IBM Cyber Campus

Pioneering the Future of Cybersecurity Training

Udit Sharma

Business Development Leader – IBM Cyber Campus

IBM Consulting

Vice Chair – IEEE LI Section

Email : udit.sharma1@ibm.com

•Size of the **Active** Cybersecurity Workforce: 5.5 M Globally (0.1% YoY)

•Size of the Cyber Workforce **Gap**: 4.8 M Globally (Up 19% YoY)

•Total Cyber Workforce Needed to Satisfy Demand:

10.3 M Globally (8.1% YoY)

Total US job Openings (2025) : 460,000

67% of organizations worldwide report a **staff shortage**, impacting their ability to prevent and troubleshoot cyber security issues.

78% of organizations within the education and government sectors report cyber security staffing shortages.

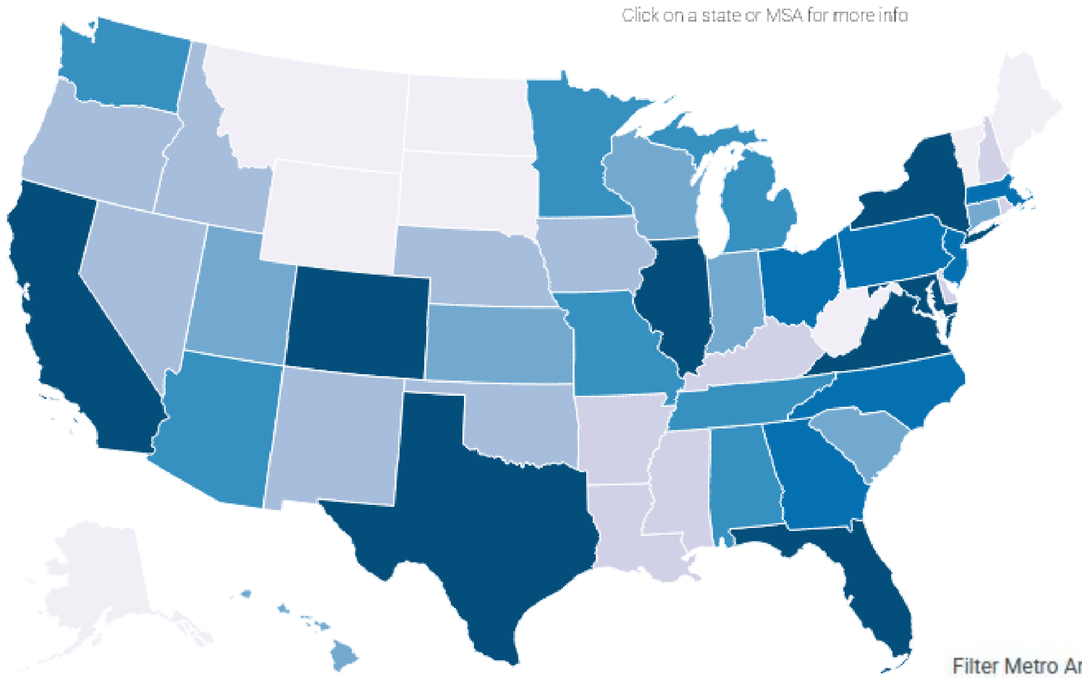
41% of security leaders within organizations with a shortage of cyber security staff cite the **inability to find enough qualified talent as** the primary reason.

90% of security leaders believe a skills shortage has **impacted their ability to implement** their cyber security strategy.

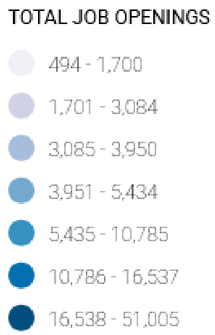
70% of security leaders say they **would value entry-level cyber experience** (1-3 years) over entry-level education (e.g., just a **bachelor's degree of 3-4 years**) when hiring for entry-level cybersecurity roles.

54% of security professionals would value cyber security **certifications** over just independent **competition** experience (e.g., hackathon etc) if asked to design their **ideal job candidate.**

