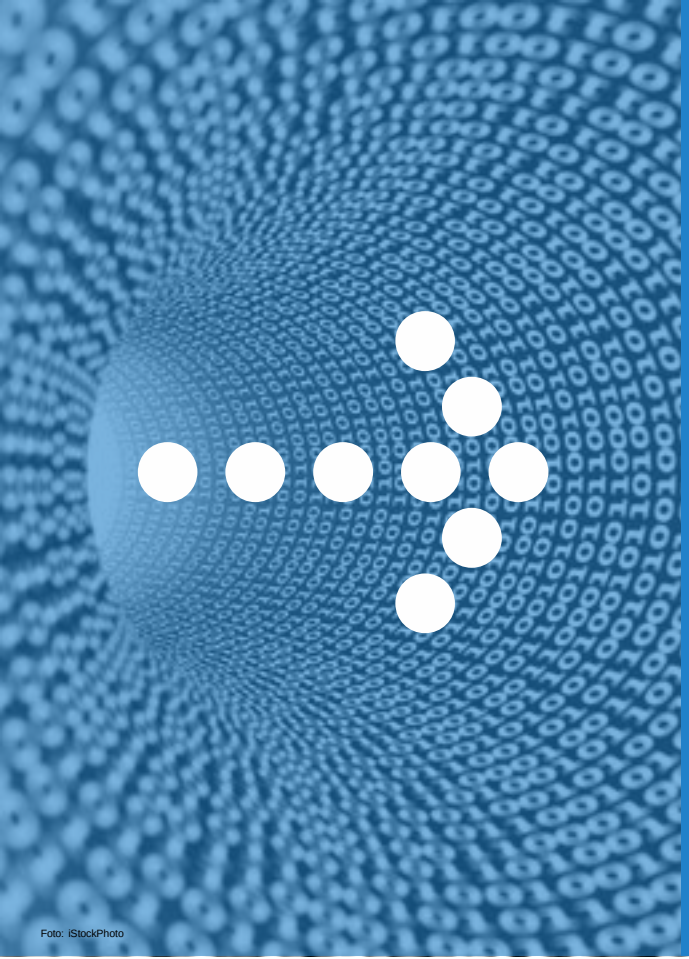


Foto: iStockPhoto

Pass 6
Hantera – Identifiera

Praktisk incidenthantering i industriella informations- och styrsystem

Myndigheten för samhällsskydd och beredskap

NCS3

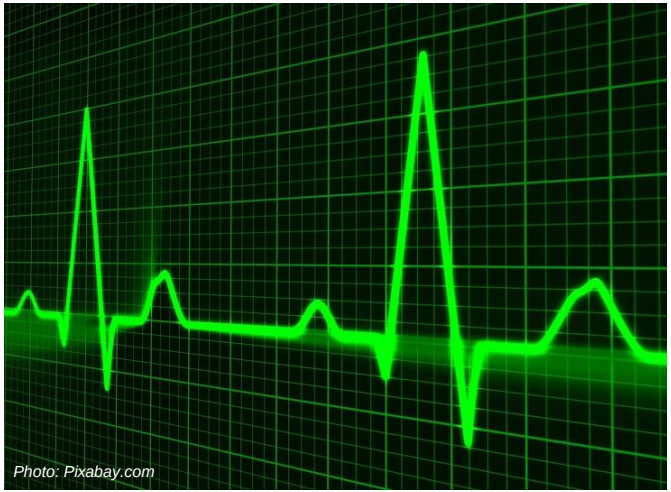
FOI

I detta pass:

