SYTECH LABS
PVT. LTD.

REINFORCING CYBER SECURITY
BY PREDICTING AND MITIGATING
CYBER THREATS

RECOGNISED BY
SILICON INDIA AND CONSULTANT
REVIEW MAGAZINES

ETHICAL HACKER
WHO FIGHTS AGAINST CYBER CRIMES

SECURING PERSONAL DATA

Ensuring Data Privacy through Personal Data and Protection Solutions

HIS SPECIALIZATIONS INCLUDES

- *Information Security Professional & Researcher*
- *Vulnerability Research and Disclosure*
- *Penetration Testing*
- *Vulnerability Assessment of Networks and Systems*
- *Cyber Crime and Forensic Investigator*

SANDEEP MUDALKAR
FOUNDER AND CEO

CYBER SECURITY & FORENSIC EXPERT

www.sytechlabs.com | www.sandeepmudalkar.com

Organization's Essential Deliberations in managing the Risks to CYBER-WORLD

Over the years, there has been gigantic development in the cyber-world due to the extreme growth in the information technology. But the security of this cyber-world is often exploited and is at risk. Currently, there is a severe threat to very basic and highly confidential data. The security organizations are majorly focusing on cyber-security threats rather than other means of attack/ than any other means of attack. We are presently working on the cutting-edge spying techniques and other methodologies to manage Cyber security risk. The expansion of technology from cell phone to the smartphone has engaged the government to work closely with the private sector to secure the cyber network.

Sharing the Information

The confidential information leaking can bring the stability of an organization into danger. Securing and managing this information is a perfect insight to create a strong base for an organization. The investors must be alert to the risks, predominantly of cross-cutting and shared risks, and be involved in complex decision-making processes.

- Information sharing strengthens organizational resilience.
- It enables early identification of cyber threats.
- Effective communication builds trust among stakeholders.
- Clear processes ensure timely response to cyber risks.
- A collaborative approach leads to a more secure cyber environment.

> Information sharing should involve appropriate communication processes. These processes must embrace thresholds and criteria for communicating and escalating risks. Tools used for sharing information, such as dashboards of pertinent metrics, can keep investors conscious and involved. Sharing the information helps to identify, asses, and respond to a cyber-security risk and permit risk decisions to be well informed, well considered, and built with a perspective to satisfy organizational objectives.

SYTECH LABS PVT.LTD

With the advancement of technology, the knowledge resources are becoming an open source by boosting students and researchers to learn more about Cyber Security. The new era of Cyber Defense in India has grown to maximum from personal to corporate level, social networking, social media; knowledge sharing websites that are very rapidly growing in securing the people. As security is the major aspect for every nation. The government of India has secured ambitious plans to raise cyber connectivity with various activities related to e-governance and e-commerce that are now being carried out over the Internet.

Sytech Labs Pvt Ltd is one of the leading IT Security Firms in India, that is known for providing business solutions to their clients in terms of training, systems integration, consulting, outsourcing, application development, and networking. Sytech Labs Pvt Ltd services line include Information Security Training, Seminars & Workshops, Cyber Crime Investigation & Consulting, Vulnerability Assessment & Penetration Testing (VA/PT), IT Security Consulting & Auditing, Web Application Development, Search Engine Optimization, Network Solutions etc.

Sytech Labs Pvt Ltd was Founded in year **2014** by Headquartered at Hyderabad **Mr.SANDEEP MUDALKAR - Cyber Crime Investigator & Trainer** with motivation of his father **M.K.Vishwanatham, Deputy Conservator Forest (Rted).** In short span, Sytech Labs Pvt Ltd has improved the infrastructure. Sytech Labs Pvt Ltd has conducted plenty of seminars & workshops for police department and various educational institutes across the India. Our team always cop with Crime Branch Departments of various states for Investigating Cyber Crimes. As the world facing increased number of cyber-crimes, our training department is working hard to deliver best IT Security knowledge to our students to make them best for the IT industries. Our team includes experts from most of the states of the India. Sytech Labs Pvt Ltd Team has helped the society by offering consultancy of cyber laws & cyber-crime investigation for victims. Our qualified team of Software Developers & Web Developers is been always appreciated by our clients for providing them best out of the best Web Solutions.

OBSTACLES FACED AT IGNITION POINT

At the beginning of the journey, while establishing the organization, Sytech Labs faced several difficulties over a year in finding a good team for sorting out issues in their projects and there was also a tough task in forming cyber security expert's team which is very rare especially in India. They also faced multitask Investigation across critical cases from various police department regarding Fake profiles of Social Networking Cases, Credit & Debit Card cloning, Cyber Stalking, Fake Lotteries, Data Integrity, Phishing, Email Hacks, Denial-of-service (DoS), Programming flaws, Spoofing attacks, Virus & Worms in Networks, Website Hacks, Leakage of Private information on blogs etc.

PRIORITIZING DATA SECURITY IN THE DIGITAL AGE

ENLIGHTENING STUDENTS & PROFESSIONALS VIA NONPAREIL TRAINING & CONSULTANCY

Besides the fact that Internet, the sophisticated creation of mankind, has eased the lives of people through diversified means, it has also evolved into a space posed with proliferating menaces that are incomprehensible even to cyber professionals. Sytech Labs extends its training centre & consultancy to a wide range government organisations in which conducted trainings for on Cyber Security for MCEME, Indian Army, Judges and Public Prosecutor, National Institute of Smart Governance(NISG), Customs and Central Tax, Central Detective Training Institute(CDTI), MCRHRDI, APHRDI, Cyber Crime Department of Hyderabad and many more on not just modifying their investigation strategy as per the cyber crime case, but also on spreading awareness about the security parameters evolving with technological changes.

SECURED FUTURE OF SYTECH LABS

The cyber threats will certainly pose a significant challenge to IT professionals across all sectors with the increase in technologies such as cognitive computing, and big data analytics. Besides the IoT is further influencing the increasingly connected world in unprecedented ways.

"While talking about the future steps that are taken on cybercrimes by the organization, Sandeep states "Our goals is to be one among the best cyber security experts over India, trying hard to get tie-up with various governments across India as there are many flaws in government systems & apart from this we are focusing on M-Commerce & E-Commerce projects etc." "

> *" Sytech Labs assures to provide rigorous training to them on promoting security and identifying potential risks like database leakages, system & email hacks and a lot more "*

OFFERINGS :

- Cyber Crime Investigation & Consulting
- Information Security Training
- Seminars & Workshops
- Vulnerability Assessment & Penetration Testing (VA/PT)
- IT Security Consulting & Auditing
- Web Application Development and Auditing
- Search Engine Optimization
- Network & Its Penetration Testing

SANDEEP MUDALKAR

FOUNDER & CEO

During his early days of schooling at **St. Marys High school** in Hyderabad, Sandeep was an ardent follower of technology and science. Participating and winning a few science exhibitions and tech competitions, hi--vs interest was rapidly holding the reins of technology. As the next step, he completed his **Bachelor Degree in Electronic & Communication Engineering** from the prestigious college from Aurora College, JNTU University where his inclination towards computer science and technology started shaping up. This was the time when Sandeep recognized the necessity of **'Security'** in an application, database, code or network, which catapulted him towards **Ethical Hacking** and motivated him to pillar his career in IT security.

After completing his graduation, Sandeep joined **TATA consultancy service** as an **Network Security Analyst Evangelist** and successfully stirred his role of **IT Security Trainings** for corporate. This volume exposed Sandeep to **real-time VAPT projects** and contributed in shaping up his professional life at its best.

RENOWNED ETHICAL HACKER & CYBER SECURITY EXPERT

With this substantial amount of experience and good industry contacts, **Mr.Sandeep Mudalkar** established Sytech Labs Pvt Ltd in the year **2014** with the motivation from his father **Mudalkar Kashi Vishwanatham (Deputy Conservator of Forest-Red)**, family, well-wishers and his wife **Shalini Mudalkar-Co-Founder** and today he is a Cyber Security Trainer, Investigator and Consultant with various government departments, and researcher of cyber security.

- He was interviewed and participated in live debates by several print and electronic media.
- The Hindu, Deccan Chronicle, The New Indian Express, India Ahead, Zee TV, Zee News (Hindi), TV9, NTV, Eenadu Etharam, T-News, V6, Express TV, CVR News etc.
- He was even rewarded by IAS & IPS officers for solving complex cases of cyber crimes.
- Identifying bugs in government sites, & helped them to improve security and reowned as Cyber Crime Investigator.