https://www.stationx.net/cyber-security-job-statistics/

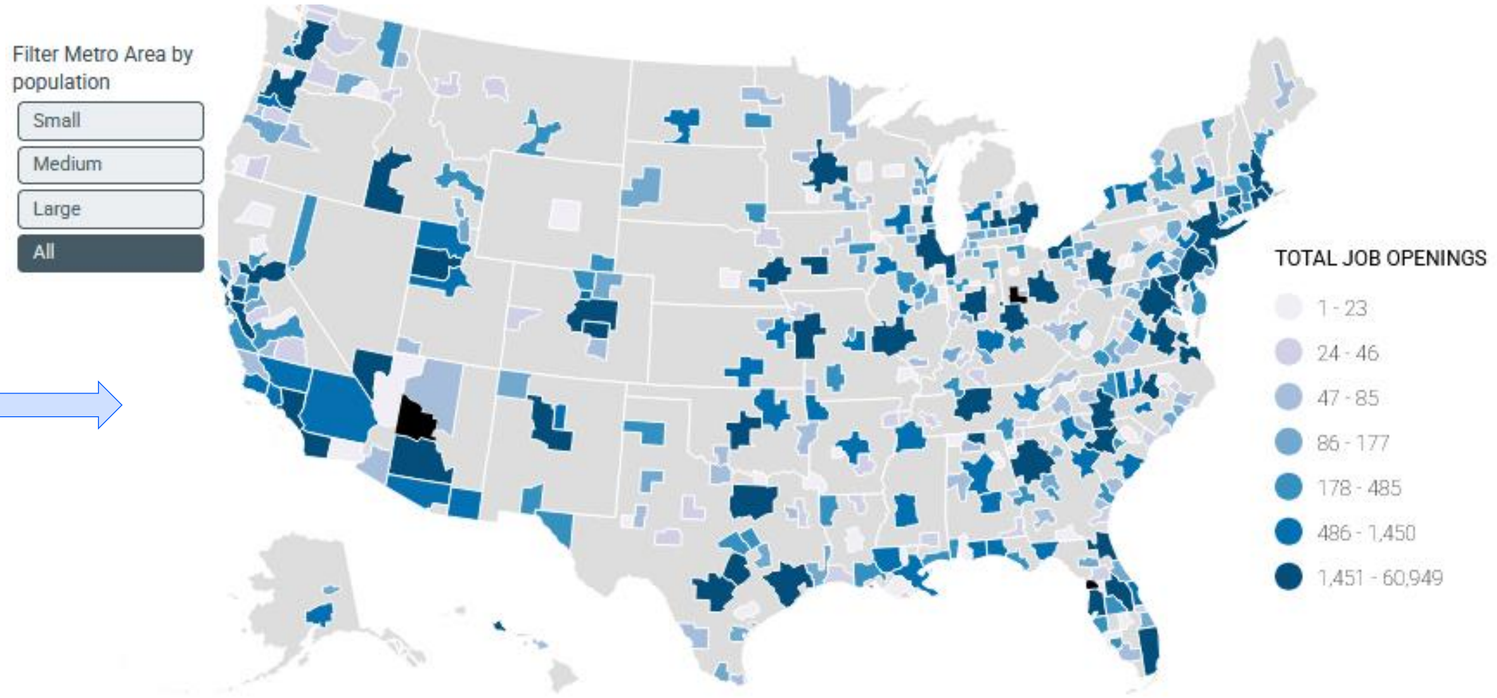


Total US job Openings (2025) : 460,000



Cybersecurity Job Openings by States

CyberSecurity Openings by Metro Areas



“Talent is everywhere; training opportunities are not”

Source: Arvind Krishna, IBM Chairman and CEO

Building Skills

IBM Commits to Skill 30 Million People Globally in Emerging Tech by 2030

One hundred seventy new partnerships and program expansions in more than 30 countries across the Americas, Asia Pacific, Europe, the Middle East, and Africa.

IBM Commits to Train 2 Million in AI in 3 Years (2023-2026)

With a Focus on **K-12**, **Underrepresented Communities, Universities and Colleges**.

Learners will benefit from a new generative AI course roadmap and collaborations with Non-Governmental Organizations (NGOs) worldwide.

Skills to Careers

IBM X-Force Cyber Ranges

Strengthening Business

The elite training your business leaders need to improve your readiness to respond to a breach effectively.

The IBM Cyber Campus

Growing the Workforce

Supporting universities and colleges with cutting-edge cyber range technology and learning resources to train students in the ever-evolving cybersecurity landscape.

The Student Career Journey Map

Educational Institutions & IBM Cyber Campus are teaming with Students on their Career Journey

Start of Cyber Journey

Predict Student Career Path

Student Career Exploration and Cyber Aptitude Assessments

Skills Development

Develop Student Career Skills

Educational Institutions powered by IBM Training and Challenge Labs and Skills Packs to earn industry IT and Security certifications

Experiential Learning

Connect the classroom with real-world experiences

Educational Institutions with IBM's immersive learning and real-world cyberattack simulations

Skills Measurement

Test Student proficiency levels and strengths

Connect learned skills and performance to verifiable data through learning pathways to earn IBM badges and certification

Job Market

Match Graduates to open jobs

Headhunters & Employers receive Graduates with validated evidence of acquired skills and experiences

Pathways to Careers

High School

Freshman through Senior Years

Earned IBM Badges and Industry Certifications

Jobs

Junior Cybersecurity Analyst ($50,000)

College

2 Years of Postsecondary Education

Associate Degree

Jobs

Cybersecurity Analyst ($73,000)
IT Security Specialist ($93,000)
Digital Forensic Examiner ($103,000)

University

4 Years of Postsecondary Education

Bachelor's Degree

Jobs

Cybersecurity Analyst ($92,000)
Information Security Analyst ($120,000)
Cybersecurity Engineer ($116,000-$208,000)

