**Specialized Training Programme in** **Cyber Security and Malware Analytics**

1. **Introduction to Computer Networks (1 day)**
	* Introduction to Networking with Lab
	* OSI Model, TCP/IP Headers
	* TCP Flags
	* IP Protocol and Addressing
	* Basic Networking Devices & their Functionality
	* Domain Name System (DNS)
	* UDP Header and ICMP Message
	* ARP Protocol
	* Routing process and Routing tables with Lab
	* Access Control lists
	* System Administration tools
	* Network Designing, Configuring and Administration
2. **Cyber attack (2 days)**
	* Introduction to Cyber Attacks
	* Impact of Cyber Attacks
	* Types of Cyber Attacks (demonstration)
		+ Malwares
		+ Password Attacks
		+ DDos Attacks (Distributed Denial of Service Attacks)
		+ Pop-Ups
		+ Software Updates
		+ Public Unsecured Wi-Fi Network Attacks
		+ Phishing Scams
		+ Cross Site Scripting
		+ SQL Injection
		+ Man-in-Middle Attacks
		+ Eavesdropping
		+ Session Hijacking
		+ Social Engineering
	* Prevention of Cyber Attacks
		+ Basic Security Tips
		+ How to deal with Cyber Attack
3. **Cyber Security Methods (2 days)**
	* Perimeter Security Fundamentals
	* Administration and Security
	* Linux Fundamentals and Commands
	* Network Monitoring
	* Packet Crafting
	* PCAP (Packet) Capturing
	* IP tables
	* Antivirus and Firewalls
	* Intrusion Detection/Prevention System (IDS/IPS)
	* Honeypots / Honeynets
	* Vulnerability Assessment
	* Attacks (Test Cases)
4. **Cryptographic Methodologies (3 days)**
	* Understand Basic Encryption Concepts
	* Attacks Against Encryption
	* Understand Private Key Encryption
	* Understand Public Key Encryption
	* Cryptography Fundamentals
	* Symmetric Key Encryption Algorithms
		+ Data Encryption Standard (DES) & Tripple DES
		+ Blowfish
		+ AES (Rijndael)
	* Public Key Algorithms
		+ Diffie-Hellman Exponential Key Exchange
		+ RSA
		+ EIGamal
		+ Schnorr’s Public Key Cryptosystem
	* Cryptographic issues
	* Secure Hash Functions
		+ MD5
		+ SHA1
	* Digital Signatures
	* HTTPS
	* PKI (Public Key Infrastructure)
		+ What is PKI?
		+ Components of PKI/PKI Architecture & Working
5. **Practical Network Packet Analysis (2 days)**
	* Traffic Analysis-Fundamental
		+ Packet Analysis and Network Basics
		+ Tapping into the wire
		+ Introduction to Wireshark
			- Navigating around Wireshark
			- Examination of Wireshark statistics
			- Stream reassembly
			- Finding content in packets
			- Wireshark display filters
			- TCPDUMP- writing tcpdump files
	* Packet Capturing and its analysis.
	* Application protocol and Traffic analysis
6. **Network Monitoring and Deep Packet Inspection (2 days)**
	* Network Architectures
		+ Instrumenting the network for traffic collection
		+ IDS/IPS deployment strategies
		+ Hardware to capture traffic
	* Introduction to IDS/IPS Analysis
		+ Function of an IDS
		+ The analyst’s role in detection
		+ Flow process to Snort
	* Snort
		+ Introduction to Snort
		+ Running Snort
		+ Writing Snort rules
		+ Solutions for dealing with false negatives and positives
		+ Tips for writing efficient rules