Pre assessment 3rd try

Wednesday, October 25, 2023 6:22 PM

threat hunting = threats
- vuln scanning =/= threats

separation of duties = single point of failure

hashes are the same = infected when downloaded

incident response
- preparation
- identification
- containment
- eradication
- response and recovery
- lessons learned

you are already given hard drive = use dd
- order of volatility doesn't matter
- chain of custody "already created"
- memdump = memory not drive

tokenization stores token instead of card info