OWASP RANCHI

Join the WhatsApp Group!

Navigating the Cybersecurity Skills Landscape

Understanding the Most In-Demand Expertise

Zeshan Ahmad

Cybersecurity Professional, CISA, CISM, ISO 27001 Lead Auditor

Security Risk Analyst

TIAA Cyber Associate

Deloitte. Solution Delivery Advisor

OWASP RANCHI

whoami

Performance Management | Risk Management | M&A | Cloud | Supply Chain

My Skill-sets

- Technical Reviewer: CISM Exam
- Published Google Dorks
- Certified Information Security Manager
- Certified Information Systems Auditor
- ISO 27001 Lead Auditor
- Judge for various ISACA scholarships

Scan to know more about me

In-Demand

According to study by TeamLease Digital, as of May 2023, there were around 40,000 job opportunities in the industry, indicating a high demand for skilled cybersecurity professionals. However, there is a significant skill gap of 30 per cent, posing a challenge for the industry.

Cybersecurity skills are critical for protecting organizations from cyber threats. Stay ahead with these top in-demand skills for 2024.

2025 Salary & Skills Matrix (India)

OWASP RANCHI

Role	Experience Level	Salary Range (INR)	Top Required Skill
Security Analyst	Entry (0-2 Yrs)	₹5,00,000 - ₹8,00,000	Log Analysis, SIEM (Splunk)
Penetration Tester	Mid (2-4 Yrs)	₹10,00,000 - ₹18,00,000	Burp Suite, Python, Web App Sec
Security Engineer	Mid (3-5 Yrs)	₹12,00,000 - ₹25,00,000	Cloud Security (AWS), Automation
Incident Responder	Senior (4+ Yrs)	₹15,00,000 - ₹25,00,000	Forensics, Crisis Management
Red Teamer	Senior (5+ Yrs)	₹20,00,000 - ₹35,00,000+	Advanced Evasion, C2 Frameworks
Malware Analyst	Specialist	₹18,00,000 - ₹30,00,000	Assembly, Reverse Engineering

Cyber Skills Demand

Cybersecurity is essential in today's tech world. Stay ahead with these technical skills.

Network Security

Definition

Measures taken to protect the integrity, confidentiality, and availability of network and data.

Importance:

- Data Protection: Prevents unauthorized access and data breaches.
- Integrity: Ensures that data remains unchanged and trustworthy.
- Availability: Guarantees that network resources are accessible to authorized users.

Key Components

- Firewalls: Filters incoming and outgoing traffic to prevent unauthorized access.
- VPNs (Virtual Private Networks): Secures remote connections.
- IDS/IPS (Intrusion Detection/Prevention Systems): Monitors and responds to suspicious activities.

OWASP RANCHI

Network Security Key Skills

Firewall Management:

- Definition: Configuring and managing rules to control network traffic.
- Example Tools: pfSense, Cisco ASA, Palo Alto

VPNs

- Definition: Creating secure connections over the internet for remote access.
- Example Tools: OpenVPN, Cisco AnyConnect, NordVPN.

IDS & IPS

- Definition: Monitoring network traffic for suspicious activity and responding accordingly.
- Example Tools: Snort, Suricata, Cisco Firepower.

Where can I acquire these skills?

- Cisco CCNA
- Comptia Network +

- THM: Firewalls
- THM: Extending Your Network
- Udemy:OpenVPN Server for your home
- THM Snort

OWASP RANCHI

Cloud Security

Definition

A set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Importance:

- Data Protection: Ensures data privacy and security in the cloud.
- Application Security: Protects applications hosted on cloud platforms from vulnerabilities and breaches.
- Infrastructure Security: Safeguards the physical and virtual components of cloud environments from unauthorized access and cyber threats.

Trends

- Increased Adoption: Growing number of organizations migrating to the cloud.
- Advanced Threats: Rise in sophisticated cyber attacks targeting cloud environments.
- Regulatory Compliance: Need to adhere to industry standards and regulations.

OWASP RANCHI

Cloud Security Key Skills

Cloud Platforms

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Cloud Security Tools

- Definition: Proficiency in tools that help secure cloud environments.
- Importance: Vital for monitoring, protecting, and managing cloud security.
- Examples: AWS Security Hub, Azure Security Center, Google Cloud Security Command Center.

Data Encryption

- Definition: Techniques and tools used to protect data at rest and in transit.
- Importance: Ensures data privacy and compliance with regulations.
- Examples: AWS Key Management Service (KMS), Azure Key Vault, Google Cloud Key Management.

Where can I acquire these skills?

