GURU GOBIND SINGH
INDRAPRASTHA UNIVERSITY
NEW DELHI

SBIT TechMentors
Learn · Innovate · Lead

Enhance Your Career:

Step into the Cybersecurity World Projected to Grow at a 9.72% CAGR!

PG Level Advanced Certification Programme in

CYBERSECURITY & FORENSICS

Investigate and Protect: The Science of Cybersecurity and Forensics

9 MONTHS PROGRAMME

Only NAAC A++ Govt University Programme	Offline and Online Classes	Mentoring by Industry Experts	IP University Alumni Status

Exclusively designed for professionals in Mathematics, Science or Engineering

Admission Helpline : 9560361410 | www.techmentors.sbit.in | info.techmentors@sbit.in

Are YOU looking for an exceptional Education Experience that will reignite your mind ?

A programme where Innovation and Learning by doing are the presiding principles ?

Then come to the Source
There's only one: SBIT TechMentors


ACADEMIC BLOCK 1
SHRI RAM MURTI INSTITUTE OF TECHNOLOGY

Build Smart Systems. Build Your Career. Enroll in Cyber Security and Forensics !

"

$10.5T is estimated yearly cost of cybercrime in 2025

accenture

"

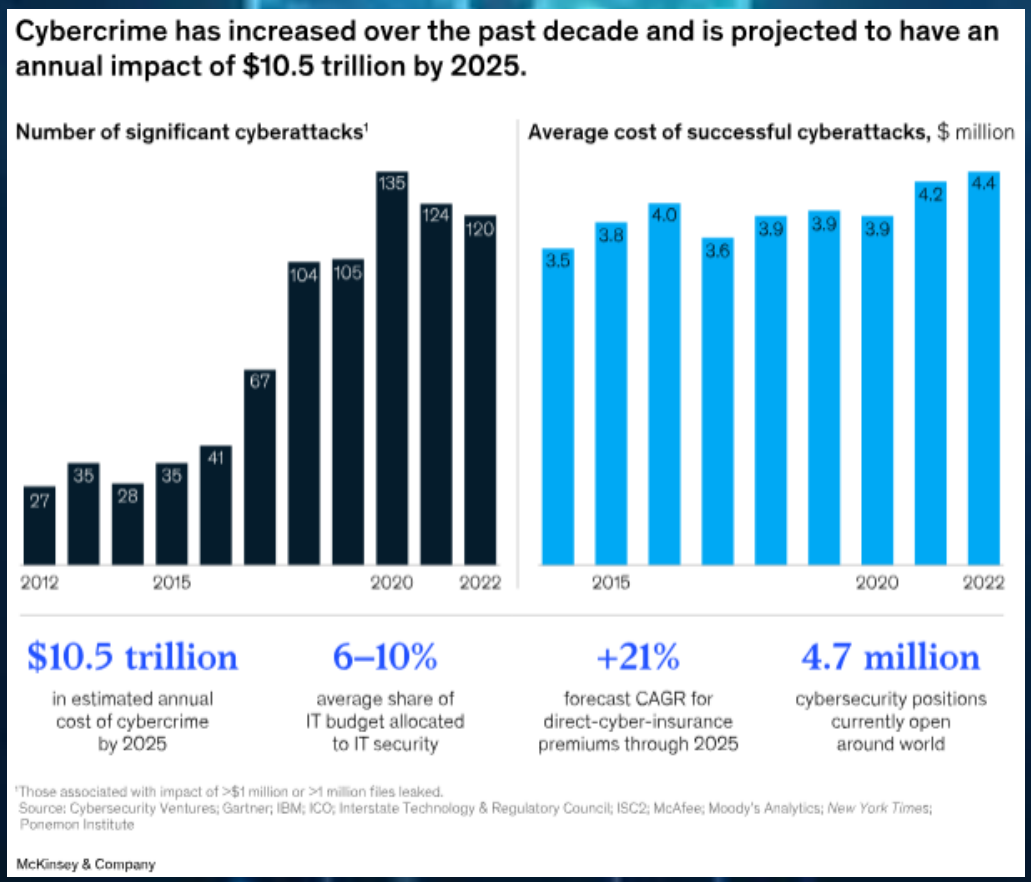
India's Cybersecurity spending to grow 16.4% in 2025

