DEVSECOPS YÜKSEK GÜVENLİKLİ YAZILIM GELİŞTİRME

Günümüzün hızla değişen dijital dünyasında, yazılım geliştirme süreçlerinin güvenli, hızlı ve verimli olması her zamankinden daha önemli hale gelmiştir. Bu noktada DevSecOps devreye giriyor. DevSecOps, yazılım geliştirme (Dev), operasyon (Ops) ve güvenlik (Sec) alanlarını birleştirerek güvenliği yazılım geliştirme süreçlerinin her aşamasına entegre eden bir yaklaşım sunar.

DEVSECOPS YÜKSEK GÜVENLİKLİ YAZILIM GELİŞTİRME

KURUMSAL ÖZEL EĞİTİM

Bu konuyu istediğiniz gibi özelleştirebilirsiniz. Kullandığınız teknolojiye özel uygulamalar ile anlatılmasını, projenize uygun içerik haline getirilmesini ...

DEVSECOPS YÜKSEK GÜVENLİKLİ YAZILIM GELİŞTİRME EĞİTİMİ

NEDEN DEVSECOPS?

Geleneksel güvenlik yaklaşımları genellikle yazılım geliştirme sürecinin son aşamalarına odaklanır. Ancak DevSecOps, güvenliği baştan sona dahil ederek, daha güvenli bir yazılım geliştirme ortamı sağlar. Erken aşamalarda yapılan güvenlik taramaları ve testler, zafiyetlerin erken tespit edilmesine ve minimize edilmesine olanak tanır.

EĞİTİM HEDEFİ

1. **Güvenli Yazılım Geliştirme:** Katılımcılar, güvenliği yazılım geliştirme sürecine entegre etmeyi öğrenecek.
2. **Otomasyon ve Sürekli İzleme:** Güvenlik testlerini otomatikleştirme ve erken müdahale yöntemleri.
3. **Tehdit Yönetimi:** Güvenlik tehditlerini tanıma ve müdahale yöntemleri.
4. **Ekip İçi İşbirliği:** Daha güvenli yazılım geliştirme süreci için işbirliği yöntemleri.
5. **DevSecOps Araçları:** Gerçek dünya projelerinde kullanılan araç ve teknikler.

Vebende
Bilişim, Eğitim ve Danışmanlık

EĞİTİM İÇERİĞİ

DEVSECOPS TEMELLERİ

- DevOps ve DevSecOps arasındaki farklar
- DevSecOps kültürü ve temel ilkeleri
- Yazılım geliştirme yaşam döngüsünde (SDLC) güvenliğin rolü
- "Shift Left" güvenlik yaklaşımı
- Güvenli kodlama ve güvenlik bilinci oluşturma

DEVOPS ARAÇLARINA GİRİŞ

- CI/CD nedir? Temel kavramlar ve önemi
- Jenkins, GitLab CI, CircleCI, Travis CI gibi araçların tanıtımı
- CI/CD pipeline'larında güvenlik testlerinin rolü
- Otomasyon ve test süreçlerinin entegrasyonu

SÜREKLİ ENTEGRASYON (CI)

- CI araçlarının kullanımı
- Test otomasyonu: Unit testler, fonksiyonel testler ve code coverage
- API ve UI testlerinin entegrasyonu
- Kod kalitesi ve statik analiz araçları (SonarQube vb.)

GÜVENLİK OTOMASYONU

- CI/CD süreçlerinde güvenlik testlerinin otomasyonu
- SonarQube, Snyk, Trivy gibi güvenlik açıkları tarama araçları
- Statik kod analizi (SAST) ve CI süreçlerine entegrasyonu
- Güvenlik açığı tarama sonuçlarının yönetimi

YAZILIM GÜVENLİĞİ VE GÜVENLİ KODLAMA PRATİKLERİ

- OWASP Top 10: En yaygın güvenlik zafiyetleri
- SQL Injection, XSS ve CSRF saldırıları ve önlenmesi
- Güvenli kod inceleme süreçleri ve teknikleri

STATİK VE DİNAMİK GÜVENLİK TESTLERİ

- Statik analiz araçları: SonarQube, Checkmarx
- Dinamik güvenlik test araçları: OWASP ZAP, Burp Suite
- SAST ve DAST karşılaştırması
- Pipeline'da SAST ve DAST entegrasyonu

SÜREKLİ DAĞITIM (CD)

