Palo Alto
ENDPOINT PROTECTION
INTERVIEW QUESTIONS GUIDE
One Step Closer Towards Your Dream Job...
A Security Operations Center, or SOC, is a physical room or area in an organization's office where cybersecurity analysts work to monitor enterprise systems; defend against security breaches; and identify, investigate and mitigate cybersecurity threats. SOCs were created to facilitate collaboration among security personnel. They streamline the security incident handling process as well as help analysts triage and resolve security incidents more efficiently and effectively.
Security incident handling requires several key functions, which security operations teams commonly deliver using a tiered structure that accounts for the experience levels of their analysts:

**Tier 1 - Triage:** This is where security analysts typically spend most of their time. Tier 1 analysts are typically the least experienced analysts, and their primary function is to monitor event logs for suspicious activity. When they feel something needs further investigation, they gather as much information as they can and escalate the incident to Tier 2.

**Tier 2 - Investigation:** Tier 2 analysts dig deeper into suspicious activity to determine the nature of a threat and the extent to which it has penetrated the infrastructure. These analysts then coordinate a response to remediate the issue. This is a higher-impact activity that generally requires more experienced analysts.

**Tier 3 - Threat Hunting:** The most experienced analysts support complex incident response and spend any remaining time looking through forensic and telemetry data for threats that detection software may not have identified as suspicious. The average company spends the least time on threat hunting activities as Tier 1 and Tier 2 consume so many analyst resources.

Q2. WHAT DOES A SOC DO?
Q3. HOW IS A SOC STRUCTURED?

For most organizations, cybersecurity has evolved into a major priority from its roots as a part-time function of the IT team. Some security operations teams still function as part of IT, whereas others are separated into their own organization. SOCs may operate:

1) As part of an infrastructure and operations team
2) As part of the security group
3) As part of the network operations center, or NOC
4) Directly under the CIO or CISO
5) As an outsourced function (wholly or in part)
INDIA'S MOST TRUSTED NETWORKING TRAINING COMPANY
Q4. WHAT TOOLS ARE USED IN SOC?

SOCs use a range of tools for prevention, event logging, automation, detection, investigation, orchestration and response. Many SOC teams have multiple sets of siloed tools for different parts of their infrastructure. Research by analyst firms such as Ovum and ESG have found that the majority of enterprises use more than 25 separate tools in their SOCs.

XDR is a new class of detection and response tool that integrates as well as correlates data from the endpoint, network and cloud. XDR replaces several of the key tools security operations teams rely on and is designed to increase security visibility, efficiency and efficacy.
Q5. WHAT IS XDR?

XDR is an alternative to traditional reactive approaches that provide only layered visibility into attacks, such as endpoint detection and response, or EDR; network traffic analysis, or NTA; and security information and event management, or SIEM. Layered visibility provides important information, but can also lead to problems, including:

- **Too many alerts that are incomplete and lack context.** EDR detects only 26 percent of initial vectors of attack,1 and due to the high volume of security alerts, 54 percent of security professionals ignore alerts that should be investigated.
- **Time-consuming, complex investigations that require specialized expertise.** With EDR, the mean time to identify a breach has increased to 197 days,3 and the mean time to contain a breach has increased to 69 days.
- **Technology-focused tools rather than user- or business-focused protection.** EDR focuses on technology gaps rather than the operational needs of users and organizations. With more than 40 tools used in an average Security Operations Center,4 23 percent of security teams spend time maintaining and managing security tools rather than performing security investigations.

**With XDR, security teams can:**
- Identify hidden, stealthy and sophisticated threats proactively and quickly
- Track threats across any source or location within the organization
- Increase the productivity of the people operating the technology
- Get more out of their security investments
- Conclude investigations more efficiently

From a business perspective, XDR enables organizations to prevent successful cyberattacks and, simplify and strengthen security processes.
To prevent security breaches, organizations must protect themselves from known and unknown cyberthreats, as well as the failures of traditional antivirus solutions. This means they must focus on prevention. Prevention is the only effective, scalable and sustainable way of reducing the frequency and impact of cyber breaches. So, what should endpoint security do to be able to effectively and comprehensively protect systems, users and endpoints? Below are the 10 requirements:

