Rethinking How We Approach Cyberspace Training and Certification

Jondi Bernardo

Introduction

- We are engaged in a long-term strategic competition with our adversaries to include persistent campaign in cyberspace that pose a vital strategic risk to our nation and our allies and partners.

- Ensure our military's ability to fight and win in any domain, including cyberspace is paramount to the long-term strategy. Defend the networks, systems, and information from malicious cyber activity.

- "The Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident."

-2018 DoD Cyber Strategy

Key Take Aways

- Training must be measurable and proven
- Train with real world scenarios
- Role-based training is paramount

Future Development of Joint Cyber Workforce

U.S. cyber forces will be prepared to operate alongside our warfighting forces in the air, land, sea, and space.

"The Integration of cyber, electronic warfare (EW) and information operations (IO) is becoming increasingly critical…we are starting to see the fusion of cyber operations with electronic warfare operations coming to fruition in a repeatable fashion."

LTG Maria B. Barrett, U. S. ARCYBER Command

"The U.S. Space Operations Command is assigning cybersecurity and intelligence specialists to work side-by-side with satellite operators so they're better prepared to protect U.S. systems from electronic and physical threats"

MG Douglas Scheiss, U.S. Space Force

Challenges to Cyber Professionals

- As malicious cyber activity continues to rise, the Department must have an agile highly skilled workforce of cyber professionals to combat cyber attacks.
- Consistency throughout DoD and Federal Agencies
- Lack of clearly-defined career paths for cyberspace professionals across DoD
- Shortage of cybersecurity experts

We need a new perspective: Cyber Workforce Resilience

> We must change our cybersecurity approach to better compete in today's contested cyberspace.
> *--Carlos Del Toro, SECNAV*

Principles

It's about **People**

Defense is a **team sport**

Learning is not for spectators

Individual and team capabilities are **measurable and provable**

Forrester Report: Rethink Your Reliance on Cybersecurity Certifications

There’s no shortage of cybersecurity training or certifications for security professionals. Despite this availability, many programs prioritize session completion over outcomes and fail to provide the necessary data to prove readiness for real-world threats.

Findings include:

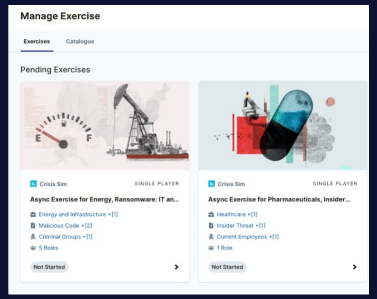
1. Certification training, acquisition, and maintenance costs are seen as problematic.
2. Certification value decreases as hands-on experience and specialization increases.
3. Required certifications are often misaligned with job levels.

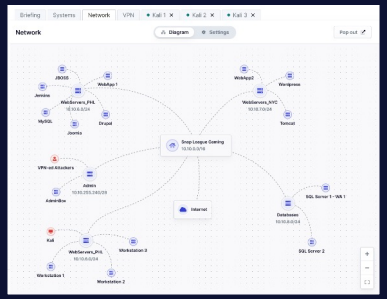
Cybersecurity Certification is Costly

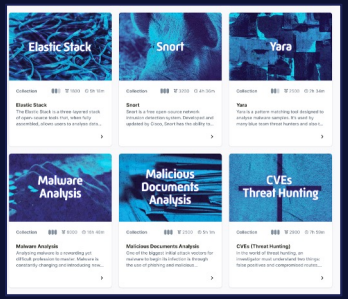
- Entry Level: $9,767
- Management Level: $3,829
- Specialized: $5,821

- Based on list pricing for 47 certification examination processes and 34 certification and education training programs.
- Source: Certification provider websites, certification education and training websites.

