UiO : Universitetet i Oslo

ELK i solnedgang

Espen Grøndahl
IT-sikkerhetssjef
UiO

Agenda

- Litt om UiO
- IT-sikkerhetsutfordringer ved UiO
- Litt historikk
- ELK ved UiO
- Loggkilder
- Automatisering og deteksjon

Litt om UiO

- Ca. 28000 studenter
- Ca. 7000 ansatte
- Ca. 65000 brukerkontoer
- Mange tilknyttede enheter og organisasjoner
- USIT – Universitetets senter for informasjonsteknologi
  - Ca. 230 årsverk, sentral IT ved UiO.
  - 50/50 leveranser til UiO og til resten av sektoren
- Lokal IT
  - Lokal IT ved fakulteter og institutter

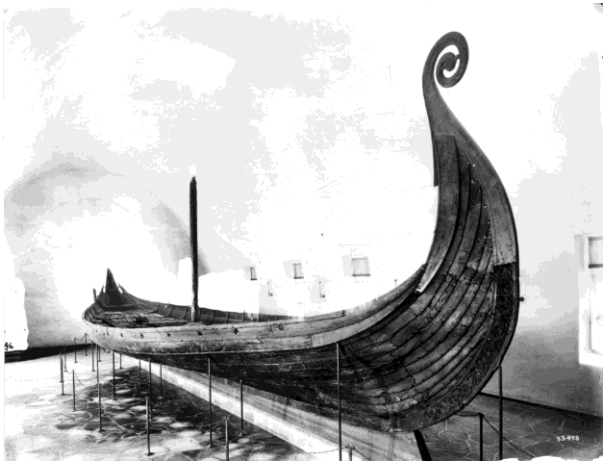
IT-sikkerhetsutfordringer ved UiO

- Kompleksitet
  - 15000+ pcer med Windows (Win10 / Win7)
  - 1000+ Linux klienter (RHEL)
  - 3000+ Linux servere (RHEL)
  - 1000 Windows servere
  - 2000 Macer
  - I tillegg ca. 18000 unike brukere på trådløst i uka…

IT-sikkerhetsutfordringer ved UiO

- Sammensatt bruksmønster
  - Fra skrivemaskin til partikkel-akseleratorer
  - Mer enn 65000 forskjellige programpakker/linjer i SCCM
  - Det som er unormalt andre steder – kan være helt normalt hos oss
- Åpenhet
  - Alle maskiner (nesten) har offentlig ip-adresse
  - En del sperrer, men ingen tradisjonell brannmur
  - Utfordring å standardisere på alle områder

Litt historikk (før 2015)



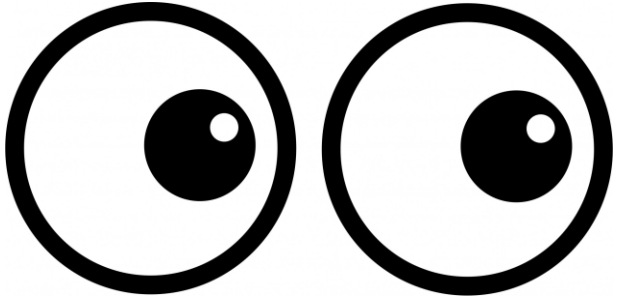
- Sentralisert logging
  - Har ”alltid” hatt det på Linux/Unix
  - Noe deteksjon i form av script og søk
  - Lite og ikke formalisert på Windows
- Driftsopplegg ”daily” og ”daily2”
  - Gammel perl-løsning som samlet inn en del data hver natt
  - Fungerte bra for drift, men ikke så bra for sikkerhet
- Antivirus
- Lokale varianter
  - Vi hadde mange lokale installasjonsopplegg for Windows

Litt historikk

- Deteksjon
  - Stort sett hendelsesstyrt – noen varslet om at ”noe” var rart
  - Fanget misbruk i e-postsystemet
  - Fanget noe med netflow
  - Detektert i form av portscan med mer.
- Sentralisert logging for Windows
  - Har vært planlagt lenge
  - Gjorde tester med Splunk – ble for dyrt pga. store loggmengder
  - Testet med WEF – skalerte ikke
  - Søk og sammenstilling av Windows logger var veldig tidkrevende

Noen milepæler

- Windows 7 utrulling – felles image for hele UiO, kun 64bit
- Rullet ut EMET på alle maskiner
- SCCM med Windows Defender
  - Dekket noe logging
  - Gir god oversikt over maskiner
  - Men ikke ”realtime” - tid fra hendelse til innsamling > 24t
  - Tungt å hente ut med API
- AppLocker på alle maskiner, men med få regler
  - Logger, sperrer exe fra zip filer + noe mer.



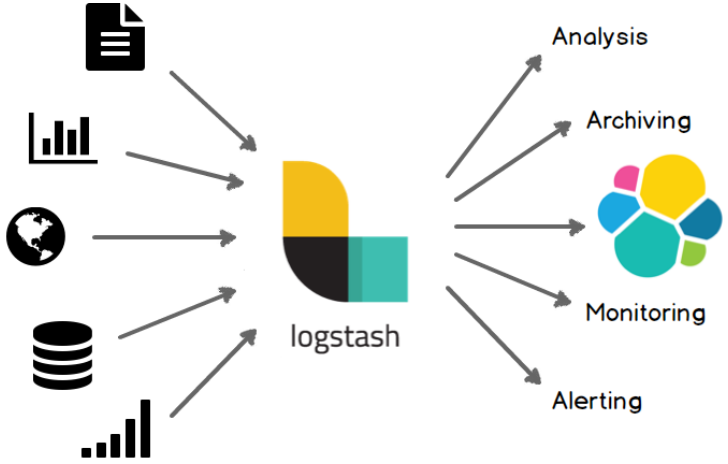
ELK VED UIO

"I WAS BLIND BUT NOW I SEE!"

