RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: PROF-W04

A NICE WAY TO FIND AND KEEP CYBERSECURITY WORKERS

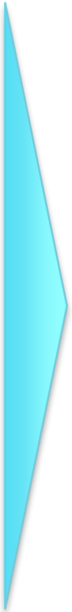
Greg Witte

Sr. Cybersecurity Engineer
G2, Inc.
@TheNetworkGuy

Tom Conkle

Cybersecurity Engineer
G2, Inc.
@TomConkle

In this digital world, it is critical that we train, hire, and retain top quality cyber workforce

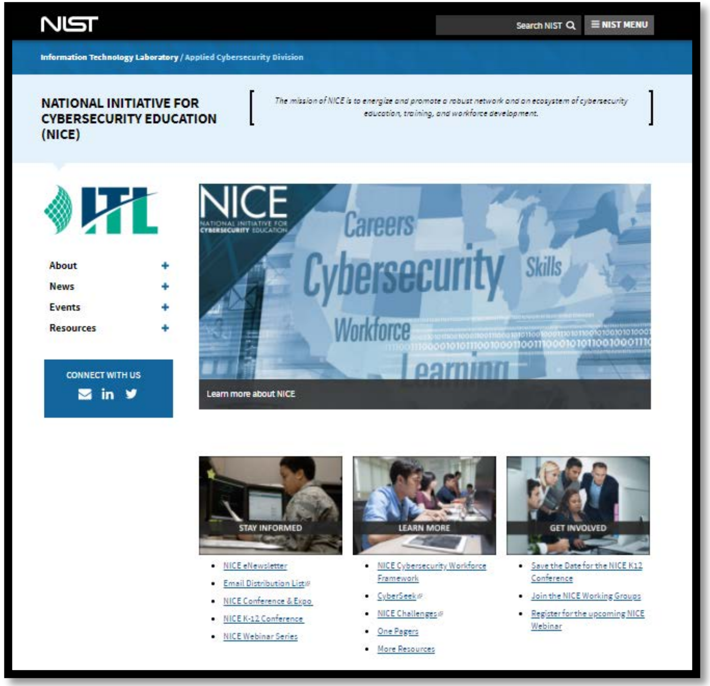


Cybersecurity Expert

The National Initiative for Cybersecurity Education (NICE)

Homeland Security

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION



Information Technology Laboratory / Applied Cybersecurity Division

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.

- NICE eNewsletter
- Email Distribution List
- NICE Conference & Expo
- NICE K-12 Conference
- NICE Webinar Series

- NICE Cybersecurity Workforce Framework
- CyberSeek
- NICE Challenges
- One Pagers
- More Resources

- Save the Date for the NICE K12 Conference
- Join the NICE Working Groups
- Register for the upcoming NICE Webinar

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.

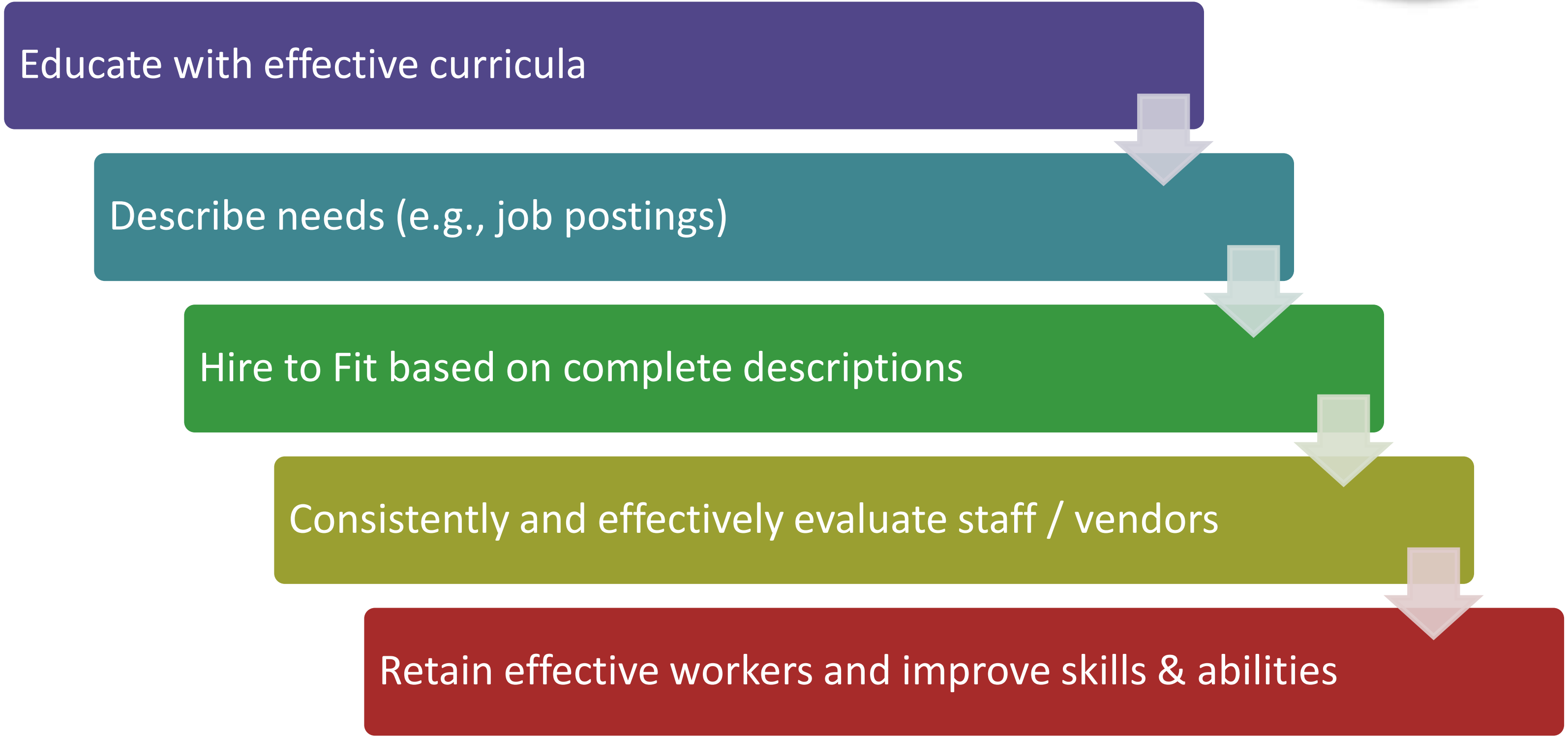
The NICE Strategic Plan goals for improving awareness and education

