Cyber Security DevSecOps Entwicklung

IT-Sicherheit / Cybersecurity · Anbieter: IU Akademie IU Internationale Hochschule

FÖRDERUNG & KOSTEN

Kurspreis: auf Anfrage

Förderfähig über: Bildungsgutschein

AZAV-zertifizierter Bildungsträger — Förderung durch die Agentur für Arbeit möglich

Kursdaten auf einen Blick

Durchführung	Online
Lernformat	Self-Paced
Dauer	4 Monate in Vollzeit oder 8 Monate in Teilzeit
Unterrichtssprache	Deutsch
Kursstart	Startet alle 14 Tage
Vorkenntnisse	Keine Vorerfahrung
Abschluss	Zeugnis auf Hochschulniveau
Inklusive	Berufscoaching, Notebook / Tablet (geliehen)

Bildungsträger & Kontakt

IU Akademie IU Internationale Hochschule

Juri-Gagarin-Ring 152, 99084 Erfurt

Telefon: 030 22027283

E-Mail: weiterbildung@iu-akademie.de

Web: https://www.iu-akademie.de

Kurs online ansehen

01 Kursbeschreibung

Sowie der technologische Wandel fortschreitet, erhöht sich auch die Notwendigkeit, Systeme und Daten gegen Cyberbedrohungen abzusichern. Seitdem Softwareentwicklung und IT-Sicherheit immer mehr zusammengewachsen sind, gewinnt die Rolle der Cyber Security DevSecOps Entwicklung immer mehr an Bedeutung. Du erkennst zur richtigen Zeit den Bedarf und nutze Deine Chance - mit Deiner Online-Weiterbildung IT Security DevSecOps Entwicklung.

In Deiner Online-Weiterbildung Cyber Security DevSecOps Entwicklung lernst Du die Grundzüge des System-Pentestings kennen und erfährst, wie Du Schwachstellen in IT-Systemen aufspüren und beheben kannst, bevor sie von Angreifern ausgenutzt werden. In Deiner Weiterbildung bei der IU Akademie wirst Du auch mit den Techniken und Methoden der agilen Softwareentwicklung vertraut gemacht. Du lernst, Softwareprojekte effizient und flexibel zu steuern und die Prinzipien des Continuous Delivery in der Praxis anzuwenden. Darüber hinaus erhältst Du Einblicke in die Welt des DevSecOps und lernst, gängige Software-Schwachstellen zu erkennen und zu beheben. Mit diesem Wissen bist Du bestens gerüstet, um in der IT- und Cyber Security-Branche durchzustarten. Mit Deiner Online-Weiterbildung IT Security DevSecOps Entwicklung wirst Du zur gefragten Fachkraft in der IT- und Cyber Security-Branche.

02 Lehrplan & Module

1. Grundzüge des System-Pentestings

System-Penetrationstests sind ein wichtiger Prozess, um Schwachstellen in IT-Systemen zu finden und deren Behebung zu unterstützen, bevor Angreifer sie ausnutzen können. Aus diesem Grund setzen viele Organisationen solche "Pentester" oder ethische Hacker ein, um ihre Software- und Hardwarebasis (einschließlich Konnektivität) zu testen und die gefundenen Sicherheitsprobleme zu beheben. Dies ist zu einem Eckpfeiler moderner Sicherheitskonzepte geworden. Um bei diesem Unterfangen erfolgreich zu sein, ist jedoch eine gute Kenntnis der verschiedenen Arten von anvisierten IT-Systemen erforderlich. Wir beziehen uns auf Hosts, Netzwerke, Web Apps und sogar Cloud Computing. In diesem Kurs stellen wir die grundlegenden Aspekte von IT-Systemen sowie die Prozesse, Hilfsmittel und Techniken vor, die die industrielle Praxis der Penetrationstests ausmachen. Ausgerüstet mit diesem Wissen werden die Studierenden die Mechanismen eines bestimmten Angriffs verstehen und sich auf den Weg eigener Penetration Tests begeben.
Kursinhalte
Ziele von Penetrationstests und industrielle Perspektive Organisatorischer Nutzen
Rahmenbedingungen für Ethical Hacking
Rechtliche Aspekte
Verantwortungsvolle Offenlegung von Schwachstellen
Professionelle Penetrationstest-Dienstleistungen und Zertifizierungen
Hintergrundkonzepte Betriebssysteme
Hardware-Architekturen
Netzwerke und Protokolle
Web-basierte Anwendungen
Cloud-Computing
Ablauf von Penetrationstests Planung und Erkundung
Whitebox-, Blackbox- und Graybox-Scanning
Zugang erhalten
Aufrechterhaltung des Zugangs
Analyse und Berichterstattung
Härtung und Entschärfung
Betriebssystembasierte Penetrationstests Häufige Fehlkonfigurationen
Shellcode-Angriffe
Speicherkorruption und Pufferüberlauf-Schwachstellen
Metasploit und Kali-Tools
Härtung des Betriebssystems
Netzwerk-Penetrationstests Scoping und Recon der Netzwerkinfrastruktur
Ausnutzen von Netzwerkdiensten
Seitliche Bewegung im Netzwerk
Kerberos-Angriffe
Werkzeugsatz: Nmap, PowerShell, Bloodhound und Tcpdump
Entwickeln von Korrekturmaßnahmen
Web-App-Penetrationstests Die OWASP-Methodik
Open-Source-Intelligenz (OSINT)
Häufig ausgenutzte Web-App-Schwachstellen
Ausnutzungs-Toolset: BurpSuite, sqlmap, BeEF und ExploitDB
Berichterstattung über Ergebnisse und Abhilfemaßnahmen
Spezialisierte Penetrationstests auf einen Blick Ausnutzungs-Entwicklung
Ethisches Hacking
Penetrationstests für drahtlose und mobile Geräte
Bewertung von Cloud-Bedrohungen und Schwachstellen
Fakten zum Modul: Niveau: Bachelor · 5 ECTS-Punkte · Modulprüfung: Examen, 90 Minuten