Hva er ELK

- Elasticsearch
  - Distribuert søkemotor / database
  - Lagrer JSON dokumenter
  - Aksesseres via. HTTP GET
  - Veldig god skalerbarhet
- Logstash
  - Mottak, prosessering og videresending av logger
  - Sørger for at en ”host er en host på tvers av logger”
- Kibana
  - Web-basert dashboard for å drille i data

Logstash



- Mottak
  - Fra filebeat, nxlog
- Tolking
  - Hva brukernavn, hostnavn, ip-adresse med mer.
- Normalisering
  - User, Username, name, TargetUsername osv. -> user
- Beriking
  - Geoip, Alexa Top X, vlan osv.
  - Samkjøring med andre lokale kilder, vlan, brukerdatabase med mer.
  - Fjern data som ikke skal lagres, maskere mulig sensitive felter
- Send til Elastic

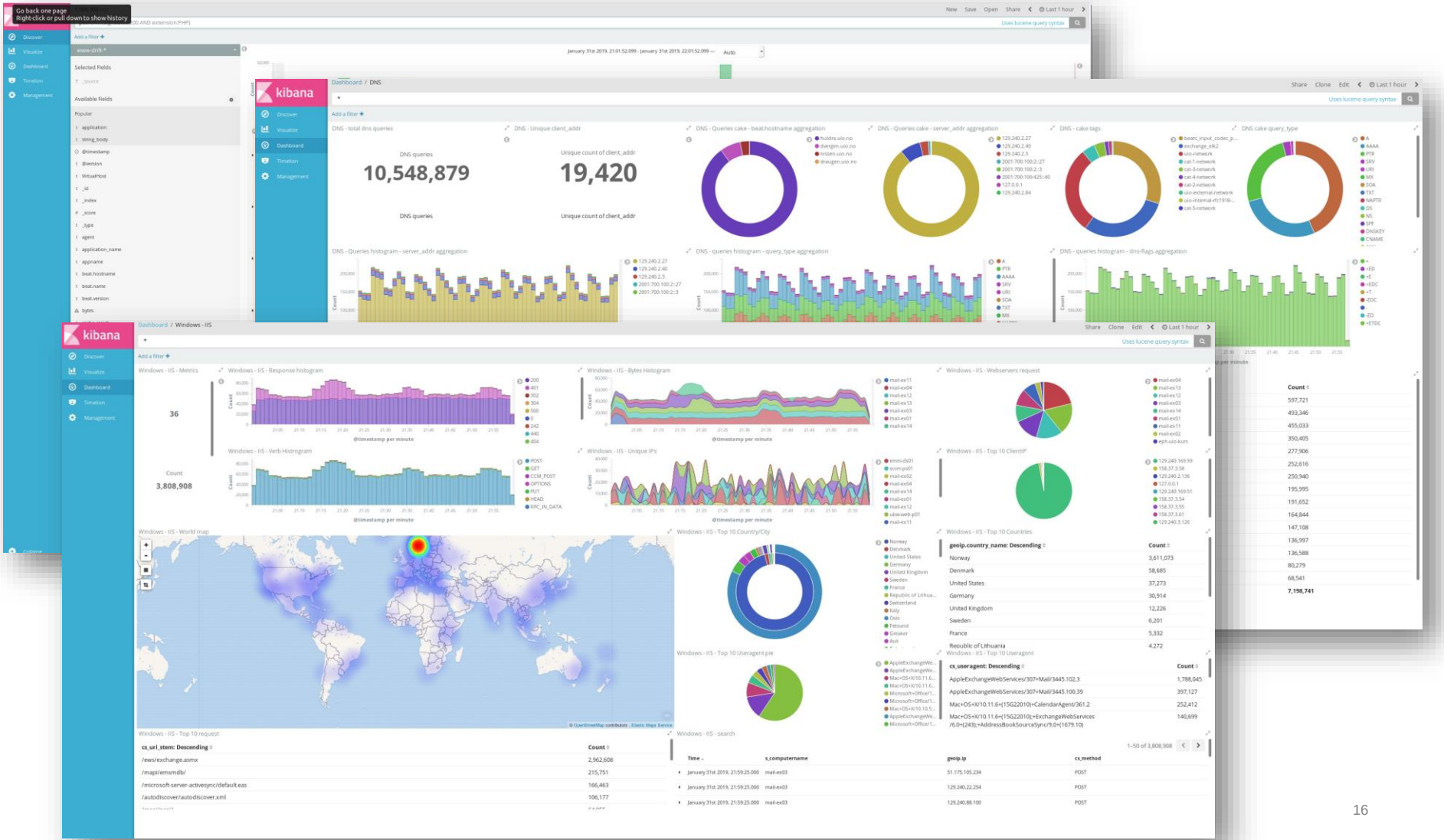
Elastic

elasticsearch

- Søkemotor basert på Lucene
- Realtime, skalerbar, multitenant
- Lagrer og søker i JSON dokumenter
- Aksesseres via HTTP basert REST-API

Kibana

- Grafisk grensesnitt for å søke og «drille» i data
- Grafing, diagram, filtrering med mer.
- Effektivt for realtime analyse og for å ha oversikt
- Noen utfordringer
  - Analyse i store datasett (typisk noen 100 millioner)
  - Eksport av data
  - Automatisering og tilgang via API

