Açık Kaynak Kodlu Saldırı Tespit Sistemi

(Open Source Host-based Intrusion Detection System)

Çağrı Ersen
cagri.ersen@gmail.com
http://www.syslogs.org

Ajanda

- **Ossec Nedir ?**
- **Mimari**
  - Local
  - Manager/Agent
  - Agentlesss
- **Temel Ossec Görevleri**
  - Log Monitoring
  - Active Response
  - Dosya Bütünlük Kontrolü
  - Rootkit Tespiti

OSSEC NEDİR ?

Nedir ?

- HIDS (Host-based Intrusion Detection System) olarak adlandırılan bir saldırı (sızma) tespit sistemidir.
- Daniel Cid tarafından geliştirilmeye başlanmıştır.
- GPLv3 lisanslı açık kaynak kod bir uygulamadır.
- 2009 yılında Trend Micro tarafından alınmıştır.

Özellikler

- Log analizi, dosya bütünlük kontrolü, rootkit tespiti yapar.
- Gerçek zamanlı ve yapılandırılabilir alarmlar üretir.
- Active Response özelliği ile otomatik aksiyonlar alabilir.

Özellikler

Öntanımlı olarak bir çok decoder ve rule ile gelir

apache_rules	Apache HTTP server rules
arpwatch_rules	Arpwatch rules
attack_rules	Common attack rules
cisco-ios_rules	Cisco IOS firmware rules
courier_rules	Courier mail server rules
firewall_rules	Common firewall rules
ftpd_rules	Rules for the ftpd daemon
hordeimp_rules	Horde Internet Messaging Program rules
ids_rules	Common IDS rules
imapd_rules	Rules for the imapd daemon
local_rules	OSSEC HIDS local, user-defined rules
mailscanner_rules	Common mail scanner rules
netscreenfw_rules	Juniper Netscreen firewall rules
mysql_rules	MySQL database rules
named_rules	Rules for the named daemon

Özellikler

ossec_rules	Common OSSEC HIDS rules
pam_rules	Pluggable Authentication Module (PAM)
pix_rules.xml	Cisco PIX firewall rules
policy_rules	Policy specific event rules
postfix_rules	Postfix mail transfer agent rules
postgresql_rules	PostgerSQL database rules
proftpd_rules.xml	ProFTPd FTP server rules
pure-ftpd_rules.xml	Pure-FTPd FTP server rules
racoon_rules.xml	Racoon VPN device rules
rules_config.xml	OSSEC HIDS Rules configuration rules
sendmail_rules.xml	Sendmail mail transfer agent rules
squid_rules.xml	Squid proxy server rules
smbd_rules.xml	Rules for the smbd daemon
sonicwall_rules.xml	SonicWall firewall rules
spamd_rules.xml	Rules for the spamd spam-deferral daemon

Özellikler

- Multi Platform: Linux, Solaris, AIX, HP-UX, BSD, Mac ve Vmware ESX üzerinde çalışabilir.
- Agentless monitoring ile Router ve Firewall gibi agent kurulamayacak cihazlar monitor edilebilir.
- İstemci/Sunucu Mimarisi ile merkezi yönetim sağlar.

