CYBER ZIKSA

91213 07637

CyberZiksa is a cybersecurity training and career-oriented learning platform focused on building job-ready skills through hands-on, practical cybersecurity education.

It offers structured programs in areas like SOC operations, ethical hacking, penetration testing, malware analysis, digital forensics, cloud security, and threat intelligence.
The training is designed with a strong real-world simulation approach, including attack–defense labs and industry-relevant scenarios.

CyberZiksa emphasizes hands-on labs, expert mentorship, and certification-aligned curriculum mapped to standards like CompTIA, EC-Council, and (ISC)².It also focuses on placement support, resume building, interview preparation, and career guidance for cybersecurity roles.
Overall, it is positioned as a job-oriented cybersecurity training institute aiming to bridge the skills gap and prepare learners for SOC and security engineering roles

Introduction to Cybersecurity

- ↻ Understanding Devices and Infrastructure
- ↻ The evolution of Cybersecurity
- ↻ Cybersecurity & situational awareness
- ↻ The Cybersecurity skills gap
- ↻ Difference between
- ↻ Information Security & Cybersecurity
- ↻ Cybersecurity objectives
- ↻ Cybersecurity Roles

Hands On Labs - MITRE ATT&CK framework, NIST Cybersecurity Framework basics, and CERT

Understanding Devices and Infrastructure

- ↻ Infrastructure Terminology
- ↻ Designing with Security in Mind
- ↻ Network Topology
- ↻ OSI Layers & TCP/IP Model
- ↻ IPv4 & Ipv6
- ↻ Ports & protocols
- ↻ Port numbers
- ↻ Firewalls
- ↻ VPNs and VPN Concentrators
- ↻ Intrusion Detection Systems
- ↻ Router
- ↻ Switch
- ↻ Proxy
- ↻ Load Balancer
- ↻ Access Point
- ↻ Network Access Control (NAC)
- ↻ Mail Gateway

Hands On Labs - Windows/Linux command line (ipconfig, ifconfig, ping, traceroute, netstat, nslookup), network analysis using Wireshark, basic network topology

Ethical Hacking Content

- Introduction to Ethical hacking
- Lab setup for Virtual Machines
- Penetration Testing
- Foot Print/Information Gathering
- Scanning
- Vulnerability Analysis
- Sniffing & Man-In-Middle
- System Hacking
- Metasploit Attacks.
- Malware Threats
- Phishing Attacks
- Social Engineering Attacks
- Hacking webserver
- Web Applications Threats
- OWASP Top 10
- SQL Injection
- Wireless Attacks
- Mobile Threats
- IOT Attacks
- Cloud Threats
- Morden AI Threats
- Cryptography

Hands on Labs - Kali Linux, Parrot OS, Nmap, Zenmap, Metasploit, Burp Suite, Wireshark, Nessus, OpenVAS, SQLmap, Aircrack-ng, Hashcat, Ettercap, Bettercap, Hydra, John the Ripper, OWASP ZAP, Gophish, Social-Engineer Toolkit (SET), theHarvester

Security Operations Center (SOC)

- SOC Overview
- SOC Team Structure
- Security Devices
- Tier 1 Responsibilities
- Tier 2 Responsibilities
- Tier 3 Responsibilities
- SOC Workflow and Escalation Path
- Cyber Kill Chain

Cyber Incident Response

- Introduction to SIEM
- Overview of Splunk Architecture
- Installation and Setup of Splunk
- Splunk Ingestion and Indexing
- Writing SPL Queries
- Splunk Dashboards and Alerts
- QRadar Architecture and Flow Collection
- Types of Alerts Handled in SOC
- Daily SOC Monitoring Activities
- KPIs and Metrics for SOC
- Log Collection Strategy
- Log Parsing and Normalization
- Key SOC Log Sources
- Firewall Logs
- IDS/IPS Logs
- DNS Logs
- Endpoint Logs (Sysmon/EDR)
- Active Directory Logs
- Cloud Logs (CloudTrail, Azure Activity)
- Use Case Design in SIEM

- ↻ Rule Writing – SPL (Splunk), AQL (Qradar)
- ↻ MITRE ATT\&CK Mapping to Alerts
- ↻ Threat Hunting Basics
- ↻ Alert Enrichment Techniques
- ↻ Alert Suppression & False Positive Handling
- ↻ Ticketing Systems (ServiceNow, JIRA) Integration

Hands On Labs - Splunk, IBM QRadar, Jira, Windows Event Viewer, Sysmon, Cyber Kill Chain Analysis, MITRE ATT&CK Navigator, Report Writing

Email Security

Core Principles: Phishing, Spear Phishing, BEC, Malware Delivery, Domain Spoofing
Authentication & Analysis: Header Forensics, SPF, DKIM, DMARC, Mail Flow Analysis
Security Stack: Microsoft Defender for Office 365, Mimecast, Secure Email Gateways, Sandboxing

SOC Operations: Phishing Triage, IOC Extraction, Mailbox Threat Hunting
Response & Mitigation: Quarantine, Message Purge, User Awareness & Reporting

Hands On Labs - Phishing Analysis, Mimecast, Proofpoint, Gmail Admin Console, Email Header Analyzer tools, MXToolbox, Sandbox Analysis, Any.Run, VirusTotal, MailHog.