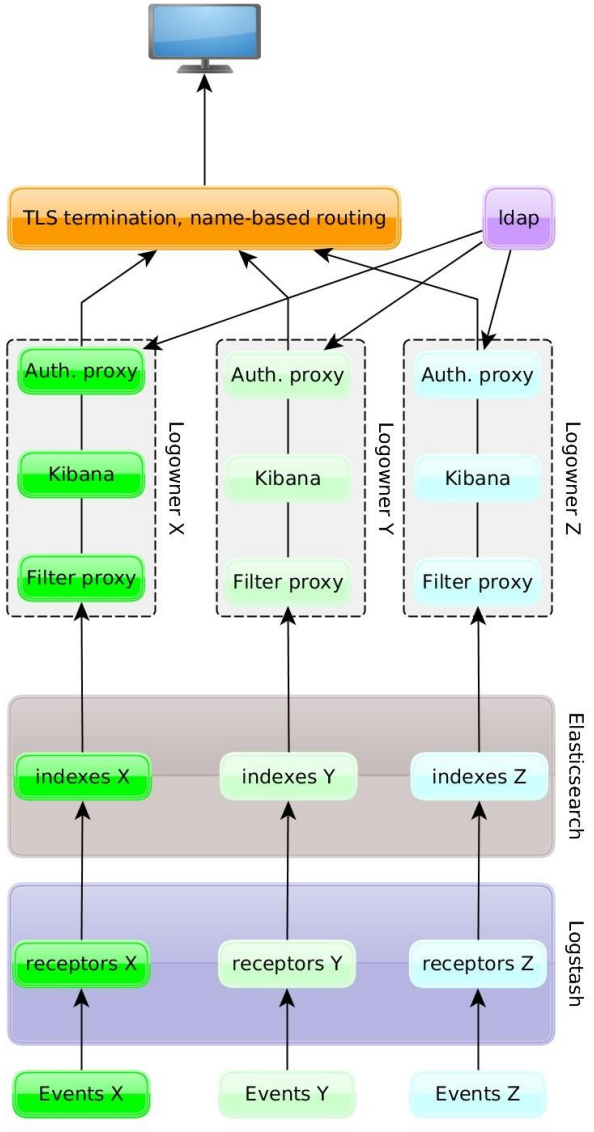

kibana
Dashboard / DNS
DNS - total dns queries
DNS queries
10,548,879
DNS queries
DNS - Unique client_addr
Unique count of client_addr
19,420
Unique count of client_addr
DNS - Queries cake - beat.hostname aggregation
DNS - Queries cake - server_addr aggregation
DNS - cake tags
DNS cake query_type
DNS - Queries histogram - server_addr aggregation
DNS - queries histogram - query_type aggregation
DNS - queries histogram - dns-flags aggregation
kibana
Dashboard / Windows - IIS
Windows - IIS - Metrics
36
Count
3,808,908
Windows - IIS - Response histogram
Windows - IIS - Verb Histrogram
Windows - IIS - Bytes Histogram
Windows - IIS - Unique IPs
Windows - IIS - Webservers request
Windows - IIS - Top 10 ClientIP
Windows - IIS - World map
Windows - IIS - Top 10 Country/City
Windows - IIS - Top 10 Useragent pie
Windows - IIS - Top 10 Countries
geoip.country_name: Descending
Count
Norway 3,611,073
Denmark 58,685
United States 37,273
Germany 30,914
United Kingdom 12,226
Sweden 6,201
France 5,332
Republic of Lithuania 4,272
Windows - IIS - Top 10 Useragent
cs_useragent: Descending
Count
AppleExchangeWebServices/307+Mail/3445.102.3 1,788,045
AppleExchangeWebServices/307+Mail/3445.100.39 397,127
Mac+OS+X/10.11.6+(15G22010)+CalendarAgent/361.2 252,412
Mac+OS+X/10.11.6+(15G22010)+ExchangeWebServices/6.0+(243)+AddressBookSourceSync/9.0+(1679.10) 140,699
Windows - IIS - Top 10 request
cs_uri_stem: Descending
Count
/ews/exchange.asmx 2,962,608
/mapi/emsmdb/ 215,751
/microsoft-server-activesync/default.eas 166,463
/autodiscover/autodiscover.xml 106,177
Windows - IIS - search
Time
s_computername
geoip.ip
cs_method
January 31st 2019, 21:59:25.000 mail-ex03 51.175.105.234 POST
January 31st 2019, 21:59:25.000 mail-ex03 129.240.22.254 POST
January 31st 2019, 21:59:25.000 mail-ex03 129.240.88.100 POST

ELK ved UiO

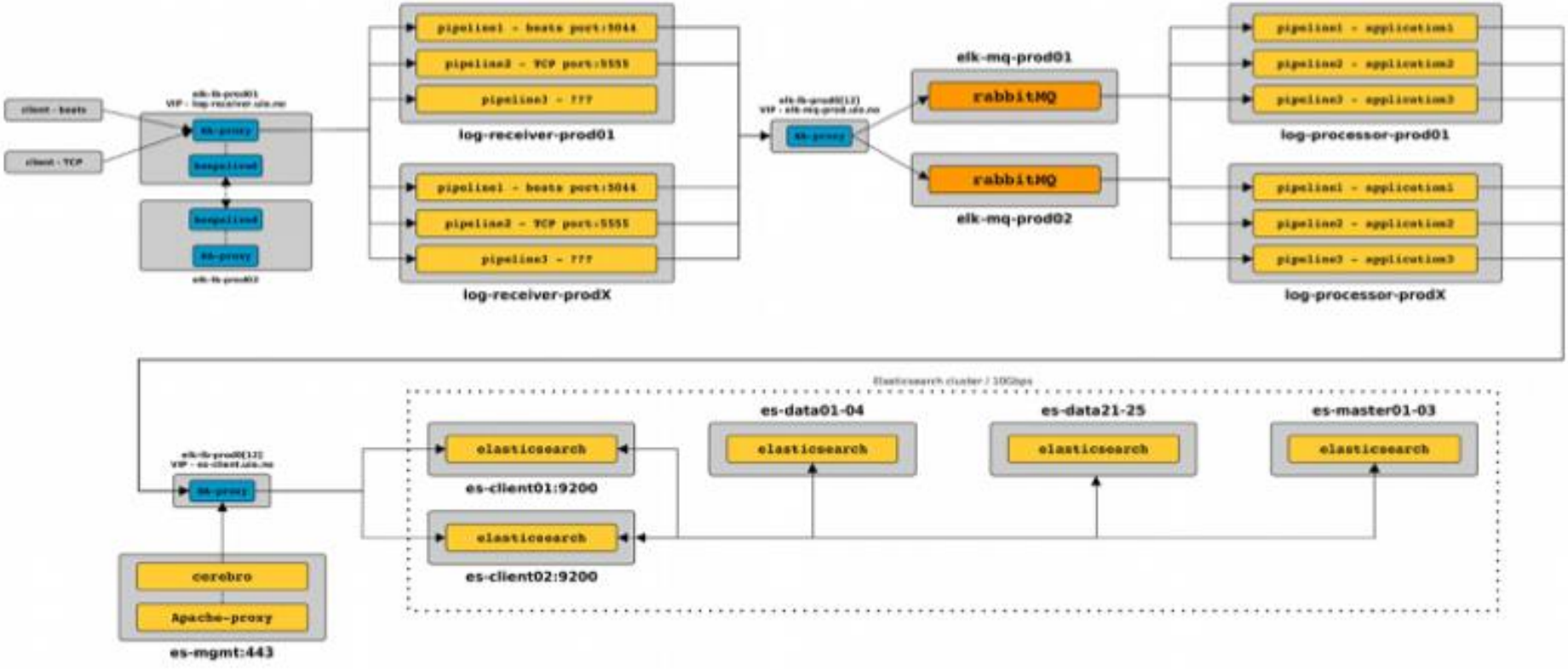
- UiO-CERT hadde deteksjon på årsplanen for 2015 (og før)
  - Vi ble innhentet av et fellesprosjekt for logging :-)
- Vi har nå en stor løsning med selvbetjening
  - Dekker både sikkerhet og drift
- Implementert egen løsning for tilgangsstyring basert på ngnix og LDAP
- Automatisert med Docker, Ansible, Consul med mer.
- Innført et eget begrep ”logowner”, en kibana instans pr. Logowner – brukes for tilgangstyring.

