800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Hack The Box Certified Defensive Security Analyst (CDSA) Training

Hack The Box Authorized Training · Applied Technology Academy

HTB Certified Defensive Security Analyst (HTB CDSA) is a highly hands-on certification that assesses the candidates' security analysis, SOC operations, and incident handling skills. HTB Certified Defensive Security Analyst (HTB CDSA) certification holders will possess technical competency in the security analysis, SOC operations, and incident handling domains at an intermediate level.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**eLearning**	**1 year: Penetration Tester**	**$119,122**	**Yes**

Course Overview

This On-Demand product includes HTB Academy and Dedicated Labs.

The HTB Academy allows learners to navigate through Modules, that provide a more guided experience. Modules are broken into parts that include explanations, examples, and assessments.

With the HTB dedicated labs learners utilize virtualized machines that simulate a black-box pentesting experience. Challenges in Dedicated Labs are available in three difficulty levels: easy, medium, and hard. More difficult challenges are worth more points. Dedicated Labs are designed to work like the networks, endpoints, and servers that businesses use, so users can try advanced cyber exploitation techniques.

HTB Certified Defensive Security Analyst (HTB CDSA) is a highly hands-on certification that assesses the candidates' security analysis, SOC operations, and incident handling skills. HTB Certified Defensive Security Analyst (HTB CDSA) certification holders will possess technical competency in the security analysis, SOC operations, and incident handling domains at an intermediate level. They will be able to spot security incidents and identify avenues of detection that may not be immediately apparent from simply looking at the available data/evidence. They will also excel at thinking outside the box, correlating disparate pieces of data/evidence, and pivoting relentlessly to determine the maximum impact of an incident. Another skill they will bring is the creation of actionable security incident reports tailored for diverse audiences.

Key Differentiators

Continuous Evaluation - To be eligible to start the examination process, one must have completed all modules of the "SOC Analyst" job-role path 100% first. Each module in the path comes with its own hands-on skills assessment at the end that students must complete to prove their understanding of the presented topics. The answers to the skills assessment exercises are not provided. Evaluation takes place throughout the journey not only during the examination!

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Hands-on & Real-world Exam Environment - HTB Certified Defensive Security Analyst (HTB CDSA) candidates will be required to perform actual security analysis, SOC operations, and incident handling activities on multiple real-world and heterogeneous networks. HTB certifications are not based on and do not include multiple-choice questions!

Outside-the-box Thinking & Data Correlation - HTB Certified Defensive Security Analyst (HTB CDSA) candidates will be required to think outside the box and correlate different data/evidence to achieve the exam's objectives. Like in real-world engagements, creativity, and in-depth knowledge will be necessary for a successful outcome.

Commercial-grade Report Requirement - Successfully completing all security analysis, SOC operations, and incident handling activities is not enough to obtain the HTB Certified Defensive Security Analyst (HTB CDSA) certification. Candidates will also be required to assess the risk at which the defended infrastructure is exposed and compose a commercial-grade security incident report as part of their assessment. HTB Certified Defensive Security Analyst (HTB CDSA) candidates will have to prove they are market-ready and client-centric professionals.

Seamless Experience Powered By Pwnbox - The entire exam and certification process can be conducted through the candidates' browser, from start to finish. All security analysis, SOC operations, and incident handling activities can be performed via the provided and in-browser Pwnbox. There are no infrastructural or tool requirements.

Course Outline

- Modules
- Incident Handling Process
- Security Monitoring & SIEM Fundamentals
- Windows Event Logs & Finding Evil
- Introduction to Threat Hunting & Hunting with Elastic
- Understanding Log Sources & Investigating with Splunk
- Windows Attacks & Defense
- Intro to Network Traffic Analysis
- Intermediate Network Traffic Analysis
- Working with IDS/IPS
- Introduction to Malware Analysis
- JavaScript Deobfuscation
- YARA & Sigma for SOC Analysts
- Introduction to Digital Forensics
- Detecting Windows Attacks with Splunk
- Security Incident Reporting
- Knowledge Domains

- SOC Processes & Methodologies
- SIEM Operations (ELK/Splunk)
- Tactical Analytics
- Log Analysis
- Threat Hunting
- Active Directory Attack Analysis
- Network Traffic Analysis (Incl. IDS/IPS)
- Malware Analysis
- DFIR Operations

Intended Audience

- Entry level Security Analysts
- Entry level SOC Analysts
- Entry level Incident Handlers
- Entry level Forensics Analysts
- Penetration Testers
- IT Administrators
- IT Security Personnel

Prerequisites

The Exam

The candidate will have to perform security analysis, SOC operations, and incident handling activities against multiple real-world and heterogeneous networks hosted in HTB's infrastructure and accessible via VPN (using Pwnbox or their own local VM). Upon starting the examination process, a letter of engagement will be provided that will clearly state all engagement details, requirements, objectives, and scope. All a candidate needs to perform the required activities is a stable internet connection and VPN software. HTB Certified Defensive Security Analyst is the most up-to-date and applicable certification for Security Analysts, SOC Analysts, and Incident Handlers that focuses on both security incident analysis and professionally communicating security incidents.

Follow-On Courses

- Hack The Box Certified Penetration Testing Specialist (HTB CPTS)
- Hack The Box Certified Web Exploitation Expert (HTB CWEE)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.