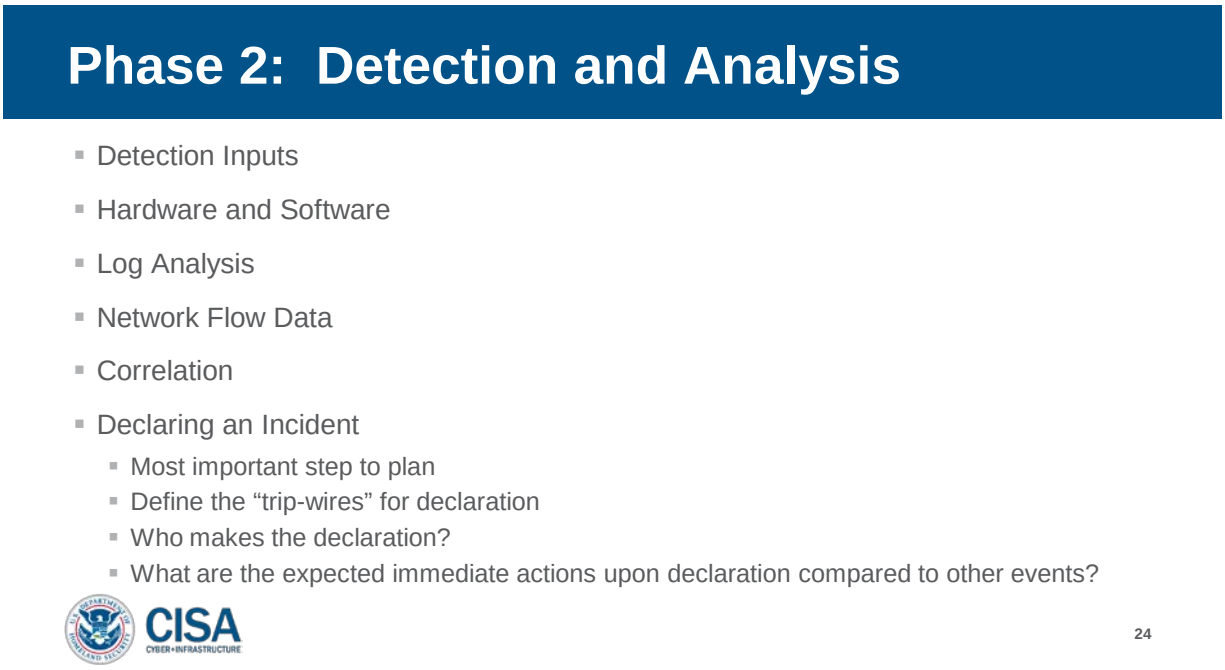
Incident Response Phase 2 of 6 – Detection and Analysis

Table of Contents

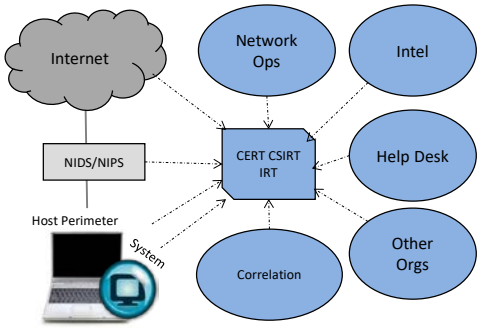


**024 Instructor: So now that we've gone through the preparation phase, now we've entered into the detection analysis phase, and to be honest with you, this is probably the phase that is taking place most regularly in your organization. These are the actual people sitting in their chairs, monitoring the organization to make sure that incidents are not happening, that events are taking place as expected.

So what we're going to talk about here a little bit more detail are the kind of inputs their people are looking for and the tools that they need to have at their ready disposal, so that way they can understand if an event is taking place.

Detection – Where Does It Come From?

- Events can come from anywhere.
  - IDS/IPS, Help Desk, Logs, Intel, Correlation Tools, etc.
  - Enable your team to separate regular operations from abnormal operations.



CISA CYBER+INFRASTRUCTURE

25

**025 Let's talk about detection first. You're going to really want to understand what kind of traffic you have coming into your system. This can be done in a whole number of ways. Really what you want to do though is to make sure that the people are looking carefully for abnormal events taking place, regardless of the tool that they may be looking at. Some of this may be automated.