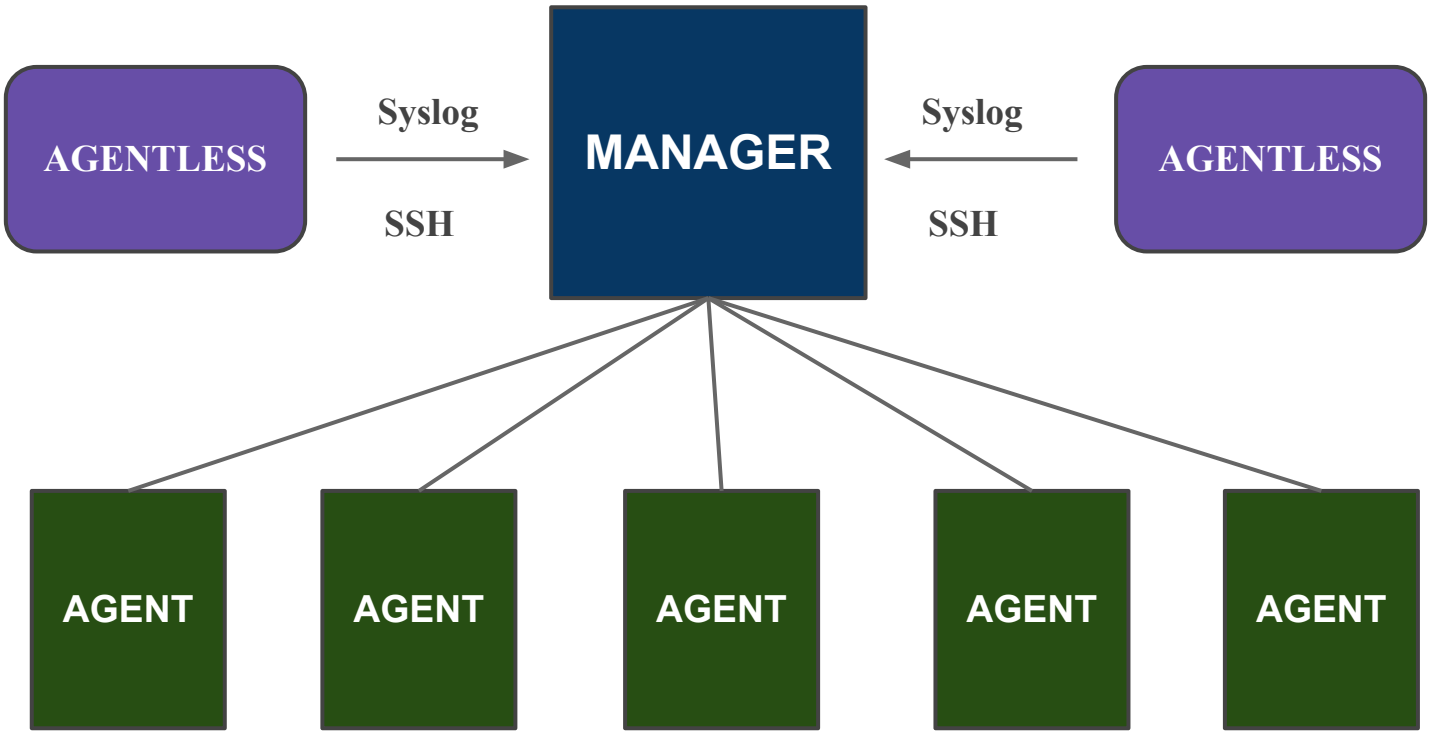
MİMARİ

KURULUM MODLARI

- Lokal Mod
  - Aynı sistem üzerinde hem server hem agent.
  - Tek sistemli ortamlar için ideal.

- Manager/Agent Mod
  - Merkezi Yapılandırma ve Yönetim
  - Birden fazla sistemden oluşan yapılarda kullanışlı.

MANAGER / AGENT



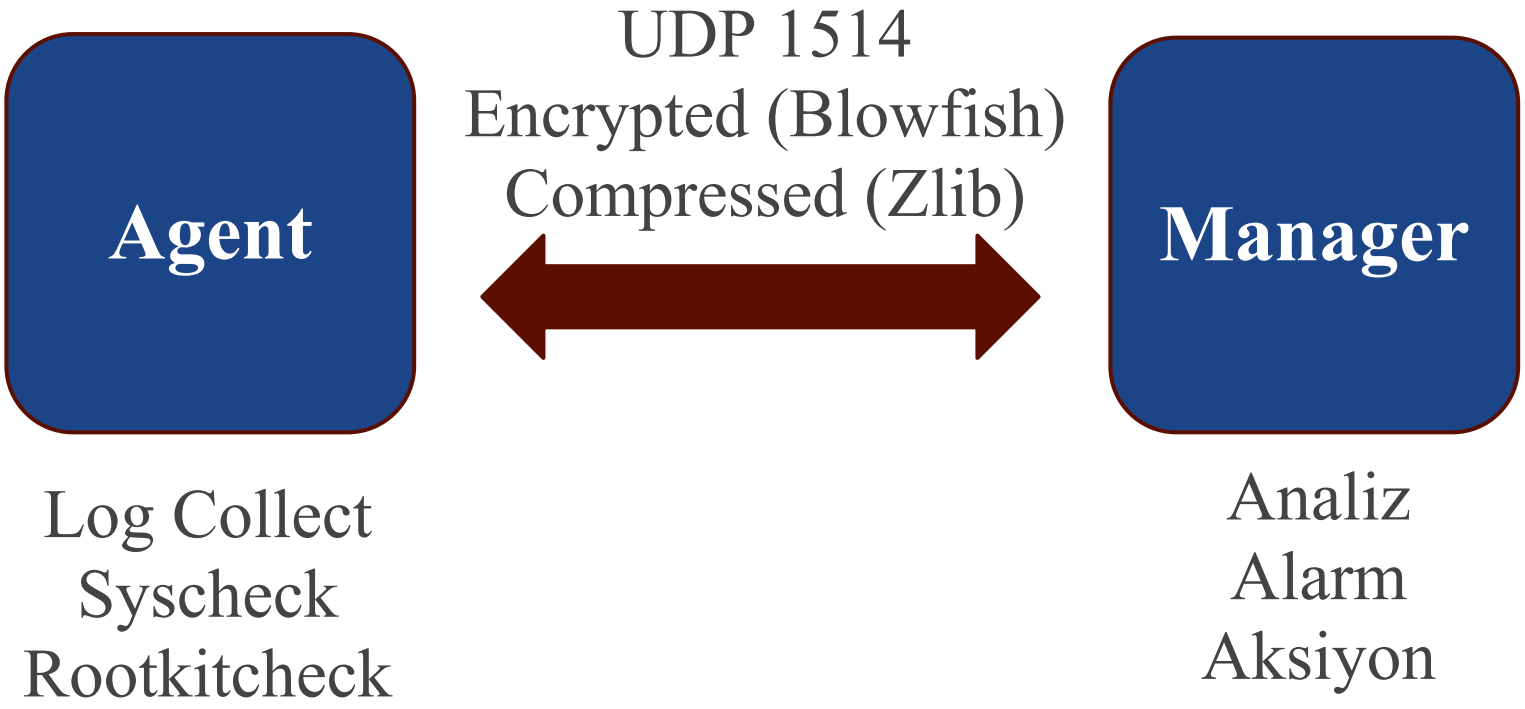
MANAGER

- Agentlar için merkezi yönetim noktasıdır.
- Ana yapılandırma dosyaları,
- Decoder ve kurallar,
- Agentlara ait dosya bütünlük veritabanları,
- Logları, event ve sistem audit girdilerini barındırır."

