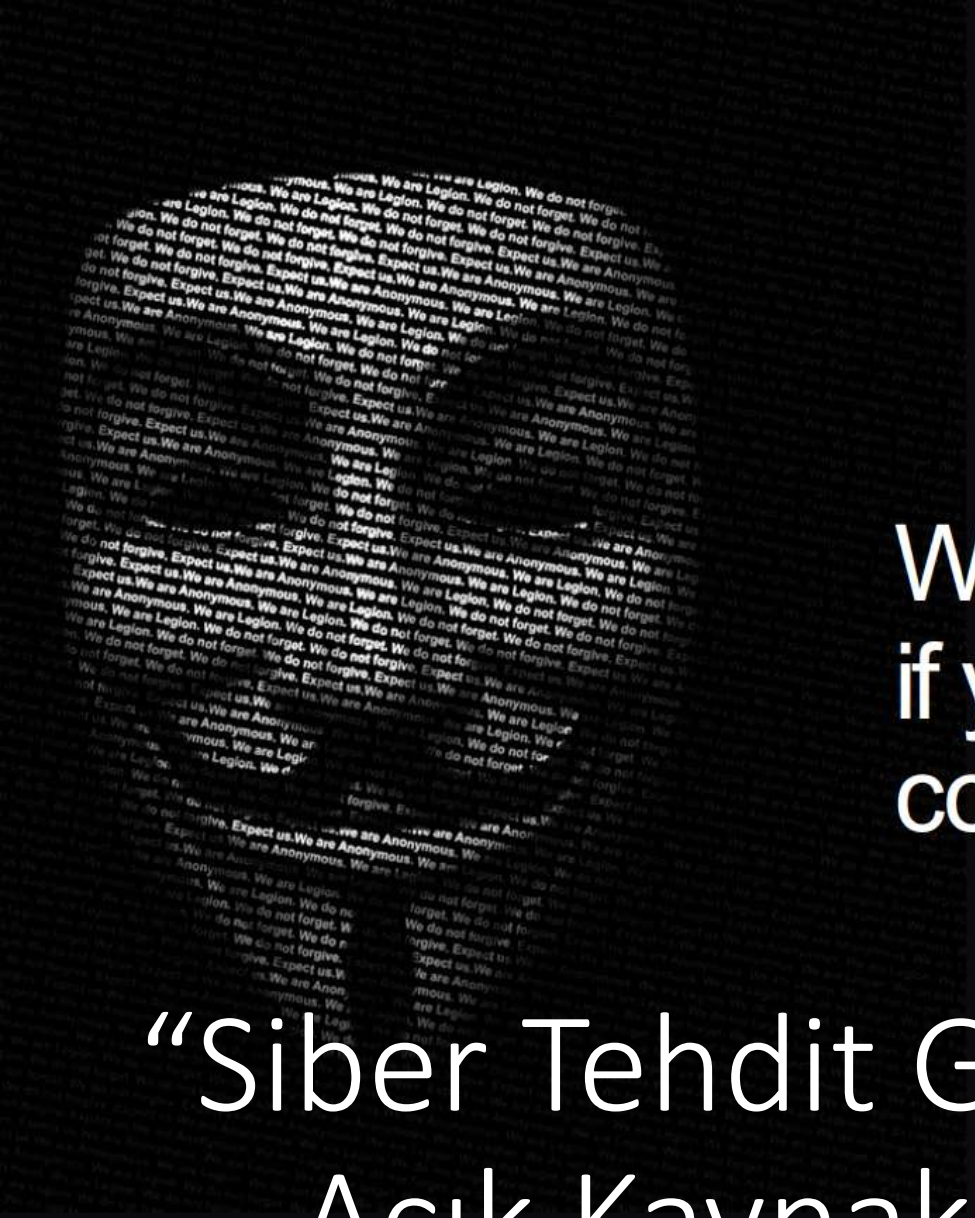
Huzeyfe ÖNAL

Bilgi Güvenliği AKADEMİSİ



“Siber Tehdit Gözetleme ve SIEM Olarak Açık Kaynak Sistemlerin Kullanımı”

Huzeyfe ÖNAL

- Yönetici Ortak – BGA Bilgi Güvenliği A.Ş.
- Sektör tecrübesi :2002-…
- Siber Güvenlik İnsiyatifi Kurul Üyesi (UDHB Bünyesinde)
- Öğretim Görevlisi (Siber Güvenlik Yüksek Lisans Programı)
  - Bilgi Üniversitesi (*Bilişim hukuku Yüksek Lisans Programı*)
  - Bahçeşehir Üniversitesi (*Siber Güvenlik Yüksek Lisans Programı*)
  - Şehir Üniversitesi (*Siber Güvenlik Yüksek Lisans Programı*)

Firma Hakkında: BGA Bilgi Güvenliği A.Ş.

- BGA markası ile 6 yıldır kurumlara stratejik siber güvenlik danışmanlığı sunmaktadır
- 45 teknik personel (Mühendis ağırlıklı)
- 2016 itibariyle Ankara, İstanbul, Bakü ve Virginia(USA) ofisleri
- Ağırlıklı çalışılan sektörler
  - Finans (32 Banka)
  - Enerji
  - Telekom
  - Savunma Sanayi
  - Kamu
- Bilgi Güvenliği AKADEMİSİ markası ile siber güvenlik konusunda üretim merkezi rolü

Open Source☺

Sunum İçeriği:Ajanda

1. SIEM Dünyası Genel Kavramlar
2. Açık Kaynak Tehdit İzleme
3. Açık Kaynak Log/SIEM Bileşenleri

Neden Açık Kaynak Çözümler?

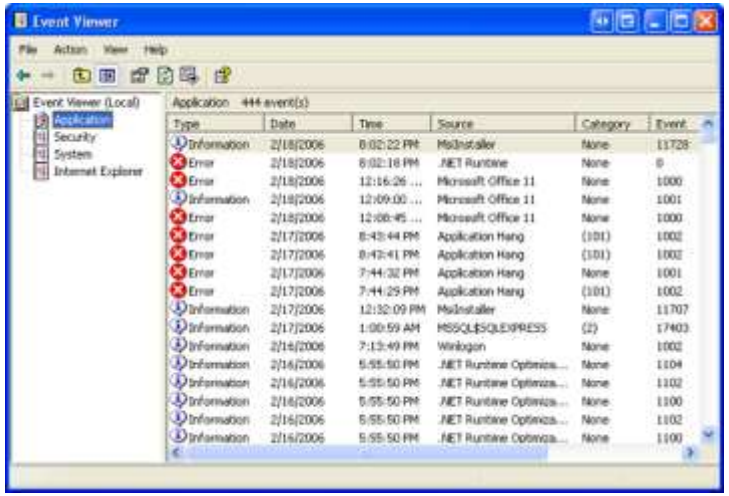
Siber Güvenlikte Yönetim ve Hakimiyet Problemi

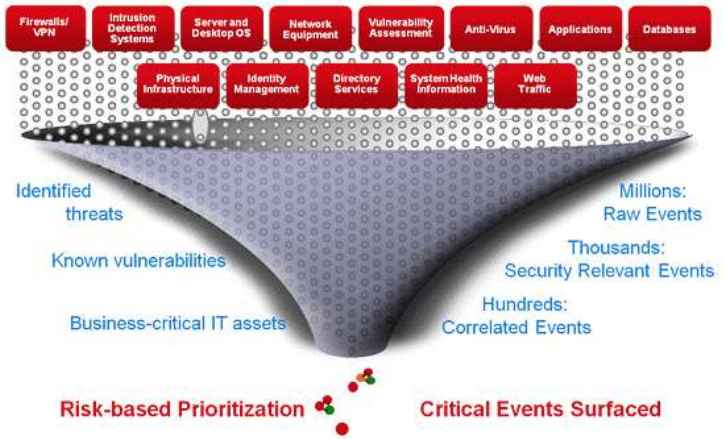
- Günümüz Siber Güvenlik problemleri incelendiğinde <anket çıktısı> büyük oranda problemin kurumların siber güvenlik altyapılarına hakim olmadıkları ortaya çıkmaktadır.
- Son iki yılda iç, dış veya kaynağı bilinmeyen siber saldırı olayı yaşanma oranı %63~ (Ortalama 100 şirket ve kamu kurumu için)
- Zamanında siber saldırıyı farketme ve önleme oranı %5
- Siber güvenlik ürünlerinin gerçek saldırılar karşısındaki uyarı ve engelleme kabiliyeti: %20
- Yapılan güvenlik yatırımlarının verimli kullanım ölçümü %17

Yeni Nesil Siber Güvenlik Modeli - “Zero Trust”

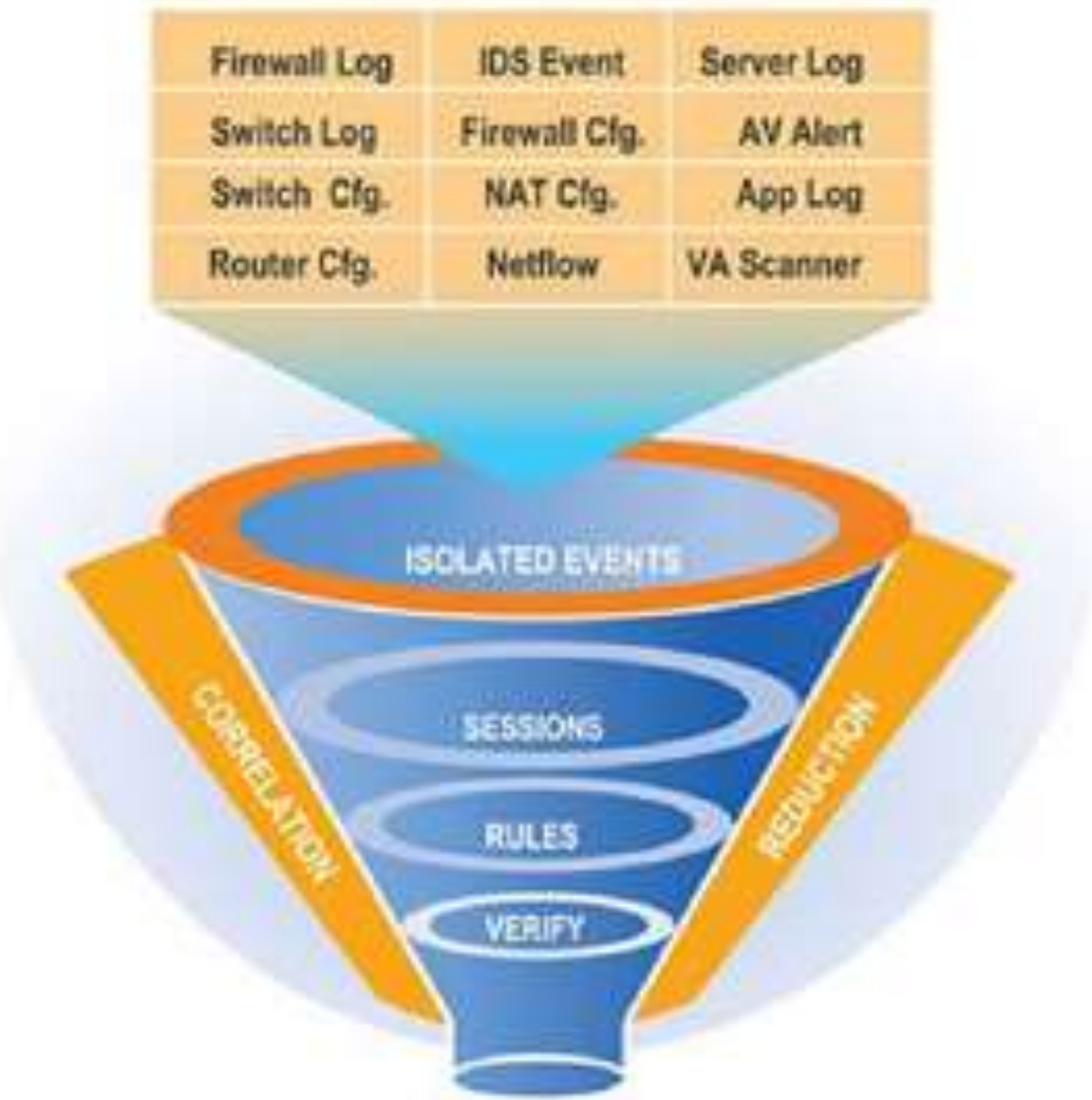
- “Zero Trust Model” Uygulaması.
- Başkan Obama tarafından Amerika’nın Siber Güvenliğinin uzun vadeli sağlanması açısından “Forrester Research” e geliştirilmiştir.
- Temel amaç, siber güvenlik işlerinde insana olan güvenin oyun dışına çıkartılması ve sistemin kendisini güvenli hale getirecek bir altyapının kurulumu.
- Klasik güvenlik anlayışında sınırları korumak ve yatırım yapmak yeterliyken “Zero Trust Model” de her noktanın güvenliğinin eşdeğer düşünülerek hareket edilmesi önerilmektedir.
- “Hattı müdafaa yoktur sathı müdafaa vardır, o satıh bütün vatandır''

Kavramlar Kavramlar…[Log, Siem, TM…]





SIEM’den Beklenen



Gerçekte Olan

Sonuç Olarak…

of successful advanced threat attacks are spotted by SIEM systems

Source:2014 Verizon Data Breach Investigation Report

Başarılı bir SIEM/Log Projesi için…

- Kapsama neler alınacak (hangi sistemler vs)
- Uymakla yükümlü olduğum standartlar/kanunlar vs var mı
- Günün sonunda ne elde etmeyi umuyorum
  - “Can alıcı soru”

SIEM Ürün Seçimi

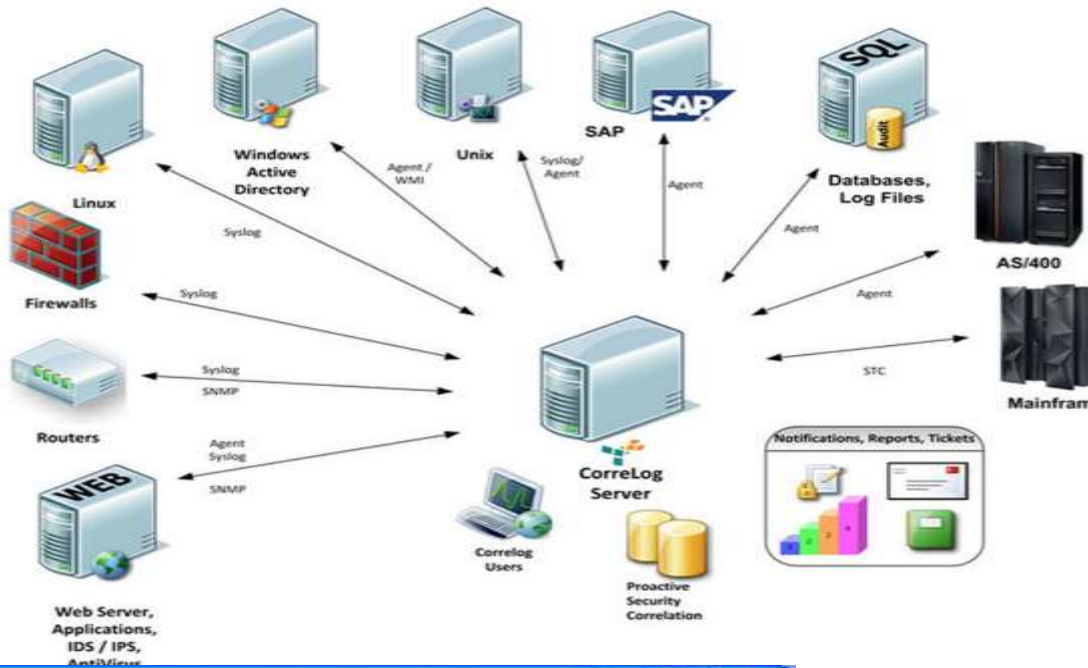
Sahadaki SIEM Ürünleri

As of November 2014, Mosaic Security Research identified 73 SIEM and log-management products.[5]

