Root Cause Analysis Methods

Table of Contents

Root Cause Analysis Methods

There are many different approaches, methods, and techniques for conducting root cause analysis in other fields and disciplines.

The analysis method used to identify the root cause(s) of a cybersecurity incident depends on

- the circumstances of the incident
- the information that is available/discoverable
- your specific incident taxonomy and types/categories of causes (or threat vectors)

Adapt your root cause analysis method to the incident being analyzed, as needed.

- You might use more than one method, or a hybrid approach.

A cause analysis process can guide analysts through the multiple questions and paths to identify the initiating cause(s) and threat vector(s) that enabled an attack to occur.

**012 So there are a variety of different approaches, methods, techniques that you can use for conducting root cause analysis, and we can adapt some of the ones that are used in other fields outside of information security and see how we can apply these to cybersecurity incident root cause analysis.

So generally the analysis method is going to depend on specifically the type of incident that we're looking at. Root cause analysis of a privileged compromise incident is going to be different from a denial-of-service attack incident. So it depends on the type of activity that's occurring, what

information is available to analyze, or accessible, or even in existence. If an intruder has gained privileged access on a particular vulnerable system, they may have deleted or tampered with some of the logs or evidence or information that's available to analyze on that system.

And then it's also going to depend, again, on your type of categories of the incidents or root causes or threat vectors in your particular process.

So again, there's a variety of different ways, different approaches that you're going to need to adapt as needed, depending on the type of incident, and even some of the examples that we used from other fields here in this example, you might have to use a hybrid or combination approach depending on the specific circumstances of that incident you're analyzing.

So the most important thing is coming up with some kind of process to help guide you or your analysts through the various questions that they need to address that are important to them for going to the next step and providing an appropriate response and course of actions to identify the underlying cause of the particular threat that allowed the incident to occur, and therefore provide a follow-up response appropriate and relevant to that particular underlying cause.

5 Whys

The 5 Whys (a.k.a. Five Whys) method iteratively asks "Why…?" to identify the root cause of a problem.

- This method is used in many cause analysis techniques, including the Analyze phase of Six Sigma.

Continue asking "Why…?" questions until the root cause is identified or until no further data/information is available (i.e., the cause is "unknown").

- This method may require more or fewer than five iterations of questions, depending on the problem.

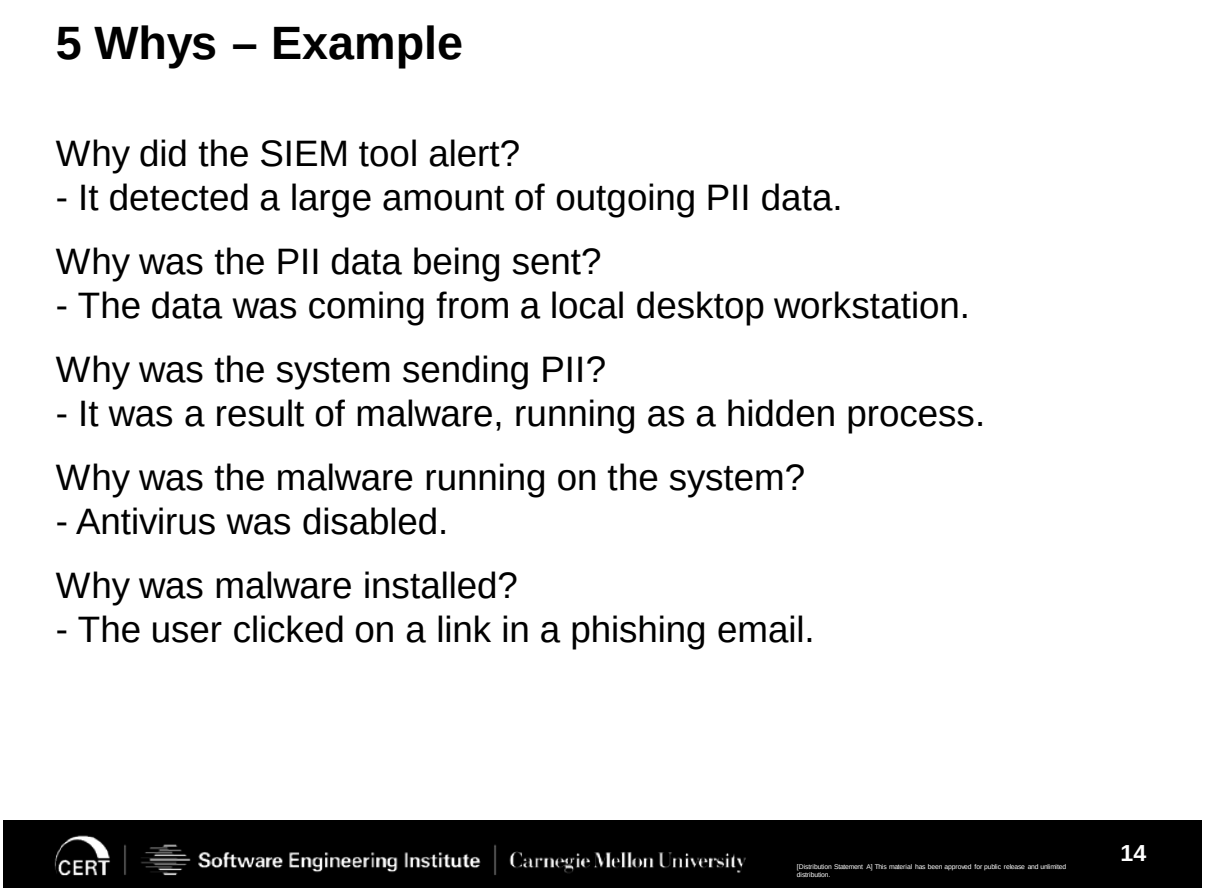
To answer the Why questions, you often also need to answer related What and How questions (as well as Who and When).