LEARNING & SKILLS DEVELOPMENT
ACCELERATE

A DIVERSE LEARNING COMMUNITY
NURTURE

CAREER DEVELOPMENT & WORKFORCE PLANNING
GUIDE

NICE supports the cyber workforce lifecycle



Educate with effective curricula

Describe needs (e.g., job postings)

Hire to Fit based on complete descriptions

Consistently and effectively evaluate staff / vendors

Retain effective workers and improve skills & abilities

Failure to hire, train, and develop qualified staff has negative effects

Has a shortage of cybersecurity skills had a negative effect on your organization?

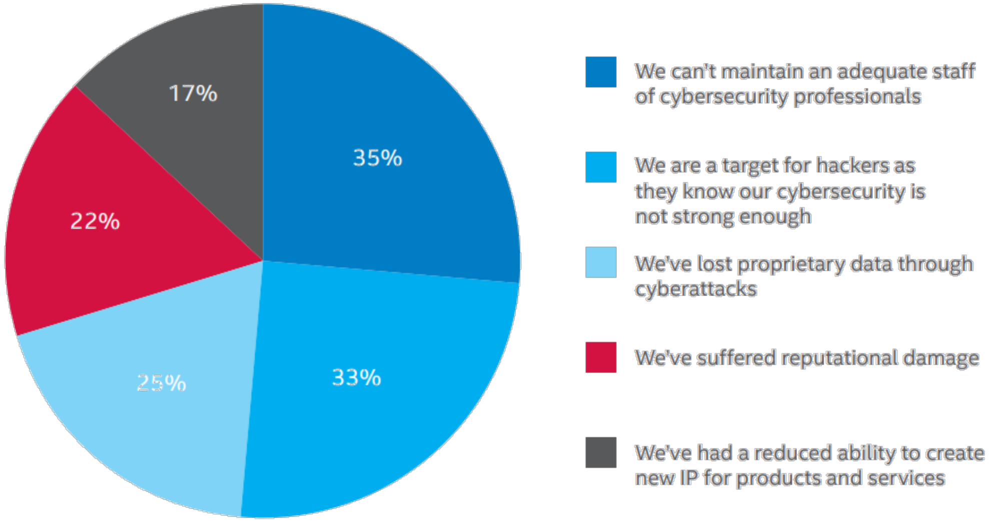
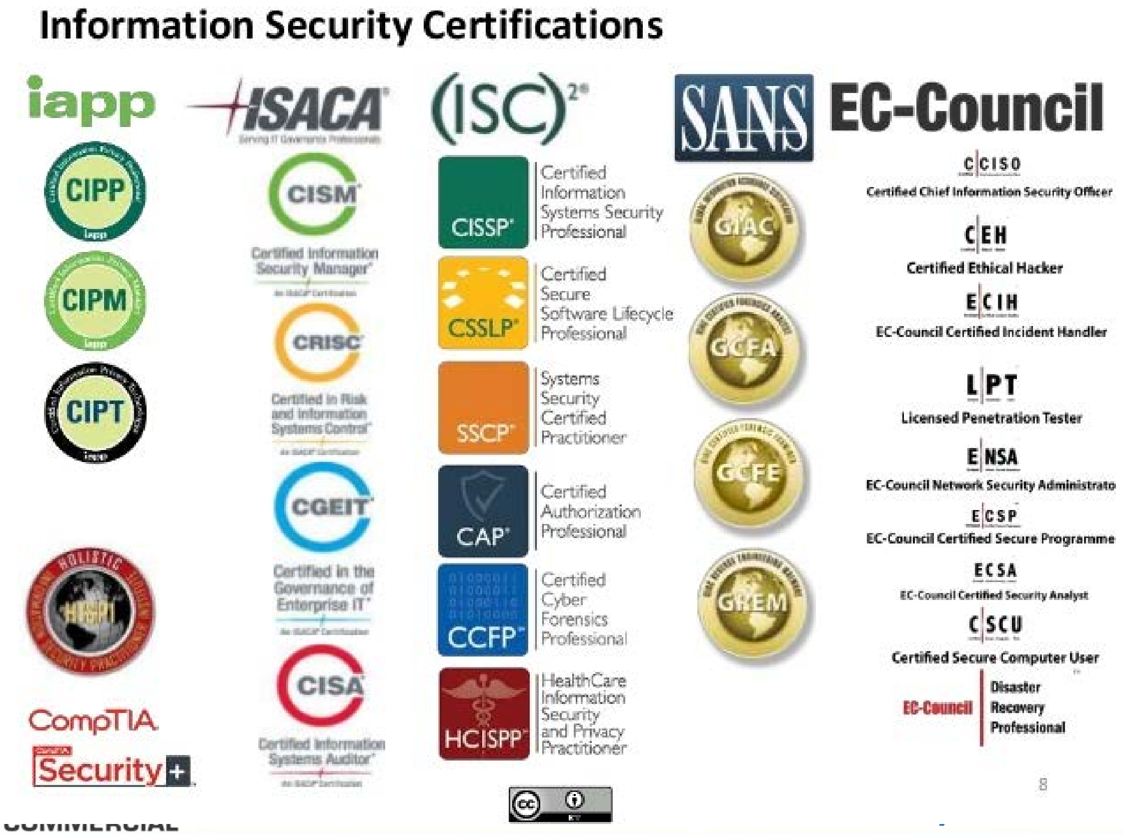


