4.3

Tuesday, September 26, 2023 4:25 PM

to reduce false +/- in SIEM,
need to adjust rules

email headers

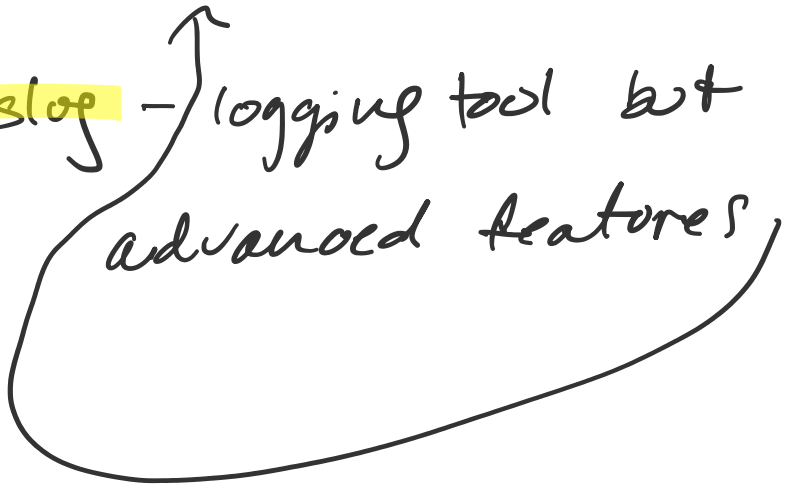
- sender addr
- servers carrying message
  - mail user agent MUA
  - mail delivery agent MDA
  - mail transfer agent MTA
  - geo-info of email
- Spam checks
  - performed by message transfer agents
    - MTA

NXLog - open source central logging tool
similar to SIEM

Similar to SIEM

- alert
- aggregation
- normalization
- correlation
- retention

syslog - logging tool but doesn't have advanced features



journalctl - querying and displaying logs in Linux systems

test access point TAP - device that copies signals from physical layer to data-link layer

to data-link logic

No frame loss because no network or transport logic needed

packet monitoring

Sensor to install w/ IDS

Switched port analyzer SPAN - feature of many network switches

port mirroring

copy of net traffic sent to other port

frames w/ errors will be dropped

SNMP trap - push data to SIEM

Mobile metadata

Mobile metadata

- call detail records CDR
- data transfer volume

Email metadata

- sender/receiver adder
- spam checks
- server transfer info

website metadata

- cookies
- data type of resource
- authorization info

file meta data

- created / accessed / modified
- ACL
- copyright
- tags for indexing

. tags for indexing

OSSEC - HIDS that can collect DNS server logs for trend and crosscheck w/ malicious domains

can perform frequency-based trend analysis on NXDomain errors by comparing to baseline

Authentication attacks

- SIEM
- auth logs
- app logs

SPAN is not hardware

TAP can be either active or passive

SPAN = active