Dynamic Solutions







Organizational Exercises

Engaging attack scenarios for executive decision-makers

- Executive Teams
- Crisis Management Teams
- Governance, Risk & Compliance Teams
- Boards of Directors
- Entire Workforce

Technical Exercises

Realistic technical simulations to collaboratively exercise capabilities

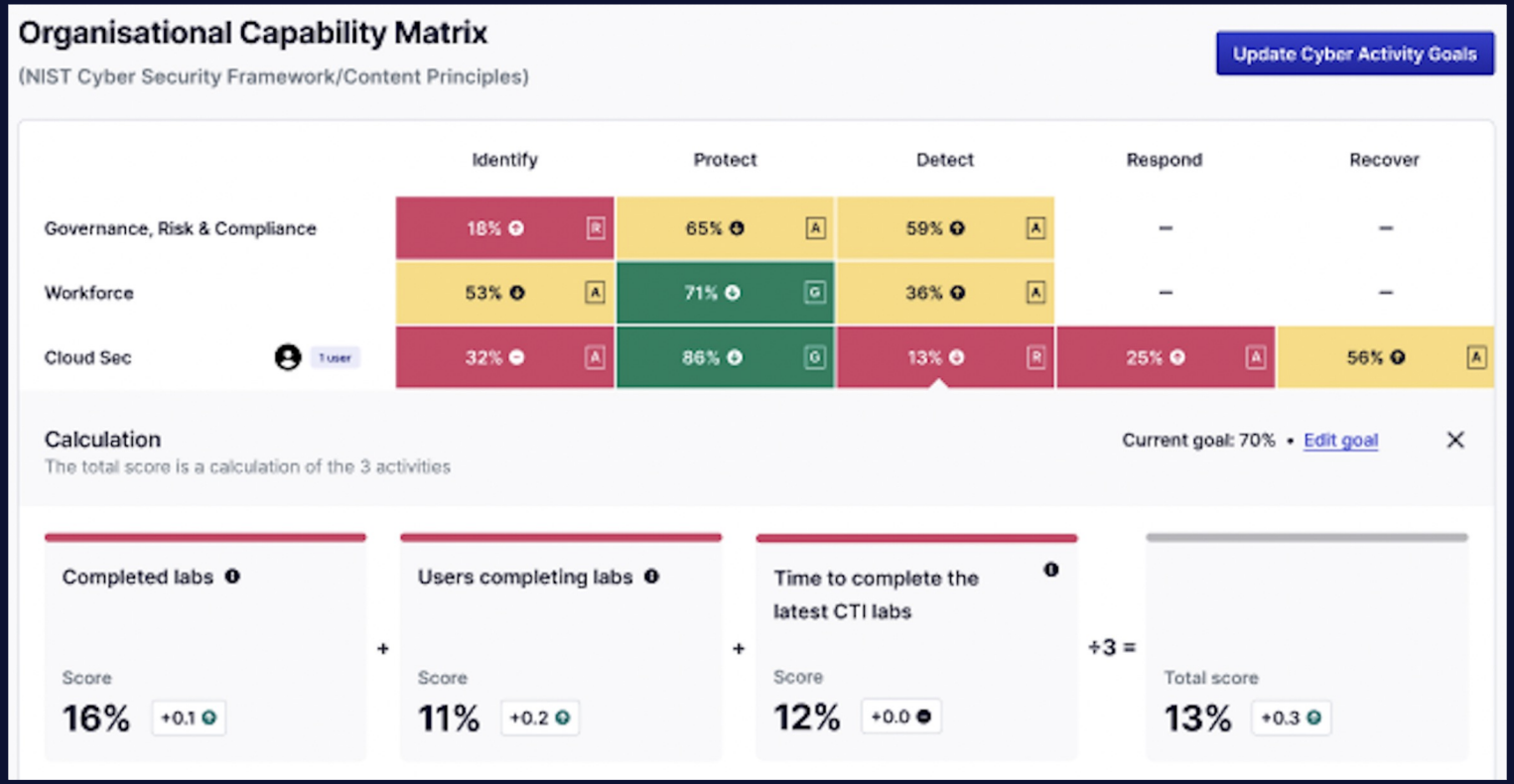
- Defensive Teams
- Penetration Testing Teams
- SOC Teams

Hands-On Labs

Hands-on role-based technical training for multiple audiences

- Defensive Cybersecurity Professionals
- Penetration Testers
- Developers
- Application Security Experts
- Cloud & Infrastructure Security
- Entire Workforce