Under the leadership of young entrepreneur Sandeep, the team has always copped up with Crime Branch Departments of various states for Investigating Cyber Crimes. In a short span of time, Sytech Labs has improved the in-frastructure by conducting plenty of seminars & workshops across India. He has also conducted awareness on Cyber Crimes for more than **200+ schools**, Intermediate & Degree Colleges & more than **150+ workshops** on **Ethical Hacking** at various engineering colleges where as many students and professionals got benefited by his lectures.

A Zealous
IT SECURITY PROFESSIONAL

OBSTACLES FACED AT IGNITION POINT

At the beginning of the journey, while establishing the organization, Sandeep faced several difficulties over a year in finding a good team for sorting out issues in their projects and there was also a tough task in forming cyber security expert's team which is very rare especially in India. They also faced multitask Investigation across critical cases from various police department regarding Fake profiles of Social Networking Cases, Credit & Debit Card cloning, Cyber Stalking, Fake Lotteries, Data Integrity, Phishing, Email Hacks, Denial-of-service (DoS), Programming flaws, Spoofing attacks, Virus & Worms in Networks, Website Hacks, Leakage of Private information on blogs etc.

CONTRIBUTING VARIOUS SECTORS THROUGH CYBER CRIME SOLUTIONS

Being a Cyber Crime Investigation & Law Consultancy, Sytech Labs provides consultancy services to Cyber Law issues, helping Cyber Crime Victims and how to carry out Cyber Crime Investigations, etc. For this purpose, they have a panel of advocates/consultants specializing in Cyber Law matters and practicing at various levels over India.

HE IS CERTIFIED IN

- Redhat Certified Security Specialist (RHCSS)
- Diploma in Microsoft Certified IT Professional (MCITP) Certification
- Diploma in Cisco Certified Network Professional (CCNP)
- Red Hat Linux (RHCE)
- CISCO Pix Firewall
- Certified Information Systems Security Professionals (CISSP).

POST GRAGUATION IN

- Post Graduate Diploma Cyber Law and Intellectual Property Law **(PGDCL&IPR)**
- Post Graduate Diploma Criminal Justice and Forensic Science **(PGDCJ&FS)**

WHEN RECOGNITION OVERCOMES SUCCESS

AWARDS & ACHIEVEMENTS

FROM IPS OFFICERS

On his remarkable success and well-deserved recognition as a Cybersecurity Expert. His dedication, expertise, and unwavering commitment to safeguarding digital infrastructure have set a benchmark of excellence in the field.

His proactive approach, innovative solutions, and deep technical knowledge have not only strengthened security frameworks for LEA but also inspired confidence among peers and organizations alike. So this recognition is a true reflection of your hard work, **perseverance**, and the positive impact you continue to make in the cybersecurity domain.

RECOGNIZED FOR EXCELLENCE

Honored with an Appreciation Letter in recognition of outstanding contribution and commitment towards cyber security and awareness.

HONORING DEDICATION

A token of appreciation for his relentless efforts and valuable support in strengthening cybersecurity initiatives.

UNLOCKING SUCCESS WITH

REWARDS & RECOGNITION

FROM DGP OF TAMIL NADU & HIMACHAL PRADESH

In India, working with LEA to teach and look into cybercrime cases has paved the way for his success. Even though his difficult assignments have inspired and forced him to put in a lot of effort in analyzing data such as CDR and IPDR and teaching LEA, Judicial how to uncover hints for an investigation.

A key challenge is to extract data with minimal impact on the live system to maintain its integrity, as the process itself can potentially alter evidence.

His dedication, expertise, and unwavering commitment continue to inspire peers and set a benchmark for excellence in the cybersecurity domain.

RECOGNIZED BY DGP, TAMIL NADU

HONORED BY DGP, HIMACHAL PRADESH

RECEIVING APPRECIATION FROM
MR. SANDEEP RAI RATHORE, IPS. (DGP) DIRECTOR OF TAMIL NADU WITH OTHER SENIOR IPS OFFICIALS

APPRECIATED FOR OUTSTANDING CONTRIBUTIONS TO CYBERSECURITY

CENTRAL DETECTIVE TRAINING INSTITUTE, BENGALURU

Course on "Social Media Investigation & Data Analytics"

(Exclusively for IAF Personnel)

22-07-2024 to 24-07-2024

INTERACTION WITH AIRFORCE OFFICIALS

The Indian Air Force (IAF) must be cognizant of cybercrime in order to defend its vital systems, weaponry platforms, and private information from enemies who could undermine its ability to wage wars and jeopardize national security. In the face of changing digital warfare, training staff on cybersecurity threats and best practices helps to fortify defensive measures, preserve operational preparedness, and guarantee the integrity of its critical infrastructure.

SAFEGUARDING SENSITIVE INFORMATION

Data Protection:

- Awareness helps personnel understand the importance of protecting sensitive and financial data from unauthorized access, which can lead to breaches and fraud.

REPUTATIONAL AND FINANCIAL INTEGRITY

- By preventing data breaches, the Air Force can avoid significant financial losses and damage to its reputation.

INTERACTION WITH SSB OFFICIALS

Cyber crime awareness is crucial for the Sashastra Seema Bal (SSB) army to protect critical military information, prevent operational disruptions from cyber warfare, and safeguard personnel from evolving threats like phishing and social engineering attacks. By training SSB personnel to recognize and counter these digital threats, the army builds a stronger defense, maintains operational security, and ensures their personal and professional digital lives remain secure in an increasingly interconnected digital landscape.

PROTECTING SENSITIVE MILITARY INFORMATION

- **Operational Security:**
  Cyber threats can compromise sensitive military data and systems, impacting mission effectiveness and national security.

BUILDING A STRONGER DEFENSE

- **Awareness & Prevention:**
  Awareness training helps SSB personnel act as a first line of defense by preventing data breaches and unauthorized access.

CAPACITY BUILDING
IN COLLABORATION WITH
NATIONAL E-GOVERNANCE DIVISION (NEGD), MEITY, GOI.

Government capacity building programs in cybersecurity are focused on strengthening the skills, knowledge, and infrastructure required to defend against cyber threats, ensure digital trust, and build cyber resilience.

KEY CAPACITY BUILDING AREAS

- Cyber Audit, Awareness & Cyber Hygiene
- Strengthening Govt. Institutional, Policy & Governance
- Capacity Building through Indian Government Initiatives

> Capacity building programs by governments are structured initiatives aimed at enhancing the skills, knowledge, systems, and institutions needed for effective governance, service delivery, and sustainable development.
>
> These programs are implemented across multiple sectors – such as education, healthcare, agriculture, digital literacy, law enforcement, and disaster management.

Government capacity building programs in cybersecurity are focused on strengthening the skills, knowledge, and infrastructure required to defend against cyber threats, ensure digital trust, and build **cyber resilience.**

STATE CAPACITY BUILDING WORKSHOP ON CYBER SECURITY IN THIRUVANANTHAPURAM, KERALA

12th–14th November 2024

CAPACITY BUILDING IN COLLABORATION WITH THE NATIONAL INSTITUTE OF SMART GOVERNANCE (NISG) AND COLLABORATION WITH MEITY, GOI.

Government capacity building programs in cybersecurity are focused on strengthening the skills, knowledge, and infrastructure required to defend against cyber threats, ensure digital trust, and build cyber resilience.

> In collaboration with **NISG** and **NeGD, MeitY** and the **Govt. of India** conducted many capacity building programs, specially focusing on their objectives and key capacity-building areas like Cyber Audit, awareness, and cyber hygiene for strengthening government institutions, policy, and governance by Indian government initiatives.

CYBER SECURITY AWARENESS PROGRAMME
ORGANIZED BY
ADMINISTRATIVE TRAINING INSTITUTE, GOVT OF ARUNACHAL PRADESH
IN COLLABORATION WITH NATIONAL INSTITUTE FOR SMART GOVERNMENT
FROM 12/02/2024 TO 14/02/2024

KEY FOCUS AREAS

Strengthening Institutions
Enhancing the skills, knowledge, systems, and institutional frameworks required for effective governance, service delivery, and sustainable development.

