Workshop tasks 13.02.25 - Network defence and security data

In the lecture we discussed several tools that are available for free or have online demo versions. The goal of these tasks is to familiarise yourself with some of them and get a better understanding of what they provide. These tasks are for self-study.

1. Inventory and asset management – SolarWinds

https://oriondemo.solarwinds.com/Orion

Familiarise yourself with the tool. Under Alerts & Activity open pages for Events, Alerts and Syslog - what are they collecting?

Open the Netflow dashboard and get an overview of the most active conversations. How might this be collected? What does it mean?

Open "Device tracker summary" dashboard. Are there any active alerts?

There are alerts for new MAC addresses in the network and new DNS names – why could these alerts be important to track?

2. Vulnerabilities - The CVE database

Open CVE database and search for your operating system and version. Do you see any critical CVEs? Are you protected against them?

https://cve.mitre.org/cve/search_cve_list.html

Use the Solarwinds applications dashboard to get an overview of the applications in use ("My dashboards" -> "Applications"). Search for one of the applications in the CVE database. Did you find any recent vulnerabilities?

https://hco.demo.solarwinds.com/Orion/APM/Summary.aspx?viewkey=Application+Summary+Narrow

3. Security policy

See https://www.sans.org/information-security-policy -- based on what we discussed in the lecture, review some of the templates and consider how they could improve security in the organisation. Start with AUP – Acceptable Use Policy

4. End device information - logs

We discussed how gathering event logs from hosts and servers (e.g. in a SIEM) is important to get an overview of what's happening in the network infrastructure.

Do you see anything interesting in your local logs? Can you find information about a specific event, e.g. when you logged into the computer the last time?

On Windows; open Event Viewer and view the local logs as described in the lecture.
On MacOS; open Console.app – start streaming logs and filter on keywords (e.g “network”)
On Linux; look for logs in /var/log – use journalctl. Live logs can be followed with -f