Reports: Organizational Capability Matrix



“

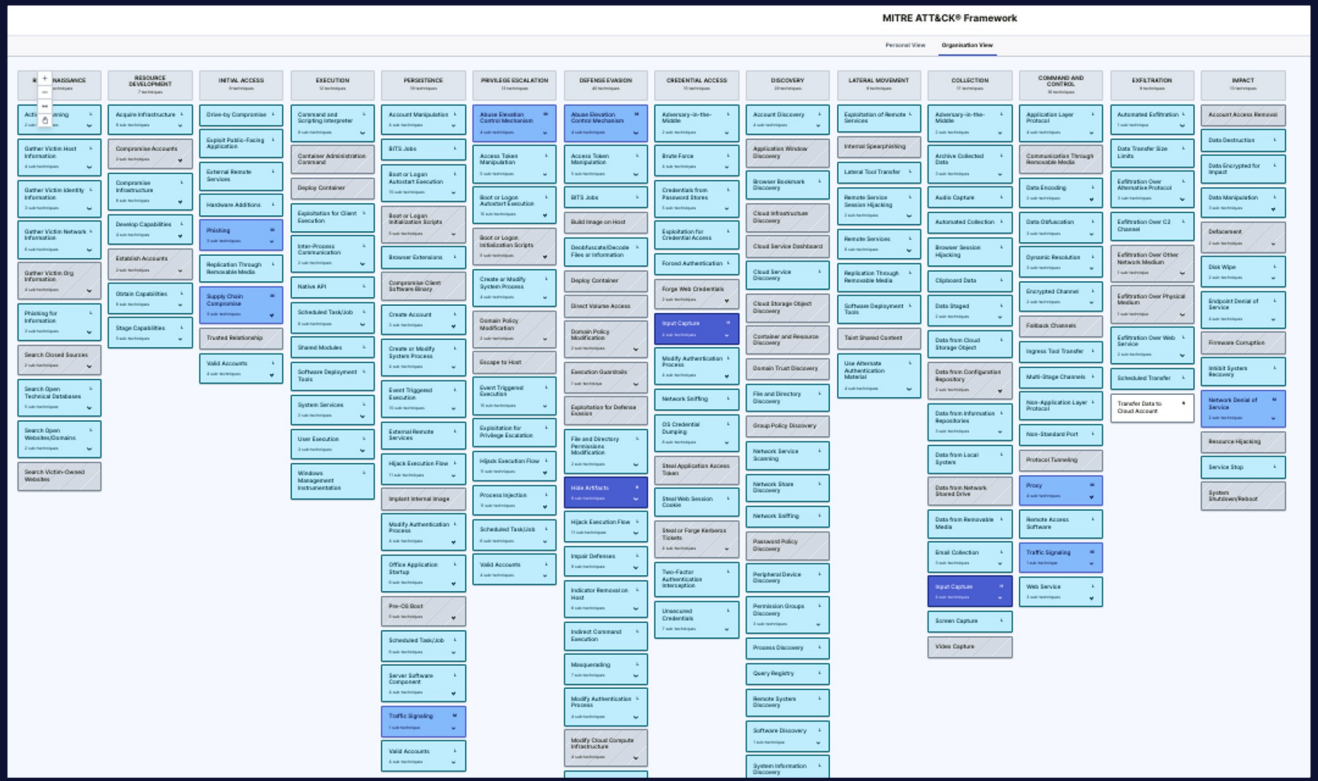
In the wake of global crisis, C-suite and functional leaders are telling us they must build the capability to bounce back from any kind of setback — whether it’s a pandemic, natural disaster, economic change, government decision, competitive onslaught, cyberattack or espionage.

Resilience is an Urgent C-Suite Priority

Gartner

Gartner, Inc. “Resilience Is an Urgent C-Suite Priority”. Corporate Strategy Research Team. 16 May 2022.

MITRE Coverage



Sources

- DoD Cyber Exchange
- 2018 Department of Defense Cyber Strategy
- DoD Cyber Workforce Framework
- Forrester Report October 24, 2022; Rethink Your Reliance on Cybersecurity Certifications
- Immersive Labs Cyber Workforce Resiliency platform
- IBM Security

Key Take Aways

- Training must be measurable and proven
- Train with real world scenarios
- Role-based training is paramount

TEAM | TEAMMATE | SELF

Thank You

Jondi Bernardo
Immersive Labs
Jondi.Bernardo@immersivelabs.com