What are the challenges of collecting huge amounts of log data? How do security analysts deal with them?

A lot of security analysts will face the problem of what data should be kept and logged or should just be monitored and, for lack of better terms, kept a mental note of said logs. With every company data storage should be a priority to protect themselves and most importantly, save them money.

In my cybersecurity boot camp program, we were taught how to monitor data while simulating what normal activity looks like and even going as far as trying to DOS our virtual machines to identify them. Every company should have their analyst be knowledgeable enough to spot suspicious activity in order to assess what data should be collected.

We dealt with Kibana which is a system that tracks information from virtually anywhere. It can track the data from any virtual machine that the company has set up showing things such as, what machine is downloading what, from where, how big or small the file is, and much more things. It can also track file types, like gzip, zip. Essentially it can track just about any file type associated with malicious behavior.The types of data crucial to our mission was what files in particular were being downloaded and monitoring spikes in the charts. Basically spotting anomalies in activity. Knowing that traffic can be monitored as often as a real time clock, it's important to collect data from those anomalies to determine what is essential or not.