CYBERSECURITY ANALYST INTERVIEW GUIDE
TOP 100 QUESTIONS (& BEST ANSWERS)

As part of our job placement process graduating over 1,000 successful analysts, we have curated a Top 100 list of interview screening questions (and best answers) that help our Academy graduates secure their jobs.

Recruiter Phone Screen Questions

1.	Tell me about yourself?	Be likeable and a real person. Example: My name is Richard Chapman. I'd like to say thank you for having me here today. I spent many years as a successful business manager and team builder. I am very excited to be able to merge my professional business management knowledge and experience with cybersecurity. After watching my brother-in-law do well in this field and realizing the importance of the industry, I decided I wanted to be a part of it. I studied and got my Comp TIA Security+ certification and now I currently work incident response in a SOC environment for CyberNow Labs! I investigate offenses in QRadar, alerts in Crowdstrike, and Proofpoint. I work through the incident response process to investigate and document threats to the CNL Network. I am excited to continue to grow my experience and knowledge and I am currently working toward my CySA+.
2.	Are you legally eligible to work in the USA?	Give your current status, no matter what it is. Yes - I am legally eligible to work in the US.
3.	What is motivating you to look for a new opportunity?	Example: CyberNow Labs is a great environment, however it is a small SOC. I am looking for more opportunities to grow. I would like to see more event types, use additional tools and grow my skills.
4.	Why did you leave your last position? (If you are coming from a completely different field, they will question why or how you made the leap? Question asked in all stages of interview)	Example: I am growing in my knowledge every day and I am wanting to challenge myself with a larger environment that will have more attack types, different tools, and different challenges. Example, from another career: I had an opportunity to join CyberNow Labs to get Security+ certified and work in a hands-on capacity. Now I am able to engage in security tool monitoring, investigating, and documenting my findings as an analyst.
5.	What made you decide to start a career in Cybersecurity?	Example: I had the opportunity to get to know cybersecurity while watching my brother-in-law who has been in the field for 15+ years. He has a great work-life balance, makes great money, and loves what he does. Once I understood it more, I was hooked and here I am today. Note: You can relate it to the field you are coming from, you can bridge a connection between these jobs and how it caught your interest.
6.	What would you consider to be your areas of strength and what are some areas you'd like to improve?	• What skills do you possess that the interviewer can use in their SOC? • What is a weakness that you have that you are aware of and are working on or have worked on? Be sure to explain how you are working on it or solved it. Example: As for my strength, I am a successful team builder and team leader. I love building people up and have had tremendous success doing that over my management career. As for my weakness, it has always been that I focus so much on my people that I have sometimes forgotten about myself and what I need. So, I have found that scheduling specific times to spend on just me is an important part of keeping this under control.

CYBERSECURITY ANALYST INTERVIEW GUIDE
TOP 100 QUESTIONS (& BEST ANSWERS)

Recruiter Phone Screen Questions

7.	What is your salary range expectation?	Example: Based on my understanding of the expected pay for an analyst with my experience as well as all the other skills I bring to the table that will benefit my employer, I would expect a salary between (Give a range of salary, example: $60K/yr - $80K/yr). Note: The national median average for this role is $99K USD, according to Ziprecruiter. Your range would depend on your background, experience and any intel can find on the average rate for the organization and market value.
8.	Are you open to working on a 24x7 shift schedule?	Our recommendation is to work whatever shift you can. If you cannot because of family obligations, then so be it. That being said, if you can work an overnight shift or weekend shift for 6 months or so, you could then move into a day shift or M-F shift. Example: I am open to working shifts other than a day shift. May I ask what the shift is for this position?
9.	Are you willing to relocate?	This is now a tricky question given what we've been through since 2020. If you have any inclination to move, say yes and see where it goes. If you are somewhat considering, say yes and when they ask you how long you will need to relocate, you can give a ballpark estimate of around 6 months. If you have no desire to relocate but hope that they have a remote availability, still say "yes" that it is a possibility. You can go through the phone interview and often find that they are trying to weed out candidates based on this question. If you get to the next step and they like you and trust that you are a good fit for the company, then they will be more flexible with revealing that the position is actually remotely available. Do not limit yourself and ruin your chance to show yourself before you have had another interview round.
10.	Walk me through your resume.	This is your time to shine. This is a question that you will need to practice considerably. The focus is not so much on what you have done in your past, but mostly on what you have done at CyberNow Labs. If you are coming from any field related to IT etc, then definitely say this in your explanation. If you are coming from other fields, please share this as well because there are many ways skills are transferrable. Do not get stuck on your roles, degrees, and dates related to your previous job and schooling (unless they elaborate or ask for more information specifically). List them off and then get to your current achievements at CNL. Be confident, SMILE, look at the interviewer. Tell them your certifications, describe your technical skills based on your toolset and how you use them. This question usually paves the way for the following questions about what you do daily and what tools you use.
11.	Walk me through your day-to-day work at CyberNow Labs.	At CyberNow Labs, I do Incident response based on the alerts given, review logs, write tickets based on my findings, and triage and inspect for phishing campaigns.
12.	What is your expected salary?	Note this is slightly different than question 7 (a range vs. a specific annual salary or contract rate). There is no avoiding answering. Definitely look into the average rate for the company and market value when applying and answering. Yearly salaries with benefits are different from contracting salaries by the hour. Shooting too high in a phone interview might limit your acceptance to continue, but remember that nothing is written in stone until you sign your contract.

