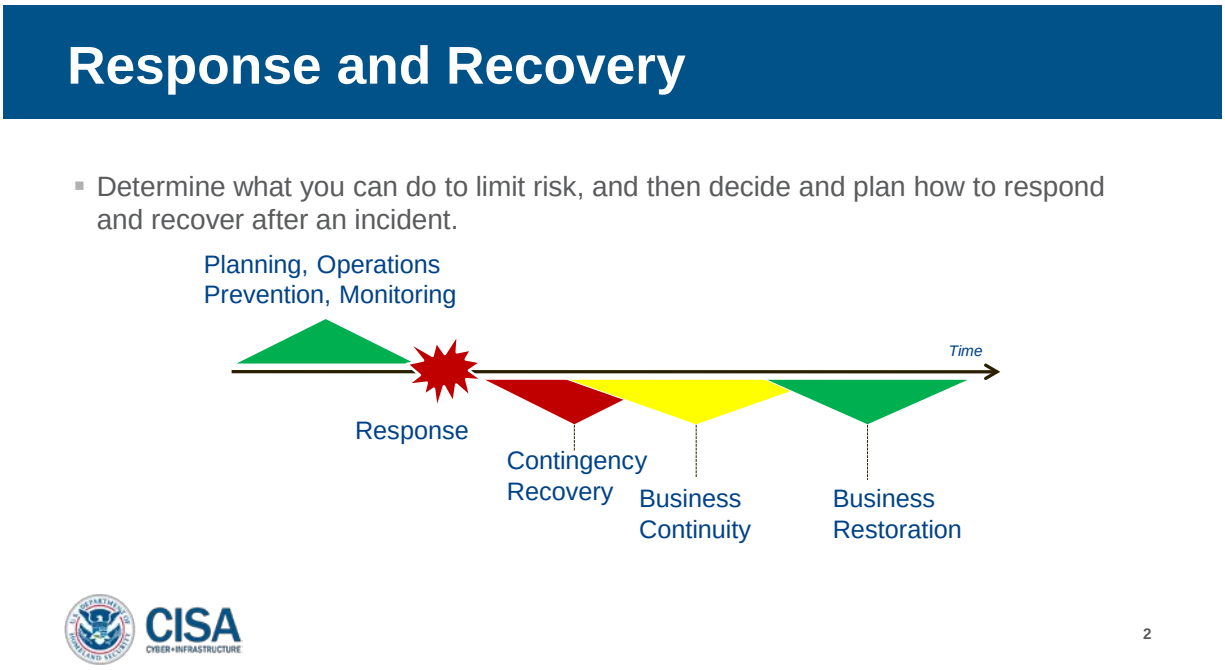
Incident Response Terms and Life Cycle

Table of Contents

Incident Response

**001 Instructor: Today we're
going to talk about incident response.

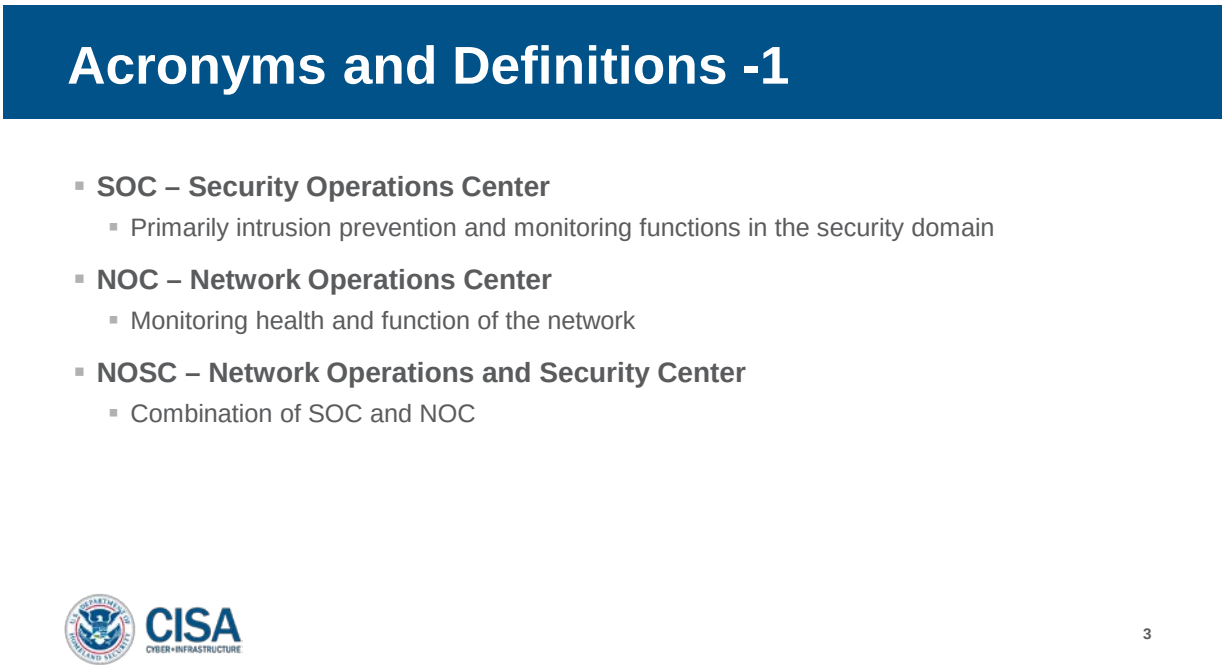


**002 Now, to this point, what we've done is we've identified the critical services and assets that support our business or our organization. We now understand too that we have risks, uncertainties that contain threats, vulnerabilities, and impacts to the organization. We've defined those and we've now understand what responses we've put in place. We've maybe even selected some security controls and put those in place so that way we can prevent the risks from happening.

Now, just because we've done that, there's always residual risk or risk that's leftover. Things can still happen. So what we want to do is understand how an event could eventually become an incident if it's a negative risk that has come to

realization, and this is going to happen over like an arc of events.

So what we've done is everything in the green triangle all the way at the left of the slide there. We've done the planning, the operations, and we're maybe even doing some prevention and monitoring, but then we actually have the event happen. Like to think of this as like that cold, dark day, right, the day that you never really even thought would happen, and you have to actually initiate your response, and following that immediate response you're going to actually have recovery phases that you're going to go through too. The red, the yellow, the green, those are all events taking place. You're actively participating as an organization to get your organization back on track and operating again.



**003 So let's look at these with greater detail. But before we do, let's talk about some base definitions so that way you understand if you're ever talking to somebody about incident response or even as I go through this presentation, we have a baseline set of ideas as to what we're talking about here.

Now, by the way, a lot of these words are used interchangeably, so just bear with me and what we can do is we can adjust the definition to your organization, how it's used at a later point. But for right now, let's understand that all these actions may take place within the context of a Security Operations Center. This is like your front line, if you will. Now, it doesn't necessarily have to be a dark room with big monitors and people sitting around all the time just

looking at screens. It could be a virtual environment. It could be automated. But basically, it's that front line that's looking to prevent intrusion and it's monitoring traffic flow and different functions the organization and within your security stack.

You may also have doubling a Network Operations Center, and what's going on there is maybe that you have people who are actually looking at the health and the general function of your network to make sure that things are running smoothly. We may also have a combination of the two, where the SOC and the NOC are actually working together. We could call this a NOSC or the Network Operations Security Center, and just think about the same folks doing the same thing in the same room.

