

Duration: 12 Month

Diploma in Cybersecurity

Overview:

The world of cybersecurity encompasses a broad spectrum of fields and disciplines. From foundational knowledge in Linux, networking, and Python programming, to understanding the basics of cybersecurity and ethical hacking, individuals delve into advanced areas like penetration testing, web and mobile application security, network security, IoT security, endpoint security, and cloud security. These areas require specialized skills and expertise to safeguard digital assets, networks, and systems against evolving threats in the modern digital landscape.

What you'll learn

- In this comprehensive course, you'll gain proficiency in Linux fundamentals, networking principles, and Python programming.
- You'll also delve into the basics of cybersecurity, advancing through ethical hacking techniques, penetration testing, and securing web, mobile, and network applications.
- Bug bounty hunters interested in formalizing their knowledge and gaining a broader perspective on cybersecurity.
- Mobile application developers and testers looking to specialize in mobile application penetration testing.
- Additionally, you'll explore IoT, endpoint, and cloud security, acquiring a holistic understanding of modern cybersecurity practices.

Target Audience:





The Diploma in Cybersecurity training course will significantly benefit:

- Targeting aspiring cybersecurity professionals, our comprehensive course covers Linux fundamentals, networking principles, Python programming, and delves into the basics of cyber security.
- Advanced modules cover ethical hacking, penetration testing, and specialized areas such as web, mobile, network, IoT, endpoint, and cloud security.

Prerequisite Knowledge:

- Familiarity with Linux, networking, Python, and cybersecurity basics.

You can reach us:

-  www.cyberous.in
-  info@cyberous.in
-  [@cyberous](https://www.instagram.com/cyberous)
-  [Cyberous](https://www.youtube.com/Cyberous)



Cyberous

Month :-1

LINUX FUNDAMENTALS MODULES

Course Outline:

Module 01: Linux Basics

- History and philosophy.
- Different distributions.
- Command line interaction.

Module 02: File System Navigation

- Commands: cd, pwd, ls.
- Permissions.
- Manipulating files: mkdir, touch, rm, mv.

Module 03: File Manipulation

- Text editing: nano, vim.
- Searching: grep.
- Compression: gzip, tar, zip.

Module 04: User and Group Management

- Commands: useradd, usermod, passwd.
- Permissions.
- Group management.



CyberouS

Module 5: Process Management

- Commands: ps, top, kill.
- Background and foreground processes.
- Priority and scheduling: nice, renice.

Module 6: Package Management

- Package managers: apt, yum, pacman.
- Searching and repositories.
- Dependencies and conflicts.

Module 7: Networking Basics

- Configuration: ifconfig, ip.
- Troubleshooting.
- Protocols: TCP/IP.

Module 8: System Administration

- Services: systemctl, service.
- Startup/shutdown.
- Performance monitoring.



Module 9: Shell Scripting

- Scripting basics.
- Variables, conditionals, loops.
- Task automation.

Module 10: File System Permissions

- Ownership and permissions.
- chmod.
- chown, chgrp.

Module 11: Text Processing Tools

- sed, awk.
- Text manipulation.
- Regular expressions.

Module 12: File System Hierarchy

- Structure overview.
- Important directories.
- Navigation.



CyberouS

Module 13: Backup and Restore

- Backup tools: tar, rsync.
- Strategies.
- Restoration.

Module 14: File System Integrity

- Checksums.
- Error detection and repair.
- Journaling.

Module 15: Security Essentials

- Firewalls.
- Authentication.
- Log monitoring.

Module 16: Remote Access

- SSH.
- File transfer: SCP, SFTP.
- Remote desktop.



CyberouS

Module 17: System Updates and Upgrades

- Package updates.
- System upgrades.
- Repositories.

Module 18: Shell Customization

- Prompt customization.
- Aliases, functions.
- Configuration files.

Module 19: Virtualization and Containers

- Virtualization: VirtualBox, VMware.
- Containers: Docker, Podman.
- Management.

Module 20: Monitoring and Performance Tuning

- Performance tools: sar, vmstat.
- Bottleneck identification.
- System tuning.