First-year starting salaries are illustrated

IBM Cyber Campus Components

- **Cyber Command/Training Centers (Physical Classrooms)**
  New and customized spaces equipped with cutting-edge education technology supporting today's dynamic cyber education use cases

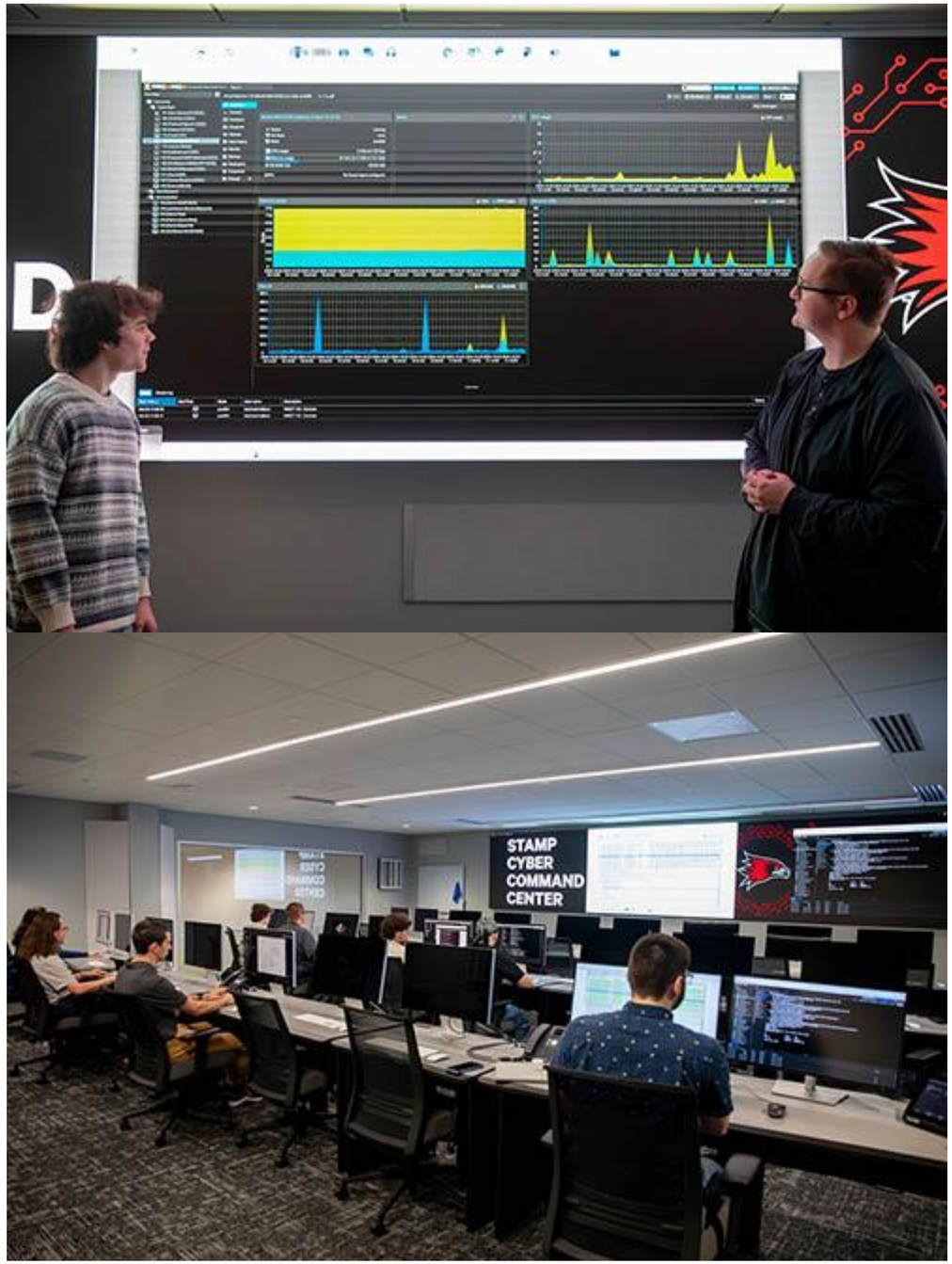
- **Enterprise Cyber Range Platform (Virtual)**
  No hardware or additional software costs

- **Learning Portal & Supplemental Learning Content**
  Tracking team and individual performances. Catalogs of cyber aptitude assessments, training & challenge labs, skill packs, and immersive cyberattack simulations

- **IBM Consulting Services**
  Supporting your curriculum, revenue generation opportunities, training, and faculty and staff support with **AI/Gen AI/Quantum/Cloud Services**.

