CoLAB TalentReady IT Pathways
Cyber Technologist KSAs for Curriculum Alignment

5. Incidence Response

	KSA Description	Knowledge, Skill, or Ability?	Bloom's Taxonomy Level?	Cross-cutting KSAs	Notes
a	Understand the concept of Cybersecurity Operations Center (CSOC).	Knowledge	2		
b	Understand how network security is implemented in a Cybersecurity Operations Center (CSOC).	Knowledge	2		
c	Understand log filtering and aggregation.	Knowledge	2		
d	Understand SIEM technology.	Knowledge	2		
e	Understand the role of alert signatures.	Knowledge	2		
f	Run queries on event data.	Ability	3		
g	Understand forensics and chain of custody.	Knowledge	2		
h	Apply procedures and workflow of ticketing.	Skill	3		
i	Apply Situational awareness.	Skill	3		
j	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, Data breach).	Skill	3		
k	Construct a timeline of cybersecurity incident.	Ability	3		
l	Implement a recovery procedure.	Skill	3		
m	Conduct periodic cybersecurity training exercises.	Skill	3		
n	Differentiate between detection controls and prevention controls (e.g., IDS vs. IPS, Camera vs. guard).	Knowledge	4		
o	Create, edit and use roles and system management tools.	Ability	3		
p	Implement endpoint security.	Skill	3	Cyber Security Specialist 8d	
q	Implement Access Control Lists (ACL).	Skill	3		
r	Deploy a server hardening plan.	Skill	3		
s	Implement a Network Access Control (NAC) plan.	Skill	3		
t	Interpret alarms and alert trends.	Knowledge	2		
u	Differentiate between types of Penetration testing (e.g., Black box, White box, Gray box).	Knowledge	4		