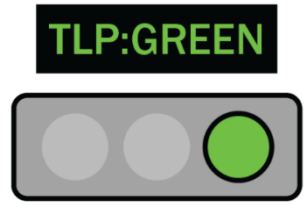


RNEP-GW

MÓDULO PROTECÇÃO DE ENDPOINTS

fct csirt

RNEP-GW

ENDPOINT

É tudo o que se liga à rede e executa código.

Porque proteger?

- Exfiltração
- Ransomware
- Botnets

EVOLUÇÃO DO MALWARE

Malware atual utiliza técnicas avançadas para se esconder de antivírus:

- Ser fileless
- Mudar de assinatura
- Binários *living-of-the-land* (Lolbin)

Malware evolui mais rápido que antivírus tradicionais. Estes já não bastam.

ANTIVIRUS/EDR/XDR

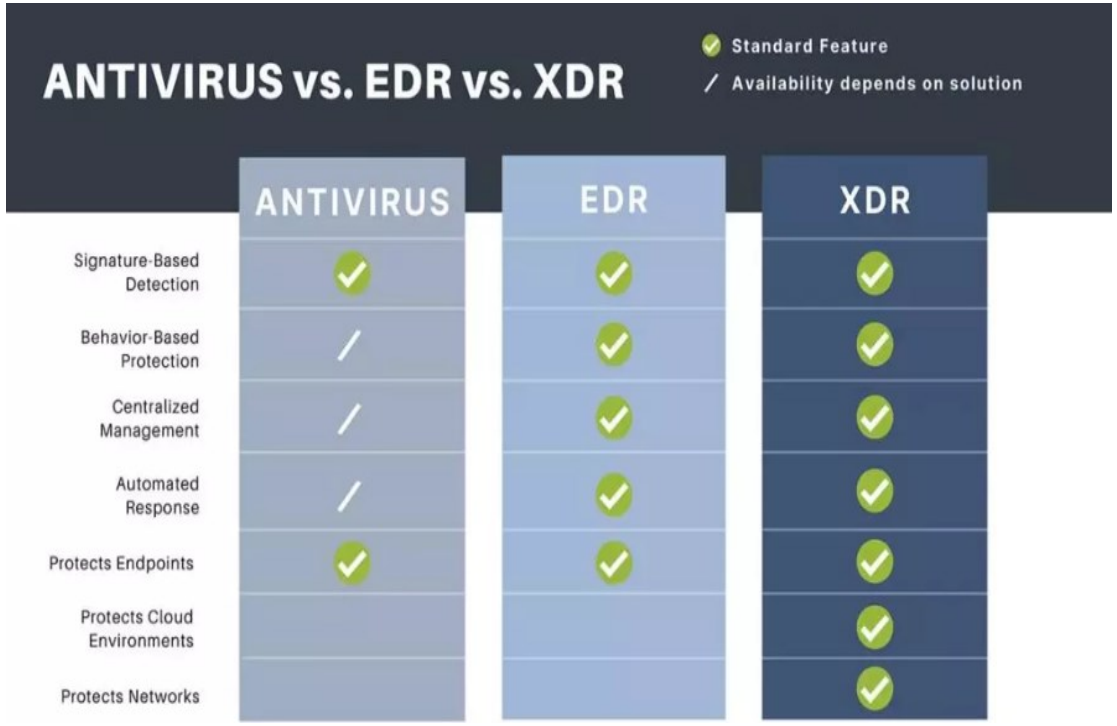
Proteção em tempo real

Constante captação de dados

Constante análise de dados

Threat Hunting

Resposta automática



BENEFÍCIOS CHAVE

Porque obter um XDR?

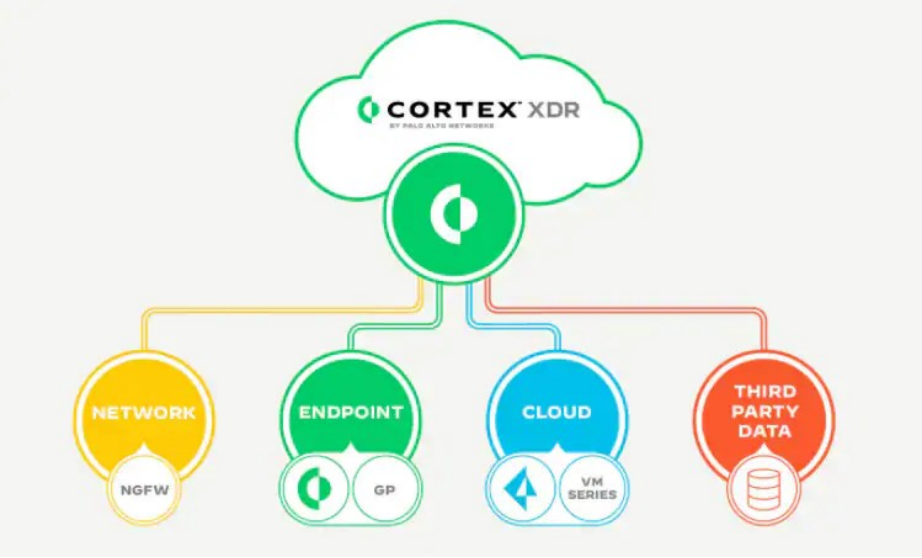
- Monitorização em tempo real
- Bloqueio de processos suspeitos
- Contenção de máquinas
- Timeline de eventos
- Threat intelligence integrada

