CYBER SECURITY INTERNSHIP

30 Days 160* hours Intensive Certified Internship

Highlights of the Internship

- **Dedicated Industry Expert to clarify doubts and give reviews on your work.**
- **High Quality Study Materials.**
- **Case Study based approach for better problem solving.**
- **Project based working model to give Hands-on learning experience**
- **Various High quality Technical Assignments.**
- **ISO 9001: 2015 by UKAS, UK, EIAC DUBAI AND LMS a Globally Valid one month internship certification to boost your career prospects.**
- **Higher Education and Career Guidance Counselling Sessions by Experts.**

Top Performers will be selected and given opportunity to work on projects with companies.

Internship Structure

- **No of Days: 8** (Offline) + 3 Weeks (Online)
- **No of Hours:** Total 160Hrs (70 Hands-On Training & Hands-On Projects) + (90 Hours of Online learning + Major Project)

Technologies you learn

- Ethical Hacking
- Various Hacking Concepts
- Penetration Testing
- Vulnerability Analysis
- Social Engineering Techniques
- IoT Hacking

- Cloud Computing Hacking
- Various Cyber Security & Protection Tools
- Cryptography
- Cyber Forensics

Week 1: 70 Hours Offline Internship conducted at our Centers.

Week 2: Computer Crime – Case Studies Threat Scenarios

- Hacking Incidents
- Financial Theft
- Theft of Identity
- Corporate Espionage
- Email Misuse
- Pornography

Introduction to Incident Response and Computer Forensics

- Pre-Incident Preparation
- Detection of Incidents
- Initial Response Phase
- Preserving "Chain of Custody"
- Response Strategy Formulation
- Evidence Collection and Analysis
  - Defining Evidence
  - Forensically Sound Evidence Collection
  - Evidence Handling
  - Host Vs Network Based Evidence
  - Online Vs Offline Response
- Digital Forensics - Putting on the Gloves
  - The 6 A's
  - The Investigative Guidelines
  - Disk-based Forensics Vs Network-based Forensics
- Reporting the Investigation

Week 3: Computer Crime – Case Studies Threat Scenarios

- Network Devices
- Introduction to Log Analysis
- Analyzing Snort and Firewall Logs
- Analyzing Apache, IIS, Squid Logs
- Network Intrusion Case Study
- Using Tcpdump, Snort, Tcpdstat, argus, tcpflow, tcptrace

Evidence Collection and Analysis - Introduction to Live response

- The Do's and the Don'ts
- Windows Live Response
- Linux Live Response

Data Acquisition / Disk Imaging

- Learning the rope – the essentials
- Risk Imaging using Linux (dd, sdd, dcfldd) and Netcat
- Disk Imaging using **Encase, Helix** Bootable disk

Forensics Analysis of the Evidence

- Analysis using Helix
- Basic and advanced analysis using **Encase v5 Forensic edition**

Forensics Analysis - Internet Misuse - Browser Forensics

- Understanding Browser history artifacts
- Browser Forensics
  - Using **Encase**
  - Using Netanalysis, WebHistorian

Week 4: Digging Deep into the Cyber World - Email and Website Tracing

- Understanding Registry structure
- Understanding MRU lists
- Understanding UserAssist
- Registry Forensics using ENCASE

Malicious Binary Analysis

- Using IDA freeware
- Using strings.exe
- Using BinText
- Using Regmon, Tcpmon
- Using Peid

Documenting the Investigation Forensics Challenge Case Study A peek into the Indian Cyber Law Tools Used

- Encase Forensic edition
- Helix Bootable CD
- The Coroner's Toolkit
- Tcpdump
- Snort
- Tcpdstat
- Argus
- Tcpflow
- Tcptrace
- Ethereal
- Neotrace
- Smartwhois
- Peid
- NetAnalysis
- Web Historian
- Bintext
- IDA freeware