Network Threat Hunting - Zeek/RITA Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/RITA/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AC-Hunter
Passer
espy

https://www.activecountermeasures.com/free-tools/

https://securityonionsolutions.com/

CDV2_0421

Backdoors™ & Breaches

PROCEDURES

Created by: BLACK HILLS | Information Security