacting operational systems. There’s no need to deploy agents or make changes to the infrastructure.



1

Define scope

We started with defining the scope of the screening. As our client was particularly concerned about orphaned accounts and their use for attacks such as ransomware, the screening at least had to cover those applications so that orphaned accounts could be detected. On top of that, we identified the applications where most of the relevant identity data resides. The scope: Active Directory, SAP HR and SAP ERP. They didn’t have a dedicated IAM system yet, otherwise that would have been part of the scope as well.

2

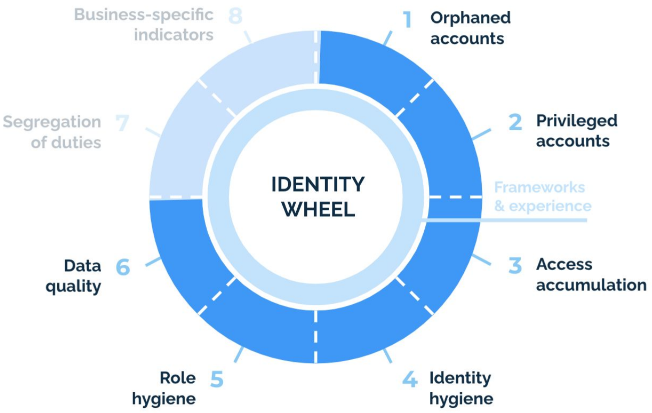
Collect data

We then collected and consolidated the relevant identity data from those applications in our platform. To avoid setting up costly data connections specifically for this screening, we quickly imported the data from the standard export formats of these systems (i.e., Excel sheets and CSV files) using our out-of-the-box and custom connectors.

3

Analysis

With powerful identity analytics and a comprehensive set of out-of-the-box controls, our platform instantly measures the results for various key access risks (see figure below). For some controls customization took place in terms of modification of some out-of-the-box controls and creation of several new controls specific for their operations.



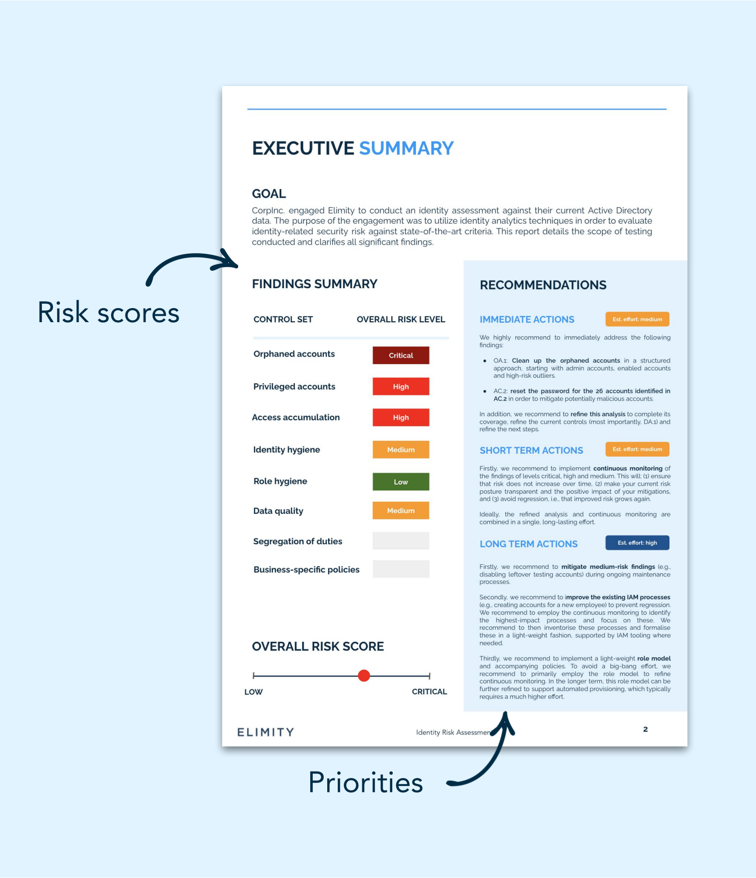
In most cases, the screenings we perform include orphaned accounts, privileged accounts, access accumulation, identity hygiene and role hygiene. However, some of our clients also want to assess how well their SoD policies are being followed in practice. That requires different input from the client than the identity data, namely the SoD policies themselves. As a result, this is often considered as a dedicated project. A similar way of working is often followed in case of assessing heavy, overarching specific policies.

Read more about the 8 key identity indicators
(www.elimity.com/prove-control-guide)

4

Interpretation

Our platform allowed us to dig a little deeper into the results to investigate the inherent risk associated with the findings. This allowed our team of experts to understand the nature of the risks and enabled them to interpret the results and provide recommendations in terms of priorities.


Risk scores

Priorities

EXECUTIVE SUMMARY

GOAL

CorpInc. engaged Elimity to conduct an identity assessment against their current Active Directory data. The purpose of the engagement was to utilize identity analytics techniques in order to evaluate identity-related security risk against state-of-the-art criteria. This report details the scope of testing conducted and clarifies all significant findings.

FINDINGS SUMMARY

CONTROL SET	OVERALL RISK LEVEL
Orphaned accounts	Critical
Privileged accounts	High
Access accumulation	High
Identity hygiene	Medium
Role hygiene	Low
Data quality	Medium
Segregation of duties	
Business-specific policies	

OVERALL RISK SCORE

LOW — CRITICAL

RECOMMENDATIONS

IMMEDIATE ACTIONS — Est. effort: medium

We highly recommend to immediately address the following findings:

- OA.1: **Clean up the orphaned accounts** in a structured approach, starting with admin accounts, enabled accounts and high-risk outliers.
- AC.2: **reset the password for the 26 accounts identified in AC.2** in order to mitigate potentially malicious accounts.

In addition, we recommend to **refine this analysis** to complete its coverage, refine the current controls (most importantly, DA.1) and refine the next steps.

SHORT TERM ACTIONS — Est. effort: medium

Firstly, we recommend to implement **continuous monitoring** of the findings of levels critical, high and medium. This will: (1) ensure that risk does not increase over time, (2) make your current risk posture transparent and the positive impact of your mitigations, and (3) avoid regression, i.e., that improved risk grows again.

Ideally, the refined analysis and continuous monitoring are combined in a single, long-lasting effort.

LONG TERM ACTIONS — Est. effort: high

Firstly, we recommend to **mitigate medium-risk findings** (e.g., disabling leftover testing accounts) during ongoing maintenance processes.

Secondly, we recommend to i**mprove the existing IAM processes** (e.g., creating accounts for a new employee) to prevent regression. We recommend to employ the continuous monitoring to identify the highest-impact processes and focus on these. We recommend to then inventorise these processes and formalise these in a light-weight fashion, supported by IAM tooling where needed.

Thirdly, we recommend to implement a light-weight **role model** and accompanying policies. To avoid a big-bang effort, we recommend to primarily employ the role model to refine continuous monitoring. In the longer term, this role model can be further refined to support automated provisioning, which typically requires a much higher effort.

ELIMITY — Identity Risk Assessment — 2

Want increased visibility in your access risks?

Get in touch

ELIMITY

Corporate Headquarters
Motstraat 30
2800 Mechelen, Belgium

Global Offices
EU +32 (0) 474 907 266
UK +44 (0)20 7129 7069

Reach us by mail
info@elimity.com