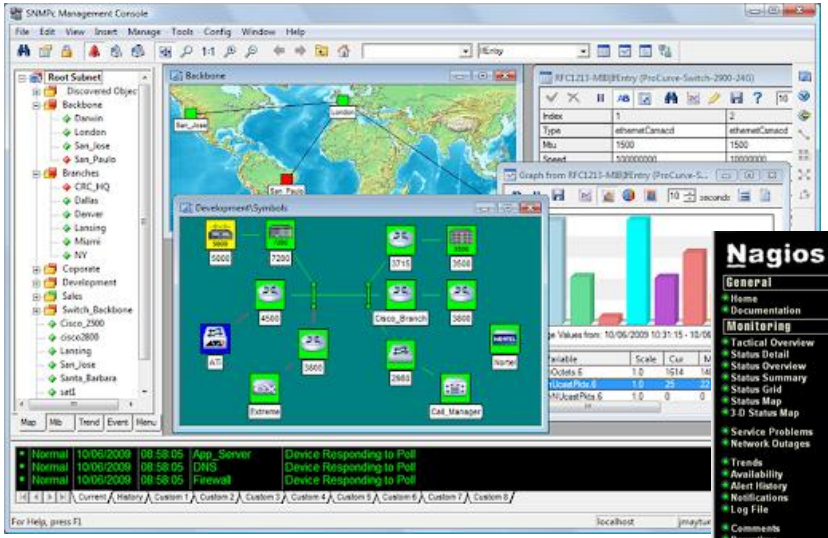
- Övervakningsverktyg
- Relevanta skyddsåtgärder
- Medarbetare
- Analysera vad som händer
- Bedöm vad som kan påverkas
- Planera åtgärder

Övervakningsverktyg

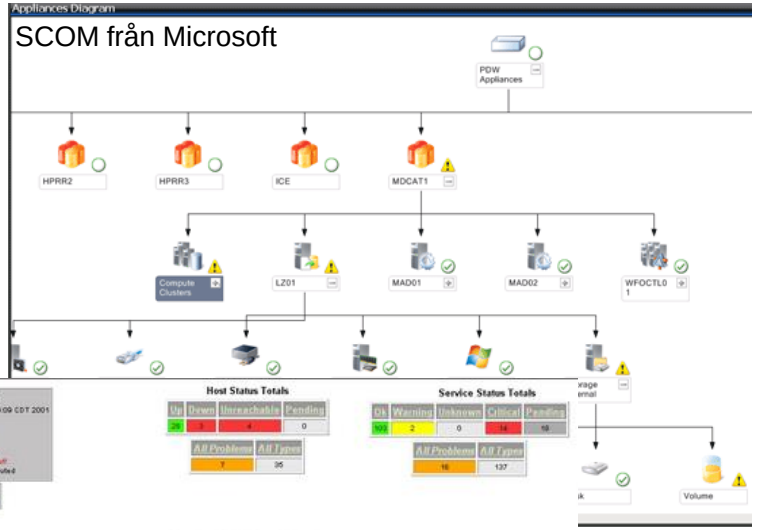
- För detektion av avvikelser
- Exempel
  - Pingers
  - SNMP
  - Tjänsteövervakning
  - Filövervakning
  - Syntetiska operationer
  - SIEM



Exempel



SNMPc från Castlerock



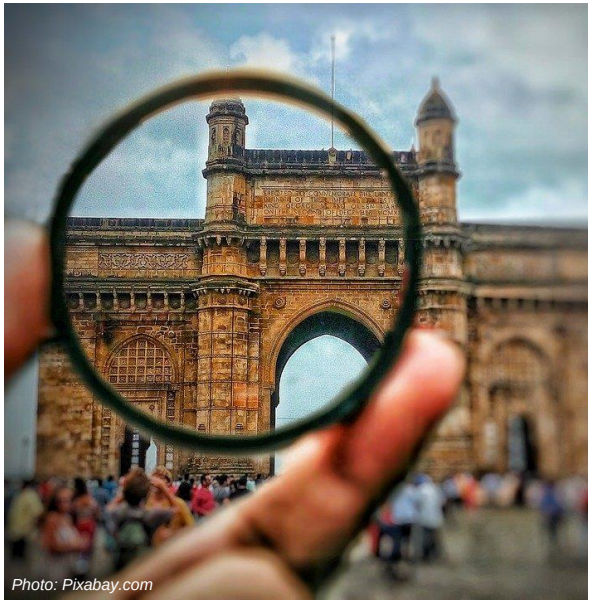
NCS3

Myndigheten för samhällsskydd och beredskap

FOI

Skyddsåtgärder

- Intrution detection prevention (IDP)
- Virusskydd
- Brandväggar och proxies
- Data Leakage Prevention (DLP)
- Loggar och logganalyssystem



Teknisk bevakning

- Eftersträva
  - Automatiserade larm och system
  - Korrekta tröskelvärden
  - Samverkande källor
- Organisation
  - Intern
  - Extern

Omvärldsbevakning

- Håll koll på vad som händer
- Prenumerera på säkerhetsinformation
  - Från Cert.se
  - Från leverantörerna
  - Generella säkerhetsnyheter
- Glöm inte den egna verksamheten!

