K7 ACADEMY

Creating the Cybersecurity Talent that will Build a Cybersafe World

K7 Academy is a unit of K7 Computing,
a Leader in Cybersecurity for More Than 30 Years

Association & Marketing By VELATEC

The Cybersecurity Talent Deficit is Threatening the Future of Digital Transformation

More than 3.5 million unfilled cybersecurity openings are estimated to exist across the world[1] by 2025. India alone is projected to have 1.5 million unfulfilled job vacancies[2] in cybersecurity by 2025. Over 450,000 new cyberthreats are registered every day[3]. Securing the digital world will require an army of cybersecurity professionals armed with appropriate skills and tools, but a severe talent deficit is threating the stability of cyberspace.

K7 Academy Creates Cybersecurity Warriors to Fight Real-world Cyberattacks

K7 Academy provides world-class cybersecurity training to students from across the world, creating cybersecurity professionals with the knowledge, skills, tools, and mindset to excel in an environment where a single cyberattack can result in an organisation shutting down operations.

K7 Academy is a division of K7 Computing, an international award-winning cybersecurity solution provider with more than 30 years' expertise in cybersecurity. K7 Computing protects 25+ million users and 40+ million devices across 27 countries, and K7 Labs is an internationally acclaimed malware research centre analysing hundreds of thousands of cyberthreat samples every day.

[1] Cybersecurity Ventures

[2] Michael Page India

[3] AV-TEST

Why K7 Academy?

- Real-time learning to develop role-based competencies
- Well-established domain expertise recognised by peers and institutions
- Robust infrastructure, courseware, and work-oriented instructional aids
- Job-oriented training programmes conducted by industry veterans
- Real-world threat lab environment
- Programmes with more than 75% hands-on and activity-based learning

Association & Marketing By VELATEC

Programmes Designed To Suit Your Needs

Segment	Benefits
Corporate Cybersecurity training programmes customised to suit the needs of business users, IT teams, and management.	• Improvement in cybersecurity awareness across the organisation • Cybersecurity skill development and tool familiarity for IT staff • C-suite knowledge download to enable the development of strategic cybersecurity initiatives
Academia Cybersecurity training for faculty and assistance in development of academic programmes that will improve institutional ranking and enable students to access lucrative opportunities.	• Industry-recognised certifications • Malware lab setup assistance with supply of malware samples • Internship programmes • Train-the-trainer programmes • Guest lectures • Job-oriented programmes • NAAC accreditation4enablement
Learn @ K7 Training programmes for aspiring cybersecurity professionals and skill upgrade programmes for experienced cybersecurity specialists.	• Training at the K7 facility • Exposure to real-world cyberthreat events and cybersecurity industry environment • Industry-recognised certifications • Direct access to K7's cybersecurity knowledge leaders • Internship programmes

Association & Marketing By VELATEC

[4]Cybersecurity is a Key Indicator for IT Infrastructure under the Quality Indicator Framework for NAAC Accreditation

K7 Academy
Programme Outlines

Programme	Outline
Certified Malware Researcher – Windows	• Develop expert hands-on skills and techniques to reverse engineer and perform forensic investigation of malware and secure the Windows environment • Includes case studies, discussions on current threats and past attacks, and industry perspectives
Certified Malware Researcher – Android	• Creates expert proficiency in advanced analysis of mobile threats • Includes demonstrations and activities on Android app development, and case studies and discussions on the current Android threat landscape
Network Security	• Enables management of complex networks through understanding of network fundamentals and security layers • Includes demonstrations and activities on network protocols, layer-wise attacks, network monitoring tools, log and packet capture and parsing, as well as case studies and discussions
Vulnerability Assessment and Penetration Testing	• Provides hands-on learning of the steps taken by an ethical hacker to pentest a website • Includes demonstration and activities on footprinting, scanning, enumeration, and hacking a WordPress website, as well as case studies and discussions
Cybersecurity Sentinel	• Creates awareness of key cybersecurity concepts, cyber ethics, laws, and standards • Includes case studies, discussions on current threats and past attacks, and industry perspectives
Security Incident Response	• Develops skills to respond to attacks and isolate malware • Includes malware testing in secure environments, incident response plan and practice, as well as case studies and discussions

K7 ACADEMY

Certified Malware Researcher – Windows

Duration:
15 Days (80 Hours)

