The Lack of Incident Response Curriculum in the CAE Community: Call to Action

CAE in Cybersecurity Community Symposium

June 9, 2022

Hub & Spoke Project

:: *"Research and Deliverables on Utilizing an Academic Hub and Spoke Model to Create a National Network of Cybersecurity Institutes"*

Hub & Spoke Project (con't)

:: Included 3 partners: Auburn Univ., Purdue Univ., Univ. of Tulsa

:: Network of 2/4-year schools (Hubs and Spokes)

:: IR and ICS security-related education and training (initially)

:: Emphasis on underserved populations

Hub & Spoke Project (con't)

:: **Project Deliverables**: Various reference documents, including degree & certificate templates mapped to various curriculum & workforce frameworks and IR-related work roles

Hub & Spoke Project (con't)

305

Hub & Spoke Project (con't)

77

Hub & Spoke Project (con't)

22

Hub & Spoke Project (con't)

10

What shapes IR in workforce development?

:: Frameworks

National Initiative for Cybersecurity Education (NICE)

NIST Cybersecurity Framework

Skills Framework for the Information Age (SFA)

ACM: Cybersecurity Curriculum 2017, Computing Curricula 2020

:: Certifications

CISSP, CREST, EC CSA

:: Bodies of Knowledge

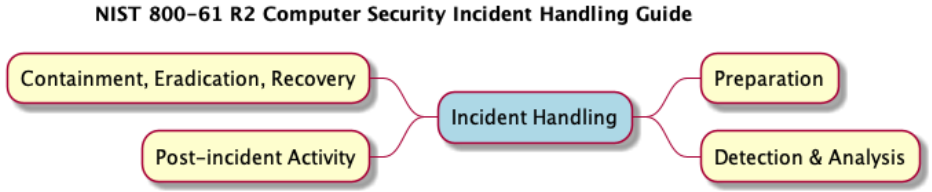
CyBok, SANS Incident Handler's Handbook

:: Assessment

CMMC, O-ISM3, Incident Management Capability Assessment

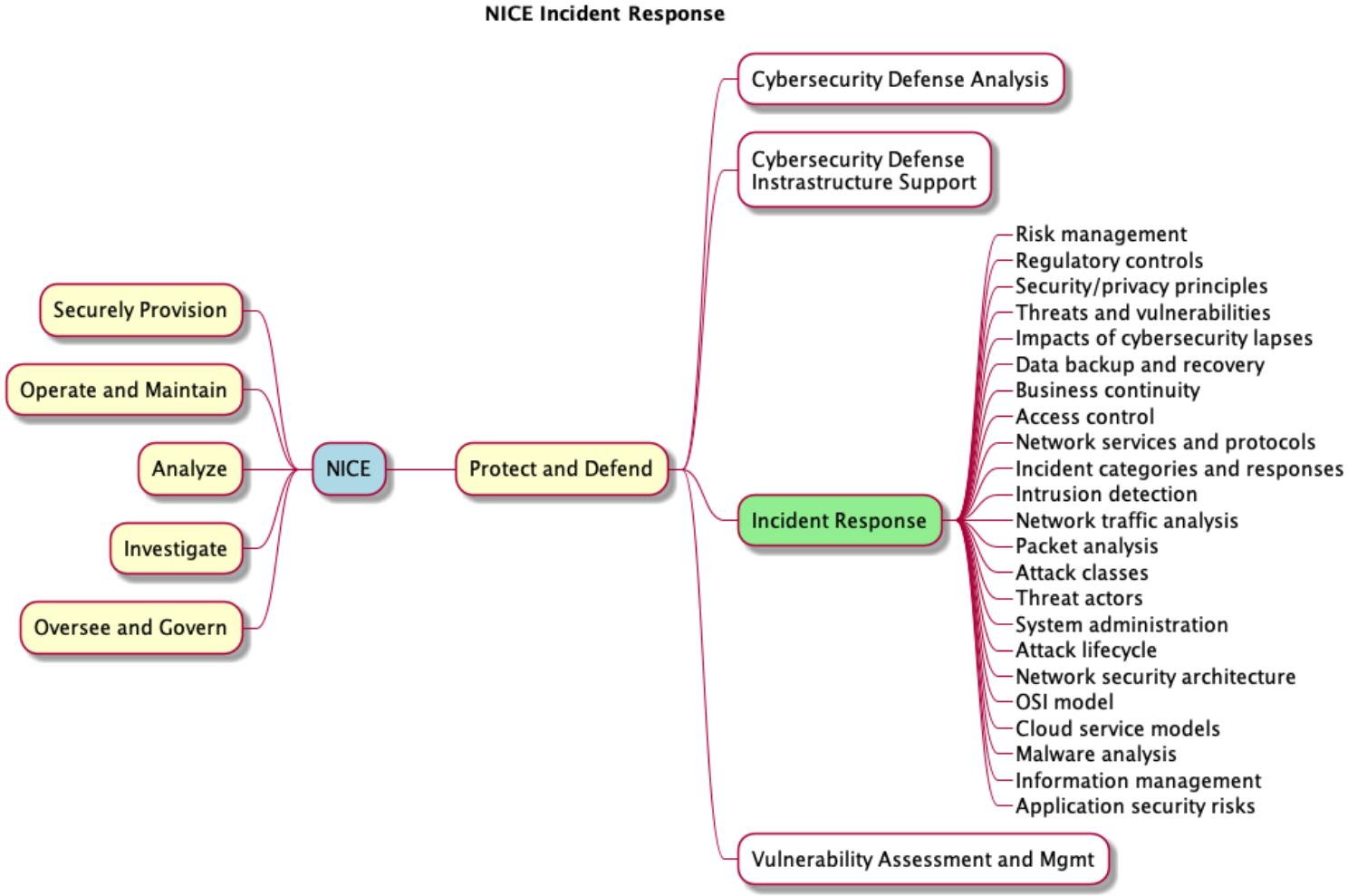
:: Standards

NIST 800-61 R2: Computer Security Incident Handling Guide



Source:https://www.nist.gov/document/supplementnicespecialtyareasandworkroleksasandtasksxlsx

VS



Source:https://www.nist.gov/document/supplementnicespecialtyareasandworkroleksasandtasksxlsx

Observations on the state of IR

:: Inconsistent use of the term *cyber incident response* points to an under-developed integration of technical vs non-technical knowledge requirements of cybersecurity.

incident response tends to associate with technical

incident management tends to associate with non-technical

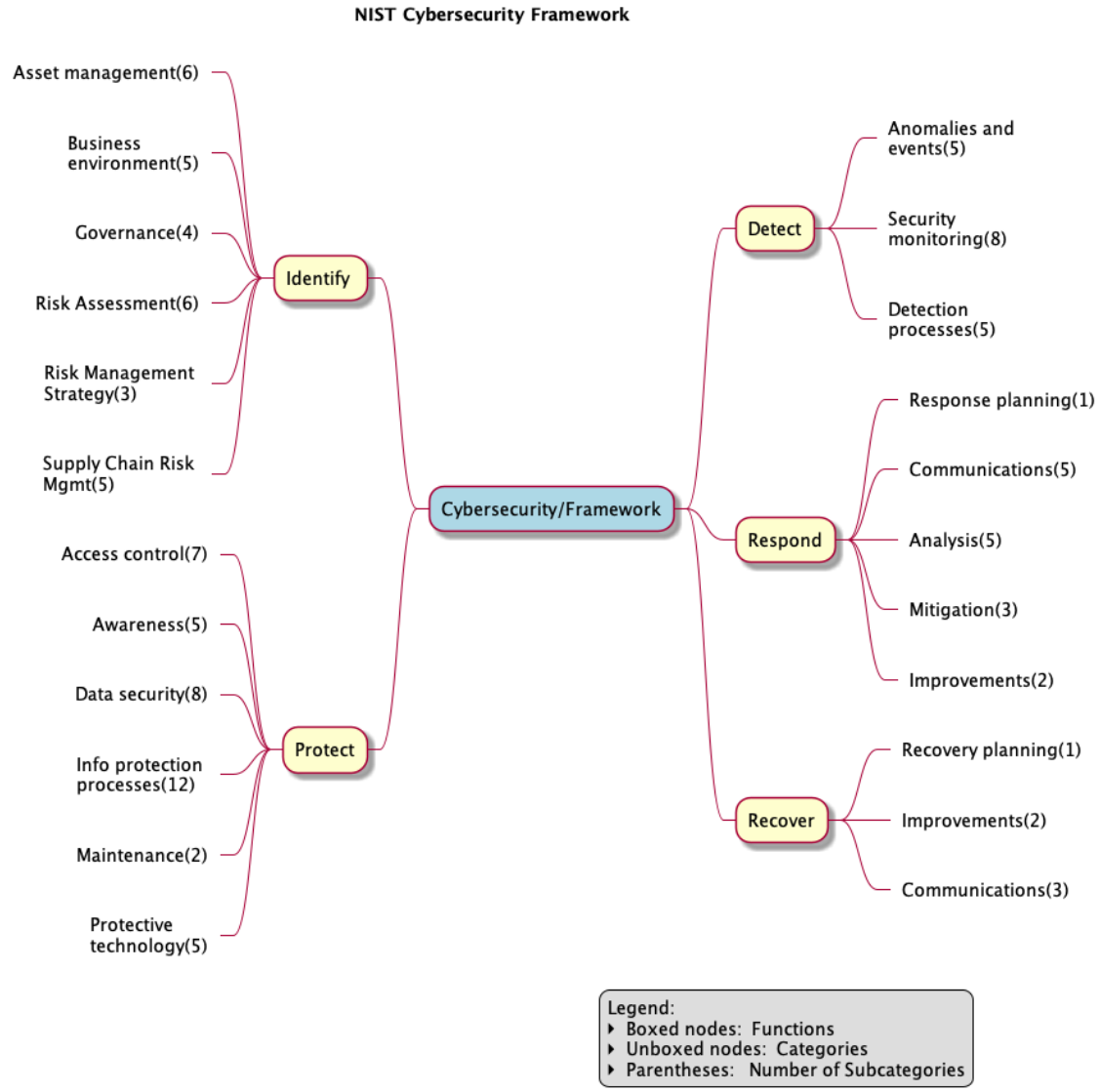
:: The output of workforce development efforts does not synch effectively with workforce needs.

