Cybersecurity for Curriculum Alignment

7. Incident Response

	KSA Description	Knowledge, Skill, or Ability?	Bloom's Taxonomy Level?	Cross-cutting KSAs	Course Number/Name	Learning Outcome
a	Understand the concept of a Cybersecurity Operations Center (CSOC).and how network security is implemented in the CSOC	Knowledge	2			
b	Understand log filtering and aggregation.	Knowledge	2			
c	Understand SIEM technology.	Knowledge	2			
d	Understand the role of alert signatures.	Knowledge	2			
e	Run queries on event data.	Ability	3			
f	Understand forensics and chain of custody.	Knowledge	2			
g	~~A~~pply procedures and workflow of ticketing.	Skill	3			
h	~~A~~pply situational awareness.	Skill	3			
i	Apply Incident Response procedures (e.g. preparation, incident identification, escalation and notification, mitigation steps, lessons learned, reporting, recovery procedures, first responder, incident isolation, quarantine, device removal, and data breach).	Skill	3			
j	Construct a timeline of a cybersecurity incident.	Ability	3			
k	Implement a recovery procedure.	Skill	3			
l	Conduct periodic cybersecurity training exercises.	Skill	3			
m	Differentiate between detection controls and prevention controls (e.g., IDS vs. IPS, camera vs. guard).	Knowledge	4			
n	Create, edit and use roles and system management tools.	Ability	3			
o	Implement Access Control Lists (ACL).	Skill	3			
p	Deploy a server hardening plan.	Skill	3			
q	Implement a Network Access Control (NAC) plan.	Skill	3			
r	Interpret alarms and alert trends.	Skill	2			
s	Differentiate between types of enetration testing (e.g., Black box, White box, Gray box).	Knowledge	4			