Cyber Audit & Awareness
Promoting regular cyber audits, awareness programs, and cyber hygiene practices to mitigate risks and build a culture of security.

Policy & Governance
Supporting the formulation and implementation of robust policies and governance mechanisms aligned with national priorities and digital transformation goals.

Multi-Sectoral Impact
Implemented across sectors such as education, healthcare, agriculture, digital literacy, law enforcement, and disaster management for inclusive and holistic development.

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY GOVERNMENT OF INDIA

Digital India Power To Empower

Architecting e-Government

Training Programme on Information & Cyber Security

17th - 18th March 2023 (The Abduz, Leh)

E-HACK
CYBER SECURITY SUMMIT

The Cyber Security Summit is a premier global platform held across 10+ cities and multiple continents, bringing together top executives, thought leaders, and visionaries in the cybersecurity domain. The summit offers unparalleled networking opportunities, in-depth insights, and peer-to-peer exchanges, empowering leaders to drive growth and innovation within the cybersecurity landscape.

In today's rapidly evolving business environment, organizations face increasing pressure to balance security resilience with strategic foresight. Amidst economic uncertainty, technological advancements, and shifting market dynamics, the summit's carefully curated agenda addresses these challenges head-on, providing actionable strategies in areas such as risk management, financial planning for cybersecurity, digital tools, and the development of sustainable security models.

As cyber threats become more frequent and sophisticated, the need for robust cybersecurity has never been clearer. Safeguarding critical systems and sensitive data is no longer optional; it is an imperative. As organizations increasingly adopt technologies like AI, IoT, and cloud computing, the need to bolster cybersecurity defenses against emerging threats is paramount. Cybersecurity is essential for maintaining trust, protecting intellectual property, and ensuring business continuity.

The summit emphasizes the importance of security frameworks that evolve with the digital landscape, equipping leaders with the tools and knowledge to proactively defend their organizations against the ever-present risk of cyberattacks.

MESSAGE *for small*

No matter your background or skill level, SYTECH LABS Summits give you the chance to learn, connect, and share with cybersecurity professionals from around the globe.

Enjoy world-class content from industry practitioners on the frontlines, and walk away with actionable information, a fresh perspective, and new tools that you can immediately leverage in your work to protect your organization from ever-evolving threats.

SRI JD LAKSHMI NARAYANA SIR, IPS
Ex-CBI JOINT DIRECTOR

SYTECH LABS PRESENTING

CYBER SECURITY SUMMIT "E-HACK"

HACK THE HACKER BEFORE THEY HACK YOU

CYBER SECURITY

Cybersecurity is the practice of protecting computers, networks, systems, and data from cyber threats such as hacking, malware, phishing, and unauthorized access. Its main goal is to keep digital information confidential (private), accurate (unchanged), and available (accessible when needed).

CYBER FORENSIC

Cyber Forensics (also called Computer Forensics or Digital Forensics) is the process of collecting, analyzing, and preserving digital evidence from computers, mobile devices, networks, and cloud systems in a way that can be presented in a court of law.

It is widely used in cybercrime investigations, corporate fraud detection, and legal proceedings.

VAPT AND WAPT

Different businesses cover up digital assets, for instance, they perform Web Application Penetration Testing (WAPT) and Vulnerability Assessment and Penetration Testing (VAPT). Both methodologies try to find and eliminate security vulnerabilities with different aims, scopes, and executions.

SYTECH LABS INDUSTRIAL VISIT TO
CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD
BPRD, GOVERNMENT OF INDIA.

SYTECH LABS INDUSTRY VISIT

An industrial visit to a cyber forensic lab offers practical insight into digital forensics tools and techniques used in cybercrime investigations, covering areas like disk, mobile, and network forensics. During these visits, students learn about the identification, preservation, analysis, and documentation of digital evidence from devices such as computers, mobile phones, and the cloud.

WHAT TO EXPECT FROM AN INDUSTRIAL VISIT

Exposure to Tools and Techniques:
You'll see and learn about specialized software for digital forensics, including tools for disk imaging, data recovery, and mobile forensics.

Understanding the Forensic Process:
- The visit will likely cover the key steps of digital forensics: identification, preservation, analysis, documentation, and presentation of digital evidence.

Real-World Application:
- You'll gain an understanding of how these processes are applied to investigate cybercrimes, collect evidence from digital devices, and support law enforcement.

STUDENT EXPERIENCING IN LIVE FORENSICS

Experiencing live forensics involves conducting digital investigations on operational computer systems to collect volatile data, such as running processes and network connections, in real-time to detect ongoing threats or fraudulent activities. This requires specialized tools to acquire data like memory dumps without disrupting system function, and offers insights into live cyberattacks, though it presents challenges like potential evidence alteration and the need for specialized expertise to analyze dynamic, non-reproducible snapshots of a system.

- **Real-time Data Collection:**
  Live forensics focuses on gathering information from a system while it's running, making it crucial for understanding dynamic events and active threats.

- **Volatile Data Capture:**
  The primary goal is to capture volatile data – information that is lost when the system is shut down – such as active processes, open files, and network connections.

IN CHAIR WITH SRI. SALMANTAJ PATIL, IPS, DIRECTOR OF CDTI, DR.SRIRAM BIRUDAVOLU
CEO OF CYBER SECURITY CENTRE OF EXCELLENCE (DSCI) AND OTHER OFFICIALS WITH SRI LANKAN OFFICERS

SRI LANKA

HOURS OF WONDER

Combating towards the international border of cybercrime investigation and mitigation.

Combating cross-border cybercrime requires a robust international framework, including standardized laws, enhanced information sharing, and coordinated law enforcement efforts to overcome the jurisdictional challenges posed by the internet's borderless nature. Key strategies include establishing new treaties like the UN Convention on Cybercrime, strengthening existing mechanisms such as Interpol and Mutual Legal Assistance Treaties (MLATs), fostering public-private partnerships, and building capacity in developing nations to address the growing threat.

International cyber crimes are illegal activities conducted via the internet or digital systems across borders. Since cybercrime is not restricted by geography, criminals often operate from one country and target victims in another, making global cooperation and legal frameworks essential.

परिवर्तन PARIVARTAN

13th to 25th Sep' 2021

MID-CAREER TRAINING PROGRAMME

- Training & Development Department

MIDHANI

TECHNOLOGICAL EXPERT IN AEROSPACE

INTERACTING WITH THE OFFICIALS DURING MID-CARRIER TRAINING PROGRAM

The overall objective of the training programme was designed with a frame work to ensure that participants of middle level management build their core competencies and enhance their skills and area of expertise to utilize the same for their organization development and prevention from cyber attacks.

- Alongside land, sea, air, and space, cyberspace is now recognized as a critical warfighting domain.
- Modern defence forces must be prepared for cyberattacks that can cripple military systems without firing a bullet.

Understanding and combating cybercrime is vital for defence forces to protect national sovereignty, secure military operations, and prepare for the future of digital warfare. Cybercrime is no longer just a law-enforcement issue

— it's a strategic defence priority.

ADMINISTRATIVE STAFF COLLEGE OF INDIA
ASCI

ITS ALL ABOUT MALWARE ATTACKS

IN CHAIR DR.GULSAN RAI SIR, FORMER NATIONAL CYBER SECURITY COORDINATOR, FORMER DIRECTOR-GENERAL. CERT-IN (INDIAN COMPUTER EMERGENCY RESPONSE).

"Consider all tabulation systems infected by bad actors until a third party, not affiliated with the manufacturer or election officials, proves they are secure."

"A single spear-phishing email carrying a slightly altered malware can bypass multi-million dollar enterprise security solutions if an adversary deceives a cyber-hygienically apathetic employee into opening the attachment or clicking a malicious link and thereby compromising the entire network."

The practice of examining harmful software (malware) to learn about its traits, actions, intent, and source in order to strengthen defenses against online threats is known as malware analysis. In order to help security experts create signatures, fix vulnerabilities, and efficiently handle incldents, it uses techniques including static analysis, which involves looking at code without running it, and dynamic analysis, which involves watching how it behaves in a controlled setting.

- Its behavior (what it does).
- Its purpose (data theft, system disruption, persistence, etc.).
- Its origin and indicators of compromise (IOCs).

The goal is to improve threat detection, incident response, and defense strategies.

