Aprenda com quem faz

Soluções de Segurança, Governança, Compliance e Migração

Capítulo 5. Defesa em Profundidade, Security Center e Azure Sentinel

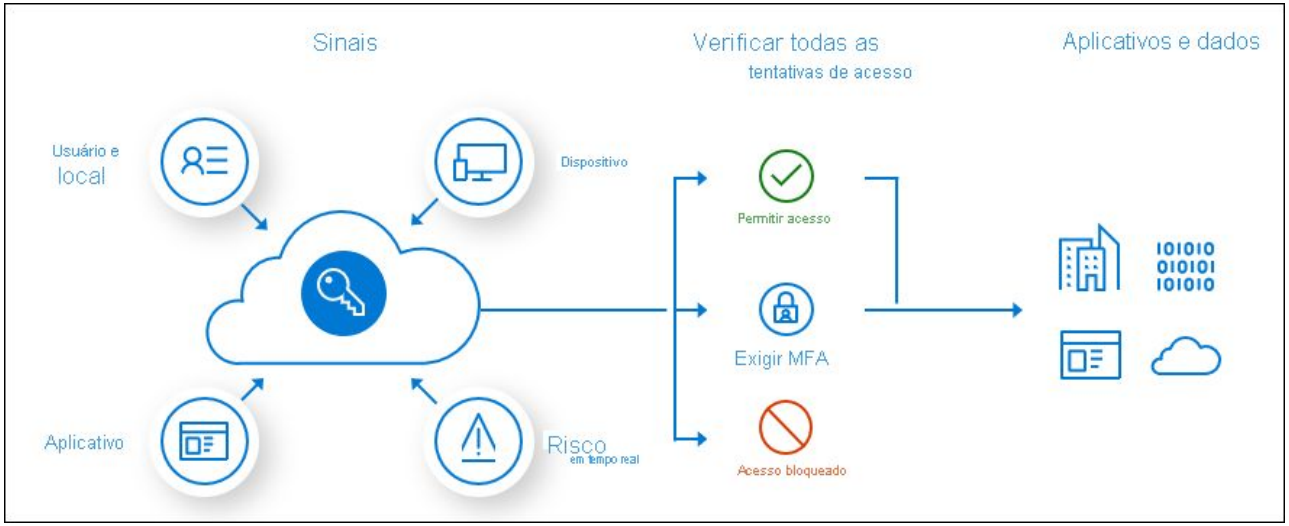
Aula 5.1. Conditional Access

Prof. Rafael Alves Amaral

Nesta aula

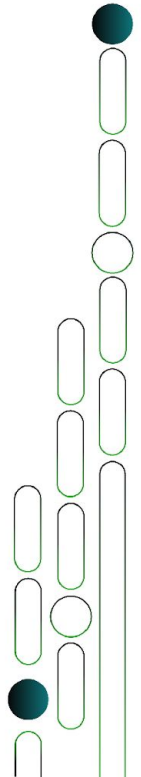
- Vamos entender:
  - O que é o Acesso condicional do Azure AD.
  - Com ele ajuda a proteger as nossas contas e serviços.
  - Padrões de Segurança do Azure.
  - Como configurar o Acesso Condicional.
  - Termos de Uso.

Conditional Access



Azure Conditional Access

Hands-on



Conclusão

- O acesso condicional do Azure ajuda a proteger nossas contas e aplicativos vinculados ao Azure AD de acessos indesejados.
- Funciona apenas com o Azure AD Premium P1.
- Também pode ser usado para colher assinaturas de termos de uso.

Próxima aula

- Identity Protection.
- Protegendo contas e gerenciando o Identity Protection.

