infoSorse

CYBER SECURITY

PROFESSIONAL DIPLOMA IN CYBERSECURITY

Secure Your Future Career with **In-Demand Cybersecurity Skills**

24 Months | **Live Mentorship with Experts** | **Industry Certifications** | **Professional Diploma in Cybersecurity**

infoSorse

95% of Cybersecurity breaches result from human error

Cybersecurity is no longer optional; it is a critical foundation of modern society. Sensitive data, financial systems, infrastructure, and national defense depend on resilient digital protection. Cyber attackers use increasingly advanced tools, exploiting vulnerabilities across networks, devices, and cloud platforms. Developing skilled cybersecurity professionals has become an urgent global priority.

OVER 50%

of organizations now prioritize security from the start of any transformation effort

3.5 MILLION JOBS

in Cybersecurity to be available by 2025

$265 BILLION

are the projected annual ransomware costs by 2031

The 18-month Professional Diploma in Cybersecurity at InfoSorse offers a comprehensive and immersive learning experience designed to equip learners with the skills and knowledge needed to excel in the dynamic field of cybersecurity. With flexible enrollment options—including fully online (weekday or weekend), recorded self-paced study, on-campus, or workplace training—students can choose the mode that best fits their schedule while benefiting from live mentorship by industry experts.

infoSorse

PROGRAM HIGHLIGHTS

- Interactive live mentorship with industry experts
- A final Capstone Project & Job-Ready Portfolio
- Earn a Professional Diploma in Cybersecurity
- Practical Training, Real-World Case Studies, and Hands-On Projects
- Guaranteed Internship to gain real world experience
- Earn real industry certifications from AWS, Microsoft, Google etc.

WHO IS THIS PROGRAM FOR?

An early-career professional looking to transition into Cybersecurity

Beginners seeking to begin a tech career journey in cybersecurity

An experienced professional looking to specialize in the Cybersecurity domain

A fresh graduate wanting to break into the Cybersecurity domain

DISCOVER **TOP-PAYING ROLES IN CYBERSECURITY**

CYBER THREAT INTELLIGENCE ANALYST

Gather and analyze intelligence on cyber threats, proactively identifying and mitigating risks

Average Salary

USD 121,000

CYBERSECURITY ANALYST

Analyze security threats, vulnerabilities, and incidents to safegaurd systems and data

Average Salary

USD 110,000

SOC SPECIALIST

Monitor and analyze security within a security operations center (SOC).

Average Salary

USD 92,000

iNFORMATION SECURITY SPECIALIST

implement and manage security controls to protect an organization's information assets

Average Salary

USD 90,425

SOC ANALYST

Provide ongoing support within an SOC, playing a crucial role in threats detection, analysis and response

