Securing Kubernetes Clusters with Red Hat Advanced Cluster Security (DO430) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Securing Kubernetes Clusters with Red Hat Advanced Cluster Security , OpenShift üzerinde çalışan Kubernetes kümelerinin güvenliğini sağlamak ve Red Hat Advanced Cluster Security for Kubernetes (RHACS) platformunu etkin şekilde kullanmak isteyen BT ve güvenlik profesyonelleri için hazırlanmış ileri seviye bir eğitimdir.

Program boyunca katılımcılar, RHACS mimarisini kurmayı, yapılandırmayı ve yönetmeyi öğrenirken; konteyner tabanlı uygulamaların yaşam döngüsü boyunca güvenlik kontrollerini uygulamayı da deneyimleyeceklerdir. Eğitim; zafiyet yönetimi, güvenlik politikalarının uygulanması, ağ segmentasyonu, uyumluluk denetimleri ve üçüncü taraf sistemlerle entegrasyon gibi modern Kubernetes güvenliği konularına odaklanmaktadır.

Katılımcılar ayrıca RHACS'u DevSecOps süreçlerine entegre ederek yazılım tedarik zincirinin korunması, CI/CD süreçlerinde güvenlik kontrollerinin otomatikleştirilmesi ve sektör standartlarına uygun güvenlik politikalarının uygulanması konusunda pratik deneyim kazanacaktır.

Eğitim sonunda katılımcılar, Kubernetes kümelerini daha güvenli yönetebilecek, güvenlik açıklarını önceliklendirebilecek ve kurumsal güvenlik gereksinimlerine uygun koruma mekanizmalarını uygulayabilecek bilgi ve beceriye sahip olacaktır.

Kurumsal Kazanımlar

Bu eğitim sonunda kurumlar aşağıdaki avantajları elde edecektir:

- Kubernetes ortamlarında güvenlik risklerinin azaltılması
- Güvenlik kaynaklı dağıtım gecikmelerinin en aza indirilmesi
- DevSecOps süreçlerinin güçlendirilmesi
- Yazılım tedarik zincirinin daha güvenli hâle getirilmesi
- Güvenlik kontrollerinin CI/CD süreçlerine entegre edilmesi
- Geliştirici ekiplerinin güvenlik süreçlerinde daha verimli çalışması

Bireysel Kazanımlar

Eğitimi tamamlayan katılımcılar aşağıdaki yetkinlikleri kazanacaktır:

- RHACS Central kurulumu ve güvenli Kubernetes kümelerinin eklenmesi
- Kurulum problemlerinin giderilmesi
- Güvenlik açığı raporlarının yorumlanması
- Dağıtım risklerinin analiz edilmesi
- Build, Deployment ve Runtime politikalarının oluşturulması
- CI/CD güvenlik kontrollerinin uygulanması
- Ağ segmentasyonu ve ağ politikalarının yönetimi
- Uyumluluk raporlarının hazırlanması
- SIEM, kimlik yönetimi ve yedekleme çözümleriyle entegrasyon gerçekleştirilmesi

Sonraki Eğitim / Sertifikasyon

Bu eğitimin ardından aşağıdaki eğitim ve sertifikalar önerilmektedir:

Securing Kubernetes Clusters with Red Hat Advanced Cluster Security (DO430) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- **Red Hat Certified Specialist in OpenShift Advanced Cluster Security (EX430)**
- **Red Hat Advanced Cluster Management for Kubernetes (DO432)**

Prerequisites

Bu eğitime katılacak kişilerin aşağıdaki bilgi ve deneyime sahip olmaları önerilir:

- Kubernetes ve OpenShift yönetimi konusunda temel bilgi
- Red Hat tarafından sunulan **Red Hat OpenShift Administration II: Configuring a Production Cluster (DO280)** eğitimini tamamlamış olmak veya eşdeğer bilgi seviyesine sahip olmak
- Red Hat'in ücretsiz beceri değerlendirme sınavının tamamlanması tavsiye edilmektedir.