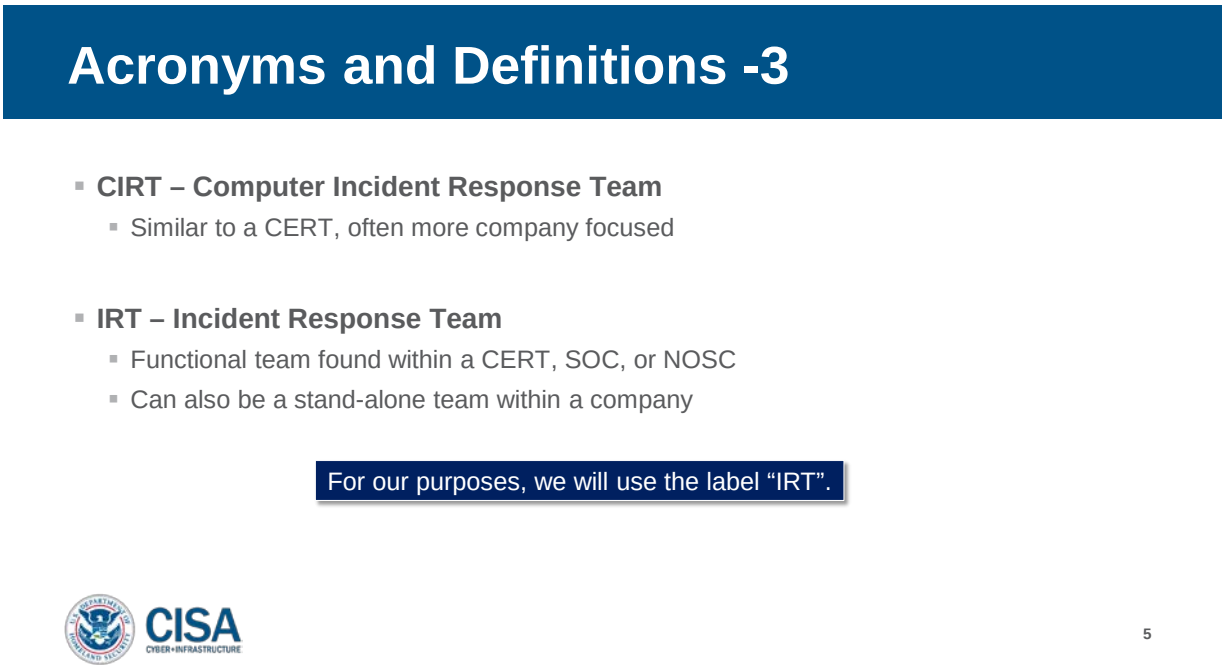
Acronyms and Definitions -2

- **CSIRT – Computer Security Incident Response Team**
  - Responsible for cyber incident response processes
- **CERT – Computer Emergency Response Team**
  – Computer Emergency Readiness Team
  - Often synonymous with the CSIRT/CIRT
  - Can contain more functions and operations than a CSIRT such as 2nd and 3rd tier analysis, research, and coordination
  - Often associated with a country, industry, or community

CISA CYBER+INFRASTRUCTURE

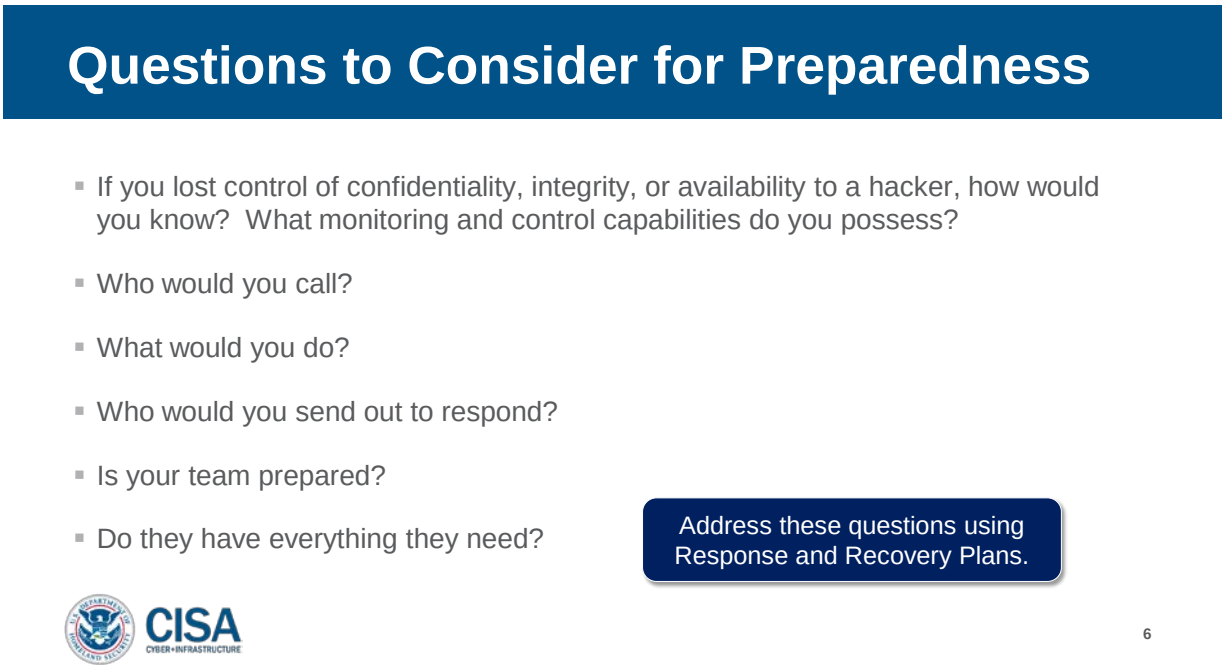
4

**004 Moving on, we also have a Computer Security Incident Response Team, a CSIRT. If you think about it, as that event happens at that red mark that we had on the first slide, this is where your CSIRT would actually come to life. You may have it also called a CERT or a Computer Emergency Response Team, or a Computer Emergency Readiness Team. Either way, they're pretty much doing the same things. A CERT though may actually go a little bit further, because it may actually be doing additional analysis and research and additional tasks down the road from what an actual immediate response team would provide, an incident response team would immediately provide.



