Welcome to

Teknisk hvad er logning

Logningsseminar hos IDA

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

logning-ida.tex in the repo security-courses

Kontaktinformation

- Henrik Kramselund Jereminsen, internet samurai, primært netværk og sikkerhed
- Netværk og it-sikkerhedskonsulent Zencurity, underviser på KEA og aktivist
- Cand.scient fra Datalogisk Institut ved Københavns Universitet, DIKU
- Email: hkj@zencurity.dk Mobil: +45 2026 6000

I er velkomne til at sende email

Mine mål

- Introducere nogle termer omkring logning
- Nogle problemer med logning - konvertering af data
- Eksempelvis Logging og SIEM

Verden er *mostly harmless*

- **Keeping an organization safe from attack, as well as having a talented team available to respond quickly, minimizes damage to your reputation and business**
- You can't properly protect your network if you don't know what to protect.
- **Define and understand** your **critical assets** and what's most important to your organization
- Ensure that you can attribute **ownership or responsibility** for **all systems** on your network
- Understand and leverage the **log data** that can help you determine host owner- ship
- **A complex network** is difficult to protect, unless you understand it well

Source: Chapter 1 Incident Response Fundamentals
Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan
ISBN: 9781491949405

Logning er nødvendig

Kriminalitet er fakta

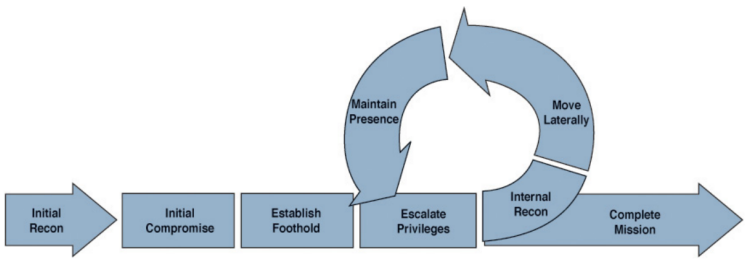


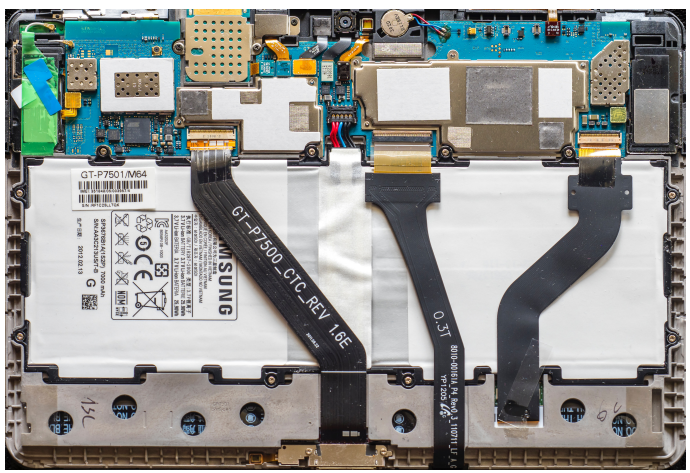
Figure 7-1 *Targeted Attack Lifecycle*

Nogle mennesker er kriminelle, og vores systemer, netværk og samfund er under angreb. Vi bruger derfor logning til

- Se traffik i vores netværk – **netflow data**
- Se **bruger login** – fejlslagne men også succesfulde logins
- Se afsendte mails – **spam** er stort problem, virus og **ransomware** ligeså
- Adgange til data – hvem har set på data – **GDPR**
- samt generel fejlfinding, som ignoreres i dag