Figure 5. Impact of cybersecurity workforce shortage.

Intel Corporation, "Hacking the Skills Shortage: a study of the international shortage in cybersecurity skills," 2016, www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

Certs are critical, but yesterday's ways of training & hiring must improve


Information Security Certifications
iapp
CIPP
CIPM
CIPT
GISP
CompTIA
Security+
ISACA
Serving IT Governance Professionals
CISM
Certified Information Security Manager
CRISC
Certified in Risk and Information Systems Control
CGEIT
Certified in the Governance of Enterprise IT
CISA
Certified Information Systems Auditor
(ISC)²
CISSP
Certified Information Systems Security Professional
CSSLP
Certified Secure Software Lifecycle Professional
SSCP
Systems Security Certified Practitioner
CAP
Certified Authorization Professional
CCFP
Certified Cyber Forensics Professional
HCISPP
HealthCare Information Security and Privacy Practitioner
SANS
GIAC
GCFA
GCFE
GREM
EC-Council
CCISO
Certified Chief Information Security Officer
CEH
Certified Ethical Hacker
ECIH
EC-Council Certified Incident Handler
LPT
Licensed Penetration Tester
ENSA
EC-Council Network Security Administrato
ECSP
EC-Council Certified Secure Programme
ECSA
EC-Council Certified Security Analyst
CSCU
Certified Secure Computer User
EC-Council
Disaster Recovery Professional
8
COMMERCIAL

Certification is ***one*** great way to demonstrate acquired abilities and for employers to help quickly identify potential hires with needed qualifications

Source: http://becomeacybersecurity.expert

Cybersecurity activities are supported by many roles.

