Cybersecurity Functional Areas (NICE Framework)



Organizado por:











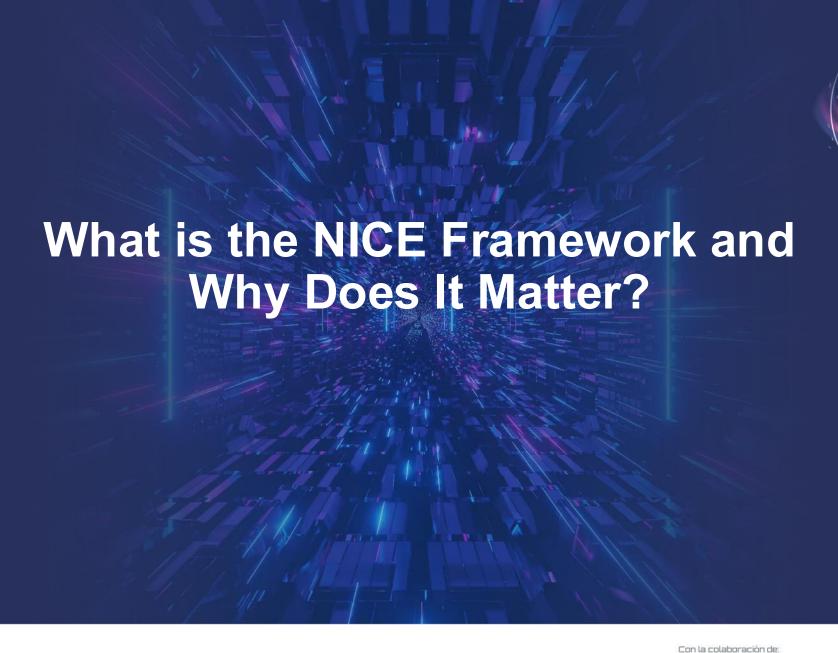


































Definition



The NICE Framework is a guide developed by the U.S. government (specifically, NIST — the National Institute of Standards and Technology) to describe and organize cybersecurity work roles, the skills and knowledge needed, and the tasks involved in each.























Analogy

Cybersecurity as a Symphony Orchestra

Imagine cybersecurity is a giant orchestra:

- Some play violins (network defense).
- Some play drums (incident response).
- Some write music (policy, governance).
- Some tune instruments (system maintenance).

But imagine if no one agreed on who does what. Chaos, right?























The NICE Framework is a musical score

It defines roles, skills, and tasks so everyone is in harmony.























Why It Exists



- NICE isn't just for experts—it helps:
- Students and career changers understand roles in cybersecurity.
- Employers describe job requirements clearly.
- Educators align training to real-world needs.

It makes the chaotic world of cybersecurity jobs structured and understandable.



















Version 2.0

Version 2.0, released in March 2025, is a refined and more flexible model. It:

- **♦**Removed outdated or military-specific categories.
- **◆**Added new work roles like OT Cybersecurity Engineering.
- **◆**Enhanced clarity and modernized skills and competencies.





















Question?



Why do you think it's helpful to have a standardized framework in a fast-changing field like cybersecurity?