Average Salary

USD 88,425

CLOUD SECURITY ANALYST

secure cloud environments and data, ensuring compliance with cloud

Average Salary

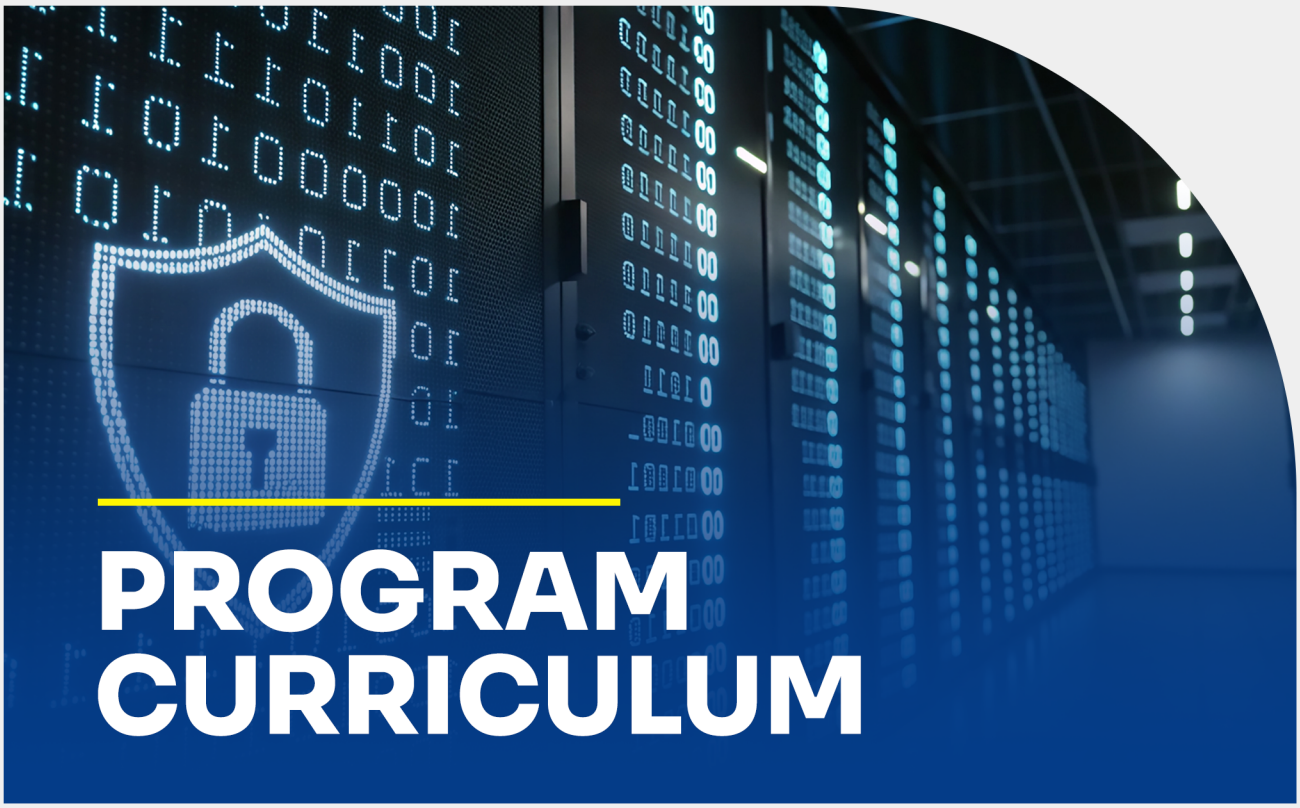
USD 82,000

NOTE: The information above may vary based on your specific skills and professional experience within the field of cybersecurity.

PROGRAM OUTCOMES

Upon completion of the program, you will have accquired the skills necessary to:

- Perform incident investigations to identify the source of the threat, assess, respond, and write clear incident reports.
- Familiarize yourself with the standards and frameworks such as: National Institute of Standards and Technology (NIST), MITRE ATT&CK, Center for Internet Security (CIS) Benchmarks.
- Demonstrate an understanding of how to identify and defend against mod-ern-day threats such as Ransomware.
- Comprehend the evolving threat land-scape by understanding the biggest cyberattacks to date.
- Build muscle memory for responding to cyberattacks by following Incident Response Playbooks.



PROGRAM CURRICULUM

Diploma **Program Calendar**

- **Root Phase** (2 months) : Develop foundational skills in digital literacy, programming basics,
- **Specialization Phase** (16 months) : Advanced technical training, hands-on labs, projects, and capstone development.
- **Mastry Phase** (6 months) : Real-world internship with industry partners, applying skills in practical environments.
- **Industry Certifications** (6 months) concurrent : Preparation for 3+ international certifications (e.g., AWS, Microsoft, CompTIA, etc).
- **Career Launch Support** (6 months) concurrent : CV/LinkedIn optimization, interview preparation, and job placement support.
- **Graduation & Project Defense** (24 months) : Diploma award and project defense before industry expert panel.

infoSorse

MODULE 1:

CYBERSECURITY 101 | 4 WEEKS

This module introduces core cybersecurity concepts, including the CIA triad, common threats, threat actors, and defense tools such as firewalls, antivirus, and encryption. Students also learn cyber hygiene, networking and OS security, cryptography, and security policies to build a strong foundation for protecting systems and data.

TOPICS:

- Introduction to Cybersecurity
- Information Security Fundamentals (CIA Triad, Security Principles)
- Common Cyber Threats and Attack Vectors (Malware, Social Engineering)
- Cyber Hygiene and Best Practices (Updates, Patching, User Awareness)
- Networking Basics for Security (OSI Model, TCP/IP Overview)
- Operating System Security Essentials (Account and Permissions Basics)
- Fundamentals of Cryptography (Symmetric/Asymmetric, Hashing)
- Security Policies, Compliance and Risk Management (Policies, Frameworks

KEY TAKEAWAYS:

- Explain the CIA triad and its importance in security.
- Identify and describe common threat types (malware, social engineering).
- Recognize different threat actor categories and their goals.
- Understand basic risk concepts (how loss of CIA attributes creates risk).
- Use fundamental security tools (firewalls, antivirus) to protect systems.