For example, maybe you have an intrusion detection system or an intrusion prevention system that's set up. Now, there's some critical decisions that you need to make here in terms of setting up something like that. You can easily dial up the sensitivity of those tools to a point where they're going to actually inhibit some actions taking place in your

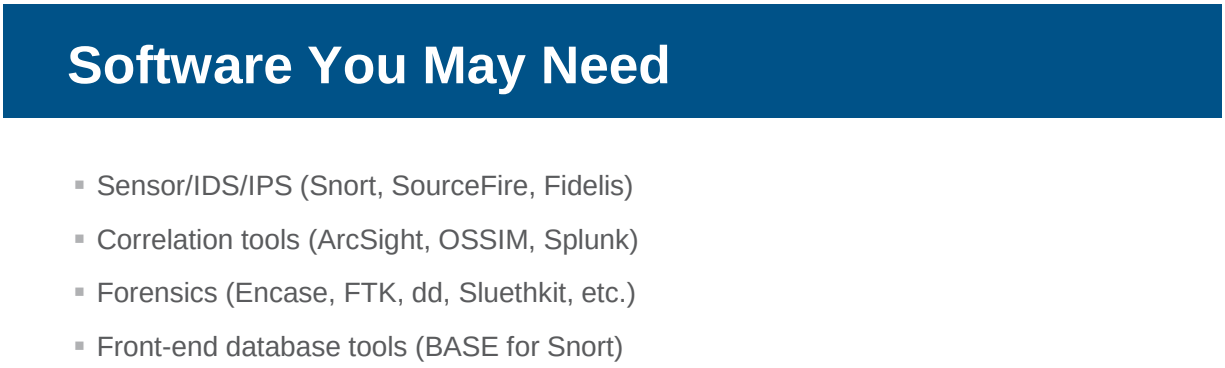
system, and those actions may be quite regular. So there's going to have to be some kind of analysis or risk assessment to make sure that your IDS and IPS is operating, such as it's being effective for you but it's not interfering with your organization too much. It's okay to have a hiccup every once in a while, but to be honest, if it's shutting down your business to a point where it's actually inhibiting production, it may be a problem.

Hardware You May Need

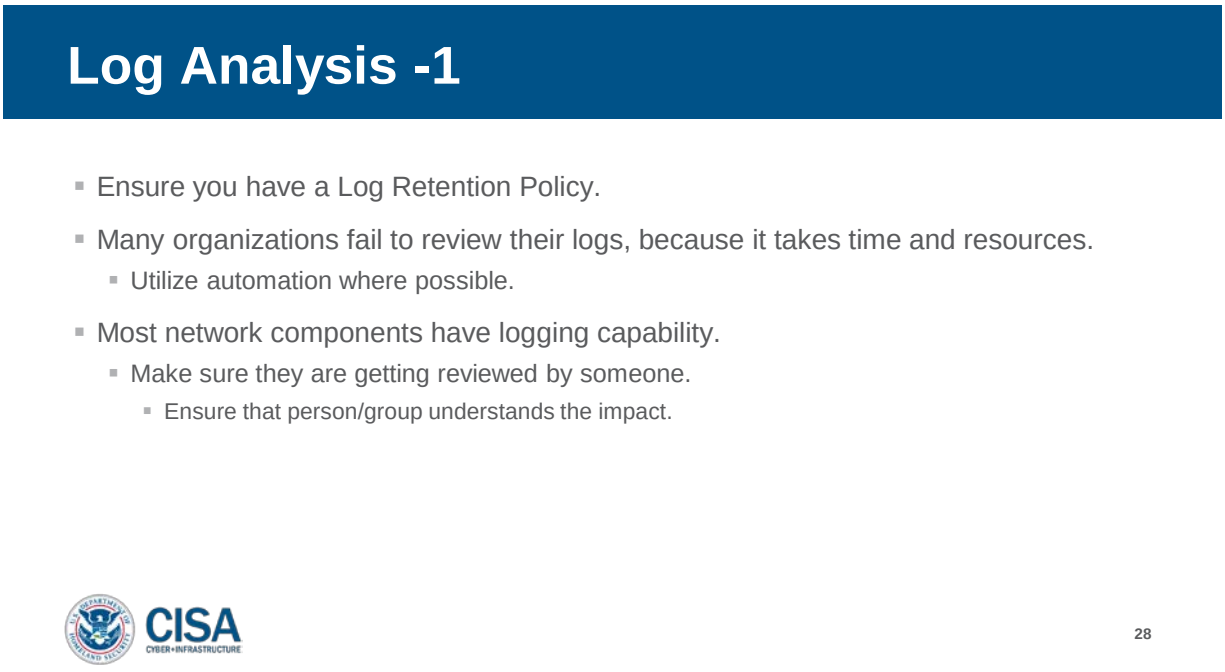
**026 Here's a list of some hardware tools that you may need to provide to your folks, and I'm not going to go through this exhaustively, but what I want to call to mind here is the idea that no matter what you bring to the table in terms of this hardware, it's going to need maintained. So you're going to have

to have your people trained such that they can maintain it and operate it properly.

