SIR Overview

Security Incident Response = SIR (DFIR)

Post incident activity

- Samling af alle invilverede til debriefing
- Hvad gik godt hvad gik skidt
  - Hvad kan vi lære af det?
- Forankring af nyt udstyr og dokumentation af dette
- SIR rapporten
  - Hvad er opsamling på hele incidentet.
- Opsamling og opfølgning af dokumentation til Preperation fasen. Opdatering af Governance og dokumentation og systemer

Preperation

- Ledelses opbakning
- Jump bag
- Udskrifter af dokumenter
- Labs
  - Oprettede og klar til brug
  - Eller klar til at installere ?
- Software og strategi klar
- Logs. Har vi adgang til at få dem?

Detection

- Hvordan kommer alarmene ind?
- Hvilke systemer giver alarmer?
- Hvad siger vores IDS, SIEM, IPS
- Har vi adgang til logs (Fra ovenstående)?
- Klargøring af Labs
- Har vi et warroom?
  hvordan bliver der kommunikeret
  Hvem sørger for det praktiske? (Mad og drikke)
  Kommunikation til partnere

Analyse

- Anvendelsen af analyse output?
  - Hvordan vil vi analysere og hvad forventer vi at få ud?
- Hvad har vi af artefakter?
  - Hvordan fik vi dem?
  - Hvor ligger filerne og er de samlet ?

Containment

- Hvad lærte vi af analyse fasen
- Hvordan kan vi hæmme spredning
- Hvordan fjerner vi inficeret udstyr?
- Ledelsen skal godkende valg i denne her fase, da de kan have stor indvirkning på fremtidige resultater
- Klargøring til Eradication and Recovery

Eradication and Recovery

- Hvordan genskaber vi?
- Hvad gør vi med re-.installeringer og hvad skal re-installeres?
- Kan vi scanne efter artefakter?
- Vi skal alligne med ansvarlige for BCP og Disaster recovery
- Etablere ekstra monitorering for systemerne og aftale tidshorrisont for ekstra monitorfase