BANKING FINANCIAL SERVICES AND INSURANCE

BFSI

FIND YOUR SOLUTION FOR FINANCIAL FRAUDS

The BFSI sector is a prime target for cyber criminals because of its high-value data, financial assets, and customer trust. Protecting systems, networks, and information is crucial for business continuity and regulatory compliance.

Cybersecurity in BFSI is not just about deploying firewalls and anti-virus—it requires a multi-layered defense strategy, continuous monitoring, and awareness programs for both employees and customers.

In order to find solutions for phishing and social engineering, ransomware attacks, insider threats, API and their party risk, threat vectors, DDOS attacks, identity theft, and frauds, officials from various banking, finance, insurance, and service sectors interacted at an event hosted by the Administrative Staff College of India in Hyderabad.

Regulatory & Compliance Requirements

- RBI Guidelines on Cybersecurity Framework (India-specific)
- PCI-DSS (for payment card data security)
- GDPR (if dealing with EU customers)
- ISO 27001 / NIST CSF for information security management

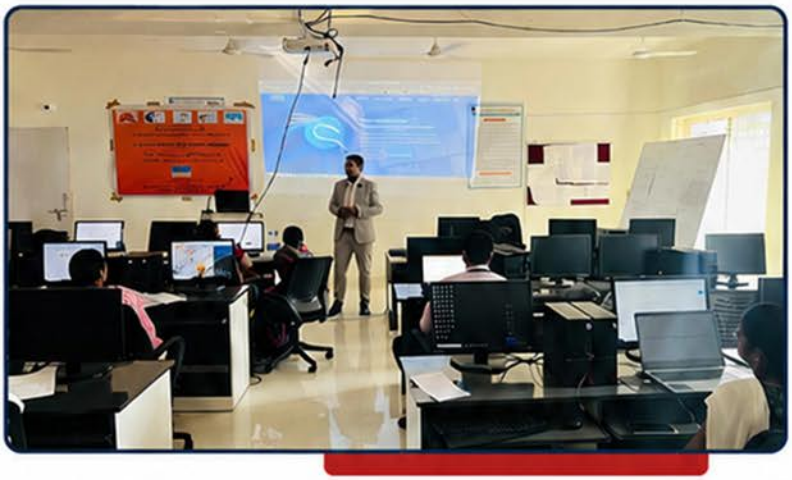
> IT and cybersecurity departments have been isolated in the past, but we have learned that we need to coordinate with others to secure banking groups.

In an era defined by rapid technological evolution, the Banking, Financial Services, and Insurance (BFSI) sector stands at the forefront of innovation, playing a pivotal role in the economic landscape. However, with the relentless advancement of technology comes the persistent threat of cyberattacks, targeting institutions for financial gain and operational disruption.

CYBER SECURITY FACULTY DEVELOPMENT PROGRAMS

The FDP is designed to enhance the knowledge and skills of faculty members in cybersecurity. It aims to equip them with the tools and insights needed to effectively teach and guide students in these rapidly evolving areas.

A Faculty Development Program (FDP) on Cyber security and Digital Ethics for Global Safety would aim to provide educators and professionals with a comprehensive understanding of the various cyber security principles and digital ethics that can be leveraged to ensure global safety in an increasingly interconnected world. This hybrid FDP would be valuable for educators looking to integrate cyber security and ethical frameworks into their curriculum, as well as for professionals seeking to enhance their skills in safeguarding digital infrastructure, mitigating cyber threats, and promoting responsible technology use.



A faculty development program (FDP) in cyber security provides educators with the knowledge and skills to teach and integrate cyber security concepts into their curricula. These programs cover topics like fundamental principles, threat detection, incident response, digital forensics, and ethical hacking. Key objectives include enhancing faculty expertise, preparing students for the digital age, fostering a culture of cybersecurity, and incorporating emerging threats and technologies.

CYBER WARRIORS, SPECIAL OPERATION TEAM & CENTRAL CRIME STATION

FIGHTING AGAINST ECONOMIC OFFENCE

A cyberwarrior refers to an individual who participates in cyberwarfare, motivated either by personal, patriotic, or religious reasons. While the term is often used to describe people who perform attacks on computer systems, cyberwarriors also include the defense force employed by governments that was trained to build their skills in tackling crimes.

COMBATING TRACES OF CYBER CRIMES

A cyberwarrior refers to an individual who participates in cyberwarfare, motivated either by personal, patriotic, or religious reasons. While the term is often used to describe people who perform attacks on computer systems, cyberwarriors also include the defense force employed by governments and businesses.

BUILDING CYBER COPS TO CYBER WARRIORS






Success Achievement Recognition

"WITHOUT CONTINUAL GROWTH AND PROGRESS, SUCH WORDS AS IMPROVEMENT, ACHIEVEMENT, AND SUCCESS HAVE NO MEANING. HAPPINESS DOES NOT COME FROM DOING EASY WORK BUT FROM THE AFTERGLOW OF SATISFACTION THAT COMES AFTER THE ACHIEVEMENT OF A DIFFICULT TASK THAT DEMANDED OUR BEST."

RAILWAY PROTECTION FORCE (RPF)

LATEST TECHNIQUES AND METHODS

With an emphasis on topics like e-touting, human trafficking, and data analysis utilizing cutting-edge techniques, RPF Cybercrime training entails specific courses and ongoing skill development to counteract increasing digital threats on railroads.

CYBER SURVEILLANCE.

Through programs provided by Sytech Labs, staff members receive training in digital forensics, social media analytics, and cyber surveillance.

- Advanced Training Programs
- Digital Forensics Expertise
- Data Analysis & Threat Detection
- Building Skills. Strengthening Security.

TAMILNADU POLICE ACADEMY, VANDALUR, CHENNAI

Two Days Capacity Building Course on
"A workshop on the use of Artificial Intelligence and Machine Learning"
28. 10. 2025 TO 29. 10. 2025

EMPOWERING
LAW ENFORCEMENT

The rapid growth of information technology and digital connectivity has transformed modern society, but it has also led to a sharp rise in cyber crimes such as online fraud, identity theft, hacking, cyberstalking, ransomware attacks, and data breaches. These crimes are often complex, borderless, and technology-driven, making traditional policing methods insufficient. Therefore, empowering law enforcement agencies for effective cyber crime investigation has become a critical necessity.

Empowering law enforcement refers to strengthening their legal authority, technical capability, institutional support, and operational efficiency to prevent, detect, investigate, and prosecute cyber crimes successfully.

STRENGTHENING LEGAL AUTHORITY | ENHANCING TECHNICAL CAPABILITY | INSTITUTIONAL SUPPORT | IMPROVING OPERATIONAL EFFICIENCY | EFFECTIVE INVESTIGATION & PROSECUTION

WHY MILITARY MUST FOCUS ON CYBER SECURITY, MORE IMPORTANT THAN EVER BEFORE

The Prime Objective of the Indian Cyber Army is to establish a Professional Platform of understanding and thereby carrying out the development of cyber defence skills which in-turn will protect citizens, businesses, critical infrastructures of the state, and e-governance by establishing a collaborative platform for cybersecurity to provide a secure cyberspace to the society.

When we think of potential threats against commercial entities, the first thought is industry competitors wanting to steal company secrets and proprietary information. The military has secrets that, if leaked, could damage the security of the entire nation. So, their number one threat is potentially bad foreign actors wanting to learn military secrets, tactics, and plans. National defence is central to protecting the territorial and political sovereignty of our republic. This defence is primarily provided by the military (Army, Navy and Air Force), with its soldier-and-weapon capability.

The effectiveness of military operations is finally based on the backup that the nation provides with its infrastructural, economic and political resources. Boots-on-the-ground in real-time combat situations cannot succeed without cyber-dependent operations and logistics. Thus there is a need for both offensive and defensive cyber capability and this is intimately linked with the cyber capability of the nation.

> *"THERE ARE REAL THREATS TO NATIONAL SECURITY FROM LOSS, LEAKAGE OR CORRUPTION OF DATA WHETHER DUE TO IGNORANCE, INADVERTENCE OR CYBERATTACK..."*

BUILDING SKILLS, STRENGTHENING DEFENCES

AWARENESS TODAY, SECURITY TOMORROW

TRAINING INDIAN ARMY OFFICIALS ON CYBER SECURITY, CYBER CRIMES, THREAT MANAGEMENT SYSTEM AGAINST DEFENCE AND CYBER WARFARE TOOLS AT MILITARY COLLEGE OF ELECTRONICS & MECHANICAL ENGINEERING (MCEME), HYDERABAD

The effectiveness of military operations is finally based on the backup that the nation provides with its infrastructural, economic and political resources. Boots-on-the-ground in real-time combat-situations cannot succeed without cyber-dependent operations and logistics. Thus there is a need for both offensive and defensive cyber capability and this is intimately linked with the cyber capability of the nation.

