Incident Containment & Threat Hunting

O que é

Incident Containment & Threat Hunting é a combinação entre resposta estruturada a incidentes de segurança e a procura proativa de ameaças no ambiente tecnológico. A contenção visa limitar o impacto e impedir a propagação de um ataque após a sua deteção, enquanto o threat hunting parte do princípio de que podem existir compromissos ainda não identificados, procurando sinais de atividade maliciosa antes que causem dano significativo. Em conjunto, estas práticas reduzem risco, tempo de exposição e impacto no negócio, reforçando a resiliência operacional e a confiança.

Boas Práticas

- Definir playbooks claros de resposta
- Integrar SIEM, EDR e threat intelligence
- Garantir visibilidade sobre rede, endpoints e identidades
- Medir MTTD, MTTR e dwell time
- Testar regularmente cenários de incidente

Em caso de falha

- Avaliar impacto e isolar sistemas afetados
- Bloquear indicadores de compromisso
- Preservar evidência e monitorizar o ambiente
- Rever o incidente e reforçar controlos

up_ motion PRR Plano de Recuperação e Resiliência REPÚBLICA PORTUGUESA Financiado pela União Europeia NextGenerationEU