EMENTA DO CURSO

Security Operations Architect

Código: **EDU-FTN-SOARCH** Categoria: **Fortinet**

InLearn

PÚBLICO

Security professionals involved in the design, implementation, operation, and monitoring of Fortinet SOC solutions using FortiSIEM and FortiSOAR should attend this course.

PRÉ-REQUISITOS

You must have an understanding of the topics covered in the FortiSIEM Analyst course, or have equivalent experience.

VISÃO

After completing this course, you will be able to:

Describe the main functions and roles within a SOC
Identify the challenges that can be solved by the Fortinet SOC
Describe the MITRE ATT&CK Enterprise Matrix and the Cyber Kill Chain
Describe how to identify and reduce the attack surface
Describe common attack vectors
Describe the benefits of using FortiSIEM and FortiSOAR
Describe different Fortinet SOC deployment architectures
Describe the FortiSOAR Content Hub and connectors
Describe FortiAI features
Describe FortiAI in FortiSIEM and FortiSOAR
Describe reactive and proactive threat hunting processes
Generate threat hunting hypotheses
Identify and configure data sources
Configure data ingestion
Configure FortiSIEM rules
Execute attack vectors
Describe the NIST SP 800-61 incident handling process
Describe the incident handling workflow with FortiSIEM and FortiSOAR
Analyze, handle, and tune incidents on FortiSIEM
Ingest FortiSIEM incidents into FortiSOAR for incident handling
Escalate FortiSOAR alerts into incidents
Describe automation requirements
Describe FortiSOAR playbook steps
Run playbooks to enrich indicators
Configure a playbook to retrieve a hash rating from FortiSandbox
Perform containment on FortiGate, Windows Active Directory, and FortiClient EMS using FortiSOAR connectors
Eradicate artifacts from a compromised host
Release a compromised host from quarantine after recovery
Manage playbook history logs

CONTEÚDO

SOC Concepts and Security Frameworks
Fortinet SOC with FortiSIEM and FortiSOAR
Incident Handling and FortiSIEM
Incident Handling and FortiSOAR
SOC Playbook Development
Threat Hunting

Próximas turmas

11/01/2027

Carga horária	16 horas
Modalidade	Online
Horário	09:00 às 18:00

Prevista

Fale com a InLearn

Acompanhe nossos canais e fale com a nossa equipe para saber mais sobre cursos, próximas turmas e soluções de capacitação.

WhatsApp: +55 (11) 92058-5393

Site · LinkedIn · Instagram · Facebook · YouTube