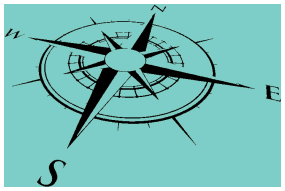
Organizational Role Description

This is an alpha version of a proposed set of roles for Cyber Defense Incident Responders transmitted via E-mail by Dorian J. Cougias, Co-Founder and Compliance Scientist, Unified Compliance Framework (grcschema.org) on March 29, 2021

Contents



Cyber Defense Incident Responder (CDIR)

Stakeholder(s):

Executive Cyber Leaders :
Reports To: executive cyber leadership

Vision

Cyber incidents are quickly and effectively addressed

Mission

To investigate, analyze, and respond to cyber incidents within a network environment or enclave.

1. Abilities

Demonstrate the following abilities

Role Abilities ~ These are the required abilities associated with the performance of this role.

1.1. Responses

Design incident response for cloud service models.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

1.2. Detection

Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2. Knowledge

Demonstrate the following knowledge

Role Knowledge ~ This is the required knowledge associated with the performance of this role.

2.1. Networks

Comprehend computer networking concepts and protocols, and network security methodologies.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.2. Risk

Comprehend risk management processes (e.g., methods for assessing and mitigating risk).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.3. Laws, Regulations, Policies & Ethics

Comprehend laws, regulations, policies, and ethics as they relate to Cybersecurity and privacy.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.4. Cybersecurity & Privacy

Comprehend cybersecurity and privacy principles.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.5. Rhreats & Vulnerabilities

Comprehend cyber threats and vulnerabilities.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.6. Operational Impacts

Comprehend specific operational impacts of cybersecurity lapses.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.7. Backup & Recovery

Comprehend data backup and recovery.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.8. Continuity

Comprehend business continuity and disaster recovery continuity of operations plans.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.9. Access

Comprehend host/network access control mechanisms (e.g., access control list, capabilities lists).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.10. Interactions

Comprehend network services and protocols interactions that provide network communications.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.11. Incidents & Responses

Comprehend incident categories, incident responses, and timelines for responses.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.12. Incident Methodologies

Comprehend incident response and handling methodologies.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.13. Detection Methodologies

Comprehend intrusion detection methodologies and techniques for detecting host and network-based intrusions.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.14. Traffic Analysis

Comprehend network traffic analysis methods.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.15. Packets

Comprehend packet-level analysis.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.16. Systems & Applications

Comprehend system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.17. Attacks

Comprehend what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.18. Defense

Comprehend cyber defense and information security policies, procedures, and regulations.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.19. Attack Classes

Comprehend different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.20. Attackers

Comprehend cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.21. Administration & Hardening

Comprehend system administration, network, and operating system hardening techniques.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.22. Attack Stages

Comprehend cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.23. Security Architecture

Comprehend network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.24. OSI & Protocols

Comprehend OSI model and underlying network protocols (e.g., TCP/IP).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.25. Cloud

Comprehend cloud service models and how those models can limit incident response.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.26. Malware

Comprehend malware analysis concepts and methodologies. [bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.27. Information Classification

Comprehend an organization's information classification program and procedures for information compromise.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.28. Network Protocols

Comprehend network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

2.29. Application Risks

Comprehend Application Security Risks (e.g. Open Web Application Security Project Top 10 list) [bloom level 3] program and procedures for information compromise.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

3. Skills

Demonstrate the following skills

Role Skills ~ These are the required skills associated with the performance of this role.

3.1. Malware

Identify, capture, contain, and report malware.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

3.2. Evidence

Preserve evidence integrity according to standard operating procedures or national standards.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

3.3. Communications

Secure network communications.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

3.4. Vulnerabilities & Attacks

Recognize and categorize types of vulnerabilities and associated attacks.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

3.5. Protection

Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

3.6. Damage

Perform damage assessments.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

3.7. Events

Use security event correlation tools.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

3.8. Responses

Design incident response for cloud service models.

[bloom level 3]

Performance Indicators

Description	Type	Start Date	End Date
	Target		
	Actual		

Administrative Information

Start Date:
End Date:

Publication Date: **2021-05-12**
Source: https://stratml.us/carmel/iso/part2/CDIRwStyle.xml

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone:

_07a53132-91c6-11eb-96ab-e2642a83ea00