



# Bilgi Sistemlerinde Olay İlişkilendirme

**Burak Bayođlu**  
**Ađ Güvenliđi Grubu**  
**Başuzman Araştırmacı**  
**CISM, CISA, CISSP**

[bayoglu@uekae.tubitak.gov.tr](mailto:bayoglu@uekae.tubitak.gov.tr)

14 Mart 2008, İstanbul

- Olay ilişkilendirme nedir?
- Olay ilişkilendirmenin faydaları nelerdir?
- Mevcut olay ilişkilendirme sistemleri
- Örnek

- Olay ilişkilendirme nedir?
- Olay ilişkilendirmenin faydaları nelerdir?
- Mevcut olay ilişkilendirme sistemleri
- Örnek

# Motivasyon

- **Bilgisayar ađları, sistem bileşenleri ve uygulamalar çok sayıda tehditle karşı karşıyadır.**
- **Erişim kolaylığı ve dünya genelinde yayılmış olması sebebiyle internet sisteminde sınırlar mantıksal olarak kalkmıştır.**
- **Kritik bilgi sistemlerini hedef alan saldırılar titizlikle takip edilmeli ve incelenmelidir.**
- **Gerçekleşen saldırılarla ilgili yerinde ve zamanında önlemler alınmalıdır.**
- **Saldırıların etki derecesinin ölçülebilmesi ve gerçek zararın öğrenilebilmesi gereklidir.**

## BT Sistemlerinde Kayıt(Olay) Kaynaklarından Bazıları

Saldırı tespit sistemleri

Güvenlik duvarları

İşletim sistemleri

Veritabanı yönetim sistemleri

Antivirüs yazılımları

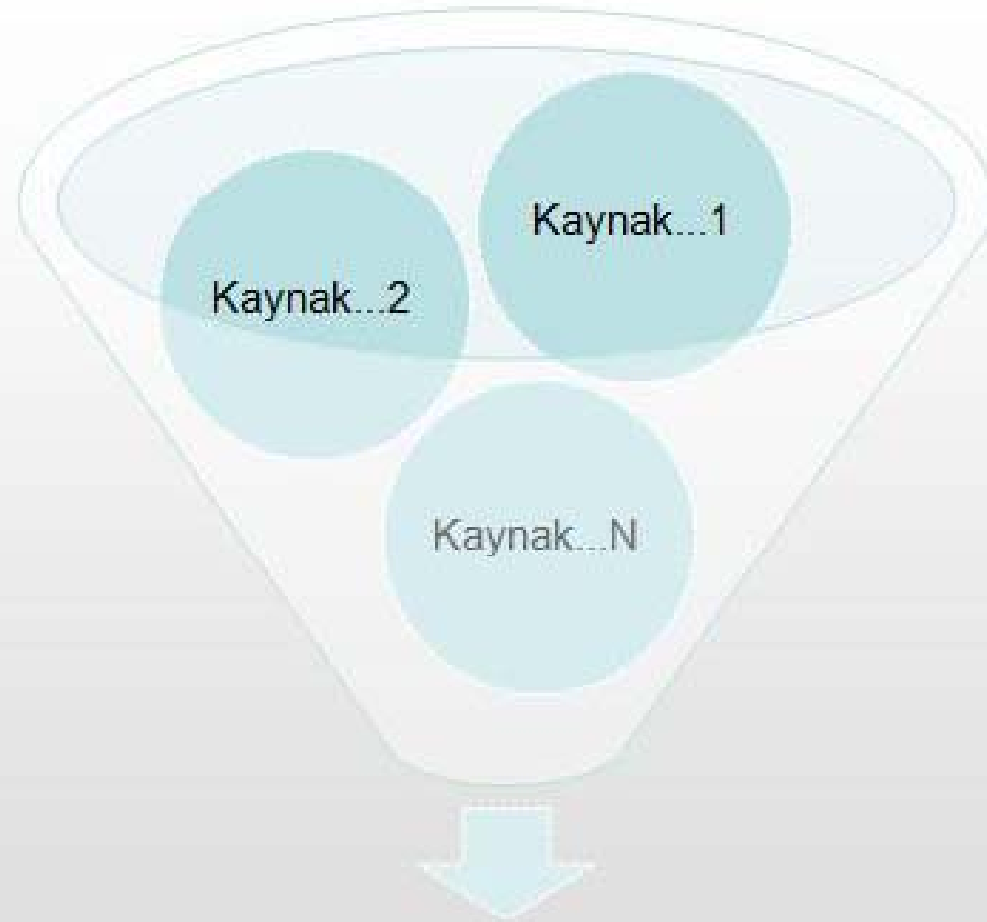
Aktif/Pasif ağ cihazları

Uygulamalar

## Olay İlişkilendirme

- BT bileşelerinde üretilen olay kayıtlarının merkezi bir sistemde toplanması ilk şart.
- Toplanan olay kayıtlarının saldırı senaryolarındaki ilerleme adımlarına denk düşen parçalarının farklı bileşen kayıtlarından takip edilmesi işine “Olay İlişkilendirme” diyoruz.
  - Saldırı senaryolarının oluşturulması gereklidir.
  - Saldırının son safhasına kadar yol üzerinde kayıt üretmesi beklenen sistem bileşenleri belirlenip olaylar mantıksal olarak ilişkilendirilmelidir.

