



# **Merkezi Kayıt Yönetimi ve Denetim Amaçlı Kullanımı**

**Ali Dinçkan, CISA**

**Uzman Araştırmacı  
Ağ Güvenliği / OKTEM**

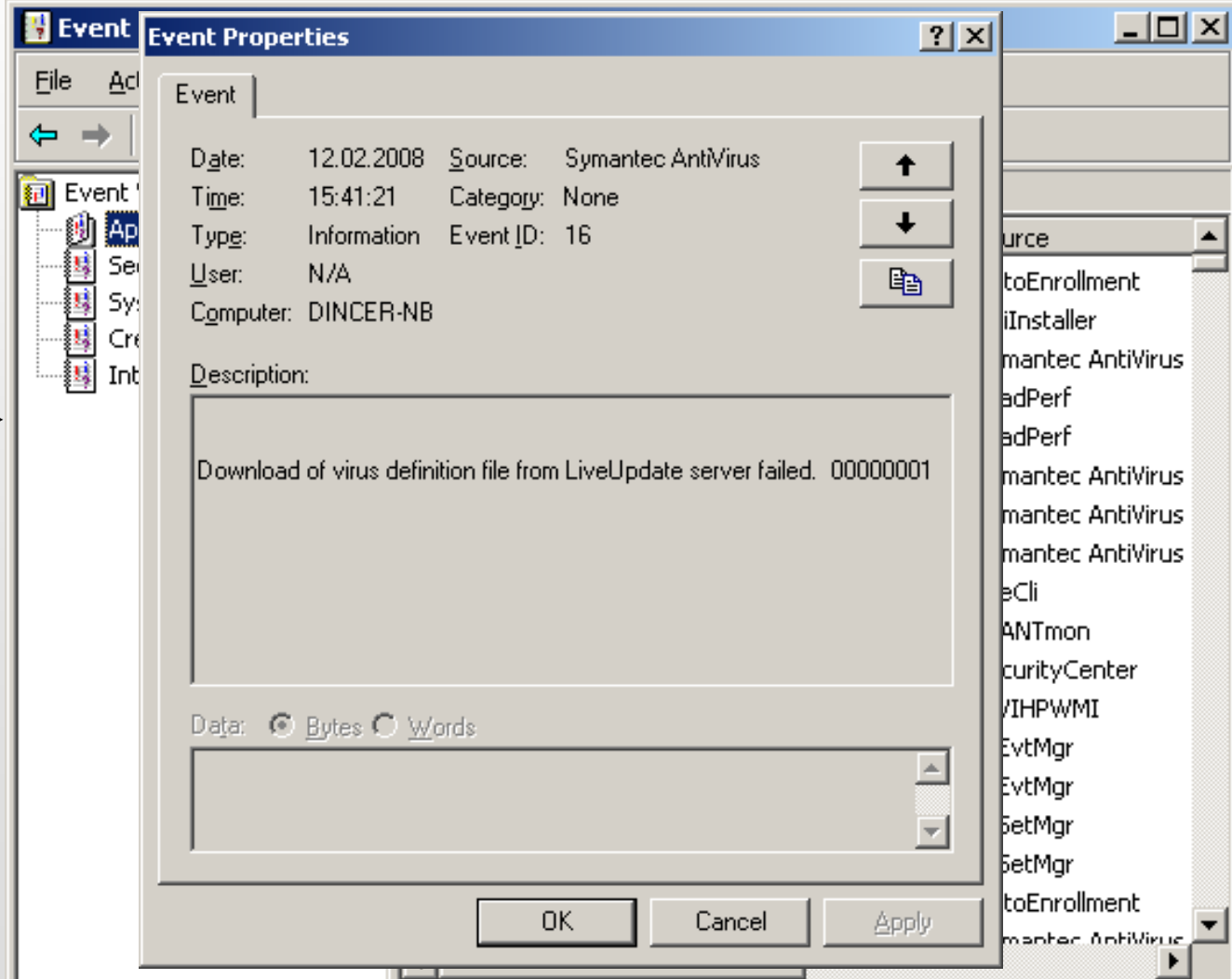
14 Mart 2008, İstanbul

- Kayıt Yönetimi
  - Kayıt nedir?
  - Kayıt yönetimi nedir?
  - Niçin ihtiyacımız var?
- Kayıt Yönetimi İle İlgili Zorunluluklar
  - PCI DSS
  - ISO/IEC 27001
  - CoBIT
  - HIPAA
- Merkezi Kayıt Yönetimi Kurulumu
- ISO/IEC 27001 Denetim Örnekleri

- Gerçekleşen bir olaya dair oluşturulan mesajdır.