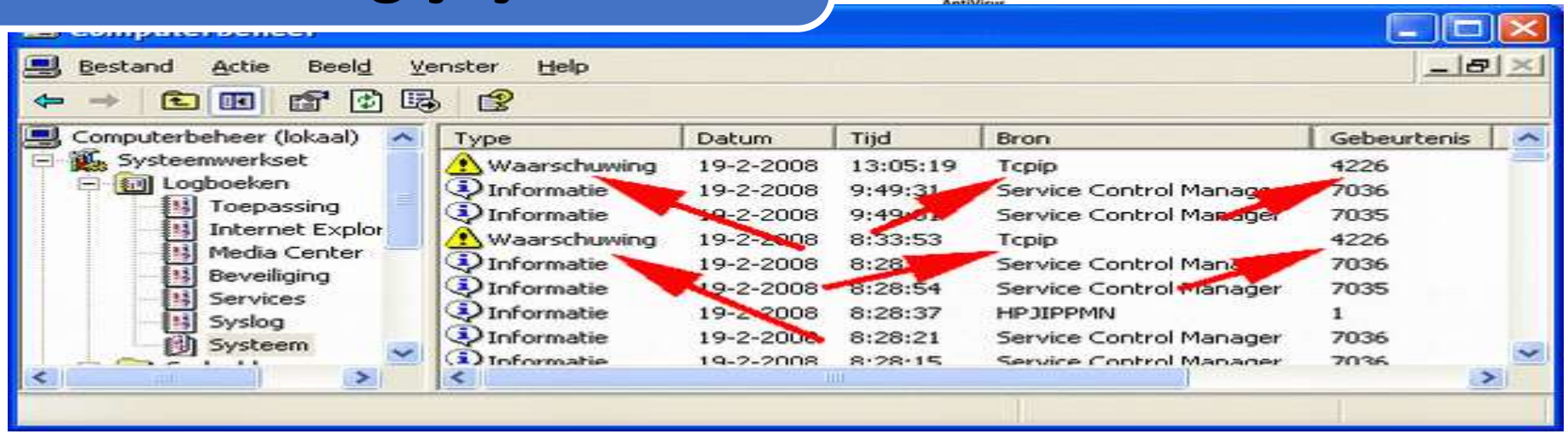
Hatalı Seçim Durumu

Log Kaynaklarının Tespiti & Detaylandırma

- Log Kaynaklarının Tespiti
- Hangi log kaynağından hangi detayda log



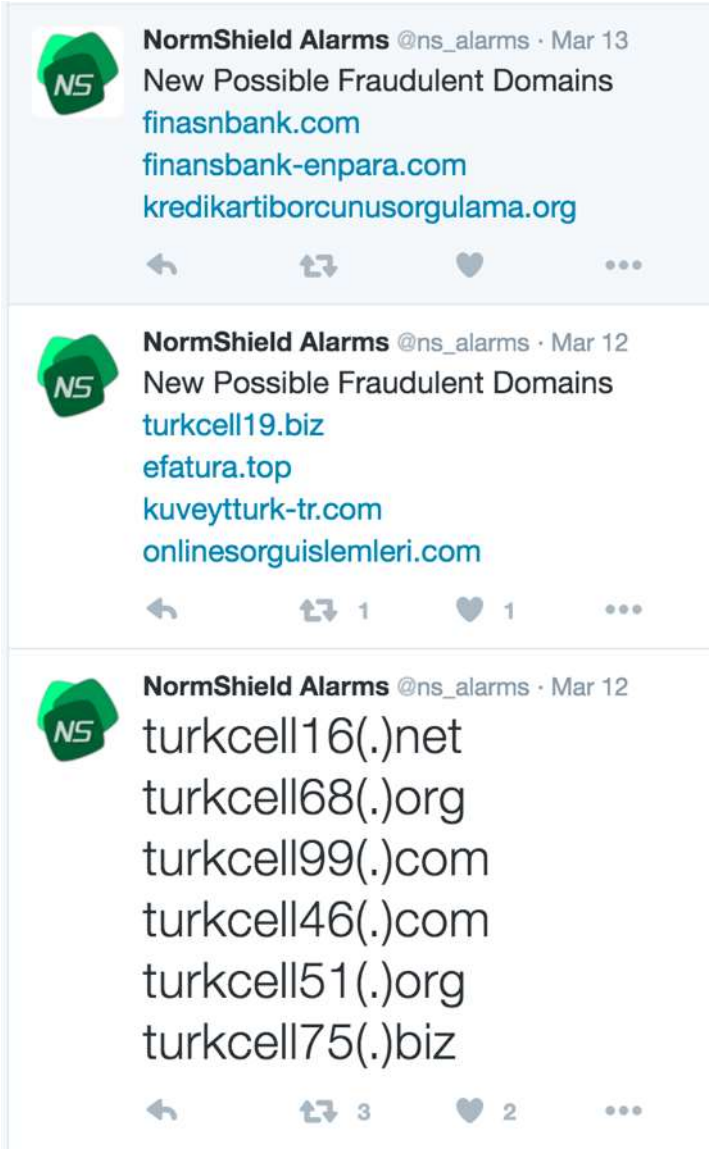
52 farklı kategoride 400 çeşit ürün, ortalama 3.500 log çeşidi…

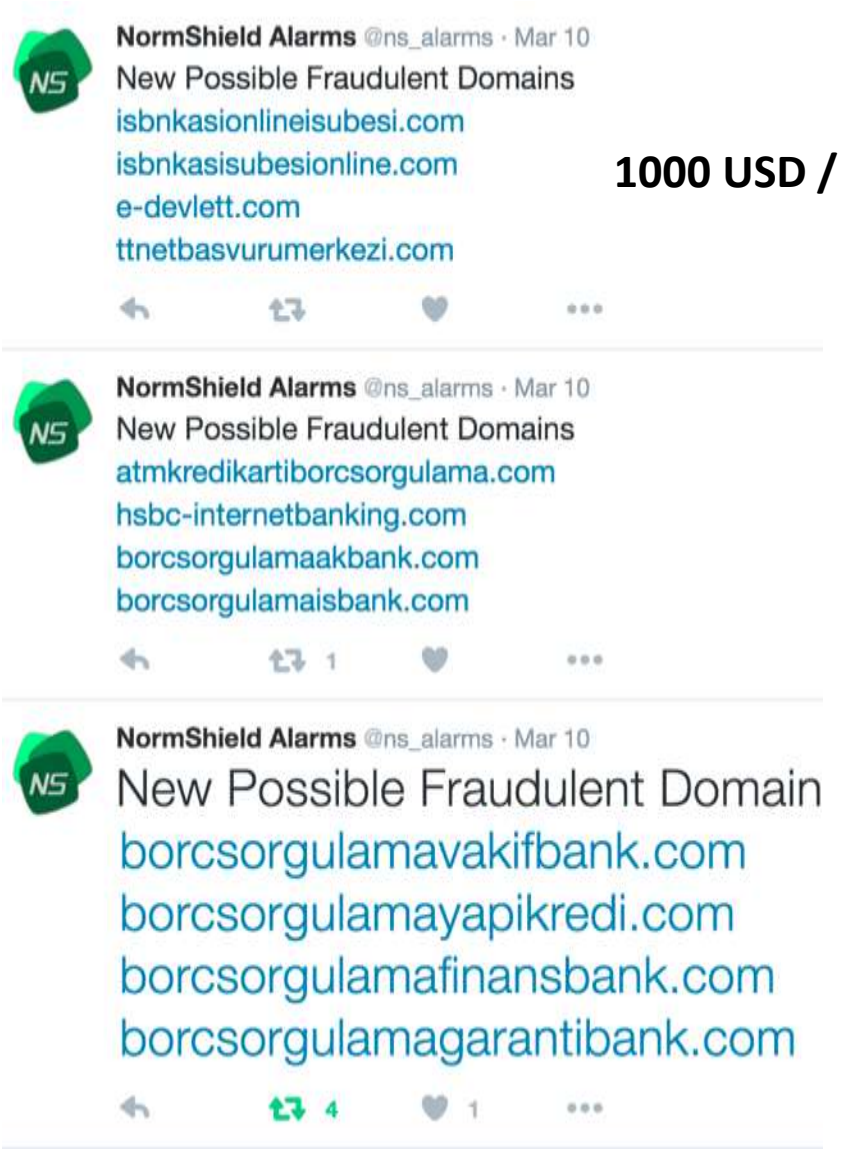


“Siber Tehdit İstihbaratı” Kullanımı

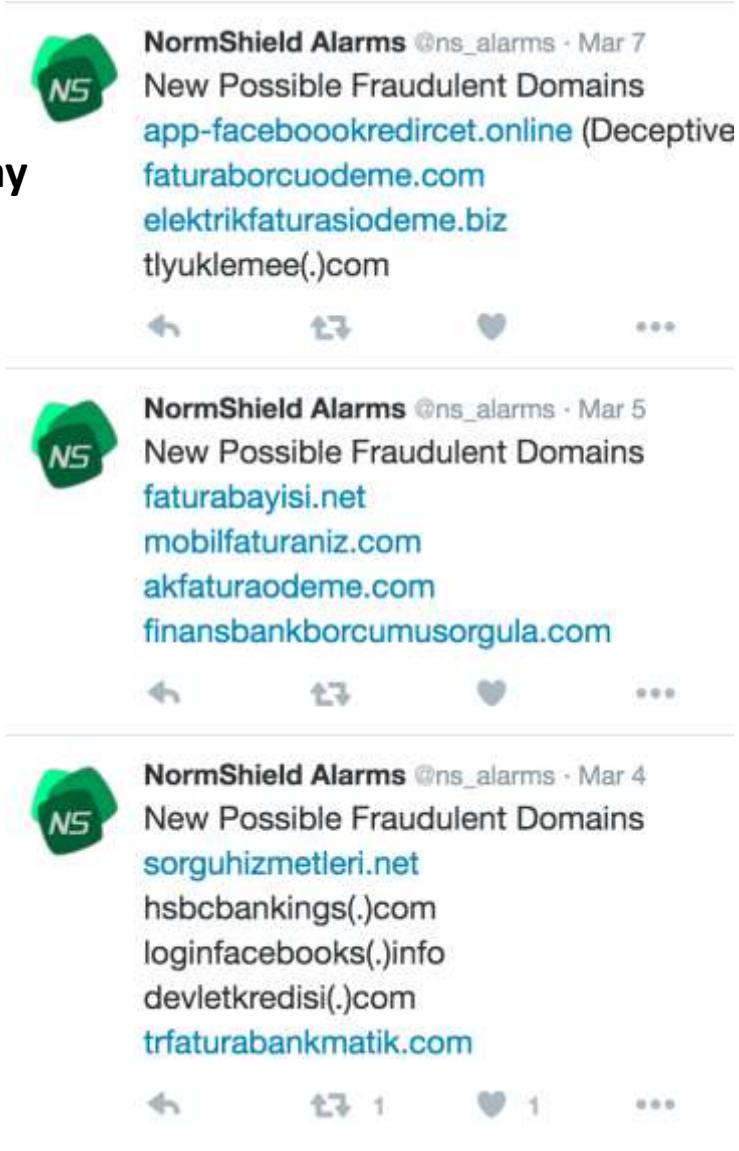
- **OSINT (free Sources)**
- Dell SecureWorks
- Verisign iDefense
- **Symantec Deepsight**
- McAfee Threat Intelligence
- **SANS/Whitelist/Blacklist**
- **CVEs CWEs, OSVDB (Vulns)**
- **iSight Partners**
- **ThreatStream**
- ATLAS
- **ThreatConnect**
- **Farsight**
- **Palo Alto Wildfire**
- **Crowdstrike**
- **AlienVault OTX**
- **RecordedFuture**
- **Team Cymru**
- **ISACs or US-CERT**
- **FireEye/Mandiant**
- Vorstack
- cyberUnited
- ThreatGrid
- **ZeroFox**
- **Norse Corporation**

