IDENTITY DAYS
webinars

CROWDSTRIKE

BLOCAGE DES MENACES MODERNES : VERS UNE CONVERGENCE NÉCESSAIRE DE LA SÉCURITÉ DES IDENTITÉS ET DES ENDPOINTS

ANNE-SOPHIE GOELDNER : IDENTITY SALES SPECIALIST
EMAIL : ANNE-SOPHIE.GOELDNER@CROWDSTRIKE.COM

MATTHIEU MASSON : IDENTITY TECHNICAL EXPERT

KEY NUMBERS FROM EXTERNAL SOURCES

- 71% increase in attacks involving fraudulent use of valid accounts globally (66% increase in Europe)
- Abuse of valid accounts represents the most common entry point (30% of initial access)
- 100% increase in kerberoasting attacks in 2023
- Detection and response time for breaches caused by stolen or compromised credentials is approximately 11 months (longest response lifecycle among all infection vectors).

Source : IBM X-Force 2024 Report

CROWDSTRIKE

TOP ADVERSARY TECHNIQUES

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Valid Accounts	Command and Scripting	Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping	System Owner/ User Discovery	Valid Accounts	Archive Collected Data	Ingress Tool Transfer	Exfiltration Over Alternative Protocol	Service Stop

CROWDSTRIKE

ENDPOINT PROTECTION COVERAGE TRADECRAFT

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	✓ Command and Scripting				✓ OS Credential Dumping	✓ System Owner/ User Discovery		✓ Archive Collected Data	✓ Ingress Tool Transfer	✓ Exfiltration Over Alternative Protocol	✓ Service Stop

CROWDSTRIKE

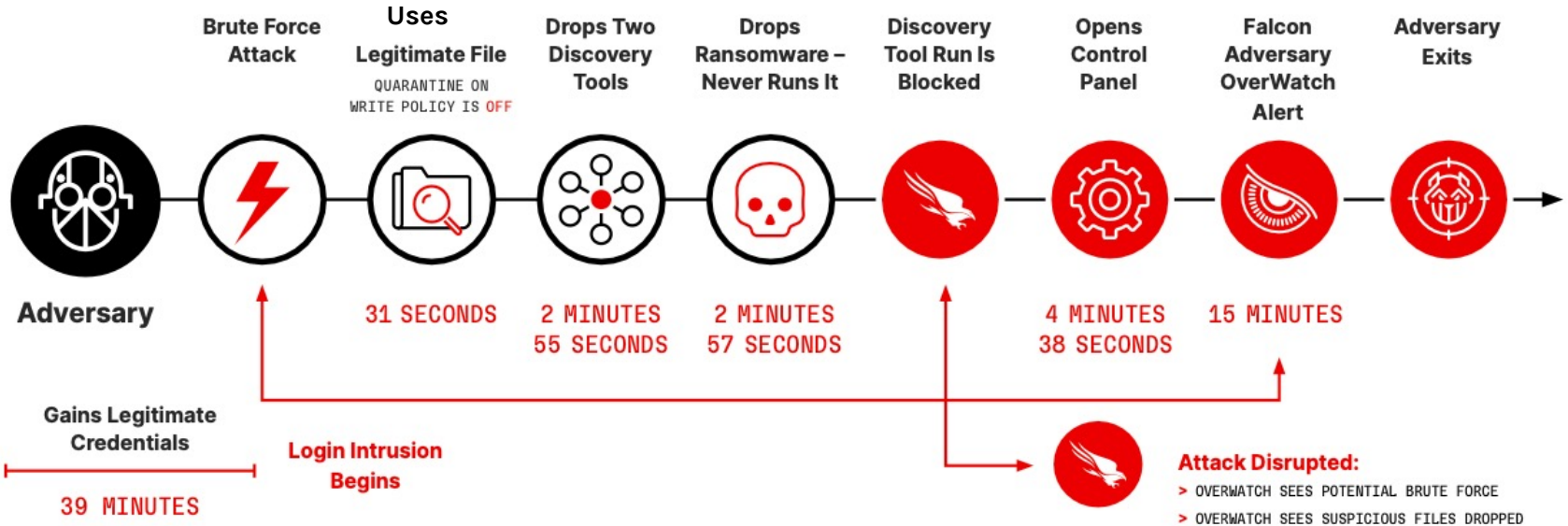
BETTER TOGETHER ENDPOINT + IDENTITY

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Valid Accounts	Command and Scripting	Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping	System Owner/ User Discovery	Valid Accounts	Archive Collected Data	Ingress Tool Transfer	Exfiltration Over Alternative Protocol	Service Stop