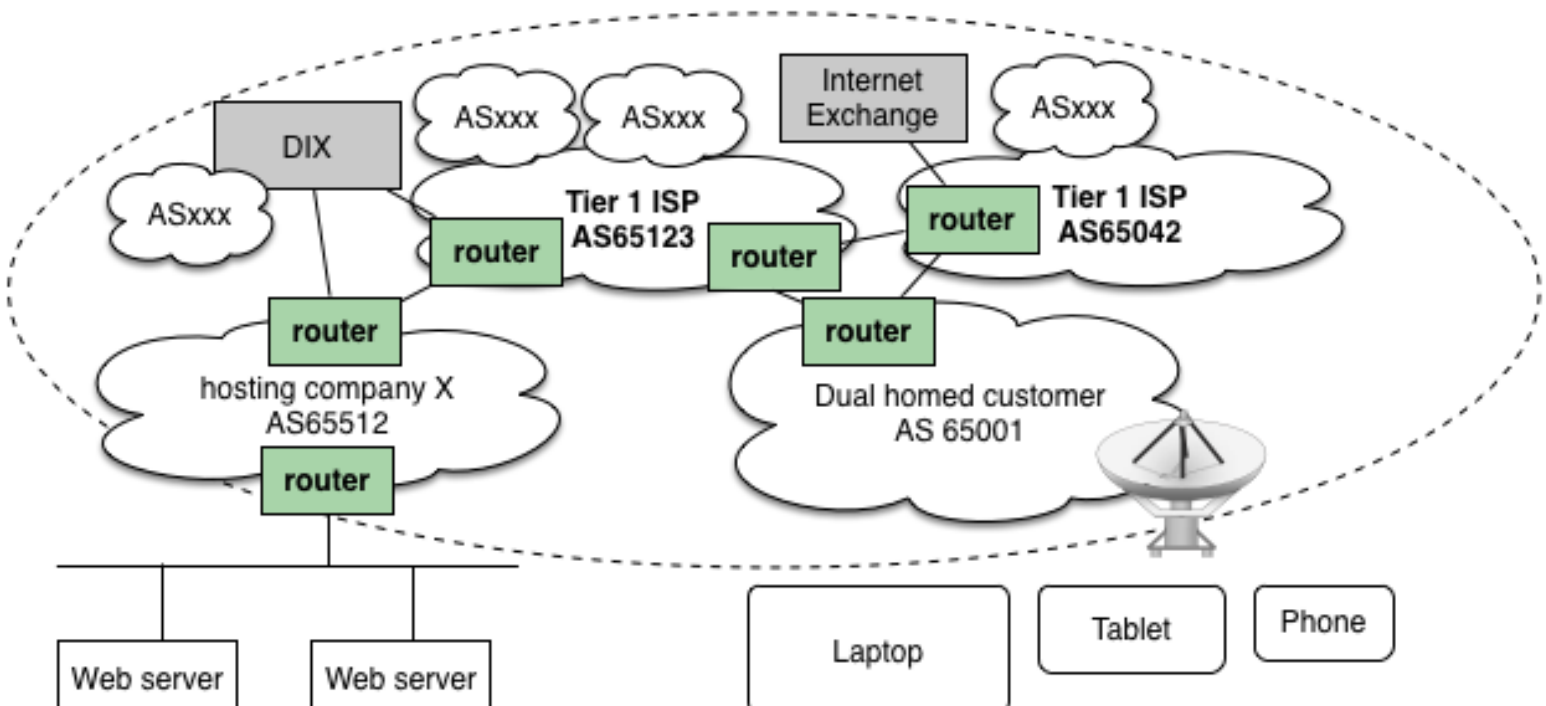
Kilde: Billede er Mandiant's Targeted Attack Lifecycle

Hvad er infrastruktur



- Virksomheder og organizationer har en mængde computersystemer, netværk og data
- Ofte er der et mix af gamle, nyt, under udvikling, under afvikling – forældede
- Samtidig skal vi arbejde tæt sammen med partnere, leverandører m.v.
- Vi har udskiftning i medarbejderstaben – løbende

