SOC

Stage MPI Oosterlo
Michiel Kuyken

Inhoud

- Achtergrond
  - Wie?
  - Wat?
- Business case
- Doelstelling
- Planning
- Project scope
  - MoSCoW-analyse
  - Risico-analyse
  - Aflevering

Achtergrond

Wie?

- MPI Oosterlo vzw
- Zorginstelling mensen verstandelijke beperking
- BKLO en BUSO

Wat?

- SOC
  - Dashboard
  - CVE detectie
  - Meldingen via Teams
  - Mogelijkheden Wazuh
  - Integratie Crowdsec
- Meedraaien helpdesk en lopende projecten

Business Case

Business Case

- Bescherming
- Snelle incidentrespons
- Continue monitoring
- Compliance met GDPR, NIS2,…

Business Case

- Bescherming cliënt gegevens
- Automatisering
  - Veel on-premise
  - Veel tijd in kleine foutjes oplossen

Doelstelling

Doelstelling

- SIEM (Security Information and Event Management)
  - Wazuh
- SOAR (Security orchestration, automation and response)
  - TheHive
  - Cortex
  - Virustotal
  - Shuffle
  - Teams/Outlook
- Threat Intel
  - STIX/TAXII
  - MISP
  - Crowdsec

Doelstelling

- Protection
  - Crowdsec
  - ClamAV
- Collection
  - Suricata/Snort
  - Zeek
  - Graylog
  - Yara/Sigma
- Threat hunting
  - Velociraptor

Planning

Planning

- Week 1-3:
  - Projectplan uitwerken
- Week 4-8:
  - SIEM + SOAR realiseren
- Week 8-11:
  - Meldingen toepassen
  - Threat Intel integreren
- Week 12-13:
  - Collection implementeren
- Tijd over:
  - Threat hunting implementeren
  - Protection realiseren

9	24/2	Initiation phase	Internship 1
10	3/3		Internship 2: kick-off meeting
11	10/3		Internship 3
12	17/3	Realization phase	Internship 4: 1st meeting at school
13	24/3		Internship 5
14	31/3		Internship 6: intermediate internship evaluation
15	7/4		Internship 7
16	14/4		Internship 8: 2nd meeting at school
17	21/4		Internship 9
18	28/4		Internship 10
19	5/5		Internship 11
20	12/5		Internship 12: submit internship evidence documents for review
21	19/5		Internship 13

Project scope

MoSCoW-analyse

Must have	Should have	Could have	Won't have
SIEM	Collection	Threat hunting	Audit
SOAR		Protection	
Meldingen			
Threat intel			

Risico-analyse

- Alle endpoints mogelijk?
- False positives
- Problemen integratie scholen

Aflevering

- Werkend SOC
  - Alerts genereren
  - Alerts analyseren
  - Alerts automatisch afhandelen
  - Centraal dashboard
  - Melding sturen
- Realisatiedocument
- Handleidingen

Bedankt