



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).



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

















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



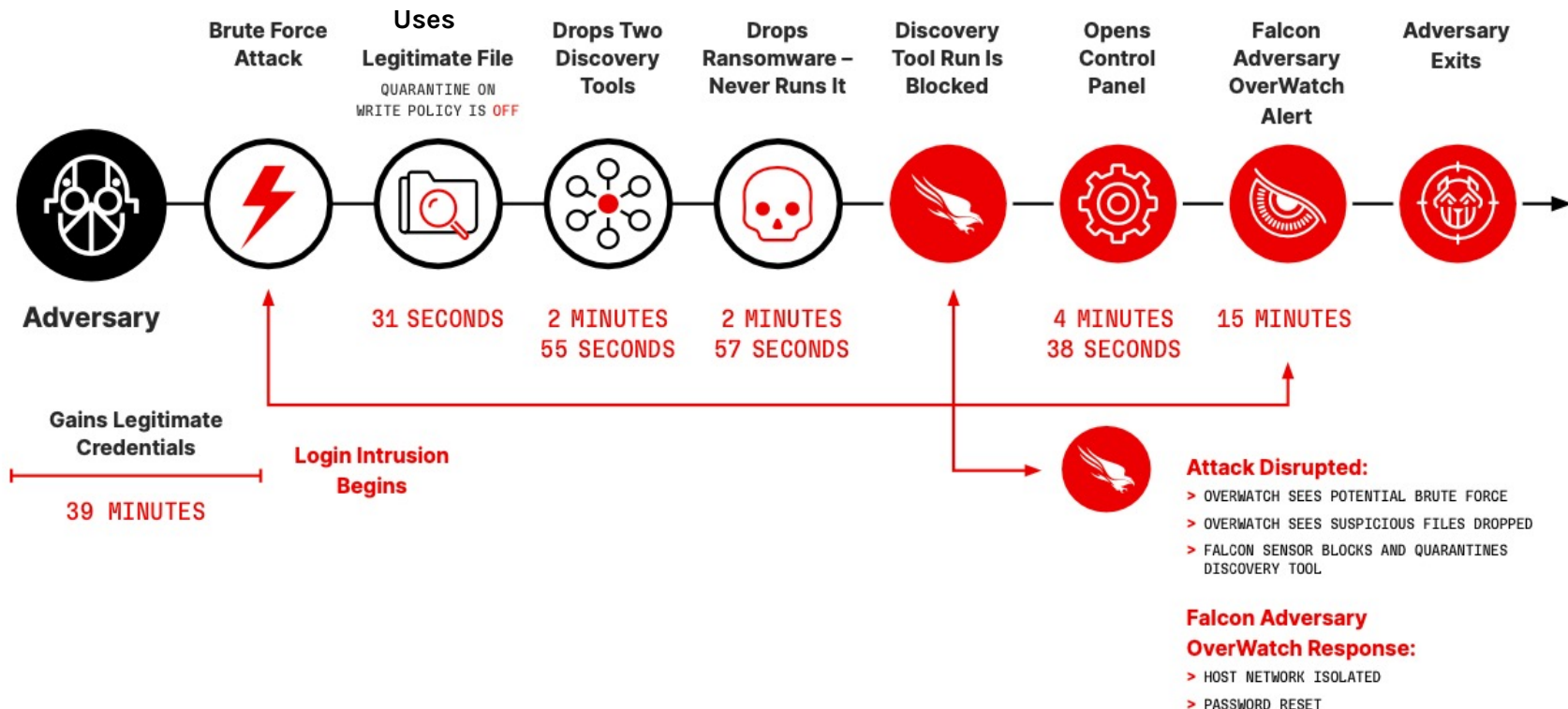
BETTER TOGETHER ENDPOINT + IDENTITY

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

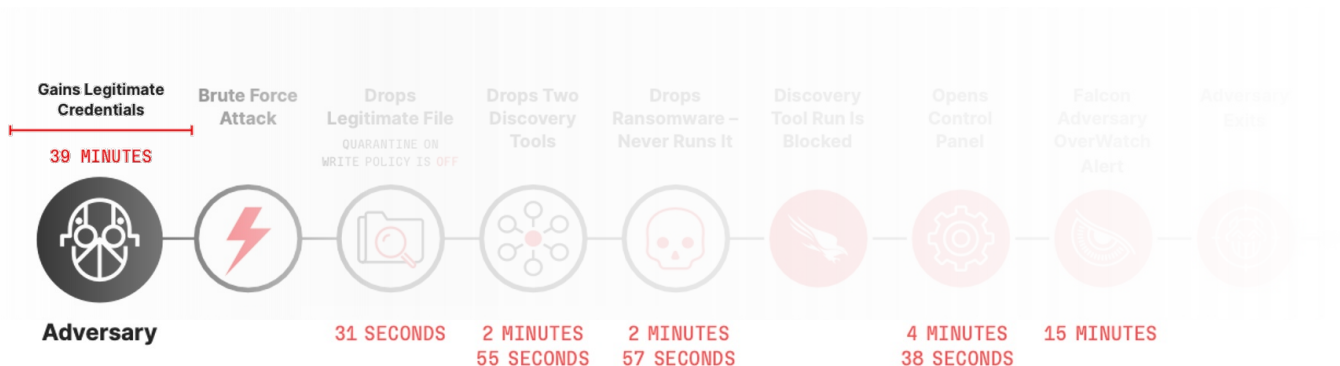


Identity Is the **Critical** Battleground



Identity Is the **Critical** Battleground

88%



Identity Is the **Critical** Battleground

88%

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

Gains Legitimate
Credentials



39 MINUTES

CLOSING THE GAP BETWEEN IDENTITY AND SOC

Identity infrastructure

AD / ENTRA ID
SSO
MFA
IAM
PAM
IGA
...

