Nagios & Squared up (SCOM)

SECURITY – LOGS ANALYSEREN / FILTEREN / DASHBOARDS

PVA

Bachelor in de Elektronica-ICT
keuzerichting Cloud en Cyber security

Timo Goossens

Academiejaar 2023-2024

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

Inhoud

1 INLEIDING 4

2 PLAN VAN AANPAK 5

2.1 De kennismaking met de omgeving 5
2.2 Praktisch gedeelte 5

1 INLEIDING

Beste lezer, dit document bevat de nodige documentatie voor mijn plan van aanpak. Het plan van aanpak wordt uitgelegd aan de hand van mijn ervaring en hoe ik het ga aanpakken.

2 PLAN VAN AANPAK

2.1 De kennismaking met de omgeving

Het begint allemaal met de kennismaking van de producten die ik ga gebruiken. Hier ga ik kennismaken met Nagios en Squared up/SCOM.

Tijd: 2/3 weken

2.2 Praktisch gedeelte

Aan de start van dit gedeelte mag ik experimenteren met de producten om de feeling te krijgen en daarna krijg ik een word document waarin de volgende informatie verwerkt is zodat ik een basis heb voor wat ik moet doen.

- Prioriteit
- Wat er moet gemonitord worden
    - Servers
        - Services
          → De grote focus ligt hierop omdat services belangrijke processen zijn en je hier meer uit kan afleiden dan een ping alleen.
    - Extra informatie voor de dashboards/logging
- De experten binnen Essers per onderdeel
- De +- tijd die eraan besteed wordt
  → Dit geldt voor de 2 grote onderdelen Nagios & Squared up/SCOM.

Alles wat niet vernoemd is in deze lijst, is vrij voor mij om te bepalen en als alles goed gaat doet Tommy (mijn stagementor) een wekelijkse meeting met mij om te kijken hoe ver ik sta. In deze wekelijkse meeting wordt er dan bekeken waar de doelstellingen moeten worden bijgestuurd.

Het testen van mijn doelstellingen/realisaties: alerts, filters en query's etc. v/d verschillende servers. Het controleren of deze werken door bv. Alerts naar mezelf te sturen via mail of in Nagios/Squared up zelf door in de dashboards de query's of filters toe te passen.

Tijd: resterende weken → zelf tijd verdelen onder Nagios en Squared up