**013 So one method that's been used in a number of different fields is called the Five Whys approach, the Five Whys method, and basically what it does is repeatedly, iteratively asks the question why something occurred until you can identify the ultimate cause of the particular problem. So this technique is used, like I said, in other areas, such as the Six Sigma, the Analyze phase, and basically you just keep on asking those questions until the cause is either unknown or until you get to the answer. And even though the technique is called Five Whys, that's just kind of a generalized number. In many cases, you may be able to get

to the answer in fewer than five iterations, or in many cases, it may take more than five questions to address the particular type of answers for the root cause of this particular incident.

And as we mentioned earlier, To answer some of these why questions, maybe you can reword these or paraphrase them, or they might be related to the what and how questions, or even sometimes the who and the when.

5 Whys – Example



**014 So here's an example of applying the Five Whys approach to a

cybersecurity incident. Your security incident and event management tool might set off an alert, and the first why is why did this alert go off, and then looking at the details of it. The SIEM alert detected some amount of personally identifiable information, some data being exfiltrated or going out, was detected by some rule set, and it set off this alarm.

So then further analysis, digging down into why did this alert go off, was the threshold set correctly, and you find that it was indeed a correct positive and that data was coming from a local workstation within our network and it set off this threshold, this trigger-- so then the next question is why was this system sending PII data, and upon further analysis-- again, if those resources are available to you-- you may eventually discover that the PII was being sent by a hidden malicious code, malware process, that was undetected, and this malware program was actually sending out the PII data across the network.

So the next question may be: Well, how did this malware get on there? Why was it running undetected on the system? And further analysis was that for some reason the antivirus program that was expected to be running on this had been disabled. Maybe it was part of the installation of the malware or some other process, or maybe the intruder manually went in and disabled the antivirus product.

And then another why question is: Well, why or how did the malware get installed in the first place? And again, further analysis of the different data sources, or perhaps talking with the users involved, ultimately identified that the user had clicked on a phishing email that they received that contained a link, and by following this link they unknowingly downloaded and installed this malware, which caused all the other processes, which triggered the cause and effect, ultimately leading to the initial detection of the SIEM tool setting off the alert.

So this is just one kind of simplified example of how you might keep on asking questions until you eventually get to the underlying, initiating cause of the problem, so then you can address all the different phases, the different steps in the process, to fully mitigate against the problem.

