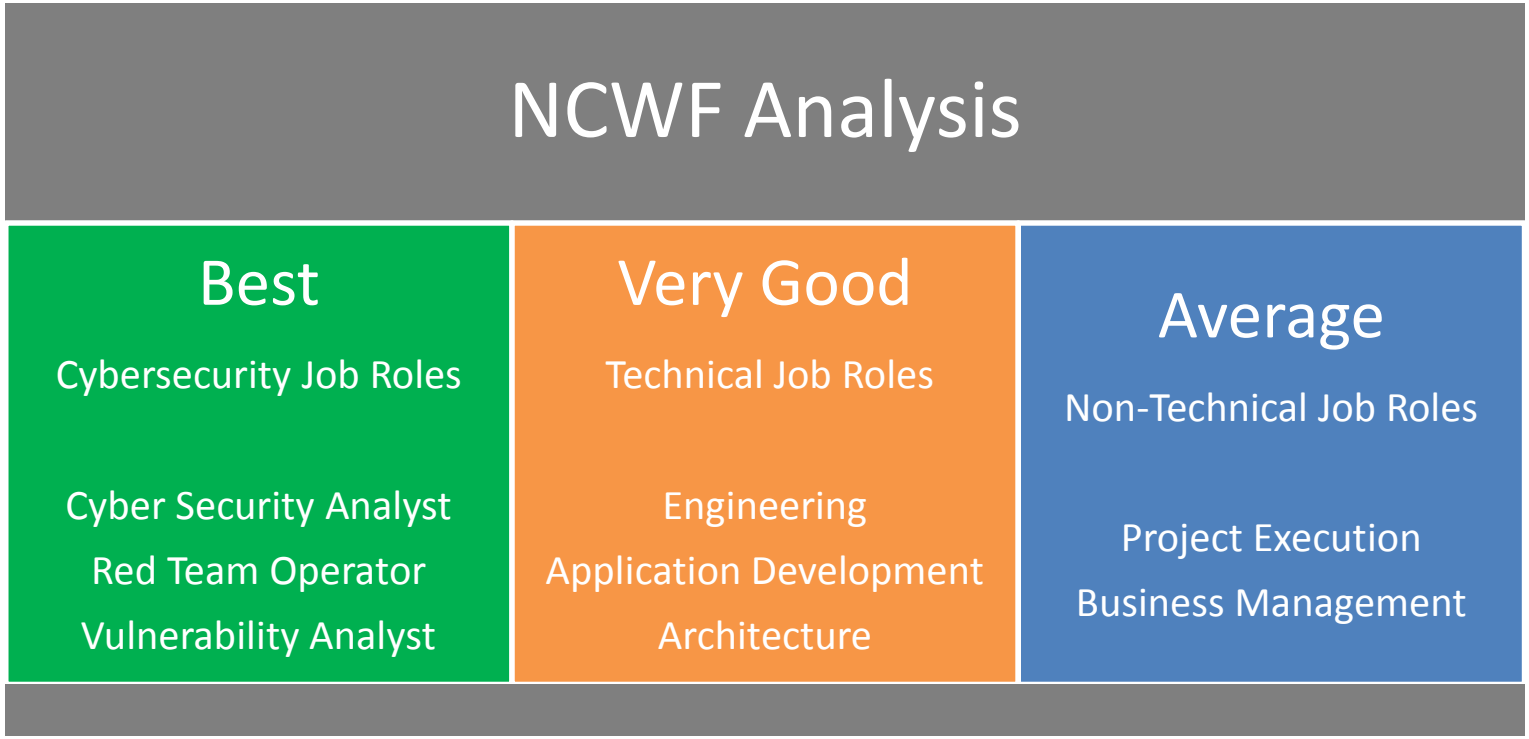
A NICE Overview of the NCWF

Leo Van Duyn

High Level Review



- Provides a solid foundation of KSAs (Knowledge, Skill and Ability) to define your workforce profiles.
- KSA's are high level and require context to make them measurable.
- Enhancing 'soft skills' (communication, presentation, listening, management, etc.) would make the NCWF more rounded.

Objective

Discuss lessons learned during the 1st phase of adopting the NCWF (National Cybersecurity Workforce Framework) for the organizational needs below.

BUILD

What Should a Cybersecurity Team Look Like?

Roles that make up a great cybersecurity team; cybersecurity talent profiles to help make informed hiring decisions; and tips for recruiting cybersecurity staff.