1. Pre-emptively block known and unknown threats
2. Have no negative impact on user productivity
3. Turn threat intelligence into prevention automatically
4. Protect all applications
5. Don't let security impact system performance
6. Keep legacy systems secure
7. Be enterprise-ready
8. Provide independent verification for industry compliance requirements
9. Provide independent verification as an antivirus replacement
10. Receive recognition from a top-tier industry analyst and/or research firm

Want to read about each point above in detail? Click on the link below:
https://www.paloaltonetworks.com/cyberpedia/10-requirements-for-securing-endpoints
GET TRAINED BY CERTIFIED AND WORLD CLASS TRAINERS

Baldev Singh
CCIE SECURITY #37094

Saurabh Yadav
Triple CCIE (R&S, Sec, SP) #46962

Sudhanshu Bhat
CCIE VOICE #41212

Surendra Singh
CCIE R&S #60346
Zero Trust is an increasingly accepted and celebrated network architecture security model. The phrase “never trust, always verify” rings a familiar tune for those focused on securing networks. Zero Trust focuses on the principle that an organization should not trust anything inside or outside its perimeter and that everything trying to connect to the network should be verified before access is granted.

Accomplishing a Zero Trust architecture requires network segmentation and granular enforcement based on user, data and location. All traffic must be logged and inspected at various inspection points that identify and permit traffic based on established rules. This maintains least-privileged access and strict access control that gives you the network visibility and context necessary to limit lateral movement and identify attacks from within your network.

Four criteria must be met to extend Zero Trust to the endpoint:

1. Protect Endpoints With Multiple Layers of Security
2. Integration With Network Security
3. Managing Multiple Kinds of Endpoints
4. Layer 2–7 Access Control
Palo Alto Networks® Next-Generation Security Platform is designed to enable and align to a Zero Trust architecture.

A key component of Palo Alto Networks Next-Generation Security Platform is Traps™ advanced endpoint protection, which employs multiple methods of protection at critical stages of the attack lifecycle to prevent known and unknown malware, exploits and ransomware, as well as zero-day threats. Traps performs local analysis to identify malicious and benign files based on file property classification and previously known verdicts.

On top of local analysis, Traps integrates with WildFire® cloud-based threat analysis service. On its own, WildFire performs dynamic and static analysis, machine learning and bare metal analysis to identify even the most evasive threats. As part of the platform, WildFire enables Traps and the next-generation firewalls to become sensors and enforcement points for your network and endpoints.

Palo Alto Networks next-generation firewalls inspect all traffic, including applications, threats and content – even if it's encrypted – and tie that traffic to the user. The resulting visibility and data help security policy align with your organization's unique needs and initiatives. Like Traps, the next-generation firewall works with WildFire to protect against known and unknown threats. When WildFire identifies a new threat anywhere, it automatically creates and disseminates updated protections throughout the platform and to other members of the WildFire community to support a coordinated security infrastructure. These updates include threats newly identified by Traps for more comprehensive and effective protection across the architecture.
Tying the policies from your network to your endpoints is GlobalProtect™ network security for endpoints, which extends your security policy to remote networks and mobile users. GlobalProtect inspects traffic using next-generation firewalls for full visibility of all network traffic, applications, ports and protocols. This visibility allows the seamless enforcement of security policy on endpoints, wherever the user is located. GlobalProtect provides user information to power User-ID™ technology and integrates with MFA protections in the firewall to prevent attackers from moving laterally using stolen credentials.
Cisco is bridging networking and security together like no other vendor. With Cisco SD-WAN we provide highly effective and scalable security that is easy to manage, deploy, and maintain, empowering businesses to adopt the latest cloud services with Endpoint security describes the tools, products and techniques designed to protect users’ devices – such as desktop computers, laptops, smartphones and tablets – and ensure the security of individual access points to an organization’s network and sensitive data. The number of vulnerable entry points continues to grow as remote and mobile workers as well as bring-your-own-device policies become more commonplace, extending the protection perimeter. Any organization must ensure all internet-enabled devices with access to its internal data are protected against cyberattacks.

“Endpoint security” is often used interchangeably with “Endpoint Protection Platform,” or EPP, a term coined by Gartner. These platforms sit on endpoint devices and secure them against cyberattacks using a comprehensive approach to combat sophisticated malware. EPPs use multiple techniques for prevention, including static analysis to evaluate potential malware based on file inspection, heuristics rules to block exploits, and behavioral analysis to evaluate file maliciousness based on the functions they perform.confidence.