- Dağıtım stratejileri: Blue-Green, Canary, Rolling
- CD araçları ve dağıtım süreçlerinin güvenliğe entegre edilmesi
- Uygulama izleme ve geri dönüş stratejileri
- Load ve performans testleri

KONTEYNER VE KUBERNETES GÜVENLİĞİ

- Docker ve Kubernetes güvenliği
- Güvenli Docker imajları oluşturma
- Aqua Security, Twistlock gibi konteyner güvenlik araçları
- Kubernetes'te güvenli yapılandırma ve izleme

GİZLİ BİLGİLERİN YÖNETİMİ (SECRETS MANAGEMENT)

- Gizli anahtarlar ve şifrelerin güvenli yönetimi
- Vault, AWS Secrets Manager, Azure Key Vault kullanımı
- CI/CD pipeline'larında secrets yönetimi

AÇIK KAYNAK GÜVENLİK AÇIKLARI YÖNETİMİ

- Açık kaynak bağımlılıklarının güvenli yönetimi
- Snyk, Dependabot ile açık kaynak güvenlik açıklarını tarama
- Açık kaynak güvenlik yamalarının uygulanması

INFRASTRUCTURE AS CODE (IAC) VE GÜVENLİK

- Infrastructure as Code kavramı ve araçları (Terraform, CloudFormation)
- IaC güvenlik açıkları ve güvenli yapılandırma
- Bridgecrew, Checkov gibi güvenlik araçları ile IaC güvenliği

SÜREKLİ İZLEME VE TEHDİT TESPİTİ

- Güvenlik olaylarının izlenmesi ve raporlanması
- SIEM sistemleri: Splunk, ELK
- Log yönetimi ve anomali tespiti
- Wazuh ve OSSEC kullanımı

ZARARLI YAZILIM ANALİZİ VE KORUMA

- Zararlı yazılımların tespiti ve analizi
- CI/CD süreçlerinde anti-malware araçlarının entegrasyonu

PENETRASYON TESTİ VE RED TEAMİNG

- Penetrasyon testleri ve CI/CD entegrasyonu
- Pentest araçları: Metasploit, Nmap, Wireshark
- Red Team operasyonları ve güvenlik savunmalarının testi

BULUT GÜVENLİĞİ

- AWS, Azure ve Google Cloud güvenlik mimarileri
- Cloud Security Posture Management (CSPM) araçları
- Bulutta kimlik ve erişim yönetimi (IAM) güvenliği

ZERO TRUST GÜVENLİK MODELİ

- Zero Trust güvenlik yaklaşımı
- Kullanıcı doğrulama ve yetkilendirme stratejileri
- Mikro segmentasyon ve ağ güvenliği

OLAY MÜDAHALESİ (INCIDENT RESPONSE)

- Güvenlik ihlalleri karşısında olay müdahale süreçleri
- CI/CD pipeline'ında otomatik ihlal tespiti
- Incident response araçları ve playbook'lar

SÜREKLİ GÜVENLİK TESTLERİ VE GERİ BİLDİRİM DÖNGÜSÜ

- CI/CD pipeline'ında sürekli güvenlik testleri oluşturma
- Güvenlik testlerinin analiz edilmesi ve optimize edilmesi
- Sürekli güvenlik geri bildirim döngülerinin oluşturulması

DEVSECOPS KÜLTÜRÜ VE ORGANİZASYONEL DEĞİŞİM

- DevSecOps kültürünün organizasyona entegrasyonu
- Güvenlik ve geliştirme ekipleri arasında iş birliği
- Güvenlik bilincini artıran atölye çalışmaları
- Yalın (Lean) ve Agile metodolojilerinin DevSecOps ile entegrasyonu

EĞİTİM SÜRESİ

- Süre: 20 Gün
- Ders Süresi: 50 dakika
- Eğitim Saati: 10:00 - 17:00

Eğitim formatında eğitimler 50 dakika + 10 dakika moladır. 12:00-13:00 saatleri arasında 1 saat yemek arasındaki verilir. Günde toplam 6 saat eğitim verilir. 20 günlük formatta 120 saat eğitim verilmektedir.

Eğitimler uzaktan eğitim formatında tasarlanmıştır. Her eğitim için teams linkleri gönderilir. Katılımcılar bu linklere girerek eğitimlere katılırlar. Ayrıca farklı remote çalışma araçları da eğitmen tarafından tüm katılımlara sunulur. Katılımcılar bu araçları kullanarak eğitimlere katılırlar.