The Struggle is Real, but the Glass is ½ Full

CSX
CYBERSECURITY NEXUS

State of Cyber Security 2017

Part 1: Current Trends in Workforce Development

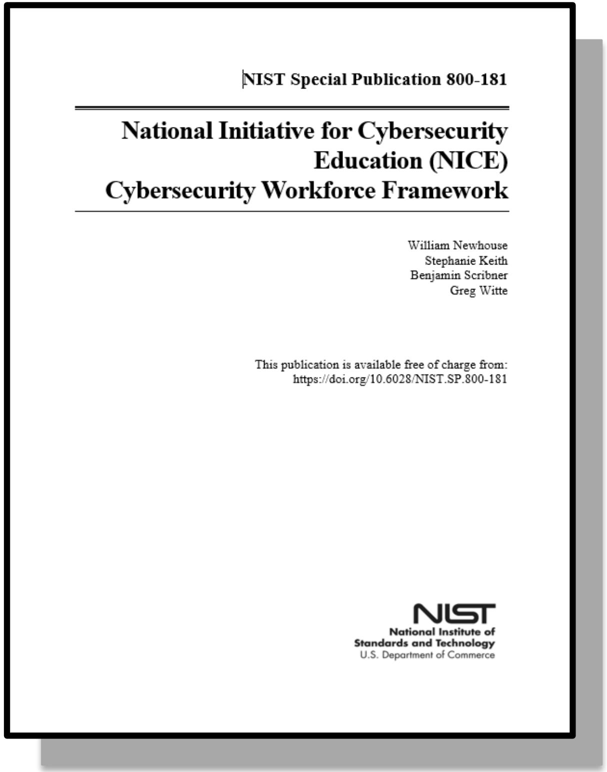
Abstract

State of Cyber Security 2017 reports the results of the annual ISACA global cyber security survey, conducted in October 2016. The survey results bolster the belief that the field of cyber security remains dynamic and turbulent during its formative years. Weekly news headlines confirm that cyberattacks are not a seasonal threat or dependent on specific industry environmental attributes, but are constant and should remain forefront in every enterprise executive's thought process. To equip you with a comprehensive understanding of the cyber security industry through the lens of those who define it—the managers and practitioners—ISACA is presenting the survey results in a series of reports that focus on individual topics. This report is the first in the *ISACA State of Cyber Security 2017* white paper series and presents timely information about cyber security workforce development and its current trends.

ISACA
Trust in, and value from, information systems

There are significant benefits to a more diverse cybersecurity workforce

NIST released the NICE Framework in 2017



NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181

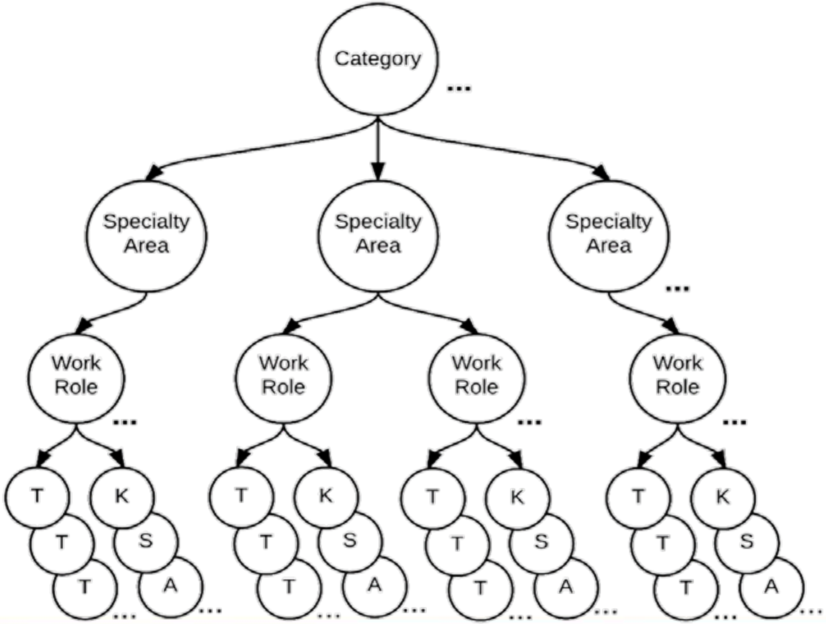
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- NIST Special Publication 800-181
  - NICE Cybersecurity Workforce Framework
- URL: *https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework*

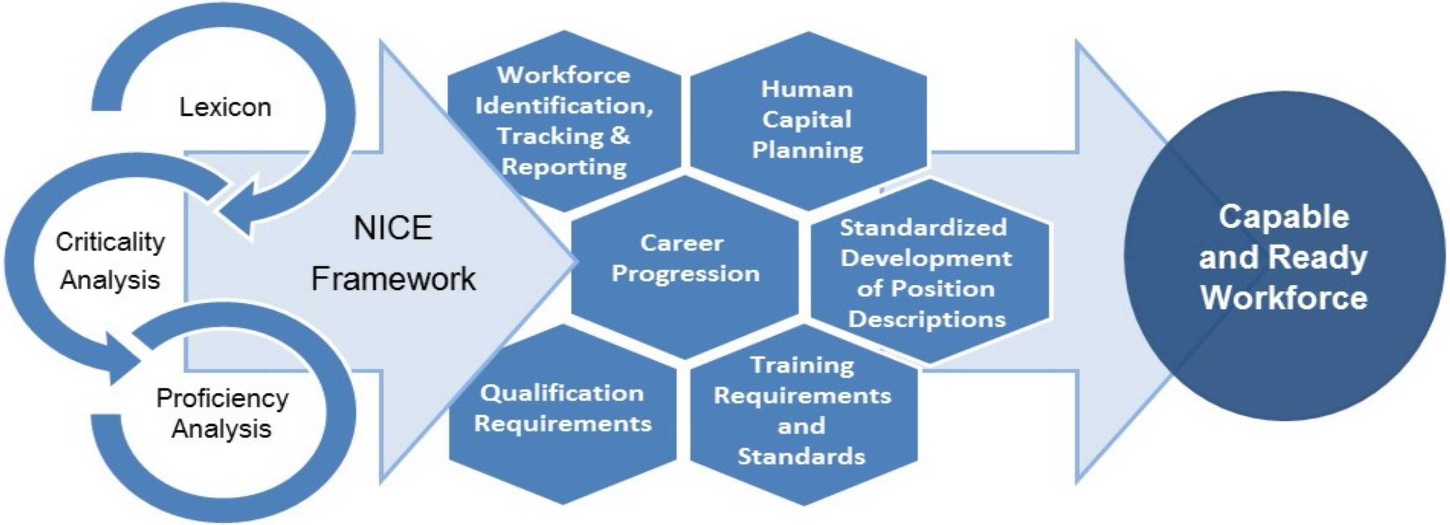
NIST 800-181 categorizes cybersecurity roles

