1.7

Wednesday, September 20, 2023 11:51 AM

health and sec of individual clients

- win10 hosts
- vuln scanners
- DLP systems

web app scanner

nikto

searches for known exploits like SQL inject and XSS

network vulnerability scanner

Tenable Nessus

tests net hosts including clients for known vulns

threat feeds - notis of current or new threats log aggregation - normalize data from diff sources so it is consistent and searchable + dynamic report engines

Syslog collecter - centralized collection of events from multiple sources

Sensors - example of data input

intelligence fusion w/ SIEE and threat anal to develop queries and filters to correlate threat data

maneuver - military doctrine term relating to taking positional advantage

defensive maneuver is for analyst

[illegible] passive discovery

defensive

to make passive discovery
so threat actors have no hint
analyst discovered them

advisories - from vendors may init
check for new vulns

threat feeds may init updates
to sec policies or sigs

security content automation protocol
SCAP - determines if pc meets
baseline

perform config review

port scanning is more passive

more false +