Mode:
Lecture, Tutorials, Projects

Programme Outcomes

- Define and relate to cybersecurity
- Familiarise with the Windows OS
- Relate to the fundamentals of Windows internals
- Practice in virtual environments for testing
- Learn about malware types and behaviour
- Build proficiency in malware analysis tools
- Learn reverse engineering & assembly programming
- Investigate malware forensics in Windows

Programme Audience

- Forensic Engineer/Forensic Specialist
- Threat Analyst/Malware Analyst
- Malware Researcher/Anti-malware Research Lead
- Software Testing Lead/Secure Coding Specialist

Programme Information

1. Introduction to Malware
   a. Malware types
   b. Behaviour of malware
   c. Malware infection vector

2. Windows Basics Relevant to Malware Behaviour
   a. File system
   b. Windows Directory structure
   c. Registry
   d. Protection rings
   e. Boot sequence

3. Dynamic Malware Analysis
   a. Virtualisation software
   b. Monitoring tools
   c. Classifying malware based on their behaviour

4. Number System
   a. Base conversions
   b. Arithmetic and logical operations

5. Basic Static Malware Analysis
   a. File formats
   b. PE file structure
   c. Static malware analysis tools
   d. Packer identification

6. Advanced Static Malware Analysis
   a. Reverse engineering
   b. x86 assembly programming
   c. Introduction to OllyDbg
   d. Introduction to IDA Pro
   e. Advanced malware analysis
   f. Packed sample analysis

K7 ACADEMY

Cybersecurity Sentinel

Duration:
1 Day (6 Hours)

Mode:
Lecture & Demonstration

Programme Outcomes

- Define and relate to cybersecurity
- Understand the current cyberthreat landscape
- Explore current cyber ethics, laws, and standards
- Articulate and demonstrate essential cyberhygiene

Programme Audience

- Employees/Government Staff/IT Teams/ Professionals
- Faculty/Students/Computer Users
- Business Users

Programme Information

1. Definition of Security & Cybersecurity/Current Trends in Cybersecurity
2. The Need for Enterprise Cybersecurity/Leader's Speak/ Misconceptions about Cybersecurity
3. Digital Landscape & Assets such as Social Media/ Dark Web/Internet of Things
4. Definition & Relevance of the Threat Landscape/ Attack Surface
5. Threat Landscape in Social Media
6. Threat Landscape in Business/Finance/Automobiles/ Devices/Infrastructure
7. Threat Landscape in Telecom/Healthcare/Education/ Defence/Government
8. Definition & Relevance of Vulnerabilities, Risks, Exploits, and Threat Vectors
9. Common Vulnerabilities & Exploits
10. Definition & Purpose of Cyber/Privacy Laws
11. Cybersecurity Laws, Regulations & Standards – IT Act, 2000 & Important Sections
12. Cybercrime Investigations & Collection of Evidence
13. Introduction to Cyber Hygiene
14. Passwords/Software Downloads/Emails/Messages/ Safe Browsing
15. Laptop Security/Public Wi-Fi/Mobile Security

K7 ACADEMY

Network Security

Duration:
4 Days (24 Hours)

Mode:
Lecture, Demonstration, Activity

Programme Outcomes

- Relate to the various OSI security layers in a network
- Monitor traffic, sniff and analyse packets
- Familiarity with and uses of network tools such as
  - Message Analyzer
  - Wireshark
- Tracing network anomalies using PowerShell
- Exploring automation in monitoring

Programme Audience

- System/Network/Database Administrators
- Network/DDoS /Firewall Security Engineers
- Infosec/Security Engineers

Programme Information

1. Introduction to Network Security
   a. Importance of securing networks
   b. OSI layers and security challenges
   c. Importance of understanding attacks in each OSI layer

2. Physical Layer
   a. Topologies/Switches/Modems/Routers
   b. Popular attacks in this layer

3. Data Link Layer
   a. Sub layers/ARP tables/Frames
   b. Popular attacks in this layer

4. Network Layer
   a. IP Address classes, IPv4 vs IPv6 transition
   b. Number of networks & hosts in a subnet
   c. Popular attacks in this layer

5. Transport Layer
   a. TCP vs UDP, TCP Connection Establishment
   b. Popular attacks in this layer

6. Session Layer
   a. Session IDs\Cookies\Transmission methods\Checkpoints
   b. Popular attacks in this layer

7. Presentation Layer
   a. Compression, encryption & decryption, NetBIOS, SMB
   b. Popular attacks in this layer

8. Application Layer
   a. Popular protocols such as SNMP, HTTP, FTP, RDP, SSH, Telnet
   b. Popular attacks in this layer

