Microsoft Sentinel, 2-day workshop

Fast track into taking Microsoft Sentinel into use as part of your organization's security event management. Discover the capabilities Sentinel can offer in the field of SIEM and SOAR and get insights into your organization's security landscape.

Microsoft Sentinel is a fully could native SIEM/SOAR solution that provides a single pane of glass view to your organization's security landscape. Sentinel is fully integrated with other Microsoft security solutions and Microsoft services, but its capabilities span over also other cloud providers and on-premises infrastructure and servers. Microsoft Sentinel is a cost-effective solution that provides security teams the ability to hunt and investigate incidents across the whole infrastructure.

During the workshop, Digia will provide and introduction into Sentinel and its capabilities and performs a Sentinel deployment into customer's Azure subscription. The Sentinel instance deployed remains in the customer's Azure after the workshop. The actual deployment will be done under instruction of Digia, without the need to provide Digia any access to the customer's Azure resources.

WORKSHOP RESULTS

Digia, as a Microsoft partner, provides a Sentinel workshop with the following results:

- Deployment of Microsoft Sentinel into customer's Azure subscription
- Introduction into Microsoft Sentinel product and its capabilities
- Insights into customer's current security landscape
- A fully operational Microsoft Sentinel deployment
- Recommendations of Microsoft Sentinel use in the customer's organization.

CONTENTS OF THE WORKSHOP

- **Day 1. Kick-off call: Preparation**

- Agreeing on workshop goals and fine tuning the workshop content as needed

- Scheduling of workshops 1 and 2

- Collecting preliminary information

- **Day 2, Workshop 1: Deployment, and Introduction to Sentinel**

- Deployment of Microsoft Sentinel

- Connecting Sentinel to data sources

- Overall solutions description including cost optimization

- **Day 3, Workshop 2: Observations and Recommendations**

- Alerts and incidents handling

- Cost analysis

- Recommendation for Sentinel use

Delivery timeline

Preparations

- Fine tuning the workshop contents for the customer if needed.
- Schedule date and time for the 1st and 2nd workshop.
- Get preliminary information about the customer's Microsoft license levels and configured security solutions.

Deployment

- Microsoft Sentinel deployment and configuration
- Connecting the Sentinel Data Connectors

Introduction to Sentinel

- Overall solution description
- Cost structure and pricing
- Alerts and Incidents
- Analytics rules
- Playbooks
- Workbooks
- Investigation and hunting
- Cost optimizations

Observations

- Going through the Incidents raised in Sentinel during the logging period.
- Cost analysis based on the logging period
- Other topics if interest

Recommendations

- Recommendations for Sentinel use as part of security event management