Top Thirty Threat Hunting Questions

Introduction

In this article, we examine the top thirty interview questions that could be asked of you, the Threat Intelligence Hunter applicant by an IT Recruiter. The idea behind this is to get you prepared as much as possible, so that you can land that Threat Hunting that you have aspired for so long. Remember, Threat Hunting takes a very unique skillset in order to be successful.

Use this article to prepare for that next interview!

Level 1 Questions

Question 1:

Why do you want to become a Threat Intelligence Hunter? Is it the money that is making you attracted to this position?

Obviously, many Cybersecurity professionals apply for positions once they see the high salary levels that they can command for a particular role. But remember, the recruiter is wanting to understand your motive here as to why you are applying for this particular position. They want to see that you attracted to this position not just from the standpoint of money. If this is the case, that is a huge red flag to them, as they know you will not stay for a long time. They want to know for sure that you will be around for quite some time, and will be a dedicated employee. The reason for this is that they will be also ***making a substantial investment in you***, in order to bring you up to speed on the Security requirements of the organization.

Probably the best way to answer this question is to angle the answer as to how the company can benefit from your skillset. Tell them that you have a "burning" desire to help others and your company to fend off Cyberattacks, but above all you also want to help protect their brand in the eyes of their customers.

Question 2:

What makes your skillset different from the other candidates that we have looked at?

In this kind of question, the recruiter wants to see your confidence shine through, as there will be many other candidates applying for the same position as well. In other words, they want to see that one differentiating that separates you from the rest of the crowd. Yes, everybody will have certs, work experience, and some sort of educational degree, but you need to look into yourself as to what makes you different.

Question 3:

What are the needed skills in order to be a successful Threat Intelligence Hunter?

It is important to keep in mind that becoming a successful Threat Intelligence Hunter in many ways is different than other Cybersecurity positions. For example, not only do you need a relatively strong quantitative background, but you need to have exceptional qualitative skills. This is what the recruiter is trying to determine if you have this by asking this particular question. For instance, not only must you have very keen eye in order to find unseen trends in the information and data that you collect, but you must be able to break that down to a level that your client can understand as well. Also, you must have

the ability and patience to work long hours, but most importantly, you must have that all important investigative mind in order to thoroughly complete a Threat Hunting exercise.

Question 4:

How do you deal with a difficult client? How do you address their needs?

By the tone of this particular question, this is obviously a psychological based question. In this question, the recruiter is trying to determine your communications style. Remember, as mentioned before, not only will you be working with a dedicated team, but you will also be interfacing directly with the client as well. Many times, the client can be difficult to work with. For example, there may risks out there in their organization that you want to further investigate. But the client may be demanding and on want something else checked out. Perhaps the best way to answer this question is that you should offer the client different options as to what should be investigated, and what you think is important. But remember in the end, it is the client that has the final say so in what will be examined, as they will be signing the documents that lays out the Statement and Cope of Work. If you step out of these bounds without prior client approval, you put not only yourself but the business or corporation that you work for at grave risk for a major lawsuit.

Question 5:

What is Threat Hunting?

You can be guaranteed that this will be one of the first questions that will be asked of you. The recruiter is not just looking for a memorized, textbook answer; rather they are examining to see if you can give a simple explanation if asked, especially by your client. A possible answer is:

“Threat hunting is the process of seeking out adversaries before they can successfully execute an attack.”

(SOURCE: 1)

This answer, while very broad in nature and scope, is succinct and to the point. You basically want to phrase it in such a way that the bottom line (or the primary goal of it) is to literally “hunt down” those Cyber threats that are appear to be imminent on the horizon and mitigate them before they execute their malicious payload and cause widespread damage to the IT Infrastructure.

Question 6:

What is the difference between Threat Hunting and other Prevention and Detection based methods?

