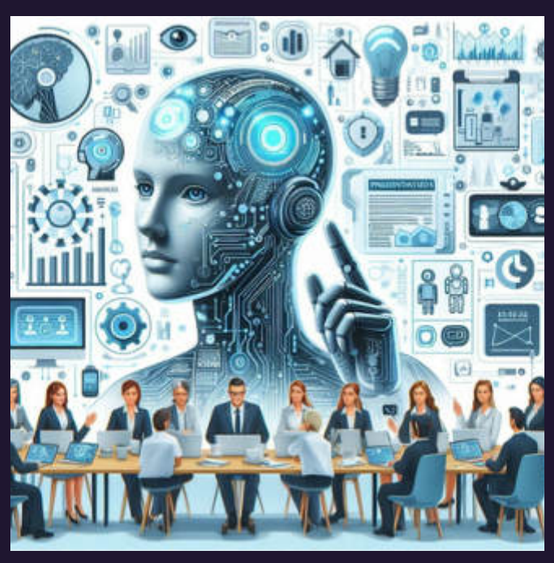
VEBENDE A.Ş.

KURUMSAL BUTİK SİZE ÖZEL EĞİTİM İÇERİKLERİ



BUTİK KURUMSAL CANLI EĞİTİMLER

Her eğitim için özel içerikler materyaller ve uygulamalar-kodlar üretiyoruz. Taleplerinizi dikkatle dinliyor, en güncel teknolojileri kullanarak size özel eğitim deneyimi sunuyoruz. Eğitim sürecinde kullanılan kodlar, senaryolar ve deneyimler tamamen size özgü olarak hazırlanır ve tüm çalışmalar GitHub depolarında ömür boyu erişilebilir hale getirilir. Bu, sadece eğitim sürecinde değil, gelecekte de sürekli gelişiminiz için güçlü bir kaynak sunar.

Bizim için her eğitim, yeni bir fırsat ve heyecan verici bir süreçtir. Eğitim ihtiyaçlarınıza göre dünya çapında kapsamlı incelemeler yapıyor, en yeni teknolojileri keşfediyor ve sizinle yapılan görüşmelere dayanarak tüm içeriklerimizi sıfırdan tasarlıyoruz. Eğitim başlamadan önce sunumlar, kitaplar, senaryolar ve kodlar özel olarak hazırlanır ve titizlikle test edilir. Böylece eğitim süreciniz, sektördeki en güçlü ve verimli kaynaklara sahip olmanızı sağlar.

“KURUMSAL TERZİ USULÜ SİZE ÖZEL EĞİTİMLER VE ULUSLARARASI DENEYİME SAHİP EĞİTMENLER İLE ÇALIŞMANIN KEYFİ”

www.vebende.com.tr

Whatsapp mesaj 0542 5505704

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

KUBERNETES MİMARİSİ ÜZERİNDE UÇTAN UCA DEVSECOPS YAZILIM GELİŞTİRİCİLER İÇİN

Bu **on günlük, uygulamalı teknik atölye çalışması, Kubernetes-yerel ortamlarda DevSecOps pratiklerinde** ustalaşmayı hedefleyen yazılım geliştiriciler ve DevOps mühendisleri için özel olarak yapılandırılmıştır. Küresel tedarikçilere hizmet veren yüksek ölçekli bir B2B pazar yeri olan kurgusal dijital platform **“SecureBazaar”** senaryosu etrafında kurgulanan program, sürekli entegrasyon, sürekli teslimat ve çalışma zamanı savunmasını içeren **gerçek dünya güvenlik ve teslimat işlem hatlarına** vurgu yapmaktadır.

Katılımcılar, Kubernetes'te **yazılım teslimat yaşam döngüsünün tamamını** deneyimleyecektir — mikroservis mimarisi tasarımı, uygulamaların konteynerleştirilmesi, güvenli işlem hatlarının tanımlanması, uyumluluk geçitlerinin uygulanması, kod olarak ilke (policy-as-code) prensiplerinin zorlanması ve farklı ortamlara (geliştirme/hazırlık/üretim) sıfır güven iş yüklerinin konuşlandırılması süreçlerini içerecektir.

