Analytical Methodologies - Contrarian Technique

Table of Contents

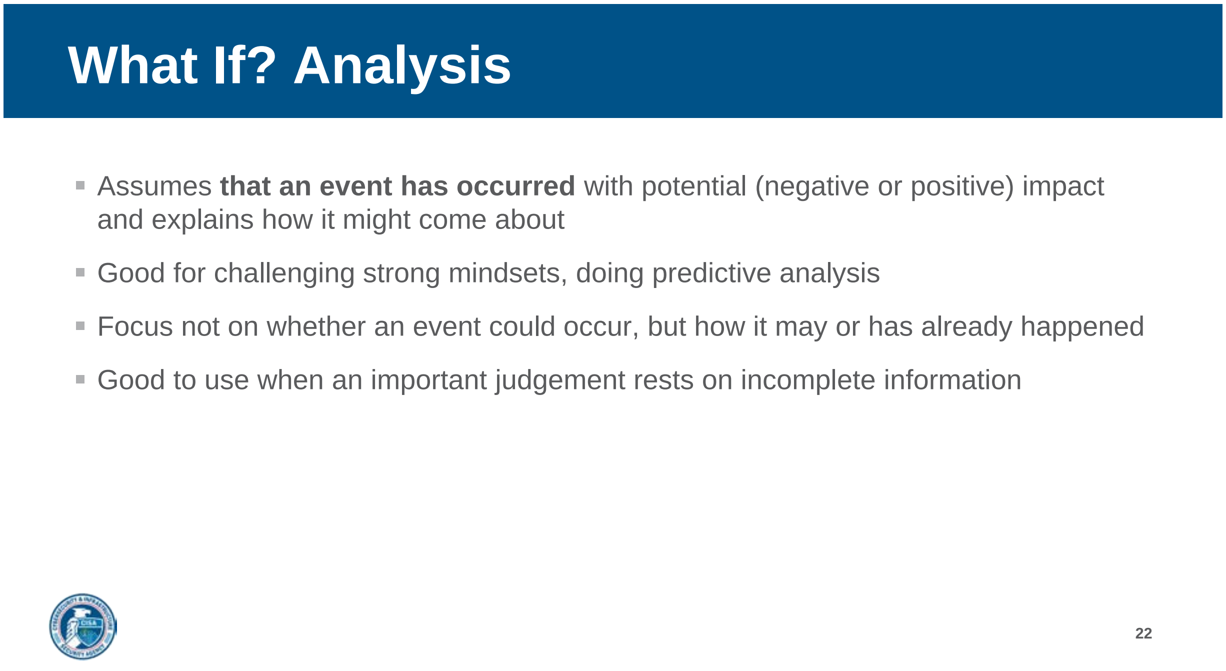
Analytic Methodologies – Contrarian Technique

Analytic Methodologies – Contrarian Technique

21

**021 Let's look at a contrarian analytical technique a What If? analysis. Contrarian techniques explicitly, again, challenge current thinking.

