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
0532 512 7811

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

KUBERNETES ÜZERİNDE GÜVENLİ .NET İŞ YÜKLERİ – KURUMSAL ORTAMLARDA OWASP UYUMLU MİKROSERVİSLER

Bu **on günlük, senaryo tabanlı teknik atölye çalışması, Kubernetes ortamlarında güvenli ve ölçeklenebilir .NET Core tabanlı mikroservisler** geliştiren ekipler için özel olarak tasarlanmıştır. Yeni nesil altyapı güvenlik çözümleri sağlayan, kurgusal ancak gerçekçi bir kurumsal yapı olan **“Infrasec Dynamics”** senaryosu etrafında merkezlenen eğitim, **konteynerize .NET dağıtım işlem hatlarından (pipelines),** üretim Kubernetes iş yüklerindeki **OWASP Top 10 hafifletme tekniklerine** kadar uzanan günlük uygulamalı (hands-on) alıştırmalarla katılımcıları kapsamaktadır.

Katılımcılar, açık kaynaklı ve kurumsal düzeyde araç setlerini kullanarak **mikroservis kodunu ve altyapısını güçlendirmeyi** öğrenirken, **RBAC güdümlü iş yükü izolasyonu, sıfır güven hizmet ağı uygulaması, güvenlik geçitleri içeren çok aşamalı CI/CD ve OWASP ZAP entegre işlem hatları** gibi ileri düzey senaryolarla etkileşimde bulunacaktır.

Senaryo özelleştirmesi mevcuttur ve müşteriye özgü kullanım senaryolarını yansıtacak şekilde ayarlanabilir: Ekiplerinizin bankacılık düzeyinde kimlik hizmetleri, sağlık verisi hassasiyetine sahip SaaS platformları veya kamu düzeyinde kısıtlı mikroservisler geliştirmesi fark etmeksizin, tüm modüller ve laboratuvarlar kurumunuzun uyumluluk ve teknik mimarisiyle uyumlu hale getirilecektir.

Bu atölye, güvenlik odaklı pratikleri Kubernetes-yerel uygulama yaşam döngüsüne dahil etmek isteyen **.NET Geliştiriciler, DevSecOps Mühendisleri, Uygulama Mimarları ve Platform Mühendisleri** için idealdir.

KAZANIMLAR

Atölye sonunda katılımcılar aşağıdaki yetkinliklere sahip olacaktır:

- Üretim düzeyinde Kubernetes ortamları için **.NET mikroservisleri inşa etme ve konteynerleştirme yetkinliği**.
- GitHub Actions, GitLab CI veya Azure DevOps gibi araçları OWASP ZAP, Trivy ve Snyk entegrasyonu ile kullanarak **güvenlik odaklı CI/CD işlem hatları uygulama yetkinliği**.
- Pod Güvenlik Politikaları, SecurityContext, Seccomp ve AppArmor profilleri aracılığıyla Kubernetes iş yüklerini **güçlendirme yetkinliği**.
- HTTPS, karşılıklı TLS ve giriş kimlik doğrulama mekanizmaları (OAuth2, JWT) ile güvenli API iletişimini **zorlama yetkinliği**.
- Kod olarak ilke (OPA/Gatekeeper) ile ArgoCD veya Flux kullanarak GitOps tabanlı dağıtım iş akışlarını **tasarlama yetkinliği**.
- Istio, Linkerd veya Cilium servis ağı kullanarak sıfır güven ağ modellerini **entegre etme yetkinliği**.
- Enjeksiyon, XSS, bozuk kimlik doğrulama ve SSRF gibi OWASP Top 10 tehditlerini uygulama kodu ve altyapı sınırları aracılığıyla **hafifletme yetkinliği**.
- Trivy, Kube-bench ve Falco gibi araçlarla konteynerlerin, kodun ve çalışma zamanının güvenlik taramasını **gerçekleştirme yetkinliği**.
- Kümeler ve iş yükleri genelinde en az ayrıcalık erişimi için RBAC modellerini **tasarlama yetkinliği**.
- Prometheus, Grafana ve Alertmanager kullanarak güvenlik bağlamı görünürlüğü ile izleme ve uyarı **uygulama yetkinliği**.

Atölye Programı

Gün 1

Konteynerize .NET Temelleri

ASP.NET Core API'leri, Dockerfile'lar, Derleme Optimizasyonları, Çok Aşamalı Derlemeler

Gün 2

Kubernetes Dağıtım Esasları

YAML Temelleri, Dağıtımlar (Deployments), Servisler, ConfigMap'ler, Gizli Veriler (Secrets), Helm, Kustomize

Gün 3

Güvenli Kodlama Pratikleri

.NET Uygulamalarında Girdi Doğrulama, Kimlik Doğrulama Desenleri, OWASP Top 10 Eşleştirmesi

Gün 4

CI/CD Güvenlik Geçitleri

GitHub Actions + Trivy, Snyk, ZAP, CodeQL Entegrasyonu İşlem Hatlarına

Gün 5

Kubernetes Güvenlik Mimarisi

Pod Güvenliği, RBAC, SecurityContext, Kabul Denetleyicileri (Admission Controllers), OPA/Gatekeeper