Medarbetare

- Information från personal
  - Rapporterad misstänkt händelse
  - Innan, under och efter
- Incidentrapportering
  - Omständighet
  - Händelse
  - Incident
  - Hjälper till att undvika incidenter

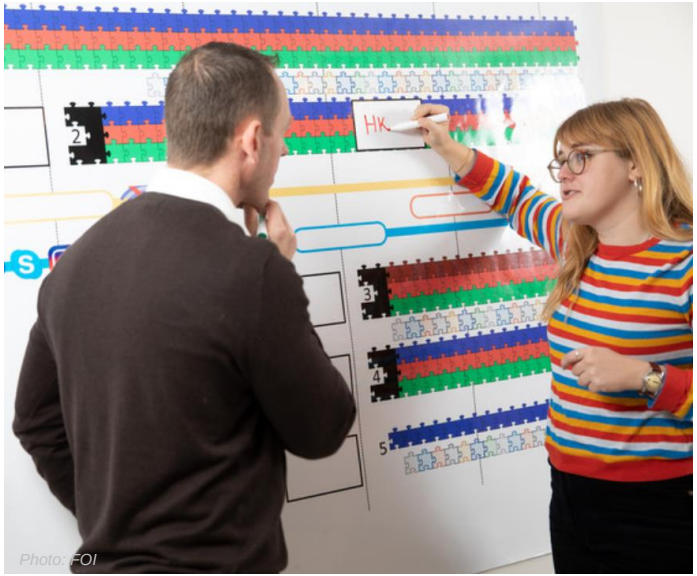

Photo: Pixabay.com

Revision och threathunting

- Görs proaktivt och regelbundet
- Ta in hjälp
- Gör acceptanstest av nya system
- Åtgärda identifierade sårbarheter

Analysera

- Typ av händelse
  - Vad har skett eller vad sker
  - Incident/Avvikelse
- Orsak
  - Hur och varför har det hänt?
- Hur stor påverkan har den
  - Påverkas enskild, grupp eller alla?
  - Påverkas viktiga system?
  - Kan den förvärras?



Plan för hur den kan hanteras

- Behövs mer information?
  - Även uppdaterad info under incidenten
- Akuta åtgärder
  - Begränsa spridning
  - Prioriterade åtgärder
- Åtgärder för att återställa

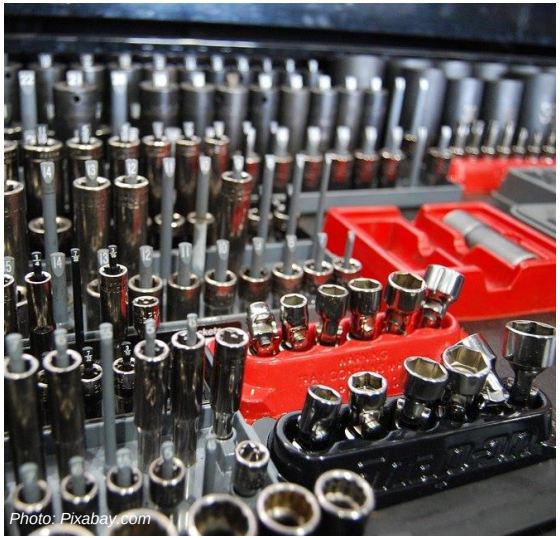


Photo: Pixabay.com

Sammanfattning

- Identifiera incidenten
  - Påverkan
  - Risk för spridning
- Nyttja den indata ni har
  - Behövs mer information?
- Analysera snabbt
- Ta fram en plan för hantering