Tilgangsstyring

- Valgte å ikke kjøpe
- Innførte et eget begrep «logowner»
- Logger tagges med en eller flere «logowner» tag'er
- Noen markeres som «felleslogger»
- Du kan kun søke i de logger du har tilgang til
- UiO-CERT kan søke på tvers av alle
- Fungerer også via API'et – mer om det senere

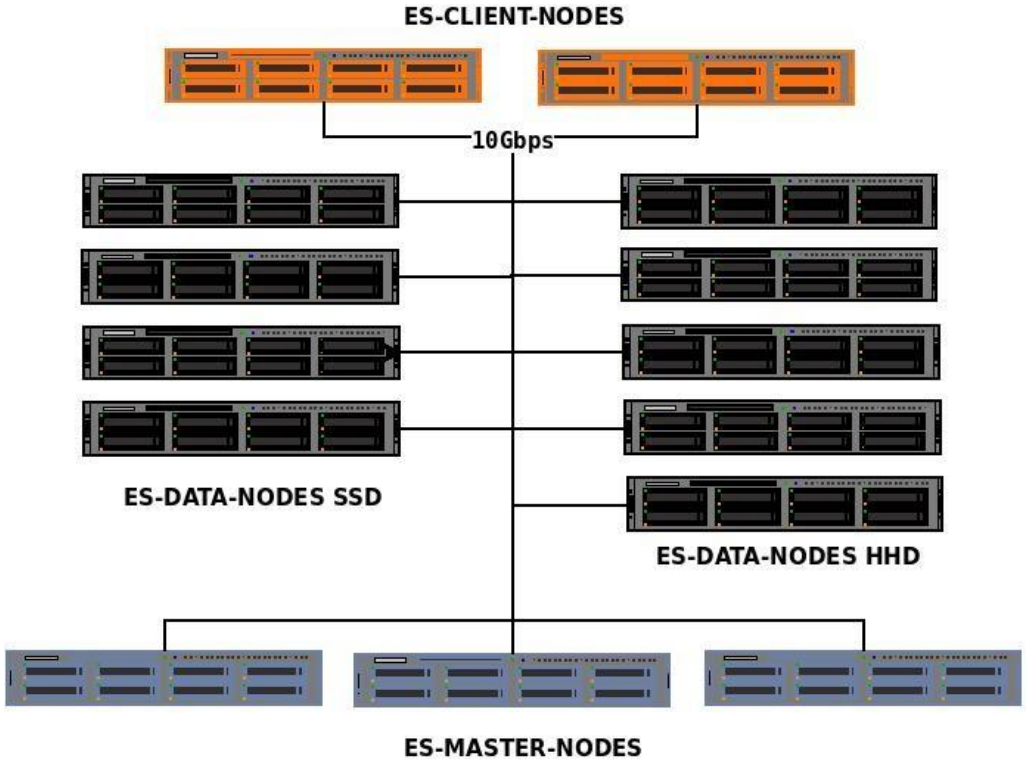


Det «store bildet»™


pipeline1 - beats port:5044
pipeline2 - TCP port:5555
pipeline3 - ???
log-receiver-prod01
log-receiver-prodX
elk-mq-prod01
rabbitMQ
rabbitMQ
elk-mq-prod02
pipeline1 - application1
pipeline2 - application2
pipeline3 - application3
log-processor-prod01
log-processor-prodX
es-data01-04
es-data21-25
es-master01-03
elasticsearch
es-client01:9200
es-client02:9200
cerebro
Apache-proxy
es-mgmt:443