Cyberous

Month :-2

NETWORKING

Course Outline:

Module 01: Networking Basics

- OSI/TCP/IP models.
- LAN/WAN/WLAN.
- Networking devices: routers, switches, modems.

Module 02: Network Protocols

- TCP/IP suite: IPv4, IPv6, TCP, UDP.
- Application layer: HTTP, FTP, SMTP.
- Data link layer: Ethernet, ARP.

Module 03: IP Addressing

- IPv4: classes, subnetting, CIDR.
- IPv6: addressing scheme, types.
- DHCP: dynamic IP allocation.

Module 04: Routing and Switching

- Routing: tables, protocols.
- Switching: MAC, VLANs.
- Protocols: OSPF, BGP, RIP.



CyberouS

Module 5: Network Security

- Firewalls: types.
- VPN: tunneling, encryption.
- IDS/IPS: detection, prevention.

Module 6: Wireless Networking

- Wi-Fi standards: 802.11.
- Security: WPA, WPA2.
- Access points, SSIDs.

Module 7: Network Services

- DNS: resolution.
- DHCP: IP allocation.
- NAT: address translation.

Module 8: Network Troubleshooting

- Ping, traceroute.
- Wireshark: traffic analysis.
- Connectivity issues.



Module 9: Network Design

- Scalability, redundancy.
- Topologies: star, mesh.
- VLANs, virtual switches.

Module 10: Quality of Service (QoS)

- Bandwidth management.
- Traffic prioritization.
- QoS techniques: shaping, scheduling.

Module 11: Network Monitoring

- SNMP: management protocol.
- Monitoring tools: Nagios.
- Performance metrics: throughput, latency.

Module 12: Cloud Networking

- VPC setup.
- Direct Connect, ExpressRoute.
- Hybrid cloud networking.



CyberouS

Module 13: SDN

- Architecture.
- OpenFlow.
- Use cases.

Module 14: Network Virtualization

- VLANs.
- VPNs.
- NFV.

Module 15: Network Access Control (NAC)

- Authentication.
- Deployment.
- Solutions/vendors.

Module 16: Network Performance Optimization

- Bandwidth optimization.
- Traffic shaping.
- Load balancing.



Cyberous

Module 17: IPv6 Implementation

- Addressing.
- Transition.
- Adoption challenges.

Module 18: VoIP and Unified Communications

- VoIP protocols.
- Unified comms platforms.
- QoS for VoIP.

Module 19: Network Automation

- Configuration management.
- Automation frameworks.
- Benefits, challenges.

Module 20: IoT Networking

- IoT protocols.
- Security considerations.
- Scalability challenges.



CyberouS

Month :-3

PYTHON

Course Outline:

Module 01: Python Basics

- Syntax and data types.
- Control flow.
- Functions and modules.

Module 02: Data Structures

- Lists, tuples, dictionaries.
- Operations and methods.
- Mutability and immutability.

Module 03: File Handling

- Opening, reading, writing files.
- Exception handling.
- Context managers.

Module 04: Object-Oriented Programming (OOP)

- Classes and objects.
- Inheritance.
- Encapsulation, polymorphism.



Module 5: Pythonic Idioms

- List comprehensions.
- Generators, iterators.
- Decorators.

Module 6: String Manipulation

- String methods.
- String formatting.
- Regular expressions.

Module 7: Exception Handling

- Try-except blocks.
- Handling specific exceptions.
- Finally block.

Module 8: Debugging Techniques

- Print statements.
- Debugging tools: pdb.
- Tracebacks.



Module 9: Functional Programming

- Lambda functions.
- Map, filter, reduce.
- Recursion.

Module 10: Concurrency and Parallelism

- Threading, multiprocessing.
- Thread synchronization.
- GIL.

Module 11: Database Interaction

- SQLite, ORM frameworks.
- CRUD operations.
- Connection management.

Module 12: Web Development with Python

- Flask, Django frameworks.
- Routing, views.
- Templating engines.



Module 13: API Integration

- RESTful APIs.
- HTTP requests: requests library.
- Authentication, authorization.

Module 14: Data Analysis and Visualization

- Pandas: data manipulation.
- Matplotlib, Seaborn: plotting.
- Jupyter Notebooks.

Module 15: Testing in Python

- Unit testing: unittest.
- Test-driven development (TDD).
- Mocking, patching.

