



CROWDSTRIKE LEARNING PATHS

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

[CSU HOME](#) | [FALCON CERTIFICATION](#) | [TRAINING CATALOG](#) | [CERTIFICATION GUIDE](#) | [SCHEDULE EXAM](#)

INCIDENT RESPONDER



CROWDSTRIKE CERTIFIED FALCON INCIDENT RESPONDERS INVESTIGATE, ANALYZE AND RESPOND TO INCIDENTS, INCLUDING:

- CONDUCTING INITIAL TRIAGE OF DETECTIONS IN THE FALCON CONSOLE
- MANAGING FILTERING, GROUPING, ASSIGNMENT, COMMENTING AND STATUS CHANGES OF DETECTIONS
- PERFORMING BASIC INVESTIGATION TASKS SUCH AS HOST SEARCH, HOST TIMELINE, PROCESS TIMELINE, USER SEARCH AND OTHER CLICK-DRIVEN WORKFLOWS
- CONDUCTING BASIC PROACTIVE HUNTING FOR ATOMIC INDICATORS SUCH AS DOMAIN NAMES, IP ADDRESSES AND HASH VALUES ACROSS ENTERPRISE EVENT DATA

WORK ROLE COMPETENCIES:

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

CROWDSTRIKE UNIVERSITY

LOG IN



CROWDSTRIKE UNIVERSITY ORIENTATION

FHT 100: FALCON PLATFORM ARCHITECTURE OVERVIEW

FHT 101: FALCON PLATFORM TECHNICAL FUNDAMENTALS

FHT 114: FALCON FUSION FUNDAMENTALS

FHT 106: FALCON CUSTOMIZABLE DASHBOARDS

FHT 104: GETTING STARTED WITH THE ENDPOINT SECURITY MODULE

MONTH 1

FHT 120: INVESTIGATION FUNDAMENTALS

FHT 150: INCIDENTS FUNDAMENTALS

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

FHT 202: INVESTIGATING AND QUERYING EVENT DATA WITH FALCON EDR

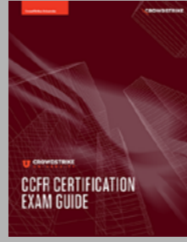
FHT 201: FALCON PLATFORM FOR RESPONDERS

FHT 140: REAL TIME RESPONSE FUNDAMENTALS

MONTH 2

FHT 240: INVESTIGATING AND MITIGATING THREATS WITH REAL TIME RESPONSE

CCFR EXAM GUIDE



DOWNLOAD

MONTH 3

CROWDSTRIKE CERTIFIED FALCON RESPONDER: PRACTICE EXAM

MONTH 6

TAKE THE CCFR EXAM AT PEARSON VUE

SCHEDULE NOW



EARN YOUR WINGS



AND RECEIVE YOUR DIGITAL BADGE