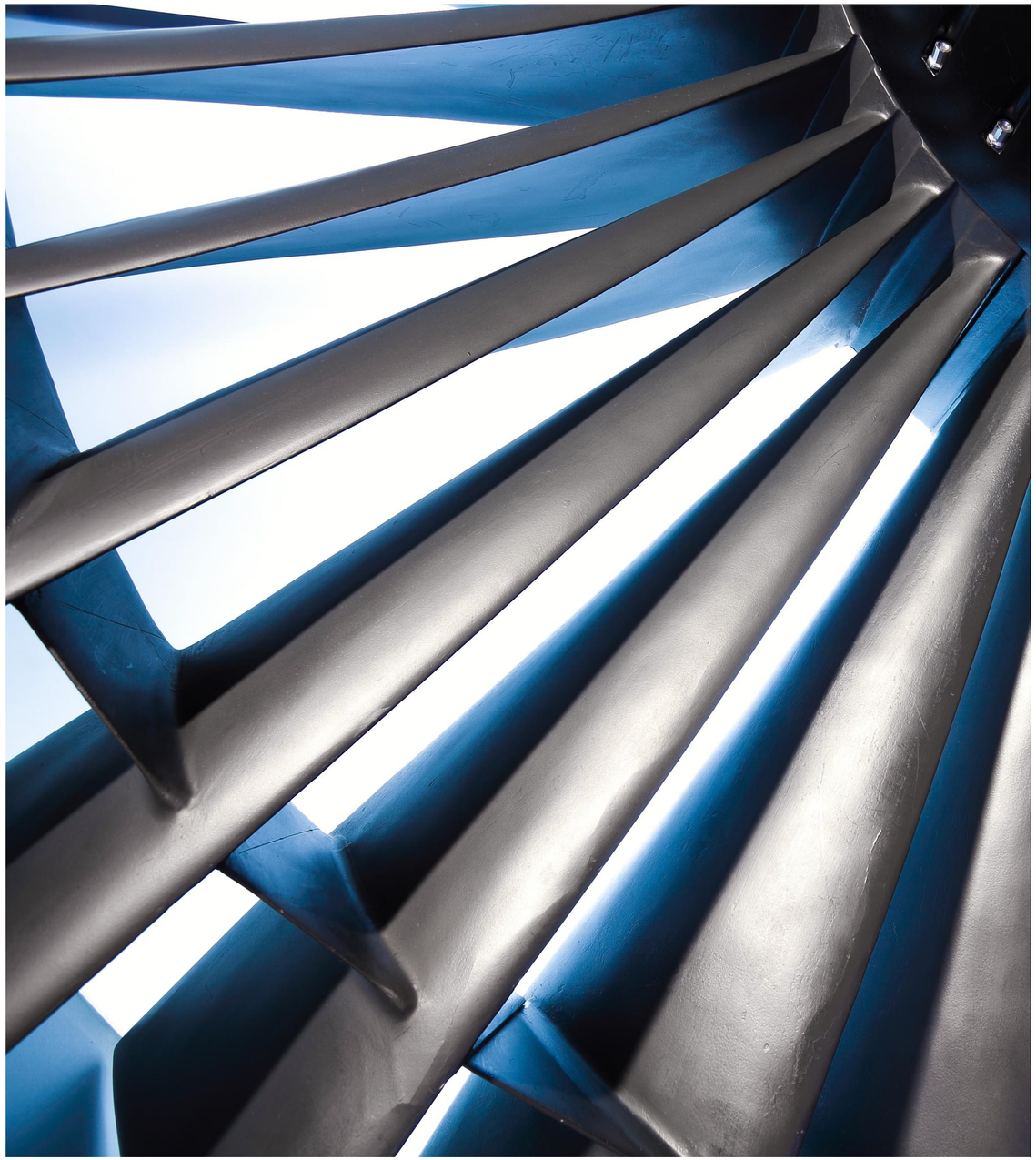
- **IBM Partners Ecosystem**
  Supporting the Student Career Journey and Career Success

Range & Center may be used together or separately.



Generative AI has given rise to a new generation of cyber threats.

Fortunately, the opposite is also true: Generative AI can fortify business defense. It will speed up security processes and recognize threats as quickly as they materialize.



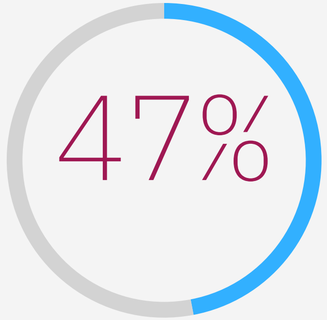
AI + Cybersecurity

When it comes to cybersecurity, fight fire with fire

	1	2	3
What leaders need to know	Generative AI ushers in a world of new risks and threats	Trustworthy generative AI isn't possible without secure data	Using generative AI for cybersecurity is a force multiplier
What leaders need to do	Treat generative AI like a burning platform and secure it now	Make trusted data the backbone of your organization	Reorient cybersecurity investments around speed and scale

Generative AI ushers in a world of new risks and threats

Executives believing adopting generative AI will lead to new kinds of attacks targeting their own AI model or services



$4.45m

the average cost of a data breach globally

$9.48m

the average cost of a data breach in US

51%

increase in AI cybersecurity budgets in 2023 compared to 2021 according to executives

43%

additional in AI cybersecurity budgets expected by 2025

96%

of executives say adopting generative AI makes a security breach likely in their organization within the next three years.

