English version at the end of this document

Ano Letivo	2023-24
Unidade Curricular	SEMINÁRIO II
Cursos	CIBERSEGURANÇA
Unidade Orgânica	Faculdade de Ciências e Tecnologia
Código da Unidade Curricular	19381017
Área Científica	CIÊNCIAS INFORMÁTICAS
Sigla	
Código CNAEF (3 dígitos)	481
Contributo para os Objetivos de Desenvolvimento Sustentável - ODS (Indicar até 3 objetivos)	4,9,11
Línguas de Aprendizagem	Português

Modalidade de ensino

B-Learning

Docente Responsável Joel David Valente Guerreiro

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
Joel David Valente Guerreiro	S	S1	2.5S

* 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	2.5S	156	6

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

Precedências

Sem precedências

Conhecimentos Prévios recomendados

Não Aplicável.

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

Seminário II tem como objetivo apresentar e partilhar o conhecimento de pessoas ou entidades de referência na área da Cibersegurança e dotar o estudante com os conhecimentos mais atualizados e a experiência dos oradores. Seminário II tem ainda três objetivos distintos, desenvolver conhecimento de implementação de segurança no desenvolvimento de frontend e backend, implementar e configurar um sistema de monitorização de integridade de ficheiros (FIM) e cibersegurança e ciberesiliencia em centros de dados modernos.

Conteúdos programáticos

- Os mais modernos métodos de segurança informática em desenvolvimento aplicacional e web;
- Padrões de arquitetura para um desenvolvimento ágil e seguro;
- Segurança no desenvolvimento de frontend e backend;
- Serviços de Bases de Dados, armazenamento de objetos, infraestruturas de segurança e redundância, load balancers, orquestradores e contentorização;
- Erros tipicos conhecidos pela OWASP;
- Técnicas mais conhecidas de Safecoding, Code revision e plataformas de secure coding enforcement;
- Implementação de um software Development Life Cycle Software (SDLC)
- 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).
- Conceitos de Segurança de Centros de Dados;
- Principais riscos e vulnerabilidades em infraestruturas cloud;
- Riscos da Indústria, dos centros de dados e das infraestruturas de Cloud

Metodologias de ensino (avaliação incluída)

A presente unidade curricular utiliza o método de ensino expositivo de conteúdos. A avaliação será efetuada através do desenvolvimento de trabalho científico no âmbito dos temas apresentados no seminário. O trabalho deverá ser apresentado e discutido cientificamente com júri de docentes do curso de pós-graduação em cibersegurança.

Bibliografia principal

Liz Rice (2020), Container Security, O?Reilly, ISBN-10: 1492056707

Kasun Indrasiri and Prabath Siriwardena, Microservices for the Enterprise: Designing, Developing and Deploying, Apress, ISBN-10: 1484238575

Andrew Hoffman (2020), Web application Security: Exploitation and Countermeasures for Modern Web Applications, O?Reilly, ISBN-10: 1492053112

Malcolm McDonald (2020), Web Security for Developers: Real Threats, Practical Defense, No Starch Press, ISBN-10: 1593279949

Dafydd Stuttard and Marcus Pinto (2011), The Web Application Hacker?s Handbook, Wiley, ISBN-10: 1118026470

Mark A. Russo (2019), The Agile/Security development Life Cycle, Independently Published, ISBN-10: 1794490574

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

Academic Year	2023-24
Course unit	
Courses	CIBERSECURITY
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	Portuguese
Teaching/Learning modality	B-Learing

Coordinating teacher Joel David Valente Guerreiro

Teaching staff	Type	Classes	Hours (*)
Joel David Valente Guerreiro	S	S1	2.5S

* 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	2.5	0	0	0	156

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

Not Applicable.

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

Seminary II has the goal to present and share people or entities knowledge in cybersecurity areas for the student to acquire the experience and knowledge of the seminary presenters.

Seminary II has three different objective, the first is to develop security implementation in frontend and backend application developing, the second is to implement an file integrity monitorization system (FIM) and the last to acquire knowledge in cybersecurity and cyber resilience in modern data centers.

Syllabus

- Modern information security methods in software development.
- Architecture patterns, agile and secure development.
- Frontend and Backend Secure development.
- Database services, object storing, security infrastructures and redundancy, load balancers, orchestrators, and containers.
- Typical OWASP known errors.
- Safecoding, Code Revision and Coding enforcement most known techniques.
- Development Life Cycle Software (SDLC) implementation.
- Central Register System concepts.
- Endpoint Detection and response (EDR) concepts.
- Implementing a SIEM.
- Implementing a EDR.
- Learn and implement a monitorization file integrity system (FIM).
- Datacenter Security Concepts.
- Mais risks and vulnerabilities in cloud infrastructures.
- Industry, datacenter and infrastructural risks.
- Practical cloud system attacks.
- Datacenter and cloud infrastructure cybersecurity implementation

Teaching methodologies (including evaluation)

This curricular unit uses expositive teaching methods

The development of a scientific work based on the themes presented on the seminary will be presented and discussed scientifically with a Cybersecurity Post-Graduation teacher Juri that will evaluate the work and presentation.

Main Bibliography

Liz Rice (2020), Container Security, O?Reilly, ISBN-10: 1492056707

Kasun Indrasiri and Prabath Siriwardena, Microservices for the Enterprise: Designing, Developing and Deploying, Apress, ISBN-10: 1484238575

Andrew Hoffman (2020), Web application Security: Exploitation and Countermeasures for Modern Web Applications, O?Reilly, ISBN-10: 1492053112

Malcolm McDonald (2020), Web Security for Developers: Real Threats, Practical Defense, No Starch Press, ISBN-10: 1593279949

Dafydd Stuttard and Marcus Pinto (2011), The Web Application Hacker?s Handbook, Wiley, ISBN-10: 1118026470

Mark A. Russo (2019), The Agile/Security development Life Cycle, Independently Published, ISBN-10: 1794490574

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