Software You May Need



**027 The same thing goes for software. Now, once again, this software may change, especially over time when you get new tools in and old ones leave, which is fine. But regardless of what you're doing, whether you're trying to sense or whether you're correlating data or whether you're collecting forensic data, all this stuff needs to be maintained, and once again, needs to be operated properly. This goes to saying that your people need to be trained to know how to use the materials that are available to them.

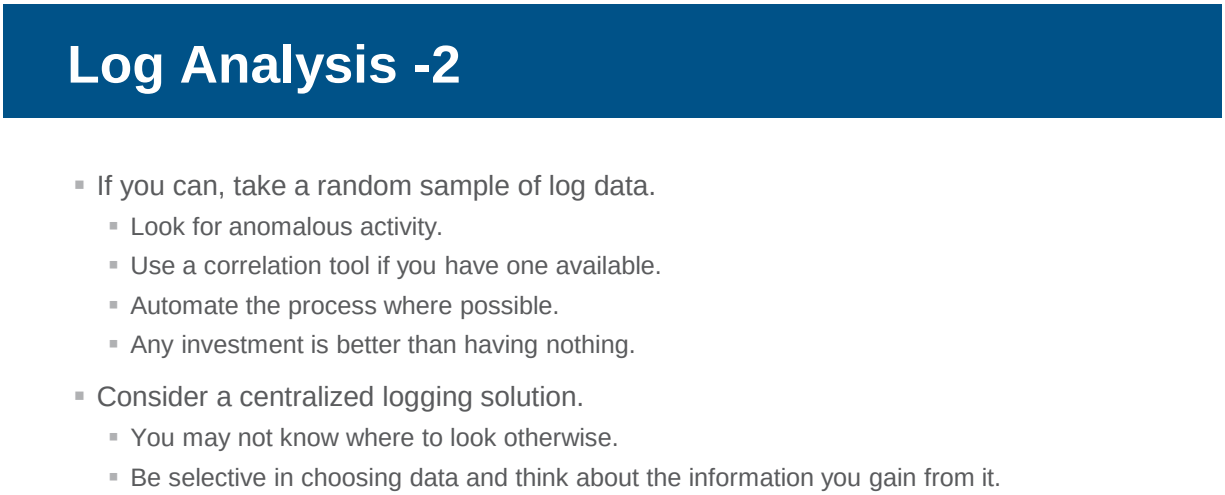


**028 Now, let's talk a little bit about logs. I talked about the fact that you're going to have a lot of traffic coming into your organization and leaving as well. That's a lot of data, if you think about it. You're going to want to think about how long you're going to actually retain that data. It costs money. It's going to take some resources. Maybe not a lot, but over time it could become cumbersome. So you're going to think about how long you retain that information. Similarly, you're going to think about who's reviewing these logs.

Now, a lot of organizations have trouble doing this, because let's face it, it takes time, it takes money. So try to automate wherever you can. Also, you want to think about what components in your organization are

actually doing the logging, and what kind of data are they collecting? Your people need to know and understand how to assess that data and get meaningful information out of it.