Trustworthy Generative AI isn’t possible without secure data

While…

84%

Of executives expect a wide variety of risks including catastrophic cybersecurity attacks to materialize, as they adopt generative AI,

And…

94%

of executives say it is important to secure AI solutions before deployment.

But only…

24%

of executives say, their generative AI projects will include a cybersecurity component within the next six months

&

69%

say innovation takes precedence over cybersecurity for generative AI

One in three executives say these risks can’t be managed without fundamentally new forms of governance, such as comprehensive regulatory frameworks and independent third-party audits

Using Generative AI for Cybersecurity is a force multiplier

52%

of executives say generative AI will help them better allocate resources, capacity, talent, or skills

92%

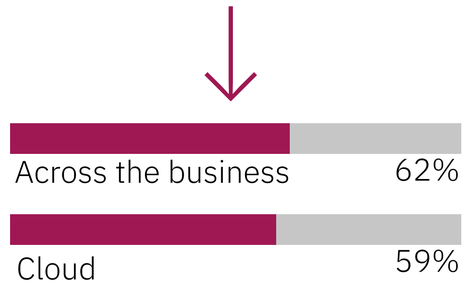
of executives they are more likely to augment or elevate than replace their cybersecurity workforce as they adopt generative AI

84%

of executives plan to prioritize generative AI cybersecurity solutions over conventional cybersecurity solutions

AI in cybersecurity can extend the multiplier effect across your enterprise ecosystem

84% of executives say that open innovation and ecosystems are important for their future growth strategy



Areas where generative AI capabilities will influence the selection of ecosystem partners over the next 2 years

Three things

Cyber-risk.
Data.
Cyber-resilience.

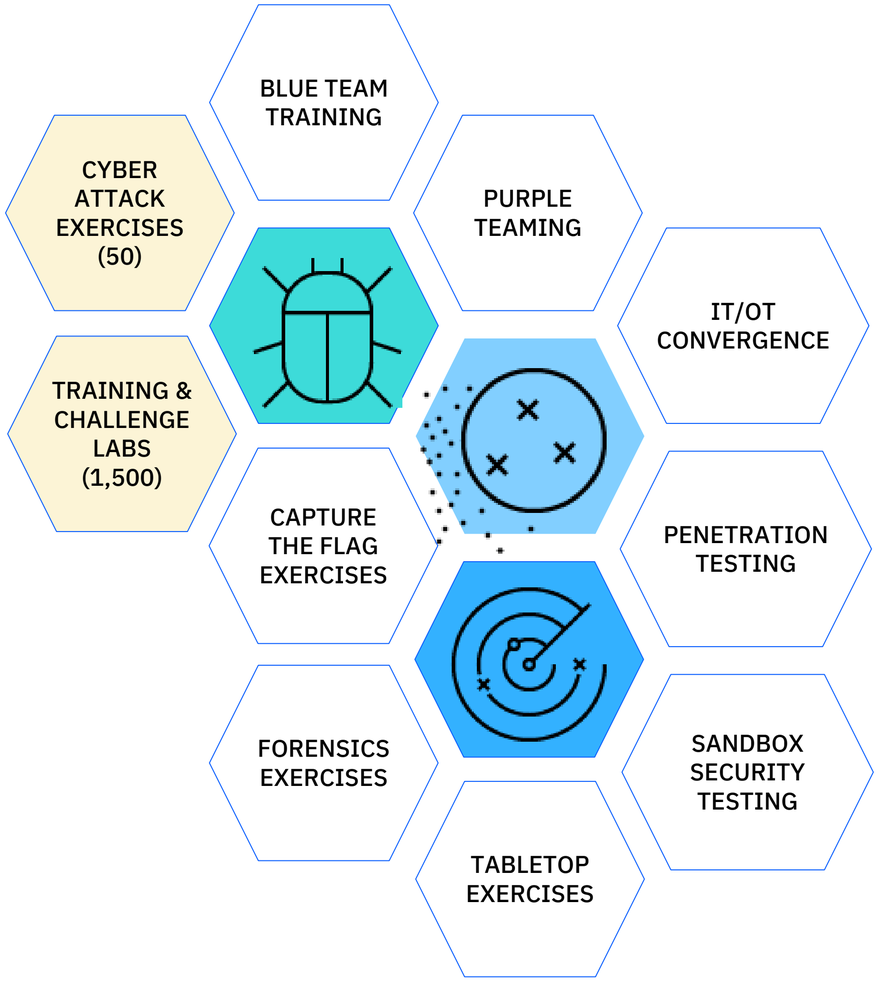
Commercial Cyber Range

IBM Cyber Ranges are the Modern Classrooms providing the knowledge of living the intensity of securing cyber today through immersive, gamified experiences in a simulated security operations center.

