



Bilgi Sistemlerinde Merkezi Kayıt Yönetimi ve Olay İlişkilendirme

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

bayoglu@uekae.tubitak.gov.tr

06 Haziran 2008, Ankara

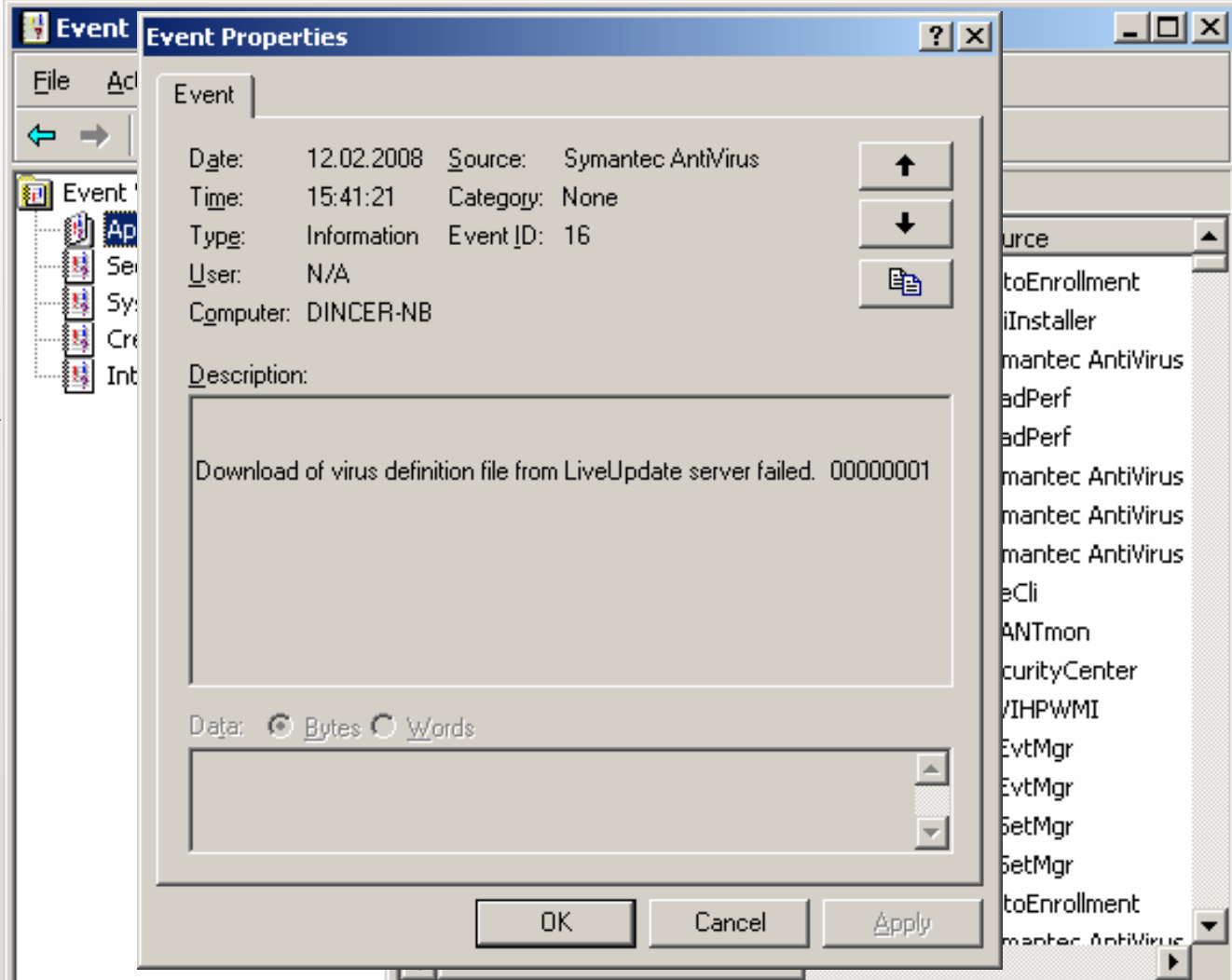
- Merkezi Kayıt Yönetimi
 - Kayıt nedir?
 - Kayıt yönetimi nedir?
 - Niçin ihtiyacımız var?
- Olay İlişkilendirme
 - Olay ilişkilendirme nedir?
 - Olay ilişkilendirmenin faydaları nelerdir?
 - Mevcut olay ilişkilendirme sistemleri
 - Örnek

- Kayıt nedir?
- Kayıt yönetimi nedir?
- Niçin ihtiyacımız var?

- Gerçekleşen bir olaya dair oluşturulan mesajdır.