Cyber Intelligence Dünyasında Sıradan Bir Gün

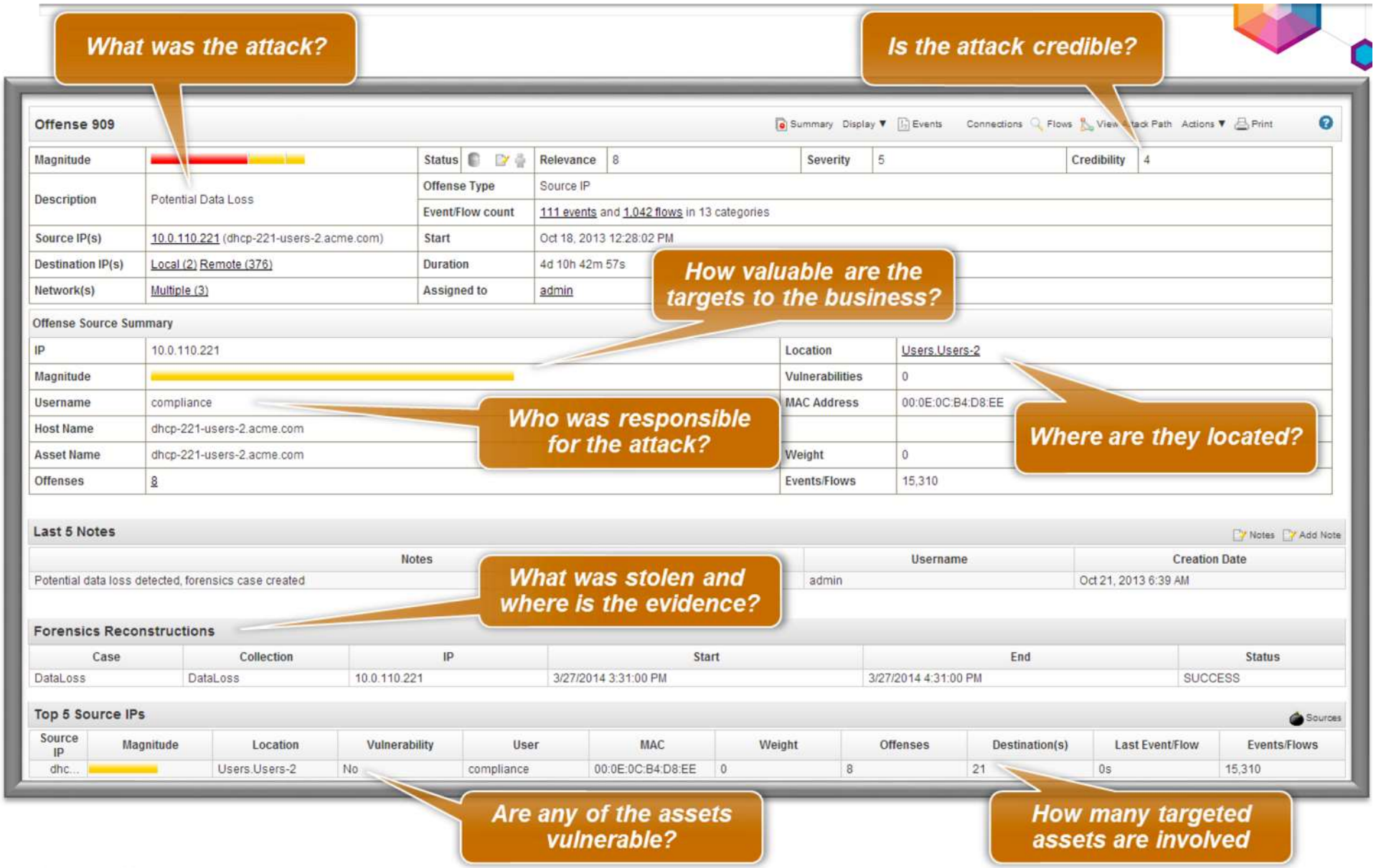




1000 USD / Day



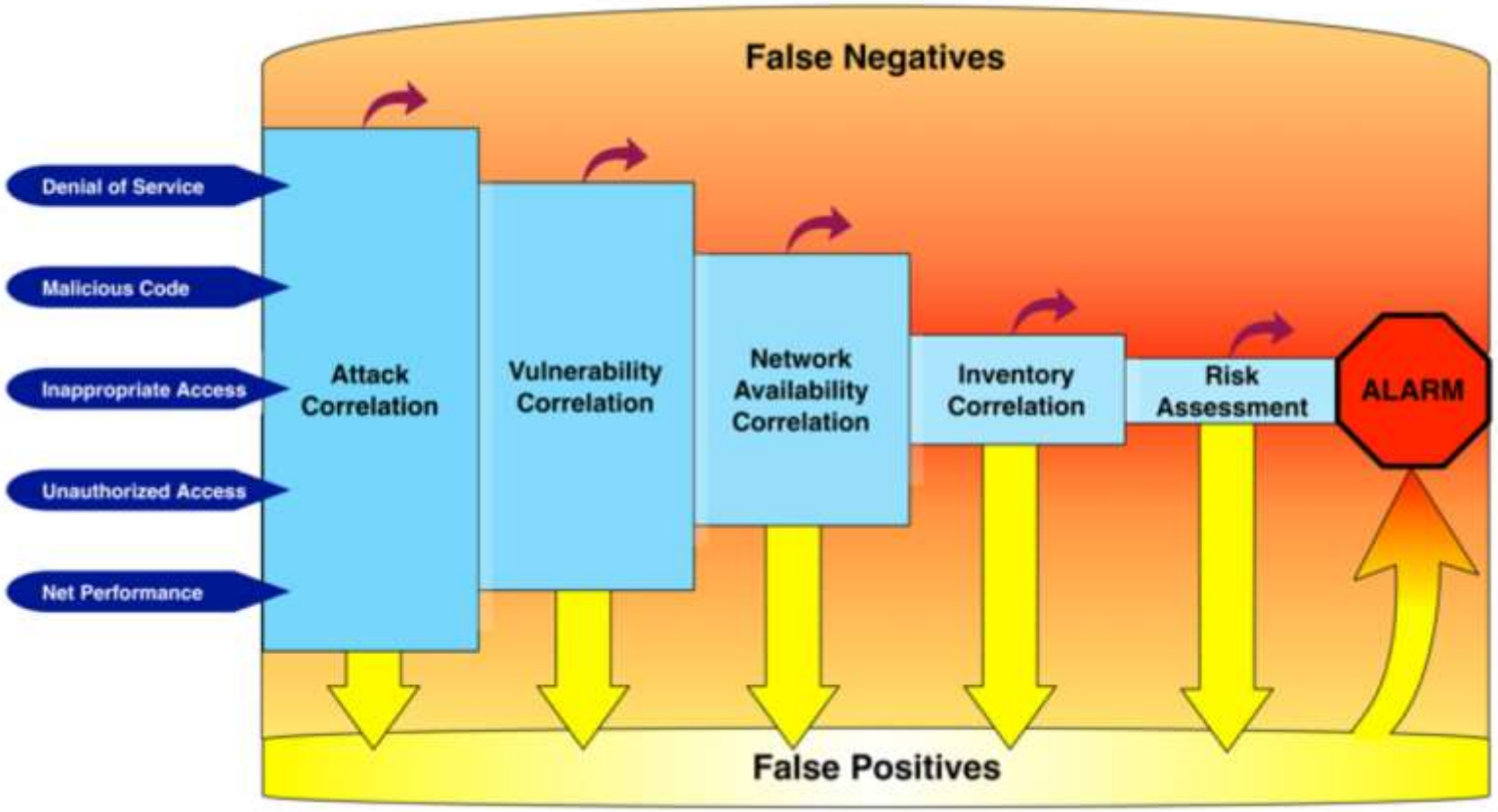
Örnek Log/Alarm İnceleme



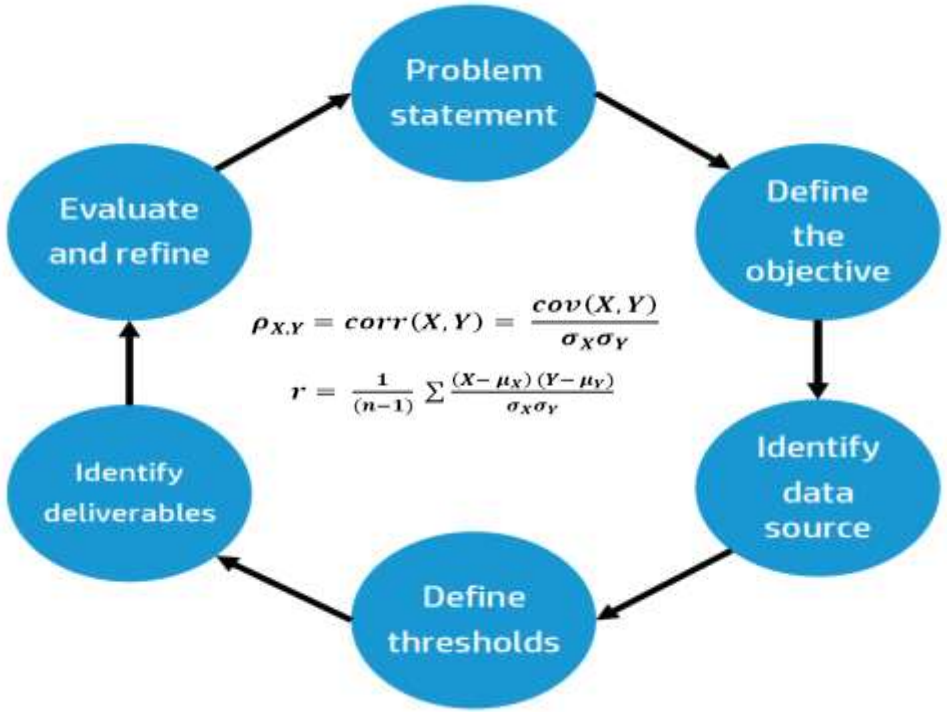
IBM Qradar

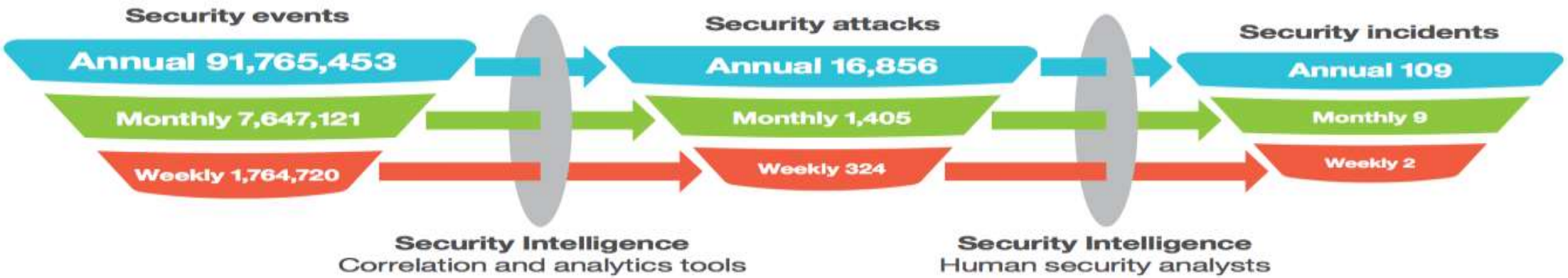
Korelasyon Kavramı ve Çeşitleri

- **Korelasyon**, olasılık kuramı ve istatistikte iki rassal değişken arasındaki doğrusal ilişkinin yönünü ve gücünü belirtir. Genel istatistiksel kullanımda korelasyon, bağımsızlık durumundan ne kadar uzaklaşıldığını gösterir.



Gelişmiş Korelasyon Kuralı Yazma





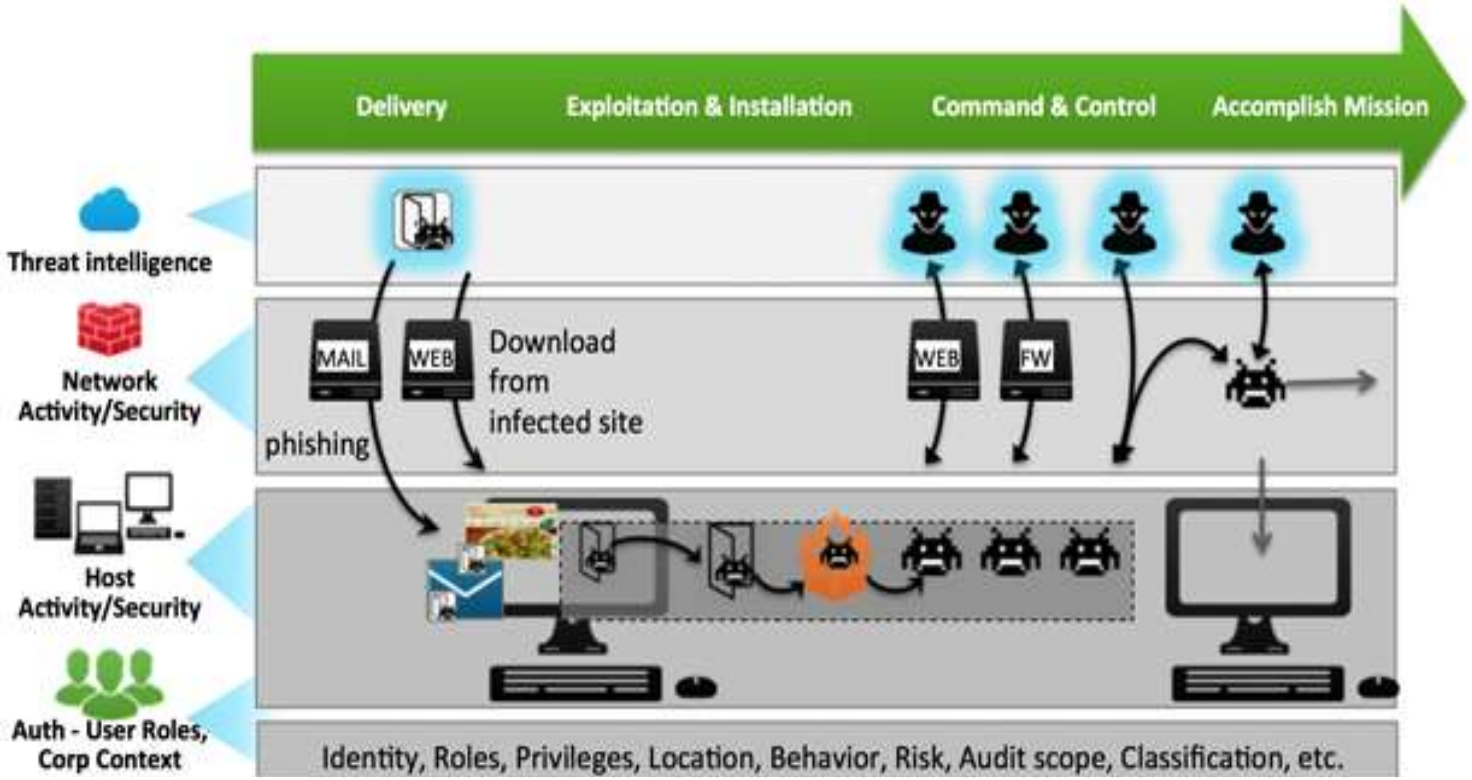
Kaynak:HP, proficio, Google

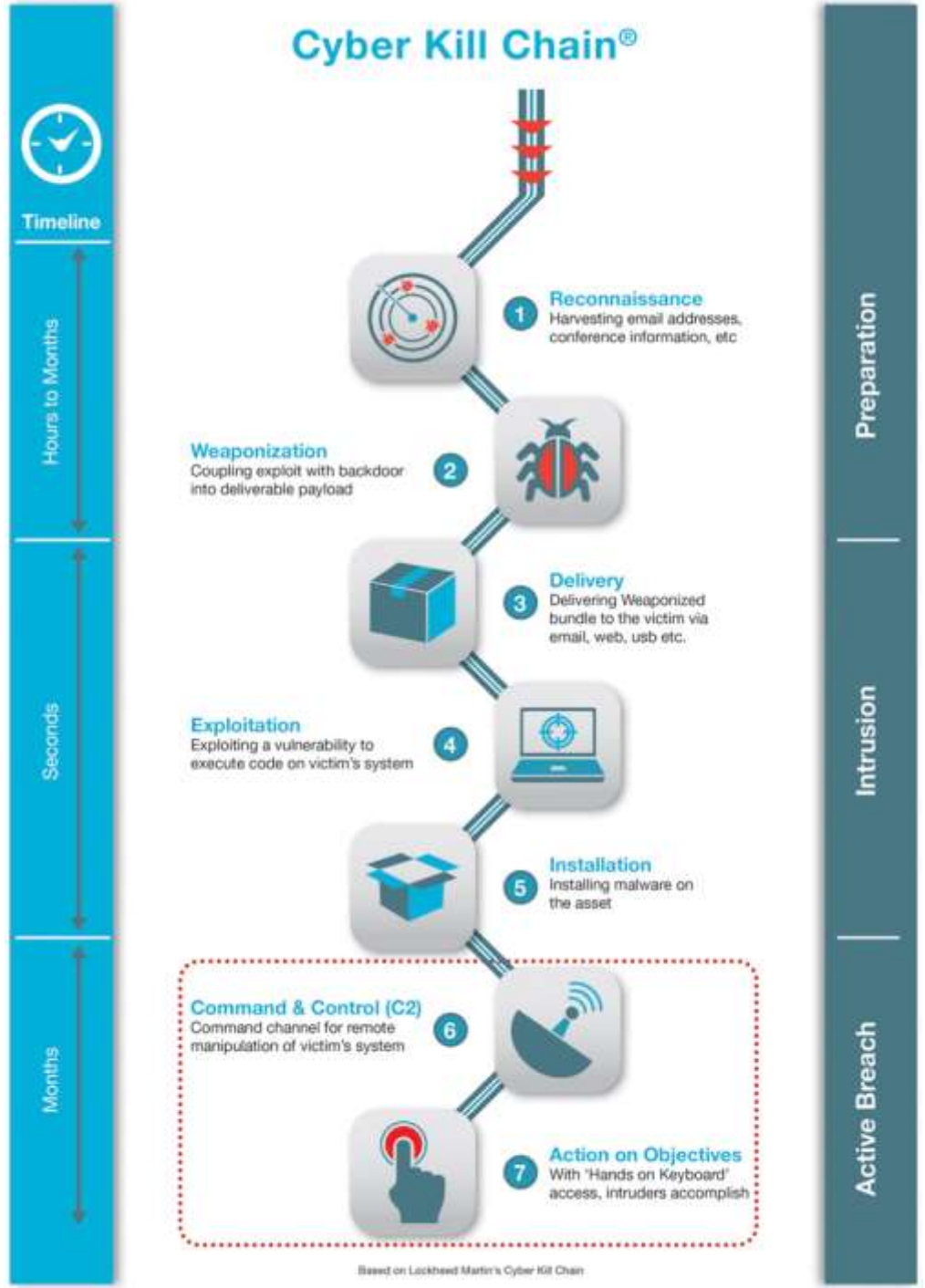
SOME Tatbikat/Siber Tehdit Simülasyonu

- Siber Güvenlik Tatbikat çalışması bir kurumun dış ve iç siber saldırgan gözüyle kurumdaki tüm güvenlik bileşenleri (çalışanlar dahil) gerçek hayattakine benzer bir saldırı simulasyonu ile ölçümüdür.