Endpoint detection and response, or EDR, tools have emerged as a complement to EPP tools, allowing security teams to investigate and mitigate threats their prevention tools may have missed. An endpoint security toolkit may also include technologies such as endpoint management (which includes asset, vulnerability, patch and mobile device management), encryption, data loss prevention, and identity and access management. These tools can be used alone or bundled with other EPP products for more comprehensive protection.
The best EPP offerings tend to be cloud-managed so endpoint activity can be monitored continuously and issues can be resolved automatically, regardless of the network to which the endpoint device is connected.

**Key capabilities of an EPP:**

- Blocking of known malware and viruses based on signatures, hashes or other such methodologies.
- Blocking of unknown malware based on static file analysis, emulation, behaviors and techniques.
- No dependency on signatures as sole method for malware detection.
- Actions powered by threat intelligence. Anti-exploit and anti-ransomware protection.
- Effective management console (a poor management console should not create the need for EDR).
- Cloud-based sandboxing for deep inspection and second-opinion analysis.
- Lightweight agent to minimize performance impact. Single agent for both EPP and EDR.
- Hardening, such as application control, or another feature that reduces the attack surface.
- Authentication enhancements such activity monitoring (behavioral biometrics).
WORLD CLASS INFRASTRUCTURE
In a SaaS model—where a company's applications and data reside on third-party infrastructure, and the company's employees can access those apps anywhere, from any device—taking a traditional approach to security is not enough.

Endpoint detection and response, or EDR, refers to a category of tools used to detect and investigate threats on endpoint devices. EDR tools typically provide detection, analysis, investigation and response capabilities.

EDR tools monitor events generated by endpoint agents to look for suspicious activity, and alerts EDR tools create help security operations analysts identify, investigate and remediate issues. EDR tools also collect telemetry data on suspicious activity and may enrich that data with other contextual information from correlated events. Through these functions, EDR is instrumental in shortening response times for incident response teams.

EDR has become a critical component of the endpoint security toolkit as endpoints have become more vulnerable targets for cyberattackers. Trends such as the internet of things and the increase in mobile and remote workers have made endpoints popular entry points for cybercriminals to launch sophisticated attacks on individuals or organizations.

Q10. WHAT IS AN EDR PLATFORM?
The key capabilities of EDR include:

- Aggregation of endpoint data.
- Malware analysis.
- Behavioral analysis – the ability to connect a chain of seemingly benign events to uncover suspicious behavior.
- Data correlation/enrichment.
- Correlation of related alerts into incidents.
- Prioritization based on the confidence and severity of incidents.
- Investigation tools that provide an alert management workflow, integrated with ticketing systems to enable incidents to be assigned, transferred, annotated and resolved.
- Click-down attack chain visualization tools to allow investigators to pivot.
- Querying activity across multiple cybersecurity tools, including messaging, web, endpoint and network.
- Automated, integrated analysis with a sandbox.
- Remediation, including network isolation, file quarantine, file removal, re-imaging, process killing and behavior blocking.
- Automated response/remediation workflows based on policies or predefined playbooks.
Antivirus scanning struggles to protect against today's threats - relying on frequent updates, identifying only known threats, and impacts system performance.

Antivirus has undoubtedly been the default solution for protecting endpoints for decades. Most antivirus solutions will scan the endpoint, cross-referencing files against a signature database of known threats. While adequate for identifying known threats, scanning technology cannot keep up with the advanced threats targeting endpoints today. Below are the four primary reasons why scanning shouldn't be your first line of defense when securing endpoints.

1. Reliance on Signature Database
2. Identifies only Known Threats
3. Performance Impact
4. Files at Rest not seen as Threats

To read up more in detail about the above 4 points, click on the link below:
Wrong endpoint security solution can leave your endpoints vulnerable to threats and undo the work that has gone into securing the network.

With network security, no single solution will protect against the variety of threats that organizations face. For more comprehensive protection, a combination of hardware and software provides multiple layers of security to defend the network against various threats. The time, cost and manpower required to carefully select, implement and maintain these tools is a huge investment for any organization. However, those within the network environment will not always be inside the perimeter, and the network protection capabilities will not always apply to them. If endpoints are not protected with the right security solution products, these individuals could bypass the perimeter security and introduce outside threats into the environment. The wrong endpoint security product can undo all of the work that has been done to secure the network.

