

Security



Security – **Securing Identities and Access**

Objetivo



- Dada a complexidade do número de identidades, dados, aplicativos e dispositivos, é essencial aprender como garantir que as pessoas certas acessem as informações a que tem direito e com segurança.

Abordagem



- Identifique potenciais riscos relacionados às identidades.
- Saiba onde e como melhorar a segurança das identidades de sua organização.
- Obtenha uma avaliação e um score da segurança de identidade em seu ambiente.
- Veja quais são os apps que seus usuários estão usando e se eles são ou não suportados pela sua TI.

Atividades Planejadas



- Descoberta da aplicação
- Avaliação da postura de segurança
- Fundamentos de Identidade
- Self-Service reset password
- Autenticação Multi-fator
- Acesso Condicional
- Autenticação sem senha (passwordless)
- Gestão de Aplicações com Azure AD
- Principais resultados, recomendações e próximos passos



Público sugerido

Sessão 1: Todo o time de TI e segurança

Security – Defend Against Threats with SIEM plus XDR

Objetivo



- Devido ao volume e a complexidade da administração de identidades, dados, aplicativos, dispositivos e infraestrutura, é essencial entender o quão segura sua organização está.

Abordagem



- Identificar os principais objetivos e prioridades de segurança em seu ambiente de nuvem.
- Análise de ameaças de cyber-ataques que sejam encontrados em sua organização.
- Assessment detalhado no seu ambiente, relacionado à iniciativas de segurança aplicáveis.
- Demonstração do modelo de segurança integrada proposto pela Microsoft.

Atividades Planejadas



- Analisar ameaças ativas e fraquezas relacionadas com endpoints do Windows 10, utilizando licença existente ou trial do Microsoft Defender for Endpoint.
- Analisar riscos e ameaças relacionados ao AD, utilizando o Microsoft Defender for Identity.
- Identificar os principais objetivos e prioridades de segurança em seu ambiente de nuvem.
- Análise de verificação de ameaças no ambiente de produção
- Recomendações diversas e próximos passos.



Público sugerido

Sessão 1: Todo o time de TI e segurança

Sessão 2: Todo o time de TI, segurança e gestores