Hello,
Here my assumption. I dont expect to pass this challenge, but is it still possible to have challenge 3 and 4 even without participating?

Assumptions:
Assumption 0: The intruder is operating on the earth's DC.
Action 0: Perform BAU (antivirus update, system patching, application and system upgrade, system monitoring…), Use passive tools to track back the intruder to avoid more leak and secure earth reconquest. Justification 0: Use the same technic as an intruder to execute agent (clean log, clean tmp file, use system stream, small technical software…)

Assumption 1: Data are modify, we do not know since we they are modify or read by the intruder
Action 1: Set up an File Integrity Monitoring Infrastructure Justification 1: By using a File Integrity Monitoring we can tract the change, who, when a file has been accessed. Product Cimcor to use agent and agentless.

Assumption 2: The data can be moved (leaks, copy/past, mailed, whatever)
Action 2: Set up an Data Loss Prevention infrastructure Justification 2: A Data Loss Prevention track data leaks. Use GreenCode appliance for TrueDLP (network, and discovery).

Assumption 3: The system have vulnerability
Action 3: Use a Passive Vulnerability Scanner and a Remote Vulnerability Scanner (OS level) Justification 3: identify all the vulnerability on the system. Use tenable 2 appliance one for the PVS and Nessus and 1 for Security Center continuous view

Assumption 4: When time to clean up the system, automate the action and do it in one shot Action 4: all component of the system must be cleaned up at the same time, hardened… Justification: deploy local agent for desired state of configuration to perform the action of cleaning, patching, upgrade and hardening (script, vro)

Assumption 5: the passive PRA system on mars it a bit to bit copy, on a second network core lockdown, without external communication possibility in nominal state.
Action 5: Use this passive PRA system to track the information modify on the earth DC, to fix it there and perform a full roll out of a cleaned infrastructure from the PRA to the earth DC. Justification 5: one's all to keep earth dc on control back, better lose data and time than all control the earth dc
Best regards,

Manuel Heurtin.