HACKTHEBOX

HTB Defense Operations Analyst

CERTIFICATE PROGRAM

✓ DoW 8140 Approved ✓ ANAB-accredited ✓ Real-world applicable curriculum

The Hack The Box certificate programs accelerate professional growth through hands-on training and real-world cybersecurity simulations. By validating job-ready skills and technical proficency, these programs contribute to building an advanced and highly skilled cybersecurity workforce.

The HTB DOA Certificate is formally recognized for the following DCWF roles:

Code	Work Role	Proficency Level
511	Cyber Defense Analyst	Intermediate
212	Cyber Defense Forensics Analyst	Intermediate
531	Cyber Defense Incident Responder	Advanced

Learning Objectives

✓ Use Elastic as a SIEM to analyze incidents and detect/respond to breaches in compromised Windows environments.

✓ Perform memory forensics on Windows systems to uncover hidden threats and identify adversarial activity.

✓ Interpret ETW data to accurately detect adversarial actions during security incidents.

✓ Use Splunk as a SIEM to identify and respond to breaches in compromised Windows environments.

✓ Analyze adversarial behavior across the cyber kill chain, providing detailed insight into complex attack vectors.

✓ Conduct endpoint forensics on Windows systems to identify specific adversarial actions through hands-on techniques.

✓ Analyze logs and forensic data to detect breaches and determine the root cause of incidents.

✓ Correlate and pivot across multiple data sources to uncover adversarial activity with advanced analytical skills.

✓ Apply YARA-based memory forensics on Windows systems to reveal hidden or latent threats using advanced techniques.

VALID FOR **3** YEARS TERM

EARN **131** CPEs

AVAILABLE VIA

ITES-SW2	NASA SEWP V	GSA MAS
W52P1J-20-D-0042	NNG15SC03B/NNG15SC27B	47QSWA18D008F

HACKTHEBOX

Coursework & Requirements

To successfully earn the HTB Defense Operations Analyst certificate, participants must:

- Complete all coursework (including completing all module content, completing all learning activities such as Sherlocks and challenges)
- Pass the final exam.

15 Modules · 11 Labs · 1 Final Exam

Academy Module	Intro to Network Traffic Analysis
Academy Module	Intermediate Network Traffic Analysis
Academy Module	Working with IDS/IPS
Dedicated Lab	Meerkat
Dedicated Lab	Superset-D
Dedicated Lab	Knock Knock
Academy Module	Security Monitoring & SIEM Fundamentals
Academy Module	Incident Handling Process
Academy Module	Introduction to Threat Hunting & Hunting with Elastic
Academy Module	Understanding Log Sources & Investigating with Splunk
Dedicated Lab	Nubilum2
Academy Module	Windows Event Logs & Finding Evil
Dedicated Lab	Horsepanda-D
Academy Module	Detecting Windows Attacks with Splunk
Academy Module	Windows Attacks & Defense
Academy Module	Introduction to Malware Analysis
Dedicated Lab	Einladen
Dedicated Lab	Logjammer
Academy Module	Introduction to Digital Forensics
Dedicated Lab	Jingle Bell
Dedicated Lab	BFT
Dedicated Lab	Event Horizon
Dedicated Lab	RogueOne
Academy Module	YARA & Sigma for SOC Analysts
Academy Module	Javascript Deobfuscation
Academy Module	Security Incident Reporting
Final Exam	