ET CISO.in
From The Economic Times

"

India's Digital Forensics Market Growth reached USD 450 Million in 2023

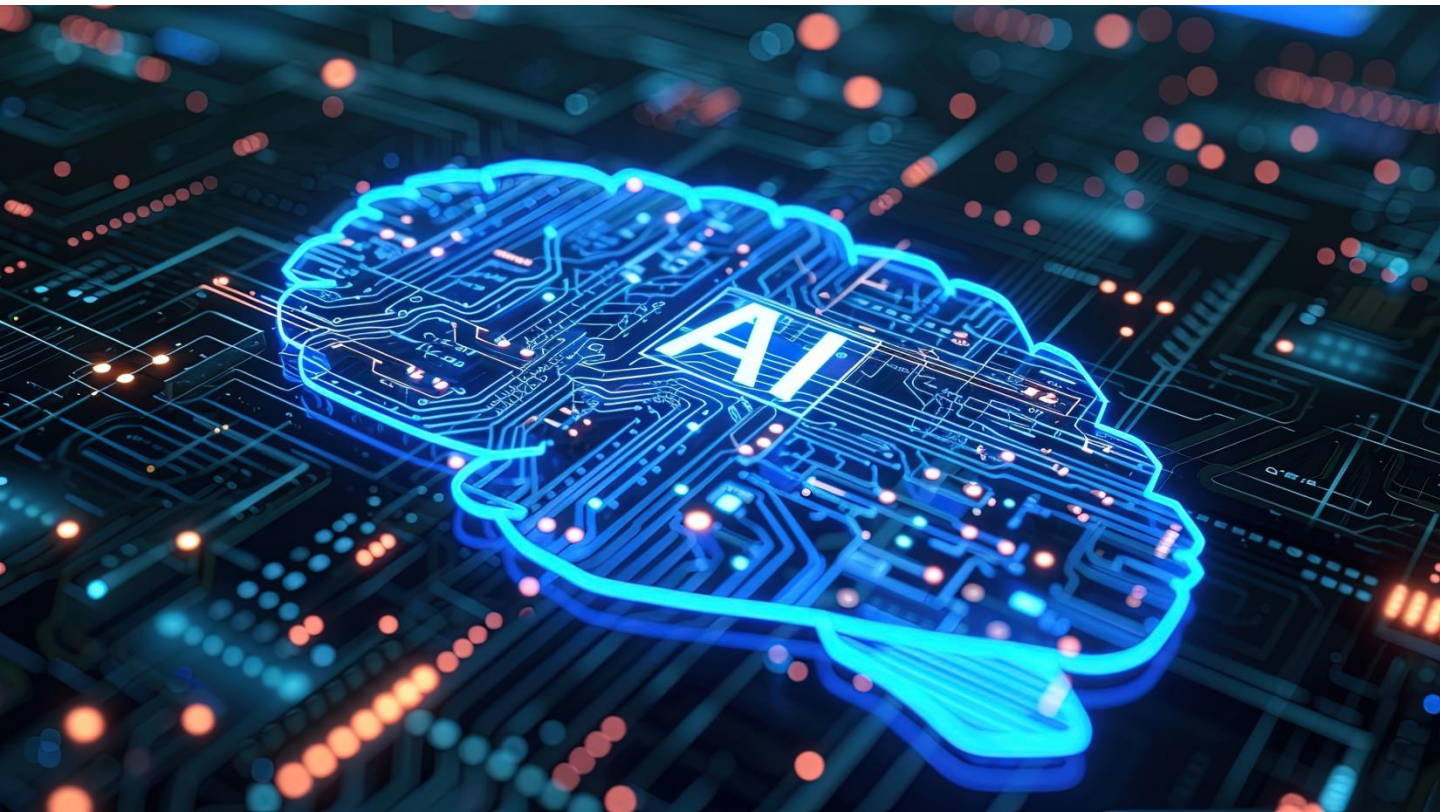
GlobeNewswire by notified



Trending Career Opportunities in Cyber Security and Forensics

About the Programme

- The Certification Course in Cyber Security and Forensics is offered by SBIT TechMentors in collaboration with GGS IP University.
- The 9-months weekend programme enables both aspiring and practicing Security professionals to build expertise in Cybersecurity and Digital Forensics.
- The programme covers the essential foundations of Cybersecurity and teaches students how to apply them in the real world effectively.
- The course is best suited for individuals with programming knowledge who want to create a practical understanding to identify vulnerabilities, implement robust security measures, and conduct thorough forensic investigations.



Key Features of the Programme

Experienced Instructors
Learn from industry professionals with real-world experience

Flexible Formats
Choose from online, in-person, or hybrid classes

NAAC A++ Govt University Programme
Only NAAC A++ Govt University to offer such programmes

Ideal Duration
9 months of duration is ideal for getting solid foundation

Industry-Relevant Curriculum
Course designed in collaboration with industry experts

Experiential Learning
Hands-on projects with integrated labs

Easy access to faculty
Dedicated faculty hours to address doubts and questions

Industry relevant projects
Significant weightage on industry relevant projects

Mentoring from Industry veterans
Guidance on finer aspects of technologies and further learning

Career Assistance
Benefit from job placement assistance and resume workshops

Programme Outcomes

By participating in this programme, you will:

- Comprehend key cybersecurity concepts and assess various cyber threats and vulnerabilities.
- Perform digital forensic investigations and analyze digital evidence across various platforms.
- Implement and manage network security measures, including firewalls, VPNs, and IDPS, and design secure network architectures.