The larger picture requires that data systems which include the bits and bytes which every civil and military computer stores, uses and processes, the enabling software, the basic hardware and the human resources which are the final users, are secure against loss, corruption, theft and infiltration. Thus, there are real threats to national security from loss, leakage or corruption of data whether due to ignorance, inadvertence or cyber attack. This calls for policy and coordination at the highest level, namely, the National Security Council (NSC).

Security of data at government or military levels is not unlike the privacy of personal data at the level of the individual. When the government stores and handles personal data of millions of its citizens in a national database, a cyber attack on such a database is an attack on national sovereignty.

THREATS TO INTER-CONNECTED DATABASES

In an age of exploding data, information and knowledge, both human and machine, cyber security is as much a necessity for personal privacy as it is for internal and external national security or for day-to-day economic activities and operation of social and economic infrastructure systems.

Cyber security also constitutes the defensive part of modern warfare which is intimately connected with the blood-and-guts, on-the-ground military operations. Thus, the threats to privacy and to national security from loss, leakage or corruption of data whether due to ignorance, inadvertence or cyber attack, need to be understood clearly.

TRAINED VARIOUS STATE POLICE OFFICERS OF INDIA, JUDICIAL OFFICERS AND PUBLIC PROSECUTORS ON CYBER CRIME INVESTIGATION AND CYBER LAW AT CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Cyber crime has an expansive definition that includes any crime conducted via the Internet, network or digital device. Capturing digital evidence, such as that found on cellular phones, GPS devices, computers, tablets and network servers, is crucial to investigating and solving cyber crimes. Strong cyber crime investigative capabilities are also critical for solving traditional crime.

We describe the basic steps necessary when conducting the investigation, steps required to identify potential digital evidence, and how to work with different kinds of digital evidence (e.g. mobile devices, social media, IP addresses, etc).

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD
Course on "Handling CCTV Footages & DVR/NVR Forensic" and Use Of NetworkFootage"

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD
Course on "Protection of Data and Digital Public Goods"

TRAINING OFFICERS ON CYBER CRIME PROTOCOL

Chiefs should ensure that officers, investigators, and other relevant personnel receive regular training on handling cyber crimes.

CYBER CRIME POLICIES

Departments should develop policies and protocols for handling cyber crime investigations and what to do in case the agency is the victim of a hacking attack.

JURISDICTIONAL ISSUES

Cyber crime frequently crosses state and national borders. Chiefs should work with their federal law enforcement partners & local prosecutors to understand the jurisdictional issues involved with cyber crimes.

ENSURING OFFICER/INVESTIGATORS UNDERSTAND DIGITAL EVIDENCE

Chiefs need to be aware of the wide variety of digital evidence their officers and investigators handle, and ensure that evidence is properly processed and stored.

BUILDING CAPACITY
Strengthening skills and competencies for cyber investigations.

ENHANCING KNOWLEDGE
Keeping up with emerging cyber trends and laws.

IMPROVING INVESTIGATIONS
Using the right tools and techniques for effective results.

SAFER SOCIETY
Collaborative efforts for a secure digital future.

EMPOWERING OFFICERS THROUGH EXPERT TRAINING

ENHANCING CAPABILITIES WITH ADVANCED TECHNOLOGY

STRENGTHENING TEAMWORK FOR A SECURE TOMORROW

CYBER AWARENESS | SKILLED PROFESSIONALS | DIGITAL FORENSICS | STRONGER INVESTIGATIONS

> *"SOURCES OF DIGITAL EVIDENCE MAY NOT ALWAYS BE AS EASY TO RECOGNIZE AS A COMPUTER OR CELL PHONE FOUND AT THE SCENE."*

"It's important for all Police officers to understand cyber security as fully as possible. By doing so, they can develop their Knowledge in this increasingly important area, improving security in both their professional and personal lives."

When conducting a cybercrime investigation, normal investigative methods are still important. Asking who, what, where, when, why and how questions is still important.

DIGITAL EVIDENCE

- Digital evidence has become a ubiquitous part of criminal investigations with a presence that extends well beyond computer-specific crime. Frequent contact with digital devices in every facet of life produces so called 'digital exhaust' that can yield important clues regarding associations, location, and intent of both victims and suspects.
- Sources of digital evidence may not always be as easy to recognize as a computer or cell phone found at the scene. Automobile navigation systems, video game consoles and other networked devices can also contain extremely important data. Similarly, online user accounts without any physical connection to a crime scene can yield important information about offline activities.
- Recognizing and preserving digital evidence is only one intersection with the lifecycle of a criminal investigation.
- Technical skills and infrastructure must be planned for in advance in order to field robust capabilities that can respond to investigative needs in a timely fashion.
- Coordination with other elements of the criminal justice system such as prosecutors, defense attorneys and judges are also crucial for employing digital evidence towards a successful prosecution.

RECOVERING DIGITAL EVIDENCE (DIGITAL FORENSICS)

Recovering and analyzing data and material obtained from electronic devices and cloud-based services, also known as digital forensics, can provide significant leads and digital evidence. While digital forensic analysts are responsible for conducting in-depth investigations of devices, first responders also play an important role in ensuring that any devices, and their content, are properly recovered and preserved.

CONDUCTING HANDS ON CYBER CRIME INVESTIGATION, DATA PRESERVING, COLLECTION OF DIGITAL EVIDENCE TO VARIOUS STATE POLICE OF INDIA AT POLICE STATE HEAD QUARTERS

LAW ENFORCEMENT OFFICERS TRAINED TO TACKLE CYBERCRIME

As technologies become ever more sophisticated, so too do the modus operandi of criminals, who are increasingly using information and communication technologies to carry out such illegal activities as fraud, online child sexual exploitation and abuse and phishing, to name only a few.

Cybercrime, also known as computer crime, e-crime, hi-tech crime or electronic crime, generally refers to any criminal activity in which a computer or network is the source, tool, target or place of a crime. Such crimes may be divided broadly into two categories: the first covers crimes that target computer networks or devices directly, while the second refers to those facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

> ***"Digital evidence preservation and maintenance should, at a minimum, follow agency standards and protocols."***

Practical session on digital evidence handling and investigation.

Certificates and awareness materials distributed to participants.

Expert guidance on cyber laws and investigation techniques.

TRAINING CUSTOMS AND COMMERCIAL TAX OFFICERS ON DATA EXTRACTION OF INFORMATION FROM DIGITAL DEVICES & CYBER SECURITY AT NATIONAL ACADEMY OF CUSTOMS, INDIRECT TAXES AND NARCOTICS(NACIN), VISAKHAPATNAM, ANDHRA PRADESH.

TAX PRACTITIONERS AND THE DIGITAL ADVANTAGE

Tax practitioners have learned that they possess something that a new breed of criminals, namely cybercriminals, desire information.

The storage of taxpayer data in the Cloud and on open network systems provides a competitive advantage to tax practitioners to access. Client information quickly and transmit data efficiently to the Internal Revenue Service and other state authorities on behalf of their clients.

CYBERCRIMINALS ADAPT TO A CHANGING ENVIRONMENT

The cybercriminals have evolved, adapted, and specialized in infiltrating electronic devices and exploiting the information stored therein. Additionally, the criminals have refined both who they target and how they pursue their ill-gotten gains.

As new defenses are erected that mitigate specific fraud schemes, cybercriminals develop new uses or avenues that attack different participants in the tax return preparation process that may offer an easier path to success—the weakest link in the data security chain.

> *Preservation of evidence has become more complicated in recent years because of society's increasing reliance upon electronic communications.*

WHY SECURITY AWARENESS TRAINING IS IMPORTANT TO EVERY ORGANIZATION

According to Verizon's 2018 Data Breach Investigations Report, phishing or other forms of social engineering cause **93%** of all data breaches. In order for phishing or social engineering attacks to be successful, the attacker needs a target to take the bait. Your employees often are the targets, aka the fish that bite. Employers must make employees aware of the risks associated with clicking on a link in a phishing email, downloading an attachment from an unknown sender or responding to requests for credential/login information or other data.

