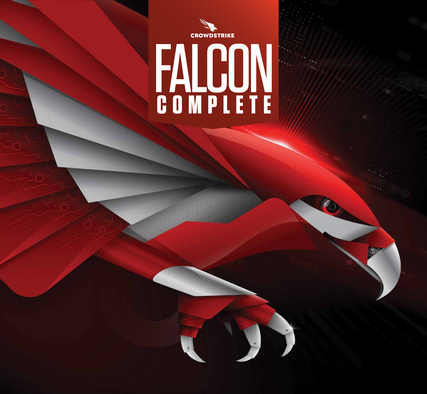

FALCON COMPLETE IN ACTION

Defending against today's threats demands constant vigilance by skilled analysts.

CrowdStrike® Falcon Complete™ is a turnkey managed detection and response (MDR) service that delivers expert investigation and surgical response 24/7/365.

See the difference Falcon Complete can make for you.

BEST-EFFORT INCIDENT RESPONSE	ADVERSARY ACTIVITY Time Elapsed (HR:MIN)	FALCON COMPLETE EXPERT INCIDENT RESPONSE
	0:00 Adversary obtains credentials via **phishing**	
Malware is blocked by local endpoint protection solution Low-criticality alert is generated, but ignored as non-critical	**0:02** Phish establishes connection to malicious domain and attempts to deploy second-stage **malware**	**Malware is blocked** by Falcon Prevent™ Low-criticality alert is generated
	0:30	Low-criticality **alert is investigated** by Falcon Complete team Falcon Complete team performs triage on blocked malware and identifies it as associated with a threat actor group known for ransomware targeting organizations in the finance sector Analyst verifies that policies are properly configured to reveal adversary activity that may be coming
	6:00 **Adversary logs in** to the system **via RDP** with valid user credentials	
	6:10 Adversary realizes that the initial implant failed, suspects that local endpoint protection is in place, engages in **stealth tactics** and uses native OS functionality to perform local reconnaissance	
Adversary identifies a new **development server that happens to be unprotected** by the local endpoint	**7:30**	Adversary is frustrated to find **no unprotected systems** and continues exploring, including downloading additional tooling
Adversary **pivots to the unprotected server** Server will need to be wiped and reimaged	**7:45**	Falcon Complete analyst identifies adversary activity and **begins investigation and response**
	7:55	Falcon Complete analyst network-isolates the affected system, and the **adversary is ejected**
Adversary downloads customized Mimikatz malware, dumps credentials and **obtains admin credentials** All global admin accounts need to be reset	**8:00**	Customer receives critical escalation to **reset the single affected user account**
Adversary **moves laterally** across the organization Investigation required to track adversary movement	**8:05**	Falcon Complete analyst **removes all tooling and remaining artifacts** left behind by the adversary
	8:30	Customer receives notification with details of the intrusion, including background details and recommendations for improving security posture to **eliminate risk of future similar intrusions**
Adversary **stages targeted malware** and deploys **persistence** mechanisms as it moves laterally across the organization Some activities are blocked, and others are logged as security alerts, but staff has gone home for the day	**18:45**	
Investigation required to track adversary movement Multiple additional hosts will need to be wiped and reimaged		
Security team identifies critical alerts and engages emergency response Team engaged in fire drill for days to come	**31:30**	

BEST EFFORT OUTCOME: COSTLY AND DISRUPTIVE RESPONSE

Hours of labor-intensive investigation

Cumbersome and expensive reimaging

Unsure of whether the adversary will be back

FALCON COMPLETE OUTCOME: FAST AND EFFECTIVE RESPONSE

Intrusion contained and remediated in minutes

Zero intervention by IT staff

Zero disruption to business processes or users

Confidence that the threat was handled completely and correctly