ADVANCE

Develop Your People

Templates to create custom cybersecurity career paths; links to training, certifications and professional events; and ideas for retaining staff at every level.

BUILD What Should a Cybersecurity Team Look Like?

1. Choose from a list of Specialty Areas (found in the Workforce Framework) for each position that includes cybersecurity work.

2. Compare current tasks performed to additional tasks recommended for each Specialty Area.

Challenge: Classified Specialty Areas are not defined or existing Specialty Area definitions are too constrained.

Computer Network Defense Analysis

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 in order to protect information, information systems, and networks from threats.

Competencies

KSAs for this Specialty Area roll-up into the following:
- Computer Forensics
- Computer Languages

KSAs

Experts in this Specialty Area have the following Knowledge, Skills, and Abilities:
- Ability to interpret and incorporate data from multiple tool sources
- Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. ...
- Knowledge of basic system administration, network, and operating system hardening techniques

Tasks

Professionals involved in this Specialty Area perform the following tasks:
- Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information
- Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources

Related Job Titles

Persons working in this Specialty area may have job titles similar to:
- CND Analyst (Cryptologic)
- Cyber Security Intelligence Analyst
- Focused Operations Analyst

Cyber Operations

Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Competencies

KSAs for this Specialty Area roll-up into the following:
- Classified

KSAs

Experts in this Specialty Area have the following Knowledge, Skills, and Abilities:
- Classified

Tasks

Professionals involved in this Specialty Area perform the following tasks:
- Classified

Related Job Titles

Persons working in this Specialty area may have job titles similar to:
- Classified

BUILD What Should a Cybersecurity Team Look Like?

Challenge: Classified Specialty Areas are not defined or existing Specialty Area definitions are too constrained.

Solution: Use the full KSA and Task taxonomy to create custom Specialty Area/Role based mappings.

NOTE: 'Competency Area' associations occur when you select your KSAs

Cyber Operations

Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

KSAs

- Knowledge of electronic evidence law
- Knowledge of encryption algorithms (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)
- Knowledge of file system implementations (e.g., NTFS, FAT, EXT)
- Knowledge of hacking methodologies in Windows or Unix/Linux environment
- Knowledge of how different file types can be used for anomalous behavior
- Knowledge of incident response and handling methodologies
- Knowledge of investigative implications of hardware, Operating Systems, and network technologies
- Knowledge of legal governance related to admissibility (Federal Rules of Evidence)