Module 16: Python Packaging and Distribution

- Creating packages.
- PyPI distribution.
- Virtual environments.



CyberouS

Module 17: Asynchronous Programming

- Asyncio library.
- Async/await syntax.
- Event loops, coroutines.

Module 18: Machine Learning with Python

- Scikit-learn: ML algorithms.
- TensorFlow, PyTorch: deep learning.
- Model evaluation, deployment.

Module 19: Deployment and Automation

- Creating executables.
- Docker containerization.
- CI/CD pipelines: Jenkins, GitLab CI.

Module 20: Documentation and Best Practices

- Docstrings.
- PEP 8: style guide.
- Code review, version control.



Cyberous

Month :-4

Basic of Cyber Security

Course Outline:

Module 01: Cybersecurity Fundamentals

- Core principles.
- Common threats.
- Importance in modern society.

Module 02: Security Policies and Procedures

- Policy development.
- Incident response procedures.
- Security awareness training.

Module 03: Risk Management

- Risk identification and assessment.
- Mitigation strategies.
- Continuous monitoring.

Module 04: Network Security

- Firewalls and IDS/IPS.
- Securing network devices.
- Regular security audits.



Cyberous

Module 5: Endpoint Security

- Antivirus/antimalware.
- Endpoint security solutions.
- Encryption and access controls.

Module 6: Identity and Access Management (IAM)

- Strong authentication.
- User account management.
- Multi-factor authentication.

Module 7: Data Protection

- Data encryption.
- Data loss prevention (DLP).
- Backup and recovery.

Module 8: Security Awareness Training

- Employee education.
- Phishing awareness.
- Cultivating a security-conscious culture.



CyberouS

Module 9: Incident Response

- Response planning.
- Incident roles and responsibilities.
- Post-incident analysis.

Module 10: Vulnerability Management

- Vulnerability assessments.
- Patch management.
- Risk-based prioritization.

Module 11: Security Compliance

- Regulatory requirements.
- Compliance frameworks.
- Audits and assessments.

Module 12: Cloud Security

- Securing cloud services.
- Identity management in the cloud.
- Monitoring and auditing.



CyberouS

Module 13: Mobile Security

- Mobile device management (MDM).
- Security policies.
- App security.

Module 14: Social Engineering Awareness

- Employee education.
- Simulation exercises.
- Reporting protocols

Module 15: Wireless Security

- Wi-Fi security measures.
- Wireless IDS/IPS.
- Security assessments.

Module 16: Cybersecurity Tools and Technologies

- SIEM, IDS/IPS, DLP.
- Tool evaluation and selection.
- Integration into infrastructure.



Cyberous

Module 17: Cybersecurity Governance

- Governance frameworks.
- Stakeholder roles.
- Alignment with business goals.

Module 18: Security Architecture and Design

- Secure network design.
- Defense-in-depth.
- Architecture reviews.

Module 19: Security Monitoring and Analytics

- Monitoring solutions.
- Log analysis.
- Threat detection.

Module 20: Emerging Threats and Trends

- Staying updated.
- Monitoring trends.
- Proactive measures.



CyberouS

Month :-5

Advance Ethical Hacking

Course Outline:

Module 01: Ethical Hacking Fundamentals

- Ethical concepts.
- Legal considerations.
- Distinction from malicious hacking.

Module 02: Footprinting and Reconnaissance

- Information gathering.
- OSINT tools.
- Footprinting methodologies.

Module 03: Scanning Networks

- Port scanning.
- Network mapping.
- Vulnerability scanning.

Module 04: Enumeration

- Service enumeration.
- User enumeration.
- SNMP enumeration.



Module 5: System Hacking

- Exploiting vulnerabilities.
- Privilege escalation.
- Password cracking.

Module 6: Malware Threats

- Types of malware.
- Malware analysis.
- Antivirus evasion.

Module 7: Sniffing and Spoofing

- Packet sniffing.
- ARP/DNS spoofing.
- Sniffing tools.

Module 8: Social Engineering

- Psychological manipulation.
- Phishing.
- Social engineering toolkits.



CyberouS

Module 9: Web Application Hacking

- SQL injection.
- XSS.
- Session hijacking.