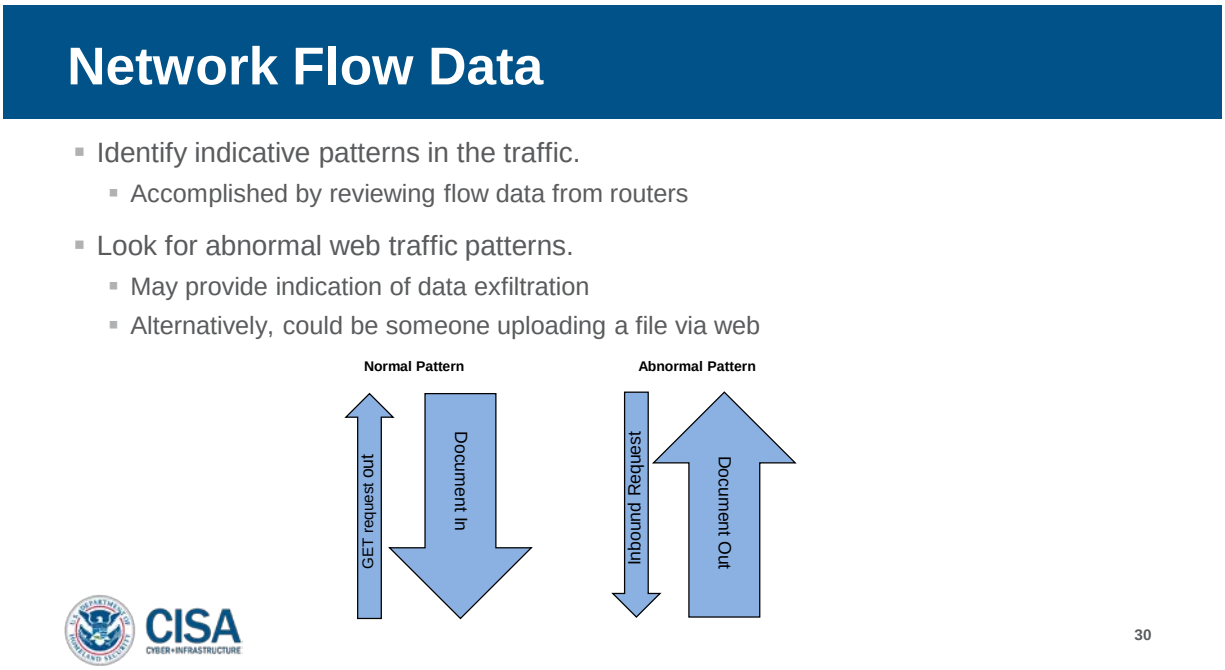
Log Analysis -2



**029 Now, some things that may help you could be sampling, for example. I may look specifically at just trends or activities that may not otherwise be indicative of normal operations. You could also have tools that actually help you correlate the data. Whatever you do, it really helps to automate. It could be laborious at times to go through all this data, so try your best to let the tools help you understand if there are trends taking place that may not necessarily be processable by a human eye and mind.

The other thing you may want to consider here is that you're going to have all these logging activities take place all over your organization, and if that's the case, they could be disparate and you could have important trends going on in one spot and an important trend going in another, and if correlated you know that a risk is come to realization, but otherwise you wouldn't know. So you may want to consider integrating that picture somehow and this centralized logging solution will provide you that critical information so you can get ahead of an event before it actually takes place.

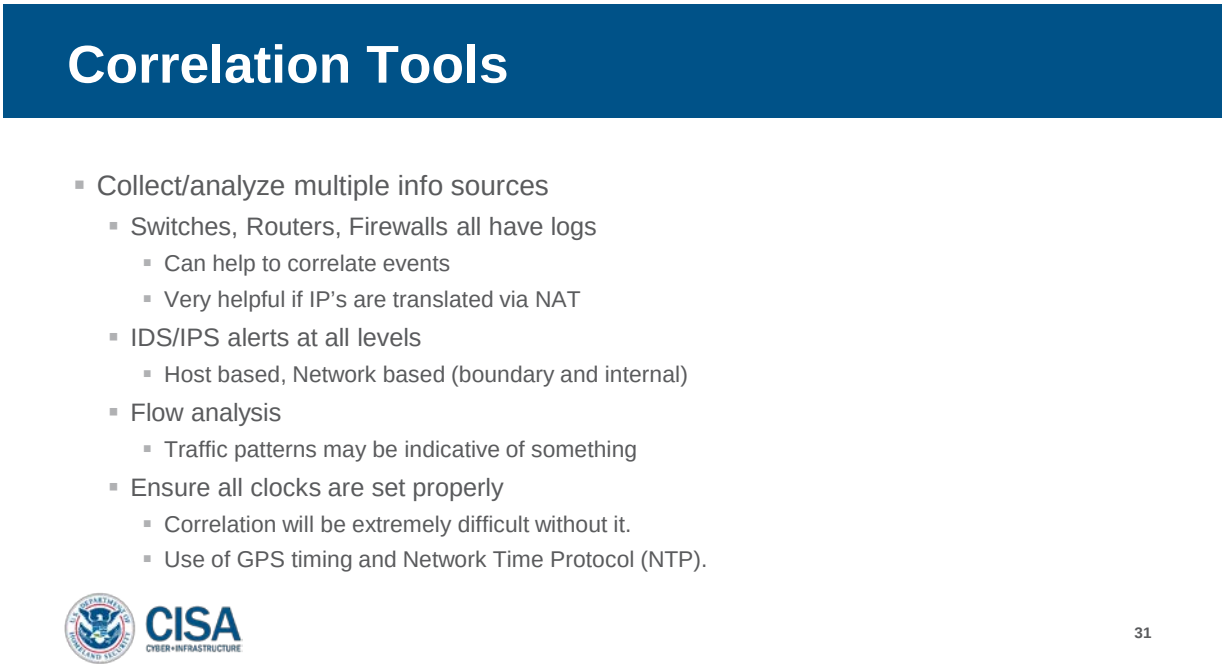
Network Flow Data



**030 That flow of data can be immense sometimes, and quite a bit overwhelming. So there are things that you may want to look at here in terms of specific patterns of traffic

that are coming in and out of your organization. A good example here could be if I have an insider who is exfiltrating critical data. You could be looking for the kind of data that leaves your organizations, and if you have the data classified properly, you could see that it's leaving with a simple flag on it.