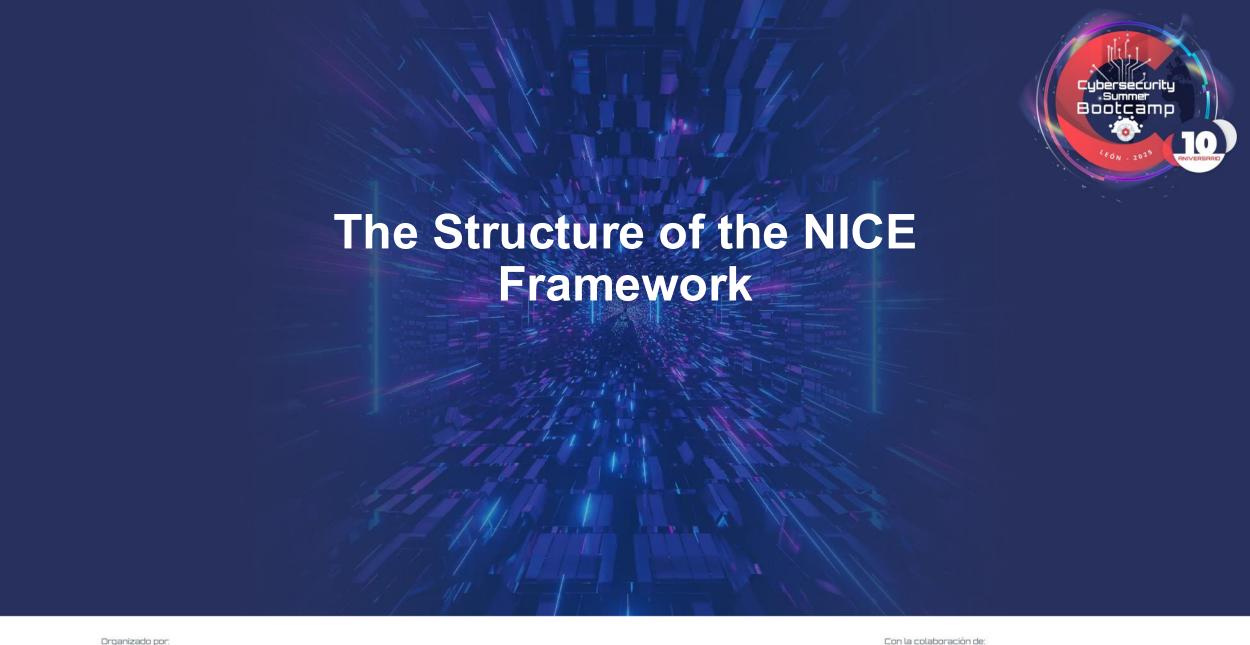


































The Four Core Components



NICE v2.0 is structured around four flexible, connected components

Component

1. Work Roles

2. Competency Areas

3. Task Statements (T)

4. Knowledge and Skill Statements (KS)

What It Describes

Specific cybersecurity jobs (e.g. Penetration Tester, Forensic Analyst)

The broad skills or knowledge themes needed across jobs

What someone in the role actually does

What someone needs to know or be able to do to perform those tasks



















Analogy

Building a House



Let's say you're building a house. Here's how these components work:

Work Role = The job title (e.g., Electrician).

Competency Areas = The disciplines they need (e.g., wiring, safety standards).

Tasks (T) = What they do (e.g., install fuse box, test voltage).

Knowledge/Skills (KS) = What they must know (e.g., circuit diagrams, safe handling).

Just like you can reuse an electrician's skills across many buildings, in NICE, skills can apply across many roles. That's what makes v2.0 more flexible than earlier versions.





















New in v2.0

Here's what makes this version different from earlier NICE versions

You can use Competency Areas independently, even outside of work roles (e.g., for training design).

Work roles are no longer tied to rigid **Categories** — they're **modular**.

Tasks and KS are now sharper, fewer, and clearer.

This means:

You can now build **your own custom career path** by mixing competencies and roles, instead of being stuck in predefined categories.