Module 10: Wireless Network Hacking

- WLAN security.
- Cracking keys.
- Rogue APs.

Module 11: Evading IDS, Firewalls, Honeypots

- IDS evasion.
- Firewall evasion.
- Honeypot detection.

Module 12: Cryptography

- Encryption algorithms.
- Cryptanalysis.
- Steganography.



CyberouS

Module 13: Penetration Testing Methodologies

- Planning.
- Execution.
- Reporting.

Module 14: Post-Exploitation Techniques

- Maintaining access.
- Covering tracks.
- Pivoting.

Module 15: IoT Hacking

- Device vulnerabilities.
- Exploitation.
- Penetration testing.

Module 16: Cloud Computing Security

- Cloud infrastructure flaws.
- AWS/Azure/GCP security.
- Cloud pen testing.



CyberouS

Module 17: Mobile Application Hacking

- Android/iOS security.
- Reverse engineering.
- Exploiting vulnerabilities.

Module 18: Physical Security

- Social engineering attacks.
- Lock picking.
- Physical security audits.

Module 19: Red Team Operations

- Simulating attacks.
- Covert ops.
- Adversarial tactics.

Module 20: Ethical Hacking Best Practices

- Responsible disclosure.
- Continuous learning.
- Upholding ethical standards.



CyberouS

Month :-6

Advance Penetration Testing

Course Outline:

Module 01: Penetration Testing Overview

- Conceptual understanding.
- Objectives and scope.
- Types of tests.

Module 02: Pre-engagement Phase

- Planning and scoping.
- Rules of engagement.
- Legal considerations.

Module 03: Intelligence Gathering

- OSINT methods.
- Active reconnaissance.
- Data aggregation.

Module 04: Vulnerability Analysis

- Identifying vulnerabilities.
- Manual and automated scans.
- Vulnerability assessment tools.



CyberouS

Module 5: Exploitation

- Exploiting vulnerabilities.
- Unauthorized access.
- Privilege escalation.

Module 6: Post-Exploitation

- Maintaining access.
- Network pivoting.
- Data exfiltration.

Module 7: Password Attacks

- Cracking techniques.
- Password spraying.
- Brute force.

Module 8: Web Application Testing

- OWASP Top 10.
- SQL injection.
- Cross-site scripting.



CyberouS

Module 9: Network Testing

- Exploiting misconfigurations.
- Man-in-the-middle.
- Sniffing and interception.

Module 10: Wireless Testing

- Wi-Fi security assessment.
- Key cracking.
- Rogue AP detection.

Module 11: Social Engineering Testing

- Phishing.
- Pretexting.
- Physical bypass.

Module 12: Physical Security Testing

- Tailgating.
- Lock picking.
- Physical assessments.



CyberouS

Module 13: Cloud Infrastructure Testing

- Security configurations.
- IAM permissions.
- Data exposure testing.

Module 14: Mobile Application Testing

- iOS/Android security.
- Reverse engineering.
- API security.

Module 15: IoT Testing

- Device vulnerabilities.
- Protocol exploitation.
- Network reconnaissance.

Module 16: Red Team Exercises

- Real-world simulations.
- Defensive capability assessment.
- Incident response evaluation.



CyberouS

Module 17: Report Writing and Documentation

- Findings documentation.
- Vulnerability prioritization.
- Remediation recommendations.

Module 18: Continuous Testing and Monitoring

- Continuous testing implementation.
- Vulnerability monitoring.
- Security posture assessment.

Module 19: Advanced Techniques and Tools

- Exploitation advancements.
- Custom tool development.
- Exploit creation.

Module 20: Ethical and Professional Conduct

- Ethical adherence.
- Professionalism.
- Confidentiality respect.



CyberouS

Month :-7

Web Application Security

Course Outline:

Module 01: Understanding Web Application Security

- Importance.
- Common vulnerabilities.
- Impact of breaches.

Module 02: OWASP Top 10

- Injection attacks.
- Broken authentication.
- Sensitive data exposure.

Module 03: Input Validation and Sanitization

- Validating inputs.
- Sanitizing data.
- Preventing injections.