NICE Framework Categories

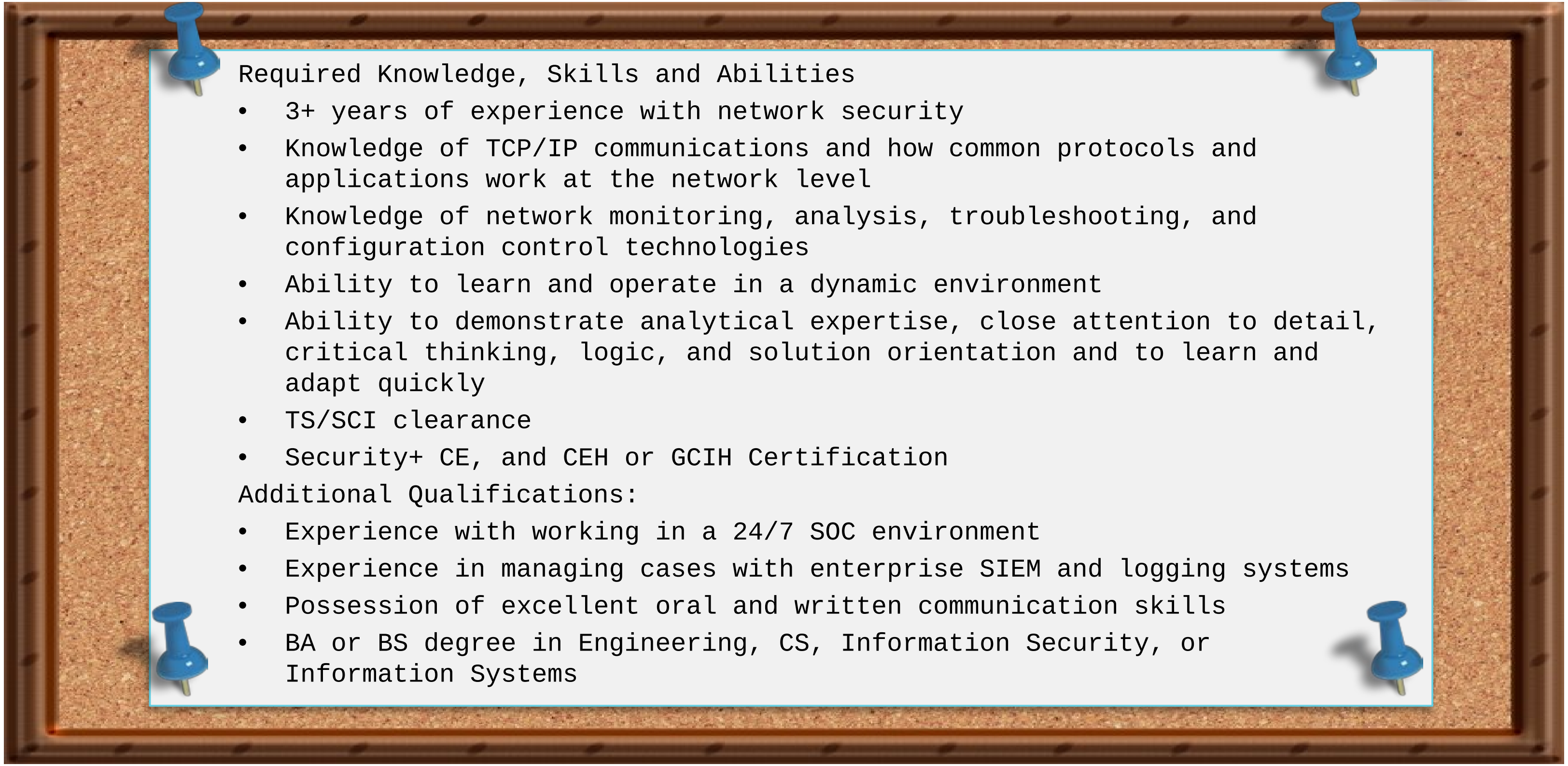
SECURELY PROVISION	OPERATE AND MAINTAIN	OVERSEE AND GOVERN	PROTECT AND DEFEND	ANALYZE	COLLECT AND OPERATE	INVESTIGATE



The NICE Framework builds a cybersecurity capable and ready workforce


Lexicon
Criticality Analysis
Proficiency Analysis
NICE Framework
Workforce Identification, Tracking & Reporting
Human Capital Planning
Career Progression
Standardized Development of Position Descriptions
Qualification Requirements
Training Requirements and Standards
Capable and Ready Workforce

