Endpoint Analysis

This is where the Defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.

TOOLS

DeepBlueCLI
Velociraptor
SANS IR Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

https://www.velocidex.com/

CDV2_0421

Backdoors & Breaches™

PROCEDURES

Created by: BLACK HILLS | Information Security