

LOG Yönetimi

Windows Security Audit Analizi Eğitimi

Log yönetimi projelerinde ve Suistimal analiz v.b. durumlarda binlerce log kaydı içerisinde kaybolup gitmeden hangi log kaydına, hangi kriterlere bakmamız gerektiğini ve ilgili konfigürasyonların nasıl yapılacağı, SOX, HIPAA, GLBA gibi uyumluluk gereksinimleri ve 5651 sayılı kanunun gereği yapmamız gerekenlerin neler olduğunun anlatılacağı bir eğitim olacaktır. Eğitim içerisinde Log parser v.b. log analiz programları ve log management çözümü üzerinden bu log kayıtlarının nasıl inceleneceği ile ilgili uygulamalar yapılacaktır.

Bilgisayar ve internet sadece kişisel uygulamalar için değil, elektronik, sağlık, ticaret ve benzeri bir çok sektör içinde kullanılan bir ortam . durum böyle olunca bu uygulamaların ve ilgili sistemlerin güvenliği her zaman olduğundan daha kritik bir durum almıştır. kimin ne yaptığının takibi, güvenlik ihlallerinin tespiti gerek kanuni yaptırımlar gerek müşteri açısından son derece önemli bir görev haline gelmiştir.

Sadece internet uygulamaları değil aynı zamanda şirket içindeki çalışanların da ne yaptığının takibi ve gerektiği zaman raporlanması da bir çok güvenlik standardı tarafından tavsiye edilmektedir.

Eğitim Tarihi ve Eğitim Süresi

Toplam 14 Saat olan bu eğitim 23-24 Ekim 2010 tarihinde gerçekleşecektir. Kontenjan maksimum 12 kişi ile sınırlıdır bu nedenle kayıt olmak için acele etmenizde fayda var !

Eğitim Saatleri ; 10:00 - 18:00

Eğitimle birlikte; Windows Security Audit Analizi Dökümanları, sunumları ve demo uygulamalar katılımcılarla paylaşılacaktır.

Eğitim İçeriği

Windows Güvenlik Denetleme Eğitimi

Konu Başlıkları

- Win 2008 Event Log Mimarisi
- Win 2003 Event Log Mimarisi
- Kimlik Doğrulama (Account Logon) ve Oturum Açma (Logon/Logoff)
- Kimlik Doğrulama Olaylarının İncelenmesi
- Oturum Açma Olaylarının İncelenmesi
- Process Tracking (Detaylı Takip) Olaylarının İncelenmesi
- Nesne Erişim Olaylarının İncelenmesi

- Hesap Yönetim Olaylarının İncelenmesi
- Dizin Hizmetleri Olaylarının İncelenmesi
- Yetki Kullanım Olaylarının İncelenmesi
- Politika Değişiklik Olaylarının İncelenmesi
- Sistem Olaylarının İncelenmesi
- Standartlara Uyum İçin Yapılması Gerekenler

Windows Güvenlik Denetimi

- Denetleme (Auditing)
- Denetleme Politikalarının Ayarlanması
- Audit Policy Ayarları
- Audit Kategorileri
- EventLog Anatomisi
- Event Yazma İşlemi
- Event Okuma İşlemi
- EventLog Kayıt Yapısı
- Event Viewer
- Event Source
- Log Dosya Büyüklüğü
- Log Seçenekleri
- LOGPARSER
- LogParser Örnekleri
- Önemli Not
- VB Script ile Olayların Gözlenmesi
- Logon ve Kimlik Doğrulama Olayları
- Logon Tipleri
- DOMAIN LOGON
- LOCAL LOGON
- Domain Kimlik Doğrulama
- Başarısız Logon Olayları
- Downgrade Attack
- NTLM Kimlik Doğrulama İşlemi
- NTLM Hata Kodları
- Lokal Kimlik Doğrulama
- LogParser ile Unlock olaylarının listelenmesi:
- Logon Tipleri
- Kullanıcı Aktivitesinin Gözetlenmesi
- Object Access
- Process Tracking
- Hesap Yönetimi ve Sistem Yöneticilerinin yaptığı kullanıcı işlemlerin izlenmesi
- Kullanıcı ve Grup Olayları
- Kullanıcı Yaratma
- Kullanıcı Silme
- Grup İşlemleri (Yaratma / Silme / Değişiklik)
- Bilgisayarı Etki Alanına Dahil Etme (Domain Join)