CORTEX XDR - ARQUITETURA

É a proteção de endpoints utilizada pelo CSIRT FCT.

Contém:

- Agentes
- Data Lake
- Motor de Análise
- Console Cortex XDR



Não é instalado nem mantido localmente, apenas utilizado pela nossa equipa.

PROCESSO

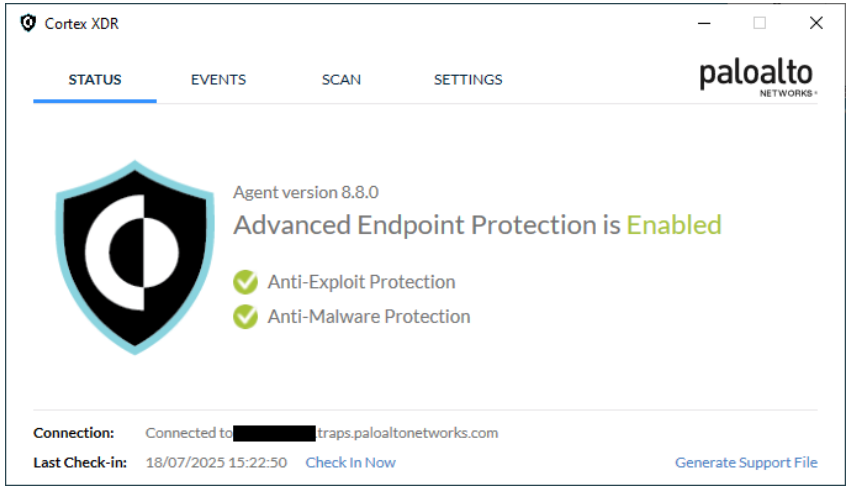
1. Atacante envia payload por e-mail
2. Utilizador clicka → Processo malicioso arranca
3. Cortex XDR deteta comportamento anómalo → bloqueia execução
4. Criado um incidente e o CSIRT é notificado
5. Analista investiga incidente
6. Analista resolve o incidente remotamente

PRIMEIRO ALVO DO MALWARE

Para o malware funcionar, tem de “desligar” ou iludir o EDR/XDR.

Técnicas comuns:

- Desativação do agente
- Desinstalação silenciosa
- Uso de *living-off-the-land binaries*



BOAS PRÁTICAS

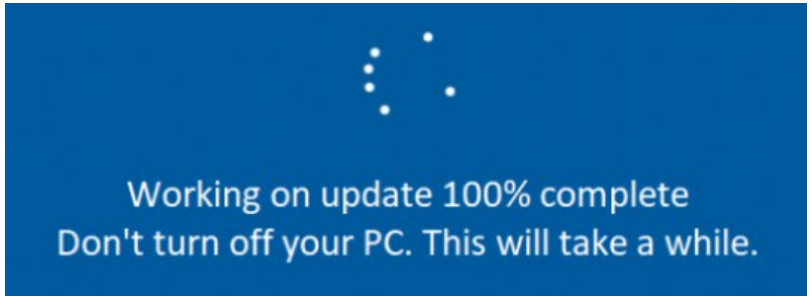
Atualizações automáticas

Mínimos privilégios

Segmentação de rede

Uso obrigatório de EDR/XDR

Formação do utilizador



DICAS PARA APLICAÇÃO

Começar com inventário de endpoints

Priorizar endpoints críticos

Deploy gradual do agente

Monitorização antes de automação

IDEIAS CHAVE

- O tradicional «anti-vírus» deixou de ser suficiente
- A protecção de endpoints é a nova abordagem em que o software bloqueia acções consideradas potencialmente malignas para o sistema
- Quem produz malware tem que atacar primeiro a protecção de endpoints para que o malware seja eficaz

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc