ELK STACK

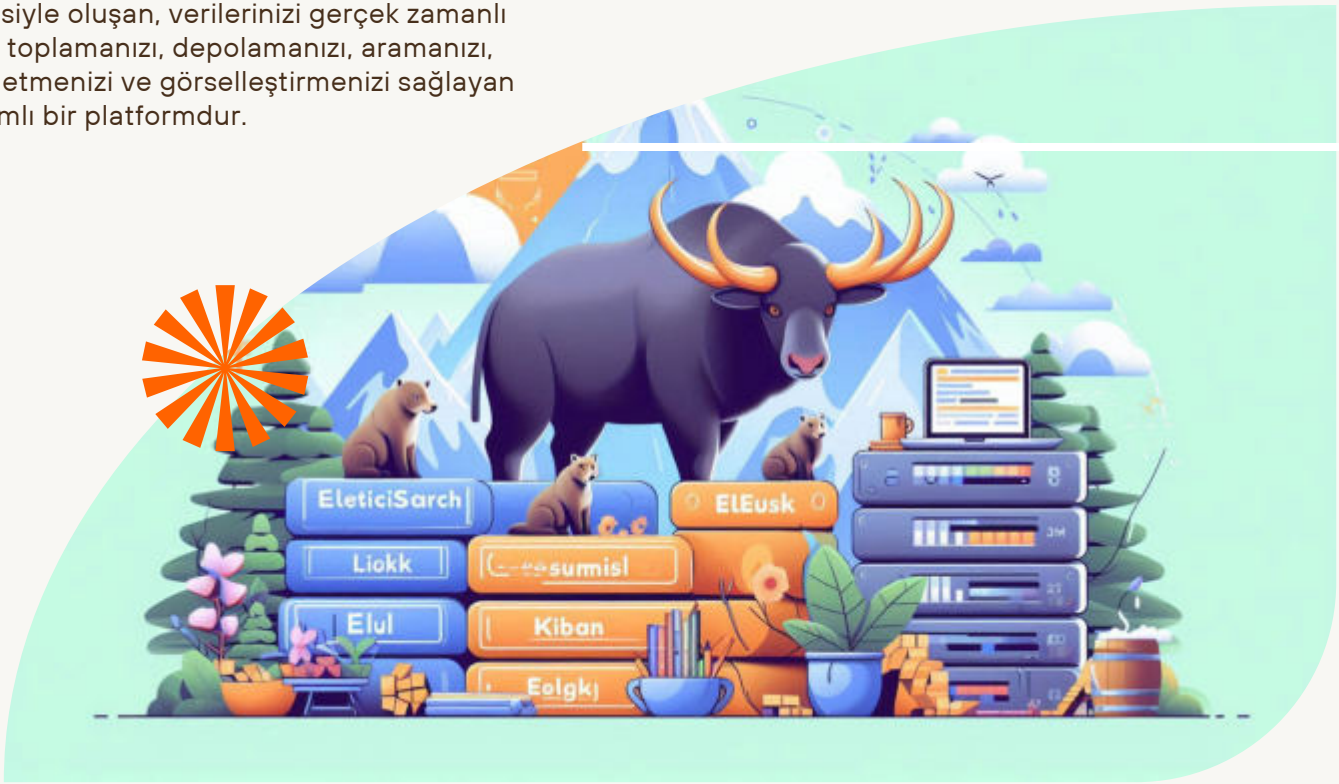
Günümüz iş dünyasında, her ölçekten şirket büyük miktarda veri üretmekte ve bu verilerden değerli içgörüler elde etmek, rekabet avantajı sağlamanın anahtarı haline gelmiştir. Loglar, metrikler, güvenlik olayları ve daha fazlası... Bu dağınık veri yığınını anlamlı bilgilere dönüştürmek, bazen zorlu bir görev olabilir. İşte tam da bu noktada, ELK Stack devreye giriyor.

ELK Stack (şimdiki adıyla Elastic Stack), Elasticsearch, Logstash ve Kibana olmak üzere üç güçlü açık kaynak bileşenin bir araya gelmesiyle oluşan, verilerinizi gerçek zamanlı olarak toplamanızı, depolamanızı, aramanızı, analiz etmenizi ve görselleştirmenizi sağlayan kapsamlı bir platformdur.

ELK STACK

KURUMSAL ÖZEL EĞİTİM

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



Vebende

ELK STACK EĞİTİMİ

1. Kapsamlı Veri Yönetimi ve Analiz Becerisi Kazandırmak
Eğitim, katılımcıların çeşitli kaynaklardan (uygulama logları, sistem metrikleri, güvenlik olayları vb.) gelen verileri toplama (Beats, Logstash), depolama ve indeksleme (Elasticsearch), arama ve sorgulama (Elasticsearch Query DSL) süreçlerini derinlemesine öğrenmelerini hedefler. Böylece, dağınık haldeki veriyi anlamlı ve analiz edilebilir bir yapıya dönüştürme yeteneği kazanılır.

2. Gerçek Zamanlı İzleme ve Sorun Giderme Yeteneğini Geliştirmek
Katılımcıların, sistem ve uygulama performansını gerçek zamanlı olarak izleyebilme, potansiyel hataları ve darboğazları hızlıca tespit edebilme becerisini geliştirmesi hedeflenir. Bu sayede, olası kesintilerin önüne geçmek veya kesinti sürelerini minimize etmek için gerekli aksiyonları proaktif olarak alabilecek bilgi birikimine sahip olmaları sağlanır.

3. Etkili Veri Görselleştirme ve Raporlama Yetkinliği Sağlamak
Eğitimin önemli bir hedefi, katılımcıların Kibana'yı etkin bir şekilde kullanarak verilerinden anlamlı ve etkileşimli panolar (dashboard) oluşturabilmelerini sağlamaktır. Bu, teknik veya iş birimlerinin, karmaşık verileri kolayca anlayabileceği görsel çıktılar üreterek, daha bilinçli kararlar almalarına olanak tanır.

4. Güvenlik Olayı Yönetimi ve Tehdit Avcılığı Becerilerini Artırmak
Siber güvenlik alanında ELK Stack'in nasıl kullanılabileceğini öğretmek, eğitimin kilit hedeflerindendir. Katılımcıların güvenlik loglarını analiz ederek anormal davranışları, yetkisiz erişim denemelerini ve olası siber tehditleri tespit etme, hatta proaktif olarak tehdit avcılığı yapabilme yeteneğini kazanmaları amaçlanır.

5. Kurumsal İhtiyaçlara Uygun Çözümler Geliştirebilme
Eğitim, sadece ELK Stack bileşenlerinin nasıl çalıştığını öğretmekle kalmaz, aynı zamanda katılımcıların kendi kurumlarının özel ihtiyaçlarına yönelik esnek ve ölçeklenebilir çözümler tasarlayabilme ve uygulayabilme yeteneğini kazanmalarını da hedefler. Bu, mevcut altyapılarla entegrasyon ve gelecekteki büyüme gereksinimlerini karşılama becerisini içerir.

EĞİTİM İÇERİĞİ

Modül 1: ELK Stack'e Giriş ve Temel Mimari

ELK Stack Mimarisine Giriş
- Elasticsearch, Logstash ve Kibana nın temel bileşenleri ve bu bileşenlerin log ve metrik yönetimindeki rolü.
- ELK Stack in log ve metrik yönetiminde sağladığı avantajlar ve neden kurumsal çözümlerde tercih edildiği.

Basit Veri Akışı Anlatımı
- Dosyadan (File) Logstash'e, oradan Elasticsearch'e ve son olarak Kibana'da görselleştirme sürecinin temel mantığı ve adımları.

ELK Stack'in Kurumsal Ortamdaki Yeri
- Sistem izleme, performans analizi, güvenlik loglarının toplanması ve merkezi yönetim ihtiyaçları bağlamında ELK Stack'in önemi.

Modül 2: Elasticsearch Temelleri ve Veri Modeli

Elasticsearch'e Giriş
- Elasticsearch'in dağıtık yapısı ve temel amacı (hızlı arama ve analiz motoru).