Organizado por









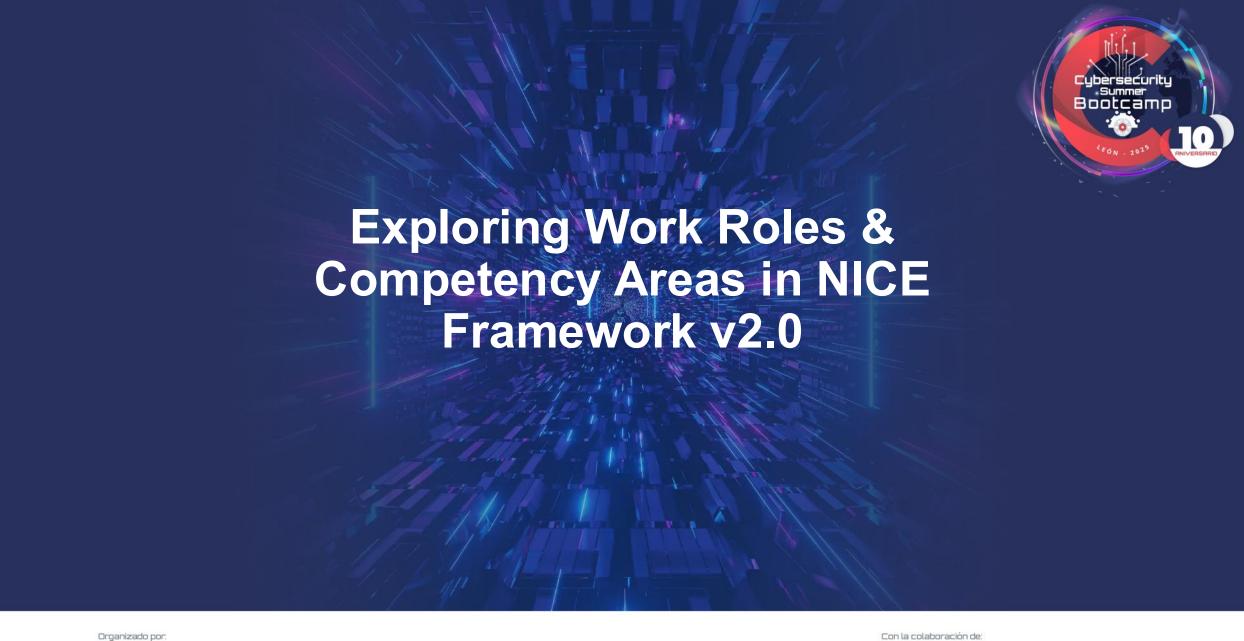


































"What kind of cybersecurity professional could I become?"

That's the question we'll explore today. You'll get a feel for several roles, the skills behind them, and the competency areas they rely on.

Let's approach this like a personality quiz — I'll show you different types of cybersecurity careers, and you tell me which ones click with your interests.



















Penetration Tester

ID: PR-WRL-004

"I try to break into systems to help secure them."

Competency Areas: Vulnerability Assessment, Ethical Hacking, Exploitation

Tasks: Simulate attacks, document findings, recommend fixes

Skills:

- Network scanning tools (e.g. Nmap)
- Exploiting known vulnerabilities
- Reporting security weaknesses

Personality Fit: Curious, enjoys puzzles, bold thinker



















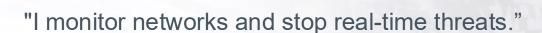






Cyber Defense Analyst

ID: PD-WRL-001



Competency Areas: Network Monitoring, Threat Detection, Cyber Resiliency

Tasks: Review logs, detect anomalies, respond to alerts

Skills:

- Log analysis tools (e.g. Splunk)
- Understanding malware behavior
- Incident response procedures

Personality Fit: Vigilant, detail-oriented, steady under pressure

























Digital Forensics Analyst

ID: IN-WRL-002

"I uncover what happened after a cybercrime."

Competency Areas: Digital Evidence, Cyber Law, Incident Analysis

Tasks: Collect data, preserve evidence, report to legal teams

Skills:

- Chain-of-custody handling
- File system analysis
- Forensic tools like EnCase or Autopsy

Personality Fit: Investigative, methodical, justice-oriented

























OT Cybersecurity Engineer

ID: DD-WRL-009



"I protect industrial systems like power grids and water plants."

Competency Areas: Operational Technology, Industrial Controls, Risk Management

Tasks: Secure SCADA systems, apply patches, monitor threats

Skills:

- Understand control systems (e.g. PLCs)
- Apply security to physical systems
- Collaborate with engineers

Personality Fit: Practical, systems thinker, loves infrastructure





















Competency Areas: A Few Examples

These are the building blocks of each role — areas of skill and knowledge that apply across roles.

