INTERNSHIP

Exploring Cybersecurity Operations with Microsoft Sentinel

Description of assignment

In an era where digital threats have gotten more sophisticated and prevalent, the need for strong cybersecurity measures has never been more pressing. Enter Microsoft Sentinel, a cutting-edge cloud-native Security Information and Event Management (SIEM) solution built to serve as a sentinel in the ever-changing cyber threat scenario. Sentinel, created by Microsoft, emerges as a strong tool that enables enterprises to identify, analyze, and respond to security issues with remarkable efficiency.

Microsoft Sentinel's primary goal is to give enterprises with a complete and unified platform for managing their security operations. This is accomplished by consolidating data from several sources, such as security, logs, apps, devices and cloud services, into a single repository. This unified method allows security professionals to acquire comprehensive insights about their organization's security posture, providing a bird's-eye perspective of possible threats and weaknesses. Sentinel assists security teams in identifying aberrant trends, responding quickly to occurrences, and eventually fortifying their defenses against cyber threats by deploying sophisticated analytics, machine learning and automation. Sentinel provides organizations with the tools they need to not only protect but also manage their digital assets by leveraging the power of Microsoft's cloud infrastructure and expertise.

During this traineeship assignment, you will dive into the world of modern cybersecurity operations by focusing on Microsoft Sentinel, a cloud-native Security Information and Event Management (SIEM) system. Microsoft Sentinel is designed to provide a comprehensive view of an organization's security posture by aggregating and analyzing data from various sources, helping security teams detect, investigate and respond to threats effectively.

Ansible is already used as an automation tool by several of our clients. The output of Ansible is usually only shown via the command line. This makes it not user-friendly and, because the playbooks contain multiple tasks, also not very clear. Ansible Tower can be used to get an overview of an executed playbook via dashboards and a web interface.

Ansible Tower has quite high licensing costs. There are several open-source alternatives to Ansible

Objectives

1. Explore a M365 environment with all security features enabled
2. Investigate security related data generated by Microsoft 365
3. Enable data connectors within Microsoft Sentinel and perform normalization and data mapping
4. Create custom detection rules and playbooks
5. Perform incident analysis and investigation

Optional extensions

1. Build an incident response workflow
2. Create a multi-tenant security reporting dashboard

Project methodology

1. Project Kickoff:
   Objective Definition: The primary aim of this project is to equip you with the skills needed to create insightful security reports using Microsoft Power BI based on Microsoft 365 security data.
   Project Scope: The project will cover various aspects of Microsoft 365 security data, visualization techniques, and hands-on experience with Power BI.
   Resources: You will be provided with access to the necessary tools, resources, and guidance to complete the project successfully.

2. Understanding Microsoft 365 Security Data:
   - Gain insights into the types of security data generated by Microsoft 365 services and their significance in detecting and responding to potential threats.

3. Setting up Data Connectors:
   - Learn how to configure data connectors within Azure Sentinel to seamlessly collect security logs and events from Microsoft 365 services.

4. Data mapping and normalization:
   - Discover the process of mapping and normalizing incoming data to ensure consistency and accuracy in analysis.

5. Custom detection rules:

- Get hands-on experience in creating custom detection rules within Azure Sentinel to identify security incidents and anomalies in Microsoft 365 data.

6. Threat intelligence integration:

- Explore the integration of threat intelligence feeds into Azure Sentinel to enhance detection capabilities and stay ahead of emerging threats.

7. Creating playbooks and automation:

- Learn to develop playbooks that automate response actions in Azure Sentinel. Apply this knowledge to develop playbooks for common Microsoft 365 security scenarios.

8. Incident analysis and investigation:

- Utilize Azure Sentinel's investigation features to analyze detected incidents and gather evidence from Microsoft 365 data.

9. Incident response workflow:

- Take on the challenge of creating a comprehensive incident response workflow for a simulated Microsoft 365 security incident, leveraging Azure Sentinel's capabilities.

10. Reporting and visualization:

- Master the creation of custom dashboards and reports in Azure Sentinel to visualize insights derived from Microsoft 365 security data.

11. Documentation and presentation:

- Document your journey by detailing the data connectors used, custom rules created, incident response workflows developed, and any obstacles you encountered.

Contact details

Contact person

Cindy Van den Hoecke (Cindy.vandenhoecke@acen.eu)

Internship supervisor

Yoni Govaerts