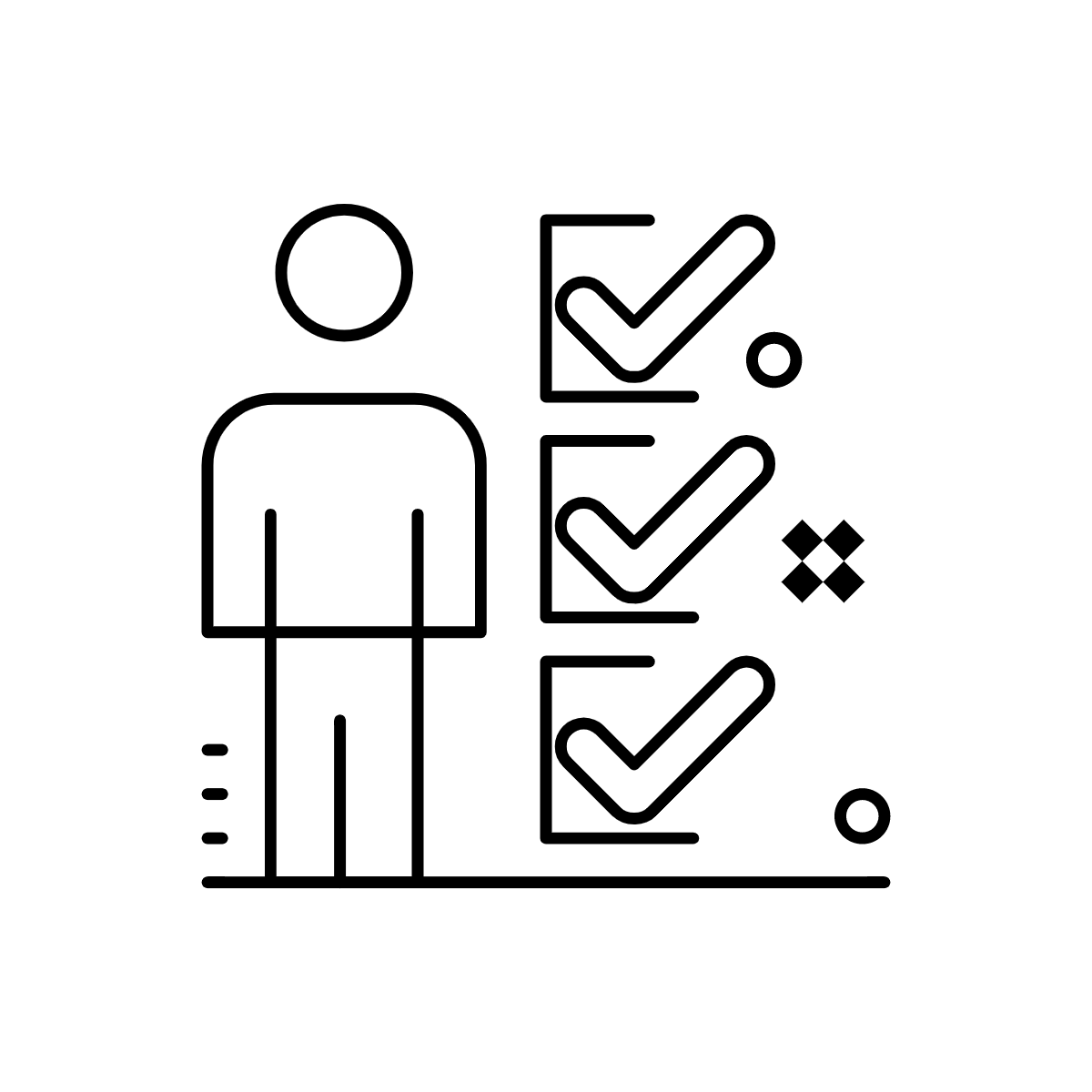
Tjekliste

Bilag: SIR Tjekliste  
Udarbejdet af Lars Blomgaard - [XLEB@kea.dk](mailto:XLEB@kea.dk), defencia.dk****

**Skal udskrives og ligges i jumpbag i aflåst rum og tasken skal plomberes.**

Husk, at dette er kun vejledende, det er en god ide, at have ekstra papir og mappe med plads til beskrivelse af artefakt fund. Når artefakter findes, beskriv fundet. Eks hvilke system og version af systemet. hvem fandt det og dato tidspunkt for fundet.