Another Approach

Ask the 5W + H (Who, What, Where, When, Why, How) questions:

- What happened?
  - Outgoing PII data was detected by the SIEM tool.
- Where did the traffic originate?
  - It originated on a local desktop workstation.
- Who/what was sending the data?
  - Malware, running as hidden process, sent the data.
- Why/how was malware installed?
  - The user clicked on a link in a phishing email.

**015 Another approach, using a variation of Five Whys, is maybe the Five W's: who, what, where, when, why, and how questions. So again, this is just a slight variation, but again, asking questions to try to identify a particular cause.

So applying this approach to the previous scenario: What happened? Well, there was PII data that was detected by your SIEM tool. Where did that particular traffic originate? In this case, the where, we're identifying it as a particular host workstation within our network. Who or what was sending the data? Now, the who, the person, sometimes this

may never be known fully. Attribution of who the intruders are can often be difficult, and maybe the best you can hope is you might be able to trace it back to a particular IP address or host name coming from a location, and that may just be one link in a chain of other systems that the intruder may have used. But in this case, for what we're sending, is a particular piece of malicious code, this malware that was sending the data, and it was running as a hidden process on the system.

And then asking the question of how or why did the malware get installed, again, we come back to the answer that it was due to user involvement. They received a phishing email and they clicked on a malicious link in there to install the malicious code.

So that's applying a slight variation of asking different questions to come to identify the underlying root cause.

Ishikawa “Fishbone” Diagram

The Ishikawa diagram is also known as a cause-and-effect diagram.

The primary “bones” in the diagram are categories of related causes.

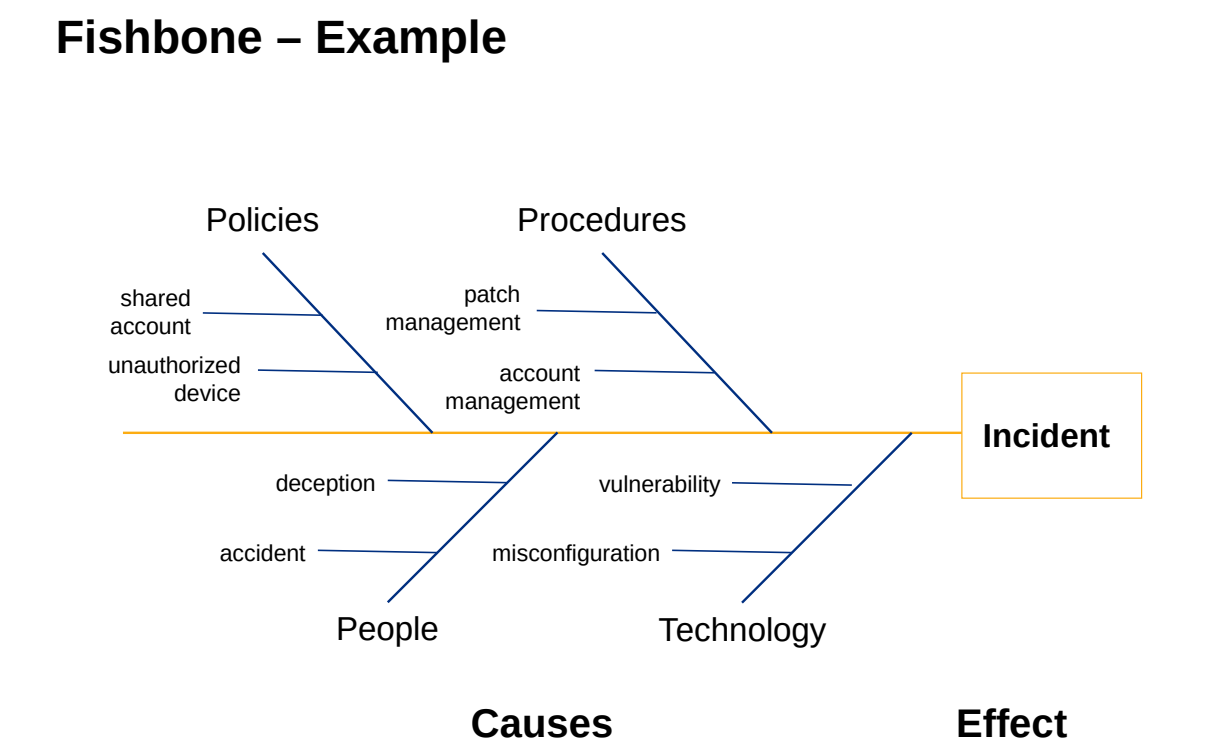
Each bone in the diagram can branch out into further categories/subdivisions, down to the specific root causes.

