Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

Red Hat Güvenliği: Fiziksel, Sanal ve Bulutta Linux (RH415)

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Gün**

https://bilginc.com/tr/egitim/red-hat-guvenligi-fiziksel-sanal-ve-bulutta-linux-rh415-826-egitimi/

Overview

Bilgi işlem sistemlerinin güvenliğini sağlamak, teknolojiler ve araçlarla desteklenen süreçlerin ve standartların uygulanması yoluyla riski yönetme sürecidir. Bu eğitimde, güvenlik gereksinimlerinizi uygulamanıza ve bunlara uymanıza yardımcı olmak için kullanılabilecek kaynaklar hakkında bilgi edineceksiniz.

Eğitim içeriği özeti

- OpenSCAP ile uyumluluğu yönetin
- Bir sunucuda SELinux'u devre dışı durumdan etkinleştirin, sistem politikasının temel analizini gerçekleştirin ve gelişmiş SELinux teknikleriyle riski azaltın
- Red Hat Insights ile sorunları proaktif olarak belirleme ve çözme
- Linux Audit ve AIDE ile bir sunucudaki etkinlikleri ve değişiklikleri izleyin
- USBGuard ve depolama şifrelemesi ile verileri tehlikeye karşı koruyun
- PAM ile kimlik doğrulama denetimlerini yönetme
- Güvenlik ve uyumluluk sorunlarının azaltılmasını otomatikleştirmek için sağlanan Ansible Playbook'ları manuel olarak uygulayın
- Red Hat Satellite ve Red Hat Ansible Tower ile OpenSCAP ve Red Hat Insights yönetimini ölçeklendirin

Prerequisites

Red Hat Certified Engineer (RHCE®) sertifikası ya da eşdeğer bilgi ve deneyime sahip olmak.

Who Should Attend

Sistem yöneticileri, BT güvenlik yöneticileri, BT güvenlik mühendisleri ve Red Hat Enterprise Linux sistemlerinin güvenliğini tasarlamak, uygulamak, sürdürmek ve yönetmek ve kuruluşun güvenlik politikalarına uygunluğunu sağlamaktan sorumlu diğer profesyoneller.

What You Will Learn

Bu eğitimi tamamladığınızda, güvenlik riskini yönetmek ve uyumluluk gereksinimlerini karşılamaya yardımcı olmak için Red Hat Enterprise Linux'ta bulunan güvenlik teknolojilerini başarıyla kullanabileceksiniz.

Neler Öğreneceksiniz:

- Red Hat Enterprise Linux ile sağlanan temel ilke içeriğini kullanarak ve özelleştirerek OpenSCAP ve SCAP Workbench kullanarak sistem uyumluluğunu analiz etme ve düzeltme.
- Çekirdeğin denetim altyapısı ile sistemlerinizdeki güvenlikle ilgili etkinlikleri izleme.
- Kullanıcıların, süreçlerin ve sanal makinelerin erişimini kısıtlamak için gelişmiş SELinux tekniklerini açıklamak ve uygulamak.
- AIDE ile dosyaların bütünlüğünü ve izinlerini doğrulayın.
- USBGuard ile yetkisiz USB cihazlarının kullanılmasını önleyin.
- Bekleyen verileri koruyun ancak NBDE kullanarak önyükleme sırasında güvenli otomatik şifre çözme sağlayın.
- Red Hat Insights ile sistemlerin risklerini ve yanlış yapılandırmalarını proaktif olarak belirleyin ve düzeltin.
- OpenSCAP, Red Hat Insights, Red Hat Satellite ve Red Hat Ansible Tower ile uyumluluğu geniş ölçekte analiz edin ve düzeltin.

Eğitimin kurum üzerindeki etkisi

Bu eğitim, güvenlik riskini azaltmak ve uyumluluk ve güvenlik sorunlarını etkin bir şekilde uygulamak, yönetmek ve düzeltmek için gereken becerileri geliştirmeyi amaçlamaktadır. Araçlar ve teknikler, sistemlerin güvenlik ve uyumluluk ihtiyaçlarını karşılayacak şekilde yapılandırılmasını ve konuşlandırılmasını, bu gereksinimleri karşılamaya devam etmesini ve mevcut tüm sistemlerin denetlenebilmesini ve bu gereksinimler revize edildikçe düzeltmelerin ve değişikliklerin tutarlı bir şekilde uygulanmasını sağlamak için kullanılabilir. Bu esneklik, işletmenin iş kesintisi, marka erozyonu, müşteri ve hissedar güveninin kaybı ve olay sonrası iyileştirme için finansal maliyetler açısından yüksek bir maliyeti olan güvenlik ihlalleri riskini verimli bir şekilde azaltmasına yardımcı olabilir. Ayrıca kuruluş, müşteriler, denetçiler veya diğer paydaşlar tarafından belirlenen uyumluluk gereksinimlerinin karşılandığını göstermeye yardımcı olmak için bu eğitimdeki araçları kullanabilir.

Red Hat bu eğitimi müşterilerimize fayda sağlayacak şekilde oluşturmuştur, ancak her şirket ve altyapı kendine özgüdür ve gerçek sonuçlar veya faydalar değişiklik gösterebilir.

Outline

Güvenlik ve riski yönetin

Red Hat Enterprise Linux sunucularında güvenliği yönetmek için stratejiler tanımlayın.

Ansible ile yapılandırma ve düzeltmeyi otomatikleştirme

Ansible Playbooks ile yapılandırma ve güvenlik sorunlarını düzeltin.

LUKS ve NBDE ile verileri koruyun

Depolama aygıtlarındaki verileri LUKS ile şifreleyin ve sunucular önyüklendiğinde otomatik şifre çözmeyi yönetmek için NBDE'yi kullanın.

USB cihaz erişimini kısıtlayın

USBGuard ile sistemi sahte USB cihaz erişimine karşı koruyun.

PAM ile kimlik doğrulamayı kontrol edin

Takılabilir kimlik doğrulama modüllerini (PAM'ler) yapılandırarak kimlik doğrulama, yetkilendirme, oturum ayarları ve parola denetimlerini yönetin.

Denetim ile sistem olaylarını kaydedin

Linux çekirdeğinin denetim alt sistemini ve destekleyici araçları kullanarak güvenlikle ilgili sistem olaylarını kaydedin ve inceleyin.

Dosya sistemi değişikliklerini izleyin

AIDE kullanarak bir sunucunun dosya sistemlerinde ve içeriklerinde yapılan değişiklikleri tespit edin ve analiz edin.

SELinux ile riski azaltın

SELinux ve gelişmiş SELinux tekniklerini ve analizlerini kullanarak süreçler arasındaki güvenliği ve sınırlamayı iyileştirin.

OpenSCAP ile uyumluluğu yönetin

OpenSCAP kullanarak bir sunucunun güvenlik ilkeleriyle uyumluluğunu değerlendirin ve düzeltin.

Red Hat Satellite ile uyumluluğu otomatikleştirin

Red Hat Satellite kullanarak OpenSCAP denetimleri gerçekleştirme ve uyumluluk sorunlarını düzeltme becerinizi otomatikleştirin ve ölçeklendirin.

Red Hat Insights ile sorunları analiz edin ve düzeltin

Red Hat Insights'ı kullanarak Red Hat Enterprise Linux sistemlerindeki yaygın sorunları ve güvenlik açıklarını belirleyin, tespit edin ve düzeltin.

Kapsamlı bir inceleme gerçekleştirin

Uygulamalı gözden geçirme alıştırmalarını tamamlayarak bu eğitimde ele alınan içeriği gözden geçirin.