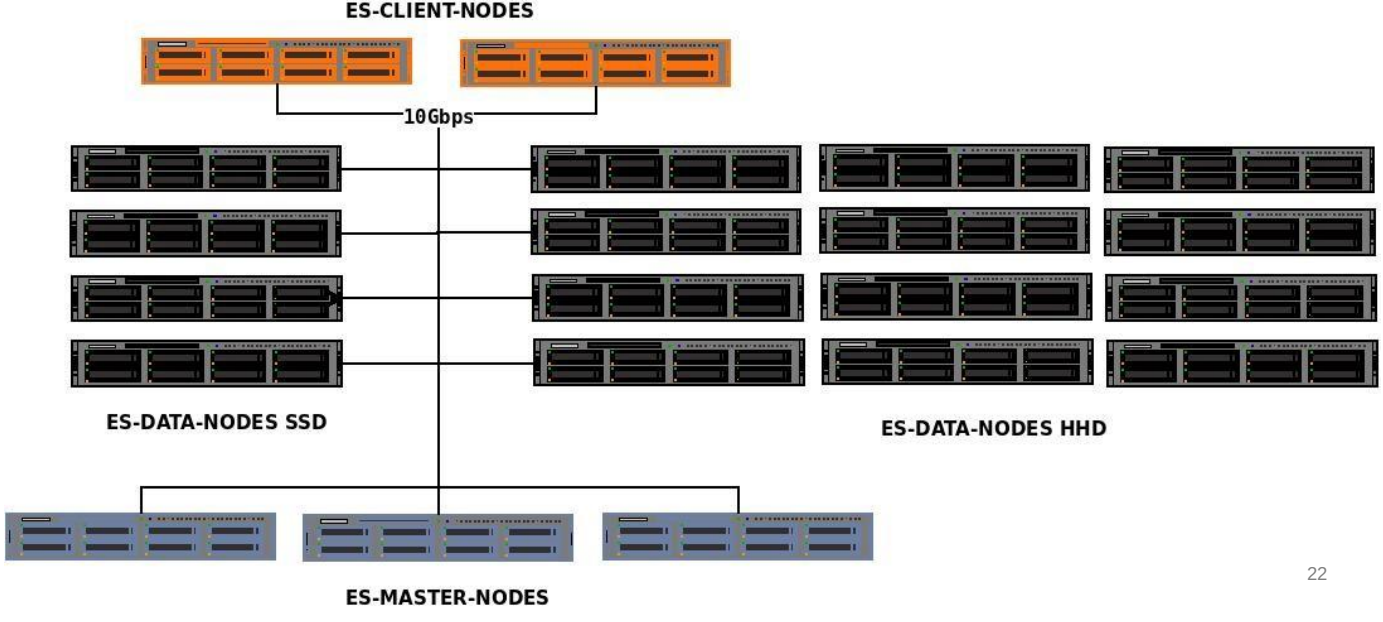
ELK ved UiO – noen tall

- ES Logs/sec (last week):
  - avg: ~10.000
  - max: ~37.000
  - min: ~7.500
- ES indexes: ~1.378
- ES-shards: ~5.500
- Total logs: ~52.000.000.000
- Total docs: ~104.000.000.000
- Total data: ~85-95TB
- 21 elasticsearch servers
- Version: 6.7.x Elasticsearch



ELK - hardware

- SSD-raid: 11TB x 4 = 44TB netto
- HDD-raid5: 12,8 x 12 = 153TB netto
- SSD-node: 4 x 64GB = 256GB ram
- HHD-node: 8 x 128GB + 4 x 198GB =
- 1.816GB RAM
- 3 master noder
- 2 client noder
- 2 x 10Gbit
- Dedikert subnet



Loggkilder

- Sysmon (!)
  - ca. 30 millioner pr døgn (15000 pc'er, 700 servere)
  - En av de viktigste kildene for deteksjon
- Windows logger
  - Alt fra serverene
  - Noen utvalgte fra klientene – f.eks
- (R)syslog – 75 millioner pr døgn (3000 klienter)
- Apache
- DNS - 250 millioner pr døgn
- Portscan av hele UiO-nettet 3 ganger pr døgn
- Radius
- IIS
- Office 365 – hentes hjem via API
- Dropbox – I test
- Google – I test
- Totalt ca 100 kilder og økende

Sysmon

- August 2015 – Microsoft sysinternals
  - https://technet.microsoft.com/en-gb/sysinternals/sysmon
- Logger prosesser som starter, bruker, hash av exe fil, parent prosess med mer.
- Finnes nå i versjon 10.2
  - Prosesser, registry, nettverk, lasting av drivere, hash av filer med mer.
- Vi benytter sysmon på alle Windows maskiner sammen med nxlog som sender til logstash

Sysmon konfigurasjon

- Styres med XML, kan logge veldig mye
  - Balanse mellom nytte, personvern og volum
- Finnes etter hvert en del eksempler på github
  - For eksempel https://github.com/SwiftOnSecurity/sysmon-config
- Anbefaling;
  - Rull det ut, skru opp loggstørrelse
  - Kan da i alle fall hente logger etter en hendelse «flight recorder»
  - Fortsett så med sentral innsamling
- En av de beste kildene for Windows miljøer

DNS

- Dns-query logging – logg fra bind-resolvere
- «Alt» genererer ett dns-oppslag
- Hentes inn via filebeat
- Ca 250 000 000 log-dokumenter pr døgn
  - Benyttes til deteksjon av phishing
  - Alle domener som inneholder uio, password + + - som ikke er uio.no – send varsel
  - Søk etter alle som har resolvet detekterte kampanjer
  - Deteksjon av “rouge ap” og skjulte nett
  - Varsel på bestemte domener – styrt av chatbot

Nxlog

- Sender logg fra Windows til log-mottak
- http://nxlog.co
- Finnes i en community og en enterprise edition
- Vi kjører community edition på ca. 15000 pc'er og 1000 servere
- Foretar grovsortering av eventer og køing

De siste bitene

- CERT-WS
  - Web-service skrevet i Go for å lette søk i ELK
  - Syntax inspirert av unix – grep, sed, awk, sort, wc osv.
  - For eksempel:
  - **https://cert-mgmt.uio.no:9010/v1/generic/search?index=*sysmon*&must=ParentImage:*Office*&Image=*cmd.exe*&size=10&start=now-7d&csv**
  - Søk etter alle cmd.exe som har «Office» som parentprosess, siste uke, skriv ut 10 linjer i csv format
  - Egen kommandlinjeklient for å lette drilling i data
- KarbonBlakk™ – vi hadde ikke penger til Carbon Black :-)
  - Service som søker i alle kjørte programmer kjørt – sjekker mot alle kjente, varsler basert på hash med mer.
  - Varsler på kjente skumle programmer

mattermost-cert 11:00

3427F732C07388DCF87CEDCBF6AF0B3D : usit-gdw, f[redacted].no, [redacted], C:\\Jobb\\ESS_INKIND\\CameraLink _Filter_UL_SIM\\CameraLink.sim\\sim_6\\synth\\func\\xsim\\xsim.dir\\top_sim_func_synth\\xsimk.exe, C:\\Xilinx\\Vivado\\2018.3\\bin\\unwrapped\\win64.o\\vivado.exe Hashdd: NOT_FOUND

B9770DCBA1D3DF56FC365895FE6A4AD4 : usit-gdw, f[redacted]AppData\\Local\\Programs\\Microsoft VS Code Insiders\\Code - Insiders.exe, C:\\Users\[redacted]AppData\\Local\\Programs\\Microsoft VS Code Insiders\\Code - Insiders.exe Hashdd: NOT_FOUND

1D40001F2E9E1672004C268D8DE6E79D : usit-gdw, f[redacted], C:\\Users\[redacted]\\AppData\\Local\\Programs\\Microsoft VS Code Insiders\\resources\\app\\node_modules.asar.unpacked\\node-pty\\build\\Release\\winpty-agent.exe, C:\\Users\[redacted]ppData\\Local\\Programs\\Microsoft VS Code Insiders\\Code - Insiders.exe Hashdd: NOT_FOUND