Talep üzerine her senaryo uyarlanabilir; bu uyarlamalar, finans sektörüne özgü uyumluluk standartları (örn. PCI-DSS, SOX), sağlık sektörüne özgü gizlilik kontrolleri (örn. HIPAA) veya kamu siber güvenlik çerçeveleri (örn. NIST 800-53, MITRE ATT&CK eşlemesi) gibi spesifik endüstriyel gereksinimleri yansıtacak şekilde gerçekleştirilebilir.

Yazılım Geliştiriciler, DevOps Mühendisleri ve Teknik Ekip Liderleri için ideal olan bu atölye, güvenli kodlama ile güvenli konuşlandırma arasındaki boşluğu kapatmayı hedefler; ekiplere yazılımlarını güvenli bir şekilde, yüksek ölçekte inşa etme, gönderme ve çalıştırma yetkinliği kazandırır.

KAZANIMLAR

Atölye sonunda katılımcılar aşağıdaki yetkinliklere sahip olacaktır:

- Kubernetes-yerel güvenlik desenlerini (sidecar'lar, init konteynerler, servis ağı) kullanarak **mikroservis mimarisi tasarlama yetkinliği**.
- Dockerfile en iyi pratikleri, çok aşamalı derlemeler, SBOM üretimi ve root olmayan kullanıcı ile çalıştırma prensiplerini uygulayarak **güvenli konteynerler inşa etme becerisi**.
- Jenkins, GitHub Actions, GitLab CI ve Tekton gibi araçları kullanarak entegre güvenlik geçitleri içeren **CI/CD işlem hatları uygulama yetkinliği**.
- Konuşlandırma öncesinde Kubernetes kaynak tanımlarını doğrulamak için OPA/Gatekeeper kullanarak **kod olarak ilke (policy-as-code) prensiplerini zorlama becerisi**.
- Denetim izleri ve RBAC destekli dağıtım akışları ile ArgoCD veya Flux aracılığıyla konuşlandırmaları otomatize etmek için **GitOps kullanma yetkinliği**.
- Konteynerler, bağımlılıklar ve IaC (Kod Olarak Altyapı) yapılandırmaları üzerinde statik/dinamik güvenlik taramaları **uygulama yetkinliği** (Trivy, Snyk, Checkov).
- HashiCorp Vault, SealedSecrets ve External Secrets gibi araçlarla **gizli veri yönetimini (secrets management) otomatize etme becerisi**.
- Falco, Kyverno, AppArmor ve seccomp gibi Kubernetes-yerel araçları kullanarak **çalışma zamanı koruması uygulama yetkinliği**.
- Güvenlik açığı teşhiri, yetkisiz erişim ve çalışma zamanı davranışı için uyumluluk denetimi ve gözlemlenebilirlik **yapılandırma yetkinliği**.
- Loglar, denetim izleri ve konteyner çalışma zamanı analiz araçlarından elde edilen adli (forensics) verileri kullanarak **olaylara müdahale etme yetkinliği**.

Atölye Programı

Gün 1

Güvenli Bir Platform Olarak Kubernetes

Ad Alanları (Namespaces), RBAC, PSP/PSS, Ağ Politikaları (Network Policies), Kabul Denetleyicileri (Admission Controllers)

Gün 2

Güvenli Konteyner Geliştirme Pratikleri

Güvenli Dockerfile Yazımı, Root Olmayan Konteynerler, SBOM Üretimi, SLSA Çerçevesi

Gün 3

İşlem Hattı Temelleri (CI/CD)

CI/CD Sistemleri, SCM Entegrasyonları, Jenkins/GitLab İşlem Hatları

Gün 4

İşlem Hattı Güvenliği

Gizli Veri Yönetimi (Secrets Management), Kod Tarama, Yapıt (Artifact) İmzalama, Geliştirme/Test Ortamları Güvenliği

Gün 5

Kod Olarak İlke ile GitOps

ArgoCD/Flux GitOps İşlem Hatları, Konuşlandırma Kontrolleri için OPA/Gatekeeper Uygulamaları

Atölye Programı

Gün 6

İmaj ve Bağımlılık Tarama

Trivy, Clair, Snyk, OSS Index Kullanımı, Yazılım Tedarik Zinciri Koruması

Gün 7

Kod Olarak Altyapı (IaC) Güvenliği

Terraform, Helm, Kustomize Güvenlik En İyi Pratikleri, IaC Tarama (Checkov)