Module 04: Session Management

- Secure handling.
- Fixation prevention.
- Hijacking detection.



CyberouS

Module 5: Authentication and Authorization

- Secure methods.
- Multi-factor auth.
- Role-based access.

Module 6: Cross-Site Scripting (XSS) Prevention

- Output encoding.
- Content security policy.
- XSS filtering.

Module 7: Cross-Site Request Forgery (CSRF) Protection

- CSRF tokens.
- SameSite cookie.
- Anti-CSRF tokens.

Module 8: SQL Injection (SQLi) Mitigation

- Prepared statements.
- Parameterized queries.
- Input validation.



CyberouS

Module 9: Security Headers Implementation

- Content Security Policy.
- Strict-Transport-Security.
- X-Content-Type-Options.

Module 10: Secure File Uploads

- File validation.
- Renaming uploads.
- Secure storage.

Module 11: Secure Coding Practices

- Least privilege.
- Coding standards.
- Code reviews.

Module 12: Error Handling and Logging

- Proper handling.
- Sensitive info logging.
- Monitoring.



CyberouS

Module 13: Security Testing Techniques

- Vulnerability scanning.
- Penetration testing.
- Code review.

Module 14: HTTPS Implementation

- SSL/TLS certificates.
- HTTPS redirection.
- Configuration.

Module 15: Security Headers Configuration

- HSTS.
- X-Content-Type-Options.
- X-Frame-Options.

Module 16: API Security

- Authentication.
- Rate limiting.
- Validation.



CyberouS

Module 17: Content Security Policy (CSP)

- Content sources.
- XSS mitigation.
- Violation reporting.

Module 18: Server-Side Request Forgery (SSRF) Prevention

- Domain whitelisting.
- URL parameter validation.
- Network limits.

Module 19: Browser Security

- Sandboxing.
- Security features.
- Same-origin policy.

Module 20: Security Education and Training

- Awareness programs.
- Developer training.
- Continuous improvement.



CyberouS

Month :-8

Mobile Application Security

Course Outline:

Module 01: Understanding Mobile App Security

- Importance.
- Common vulnerabilities.
- Impact of breaches.

Module 02: OWASP Mobile Top 10

- Data storage.
- Server-side controls.
- Transport layer protection.

Module 03: Authentication and Authorization

- Secure methods.
- Role-based access.
- Token-based authentication.

Module 04: Secure Data Storage

- Encryption.
- Key management.
- Data leak prevention.



Module 5: Network Security

- Secure protocols.
- Certificate pinning.
- Network configuration.

Module 6: Secure Coding Practices

- Input validation.
- Output encoding.
- Avoiding hardcoding.

Module 7: Authentication Bypass

- Weak mechanisms.
- Session vulnerabilities.
- Biometric security.

Module 8: Authorization Flaws

- Access control assessment.
- Privilege escalation.
- Access control checks.



CyberouS

Module 9: Insecure Communication

- SSL/TLS assessment.
- Man-in-the-middle.
- Data interception.

Module 10: Code Tampering

- App integrity.
- Code modification.
- Anti-tampering measures.

Module 11: Reverse Engineering

- Code obfuscation.
- Data storage.
- Decompilation prevention.

Module 12: Input Validation

- User input sanitization.
- Injection prevention.
- External data validation.



CyberouS

Module 13: Side Channel Data Leakage

- App permissions.
- Data exposure.
- Clipboard security.

Module 14: Sensitive Information Disclosure

- Memory security.
- Log protection.
- Error message security.

Module 15: Session Handling

- Fixation prevention.
- Secure management.
- Timeout settings.

Module 16: Client-Side Security Controls

- Data storage.
- WebView controls.
- Injection prevention.



CyberouS

Module 17: Push Notification Security

- Secure handling.
- Data in notifications.
- Prevention measures.

Module 18: Mobile App Testing Techniques

- Dynamic analysis.
- Static analysis.
- Manual testing.

Module 19: Secure Update Mechanisms

- Update security.
- Authenticity validation.
- Secure channels.

Module 20: Security Education and Awareness

- Developer training.
- User education.
- Promoting awareness.



CyberouS

Month :-9

Network Security

Course Outline:

Module 01: Understanding Network Security

- Importance.
- Threat landscape.
- Security objectives.