Recruiter Phone Screen Questions

13.	Which security tools do you currently use? Give examples.	Be familiar with all the current tools by saying their names causally and knowing what they do. The best way is to use them, explore them, write tickets, and be able to use technical jargon correctly, even if it is only one or two sentences that you rely on during these calls. Choose one SIEM and one EDR.
14.	When are applying for any job that is marketed towards an MSSP, questions about customer service and communication skills are going to be asked.	How are your customer-facing skills? Is there anything in your previous job that you can use to correlate these two? Example: if you came from a people-facing environment, (teaching, business, politics), use this to your advantage when answering. Give short and simple examples if needed. Combine these and use situations to help you answer the question. If you come from a Sales background, give numbers or percentiles. You improved % much, you increased sales by% this much, etc. Use all of your assets to help bring in your value.
15.	What is the difference between blue, black, and white hats?	Each color signifies the different types of hackers: • White Hat - Use their skills for good • Black Hat - Malicious hackers • Gray Hat - fall between white and black. Do illegal activities but not always focused on malicious attacks • Red Hat - Kind of like gray hat however they are vigilantes. They seek out Black Hat hackers • Blue Hat - Penetration testers or they can also be hackers that act out of revenge • Green Hat - Newer hackers
16.	Why should we hire you instead of other candidates? What makes you better than others?	You want to sound confident but not arrogant. You need to make yourself stand out as a valuable addition to their team. Use your own adjectives to describe yourself in a way that shows benefits to their organization. Example: I cannot speak to the other candidates and what they bring to the equation, though I am sure they are good candidates. I can only speak about myself. I am the type of person that a team environment benefits from because I am a hard worker who takes pride in what I do. I am constantly looking to make myself better, while also helping the rest of the team and organization to get better as well. Having a successful career while enjoying what I do guides my daily attitude and has a tendency to rub off on others.
17.	Where do you see yourself in 5 years? 10 years?	Think about realistically where you will be in your career in 5 and 10 years. Think about this now so you can prepare and say where you truly think you will be. Example: In 5 years, I see myself with a few additional certifications with a lot more experience and knowledge as a Tier 2 Analyst. I would love to eventually move into a management role, so in 10 years, I could see myself applying my leadership skills in an official capacity with a great cybersecurity organization.

Behavioral Interview Questions

18.	Do you do anything outside of work to continue your cybersecurity learning?	Example: I do read a lot of cybersecurity news (daily SANS emails, Crowdstrike updates), listen to podcasts such as (CyberWire Daily, Darknet Diaries, or The Threatpost Podcast). I also have a small home lab that consists of a virtual environment where I can download malware and learn more about the IOC's, TTP's, and threat actors themselves. (Note: Pick a "favorite" threat actor group, and a malware/virus to be able to describe.)
19.	As a SOC analyst, what would you do if you found 1,000 alerts triggered at once?	Example: If I were working and I saw 1,000 alerts all at the same time, the first thing I would do is stay calm and analyze the situation like any other alert. I can use the playbook for guidance based on the type of alert, however, I would initially want to know what the alert is. Is this a repeat alert? Then I can begin to dive into the investigation. I would investigate as far as I could take it. The end goal being able to determine the nature of the alert. True positive, a true positive non-issue, or false positive. If I could determine the nature of the alert, then I would take the appropriate steps from there such as completing the ticket and closing out the alerts. If there needs to be an escalation, then I would take those steps to involve other members of the team. If it is a false positive alert, I would take the appropriate information and partner with the engineer so that we could see if this is an opportunity to tune these alerts out. Especially if it is a repeat alert. (Note: Make sure that you are not afraid to ask for help from a tier 2 or above. Working together and asking questions is a big part of your role, not a weakness.)
20.	Have you ever had a disagreement with a fellow employee? How did you handle it?	In this behavioral question, they are looking to see how you get along with people, and if you have had an issue with one, how you handled it. Make sure it is a positive interaction or at least a positive ending because of the way you handled it. Be specific if you can. If not, think of a possible specific situation and speak hypothetically but give information on how to resolve the issue. Example: I remember this guy I worked with Adam who would bend the truth when helping customers. We disagreed with what we could tell the customer in order to get a sale. I didn't think this was right and had a discussion with him about it. I listened to him talk about why he did it, he listened to me about why we shouldn't do that and we worked together to figure out a better way to work with the customers.
21.	If selected for the position, what would you hope to achieve in the first six months after being hired?	The answer to this combination of behavioral and technical interview questions depends on the role. A developer, for example, may hope to have developed a small project during that time, while a tech manager may want to have analyzed internal processes. A candidate's response will give the interviewer insights into their overall understanding of the position. If their goals and ambitions don't match the job description, this may not be the right position for them. Describing the desire to be familiar and have a good understanding of the team, the playbooks, how to use the tools effectively, and shadowing/learning from those that have more experience and working on a new certification or training that is in line with your job can be an effective way to answer the question.

