Microsoft Sentinel advanced implementation and cost optimization, 4-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. Configure Sentinel specifically for your organization with the selected event sources, align it with the organization's log management policy and implement cost optimizations.

Microsoft Sentinel advanced workshop

This workshop is an extended version of "Microsoft Sentinel, 2-day Workshop with the first two days covering the basic introduction and deployment of Microsoft Sentinel to customer's Azure. In addition to basic deployment, other customer specific data sources are connected to Sentinel (e.g., on-premises servers, network equipment, AWS., GCP etc.) and analytics rules are activated to detect security events from these. When connecting the custom log sources, the cost impact is estimated, and optimizations are applied, as necessary. Log retention and long-term log storage is planned.

THE ASSESSMENT 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 with custom log sources identified by the customer
- Log retention and long-term log storage plan. Instructions of how to implement the plan.
- Recommendations of Microsoft Sentinel use as part of the security event management in the customer's organization.

CONTENTS OF THE ASSESSMENT

- **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

- **Day 3, Workshop 2: Costs and Logs**

- Cost optimizations

- Log retention

- Long-term log storage plan

- **Day 4, Workshop 3: Observations and Recommendations**

- Alerts and incidents handling

- Cost analysis

- Recommendation for Sentinel use