**005 There's also a Computer Incident Response Team similar to a CERT, and there's also an Incident Response Team, and now we're really starting to just mince terms here. Let's just say for the sake of this presentation that we're going to talk about instant response teams from here on out.

Questions to Consider for Preparedness

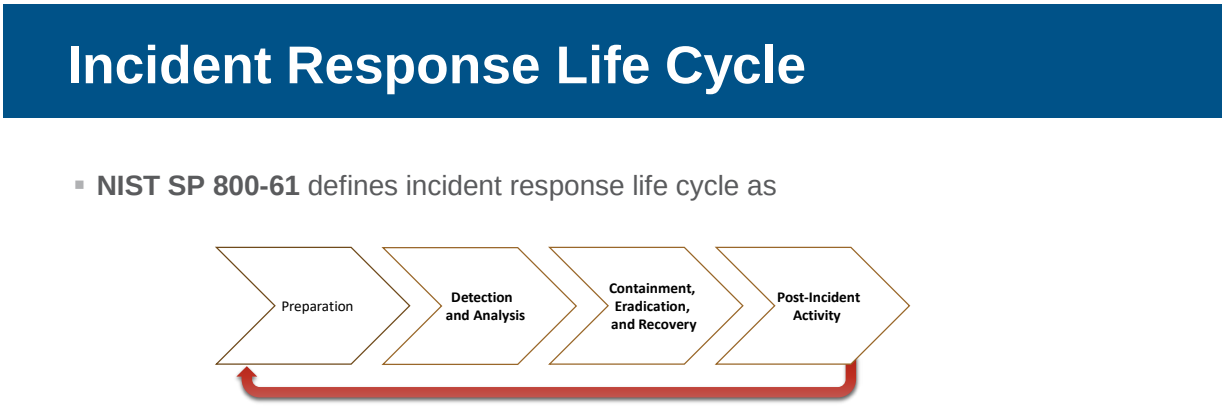


**006 Now, it's time to get a little bit introspective about this. Think about your organization. What is it that you're trying to defend? Here's some critical questions that you're going to want to consider to determine if you're prepared or not. Now, there may be different ways to answer these questions. It may be just a self-assessment or maybe you bring in someone external to the organization to come in and ask you or run you through exercises so that way you know you're prepared.

Things to think about would include, "Who do I call if something happens? What would my people do? Are they trained to do it? Who would actually be doing the response, and are they prepared? Do they have the materials necessary to effect a response?" And, "Do they have all

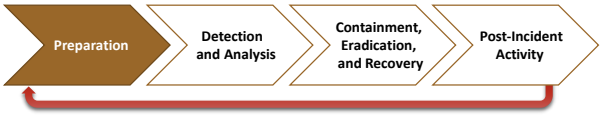
the training necessary so that way they know actually physically what to do?"

Incident Response Life Cycle



**007 If you go and look at NIST SP 800-61, we can break up an incident into four distinct phases, and here they are. You're going to actually prepare. You're going to have a phase of detection and analysis, and then if something happens, you're going to actually have containment, eradication, recovery, and then you're going to have some things that you're going to do actually after the incident.

Incident Response Life Cycle – Preparation



- For **Preparation**
  - Align security with business needs
  - Create an incident response **plan**
  - Develop incident response procedures
  - **Prevent incidents**
    - Note that you are not just preparing for incidents.