2. DevSecOps und gängige Software-Schwachstellen

Moderne Organisationen sind bis zu einem gewissen Grad von Software abhängig. In vielen Fällen ist es die kundenspezifische Software in Geschäftsprozessen oder Produkten, die das Hauptunterscheidungsmerkmal darstellt. Aber auch Unternehmen, die keine eigene Entwicklung betreiben, sind auf Software angewiesen, und das Verständnis von Software-Schwachstellen ist für ihren Betrieb lebenswichtig, wie die jüngsten Ransomware-Angriffe gezeigt haben.
In diesem Kurs beschäftigen wir uns mit moderner Software-Entwicklung und Lebenszyklus-Prozessen. Seit den Anfängen mit Extremer Programmierung hat es eine Verlagerung weg vom linearen Wasserfallmodell hin zu einem agilen Entwicklungsprozess gegeben. In jüngerer Zeit hat sich die „Shift-Left“-Entwicklung dafür eingesetzt, dass Sicherheit von Anfang an und nicht erst im Nachhinein berücksichtigt wird.
Um sichere Software zu entwerfen, ist es natürlich wichtig zu verstehen, wie sich Schwachstellen in den Code einschleichen. Wir sehen uns die wichtigsten Aufzählungen von Softwarefehlern an: OWASP und die CWEs von Mitre. Schließlich ist das Patch-Management zum wichtigsten Abwehrinstrument für eine Organisation geworden. Wir betrachten dieses Thema sowohl aus der Perspektive der Softwareentwicklung als auch aus der Sicht des Kunden.
Kursinhalte
Einführung in den Software-Entwicklungsprozess Traditionelle Software-Entwicklung: Wasserfall-Methodik Iterativer Entwurf
Agile Software-Entwicklung
Operationen als separater Prozess
Infrastruktur als Code
Zusammenlegung von Entwicklung und Betrieb: DevOps
Bewährte Praktiken von DevOps Codierung: Code-Entwicklung und -Überprüfung, Quellcode-Verwaltungstools, Code-Zusammenführung.
Build: kontinuierliche Integrationswerkzeuge, Build-Status.
Tests: Instrumente für kontinuierliche Tests, die ein schnelles und zeitnahes Feedback zu Geschäftsrisiken liefern.
Paketierung: Artefakt-Repository, Staging vor der Bereitstellung der Anwendung.
Freigabe: Änderungsmanagement, Freigabegenehmigungen, Freigabeautomatisierung.
Konfigurieren: Konfiguration und Verwaltung der Infrastruktur, Infrastruktur als Code-Tools.
Überwachung: Überwachung der Anwendungsleistung, Endbenutzer-Erfahrung.
Quellen von Sicherheitsfehlern Allgemeine Klassen von Fehlern
Ein Blick auf die OWASP-Top Ten
Blick auf die Mitre CWE™
DevSecOps Schutzziele
Modellierung von Bedrohungen
Wahl der Programmiersprache, Werkzeugkette und Infrastruktur
Linting bei Fragen der Codesicherheit
Prüfung auf Sicherheit
Sicherheit durch Design/Shifting Left
Der Mensch als ein Problem der Sicherheit
Entwerfen in einem Fehlerbericht- und Antwortprozess
Steuern eines Bug-Bounty-Programms
Patch-Verwaltung Dilemma: Auslassen von Software-Update- vs. Sicherheit
Offenlegung von Schwachstellen und der Mitre CVE™ Prozess
Koordinierte Offenlegung von Schwachstellen
Programmsicherheit vs. Software-as-a-Service-Patching
Einsatzstrategien für das frühzeitige Abfangen von Bugs
Zusammenfassung und Forschungsprobleme
Fakten zum Modul: Niveau: Bachelor · 5 ECTS-Punkte · Modulprüfung: Hausarbeit

