Active Directory & Entra Connect Sync

- Microsoft Defender for Endpoint on all servers with hybrid identity components
- Microsoft Defender for Identity (MDI) sensor health alerts on AD DS and Connect servers
- Review Connect sync rules and scopes (excl. on-prem admins & service accounts)
- ACEs and monitoring on Connect Server service accounts and Sync Health
- Use application identity authentication (with TPM)

Tenant (Security) Configuration

- Maester to analyze security configs on regular basis and track changes of test result
- Monitor changes of critical policies (e.g., Authorization or CA Policy) and impact by EIDSCA/Maester checks
- Monitor and resolve findings in Entra ID Recommendations, XSPM Initiative and Identity Secure Score
- Monitor metrics from sign-in Analysis and other Operational Workbooks

Authentication and Conditional Access Policies

- Conditional Access Insights, Gap and Health Alerts
- Policy Effectiveness (WhatIf, Sign-in Logs), review with CA Optimization Agent
- Analyze sign-in with strong authentication methods and protection of keys by TPM or secure enclave
- Track Authentication Methods Activity (Register, Usage) and SSPR Reports
- Health status of analytics rules, playbooks and data connector in Sentinel

Privileged Identity and Access Management

- Analyse and monitor high-privileged access with EntraOps
- Protect privileged users by using Role-assignable groups or (R)MAUs
- Identify sensitive groups and their assignment to Access Packages and Catalogs
- Classify and analyze your privileged assets in Exposure Management
- Monitor PIM Alerts for Entra ID roles with Maester

Application and Workload Identities

- Identify high privileged workload identities and any potential attack paths in Exposure Management
- Monitor MDA App Governance Policy Alerts (for example, unused API permissions) and Entra Recommendations
- Tracking changes on assigned (API) permissions and delegations.
- Usage & Insights Reports about application, service principal sign-in and credential activity

Internal/External Configuration and Attack Analyses

- Security Awareness Training for Users (Attack Simulation, for example phishing)
- Penetration to validate security posture and ITDR detections (AADInternals, ROADtools,...)
- Attack Path Management (Exposure Management, BloodHound, Forest Druid)