- Apply secure software development practices and mitigate common application vulnerabilities.
- Implement cryptographic techniques for data protection and manage cryptographic keys effectively.
- Develop and execute incident response plans and analyze incidents to improve future responses.
- Build the foundational skills necessary for certifications like CISSP, CEH, and EnCE.
- Complete a capstone project that addresses a real-world cybersecurity or forensic problem and stay informed on emerging trends.

Re Imagine Education

Take Your Career to a Whole New Level

Its Not About the Degree
Its About You

At this point in your career, you don't need only a degree. you need an experience.
Follow our 4 edge Approach.

Engineering Futures of Excellence with Firm Foundations
Winning Edge for the NextGen

GGSIP University Edge

Guru Gobind Singh Indraprastha University (GGSIPU), established in 1998 by the Government of NCT of Delhi, is a State University of Delhi recognized by the University Grants Commission (UGC). The University is also globally recognized for its academic and research excellence and has earned prestigious accolades which include NAAC A++ Accreditation, the highest honour for academic distinction; a strong position in the QS World University Rankings 2025, securing 81st rank in Southern Asia; and a notable 80th position in the NIRF Rankings 2024. The University's rapid stride in global rankings has been acknowledged with the QS 'Rising Star' Award, while its unwavering commitment to research excellence has been honoured with the QS 'Performance Improvement Award', reaffirming its excellence in higher education.

GGSIPU offer a wide spectrum of multidisciplinary, professional and technical programs, spanning across Artificial Intelligence, Machine Learning, Robotics, Computer Science, Management, Law, Education, Journalism, Medicine (MBBS), Ayurveda and super-specialty medical courses, among others. The University actively promotes entrepreneurial initiatives and job creation through its innovative incubation centres and industry associations.