Aprenda com quem faz

Soluções de Segurança, Governança, Compliance e Migração

Capítulo 5. Defesa em Profundidade, Security Center e Azure Sentinel

Aula 5.2. Identity Protection

Prof. Rafael Alves Amaral

Nesta aula

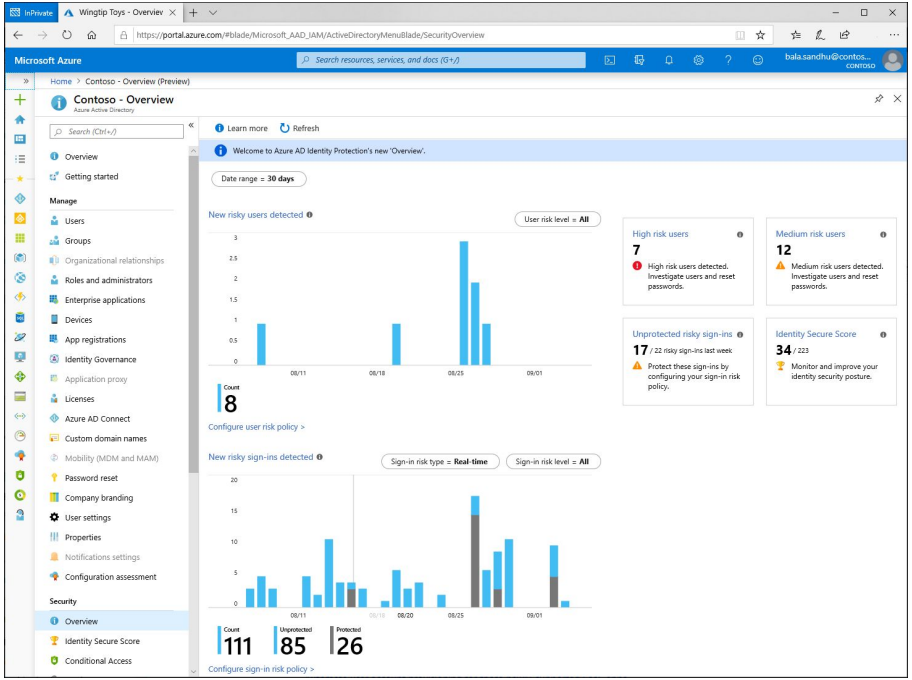
- Vamos entender:
  - O que é o Identity Protection.
  - Como configurar ele.
  - Como testar o comportamento.

Azure Identity Protection

User Risk

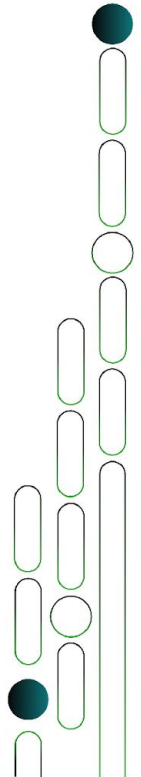
Sign-in Protection

User Protection



Azure Identity Protection

Hands-on



Conclusão

- Apesar de não possuir muitas configurações, o Identity Protection consegue bloquear ações suspeitas de usuários e até bloqueá-los automaticamente.
- Funciona apenas com o Azure AD Premium P1.

Próxima aula

- Security Center.
- Security Score.
- Conformidade e Segurança.
- Proteção de Workloads.
- Gerenciados de Firewall.

