Cheat Sheet

General terms:

- **OT** (operational technology) – Combination of hardware and software to monitor physical devices and infrastructure
- **IT** (information technology) - Defending computers, servers, and networks from attacks
- **NIST** – National Institute of Standards and Technology framework
    - A group of standards and best practices to help improve security
    - Five pillars
        - **1: Identify** – understand all assets and risks in the environment
        - **2: Protect** – securing all critical services
        - **3: Detect** – identifying and responding to threats and vulnerabilities
        - **4: Respond** – taking action regarding a detected incident
        - **5: Recover** – restoring systems/operations after an incident

Security Onion related terms:

- **SIEM (Security Information and Event Management)** – A security system that:
    - Helps organizations identify potential threats before they can disrupt the environment.
    - Helps security teams detect anomalies.
- **RTU** – Remote Terminal Unit
    - Remotely monitors and controls equipment in the power grid
- **IDS (Intrusion detection system) sensor** – monitors network traffic for suspicious activity
- **IAM** – Identity and Access Management
    - A framework for managing and securing user identities and their access to resources
- **Elastic Stack** – a suite of software tools for searching and analyzing data in real-time
    - **Elastic fleet** – a management tool within the Elastic Stack that manages and deploys data collection across multiple hosts
    - **Kibana** - visualization and management tool for Elasticsearch that is used to analyze data

Machine learning terms:

- **Splitting** - where data is split into two subsets, one subset will be used to train the machine learning model and the other as an unseen subset to test the model and ensure it can generalize well with new data.
- **Bagging classifier** – makes several copies of the training data, each slightly different, and trains a simple model on each copy, then averages the results to make predictions less likely to be over-tuned to one specific data set.
- **Overfitting** – when a model learns the details of the training data to the extent that it performs poorly on unseen data

Testing/attack terms:

- **Nmap** – an attack that uses the Nmap tool to scan the network and find vulnerabilities or open ports that can be exploited
- **Ping** – An attack that overwhelms the network with ping requests to slow it down or cause it to crash
- **Curl** – An attack that uses the curl tool to send malicious requests to the server to disrupt services
- **Brute force** – An attack where the attacker tries every possible combination of passwords until they find the right one to gain access