Competency Area

Vulnerability Assessment

Digital Forensics

Cyber Resiliency

Risk Management

Secure Software Development

Threat Analysis

What It Covers

Finding and analyzing security weaknesses

Investigating devices for legal evidence

Keeping systems running through disruption

Measuring and mitigating threats

Building safe, reliable apps

Understanding and predicting cyber adversaries













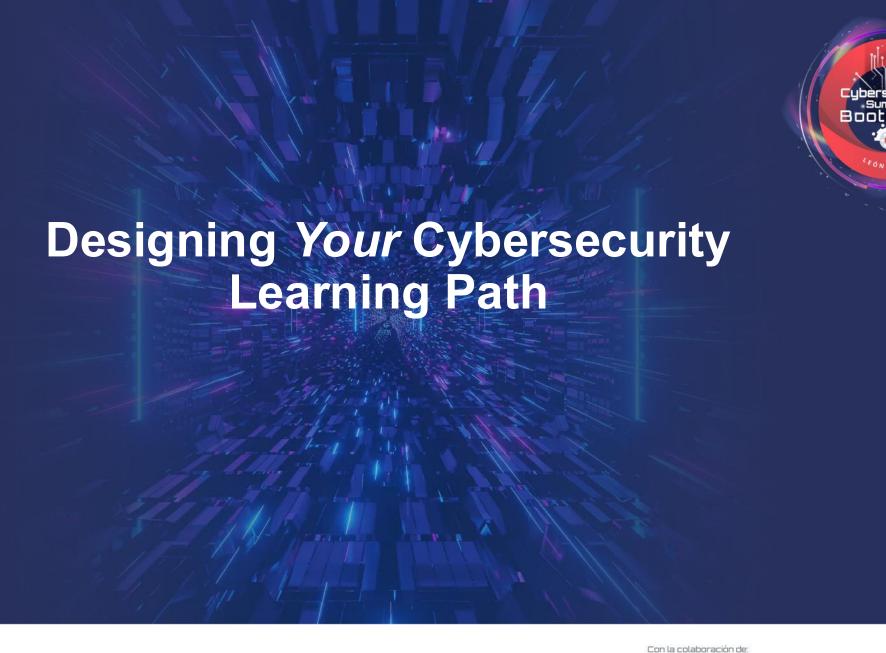


































What about to...



- Identify what you already bring to the table
- Pinpoint what to learn next
- Build a simple roadmap for growth based on the NICE Framework





















Define the Destination



Let's clarify the role so we always know what we're aiming for























Understand the Skills Needed



We'll break this into 3 layers — based directly on NICE v2.0.

- Tasks
- Knowledge Areas
- Skills



Organizado por



















Map Out Your Personalized Learning Path



- Phase 1 Foundations
- Phase 2 Specific Skills
- Phase 3 Specialization + Certification























Important Questions...



- What skills do you already have that overlap with this roadmap?
- What would be your next natural step from here?





















Gap Analysis — Discover What You Don't Know Yet

Think of this like a treasure map with X marks the spots you need to explore.

How to Do It:

- List the NICE skills and knowledge about the Work Role you feel confident about.
- Identify areas you feel less familiar with or haven't practiced recently.
- Set learning goals for those gaps.





















Skill / Knowledge Area

Comfortable (√)



Networking basics (IP, DNS)

MITRE ATT&CK framework

Threat Intelligence sources

Log analysis (Splunk, ELK)

Writing threat reports

OSINT tools (Shodan, etc.)

Cybercrime trends awareness

Critical thinking





















Quick Task for You



Fill this table out on paper. What do you feel ready for? What needs work?























Thoughtful Question



- How might focusing on your weakest areas first accelerate your growth?
- Which of those gaps would make the biggest difference in your daily work as the work role you choose?













































What Are SMART Goals?



Specific, Measurable, Achievable, Relevant, Time-bound — a simple way to make your learning focused and trackable.























Example SMART Goals for a Threat Analyst



Goal

Learn MITRE ATT&CK framework basics

Improve OSINT skills

Practice report writing

Example SMART Version

"Study the MITRE ATT&CK framework by completing the official MITRE online course and creating a mind map summarizing all tactics within 3 weeks."

"Complete 5 OSINT exercises using Shodan and the Harvester in 2 weeks and document findings."

"Write a 1-page threat intelligence report weekly for 4 weeks, getting feedback from a peer or mentor."























Resources to Get You Started



Skill/Topic

MITRE ATT&CK

OSINT Tools

Log Analysis

Threat Reports

Writing Practice

Resource

MITRE ATT&CK Website

Try Shodan, the Harvester

Splunk Fundamentals 1

Mandiant Reports

Use a template from **SANS** Reading

Room

Type

Official Framework & Docs

Free Tools

Free Course

Real-World Examples

Templates & Samples























Your Turn: Draft 2-3 SMART goals you want to start with



I'm here to help you refine them if you want.























Quick Check-In



What goals would you like to commit to right now? Or would you prefer I help you craft them based on your current skills and gaps?























Quick Check-In



Can yo create learning paths for your work force?













