What If? Analysis



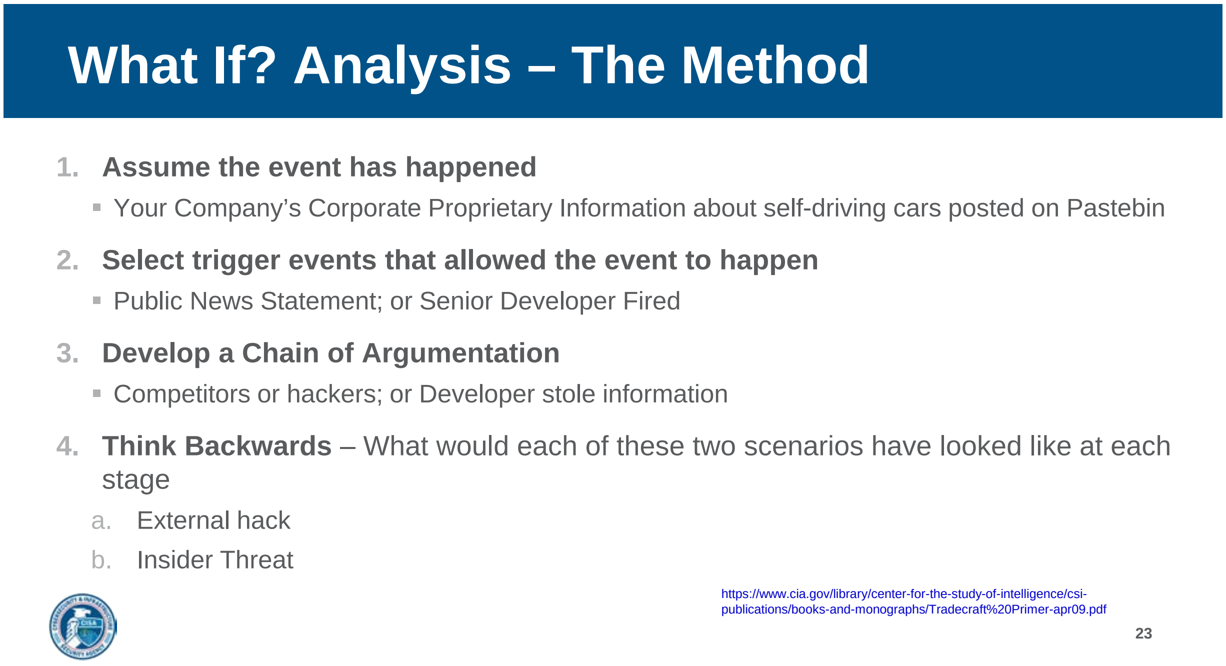
What If? Analysis

- Assumes **that an event has occurred** with potential (negative or positive) impact and explains how it might come about
- Good for challenging strong mindsets, doing predictive analysis
- Focus not on whether an event could occur, but how it may or has already happened
- Good to use when an important judgement rests on incomplete information

22

**022 What If? analysis is beneficial because if frees analysts from arguing about whether an attack will occur. This analysis is good to do and should be done, especially if you have time to do it. It assumes that an event has occurred with potential negative or positive impact and explains how it might come about. So the focus is not on whether an event can occur, but that it has already happened.

What If? Analysis – The Method



What If? Analysis – The Method

1. **Assume the event has happened**
   - Your Company’s Corporate Proprietary Information about self-driving cars posted on Pastebin
2. **Select trigger events that allowed the event to happen**
   - Public News Statement; or Senior Developer Fired
3. **Develop a Chain of Argumentation**
   - Competitors or hackers; or Developer stole information
4. **Think Backwards** – What would each of these two scenarios have looked like at each stage
   a. External hack
   b. Insider Threat

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

23

**023 Let's do a very simple example here at a high general level, and I completely made this example up. It's not complete, but I think you'll get the gist.

So let's say you're working at a startup company that specializes in automation and self-driving cars, and let's assume that an event has happened. Let's say that the event was that your company's corporate secrets or proprietary information was posted on Pastebin or Reddit.

Next, you select a trigger event or events that would have permitted this event to have happened. For this case, I made up two possible trigger events, and I'm sure there could be more. Maybe one was that there was a recent public news statement on the company's website that your company had recently discovered and patented some incredibly new, amazing algorithm that allowed for a hundred percent, fully safe driving cars. The next trigger event was maybe that it was the chief software developer for your company who was fired last week for ethical violations.