MODULE 2:

NETWORKING & NETWORK SECURITY | 4 WEEKS

This module covers networking fundamentals and securing network infrastructures. Students explore network models (OSI, TCP/IP), protocols (DNS, HTTP), devices and topologies (routers, switches, firewalls), and addressing (IP, subnets, VLANs). It also introduces key security measures such as segmentation, VPNs, firewalls, and intrusion detection.

TOPICS:

- OSI and TCP/IP Networking Concepts (Subnets, Routing, Switching)
- Network Protocols and Analysis (TCP/UDP, HTTP, DNS Analysis)
- Secure Network Architecture (VLANs, DMZs, Segmentation)
- Firewalls and IDS/IPS Technologies (Packet Filtering, Alerting)
- Wireless Network Security (Wi-Fi Encryption, Rogue APs)
- Remote Access and VPN Security (IPsec, SSL/TLS VPNs)
- Network Monitoring and Traffic Analysis Using Snort
- Network Monitoring and Traffic Analysis Using Wireshark

KEY TAKEAWAYS:

- Understand OSI and TCP/IP models and their layers.
- Configure basic network devices (router, switch) and services.
- Apply network segmentation and IP addressing to isolate resources.
- Implement core network security (set up firewalls, IDS/IPS).
- Secure wireless networks and remote access connections (WPA2, VPN).
- Use monitoring tools and logs to diagnose network issues.

MODULE 3:

OPERATING SYSTEMS & VIRTUALIZATION | 4 WEEKS

This module introduces operating system basics and virtualization. Students study OS components, security features, and learn how hypervisors, virtual machines, and containers provide isolation and secure environments.

TOPICS:

- OS Fundamentals (Windows and Linux Installation, File Systems)
- OS Fundamentals (Windows)
- User and File System Security (Account Policies, Permissions)
- Virtualization and Container Basics (VMware/ VirtualBox, Docker, KVM)
- Virtualization and Container Basics (Proxmox)

  Virtualization and Container Basics (Docker)
- OS Hardening and Patch Management (Secure Configurations) – Windows
- OS Hardening and Patch Management (Secure Configurations) – Linux
- Windows Administration Essentials (Services, Registry, PowerShell)
- Active Directory Fundamentals (Domains, Group Policy Basics)
- Active Directory Fundamentals (Setup & Installation)
- System Monitoring and Logging (Event Logs, Syslog)

KEY TAKEAWAYS:

- Describe how an OS manages resources and isolates processes.
- Manage user accounts and file permissions securely.
- Explain hypervisor types and deploy virtual machines.
- Isolate and manage multiple VMs on one physical host.
- Utilize virtualization for testing and secure isolation.
- Apply OS security measures (regular updates, firewall setup).

MODULE 4:

LINUX SYSTEM ADMIN & SECURITY | 4 WEEKS

This module focuses on Linux administration and security. Students learn shell commands, file systems, user and group management, package installation, and updates. Security topics include firewalls, SELinux/ AppArmor, SSH hardening, and log monitoring.

TOPICS:

- Linux System Architecture and Distributions (Ubuntu, CentOS, Kali)
- User and Process Management (Users, Groups, Daemons)
- File System Hierarchy and Permissions (chmod, SELinux/AppArmor)
- Linux Networking and SSH Security (ip, netstat, OpenSSH)
- Package and Service Management (apt, yum, systemd)
- Hardening Linux Servers (Firewalls – iptables, UFW)
- Shell Scripting and Automation (Bash Scripting, Cron Jobs)

KEY TAKEAWAYS:

- Navigate the Linux shell and manage files and directories.
- Configure user accounts and groups with least privilege.
- Set and audit file/directory permissions correctly.
- Apply updates and patches promptly to secure a Linux system.
- Configure the Linux firewall and use SELinux for enhanced protection.
- Secure SSH (use key-based auth) and monitor logs for anomalies.