Hosting and internet providers



BGP networks are used for all of the Internet

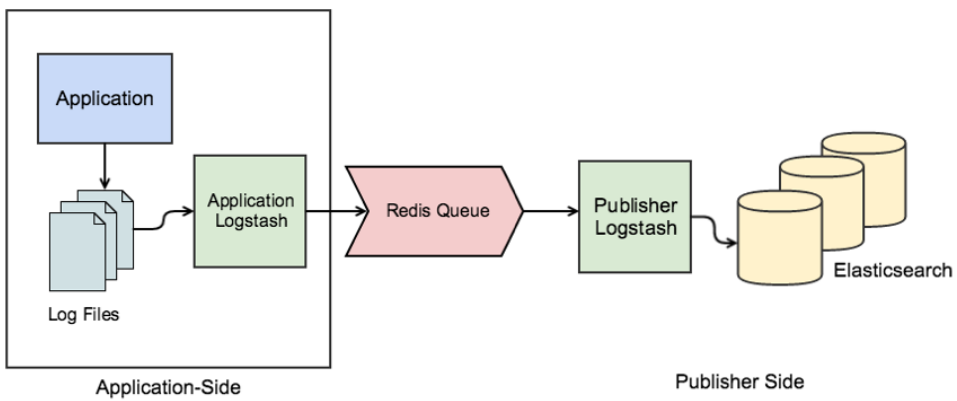
Teknisk logging

```
Jun  5 11:53:15 pumba sshd[64505]: Accepted publickey for hkj from 192.0.2.18 port 43902
ssh2: ED25519 SHA256:l8OJMcabcabcabcbababaqVvlVyfEI
Jun  5 11:53:19 pumba sudo:      hkj : TTY=ttyp2 ; PWD=/home/hkj ; USER=root ; COMMAND=/usr/bin/su -
```

Eksempel loging med Secure Shell (SSH) og kommando `sudo su -`

- Logs er oftest i tekst – mindste (og værste) fællesnævner
- Andre gange mere formelle formater
- Andre gange **binære formater**
- Worst case – proprietære formater uden beskrivelse
- Mange datatyper heriblandt **IP-adresser**, **hostnavne**, **AS numre**, **port numre**, **tidstempler**, **tidszoner**, ...
- Plus **metadata**, hvornår er det opsamlet, hvor er det opsamlet, **GeoIP**

Overview logning



- Find and Collect Relevant Data
- Learn through Iteration
- Find Statistics

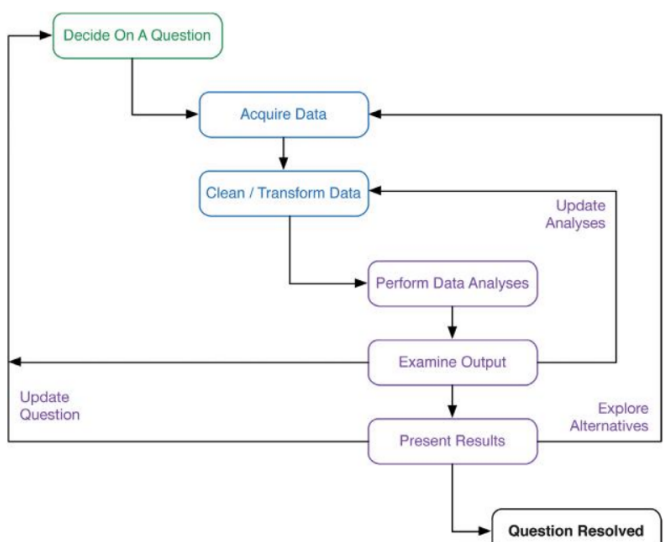


FIGURE 12-2 *The data science workflow*

Source: DDS 12. Moving Toward Data-Driven Security

DNS data og session data

Zeek DNS collection:

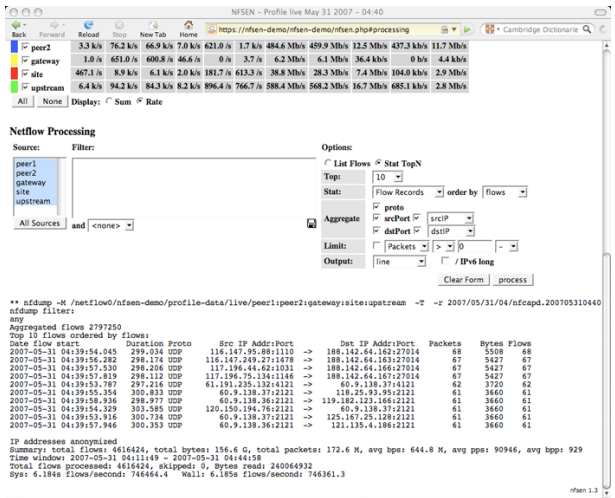
```
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   trans_id
        rtt     query   qclass  qclass_name     qtype   qtype_name      rcode   rcode_name      AA
        TC      RD      RA      Z       answers TTLs    rejected

1538982372.416180 CD12Dc1SpQm42QW4G3 192.0.2.145 57476 192.0.2.141 53 udp 20383
0.045021  www.dr.dk 1 C_INTERNET 1 A 0 NOERROR F F T T 0
www.dr.dk-v1.edgekey.net,e16198.b.akamaiedge.net,2.17.212.93 60.000000,20409.000000,20.000000 F
```