Module 02: Firewalls

- Types (stateful, stateless).
- Access control lists (ACLs).
- IDS/IPS.

Module 03: Network Segmentation

- VLANs.
- Subnetting.
- DMZ setup.

Module 04: Encryption

- VPN.
- SSL/TLS.
- IPsec.



Cyberous

Module 5: Access Control

- User authentication.
- RBAC.
- NAC.

Module 6: Wireless Security

- WPA3/WPA2.
- SSID hiding.
- MAC filtering.

Module 7: Network Monitoring

- Traffic analysis.
- Log monitoring.
- Behavior analysis.

Module 8: Intrusion Detection/Prevention

- Signature-based.
- Anomaly-based.
- Real-time blocking.



CyberouS

Module 9: Vulnerability Management

- Scanning.
- Patching.
- Updates.

Module 10: Network Hardening

- Service disablement.
- Least privilege.
- Strong passwords.

Module 11: DNS Security

- DNSSEC.
- Filtering.
- DDoS protection.

Module 12: Network Forensics

- Incident response.
- Analysis.
- Evidence gathering.



CyberouS

Module 13: Virtualization Security

- Hypervisor security.
- VM isolation.
- Migration security.

Module 14: Cloud Network Security

- Firewall setup.
- API security.
- Data transfer security.

Module 15: Network Access Control (NAC)

- Compliance checks.
- Authentication.
- Access enforcement.

Module 16: Secure Protocols

- SSH.
- HTTPS.
- SNMPv3.



CyberouS

Module 17: Network Device Security

- Router/switch hardening.
- Firmware updates.
- Access control.

Module 18: Web Application Firewalls (WAF)

- Protection.
- Filtering.
- Updates.

Module 19: BYOD Security

- MDM.
- Containerization.
- Data segregation.

Module 20: Network Security Best Practices

- Audits.
- Training.
- Incident response planning.



Month :-10

IoT

Course Outline:

Module 01: Understanding IoT

- Definition and importance.
- Diverse device range.
- Connectivity significance.

Module 02: IoT Security Challenges

- Large attack surface.
- Resource constraints.
- Lack of standardized protocols.

Module 03: Device Authentication

- Secure provisioning.
- Strong authentication.
- Identity management.

Module 04: Data Encryption

- End-to-end encryption.
- In transit and at rest.
- Key management.



CyberouS

Module 05: Secure Communication Protocols

- MQTT.
- CoAP.
- HTTPS.

Module 06: Firmware Security

- Secure boot.
- Code signing.
- Update mechanisms.

Module 07: Access Control

- RBAC.
- Access policies.
- ACLs.

Module 08: Network Segmentation

- Separating networks.
- VLANs.
- Subnetting.



CyberouS

Module 09: Device Management

- Remote monitoring.
- Configuration.
- Lifecycle management.

Module 10: Physical Security Measures

- Tamper resistance.
- Secure enclosures.
- Access controls.

Module 11: Privacy Protection

- Minimize data collection.
- Data anonymization.
- Consent-based sharing.

Module 12: Secure Supply Chain

- Vendor assessments.
- Secure coding.
- Third-party validation.



CyberouS

Module 13: OTA Updates

- Secure mechanisms.
- Integrity checks.
- Rollback protection.

Module 14: Security Monitoring

- Anomaly detection.
- IDS.
- Event logging.

Module 15: Edge Computing Security

- Edge device security.
- Containerization.
- Access controls.

Module 16: Cloud Integration Security

- Secure communication.
- Data encryption.
- IAM.



CyberouS

Module 17: Blockchain for IoT Security

- Immutable records.
- Identity management.
- Supply chain transparency.

Module 18: Cyber-Physical System Security

- Physical process integrity.
- Integration with IoT.
- Fail-safe mechanisms.

Module 19. IoT Forensics

- Incident investigation.
- Evidence collection.
- Root cause analysis.

Module 20. Standardization and Regulation

- Security standards.
- Regulatory compliance.
- Industry initiatives.



CyberouS

Month :-11

End Point Security

Course Outline:

Module 01: Understanding Endpoint Security

- Definition.
- Importance.
- Role in network protection.