F58E81498BBBCD3A3DA0FE624D0DAC16 : usit-gdw, [redacted], NT AUTHORITY\\SYSTEM, C:\\Program Files\\AVG\\Antivirus\\defs\\19082600\\engsup.exe, C:\\Program Files\\AVG\\Antivirus\\setup\\instup.exe Hashdd: Unknown

50CD6DE83EDB71D9A8F70EF28E3E58C0 : usit-gdw, [redacted], C:\\Users[redacted]\\AppData\\Local\\Temp\\7zS3876.tmp\\Install.exe, C:\\Users[redacted]\\AppData\\Local\\Temp\\7zS3876.tmp\\InstallLauncher.exe Hashdd: NOT_FOUND

F0879E5FF33D469B64D26846CEB13AE3 : usit-gdw, [redacted]uio.no, UIO\[redacted], C:\\Users[redacted]\\AppData\\Local\\Temp\\7zS3876.tmp\\InstallLauncher.exe, C:\\Users\[redacted]\\AppData\\Local\\Microsoft\\Windows\\INetCache\\IE\\I4BNC34L\\MediaCenter250092.exe Hashdd: Unknown

FD13398500BB779133794C3E12628787 : usit-gdw, [redacted], UIO\[redacted], C:\\Users\[redacted]\\AppData\\Local\\Microsoft\\Windows\\INetCache\\IE\\I4BNC34L\\MediaCenter250092.exe, C:\\Program Files\\internet explorer\\iexplore.exe Hashdd: Unknown

09221BBE7BA28EB7BD0169CF871174CD : usit-gdw, [redacted], C:\\Users\[redacted]AppData\\Local\\Temp\\unityhub-2f26c5f0-c7e1-11e9-896a-5d348c36b4a8\\UnitySetup-WebGL-Support-for-Editor-2019.2.2f1.exe, C:\\Windows\\System32\\cmd.exe Hashdd: Unknown

C6B2C9494952C7C1F7629276DDE77038 : usit-gdw, [redacted]C:\\Program Files\\Adobe\\Adobe Premiere Pro CC 2019\\dvaaudiofilterscan.exe, C:\\Program Files\\Adobe\\Adobe Premiere Pro CC 2019\\Adobe Premiere Pro.exe Hashdd: Unknown

8FDD502E54FA194FE24E326CBBBFE192 : usit-gdw, [redacted], C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\Data\\Resources\\PackageManager\\Server\\UnityPackageManager.exe, C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\Unity.exe Hashdd: NOT_FOUND

8BB58003B36831F14EB799D18562019A : usit-gdw, [redacted], C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\Unity.exe, C:\\Program Files\\Unity Hub\\Unity Hub.exe Hashdd: NOT_FOUND

9F8F2741752A32F2BBACEA331CC2207B : usit-gdw, [redacted], C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\Data\\Tools\\UnityCrashHandler64.exe, C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\Unity.exe Hashdd: Unknown

New Messages

05112F8223322F8C257BD24A7F1EE71C : usit-gdw, [redacted]C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\UnityHelper.exe, C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\Unity.exe Hashdd: NOT_FOUND

3C33A525545D498A5B1B36B463D0D9AC : usit-gdw, [redacted], C:\\VS2013\\GMAP2019\\bin\\GMAP2016.exe, C:\\Program Files (x86)\\Microsoft Visual Studio 12.0\\Common7\\IDE\\devenv.exe Hashdd: NOT_FOUND

7074835E13F6BA2CA579BF473016A078 : usit-gdw, [redacted].no, UIO\[redacted], C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\Data\\Tools\\UnityShaderCompiler.exe, C:\\Program Files\\Unity\\Hub\\Editor\\2019.2.2f1\\Editor\\Unity.exe Hashdd: NOT_FOUND

1A55597E2AEB13CF813A4A72231D76D1 : usit-gdw, [redacted]C:\\VS2013\\GMAP2019\\bin\\GMAP2016.exe, C:\\Program Files (x86)\\Microsoft Visual Studio 12.0\\Common7\\IDE\\devenv.exe Hashdd: NOT_FOUND

30E3A4012CF9D059DE83C91A05D763D3 : usit-gdw, [redacted]C:\\VS2013\\GMAP2019\\bin\\GMAP2016.exe, C:\\Program Files (x86)\\Microsoft Visual Studio 12.0\\Common7\\IDE\\devenv.exe Hashdd: Unknown

8E975E9ACD5D61CDA42E4FF2AF7586F6 : usit-gdw, [redacted]C:\\VS2013\\GMAP2019\\bin\\GMAP2016.exe, C:\\Program Files (x86)\\Microsoft Visual Studio 12.0\\Common7\\IDE\\devenv.exe Hashdd: NOT_FOUND

DD10198F803E8C18EFAC541576DEF9F8 : usit-gdw, [redacted], D:\\Downloads\\ScanSnap\\WinSSHDownloadInstaller_1_3_1.exe, C:\\Windows\\explorer.exe Hashdd: NOT_FOUND

47ADB37FF8904DFAC0F2D8B2FFB46554 : usit-gdw, [redacted], C:\\Users\[redacted]AppData\\Local\\Temp\\SSHomeDownloadInstaller\\SSHDownloadInstaller.exe, D:\\Downloads\\ScanSnap\\WinSSHDownloadInstaller_1_3_1.exe Hashdd: NOT_FOUND

EC204ECB57EE548E8A972138676EFA8C : usit-gdw, [redacted], C:\\ProgramData\\ScanSnapHomeInstallerWork\\GetAppdata.exe, C:\\Users\[redacted]AppData\\Local\\Temp\\SSHomeDownloadInstaller\\SSHDownloadInstaller.exe Hashdd: Unknown

26D98DD6C4B9376D2C6E2EA8905C6710 : usit-gdw, [redacted], C:\\Users\[redacted]\\AppData\\Local\\Temp\{82F7BC99-0001-4349-B9AD-FC06DF748F66}\{1806D5A5-0B2C-4E54-8219-7BD4CB9CB690}\\SsDevSet-x64.exe, C:\\Users\[redacted]AppData\\Local\\Temp\{B7B3499A-D96B-45C2-BA5A-69BEE723AA25}\\WinSSHomeInstaller_1_3_1.exe Hashdd: Unknown

