# GEN NORTON – TECHNICAL ROUND INSIGHTS

## 1️⃣ ENDPOINT + MALWARE BASICS (MOST IMPORTANT)

Norton is endpoint-focused (AV + EDR).
They expect strong fundamentals on **malware, detection, logs, threats**.

**Must-Know Malware Concepts**

✔ **Types of Malware**

- Virus
- Worm
- Trojan
- Ransomware
- Spyware
- Stealer
- Adware

✔ **Key Malware Actions**

- Persistence
- Privilege escalation
- File encryption
- Network propagation
- Data exfiltration

✔ **Indicators of Compromise (IOC)**

- File hashes
- Malicious URLs
- Registry changes
- Suspicious startup entries
- Unusual CPU/network behavior

✔ **Detection Methods**

- Signature-based
- Heuristic
- Behaviour-based
- Sandboxing

✔ **Quarantine**

- How malware is isolated
- What happens after removal

## 2 WINDOWS SECURITY + SYSTEM FORENSICS

Norton expects **excellent Windows OS investigation skills**.

**Key Areas to Master**

✔ **Task Manager**

- High CPU/memory usage
- Suspicious process names
- Parent–child relationship

✔ **Windows Registry**

Common malware locations:

- Run / RunOnce keys
- Startup folders

✔ **Services**

- Checking malicious services
- Disabled security services

✔ **Event Viewer**

Log types to check:

- Application
- System
- Security
- PowerShell

✔ **Network Monitoring**

- netstat -ano
- Suspicious foreign IPs
- Outbound traffic anomalies

## 3 INCIDENT HANDLING + SOC THINKING

Norton checks the candidate's **response flow**, not just knowledge.

**Must Know the 6-Step IR Flow**

1. Detection
2. Analysis
3. Containment
4. Eradication
5. Recovery
6. Reporting

Students must use this framework when answering scenario questions.

**Common Norton Scenarios**

**Scenario 1 – Malware Alert**

Norton detects “Trojan.Gen” on a system. User says the file is safe.

Steps:

- Check hash

- Check file location
- Reputation check
- Sandbox analysis
- Review logs
- Allow or block

**Scenario 2 – Suspicious CPU Usage**

A process xmrig.exe is using 80% CPU.

Possible cause:

- Crypto miner

Steps:

- Check startup
- Kill process
- Remove related files
- Check registry
- Isolate system

**Scenario 3 – Browser Redirects**

User redirected to fake search engines.

Causes:

- Adware
- Malicious extensions
- DNS hijack

**Scenario 4 – PowerShell Attack**

Log shows:

powershell -nop -w hidden -encodedcommand ....

Indicates:

- Fileless malware
- C2 communication
- Script-based attack

**Scenario 5 – Ransomware**

Files changed to .locked

Steps:

- Isolate network
- Stop encryption process
- Identify strain
- Restore from backup
- Report incident

## 4️⃣ COMMUNICATION + REPORTING (VERY IMPORTANT)

Even for Norton, communication matters because analysts talk to:

✔ customers
✔ team members
✔ threat intelligence
✔ management

**Norton Wants Candidates Who Can:**

- Explain malware behavior in simple terms
- Provide step-by-step response
- Not panic during high-severity alerts
- Write clear incident summaries

**How Students Should Answer**

**1. Explain simply**

"Ransomware is a malware that encrypts files and demands money."

**2. Be analytical**

"First I will check logs and the process involved."

**3. Be structured**

Use Detection → Analysis → Containment format in scenarios.

**4. Calm tone**

Especially when describing high-risk attacks.

## FINAL SUMMARY (What Norton Expects)

**MALWARE BASICS (highest weightage)**

- Types
- Detection
- IoCs
- Behaviour
- Quarantine

**WINDOWS SECURITY**

- Processes
- Registry
- Logs
- Services
- Network calls

**INCIDENT RESPONSE**

- Flow
- Scenarios
- Containment steps

**COMMUNICATION**

- Clear

- Step-by-step
- Confident