MODULE 5:

PROGRAMMING & SCRIPTING FOR SECURITY | 4 WEEKS

This module builds programming and scripting skills for security. Students practice Python for automation, Bash/PowerShell for administration, and learn C/C++ basics related to vulnerabilities. Topics include log parsing, APIs, vulnerability testing, and secure coding practices.

TOPICS:

- Introduction to Python for Security (Syntax, Libraries)
- Bash Scripting Basics (Automation, Task Scheduling)
- PowerShell Scripting Basics (Automation, Task Scheduling)
- Data Analysis and Visualization with Python (Pandas, Matplotlib)
- Secure Coding Principles (Input Validation, Error Handling)
- Web and Network Programming (Sockets, APIs, HTTP Requests)
- Automating Security Tasks (Log Parsing, Automation Scripts)
- Version Control for Security Projects (Git/GitHub Basics)

KEY TAKEAWAYS:

- Write Python scripts to automate security tasks (scanning, data analysis).
- Create Bash scripts to streamline system administration tasks.
- Understand memory-related vulnerabilities (buffer overflows) in C/C++.
- Apply secure coding techniques to prevent common flaws.
- Recognize how web languages (JavaScript/SQL) relate to security vulnerabilities.
- Use version control (Git) to manage and collaborate on code.

MODULE 6:

WEB APP & SECURE DEVELOPMENT | 4 WEEKS

This module covers web application security and secure development. Students study the OWASP Top 10 risks, including injection and cross-site scripting, and learn practices like input validation, secure authentication, session management, and HTTPS/TLS for safe communication.

TOPICS:

- Web Technologies Overview (HTTP, HTML, JavaScript)
- Common Web Vulnerabilities (OWASP Top 10, Injection, XSS)
- Secure Web Architecture (Authentication, Sessions, SSL/TLS)
- Web Penetration Testing Tools (Burp Suite)
- Web Penetration Testing Tools (ZAP)
- API and Microservices Security (REST, JSON, OAuth)
- Secure SDLC Practices (Code Reviews, Threat Modeling)
- DevSecOps Principles (CI/CD Security, Container Hardening)

KEY TAKEAWAYS:

- Identify and explain OWASP Top 10 risks.
- Prevent injection and XSS by validating inputs and using parameterized queries.
- Implement secure authentication (strong passwords, multi-factor) and session handling.
- Ensure all web traffic is encrypted (HTTPS/TLS).
- Use security tools to test and find web application vulnerabilities.

MODULE 7:

VULNERABILITY ASSESSMENT & PENETRATION TESTING | 4 WEEKS

This module introduces vulnerability assessment and penetration testing (VA/PT). Students use scanners and tools like Nmap and Nessus to find weaknesses, then apply penetration testing phases—reconnaissance, scanning, exploitation, and reporting—while focusing on risk analysis and remediation.

TOPICS:

- Reconnaissance and Information Gathering (OSINT, Scanning)
- Network Scanning and Enumeration (Nessus)
- Network Scanning and Enumeration (Nmap)
- Vulnerability Analysis and Exploitation Planning (Prioritization)
- Exploitation Fundamentals (Metasploit)
- Exploitation Fundamentals (Buffer Overflows)
- Post-Exploitation Techniques (Maintaining Access, Pivoting)
- Reporting and Documentation (Writing Technical Reports)
- Ethics and Legal Aspects of Hacking (Laws, Responsible Disclosure)

KEY TAKEAWAYS:

- Use vulnerability scanners to identify security weaknesses.
- Conduct structured penetration tests to exploit and verify vulnerabilities.
- Analyze and prioritize findings based on potential impact.
- Develop clear reports with remediation guidance.
- Gain familiarity with common pentest tools (Nmap, Metasploit).

MODULE 8:

ADVANCED PENETRATION TESTING & EXPLOITATION | 4 WEEKS

This module explores advanced exploitation techniques and red-team strategies. Students practice writing and using exploits for buffer overflows, privilege escalation, pivoting, and evasion. Labs include Metasploit and custom exploit development for hands-on experience.