- Çalışma boyunca kurum icin yapılan tüm güvenlik yatırımlarının(Loglama, Antivirüs, IPS, Firewall, bilgilendirme vs) gerçek bir siber saldırı karşısında ne kadar işe yaradığı somut bulgularla ortaya çıkacaktır.

Cyber Kill Chain





Tatbikat Senaryoları İçerik

- Internete Açık Sistemler için Gerekli Senaryoların Denenmesi
- Web Sunuculara Yönelik Senaryoların Denenmesi ve Aksiyon Planı
- Endpoint Sistemlere (AV, APT, Mlwr) Yönelik Senaryo Denemeleri
- Veritabanı Sistemlerine Yönelik Senaryo Denemeleri
- LAN & DMZ Senaryolarının Denenmesi
- Windows Sistemlere Yönelik Senaryo Denemeleri
- Linux/UNIX/Embeddes Sistemlere Yönelik Senaryo Denemeleri
- Mail & SPAM & Exchange Sistemlere Yönelik Senaryo Denemeleri
- Network Altyapı Sistemlerine Yönelik Senaryo Denemeleri
- Firewall & IPS Sistemlere Yönelik Senaryo Denemeleri
- VPN & OWA Sistemlerine Yönelik Senaryo Denemeleri
- DLP & SIEM Sistemlerine Yönelik Senaryo Denemeleri

Açık Kaynak SIEM ve Tehdit Gözetleme

Neden Açık Kaynak Tehdit Gözetleme – Log/SIEM

- Ne istediğini bilenler için
- Genel korkular…

Türkiye’den örnek rakamlar…

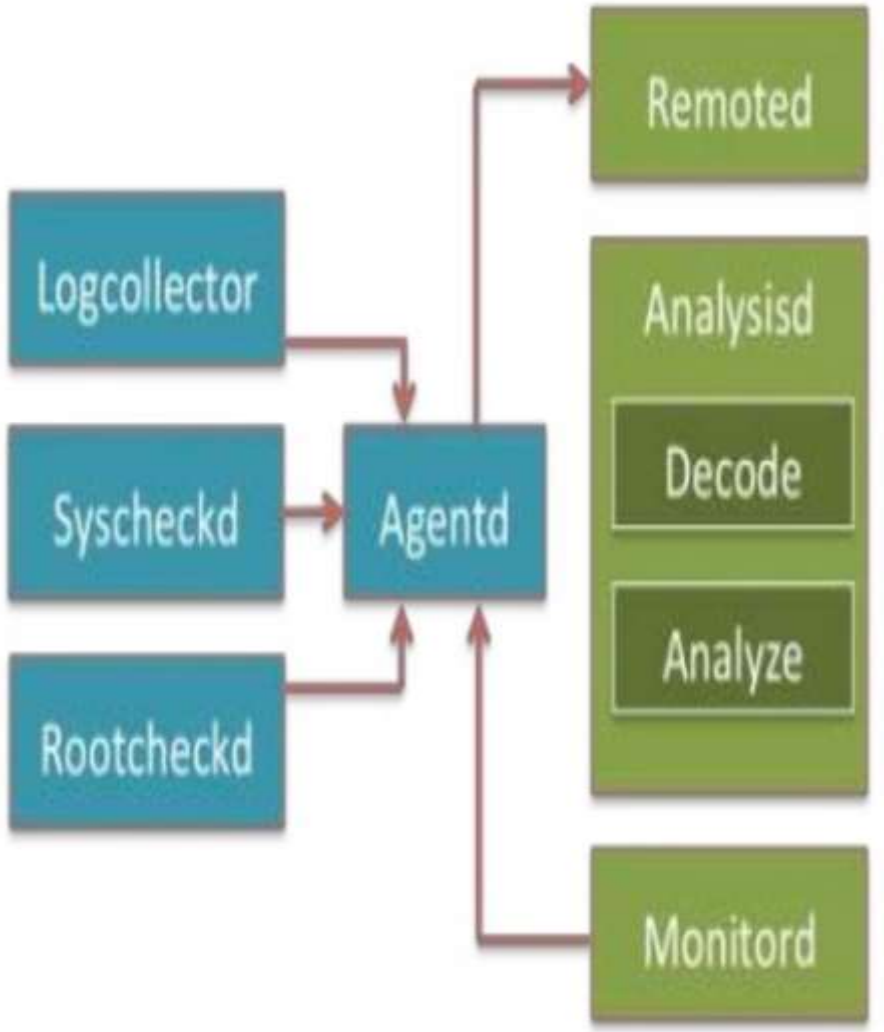
Tehdit Gözetleme Altyapı Bileşenleri

Host Tabanlı Log/Anomali Üretme-İletme-Toplama

- Kullanıcı bilgisayarları, sunucular ve doğrudan log gönderme yeteneğine sahip olmayan sistemler için ajan tabanlı (veya wmi vs benzeri) log anormallik tespiti
- Genellikle HIDS ya da LIDS olarak adlandırılır
  - En bilinen ve kullanılan açık kaynak örneği - OSSEC

OSSEC ile Neler Yapabiliriz?

- Windows sistemler için registry değişikliklerinin tespiti
- Sistemde yüklü olası rootkit ve benzeri programların tespiti (Signature based)
- Anlık alarm üretme
- Talebe göre otomatik engelleme özelliği (Active response)
- IP, domain karşılaştırma (Aktif Liste mantığı)
- Yeni log formatları ekleme
- İsteğe göre kural yazma
- …



```
<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.

```
<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.

```
<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.

```
<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.

OSSEC Ekran Görüntüleri - Alarm

OSSEC Notification - (pentest3) 85.95.242.68 - Alert level 12 OSSEC-BGA

OSSEC HIDS <bgaossec@bgasoc.bga.com.tr>
to omer.albayrak, me, cihat.isik

OSSEC HIDS Notification.
2016 Mar 27 07:36:17

Received From: (pentest3) 85.95.242.68->/var/log/auth.log
Rule: 40101 fired (level 12) -> "System user successfully logged to the system."
Portion of the log(s):

Mar 27 07:35:03 pentest3 su[24342]: + ??? root:nobody

--END OF NOTIFICATION

OSSEC HIDS Notification.
2016 Mar 27 07:36:17

Received From: (pentest3) 85.95.242.68->/var/log/auth.log
Rule: 40101 fired (level 12) -> "System user successfully logged to the system."
Portion of the log(s):

OSSEC Notification - bgasoc - Alert level 12 OSSEC-BGA x

OSSEC HIDS <bgaossec@bgasoc.bga.com.tr>
to omer.albayrak, me, cihat.isik

OSSEC HIDS Notification.
2016 Mar 26 03:10:44

Received From: bgasoc->/var/log/messages
Rule: 5108 fired (level 12) -> "System running out of memory. Availability of the system is in risk."
Portion of the log(s):

Mar 26 03:10:43 bgasoc kernel: Out of memory: Kill process 9334 (Suricata-Main) score 259 or sacrifice child

--END OF NOTIFICATION

OSSEC Notification - (web01.bilg.io) 52.18.50.18 - Alert level 10 OSSEC-BGA x

OSSEC HIDS <bgaossec@bgasoc.bga.com.tr> 11:51 AM (21 hours ago)
to omer.albayrak, me, cihat.isik

OSSEC HIDS Notification.
2016 Mar 26 11:51:24

Received From: (web01.bilg.io) 52.18.50.18->/var/log/nginx/access.log
Rule: 31154 fired (level 10) -> "Multiple XSS (Cross Site Scripting) attempts from same souce ip."
Portion of the log(s):

141.101.104.103 - - [26/Mar/2016:11:50:10 +0200] "GET /zt7tni6x.exe?<script>document.cookie=%22testmanz=8371;%22</script> HTTP/1.1" 301 184 "http://linuxakademi.com.tr/https://www.bilgio.com/zt7tni6x.exe?<script>document.cookie=%22testmanz=8371;%22</script>" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)" "31.169.69.37"
141.101.104.103 - - [26/Mar/2016:11:50:10 +0200] "GET /zt7tni6x.exe?<script>document.cookie=%22testmanz=8371;%22</script> HTTP/1.1" 301 184 "http://linuxakademi.com.tr/zt7tni6x.exe?<script>document.cookie=%22testmanz=8371;%22</script>" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)" "31.169.69.37"
141.101.104.103 - - [26/Mar/2016:11:50:10 +0200] "GET /zt7tni6x.cgi?<script>document.cookie=%22testmanz=8371;%22</script> HTTP/1.1" 301 184 "http://linuxakademi.com.tr/https://www.bilgio.com/zt7tni6x.cgi?<script>document.cookie=%22testmanz=8371;%22</script>" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)" "31.169.69.37"
141.101.104.103 - - [26/Mar/2016:11:50:10 +0200] "GET /zt7tni6x.cgi?<script>document.cookie=%22testmanz=8371;%22</script> HTTP/1.1" 301 184 "http://linuxakademi.com.tr/zt7tni6x.cgi?<script>document.cookie=%22testmanz=8371;%22</script>" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)" "31.169.69.37"
141.101.104.103 - - [26/Mar/2016:11:50:09 +0200] "GET /zt7tni6x.pl?<script>document.cookie=%22testmanz=8371;%22</script> HTTP/1.1" 301 184 "http://linuxakademi.com.tr/https://www.bilgio.com/zt7tni6x.pl?<script>document.cookie=%22testmanz=8371;%22</script>" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)" "31.169.69.37"
141.101.104.103 - - [26/Mar/2016:11:50:09 +0200] "GET /zt7tni6x.pl?<script>document.cookie=%22testmanz=8371;%22</script> HTTP/1.1" 301 184 "http://linuxakademi.com.tr/zt7tni6x.pl?<script>document.cookie=%22testmanz=8371;%22</script>" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)" "31.169.69.37"

OSSEC Notification - (pentest3) 85.95.242.68 - Alert level 7 OSSEC-BGA x

OSSEC HIDS <bgaossec@bgasoc.bga.com.tr>
to omer.albayrak, me, cihat.isik

OSSEC HIDS Notification.
2016 Mar 10 21:05:25

Received From: (pentest3) 85.95.242.68->netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort
Rule: 533 fired (level 7) -> "Listened ports status (netstat) changed (new port opened or closed)."
Portion of the log(s):

ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':
tcp 0 0 0.0.0.0:4443 0.0.0.0:* LISTEN
tcp6 0 0 :::4443 :::* LISTEN
tcp6 0 0 :::80 :::* LISTEN
Previous output:
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':
tcp 0 0 0.0.0.0:4443 0.0.0.0:* LISTEN
tcp6 0 0 :::4443 :::* LISTEN

File Integrity Module

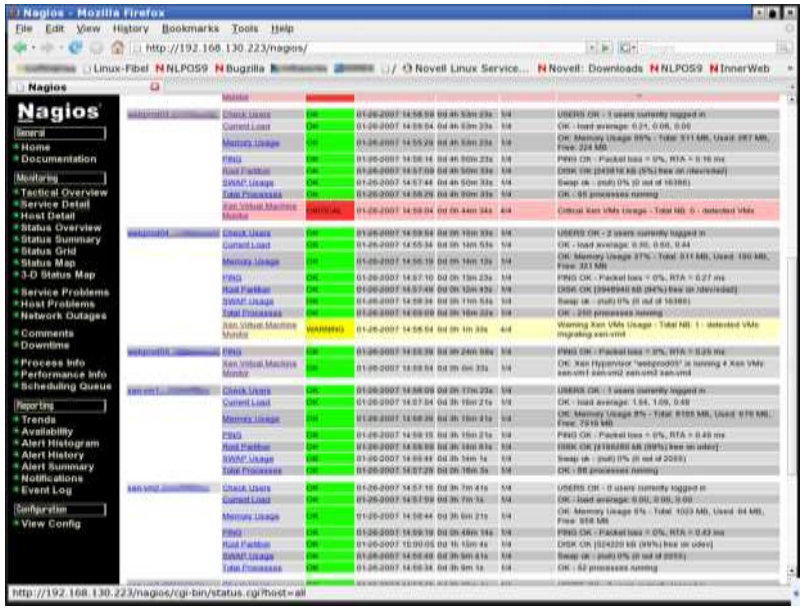
- Dosya bütünlük doğrulama neden ihtiyaç duyulur?