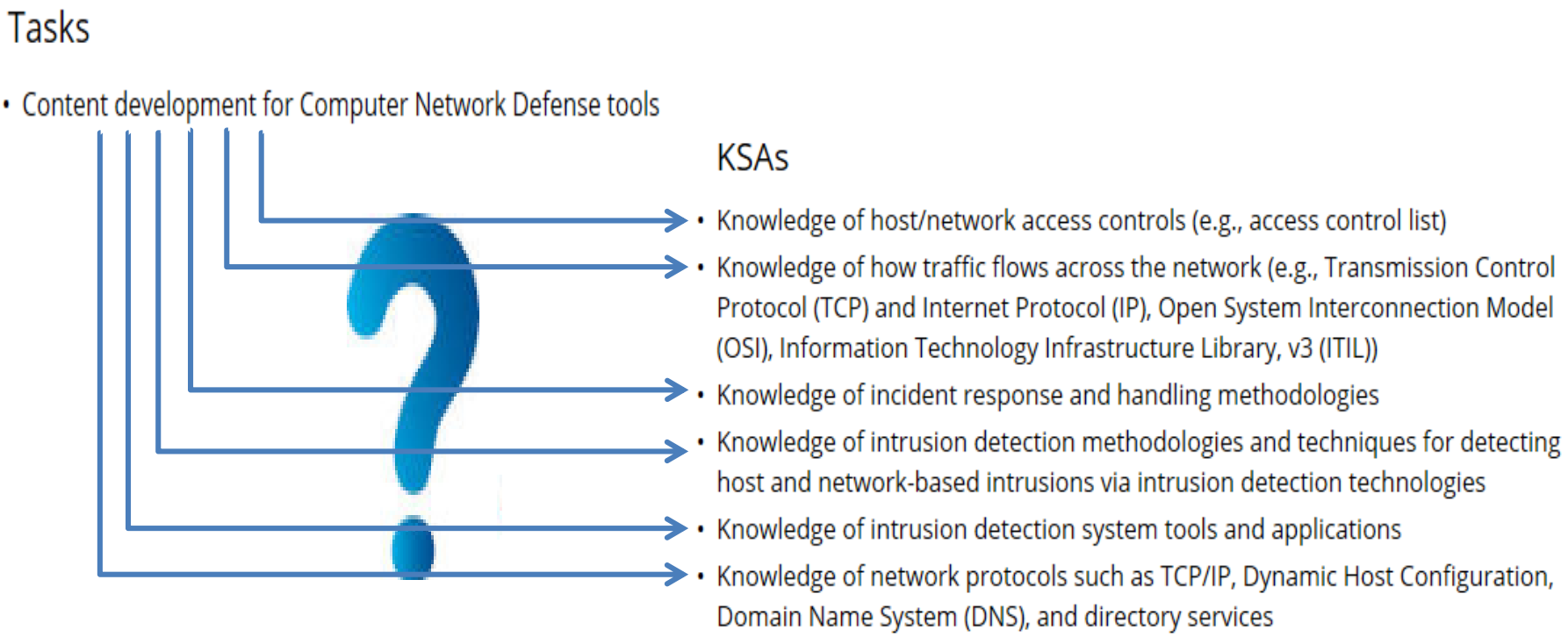
Tasks

- Ensure chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence
- Examine recovered data for information of relevance to the issue at hand
- Formulate a strategy to ensure chain of custody is maintained in such a way that the evidence is not altered (ex: phones/PDAs need a power source, hard drives need protection from shock and strong magnetic fields)

BUILD What Should a Cybersecurity Team Look Like?

1. Align position descriptions, job duties, and competencies to the Workforce Framework to operate successfully. For example, you can use Specialty Area definitions, as well as Tasks and knowledge, skills and abilities (KSAs), to develop position descriptions and establish competency models.

Challenge: For defined Specialty Areas there is no association between the areas 'Tasks' and the 'KSA's' required to accomplish the 'Task'



BUILD What Should a Cybersecurity Team Look Like?

Challenge: For defined Specialty Areas there is no association between the areas 'Tasks' and the 'KSA's' required to accomplish the 'Task'

Solution: Leverage role based SME's (subject matter experts) to map the 'Specialty Area' tasks to the respective KSAs.

NOTE: The Task listed is from the 'Specialty Area' Incident Response but is relevant to a role we mapped to a different 'Specialty area'. Another reason to consider custom Specialty Area/Role based mappings.

Tasks

- Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security

KSAs

- Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
- Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep).
- Knowledge of security event correlation tools.

ADVANCE Develop Your People

1. Develop and share career paths with employees to help staff identify their proficiency levels and advance in their chosen paths.

Challenge: What is the best method for establishing proficiency levels; 'Specialty Area/Role Based', 'Competency Area' or 'KSA' level?

Specialty/Role Level	Competency Level	KSA Level
Highest Level Mapping	Defines a Group of KSAs	Most Granular Level Mapping
Required Creation of More Role Profiles (BIAE)	Easier to Maintain as NCWF Taxonomy evolve	Difficult to Maintain as NWCF Taxonomy evolves
Difficult to integrate into Learning Management System Skill Categories	More Closely Aligned to Learning Management System Skill Categories.	Can Leverage Competency Area Association for Learning Management System Skill Categories
Only Maps Training/Courses to the Role	Create IDPs (Individual Development Plans) When Coupled with Specialty/Role Level Mapping	Difficult to Map to Training/Course Offerings

ADVANCE Develop Your People

Challenge: What is the best method for establishing proficiency levels; 'Specialty Area/Role Based', 'Competency Area' or 'KSA' level?

Solution: 'Competency Area' based proficiency levels were selected

NOTE: The KSA profile applies to all grades selected. The KSA profile represents what is required for the highest grade.

Job Title - **FreeText**	SOC Analyst		
NICE Specialty Area - **Dropdown**	Computer Network Defense Infrastructure Support		
Competency Area	Grade 1 Competency Proficiency Rating	Grade 2 Competency Proficiency Rating	Grade 3 Competency Proficiency Rating
Computer Forensics	N/A	Beginner	Beginner
Computer Languages	Beginner	Beginner	Intermediate
Computer Network Defense	Beginner	Intermediate	Advanced
Cryptography	Beginner	Intermediate	Intermediate
Encryption	Beginner	Intermediate	Intermediate
External Awareness	Beginner	Intermediate	Intermediate
Incident Management	Beginner	Intermediate	Advanced
Information Systems/Network Security	Beginner	Intermediate	Advanced
Operating Systems	Beginner	Beginner	Intermediate
Oral Communication	Beginner	Intermediate	Advanced
Vulnerabilities Assessment	N/A	Beginner	Intermediate

ADVANCE Develop Your People

1. Develop and share career paths with employees to help staff identify their proficiency levels and advance in their chosen paths.