Behavioral Interview Questions

22.	How do you manage your work-life balance?	With on-call duties and multiple pressing deadlines, some tech workers struggle with the always-on, workaholic culture of this field. While the hiring managers want dedicated team members, they also seek employees who know how to relax and take care of themselves. Burnout is a very real problem in IT, and top performers have good strategies in place to prevent that. Have a go-to answer as this is usually asked. Being able to know when to turn off the screen and not get too wrapped up in the cyber world is important and can show that you are a well-rounded individual.
23.	Can you tell me about a time when things didn't go the way you wanted at work, such as a project that failed or you were passed over for a promotion?	Everyone deals with professional setbacks at some point in their career. Speak to the interviewer about how you've handled and what you've learned from situations. The best employees are resilient, using setbacks as a springboard toward positive changes. Speak not only about the problem, but also what you did after the disappointment. Note: Do not complain about previous employers or the company.
24.	Have you worked on any projects or written any documentation?	Be honest. If you have, then talk about it and what you did to complete it. If you have not, then it's ok to say no. You could talk about creating documentation in another career previously, if you have a good example.
25.	What are some of the ways you have implemented security in your everyday life?	Examples of security in your life: • Online banking and other account access (2MFA) • Secure passwords, Password application (Keepass/Lastpass) • Don't click links you are not familiar with, be careful of strange emails and texts • Home wifi security (firewall, passwords), not using public wifi or using a VPN if necessary • Not allowing others to enter office buildings without their badge being swiped (from a previous company experience).
26.	Where do you see yourself in 5 years?	Think about this question before you enter an interview. Know realistically where you see yourself in 5 years. If you say, "Running the company" you might not be taken seriously. However, if your answer is based on realistic expectations such as, "I see myself in 5 years with having had successfully gotten my CySA+ and maybe GCIH certifications and working as an experienced Tier 2 Analyst."
27.	How do you prioritize your work?	Example: I like to keep a notebook right there with me to list what I need to work on and what I would like to work on. I list them in order of importance to the organization. This list may change throughout the day depending on what comes up, so it has to be a flexible list. As I complete the tasks, I check them off and move to the next. Time blocking is also a way to get work done in chunks. If you make sure to take a break every 50 minutes, even if it is just for 5 minutes, it helps. Since you are in front of a screen all the time for this job, you will be faced with these challenges, so having a way to go about it beforehand will lead to your answer being genuine. Not having your phone by you could also be a way to stay focused since constant interruptions and the dopamine boost can cause your work focus to suffer.

CYBERSECURITY ANALYST INTERVIEW GUIDE
TOP 100 QUESTIONS (& BEST ANSWERS)

Behavioral Interview Questions

28.	How would your last boss describe you?	Keep it positive and mention traits that your boss would mention that will benefit the new position you are interviewing for. Example: if you were to speak to my previous boss, I'm sure that he/she would state that I am a hard-working, respectful professional who works well with others and is successful in any activity I put my mind to.
29.	What frustrates you at work?	You can speak about the fact that you don't get very frustrated because you are an easy-going person who takes things in stride, or if you must, discuss something that is related to your strengths and the company's success. Example: I consider myself to be a dedicated hard worker that works during my time on the clock. My expectations of people are higher because my own values are set pretty high. I have been frustrated in the past with someone that didn't work as hard as I do, but I have learned to focus on myself and what I do and it has helped me to not get frustrated in those situations.
30.	How do you handle having to do the parts of the job which you don't even like?	If you have an example, you can talk about it. However, be sure to talk about how you overcame not liking that task or how you realized it was important so you did your best to do it well. Example: There are almost always small parts of any role that you may not like as much. However, they are a part of the process and important in some way. So, as much as one may not like those tasks, they are important and are a part of the job.
31.	Work can be stressful. What do you do to deal with the stress in your workplace?	Stress is inevitable, so the interviewer wants to see how you handle stress. You can talk about stress being a normal part of life and how you deal with it so that it doesn't impact your work. We are human and this is a universal feeling/emotion. This can be a good time to mention the ways you stay focused or use your prioritizing skills to manage your day. Example: Stress is a part of everyday life. It can be an overwhelming feeling for some people. I have found that breathing and thinking through the stress has worked for me. I like to just pause for a moment and let my mind settle into the actions that need to happen and then give myself the positive reinforcement I need to say "I can do this" or "I can handle this". Then move on!
32.	Tell me about a time you made a mistake and what you learned from it.	This question shows that you can grow and have grown from personal mistakes. We all make them but how we grow and learn from them is paramount. (*Do not spend 5 minutes talking about the details and give a whole story, get to the point, be concise).