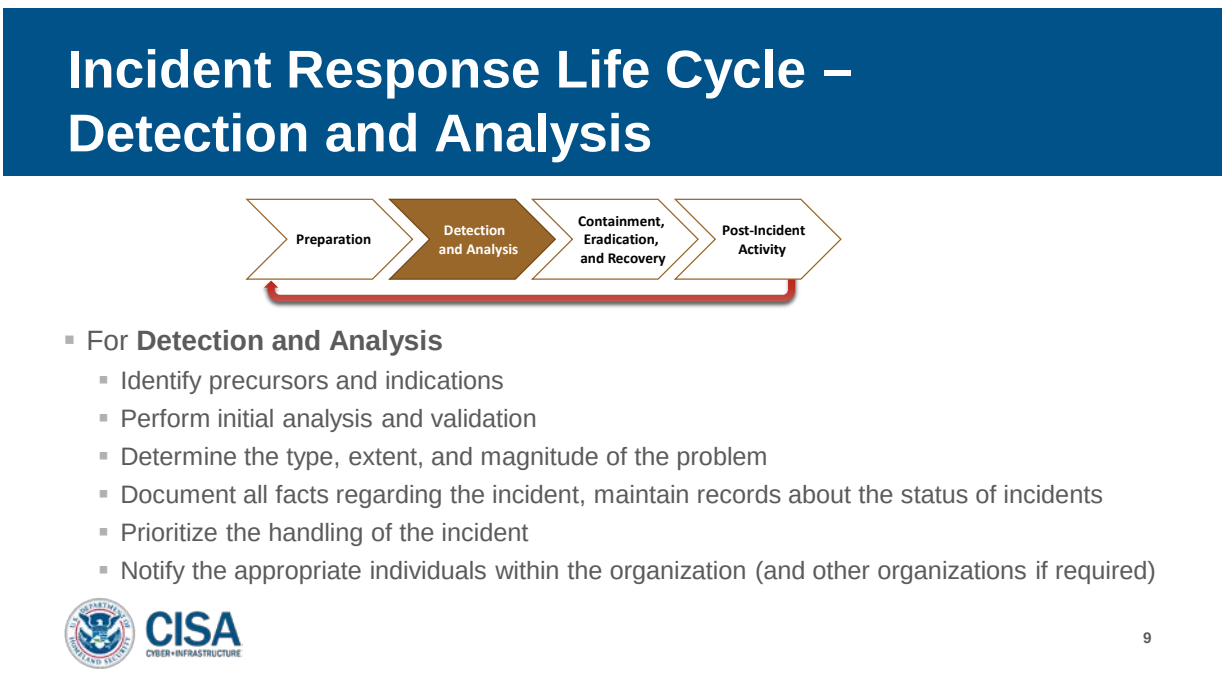
CISA CYBER+INFRASTRUCTURE

8

**008 So let's go into each of these at a high level. First of all, the preparation step. What we're trying to do here is we understand what our organization's needs are, we understand the risks, and we align those with what we need to do in terms of response. We may put all these in an integrated incident response plan so we know the actual things that we're actually doing and the things that we need to accomplish to have a more secure organization, and we also may have detailed procedures in there for our security professionals so they know what to do when that dark day comes. Ultimately you may also be preventing incidents. Now, you may think of this as, in your preparation phase you're implementing, let's say, a firewall, simply said, and in doing that, you may be preventing

incidents from taking place. This is happening in your preparation step.

Incident Response Life Cycle – Detection and Analysis

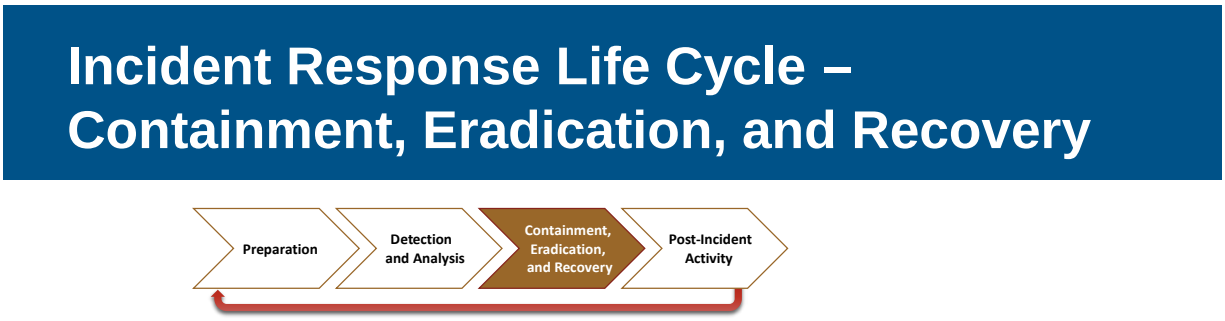


**009 Now we're under the detection/analysis phase. What we're doing here is we're thinking carefully about key risk indicators or precursors, if you will, that are going to give us indication that that risk may actually be coming to realization. There's some analysis and some validation that goes along with that, and really what you're trying to do is understand what the magnitude of the problem is that may be actually occurring. The step here, or the most important thing to remember in this particular step, is documentation. You really want to keep a close and careful record of all the things that are happening. Keep the facts. This is really going to come in handy, especially if you're going to do

forensics down the road, and we'll talk about that a little later. You're also thinking about continually prioritizing the events that are taking place in your day.