Malware Analysis

Core Principles : Virus, Worm, Trojan, Ransomware, Spyware, Rootkit, Fileless Threats
Threat Landscape: Infection Chain, Behavioral Profiling, Persistence Mechanisms
Static Analysis: PE Structure Inspection, String Deobfuscation, Hashing (MD5/SHA256), Metadata Analysis

Dynamic Analysis: Sandbox Detonation (e.g., ANY.RUN), Runtime Monitoring (Process Monitor, RegShot, Wireshark, TCPView)
Reverse Engineering & IOCs: Disassembly (Ghidra / IDA Free), Debugging (x64dbg), Packing/Obfuscation, IOC Extraction

Hands On Labs - Process Explorer, Process Monitor, PEView, OllyDbg, Strings, IDA Free, Wireshark, RegShot, TCPView, ANY.RUN, VirusTotal, Cuckoo Sandbox.

Threat Intelligence

Core Principles: Threat Intelligence Concepts, Intelligence Lifecycle, Strategic / Tactical / Operational / Technical TI
Data Sources & Frameworks: IOC Formats (IP, Hash, URL, Domain), VirusTotal, AlienVault OTX, Recorded Future, Shodan, urlscan.io, MITRE ATT&CK
Operationalization: IOC Enrichment, Correlation & Integration in SIEM

Hands On Labs - VirusTotal, AlienVault OTX, Shodan, urlscan.io, MITRE ATT&CK Navigator, MISP (Malware Information Sharing Platform), OpenCTI, IBM X-Force Exchange, Recorded Future, Splunk, Qradar.

Cloud Security

Core Principles: Cloud Security Fundamentals, Shared Responsibility Model
Threat Landscape: Misconfigurations (e.g., Amazon S3 Buckets), API Abuse, Credential Theft, Identity Attacks, Lateral Movement
Response & Mitigation: Cloud Resource Exploitation, Logging Gaps, Monitoring & Access Control
Hands On Labs - AWS (IAM, S3)

AI in Cybersecurity

Core Principles: AI/ML Fundamentals, Supervised vs Unsupervised Learning, Use Cases in Cyber Defense
AI for Detection: Anomaly Detection, Behavioral Analytics, Threat Prediction, UEBA
AI in SOC Operations: Automated Alert Triage, Threat Hunting Augmentation, SOAR Integration
Adversarial AI & Risks: AI Evasion Techniques, Data Poisoning, Model Abuse, Security Challenges

Identity & Access Management (IAM)

Core Principles & Lifecycle: IAM Fundamentals, Authentication vs Authorization, Identity Lifecycle (Joiner–Mover–Leaver)

Authentication & Federation: MFA, SSO, SAML, OAuth, OpenID Connect
Access Control Models: RBAC, ABAC, Least Privilege, Zero Trust
Identity Governance & Security: PAM, Access Reviews, Compliance, Role Mining
Monitoring & Practical (Okta): Hands-on with Okta (User Provisioning/Deprovisioning, SSO Setup, MFA Policies, Directory Integration

Hands On Labs - Okta Admin Console, Okta Identity Cloud, SAML Tracer, OAuth 2.0 Playground, Postman, Active Directory (AD), Azure AD, LDAP tools, MFA simulator.

Capstone Projects

1. SOC Simulation Project
Build a SOC environment using Splunk/QRadar to analyze logs, detect attacks mapped to MITRE ATT&CK, and perform alert triage with incident reporting.

2. Penetration Testing Project
Conduct full ethical hacking on a lab system using Kali Linux covering recon, scanning, exploitation, and OWASP Top 10 vulnerabilities with final report.

3. Email Security & Phishing Analysis
Simulate phishing attacks using Gophish, analyze emails using headers and sandbox tools, and perform SOC-style IOC extraction and mitigation.

4. Cloud Security Attack & Defense Project
Exploit AWS misconfigurations using IAM/S3 labs, detect activity through logs, and implement cloud monitoring and security hardening.

5. Malware & Threat Intelligence Pipeline
Analyze malware using static/dynamic tools, extract IOCs, enrich them via VirusTotal/Shodan, and integrate findings into SIEM for detection.

Career Opportunities after this Course

- SOC Analyst (L1/L2/L3)
- Cyber Security Analyst
- SIEM Engineer
- Incident Responder
- Threat Intelligence Analyst
- Threat Hunter
- Network Security Engineer
- Cloud Security Engineer
- Penetration Tester (Ethical Hacker)
- DevSecOps Engineer

Industry-Recognized Certifications You Can Write with This Course

- CompTIA Security+
- Certified SOC Analyst (CSA)
- Certified Ethical Hacker (CEH)
- GIAC Security Essentials (GSEC)
- Cyber Threat Intelligence Analyst (CTIA)

Why CYBER ZIKSA

Cyber Ziksa is a job-oriented cybersecurity program focused on hands-on SOC, Ethical Hacking, Cloud, and IAM skills using real-world tools and industry-aligned labs.

- All trainers are real-time industry professionals with hands-on experience
- 70% practical and 30% theory-based learning approach
- Individual lab access for every student for real practice
- Weekly assignments including presentations, mock interviews, and online exams
- Job-ready curriculum focused on real-world SOC, Ethical Hacking, Cloud, and IAM skills
- Continuous mentorship and career guidance until placement readiness

More Details

91213 07637

Cyberziksa.com