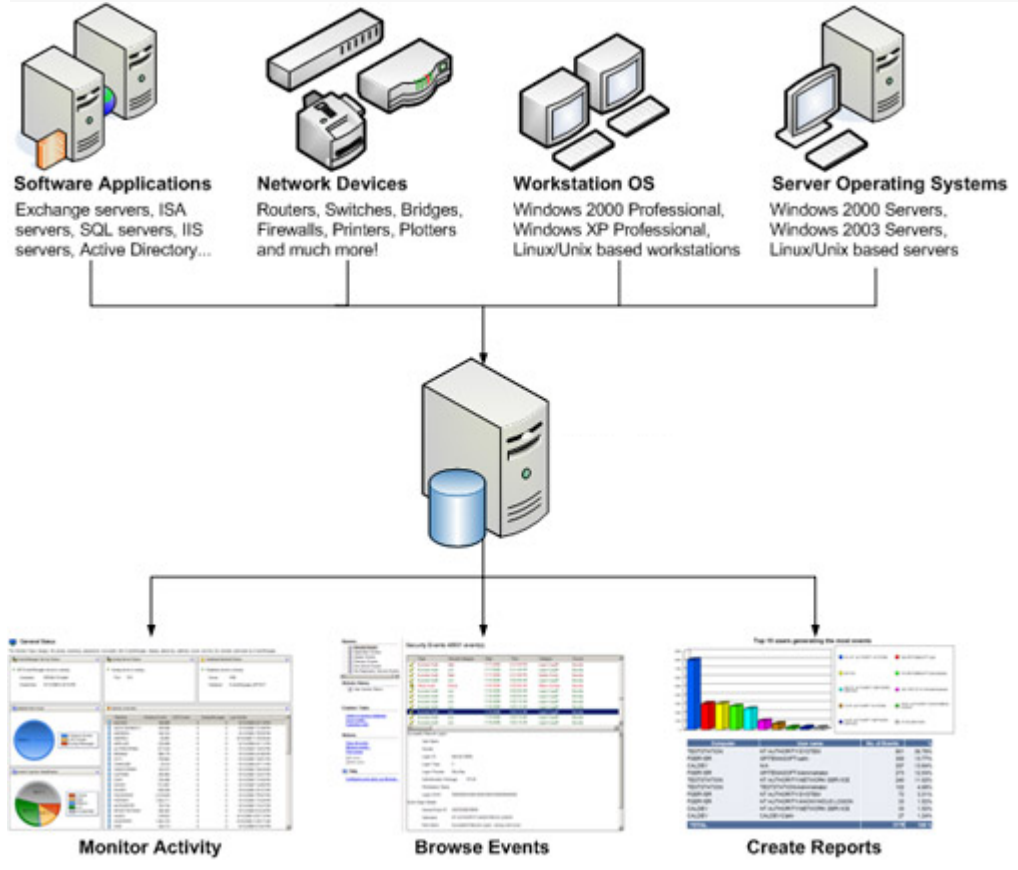


**Microsoft  
Windows XP**



# Kayıt Yönetimi Nedir?

- BT altyapısı içerisinde gerçekleşen olaylara ait kayıtların belirlenmiş kriterlere göre toplanması ve işlenmesidir.



- BT altyapısı içinde izlenmesi gereken çok sayıda bileşen var.
- Olay kayıtları dağınık biçimde.
  - İstemcilerde, sunucularda, uygulamalarda ...
- Çok fazla sayıda olay kaydı var.
  - Olay kayıtlarını izlemek zor.
- Olay kayıtlarının yedeklenmesi zor.
- İşletim sistemleri ile veya uygulamalar ile gelen olay inceleme araçları yetersiz.
- Olay kayıtlarının farklılığı ilişkilendirmeyi zorlaştırıyor.
  - Windows events, Syslog, W3C logs...