One last thing. In this detection phase, it's important to have your people understand when they need to notify people.

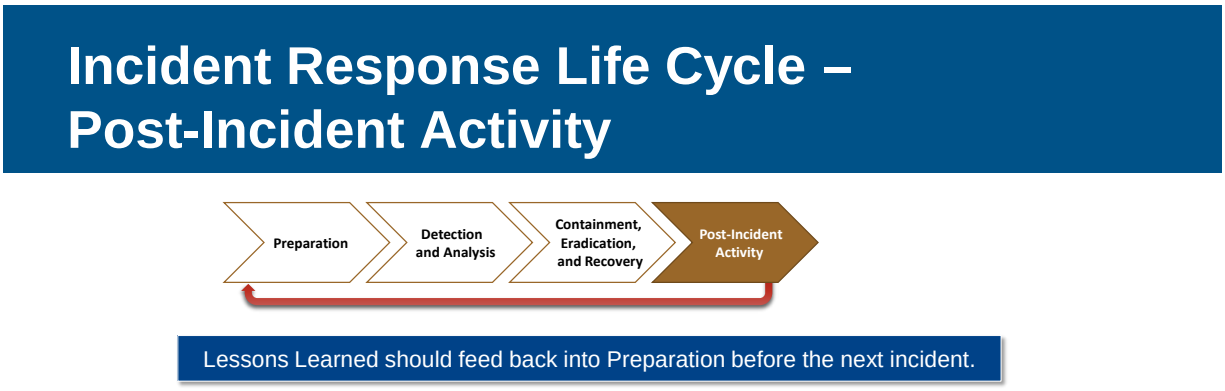
Incident Response Life Cycle – Containment, Eradication, and Recovery



**010 Now, suppose that risk has been realized. You're now to a point where you need to actually contain this incident to make sure that whatever is happening, whatever's impacting your organization negatively, is not going to incur additional negative impact, and you're actually going to want to remove or eradicate the problem altogether and get your organization back on track. That's what we're

doing in this particular step. Once again, it's important to keep track of all the facts and the data as it happens. So that way you can have some forensic analysis down the road. Even more importantly, you have to have your people in a mindset that they need to actually get the organization back up and running in a safe manner. Safety is key here.

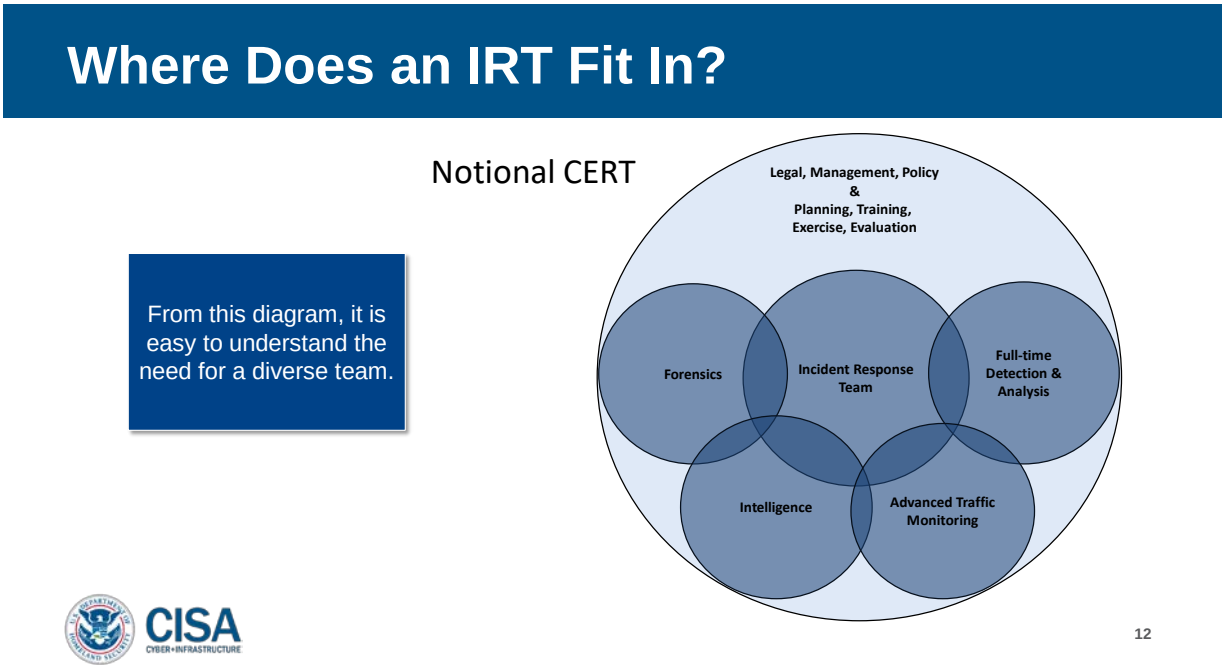
Incident Response Life Cycle – Post-Incident Activity