- DNS query logging – will enable multiple cases to be resolved, example malware identification and tracing, when was a malware domain queried, when was the first infection
- Session data from Firewalls, Netflow – traffic patterns can be investigated and both attacks and cases like exfiltration can likely be seen

Jeg anbefaler DNS query logging til firmaer, IKKE til ISPer

Netflow



Network Flows oprindeligt Cisco NetFlow:

Ingress interface (SNMP ifIndex), IP protocol, Source IP address and Destination IP address, Source port for UDP or TCP, 0 for other protocols, Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols, IP Type of Service

Jeg anbefaler Netflow logging til firmaer, IKKE til ISPer

A warning about dates!

```
$ cal 9 1752
   September 1752
Su Mo Tu We Th Fr Sa
        1  2 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
```

- Dates can be tricky
- Use a standard date format ISO 8601
- *Falsehoods programmers believe about time*
  `https://infiniteundo.com/post/25326999628/falsehoods-programmers-believe-about-time`
- Updated with more:
  `https://infiniteundo.com/post/25509354022/more-falsehoods-programmers-believe-about-time`

Computere konverterer hele tiden mellem forskellige data typer, ofte med fejl

Konvertering af data – Ofte sker der fejl

Don't use spreadsheets! Spreadsheets are great for some tasks, but ...

- They don't scale
- The model can be broken – edit a single formula
- Rounding errors accumulate
- Input and output are limited
- Most functions require manual work

- Dato og tidstempler er evig kilde til problemer
- Fortolkning af fri tekst
- Uventede data
- Manglende data
- Direkte forkerte inddata

Grok expresssions, sample from my archive

```
filter {
# decode some SSHD
if [syslog_program] == "sshd" {
  grok {
# May 20 10:27:08 odn1-nsm-01 sshd[4554]: Accepted publickey for hlk from
10.50.11.17 port 50365 ssh2: DSA 9e:fd:3b:3d:fc:11:0e:b9:bd:22:71:a9:36:d8:06:c7

match => { "message" => "%{SYSLOGTIMESTAMP:timestamp} %{HOSTNAME:host_target}
sshd\[%{BASE10NUM}\]: Accepted publickey for %{USERNAME:username} from
  %{IP:src_ip} port %{BASE10NUM:port} ssh2" }

# "May 20 10:27:08 odn1-nsm-01 sshd[4554]: pam_unix(sshd:session):
session opened for user hlk by (uid=0)"
match => { "message" => "%{SYSLOGTIMESTAMP:timestamp} %{HOSTNAME:host_target}
sshd\[%{BASE10NUM}\]: pam_unix\(sshd:session\): session opened for user
%{USERNAME:username}" }
```

- Logstash filter expressions grok can normalize and split data into fields
- Dependent on certain text input, very fragile method

