Here are a couple of links to help find the data I was referring to:

- **https://www.ncdc.noaa.gov/cdo-web/webservices**
- **https://webscope.sandbox.yahoo.com/** (account needed, free for university students and faculty)
- **https://data.nasa.gov/browse?limitTo=datasets**

Use this Elastic blog and read about how they prepared the CTF environment.

https://www.elastic.co/blog/threat-hunting-capture-the-flag-elastic-security-bsides-2020

Threat hunting capture the flag with Elastic Security at BSides SATX 2020 | Elastic Blog
Last month, members of the Elastic Security team hosted a threat hunting capture the flag (CTF) event at BSides SATX. We provided the community with an environment to learn and practice threat hunting with our team, and cultivated new relationships with attendees.
www.elastic.co

Preparing the CTF environment
While designing the environment for the CTF, we decided to keep it relatively simple. We configured the following components, as shown in Figure 3:

- x1 Windows Server 2016 host configured as a domain controller
- x20 Windows 10 endpoints joined to the domain
- We installed several applications on each endpoint using **Ninite** in order to generate benign events and make the task of finding the flags in the dataset a bit more challenging for participants — after all, the goal of a threat hunter is to find the true threat amidst the noise
- **Winlogbeat** was installed on all endpoints and configured to ship Windows event logs, PowerShell logs, and **Sysmon** events to **Elasticsearch**. We used Olaf Hartong's popular **sysmon-modular** configuration with Sysmon
- **Packetbeat** was installed on all endpoints to ship network events to Elasticsearch
- All events were shipped to Elasticsearch running in an **Elastic Cloud** cluster
- Participants utilized **Kibana** to search and visualize the events indexed in Elasticsearch
- A **CTFd** platform was setup for participants to submit flags and score points during the event

Use this Elastic blog and review how they setup another CTF environment with a known CVE

https://www.0ldmate.com/posts/tech/elastic-ctf-a2f4ee2043f5426e9233a5b318796535/
Elastic CTF
The Elastic CTF is a capture the flag competition that I built based on the Elastic Stack (formerly ELK Stack). I created it for the Sectalks Ninja Night as a way to give back something

to the community that has given me so much. It was designed to give people a chance to play with a platform that is used quite often in security teams in many companies. This was my first time developing a CTF challenge and I hope I get the chance to do it again another time.
www.0ldmate.com

Focused on CVE-2019-7609
I installed an older version of the Elastic Stack (6.5.4) that was vulnerable to remote code execution (https://github.com/LandGrey/CVE-2019-7609) on the internal server and opened up SSH on the external facing server. I then simulated the attack from the attacker box making sure all logs are being sent to the Elastic Stack.

This is more forward leaning but gives you an idea of where we want to go once the teams understand the fundamentals.

https://www.elastic.co/blog/embracing-offensive-tooling-building-detections-against-koadic-using-eql

Embracing offensive tooling: Building detections against Koadic using EQL | Elastic Blog
This year at BSidesDFW, my local security conference, I highlighted a continuing trend of adversaries using open source offensive tools.The talk reviewed one of these post-exploitation frameworks named Koadic and walked through different ways defenders can build behavioral detections through the use of Event Query Language (EQL). In this post, I wanted to review this research by providing ...
www.elastic.co

Consume Mordor Datasets:

For next year….. We need to discuss **data generation** before the end of the first semester - request **focused guidance**. Also, **in the near term**, as it relates to data generation identify **quick first steps** (see below).

Where to begin - **quick first steps**:

- Consume Mordor Datasets from here: AWS — The Mordor Project (mordordatasets.com)
- We chose *mordor* because they're datasets are small and we want you all to focus on the *structure*.
- Download datasets individually, unzip them and verify JSON format - sometimes a file will fail - just download it again.
- Ingest though Kibana dev tools - *Judy will demo this on Friday*. Once ingested go to Kibana Discover and *learn the dataset*.
- *Create a job* using a *single metric*.
- If time permits explore classification, population, multi metric (more complicated and advanced)

Threat Hunter Playbook: https://threathunterplaybook.com/notebooks/windows/intro.html