Challenge: What criteria do you use to define your proficiency level; **Qualifying Statements** or Specialty Area Behavioral Indicators?

Level	Area	Qualifying Statement
Beginner	Knowledge	Employee can identify basic facts and terms about the subject.
Intermediate	Knowledge	Employee can identify relationships of basic facts and state general principles about the subject.
Advanced	Knowledge	Employee can analyze facts and principals and draw conclusions about the subject.
Expert	Knowledge	Employee can evaluate conditions and make proper decisions about the subject.
Beginner	Skill/Ability	Can do simple parts of the task. Needs to be told how to do most of the task.
Intermediate	Skill/Ability	Can do most parts of the task. Needs help performing only on the hardest parts of the task.
Advanced	Skill/Ability	Can do all parts of the task. Needs only a spot check of completed work to ensure task performed correctly.
Expert	Skill/Ability	Can do the completed task quickly and accurately. Can tell and show others how to do the task.

1. Develop and share career paths with employees to help staff identify their proficiency levels and advance in their chosen paths.

Challenge: What criteria do you use to define your proficiency level; Qualifying Statements or **Specialty Area Behavioral Indicators**?

Incident Response	Responds to crisis 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.
	BEHAVIORAL INDICATORS
1 Basic	• Maintains awareness and reports alerts from various sources within the enterprise to management; requests digital media (e.g., thumb drives, flash drives, and hard drives), and provides it to incident response/field support teams for further analysis • Performs internal and external research with guidance, searching for similar or related network events or incidents in tracking tools (e.g., Remedy) • Maintains a status (situational awareness) of security sensor events and incidents to provide real-time status reporting on systems, controls and resources • Uses an event as an opportunity to observe and understand the formal protocols and procedures for an incident investigation • With guidance, queries proxy logs to assist CND personnel and assist with mitigation of incidents as directed
2 Intermediate	• Maintains and administers computer networks and/or related computing environments, including computer hardware, software, applications software and all configurations to protect, defend and restore cyber related services and capabilities • Performs analysis of log files from a variety of sources to identify threats and assists in the development of signatures that trigger network based event alerts and conducts backup and recovery to prevent events and incidents • Performs incident triage by determining scope, urgency, and potential impact, and collaborating with incident responders to mitigate the incident • Tracks and documents cyber related incidents from initial detection through final resolution by following established procedures and protocols; verifies that incidents have reached final resolution prior to completing tracking documentation
3 Advanced	• Analyzes cyber related alerts from various sources and performs log analysis (e.g. firewall logs and intrusion detection system logs) and synthesizes this information to identify abnormal activity • Collects and analyzes intrusion artifacts (e.g., source code and security event logs) to troubleshoot, diagnose, and mitigate cyber related incidents • Reviews and analyzes a cyber related incident and develops cyber related guidance and reports on incident findings for appropriate constituencies • Designs and oversees the construction of signatures that trigger network based event alerts • Reverse engineer and/or conducts root-cause analysis
4 Expert	• Develops enterprise-wide (to include corporate, federal department, public service agency) mitigation strategies for identified or abnormal cyber related activities • Oversees and coaches others in network mapping, hardening, configuration, diagnostics, and mitigation strategies • Correlates incident data to identify exploited vulnerabilities; makes recommendations that enable expeditious remediation and provides enterprise-wide strategies to prevent future occurrences • Reviews and validates the construction of signatures that trigger network based event alerts

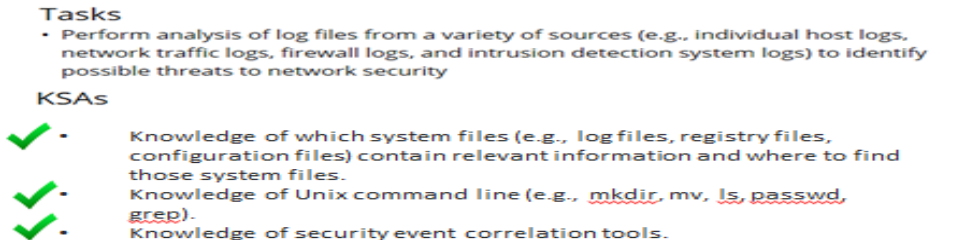
ADVANCE Develop Your People

1. Develop and share career paths with employees to help staff identify their proficiency levels and advance in their chosen paths.