For more information, http://www.ipu.ac.in/

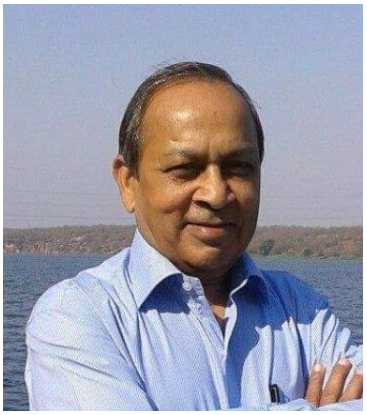
SBIT Advantage

Shri Balwant Institute of Technology (SBIT), established in 2006, is an AICTE approved Institute located in NCR Delhi and Affiliated with Guru Gobind Singh Indraprastha University (GGSIPU), New Delhi. SBIT offers full time undergraduate and postgraduate degree programmes in Engineering, Management and Computer Applications - B.Tech., BBA, MBA, BCA, MCA, B.Com.(H).

SBIT programmes are meticulously designed to equip students with the latest skills and knowledge, particularly in the high-demand fields Cyber Security and Forensics. Recognized among the Top 10 Colleges in India for AI, SBIT is renowned for its academic excellence and state-of-the-art infrastructure.

Over the last 19 years, SBIT has established a strong legacy of producing thousand of successful engineers and managers who have been placed in top companies like Apple, Amazon, TCS, and Deloitte across the globe. The Institute’s rigorous academic programmes combined with hands-on industry training and corporate mentorship from global leaders, have ensured that students are not only technically proficient but also equipped with the skills to excel in the professional world.

Academic Advisory Council



Prof. (Dr.) P C Jain
Former Principal, SRCC

Suresh Dutt Tripathi
Advisor, HR, Air India

Rajeev Dubey, Former
Group President, Mahindra

R Anand
Principal Consultant, HCL

Dr. Brijesh Kumar
Director (Planning), IGDTUW

Rajarshi Chakravorty
Centre Head, Amdocs

Dr. Asha Bhandarker
Former Prof., MDI

Dr. Nishant Sinha
Head, Times Internet

Dr. Amit Kumar Jain
Director, Delhi Metro

Academic Advisory Council

Rajneesh Singh
CTO, Simply HR

Prof. (Dr.) Dharmendra Singh
Director, IIIT Gandhinagar

Dr. Shrikant Ojha
Former Scientist 'H', DRDO

Prof. (Dr.) Vinod Kumar
HOD, CSE, DTU

Prof. (Dr.) A. K. Bhateja
Prof, IIT Delhi

Prof. (Dr.) V K Panchal
Former Scientist 'H', DRDO

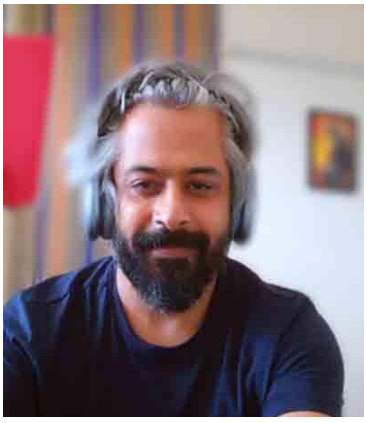
Mentorship Board

Gurpreet Sachdeva
Senior Director, Capgemini

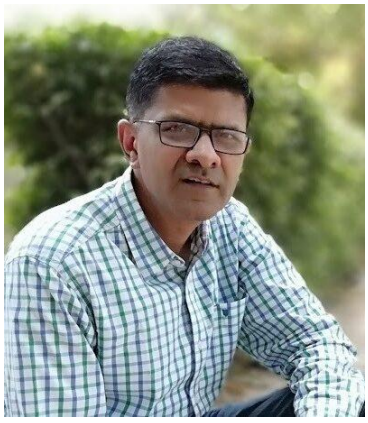
Nitin Gera, Co-founder
& COO, AiRo Digital Lab