# Olay ilişkilendirme



Doğruluk analizinden geçirilmiş,  
önceliklendirilmiş, etkisi bilinen, **daha**  
**az sayıda kayıt.**

- Olay ilişkilendirme nedir?
- Olay ilişkilendirmenin faydaları nelerdir?
- Mevcut olay ilişkilendirme sistemleri
- Örnek

## Kayıtların Takip Edilemezliđi

- Özellikle saldırı tespit sistemlerinin ürettiđi çok sayıda hatalı pozitif kayıt mevcuttur.
- Güvenlik duvarı, işletim sistemleri, uygulamalar vb. BT bileşenlerinin kayıtları, sürekli gözlem altında tutulamayacak kadar fazladır.
- Bu kayıtlar düzenli olarak gözden geçirilse bile öncelik sırası ve ilerleme seviyesine göre saldırılardan en kısa zamanda haberdar olunması manuel incelemeye mümkün değildir.

## Sistem Yetkilerinin Dağıtılmış Olması

- Özellikle çok sayıda bileşenin bulunduğu sistemlerde yetkiler dağıtılmıştır.
- Sistem güvenlik sorumlusu ayrı olsa bile genel olarak sadece güvenlik bileşenlerine yoğunlaşmaktadır.
- Bazı saldırıların analizi sadece uygulama seviyesinde kayıtların incelenmesiyle mümkündür.
- Uygulama kayıtlarını analiz edebilecek uzmanlar da rollerinin gereği olarak genelde diğer güvenlik bileşenlerinin kayıtlarına ulaşamamaktadır.

## Teknolojik Faydalar

- Olay ilişkilendirme sayesinde;
  - Gelişmiş saldırıların analizi kolaylaşmaktadır.
  - Saldırıların ilerleme seviyeleri (zarar derecesi) hakkında bilgi edinilebilmektedir.
  - Çok sayıda kayıt arasından gerçekten ilgilenilmesi gereken olaylar ayıklanabilmektedir.
  - Saldırılar önceliklendirilebilmektedir.
- Böylece;
  - Saldırılardan zamanında haberdar olunabilmektedir.
  - Karşı önlemler yerinde ve zamanında alınabilmektedir.

## Kurumsal Faydalar

- Olay ilişkilendirme sayesinde;
  - Olay analizi kolaylaşmakta ve olay analizi yapması gereken personel sayısı azalmaktadır.
  - Personel sayısı zaten az ise (Genel durumdur 😊 ) ilgili personelin daha etkin çalışması sağlanmaktadır.
  - Hatalı pozitif olay kayıtları için iş gücü harcanmamaktadır.
- Böylece;
  - İş gücü verimi artırılmaktadır.
  - Kurum öncelikleri ve teknolojik riskler karar ağacına dahil edilebilmektedir.
  - Saldırının erken safhalarında fark edilmesi yoluyla kurum daha büyük zararlardan kaçabilmektedir.

- Olay ilişkilendirme nedir?
- Olay ilişkilendirmenin faydaları nelerdir?
- **Mevcut olay ilişkilendirme sistemleri**
- Örnek

## Olay İlişkilendirme Sistemleri

- Açık kaynak kodlu ücretsiz yazılımlar:
  - OSSIM
    - <http://www.ossim.net/>
  - SEC (Simple Event Correlator)
    - <http://simple-evcorr.sourceforge.net/>
  - Prelude-IDS
    - <http://www.prelude-ids.org/>
- Ayrıca çok sayıda ticari yazılımlar mevcut.

- Olay ilişkilendirme nedir?
- Olay ilişkilendirmenin faydaları nelerdir?
- Mevcut olay ilişkilendirme sistemleri
- Örnek

# Saldırı Senaryosu

HEDEF



Windows 2000 Server  
IIS 5.0 Web Sunucu

- Amaç: Web sunucu üzerinde SYSTEM haklarını ele geçirmek ve açılış dosyasını değiştirmek.
- Kullanılacak Açıklık: “Microsoft IIS 5.0 Printer Host Header Overflow”
- Var mısın yok musun?
  - Örneği eğlence soslu mu alırsınız?
  - Yoksa Hamdi Bey’in eğlencesiz teklifini kabul ediyor musunuz?

