



INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Fundamentos de Cibersegurança

Caso 1

Paulo António Tavares Abade - 23919



Beja, outubro de 2025

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Fundamentos de Cibersegurança

Caso 1

Paulo António Tavares Abade - 23919

Orientadores: Rui Silva & Rogério Bravo

Beja, outubro de 2025

Resumo

Resolução do trabalho

Keywords: cibersegurança

Abstract

Work Resolution

Keywords: cybersecurity

Índice

1	Grupo I - Professor Rui Silva	1
1.1	1.1	1
1.1.1	Malware Protection	1
1.1.2	Incident Coordination	1

Índice de Figuras

1 Grupo I - Professor Rui Silva

Nesta secção serão respondidas as questões do Grupo I, focando-se na áreas do MITRE ATT&CK lecionadas pelo professor Rui Silva.

1.1 1.1

Em resposta à questão 1.1, foram escolhidas para apresentar as áreas de *Malware Protection* e *Incident Coordination*, que podem ser consideradas como mutualismo/simbiose, uma vez que ambas as áreas trabalham em conjunto para fortalecer a defesa contra ameaças. Caso uma ameaça seja detectada, pela área de *Malware Protection*, a área de *Incident Coordination* entra em ação para coordenar a resposta ao incidente, assegurando que as medidas adequadas sejam tomadas para mitigar o impacto da ameaça.

1.1.1 Malware Protection

A proteção de Malware é uma área que tem como objetivo impedir o acesso, a propagação e o impacto de softwares maliciosos (malware) em sistemas informáticos. Esta área é efetiva contra ameaças já conhecidas, porém quando se trata de ameaças que utilizam exploits zero-day, ou seja, vulnerabilidades desconhecidas, a eficácia pode ser limitada. Mesmo assim, a proteção de malware é uma componente crucial na defesa em profundidade, sendo que esta pode incluir várias técnicas e ferramentas, tais como integrar e correlacionar informação de multiplicas fontes estáticos e dinâmicas para detetar com cada vez mais qualidade a presença de malware através da análise da sua assinatura.

1.1.2 Incident Coordination

A coordenação de incidentes é uma área que se concentra na gestão e resposta a incidentes de segurança informática. Esta área é responsável por coordenar as ações necessárias para lidar com incidentes, desde a deteção até à resolução. A coordenação de incidentes envolve a comunicação eficaz entre diferentes equipas, para que as decisões sejam tomadas o mais rapidamente possível para minimizar os danos.