/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>
```

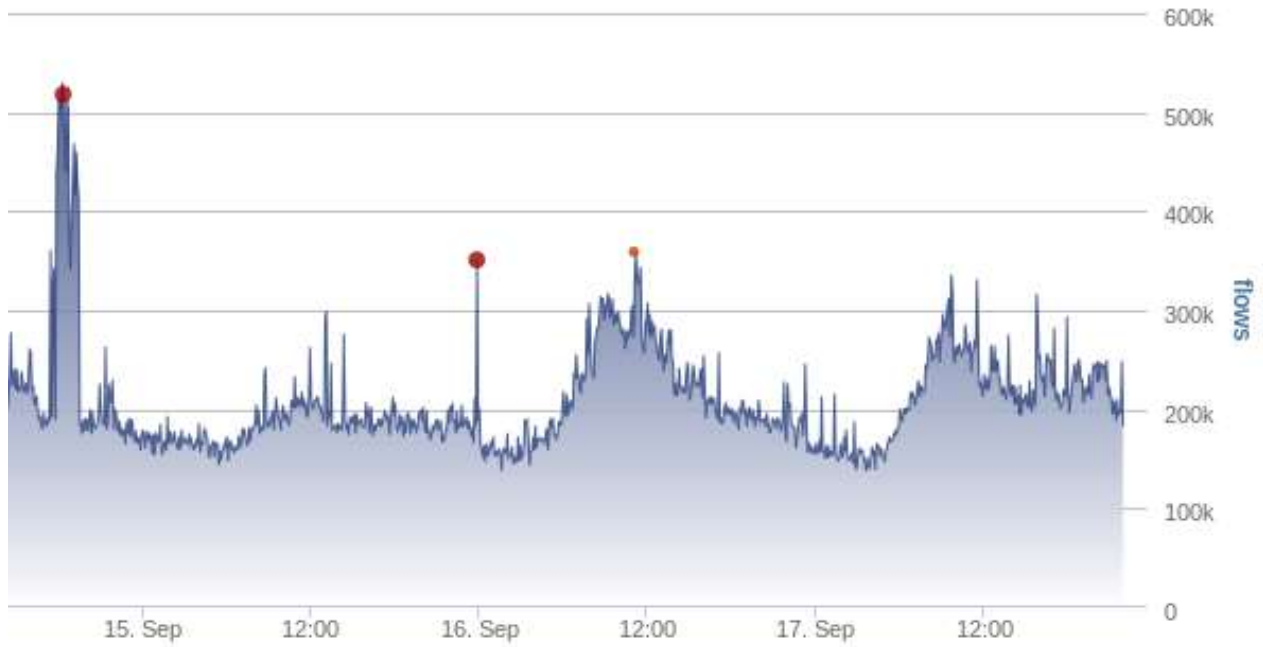
Sistem Durumu Gözetleme – Unutulan Bileşen!

- 360 derece alan hakimiyeti sağlamak için gerekli en temel bileşenlerden biri sistemlerin anlık durumlarıdır
  - Disk durumu
  - CPU , RAM durumu
  - Ağ trafiğindeki dalgalanmalar
  - Çalışan processlerin durumu…
- Sistemlerden gelecek bu bilgi sayesinde SIEM korelasyonları daha gerçekçi ve sağlıklı olacaktır.



Ağ Seviyesi Anormallik Tespiti

- Belirlenecek anormalliklerin otomatik olarak tespit edilmesi
  - Anormallik kavramı tanımı
- Zaman tabanlı anormallikler
- Veri tabanlı anormallikler
- Hedef, kaynak tabanlı anormallikler
- Genellikle Netflow tercih edilir



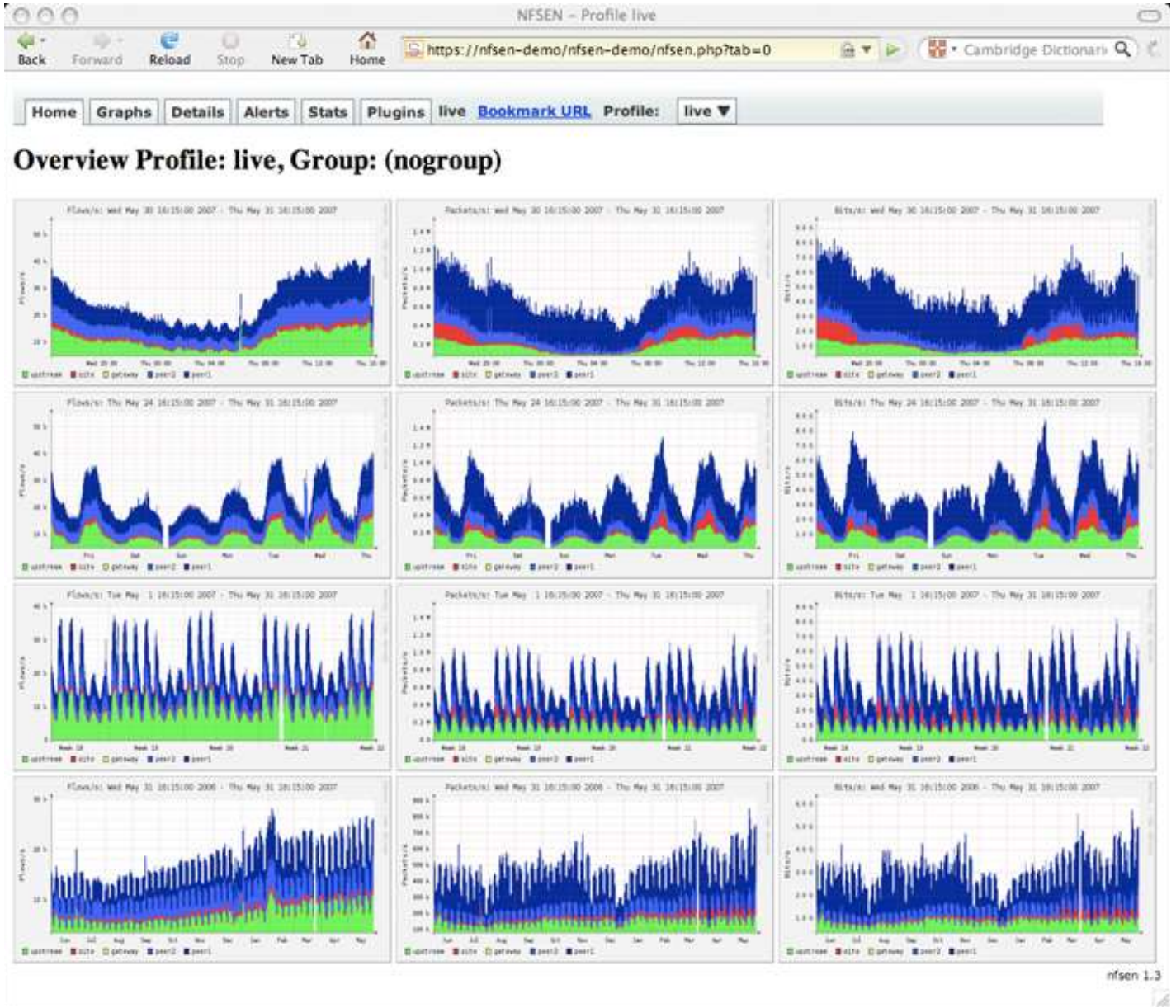
Ağa Yeni Bağlanan Sistemlerin Otomatik Tespiti

- PradS- Passive Real-Time Asset Detection System (PRADS)

10.43.2.181,0,54354,6,SYN,[65535:64:1:64:M1460,N,W2,N,N,T,S,E,E:P:Mac OS:iPhone OS 3.1.3 (UC) ethernet/modem:uptime:1574hrs],0,1300882012
10.43.2.181,0,0,0,ARP (Apple),C8:BC:C8:48:65:CA,0,1300882017

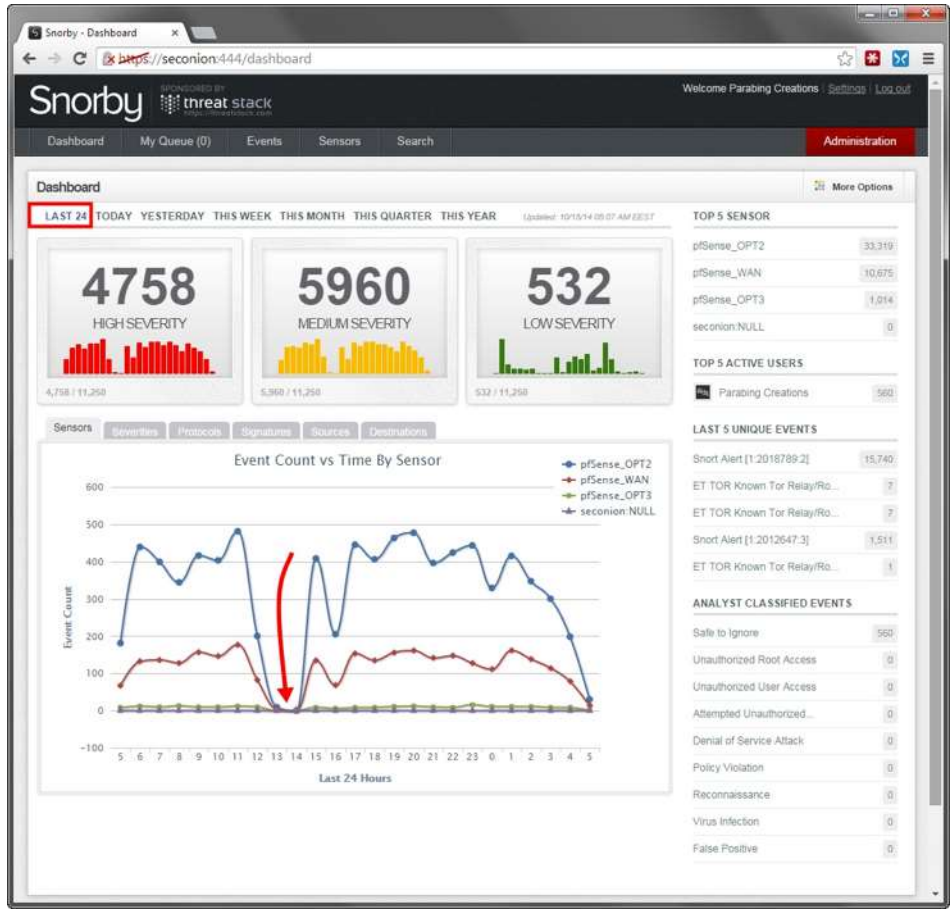
Netflow Kullanarak Ağda Anormallik Tespiti #Nfsen

- Payload Anomaly Detection
- Protocol Anomaly: MAC Spoofing
- Protocol Anomaly: IP Spoofing
- Protocol Anomaly: TCP/UDP Fanout
- Protocol Anomaly: IP Fanout
- Protocol Anomaly: Duplicate IP
- Protocol Anomaly: Duplicate MAC
- Virus Detection
- Bandwidth Anomaly Detection
- Connection Rate Detection



Ağ Tehdit Gözetleme Sistemi – Snort / Suricata

- “Gelişmiş” ağ tabanlı tehdit algılama, saldırı tespit, anormallik tespit, ddos tespit, …. Tespit ve engelleme aracı
- Snort->Sourcefire->Cisco
- 35.000 aktif saldırı imzası
- Basit kural dili ile saldırı imzası tanımlama kolaylığı
- Snorby benzeri arabirimlerle kolay analiz ve yönetim(alarm)
- ELK stack ile doğal entegrasyon
- Eklentilerle ML kabiliyeti



Suricata-vs-Snort

Param	Suricata	Snort
IPS feature	optional while compiling (--enable-nfqueue)	Snort_inline or snort used with -Q option
Rules	• VRT::Snort rules • EmergingThreats rules	• VRT::Snort rules • SO rules • EmergingThreats rules
Threads	Multi-thread	Single-thread
Ease of install	Not available from packages. Manual installation.	Relatively straightforward. Installation also available from packages.
Documentation	Few resources on the Internet	Well documented on the official website and over the Internet
Event logging	Flat file, database, unified2 logs for barnyard	
IPv6 support	Fully supported	Supported when compiled with --enable-ipv6 option.
Capture accelerators	PF_RING, packet capture accelerator	None, use of libpcap
Configuration file	suricata.yaml, classification.config, reference.config, threshold.config	snort.conf, threshold.conf
Offline analysis (pcap file)	yes	
Frontends	Sguil, Aanval, BASE, FPCGUI (Full Packet Capture GUI), Snortsnarf	

```
#
alert udp !$DNS_SERVERS any -> $DNS_SERVERS 53 (msg:"ET CURRENT_EVENTS Wordpress possible Malicious DNS-Requests -
flickr.com.* "; content:"|05|flickr|03|com"; nocase; content:!"|00|"; within:1; reference:url,markmaunder.com/2011/
zero-day-vulnerability-in-many-wordpress-themes/; reference:url,www.us-cert.gov/current/
index.html#wordpress_themes_vulnerability; reference:url,blog.sucuri.net/2011/08/timthumb-security-vulnerability-
list-of-themes-including-it.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SucuriSecurity+%28Sucuri
+Security%29; classtype:web-application-attack; sid:2013353; rev:3;)

#
alert udp !$DNS_SERVERS any -> $DNS_SERVERS 53 (msg:"ET CURRENT_EVENTS Wordpress possible Malicious DNS-Requests -
picasa.com.* "; content:"|06|picasa|03|com"; nocase; content:!"|00|"; within:1; reference:url,markmaunder.com/2011/
zero-day-vulnerability-in-many-wordpress-themes/; reference:url,www.us-cert.gov/current/
index.html#wordpress_themes_vulnerability; reference:url,blog.sucuri.net/2011/08/timthumb-security-vulnerability-
list-of-themes-including-it.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SucuriSecurity+%28Sucuri
+Security%29; classtype:web-application-attack; sid:2013354; rev:3;)

#
```

```
#
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET DNS DNS Query for vpnoverdns - indicates DNS tunnelling";
content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|03|tun|10|vpnoverdns|03|com|00|";
fast_pattern; nocase; distance:0; reference:url,osint.bambenekconsulting.com/manual/vpnoverdns.txt; classtype:bad-
unknown; sid:2018438; rev:2;)

#
alert udp any 53 -> $HOME_NET any (msg:"ET DNS Reply Sinkhole FBI Zeus P2P 1 - 142.0.36.234"; content:"|00 01 00
01|"; content:"|00 04 8e 00 24 ea|"; distance:4; within:6; classtype:trojan-activity; sid:2018517; rev:1;)