**HUSK: Begrundet gyldig viden**

# 

# **Information til ansvarlige**

Inden noget andet foretages, informeres ledelsen og der skal tildeles en ansvarlig leder for Security Incident Response.

Dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sagsnummer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SLA level: ▢ GULD (24x7x365) ▢ SØLV (24x5x365) ▢ BRONZE (8:00 til 16:00 x 5)

Navn på ansvarlig SIR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Navn på ansvarlig IR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Navn Informationsansvarlig: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Navn Dataansvarlig: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Informations interval timer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ GDPR sag

Hvis GDPR sag, hvem er informeret: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Brugere

▢ Ledelse

Dato og tidspunkt for opdagelse af incident: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Information til eksterne parter via ??

E-mail, hjemmeside

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 

# **Information til ansvarlige**

**HUSK informere** følgende personer/ afdelinger.

▢ Backup ansvarlig

▢ Netværk

▢ Service desk

▢ Server teamet

▢ Ledelse

▢ Service account managere

Myndigheder : Navn / tlf / email

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Leder Informeret Dato / tidspunkt:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chef / IT-ledelse Informere Dato / tidspunkt:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hændelse (beskrevet i korte termer):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Indicator Of Compromise (IOC) (Hvilken alarm i hvilket system blev aktiveret)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Systemets Version?: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signatur(AV miljø):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Preperation**

## Jump Bag

▢ Jump Bag forseglet ?

Hvad manglede? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ansvarlig for indhentning: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dato for sidste tjek \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Person ansvarlig for tjek: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Indhold

▢ Papir og kuglepen

▢ 3 x USB 64 GB

▢ 1 x 2 TB USB harddisk.

▢ USB 64 gb “toolbox”

▢ Write Blocker

▢ Computer

▢ Netværkskabel

▢ 2 x Vand 2 x Protein bar

▢ 10 x Forseglings poser

▢ Write Blocker

## Forensics rummet

▢ Stationær Computer med Linux og VM miljø

▢ 10 SSd Harddiske 240 GB; Mærke : \_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ 1 x 4 TB USB harddisk.

▢ 2 x NAS

## Computer til forensics og analyse

Er udstyret opdateret ?

Hvornår er der sidst opdateret ? (Se Drifts Seddel[[1]](#footnote-0))

Version af VM Software (VMware): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Version af Host OS Software (Linux): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Version af VM OS Software (Linux/WinXX): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ved afvigelser, kontakt nærmeste leder/ansvarlige

Dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ansvarlige informeret. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Forensics Netværk til ADSL

▢ Router IP-adresse: 192.168.1.1

▢ Switch IP-adresse: 192.168.1.2

▢ DNS filter IP-adresse: 192.168.1.3

▢ Maltrail system (sensor / server) IP-adresse: 192.168.1.4

▢ TCPdump maskine IP-adresse: 192.168.1.5

▢ Maskine 1 (Kali Linux) IP-adresse: 192.168.1.6

▢ Maskine 2 (Debian Linux / SFTP[[2]](#footnote-1)) IP-adresse: 192.168.1.7

Dato for sidste tjek? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Identification**

Fase for identifikation af angrebet

Hvilken IOC blev aktiveret og hvor mange alarmer?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Automatiseringer specifikt for incident

▢ Antivirus rapport udtræk Dato / tidspunkt for oprettelse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ IDS rapport Dato / tidspunkt for oprettelse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Proxy Dato / tidspunkt for oprettelse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Firewall Dato / tidspunkt for oprettelse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Log mgmt. Dato / tidspunkt for oprettelse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Kontakt til samarbejdspartnere. (informere dem om vigtigheden baseret på SLA.)

▢ Cisco Dato / tidspunkt for oprettelse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Juniper Dato / tidspunkt for oprettelse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ McAfee Dato / tidspunkt for oprettelse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Beskriv selv teknologi

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Artefakter

Her skal hver artefakt beskrives. Hvor blev den fundet?

Hvilket tool (IDS, Antivirus, proxy, Bruger, Computer), var artefakterne skjulte eller tilgængelige? var de sat på autorun og hvilke priveliger+

Artefakt A

▢Autorun ▢Service, navn på service:\_\_\_\_\_\_\_\_ ▢Skjult ?

Hvilket tool fangede denne ? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hash: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Er filen testet på malwr.com og eller virustotal.com?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Beskrivelse:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dato for dataopsamling? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ansvarlig for dataopsamling? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data sikret med Imager? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Version af Imager? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

MD5 af samlede pakke? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SHA256 af samlede pakke? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Hvis disciplinærsag

Der skal udarbejde separat dokument for dette. Se forensics rummet hylde 4.