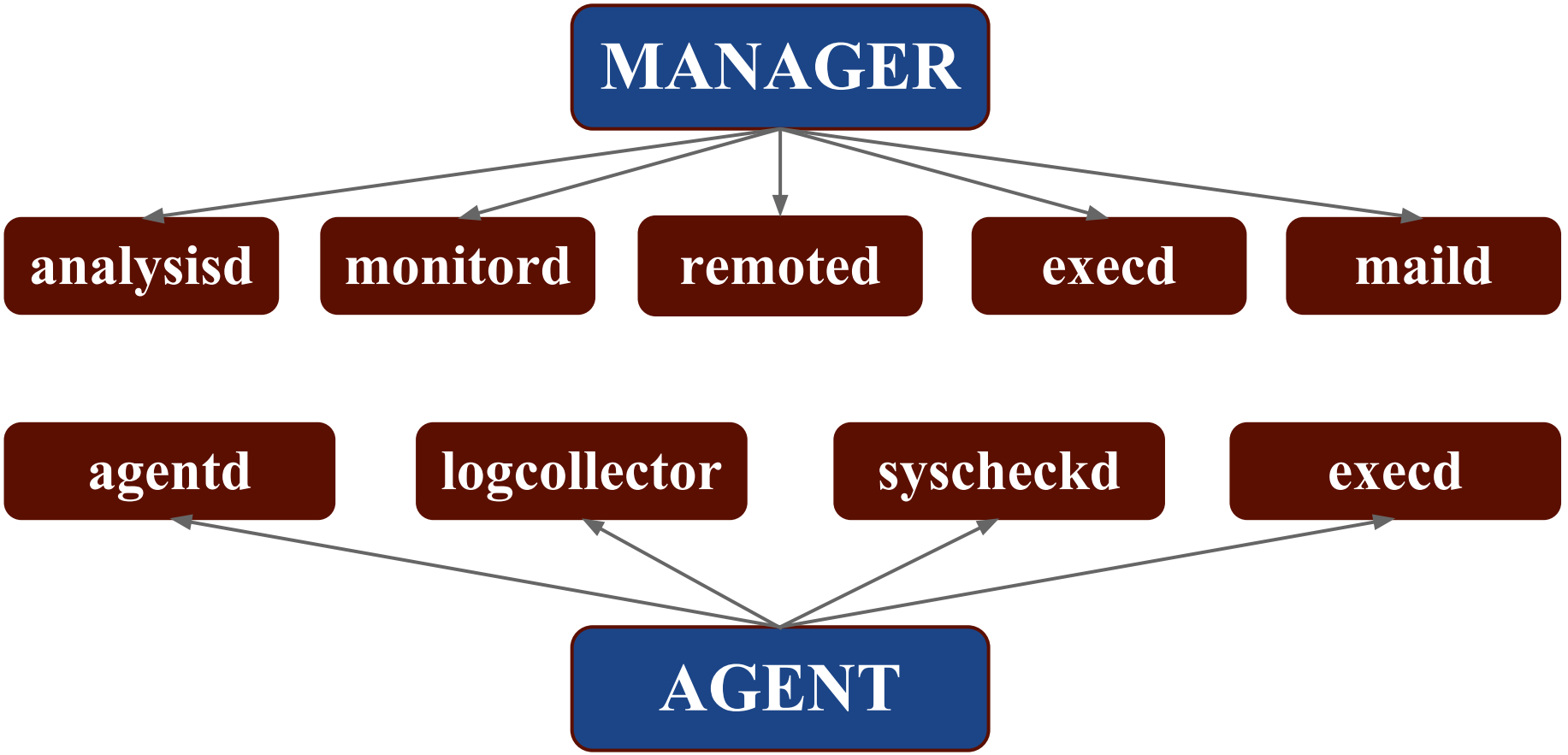
AGENT

- Kurulu olduğu sistemdeki olayları analiz edilmek üzere managera yollar.
- Memory ve CPU footprinti çok küçüktür.
- Sistemde yetkisiz bir kullanıcı üzerinden çalışır.
- Yapılandırma manager tarafından push edilir.
- Yapılandırmada değişiklik olması durumunda alarm üretilir.

