

# **OSSEC-HIDS**

***(Open Source – Host-based  
Intrusion Detection System)***

Daniel B. Cid ([daniel.cid@gmail.com](mailto:daniel.cid@gmail.com))

Ahmet Ozturk ([oahmet@metu.edu.tr](mailto:oahmet@metu.edu.tr))

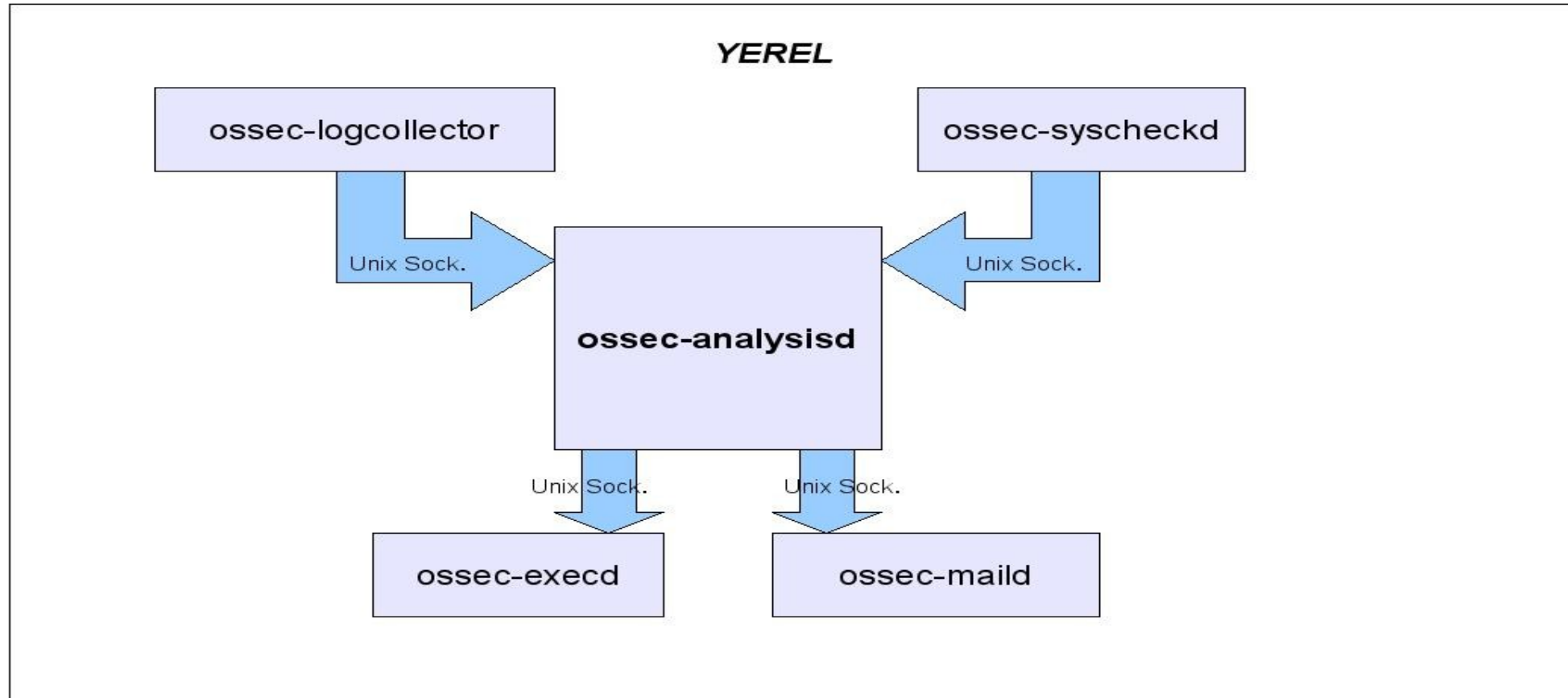
# İçerik

- Kabiliyetler
- OSSEC-HIDS Mimari
- Demo Kurulum
- Gelecek Planları
- Sorular

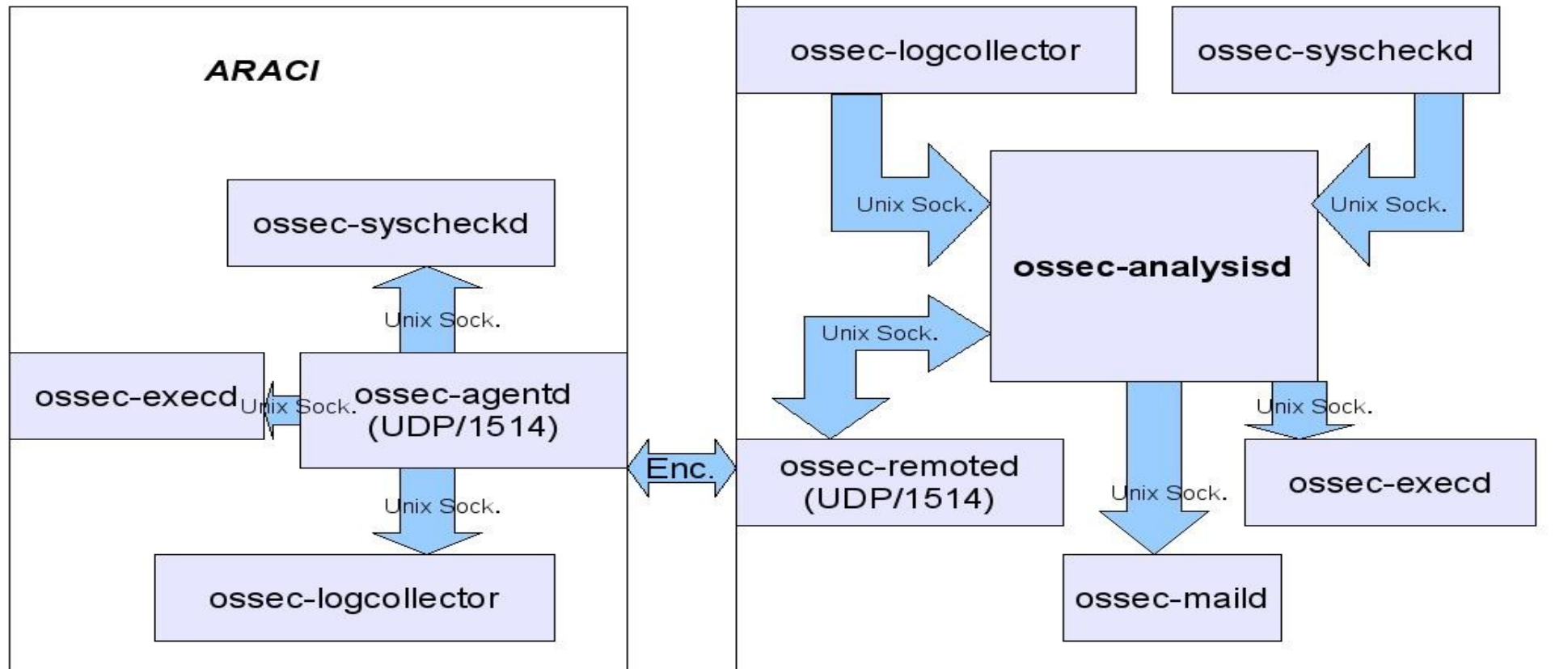
# Kabiliyetler

- Rootkit belirleme
- Sistem bütünlük testleri
- Log inceleme ve uyarı üretme (Apache, Sendmail, Postfix, Squid, Proftpd, Bind, Openssh, Cisco-pix vb.)
- Aktif yanıt üretme (IP ve kullanıcı tabanlı engelleme )
- Tek başına veya Sunucu-İstemci(Aracı) şeklinde çalışabilme

# OSSEC-HIDS Mimari - I



# OSSEC-HIDS Mimari - II



# Program Parçaları-I

## *ossec-syscheckd*

- syscheck
  - Dosya değişiklik kontrolleri
    - md5sum
    - tarih
    - dosya sahipliği
    - dosya izinleri
- rootcheck
  - Rootkit / truva atı belirleme (imza ve sıradışılık testleri)
  - Süreç kontrolleri
  - Port kontrolleri

# Program Parçaları-II

## *ossec-logcollector*

- Desteklenen Günlük Kayıt (Log) Formatları:
  - Syslog
  - Apache
  - Squid
  - Snort-full / Snort-fast
  - Windows Eventlog / IIS Log

# Program Parçaları-III

## *ossec-agentd*

- Olay bilgisi yönlendirme
