Azure Sentinel-as-a-Service

Enterprise-Level Security for Small and Medium Businesses

Security

AccountabilIT builds out a proper SIEM experience from deployment to go-live, all within Microsoft Azure. Connect to AIT's 24x7x365 Security Operations Center (SOC) to quickly and affordably strengthen your security posture and protect against threats.

Integration

Included Data Connectors:

- Azure Active Directory
- Azure Security Center
- Cloud App Security
- Security Events
- Defender (ATP)
- Syslog and CEF
- Azure Activity
- DNS
- O365

Analytics

- Log aggregation from configured connectors and sources
- Security Incident Alert and Event correlation & monitoring
- Security Incident notification and run book escalations determined in collaboration with the customer

Reporting

Azure Sentinel comes equipped with security reporting displays available in the Azure Portal. AIT will provide a selection of these dashboards tailored and customized for the environment.