In this kind of question, the recruiter wants to make sure that you have a good understanding of how Threat Hunting is different from other methodologies, and why it is so important to their particular organization. A good answer here would be to state that Threat Hunting is very much a proactive Security Methodology that makes use of sophisticated analytical tools (such as those of Artificial Intelligence and Machine Learning). The Threat Hunting process first starts with formulating a specific hypothesis, in which the catalyst for this was some kind of alert, assessment, or even the results of a Penetration Test. This hypothesis will then be tested by using the above-mentioned tools to search for this potential Cyberthreat that has not been formally detected yet.

Question 7:

What is the primary difference between Threat Hunting and Threat Detection?

Although these two sounds very similar amongst one another, they are actually very different. The answer here is Threat Hunting is geared towards the ***potential determination*** of Cyber related threats at their earliest stages possible. With Threat Detection, ***an actual Cyberthreat has been found***, and all efforts are dedicated in order to mitigate it.

Question 8:

What are some of the benefits of Threat Hunting?

Obviously, the main benefit of Threat Hunting is that you are taking a proactive stance on the Cybersecurity Landscape to see what potential threats are possible lurking from within your IT Infrastructure. But it is important to keep in mind that the recruiter is trying to test if your understanding of Threat Hunting goes much deeper than just the obvious. In order to prove your level of expertise, you could mention some statistics such as the following:

According to a recent SANS survey:

*Clients reduced their attack surface by at least 75%;

*59% of respondents felt that Threat Hunting greatly improved their Incident Response timing;

*52% of respondents found Cyberthreats via Threat Hunting; otherwise they would not have been detected by other means.

(SOURCE: 2)

Question 9:

What are some of the drawbacks of Threat Hunting?

Of course, Threat Hunting has its flip side as well. This is very important in communicating to the client, as they should ***not be given the impression*** that each and every potential will be detected. The recruiter whom is interviewing you wants to make sure that you fully understand this. A good answer here would be state that (one again, citing a few stats will show your expertise):

*From the same survey as mentioned previously, 88% of the clients polled felt that their Threat Hunting processes needed some serious improvement;

*53% of the respondents felt that their Threat Hunting processes were too transparent to the outside world;

*56% of the respondents felt that the Threat Hunting process takes too long, and is still very cumbersome.

Question 10:

What makes your cert different than the others that are other there?

In the world of IT Certification today, there are tons of certs that one can get. While you should strive to get a cert that is related to the Cybersecurity career you choose to aspire, in the end you can really choose to get any cert that you want to get. In the field of Threat Hunting, there is a premier cert that is known as the "Certified Cyber Threat Hunting Professional (CCTHP)". If you have this cert, or are at least planning to get it, you need to specifically bring this out in your interview. For example, you need to tell the recruiter that in the field of Threat Hunting, this is the premier cert to have. For example, it demonstrates that you have top level and expertise knowledge in Threat Hunting, as it covers five, very specific domains that include the following:

*The goals/objectives of Threat Hunting;

*The methodologies and techniques that are specifically utilized;

*How to hunt for Network based Cyberthreats;

*How to hunt for Host based Cyberthreats;

*The tools and technologies that are used in Threat Hunting exercises.

Level 2 Questions

Question 1:

What is the primary difference between Threat Hunting and Penetration Testing?

Very often, these two types of Security Methodologies are used together; but in reality, they are totally different. Although the ultimate goal or outcome of both of these is to unearth any unknown Cyber based threats or risks, Penetration Testing involves trying to break through an organization's lines of defenses. You are trying to see how far you can go in, without being detected. In other words, with Penetration Testing, you are taking an outside – in approach. But with Threat Hunting, this is much more of an inside – out to approach. For example, you are taking the assumption (or more specifically the hypothesis), that an adversary could already be lurking from within your IT Infrastructure; thus, you are taking steps to ascertain that. If your hypothesis is indeed confirmed, you then will try various attempts to mitigate them, so that they can penetrate from the outside environment ever again.

