MICROSOFT SENTINEL SIEM ENABLEMENT

An independent security analysis and implementation of systems

Improsec provides the activation, enrolment, and onboarding of the customer Azure platform, Microsoft 365, Firewalls, and other on-premises solutions into Microsoft Log Analytics and with Microsoft Sentinel SIEM (Security Information & Event Management) on top.
Whether you have just started a log collection journey or are looking to onboard and enroll the entire infrastructure into the Microsoft Sentinel SIEM, Improsec provides independent expert advice, guidance, and hands-on implementation throughout the process.

Value

This service will implement a fully-fledged cloud native SIEM solution that is owned, hosted, and operated by the Customer.

- Collection of relevant log sources based on requirements, demands, and threat profile
- Tuning of log source to avoid irrelevant noise in the SIEM to reduce alert fatigue and cost
- Configuration of log retention policies to meet compliance requirements and industry best practice
- Introduction to SOAR – Security Orchestration, Automation, and Response - which enables the organization to a faster and more automated containment of critical security threats.

Product

In close cooperation with the Customer, we will identify demands and requirements for the future SIEM solution.

- Discuss and match Customer expectations for the product and delivery
- Getting to know the client's infrastructure
    - o Showcase any potential existing solution (green field or brownfield)
- Present the various applicable log sources for Sentinel
- Agree on applicable log sources in scope
- Discuss and align a retention strategy with the customer

Method

Design and implementation of the Customer Microsoft Sentinel SIEM are delivered in a four-phase approach, normally within two calendar weeks, providing relevant internal resources are available. In close cooperation with the Customer, Improsec analyses the customer's current setup and receives input on the desired strategy, design, and roadmap.
Improsec conducts a technical review of the current environment, followed by an enrolment and deployment phase to meet the agreed state. The final phase is a handover session, presenting with a handover session.

Involvement

Through a close dialogue, we will, together, agree on scope and content.

Improsec A/S
www.improsec.com
Telephone: (+45) 5357 5337
Email: info@improsec.com