Technical Interview Questions, Security+ Focused

33.	What is the CIA Triad? (Could be asked by a recruiter on initial contact)	The CIA Triad is the model used to guide security: • CONFIDENTIALITY prevents unauthorized disclosure of data. • INTEGRITY provides that the data hasn't changed. • AVAILABILITY indicates that data and services are available when needed.
34.	What are the port numbers for HTTP: 80, Https: 443, LDAP:389, LDAPS: 636, FTP:21, SFTP: 22, FTPS:990, SSH:22, Telnet:23, SMTP:25, POP3:110, IMAP:143, SNMP: 161, RDP: 3389, DNS: 53	HTTP: 80, HTTPS: 443, DNS: 53, RDP:3389, SSH:22, LDAP:389, LDAPS:636, FTP:21, SFTP:22, FTPS:990, Telnet:23, SMTP:25, POP3:110, IMAP:143, SNMP:161
35.	What can you tell me about TCP vs UDP traffic?	CP -Transmission Control Protocol/ UDP - User Datagram Protocol Most traffic on the internet is TCP. TCP is connection-oriented so it establishes a connection before transferring data. It guarantees delivery through the Acknowledgement Receipt of every packet. Used where you need guaranteed delivery like a website. Uses 3-way handshake. UDP is a lightweight protocol. It is not connection-oriented. Data is transferred blindly with no verification of receipt. Often used for applications such as video and voice where the receipt is not essential.
36.	Explain the three-way handshake.	Found in TCP connections. Step 1 - Originating system sends SYN flag - Indicates that it wants to start a connection. Step 2 - Destination system receives the SYN flag and replies with a SYN/ACK flag, which acknowledges receipt of the original request and asks to open a reciprocal connection. Step 3 - The original system receives the SYN/ACK flag and sends back an ACK to begin the 2-way connection.
37.	What happens when you visit google.com(URL)?	Here's a description in words for this site. When you type "google.com" into your browser, the first thing that happens is a Domain Name Server (DNS) matches "google.com" to an IP address. Then the browser sends an HTTP request to the server and the server sends back an HTTP response. The browser begins rendering the HTML on the page while also requesting any additional resources such as CSS, JavaScript, images, etc. Each subsequent request completes a request/response cycle and is rendered in turn by the browser.
38.	How does DNS work?	DOMAIN NAME SYSTEM It is the internet's equivalent of a phonebook. They maintain a directory of domain names and translate them to the IP Addresses.

39.	What can you tell me about the OSI model? TCP/IP Model?	The OSI Model describes the 7 LAYERS that computer systems use to communicate over a network. PHYSICAL layer represents the transmission of raw bits across a physical medium. Ex: Ethernet, Fiber Optics, WiFi DATA LINK layer allows the transfer of data in chunks called “frames” between adjacent nodes. Ex: Switches NETWORK layer allows the transfer of data frames in larger chunks called “packets”. Correct node is located using IP addresses. Ex: Routers, IP Addresses TR ANSPORT layer represents the protocols for sending and receiving packets across a network via ports. Ex: TCP, UDP, ICMP SESSION layer is used when opening, closing, and controlling sessions between application processes. PRESENTATION layer represents formatting and delivering data in a usable format for the application. Ex: JPEG, SSL, HTML APPLICATION layer is what the users see. Ex: Firefox, Outlook, Chrome The TCP/IP Model is very similar to the OSI Model APPLICATION - (Application, Presentation, Session) TRANSPORT - (Transport) INTERNET -(Network) NETWORK INTERFACE - (Data Link, Physical)
40.	What is the difference between a threat, a vulnerability, and a risk?	Risk - Potential for loss or damage when a threat exploits a vulnerability. Threat - Someone with the potential to cause harm to a system or an organization. Vulnerability - A weakness of an asset that can be exploited by one or more threat actors.
41.	What is the difference between symmetric and asymmetric encryption?	SYMMETRIC - uses the same key to encrypt and decrypt, it is faster, and it is used for bulk data transmission. ASYMMETRIC - uses different keys to encrypt and decrypt, it is slower, and commonly used in initial key sharing and then communication is done through Symmetric Encryption.

42.	What is the difference between Hash, encryption, and encoding?	All of these techniques are used for converting the format of data. Encoding transforms data into another format using a scheme that is publicly available so that it can easily be reversed. It does not require a key. Encryption transforms data into another format, and it is used for keeping the data secret. In Hashing technique, data is converted to a message digest or hash, which is usually a number generated from a string of text. Hashing is not reversible.
43.	Can you describe a salted hash?	SALT is RANDOM DATA added to the hashing process to enforce uniqueness. It prevents damage that a rainbow table or dictionary attack could do.
44.	What is the difference between HTTP and HTTPS?	HTTP uses port 80 and it transmits unencrypted data over the Internet. HTTPS uses port 443 and encrypts and transmits data over the internet (with either SSL or TLS) and is secure.
45.	What is the difference between Dynamic Malware Analysis and Static Malware Analysis?	The difference is whether you are observing the behavior or reporting what happened. Static is reporting what has been found where dynamic is reporting as the behavior is occurring. Static Malware Analysis is based on signatures such as hashes and metadata without executing the malware, whereas Dynamic Malware Analysis is based on monitoring how the malware behaves as it is executed in a sandbox.
46.	What is the difference between EDR and AV?	Anti-virus (AV) is limited in terms of capabilities and marketed for personal use cases, whereas Endpoint Detection and Response (EDR) tools are very powerful and exclusively marketed for enterprise environments. Anti-virus serves basic purposes like scanning, detecting, and removing malware. EDR tool, on the other hand, provides antivirus AND whitelisting, blacklisting, real-time monitoring, behavioral detections using AI.