Question 2:

Is Threat Hunting simply just devoted to finding internal Cyber threats, or does it involve more than just that?

In this kind of question, the recruiter is trying to determine (generally speaking) the depth of your Threat Hunting knowledge. The answer to this is yes, you are trying to find to them, but there is much more involved than that. For example, with the information and data that you have collected, part of your other job responsibilities is to sift through it and determine any unseen trends with the analytical tools that you have on hand. With this, you should also be able to ultimately create various models of the future Cyberthreat landscape, which will be indicative of what potential Cyberattacks could like down the road for your organization.

Question 3:

What happens if I don't find anything in the Threat Hunting Exercise that I have just engaged in?

Yes, it is theoretically possible to not find anything at all, and to prove hypothesis was false. Was this a complete waste of time then? No, not at all. There is a very good chance that you discover other kinds of Security Vulnerabilities which you thought never existed before. For instance, suppose that your Threat Hunt reveals something else, such as that there is an abnormally larger amount of bandwidth that is being used by other employees of the company. You report this to your CIO or CISO, and they want more analysis done. A further investigation reveals that many of them are using the FTP Protocol to back up their work-related files. This would obviously be a complete violation of your Security Polices, and as a result, you have discovered that "Shadow IT" is clearly evident in your company (this is when employees use non-authorized IT tools to conduct work related duties).

Question 4:

What is the ATT&CK Framework?

This is an expansive Threat Hunting Methodology that stands for "Adversarial Tactics, Techniques, and Common Knowledge". It was developed by the Mitre Corporation, and has been around for quite some time. The basic premise of AAT&CK is to further break down Cyberthreats into a multipurpose classification scheme, so that you can compare the information and data that is available here to what is actually transpiring with regards to threats and vulnerabilities in the Cyber environment of your organization. This is actually more of a knowledge base, and much more detailed information on it can be seen here, at this link.

Question 5:

Should I just pick any random area of the ATT&CK Framework to start my Threat Hunting exercise?

While it is very important for the Threat Intelligence Hunter to have an overall open mindset, they should not just at random pick something off of it and start looking around. Rather, you need to first analyze the log files (as well as the respective warnings and alerts) to see what trouble points exist. You also need to make sure that you have the right access permissions and privileges for those resources in which you need to conduct your Threat Hunt. For example, don't search for Account Manipulation adversaries if the access permissions and tools are not in place first. In other words, it is first very important to determine what you want to specifically achieve from your Threat Hunt. This is best accomplished by first formulating your hypothesis, as described earlier. It is important to keep in mind as well that a Threat Hunting exercise should be viewed as a scientific experiment: You are collecting information/data in order to prove or disprove your hypothesis. Also, be resourceful and use the other Security Technologies that you have on hand to further substantiate your hypothesis.

Question 6:

Where does one draw the line between Threat Hunting and Incident Response?

Like Penetration Testing, there can be confusion between these two. Thus, it is important to keep in mind the literal meaning of these two terms. For instance, Threat Intelligence Hunters "hunt" for the adversaries that could be potentially lurking from within the IT Infrastructure, and to confirm their existence. The Incident Responders do just exactly that: They respond to Cyberthreats once they have been alerted to that fact, and use the resources that they have at their disposal to mitigate them. Usually it is the Incident Response Team that the Threat Hunting Team turns to first. The Threat Hunting

Team should not be called upon to specifically mitigate a Cyberthreat; but rather, they should have the capabilities to work closely with the Incident Response to share their expertise in order to contain it.

Question 7:

Should I move from left to right when using the ATT&CK Framework when executing my exercise?

Really, in the end there is no specific order in which to move in ATT&CK. In other words, don't feel that you have to address each and every Cyber related issue in the Framework, and above all, don't feel overwhelmed by it. Use the ATT&FM as a support anchor for your hypothesis, and start from there. If you don't have a hypothesis at first, then start your Threat Hunting exercise where you feel that your high risk and first impact areas are in your IT Infrastructure, then work from a top-down approach from there. While speed is important is important in Threat Hunting, addressing issues in an incremental and accurate fashion is equally important. But if you feel that you must take a macro level when first assessing the Cyberthreat environment, give serious consideration to using the methodology known as the "Mandiant Cyber Attack Lifecycle". More detailed information on this can be seen here.