3. Techniken und Methoden der agilen Softwareentwicklung

Der Kurs vermittelt den Studierenden einen umfassenden Einblick in die agile Softwareentwicklung. Hierbei werden sowohl die grundlegenden agilen Prinzipien dargestellt als auch deren Anwendung im Kontext von kleinen und großen Softwareentwicklungsprojekten. Anhand praktischer Beispiele lernen die Studierenden agile Techniken zur Durchführung der Kernaktivitäten im Software-Engineering kennen. Als besonderer Schwerpunkt wird dabei auch auf den Ansatz des Continuous Delivery eingegangen und dessen Methoden und Werkzeuge vorgestellt.
Kursinhalte
Merkmale und Prinzipien von Agilität Merkmale und Herausforderungen von Softwareprojekten
Klassifikationen von Unsicherheit
Gegenüberstellung von agiler und klassischer Softwareentwicklung
Prinzipien der Agilität
Agile Softwareentwicklung mit Scrum Grundlagen und allgemeiner Aufbau von Scrum
Zentrales Managementartefakt: Product Backlog
Weitere Scrum-Artefakte und Managementwerkzeuge
Agiles Portfolio- und Projektmanagement Planungsebenen im agilen Projektmanagement
Agiles Portfoliomanagement
Organisation mehrerer Teams in einem Projekt
Produkt- und Release-Planung
Requirements Engineering und agiles Architekturmanagement Requirements Engineering in agilen Projekten
Architekturmanagement in agilen Projekten
Agiles Testen Grundlagen des agilen Testens und Anforderungen an die Qualitätssicherungsorganisation
Teststufen und Agilität
Testautomatisierung
Continuous Delivery Grundlagen und Continuous Delivery Pipeline
Continuous Build und Continuous Integration
Akzeptanztests, Lasttests und Continuous Deployment
Fakten zum Modul: Niveau: Bachelor · Unterrichtssprache: Deutsch · 5 ECTS-Punkte · Modulprüfung: Klausur, 90 Minuten

4. Projekt: Agiles DevSecOps-Software-Engineering

Trotz der breiten Akzeptanz von DevOps in der Industrie ist die Integration von Sicherheitsprinzipien in dieses Paradigma (d.h. DevSecOps) für viele IT-Fachleute immer noch eine große Herausforderung. In diesem Kurs lernen die KursteilnehmerInnen grundlegende DevSecOps-Konzepte kennen, wie z.B. die Modellierung von Bedrohungen, die Definition von Sicherheitsgrundsätzen, die kontinuierliche Überwachung der Einhaltung und die Integration der Automatisierung von IT-Sicherheitsprozessen in DevOps.
Kursinhalte
Dieser Kurs behandelt die grundlegenden Sicherheitsprinzipien zur Nutzung des DevSecOps-Ansatzes in Softwaretechnologie Szenarien. Der Inhalt dieses Kurses veranschaulicht die Anwendung von DevSecOps, um die Sicherheit einer Organisation kontinuierlich und ganzheitlich zu verbessern, anstatt sich nur auf den Schutz der zugrundeliegenden Software-Infrastruktur zu konzentrieren (wie im Fall traditioneller, nicht-agiler Methoden). Durch die Präsentation von DevSecOps-Prinzipien wie Bedrohungsmodellierung, Definition von Sicherheitsgrundsätzen, Werkzeuge der Automatisierung von IT-Sicherheitsprozessen und kontinuierliche Überwachung der Einhaltung von Vorschriften wird dieser Kurs vermitteln, wie Sicherheit bei der Entwicklung eines Softwaretechnologie Produkts integriert werden kann.
Fakten zum Modul: Niveau: Bachelor · Unterrichtssprache: Deutsch · 5 ECTS-Punkte · Modulprüfung: Projektbericht

03 Enthaltene Zertifikate

Trägerzertifikat: Zeugnis auf Hochschulniveau

04 Voraussetzungen

Vorkenntnisse

Niveau: Keine Vorerfahrung

Zulassungsvoraussetzung: gute Deutschkenntnisse auf B2-Niveau.

Die Weiterbildung ist auf dem inhaltlichen Niveau eines Bachelor Studiengangs. Eine Weiterbildung auf Bachelor-Niveau vermittelt grundlegende Kenntnisse und Fähigkeiten in einem bestimmten Fachbereich.

Technische Voraussetzungen

Laptop mit Internetzugang.

05 Zielgruppen & Berufsperspektiven

- Arbeitssuchende
- Fachkräfte

Mögliche Berufsbilder: DevSecOps Engineer, DevOps Engineer, Application Security Engineer

NÄCHSTER SCHRITT

Kursdetails online ansehen und Anbieter kontaktieren

IU Akademie IU Internationale Hochschule · Juri-Gagarin-Ring 152, 99084 Erfurt
030 22027283 · weiterbildung@iu-akademie.de · https://www.iu-akademie.de

Online ansehen