#
```

PDF Dosyalarını Kaydetme, Uyarma…

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:”pdf upload claimed, but not pdf”; flow:established,to_server; content:”POST”; http_method; fileext:”pdf”; filemagic:!”PDF document”; filestore; sid:1; rev:1;)

alert http any any -> any any (msg:"FILE PDF file claimed"; fileext:"pdf"; filestore; sid:2; rev:1;)

alert http any any -> any any (msg:"FILE pdf detected"; filemagic:"PDF document"; filestore; sid:3; rev:1;)

BRO IDS

- Ağ trafiğinde dolaşan dosyaların hash değerlerini alabilir
- Ağ trafiğindeki dosyaların bir kopyasını kayıt edebilir
- Ağ seviyesi DLP olarak kullanılabilir
- Ağ seviyesi ve protokol anormallikleri için kullanılabilir
- Pasif DNS trafiği inceleme ve alarm amaçlı kullanılabilir

100G Intrusion Detection

After extensive evaluation, deployment and testing, the Berkeley Lab Cyber Security Team brought our 10
2015. We created the following technical document to help other security teams and interested individuals
used to create our monitoring system.

100G Intrusion Detection, Rev. 1.0, published August 2015

Tehdit İstihbaratı Bilgisi Kullanımı

- Günümüz siber güvenlik camiası için en değerli ve sıcak konularından biri
- Kara liste->IP repütasyonu->Tehdit istihbaratı
- Her popüler kavram gibi hatalı kullanımı doğru kullanımından fazla
- AntiSpam dünyasında çok uzun süredir aktif olarak kullanımda
- Örnek kullanım: Cryptolocker saldırıları nasıl erkenden tespit edilir?

Maltrail

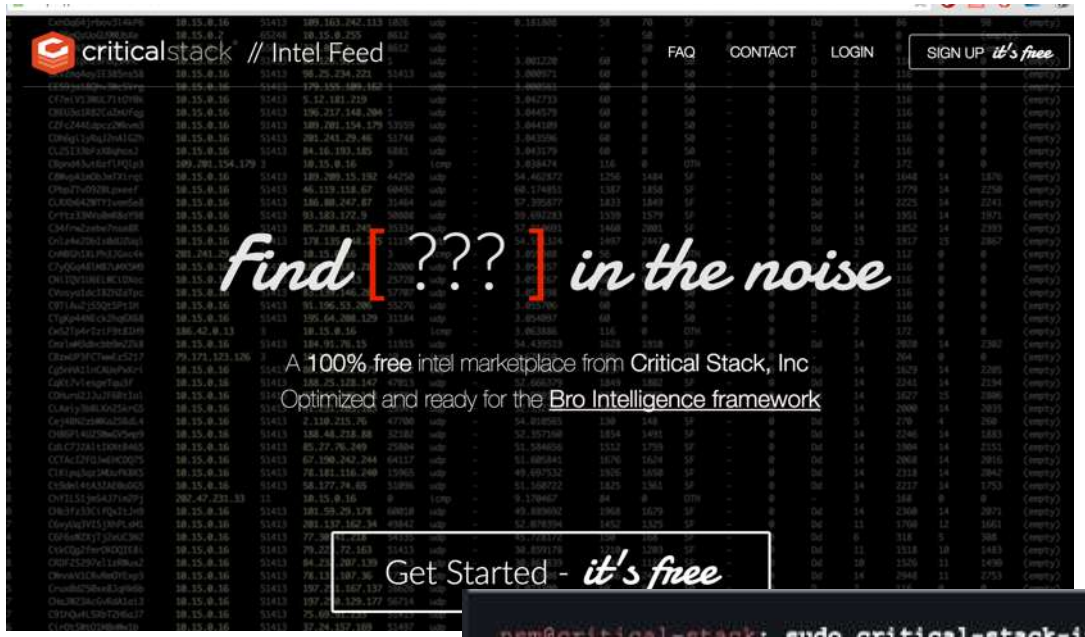
- Maltrail-Malicious traffic detection system

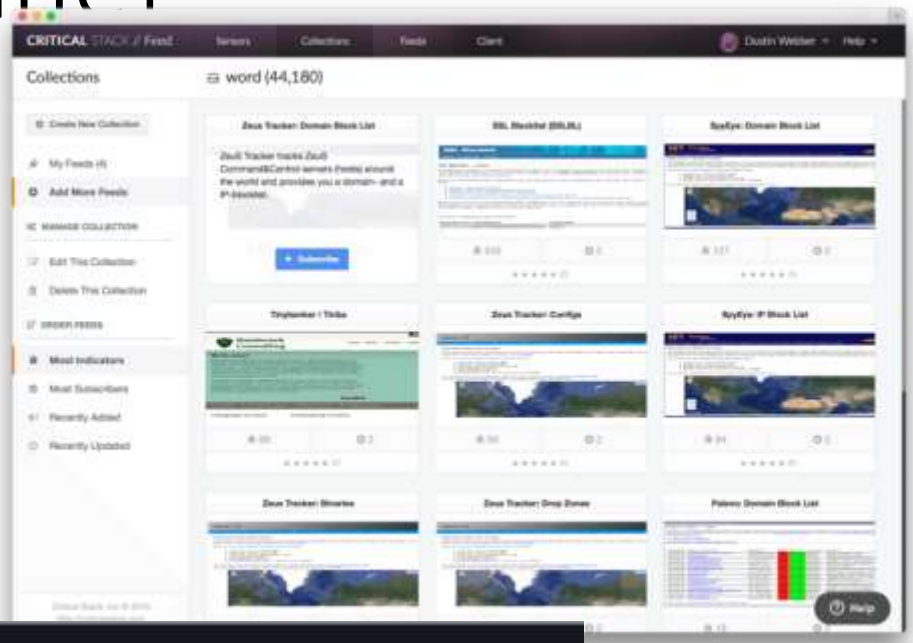
- Belirli merkezlerden sunulan ip, domain, url reputasyon verilerini çekerek anlık ağ trafiği ile karşılaştırıp rapor sunar

- Kolay kurulum & kullanım

alienvault, autoshun, badips, bambenekconsultingc2dns, bambenekconsultingc2ip, bambenekconsultingdga, bitcoinnodes, blocklist, botscout, bruteforceblocker, ciarmy, cruzit, cybercrimetracker, deepviz, dragonresearchgroupssh, dragonresearchgroupvnc, dshielddns, dshieldip, emergingthreatsbot, emergingthreatscip, emergingthreatsdns, feodotrackerdns, malwaredomainlist, malwaredomains, malwarepatrol, maxmind, myip, nothink, openbl, openphish, packetmailcarisirt, packetmailramnode, palevotracker, policeman, proxylists, proxyrss, proxy, ransomwaretrackerdns, ransomwaretrackerip, ransomwaretrackerurl, riproxies, rutgers, sblam, securityresearch, snort, socksproxy, sslipbl, sslproxies, torproject, torstatus, turris, urlvir, voipbl, vxvault, zeustrackerdns, zeustrackerip, zeustrackermonitor, zeustrackerurl, etc.

Intel Critical Stack Kullanımı [Offline]



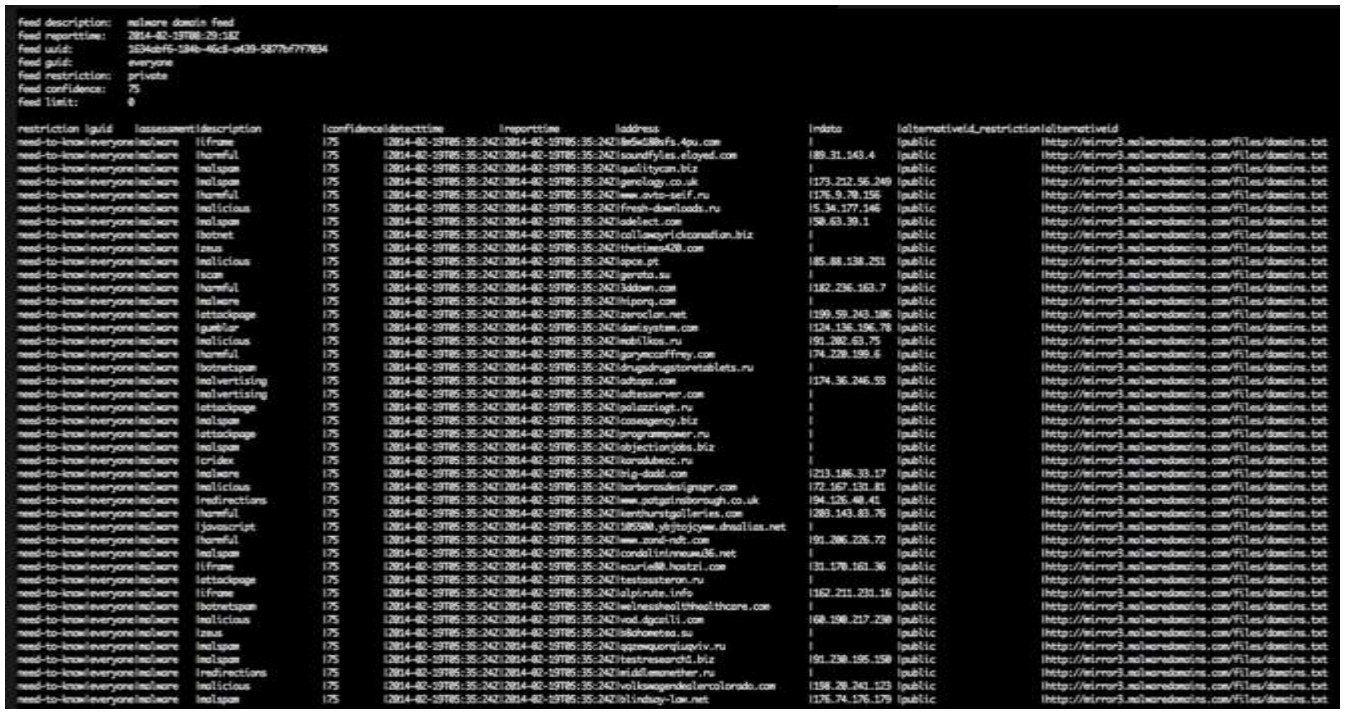


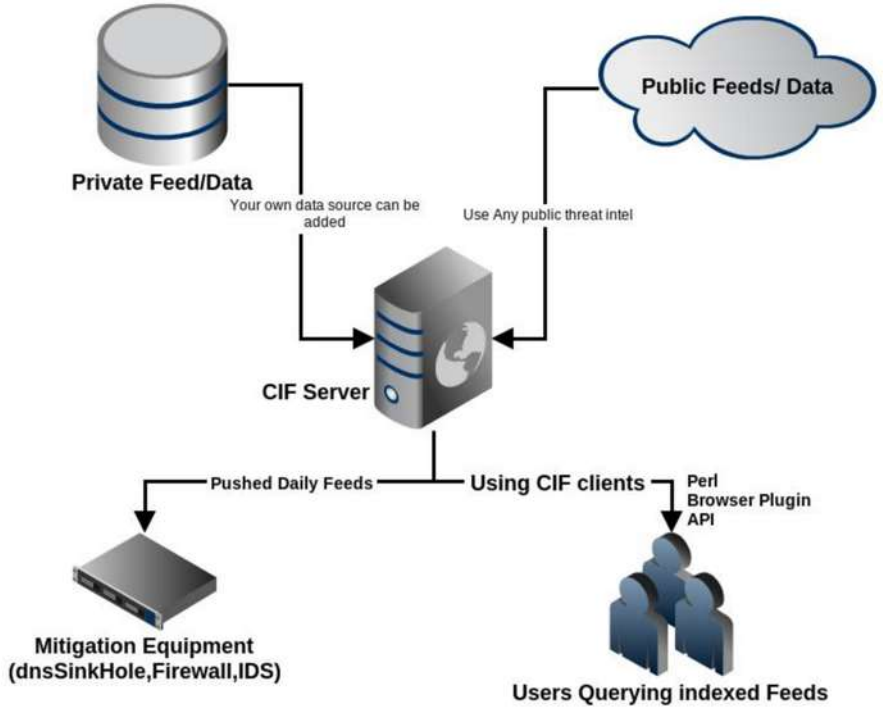