AGENT / MANAGER



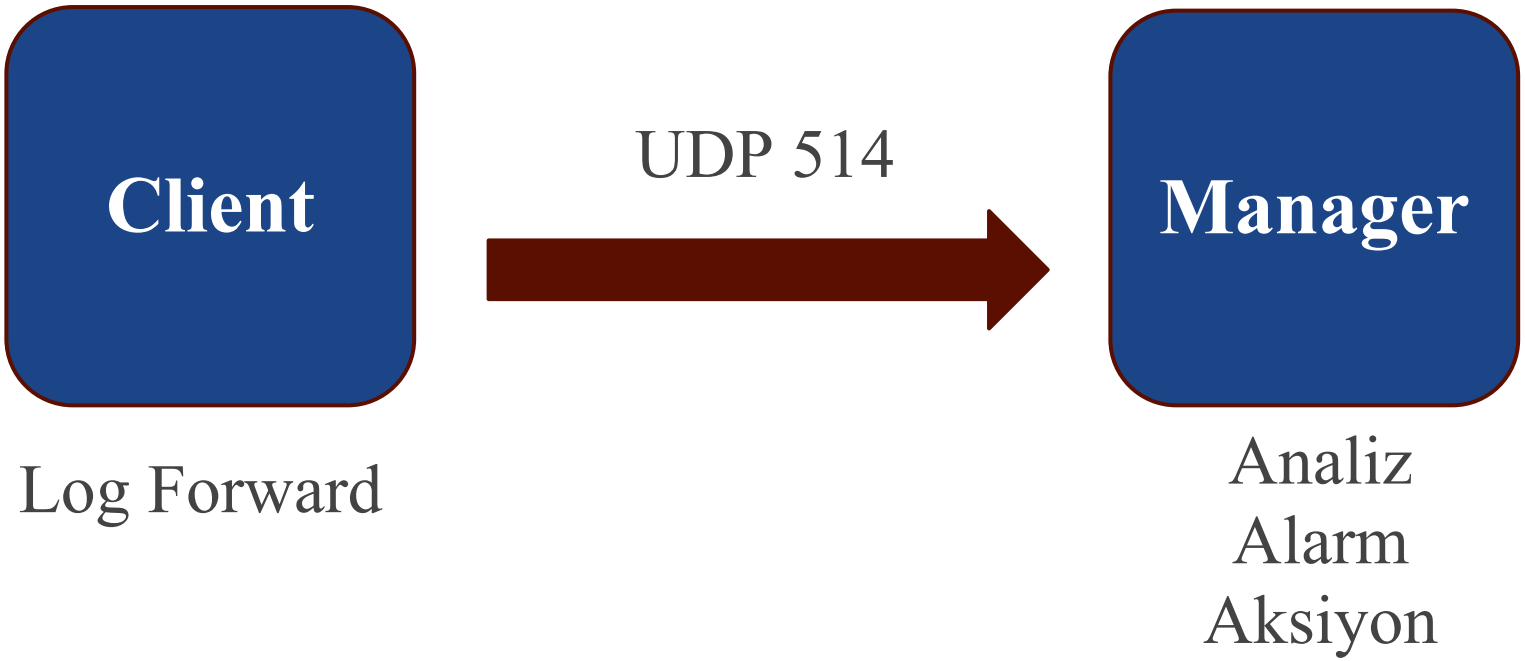
SÜREÇLER


MANAGER
analysisd
monitord
remoted
execd
maild
agentd
logcollector
syscheckd
execd
AGENT

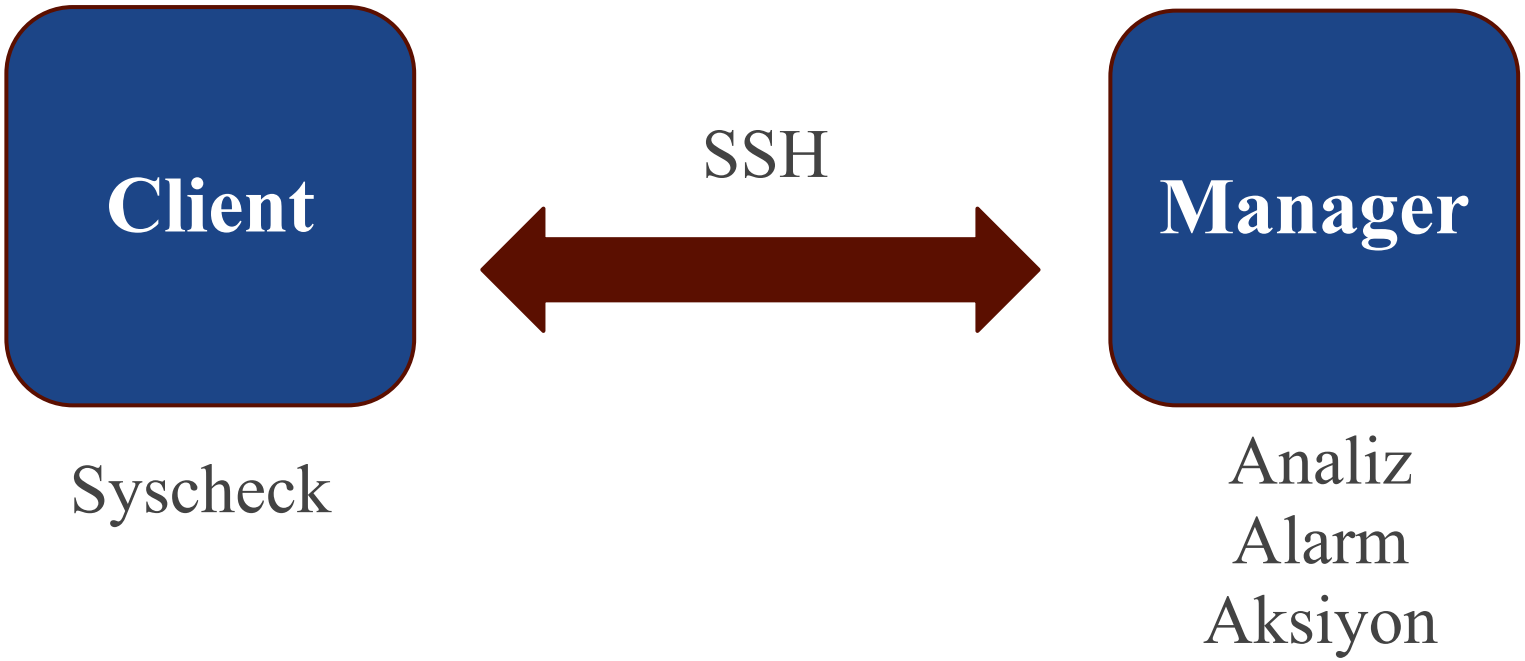
Mimari

- **analysisd** Server side çalışır; tüm analiz işlerinden sorumludur.
- **remoted** Agentlarla iletişim kuran süreçtir.
- **monitord** Agentların bağlantı durumlarını monitor eder.
- **maild** Alarmları göndermekten sorumlu süreçtir.
- **execd** Active response komutlarını çalıştırır. (Client/Server)
- **agentd** Agent'da çalışır; server ile iletişimden sorumludur.
- **logcollector** Monitor edilen log dosyalarını okur.
- **syscheckd** Dosya bütünlük kontrolünden sorumludur.