TOPICS:

- Advanced Reconnaissance and OSINT (Maltego)
- Advanced Reconnaissance and OSINT (Shodan)
- Exploit Development and Buffer Overflows (Pattern Creation, Debugging)
- Bypassing Defenses (AV)
- Bypassing Defenses (AMSI)
- Bypassing Defenses (Web Application WAF Evasion)
- Web Application Exploitation (Advanced SQLi)
- Web Application Exploitation (Cross-Site Scripting)
- Wireless Penetration Testing (Wi-Fi Attacks)
- Mobile Penetration Testing (Mobile App Testing)
- Social Engineering Techniques (Phishing, Pretexting)
- Credential Harvesting
- Red Team Operations (C2 Frameworks)
- Windows Privilege Escalation
- Linux Privilege Escalation
- Lateral Movement etc.

KEY TAKEAWAYS:

- Develop and deploy custom exploits for known vulnerabilities.
- Use advanced pentesting tools and techniques (Metasploit, custom scripts).
- Escalate privileges on compromised systems.
- Navigate internal networks via pivoting.
- Understand how to bypass common defenses (anti-virus, firewalls).

MODULE 9:

CLOUD COMPUTING & SECURITY | 4 WEEKS

This module introduces cloud computing and security. Students study service models, the Shared Responsibility Model, cloud architectures (networks, containers, serverless), key controls like IAM and encryption, plus common threats and compliance.

TOPICS:

- Cloud Concepts and Service Models (IaaS, PaaS, SaaS Overview)
- AWS Fundamentals (Core Services, Use Cases)
- Azure Fundamentals (Core Services, Use Cases)
- Cloud Identity and Access Management (AWS IAM)
- Cloud Identity and Access Management (Azure AD / Microsoft Entra ID)
- Cloud Network Security (AWS Security Groups)
- Cloud Network Security (Microsoft Entra ID Security Groups)
- Cloud Network Security (AWS VPC, Firewalls)
- Cloud Network Security (Microsoft Azure VPC, Firewalls)
- Cloud Data Protection (Encryption, Key Management Services)
- Cloud Security Operations (AWS Logging, Monitoring, CloudTrail) etc.

KEY TAKEAWAYS:

- Explain the shared responsibility model in cloud security.
- Securely configure cloud resources (VPC, IAM roles, security groups).
- Encrypt data in cloud storage and transit.
- Implement strong API security (authentication, input validation).
- Understand container/Kubernetes security essentials.
- Use cloud-native monitoring and logging for incident detection.

MODULE 10:

IDENTITY & ACCESS MANAGEMENT | 4 WEEKS

This module explores IAM principles and practices. Students learn authentication vs. authorization, identity stores (LDAP, Active Directory), and account lifecycle management. Topics include password policies, MFA, RBAC, SSO, and identity federation for secure access.

TOPICS:

- Authentication Protocols and Services (Kerberos)
- Authentication Protocols and Services (LDAP)
- Authentication Protocols and Services (SAML)
- Authentication Protocols and Services (OAuth)
- Authorization and Access Control Models (RBAC, ABAC, Least Privilege)
- Directory Services (Active Directory, Azure AD Pentesting)
- Single Sign-On and Federation (SSO, ADFS, SAML-based SSO)

  Multi-Factor Authentication (MFA, Biometrics)
- Privileged Access Management (PAM Tools, Service Accounts)
- Identity Governance and Compliance (Account Auditing, IAM Policies)

KEY TAKEAWAYS:

- Differentiate authentication and authorization.
- Configure and manage user identities and roles.
- Implement multi-factor authentication to harden login security.
- Design RBAC policies to enforce least privilege.
- Set up single sign-on and federated identity.
- Monitor and audit access controls.

MODULE 11:

SECURITY OPERATIONS & SIEM | 4 WEEKS

This module covers security operations and monitoring. Students learn the role of a SOC and how SIEM systems collect logs, correlate events, and generate alerts. It also introduces threat hunting and incident response within a SOC environment.

TOPICS:

- Security Operations Center (SOC) Fundamentals and Processes
- SIEM Fundamentals (Log Collection, Normalization)
- SIEM Fundamentals (Correlation)
- Threat Intelligence (Indicators of Compromise)
- Threat Hunting (Indicators of Compromise)
- Endpoint Detection and Response (EDR) Tools (CrowdStrike, OSSEC)
- Network Traffic Monitoring (Zeek, Suricata)
- Incident Triage and Escalation (Playbooks, Severity Levels)
- Metrics, Dashboards, and Continuous Improvement (KPIs, Reporting)

KEY TAKEAWAYS:

- Configure a SIEM to collect and analyze security logs.
- Define correlation rules to detect suspicious patterns.
- Understand SOC processes for monitoring and responding to alerts.
- Analyze SIEM alerts and escalate true incidents.
- Leverage threat intelligence to prioritize investigations.
- Collaborate within a SOC team to improve security posture.