Atölye Programı

Gün 6

Servis Ağı ve Sıfır Güven

Istio/Linkerd Kurulumu, Karşılıklı TLS, Giriş Kimlik Doğrulama/Yetkilendirme, Trafik Şifrelemesi

Gün 7

Güvenlik İçin Gözlemlenebilirlik

Prometheus, Grafana, Loki, Güvenlik Gösterge Panelleri, Denetim Kayıtları (Audit Logs)

Gün 8

Çalışma Zamanı Tehdit Tespiti

Falco, Sysdig Secure, Olay İzleme, Alertmanager İşlem Hatları

Gün 9

Uçtan Uca Güvenli GitOps Teslimatı

ArgoCD + İlke Zorlama, Helm/Kustomize ile GitOps, Canary ve Blue/Green Dağıtımlar

Gün 10

Bitirme Projesi

OWASP Uyumlu Yığın ile Bir .NET Mikroservisi İnşa Etme, Güvenliğini Sağlama, Konuşlandırma ve İzleme

Atölye Programı Uygulama

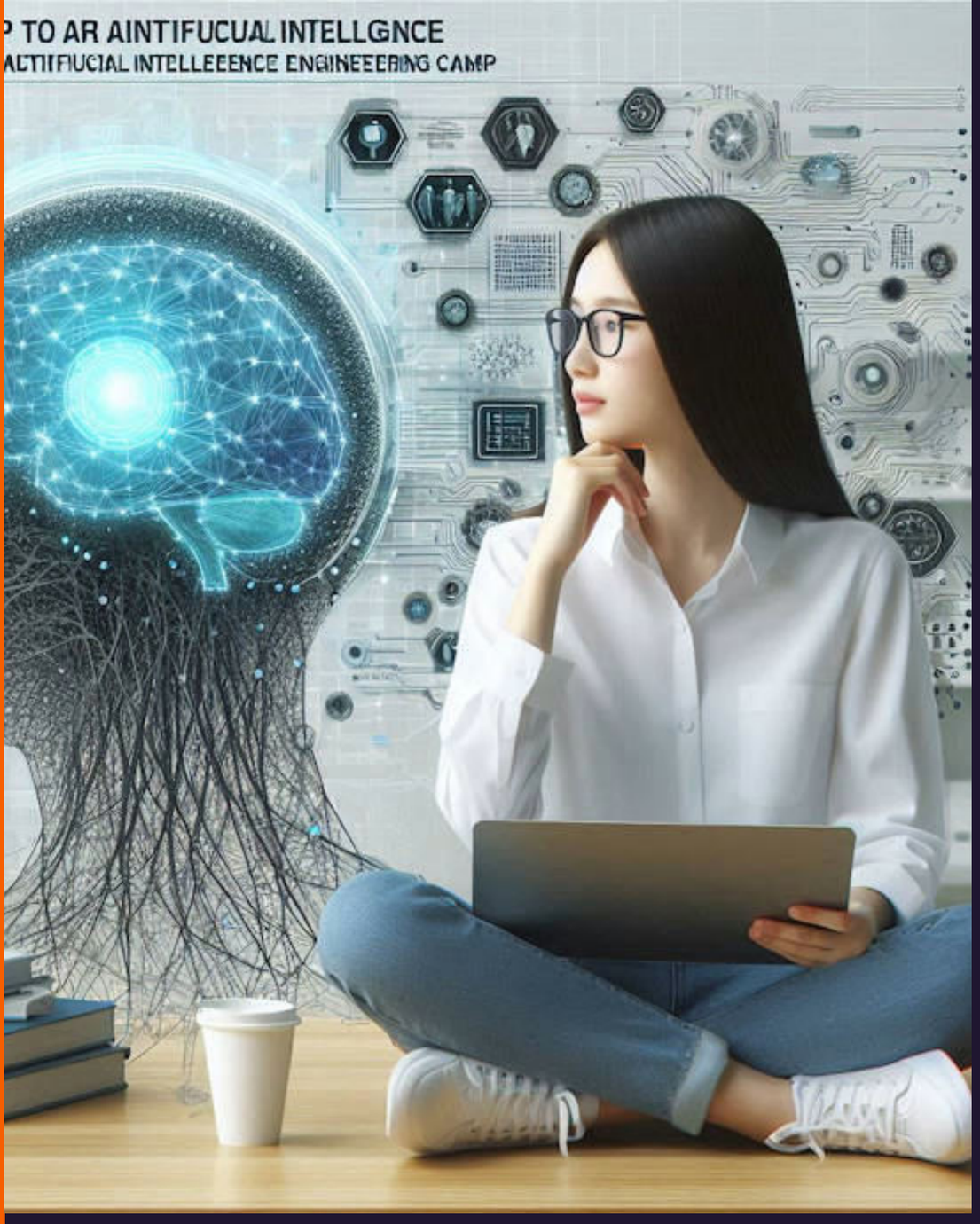
Eğitim programı başlamadan önce, kurum temsilcileriyle kapsamlı bir çevrimiçi toplantı yapılır. Bu görüşme, sadece tanışmak için değil; aynı zamanda kurumun ihtiyaçlarını, önceliklerini ve hedeflerini net bir şekilde anlamak için kritik bir adımdır. Toplantı sırasında hangi konulara odaklanılacağı, hangi 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
0532 512 7811

iletisim@vebende.com.tr

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.