Who Should Attend

Bu eğitim aşağıdaki profesyoneller için tasarlanmıştır:

- Kubernetes ortamlarında güvenlik tehditlerini analiz eden ve yöneten siber güvenlik uzmanları
- Kubernetes kümelerini yöneten altyapı yöneticileri
- DevOps ve DevSecOps süreçlerini yöneten platform mühendisleri
- CI/CD güvenliğini geliştirmek isteyen yazılım platform ekipleri
- Konteyner tabanlı uygulamaların güvenliğinden sorumlu sistem yöneticileri
- Kurumsal Kubernetes altyapılarında güvenlik ve uyumluluk süreçlerini yöneten teknik ekipler

What You Will Learn

Bu eğitimin sonunda katılımcılar aşağıdaki bilgi ve becerileri kazanacaktır:

- Red Hat Advanced Cluster Security platformunu kurabilmek ve güvenli Kubernetes kümelerini sisteme dahil edebilmek.
- RHACS kurulumunda karşılaşılan yaygın sorunları analiz ederek çözebilmek.
- Güvenlik açığı taramalarını yorumlayabilmek ve risk önceliklendirmesi yapabilmek.
- Dağıtım, çalışma zamanı ve CI/CD süreçleri için güvenlik politikaları oluşturabilmek ve uygulayabilmek.
- DevSecOps süreçlerinde yazılım tedarik zincirini koruyacak güvenlik kontrollerini uygulayabilmek.
- Ağ segmentasyonu politikaları oluşturabilmek ve bunları otomatik dağıtım süreçlerine entegre edebilmek.
- Uyumluluk denetimlerini gerçekleştirerek güvenlik standartlarına ilişkin raporlar üretebilmek.
- RHACS'u SIEM çözümleri, kimlik yönetimi sistemleri, yedekleme platformları ve diğer üçüncü taraf servislerle entegre edebilmek.

Securing Kubernetes Clusters with Red Hat Advanced Cluster Security (DO430) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Modül 1 - Red Hat Advanced Cluster Security Kurulumu

- RHACS mimarisinin incelenmesi
- Merkezi yönetim bileşenlerinin kurulumu
- Güvenli Kubernetes kümelerinin sisteme eklenmesi
- Kurulum için önerilen en iyi uygulamalar
- Yaygın kurulum ve yapılandırma sorunlarının giderilmesi

Modül 2 - Güvenlik Açığı Yönetimi

- Güvenlik açığı tarama sonuçlarının analiz edilmesi
- Risk seviyelerinin değerlendirilmesi
- Zafiyet raporlarının oluşturulması
- Öncelikli güvenlik aksiyonlarının belirlenmesi
- Güvenlik risklerinin azaltılmasına yönelik yöntemler

Modül 3 - Güvenlik Politikalarının Yönetimi

- RHACS güvenlik politikalarının oluşturulması
- Build, Deployment ve Runtime aşamalarında politika uygulamaları
- CI/CD süreçlerinde otomatik politika kontrolleri
- Yazılım tedarik zincirinin korunmasına yönelik güvenlik yaklaşımları

Modül 4 - Ağ Segmentasyonu

- Kubernetes ağ güvenliğinin güçlendirilmesi
- Network Graph kullanılarak iletişim analizlerinin yapılması
- Ağ güvenlik açıklarının belirlenmesi
- Ağ politikalarının oluşturulması ve uygulanması
- roxctl ve CI/CD süreçleriyle otomatik ağ politikası yönetimi

Modül 5 - Güvenlik Standartlarına Uyum Yönetimi

- Yerleşik uyumluluk taramalarının çalıştırılması
- Compliance Operator kurulumu ve kullanımı
- Güvenlik standartlarına uygunluk değerlendirmeleri
- Uyumluluk raporlarının hazırlanması
- Denetim süreçleri için kanıt (evidence) oluşturulması

Modül 6 - Harici Sistem Entegrasyonları

- RHACS'un kurumsal güvenlik çözümleriyle entegrasyonu
- SIEM platformlarına merkezi alarm gönderimi
- Yedekleme ve geri yükleme süreçlerinin yönetimi
- Kimlik ve yetkilendirme sistemleriyle entegrasyon
- Mevcut güvenlik altyapısıyla birlikte çalışabilirlik