A sample of a recent cyber defense incident responder requisition



Required Knowledge, Skills and Abilities

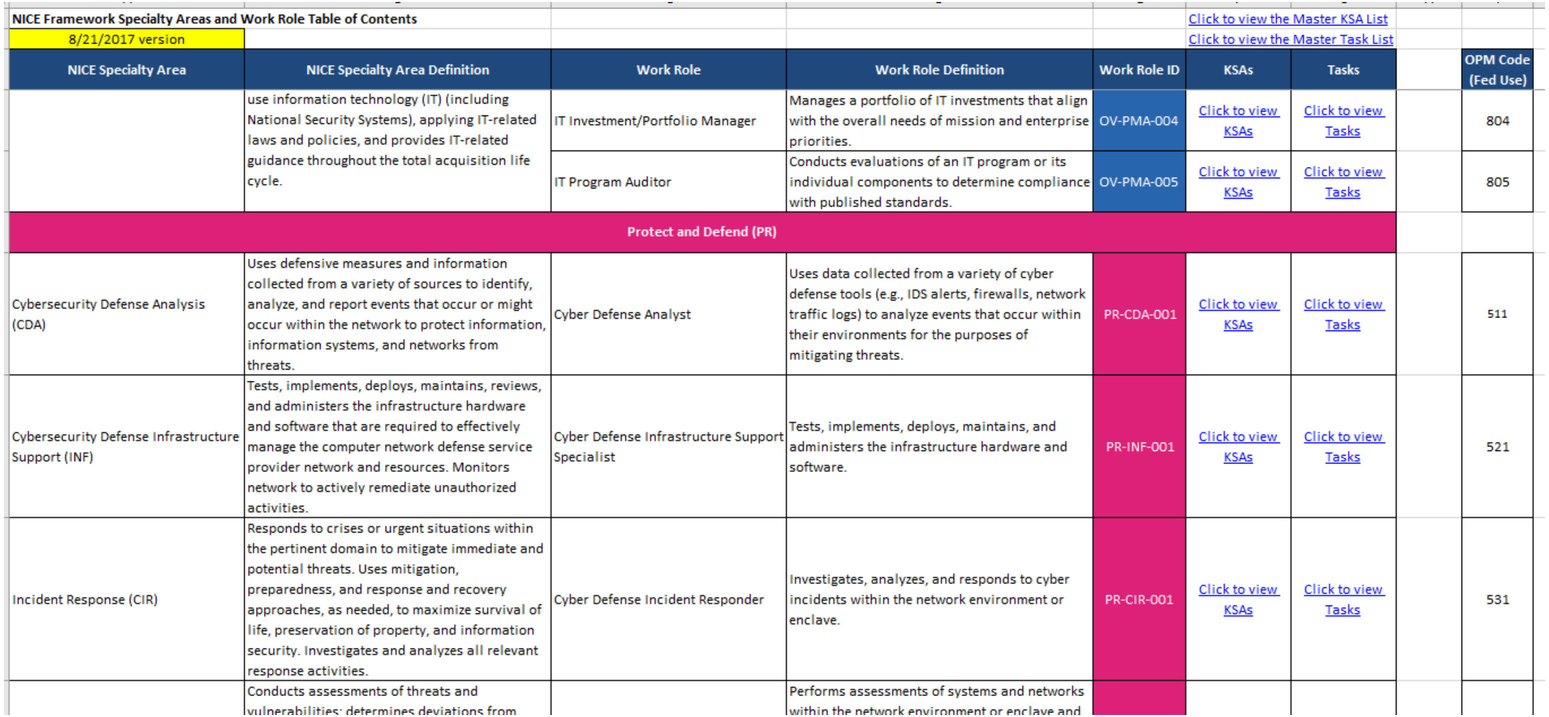
- 3+ years of experience with network security
- Knowledge of TCP/IP communications and how common protocols and applications work at the network level
- Knowledge of network monitoring, analysis, troubleshooting, and configuration control technologies
- Ability to learn and operate in a dynamic environment
- Ability to demonstrate analytical expertise, close attention to detail, critical thinking, logic, and solution orientation and to learn and adapt quickly
- TS/SCI clearance
- Security+ CE, and CEH or GCIH Certification

Additional Qualifications:

- Experience with working in a 24/7 SOC environment
- Experience in managing cases with enterprise SIEM and logging systems
- Possession of excellent oral and written communication skills
- BA or BS degree in Engineering, CS, Information Security, or Information Systems