Module 02:Endpoint Security Challenges

- Proliferation.
- Diverse devices.
- Remote work impact.

Module 03: Antivirus and Antimalware Protection

- Real-time scanning.
- Signature-based detection.
- Behavioral analysis.

Module 04: Firewall Protection

- Host-based.
- Application control.
- Traffic filtering.



CyberouS

Module 05: Patch Management

- Vulnerability assessment.
- Deployment.
- Timely updates.

Module 06: Device Encryption

- Full disk encryption.
- File-level encryption.
- BitLocker/FileVault.

Module 07: Data Loss Prevention (DLP)

- Content inspection.
- Data classification.
- Policy enforcement.

Module 08: Endpoint Detection and Response (EDR)

- Threat detection.
- Incident response.
- Endpoint remediation.



Cyberous

Module 09: Application Whitelisting

- Approved apps list.
- Unauthorized software prevention.
- Attack surface reduction.

Module 10: Behavior Monitoring

- Abnormal behavior detection.
- Anomaly-based detection.
- Behavioral analysis.

Module 11: Email Security

- Spam filtering.
- Phishing protection.
- Attachment scanning.

Module 12: Web Security

- URL filtering.
- Malicious site blocking.
- Content filtering.



CyberouS

Module 13: Endpoint Isolation

- Infected endpoint isolation.
- Network segmentation.
- Containment measures.

Module 14: Mobile Device Management (MDM)

- Device enrollment.
- Remote wipe.
- App blacklisting.

Module 15: Remote Access Security

- VPN connections.
- Multi-factor authentication.
- Access control policies.

Module 16: Identity and Access Management (IAM)

- User authentication.
- Access control policies.
- Privileged access management.



CyberouS

Module 17: Security Policies and User Awareness

- Security training.
- Policy enforcement.
- User behavior monitoring.

Module 18: Host Intrusion Prevention Systems (HIPS)

- System integrity monitoring.
- Unauthorized change prevention.
- File integrity checking.

Module 19: Secure Configuration Management

- Hardening guidelines.
- Baseline configurations.
- Continuous monitoring.

Module 20: Endpoint Security Best Practices

- Regular updates.
- Layered security.
- Continuous improvement.



CyberouS

Month :-12

Cloud Security

Course Outline:

Module 01: Understanding Cloud Security

- Definition.
- Importance.
- Deployment models.

Module 02: Cloud Security Challenges

- Breaches.
- Compliance risks.
- Insider threats.

Module 03: Identity and Access Management (IAM)

- Authentication.
- RBAC.
- MFA.

Module 04: Data Encryption

- In transit.
- At rest.
- Key management.



CyberouS

Module 5: Network Security

- VPCs.
- Segmentation.
- Firewalls.

Module 6: Security Compliance

- Standards.
- Auditing.
- Assessments.

Module 7: Data Loss Prevention (DLP)

- Classification.
- Inspection.
- Enforcement.

Module 8: Incident Response and Forensics

- Detection.
- Response plan.
- Investigation.



CyberouS

Module 9: Cloud Access Security Broker (CASB)

- Shadow IT discovery.
- DLP.
- Access control.

Module 10: Security Monitoring and Threat Intelligence

- Continuous monitoring.
- Threat detection.
- SIEM.

Module 11: Secure DevOps Practices

- CI/CD security.
- Container security.
- IaC security.

Module 12: API Security

- Authentication.
- Authorization.
- Rate limiting.



CyberouS

Module 13: Container Security

- Image scanning.
- Isolation.
- Runtime security.

Module 14: Serverless Security

- Function security.
- Least privilege.
- Configuration security.

Module 15: Backup and Disaster Recovery

- Regular backups.
- DR planning.
- Redundancy.

Module 16: Vendor Security Assurance

- Assessments.
- Reviews.
- Compliance verification.



CyberouS

Module 17: Encryption Key Management

- Generation.
- Rotation.
- Storage.

Module 18: Cloud Security Best Practices

- Audits.
- Training.
- Improvement.

Module 19: Secure Data Migration

- Encryption.
- Integrity verification.
- Migration tools.

Module 20: Cloud Security Governance

- Policy enforcement.
- Risk assessment.
- Culture promotion.