For example, these are categories used in service industries:

- policies
- procedures
- people
- technology

**016 Another approach, using other types of fields, sectors, and service industries is called the cause-and-effect, or Ishikawa, or fishbone diagram, and the reason it's called a fishbone diagram, as we'll see in the next slide, is it looks like the outline of a skeleton of a fish. So the primary bones in the particular cause-and-effect diagram are categories of related causes, and then each bone in that category can then have subcauses and branch out into further subdivisions and subtrees in this diagram, and depending on, again, how you define your different threats or causes--

Fishbone – Example



**017 Will affect how you address or use this process.

Ishikawa “Fishbone” Diagram

The Ishikawa diagram is also known as a cause-and-effect diagram.

The primary “bones” in the diagram are categories of related causes.

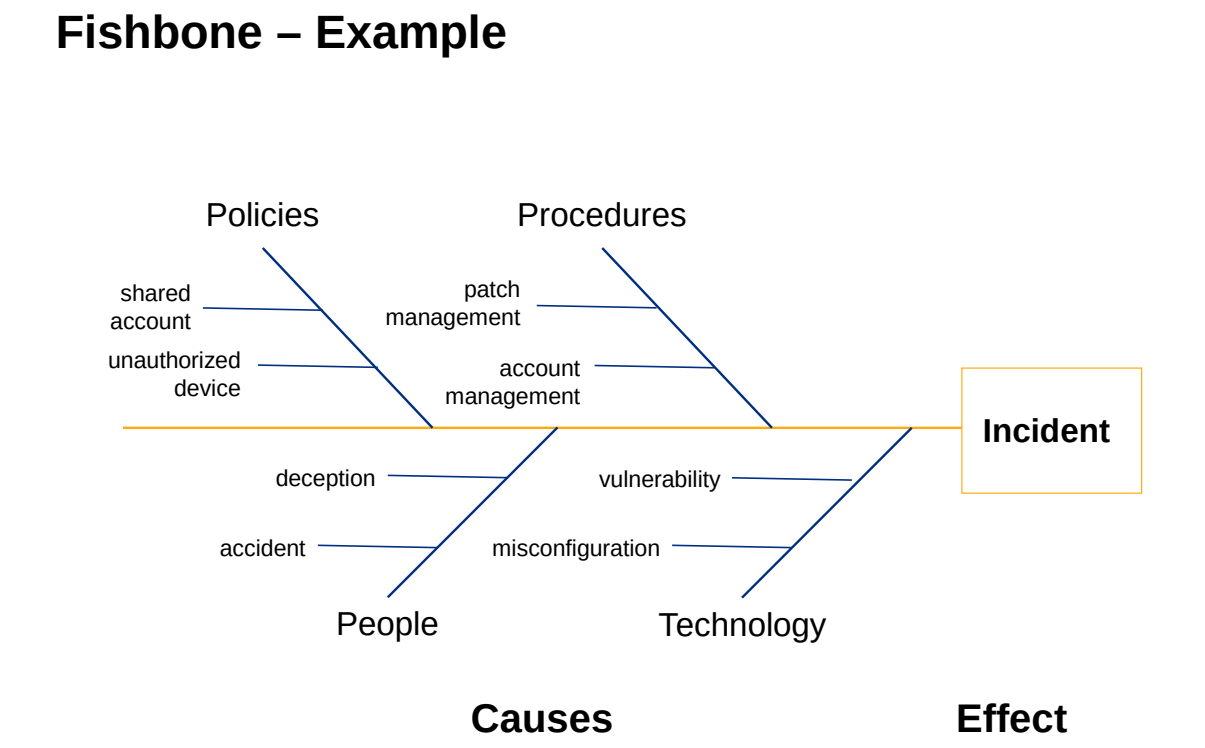
Each bone in the diagram can branch out into further categories/subdivisions, down to the specific root causes.