Let’s walk through the NICE Workforce Framework tool

#RSAC



NICE Framework Specialty Areas and Work Role Table of Contents

8/21/2017 version

Click to view the Master KSA List

Click to view the Master Task List

NICE Specialty Area	NICE Specialty Area Definition	Work Role	Work Role Definition	Work Role ID	KSAs	Tasks		OPM Code (Fed Use)
	use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.	IT Investment/Portfolio Manager	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.	OV-PMA-004	Click to view KSAs	Click to view Tasks		804
		IT Program Auditor	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.	OV-PMA-005	Click to view KSAs	Click to view Tasks		805
Protect and Defend (PR)								
Cybersecurity Defense Analysis (CDA)	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.	PR-CDA-001	Click to view KSAs	Click to view Tasks		511
Cybersecurity Defense Infrastructure Support (INF)	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	Cyber Defense Infrastructure Support Specialist	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.	PR-INF-001	Click to view KSAs	Click to view Tasks		521
Incident Response (CIR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	Cyber Defense Incident Responder	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.	PR-CIR-001	Click to view KSAs	Click to view Tasks		531
	Conducts assessments of threats and vulnerabilities; determines deviations from		Performs assessments of systems and networks within the network environment or enclave and					

COMMERCIAL

There are a broad range of work roles supporting incident response and recovery

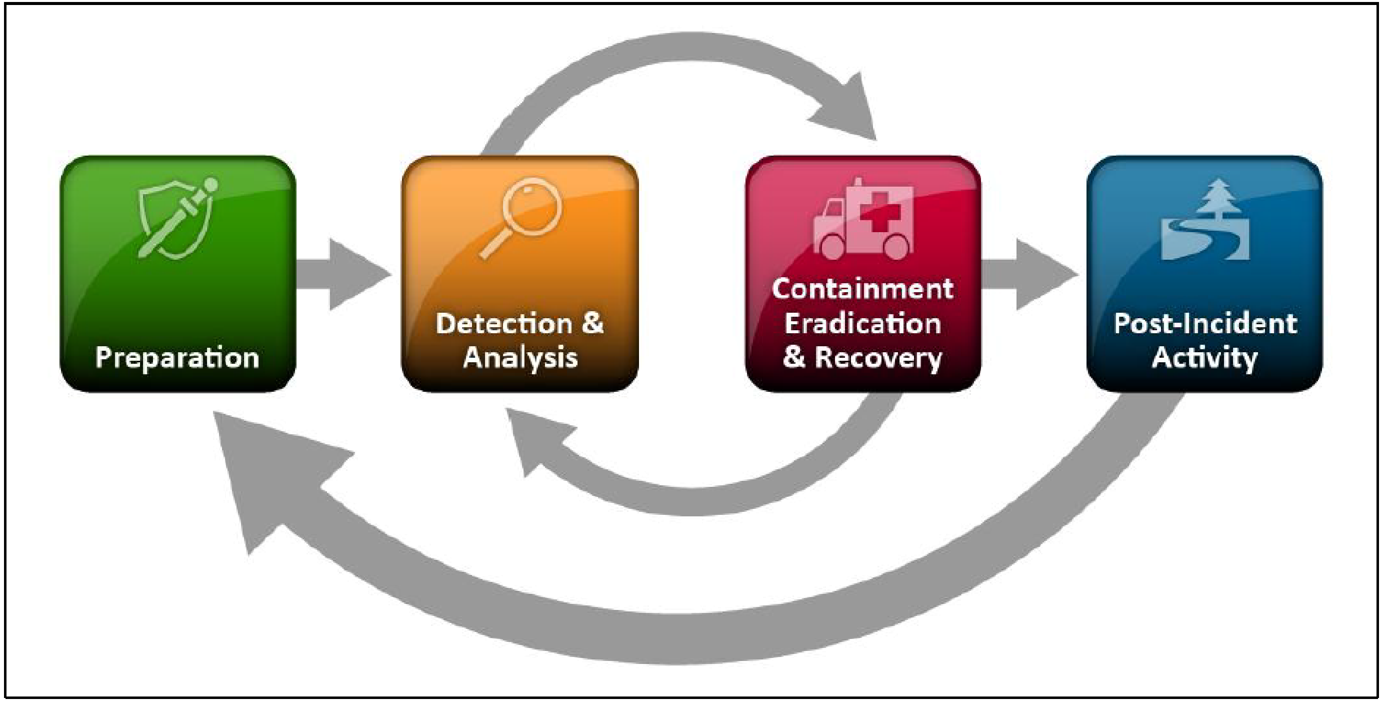
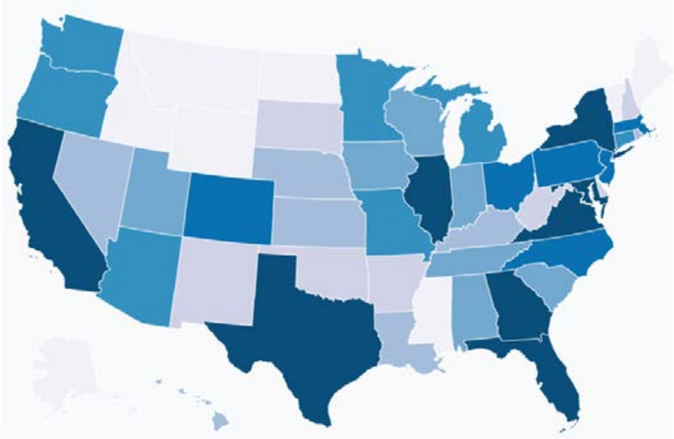
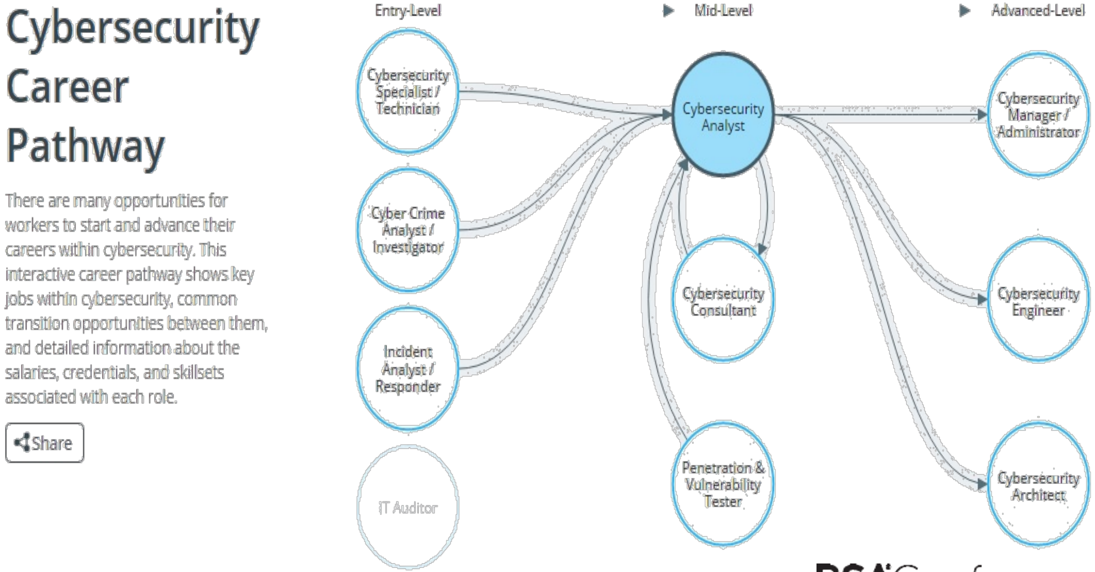