EDUCATION IS THE FIRST LINE OF DEFENSE

The only defense against such attacks is education — or in industry terms, "Security Awareness Training" — and falls squarely under the aegis of cybersecurity training. Because of the rapidly changing environment and long list of vulnerabilities, security awareness training also cannot involve a one-shot approach or a "set it and forget it" program.

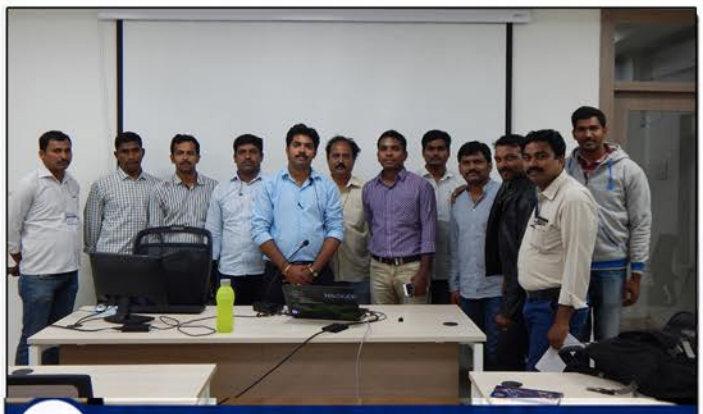
PRESERVATION OF EVIDENCE – A CRITICAL CONCERN

Preservation of evidence has become more complicated in recent years because of society's increased reliance on electronic communication. Electronic versions of documents are more transient and subject to alteration. Ironically, they are also more permanent, residing on the hard drives of many computer users for years.

Versions of documents are frequently and routinely modified, overwritten, and perhaps deleted by computerized automatic deletion programs. Such events can become a serious issue in a dispute resolution process. The legal system has come up with a name for loss or destruction of evidence known as "spoliation."

Training on Cyber Crime Investigation to Hyderabad Cyber Cell, Telangana Police.

Hands-on training on cyber crime investigation techniques and digital forensics.



Interactive sessions with experts and officials from Telangana Police.

Practical exposure to tools and technologies used in cyber crime analysis.

Strengthening investigation capabilities through practical knowledge.

Cyber Security Tranning for Collectorates in association with Telangana Academy for Skill and Knowledge (TASK)

Expert-led sessions on cyber security awareness and best practices.

Building awareness on cyber threats, prevention and safe digital practices.

Capacity building for officials to handle cyber incidents effectively.

Empowering departments to enhance cyber resilience and data security.

Digital India Programs

MOU's with Various Organisations

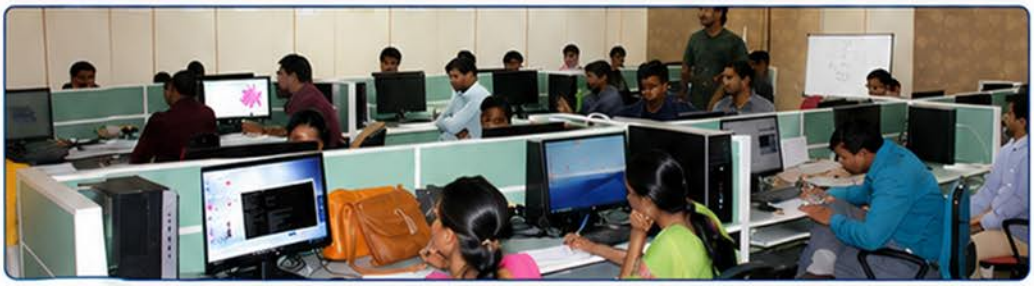
Cyber Security and its Best Practices at

Expert Sessions on Cyber Laws and Security

Awareness on Cyber Ethics and Legal Framework

Capacity Building for Public Prosecutors

Training Programme on Networking & Security



MCRHRDI (Govt of Telangana) & APHRDI (Govt of AP)

Taken steps to raise awareness about cyber crimes, including issuing alerts and advisories, and training law enforcement, prosecutors, and judicial officers. These steps are intended to prevent cyber crimes and speed up investigations.

Preserving digital evidence involves a number of steps, including:

- **Documenting the device:** Take pictures of the device from all sides to document its condition and location. Note any dents, scratches, or other physical blemishes.
- **Maintaining the original file:** Use drive imaging to maintain the original file.
- **Chain of custody:** Ensure proper chain of custody for both hardware and data. This includes not storing the device in an open access area and not leaving it unattended when it is being worked on.
- **Hash values:** Verify the authenticity and integrity of the image as an exact duplicate of the original media. Hash values are critical because altering even the smallest bit of data will generate a completely new hash value.
- **Forensic image:** Create a forensic image. This can take hours, if not days to complete.
- **Chain of custody forms:** Document all the steps conducted during the transfer of media and the evidence on the Chain of Custody (CoC) forms. Capture signatures, date, and time upon the media handoff.

Dr. MCR HUMAN RESOURCE DEVELOPMENT INSTITUTE OF TELANGANA
Training Progrmme on "Cyber Crime & Cyber Law Awareness for Public Prosecutors"
in Collaboration with Crime Investigation Department,Telangana (Batch III)
From : 06-02-2023 to 08-02-2023

CYBER SECURITY: CORPORATE TRAINING

WHY

"Every organization is responsible for ensuring Cyber Security. The ability to protect its information systems from impairment or even theft is essential to success. Implementing effective Security measures will not only offer liability protection; it will also increase efficiency and productivity."

“WE

With our Cyber Security trainings your participants will understand the different types of malware and security breaches. Develop effective prevention methods which will increase overall security. They will also understand the basic concepts associated with Cyber Security and what a company needs to stay secure.

“Cyber vulnerability is not only from critical hardware; sub-critical hardware is also vulnerable when purchased from international vendors...”

KIA AND TATA

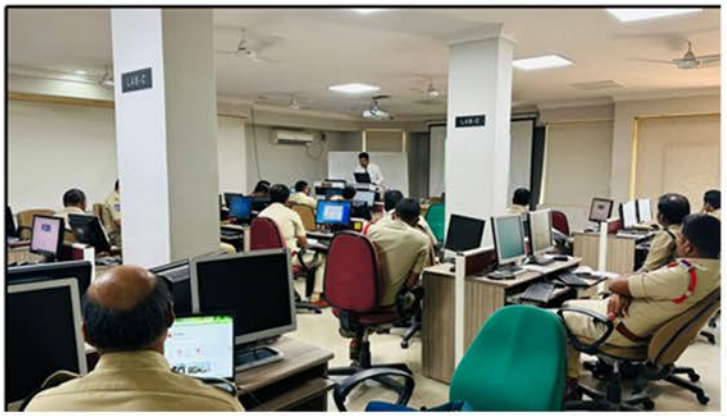
Cybersecurity scope, current trends, difficulties,
and preventive measures for KIA and TATA Motors employees.

Training Judges of Telangana State at RBVRR Police Academy (TSPA) on Latest Cyber Crimes Trends.




Training to Various Districts Police Officers of Telangana at RBVRR Telangana State Police Academy(TSPA)



Awareness Programmes on Cyber Crimes
at Various Schools Across India

Spreading Awareness,
Building a Safer Digital Future

Empowering Students with Knowledge on Cyber Safety

Interactive Sessions, Lasting Impact

Expert Insights for a Cyber-Secure Tomorrow

Engaging Young Minds, Creating Awareness

Uniting Schools and Communities for Awareness

Together Towards a Cyber-Safe India

Awareness today,
a safer tomorrow.

Workshops and Seminars
at Various Engineering Colleges
Across India

Empowering future engineers through insightful sessions, hands-on workshops, and inspiring interactions.

Interactive Session with Students

Hands-on Workshop in Progress

Engaged Audience, Eager Learners

Team with Faculty and Students

Expert Talk on Industry Trends

Knowledge Sharing Session

Building Connections, Inspiring Growth

Towards a Smarter, Skill-Ready Tomorrow

"Together, we are shaping the innovators of tomorrow.