Eğitim içeriğinde github ve codespace kullanılır. Katılımcılar bu platformlar üzerinden örnek projeler oluşturur ve eğitmenle birlikte eğitimlerde sorulan sorulara ve taleplere uygun iceriğe cevap verir. Katılımcılar bu araçlarla eğitimlerde sorulan sorulara ve taleplere uygun iceriğe cevap verir. Eğitim yapay zeka destekli kendi kendine öğrenme formasyonu ile tasarlanmıştır. Katılımcılar eğitim boyunca kendi kendine öğrenme formasyonu ile eğitimlere katılırlar. Bu eğitim formatı sayesinde tüm katılımcılar gelecek tüm yaşamlarında kendilerini güncellemeye devam edebilecekler ve her türlü sorunun karşısında çözüm bulabilecekleri yeteneklere sahip olacaklardır.

DEVSECOPS YÜKSEK GÜVENLİKLİ YAZILIM GELİŞTİRME

DEVSECOPS'UN FAYDALARI

- Erken Güvenlik Testi ve Tarama: Güvenlik testleri yazılım geliştirme sürecinin ilk aşamalarında yapılır ve maliyetleri düşürür.
- Otomasyon ve Sürekli İzleme: Güvenlik uygulamaları otomatikleşir, tehditler hızlı algılanır ve yanıt verilir.
- Hız ve Güvenlik Dengesi: Geliştirme süreci hızlanırken güvenlik riskleri minimize edilir.
- Ekipler Arası İşbirliği: Geliştirici, operasyon ve güvenlik uzmanları arasında güçlü işbirliği sağlanır.
- Risk Yönetimi: Sürekli risk değerlendirmesi ve yönetimi yapılır.

KATILIMCILARDAN BEKLENTİLERİMİZ

- **Temel Bilgisayar ve Yazılım Bilgisi:** Temel işletim sistemi (Windows, macOS veya Linux) kullanımı. Komut satırı (CLI) ile çalışmaya aşinalık.
- **Yazılım Geliştirme ve Versiyon Kontrolü Deneyimi (Tercihen):** Git ve GitHub gibi versiyon kontrol sistemleri hakkında temel bilgiye sahip olunması faydalı olacaktır. Yazılım geliştirme veya sistem yönetimi alanında çalışan katılımcılar için içerik daha hızlı ilerleyebilir.

EĞİTİM YÖNTEMİ

- Teorik Bilgi: Güncel bilgiler ve konseptlerin anlatımı.
- Uygulamalı Örnekler: Gerçek senaryolarla pratik uygulamalar.
- Etkileşimli Tartışmalar: Katılımcıların aktif katılım sağlayacağı, soru-cevap şeklinde tartışmalar yapılacak oturumlar.
- Proje Tabanlı Öğrenme: Eğitimin boyunca katılımcıların katılımcıların öğrendiklerini pratikte uygulayacakları eğitim formasyonu uygulanacaktır.

HEDEF KİTLE

- **Yazılım Geliştiriciler:** Yazılım geliştirme süreçlerinde güvenlik önlemleri almak isteyen, güvenli yazılım geliştirme pratiği kazanmak isteyen profesyoneller.
- **DevOps Mühendisleri:** DevOps süreçlerine güvenliği entegre etmek isteyen ve CI/CD pipeline'larında güvenlik testlerinin rolünü öğrenmek isteyen mühendisler.
- **Sistem ve Altyapı Yöneticileri:** Altyapı güvenliği ile ilgilenen ve DevSecOps uygulamalarıyla bulut ve container güvenliğini sağlamak isteyen profesyoneller.
- **Güvenlik Uzmanları:** Yazılım geliştirme ve operasyon süreçlerinde güvenliği daha iyi yönetmek isteyen ve güvenlik açıklarını tespit etme konusunda daha derin bilgi sahibi olmak isteyen güvenlik profesyonelleri.
- **Test Mühendisleri:** Yazılım test süreçlerinde güvenlik testlerinin nasıl entegre edileceğini öğrenmek isteyen ve güvenlik test otomasyonuna odaklanmak isteyen test mühendisleri.
- **DevSecOps ve Agile Ekip Liderleri:** DevSecOps ve Agile metodolojilerini organizasyonlarına entegre etmek ve güvenlik kültürünü yaymak isteyen liderler.