Temel Kavramlar
- Index, Document, Type (Elasticsearch 7+ ile Type kavramının değişimi), Shard ve Replica kavramlarına giriş.

JSON Tabanlı Veri Modellemesi
- Elasticsearch'te verinin nasıl saklandığı ve JSON formatının önemi.

Temel CRUD (Create, Read, Update, Delete) İşlemleri
- Elasticsearch REST API veya Kibana Console üzerinden temel veri ekleme, okuma, güncelleme ve silme pratikleri.

Modül 3: Logstash ile Veri Toplama ve Temel İşleme

Logstash Mimarisi
- Input, Filter ve Output eklentilerinin yapısı ve veri pipeline'ının nasıl çalıştığı.

Basit Bir Logstash Pipeline Konfigürasyonu
- file input eklentisi ile dosya okuma ve stdout output eklentisi ile konsola çıktı yazma örneği.

Codec Kullanımı
- Veri formatını belirlemek için plain ve json gibi temel codec'lerin kullanımı.

Logstash Kurulumu ve Temel Konfigürasyon
- Basit bir Logstash kurulumu ve yapılandırma dosyalarının (logstash.yml) temel ayarları.

Modül 4: Beats ile Hafif Veri Toplama Ajanları

Beats Ailesine Genel Bakış
- Farklı veri türlerini toplamak için kullanılan hafif ajanlar (Filebeat, Metricbeat, Packetbeat, Winlogbeat vb.).

Filebeat Kullanımı
- Filebeat kurulumu, bir log dosyasını izleme ve ELK Stack'e gönderme konfigürasyonu.

Metricbeat Kullanımı
- Metricbeat kurulumu, sistem metriklerini toplama ve ELK Stack'e gönderme konfigürasyonu (CPU, RAM, Disk vb.).

Kibana'da Beats Verilerini Görüntüleme
- Filebeat ve Metricbeat tarafından gönderilen verilerin Kibana Discover sekmesinde incelenmesi.

Modül 5: Kibana Temelleri: Keşif, Arama ve Görselleştirme

Kibana Arayüzüne Genel Bakış
- Farklı sekmelerin (Discover, Visualize, Dashboard, Management vb.) tanıtımı.

Index Pattern (İndex Kalıbı) Oluşturma
- Elasticsearch'teki verilere erişim için index pattern'lerinin nasıl tanımlandığı.

Discover Sekmesi ile Verilere Göz Atma ve Arama Yapma
- Log ve metrik verileri arasında gezinme, alanları filtreleme ve veri detaylarını inceleme.

Time Filter Kullanımı
- Belirli bir zaman aralığındaki verilere odaklanma.

Temel Arama (Querying)
- Kibana arama çubuğundaki temel arama sorguları ve Lucene Query Syntax (LQS) temelleri. Alan bazlı filtreleme örnekleri.

Modül 6: Logstash ile Gelişmiş Veri Dönüşümü (Filtreler)

Grok Filtresi
- Yapısal olmayan (unstructured) log satırlarını yapısal (structured) verilere dönüştürme. Yaygın Grok pattern'leri ve özel pattern oluşturma.

Mutate Filtresi
- Alanları yeniden adlandırma, silme, ekleme, birleştirme, dönüştürme (tip değiştirme - string to integer vb.).

Date Filtresi
- Log satırlarındaki farklı formatlardaki zaman damgalarını standart Elasticsearch @timestamp alanına dönüştürme ve zaman dilimi yönetimi.

JSON Filtresi
- JSON formatındaki log satırlarını otomatik olarak ayrıştırarak alanlar oluşturma.

Diğer Yararlı Filtreler (Temel Düzeyde)
- Drop, Remove, Rename, Convert filtrelerine kısa bakış.

Modül 7: Elasticsearch Mapping ve Query DSL ile Gelişmiş Arama

Elasticsearch Mapping
- Veri tiplerinin (text, keyword, number, date, boolean, ip vb.) ve analizörlerin (analyzer) veri arama ve analizini nasıl etkilediği.
- Explicit mapping tanımlama ve yönetimi.