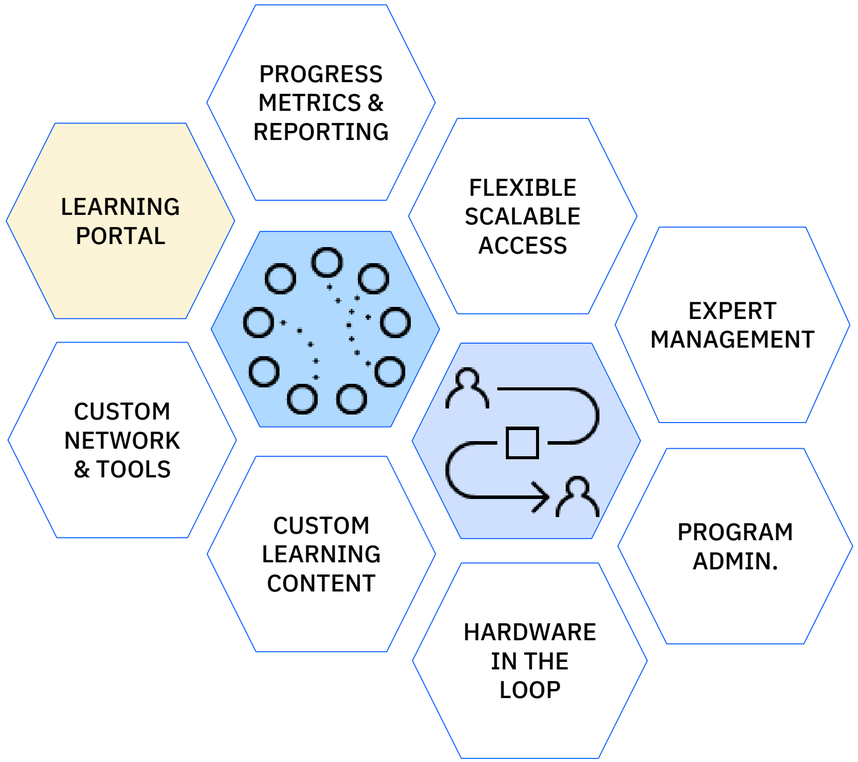

IBM X-Force Cyber Range
Washington DC

IBM Cyber Campus

Labs for Skills Development & Immersive Cyberattacks for Experience



Enterprise Cyber Campus Learning Platform



Train Anywhere Anytime

Cyber Skills Framework

- Course Content
- Industry Certifications

- Individual Skills
- Development Labs

- Virtual Cyber Range
- Full Scale Live Attack
- DFIR Simulation
- Team Focussed Collaboration

Features of the Cyber Range

Technology

Learning Portal

The Learning Portal is a central feature of the cyber range. Integral with LMS, it allows tracking team and individual performance and activities. The Portal also allows administrators to assign activities, share feedback, and communicate with learners.

Orchestration Layer

Pulls together all the service components of the cyber range. Eliminates need for customers' infrastructure of network, servers, and storage. The Cyber Range can leverage hardware-in-the-loop for nonstandard controls.

Virtualization Layer

The cyber range is a full software-as-a-Service (SaaS). Running on AWS for optimal realism of the cyber range's live fire exercises. Able to create virtualized infrastructures providing high-fidelity simulations in realistic business environments.

Target Infrastructure

The simulated environment in which students train provides the accessibility and usability for ease of use and is scalable and elastic to immediately support changes in user populations.

IBM provides the hosting and SaaS management freeing customers having to deal with any technological components.

Features of the Cyber Range

Curriculum & Learning Outcomes

Curricula

1500+ Training Labs and Skills Assessments. Labs are mapped to NICE and to industry certs such as CEH, A+, and Security+. Skill Packs are included to provide deep learning through a set of curated experiences to enable focused cyber skill development.

Adaptive Real-time

Cyber Range missions are, by design, interactive and fluid.

Students will encounter a live, dynamic environment where decisions are made in real-time, and can affect other students.

This team training, which is designed to mirror Security Operation Center (SOC) operations, provides the most realistic experiential learning available. Student interactions are observed and measured, with instructors being able to evaluate both hard and soft skills.

User Experience

students will access a multi-segment enterprise network that includes application servers, database servers, email servers, switches, and routers. The Cyber Range will have an enterprise-class IT network along with OT/ICS.

The Cyber Range can leverage hardware-in-the-loop for nonstandard controls.

Education Consulting

IBM may be engaged to assist the customer in modernizing their cyber education program to sharpen learning pathways to be more holistic and learning-centered to current experiences of securing cyber.