Mohit Saxena, Co-founder
& CTO, InMobi Group

Dr Mohit Bhatnagar, Assoc.
Prof., Jindal Global University



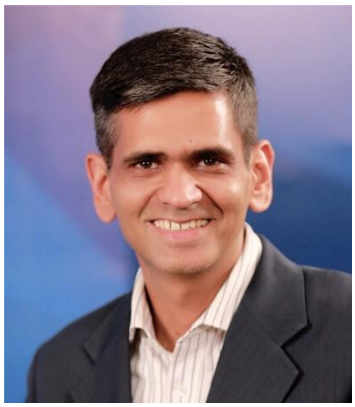
Himanshu Rai, Senior
Solutions Consultant, Google



Manish Gupta, DevSecOps
Community Leader, Thales

Mentorship Board

Rajesh Garg
EVP, Yotta Data Services Ltd



Vikas Singh Yadav
CISO, Flipkart

Gaurav Aroraa
Lead Solutions Architect, IBM

Ashish Ojha
CTO, BloomCAP

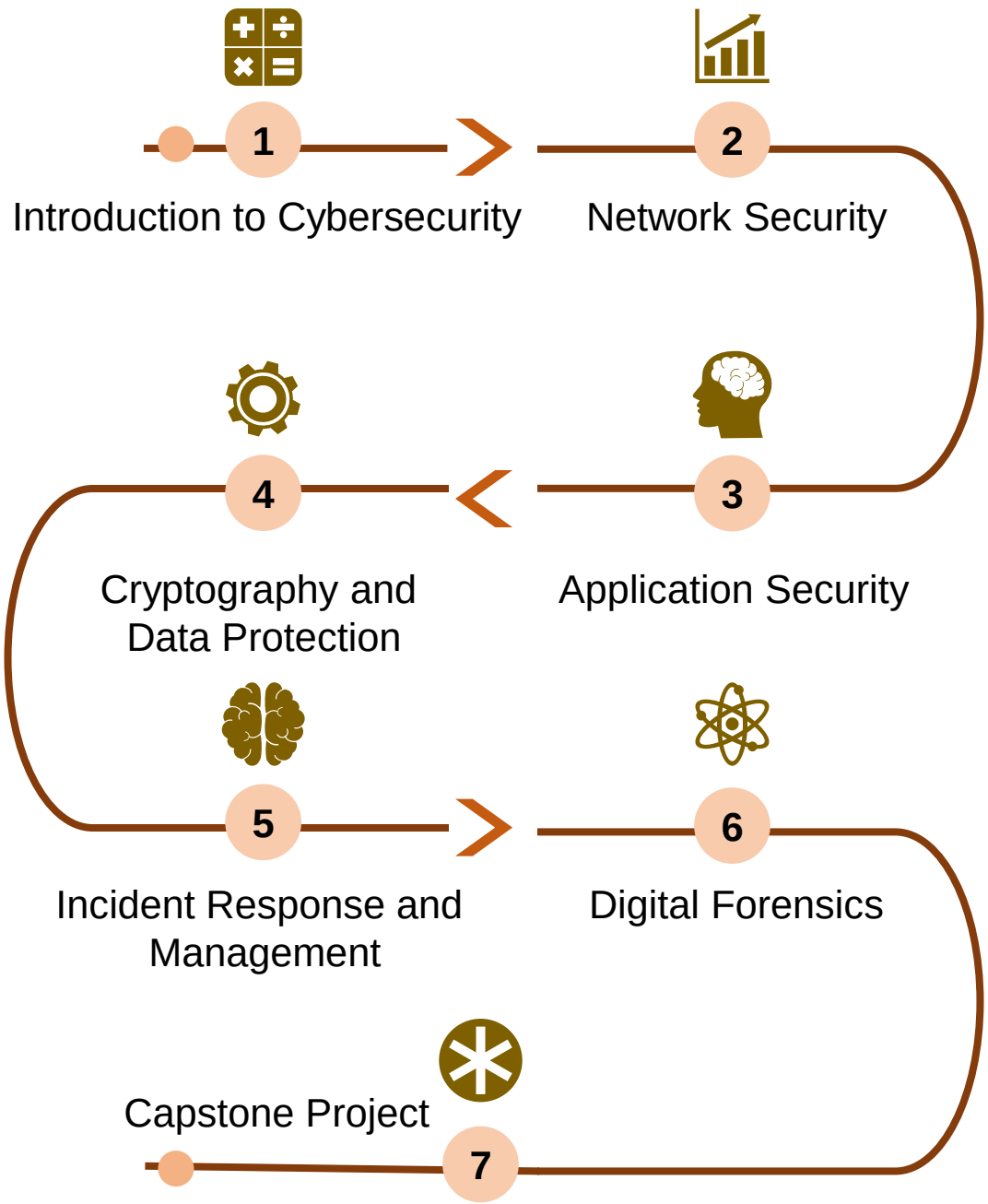
Himanshu Wadia
Director, Amdocs

Shape Your Future

Benefit from a dynamic curriculum taught in a truly Competitive Environment.

At TechMentors You spend equal time learning the fundamentals of course and specializing in the upcoming areas. The program is unique, challenging, rigorous - and absolutely the right preparation for your future success.

Learning Path



Curriculum

A comprehensive curriculum that provides an in-depth exploration of the principles, practices, and technologies used in cybersecurity and digital forensics.

Module 1: Introduction to Cybersecurity

This course explores the key concepts and importance of cybersecurity. Learners gain expertise to identify various types of cyber threats and vulnerabilities. Familiarize with cybersecurity frameworks and standards. Conduct basic risk assessments and understand mitigation strategies.

- Definition, scope, and importance of cybersecurity.
- Key concepts: Confidentiality, Integrity, Availability (CIA Triad).
- Overview of cybersecurity domains: network, application, information, operational security.
- Malware: Types (viruses, worms, trojans) and attack vectors.
- Social Engineering: Phishing, spear-phishing, and pretexting.
