User and Entity Behavior Analytics (UEBA)

It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, password sprays, and more!

TOOLS

LogonTracer
DeepBlueCLI
OpenUBA

https://github.com/JPCERTCC/LogonTracer

http://openuba.org/

CDV2_0421

Backdoors™ & Breaches

PROCEDURES

Created by: BLACK HILLS | Information Security