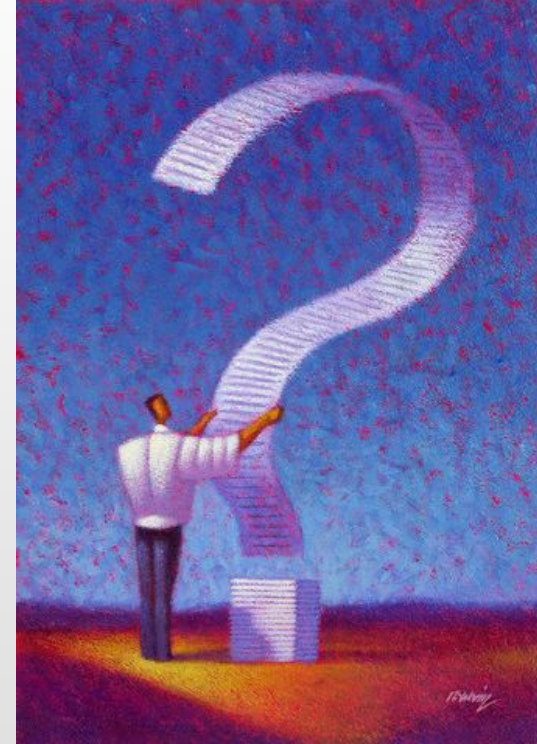
# BT Altyapısında Neler Oluyor?

- Bir çok işlem BT üzerinden gerçekleştiriliyor
  - Kritik servisler çalışıyor mu?
  - Şüpheli bir durum oluştu mu?
  - Yetkisiz erişim isteklerini kimler, nerelere yaptılar?
  - Mesai saati dışında sistemde bulunan kullanıcılar kimler?
  - Hangi dosyanın çıktısı kim tarafından, hangi bilgisayardan alındı?
  - ...



# Niçin Kayıt Yönetimine İhtiyacımız Var?

- Yanıtlanması gereken örnek sorular
  - 11 mart 2008 tarihinde 21:00-23:00 saatleri arasında kimler çalışıyordu?
  - Bu zaman aralığında USB depolama aygıtı kullanan oldu mu?
  - Bu zaman aralığında veritabanı sunucusuna kimler erişti?
  - Muhasebe bilgisayarından ekran görüntüsü alan var mı?
  - Dosya sunucuda bulunan promosyonlar.xls ve maaşlar.xls dosyasına kimler erişti?
  - Yıllık finansal analiz raporunu kim, ne zaman, hangi yazıcıdan çıktı aldı?



- Haber verme istekleri
  - E-posta, Web ve yedekleme sunucularında ilgili servisler durduğu anda
  - Etki alanı yöneticileri grubuna yeni bir kullanıcı eklendiğinde
  - Etki alanına üye olmayan bir bilgisayar ağa bağlandığında
  - Önemli sunuculara yazılım yüklendiğinde
  - ...
- Rapor istekleri
  - Önemli klasörlere yapılan erişimlerin günlük olarak sahibine raporlanması
  - Haftalık olarak yetkisiz erişim denemelerinin raporlanması
  - Haftalık olarak hesabı kilitlenen kullanıcı sayısı
  - ...

- Kayıt Yönetimi
  - Kayıt nedir?
  - Kayıt yönetimi nedir?
  - Niçin ihtiyacımız var?
- **Kayıt Yönetimi İle İlgili Zorunluluklar**
  - **PCI DSS**
  - **ISO/IEC 27001**
  - **CoBIT**
  - **HIPAA**
- Merkezi Kayıt Yönetimi Kurulumu
- ISO/IEC 27001 Denetim Örnekleri

- PCI DSS (Payment Card Industry Data Security Standard)
  - Regularly Monitor and Test Networks
    - Requirement 10: **Track and monitor all access to network resources and cardholder data**
  - PCI DSS bütün sistem bileşenleri için denetim kaydı tutulmasını ve en az günlük olarak gözden geçirilmesini ister
  - PCI DSS kayıtların en az 3 ay her an erişilebilir (online) olmak üzere bir sene saklanmasını ister



- ISO/IEC 27001
  - 10.10.1 - Denetim kaydetme
    - “Kullanıcı faaliyetleri, ayrıcalıkları ve bilgi güvenliği olaylarını kaydeden **denetim kayıtları üretilmeli** ve ileride yapılabilecek soruşturmalar ve erişim kontrolü izlemeye yardımcı olmak için **anlaşılmiş bir süre tutulmalıdır.**”
  - 10.10.4 - Yönetici ve operatör kayıtları
    - “Sistem yöneticisi ve operatör faaliyetleri kaydedilmelidir.
  - 10.10.3 - Kayıt bilgisinin korunması
    - “Kayıt olanakları ve kayıt bilgisi kurcalanma ve yetkisiz erişime karşı korunmalıdır.”