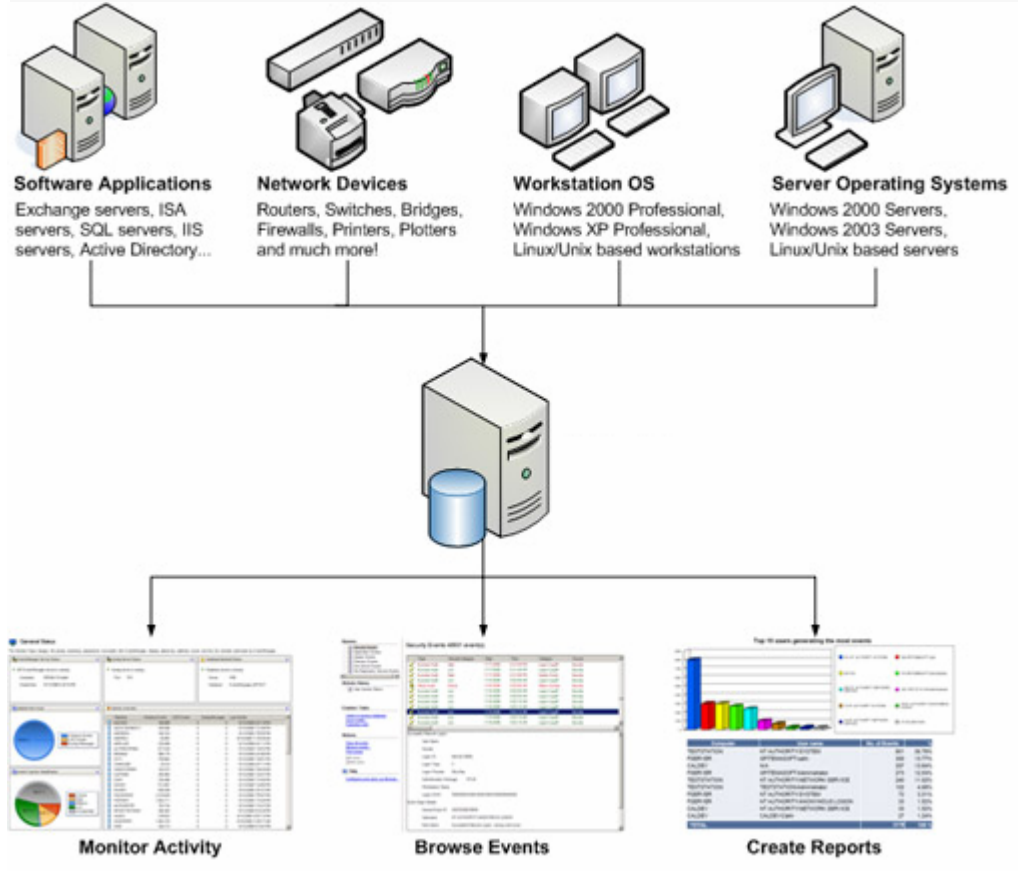


**Microsoft
Windows XP**



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...

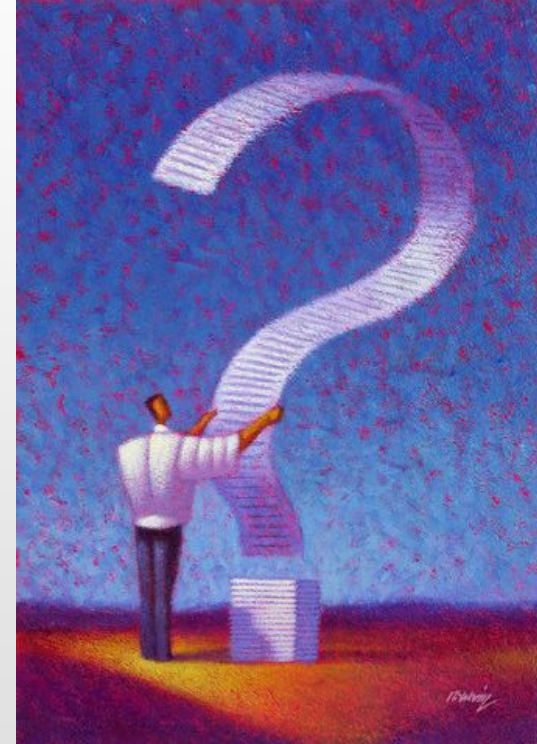
BT Altyapısında Neler Oluyor?

- 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
 - ...

