Unidade Curricular	Análise de Evidências			Área Científica	Ciências Informáticas		
CTeSP em	Cibersegurança			Escola	Escola Superior de Tecnologia e de Gestão de Bragança		
Ano Letivo	2022/2023	Ano Curricular	1	Nível	0-1	Créditos ECTS	3.0
Tipo	Semestral	Semestre	2	Código	4087-712-1004-00-22		

Horas totais de trabalho	81	Horas de Contacto	T	-	TP	7	PL	23	TC	-	S	-	E	-	OT	-	O	-

T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutórica; O - Outra

Nome(s) do(s) docente(s)	Tiago Miguel Ferreira Guimaraes Pedrosa, Rui Alexandre Coelho Alves

Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:
1. Identificar a estrutura e propriedades dos elementos de informação relevantes a extrair dessas fontes de informação.
2. Identificar as fontes de informação mais relevantes usadas na análise de evidências para os principais tipos de incidentes.
3. Identificar as principais fontes de informação pública sobre vulnerabilidades, reputação e ameaças.
4. Analisar e compreender a informação existentes nos registos.
5. Utilizar ferramentas especializadas para manipulação de logs.
6. Reconhecer a alto nível o funcionamento de sistemas de extração, filtragem, transporte e registo de logs, bem como a indexação e correlação de logs.
7. Compreender o funcionamento de sistemas de gestão de informação e eventos de segurança (SIEM).

Pré-requisitos

Não aplicável

Conteúdo da unidade curricular

Analise das informações existentes em fontes de informação que permitam analisar possíveis incidentes. Utilização de bibliotecas e ferramentas de gestão de informação e eventos de segurança, e sistemas de extração, filtragem, transporte e registo de logs, bem como a indexação e correlação de logs. Uso de fontes de informação públicas sobre vulnerabilidades, reputação e ameaças para melhor compreensão das informações que se encontram a analisar.

Conteúdo da unidade curricular (versão detalhada)

1. Estrutura e formatos de registos.
2. Fontes públicas de informação sobre vulnerabilidades, reputação e ameaças.
3. Ferramentas para análise de evidências e correlação.
4. Ferramentas para gestão de informação e eventos de segurança (SIEM).
5. Introdução a bibliotecas relevantes ao cenário da cibersegurança.

Bibliografia recomendada

1. A. A. Chuvakin and K. J. Schmidt. Logging and Log Management: The Authoritative Guide to Under- standing the Concepts Surrounding Logging and Log Management. Syngress, 1 edition, 12 2012.
2. S. Chhajed. Learning ELK Stack. Packt Publishing, 2016.
3. D. R. Miller, S. Harris, A. Harper, S. VanDyke, and C. Blask. Security Information and Event Manage- ment (SIEM) Implementation (Network Pro Library). McGraw-Hill Education, 1 edition, 11 2010.
4. D. P. Polstra. Windows Forensics. CreateSpace Independent Publishing Platform, 1 edition, 7 2016.
5. P. Polstra. Linux Forensics. CreateSpace Independent Publishing Platform, 1 edition, 7 2015.

Métodos de ensino e de aprendizagem

Exposição teórica dos conceitos acompanhada de demonstrações. Resolução de exercícios práticos. Período não presencial: Estudo individual e em grupo da matéria abordada.

Alternativas de avaliação

- Avaliação - (Ordinário, Trabalhador) (Final, Recurso, Especial)
  - Trabalhos Práticos - 20% (Análise de uma ameaça, e. g. phishing, e posterior elaboração de um relatório de análise da ameaça.)
  - Exame Final Escrito - 40%
  - Projetos - 40% (Projeto relacionado com agregação de logs, SIEM, ataques e análise de correlação de eventos.)

Língua em que é ministrada

Português

Validação Eletrónica

Tiago Miguel Ferreira Guimaraes Pedrosa	José Luís Padrão Exposto	José Carlos Rufino Amaro
06-03-2023	17-03-2023	17-03-2023