Gün 8

Çalışma Zamanı Savunması

Falco, Kyverno, AppArmor/seccomp Uygulamaları, Çalışma Zamanı İzleme

Gün 9

Uyumluluk ve Tehdit Modelleme

MITRE ATT&CK, NIST, CIS Kıyaslamaları (Benchmarks), Uyumluluk Gösterge Panelleri (Kubescape, Kubebench)

Gün 10

Olay Simülasyonu ve Müdahale

Canlı Saldırı Simülasyonu, Denetim İzleri Analizi, Triage Süreçleri, Adli Analiz, Nihai Bitirme Senaryosu

Atölye Programı Uygulama

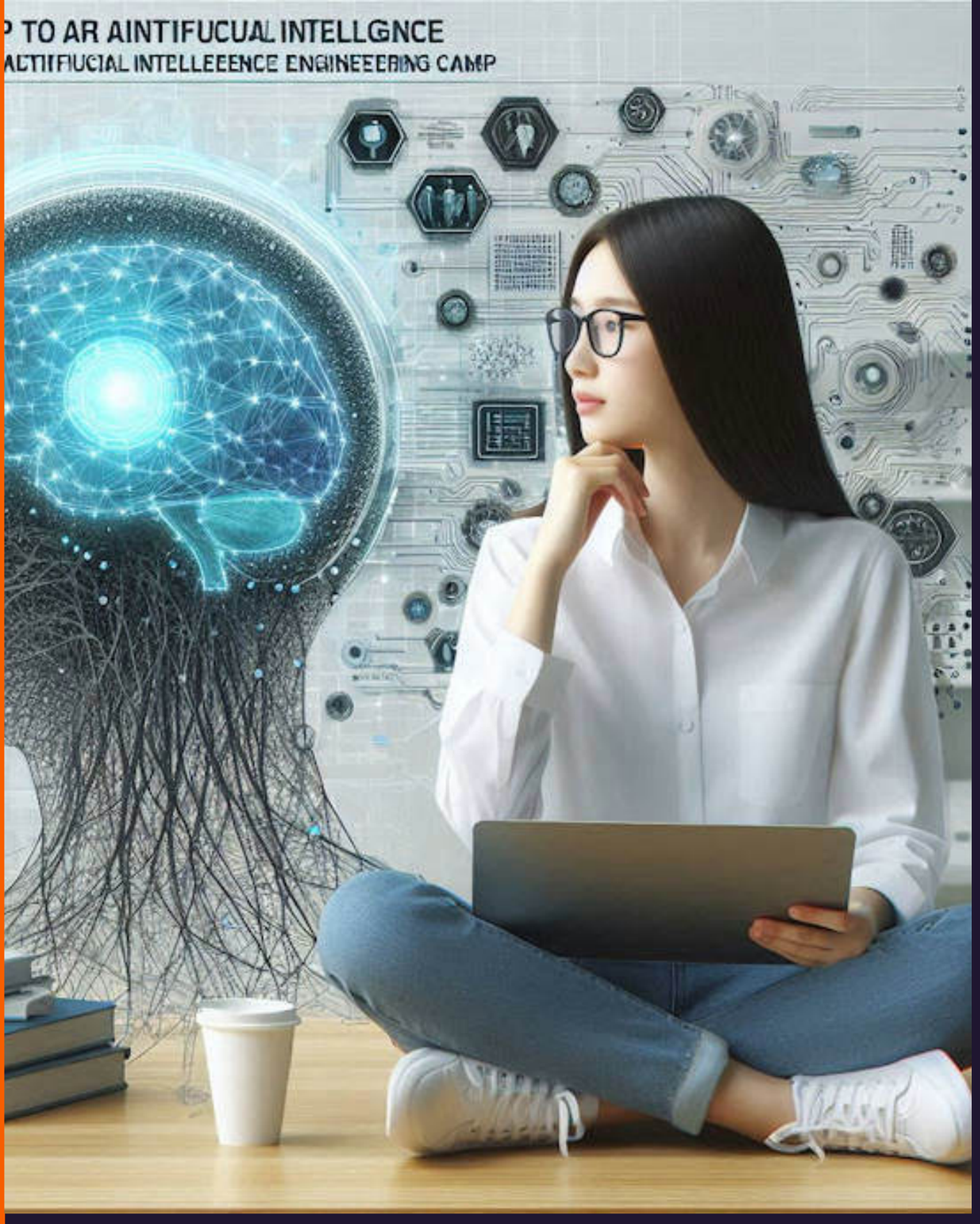
Eğitim programı başlamadan önce, kurum temsilcileriyle kapsamlı bir çevrimiçi toplantı yapılır. Bu görüşme, sadece tanışmak için değil; aynı zamanda kurumun ihtiyaçlarını, önceliklerini ve hedeflerini net bir şekilde anlamak için kritik bir adımdır. Toplantı sırasında hangi konulara odaklanılacağı, hangi teknolojilerin kullanılacağı ve eğitimin nasıl yapılandırılacağı birlikte planlanır. Böylece, yalnızca teorik bilgi sunan değil, aynı zamanda kuruma özel örnek senaryolar ve uygulamalı laboratuvar çalışmaları içeren, sahaya doğrudan dokunan bir eğitim programı ortaya çıkar.