SYSLOG



AGENTLESS



DESTEKLENEN SİSTEMLER

Agents

GNU/Linux (all)
VMWare ESX 3.0,3.5
FreeBSD (all)
OpenBSD (all)
NetBSD (all)
Solaris 2.7, 2.8, 2.9,10
AIX 5.2,5.3
Mac OS X 10.x
Windows
HP-UX 11

Syslog

Cisco PIX, ASA,FWSM
Cisco IOS routers
Juniper Netscreen
SonicWall firewall
Checkpoint firewall
Cisco IOS IDS/IPS module
Sourcefire (Snort) IDS/IPS
Dragon NIDS
Checkpoint Smart Defense
McAfee VirusScan (v8,v8.5)
Bluecoat proxy
Cisco VPN concentrators
VMWare ESXi 4.x

Agentless

Cisco PIX,ASA, FWSM
Cisco IOS routers
Juniper Netscreen
SonicWall firewall
Checkpoint firewall

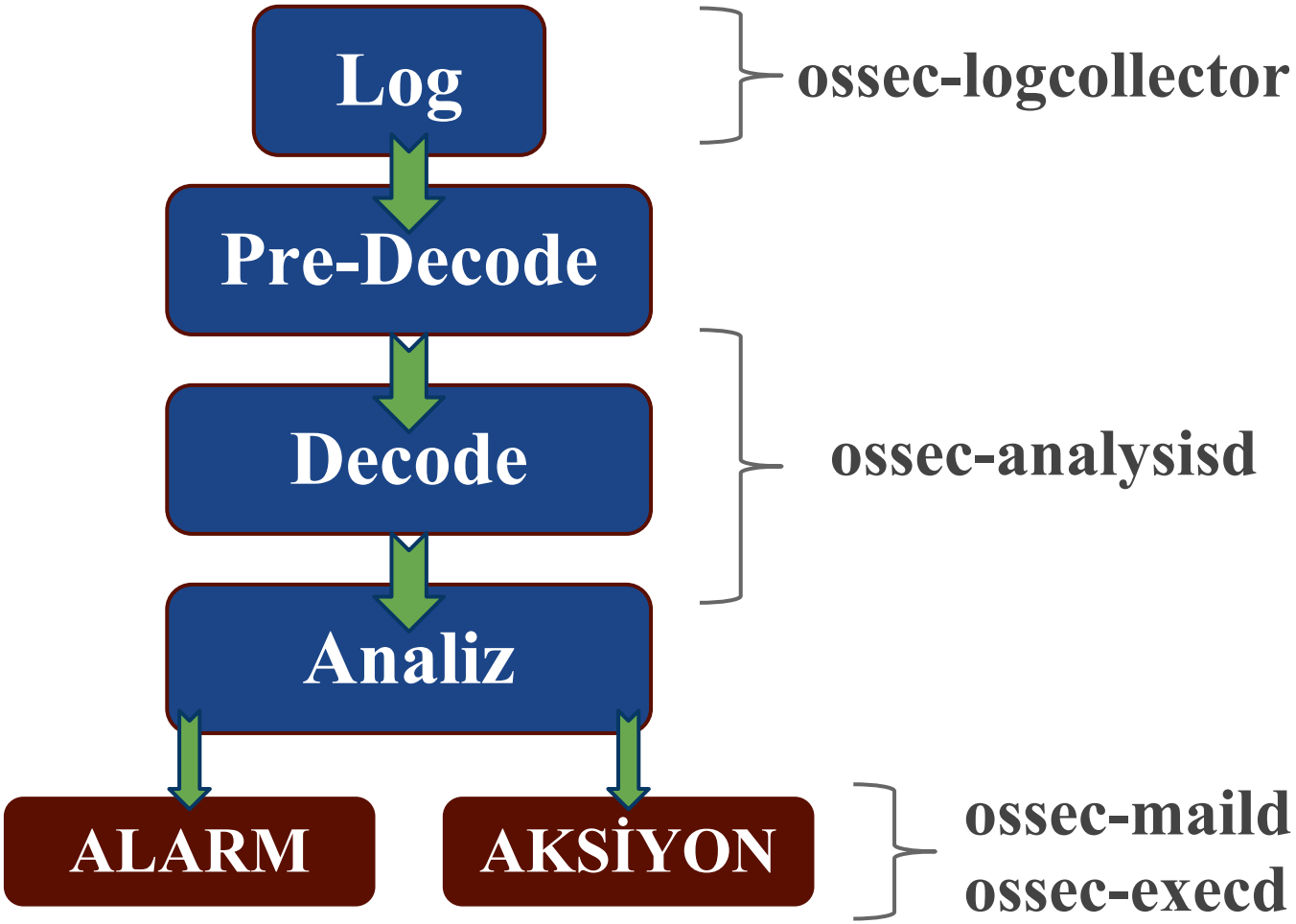
http://www.ossec.net/doc/manual/supported-systems.html

TEMEL OSSEC GÖREVLERİ

(1)

LOG MONITORING

LOG MONITORING



Pre-decoding

Log'un statik öğelerinin parse edildiği aşama
(Hostname, tarih/saat, program ismi vs.)

Mar 29 18:32:09 Lab03-Debian sshd[13633]: Failed password for cagri from 192.168.12.12 port 36179 ssh2

hostname:	Lab03-Debian
program_name:	sshd
time/date:	Mar 29 18:32:09
log:	Failed password for cagri from 192.168.12.12 port 36179 ssh2

Decoding

Log içerisinden spesifik bilgilerin parse edildiği aşama.
(IP adres, kullanıcı adı, url vs.)