- AWS Certified Security - Specialty
- Microsoft Certified: Azure Security Engineer Associate
- GCP Professional Cloud Security Engineer

OWASP RANCHI

Application Security

Definition

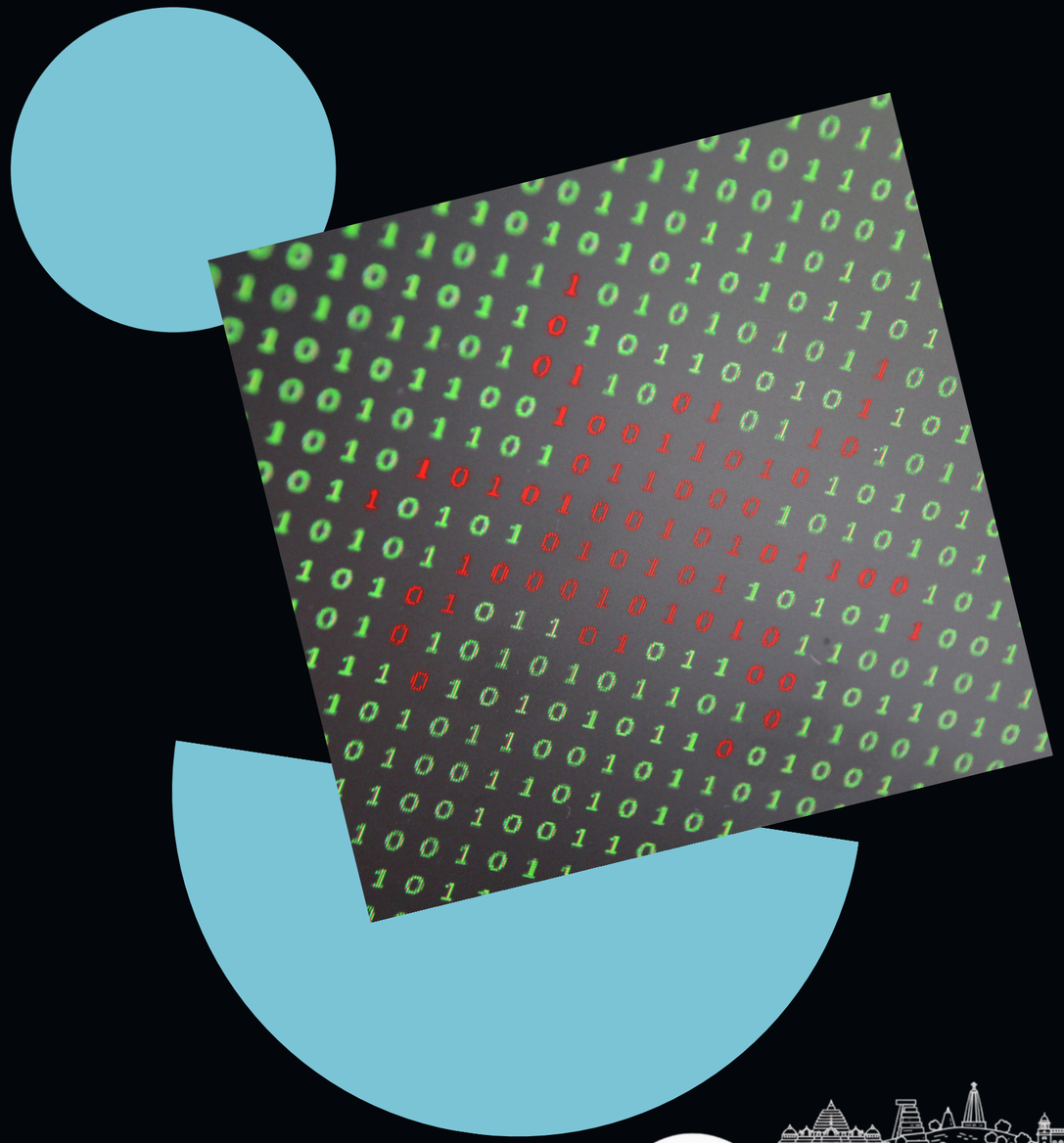
The process of making applications more secure by finding, fixing, and enhancing the security of applications.

Importance:

- Data Protection: Ensures that sensitive data handled by applications is protected from unauthorized access and breaches.
- Integrity: Maintains the trustworthiness of applications and their data.
- Compliance: Helps organizations meet regulatory requirements and industry standards.

Key Areas

- Secure Coding Practices: Writing code that is resistant to attacks.
- Vulnerability Assessment: Regularly testing applications to identify and fix security flaws.
- Security Configuration: Ensuring applications are configured securely to minimize risks.



OWASP RANCHI

AppSec Key Skills

Secure Coding Practices:

- Definition: Writing code that is resistant to common vulnerabilities and attacks.
- Importance: Prevents security flaws from being introduced during development.