IR considerations

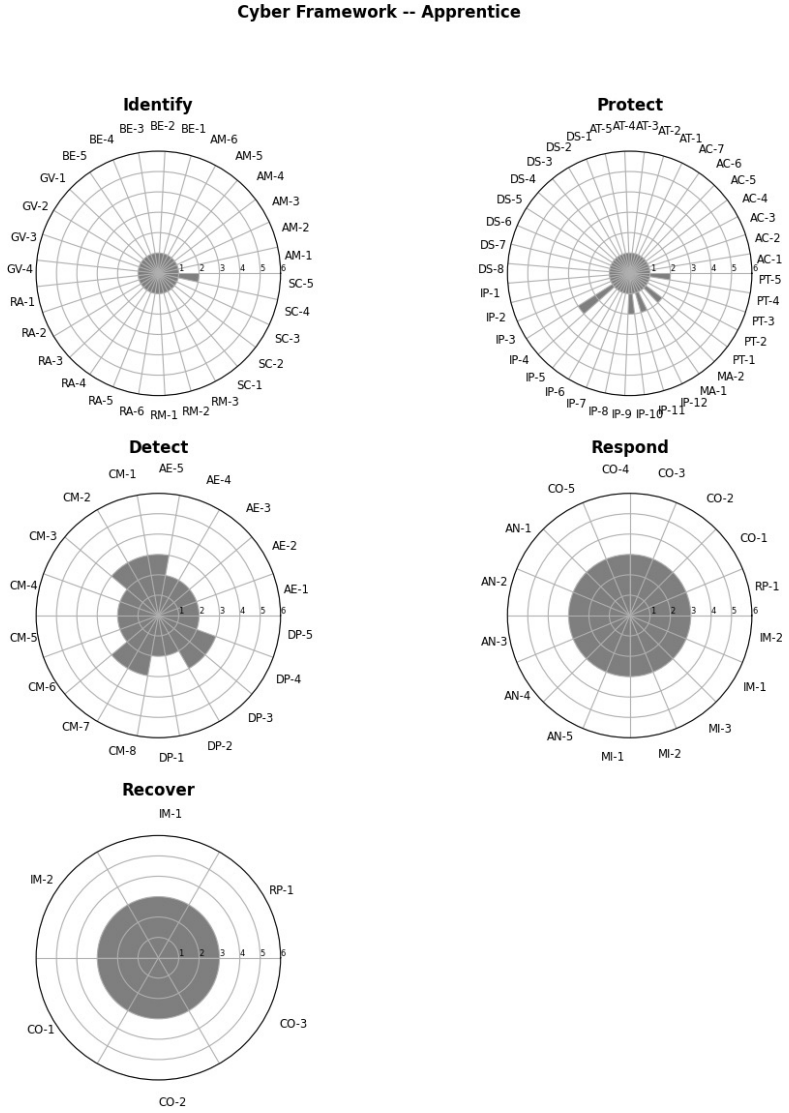
:: We envision developing a cyber incident handling body-of-knowledge (CIH BoK) that identifies concepts and relationships among concepts:

- Express the CIH BoK as an ontological list of topics showing close and supporting concepts.
- Provide dimensionality to topics based on career progression: apprentice, journeyman, specialist, master.
- Provide depth to topics based on domain: e.g., IT, OT, IoT.
- Develop curricular material for topics, to sample teaching material; pre-requisite skills and knowledge; and post-requisite learning outcomes.