Mar 29 18:32:09 Lab03-Debian sshd[13633]: Failed password for cagri from 192.168.12.12 port 36179 ssh2

srcip: 192.168.12.12
user: cagri

Analiz (1)

Mar 29 18:32:09 Lab03-Debian **sshd**[13633]: Failed password for cagri from 192.168.12.12 port 36179 ssh2

/var/ossec/etc/decoder.xml

```
<decoder name="sshd">
  <program_name>^sshd</program_name>
</decoder>
```

Analiz (2)

```
<rule id="111" level="0" noalert="1">
  <decoded_as>sshd</decoded_as>
  <description>SSHD messages grouped.</description>
</rule>

<rule id="122" level="5">
  <if_sid>111</if_sid>
  <match>^Failed|^error: PAM: Authentication</match>
  <description>SSHD authentication failed.</description>
  <group>authentication_failed,</group>
</rule>
```

KURAL 111

Log sshd olarak decode edilen (predecoding) herşeyi ID 111 olarak grupla.

KURAL 122

Eğer 111 ID'li kural match etti ise ve logda "Failed" ibaresi geçiyorsa bu kuralın level'ını 5'e yükselt ve kuralı authentication_failed grubuna dahil et.

Analiz (3)

```
<rule id=”133” level=”13”>
<if_sid>122</if_sid>
<hostname>^abraxas</hostname>
<srcip>!192.168.12.0/24</srcip>
<description>Higher severity! Failure on the main
server</description>
</rule>
```

KURAL 133

122 ID'li [SSH authentication fail kuralı] match ettiyse ve hostname "abraxas" olarak decode edildiyse, ayrıca kaynak ip 192.168.12.0/24 networkunden değilse bu kural'ın önem derecesini 13 olarak set et.

Analiz (4)

```
<rule id="100005" level="10">
<if_group>authentication_success</if_group>
<time>6 pm - 7:30 am</time>
<description>Login during non-business hours.</description>
</rule>
```

KURAL 100005

authentication_success grubuna dahil olan kurallar mesai saatleri dışında match ederse bu kuralı level 10 olarak set ederek alarm üret.

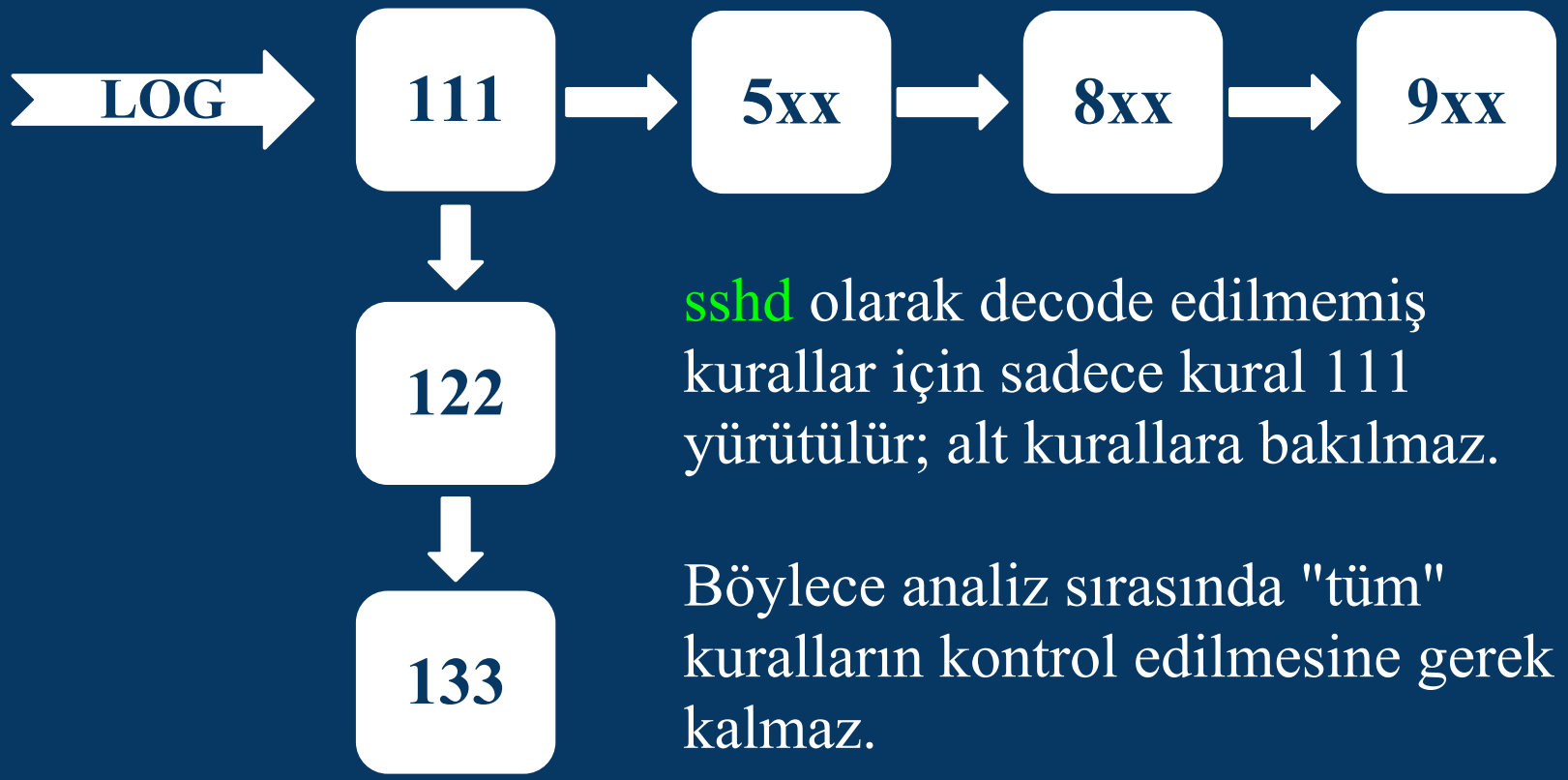
Analiz (5)

```
<rule id="144" level="11" frequency="5" timeframe="120">
<if_matched_sid>122</if_matched_sid>
<same_source_ip />
<description>Multiple failed attempts from same IP!</description>
</rule>
```

