English version at the end of this document

Ano Letivo	2022-23
Unidade Curricular	MONITORIZAÇÃO E REGISTOS DE EVENTOS
Cursos	CIBERSEGURANÇA
Unidade Orgânica	Faculdade de Ciências e Tecnologia
Código da Unidade Curricular	19381012
Área Científica	
Sigla	
Código CNAEF (3 dígitos)	481
Contributo para os Objetivos de Desenvolvimento Sustentável - ODS (Indicar até 3 objetivos)	4, 9, 11
Línguas de Aprendizagem	Inglês

Modalidade de ensino

B-Learning

Docente Responsável JÚLIO CARLOS BOTEQUILHA FERNANDES

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
JÚLIO CARLOS BOTEQUILHA FERNANDES	S	S1	4S

* Para turmas lecionadas conjuntamente, apenas é contabilizada a carga horária de uma delas.

ANO	PERÍODO DE FUNCIONAMENTO*	HORAS DE CONTACTO	HORAS TOTAIS DE TRABALHO	ECTS
1º	S2		25	1

* A-Anual;S-Semestral;Q-Quadrimestral;T-Trimestral

Precedências

Sem precedências

Conhecimentos Prévios recomendados

N/A

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

O Módulo de Monitorização e Registo de Eventos pretende dotar o estudante com conhecimentos dos modernos sistemas de Recolha de Registos Centrais (SIEM). É ainda objetivo desenvolver conhecimento de como implementar um sistema de recolha de eventos e de deteção de eventos e resposta (EDR). Pretende ainda dotar o estudante de conhecimentos de como implementar e configurar um sistema de monitorização de integridade de ficheiros (FIM).

Conteúdos programáticos

- Conceito de Sistema de Recolha de Registos Centrais;
- Conceito de Endpoint Detection and Response (EDR);
- Como implementar um SIEM;
- Como implementar um EDR;
- Conhecer e implementar um sistema de monitorização de integridade de Ficheiros (FIM).

Metodologias de ensino (avaliação incluída)

A presente unidade curricular combina diversos métodos de ensino:

- Exposição dos conteúdos programáticos, através da componente teórica
- Prática laboratorial de instalação, configuração e implementação de SIEM, ERD e FIM.
- Atendimento individual ou em grupo para esclarecimento de dúvidas
- Apoio às atividades e esclarecimento sobre funcionamento da unidade curricular.

A avaliação é efetuada através de um teste de avaliação:

- Teste individual para a avaliação de conhecimentos (100%)

Os estudantes que obtiverem uma classificação final igual ou superior a 9,5 valores em cada elemento de avaliação estão dispensados do exame final.

Bibliografia principal

David R. Miller (2010), Security Information and Event Management (SIEM) implementation, McGraw-Hill Education, ISBN-10: 00071701095

Arun E. Thomas (2018), Security Operations Center ? SIEM use cases and Cyber threat intelligence, CreateSpace Independent Publishing Platform, ISBN-10: 1986862011

Gerardus Blokdyk (2018), File Integrity Monitoring Complete Self-Assessment Guide, 5StarCooks

Gerardus Blokdyk (2020), Endpoint Detection and Response: A complete Guide, 5StarCooks

Academic Year	2022-23
Course unit	
Courses	
Faculty / School	FACULTY OF SCIENCES AND TECHNOLOGY
Main Scientific Area	
Acronym	
CNAEF code (3 digits)	481
Contribution to Sustainable Development Goals - SGD (Designate up to 3 objectives)	4, 9, 11
Language of instruction	English
Teaching/Learning modality	B-Learning

Coordinating teacher JÚLIO CARLOS BOTEQUILHA FERNANDES

Teaching staff	Type	Classes	Hours (*)
JÚLIO CARLOS BOTEQUILHA FERNANDES	S	S1	4S

* For classes taught jointly, it is only accounted the workload of one.

Contact hours

T	TP	PL	TC	S	E	OT	O	Total
0	0	0	0	0	0	0	0	25

T - Theoretical; TP - Theoretical and practical ; PL - Practical and laboratorial; TC - Field Work; S - Seminar; E - Training; OT - Tutorial; O - Other

Pre-requisites

no pre-requisites

Prior knowledge and skills

N/A

The students intended learning outcomes (knowledge, skills and competences)

The Monitoring and Event Log Module aims to provide the student with knowledge of modern Security Information and Event Management (SIEM) systems. It also aims to develop knowledge of how to implement an endpoint detection and response (EDR) system. It also wants to provide the student with knowledge of how to implement and configure a file integrity monitoring system (FIM).

Syllabus

- Security Information and Event Management (SIEM) concept;
- Central Event Collection System concept;
- Endpoint Detection and Response (EDR) concept;
- Implementing an SIEM;
- Implementing an EDR;
- Exploring and Implementing a File Integrity Monitoring System (FIM);

Teaching methodologies (including evaluation)

This curricular unit combines various teaching methods:

- Program content exhibition through theoretical lectures
- Practice laboratorial lessons, with installing, configuring and implementing a SIEM, ERD and FIM
- Individual or group attendance for out of classroom support;
- Activity support and curricular unit functioning clarification

Evaluation is determined by an individual test in which:

- Individual knowledge evaluation test (100%)

Students that achieve a final grade of 9.5 or higher in each of the evaluation components, are excused from the final exam.

Main Bibliography

David R. Miller (2010), Security Information and Event Management (SIEM) implementation, McGraw-Hill Education, ISBN-10: 00071701095

Arun E. Thomas (2018), Security Operations Center ? SIEM use cases and Cyber threat intelligence, CreateSpace Independent Publishing Platform, ISBN-10: 1986862011

Gerardus Blokdyk (2018), File Integrity Monitoring Complete Self-Assessment Guide, 5StarCooks

Gerardus Blokdyk (2020), Endpoint Detection and Response: A complete Guide, 5StarCooks