CYBERSECURITY ANALYST INTERVIEW GUIDE
TOP 100 QUESTIONS (& BEST ANSWERS)

Technical Interview Questions, Security+ Focused

47.	What is TCP Header and what are the TCP Flags? Can you walk me through each flag?	TCP HEADER is the first 24 bytes of a TCP segment; it is used to track the state of communication between 2 endpoints. TCP FLAGS are used to indicate the state of the connection; SYN (SYNCHRONIZATION): for connection establishment ACK (ACKNOWLEDGEMENT): acknowledgment of packets received. FIN (FINISH): gracefully termination of the connection. RES (RESET): abruptly stop the connection. PSH (PUSH): immediately pushes out data rather than waiting for additional data to buffer. URG (URGENT): informs the receiving side that certain data with the URG flag should be prioritized.
48.	What are XSS and CSRF?	Cross-site scripting (XSS) is a security vulnerability in web applications. Cross-site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application.
49.	What is SQL Injection?	SQL (pronounced Sequel) Injection is a code injection used to attack data-driven applications, where malicious SQL statements are injected into an entry field for execution. Example: '1'='1'
50.	What are HIDS, HIPS, NIDS, and NIPS?	HIDS - Host Intrusion Detection System - runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network. HIPS - Host lotrusjon Preventjon System - software package which monitors a single host for suspicious activity by analyzing events occurring within that host. NIDS - Network Intrusion Detection System - detects hacking activities, denial of service attacks, and port scans on a host or network. NIPS - Network Intrusion Prevention System - continually monitors an organization's computer networks for abnormal traffic patterns, generating event logs, alerting system administrators to significant events, and stopping potential intrusions when possible.
51.	What is Virus, Trojan, Worm?	Virus - a computer program that replicates itself by modifying other computer programs and inserting code. Trojan - malicious code that looks legitimate but can take control of your computer. Designed to damage, disrupt, steal, or in general inflict some harmful action on your data or network. Worm - computer code that can copy itself from machine to machine. Can carry payloads to inflict damage.
52.	What is a honeypot?	A honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

53.	Difference between firewall and proxy?	Both work toward the goal of limiting or blocking connections to or from a network. They are both security tools to protect against threats. Firewalls monitor all access requests to a local network, disallow unauthorized access, works at the network(3) layer and filters IP packets, exist between private and public networks, and protect the internal network from malicious threats and attacks. Proxies mediates and connects a local computer with a server to retrieve data on behalf of the user, provides connections over the network, banning of websites can occur to eliminate visitation, may be in and out of the local network, anonymous use of the internet forgoing restrictions and it works on the application layer.
54.	What is the difference between authentication, authorization, and accounting?	Authentication - Validating credentials to verify identity. Authorization - gives you permission to access the resources such as information and files. Accounting - Record-keeping and tracking of user activities in the network.
55.	What is IP addressing? Name the IP address classes?	It is like a phone number for communication over the internet. IP addressing is a numerical label that is connected to a computer network that uses Internet Protocol for communication. There are Class A, B, C, D, & E as well as private IP addresses. Class A - Publicl.0.0.0 - 127.0.0.0 / Private 10.0.0.0 - 10.255.255.255 Class B - Public -128.x.x.x - 191.255.0.0 / Private 172.16.0.0 - 172.31.255.255 Class C - Public - 192.0.0.0 - 223.255.255.0 / Private - 192.168.0.0 - 192.168.255.255 Class D - 224.0.0.0 - 239.255.255.255 (Not available to hosts/Multi-casting IP's) Class E - 240.0.0.0 - 255.255.255.255 (Not available to public/Re-search only)
56.	What are the 4 risk responses that organizations might use to address business risk?	The 4 risk responses are: avoidance, transfer, mitigate, and accept. Avoidance is where you avoid risky behavior. Transfer is where you transfer to someone else. Mitigate is when you put security measures in place to mitigate the risk. Accept is where you accept the level of risk because of the low potential impact.

CYBERSECURITY ANALYST INTERVIEW GUIDE
TOP 100 QUESTIONS (& BEST ANSWERS)