Question 7:

As we know, one of the ways a Cyberattacker can launch their specific threat vectors is through Privileged Escalation. What should a Threat Intelligence Hunter look for specifically in these instances?

There are different kinds of variables to look out for, but most importantly, a Threat Intelligence Hunter should first look into any known gaps or weaknesses that currently exist within the IT Infrastructure of an organization. In this instance, making use of an EDR solution (which can be viewed as a subset of Threat Hunting) would prove to be the most beneficial technique to be used. A Threat Intelligence Hunter should pay a lot if importance to what is know as "File Integrity Monitoring" (or FIM for short) on those IT Systems (for instance, servers) where the integrity of files should not be changing. If there are any suspicious changes to the files, a history of employee logins must be examined for any types of anomalous behaviors. Also, you should also any systems that have been misconfigured, as this is another backdoor for the Cyberattacker to penetrate through.

Question 8:

Should a Threat Intelligence Hunter just conduct their exercise in just one part of an Infrastructure, or should they be examining multiple areas?

Yes, by all means a Threat Intelligence Hunter and the team should be examining different areas. Just because you have a formulated a specific hypothesis, it doesn't mean that you should look in just one area. Rather, I order to get a comprehensive view of your IT Infrastructure, the Threat Intelligence Hunter needs to examine other areas, which for example include the normal, everyday IT Systems, the Virtual Machines, your Servers, and even your Production Environment, but make that in these instances, that you have the appropriate backups in place.

Question 9:

What is the value of Threat Hunting if a business or corporation already has automated tools in place?

A popular, automated tool is known as "Cb Response". It helps to keep an eye on any intrusions an organization 24 X 7 X 365. But keep in mind that systems like these can only provide information and

data that is fed into it from the various intelligence feeds that you are currently make use of. But ultimately, it takes human intervention and a keen eye to further investigate the alerts and warnings that these systems provide. It is only through this process can one truly determine if a Cyber threat is imminent, or there is actually a threat actor that is lurking in your system.

Question 10:

What are the two primary types of Threat Hunting Exercises?

The two are as types are as follows:

The On-Demand Investigation Mode

In this mode, Threat Hunting is used by IT Security teams to quickly investigate any suspicious or anomalous activities after they have been detected. Once the incident has been specifically identified, it is then passed to the Security Operations Team for deeper investigation and recommendations for containment and recovery.

Continuous Monitoring or Testing Mode

In this model, the Security Operations team is continuously monitoring and/or or testing their security posture by conducting various Penetration Testing exercises in order to proactively identify and investigate any suspicious events.

This newer type of approach may be initiated by the business entity itself; or it can be outsourced to a Managed Security Service provider.

Level 3 Questions

Question 1:

Can you describe the five parts of the Threat Hunting Maturity Model?

Yes, there are five steps that are involved, and they are as follows:

*HMO-Initial:

At this stage, the organization is 100% dependent upon the use of automated tools, such as SIEM's and other AntiMalware/Spware software packages in order to provide a warning and alert system.

HM1-Minimal

The organization is still heavily dependent upon the use of automated threat tools (as described above), but the IT staff is at least doing a minimal amount information and data collection.

HM2-Procedural:

There is more human intervention involved than in the last step, but the organization is still dependent upon using Threat Hunting procedures that other entities have created; they still have not yet crafted their own set of procedures as of yet.

HM3-Innovative:

At this stage, the organization has created a minimal set of Threat Hunting procedures on their own, and are even employing a small number of Threat Intelligence Hunters to track down any potential adversaries.

