To: 5.1.2e 2e @dji.minjus.nl]; 5.1.2e 5.1.2e [5.1.2e @dji.minjus.nl]; 5.1.2e , 5.1.2e [5.1.2e @dji.minjus.nl]; 5.1.2e , 5.1.2e [5.1.2e @dji.minjus.nl]; 5.1.2e , 5.1.2e de[5.1.2e @dji.minjus.nl]; 5.1.2e , 5.1.2e de[5.1.2e @jio.nl]
Cc: 5.1.2e 5.1.2e 1.2e @dji.minjus.nl]; 5.1.2e 5.1.2e [5.1.2e @dji.minjus.nl]
From: 5.1.2e 5.1.2e
Sent: Tue 7/22/2025 3:38:00 PM
Subject: handelingsperspectief
Received: Tue 7/22/2025 3:38:01 PM

Een eerste aanzet, handelingsperspectief en een opsomming

- **Back up offline/integriteit**
  - Uitwijk
- **Monitoring uitbreiden (5.1.2h of 5.1.2f)**
  -
  - 5.1.2h 5.1.2e uitkomst uiterlijk vrijdag
  - DC's ℌ Via 5.1.2f agent
  - DWO ℌ vrijdag nieuwe config van 5.1.2h voor DWO, volgende week bouwen en testen (tot 6 augustus), daarna uitrollen en aanzetten (tot 15 augustus)
  - DWO ℌ Tot half augustus met 5.1.2f agent
- **Whitelisting**
  - Als er gesproken wordt over de Internet verbinding door te knippen. NetScalers van Connect zijn qua kwetsbaarheid gedicht en de NetScaler beheerders richten voor de zekerheid een 5.1.2h deze week in. Dus geen issue meer aan de kant van Connect
  - Als de hackers geslaagd zijn om dieper binnen te dringen zit nu het probleem waarschijnlijk in DWO. Dan is niet de NetScaler de Internet opgang, maar onze proxy server (webgateway) 5.1.2h 5.1.2h).
  - Onze proxy server werkt 5.1.2h 5.1.2h , waarbij je in feite Internet toegang vanaf DWO uitschakelt behalve de benodigde toegang voor bijvoorbeeld 5.1.2h 5.1.2h e.d. Bij het opstellen van de whitelist moet wel opgepast worden dat we het niet te ver openzetten door de applicaties.
- **Kroonjuwelen**
  - 5.1.2h ℌ Alle 5.1.2h applicaties (dus ook alle 5.1.2h varianten) zijn in zijn geheel via 5.1.2h gekoppeld aan het SIEM.
  - 5.1.2h ℌ Alle linux is voorzien van 5.1.2h en aangesloten op het SIEM
  - 5.1.2h ℌ Alle linux is voorzien van 5.1.2h en aangesloten op het SIEM
  - 5.1.2h ℌ Alle linux is voorzien van 5.1.2h en aangesloten op het SIEM