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

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

- **İnternet sisteminde sınırlar mantıksal olarak kalkmıştır.**
- **Gerçekleşen saldırılarla ilgili yerinde ve zamanında önlemler alınmalıdır.**
- **Saldırıların etki derecesinin ölçülebilmesi gereklidir.**

Saldırı tespit sistemleri

Güvenlik duvarları

İşletim sistemleri

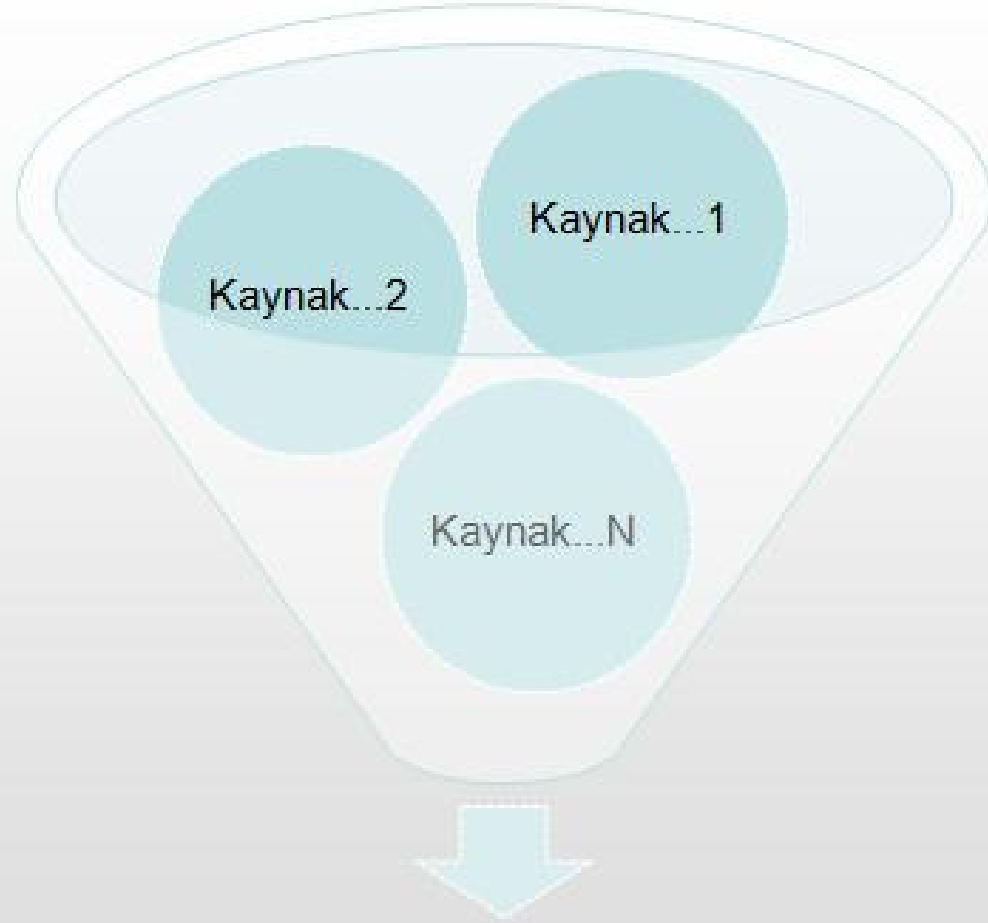
Veritabanı yönetim sistemleri

Antivirüs yazılımları

Aktif/Pasif ağ cihazları

Uygulamalar

- 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.



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

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

- 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.

- 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.

- 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.