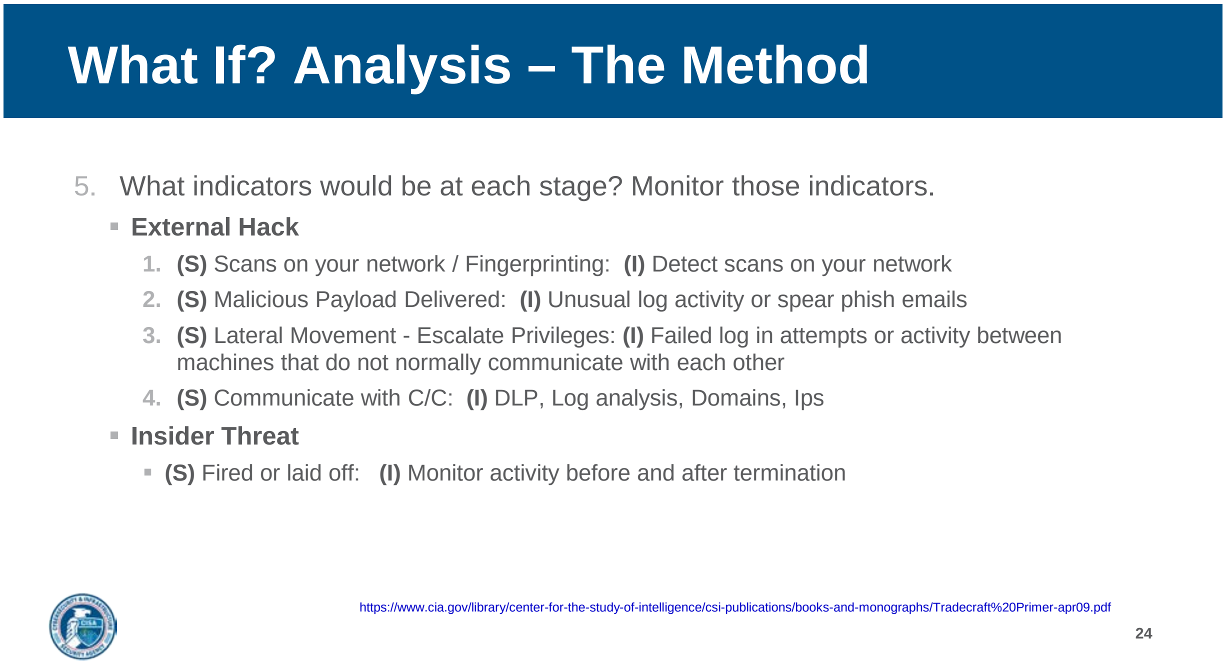
So these are just some examples, but you would need to select and figure out which triggers may have permitted such an event to have occurred.

The next thing you do is you develop a chain of argumentation based on as much logic or evidence as possible to explain how that outcome could have followed from those triggers. So for the first one, publicly available information about the new algorithm was exposed. Maybe posting the public news statement, or maybe having the public news statement, was not a smart thing to do because competitors saw this, or just some interested individuals heard about it and were interested in trying to hack in to figure out what the algorithm was. So the company was hacked in from the outside from these competitors or individuals.

The other trigger event, the senior developer being fired, maybe the developer took information with him or her before being fired out of revenge or profit.

The next thing you want to do is think backwards. In other words, what would each of these two scenarios-- the first being an external hack and the second being an insider threat-- have looked like in stages and indicators?

What If? Analysis – The Method



What If? Analysis – The Method

5. What indicators would be at each stage? Monitor those indicators.
   - **External Hack**
     1. **(S)** Scans on your network / Fingerprinting: **(I)** Detect scans on your network
     2. **(S)** Malicious Payload Delivered: **(I)** Unusual log activity or spear phish emails
     3. **(S)** Lateral Movement - Escalate Privileges: **(I)** Failed log in attempts or activity between machines that do not normally communicate with each other
     4. **(S)** Communicate with C/C: **(I)** DLP, Log analysis, Domains, Ips
   - **Insider Threat**
     - **(S)** Fired or laid off: **(I)** Monitor activity before and after termination

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

24

**024 So for stages, what you want to find is what would the indicator be at each stage. You establish these stages and indicators and then you monitor for them. So once you have listed out stages and for those change of argumentation, you would then list out the indicators for each of the stages. So as you can see on this slide, an S stands for stage and an I stands for indicator. So for publicly available information about the new algorithm that suggests that there might have been an external hack, the stage would be scans on your network, and the indicators that you would have for that stage would be you would want to detect the scans on your network for recon. You could set up your IPS or your IDS to recognize certain packets in scans, SYN scans, Xmas scans, NULL scans.