24D217AA1E7FC6495507B140CA480996 : usit-gdw, [redacted], C:\\Users[redacted]\\AppData\\Local\\Temp\\SSHomeDownloadInstaller\\download\\WinSSHomeInstaller_1_3_1.exe, C:\\Users\[redacted]\\AppData\\Local\\Temp\\SSHomeDownloadInstaller\\SSHDownloadInstaller.exe Hashdd: Unknown

711306B70C761C7E23A3DDD62C189E50 : [redacted]C:\\VS2013\\GMAP2019\\bin\\GMAP2016.exe, C:\\Program Files (x86)\\Microsoft Visual Studio 12.0\\Common7\\IDE\\devenv.exe Hashdd: Unknown

B1BD9AF70DBF3C741B150773917A8A66 : usit-gdw, [redacted], C:\\Users\[redacted]AppData\\Local\\Temp\{B7B3499A-D96B-45C2-BA5A-69BEE723AA25}\\WinSSHomeInstaller_1_3_1.exe, C:\\Users\[redacted]AppData\\Local\\Temp\\SSHomeDownloadInstaller\\download\\WinSSHomeInstaller_1_3_1.exe Hashdd: NOT_FOUND

DCDAABF82CFFCD831909EC5B82B200C5 : ERROR, ERROR, ERROR, ERROR, ERROR Hashdd: NOT_FOUND

ED17AF1E3DCC89B413B77DBE13DA3FAD : usit-gdw, [redacted], C:\\Users\[redacted]AppData\\Local\\Temp\\SSHomeDownloadInstaller\\SSHomeClean.exe, C:\\Users\[redacted]ppData\\Local\\Temp\\SSHomeDownloadInstaller\\SSHDownloadInstaller.exe Hashdd: NOT_FOUND

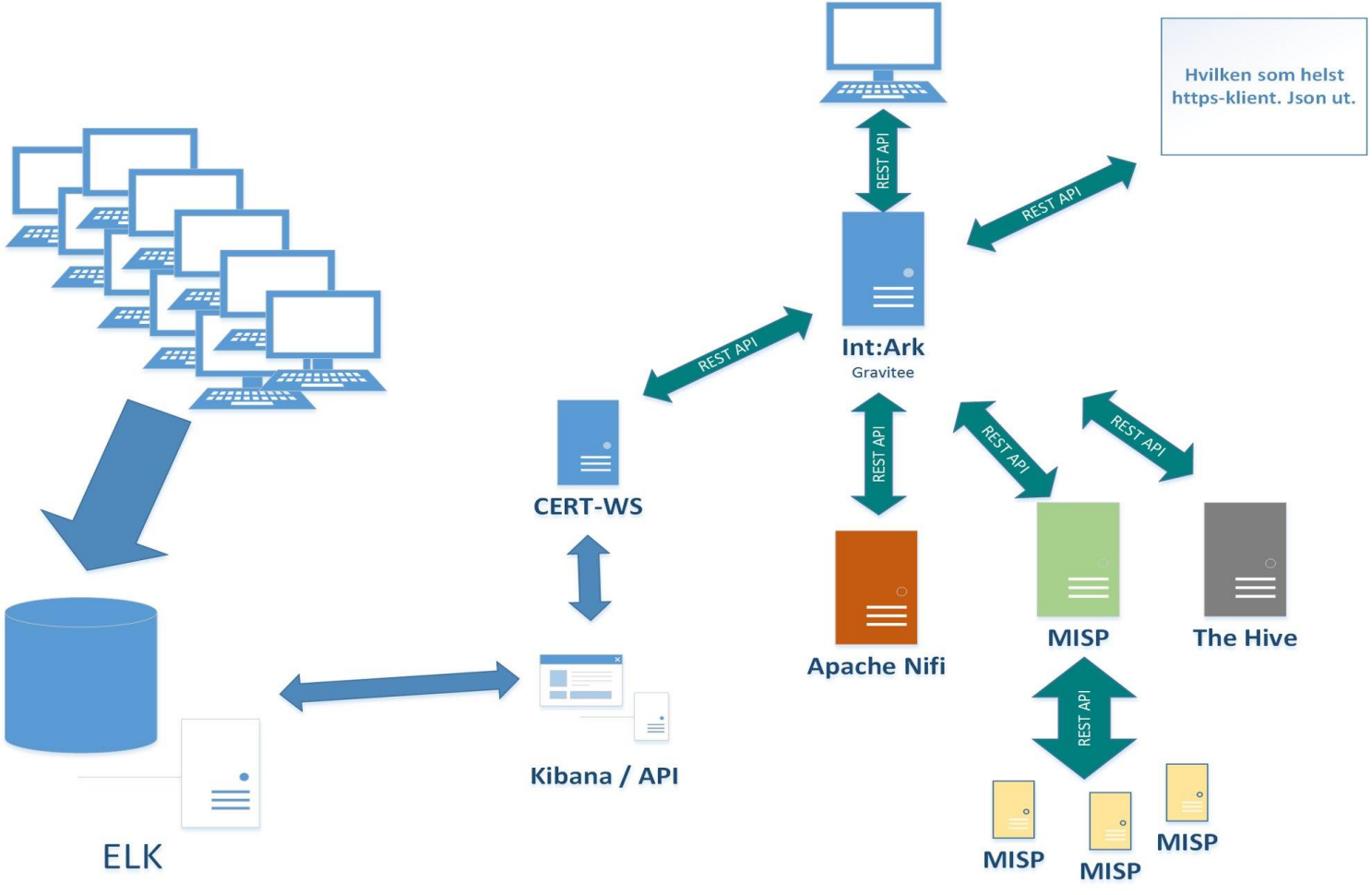
HVA NÅ?

Når dette er på plass, hva gjør vi da?