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

?

Attackers exploit this gap !



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

Endpoint security Alerts

Alerts 21 total

Search

Arch alerts Saved filters Product Vendor Data domain Severity Time Status Tactic Technique Tags Host Add/remove filters Clear all

Grouped by host Sort by Time: Newest to oldest

Alerts on host		Data domain	Last seen	Last detection	Critical	High	Medium	Low	Informational
6 on BTTF-3824		Endpoint, Identity, Email	2 minutes ago	10 minutes ago	2	2	2	0	0
Severity: Medium	Alert time: Apr. 28, 2028 22:03:45	Process on host: svchost.exe on BTTF-1452 by rachelbrown	Data domain: Endpoint	Vendor: CrowdStrike	Product: Falcon Insight XDR	Tactic & technique: Defense Evasion via Masqu...	Hostname: BTTF-3824	Username: rachelbrown	
Severity: Medium	Alert time: Apr. 28, 2028 20:56:59	Process on host: Multi-Factor Authentication Request Generation	Data domain: Identity	Vendor: Okta	Product: Intelligent Security Service E...	Tactic & technique: Credential Access via Multi...	Source endpoint name: BTTF-3824	Username: ilovegood@morla...	
Severity: Critical	Alert time: Apr. 28, 2028 13:28:00	Process on host: Phishing: Spearphishing Attachment	Data domain: Email	Vendor: Mimecast	Product: Email Security	Tactic & technique: Initial Access via Phishing	Sender: ilvmtlntr9va@proton	Recipient: jdoe@morialisba.com	
Severity: High	Alert time: Apr. 28, 2028 10:15:00	Process on host: Honeytoken account activity	Data domain: Identity	Vendor: CrowdStrike	Product: Falcon Identity Protection	Tactic & technique: Initial Access via Valid Acco...	Source endpoint name: BTTF-3824	Username: hydra_svc	
Severity: Critical	Alert time: Apr. 28, 2028 09:27:54	Process on host: Remote Services: Remote Desktop Protocol	Data domain: Network	Vendor: ExtraHop	Product: Reveal(x) 360	Tactic & technique: Lateral Movement via Remo...	Source IP: 172.17.0.165	Destination IP: 172.17.0.30	
Severity: High	Alert time: Apr. 28, 2028 07:15:38	Process on host: cmd.exe on SE-ICR-WIN10-DTS by andrewsmith	Data domain: Endpoint	Vendor: CrowdStrike	Product: Falcon Insight XDR	Tactic & technique: Machine Learning via Senso...	Hostname: BTTF-3824	Username: andrewsmith	
Alerts on host: 4 on SE-ICR-WIN10-DTS		Data domain: Endpoint, Security Service Edge	Last seen: 8 minutes ago	Last detection: 15 minutes ago	Critical: 0	High: 1	Medium: 1	Low: 2	Informational: 0
Alerts on host: 6 on STH-WIN10-2		Data domain: Identity, Email	Last seen: 16 minutes ago	Last detection: 20 minutes ago	Critical: 0	High: 0	Medium: 3	Low: 1	Informational: 1
Alerts on host: 5 on RECAST-RAY-DC		Data domain: Network, Cloud	Last seen: 33 minutes ago	Last detection: 34 minutes ago	Critical: 0	High: 0	Medium: 0	Low: 4	Informational: 1



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



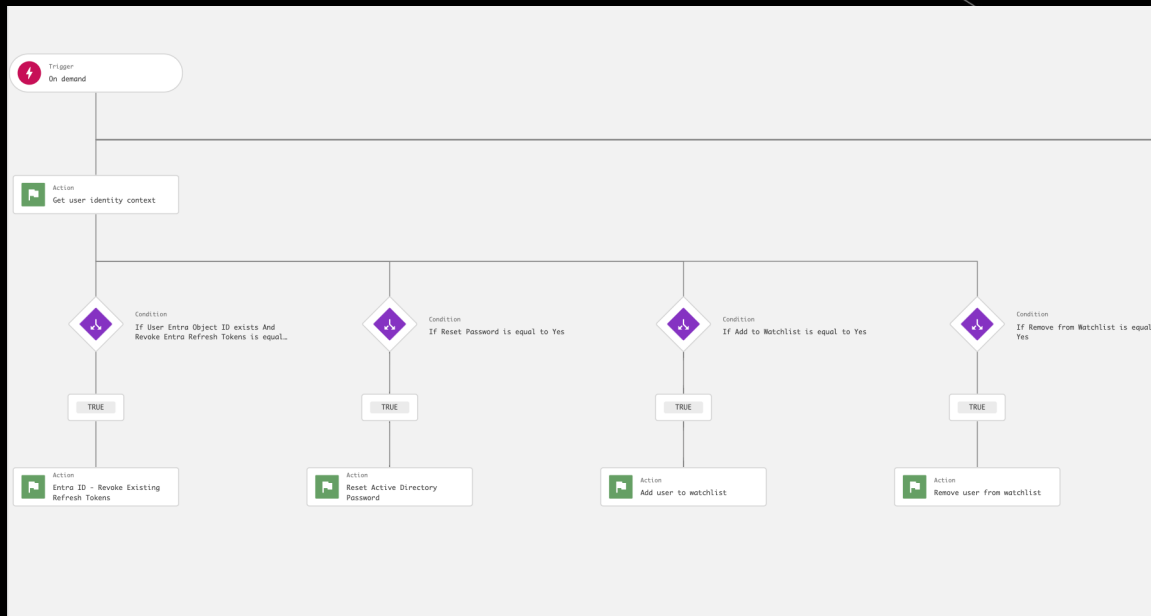
Unified Approach

Reduce time to contain and remediate



Enrichment and Remediation

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





DEMO

