Security Information and Event Management (SIEM) Log Analysis

Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tool Analysis

JPCERT CC®

https://github.com/philhagen/sof-elk

https://jpcertcc.github.io/ToolAnalysisResultSheet

CDV2_0421

Backdoors™ & Breaches

PROCEDURES

Created by: BLACK HILLS | Information Security