Endpoint coverage Identity coverage

CROWDSTRIKE

Identity Is the Critical Battleground



Identity Is the Critical Battleground

88%

CROWDSTRIKE

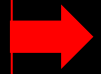
Identity Is the Critical Battleground

88% Of the time the adversary remained **SILENT**.

CLOSING THE GAP BETWEEN IDENTITY AND SOC

CLOSING THE GAP BETWEEN IDENTITY AND SOC

Identity Threats :
Password spray
Brute force
Credential scanning
SAML golden ticket
Pass-the-hash
Unusual user activity
Privilege escalation
Lateral movement
Others …



Identity infrastructure

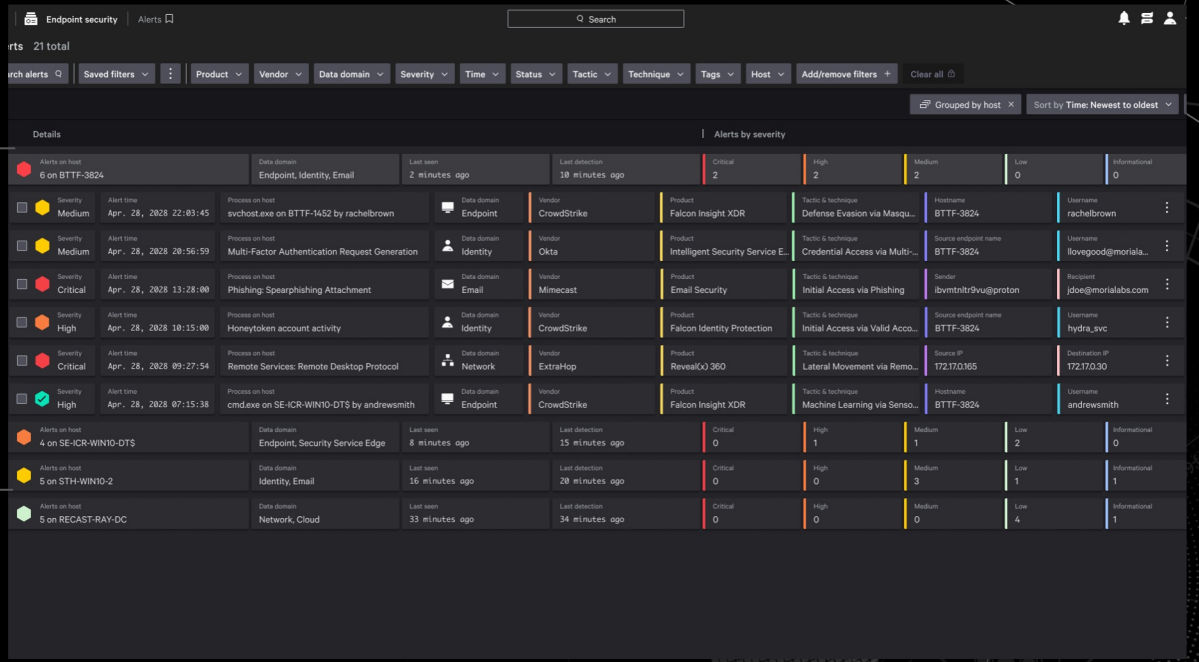
AD / ENTRA ID
SSO
MFA
PAM
IGA
…

Infrastructure Security and Operations (SOC) : EDR, XDR, SIEM, SOAR…

Identity Threat Detection & Response

ITDR is a discipline that requires coordination between SOC and IAM team and contributes to a unified approach

