5Ws 1H - question to ask when analyzing security incident

When you are analyzing security incident, what is your ultimate goal, what answers you want to get? And why? If you want answers what would be your questions? Proper questions are essential for getting useful output from your investigation. Asking the right one will give you to get full picture of situation and give proper base for next step.

What happened?

This question is general situation awarenes. Is incident a full story or what we see is just symptoms which require more context? Is incident security related or is it a failure? Is it just webpage defacement or data were stolen? Is this just irregularity in users outbound transfer or data exfiltration? Is this real incident or false positive.

Next steps based on answer **what** will be decision about if response is needed and choosing proper response playbook. **What** will be also indicator to assign priority to incident.

Where did it take place?

This question is focused on assets or identities affected. What kind of environment were affected, is it test or prod? What is location of your assets, internal or hosted? Are identities your own or outsourced? What kind of data were affected, PII, condifential?

Answering **where** is second factor together with **what** in prioritization process. Classification of affected resources may help in answering **why** and provide guidance if other than technical response is needed, ie PR or legal departament had to be involved because PII data were disclosed. Answer **where** points also on log sources which should be analyzed.

When did it happen?

Understanding of incident timeline is crucial in incident analyze. **When** incident was detected, **when** did it started and how its phases maps on killchain? How much time had attacker to work on his objectives?

Answers in this area may lead to conclusions about how much damage could be done, how much data could be extracted, is there time correlation with specific event like new project

(**why**), known phishing campain (**who**). It also determine scope of logs which has to be reviewed.

Who did this?

This is usually hardest question to answer but clues found during investigation may point on specific actors connected with incident.

Identification of attacker will support investigation by providing possible motive and TTPs connected with actor, resources which may be in scope of interest of actor (**where**). This knowledge is may be essential in process of finding all affected resources. It will also indicate if there is possibility to take legal actions against attacker.

Why did it happen? This question actually may have two meanings. First is about motives of attacker, why did he decided to attack us? Were we just random victims or rather attack was targeted? Crosshair on our back is just because our organization is from specific industry or attack was performed or inspired by competitor?

Finding motives may directly lead as to answer **who**. It may also helps with indentification **where** was interest of attacker focused.

Other aspect of this question is finding root cause of incident. **Why** it was possible to happen? Was that technology or process flaw or maybe human error or even intentional action? Look on 5**Why** technique as it may be helpful in this case.

When we know why did incident occurs, what was a cause we can use this knowledge to find countermeasures, what and how it can be fixes.

How did it happen? This question focus on TTPs used during attack. What were tactics, techniques and procedures used during attack.

This knowledge is closely connected with second **why**, finding root cause. It may also points on actors involved in attack (**who**) if TTP are specific or similar to other attacks.

There is not right order in answering to those questions, but often getting answer on one question gives a clue on other.

Not always you will find all answers on your questions. But it is important to ask all of them as getting answers is like taking of blindfold, increasing visibility on incident helps in taking better aimed actions during incident response and post-mortem.