

Incident Response Discovery and Mitigation Scoring Guide

Due Date: End of Unit 6.

Percentage of Course Grade: 8%.

CRITERIA	NON-PERFORMANCE	BASIC	PROFICIENT	DISTINGUISHED
Recommend appropriate workflows within a specific organization in response to a potential incident. 30%	Does not recommend appropriate workflows within a specific organization in response to a potential incident.	Recommends partially or at a high level appropriate workflows within a specific organization in response to a potential incident.	Recommends appropriate workflows within a specific organization in response to a potential incident.	Recommends appropriate workflows within a specific organization in response to a potential incident and provides support for the choices.
Evaluate security controls that would have aided in discovery, data collection, and analysis following a specific incident within an organization. 30%	Does not evaluate security controls that would have aided in discovery, data collection, and analysis following a specific incident within an organization.	Evaluates partially or at a high level security controls that would have aided in discovery, data collection, and analysis following a specific incident within an organization.	Evaluates security controls that would have aided in discovery, data collection, and analysis following a specific incident within an organization.	Evaluates comprehensively security controls that would have aided in discovery, data collection, and analysis following a specific incident within an organization.
Evaluate the impact to multinational organizations of having network segments in underdeveloped countries. 30%	Does not evaluate the impact to multinational organizations of having network segments in underdeveloped countries.	Evaluates partially or at a high level the impact to multinational organizations of having network segments in underdeveloped countries.	Evaluates the impact to multinational organizations of having network segments in underdeveloped countries.	Evaluates comprehensively the impact to multinational organizations of having network segments in underdeveloped countries.
Exhibit proficiency in writing, critical thinking, and research topic areas in IT security fundamentals. 10%	Does not exhibit proficiency in writing, critical thinking, and research topic areas in IT security fundamentals.	Exhibits a low level of proficiency in writing, critical thinking, and research topic areas in IT security fundamentals.	Exhibits proficiency in writing, critical thinking, and research topic areas in IT security fundamentals.	Exhibits a high level of proficiency in writing, critical thinking, and research topic areas in IT security fundamentals.