Analyzer, Tokenizer, Filter Kavramları (Temel)
- Arama sırasında metin verisinin nasıl işlendiğinin temel mantığı.

Elasticsearch Query DSL (Alan Bazlı Sorgular)
- Kibana Discover sekmesindeki arama çubuğunda kullanılan daha güçlü sorgular.
- Query context ve Filter context arasındaki farklar ve kullanım alanları.
- match, term, bool, range, exists gibi yaygın Query DSL sorgularının pratik kullanımı.

Modül 8: Kibana Gelişmiş Görselleştirmeler ve Dashboardlar

Gelişmiş Görselleştirme Türleri
- Çubuk Grafik (Bar Chart), Çizgi Grafik (Line Chart), Alan Grafik (Area Chart), Pasta Grafik (Pie Chart), Veri Tablosu (Data Table), Metrik (Metric) görselleştirmeleri oluşturma.

Gelişmiş Aggregasyonlar
- Terms, Top N, Date Histogram, Range, Geo-Grid gibi aggregasyonların veri analizi ve görselleştirmedeki rolü.

TSVB (Time Series Visual Builder) Temelleri
- Zaman serisi verilerini görselleştirmek için TSVB'nin güçlü özelliklerine giriş.

Dashboard Oluşturma ve Yönetme
- Oluşturulan görselleştirmeleri bir araya getirerek interaktif dashboardlar oluşturma. Dashboard filtreleme ve drill-down özellikleri.

Modül 9: Sistem Metrikleri Toplama ve İzleme (Metricbeat Odaklı)

Metricbeat Modül ve Metricset Yapısı
- Farklı servislerden (system, docker, kubernetes, mysql, redis vb.) metrik toplama mekanizması.

Sistem Metrikleri Konfigürasyonları
- CPU, RAM, Disk, Network metriklerinin Metricbeat ile nasıl toplandığı ve gönderildiği.

Kibana'da Sistem Metrik Dashboardları
- Metricbeat ile gelen ön tanımlı dashboardların kullanımı ve özelleştirilmesi. Performans metriklerini analiz etme pratikleri.

EĞİTİM İÇERİĞİ

Modül 10: Temel Güvenlik: Rol ve Kullanıcı Yönetimi

Kibana Spaces Kullanımı
- Farklı ekipler veya kullanım senaryoları için ayrı alanlar (Space) oluşturma ve yönetme.

Temel Roller ve Kullanıcılar
- Kullanıcı hesapları oluşturma ve reader, editor gibi ön tanımlı temel rolleri anlama.

İndex/Space Bazlı Erişim Kontrolü
- Kullanıcıların hangi indexlere ve hangi Kibana alanlarına erişebileceğinin temel düzeyde yapılandırılması.

Modül 11: Elasticsearch Küme Yönetimine Giriş ve Temel Ölçeklendirme Kavramları

Node Tipleri
- Master-eligible, Data, Ingest, Tribe, Coordinating gibi farklı node tiplerinin kümedeki rolleri ve görevleri.

Sharding ve Replica Stratejileri
- Verinin nasıl parçalandığı (sharding) ve yedeklendiği (replica) konularına giriş. Küme performansı ve yüksek erişilebilirlik açısından önemi.

Cluster Health Durumları (red, yellow, green)
- Küme sağlık durumlarını yorumlama ve olası sorunları anlama.

Shard Dağılımı ve Temel Rebalancing
- Shard'ların küme genelinde nasıl dağıldığını ve temel rebalancing prensipleri.

Modül 12: Index Lifecycle Management (ILM) Temelleri

ILM Amacı ve Faydaları
- Veri yaşam döngüsünü yönetmenin gerekliliği (disk alanı, performans).

ILM Policy Oluşturma ve Yönetme
- Verilerin farklı aşamalarda (Hot, Warm, Cold, Delete) nasıl yönetileceğini belirleyen politikaların tanımlanması.

Veri Yaşam Döngüsü Politikalarını Uygulama
- Indexlerin ILM politikalarına bağlanması ve yaşam döngüsünün otomatik olarak yönetilmesi.

