ORLOX

internship assignment

Digital Workplace: Protect enterprise assets using Microsoft XDR, SOAR and SIEM

CONTACT

Kristof Laerenbergh

Veldkant 33, 2550 Kontich
info@orlox.be
www.orlox.be

TABLE OF CONTENTS

About Orlox **3**

About this Internship assignment **4**

ABOUT ORLOX

Working from home, checking your agenda, and planning on your phone, making videocalls from a coffee shop, helping a colleague from abroad, making notes on your tablet… all obvious these days.

A good thing because the digital workplace has a positive influence on the productivity and efficiency of employees. However, many organizations are not quite ready to keep that digital workplace up to date and secure.

Orlox is a company within the Cronos group specializing in securing the digital workplace. We support our clients by having infrastructure & development teams working closely together from modern identity to modern business applications.

As Orlox we offer services based on the following pillars within an IT environment

- Identity & Access Management
- Endpoint & Messaging Security
- Infrastructure Services
- Data Protection

Thanks to the expertise of our people, we can combine this knowledge to develop solutions that can help our customers increase their overall way of working by providing them with the tools they need to keep their environment safe.

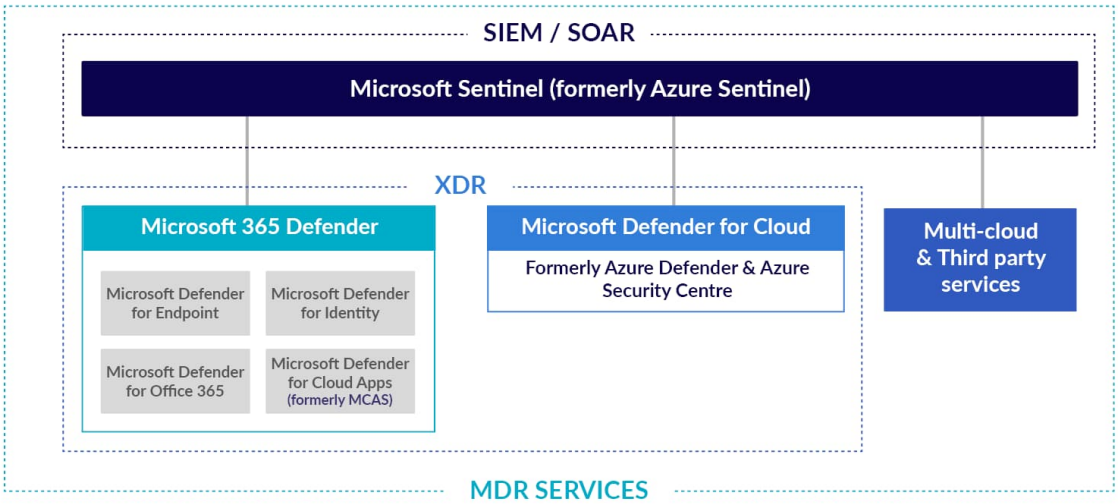
ABOUT THIS INTERNSHIP ASSIGNMENT

Cyber-attacks are becoming more common, with a serious IT breach making headlines every other day. Attackers constantly look to exploit any gap in IT systems, applications, and hardware. One of the key security approaches to prevent and combat attacks is to identify and respond to security events in real-time to minimize the damage.

To achieve this SIEM and SOAR solutions become a must-have for every organization. Security Information and Event Management Software (SIEM) allows security teams to keep on top of security alerts in real time.

The SOAR solution (security orchestration, automation & response) uses the gathered data on security issues to automate the response. SOAR also uses artificial intelligence to predict and respond to similar future threats.

As Orlox mainly focuses on Microsoft technologies, the student will explorer and implement all solutions within the M365 security framework.



This internship assignment exists out of 3 main parts

- Perform research about the Microsoft XDR, SIEM, and SOAR solutions and document these
- Set up a basic hybrid IT environment for testing
- Set up and configure the M365 security products and automate alerting, remediation of security breaches, and management tasks.

The student will be coached by an experienced and certified Microsoft security architect of the team.