MODULE 12:

INCIDENT RESPONSE | 4 WEEKS

This module introduces the incident response (IR) lifecycle based on NIST: Preparation, Detection, Containment, Eradication, and Recovery. Students learn to create IR plans, detect and contain attacks, gather evidence, eradicate threats, and conduct post-incident reviews.

TOPICS:

- Incident Response Lifecycle (Preparation, Identification, Containment)
- Evidence Collection and Preservation (Chain of Custody, Imaging)
- Malware Analysis for Incident Responders (Static & Dynamic)
- Memory and Network Forensics Basics (Volatility, Wireshark)
- Containment, Eradication, and Recovery (Backups, Patching)
- Legal, Regulatory, and Ethical Considerations (Data Breach Law)
- Incident Reporting and Lessons Learned (Post-Incident Review)

KEY TAKEAWAYS:

- Describe the incident response lifecycle.
- Develop an incident response plan and team structure.
- Detect and analyze security incidents using logs and alerts.
- Contain and remove threats effectively.
- Gather and preserve evidence during an incident.
- Perform post-mortem reviews to improve future response

MODULE 13:

DIGITAL FORENSICS | 4 WEEKS

This module covers digital forensic investigation techniques. Students learn to preserve and analyze electronic evidence, perform disk imaging and memory capture, recover deleted files, and use forensic tools while following chain-of-custody and documentation procedures.

TOPICS:

- Forensic Investigation and Chain of Custody (Legal Process)
- Disk and File System Forensics (FAT/NTFS Analysis)
- Memory Forensics and Analysis (RAM Dump Examination)
- Network Forensics (Log Analysis, pcap Analysis)
- Mobile Device Forensics (iOS, Android Basics)
- Forensic Tools and Techniques (Autopsy)
- Forensic Tools and Techniques (Sleuth Kit)
- Reporting and Testimony (Writing Forensic Reports, Court Basics)

KEY TAKEAWAYS:

- Properly acquire and preserve digital evidence.
- Use forensic tools to recover hidden or deleted data.
- Analyze forensic artifacts to reconstruct events.
- Maintain a complete chain of custody and documentation.
- Prepare findings in a clear, admissible report.

MODULE 14:

MALWARE ANALYSIS & REVERSE ENGINEERING | 4 WEEKS

This module introduces malware analysis and reverse engineering. Students learn static and dynamic analysis, safe sandboxing, and the use of tools like IDA Pro and Ghidra to identify malware behavior and indicators of compromise.

TOPICS:

- Malware Types and Infection Vectors (Trojans, Ransomware, Rootkits)
- Static Analysis Techniques (Strings, PE Header, YARA Rules)
- Dynamic Analysis and Sandboxing (Cuckoo Sandbox, Process Monitor)
- Windows Malware Analysis (API Calls, Memory Behavior)
- Linux/macOS Malware Analysis (ELF, Mach-O analysis)
- Reverse Engineering Basics (IDA Pro/Ghidra Use, Debugging)
- Creating Indicators and Signatures (YARA)
- Creating Indicators and Signatures (Suricata Rules)

KEY TAKEAWAYS:

- Perform static code analysis on malware samples.
- Execute malware in a controlled sandbox to observe behavior.
- Use reverse-engineering tools to extract malware logic.
- Identify and document malware indicators (hashes, C2 IPs).
- Develop detection signatures or rules based on analysis.

MODULE 15:

GOVERNANCE, RISK & COMPLIANCE | 4 WEEKS

This module introduces the Governance, Risk, and Compliance (GRC) framework. Students learn how governance sets policies and accountability, risk management identifies and prioritizes threats, and compliance ensures adherence to laws and standards like GDPR and ISO 27001.

