Gen NORTON CYBERSECURITY QUESTIONS

Focus: Endpoint Security, Malware, Threat Detection, Logs, SOC Basics, Windows Security, EDR, Behavioural Analysis.

Level EASY LEVEL

Basics of Malware, OS Security, General Security Knowledge

1. What is malware? Give two examples.
2. What is the difference between a virus and a worm?
3. What is a trojan?
4. What is ransomware?
5. What is a “payload” in malware?
6. What is the difference between *encryption* and *hashing*?
7. What is a hash? Why do we compare hashes?
8. What is the purpose of a firewall?
9. What is an IoC (Indicator of Compromise)?
10. Define: Threat, Vulnerability, Risk.
11. What is phishing?
12. What is the use of a quarantine folder?
13. What is the difference between **signature-based** and **behaviour-based** detection?
14. What is the purpose of the Event Viewer in Windows?
15. What is the difference between safe mode and normal boot?

Level MEDIUM LEVEL

Endpoint detection, threat identification, logs, Windows internals

16. A user reports a popup “Threat Blocked by Norton.” What steps will you take?
17. Explain how you identify a malicious EXE in Task Manager.
18. What is process injection?
19. How can a trojan maintain persistence in Windows?
20. What is the Windows Registry? Why is it important for malware analysis?
21. What is the difference between **EDR** and **Antivirus**?
22. How does Norton (or any EDR) detect suspicious behaviour?
23. What is heuristic detection?
24. What is a sandbox?
25. What is a PUP or PUA? (Potentially unwanted programs)
26. What is the difference between whitelist and blacklist?
27. Explain what a “false positive” means in threat detection.
28. Why do attackers use PowerShell-based malware?
29. Explain DLL hijacking.
30. A suspicious process is running from **Temp** folder. What will you check?
31. How do you inspect startup programs in Windows?
32. A system is slow after boot. How will you troubleshoot?
33. How do you check network connections used by a suspicious process?

34. Explain lateral movement in attacks.
35. What does it mean if multiple endpoints trigger the same malware alert?

Level HARD LEVEL

Norton-style deep scenarios, log analysis, endpoint forensics

Level 36. Scenario – Unknown EXE Running

A process named **"svhost32.exe"** is running from:

C:\Users\Public\Music\

CPU usage is high.

Questions:

- Is it suspicious?
- Steps to investigate?
- Final action?

Level 37. Scenario – Ransomware Behavior

A user reports:

- Files getting ".locked" extension
- Desktop wallpaper changed
- A note.txt requesting payment

What immediate steps will you take?

Level 38. Scenario – Suspicious Network Activity

Firewall logs show repeated outbound connections to an unknown IP on port **4444**.

What does this indicate?
What action should you take?

Level 39. Scenario – Malware False Positive

A developer says Norton keeps flagging their internal tool as malware.

What steps will you take to confirm if it's safe?

Level 40. Scenario – Word Document Macro Attack

User opens a Word doc and gets:
"Enable Content to view the file."

After enabling, system becomes slow.

Explain the likely attack & next steps.

Level 41. Scenario – Browser Redirection

User browser keeps redirecting to random search engines.

What checks do you perform?

Level 42. Scenario – Multiple Login Failures

You see 50 failed RDP login attempts in 5 minutes.

What does this mean?
What action will you take?

Level 43. Scenario – USB Malware Infection

User plugs a pen drive and system becomes slow. A .vbs file appears.

What does it indicate?

Level 44. Scenario – Suspicious PowerShell

Log shows:

powershell.exe -nop -w hidden -encodedcommand JABX...

What kind of attack is this?
What next?

Level 45. Scenario – Malicious Persistence

You find a suspicious entry in:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

What does this imply?

Level 46. Scenario – Privilege Escalation Attempt

Event log shows repeated:
"Access denied – attempt to escalate privileges."

What does it indicate?

Level 47. Scenario – Memory Injection

Norton detects:
"Malicious code injected into explorer.exe"

Explain what's happening.

Level 48. Scenario – Fileless Malware

An attack runs entirely through PowerShell & memory without saving files.

What type of malware is this, and how do you detect it?

Level 49. Scenario – C2 (Command & Control) Suspicion

You see traffic from an endpoint to:

hxxp://abcxyz-darkweb[.]top

on non-standard port 8082.

What steps will you take?

Level 50. Scenario – SOC Investigation Flow

If you receive an alert **"Trojan.Gen Found in 15 endpoints"**, describe the **complete investigation flow** from:
Detection → Analysis → Containment → Eradication → Recovery → Reporting.