- Active Directory Service Erişim Denetimi
- Hangi Olayları Denetleyebiliriz?
- Group Policy Nesnelerinin Denetimi
- Nasıl Etkinleştirilir?
- Audit Ayarlarının Yapılması
- Örnek: Domain seviyesinde Organizational Unit yaratma ve silme işlemlerini denetlemek
- Yapılan Auditing ayarının test edilmesi
- Group Policy Nesneleri Üzerinde Yapılan İşlemlerin Denetimi
- Privilege Use (Kullanıcı Hakları) Denetimi
- Bu kategori ne kadar gerekli?
- Sistem Aktivitesinin Denetimi

Uyumluluk (Compliance)

HIPAA Uyumluluk Gereksinimleri

- Kullanıcı Oturum Raporları (User Logon Report)
- Başarısız Oturum Açma Raporları (Logon Failure Reports)
- Güvenlik Kayıtlarına Erişim Raporu (Audit Log Access Reports)
- Nesne Erişim Raporları (Object Access Reports)
- Sistem Olayları Raporu (System Events Report)
- Oturum Durum Raporu (Host Session Status Report)
- Başarılı Etki Alanı Oturum Açma Raporu (Domain Logon Reports)
- Başarısız Etki Alanı Oturum Açma Raporu (Domain Logon Failures)
- Güvenlik Kayıtlarının Arşivlenmesi (Security Log Archiving)
-
- SOX Uyumluluk Gereksinimleri
- Kullanıcı Oturum Raporları (User Logon Report)
- Başarısız Oturum Açma Raporları (Logon Failure Reports)
- Güvenlik Kayıtlarına Erişim Raporu (Audit Log Access Reports)
- Nesne Erişim Raporları (Object Access Reports)
- Sistem Olayları Raporu (System Events Report)
- Oturum Durum Raporu (Host Session Status Report)
- Güvenlik Kayıtlarının Arşivlenmesi (Security Log Archiving)
- Oturum Durum Raporu (Host Session Status Report)
- Hesap Yönetim Olaylarının Takibi
- Kullanıcı Grup Değişikliklerinin Takibi
- Denetim Politikalarında Yapılan Değişikliklerin Takibi
- Başarılı Etki Alanı Oturum Açma Raporu (Domain Logon Reports)
- Başarısız Etki Alanı Oturum Açma Raporu (Domain Logon Failures)
- Kullanıcı Hareketlerinin Takibi
- Uygulama Çalıştırma Olaylarının Takibi
- Dizin/Dosya Erişim Takibi

GLBA Uyumluluđu

- Kullanıcı Oturum Raporları (User Logon Report)
- Başarısız Oturum Açma Raporları (Logon Failure Reports)
- Güvenlik Kayıtlarına Eriřim Raporu (Audit Log Access Reports)
- Güvenlik Kayıtlarının Arřivlenmesi (Security Log Archiving)

Kayıt

Kayıt olmak için admin@logyonetimi.com mail adresine mail göndermeniz yeterli.

Ücretlendirme

Eđitim ücreti toplam 14 saat için 1000 TL + KDV dir.

Ödeme kesin kayıt sırasında yapılacaktır.

Ödemeyi Bilgileri

Profect Business Academy

Tel: 0-216 474 1 075 Sultan Yalçın Hn. İle irtibata geçebilirsiniz.

Vergi dairesi : Üsküdar

Vergi no: 00 50 528 487

Garanti Bankası-İstanbul-Bađlarbaşı Şubesi

Hesap No:6297336

IBAN NO : TR63 0006 2000 4220 0006 2973 36

Eđitmen

Murat ERAYDIN

www.karmasis.com

CISSP

CEH

Eđitim Yeri

Profect Business Academy Mahir İz Cad. CapitolAVM Karřısı.Detay Plaza. No: 19/2 B-Blok
Kat:2 34662 Altunizade/Üsküdar/İstanbul