KURAL 144

122 ID'li [SSH authentication fail kuralı] 120 saniye içerisinde 5 kez match ederse ve kaynak ip aynıysa bu kuralın önem derecesini 11 olarak set et.

Kural Hiyerarşisi



sshd olarak decode edilmemiş kurallar için sadece kural 111 yürütülür; alt kurallara bakılmaz.

Böylece analiz sırasında "tüm" kuralların kontrol edilmesine gerek kalmaz.

Desteklenen Log Formatları ve Uygulamalar

Pam	sshd (OpenSSH)	Solaris telnetd	Samba
su/sudo	Xinetd	Adduser/deluser	Cron/Crontab
Dpkg logs	Yum logs	Proftpd	Pure-ftpd
vsftpd	wu-ftpd	Solaris ftpd	Imapd and pop3d
Postfix	Sendmail	vpopmail	Microsoft Exchange
Courier imapd/pop3d/pop3-ssl		vm-pop3d	Procmail
Mailscanner	Apache	IIS 5/6	Zeus web server
Horde imp	Modsecurity	Iptables	Shorewall
IPFilter	AIX ipsec/firewall	Netscreen	Windows
firewall Cisco PIX	SonicWall firewall	Checkpoint	MySQL
PostgreSQ	Cisco IOS IDS/IPS	Snort	Dragon
NIDS McAfee VS Enterprise		Symantec Web	Nmap
Arpwatch			

http://www.ossec.net/main/supported-systems

Kural Seviyeleri

- Kurallar önem derecesine göre 0-15 arasında sınıflandırılmıştır.
- En önemsiz kurallar level 0, en önemliler ise level 15 olarak set edilir
- İlk yürütülen kurallar level 0 olanlardır. Ignore edilmesi istenen durumlar için oluşturulan kurallara atanır. (False positive)
- Default olarak "level 7 >= " kurallar için email notification devreye alınır.
- Default olarak "level 6 >=" kurallar için active response komutları yürütülür.

Kural ID'leri

- Her kuralın unique bir ID'si olması gerekir.
- 00000 - 109999 arası kural tiplerine göre tasnif edilmiştir.

```
00000 - 00999   Internally reserved for ossec
01000 - 01999   General syslog
02100 - 02299   NFS
02300 - 02499   Xinetd
02500 - 02699   Access control
02700 - 02729   Mail/procmail
02830 - 02859   Crond
.....
```

- Custom olarak eklenen kurallar için 100000 - 109999 kullanılmalıdır.

TEMEL OSSEC GÖREVLERİ

(2)

DOSYA BÜTÜNLÜK KONTROLÜ

Dosya Bütünlük Kontrolü (Syscheck)

- Önemli sistem dosyalarının monitor edilerek değişikliklerin saptanmasını amaçlar.
- Sistem belirli periyodlarla taranır ve monitor edilen dosyaların MD5/SHA1 checksumları Ossec Server'a gönderilir.
- Ossec Server checksumları depolar ve değişikliklere karşı kontrol eder. Herhangi bir fark tespit edilirse alarm üretir.
- Periyodik check yerine realtime monitoring de yapılabilir.

Syscheck

- checksum dışında size, owner, group ve permission değişiklikleri de monitor edilebilir.

- Öntanımlı olarak "/etc,/usr/bin,/usr/sbin /bin,/sbin" dizinleri altdizinlerle birlikte monitor edilir.
- Çok sık değişiklik gören dosyalar ignore edilebilir.

- Checksum bilgileri serverda tutulduğu için değişen dosyalarla ilgili geçmişe dönük analizler yapılabilir.

Yapılandırma

/var/ossec/etc/ossec.conf

```
<syscheck>
 <frequency>79200</frequency>
 <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
 <directories check_all="yes">/bin,/sbin</directories>
 <ignore>/etc/mtab</ignore>
 <ignore>/etc/mnttab</ignore>
 <ignore>/etc/hosts.deny</ignore>
 <ignore>/etc/mail/statistics</ignore>
 <ignore>/etc/random-seed</ignore>
 <ignore>/etc/adjtime</ignore>
 <ignore>/etc/httpd/logs</ignore>
   ....
</syscheck>
```

TEMEL OSSEC GÖREVLERİ

(3)

ROOTKIT KONTROLÜ

Rootkit Kontrolü (Rootcheck)

- /var/ossec/etc/shared dizininde bulunan rootkit imza veritabanları kullanılır.
- rootkit_files.txt isimli db'de belirtilen tüm dosyalar için stats, fopen, opendir ve chdir sistem çağrıları kullanılarak kontrol yapılır. Bu kontrol, dosyaları bazı sistem çağrılarından sakladığı bilinen rootkitlerin tespiti için yapılır.
- rootkit_trojans.txt db'si rootkitlerin değiştirdiği bilinen binary dosyalarının tespitinde kullanılır. (string search)

Rootcheck

- /dev dizini herhangi bir anormalliğe monitor edilir. device ve makedev scripti olmayan şüpheli dosyalar aranır.