- Sunucuyu periyodik bilgilendirme
- Sunucu-Aracı arasında şifreli trafik (simetrik anahtar)

# Program Parçaları-IV

## *ossec-remoted*

- Etkin yanıt (active-response) yönlendirme
- Sunucu-Aracı arasında şifreli trafik (simetrik anahtar)
- Syslog mesajlarını alabilme

# Program Parçaları-V

## *ossec-analysisd*

- Yapılandırma / Kurallar
- Günlük kayıtlarının (log) incelenmesi
- Etkin-yanıt üretme kararları
- Uyarı üretme / Kayıt tutma
- E-posta ile haber verme

# Program Parçaları-VI

## *ossec-execd*

- Üretilen Etkin-yanıtların çalıştırılması ve kontrolü
  - firewall-drop
    - iptables
    - ipfilter
    - ipfw
    - aix-ipsec
  - host-deny
  - disable-account

# Program Parçaları-VII

## *ossec-maild*

- Üretilen uyarıların e-posta ile bildirilmesi

# Kurulum Örneđi

- Kurulum
- Yapılandırma dosyaları
- Örnek uyarı üretme

# Gelecek Planları

- Kullanıcı Web arayüzü hazırlanması.
- E-posta ile ilgili aktif yanıt üretme özelliğinin eklenmesi.
- Daha fazla belge hazırlanması.
- Daha fazla uygulama için saldırı imzası oluşturulması ve varolan imzaların geliştirilmesi.
- Kodların güvenlik taramasından ve kalite kontrolden geçirilmesi ([scan.coverity.com](http://scan.coverity.com))

Teşekkürler ...  
Sorularınız ?

(<http://www.ossec.net>)