# Tahmin etmişim 😊



# Olay İlişkilendirme Yapılmayan Ortam

Bizim jenerasyon için...



He-Man'e yetişemeyenler için...



THE GOOD THE UGLY AND THE BAD

**Sistem güvenliđi Prens Adam'dan sorulur. Man-At-Arms iřleri yrtr.**



## Kötülerin işi kötülük yapmaktır...

Falanca bizim tavuğa kışt dedi.  
Tiz web sayfası rezil edile



Ne biliyoruz  
patron?

Microsoft IIS 5.0 Printer Host  
Header Overflow sadık bir  
hizmetçimdir

## Prens Adam için sıradan bir gün, geveze Orko iş başında

Abi Nimda zorluyor  
kapiyı



Ya varsa?

Aslanım Nimda mı  
kaldı?

## Geveze Orko hala iş başında

Abi sıkıcı olduğumun farkındayım ama bir kayıt daha düştü

Güzel hatrın için baktım. Yok bir problem.



## Geveze Orko can sıkılmaya başladı !

He-man! IDS  
"BLEEDING-  
EDGE Web Proxy  
Get Request"  
düşüyor. MAA!  
Senin web  
sunucu 204 ve  
1006 logu düştü  
  
Demedi demeyin!

Döncez biz  
sana!



## Kötüler beklemez...

Bittiğimizin resmidir

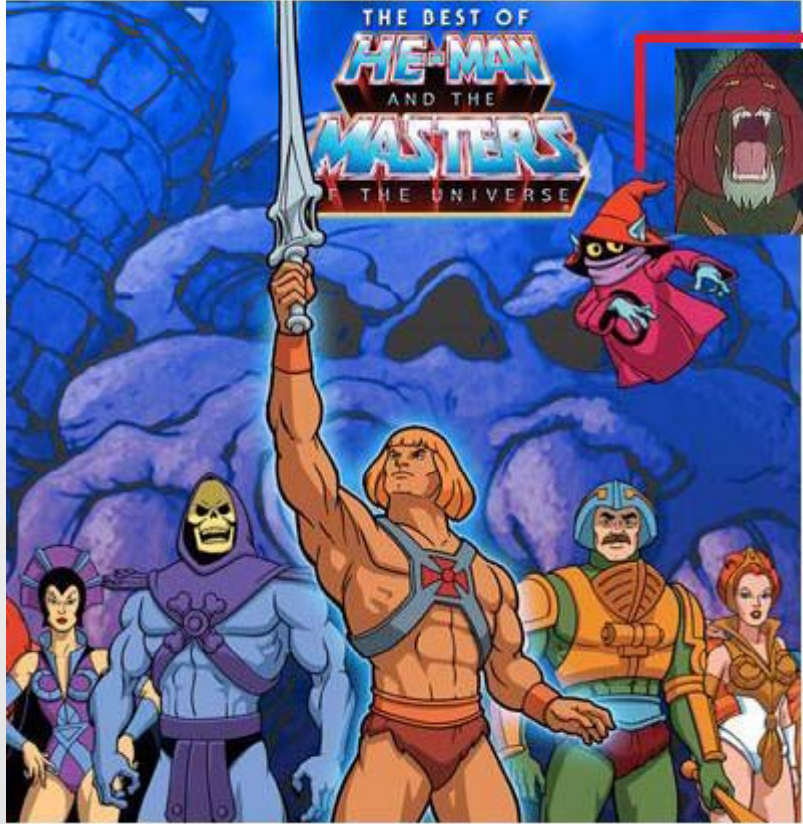


Bittiğinden daha fazla resim var orada !



# Olay İlişkilendirme Yapılan Ortam

Bizim jenerasyon için...



He-Man'e yetişemeyenler için...



~~THE UGLY~~  
THE GOOD AND THE BAD

## Orko akıllandı...



IDS Log düřtü  
Paket GD'dan geçti  
Web sunucu log düřtü



Uyan titrek!



Saldırgan paketlerini düřür.  
Kötü adamı yakala.

- Gördüğünüz gibi film daha kısa
  - Sistem akıllı olduđu için kendisi uyanıyor.
  - Karşı önlem otomatik olarak (hatalı pozitif korkusu olmadan) alınabiliyor.
  - Saldırının anlaşılması için insanlar değil sistem çalışıyor.
  - Yerinde ve zamanında karşı önlem alınabiliyor.

## Söylemeden geçemeyeceğim...



Sadece olayların ilişkilendirildiğine dikkat edin !

Dinlediđiniz iin teŖekkr ederim.

SORULARINIZ ... ?