CYBERSECURITY INTERVIEW QUESTIONS (EDR)

VAISHALI SHISHODIA

CYBERSECURITY INTERVIEW QUESTIONS ON ENDPOINT DETECTION AND RESPONSE

1. Endpoints & Antivirus:

a. What is an endpoint, and why is endpoint security important in an organization?

An endpoint is any device that connects to the network, such as computers, servers, mobile devices, and IoT devices. Endpoint security is crucial because these devices often serve as entry points for cybercriminals. A compromise of an endpoint can lead to breaches in the organization's internal network, so securing these endpoints is essential for overall network security.

b. Can you explain how traditional antivirus software detects and prevents threats?

Traditional antivirus software detects and prevents threats using signature-based detection, where known malware patterns are compared to files on a device. If a match is found, the antivirus will either quarantine or remove the infected file. Some antivirus programs also use heuristics to identify suspicious behavior or code that may not yet be recognized by their signatures.

2. Next-Generation Antivirus (NGAV):

a. How does NGAV differ from traditional antivirus solutions?

NGAV goes beyond traditional signature-based detection by incorporating techniques like machine learning, behavior analysis, and heuristics to detect previously unknown or zero-day threats. It can analyze patterns and behaviors of files or processes rather than relying solely on known signatures, making it more effective against sophisticated attacks.

b. What are some common techniques NGAV uses to detect threats (e.g., behavioral analytics, heuristics)?

NGAV typically uses:

- **Behavioral Analytics:** Analyzes actions and behaviors of programs to spot malicious activity.
- **Heuristics:** Identifies suspicious code or patterns that resemble known threats, even if they are not exact matches.
- **Machine Learning:** Uses algorithms to identify new threats by analyzing vast amounts of data to detect anomalies.

3. Endpoint Detection and Response (EDR):

a. What are the key functionalities of an EDR system?

EDR systems continuously monitor endpoints for suspicious activity. Key functionalities include:

- Real-time monitoring and detection of threats.
- Automated response capabilities, such as isolating compromised devices.
- Threat hunting tools to proactively search for hidden threats.
- Incident investigation and analysis by providing detailed logs of endpoint activities.

b. How does EDR complement antivirus or NGAV solutions in an organization?

EDR provides deeper insight into endpoint activities and can detect complex, evolving threats that may evade traditional antivirus or NGAV. While antivirus/NGAV detects known threats, EDR helps respond to incidents, providing visibility into a threat's progression and offering advanced tools for investigation and remediation.

4. SIEM vs. EDR:

a. What is a SIEM solution, and what are its primary functions?

A SIEM (Security Information and Event Management) solution collects and analyzes log data from various sources, such as servers, network devices, and security appliances, to identify potential security threats. SIEM is used for centralized monitoring, real-time alerts, and compliance reporting.

b. In your view, what are the main differences between SIEM and EDR?

While both SIEM and EDR focus on detecting threats, they operate differently:

- **SIEM:** Aggregates and correlates log data from across the network to detect broader security issues.
- **EDR:** Focuses on endpoints and provides detailed visibility into the behavior and activities of individual devices, offering advanced threat detection and response capabilities.

5. Integration of SIEM and EDR:

a. How can integrating SIEM with EDR enhance an organization’s overall security posture?

Integrating SIEM and EDR improves an organization's ability to detect, investigate, and respond to threats in real-time. The SIEM aggregates data from various sources, including EDR, and correlates this information to provide a more comprehensive view of the organization's security posture. This helps in identifying sophisticated threats and reducing the response time to incidents.

b. Can you provide a simple scenario where the combination of SIEM and EDR might help in detecting and mitigating a security incident?

Consider an attack where a user clicks on a malicious link. The EDR detects unusual activity (e.g., file modification or suspicious behavior on the endpoint) and triggers an alert. The SIEM collects log data from other sources, such as network traffic, and correlates the activity with other known indicators of compromise (IOCs). This integration helps to quickly identify the attack's origin and scope, enabling faster remediation and containment.

---

1. Advanced Endpoint Security:

a. How would you approach managing and securing endpoints in a diverse environment (multiple OS, remote work scenarios)?