**011 Finally, once you've gotten past the incident, the fire trucks have gone away, the problems are all gone, and you may even be back up and running, really what you want to do now is dig in and do a hot wash and figure out what actually took place over the course of this particular incident. So that way you can have a large body of lessons learned to prevent it from happening

again, and maybe even affect a more efficient response next it happens.

Where Does an IRT Fit In?

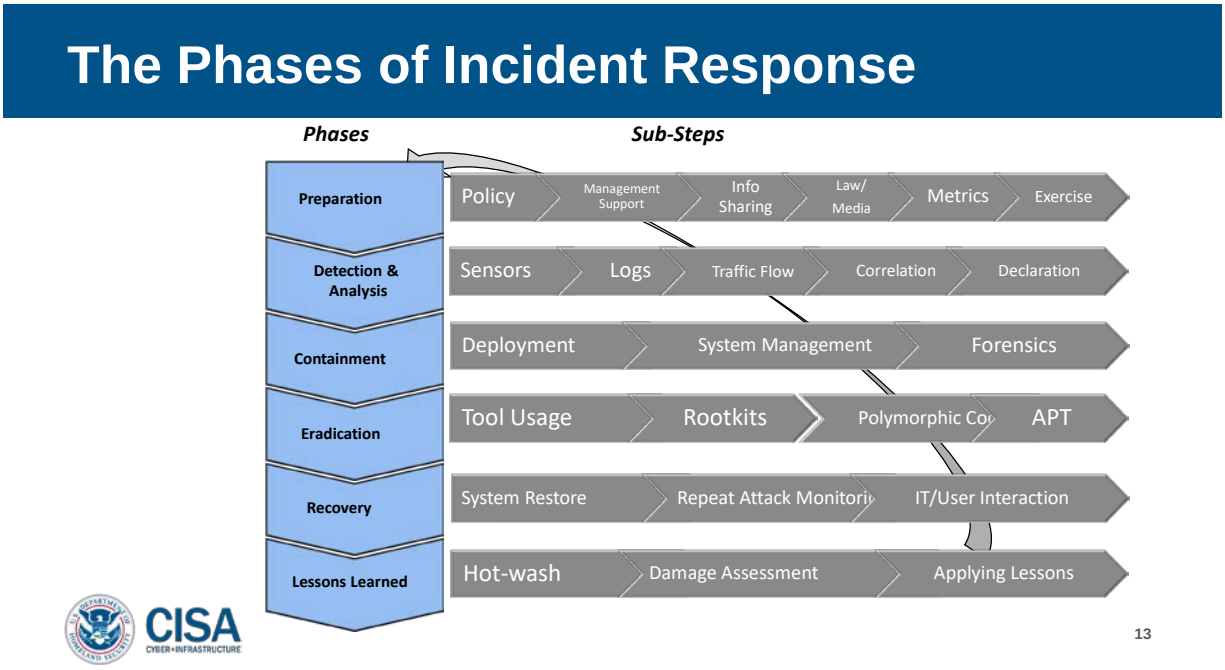


**012 So who's going to be in this team? You know, this is the response team. It has to be a team of diverse folks who have a lot of different skill sets. On this particular diagram, you see there's a Venn diagram here where you have the actual response team itself, and look at all the needs, all the critical skills that you have to have that are influencing it. Maybe people were specialists in forensics or maybe threat intelligence. You may have people who are actually doing network type work.

Monitoring. You may also have some automated systems that are taking place, and there are people who have to support that as well in terms of

maintenance and making sure things are operating properly, and then you have the broader organization around it that you may need to tap. Legal people, for example, may have to come in and help if there's a regulatory kind of an issue that's taking place. You may need decisions from a management team. You may need additional policies so that people know what to do, when to do it in terms of procedure, and you also have to make sure that everybody on this team is trained properly to do their job correctly.