```
nsm@critical-stack: sudo critical-stack-intel api 12345-6789-101112
nsm@critical-stack: sudo critical-stack-intel fetch run
2015/01/12 11:35:39 Fetching feed subscriptions.
2015/01/12 11:35:39   * critical-stack-intel-1-Matsnu-Botnet.bro.dat
2015/01/12 11:35:40   * critical-stack-intel-2-C-Cs-IPs-Domains.bro.dat
2015/01/12 11:35:40   * critical-stack-intel-3-Cryptolocker.bro.dat
2015/01/12 11:35:40   * critical-stack-intel-4-Post-Tovar-GameOver-Zeus.bro.dat
2015/01/12 11:35:40   * critical-stack-intel-5-Tinybanker---Tinba.bro.dat
2015/01/12 11:35:40   * critical-stack-intel-6-PushDo-Malware.bro.dat
2015/01/12 11:35:40   * critical-stack-intel-7-Known-Tor-Exit-Nodes.bro.dat
2015/01/12 11:35:40   * critical-stack-intel-8-Cyber-Crime-Tracker.bro.dat
2015/01/12 11:35:40   * critical-stack-intel-9-Zeus-Tracker--Configs.bro.dat
2015/01/12 11:35:41   * critical-stack-intel-17-SpyEye--Domain-Block-List.bro.dat
2015/01/12 11:35:42   * critical-stack-intel-18-PhishTank-Intel-Feed-(Verified).bro.dat
2015/01/12 11:35:42   * critical-stack-intel-19-Abuse-Reporting-and-Blacklisting.bro.dat
2015/01/12 11:35:42 Creating master file: master-public.bro.dat
2015/01/12 11:35:42 Master file created successfully.
2015/01/12 11:35:42 Intel files located at: /opt/critical-stack/frameworks/intel
2015/01/12 11:35:42 API Requests Remaining: 75 of 100
nsm@critical-stack:
```

Bro &CIF Kullanarak CTI Entegrasyonu

@load frameworks/intel/seen @load frameworks/intel/do_notice @load policy/integration/collective-intel

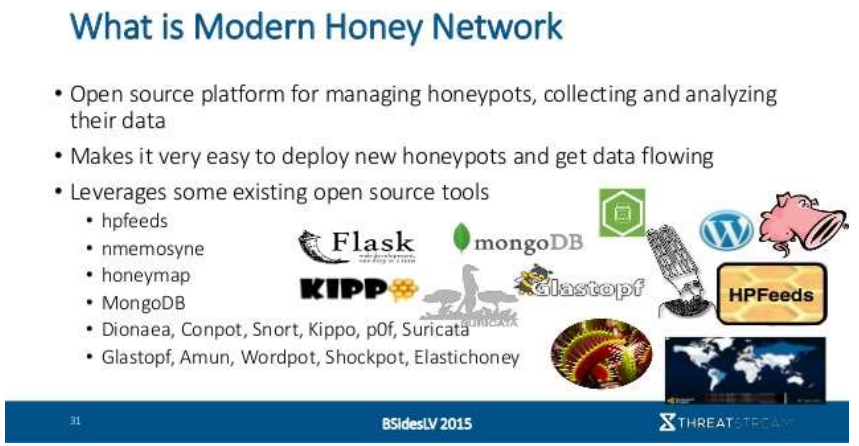
```
$ cif -q domain/malware -c 75 -p bro > domain-malware.intel
```

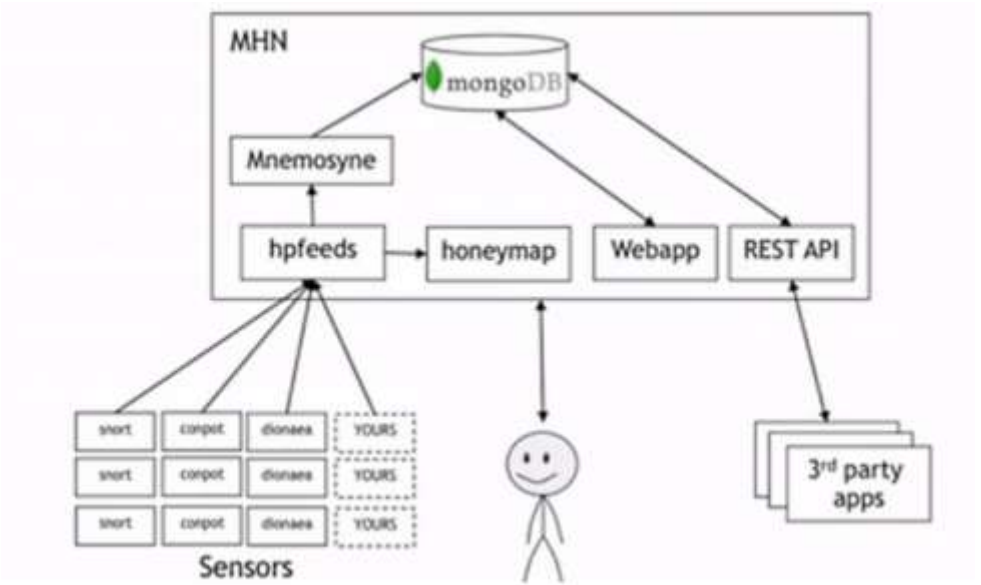




Tuzak Sistemlerin Aktif Kullanımı

- Özellikle kontrolü zor, dağıtık ve büyük ağlarda şüpheli durumları, sistemleri tespit etmek için kullanılır
  - Iç sensörler
  - Dış sensörler
- Günümüzde Siber Tehdit İstihbaratı çalışmalarının vazgeçilmez bileşenlerindendir
- Tehdit gözetleme altyapısında mutlaka farklı amaçlar için birden fazla HP kurulumu önerilmektedir.
- MHN kullanarak fazla uğraşıya gerek kalmadan birden fazla HP kurulumu otomatik olarak sağlanabilir.



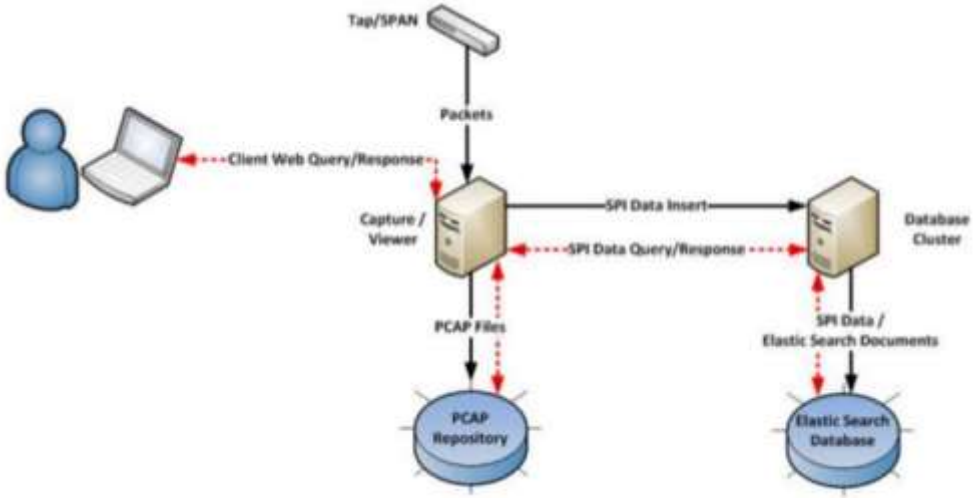


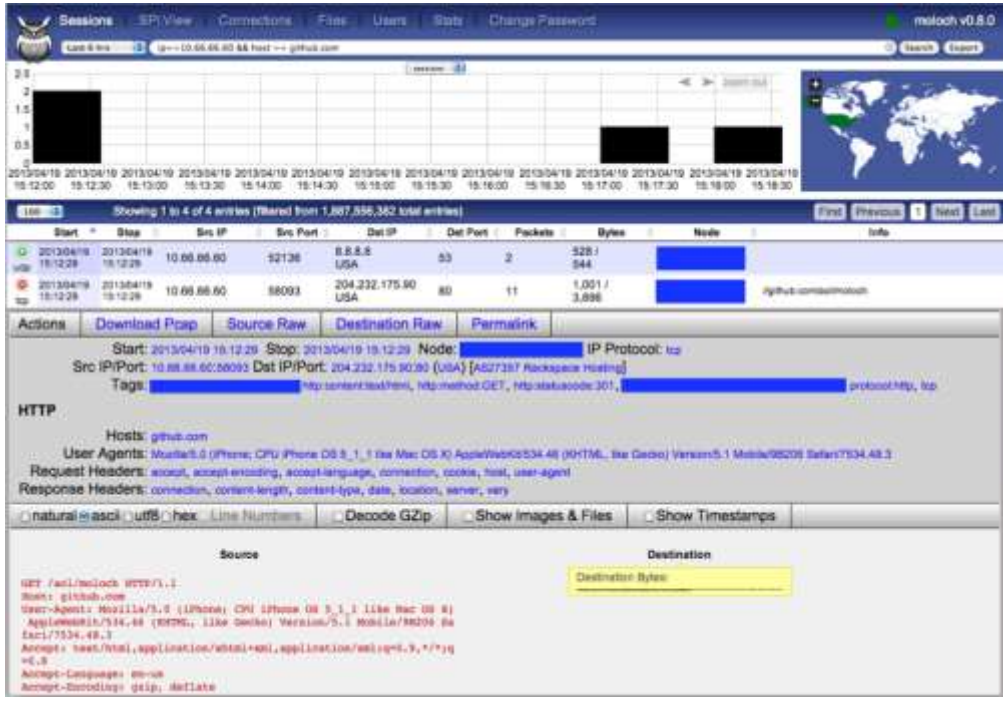
Ağ Trafiğini İnceleme Amaçlı Kayıt Etme #FPC

- Gerçekleşen ya da şüphelenilen bir olayın geriye doğru analizinde mutlak ihtiyaç duyulan bileşen
  - Anlık ağ trafiği analizi
  - Geriye yönelik araştırma (forensic, incident response vs)
- CCTV benzeri bir yapı sunar
- Hassas kurumlarda hassas sistemler için mutlaka kullanılmalı
- Göreceli olarak maliyetli bir çalışma
  - Disk maliyetleri 1 Gbps hat için aylık 180 TB
- OpenFPC ve Moloch kullanarak gerçekleştirilebilir

Moloch Kullanarak Tüm Trafiği Kayıt Altına Alma

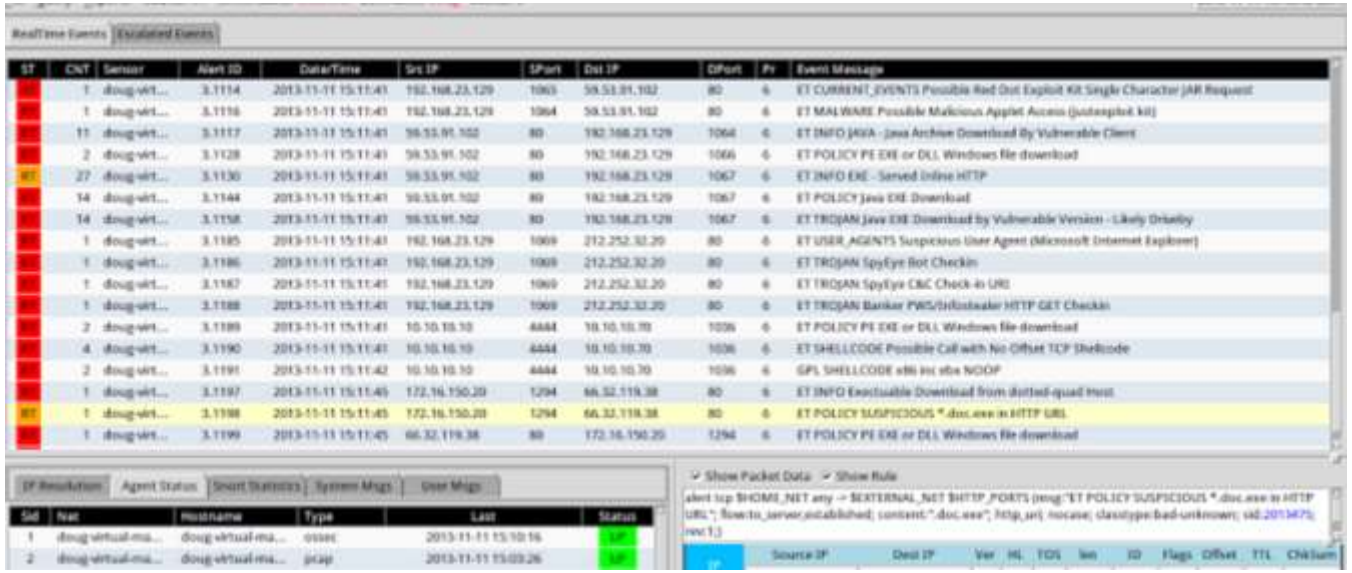
- AOL tarafından geliştirilmiş bir yazılım
- Kendi geliştirmek istediğiniz arabirimler için WEB API sunmaktadır
- Ana Bileşenler:
  - Capture (libNids)
  - Database (ElasticSearch based)
  - Viewer (NodeJs based)





SecurityOnion Dağıtımı

- Tüm bu anlatılan açık kaynak kodlu uygulamaların kurulumu, yapılandırması ve entegrasyonu işe yeni başlayanlar için zordur
- SO, bu konuda hızlıca başlamak isteyenler için geliştirimiş bir NSM dağıtımıdır.
- İndir, Çalıştır, Kur mantığı
- Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMine …

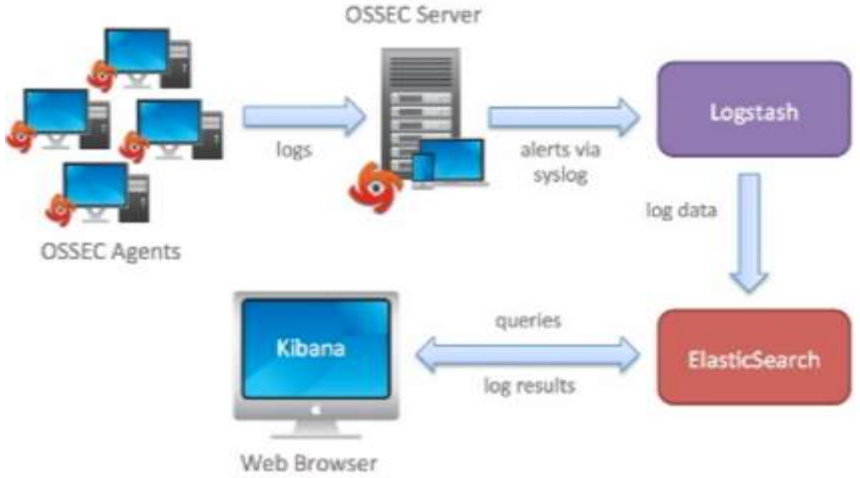


Logları Toplamak ve Yönetmek - ELK Ailesi

- ElasticSearch:> Esnek, güçlü açık kaynak kodlu dağıtık, gerçek zamanlı bir arama ve analitik motoru(Veriyi düzenleyerek, anlamlı hale getirerek depoladığımız alan)

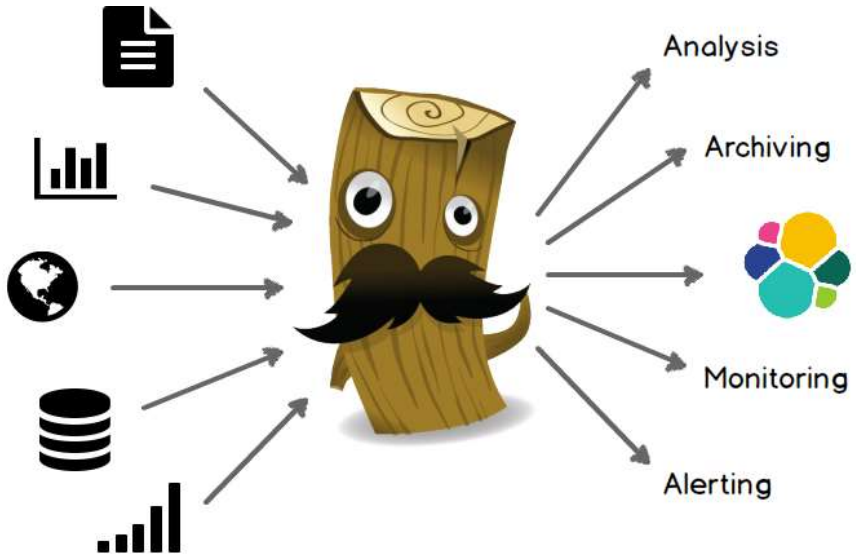
- Logstash:> Logları merkezi olarak toplamak ve anlamlandırmak için kullanılan bileşen

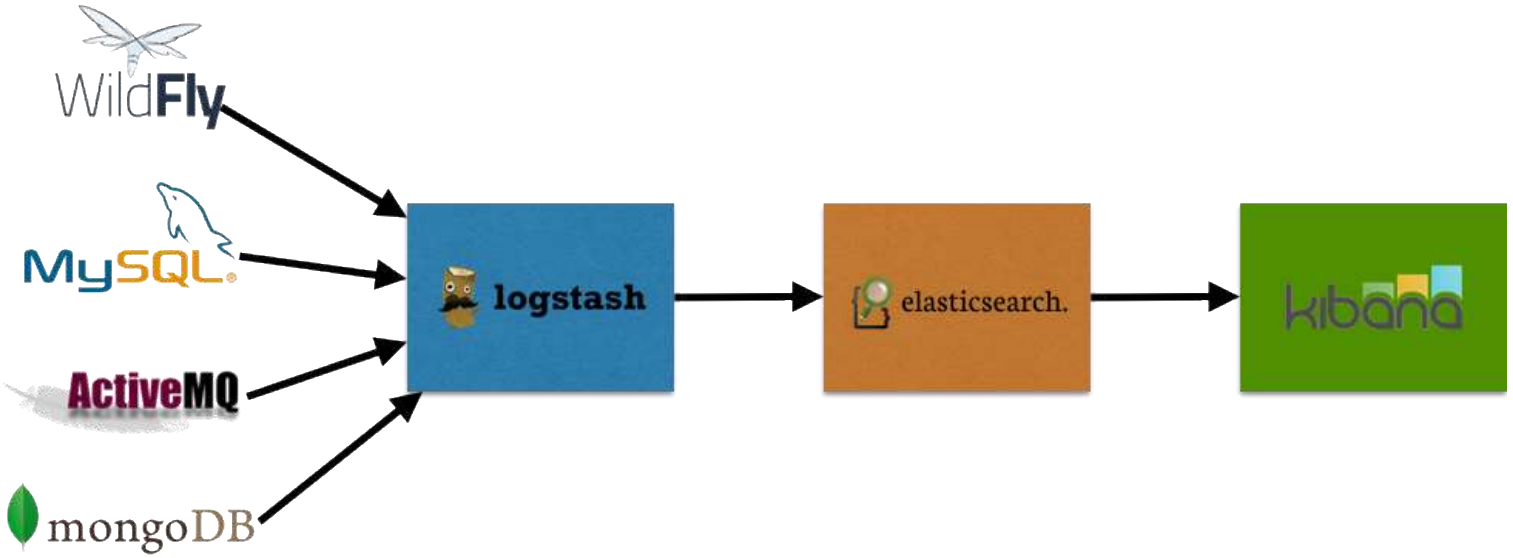
- Kibana:> ElasticSearch için veri görselleştirme paneli (Ön yüz)



Toplama ve Anlamlandırma Bileşeni - Logstash

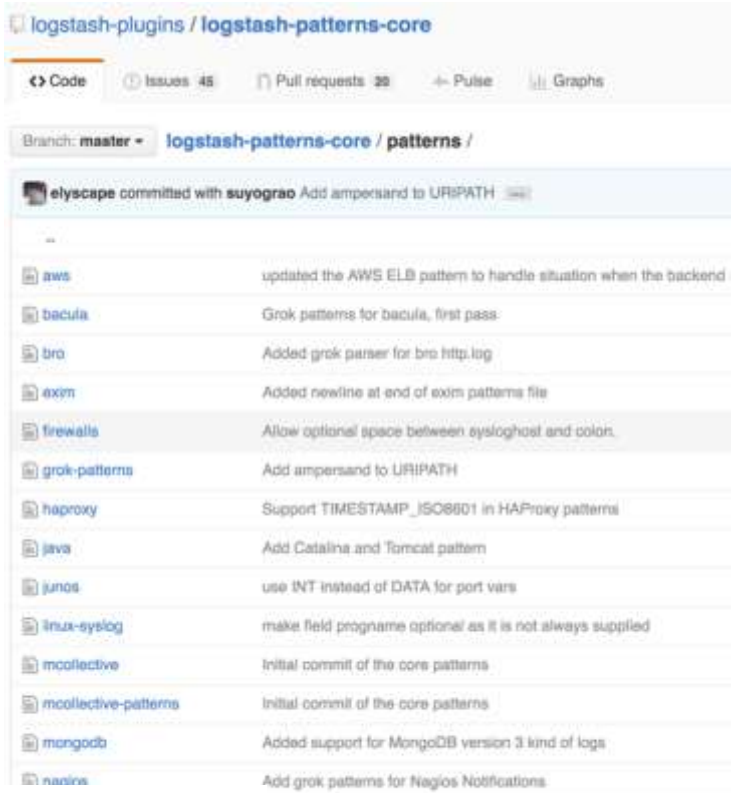
- Collect-Parse-Store/Forward
- Bir Olay'ın Yaşam Döngüsü
  - Input->Filter->Output->Codec
  - INPUT(File, syslog, redis …)





Parsing

- Grok eklentisi kullanarak anlamsız(!) log satırlarının aranabilir hale getirmek.



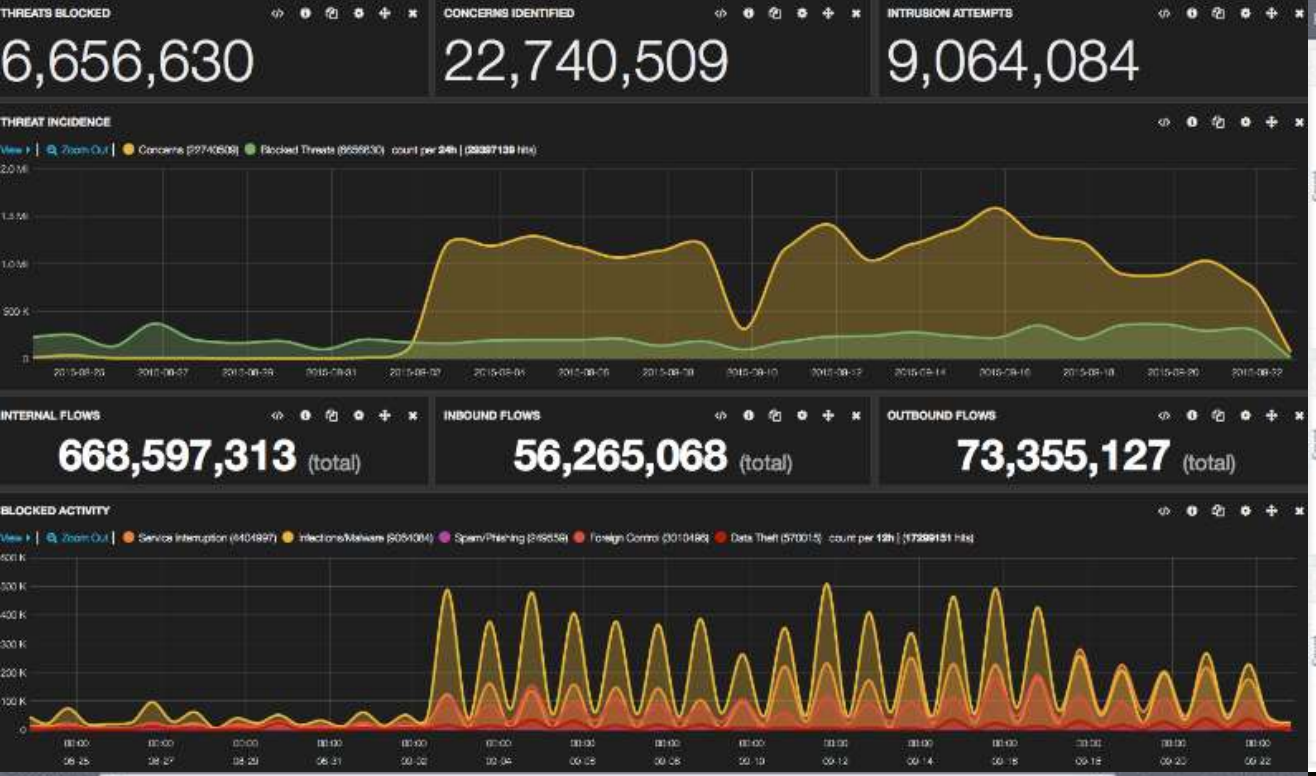
- Apache access.log event:

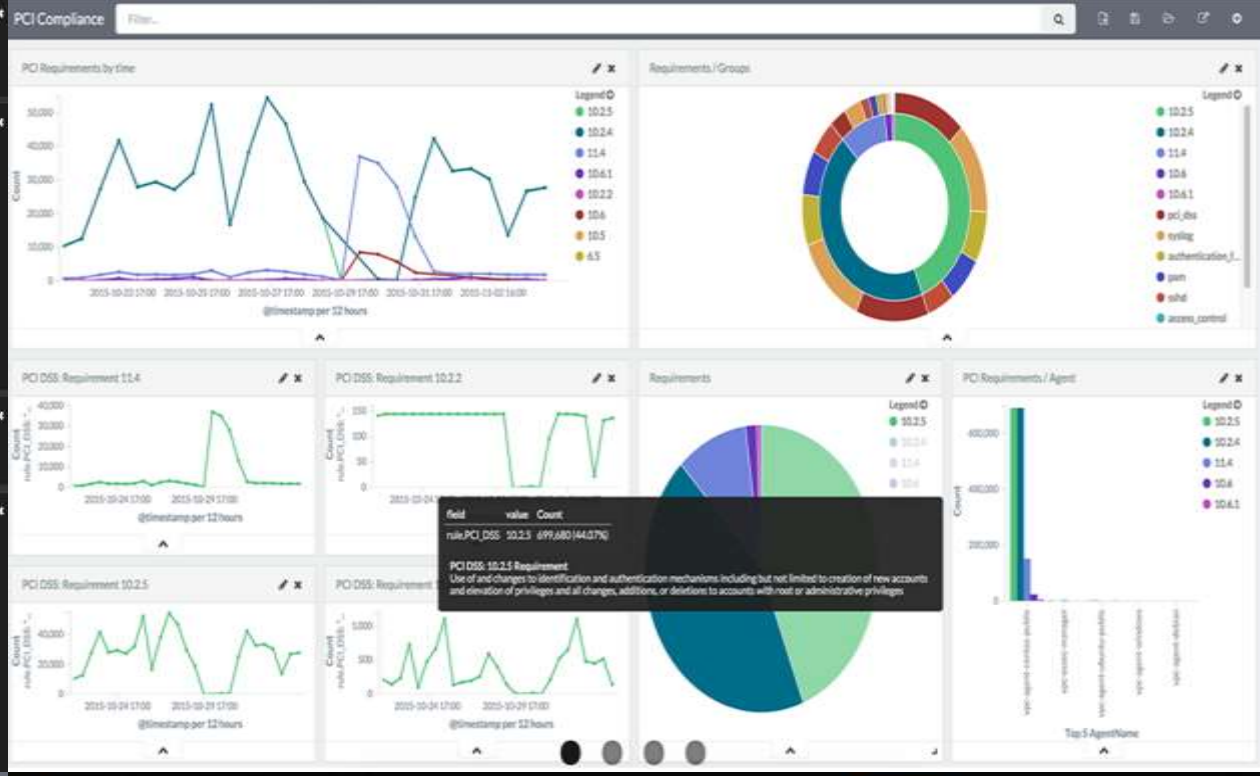
```
123.249.19.22 - - [01/Feb/2015:14:12:13 +0000] "GET /manager/html HTTP/1.1" 404 448
"-" "Mozilla/3.0 (compatible; Indy Library)"
```

- Matching grok:

