CROWDSTRIKE UNIVERSITY

CROWDSTRIKE

CROWDSTRIKE LEARNING PATHS

Take full advantage of all that the CrowdStrike Falcon platform has to offer with CrowdStrike University training and certification

THREAT HUNTER

CROWDSTRIKE CERTIFIED FALCON HUNTERS INVESTIGATE THREATS AND SECURITY INCIDENTS BY ANALYZING DIGITAL EVIDENCE, INCLUDING:

- UNDERSTANDING ALL ASPECTS OF DETECTION INVESTIGATION
- NAVIGATING AMONG AND USING MULTIPLE VIEWS IN THE FALCON CONSOLE TO PERFORM AUTOMATED QUERIES SUCH AS IP AND DOMAIN SEARCHES AND TIME-LINING USING SPLUNK EVENT SEARCHING
- UNDERSTANDING EVENT DATA STRUCTURE AND RELATIONSHIPS
- CONDUCTING SIMPLE AND INTERMEDIATE SEARCH QUERIES USING SPLUNK SEARCH PROCESSING LANGUAGE (SPL)

WORK ROLE COMPETENCIES:

- ATTACK FRAMEWORKS
- DETECTION ANALYSIS
- SEARCH TOOLS
- EVENT SEARCH
- REPORTS
- HUNTING ANALYTICS
- HUNTING METHODOLOGY
- DOCUMENTATION

CROWDSTRIKE UNIVERSITY
LOG IN

CROWDSTRIKE UNIVERSITY ORIENTATION

FHT 100: FALCON PLATFORM ARCHITECTURE OVERVIEW

FHT 101: FALCON PLATFORM TECHNICAL FUNDAMENTALS

FHT 109: USING MITRE ATT&CK AND FALCON DETECTION METHODS TO UNDERSTAND SECURITY RISK

FHT 106: FALCON CUSTOMIZABLE DASHBOARDS

FHT 104: GETTING STARTED WITH THE ENDPOINT SECURITY MODULE

MONTH 1

FHT 120: INVESTIGATION FUNDAMENTALS

FHT 121: SPOTLIGHT APP FUNDAMENTALS

FHT 130: CROWDSTRIKE FALCON INTELLIGENCE FUNDAMENTALS

MONTH 2

FHT 202: INVESTIGATING AND QUERYING EVENT DATA WITH FALCON EDR

FHT 201: FALCON PLATFORM FOR RESPONDERS

FHT 150: INCIDENTS FUNDAMENTALS

CCFH EXAM GUIDE

DOWNLOAD

MONTH 3

FHT 302: ADVANCED THREAT HUNTING WITH FALCON

MONTH 6

TAKE THE CCFH EXAM AT PEARSON VUE

SCHEDULE NOW

EARN YOUR WINGS

AND RECEIVE YOUR DIGITAL BADGE

CROWDSTRIKE UNIVERSITY

© 2023 CrowdStrike, Inc. All rights reserved.