Modül 13: Watcher ile Temel Uyarı Sistemleri

Watcher Mimarisi ve Kullanım Senaryoları
- Log veya metrik verilerindeki belirli koşullar oluştuğunda uyarı gönderme mekanizması.

Watcher Yapısı: Trigger, Input, Condition, Transform, Actions
- Bir uyarı kuralının (Watcher) temel bileşenleri.

Log ve Metrik Tabanlı Temel Uyarı Kuralları Oluşturma
- Belirli bir hata logu sayısı aşıldığında veya bir metrik eşiği geçtiğinde uyarı tetikleme örnekleri.

Temel Action Tipleri
- E-posta ile uyarı gönderme konfigürasyonu.

Modül 14: Temel Performans Optimizasyonu ve Troubleshooting

Logstash Performans Ayarları
- Batch size, worker sayıları gibi ayarların veri işleme hızına etkisi.

Elasticsearch Performansına Giriş
- Index Sharding/Replica sayıları, temel Jvm Heap ayarı düşünceleri.

Kibana Performans Ayarları
- Önbellekleme (caching) ayarları ve görselleştirme performansı.

ELK Bileşen Loglarını Analiz Etme
- Elasticsearch, Logstash, Kibana log dosyalarını inceleyerek sorun tespiti.

Bağlantı Sorunlarını Giderme
- Bileşenler arasındaki bağlantı problemlerinin teşhisi ve çözümü.

Temel Veri Kaybı Nedenlerini Araştırma
- Logstash veya Beats tarafında veri kaybına yol açabilecek temel senaryoların incelenmesi.

Modül 15: Yüksek Erişilebilirlik (HA) ve Güvenlik Kavramları

Replica Kullanımı ile HA Sağlama
- Elasticsearch'te replica shard'ların yüksek erişilebilirlik açısından önemi.

Snapshot/Restore Stratejileri (Genel Bakış)
- Veri yedekleme ve felaket kurtarma için snapshot/restore mekanizması.

TLS/SSL Konfigürasyonu (Kavramsal)
- Bileşenler arası (node-to-node, client-to-node) ve tarayıcı-Kibana arasındaki iletişimin güvenli hale getirilmesi gerekliliği.

Modül 16: Elastic Stack Monitoring ve Heartbeat ile Durum Kontrolü

Elastic Stack Monitoring
- ELK Stack kümesinin kendi sağlığını ve performansını izleme aracı.

Heartbeat ile Servis/Uptime İzleme
- Belirli servislerin (web sitesi, API endpoint vb.) ulaşılabilirliğini kontrol etme ve uptime metrikleri toplama.

Kibana Uptime Arayüzü
- Heartbeat verilerini Kibana'da görselleştirerek servislerin durumunu takip etme.

EĞİTİM SÜRESİ

- 5 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. 5 günlük formatta 30 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.

ELK STACK

Günümüzün dijital çağında, işletmelerin karşı karşıya kaldığı en büyük zorluklardan biri, devasa ve sürekli büyüyen veri yığınını anlamlandırmaktır. Bu noktada Elastic Stack (önceden bilinen adıyla ELK Stack), Elasticsearch, Kibana ve Logstash'tan oluşan güçlü bir ekosistem olarak öne çıkıyor. Bu entegre platform, loglardan metrik verilere, güvenlik olaylarından iş analitiklerine kadar her tür veriyi gerçek zamanlı olarak toplamayı, işlemeyi, depolamayı ve inanılmaz bir hızla analiz etmeyi mümkün kılıyor. Elastic Stack sayesinde şirketler, operasyonel görünürlüklerini artırabiliyor, güvenlik tehditlerini proaktif bir şekilde tespit edebiliyor, uygulama performansını optimize edebiliyor ve en önemlisi, veriye dayalı bilinçli kararlar alarak rekabet avantajı sağlayabiliyor. Bu, yalnızca verileri görmek değil, onlardan aksiyona dönüştürülebilir içgörüler elde etmek demektir.