Unified Approach
Reduce time to detect



Single View for All Detections

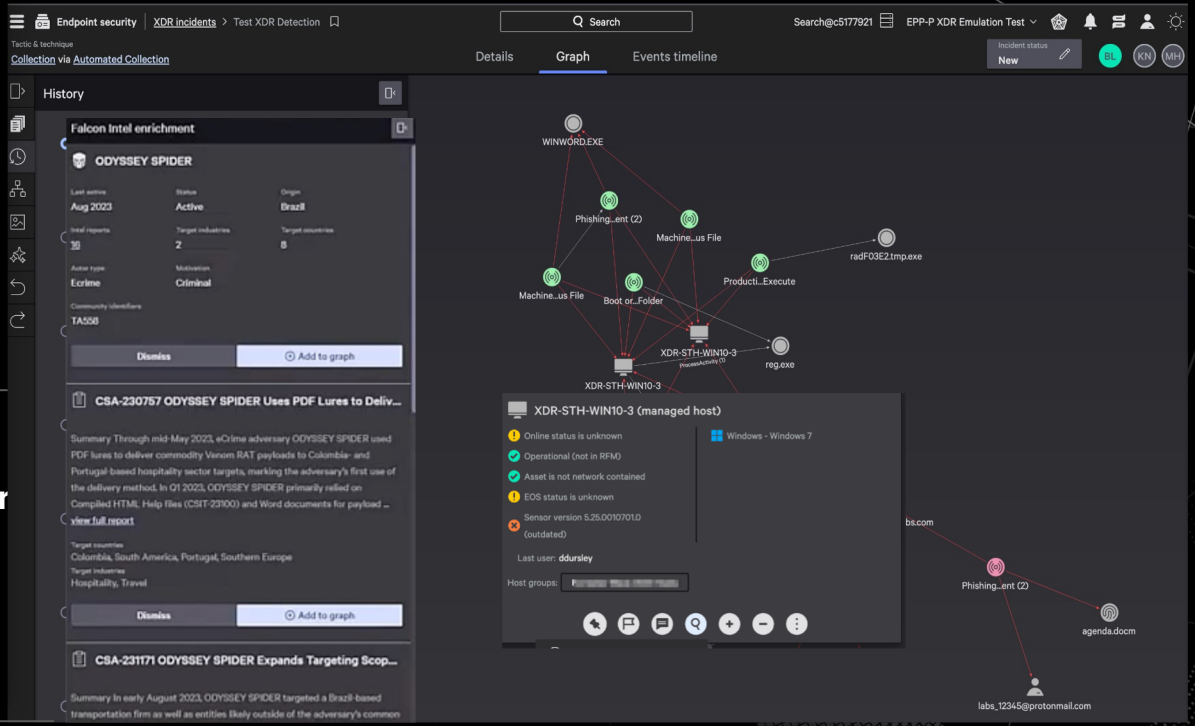
One screen to view all Falcon-originated alerts alongside third-party alerts

This slide contains forward-looking statements including, but not limited to, statements concerning the expected timing of product and feature availability, the benefits and capabilities of our current and future products and plans and objectives. Such statements are subject to numerous risks and uncertainties and actual results could differ from those statements. Any future products, functionality and services may be abandoned or delayed, and customers should make decisions to purchase products and services based on features that are currently available.

Unified Approach
Drive more efficient investigations

Centralize Investigations
Interactive graph view to support hunting and investigation workflows without having to leave the console