## • ISO/IEC 27001

- 10.10.5 - Hata kaydı
  - “**Hatalar kaydedilmeli**, çözümlenmeli ve uygun önlem alınmalıdır”
- 12.4.1 - Operasyonel yazılımın kontrolü
  - “Operasyonel sistemlerdeki yazılımların kurulmasını kontrol etmek için prosedürler bulunmalıdır.”
  - Operasyonel yazılım kütüphanesinde gerçekleşen **güncellemelere ait kayıtlar tutulmalıdır.**



- CoBIT
  - DS5.5 Security Testing, Surveillance and Monitoring
    - “... **A logging and monitoring function** will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.”



# Kayıt Yönetimi İle İlgili Zorunluluklar

- HIPAA (The Health Insurance Portability and Accountability Act) - Sağlık Sigortası Taşınabilirlik ve Sorumluluk Anlaşması
  - “Implement hardware, software, and/or procedural mechanisms that **record and examine activity in information systems** that contain or use electronic protected health information.”
    1. User account activity audits are conducted using automated audit controls.
    2. **access to & modifications of sensitive or critical files is logged.**
    3. Access to audit logs is restricted.
    4. Audit logs are reviewed periodically & retained for the same period as the original claim.
    5. ...



- Kayıt Yönetimi
  - Kayıt nedir?
  - Kayıt yönetimi nedir?
  - Niçin ihtiyacımız var?
- Kayıt Yönetimi İle İlgili Zorunluluklar
  - PCI DSS
  - ISO/IEC 27001
  - CoBIT
  - HIPAA
- **Merkezi Kayıt Yönetimi Kurulumu**
- ISO/IEC 27001 Denetim Örnekleri

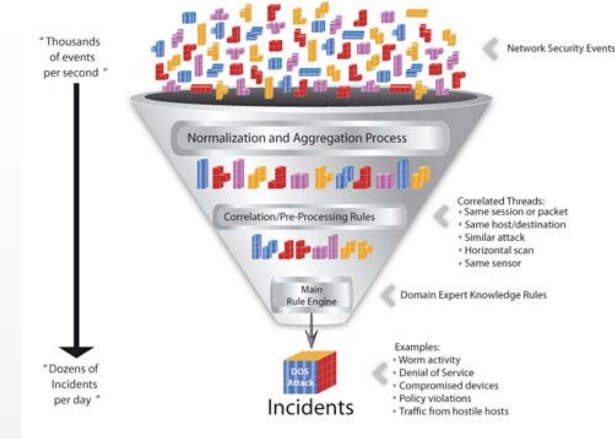
- Planlama
  - Kayıt yönetimi ihtiyaçları tespit edilir
- Seçme
  - Üretici ve ürün alternatifleri değerlendirilir
- Kurulum ve Uyarılama
  - Kayıt yönetim sisteminin ihtiyacı karşılar biçimde çalıştırılması



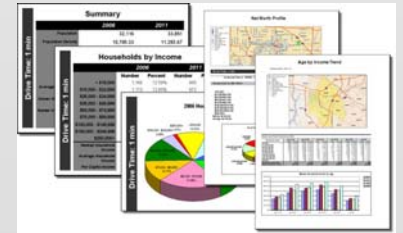
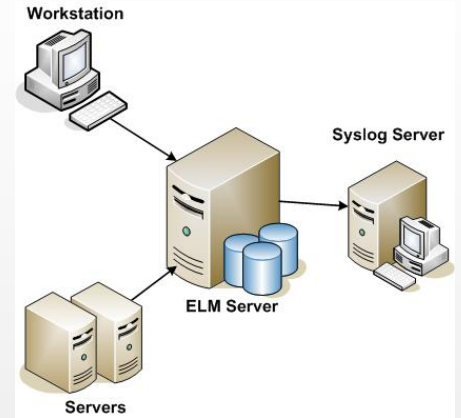
- Kayıt yönetim sistemini neden kuruyoruz?
  - Yasal düzenleme
  - İş ihtiyaçları
- Hangi kayıtları toplayacağız?
  - HIPAA uyumluluğu gerekiyorsa “logon attempts” kayıtları şart
- Toplanan kayıtların ne kadar süre saklayacağız?
- Kritik bileşenler neler?
  - Veri hangi sistemlerde
  - Tüm sunucular (etki alanı, web, dns..), tüm uygulamalar



- Olay ilişkilendirme ihtiyacı nedir?
  - Birden fazla olay kaydının bir araya gelmesi çok önemli bir olaya işaret edebilir
- Ne kadar depolama alanı gerekli?
  - Kayıtların depolanması için kullanılan depolama alanı izlenmelidir
  - Kayıtların saklama süresi dikkate alınarak ihtiyaç belirlenmelidir
- Performans ihtiyacı nedir?
  - Saniyede kaç olay işlenecek