Technical Interview Questions, Security Operations Center (SOC) Focused

57.	What are the basic responsibilities of a SOC team?	The SOC Team is responsible for implementing and managing security tools, investigating suspicious activities, containing and preventing them, reducing downtime, ensuring business continuity, planning security strategies, and maintaining successful auditing and compliance.
58.	What kind of alerts did you work on in your environment?	I would say that the most common alert types I see in our environment would be firewall denies, authentication failures, brute force attempts, connection to known malware sites, traffic from an untrusted network, and potential data loss.
59.	Pick one of them and tell me how you analyze & respond to it?	This needs to be an individual answer. The answer will come from working repeated alerts and getting familiar with them to the point of being very comfortable with walking someone through it. Pick an alert that you can easily walk an interviewer through with details.
60.	Walk me through the incident response process?	Incident Response steps are 1. Pre-incident preparation 2. Identification 3. Isolation(Containment) 4. Analysis 5. Reporting 6. Recovery and 7. Lessons Learned. Our ticketing system is designed to walk us through this process with each investigation.
61.	Name top 5 attacks from OWASP TopIO.	Remember that OWASP = Open Web Application Security Project, a non-profit organization that works to improve the security of software/website: owasp.org 1. Broken Access Control 2. Cryptographic Failures 3. Injection 4. Insecure Design 5. Security Misconfiguration
62.	How do you use the playbook in your SOC?	The playbook is designed to give us the step-by-step for each type of offense that we would work in our environment. When we have an offense, we open to the type of event in the playbook and follow the steps to ensure that we are accomplishing all items in the Incident Response Process.
63.	How would you explain phishing to a non-IT person?	Phishing emails are attempts to get an unsuspecting person to do something you want them to do such as download a malicious file or click a malicious website link. It really is like fishing in real life. You are trying to catch a fish, so you put on the bait and try to get them to bite.
64.	How do you determine whether an email is a phishing email or not?	There are signs that an email might be a phishing email when looking at the body. Poor spelling, bad grammar, and a sense of urgency in the body of the email. Attachments and links that look unusual can be a signal that the phishing email might be malicious. If you hover over a link in the email and the link doesn't match the destination that it tells you it would send you to, then that is suspicious. From an analyst's point of view, if there are failed SPF, DKIM, and DMARC, Reply to doesn't match sender email, any of the IP's in the hop present as malicious, these can all be signs of a malicious phishing email. When using tools such as Proofpoint, a lot of the determination of maliciousness is done for us. We just have to investigate and verify and provide context, as well as create the ticket to document the findings and suggest remediation steps.

65.	How do you investigate phishing emails?	The first step is to see what information is in the alert. I gather the items that are important to the investigation, such as Sender email address, Email Subject, Attachment name, URLs. I also look at how many emails were sent, how many were delivered, and if the attachment or URL was mitigated. With the URL, was the link re-written? With the attachment, was it quarantined? Was the email delivered with anything unmitigated? If it was, then I need to do an enterprise search and see if the URL was visited or the file was downloaded (if it is a malicious phishing attempt.) You can also perform triage in your EDR solutions to check to see the following events that happened after the site was connected to or document or .exe was open (or not opened). Then follow the appropriate steps to ensure the safety of the environment, (ie. request password expiry, isolation, or L2 escalation).
66.	What is The Cyber Kill Chain?	CYBER KILL CHAIN is a methodology for describing the phases of a cyber attack from early reconnaissance to the goal of data exfiltration. 1. RECONNAISSANCE: this is when the intruder selects a target, researches it, attempts to identify vulnerabilities. 2. WEAPONIZATION: is when an intruder creates remote access malware such as a virus or worm tailored towards vulnerabilities. 3. DELIVERY: is when an intruder transmits a weapon to the target. (via attachments, USB drives, websites) 4. EXPLOITATION: malware (weapon's) code triggers and takes action to exploit the vulnerabilities. 5. INSTALLATION: malware weapon installs access point (ex: backdoor) usable by the intruder. 6. COMMAND & CONTROL: malware weapon allows the intruder to target the network. 7. ACTIONS ON OBJECTIVE: intruder takes action to achieve their goals such as data exfiltration, data destruction, encryption for ransom.
67.	How familiar are you with NIST frameworks?	I know that the NIST framework or National Institute of Standards and Technology creates the guidelines for mitigating organizational cybersecurity risks. It helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. It is published by the US National Institute of Standards and Technology.

Technical Interview Questions, Security Operations Center (SOC) Focused

68.	What do you know about the Mitre Attack Framework?	The Mitre Attack Framework is used to understand security risks against known adversary behavior, plan for security improvement and provide clear and concise information to stakeholders. The Mitre Attack Framework reflects the phases of an adversary's lifecycle, the platforms they are known to attack, and the specific methods they use. When looking at the matrix, you can see that the attack progression is broken down into tactics and techniques. Tactics go across the top then there are techniques under each tactic. While investigating my alerts and potential incidents, I am able to look at the TTP and indicators of the Mitre Attack Framework to give myself a guide as to how and what is happening in the incident. If it is phishing with an attachment to a select group, I could use tactic - XYZ, 01-. Spear Phishing with attachment. When I am documenting my incident, I usually write these in my notes. (you do not have to memorize the TTP's just be able to understand the concept). When I hear about new threat actors or when I am looking online at new cybersecurity breaches, I read about the key Mitre Attack techniques, tactics, and procedures that they use so I can familiarize myself more with how to keep my SOC/Company safe from these risks. It is a guide for me to understand the way that threat actors think, as well as help me to increase my knowledge of things to watch out for.
69.	What sorts of anomalies (IOC) would you look for to identify a compromised system?	Indicators of Compromise (IOC's) help detect an intrusion or other malicious activities. IOC's can be shared and provide threat intelligence that can be shared. There are a lot of items one can look for in a compromised system such as the examples below: • Unusual Outbound Network Traffic • Anomalies in Privileged User Account Activity • Geographical Irregularities • Log-In Red Flags • Increases in Database Read Volume • HTML Response Sizes • Large Numbers of Requests for the Same File • Signs of DDoS Activity • Mismatched Port-Application Traffic • Suspicious Registry or System File Changes • Unusual DNS Requests • Unexpected Patching of Systems • Mobile Device Profile Changes • Bundles of Data in the Wrong Place • Web Traffic with Unhuman Behavior
70.	How would you handle a compromised endpoint?	I would always follow the playbook for the appropriate event type. Following the Incident response process to investigate and remediate the issue. Quick but thorough investigations are important to limit the scope and damage.

