CYBERSECURITY + IoT INTERVIEW PREPARATION ROADMAP

(Everything a candidate must prepare — crisp + industry relevant)

1️⃣ CORE CYBERSECURITY FUNDAMENTALS

Every company checks these basics.

✔ CIA Triad

- Confidentiality
- Integrity
- Availability

✔ Security Terminology

- Threat vs Vulnerability vs Risk
- Attack surface
- Zero Trust
- Hardening
- Defense-in-depth

✔ Malware Concepts

- Virus, Worm, Trojan
- Ransomware (very important)
- Spyware/Adware
- Rootkit
- Fileless malware
- Indicators of Compromise (IoCs)

✔ Authentication & Authorization

- MFA
- SSO
- OAuth / JWT (basic idea)

✔ Encryption Basics

- Symmetric vs Asymmetric
- SSL/TLS
- Certificates
- Hashing (MD5, SHA-256)

2️⃣ NETWORKING (MANDATORY for Cyber + IoT)

✔ IP, Subnet Mask, Gateway

✔ DNS, DHCP

✔ TCP vs UDP

✔ NAT, PAT, Port Forwarding

✔ VLANs

✔ Firewalls (L3, L7), WAF

✔ VPN

✔ OSI & TCP/IP models

✔ Routing basics (static vs dynamic)

Companies love asking:

- “What happens when you type google.com in browser?”
- “User can ping IP but not URL — what issue?”

3️⃣ OPERATING SYSTEM SECURITY

✔ Windows Security

- Task Manager investigation
- Startup entries
- Services
- Registry basics
- Event Viewer logs

✔ Linux Security

- File permissions (rwx)
- Processes (`ps`, `top`)
- Network (`ifconfig`, `netstat`)
- System logs (`/var/log/`)

✔ Hardening

- Disabling services
- Account/password policies
- Patching

4️⃣ SOC + INCIDENT RESPONSE BASICS

✔ SIEM (Splunk / QRadar / Sentinel)

- Alerts
- Events
- Log analysis basics

✔ Incident Response 6 Steps

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

✔ Types of Attacks

- DDoS
- Brute-force
- SQL Injection
- XSS

- MITM
- Password spraying
- Lateral movement

5️⃣ CLOUD SECURITY (NEW EXPECTATION)

Just basics needed:

- AWS / Azure security groups
- IAM (roles, policies)
- Cloud storage security (S3, blobs)
- Shared responsibility model
- VPC basics

6️⃣ COMMUNICATION & CUSTOMER HANDLING

(Companies like Sysnet, HCL, Deloitte Security, K7, Gen Norton insist on this.)

Students must practice:
✔ Explaining technical terms in simple English
✔ Handling panicked users
✔ Giving step-by-step instructions
✔ Writing short incident summaries

7️⃣ IoT SECURITY (VERY IMPORTANT — fast-growing area)

IoT = Smart devices + networks + sensors → very vulnerable.

A. IoT Architecture

1. Devices / Sensors
2. **Connectivity layer** (WiFi, Bluetooth, ZigBee, LPWAN)
3. IoT Gateway
4. Cloud / Data processing

Understanding the flow is enough.

B. IoT Protocols

Must-know:

- MQTT
- CoAP
- AMQP
- ZigBee
- BLE
- RFID

Companies ask:

- “How is MQTT different from HTTP?”

- "Why IoT devices need lightweight protocols?"

C. IoT Vulnerabilities

These are frequently asked:

- Weak/default passwords
- No firmware updates
- No encryption
- Open ports
- Hardcoded credentials
- Unsecured APIs
- Physical security issues

D. IoT Security Controls

Students must know:

- Device authentication
- Secure boot
- Firmware patching
- TLS encryption
- Network segmentation for IoT
- Monitoring IoT logs

E. IoT Attack Scenarios

1. Botnet (Mirai attack)
2. Unauthorized device access
3. Eavesdropping on smart devices
4. Replay attacks
5. API-based attacks
6. Side-channel attacks

8️⃣ PRACTICAL TROUBLESHOOTING (COMPANY FAVOURITE)

Prepare for these scenarios:

- No Internet
- DNS Resolution failure
- Slow PC
- High CPU process
- Suspicious file/process
- VPN not connecting
- Email not receiving
- Browser redirect
- IoT Device not pairing
- IoT WiFi dropping

9️⃣ BEHAVIOURAL & HR (ALWAYS ASKED)

- Why cybersecurity?
- Describe a challenging problem you solved.
- What is your approach to learning new threats?
- Example of handling pressure / incidents.

🔟 HANDS-ON PRACTICE RECOMMENDED

✔ Wireshark basics
✔ Packet capture analysis
✔ Windows event log analysis
✔ Linux log files
✔ Hashing tools
✔ Password cracking basics (John/Hashcat)
✔ Simple IoT programming (optional)
✔ Testing an insecure IoT device (open ports, weak creds)

FINAL SUMMARY – MUST MASTER (in order)

- Cybersecurity Fundamentals
- Networking + OS basics
- Malware + Windows Security
- SOC + Incident Response
- IoT protocols + attacks
- Troubleshooting
- Communication skills

This is exactly what students need to clear Sysnet, Gen Norton, Deloitte, HCL, K7, Zoho IoT roles, Wipro CyberSec, Palo Alto, SOC roles.