A second stage could be the malicious payload was delivered. So that would be a second stage, and the indicators for that that you could look for is unusual log activity or URLs or downloads from spear-phishing emails.

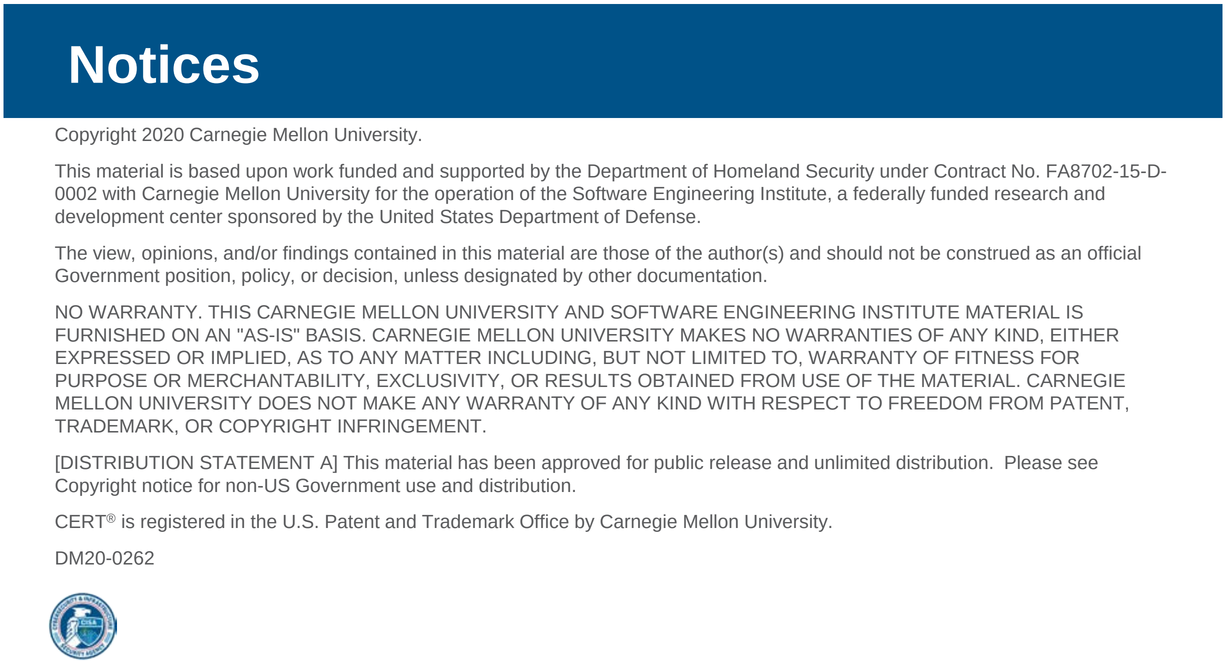
A third stage would be lateral movement. Indicators that you could monitor for-- and that's even more tricky to do for lateral movement, so you should know first what does normal activity look like on your network, have a baseline, and make sure your network is segmented. Another indicator would be to look for a number of failed access or login attempts, or if you notice activity between machines that normally don't communicate with each other.

Another stage would be communication with the command-and-control server. So indicators you could set up for that would be a DLP or log analysis, or callout to some shady domains.

So for the other trigger event, insider threat, a stage could be if someone was fired or laid off. Indicators for that could be monitoring activity before and after termination, any logins or badge-ins, and suspicious emails from those folks that may be terminated, any remote access attempt from usernames that no longer work at the company, or any odd or suspicious comments about the company by a competitor or by employees from a competitor.

So that is an example of What If? analysis and working backwards.

Notices



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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM20-0262