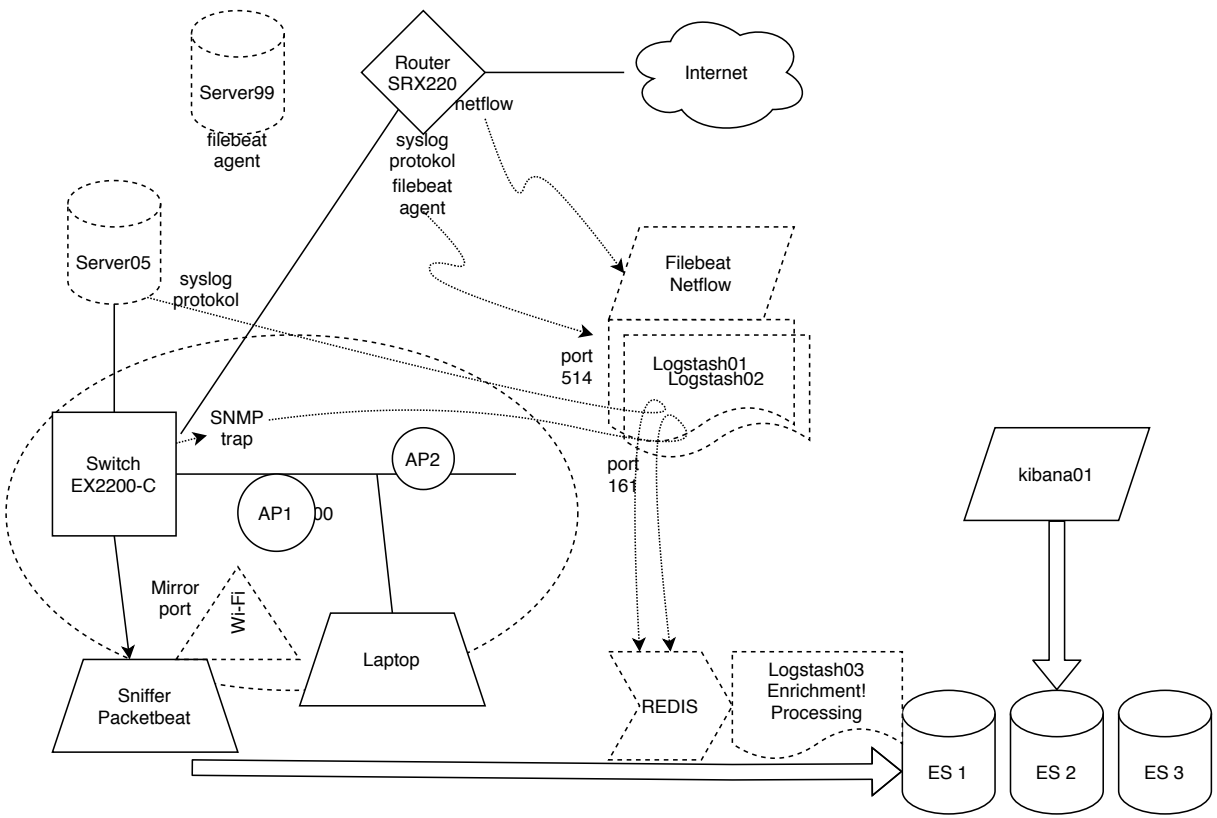
Problemer i logning

- True Positive (TP). An alert that has correctly identified a specific activity. If a signature was designed to detect a certain type of malware, and an alert is generated when that malware is launched on a system, this would be a true positive, which is what we strive for with every deployed signature.Indicators of Compromise and Signatures
- **False Positive (FP)**. An alert has **incorrectly identified a specific activity**. If a signature was designed to detect a specific type of malware, and an alert is generated for an instance in which that malware was not present, this would be a false positive.
- True Negative (TN). An alert has correctly not been generated when a specific activity has not occurred. If a signature was designed to detect a certain type of malware, and no alert is generated without that malware being launched, then this is a true negative, which is also desirable. This is difficult, if not impossible, to quantify in terms of NSM detection.
- **False Negative (FN)**. An alert has incorrectly not been generated when a specific activity **has occurred**.

Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

- Hvor er loggen – på systemerne er den sårbar overfor ændringer
- Gemt hvor ingen ser den og ingen bruger den – har jeg set gentagne gange
- I formater som ikke direkte kan bruges

Centraliseret logning – SIEM Infrastructure



SIEM

Security information and event management (SIEM) is a subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes.[1]

The term and the initialism SIEM was coined by Mark Nicolett and Amrit Williams of Gartner in 2005.[2]

Source: `https://en.wikipedia.org/wiki/Security_information_and_event_management`

- Note: there are alerting examples towards the bottom of the page, with sources
- Closely related to log management, incident response

SOC

> An information security operations center (ISOC or SOC) is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.
>
> ...
>
> A security operations center (SOC) can also be called a security defense center (SDC), security analytics center (SAC), network security operations center (NSOC),[3] security intelligence center, cyber security center, threat defense center, security intelligence and operations center (SIOC).

Source: `https://en.wikipedia.org/wiki/Information_security_operations_center`

- Større danske virksomheder overvåger selv, eller har outsourcet
- Små og mellem store (SMV) har ringe eller ingen logning

Konklusion: Logning er et stort emne

- Logning er stort og komplekst
- Nogle firmaer har årelange projekter med implementering af logning

CIS Controls also recommend Incident Response

> **CIS20 Control 19:**
> Incident Response and Management Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf from `https://www.cisecurity.org/controls/`