Figure 3-1. Incident Response Life Cycle

Online tools help track our progress in closing the cybersecurity workforce gaps





Cybersecurity Career Pathway

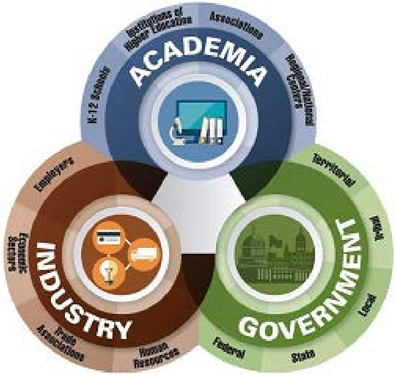
There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role.

Share
Entry-Level
Mid-Level
Advanced-Level
Cybersecurity Specialist / Technician
Cyber Crime Analyst / Investigator
Incident Analyst / Responder
IT Auditor
Cybersecurity Analyst
Cybersecurity Consultant
Penetration & Vulnerability Tester
Cybersecurity Manager / Administrator
Cybersecurity Engineer
Cybersecurity Architect

COMMERCIAL

NICE is about Partnership and Collaboration

- **NICE Staff**
  - Rodney Petersen, Director
  - Bill Newhouse, Deputy Director
  - Danielle Santos, Program Manager
  - Marian Merritt, Lead - Industry Engagement
  - Davina Pruitt-Mentle,
    Lead – Academic Engagement
  - Clarence Williams,
    Lead - Government Engagement
- **NICE Interagency Coordinating Council (ICC)**
- **Cybersecurity Credentials Collaborative (C3)**



- **NICE Working Group and Sub-Groups**
  - **K-12**
  - **Collegiate**
  - **Competitions**
  - **Training and Certifications**
  - **Workforce Management**

niceframework@nist.gov

Working together we can help achieve the NICE strategic goals

- Using the tools and collaboration described, NICE helps organizations to create, connect, retain, and improve cybersecurity professionals that are qualified, effective, and satisfied

LEARNING & SKILLS DE OPMENT
ACCELERATE

A DIVERSE LEARNING C MUNITY
NURTURE

CAREER DEVELOPMENT & WORK CE PLANNING
GUIDE

Time to go hire train and prepare your staff for the exciting challenges in cybersecurity

- Next week you should:
  - Review NIST 800-181 and familiarize yourself with the roles, tasks and KSAs
- In the first three months following this presentation you should:
  - Align training programs with the roles and tasks within NIST 800-181
  - Revise existing requisitions to properly identify the type of staff needed for the position
- Within six months you should:
  - Share your knowledge required the KSAs and how your organization uses them to standardize hiring and performance reporting reviews

We are happy to answer your questions

Greg Witte
Senior Security Engineer
greg.witte @g2-inc.com
(301) 346-2385

Tom Conkle
Cybersecurity Engineer
tom.conkle@g2-inc.com
(301) 575-5139