Triage Technical Interview

Technical Domain	Questions (interactive or not)	High level indicators	Intermediate indicators	Low level indicators
Authentication & Access Control	• What type of controls you can apply to authentication outside of MFA/2FA?			
Endpoint	• What endpoint detection products are you familiar with and what do they do?			
Perimeter	• How would you harden/protect a Web Server or Firewall			
Networking	1. Build a complex network (Interactive) 2. What happens when you type “google.com” into a brand new computer? 3. How would you troubleshoot a host that is unable to connect to the internet?			1. Small, home network environment. Unable to answer more advanced follow up questions
Security Fundamentals	1. Describe defense in depth (or layered security). What does that look like in the network you created earlier? 2. Walk through your thought process in examining an alert that appears malicious 3. Describe how you would investigate a malware infection or C&C traffic on a workstation in your environment? 4. How would you investigate a URL that a customer is saying is malicious?			
Cloud (IaaS/PaaS)	• What sort of behaviors would tell you that an EC2/VM got compromised?			
Public Key Infrastructure and Key Management	• What security recommendations would you give for an on-prem PKI environment? (AD Certificate Services). Why?			
Containerization & Orchestration				
Cloud (SaaS)	• What sort of behavior would tell you that an Office 365 account has been compromised?			
Risk & Compliance	1. How would you prioritize risks for a patch management program? 2. What strategies would you employ to get an organization through a compliance audit?	Good understanding of balancing business	High level understanding of the security functionality, with some	Basic understanding of the security functionality

	3. You run an external scan on the environment and determine port 80, 443, 445 and 3389 are all open to the internet. What are those ports? Do any concern you? What would you do about it?	requirements with security. 1. Able to balance the risk severity with the business function of the device as well as operational requirements such as business continuity, change management, etc	understanding of business implications. 1. Risk severity and what sort of device it is (what business function the device performs)	1. Based purely on CVSS scores and risk severity 2.
Complexity of Work	• What was one of your most difficult issues you've dealt with at work, and how did you solve it?			
Other (Python, documentation, etc)	• What is a skill you bring that you might consider a differentiator between you and other applicants?			
Move to technical assessment	1. Can you name two or three security vulnerabilities as per Open Web Application Security Project (OWASP)? 2. Can you name one or more phases of the Cyber Kill Chain? 3. Have you used MITRE before? Describe how you would MITRE ATT&CK could help an organization?			

Notes:

Trying to test for thinking and mentality in a specific area.

Format:

Interactive pieces (build a network, look at network traffic) during interview

Open ended technical questions for the interview

Todo: break questions and expectations by CSE/TSE level

Question pool - Draft

Technical Domain	Questions (interactive or not)		High level indicators	Intermediate indicators	Low level indicators
	What steps would you take to **enhance "event/auditing" visibility** to an organization?	CSE3/ CSE4			
	On your opinion, What is the biggest problem an organization **face with an in-house SIEM** ?	CSE4/ Tech Lead			
	Scenario Question: If multiple hosts flooding outbound traffic and impacting normal business activity, what would you do? (**More to the scenario:** Looks like streaming activity, hosts and IP addresses from different locations and subnets).	CSE2/3			
	Describe the **hardening measures** you've put on your home network.	CSE2/3			
	How do you harden a system?				
	How would you harden your work laptop if you needed it at Defcon? (**More to the scenario:** You have privileged access to all OS, MDM, GPO and all organization solutions)				
	What would do if you discovered an infected host?				
	Tell me how would you optimize and secure a subnet?				
	Tell me which is more secure and why? • Application access through HTTPS (443) without MFA, or • Application access through HTTP (80) with MFA enforced.	Critical thinking question. Both are not good. A few points to take • CIA triage. • 443, Good Integrity and Confidentiality, bad authorization • 80, Great Authorization, bad confidentiality and integrity			
	Tell me how would you analyze a suspicious email?				

	• "**Received**" lines show the address of the computer that received the email, as well as other computers' addresses that an email may have been transferred through. Unlike other email header elements, "**Received**:" lines can't be forged. (IP, SMTP Server, Time and TLS and more) • **Message-ID**: global unique identifier • DKIM signatures • From, To, Return-path and x-headers				
	Tell me how would you analyze a suspicious email link?				
	Tell me what are the biggest Active Directory vulnerabilities issues? Why				
	Explain how you would build a website that could secure communications between a client and a server and allow an authorized user to read the communications securely.	Layers • Well defined DNS record(s), IP addresses, GeoLocation inbound traffic to the web server. • Certificate (TLS version, cipher strength) • WAF • Database input sanitization • OWASP mitigations - Content Security Policy (CSP) • Harden server, web server, libraries and integrations. • MFA, vulnerability and patch management			
	Tell me how would you detect and mitigate a DDOS attack?				
	Tell me how would you secure a database? • Input sanitization • Parameterized queries				
	Tell me what **Content Network Delivery** (CND) tools do you knowledge or				

	experience with?				
	Tell me If you were left alone in office with access to a computer, how would you exploit it?				
	What does Zero Trust mean?				

	Tell me how would you measure the state of security of a system?
	• A few examples:
	  ◦ Mapping threats to current configuration
	  ◦ Security scorecard
	  ◦ Risk management
	  ◦ Maturity Model
	  ◦ Diagnostic methods				

	Explain the difference between TCP and UDP.				

Old Questions:

	Questions	Notes
Authentication (Active Directory, SSO, MFA, IAM, PAM)		
Endpoint (AWN Agent, EDR, EPP, AV, MDM)	(basic) What's the difference between AV and Endpoint Detection? What are the implications of applying MDM solutions to non-corporate owned devices?	
Perimeter (Suricata, Firewall, IDS, IPS, UTM, NTA)		
Networking (DNS, DHCP, WAF, Web Gateway, Proxy, Secure Email Gateway, Mail Server, Router, Switch, WAP, Internal Flow)	How would you design a commercial sized corporate network while keeping security in mind? What happens when a brand new computer opens a web browser and goes to www.google.com? What are some of the positives and negatives of having all web traffic route through a proxy?	Keep in mind how complex the environment they design. Do they include a DMZ? What's in the DMZ? Do they have network segregation?

IaaS/Containers (AWS, Azure, GCP, Kubernetes)	Can you tell me about the main differences between AWS and Azure? When would you use one over the other?	
SaaS (O365, G Suite, Box, Salesforce, Workday, CASB)	What sort of behaviour would tell you that an Office 365 account has been compromised?	
Risk (Vuln mgmt, BCP, DRP, IR)	You run an external scan on the environment and determine port 80, 443, 445 and 3389 are all open to the internet. What are those ports? Do any concern you? What would you do about it?	If the answer is: Close the ports: “Your customer says they need access to that machine remotely.” Set up a VPN: “What else can you do aside from VPN?” “What are some potential limitations?” Set up an ACL: “What else can you do aside from ACL?” “Is ACL best practice?” “What are some potential limitations?” If they show no concern for port 80: “What kind of traffic *would* be concerning to see over port 80?”
Soft Skills General		
Soft Skills Customer Focused		
Soft Skills Sensitivity		
Soft Skills Influencing		
Internal Systems and Tools		