INTERNSHIP

Cybersecurity: Identity under fire

Description of the assignment

Nearly every modern cyberattack starts or ends with a compromised identity. In this internship, you get to see both sides of that story: first you attack a realistic enterprise identity environment yourself, then you make sure those same attacks no longer work.

During this internship, you will take on the role of a Junior Security Consultant and focus on securing digital identities within an enterprise environment. Active Directory (AD) and Microsoft Entra ID, the backbone of identity in most organizations, are at the core of this assignment.

You will work in an existing, realistic identity lab consisting of an on-premises Active Directory environment and, depending on the duration of your internship, a synchronized Microsoft Entra ID tenant. You will then investigate how identity-based attacks are carried out, identify weaknesses within the environment, and research how attackers exploit these vulnerabilities in a controlled lab setting.

Based on your findings, you will assess the associated risks, implement security controls using Silverfort, and evaluate the effectiveness of the improvements. Throughout the project, you will learn to think from both an attacker's and a defender's perspective, developing the ability to understand and bridge the gap between the two.

You will receive a roadmap that defines the objectives, milestones, and review points, but you will be responsible for determining the approach, selecting the tools, conducting research, and deciding the depth of your analysis. A basic understanding of networking and authentication concepts such as Kerberos and NTLM helps you get started quickly. Any knowledge gaps will be addressed during the first weeks of the internship.

The lab environment is already set up and documented, so you can focus from day one on attack research, privilege escalation techniques, identity abuse scenarios, and the corresponding defensive measures. Along the way, you will work with tools that are widely used in the field, such as BloodHound, Impacket, Rubeus, Mimikatz, and PingCastle, and explore scenarios like Kerberoasting, AS-REP roasting, DCSync, and ACL abuse. You will also develop your own scripts and tools to automate attacks and security checks.

Throughout the internship, you will regularly present your progress, research findings, and recommendations. These presentations are an important part of the evaluation process and help ensure that the project remains aligned with the learning objectives. At the end of the internship, you will deliver a comprehensive report summarizing the identified risks, executed tests, implemented security controls, and strategic recommendations for a fictional customer.

Objectives

- Analyze the provided Active Directory lab environment and identify identity-related security weaknesses.
- Reproduce and demonstrate common Active Directory attack techniques using industry-standard tooling and your own scripts.
- Implement and validate security improvements through Active Directory hardening and Silverfort controls.
- Measure the effectiveness of defensive measures by comparing attack success before and after mitigation.
- Depending on the duration of the internship, extend the analysis to hybrid identity scenarios in Microsoft Entra ID.
- Deliver actionable technical and business-oriented security recommendations based on the findings.

Technologies & concepts involved

- **Entra ID**
- **Active Directory**
- **Application Development**
- **Red Teaming**
- **Silverfort**
- **Blue Teaming**
- **Networking**
- **Vulnerability Assessment**

Approach & timeline

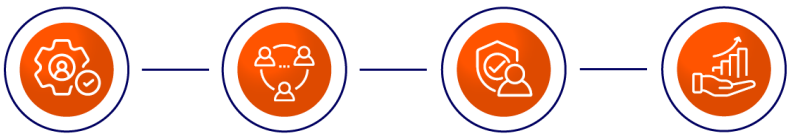
You will work in short iterations with regular check-ins and feedback from your supervisor, so you always know where you stand and can adjust course quickly. The internship roughly follows these phases:

1. **Onboarding (weeks 1–2):** get to know the lab, the roadmap, and Silverfort, and close any knowledge gaps.
2. **Attack research:** map the attack surface of the lab and reproduce identity-based attacks.
3. **Hardening and Silverfort:** implement Active Directory hardening measures and Silverfort controls.
4. **Measurement and reporting:** repeat the attacks, compare the results before and after mitigation, and finalize your report and recommendations.

What you'll gain

- Hands-on experience with real-world identity attack and defense techniques in a safe lab environment.
- Practical experience with Silverfort, a modern identity security platform.
- Personal coaching from experienced ACEN security consultants throughout the internship.
- Presentation and reporting skills that every security consultant needs.
- A final report and demos you can add to your portfolio.
- A look behind the scenes at ACEN, a European cybersecurity advisory firm that helps organizations understand, manage, and reduce their cyber risk.

Profile



The ideal intern is first and foremost motivated to improve their skills and learn about a new field of technology.

A student in cybersecurity, systems and network administration or a related field, who is curious, does not accept "it just works" as an answer and enjoys explaining things. Hands-on experience with Active Directory is a plus. No prior Silverfort experience is required; you will be introduced to it during the internship. Comfort with Windows Server, PowerShell and at least one scripting language helps. Good written and spoken communication is essential.

Not ticking every box? Apply anyway. Curiosity and motivation matter more to us than a perfect match.

Contact details

Contact person	Cindy Van den Hoecke	**cindy.vandenhoecke@acen.eu**
Internship Supervisor	Kelvin Bogaerts	**Kelvin.Bogaerts@acen.eu**