HM4-Leading:

The organization has now reached a point where they have crafted their own complete set of Threat Hunting procedures, and have even incorporated the use of automation into them.

Question 2:

One of the biggest threats that is now happening is that of data leakage, whether it is intentional or not. How would you specifically describe data leakage?

In technical terms, especially as it relates to that of the Threat Intelligence Hunter, data leakage can be defined as the separation and/or the departure of a Data Packet from the place where it was intended to be stored.

Question 3:

For the Threat Intelligence Hunter, knowing the potential sources of data leakage is a very crucial first step in formulating an observable hypothesis. Can you tell me, what are the top sources of data leakage?

Yes, and they can be broadly categorized as follows:

*Employee error (again, this could be non-intentional, but this could stem from an Inside Attack as well);

*Any unforeseen technological glitches from within the IT Infrastructure;

*Server, workstation, or wireless device misconfigurations;

*A Web based application that was developed internally in an organization, but it was created using insecure Source Code;

*Inadequate security controls that have been put into place at the organization.

Question 4:

What factors (or rather, pieces of information/data) would you consider when formulating a hypothesis that a data leakage incident is occurring?

I would look specifically at the following:

*Any risk profiles that have been created;

*Any sort of impact and severity chart that relates to critical systems;

*Any incident workflow diagrams that have been previously created (especially in the wake of previous Cyberattacks that may hit the business or the corporation).

Question 5:

As a Threat Intelligence Hunter, you could also be very well working with Threat Intelligence Analysts as well. Can you describe in more detail the three types of Threat Intelligence Analysts?

In this kind of question, the recruiter wants to ascertain that you are fully aware of other job titles that are involved heavily in Threat Hunting as well. The three types of Intelligence Roles are as follows:

*Tactical Intelligence:

These individuals are heavily involved with examining the Network Infrastructure of an organization. They primarily work at Security Operations Centers (also known as SOCs), and spending time confirming any sorts of unusual behavior and adversaries, that are trying to break through the lines of defense.

*Operational Intelligence:

These individuals spend much of their time trying to examine in close detail the operating environment of the corporation or business, focusing upon and sorts both internal and external threats.

*Strategic Intelligence:

These kinds of individuals are heavily involved with reporting findings to the C-Suite, in an easy to understand and comprehensible format, with a primary focus upon providing advice on Risk Management based decisions, and the possible Return On Investment (ROI) on investing in newer types of Security Technologies.

Question 6:

Suppose you have been asked by your CIO/CISO on what kind of Threat Hunting tools your team plans to use. He or she is not interested in tools that are developed inhouse (primarily because they are fearful of the potential use of insecure Source Code); but rather, they want a list of commercial products that are available. What would you recommend that they should invest in?

Very often, especially in Cybersecurity, people tend to become creatures of habit, and like to stick to using the same tools repeatedly. The recruiter is trying to see if you can break away from this kind of habit, by testing your knowledge of the Threat Hunting tools that are out there, and that can be easily deployed in your organization. As of now, the top five Threat Hunting tools are as follows:

*Sqrrl;

*Vectra Cognito;

*Infocyte Hunt;

*Exabeam Threat Intelligence Hunter;

*Endgame;

*DNIF.

Question 7:

Can you briefly describe the four most widely used Threat Hunting techniques?

Yes, they are as follows:

*Searching:

This can be regarded as probably the most basic form of Threat Hunting. With this technique, you are trying to support your formulated hypothesis with information and data from a very specific set of defined search criteria.

*Clustering:

This is more of a quantitative, statistical based approach to Threat Hunting. With this technique, the Threat Intelligence Hunter is attempting to "cluster" similar datasets from a much larger, aggregate pool of data. In these situations, Machine Learning (ML) and Artificial Intelligence (AI) are tools that are used to accomplish this task, in an effort to find the hidden or unseen trends in these datasets.