Features of the Cyber Range

Learning Content – New content, labs, and scenarios added monthly

Skills Assessments

- Cyber Defense Analyst
- Field Technologist
- Forensic Analyst
- Incident Responder
- Secure Software Developer
- System Administration
- Vulnerability Assessment Analyst

Skill Packs

- Cryptography
- Digital Media Forensics Basic
- Digital Media Forensics Network
- Ethical Hacking Essentials / PenTest+ / CEH
- Network Essentials / Network+
- Pentesting & Network Exploitation
- Security Essentials / Security+
- Security Professional Essentials / CISSP
- Web Application Hardening
- Web Application Pentesting (OWASP top 10)
- Advanced Web App Pentesting
- Linux Fundamentals

Training & Challenge Labs

- **1500 1-Hour Labs**
- Labs mapped to NICE and to industry certs such as CEH, A+, and Security +
- Labs have in-platform guides that help walk students through the exercise and setup
- Labs available **24x7x365**

Live Fire Exercises

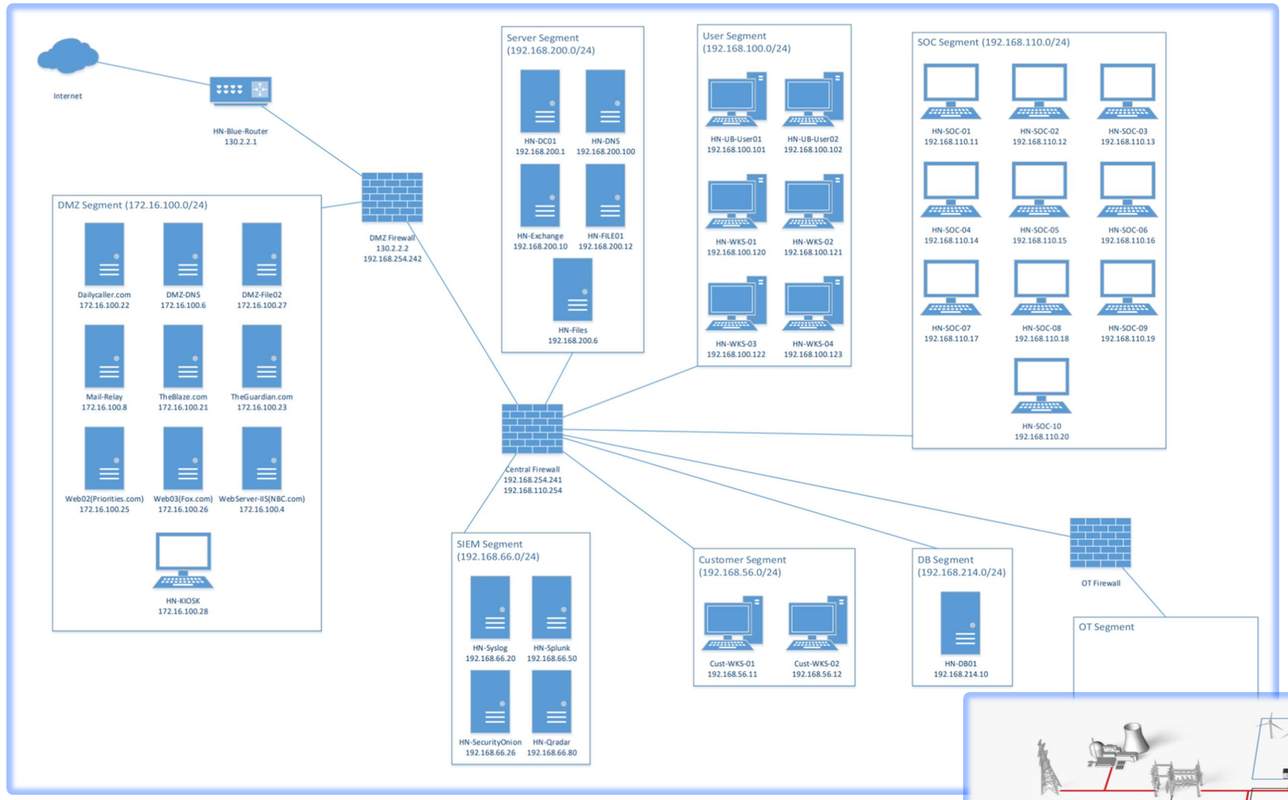
- Live, dynamic environment
- Multiple ways to investigate an attack
- Decisions made in real-time, and can affect other students
- Exercises run between 2 to 4 hours
- Exercises leveled by Novice, Intermediate, and Advance
- Complexity can be dialed in ahead and during exercise

Train like you Fight and Fight like you Train

50+ immersive simulated experiences covering the top cyber threats.
Each mission involves live malware and the ability to choose which industry-leading security and network tools to use.