71.	How would you prevent a zero-day attack?	First, you want to update software applications as soon as patches are released. Implement the use of a web application firewall (WAF). Last, install an internet security suite that has anti-virus, sand boxing, default deny protection, and heuristic file behavioral analysis.
72.	What do you think/know about the Log4J attack?	Log4J was an attack that became known at the end of 2021. It was a zero-day dealing with a dynamic link library (DLL) associated with Java. Threat attackers could use a well-crafted HTTP header to bypass authentication and directly instruct a device to reach out to a remote domain or IP in order to download a malicious payload. Luckily our environment was not affected by the zero-day, however, we were able to see attempts to exploit this vulnerability. Alerts were created when there was an instance of the "jndi" string in an HTTP header.
73.	Have you ever had a breach where you had to get an attacker out of your environment and how did you handle it?	I have not had a situation like this because of the limited scope of my SOC environment, however, the first thing to do is to gather the information as best you can. Include tier 2 and 3 analysts and ensure that you are getting to the root cause of the breach and ensuring that the threat actor has not been able to create persistency in some form. This must be done before you block their IP etc. If the threat actor has already created a backdoor for example that you are unaware of and they know that you are on to them by blocking the IP they are using to communicate, then they can re-enter through their backdoor.
74.	Tell me about your experience with the EDR tools mentioned in your resume? (Crowdstrike & SentinelOne)	In our environment, we currently use (Crowdstrike/SentinelOne) as our EDR solution. We monitor the dashboard for malicious activity on the endpoints and investigate when there is an alert. We document our findings and take the recommended steps for remediation including containing or isolating the host if a successful compromise has occurred. A ticket is created in Jira if there is a need to reset a password, remove files or re-image a device as well as block IPs and domains.
75.	Walk me through your activities using a SIEM tool. (IBM QRadar & Splunk Enterprise Security)	Daily as a SOC Analyst, I monitor our SIEM tool (QRadar/Splunk ES). Logs from the devices and security tools in our environment feed into the SIEM in order to make monitoring more streamlined. When an offense event triggers, it is given a severity level and I work them in order of most severe to least severe ie. critical to low. The first thing I do is assign the offense to myself. Then Investigate looking at all the information provided and pivoting when necessary, I am writing my notes down for my report while I am doing all of this. Then I make a declaration about the offense and write an investigation ticket in our ticketing system (Resilient) containing all of the findings as well as supporting documentation. Once the investigation is completed, notation is done in the alert and it is closed.
76.	How do you keep your technology skills current?	Example: I have a Feedly RSS feed that I use to monitor current news articles centered around cyber security. You can select from hundreds of different news sources and they all feed right into the Feedly account. Makes it super convenient to stay up to date. I read these daily. I also receive threat intelligence reports from and follow podcasts such as the Threatpost Podcast, Cyberwire Daily, and Darknet Diaries.

CYBERSECURITY ANALYST INTERVIEW GUIDE
TOP 100 QUESTIONS (& BEST ANSWERS)