For example, these are categories used in service industries:

- policies
- procedures
- people
- technology

**016 In many service industries, an example is the high-level-- they distinguish between different policies, procedures, people and technology, and then they have, underneath each of these higher-level categories, different detailed subdescriptions on how these different causes might be used to identify various effects.

Fishbone – Example



**017 So applying the fishbone root cause analysis methodology to a cybersecurity incident, we can still take those same high-level categories of policies, procedures, people and technology and map different information assurance or information security characteristics to these.

So you might have in your organization different policies that prohibit sharing of user accounts. You have to have your own account, use a password, and you're not supposed to share that with other people. You may have a policy saying that you're not supposed to connect unauthorized devices to the

corporate network or the enterprise, so you wouldn't be able to connect your own laptop or connect to the organization's wireless network, or perhaps you might not be allowed to connect USB or flash drives to a particular system. So you may have policies that are in place, and the policies may have been violated.

There may be other types of procedural factors that are in place, such as you typically would have a patch management program, but for some other reason the procedure wasn't followed or it failed, and particular security patches weren't installed on a system that allowed it to be vulnerable and exploited.

Perhaps account management procedures are in place, but a failure to follow those procedures or a violation of those procedures could allow different accounts to be created or set up or to be not tracked or monitored appropriately, and this could cause an incident to occur.

People, the people factor. There may be a variety of different interactions or involvement that they might have. It could be that they were socially engineered or received, again, a phishing email message or some other way deceived or impersonated, and they took some action to allow the initial foothold into the systems that caused the incident.

Or it may be not a malicious but an accidental action or inaction that a person committed which could have

inadvertently leaked information or caused some other problem, that allowed the incident to occur.

And then there's a whole variety of different technological issues that you will want to try to categorize and identify, things from such as configuration problems or misconfigurations that could allow an intrusion to occur, different vulnerabilities that were undetected and how these are categorized and mitigated against them. So this is, again, just one way of putting together a higher-lever taxonomy or approach for addressing, identifying as much information as you can about the various factors that could allow an incident to occur, and then identifying what that underlying cause is.

Next Steps

After identifying the root cause, an appropriate course of action can be taken to mitigate the incident, leverage new indicators, and improve future detection.

- Remember that failure to mitigate the root cause(s) can allow new or repeat incidents to occur.

The following are response actions:

- Mitigate the root cause(s) (e.g., patches, workarounds, changes).
- Recover and secure the affected system(s).
- Communicate/coordinate with others.
- Track any follow-up information.
- Close the incident.
- Conduct a post mortem, lessons learned meeting.

The following are appropriate prevention/detection actions:

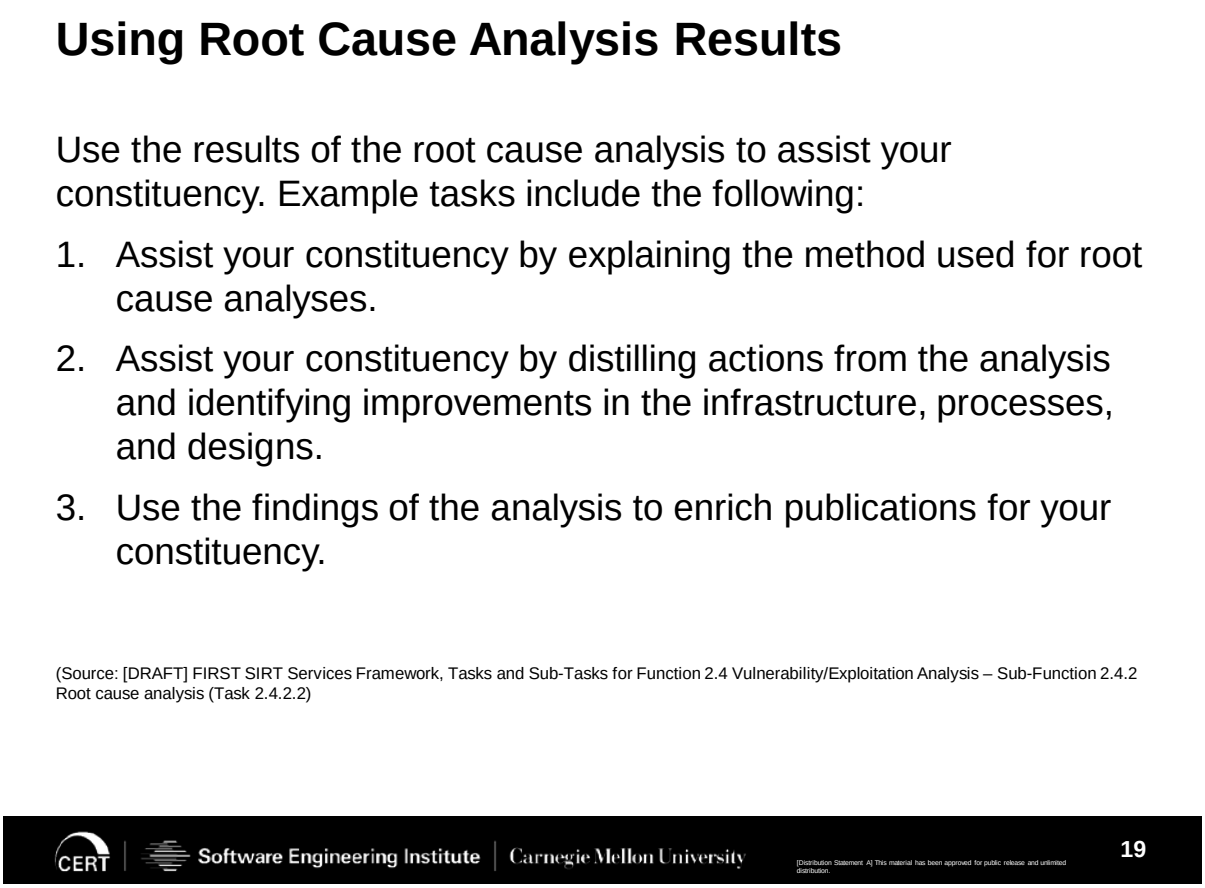
- Implement mitigation actions on other vulnerable systems.
- Add new attack signature/indicators to existing prevention/detection processes.

**018 So once you've identified what the causes are, the next steps are to feed into the response process and sometimes, like we mention also, it can also feed back into the preventative and detection processes too. So if you do not take a comprehensive approach at addressing, mitigating, eliminating the particular vulnerabilities, you may have the intruder come back and repeat the incident or occurrence. So making sure that if you don't understand what the underlying-- the root cause of the problem was, a superficial approach, such as changing the administrator root password, is not going to lock the intruder out. It may require, again, taking the system offline, completely rebuilding it, restoring data, patching

it, installing other security tools, and some of the other types of activities or courses of action that you would do in various types of response incidents.

And then feeding back to identifying the information-- if this is a new type of attack or a zero day vulnerability has been exploited, feeding that back into new indicators for detecting future incidents or preventing incidents from occurring in the prevent and detect processes.

Using Root Cause Analysis Results



**019 So again, Looking at the FIRST Services Framework, some of

the follow-up actions that might happen after the root cause analysis are helping-- perhaps one of the things you're doing is to advise your own constituency on how to perform root cause analysis, especially if you're a coordinating CSIRT, and you don't have access to a lot of the data sources, giving them some guidance on how they can perform a root cause analysis locally.

In addition, if they do perform their own local root cause analysis, you may be able to help the constituents in providing, again, recommended course of actions and response for eradicating and cleaning up after the incident, recovering from it, as well as future improvements such as detecting and preventing incidents with their own systems themselves.

And then you can also use the results of root cause analysis in providing better communications and general information and guidance to your constituents as far as outreach and communications.

Notices

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 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.

DM-0003588