Secure Training Environment

Simulated & Customizable Networks



Included & Add-on Enterprise Licenses

Security Information & Event Management (SIEM)

IBM Radar · splunk> · ELK Stack · Security Onion Solutions · Microsoft Sentinel · Chronicle part of Google Cloud · LogRhythm · MixMode

Operating Systems

Microsoft · ubuntu · linux · Open-PLC · KALI · Red Hat

Networking

paloalto NETWORKS · pfsense · FORTINET · JUNIPER NETWORKS · VYATTA

Intrusion Detection (OT)

CLAROTY · NOZOMI NETWORKS · DRAGOS · INDUSTRIAL DEFENDER

Cloud Platforms

Google Cloud · aws · Microsoft Azure

Network Detection and Response (NDR)/Threat Intelligence

VECTRA · ExtraHop · DARKTRACE

Endpoint Detection and Response (EDR)/ Endpoint Protection Platforms (EPP)

CROWDSTRIKE · Microsoft Defender

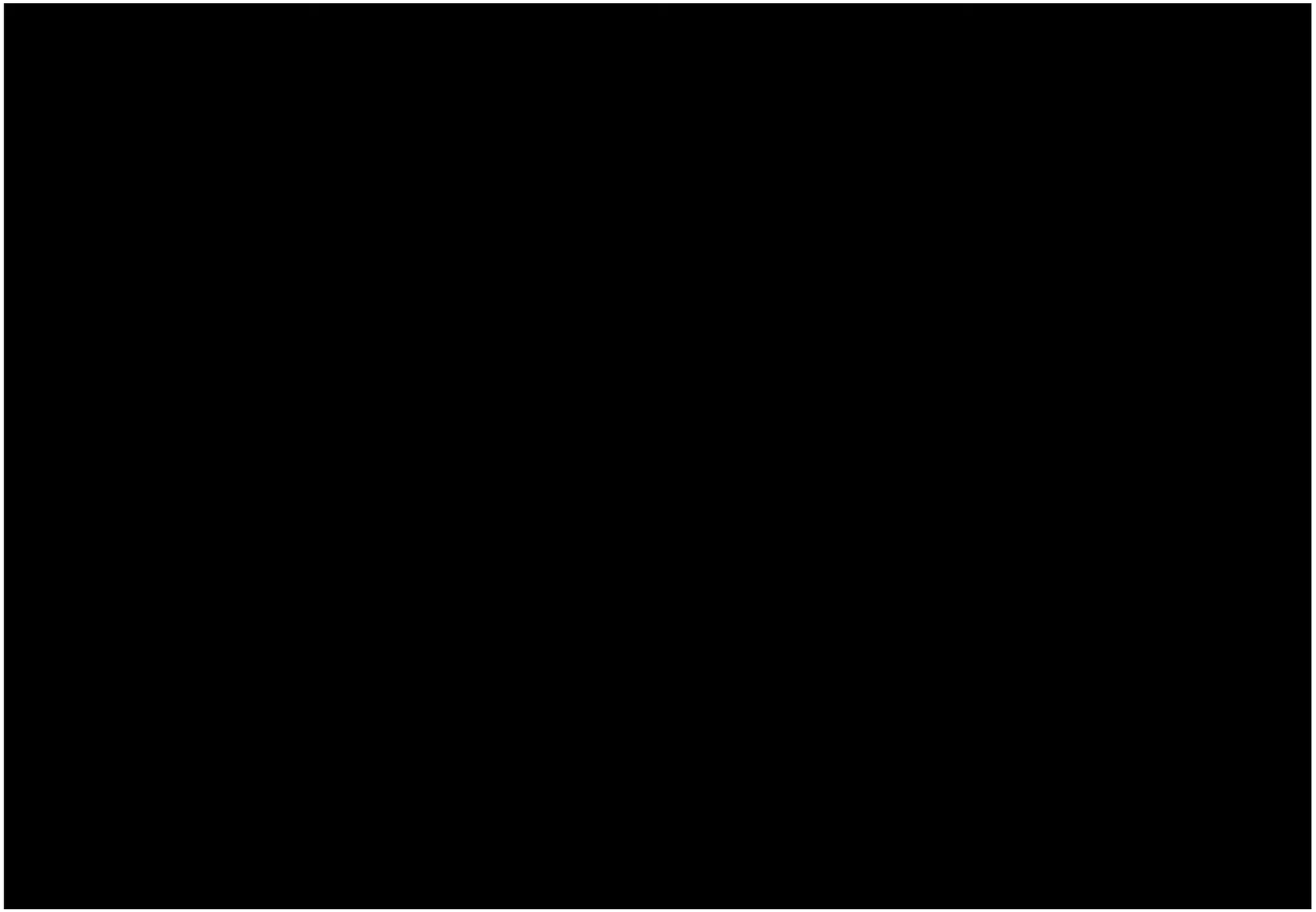
Additional Tools

ANOMALI · ScadaBR · CyberChef FOR SECURITY ANALYSTS · GHIDRA · WIRESHARK · REMnux

IBM -University of Ottawa

FMCC
SUNY

First College with IBM Cyber Campus



Southeast Missouri State University

First University with IBM Cyber Campus

IBM Cyber Campus - SEMO

Thank you

Email : udit.sharma1@ibm.com