What is Logging?

Logs are detailed lists of application information, system performance statistics, or user activities. Logs can be useful for keeping track of computer use, network activity, security issues, and error reports. Every activity on your environment, from emails to logins to firewall updates, is considered a security event. Events are, (or should be,) logged to keep tabs on everything that's happening in your technology landscape. So how can we use this for security purposes? Let's cover some examples:

- **Logging user events in Windows Active Directory domains.** This allows us to see when accounts are logged in, incorrect password attempts, administrative account usage, when new accounts are created or deleted, etc. This is a good way to detect activities such as brute-forcing attacks against login credentials or password spraying attacks.
- **Logging network connections from firewalls** can allow us to detect port scanning or vulnerability scanning activity, denial-of-service attacks, and network issues.

It's important to define exactly what logs are needed. In large organizations, the volume of data passed to a SIEM can be absolutely huge, so we need to work out what logs we actually need, and what devices we need logs from. Scoping this appropriately means there is less noise, and it's easier to analyze the data we actually need, instead of the data we have access to. SIEMs are not log repositories, they are analysis platforms!

In the next few lessons, we will cover the following important log types we need to consider when performing security event monitoring:

- **Syslog**
- **Windows Event Logs**
- **Other Logs**