The Phases of Incident Response

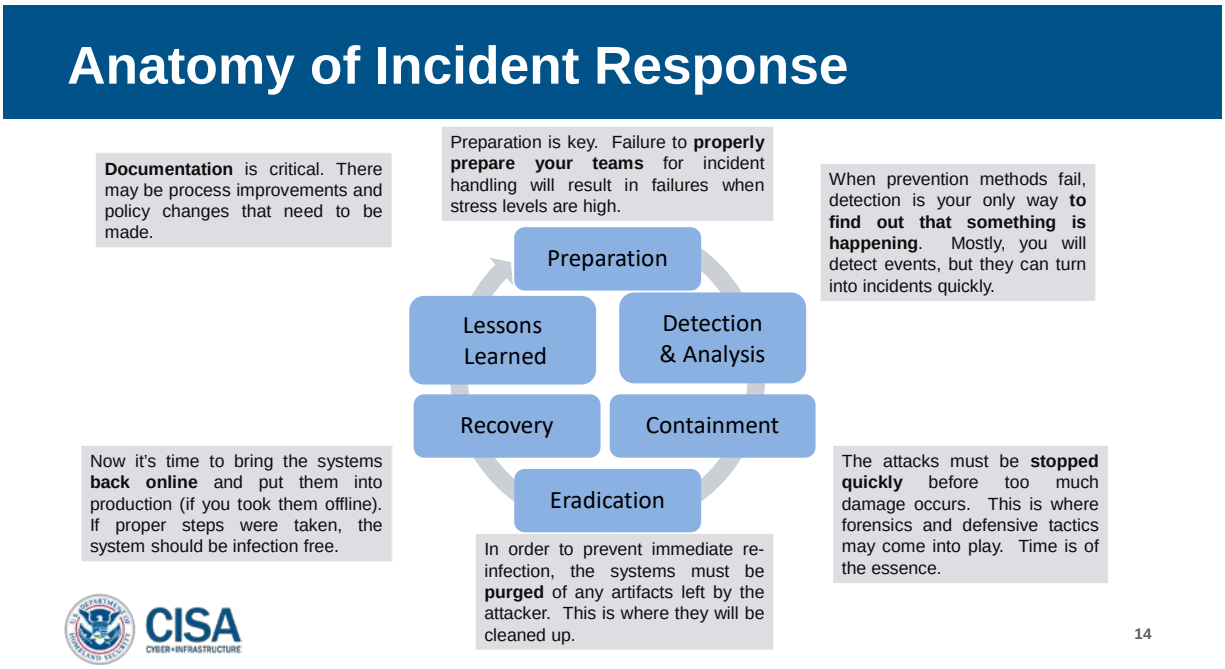


**013 So going through this, I want to bring to bear the notion that each of these steps are happening at any given point in a day, depending on what kind of traffic and the kind of action and activity that you're seeing in your network and in your system

at large. You're continually preparing for an event. That is to say that you're always looking at policy, you're always making sure that it's up to date. You're always maybe even training your people so that they're following the policy correctly.

This is going to take a lot of management support. There may be information sharing going on, there may be metrics that are being monitored. You may even be conducting exercises. Similarly, for the rest of these steps, and I'm not going to go exhaustively through each of these, I just want you to understand that there's a lot happening at any given point. So that said, you need to keep this all in a manageable picture. It's a real challenge, and you'll need help.

Anatomy of Incident Response



**014 At each of these steps, you really want to have the big picture at hand. In preparation, for example, you just want to make sure that your team is ready for that day, and how are you going to do this? You're going to make sure that they're trained, and you're going to find that as you exercise your policies and your procedures more and more, that they're going to be better prepared to handle that stress when that day happens.

You also want to make sure that they're detecting events properly. You know, do they know what they're looking for even? Do you have automated tools to actually help them do that? You also want to make sure that when the dark day happens that they know how to actually intervene, to make sure that

they stop the incident from getting any bigger or worse. So there have to be tactics in place that they can employ to actually contain the incident and then eradicate or purge the system of whatever the virus or the problem may be that's bringing your system down, and you also have to know that even if that is eradicated, the problem goes away, how is it that they can reboot the system to recover it so that way you can get your organization back into full operation? And finally, you're going to have a lot of facts left laying on the floor. You're going to have to pick it all up. You're going to have to integrate it and you're going to have to document it properly so that way you can learn from the incident, your organization can grow in maturity, such that you can address the event if it were to ever happen again.

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