VA & PT

- Definition: Regularly testing applications to identify and fix security flaws.
- Importance: Helps discover and remediate vulnerabilities before attackers can exploit them.
- Tools: OWASP ZAP, Burp Suite, Nessus

AppSec Management

- Definition: Ensuring applications are configured securely and monitored for security issues.
- Importance: Maintains the security posture of applications throughout their lifecycle.
- Tools: SIEM, WAF, RASP,

Where can I acquire these skills?

- INE EJPT
- OffSec OSCP
- ISC2 CSSLP

- picoctf.org
- TryHackMe
- Hack The Box
- Udemy

OWASP RANCHI

Endpoint Security

Definition

The practice of securing endpoints or entry points of end-user devices from being exploited by malicious actors.

Importance:

- Data Protection: Ensures sensitive data on endpoints is protected from unauthorized access and breaches.
- Threat Prevention: Helps prevent malware, ransomware, and other types of cyber attacks.
- Compliance: Assists organizations in meeting regulatory and industry standards.

Key Components

- Antivirus/Antimalware: Detects and removes malicious software.
- Endpoint Detection and Response (EDR): Provides continuous monitoring and response to advanced threats.
- Data Loss Prevention (DLP): Prevents sensitive data from being leaked or stolen from endpoints.

OWASP RANCHI

Endpoint Key Skills

Antivirus and Antimalware Management:

- Definition: The ability to deploy, configure, and manage antivirus and antimalware software.
- Importance: Ensures endpoints are protected from a wide range of malware threats.

EDR

- Definition: Skills to utilize EDR solutions for continuous monitoring and response to threats.
- Importance: Enhances the ability to detect, investigate, and respond to advanced threats in real-time.

DLP

- Definition: Implementing and managing DLP solutions to prevent unauthorized data transfer.
- Importance: Protects sensitive data from being leaked or stolen through endpoints.
- Strategies: Policy creation and enforcement, user training, monitoring and reporting.

Where can I acquire these skills?

Microsoft Certified: Security, Compliance, and Identity Fundamentals

- Microsoft Learn:Manage Microsoft Defender for Endpoint
- Qualys EDR Foundation

OWASP RANCHI

Incident Response

Definition

Incident Response is the systematic approach to identifying, managing, and recovering from cybersecurity incidents to minimize damage and restore normal operations.

Importance:

Crucial for reducing the impact of incidents on business operations, reputation, and data integrity.

Key Components

- Incident Response Planning: Creating and maintaining a structured plan for responding to security incidents promptly and effectively.
- Forensic Analysis: Conducting detailed investigations to determine the root cause, scope, and impact of security breaches.
- Crisis Management: Coordinating with stakeholders to manage communication, decision-making, and recovery efforts during and after incidents.

OWASP RANCHI

Incident Response Key Skills

Incident Response Planning

- Definition: Creating and maintaining structured plans and procedures to respond effectively to security incidents.
- Importance: Ensures a coordinated and efficient response, minimizing downtime and reducing impact on operations..

Forensic Analysis

- Definition: Conducting detailed investigations to analyze and understand the nature, extent, and impact of security incidents.
- Importance: Provides critical insights for identifying the root cause, improving security measures, and preventing future incidents.

Crisis Management

- Definition: Coordinating with stakeholders to manage communication, decision-making, and recovery efforts during and after security incidents.
- Importance: Maintains stakeholder trust, minimizes reputational damage, and facilitates swift recovery.

Where can I acquire these skills?

EC-Council Certified Incident Handler Program

- THM SOC Level 1
- THM SOC Level 2
- THM Intro to IR and IM
- HTB Incident Handling Process

OWASP RANCHI

IAM

Definition

Identity and Access Management (IAM) is a framework of policies and technologies ensuring that the right individuals have the appropriate access to technology resources.

Importance:

Critical for protecting sensitive data, ensuring regulatory compliance, and reducing the risk of unauthorized access and data breaches.

Key Components

- Identity Management: Processes and technologies for managing digital identities, including user provisioning and de-provisioning.
- Access Management: Tools and policies for controlling access to resources based on user roles and permissions.
- Authentication and Authorization: Mechanisms for verifying user identities (authentication) and determining access levels (authorization).

OWASP RANCHI

IAM Key Skills

Identity Management

- Importance: Ensures accurate and efficient management of digital identities, which is critical for maintaining security and compliance.
- Tools: Microsoft Azure AD, Okta, SailPoint

Access Management

- Importance: Controls who has access to what resources, reducing the risk of unauthorized access and data breaches.
- Tools: IBM Security Identity Governance and Intelligence, RSA SecurID, CyberArk

Authentication and Authorization

- Importance: Verifies user identities and determines their access rights, crucial for maintaining secure access to resources.
- Tools: OAuth, OpenID Connect, LDAP (Lightweight Directory Access Protocol)

Where can I acquire these skills?