KATILIMCILARDAN BEKLENTİLERİMİZ

Temel Bilgi:

- Bilgisayar Temelleri: Linux komutlarına ve ağ kavramlarına (IP, port) aşina olmak.
- Veri Anlayışı: JSON gibi yapılandırılmış verilere aşinalık (tercihen).
- İngilizce: Teknik dokümanları anlayabilecek düzeyde İngilizce bilgisi.

Aktif Katılım:

- Derslere aktif olarak katılmak ve sorular sormak.
- Konulara merakla yaklaşmak ve keşfetmeye açık olmak.
- Eğitime dair yapıcı geri bildirimlerde bulunmak.

Pratik Odaklılık:

- Öğrenilenleri kendi ortamınızda uygulamaya hevesli olmak.
- Verilen alıştırmaları ve ödevleri düzenli yapmak.
- Uygulamalar için gerekli bilgisayar ortamının hazır olması (örn. sanal makine).

EĞİTİM YÖNTEMİ

Teorik Bilgilendirme ve Kavramsal Açıklamalar: ELK Stack'in (Elasticsearch, Logstash, Kibana) temel prensipleri, mimarisi, avantajları ve sektördeki yeri, anlaşılır bir dille ve görsel desteklerle sunulacaktır. Karmaşık kavramlar (indeksleme, sharding, pipeline'lar), gerçek dünya senaryolarıyla ilişkilendirilerek basitleştirilecektir.
Canlı Demolar ve Kodlama (Live Demos & Coding): Eğitimin büyük bir bölümü, eğitmen tarafından adım adım gerçekleştirilen canlı demo ve yapılandırma seanslarından oluşacaktır. Bu seanslarda, ELK Stack'in kurulumu, veri toplama (Beats ve Logstash ile), Elasticsearch'e indeksleme ve Kibana'da görselleştirme gibi farklı özelliklerinin gerçek zamanlı olarak nasıl kullanıldığı gösterilecek, katılımcılar süreçleri anlık olarak takip edebilecektir.
Uygulamalı Laboratuvar Çalışmaları (Hands-on Labs): Her konu başlığının ardından, katılımcıların öğrendiklerini pekiştirmeleri için tasarlanmış pratik laboratuvar egzersizleri yapılacaktır. Bu egzersizler, katılımcıların kendi ortamlarında ELK Stack bileşenlerini aktif olarak deneyimlemelerini, veri akışları oluşturmalarını ve panolar tasarlamalarını sağlayacaktır. Eğitmen, bu süreçte bireysel destek ve geri bildirim sağlayacaktır.
Senaryo Tabanlı Problem Çözme: Gerçek iş dünyasından alınmış veya simüle edilmiş senaryolar (örn. bir uygulamanın hata loglarını izleme, güvenlik olaylarını analiz etme) üzerinden problem çözme yaklaşımları ele alınacaktır. Bu sayede, katılımcılar ELK Stack bilgilerini pratik zorluklara nasıl uygulayacaklarını öğreneceklerdir.
Soru-Cevap ve Tartışma Oturumları: Katılımcıların akıllarındaki soruları sormak, karşılaştıkları zorlukları paylaşmak ve farklı çözüm yollarını tartışmak için düzenli soru-cevap ve interaktif tartışma oturumları yapılacaktır. Bu oturumlar, bilginin derinleşmesine ve farklı bakış açılarının kazanılmasına olanak tanıyacaktır.
Best Practices (En İyi Uygulamalar) ve Performans Optimizasyonları: Kurumsal projelerde ELK Stack kullanırken dikkat edilmesi gereken en iyi uygulama prensipleri (indeksleme stratejileri, küme yönetimi) ve performans optimizasyon teknikleri detaylıca incelenecektir. Güvenlik ve yüksek erişilebilirlik konularına da değinilecektir.

"

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.tr

www.vebende.com.tr

İzmir - Türkiye

Kurumsal
Eğitimler

www.vebende.com.tr

İletişime Geçin

Whatsapp: 0542 5505704
Tel: 0532 512 7811

iletisim@vebende.com.tr

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.