TOPICS:

- Security Governance Frameworks (ISO/IEC 27001, NIST CSF)
- Risk Assessment and Management (Risk Matrices, Asset Valuation)
- Compliance Requirements (GDPR, HIPAA, PCI DSS Basics)
- Business Continuity and Disaster Recovery Planning
- Security Auditing and Control Frameworks (SOX)
- Security Auditing and Control Frameworks (COBIT)
- Security Awareness and Training Programs (Phishing Tests)
- Ethics and Professional Responsibility (Codes of Conduct)

KEY TAKEAWAYS:

- Explain the role of governance, risk management, and compliance.
- Conduct a security risk assessment to prioritize threats.
- Align security controls with regulatory requirements.
- Develop and enforce security policies and procedures.
- Prepare for audits and manage compliance obligations.

MODULE 16:

SECURITY ARCHITECTURE & DESIGN | 4 WEEKS

This module covers secure system and architecture design. Students learn principles like least privilege, defense-in-depth, threat modeling, segmentation, secure patterns, and Zero Trust to embed security from the start.

TOPICS:

- Secure Network and Infrastructure Design (Segmentation, DMZ, VPN)
- Cloud and Virtualization Security Architecture (Isolation, Microsegmentation)
- Secure Systems Engineering (Hardware Trust, Firmware Security)
- Cryptographic Foundations and PKI Implementation
- Endpoint and Application Hardening (Baseline Configurations)
- Emerging Technology Security (IoT, Blockchain, AI Security Basics)
- Zero Trust Architecture and Microsegmentation (Principles and Practice)

KEY TAKEAWAYS:

- Apply least privilege to minimize access risk.
- Design layered defenses (firewalls, segmentation, monitoring).
- Integrate security throughout the system development lifecycle.
- Conduct threat modeling to identify vulnerabilities.
- Choose secure defaults and minimize attack surface.

CAPSTONE PROJECT IN CYBERSECURITY | 4 WEEKS

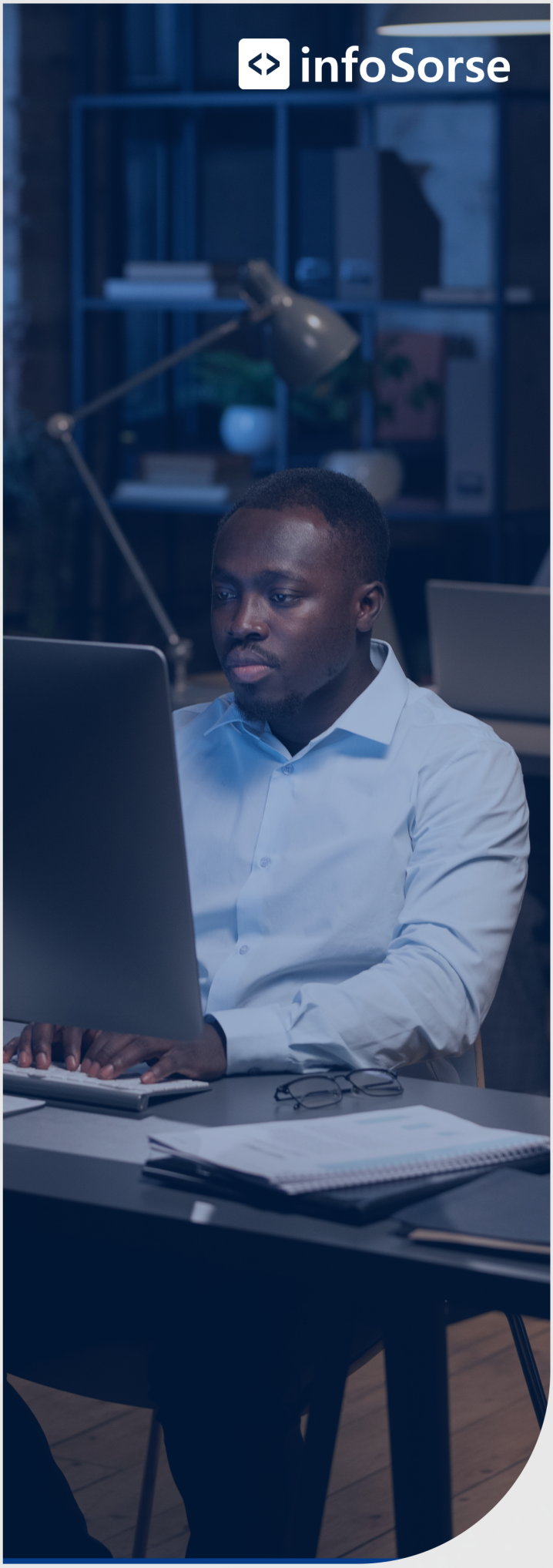
The Capstone Project is the culmination of the program, where students apply skills from all modules in a real-world scenario. Working in teams, they design, implement, and test a security solution for a simulated organization—covering planning, threat modeling, controls, testing, incident response, and reporting while demonstrating teamwork and professional communication.

