Operating Systems

Why is Windows Event ID 5140 important to monitor?

**If you have high-value computers for which you need to monitor all access to all shares or specific shares; this is why Event ID 5140 is important.**

Networking

What two frameworks is domain-based message authentication, reporting, and conformance built upon?

**Sender Policy Framework**

**Domain Keys identified mail**

Security Principles

In your own words, describe what a watering hole attack is and provide an example.

**Watering hole attack is designed to compromise users within an industry by infecting websites they normally use and then leading them to a malicious site.**

**An example is the hacker group called Lazarus that launched a water hole attack by infecting sites the organization used. It infected visitors whose Ip showed 31 different countries.**

Cyber Threat Intelligence

What is OSINT and what are some tools that can be used to automate the collection of it?

**OSINT is open source intelligence, tools used are artificial intelligence to find sensitive data around the web. Some OSINT tools are google dolls, jigsaw,OSINT framework, OpenVAS and many more.**