- Ransomware: How it works and prevention strategies.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- Advanced Persistent Threats (APTs): Tactics, techniques, and procedures.
- Cybersecurity Frameworks and Standards
- Risk identification: Asset, threat, and vulnerability analysis.
- Risk assessment methodologies: Qualitative and quantitative approaches.
- Risk mitigation strategies: Avoidance, transference, mitigation, acceptance.

Module 2: Network Security

This course explores network security principles and the OSI model. Learners gain expertise to configure and manage firewalls and VPNs for secure communication. Implement and monitor IDPS to protect networks from intrusions. Design secure network architectures to safeguard information systems.

- Understanding the OSI model and its relevance to security.
- TCP/IP protocols and their vulnerabilities.
- Types of firewalls: Packet filtering, stateful inspection, proxy firewalls.
- VPN fundamentals: IPsec, SSL/TLS VPNs, and their applications.
- Configuring firewalls for secure network access.
- Intrusion Detection and Prevention Systems (IDPS)
- Difference between IDS and IPS.
- Types of IDPS: Signature-based, anomaly-based, hybrid systems.
- Deployment strategies: Network-based vs. host-based IDPS.
- Principles of network segmentation and zoning.
- Implementing DMZs (Demilitarized Zones) for added security.
- Network security monitoring and log management.

Module 3: Application Security

This course explores secure software development lifecycle (SDLC). Learners gain expertise to identify and mitigate common application vulnerabilities. Conduct penetration testing and vulnerability scanning. Implement security measures in DevOps environments.

