

# Pass 6

## Hantera – Identifiera

Praktisk incidenthantering i industriella informations- och styrsystem

Foto: iStockPhoto



Myndigheten för  
samhällsskydd  
och beredskap



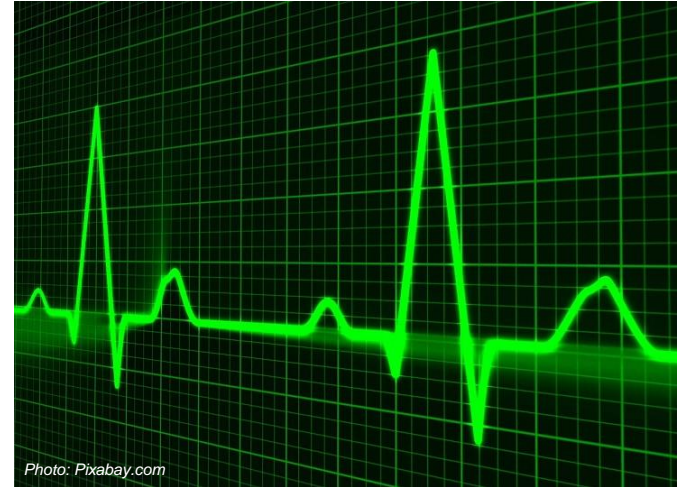
# I detta pass:

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



# Övervakningsverktyg

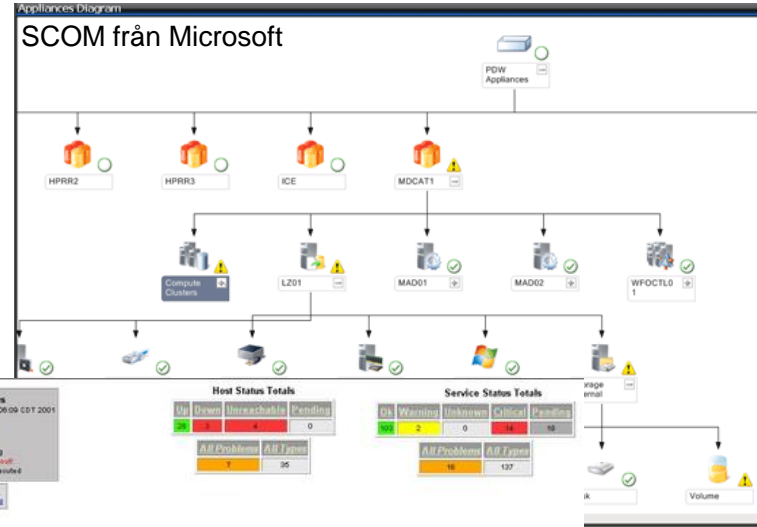
- För detektion av avvikelser
- Exempel
  - Pingers
  - SNMP
  - Tjänsteövervakning
  - Filövervakning
  - Syntetiska operationer
  - SIEM



# Exempel

The screenshot displays the SNMPc Management Console interface. On the left, a tree view shows the network hierarchy: Root Subnet, Backbone, and various branches like Dallas, Denver, and San Jose. The main area features a map of the United States with network nodes and connections. A configuration window for 'R1 CL213-M08Entry (ProCurve-Switch-2900-240)' is open, showing details like Type, Max, and Speed. A Nagios monitoring window is overlaid on the map, showing a network diagram with nodes and their status. A log window at the bottom shows system events.