Bu hazırlık süreci sayesinde her eğitim, sıfırdan ve tamamen o kuruma özel olarak tasarlanır. Hazır şablonlar ya da genellenmiş içerikler yerine, kullanılacak tüm dokümanlar, örnek uygulamalar ve teknik kaynaklar kurumun iş yapısına, sektörel ihtiyaçlara ve katılımcıların mevcut bilgi seviyelerine göre özel olarak geliştirilir.

Eğitim süreci boyunca katılımcılar, eğitmenle sürekli etkileşim halindedir. Yalnızca anlatımı dinlemekle yetinmezler; senaryo temelli uygulamalara doğrudan katılır, birlikte çalışarak örnek vakaları analiz eder ve karar süreçlerini deneyimleme fırsatı bulurlar. Sorular sorulur, cevaplar birlikte keşfedilir; her katılımcı, sürece aktif olarak dahil olur. Bu yapı, öğrenmenin yalnızca bilgi edinmekten ibaret olmadığını; deneyimleyerek, tartışarak ve uygulayarak pekiştirilebileceğini esas alır.

Atölye boyunca katılımcılar yalnızca teknik detayları öğrenmekle kalmaz; ele alınan konuyu farklı açılardan değerlendirme, neden-sonuç ilişkilerini kurma ve konunun büyük resimdeki yerini görme becerisi kazanır. **Bu sayede eğitim, katılımcılara 360 derecelik bir bakış açısı kazandırarak, konuyu bütüncül ve derinlemesine anlamalarını sağlar.**

Sonuç olarak, her atölye çalışması içerik ve yapısıyla tamamen özgün hale gelir. Eğitim, kurumun güvenlik, verimlilik ve gelişim hedeflerine doğrudan katkı sağlayacak şekilde tasarlanır ve **kuruma özel, yüksek katma değerli bir öğrenme deneyimi** sunar.



Size Neler Sunuyoruz?

- Standart eğitim yaklaşımlarının ötesinde, her katılımcı için özelleştirilmiş, uygulamalı ve sektörel ihtiyaçlara yönelik içerikler hazırlıyoruz.
- Eğitimlerimizi, her katılımcının ihtiyaç ve hedeflerine göre özelleştiriyor; sunumlar, materyaller ve senaryoları sizin için özgün olarak hazırlıyoruz.
- Katılımcılara özel GitHub depoları ile her eğitim için özgün içerikler sağlıyoruz ve eğitim sonrasında da tüm materyalleri, senaryoları ve örnekleri sürekli erişilebilir hale getiriyoruz.





Sürekli Güncellenen Eğitimlerimizi Sitemizden Takip Edin.

İletişime Geçin

Whatsapp Mesaj 0542 5505704

iletisim@vebende.com

www.vebende.com.tr

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

Misyonumuz

1. Ülkemize, dünya çapında güncel ve stratejik teknolojilerin kazandırılmasına katkı sağlamak. Takımların, küresel teknoloji trendlerine uyumlu yetkinlikler geliştirmesine destek olmak.
2. Alışılmış kalıpların ötesine geçerek, güncel ve etkili teknolojileri; deneyimli eğitmenler, uygulamalı içerikler ve sektörel senaryolarla sunuyoruz.
3. Siber güvenlik alanında titiz ve stratejik çalışmalarla, günümüzün en büyük siber tehditlerine karşı güçlü ve bilinçli takımların yetişmesine öncülük ediyoruz.