Into Media

Sytech Labs: Enlightening Students & Professionals via Nonpareil Training & Consultancy

Besides the fact that Internet, the sophisticated creation of mankind, has eased the lives of people through diversified means, it has also evolved into a space posed with proliferating menaces that are incomprehensible even to cyber professionals. The most chaotic cyber-incidents like Shadow Brokers, WannaCry, & Cloudbleed in the recent times have triggered the cyber crime organizations to ardently work on eliminating these atrocities. As the cyber crime's jargon is getting updated each day with novel crimes and internet hacks, each organization in this realm must transform its strategy accordingly in order to resolve the crime with proficiency. Catering to this dire need by comprehending the criticality of perilous cyber-incidents, Sytech Labs extends its training centre & consultancy to a wide range of government officials from crime department, CID, CBI, IB, Defence, and many more on not just modifying their investigation strategy as per the cyber crime case, but also

Sandeep Mudalkar, Founder & CEO
With profound knowledge in Cyber Crime Investigation, Cyber Security, Internet Frauds and Cyber Law Consulting, Sandeep is renowned as one of the youngest Information Security and Cyber Crime Consultants in India for his unparalleled assistance in solving cyber crime cases and spreading awareness.

Offerings:
- *Cyber Crime Investigation & Consulting*
- *Information Security Training*
- *Seminars & Workshops*
- *Vulnerability Assessment & Penetration Testing (VA/PT)*
- *IT Security Consulting & Auditing*
- *Web Application Development*
- *Search Engine Optimization*
- *Network Solutions*

This Hacker is a Crime Fighter

Ethical hacker Sandeep Madhulkar helps corporations find loopholes in their web security systems and assists the police in fighting cyber crime By SWATI SHARMA

Sandeep Madulkar, 28, goes to work just like everyone else. The only difference being that while others are paid for producing work, he makes the moolah by pulling apart computer security systems. Hyderabad-based Sandeep is a professional hacker who tests the security systems at all types of workplaces—from small businesses and multinational corporations to police departments.

It all started when Sandeep's Orkut account was hacked. He was 18 and pursuing a post-graduate diploma in computer applications. Using Google, he discovered and learnt the art of hacking. He realised that his skills could be used for more constructive endeavours.

"I got curious when my account got hacked into. I began to explore but did not know there was potential for a career," he says. "I felt this would be the most challenging field, and now I am glad I took such a decision," he says about his entry into this field. In 2011, Sandeep founded his own cyber security and IT intelligence firm, Prediqnous, which has offices in Hyderabad, Warangal, Ahmedabad, Mumbai and even the UK.

But being an ethical hacker carries great responsibility too. An ethical hacker isn't a cyber criminal, though he knows well the art and science of hacking. He exercises his hacking expertise prudently for ethical concerns. With cyber attacks on the rise, it is Sandeep's job to expose a company's vulnerabilities and prevent any sort of data breach. Every enterprise is different; they have different business objectives, different ways of operations, different needs, and hence different website traffic patterns.

"As an ethical hacker, I do not hack sites for malicious purpose. I hack them to check vulnerabilities. If I find any, I report it to the site owners and ask them to fix it as soon as possible to prevent themselves from attacks," says the digital Bond.

Sandeep believes the best security is education and awareness. "Firms often don't realise the value and importance of data." Sandeep's success has already been recognised by business experts in the IT security sector and the police department, who believe the key to ethical hacking, is to adopt the thinking of a hi-tech thief.

The first assignment that came Sandeep's way was by accident too. "One day my father, MK Vishwanatham, mentioned a case that the police wanted some help in. A jilted boyfriend had created a fake email account and had circulated inappropriate mails to his ex-girlfriend's relatives. I hacked the account, retrieved the IP address and gave it to the cyber crime cell. My job is only to hand over the IP address (in case of emails and online accounts), IMEI (for mobiles) and MAC address and serial number (for laptops) to the police. It helps them trace criminals," explains Sandeep.

Apart from educational institutes, Sandeep also trains police personnel on the latest technology essential to solving cyber crimes. "At the awareness programmes, I mainly highlight some of the common loopholes in a system," he says.

To-date Sandeep has hacked over 1,000 websites including big names, organisations and political leaders. "I have clients all over India that hire me to break in," he says. However, he cannot divulge the names. "Some names of the websites will come as a surprise to you but as the information should be confidential, I will not reveal the site names," he smiles.

These days, Sandeep is still hacking, but with the official approval of the companies he targets. Ask him whether he has been ever caught, he shrugs his shoulders and says, "To tell the truth, even to my surprise I have never been caught. I do not want to face this experience in my life. I am happy to serve my nation by preventing such attacks," he beams.

Apart from educational institutes, Sandeep also trains police personnel on the latest technology essential for solving cyber crimes

> "Internet vigilantism can dramatically change the consequences for offenders.
> — SANDEEP MUDALKAR, *Cyber crime investigator/consultant*

మచ్చిక చేసుకొని..
ముంచేస్తారు..

CYBER SECURITY CONSULTANTS 2016

Sytech Labs: Prioritizing Data Security in the Digital Age

The firm prides itself for the Corporate Security training seminars & workshops it conducts to enhance the knowledge base around Cyber security

సైబర్ నేరాల సమర సైనికుడు!

CityHans | PEOPLE | WEDNESDAY | 12

Ethical hacker who helps protect nation

జ్యోతిష్మతిలో ముగిసిన జాతీయ సదస్సు

Sat, 04 August 2018
epaper.ntnews.com/c/30899629

SANDEEP MUDALKAR, *cybercrime investigator*

Mentors at home and work

While I've chosen my career out of my own interest, my father has been the one to always support my endeavours. Till date, he's my biggest mentor. When I was young, I remember going to my friends' place and Internet cafés to use the desktops there for my needs. However, my father, Mudalkar Kashi Vishwanatham (retired Divisional Forest Officer), eased it for me by buying me a desktop. He also ensured I enrolled into various computer programmes — which contributed to my career.

Fighting cyber crime

Sandeep Mudalkar is the go-to man for city's cyber cops. But he isn't just helping them nab criminals, he is also making them sensitive towards victims

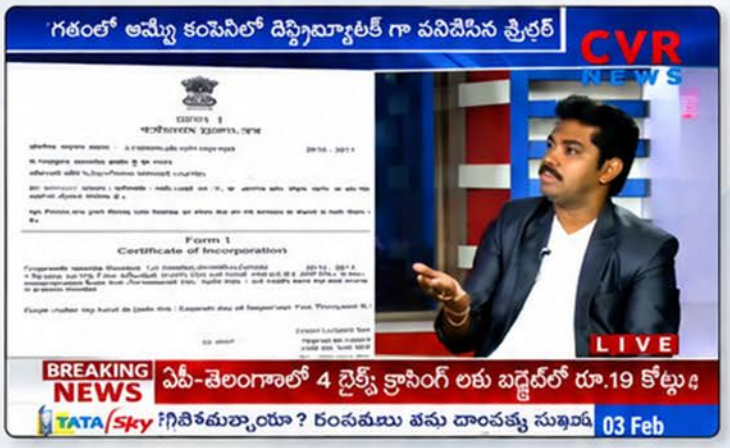
BARKHA KUMARI
DECCAN CHRONICLE

THE CASE FILE

- This February, a jilted lover circulated an image of his girlfriend with her husband along with his own photo.
- A real-estate owner got threat calls from his own number. It was traced back to his grudging business partner.
- In 2011, a boy killed his girlfriend and fled. The case was cracked only after the boy's laptop could be traced.
- In 2010, BSF in Gujarat got random mails from Afghanistan. Sandeep's team hacked over 100 mail accounts.

So far, Sandeep has solved 43 of the 82 cases handed to him by the cops since his first involvement in 2006

Electronic Media



OUR CYBER SECURITY COURSES

Industry-Relevant Skills • Hands-on Training • Globally Recognized Certifications • Career Focused Programs

01

Certified Cyber Resilience and Its Best Practices (CCRP)

Learn to build, strengthen and maintain organizational resilience against cyber threats. This course covers risk management, incident response, business continuity, disaster recovery and cyber resilience frameworks and best practices.

02

Certified Forensic and Operational Analyst (CFOA)

Master digital forensics and operational analysis techniques. Learn evidence collection, preservation, analysis, malware forensics, log analysis and reporting to support investigations and operational decisions.