Technical Interview Questions, Security Operations Center (SOC) Focused

77.	What are some of the OSINT you use on a daily basis and what do you use them for?	Some of the OSINT tools I use are Virustotal, AbuseIPDB, IBM XForce Exchange, viewDNS.info, urlscan.io, and Central Ops for IP reputation, domain reputation, and DNS information. I also use sandbox tools such as Hybrid Analysis, Joe Sandbox, and Any Run. For APT and Attack progression, I use The Mitre Attack Framework and the OWASP.org top 10 can be helpful for the top 10 web application security issues.
78.	Walk me through your experience with Linux.	If you are not familiar with using Linux, then you need to be able to talk about what it is. Example: Linux is an open-source operating system. My experience is with Kali Linux and using it for my home lab to use its built-in security tools such as Metasploit, Running Wireshark, and just getting familiar with the Operating system to understand how it works so that I can identify things in my analyst position.
79.	What is Ransomware?	Ransomware is a type of malware that is designed to encrypt data and disable access to critical systems until a ransom is paid. It is an attack on a computer network where the attacker encrypts the devices and holds the company hostage, demanding a ransom in order to get access again or stop the release of the information the attacker got access to.
80.	How would you handle a ransomware attack?	I would follow my playback and investigation order. The incident response process outlined there will guide me. I would note the time, write down information for the ticket, any information I thought was necessary to the case, and then contact my L2 or senior manager within a certain amount of time.
81.	What logs do you review? (proxy, firewall, cloud?)	The logs that get reviewed the most are Firewall, IDS/IPS, proxy logs, DNS logs, windows event logs, and the logs from the EDR tools.
82.	Where do you get your security news from?	First, I use Feedly to pull the RSS feeds from many different sources. That being said, some of the news organizations I follow are Bleeping Computer, Threat Post, Krebs on Security, Kaspersky, and Trend Micro.
83.	What is dwell time?	Dwell time is the amount of time a threat actor is in the target system or network and remains undetected. For APT's, the dwell time is traditionally longer and has been known to be as long as 6 months or more. As of 2021, the dwell time continues to decline because of advances in cybersecurity.
84.	What is a PCAP?	PCAP file extension is mainly associated with Wireshark. It is the network traffic data in packets used for investigation. They can be used to analyze the network characteristics of certain data. PCAP is basically short for Packet Capture.
85.	What is penetration testing?	Also known as ethical hacking, where you test computer systems, networks, or web applications for security vulnerabilities that an attacker could exploit. The security issues can be in operating systems, services, application flaws, improper configurations, or risky behavior by the end-users. The goal is to test before an attacker can find the security vulnerabilities. There are 5 categories of Penetration Testing: Network Services, Web Applications, Client-Side, Wireless Networks, and Social Engineering.

86.	What is vulnerability testing?	Vulnerability testing looks for known vulnerabilities in the environment and reports those exposures so they can be addressed. Some examples of vulnerability scanning tools are Port Scanners, Network Enumerator, Vulnerability Scanner, Web Application Security Scanner, and a Computer Worm.
87.	What does a 404 error code mean? (200,300,400,500)	There are a lot of specific codes, however, the main categories are: 200 - Connection Success/ 300 - Redirection / 400 - Client Error / 500 - Server Error Most common are: 200 - Connection Success, 302 - Re-Direct, 400 - Bad Request, 404 - Not Found
88.	What is a man in the middle attack?	This is exactly as it sounds. It is where a threat actor has been able to successfully place themselves between a user and the destination device that they are communicating with. This allows them to be involved in the communication either just sniffing the information or somehow manipulating the responses or results, etc.
89.	What are DKIM, SPF, & DMARC?	DKIM - Domain Keys Identified Mail - Email authentication method designed to stop Email Spoofing by detecting forged sender email addresses. SPF - Sender Policy Framework - is an authentication protocol that allows senders to specify which IP addresses are authorized to send an email on behalf of a particular domain. DMARC - Domain-based Message Authentication Reporting and Conformance - is an email authentication protocol designed to give email domain owners the ability to protect their domain from unauthorized use, a.k.a. email spoofing.
90.	What is a false positive? What is a false negative? Which one is more dangerous (false positive or false negative)?	A false positive is where an alert triggers where there is no malicious activity. The false negative is where there is no alert and there should be. The false negative is much more dangerous because there isn't any indication through an alert when there should be.
91.	Tell me about the most challenging case you have been faced with?	This needs to be a personal casework experience. If there is or was a case that you had a hard time with but were able to work through it. Talking about what steps you took and how you worked to make sure that the investigation was completed using resources, determination, staying focused and calm, etc.
92.	You see a malicious file and see what appears to be meaningless writing in the cmd line. How would you check what this writing really means?	In a command line taken from an alert in the EDR security tool, you may come across an encoded string that carries out activities. You would want to use something like Cyberchef in order to input the encoded information and see what it is doing. It might be giving direction to connect to a malicious IP or domain in order to download a payload.
93.	How do you protect against Ransomware?	Ransomware attacks mostly come from visitation to malicious websites or interaction with malicious emails. Once this occurs, files are ultimately encrypted and data can be lost or stolen. Knowing this, you can protect against ransomware by refraining from visiting malicious websites, interacting with malicious emails, keeping anti-malware programs up to date, backup the data regularly, disabling macros for office applications, and installing the latest patches for installed software.

CYBERSECURITY ANALYST INTERVIEW GUIDE
TOP 100 QUESTIONS (& BEST ANSWERS)

Interview Tips!

First, Remember that you are an Analyst! (If you've graduated from our Academy.)

- You are working Incident Response on real network traffic in a self-contained SOC for CycbeNow Labs
- Be Calm, Confident, Positive, and Focused
- Research the company you are interviewing with
- Predict the job interview questions and prepare your answers
- Dress professionally for every interview
- Make a good first impression - Smile - Be Likable
- Don't be modest, sell yourself "I did this ..... I worked on that"
- Listen to the questions and ask yourself, "What are they wanting to know"
- Identify the question as a behavioral question or technical question
- Be specific in your answers
- Do not lie or make up stories - If you can not remember a specific example, give a hypothetical situation and how things should be to answer the question they are asking
- If you do not know an answer to a technical question, state what you know and understand relating to the topic, then discuss your ability to do additional research and learn it feeling confident about your ability to master the topic. (Same with a tool)
- Don't be afraid to ask the interviewer to repeat the question
- Have good questions prepared to ask at the end of your interview.