CIBERSEGURANÇA

Resumo das camadas de segurança

Recurso	EDR (Endpoint Detection and Response)	XDR (Extended Detection and Response)	MDR (Managed Detection and Response)
Foco principal	Detecção e resposta a ameaças em endpoints individuais (computadores, servidores).	Detecção e resposta a ameaças em **múltiplos domínios e plataformas** (nuvem, e-mail, rede, endpoint).	Um **serviço de segurança gerenciado** que faz a monitorização, detecção e resposta em nome da organização.
Visão	Profunda visibilidade e análise do que acontece em um dispositivo.	Visão holística e unificada de toda a infraestrutura de segurança.	Visão externa e proativa de toda a rede, com foco em inteligência de ameaças.
Responsabilidade	A equipe interna é responsável por analisar os alertas e tomar as ações de resposta.	A equipe interna é responsável por analisar os alertas, mas tem uma visão mais completa para correlacionar ameaças entre diferentes fontes.	A equipe de um provedor terceirizado é responsável por monitorar, analisar alertas e, na maioria dos casos, **realizar a resposta e remediação**.

Caso de uso ideal	Organizações que precisam de proteção avançada para seus endpoints, com equipes de segurança capacitadas para análise.	Organizações que buscam integrar diversas ferramentas de segurança (endpoints, nuvem, rede) e precisam de uma visibilidade e resposta centralizadas contra ameaças complexas.	Organizações que não possuem a equipe, as ferramentas ou o tempo para gerenciar a segurança 24/7.