In a diverse environment, it’s essential to implement a solution that can handle various operating systems (e.g., Windows, macOS, Linux) and different user environments. Using cross-platform endpoint security solutions and ensuring remote endpoints have consistent security policies (like VPN, multi-factor authentication, and encryption) are key. Additionally, monitoring tools should adapt to the unique needs of each operating system and user scenario.

b. What challenges have you faced with endpoint security, and how did you overcome them?

One common challenge is ensuring consistent security across various device types and operating systems. This can be overcome by using endpoint management platforms that support multiple OS types and enforcing a unified security policy for all devices. Another challenge is balancing security with user productivity, which can be mitigated through user education, streamlined security tools, and automated threat response.

2. Deep Dive into NGAV:

a. Can you detail how NGAV solutions leverage machine learning or behavior analysis to detect sophisticated threats?

NGAV solutions often use machine learning to analyze large datasets for patterns or anomalies. This allows NGAV to recognize new threats based on behavior rather than known signatures. For instance, a machine-learning model may identify a previously unknown malware variant by analyzing the sequence of actions it performs on an endpoint, such as accessing sensitive files, encrypting data, or communicating with a command-and-control server.

b. Describe an incident where NGAV played a critical role in threat detection or prevention.

In one instance, NGAV detected a zero-day exploit targeting a vulnerability in a widely used application. While traditional antivirus systems failed to recognize the threat, NGAV identified the unusual behavior pattern and quarantined the file before it could execute any malicious actions, preventing a potential data breach.

3. In-Depth EDR Operations:

a. Walk us through your process when an alert is triggered by an EDR system. How do you validate and respond to such alerts?

When an EDR alert is triggered, the first step is to validate the alert by checking the affected endpoint's recent activities. This includes analyzing event logs, reviewing the timeline of suspicious activity, and determining if there's a known malicious signature or behavior. If validated, the next step is to contain the threat by isolating the endpoint and starting the remediation process (e.g., terminating malicious processes, restoring from backups).

b. Share an example of a complex incident you managed using EDR data. What were the key indicators that helped you identify the threat?

In a recent incident, the EDR system alerted us to unusual file modification behavior on a critical server. The key indicators included:

- A rapid increase in file creation and deletion.
- An attempt to encrypt files with an unknown process.
- Communication with an external IP address.

By analyzing these indicators, we identified ransomware activity, isolated the infected machine, and stopped the attack before it could spread further.

4. SIEM vs. EDR – Detailed Comparison:

a. How do you prioritize alerts from SIEM and EDR systems, and what criteria do you use to decide if an alert needs escalation?

When prioritizing alerts, the severity and context of the threat are critical. SIEM alerts are often prioritized based on risk, compliance impact, and historical correlation, while EDR alerts are prioritized by the potential impact on endpoints and the network. An alert requiring escalation typically involves a high-severity threat, such as lateral movement or a confirmed compromise of critical systems.

b. What are the strengths and limitations of SIEM compared to EDR in detecting advanced persistent threats?

- **SIEM:** Strong in correlation and providing a holistic view of the network. However, it might struggle with real-time detection and detailed endpoint data.
- **EDR:** Offers granular, real-time monitoring of endpoints but may not provide as broad a network view, making it harder to detect sophisticated, multi-stage attacks.

5. Combining SIEM and EDR:

a. Can you describe the integration process between SIEM and EDR in an enterprise environment?

The integration typically involves configuring the SIEM to receive and correlate data from EDR tools. This includes endpoint logs, alerts, and threat intelligence. The process involves setting up data pipelines and ensuring the SIEM can contextualize the endpoint data in the broader network environment, allowing for real-time detection, alerting, and incident response.

b. What are the common challenges when integrating these two systems, and how have you addressed them in your previous roles?

Challenges include ensuring proper data normalization, handling large volumes of endpoint data, and ensuring the systems work together seamlessly. In previous roles, we addressed these challenges by establishing clear data formats and ensuring both systems were configured to share critical threat intelligence in real time. We also tested and fine-tuned the integration to reduce false positives.

c. Provide an example where the combination of SIEM and EDR data led to actionable insights and improved incident response.

In a previous case, SIEM aggregated data from firewalls, network devices, and EDR systems. When an EDR alert showed unusual activity on a remote laptop, the SIEM correlated it with network traffic and identified a botnet communication pattern. By integrating the data, we quickly contained the laptop, blocked the C2 server, and conducted a full investigation across other endpoints.
