

CrowdStrike

Threat Intelligence and Hunting

Products and Services

Feature Categories	Key Features	Falcon Adversary OverWatch	Falcon Adversary OverWatch Identity ¹	Falcon Adversary OverWatch Cloud	Falcon Adversary Intelligence	Falcon Adversary Intelligence Premium	Falcon Counter Adversary Operations Elite ²
Threat Hunting	24/7 Managed Threat Hunting	✓	✓	✓			
	- Falcon Insight XDR	✓					
	- Falcon Identity Protection		✓				
	- Falcon Cloud Security			✓			
Threat Intelligence	Adversary Cards	✓					
	In-Depth Adversary Profiles				✓	✓	
	Weekly Threat Summaries				✓	✓	
	Threat Landscape Dashboards				✓	✓	
	Intelligence Reports					✓	
	Quarterly Threat Briefs					✓	
	Threat Hunting Libraries					✓	
	Requests for Information (5 Pack)					Ability to add	✓
	Priority Intelligence Requirements						✓
	Threat Graph Queries (Up to 50)						✓
Digital Risk Protection	Dark Web Monitoring				✓	✓	
	Brand and Domain Monitoring				✓	✓	
	Credential Monitoring		✓		✓	✓	
	Dark Web Activity Reports				✓	✓	
Automation and Tools	Malware Sandbox	✓			✓	✓	
	Indicator of Compromise App	✓			✓	✓	
	Vulnerability Intelligence App	✓			✓	✓	
	QuickScan Pro Analysis				1,000/month	2,500/month	
	Threat Feed (IOCs)				✓	✓	
	APIs and Integrations				✓	✓	
	Human Malware Analysis (50 per Year)					✓	
	Pre-Built Detection Rules (YARA, Snort)					✓	
Assigned Analyst	Analyst Access via Email, SMS and Phone						✓
	Customer-Directed Threat Hunts						✓
	Threat Hunt Query Optimization						✓
	External Digital Risk Investigations						✓
	Tailored Threat Briefings and Risk Reports						✓

¹ Falcon Adversary OverWatch or Falcon Adversary OverWatch Cloud is a prerequisite for Falcon Adversary OverWatch Identity.

² Falcon Adversary Intelligence Premium is a prerequisite for Falcon Counter Adversary Operations Elite.