- Integrating security into each phase of the SDLC.
- Secure coding practices: Input validation, error handling, and session management.
- Code review and security testing techniques.
- Overview of the OWASP Top 10 vulnerabilities.
- SQL Injection: How it works and how to prevent it.
- Cross-Site Scripting (XSS): Types, impact, and mitigation strategies.
- Cross-Site Request Forgery (CSRF): Understanding and prevention.
- Difference between vulnerability scanning and penetration testing.
- Tools for vulnerability scanning: Nessus, OpenVAS, and others.
- Penetration testing methodologies: Reconnaissance, exploitation, post-exploitation.
- Introduction to DevSecOps: Integrating security into DevOps practices.
- Automating security testing in CI/CD pipelines.
- Infrastructure as Code (IaC) security best practices.

Module 4: Cryptography and Data Protection

This course explores the basic principles of cryptography and encryption techniques. Learners gain expertise to apply cryptographic protocols to secure data communication. Manage cryptographic keys and implement PKI. Protect data through encryption and other data protection strategies.

- Introduction to cryptographic principles: Confidentiality, integrity, authenticity.
- Symmetric encryption: Algorithms (AES, DES), key management.
- Asymmetric encryption: RSA, ECC, key exchange mechanisms.
- Hash functions: MD5, SHA family, applications in integrity verification.
- SSL/TLS: Secure communication protocols, handshake process.
- IPsec: Modes (transport, tunnel), applications in VPNs.
- PGP/GPG: Email encryption, signing, and verification.
- Overview of blockchain and cryptographic primitives used in blockchain technology.
- Public Key Infrastructure (PKI): Components, architecture, and deployment.
- Digital certificates: Types (SSL, Code Signing), issuing and revocation processes.
- Hardware Security Modules (HSMs) and their role in key management.
- Encryption techniques for data at rest: Full disk encryption, file/folder encryption.
- Encrypting data in transit: SSL/TLS, VPNs, secure email.
- Data masking and tokenization techniques.
- Implementing Data Loss Prevention (DLP) solutions.

Module 5: Incident Response and Management

This course explores the development and implementation of an effective incident response plan. Learners gain expertise to detect and monitor cyber threats using SIEM and other tools. Respond to and contain cybersecurity incidents effectively. Conduct post-incident analysis to improve future incident response.

- Overview of incident response lifecycle: Preparation, detection, containment, eradication, recovery, lessons learned.
- Developing an incident response plan: Roles, responsibilities, communication channels.
- Incident response team (IRT): Structure, roles, and responsibilities.
- Security Information and Event Management (SIEM): Features, deployment, and best practices.
- Log analysis: Techniques, tools, and common log sources.
- Threat intelligence: Sources, integration, and application in detection.
- Containment strategies: Isolating affected systems, preventing lateral movement.
- Eradication techniques: Removing malware, closing vulnerabilities.
- Recovery: Restoring systems to normal operation, verifying system integrity.
- Conducting a root cause analysis: Techniques and tools.
- Incident reporting: Creating actionable and detailed incident reports.
- Continuous improvement: Updating response plans based on analysis.

Module 6: Digital Forensics

This course explores the fundamental principles of digital forensics. Learners gain expertise to use forensic tools to recover and analyze digital evidence. Conduct forensic investigations in network and cloud environments. Apply mobile forensics techniques to extract and analyze data from devices.

- Overview of digital forensics: History, importance, and legal considerations.
- Types of digital forensics: Computer, network, mobile, cloud forensics.
- Legal and ethical considerations in forensic investigations.
- Disk imaging: Tools (FTK Imager, dd), techniques, and importance.
- Data recovery: Techniques for recovering deleted, fragmented, or encrypted files.
- Forensic analysis: Tools (EnCase, Autopsy), methodologies, and reporting.
- Network forensics: Capturing and analyzing network traffic, tools (Wireshark, tcpdump).
- Investigating network intrusions: Techniques, tracing attackers.
- Cloud forensics: Challenges, evidence acquisition, and tools.
- Mobile device architecture: Operating systems (iOS, Android), file systems.
- Techniques for acquiring mobile data: Logical, physical, file system extractions.
- Analyzing mobile data: Call logs, messages, GPS data, app usage.

