Adversary obtains credentials via phishing

Phish establishes connection to malicious domain and attempts to deploy second-stage malware.

Adversary identifies a new development server that happens to be unprotected by the local endpoint protection solution.

Malware is blocked by local endpoint protection solution.

Low-criticality alert is generated, but ignored as non-critical.

Adversary logs in to the system via RDP with valid user credentials.

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 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.

Adversary downloads customized Mimikatz malware, dumps credentials and obtains admin credentials.

Adversary moves laterally across the organization.

Security team identifies critical alerts and engages emergency 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.

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.