Below are the five things your endpoint should do to prevent a negative impact on your network security posture:

1. Integrate Threat Intelligence natively
2. Protect against known and unknown threats
3. Be automated
4. Deliver persistent protection
5. Provide full visibility into activity on the network, endpoint and cloud

To read up more in detail about the above 5 points, click on the link below:
SHAPING CAREER
EMPOWERING FUTURE
An effective endpoint protection solution should deliver on 3 core security capabilities: performance of intended function, persistence, and flexibility.

Organizations should select security products that provide superior value in terms of both monetary cost and their security effectiveness. This effectiveness is measured by the technology’s ability to, at a minimum, deliver on these three core capabilities:

1. Performance of Intended Function
2. Inherent Persistence
3. Flexibility

To read up more in detail about the above 3 points, click on the link below:
https://www.paloaltonetworks.com/cyberpedia/3-ways-to-measure-endpoint-security-effectiveness
**Q14. WHAT IS AN END POINT?**

An endpoint is a remote computing device that communicates back and forth with a network to which it is connected.

Examples of endpoints include: Desktops, Laptops, Smartphones, Tablets, Servers, Workstations, etc.

Endpoints represent key vulnerable points of entry for cybercriminals. Endpoints are where attackers execute code and exploit vulnerabilities, and where there are assets to be encrypted, exfiltrated or leveraged. With organizational workforces becoming more mobile and users connecting to internal resources from off-premise endpoints all over the world, endpoints are increasingly susceptible to cyberattacks. Objectives for targeting endpoints include, but are not limited to:

- Take control of the device and use in a botnet to execute a DoS attack
- Use the endpoint as an entry point into an organization to access high-value assets and information
- Access assets on the endpoint to exfiltrate or hold hostage, either for ransom or purely for disruption

For several decades, organizations have heavily relied on antivirus as a means to secure endpoints. However, traditional antivirus can no longer protect against today’s modern threats. An advanced endpoint security solution should prevent known and unknown malware and exploits; incorporate automation to alleviate security team workloads; and protect and enable users without impacting system performance.
Despite attempts to pivot from outdated security methodologies, traditional antivirus (AV) continues to fail to prevent security breaches on endpoints, as evidenced by the rise in security breaches worldwide. Moreover, AV requires layers of products, saddling organizations with hidden costs that are often intangible, difficult to quantify or go unquestioned. Organizations should replace traditional AV with more advanced technologies that provide superior endpoint protection while complementing and easily integrating with a security platform for enhanced security.

**The Costs of Legacy Antivirus**

The effectiveness of signature-based file scanning has diminished as operating systems, networks and applications have evolved. Today, there are simply too many variations of new and unknown threats for a signature-based approach to identify and block them in a timely fashion. However, AV vendors still rely on traditional techniques and have only made incremental improvements in their malware coverage, while requiring multiple additional products to try to keep up. The additional products demand more maintenance, upkeep costs and burdens on staff. As a result, the costs of operating an AV system are growing.

**Modern Endpoint Protection**

Fortunately, superior technologies have emerged that eliminate the need for traditional AV. Seek an advanced security technology for endpoint protection that:

- Recognizes prevention is the only effective, scalable and sustainable way to reduce the frequency and impact of cyber breaches.
- Prevents known and unknown malware and zero-day exploits from subverting legitimate applications.
- Automatically and natively integrates with a security platform and leverages global threat intelligence. Blocks exploits and malware, regardless of a system’s online status, network connectivity or physical location. Is transparent to users and makes minimal demands on memory, bandwidth and CPU resources.
HELPING STUDENTS BECOME CERTIFIED
Q16. WHAT IS PALO ALTO NETWORKS TRAP?

Organizations can now get complete endpoint protection that meets all the above criteria – without the hidden costs and administration hassles of traditional antivirus solutions.

Palo Alto Networks Traps Advanced Endpoint Protection provides a multi-method approach to exploit prevention that combines several layers of protection to block exploit techniques and increase malware detection accuracy – without relying on virus signatures or resource-taxing scanning. Traps submits unknown files to Palo Alto Networks WildFire® threat analysis service, which continually analyzes global threat intelligence to identify and automatically prevent malware previously seen elsewhere.
Looking for Networking Training?

Join our CCNA, CCNP, CCIE, F5, Checkpoint, Palo Alto & Fortinet Certification Courses

Click here to Sign Up for a Free Demo Session

REGISTER FOR FREE DEMO