



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	Pergunta	1
1.1.1	Malware Protection	1
1.1.2	Incident Coordination	2

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 Pergunta

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 contra malware envolve a implementação de medidas e tecnologias para prevenir, detectar e remover software malicioso que possa comprometer a segurança dos sistemas informáticos. No entanto, esta proteção não é infalível, podendo ser contornada por malware que esteja camuflado ou que nunca tenha sido identificado, no caso do último, é conhecido como *Zero-Day Malware*. Esta proteção funciona através da análise de padrões comuns em ataques (CAPE), sendo que estes padrões foram identificados através do MAEC (Malware Attribute Enumeration and Characterization), que é um padrão para a representação de informações sobre malware, permitindo a troca estruturada de dados entre diferentes ferramentas e sistemas de segurança. O objetivo principal do MAEC é facilitar a detecção, análise e resposta a ameaças de malware, promovendo a interoperabilidade entre diferentes soluções de segurança. Este é utilizado pelo Incident Coordination para ajudar a prevenir novos ataques com base no que a proteção de malware não conseguiu impedir.

1.1.2 Incident Coordination

A coordenação de incidentes envolve a gestão e resposta a incidentes de segurança informática que não tenham sido superados pela proteção de malware, garantindo que as ameaças sejam tratadas de forma eficaz e eficiente. Isto inclui a identificação, análise, contenção, erradicação e recuperação de incidentes de segurança. A coordenação eficaz de incidentes é crucial para minimizar o impacto das ameaças e garantir a continuidade das operações. Integrando e correlacionando informação de múltiplas fontes estáticos e dinâmicas, mais conhecidamente como IODEF (Incident Object Description Exchange Format), que é um padrão para a troca estruturada de informações sobre incidentes de segurança informática, sendo que isto permite detetar com cada vez mais qualidade a presença de malware através da análise da sua assinatura. Isto fica automatizado com o RID (Realtime Inter-network Defense), que é um protocolo que permite a troca automática e segura de informações sobre ameaças. Existem ainda outros protocolos como o TAXII (Trusted Automated eXchange of Indicator Information) que é um protocolo para a troca automatizada de indicadores de ameaças, e o STIX (Structured Threat Information eXpression) que é uma linguagem padronizada para a representação de informações sobre ameaças cibernéticas, e estes são complementares sendo que o STIX é o formato que passa pelo TAXII para ser transmitido entre sistemas.