



Cyber Range as a Service®

Range Exercises * Training * Physical/Virtual/Hybrid * Sandbox * Branded

TSI CATALOG (12)

Microsoft Azure, STRI, DISA, CYBRScore, AT&T, DS3, DIGIFLIGHT, IACD, JITC, NERC-PO, CRaaS

114c: Cyber Defense Analyst - Incident Handling Methodology

Introduction

Scenario

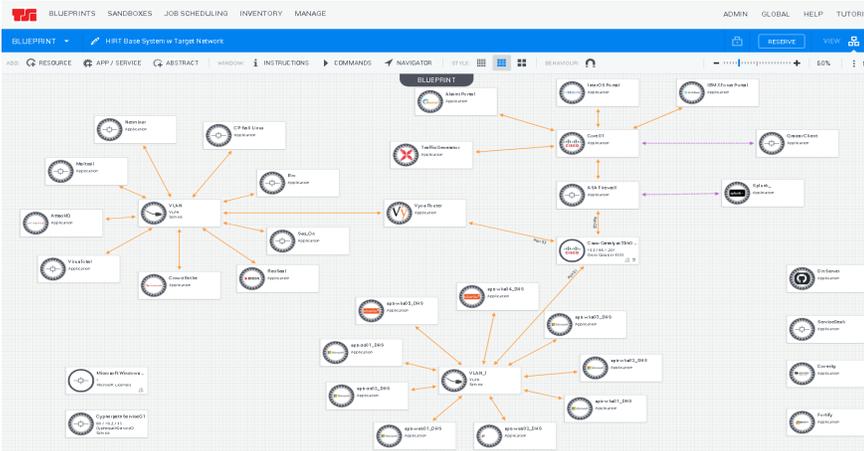
Welcome to the CDEE Cyber Defense Analyst Incident Handling Methodology Assessment

This assessment is one of five and is focused specifically on items related to incident handling.

You are assuming the role of a cyber defense analyst at a company named ProcessBox. Your task will be presented to you in the information pane at the bottom of your browser window. You can move forward by clicking the Clone button in the bottom right-hand corner, and you can move backward by clicking the arrow button in the bottom left-hand corner.

To switch the active machine, use the Resources tab in the top right-hand corner. The tab will also give you information such as operating system and password, and will allow you to send CTRL-Alt-Delete commands to a machine.

This assessment is specifically designed to test the Knowledge, Skills, and Abilities (KSA) required in the Cyber Defense Analyst job role as defined by the NIST Framework for Cyber Incident Response.



Score Assessments Work Role

Score 81

Student Information

Name: Mr. Anonymous
Email: anonymous@cyberscore.com
Organization: Cyberscore

This Assessment

Work Date: 01/10/2024
Assessment Identifier: 10068842

Training recommendations

To improve your score on this assessment, try one of these courses or labs:

Course	Lab	Description
PRN-500L	Identifying System Vulnerabilities with OpenVAS	Students will scan a system in OpenVAS (Open Vulnerability Assessment) to discover and identify systems on the network that have vulnerabilities.
NET-400	System Administration	Provides an overview of core system administrator security concepts in both the Windows and Linux environment. Topics include: Least-Privilege, Indicators of Attack/Compromise, Privileged Access, Network Segmentation, and more.
PR100-1L	Comprehensive Threat Response	In this final lab we will attempt to exercise all the relevant skills found in this domain. We are focusing on responding to incidents and the skills needed to address these sorts of problems at the "Practitioner" level.
PR100-4L	Vulnerability Scan Analysis	Students will run a Core Impact or Nessus Scan and identify vulnerabilities. Students will then view the report and prioritize vulnerabilities according to risk.
PR100-2L	Creating Recommendations Based on Vulnerability	Students will use OpenVAS to do a vulnerability analysis and then use the results to create a report.

Cyber Range

Sandbox Description

This blueprint simulates cyber range deployment as well as cyber range control to allow for war game type scenarios in a controlled and isolated manner.

Sandbox Use

A traditional cyber range requires significant, costly investments in hardware and personnel—and even then cannot scale effectively to address today's growing network traffic volume and ever-more-complex attack vectors. Government, military, and commercial organizations are deploying "cyber ranges," test beds that allow war games and simulations to strengthen cyber security defenses and skills. CloudShell provides the ability to replicate large scale, complex and diverse networks. CloudShell can orchestrate a hybrid sandbox containing both virtual and physical resources needed for the assessment of cyber technologies. Because cyber ranges are controlled sandbox, CloudShell resource management and automation features provides the ability to stand up and tear down cyber range sandboxes as needed in a repeatable manner. Operational conditions and configurations are easily replicated to retest cyber attack scenarios. This sandbox utilizes resources such as BreakingPoint, intrusion detection, malware analyzers, threat appliances, and common services such as email and file servers. The sandbox resources are isolated into white, red and blue team areas for cyber

Resource Commands

BreakingPoint VE-03

172.10.101
BreakingPoint VE

Manage (4)

Health Check
Runs a health check by delaying a...

Power Off
No description

Power On
No description

Reset
Reset all attributes being tracked...

Traffic (2)

Start Attack
Performs a load of the attack file o...

Stop Traffic
Performs stopping into traffic.



- AgileWARE—Agile Workflow And Resource Enablement Software supporting IaaS, PaaS, SaaS, TaaS, Cyber environments
- Enterprise level, agnostic data center/cloud/converged infrastructure provisioning and orchestration framework



- Academy and labs
- Skills Assessment
- PerformanceScore



- Testing, Visibility and Security solutions for physical and virtual networks and Cyber Ranges

Cyber Range as a Service®

- Self Service web based portal
- Cyber libraries ready to deploy
- Deployable On-Prem or as SaaS
- Visio like drag and drop GUI
- Reservations & Scheduling
- Scalable and standards based
- Open vendor agnostic support
- Instruction panes for training support
- Catalogs of Sandbox environments
- Save and Restore Snapshots of Sandbox
- NIST/NICE framework supported roles and training
- Complete Skill assessments against your training or NICE framework skills
- Integrated with CRaaS AgileWARE (On/Off Prem)
- Performance scoring platform
- Breaking Point and Breaking Point VE
- IxLoad-IPSec VPN and IxLoad Attack
- Application and Threat Intelligence
- Integrated with TSI AgileWARE

TSI CRaaS

SYSTEMS INTEGRATOR AND AUTHORIZED RESELLER FOR



WWW.TSIEDA.COM (407) 339-4874, EXT 111