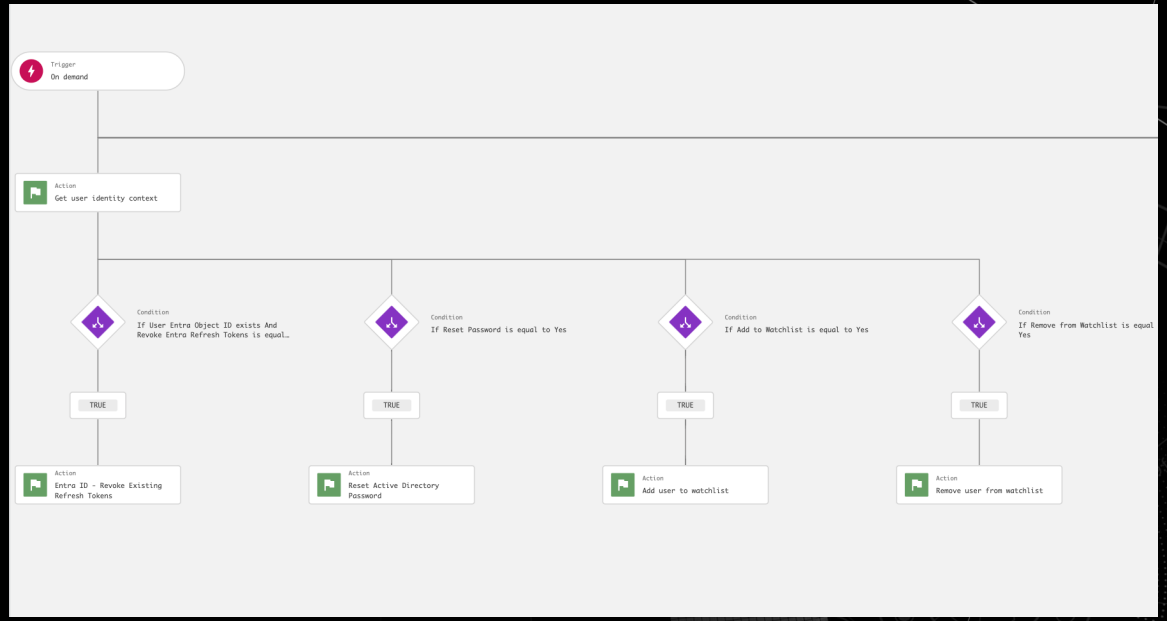
Collaborative Command Center
Supports multi-user collaboration and the ability to add annotations, notes, inputs to entities or incidents



Unified Approach

Reduce time to contain and remediate

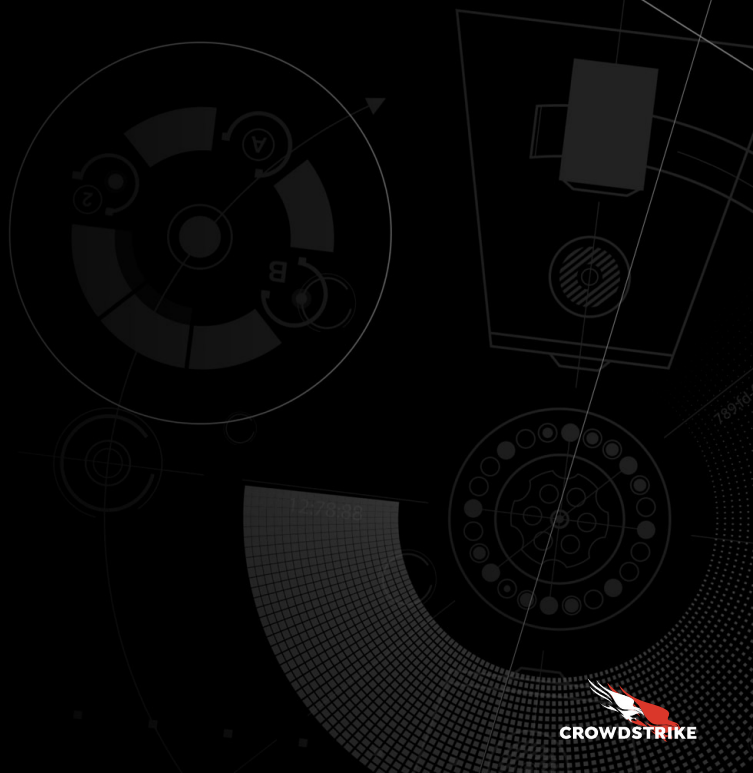
Enrichment and Remediation
Built-in automated enrichment and remediation options to run workflows and playbooks



This slide contains forward-looking statements including, but not limited to, statements concerning the expected timing of product and feature availability, the benefits and capabilities of our current and future products and plans and objectives. Such statements are subject to numerous risks and uncertainties and actual results could differ from those statements. Any future products, functionality and services may be abandoned or delayed, and customers should make decisions to purchase products and services based on features that are currently available.

CROWDSTRIKE

DEMO



CROWDSTRIKE