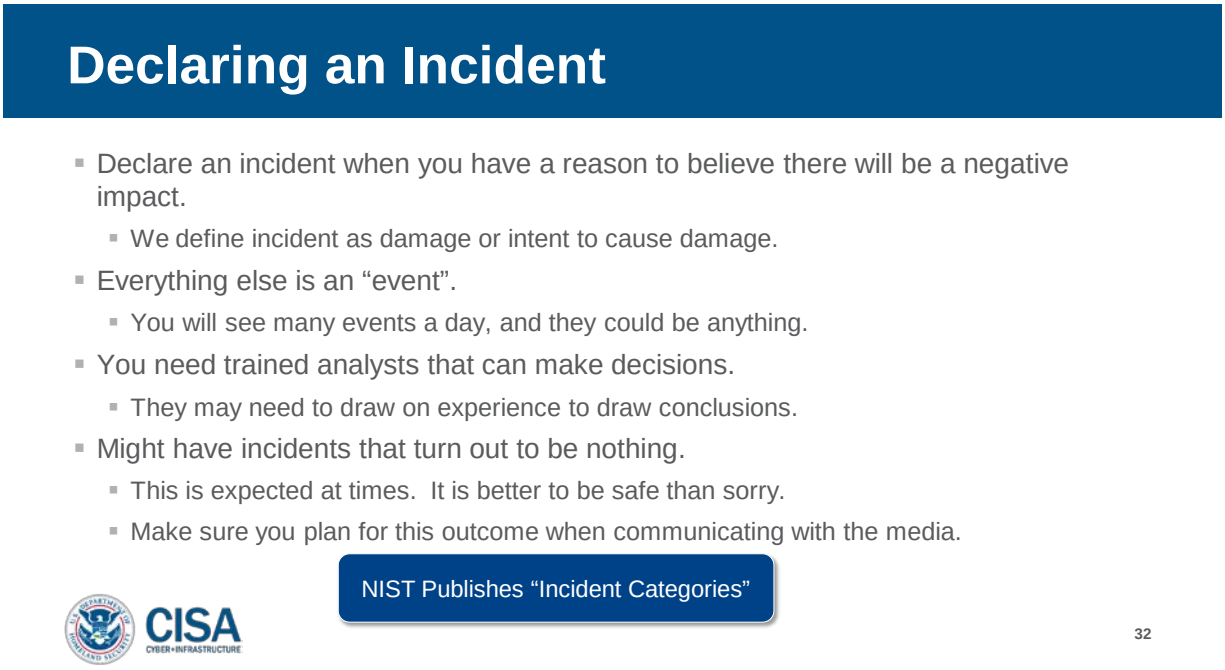
Correlation Tools



**031 Like I said before, automation is critical. Let computers help you understand what normal operations should look like after they've actually watched what normal operations look like for a while. Watched. In other words, they're collecting data and they understand, they have a basis, for that expected information flow, and then they're going to correlate it or compare it, to your every regular day network flow.

At this point, if it sees differences, it will inform the operator that something may be happening. This flow analysis is very important. It could be indicative that something is happening. Now, the other thing you need to make sure is that if you're doing this correlation, that you have the timing synced up properly. It could be very difficult to operate if that is not taking place. We recommend using very standard timing system. GPS would be a good example here.

Declaring an Incident



**032 This is probably the most important thing you need to bear in mind when thinking about incident response, and it's declaring the actual incident. Ask yourself, "Who has the authority to declare an incident in my organization? Do they know what they're looking for? What specific

trip wires must they cross over to declare that incident taking place?" If you stand up your incident response team, it's going to cost time, it's going to cost money, and you're likely going to have an interruption of your normal operations.

So you could cause damage to yourself, if you think about it, if you declare an incident and it's for a regular, every, any day event. So you have to have your people trained to make critical decisions in a timely manner, and I'm going to emphasize that timely part too. Because the longer they wait to make that decision, you could have negative impacts building in your organization. Now, they might turn out to be nothing, and that's fine. It is better safe--to be safe than sorry, but the same time, you want to make sure that you know when you actually have an incident, so that way you're not pulling off a lot of false alarms.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098