TOPICS:

- Project Planning and Requirements Gathering (Scope Definition)
- Threat Modeling and Design (Identify Threats and Controls)
- Implementation of Security Controls (Hardening, Configuration)
- Security Testing and Assessment (Penetration Test, Vulnerability Scan)
- Incident Response Simulation (Detect and Mitigate a Mock Breach)
- Documentation and Reporting (Security Architecture and Incident Reports)
- Presentation and Defense of Project (Stakeholder Briefing)

KEY TAKEAWAYS:

- Synthesize knowledge from all curriculum areas into a cohesive solution.
- Demonstrate hands-on security skills in a realistic project.
- Plan and manage a multi-phase security project.
- Collaborate and communicate security decisions effectively



Program Eligibility

This program is open to learners from all educational and professional backgrounds. A minimum of a high school education and basic digital literacy are recommended. No prior IT experience is required - our Root Phase provides the foundational skills needed for success in the specialization modules.

Education: **A minimum of a high school education. University graduates and diploma holders in any field are encouraged.**

Basic Digital Literacy: **Comfort with using computers, internet applications, and file management.**

English Proficiency: **Ability to read, write, and communicate in English, since all training, materials, and certification exams are delivered in English.**

Mindset: **Strong motivation to learn, problem-solve, and adapt in a fast-changing tech field.**

Added Advantage: **Prior exposure to IT, networking, or programming is helpful but not required, since the Root Phase builds these foundations. fast-changing tech field.**

ADMISSION PROCESS

Selection process

Our selection process ensures that every learner admitted into the Professional Diploma in Cybersecurity is prepared and ready to succeed.

Application Submission

Complete the online application form with personal details, educational background, and motivation for joining the program.

Eligibility Review

Our admissions team reviews applications to confirm that applicants meet the basic requirements: a high school education, basic digital literacy, and English proficiency.

Offer of Admission

Successful applicants receive an official admission offer, along with payment details for the program.

Enrollment & Orientation

Upon acceptance, students complete enrollment, receive access credentials, and attend the orientation session to prepare for the Root Phase.

- **Tuition: $150 / month**
- **Scholarship: 50% off**

If you enroll by month-end, pay only $75

infoSorse

Industry Certifications (Included Free)

At InfoSorse, we believe every graduate should leave with more than just a diploma — you should also hold credentials that are recognized by employers worldwide. That's why we provide up to 3 FREE industry certifications (valued at up to $360) at no extra cost.

What This Means For You:

- **Earn certifications from global leaders like AWS, Microsoft, and CompTIA.**
- **Save up to $360 in exam fees — included at no extra cost.**
- **Stand out with credentials that employers look for on CVs and LinkedIn profiles.**
- **Graduate not only with a diploma but also with globally recognized proof of your skills.**

This exclusive offer is built into your program — no hidden costs, no extra payments.

Professional Diploma in Cybersecurity

By enrolling in the Cybersecurity program at InfoSorse, you gain comprehensive training in essential skills and graduate with both a Professional Diploma in Cybersecurity and globally recognized industry certifications. Throughout your intensive journey, you will receive rigorous, hands-on training in cybersecurity techniques and tools, preparing you for certification exams and ensuring your success in the global job market.

INDUSTRY CERTIFICATIONS

- **Professional Diploma in Cybersecurity**
- **AWS Certified Cloud Practitioner**
- **Google Cybersecurity Professional Certificate**
- **CompTIA Security+**
- **Additional Certifications Aligned with Your Career Path**

READY TO BECOME A **CYBERSECURITY EXPERT?**

+233 53 996 9933

Email us anytime: **admissions@infosorse.com**

Website: **www.infosorse.com**

APPLY NOW