- Planlama aşamasında istenilen özellikleri sağlayan bir ürüne ihtiyaç vardır
- İhtiyaç kategorileri
  - Kayıt toplama
    - Desteklenen sistemler
    - Ölçeklenebilirlik
    - Performans
  - Kayıt depolama
    - Eski kayıtlara ulaşabilme
    - Eski kayıtların arşivlenmesi
  - Raporlama
    - Raporlama esnekliği
    - Bildirim yöntemleri
  - Haber ve tepki verme
    - SMS, e-posta
    - Komut çalıştırma



- Kurulum
- Uyarlama
  - Kayıt toplama kuralları
  - Olay ilişkilendirme kuralları
  - Bildirim yapılacak olaylara ait yapılandırma
  - Tepki verilecek olaylara ait yapılandırma
- Test
  - İhtiyaçlar karşılandı mı?

- Kayıt Yönetimi
  - Kayıt nedir?
  - Kayıt yönetimi nedir?
  - Niçin ihtiyacımız var?
- Kayıt Yönetimi İle İlgili Zorunluluklar
  - PCI DSS
  - ISO/IEC 27001
  - CoBIT
  - HIPAA
- Merkezi Kayıt Yönetimi Kurulumu
- **ISO/IEC 27001 Denetim Örnekleri**

## • 8.3.3 Erişim Haklarının Kaldırılması

- İnsan kaynaklarından son altı ayda işten ayrılan personelin listesi alınır.
- Kayıt yönetim sisteminden son altı ay içinde silinen/etkinliği kaldırılan kullanıcı hesaplarına ait rapor istenir ve karşılaştırılır

## • 10.7.4 Sistem Dokümantasyonu Güvenliği

- Sistem dokümantasyonuna erişim hakkı olan kullanıcıların listesi istenir. Bu liste uygulamanın sahibi tarafından onaylanmış olmalıdır.
- Kayıt yönetim sisteminden sistem dokümantasyonuna erişen kullanıcı hesaplarının listesi alınır ve karşılaştırılır.

- **10.1.2 Değişiklik Yönetimi**
  - Program kurulumları, kullanıcı hesaplarındaki etkinleştirme, silme ve hak verme gibi değişiklikler kayıt yönetim sisteminden alınır.
  - Değişikliklerin değişiklik kontrol prosedürüne uygun yapılıp yapılmadığı kontrol edilir.
- **10.10.3 Kayıt Bilgisinin Korunması**
  - Kayıt yönetim sistemi ve sistemlerin kayıt bileşenlerine erişim hakkı olan personelin listesi alınır.
  - Sistemlerin kayıt bileşenlerine ve kayıt yönetim sistemine olan erişimlerin raporu temin edilir ve karşılaştırılır

## • 11.2.1 Kullanıcı Kaydı

- Kayıt yönetim sisteminden, son altı ay içerisinde oluşturulmuş ve silinmiş kullanıcı hesaplarının listesi alınır.
- İlgili hesaplar için kullanıcı oluşturma ve silme prosedürünün işletilip işletilmediği kontrol edilir.
- İlgili hesaplar için erişim kontrol prosedürünün işletilip işletilmediği kontrol edilir.

## • 11.2.2 Ayrıcalık Yönetimi

- Kayıt yönetim sisteminden, son altı ay içerisinde ayrıcalık verilmiş kullanıcı hesaplarının listesi alınır.
- Ayrıcalıkların verilmesi sırasında erişim kontrol prosedürünün işletilip işletilmediği kontrol edilir.

- **12.4.1 Operasyonel Yazılımın Kontrolü**
  - Operasyon program kütüphanesinin güncellendiğine dair kayıtlar kayıt yönetim sisteminden alınır.
  - Söz konusu değişikliklerin ilgili prosedüre uygun gerçekleştirip gerçekleştirilmediği kontrol edilir.
  
- **12.4.3 Program Kaynak Koduna Erişim Kontrolü**
  - Program kaynak kodlarına erişim hakkı olan personelin listesi alınır.
  - Program kaynak kodlarının bulunduğu dizinlere olan erişimlere ait rapor kayıt yönetim sisteminden alınır ve yetkisiz erişim olup olmadığı kontrol edilir.

Ali Dinçkan

dinckan@uekae.tubitak.gov.tr

