SEE LIVE IDENTITY ATTACK TRAFFIC
CrowdStrike Falcon Identity Threat Detection (ITD) provides visibility for identity-based attacks and anomalies, comparing live traffic against behavior baselines and rules to detect attacks and lateral movement. Real-time identity threat detection alerts on compromised credentials and infected machines within the network or cloud, or other unusual authentication traffic. Since most breaches involve compromised credentials and lateral movement, the best path for securing every domain in your environment is by automating threat detection and creating dynamic risk profiling and alerting on identity traffic.

FALCON IDENTITY THREAT DETECTION
Save log storage costs by storing only relevant authentication logs.

REAL-TIME TRAFFIC ALERTING
Detect anomalous activity without requiring logs. Falcon ITD offers threat detection, a low false positive rate and the ability to detect threats that are difficult to detect via post-event, log-based security tools.

HYBRID IDENTITY STORE-READY
Falcon ITD works for identity stores on-premises or in the cloud, and for users/applications anywhere without any agents on endpoints or servers outside the domain controllers.

KEY BENEFITS
- Discover all identities across the enterprise, including stale accounts, with password hygiene
- Verify identity store (e.g., Active Directory, LDAP/S) security to discover weakness across multiple domains
- Investigate authentication events and questionable user behavior
- Group events around user, device, activity and more for improved incident response
- Gain unified visibility for authentication traffic to applications, resources and identity stores
- Reduce mean time to detect and respond, and improve SOC analysts’ efficiency and response times by cutting down on the need to do complex, error-prone log analysis
- Improve alert fidelity and reduce noise by recognizing true positive events of interest
KEY PRODUCT CAPABILITIES

Discover all identities — even stale accounts — and detect identity threats in real time.

EXTENDED PROTOCOL COVERAGE

Falcon ITD provides granular visibility over incidents involving protocols like NTLM, Kerberos and LDAP/S, which are impossible or difficult to detect with traditional tools like next-generation firewalls, and user and entity behavior analytics (UEBA).

SPEED TO VALUE

Most installations take less than an hour to see all identities on the network and start identifying anomalies immediately.

BEHAVIOR-BASED INDICATORS AND PROFILING

Falcon ITD profiles are based on both static information from identity stores and dynamic information in real time to catch insider threats, lateral movement and privilege or service account abuse. Eliminate risk guesswork and prioritize authentication tasks based on 100+ behavior analytics and risk scores for every account.

VISIBILITY INTO IDENTITY STORE ATTACKS

Detect identity store threats (and typical red-team exercise tests) like NTLM/LDAPS protocol threats, Golden Ticket attacks, Pass-the-Hash and other credential theft, as well as persistence techniques.

TOOLS FOR INCIDENT RESPONSE

Falcon ITD’s internal Threat Hunter feature offers visibility for all credential attacks and incident response, showing the chain of activity and subsequent increase in risk score. Threat Hunter is easy to use — no command-line interface or sophisticated security knowledge is required to operate and administer. It integrates with many popular ticketing platforms.

DEEP INTEGRATION WITH OTHER SECURITY TOOLS

Falcon ITD can export in common event format (CEF) or Log Event Extended Format (LEEF) to any SIEM or to SOAR tools via API.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform’s single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world’s most advanced data platforms for security.