Encase eller Tableau witeblocker ligger på Hylde 5. CD-rommer med Caine ligger på samme hylde med CD-rom drevet til USB.

Forensics computeren har Software write blocker installeret.

Dato for afhentning :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Afhentet af? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Bruger :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Computernavn :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Andre effekter:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢Data Sikret?

▢write blocket udlæsning?

▢Ikke writeblocket udlæsning?

Hvorfor ikke write blocket? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢Computer sat i forensics rummet ?

Placering: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Kasse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Er medarbejder bortvist?

▢ Nej

▢ Ja og på hvilket grundlag? : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Skal data sikres til retssag?

Ovenstående skal gemmes, som E01 eller AD01 filer. Til udlevering af retten / rette myndigheder, med henblik på analyse.

**VIGTIGT:**

**ALLE FILER SKAL HAVE EN HASH VÆRDI, INDEN DE FORLADER OMRÅDET!**

**ALLE DATA SKAL VÆRE PÅ KRYPTEREDE ENHEDER!**

# 

# 

# **Containment**

1. Pak alle artefakter / filer fundet i en mappe i et sikkert miljø (ex Linux).

**VIGTIGT!! I denne mappe skal alle nytilkomne artefakter tilføjes, så det ender med en samlet “database” over alle fundene artefakter. Vigtigt til step 2**Navn og kode til filen er således “infected.zip” og kode = infected

1. Pak dem ud på en “stand alone” test maskine, med samme patch og signatur niveau som på produktions netværket.
2. Scan med Antivirus og notere resultat

Hvor mange filer stod tilbage efter udpakning?

(For at tjekke hvor mange filer og artefakter der bliver detekteret)

Signatur / dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signatur / dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signatur / dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signatur / dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signatur / dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signatur / dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hvilke systemer har fået blokeret services for nedlukning.

▢ Antivirus rapport udtræk Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ IDS / IPS Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Proxy Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Firewall Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Log mgmt. Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Share drev / server Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ carbon black (app whitelist) Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Eradication**

Hvilke systemer Har fået seneste signaturer som kan eradikere artefakter / malware?

▢ Antivirus rapport udtræk Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ IDS / IPS Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Proxy Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Firewall Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Log mgmt. Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Share drev / server Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ carbon black (app whitelist) Dato / Handling. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Backup ansvarlig?: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Servicedesk ansvarlig til sager?: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 

# 

# 

# 

# 

# 

# **Lessons Learned**

Mødedato:

Hvem var fremmødte?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Punkter til notits efter Incident (Hvad gik godt og hvad skal gøres bedre?).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hvad skal tilføjes til Preparation fasen?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hvad skal tilføjes til firmapolitikker (hvis noget)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Eventuelt?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Datapakke til Politiet**

<Data som samlet til Politiet beskrives og gerne med hashes og versioner af software anvendt. >

JNR nummer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Forpost / medarbejder:

Navn: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tlf: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

e-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hvordan er Filer Pakket ? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Versionsnummer af software ? :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Harddisk nummer udleveret?: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

MD5: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SHA: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

▢ Incident rapport udleveret sammen med ovenstående.

# **Liste over teknikere og samarbejdspartnere**

Navn på vendor

Kontakt SIKKERHEDSVIRKSOMHED

TELEFON: +45 12 34 56 78

EMAIL: Emai[at]virksomhed.dk

AV leverandør

TELEFON tlf 1-111-2223-4444

EMAIL : Emai[at]virksomhed.dk

IT afdelingen

Int 1234

ekstern: 451234567

Chefen (Opdateret 15/4-2019)

Navn

Telefon +45 50 50 50 51

E-mail: [chef@etstedi.dk](mailto:chef@etstedi.dk)

# **Version**

| Dato | Ændring | Godkendt | kommentar |
| --- | --- | --- | --- |
| 14/12/2020 | **Version 1**  Nyt dokument | Leder XX XXXXX | Tilrettet og klargjort |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Se drifts seddel som ansvarlig bør udfylde for hver vedligeholdelses tidspunkt. Dette bør fremgå hvornår systemet er opdateret sidst. [↑](#footnote-ref-0)
2. Denne maskine skal kun tændes efter behov. Tjek, at en 4 TB harddisk kan ses i systemet. Denne maskine er opsamlingspunkt for data. HUSK gem som “infected.zip” og kode “infected (Uden “) [↑](#footnote-ref-1)