Laboratório 1 - Recomendar medidas de segurança de endpoint

# Objetivos

Parte 1: Recomendar procedimentos de mitigação para corrigir vulnerabilidades

Parte 2: Recomendar um produto de proteção de endpoint para uma nova rede

# Histórico/Cenário

Para oferecer segurança, os profissionais normalmente implementam várias medidas de segurança de rede que trabalham juntas em uma abordagem de segurança em camadas. Firewalls e outros dispositivos protegem o perímetro de rede contra ataques; no entanto, é sempre possível que as ameaças escapem dessas defesas. Portanto, não é necessário apenas proteger o perímetro de rede, mas também agir para proteger hosts de rede individuais contra comprometimentos. Neste laboratório, você lerá dois estudos de caso e recomendará a mitigação de ameaças de endpoint que sejam apropriadas para lidar com as explorações.

# Recursos necessários

=   Acesso à Internet

# Instruções

## Parte 1: Recomendar procedimentos de mitigação para corrigir vulnerabilidades

Você trabalha em uma equipe de segurança para uma empresa de manufatura. Um novo cliente exige que, antes de poder conceder o contrato à empresa, ele tenha que cumprir padrões mais rigorosos. Uma avaliação de vulnerabilidade da rede foi concluída e uma série de vulnerabilidades foram encontradas, incluindo os seguintes problemas de segurança de endpoint:

·         A empresa usa sistemas de controle de supervisão e aquisição de dados (SCADA) para monitorar e controlar seus processos de fabricação. O software SCADA é executado no sistema operacional Windows XP.

·         Os sistemas essenciais permitem o uso de mídia USB desconhecida.

·         Os usuários podem acessar a rede com dispositivos de computação pessoal, como smartphones, tablets e laptops.

·         Os usuários podem navegar livremente pela Web, incluindo sites de malware conhecidos.

·         O software antivírus inconsistente instalado nos hosts incluiu versões antigas com status de atualização de assinatura desconhecida.

Usando o material abordado neste curso e as informações adicionais que você encontra na Internet, preencha a tabela abaixo.

| Problema | Recomendação |
| --- | --- |
| Versões desatualizadas do sistema operacional |  |
| Sistemas essenciais permitem o uso de mídia USB |  |
| Uso de dispositivos de computação pessoal na rede |  |
| Os usuários podem navegar livremente pela Web |  |
| Problemas de antivírus |  |

Linha em branco, sem informações adicionais

Linha em branco, sem informações adicionais

## Parte 2: Recomendar um produto de proteção de endpoint para uma Nova Rede

Um amigo recebeu recentemente financiamento de capital de risco para um novo produto promissor. O crescimento rápido está previsto. Ele está abrindo um local para a startup e pediu que você o ajude com recomendações para que medidas de segurança de endpoint sejam implementadas na nova rede.

Use sua aprendizagem no curso e pesquisa de Internet para recomendar um produto de segurança de endpoint abrangente. Lembre-se de que a empresa é pequena no momento, mas vai crescer rapidamente. Apresente os motivos da sua decisão com base nos recursos do produto.

**Registre seu produto escolhido:**

Digite suas respostas aqui.

| Recurso | Valor |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Linha em branco, sem informações adicionais

Linha em branco, sem informações adicionais

Fim do documento