KOENIG
step forward

Threat Detection & Response

Duration: 1 day

1. **Understanding the Threat Landscape**

- Overview of common cyber threats
- Attack vectors: external vs. internal
- Real-world examples and case studies

2. **Threat Detection Techniques**

- Indicators of compromise (IOCs)
- Signature-based vs. behavior-based detection
- Tools and technologies (SIEM, IDS/IPS, EDR overview)

3. **Incident Handling & Containment**

- Incident response lifecycle
- Detection to containment workflow
- Roles and responsibilities during incidents

4. **Eradication & Recovery**

- Steps for threat eradication
- System restoration & validation
- Post-incident activities and lessons learned

5. **Best Practices & Proactive Measures**

- Continuous monitoring and threat intelligence
- Building resilient response teams
- Documenting and improving incident response plans