

MÓDULO: FERRAMENTAS

Pedro Silva
RCTS CERT





AGENDA

Introdução

Ferramentas



INTRODUÇÃO



Papel das ferramentas

Descrição de algumas ferramentas



ANTI VIRUS



INTELMQ



NetFlow analyzer
by NFSen

SIEM



Detetar incidentes

Melhora a eficiência

Agilizar a criação de relatórios

Pesquisar flows

Processar/Pesquisar flows por período

Criar histórico e perfis de pesquisa

Criar alertas com base em condições

Criar os próprios scripts para processar flows



Recolha automática de eventos

Harmonização de dados

Tipificação e classificação

Único formato – JSON

Facilitar a partilha da informação

Criação de blacklists



Performance (multithread)

IDS/IPS

Deteção automática do protocolo

Standard de output estandardizados

ANTIVIRUS/EDR/XDR



Proteção em tempo real

Constante captação de dados

Constante análise de dados

Threat Hunting

Resposta automática

ANTIVIRUS vs. EDR vs. XDR			
	ANTIVIRUS	EDR	XDR
Signature-Based Detection	✓	✓	✓
Behavior-Based Protection	/	✓	✓
Centralized Management	/	✓	✓
Automated Response	/	✓	✓
Protects Endpoints	✓	✓	✓
Protects Cloud Environments			✓
Protects Networks			✓



Obrigado!