Module 7: Capstone Project

The capstone project allows learners to implement the skills learnt throughout this programme. Learners will solve industry-specific challenges by leveraging various cybersecurity and forensics techniques. The capstone project is the final step in the core learning path and will help you showcase your expertise.

- Showcase your Cybersecurity skills starting from design and implementation of a Secure Web Application.
- Demonstration of applied knowledge by applying concepts like forensic investigations, secure software development practices, to solve real-world problems.
- Hands-on problem-solving skills through implementing projects in domains like Web application, zero trust architecture, secure communication systems, etc. students showcase their ability to work on end-to-end Cybersecurity solutions.
- Portfolio building by completing tangible, demonstrable work product to share in portfolios or during interviews with potential employers.
- Industry-relevant exposure by working on capstone projects aligned with real-world applications, like incident response simulation, digital forensics investigation, or intrusion detection system, prepares students for industry demands.
- Collaboration and presentation skills and the ability to present technical findings effectively to non-technical stakeholders.
- Solution-oriented thinking by addressing a real-world challenge, students foster innovation and learn to design scalable, deployable Cybersecurity and Forensics solutions.

Tools Covered

Who is This Programme Ideal For ?

Professionals keen to develop Cybersecurity and Forensics expertise, with the objective of:

- Enhancing effectiveness in their current role
- Transitioning to cybersecurity roles in their organization
- Seeking to advance their career in the industry
- Giving shape to entrepreneurial aspirations
- Getting an opportunity to network with like-minded individuals and industry experts

Eligibility Criteria

For admission to this Cyber Security and Forensics course, candidates should have:

- **Education:** Bachelors (four / three years or equivalent) or Masters in Science / Engineering / Management
- **Work Experience:** Nil. Preference will be given to candidates with Min 1 year of experience. Final year students with strong programming skills can also apply.
- **Coding Experience:** Programming Knowledge Required

Note: Graduates in other streams with relevant coding experience can apply

Application Process

Candidates can apply for this programme in 3 simple steps:

Step 1 Submit Application	Step 2 Application Review	Step 3 Admission
Tell us about yourself and why you want to take this programme	An admission panel will shortlist candidates based on their application	Selected candidates can join the programme by paying the admission fee

Talk to an Admission Counselor

We have a team of dedicated admissions counselors to help guide you in the application process and related matters. They are available to:

- Address questions related to the application
- Help you better understand the programme and answer your questions

Programme Fee

What is My Investment?

Application Fee **₹ 1,000**

Programme Fee

₹ 1,50,000

Programme Fee with Scholarship

₹ 1,30,000

(18% GST extra as applicable)

Special pricing for corporates

Fees paid is non-refundable and non-transferable

Unlock the Power of Cyber Security and Forensics

Get Support

+91 9560361410

info.techmentors@sbit.in

To apply visit

https://www.techmentors.sbit.in


The Best People, the Best Solutions and
the Best Infrastructure – This is all what it
takes to help young talent in grooming
through their development phase
ACADEMIC BLOCK 2
SHRI BALAJI INSTITUTE OF TECHNOLOGY

WE EXCEL AT DEVELOPING

PRINCIPLED INNOVATIVE

TECHNOCRATS & THOUGHT LEADERS

IN GLOBAL COMMUNITIES

SBIT

ENGINEERING TOMORROW

Campus

Meerut Road (Pallri), NH - 334B

Sonepat (NCR Delhi) - 131023

Haryana, India

Mob : +91 9560361410

Follow us on

www.facebook.com/sbittechmentors

www.twitter.com/sbittechmentors

www.youtube.com/user/sbittechmentors

in.linkedin.com/in/sbittechmentors

www.instagram.com/sbittechmentors