9. Importance of Logs
   a. Use of tools for tracing and capturing device information
   b. System & network logs
   c. Case study on the network security process
   d. Best practices for network security

10. Microsoft Message Analyzer – Network Monitoring Tool
    a. Traffic Monitoring on the Windows network
    b. Packet sniffing
    c. Filters for selecting specific data
    d. Using viewpoints to analyse messages in the analysis grid

11. Traffic Analysis and Checking of Anomalous Traffic
    a. Types of anomalous traffic
    b. Demonstration of identifying and parsing of log files
    c. Exhibit of various types of anomalous traffic

12. Applying Filters to Determine Anomalies in Traffic
    a. Detecting and analysing suspicious packets using Message Analyzer

13. Introduction to Wireshark Network Monitoring Tool
    a. Detecting and analysing suspicious packets using Wireshark

14. Case Study on Automation
    a. Capturing & archiving log files
    b. Parse log data and create semantic interpretation of logs

15. Automate Tracing Functions to Capture Anomalous Packets
    a. Using message analyser to start & stop traces

16. Application-aware Devices
    a. Firewalls
    b. IPS
    c. IDS
    d. Proxies

K7 ACADEMY
www.k7academy.com

K7 ACADEMY

Security Incident Response

Duration:
1 Month

Mode:
Lecture, Demonstration, Activity

Programme Outcomes

- Relate to cybersecurity and the threat landscape
- Explore OSI security layers in a network
- Monitor traffic and analyse packets
- Understand how Windows works under the hood
  - Command Line Interface/Windows Directory Structure
  - Registry/Processes/Services/Threads
- Setting up of isolated malware execution environment (VMs)
- Practise dynamic malware analysis
- Gain experience in incident response and reporting

Programme Audience

- Infosec Support/Security Support
- SOC Engineer/Security Engineer
- Incident Responder/SIEM Engineer
- Threat Intelligence Analyst/DevOps Engineer

Programme Information

1. Introduction to Cybersecurity & the Threat Landscape
2. Cyber Laws and Relevance in Security Operations
   a. Social Engineering
   b. Human Threat Vectors
   c. Vulnerabilities and Exploitation
3. OSI Layers and Security Challenges
   a. Importance of understanding attacks in each OSI layer
4. Physical Layer
   a. Topologies/Switches/Modems/ Routers
5. Data Link Layer
   a. Sublayers/ARP Tables/Frames
6. Network Layer
   a. IP Address Classes/Number of networks & hosts in a subnet
7. Transport Layer
   a. TCP vs UDP, TCP Connection Establishment
8. Session Layer
   a. Session IDs\Cookies\Transmission methods\Checkpoints
9. Presentation Layer
   a. Compression, encryption & decryption, NetBIOS, SMB
10. Application Layer
    a. Popular protocols such as SNMP, HTTP, FTP, RDP, SSH, Telnet
11. Network Monitoring Tool Wireshark
    a. Traffic monitoring in the Windows network
    b. Packet sniffing
    c. Filters and their uses including keyword, session, time, and view filters
12. Importance of Logs
    a. Use of tools for tracing and capturing device information
    b. System & network logs
    c. Filters and their uses including keyword, session, time and view filters
13. Traffic Analysis and Checking of Anomalous Traffic
    a. Types of anomalous traffic
    b. Exhibiting various types of anomalous traffic
    c. Collecting samples using Wireshark
14. Windows Under the Hood
    a. Windows Registry
    b. Directory structure
    c. File locations across versions
    d. Booting sequence
    e. Command Line tools
    f. Processes, Services & Threads
15. Malicious Behaviour Including Ransomware
    a. Malware infection vectors and payloads
    b. Malware types and classifications
    c. Malware persistence techniques
16. Setting Up Virtual Machines (Guest and Host OS)
    a. Persistent and non-persistent mode
17. Use of Malware Analysis Tools
    a. File Format Explorers, Dynamic State Change Monitoring Tools, Decoy Network Setup
    b. Classifying files as benign or malicious
18. Incident Response Policies & Case Study
    a. Identifying and collecting samples of malicious files in a VM
    b. Reporting the incident and collecting evidence of an attack
19. Business Continuity Plan
    a. Disaster recovery
    b. Data backups
    c. Restoring systems

K7 ACADEMY

www.k7academy.com

A Unit of

K7 COMPUTING

India | Singapore | UAE | USA

www.k7computing.com

Association & Marketing By VELATEC

Partners in Business Intelligence