As we move further into the 21st century, enterprises will need to learn to adapt to more and more cyber threats. These enterprises will need to utilize intelligence and learn how to use information in an age where the process becomes more and more important every day. A good place to start is going to be to implement a framework for intelligence gathering. The framework used will be the Intelligence Gathering Process

Planning and Direction

The first phase of enacting this will be the planning and direction phase. During this phase the Chief Information Security Officer, Yosemite Sam. To enact this process, we need to know what Sam is going to want from this. What information does the Acme Anvil company need from this. While Sam may want all of the information he can get his hands on, that will not be feasible and Sam will need to give us a list of requests that will enable us to move onto the next phase, which will be the collection phase of the process.

Collection

Once we understand what we need to collect to satisfy Sam, we will need to determine what kind of collection methods we are going to use. In order to do our job efficiently and, most importantly, effectively. It's vital to our end goals that we do not collect too much or too little information. The dangers of collecting too little information are obvious ones, but the problem with too much information can be less obvious to individuals on the outside. Too much information can lead to important information being lost in a sea of useless information. Because of this, we need to be sure that the data we are collecting is relevant. Next, we will set a framework for the third phase, which is processing and exploitation.

This part of the process is the part that is most likely to be done by a machine. It will take the raw data collected in the collection phase, which may be in something like binary or hex, and turn it into information that a human would be able to use. It is the phase that is mostly done unseen.

In the analysis and production phase, the data that has been collected and processed is analyzed to be used as intelligence. One aspect that is highlighted during this phase is the important distinction between information and intelligence. Explaining this to Acme is vital. Intelligence is actionable information that is reliable and accurate. Information can include almost anything that is collected and processed. If we treat every piece of information as intelligence, we will not be able to do our jobs properly. Once the intelligence is sifted out of the information, we will disseminate it to the rest of the enterprise in the next step.

Dissemination

To disseminate the information in the right way requires us to understand who our end user is. In this case, we want to be able to get all of the intelligence out as efficiently as possible so that the people who need it are getting it in a way that is suitable for them. This can mean different things for different people. If we want the information to be distributed across the enterprise, it means that we are going to have to come up with a way that can not only reach a large number of people, but will be read by those people. An email may be an effective way to do this for larger groups, but we will want a more direct way to get it to people like Sam, who we will see in a daily briefing.