- 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

- 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

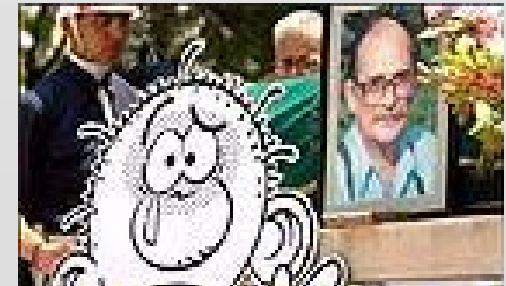
HEDEF



Windows 2000 Server
IIS 5.0 Web Sunucu

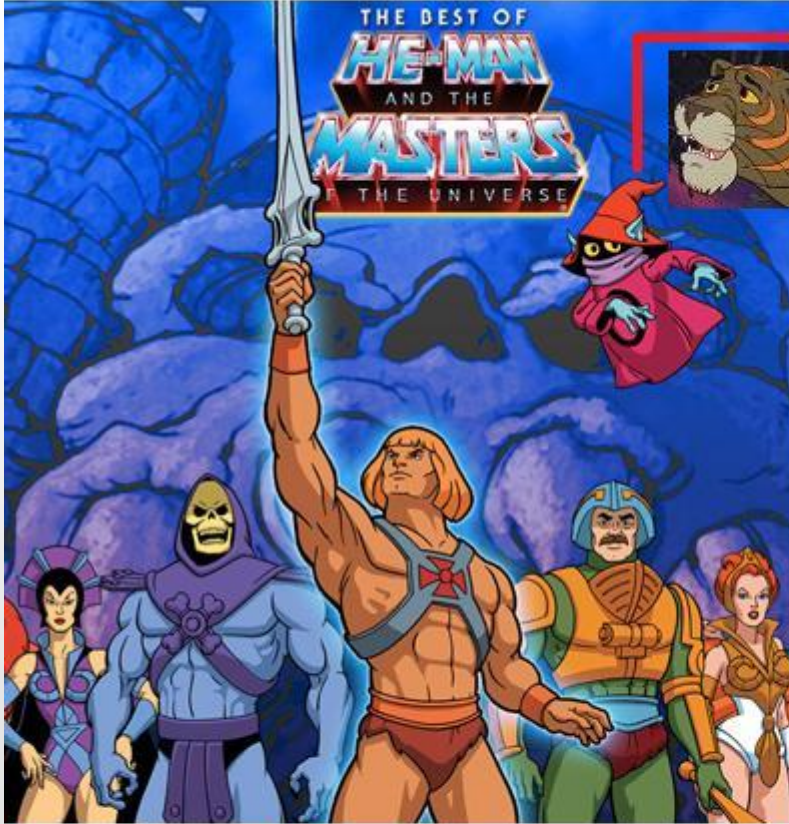
- Amaç: Web sunucu üzerinde SYSTEM haklarını ele geçirmek ve açılış dosyasını değiştirmek.
- Kullanılacak Açıklık: “Microsoft IIS 5.0 Printer Host Header Overflow”
- Var mısın yok musun?
 - Örneği eğlence soslu mu alırsınız?
 - Yoksa Hamdi Bey’in eğlencesiz teklifini kabul ediyor musunuz?

Tahmin etmiřtim ☺



Olay İlişkilendirme Yapılmayan Ortam

Bizim jenerasyon için...



He-Man'e yetişemeyenler için...



CLINT EASTWOOD
ELI WALLACH
LEE VAN CLEEF
THE GOOD THE UGLY AND THE BAD



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

Abi Nimda zorluyor
kapiyı



Aslanım Nimda mı
kaldı?

Ya varsa?

Geveze Orko hala iş başında

Abi sıkıcı olduğumun farkındayım ama bir kayıt daha düştü

Güzel hatrın için baktım. Yok bir problem.



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 beklememez...

Bittiğimizin resmidir

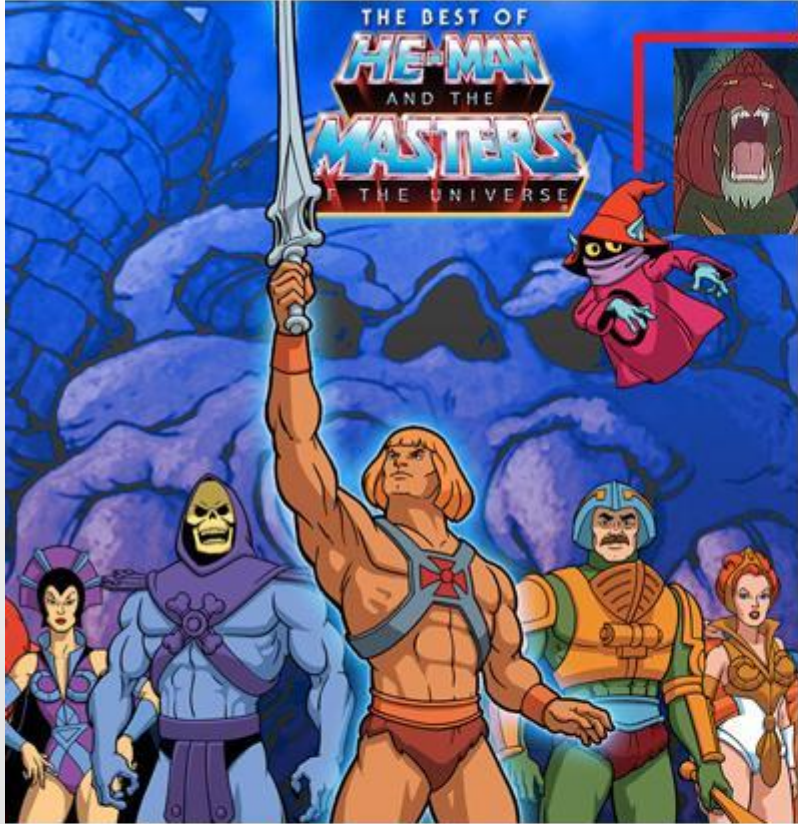


Bittiğinden daha fazla resim var orada !



Olay İlişkilendirme Yapılan Ortam

Bizim jenerasyon için...



He-Man'e yetişemeyenler için...



~~THE UGLY~~
THE GOOD AND THE BAD



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 !



Teşekkürler Sorular?

Burak BAYOĞLU

bayoglu@uekae.tubitak.gov.tr

☎: (262) 648 1529