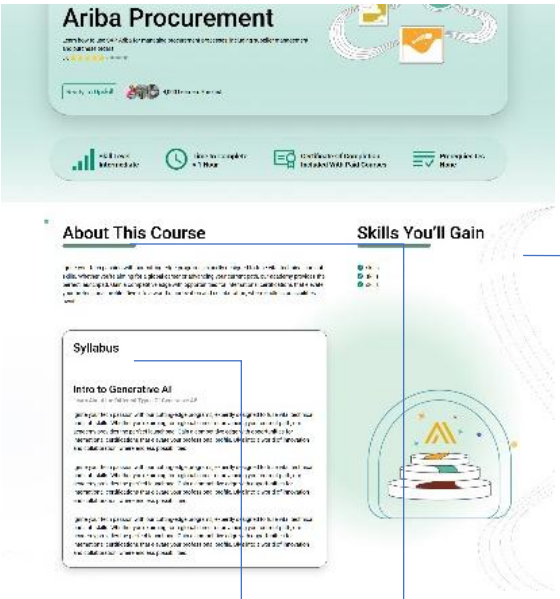

Skills:

- Threat Monitoring and Analysis
- Incident Response and Management
- Vulnerability Assessment
- Security Information and Event Management (SIEM)
- Malware Analysis and Mitigation
- Network Security Monitoring

The Cyber Security SOC (Security Operations Center) Analyst Professional course focuses on training individuals to monitor, detect, respond to, and prevent cybersecurity threats within an organization.
SOC teams play a crucial role in protecting businesses from cyberattacks by identifying potential vulnerabilities, managing incidents, and ensuring compliance with security policies.
This course covers key SOC functions, including threat monitoring, incident response, vulnerability assessment, and security information and event management (SIEM).
By the end of the course, you'll have the skills to handle cybersecurity incidents effectively and maintain a secure digital environment.

Course Outline

Introduction to Security Operations Center (SOC) Overview of SOC functions, roles, and the importance of cybersecurity.	**Vulnerability Management and Assessment** Identifying, assessing, and mitigating system vulnerabilities.
Threat Monitoring and Detection Techniques for identifying and analyzing potential cybersecurity threats.	**Malware Analysis and Mitigation** Techniques for detecting, analyzing, and neutralizing malware.
Incident Response and Management Steps and strategies for responding to and managing security incidents.	**Network Security Monitoring** Monitoring network traffic for suspicious activities and potential threats.
Security Information and Event Management (SIEM) **Using SIEM tools for real-time monitoring and event correlation.**	**SOC Automation and Tools** **Leveraging automation tools and processes to improve SOC efficiency.**
Compliance and Risk Management **Ensuring adherence to security regulations and managing cybersecurity risks.**	