```
%{IPV4} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb}
%{NOTSPACE:request}(?: HTTP/%{NUMBER:httpversion})?)" %{NUMBER:response}
(?:%{NUMBER:bytes}|-)
```

%{COMBINEDAPACHELOG}

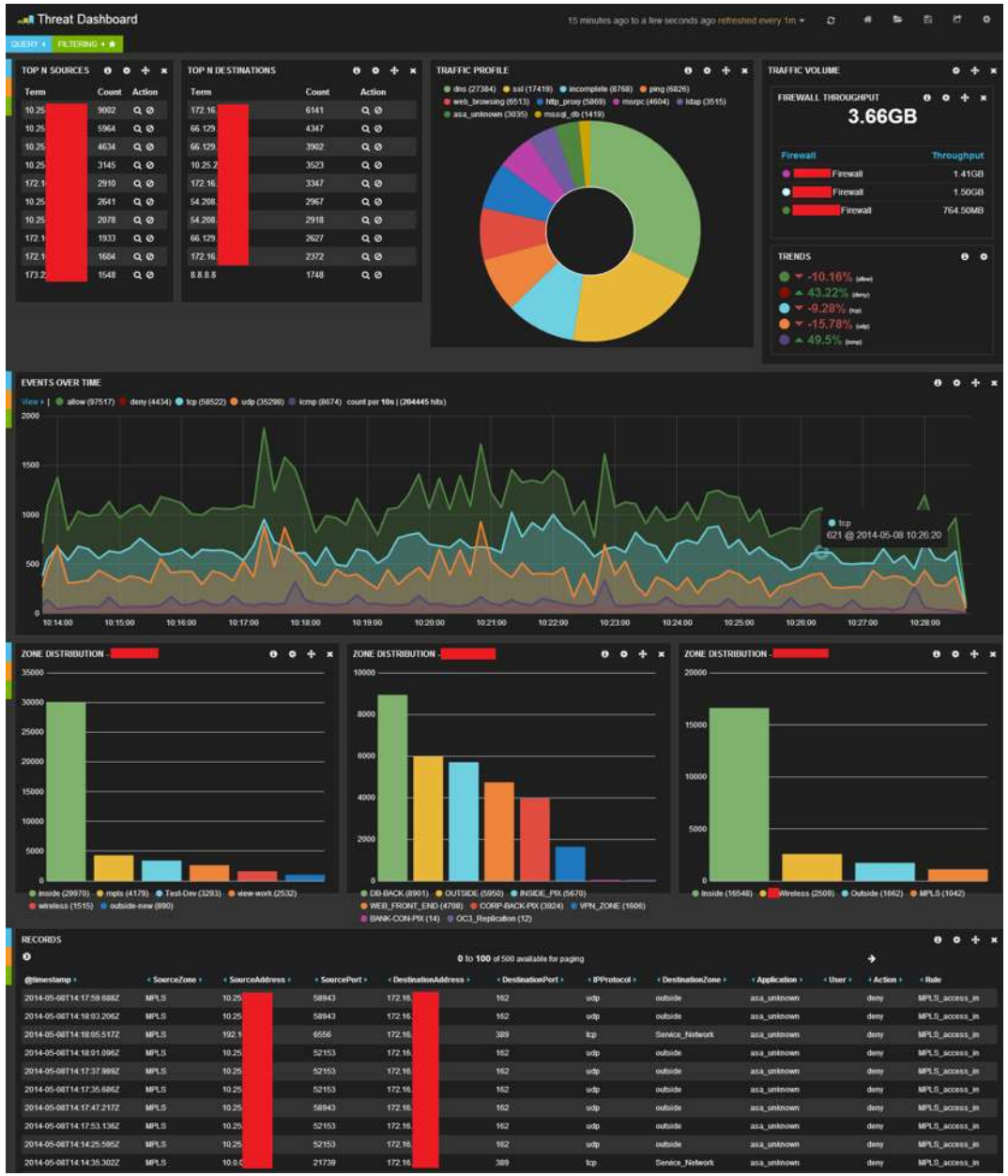

THREATS BLOCKED
6,656,630
CONCERNS IDENTIFIED
22,740,509
INTRUSION ATTEMPTS
9,064,084
THREAT INCIDENCE
INTERNAL FLOWS
668,597,313 (total)
INBOUND FLOWS
56,265,068 (total)
OUTBOUND FLOWS
73,355,127 (total)
BLOCKED ACTIVITY

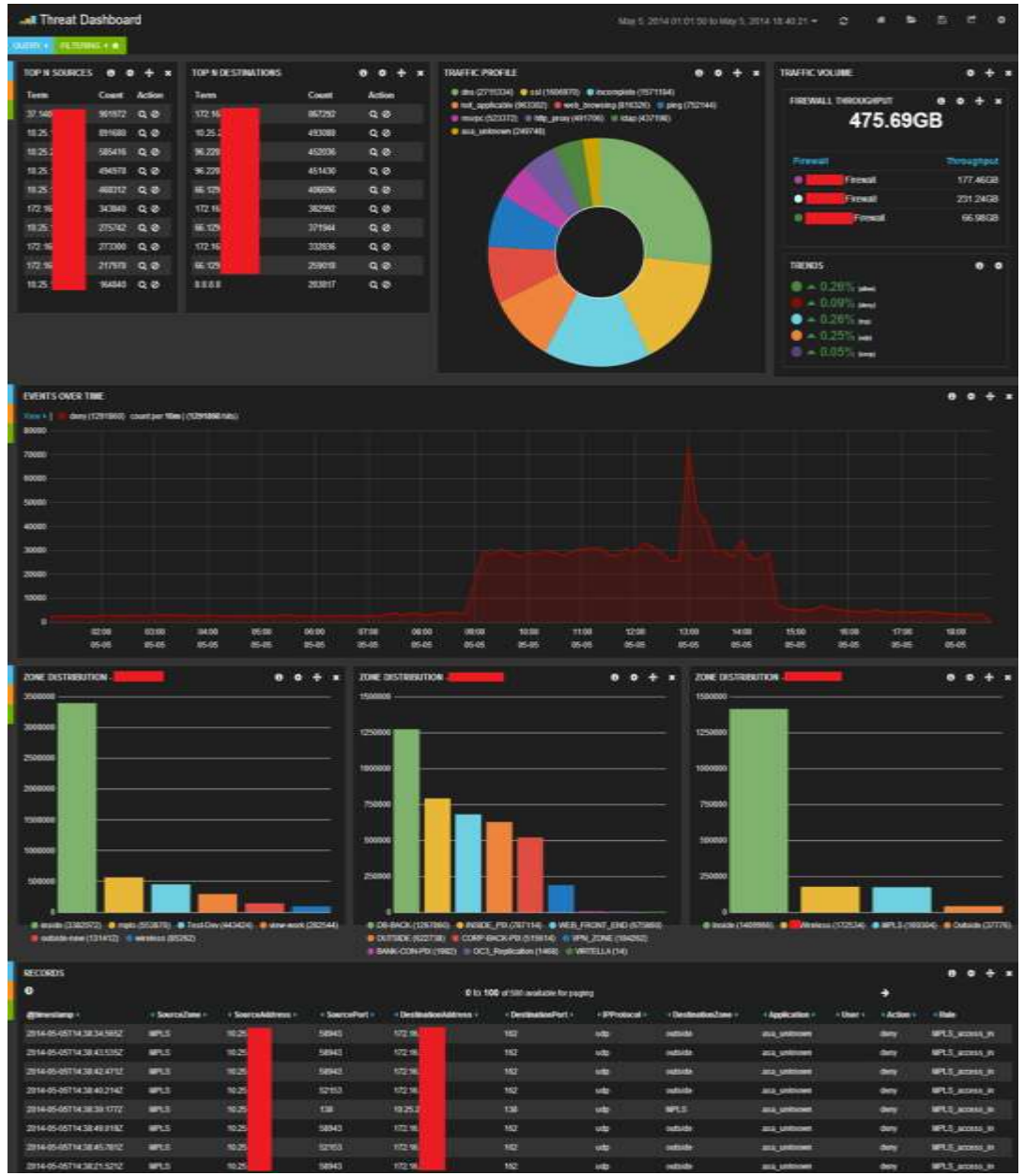

PCI Compliance
PCI Requirements by time
Requirements / Groups
PCI DSS: Requirement 11.4
PCI DSS: Requirement 10.2.2
Requirements
PCI Requirements / Agent
PCI DSS: Requirement 10.2.5
PCI DSS: Requirement
field value Count
rule.PCI_DSS 10.2.5 699,680 (44.07%)
PCI DSS: 10.2.5 Requirement
Use of and changes to identification and authentication mechanisms including but not limited to creation of new accounts and elevation of privileges and all changes, additions, or deletions to accounts with root or administrative privileges


OSSEC Alerts
Alerts Geolocation
Alerts By country
Alerts Top 5 Groups
Total Alerts Time Bar
Signature Area Chart
Stacked Groups


OSSEC & SNORT MONITORING DASHBOARD
HISTOGRAM
WORLD MAP
REPORTING SERVER
COUNTRY
ECHO
IP ADDRESS
SIGNATURE
RESULT

DDoS Atak Örneği





İletişim Bilgileri

Blog	• www.lifeoverip.net • Blog.bga.com.tr
Twitter	• @bgasecurity • @huzeyfeonal
İletişim	• huzeyfe@lifeoverip.net • Huzeyfe.onal@bga.com.tr