Aprenda com quem faz

Soluções de Segurança, Governança, Compliance e Migração

Capítulo 5. Defesa em Profundidade, Security Center e Azure Sentinel

Aula 5.3. Security Center

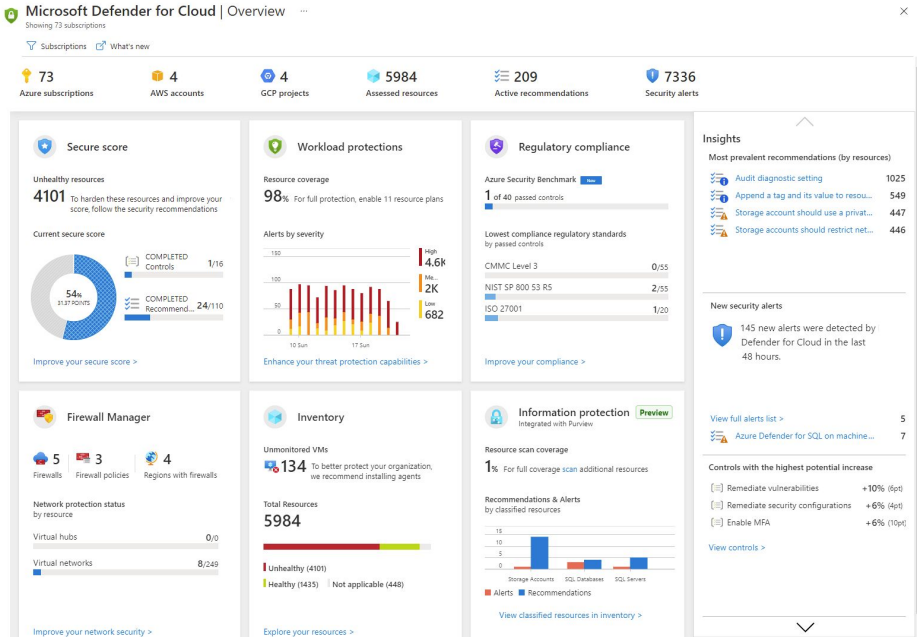
Prof. Rafael Alves Amaral

Nesta aula

- Vamos entender:
  - O que é o Security Center (Microsoft Defender for Cloud).
  - Os 4 recursos principais dele, sendo:

1. Classificação de Segurança;
2. Conformidade e Segurança;
3. Proteção de Cargas de Trabalho;
4. Valores para o Azure Security Center.

Microsoft Defender for Cloud



Azure

aws

Google Cloud Platform

Microsoft Defender for Cloud

Hands-on

Conclusão

- Microsoft defender for cloud é uma ferramenta muito poderosa Multicloud que abrange não só aspectos de segurança, mas também aspectos de conformidade da empresa.
- Nos fornece quais os possíveis problemas de segurança, o que eles podem afetar no seu ambiente e como resolvê-los.

Próxima aula

- Azure Sentinel.
- SIEM.
- Conectores.
- Workbooks.
- Análises.

Aprenda com quem faz

Soluções de Segurança, Governança, Compliance e Migração

Capítulo 5. Defesa em Profundidade, Security Center e Azure Sentinel

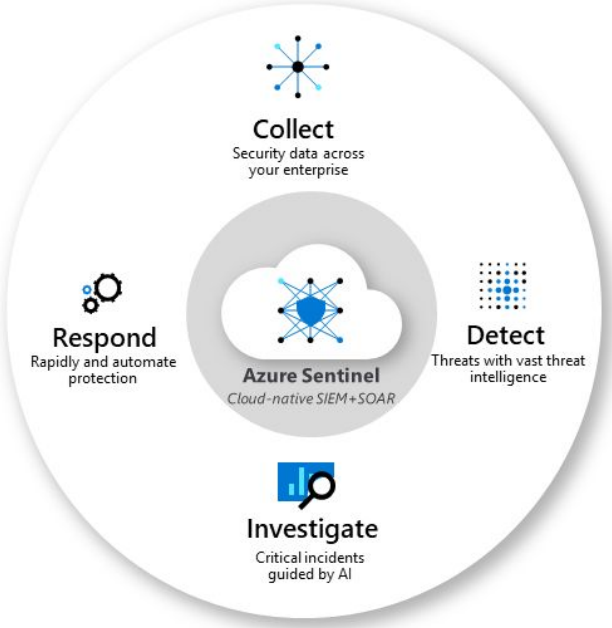
Aula 5.4. Azure Sentinel

Prof. Rafael Alves Amaral

Nesta aula

- Vamos entender:
  - O que é o Azure Sentinel;
  - O que é um SIEM;
  - Como conectar uma fonte de dados;
  - Como visualizar os dados em workbooks;
  - Como criar uma análise;
  - Módulo de Caça (Hunting Mode).

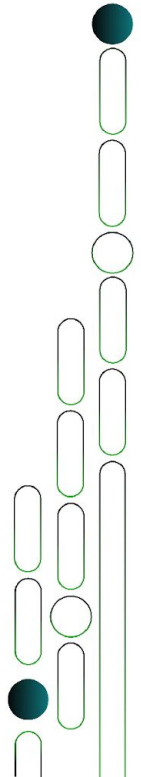
Azure Sentinel



SIEM

Azure Sentinel

Hands-on



Conclusão

- O Azure Sentinel é uma ferramenta cloud native que investiga logs de segurança de diversas fontes distintas e consegue analisar e tomar ações baseadas nesses logs.

Próxima aula

- Capitulo 6 – Azure Monitor:
  - Log Analytics Workspace;
  - Application Insigts;
  - Azure Alerts.