- Certified Identity and Access Manager (CIAM)
- CyberArk Defender
- SailPoint IdentityNow Professional

- SailPoint Community Edition
- Okta Free Trial and Developer Edition
- Duo Security Free Trial and Learning Hub

Risk Management

Definition

Cybersecurity risk management involves identifying, assessing, and prioritizing risks to an organization's information assets and implementing measures to mitigate or manage those risks.

Importance:

Protection of Assets: Ensures the confidentiality, integrity, and availability of critical information.
Compliance: Helps organizations comply with regulatory requirements and avoid legal penalties.
Business Continuity: Supports the development of strategies to maintain operations during and after a cyber incident.
Reputation Management: Reduces the risk of data breaches that can damage an organization's reputation and trustworthiness.

OWASP RANCHI

Risk Management Key Skills

Risk Assessment

- Definition: The process of identifying, analyzing, and evaluating risks to determine their potential impact.
- Tools: Risk assessment frameworks (e.g., NIST, ISO 27001), risk analysis software (e.g., FAIR, RiskWatch).

Risk Mitigation

- Definition: Implementing measures to reduce the impact or likelihood of identified risks.
- Tools: Security controls, patch management systems.

Risk Monitoring:

- Definition: Continuously tracking the risk environment to detect new threats and assess the effectiveness of existing controls.
- Tools: Continuous monitoring tools (e.g., Nessus, Qualys), security dashboards.

Communication and Reporting:

- Definition: Effectively conveying risk findings and mitigation plans to stakeholders.

Where can I acquire these skills?

- ISC2 CC
- ISACA CRISC
- ISACA CISM
- ISACA CISA

- Cybrary Courses
- NIST Publications
- ISO Standards
- SANS Reading Room
- Youtube Professor Messer

Underrated Soft-Skills

Communication Skills

Critical Thinking

Adaptability

Attention to Detail

Teamwork and Collaboration

OWASP RANCHI

EXTRA BONUS

Cybersecurity Career Pathway

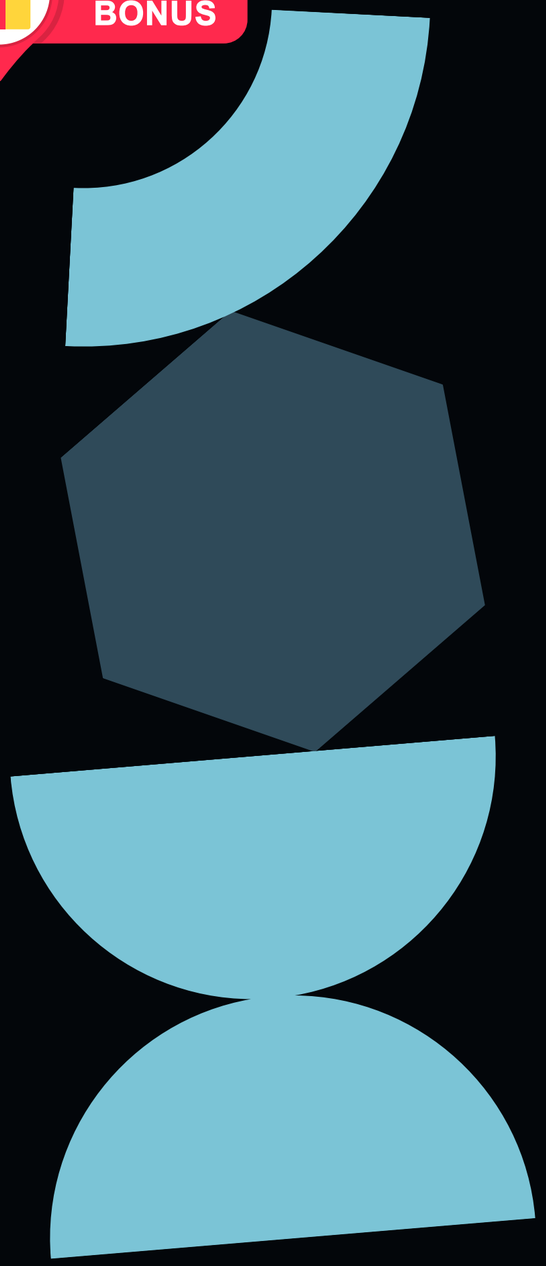
This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role.

Security Certification Roadmap

This is a roadmap for cybersecurity certifications, it l outlines various certifications and their paths, categorized by skill level and specialization.

OWASP RANCHI

EXTRA BONUS



Play this interactive game to learn what you want to do

OWASP RANCHI

Thank You

Share you feedback from the session

OWASP RANCHI

OWASP

RANCHI