SNMPc från Castlerock



Service Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Service Information
ABAGE	PNQ	OK	07-15-2001 14:04:00	46:46:7m 13s	5/5	PNQ ok - Packet loss = 0%, RTA = 0.50 ms
ABAGE	PNQ	CRITICAL	07-15-2001 14:04:30	46:35:46m 13s	5/5	CRITICAL - Plugin timed out after 10 seconds
ABAGE1	SMTPDMS...	CRITICAL	07-15-2001 14:00:30	46:45:1m 45s	5/5	(Service Check Timed Out)
ABAGE1	PNQ	CRITICAL	07-15-2001 14:02:30	46:45:1m 45s	5/5	CRITICAL - Plugin timed out after 10 seconds
ABAGE2	PNQ	CRITICAL	07-15-2001 14:04:00	46:35:47m 23s	5/5	(Service Check Timed Out)
ABAGE2	SMTPDMS...	CRITICAL	07-15-2001 14:04:30	46:35:46m 22s	5/5	(Service Check Timed Out)
ABAGE2	PNQ	CRITICAL	07-15-2001 14:05:30	46:35:46m 3s	5/5	CRITICAL - Plugin timed out after 10 seconds
ABAGE2	SMTPDMS...	CRITICAL	07-15-2001 14:02:30	46:35:33m 31s	5/5	(Service Check Timed Out)
ABAGE3	PNQ	CRITICAL	07-15-2001 14:04:00	46:35:46m 31s	5/5	CRITICAL - Plugin timed out after 10 seconds
ABAGE3	SMTPDMS...	CRITICAL	07-15-2001 14:04:30	46:35:45m 22s	5/5	(Service Check Timed Out)
ABAGE4	PNQ	CRITICAL	07-15-2001 14:05:40	46:35:44m 3s	5/5	CRITICAL - Plugin timed out after 10 seconds
ABAGE4	SMTPDMS...	CRITICAL	07-15-2001 14:02:30	46:35:33m 21s	5/5	(Service Check Timed Out)
ABAGE5	SMTPDMS...	CRITICAL	07-15-2001 14:02:30	46:35:38m 2m	0/1	Service check is not scheduled for execution...
ABAGE5	SMTPDMS...	CRITICAL	07-15-2001 14:02:30	46:35:38m 2m	0/1	Service check is not scheduled for execution...
ABAGE5	SMTPDMS...	CRITICAL	07-15-2001 14:02:30	46:35:38m 2m	0/1	Service check is not scheduled for execution...
ABAGE5	PNQ	OK	07-15-2001 14:02:30	46:46:5m 14s	5/5	PNQ ok - Packet loss = 0%, RTA = 0.50 ms
ABAGE5	PNQ	OK	07-15-2001 14:04:01	46:35:47m 34s	5/5	PNQ ok - Packet loss = 0%, RTA = 0.50 ms

The Nagios monitoring interface sidebar includes the following sections:
 

- General**
  - Home
  - Documentation
  - Monitoring
  - Tactical Overview
  - Status Detail
  - Status Overview
  - Status Summary
  - Status Grid
  - Status Map
  - 3-D Status Map
- Service Problems**
  - Network Outages
  - Trends
  - Availability
  - Alert History
  - Notifications
  - Log File
  - Comments
  - Downtime
  - Process Info
  - Performance Info
- Configuration**
  - View Config

# Skyddsåtgärder

- Intrusion detection prevention (IDP)
- Virussydd
- Brandväggar och proxies
- Data Leakage Prevention (DLP)
- Loggar och logganalysystem





# 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





# Revision och threathunting

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



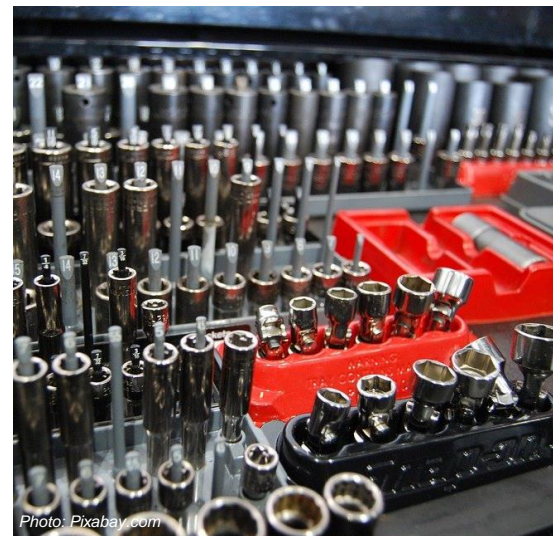
# Analysera

- 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



# Sammanfattning

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