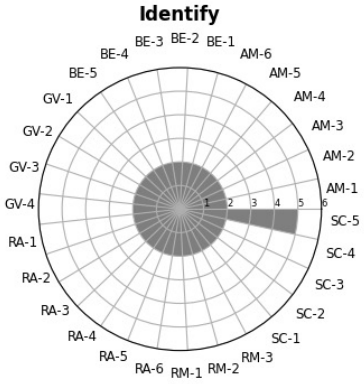
:: The NIST Cybersecurity Framework could possibly offer the richest starting point for a CIH Bok

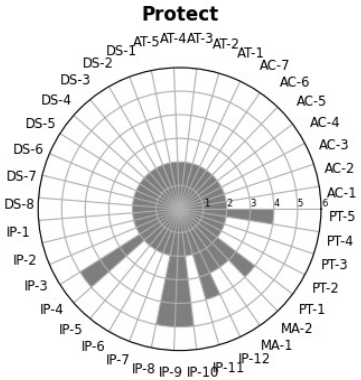


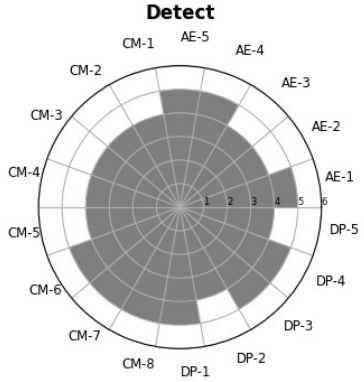
Source: https://www.nist.gov/cyberframework

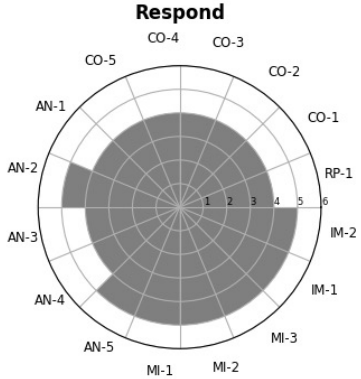


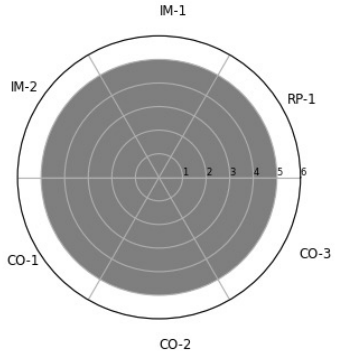
Cyber Framework -- Specialist



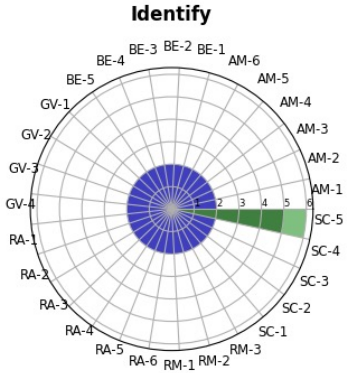


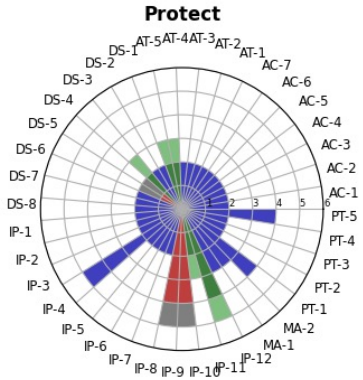


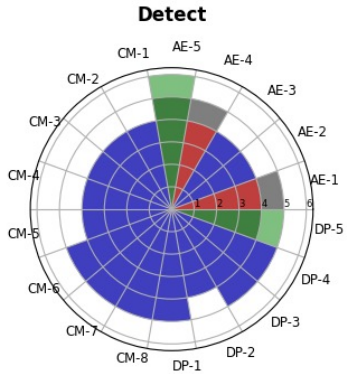


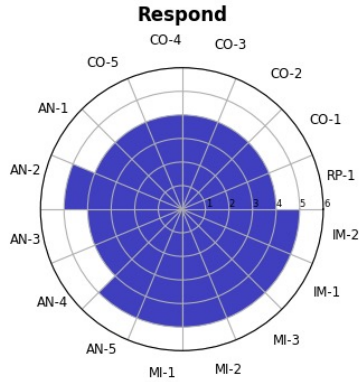


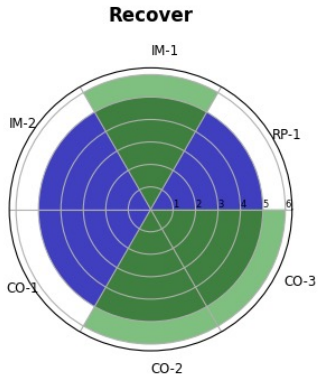
Cyber Framework -- Specialist Assessed











green=exceeded
blue=met
red=unmet

Call to Action

:: **Interested Schools**:

> Looking to adopt & adapt their curriculum to focus on IR, or

> Create new IR degrees & certificate programs

Contact Information

:: Casey W. O'Brien
:: Assistant Director, Cyber Defense Education and Training
:: Information Trust Institute, Univ. of Illinois Urbana-Champaign
:: cwobrien@Illinois.edu

:: David A. Umphress
:: COLSA Professor of Cybersecurity
:: CSSE Dept, Auburn University
:: david.umphress@auburn.edu