KOENIG
step forward

Blue Team Level 1 Certification Preparation training

Domain 1 - Security Fundamentals

- **Introduction to Security Fundamentals**
- **Soft Skills**
- **Security Controls**
- **Networking 101**
- **Management Principles**

Domain 2 - Phishing Analysis

- **Introduction to Emails and Phishing**
- **Types of Phishing Emails**
- **Tactics and Techniques Used**
- **Analysing URLs, Attachments, and Artifacts**
- **Taking Defensive Measures**
- **Report Writing**
- **Lessons Learned**
- **Phishing Response Challenge**

Domain 3 - Threat Intelligence

- **Introduction to Threat Intelligence**
- **Threat Actors and APTs**
- **Operational Threat Intelligence**
- **Tactical Threat Intelligence**
- **Strategic Threat Intelligence**
- **Malware and Global Campaigns**

Domain 4 - Digital Forensics

- **Introduction to Digital Forensics**
- **Forensics Fundamentals**
- **Digital Evidence Collection**
- **Windows Investigations**
- **Linux Investigations**
- **Volatility**
- **Autopsy**

Domain 5 - SIEM

- **Introduction to SIEM**
- **Logging**
- **Aggregation**
- **Correlation**
- **Using Splunk SIEM**

Domain 6 - Incident Response

- **Introduction to Incident Response**
- **Preparation Phase**
- **Detection and Analysis Phase**
- **Containment, Eradication, and Recovery Phase**
- **Lessons Learned**
- **MITRE ATT&CK**