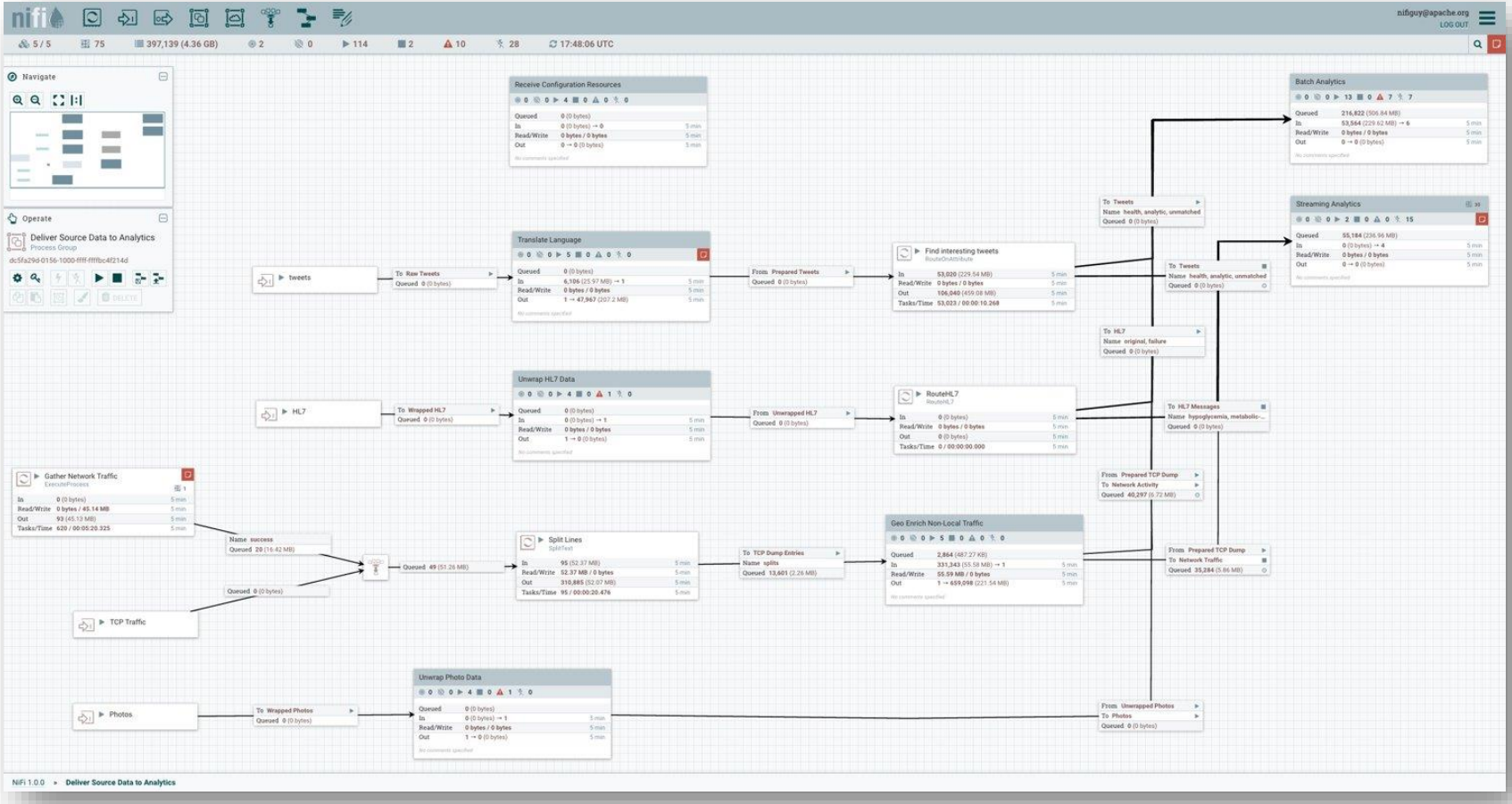
Automatisert deteksjon

- Søker å ha god dekning i MITRE ATT&CK™
- Automatiserer de med stort volum og/eller de «lette»
  - Gir tid til å konsentrere seg om de mer avanserte
  - Bedre personvern - færre som må se på data
  - For hver nye hendelse - søk å finne mer som kan automatiseres – start forfra
- Benytter en kombinasjon av verktøy
  - Enkle script i cron
  - Apache Nifi
  - Egenutviklet i Go, python med mer
  - Egen «bot» som snakker med Mattermost
- ALT via API!

Automatisering og deteksjon



Apache NIFI


nifi
nifiguy@apache.org
LOG OUT
5 / 5
75
397,139 (4.36 GB)
2
0
114
2
10
28
17:48:06 UTC
Navigate
Operate
Deliver Source Data to Analytics
Process Group
Receive Configuration Resources
Batch Analytics
Streaming Analytics
Translate Language
Find interesting tweets
RouteOnAttribute
tweets
To Raw Tweets
From Prepared Tweets
To Tweets
Name health, analytic, unmatched
To HL7
Name original, failure
Unwrap HL7 Data
HL7
To Wrapped HL7
From Unwrapped HL7
RouteHL7
To HL7 Messages
Gather Network Traffic
ExecuteProcess
From Prepared TCP Dump
To Network Activity
Geo Enrich Non-Local Traffic
Split Lines
SplitText
To TCP Dump Entries
To Network Traffic
TCP Traffic
Unwrap Photo Data
Photos
To Wrapped Photos
From Unwrapped Photos
To Photos
NiFi 1.0.0 » Deliver Source Data to Analytics

Threat hunting / response

- Jobber mot CERT-WS
  - Via Apache NIFI
  - Via curl el.l
  - Via CIA – Cert-WS InterActive – cli klient mot cert-ws
  - Vurderer fra case til case om det skal kodes inn, eller legges i script

Planer

- ML / AI
- Opensource koden – om noen har brukt for den
- Tilgjengliggjøre anonymiserte data
  - Hasher, imphash, dns-navn med mer.
- Utforske andre prosjekter for eksempel SIGMA
  - https://github.com/Neo23x0

Personvern

- Du kan risikere å logge detaljer du ikke burde
  - Filnavn, url'er med mer.
- Loggdata kan brukes til annet enn formål
- Du har lov til å logge for sikkerhet og drift av tjeneste
  - Hva er "drift av tjeneste"?
- Løses ved tilgangskontroll – og jevnlig revidering av behov
- Policy for bruk av logger
- Filtrer i logmottak – fjerne data, maskere data
- Automasjon – færre må se på data

SPØRSMÅL?

NB: Vi søker etter flere folk…

https://cyber.uio.no/jobb