Challenge: Making KSA's measureable and/or meaningful without changing the NCWF taxonomy?

NOTE: Consider using a workforce management tool or database

1. Map Tasks to profiles KSAs



2. Align objectives to Tasks

Objectives
- Basic Splunk Searching
- grep/sed/awk
- Timeline development

Task
- Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.

3. Capture employee context

Employee Context

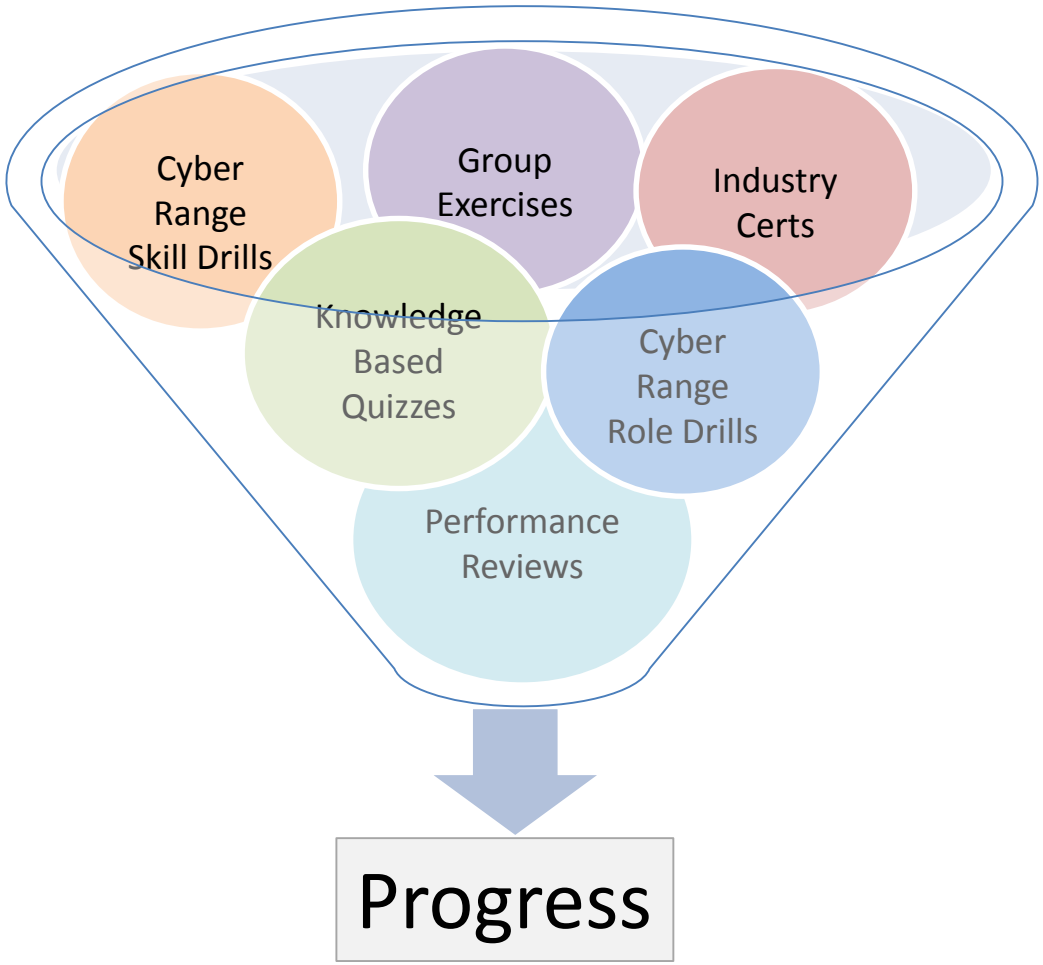
KSAs
- Knowledge of operating systems.

Context
- Windows 10
- Linux
- Red hat
- IOS 8.x

ADVANCE Develop Your People

1. Develop and share career paths with employees to help staff identify their proficiency levels and advance in their chosen paths.

Challenge: How can you measure an employees proficiency progression.



ADVANCE Develop Your People

Help Your Staff Navigate Cybersecurity Careers