*Grouping:

In this scenario, the Threat Intelligence Hunter is looking at different (or unique) artifacts that have been discovered, and identifying them based on the same set of criteria that was used to formulate the original hypothesis.

*Stack Counting:

This another type of statistical technique, in which the Threat Intelligence Hunter ascertains the total number of occurrences of a certain dataset by closely examining any sorts of outliers that may exist.

Question 8:

Apart from the ATT&CK Threat Model that I have asked you about, what are some other Threat Hunting Models that can be used?

In this question, the recruiter is trying to gauge your understanding of other models that can be used to meet the Threat Hunting needs of your organization. While the ATT&CK Framework is a very popular one that is used, there are others as well, such as the following:

*Lockheed Martin's Cyber Kill Chain;

*Fireeye's Attack Lifecycle;

*Gartner's Cyber Attack Model.

Question 9:

How do you define Endpoint Detection and Response (EDR)?

While you have answered in a previous question that it is important to analyze multiple environments in an entire IT Infrastructure, the Threat Intelligence Hunter will also be called upon just to examine certain parts of it, especially the Endpoints. A definition of EDR is as follows:

"Endpoint detection and response (EDR) provides visibility into activity occurring on the network and endpoints by continuously monitoring activity for behavioral patterns that appear to be suspicious or

anomalous. Data captured provides rich contextual information related to a threat to enable more efficient, prioritized remediation."

(SOURCE: 2)

In other words, you and your team are trying to find and determine if any potential Security risks exist where one point starts and where the other point ends within in your entire IT Infrastructure.

Question 10:

What are three important characteristics of an effective Threat Hunting tool?

You described the top 5 Threat Hunting Tools in a previous question, but this is a follow up question to see what makes them so top of the breed. These products should contain, at minimum, the following characteristics:

*It must contain logs, such as Windows events logs, EDR logs, Anti-Virus logs, and Firewall/Proxy logs.

*It must have a SIEM, which stands for a "Security Information and Event Management" system. It must be centrally located in the tool for easy access, and must be able to correlate all sorts of information and data in real time.

*A robust Analytics Engine, such as one that is Machine Learning (ML) or Artificial Intelligence (AI) based. It should be very effective in helping you and your Threat Hunting team find that "needle in the haystack".

Conclusions

Overall, this article has examined in detail thirty Threat Hunting related questions that a recruiter could potentially ask you. Remember, being an effective Threat Intelligence Hunter takes a unique blend of a very sharp mindset, as well as both quantitative and qualitative skills. If you would like to see more potential interview questions and answers as it relates to Threat Hunting, click here.

Sources

1) https://digitalguardian.com/blog/what-threat-hunting-emerging-focus-threat-detection
2) https://www.bloorresearch.com/technology/endpoint-detection-and-response/
3) http://www.infosecisland.com/blogview/24758-Threat-Hunting-is-the-New-Black-in-Security-Report.html
4) http://www.iacertification.org/ccthp_certified_cyber_threat_hunting_professional.html
5) https://www.cybereason.com/blog/blog-threat-hunting-101-you-asked-we-answered
6) https://www.csoonline.com/article/3267691/cyber-attacks-espionage/what-is-mitres-attandck-framework-what-red-teams-need-to-know.html
7) https://attack.mitre.org/
8) https://attack.mitre.org/techniques/T1098/
9) https://www.redcanary.com/blog/qa-threat-hunting-testing-visibility/
10) http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

11) https://sqrrl.com/the-threat-hunting-reference-model-part-1-measuring-hunting-maturity/
12) https://career.guru99.com/top-12-security-information-analyst-interview-questions/
13) https://www.cybervista.net/threat-intel-analyst-cybersecurity-roles/
14) https://www.firecompass.com/blog/top-5-vendors-emerging-threat-hunting/
15) https://www.cybrary.it/channelcontent/four-common-threat-hunting-techniques-with-sample-hunts/
16) https://digitalguardian.com/blog/top-tools-and-skills-threat-hunting-succes