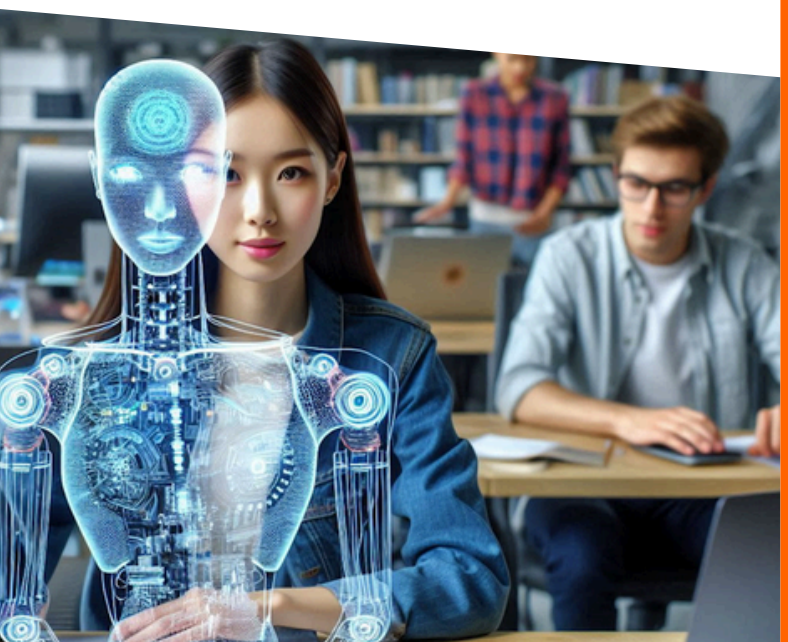
"

Kurumsal size özel eğitimler hazırlıyoruz. Her eğitim yeni bir heyecan.

Vebende A.Ş.

Kurumsal Terzi Usulü Butik Eğitimler.

Size özel hazırlanan seminer, danışmanlık, eğitim ve hizmetlerimizle yüksek verim elde edin. Paranızı boşa harcamayın. Zaman çok değerli.



Her Eğitim Yeni Bir Heyecan

2000 yılından günümüze devam eden eğitim heyecanı. Uluslararası tecrübe, proje geliştirme deneyimleri, danışmanlıklar ve arge mühendislik deneyimlerimizi ülkemize sunmak için yeni bir konsept tasarladık.
Sizi dinliyor, takımınıza uygun özel içerikler ile hazırlanmış eğitimler hazırlıyoruz. Her eğitim özel bir çalışma, içerik üretimi, uygulama örnekleri hazırlıkları, sunumlar hazırlamayı gerektiriyor. Aynı eğitimi yönetim kadrosuna farklı, teknik ve mimar ekiplerinize farklı içerikler ile hazırlıyoruz. Her eğitim yeni bir macera ve heyecan.

Bizimle İletişime Geçin

iletisim@vebende.com

www.vebende.com.tr

İzmir - Türkiye

Kurumsal
Eğitimler

www.vebende.com.tr

İletişime Geçin

Whatsapp 0542 5505704

iletisim@vebende.com

www.vebende.com.tr

Adalet Mah. Manas Bulvarı
No:39 İç Kapı N0: 3107 Bayraklı
İZMİR






Sürekli Güncellenen Eğitimlerimizi Sitemizden Takip Edin.

"

Kurumsal terzi usulu size özel eğitimler ve uluslararası deneyime sahip eğitmenler ile çalışmanın keyfi

"

Size Neler Sunuyoruz?

- Kitaptan okunan eğitimler sunmuyoruz. Sizin için özel hazırlanan içerikler ve uygulamalı eğitimler hazırlıyoruz.
- Her eğitim için sunumlar, materyaller, örnek senaryolar size özel hazırlıyoruz.
- Her eğitim için katılımcılara özel github repoları hazırlanıyor. Eğitimden sonra da katılımcılar hayat boyu kaynaklara ulaşmaya devam edebilsinler diye, **"katılımcılar ve eğitmenle birlikte yapılan tüm çalışmaları"** github repolarında saklıyoruz.

Misyonumuz

1. Ülkemizde dünyanın en güncel teknolojilerini kazandırmak. En güncel teknolojilerine hakim takımlarına katkı sağlamak.
2. Alışılmışın dışında en güncel teknolojileri deneyimli eğitmenler ve uygulamalar ile sunmak.
3. Siber güvenlik konusunda hassas çalışmalar sunarak, çağımızın büyük kabusu siber tehditler konusunda deneyimli bilgili takımların oluşmasına katkı sağlamak.