03

Certified Cyber Resilience and Forensic Investigator (CRFI)

Combine cyber resilience strategies with forensic investigation skills. This course prepares you to investigate incidents, identify root causes and improve resilience through forensic insights and risk mitigation.

04

Certified Vulnerable Assessment & Its Penetration Testing (C-VAPT)

Learn to identify, assess and exploit vulnerabilities ethically. This course covers vulnerability assessment, penetration testing methodologies, tools, reporting and remediation to secure systems and applications.

05

Certified SOC Analyst (C-SOC- Level 1 & 2)

Become a skilled SOC Analyst and monitor, detect and respond to security incidents. Level 1 covers fundamentals and alert triage. Level 2 focuses on advanced threat hunting, incident analysis and response.

06

Certified Information System Security Expert (CISSE)

Gain in-depth knowledge of information security principles, governance, risk management, cryptography, access control and security architecture to become an information security expert.

07

Certified Network & Its Penetration Testing (CNPT)

Learn to secure networks by discovering vulnerabilities and exploiting them ethically. Covers network scanning, enumeration, exploitation, privilege escalation and reporting to strengthen network infrastructure.

08

Certified Mobile Pentest (CMP)

Master mobile application security testing on Android and iOS platforms. Learn mobile architecture, static & dynamic analysis, vulnerability assessment and exploitation to secure mobile applications.

09

Certified Web Application and Its Penetration Testing (C-WAPT)

Learn to find and exploit security flaws in web applications. Covers OWASP Top 10, reconnaissance, exploitation techniques, SQLi, XSS, CSRF, security misconfigurations and detailed reporting.

10

Certified Cyber Law (CCL)

Understand legal aspects of cyber crimes, data protection, privacy laws, IT Act, compliance, intellectual property rights and cyber laws to manage legal risks in the digital world.

11

Cyber Sense (CS)

Build awareness and safe digital habits to protect yourself and your organization. Learn about phishing awareness, password security, social engineering, safe browsing, ransomware protection and cybersecurity best practices for everyday digital life.

EXPERT INSTRUCTORS
Learn from industry professionals

HANDS-ON LABS
Practical learning with real-world tools

GLOBALLY RECOGNIZED CERTIFICATIONS
Boost your career with trusted credentials

CAREER FOCUSED
Job-ready skills for high-demand roles

WIDE RANGE OF COURSES
From beginner to advanced level

SECURE TODAY • PROTECT TOMORROW • LEAD THE FUTURE

SECURE TODAY, DEFEND TOMORROW

CYBERSECURITY & FORENSIC INTERNSHIPS PROGRAM

Hands-on experience.
Real-world impact.
Future-ready skills.

Our Cybersecurity & Forensic Internships Program is designed for curious minds who want to explore, learn, and make a difference in the digital world.

WHY INTERN WITH US?

LEARN FROM EXPERTS
Work alongside industry professionals and security experts.

REAL-WORLD EXPERIENCE
Solve real problems and work on live projects.

SKILL DEVELOPMENT
Build in-demand skills in cybersecurity and digital forensics.

CAREER GROWTH
Kickstart your career in one of the fastest-growing fields.

YOU'LL GAIN

- Knowledge of cybersecurity principles and threat landscape
- Hands-on with security tools and technologies
- Digital forensics and incident response experience
- Critical thinking and problem-solving skills
- A strong foundation for future opportunities

PROGRAM HIGHLIGHTS

CYBERSECURITY TRACK
Network Security | Ethical Hacking | Threat Intelligence | Security Operations

FORENSIC TRACK
Digital Forensics | Malware Analysis | Incident Response | Evidence Handling

MENTORSHIP & GUIDANCE
Personalized support to help you learn, grow and succeed.

FLEXIBLE & INCLUSIVE
Open to students from diverse backgrounds and academic streams.

> **Be the person who protects the digital world.**

YOUR JOURNEY STARTS HERE.

SECURE. ANALYZE. PROTECT.
MAKE AN IMPACT THAT MATTERS.

Learn | Explore | Analyze | Protect

APPLY NOW!

Scan the QR code or visit

www.sytechlabs.com/courses

to learn more and apply.

FOR MORE INFORMATION
+91-8497953761/460
info@sytechlabs.com
www.sytechlabs.com

CYBER SECURITY

ONLINE & OFFLINE CLASSES

LEARN. PRACTICE. PROTECT.

Build skills today. Secure the future.

PRACTICAL TRAINING
Real-world labs and simulations

EXPERT MENTORS
Learn from industry professionals

CERTIFICATION SUPPORT
Guidance for top industry certifications

CAREER BOOST
Build skills that employers value

ONLINE CLASSES

LEARN FROM ANYWHERE

- Live interactive sessions
- Flexible schedule
- Recordings & study material
- Hands-on lab access
- Doubt clearing support

OFFLINE CLASSES

LEARN TOGETHER, GROW TOGETHER

- Classroom training
- Hands-on lab sessions
- Peer discussions
- Personalized guidance
- Better practical experience

WHAT YOU WILL LEARN

- Ethical Hacking
- Network Security
- Web Application Security
- SOC & SIEM Fundamentals
- Cloud Security
- Forensics & Incident Response

SECURE YOUR FUTURE.
GROW YOUR CAREER.

Cybersecurity is not just a skill, it's a superpower in the digital world. Start your journey with us today!

ENROLL NOW

Be a part of the future of cyber security.

www.sytechlabs.com | info@sytechlabs.com | +91-8497953761 | Hyderabad, Telangana

OUR SERVICES

Secure Today, Safer Tomorrow

Empowering individuals and businesiess with trusted cybersecurity solutions.

TRAININGS ON CYBER SECURITY

Welcome to Cyber Web..!! It's Interesting Word to Step-In.!!

- Beginner to Advanced Courses
- Hands-on Practical Training
- Certified Cyber Security Experts
- Corporate & Individual Training

CYBER CRIME INVESTIGATION & CONSULTING

If you're victim of cyber crime activity, we're here to catch them.

- Digital Forensics
- Incident Response
- Fraud Investigation
- Consulting & Advisory

SOFTWARE DEVELOPMENT & SEO

Make your business global.!!

- Custom Software Development
- Web & Mobile Applications
- SEO & Digital Marketing
- Performance & Growth Focused

SEMINARS & WORKSHOPS

For College, School Students & Corporate

- Cyber Awareness Sessions
- Interactive Workshops
- Real-world Case Studies
- Career Guidance & Support

CYBER LAWS CONSULTING

For those who need legal advice.

- Cyber Law Advisory
- Legal Compliance Support
- Data Privacy & Protection
- Litigation & Dispute Guidance

WEB APPLICATION PENTESTING

Protect your business

- Vulnerability Assessment
- Penetration Testing
- Security Audits
- Detailed Reports & Fixes

EXPERT TEAM
Certified professionals with years of hands-on experience.

TRUST & CONFIDENTIALITY
We value your privacy and ensure complete data security.

24/7 SUPPORT
Our team is always ready to support you anytime.

RESULT DRIVEN
We deliver effective solutions that drive real results.

SECURING TODAY

PROTECTING TOMORROW

Stronger Defenses. Smarter Security. Safer Future.

Sytech® Labs

Strengthening Cyber Security

Private Limited

CERTIFICATIONS

- Cyber Resilience & It's Best Practices
- Cyber Resilience & Forensic Investigator
- Information System Security Expert
- Cyber Law
- Forensic & Operational Analyst
- VA/PT & WA/PT
- Certified SOC Analyst
- Network & Its Penetration Testing
- Cyber Sense

OUR SERVICES

CYBER CRIME INVESTIGATION & CONSULTING
If you're victim of cyber crime activity, we're here to catch them.

CYBER LAWS CONSULTING
For whom who need legal advice.

SOFTWARE DEVELOPMENT & SEO
Make your business global...!

TRAININGS ON CYBER SECURITY
Welcome to Cyber Web...!!
It's Interesting Word to Step-In...!!

SEMINARS & WORKSHOPS
For College & School Students

WEB APPLICATION PENTESTING
Protect your business

YOUR TRUST. OUR MISSION.

We deliver end-to-end cybersecurity solutions to safeguard your digital assets and keep your business future-ready.

Phone
+91-8497953460
+91-8497953761

Our Location
HYDERABAD
TELANGANA

Visit Us
www.sytechlabs.com
www.sandeepmudalkar.com
www.instagram.com/sytechlabs