- Tüm dosya sistemi alışılmadık dosyalara ve izinlere karşı taranır. Sahibi root olup diğer kullanıcılar tarafından yazılabilen ya da suid biti etkinleştirilmiş dosyalar ve gizli dizin/dosyalar incelenir.

- Sistemde süreçler getsid ve kill (kill -0) sistem çağrıları kullanılarak kontrol edilir. Eğer kullanımda olan bir süreç numarası (PID) “ps” ile görüntülenemiyorsa bu, sistemde ps’in trojaned versiyonu kullanıldığı anlamına gelir.

Rootcheck

- Sistemde gizli portlar olup olmadığı araştırılır. bind sistem çağrısı kullanılarak, sistemdeki tüm TCP ve UDP portlar kontrol edilir. Eğer kullanımda olduğundan dolayı bind edilemeyen bir port, “netstat” çıktısında görülemiyorsa, sistemde netstat’ın trojanlı versiyonu kullanılıyor demektir.

- "Promisc" modda çalışan interface olup olmadğı kontrol edilir; eğer böyle bir interface var ancak ifconfig çıktısında görüntülenmiyorsa sistemde trojan bulunuyor olabilir.

Yapılandırma

/var/ossec/etc/ossec.conf

```
<rootcheck>
<rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
<rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.
txt</rootkit_trojans>
<system_audit>/var/ossec/etc/shared/system_audit_rcl.
txt</system_audit>
        <system_audit>/var/ossec/etc/shared/cis_debian_linux_rcl.
txt</system_audit>
<system_audit>/var/ossec/etc/shared/cis_rhel_linux_rcl.
txt</system_audit>
<system_audit>/var/ossec/etc/shared/cis_rhel5_linux_rcl.
txt</system_audit>
 </rootcheck>
```

ACTIVE RESPONSE

- Belirli kuralların tetiklenmesi durumunda sistemde otomatik olarak bir komut/script çalıştırılarak, kuralın tetiklenmesine neden olan olayın sonlandırılması amaçlanır.

- Atak durumlarında hızlı tepki verilmesini sağladığı için kullanışlıdır.

- Port/Web vs. Scan, brute force gibi bilgi toplamaya yönelik saldırıları engellemek için idealdir.

- Ossec öntanımlı olarak bazı AR scriptleri (tools) ile gelir ve kurulum sırasında active response devreye alınabilir.

Tools (Scripts)

- disable-account.sh: Kullanıcıyı devre dışı bırakmak için.
- host-deny.sh: Atakta bulunan source IP'yi hosts.deny dosyasına ekler. (sshd gibi tcpwrapper kullanan servisler)
- firewall-drop.sh: iptables ya da ipfilter kullanan sistemlerde için kaynak IP için drop kuralı ekler.
- ipfw.sh: ipfw kullanan sistemlerde srcip drop kuralı ekler.
- pf.sh: PF kullanan sistemlerde srcip drop kuralı ekler.
- route-null.sh: Srcip için blackhole rule ekler.

Yapılandırma

/var/ossec/etc/ossec.conf

```
<command>
  <name>host-deny</name>
  <executable>host-deny.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>firewall-drop</name>
  <executable>firewall-drop.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

Yapılandırma

/var/ossec/etc/ossec.conf

```
<active-response>
  <command>host-deny</command>
  <location>local</location>
  <level>6</level>
  <timeout>600</timeout>
</active-response>

<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <level>6</level>
  <timeout>600</timeout>
</active-response>
```

Riskler

- False positive durumlarda engellenmemesi gereken IP'ler blocklanabilir.
- Active Response kullandığınızı anlayan bir saldırgan durumu istismar edip DoS yapabilir. (Ip spoof)

Risk Mitigation

- False positive durumların önüne geçmek blocklanmaması gereken hostlar için whitelist oluşturulabilir.
- Block işlemlerinin timeout değeri vardır. (default 10 dakika).
- Active response scriptleri sadece belirli agentlar ya da sadece belirli kurallar için çalıştırılabilir.

WebApp Scan Pattern

```
207.44.184.96 - - [19:57:37 -0300] "GET /b2/xmlsrv/xmlrpc.php HTTP/1.0" 404 297 "-" "-"
207.44.184.96 - - [:19:57:37 -0300] "GET /blogtest/xmlsrv/xmlrpc.php HTTP/1.0" 404 303 "-" "-
"
207.44.184.96 - - [:19:57:37 -0300] "GET /blog/xmlsrv/xmlrpc.php HTTP/1.0" 404 299 "-" "-"
207.44.184.96 - - [:19:57:37 -0300] "GET /blogs/xmlsrv/xmlrpc.php HTTP/1.0" 404 300 "-" "-"
```

```
<rule id="31101" level="5">
  <if_sid>31100</if_sid>
  <id>^4</id>
  <description>Web server 400 error code.</description>
</rule>

<rule id="31151" level="10" frequency="10" timeframe="120">
  <if_matched_sid>31101</if_matched_sid>
  <same_source_ip />
  <description>Mutiple web server 400 error codes </description>
  <description>from same source ip.</description>
  <group>web_scan,recon,</group>
</rule>
```

Kaynaklar

http://www.ossec.net/doc/

http://www.ossec.net/main/ossec-book

TEŞEKKÜRLER