크라우드스트라이크 차세대 백신

CROWDSTRIKE FALCON PREVENT

부성현 기술이사 / GREM CISSP CISA

CROWDSTRIKE KOREA

WE STOP BREACHES

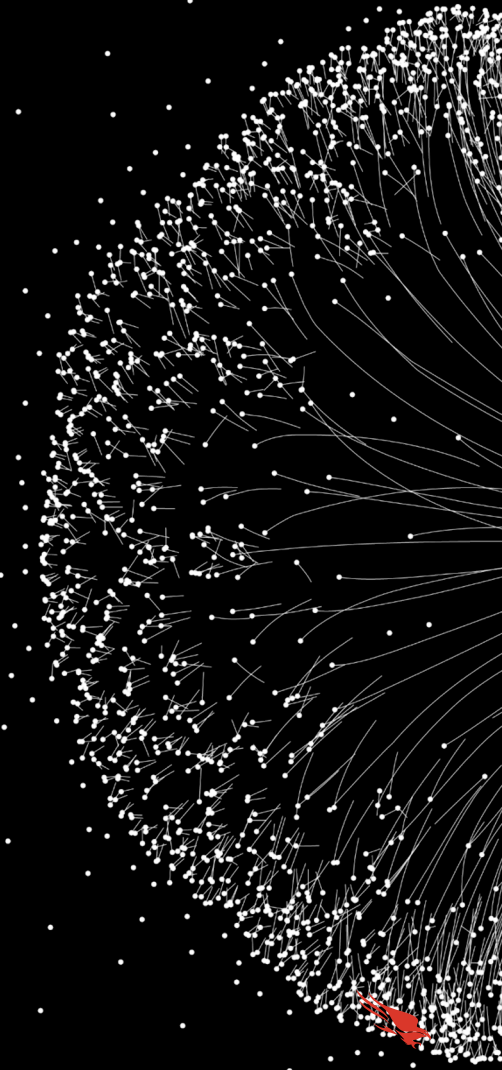
CROWDSTRIKE

THREAT GRAPH
자동화 헌팅 엔진 HUNTING ENGINE

135 MILLION
IOA DECISIONS/MIN

7 TRILLION
EVENTS/WEEK

170+
ADVERSARIES TRACKED



CROWDSTRIKE

THREAT GRAPH

자동화 헌팅 엔진 HUNTING ENGINE

135 MILLION
IOA DECISIONS/MIN

7 TRILLION
EVENTS/WEEK

170+
ADVERSARIES TRACKED

ENRICHED DATA

ACTIONABLE INSIGHTS

ANALYZED DATA

90,000

POTENTIAL BREACHES STOPPED

CROWDSTRIKE

SINGLE LIGHTWEIGHT AGENT

단일 경량화 센서 ML BASED NEXT GEN

- 알려지거나 알려지지 않은 공격 방어
- 0 days 취약점 방어
- AI/ML 차세대 엔진
- IOA 행위 기반 탐지/대응
- 오프라인 엔드포인트 보호
- NO SIG / NO SCAN
- High Performance

THE POWER
OF ONE

SINGLE LIGHTWEIGHT AGENT
단일 경량화 센서 ML BASED NEXT GEN

차별화된 차세대 백신

- 하루에도 여러 번 업데이트가 되는 레거시 백신과는 다르게 차세대 백신은 시그니쳐 없이 머신러닝 알고리즘으로 탐지하기 때문에 업데이트 스톰이 없음
- 최신 업데이트가 되어야 최상의 탐지율을 제공하는 레거시 백신과는 다르게 차세대 백신은 일관된 최상의 탐지율을 제공

A PROVEN SECURITY LEADER
엔드포인트 프로텍션 부문 글로벌 리더

Gartner® Magic Quadrant™ for
Endpoint Protection Platforms, May 2021

Gartner peerinsights customers' choice 2021™

Endpoint Protection Platforms

Gartner peerinsights customers' choice 2020™

Endpoint Detection and Response Solutions

Gartner Magic Quadrant for Endpoint Protection Platforms,Paul Webber, Peter Firstbrook, Rob Smith, Mark Harris, Prateek Bhajanka,5th May 2021
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Crowdstrike. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The GARTNER PEER INSIGHTS Logo is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences and do not represent the views of Gartner or its affiliates.. https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms and https://www.gartner.com/reviews/customers-choice/endpoint-detection-and-response-solutions

CROWDSTRIKE

A PROVEN SECURITY LEADER
엔드포인트 프로텍션 부문 글로벌 리더

Leader In

Gartner • FORRESTER® • IDC

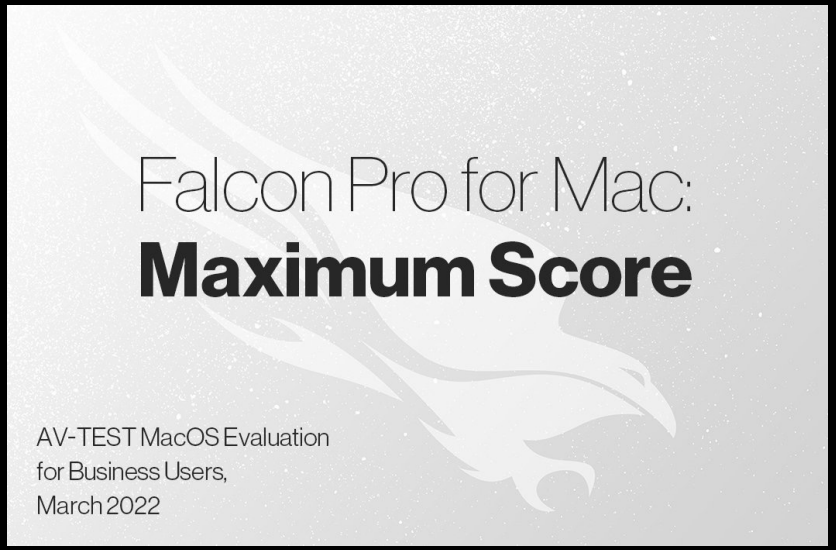
Validated

MITRE • AV comparatives • SE Labs

Compliance & Certifications

Privacy Shield Framework · FedRAMP · PCI · aws competency · amtso · FIEC · Cyber Essentials Certified · CCN · STAR Level Two · CREST

A PROVEN SECURITY LEADER
2022 AV-TEST MACOS 평가에서 최고 점수 달성



CrowdStrike는 2022년 3월 기업 사용자를 위한 AV-TEST MacOS **평가**에 참여한 벤더 중 오탐율 제로와 더불어 보호, 성능 및 사용성에서 **가장 높은 점수**를 얻은 **유일한 벤더**

CROWDSTRIKE

NEXT-GEN AV
FALCON PREVENT

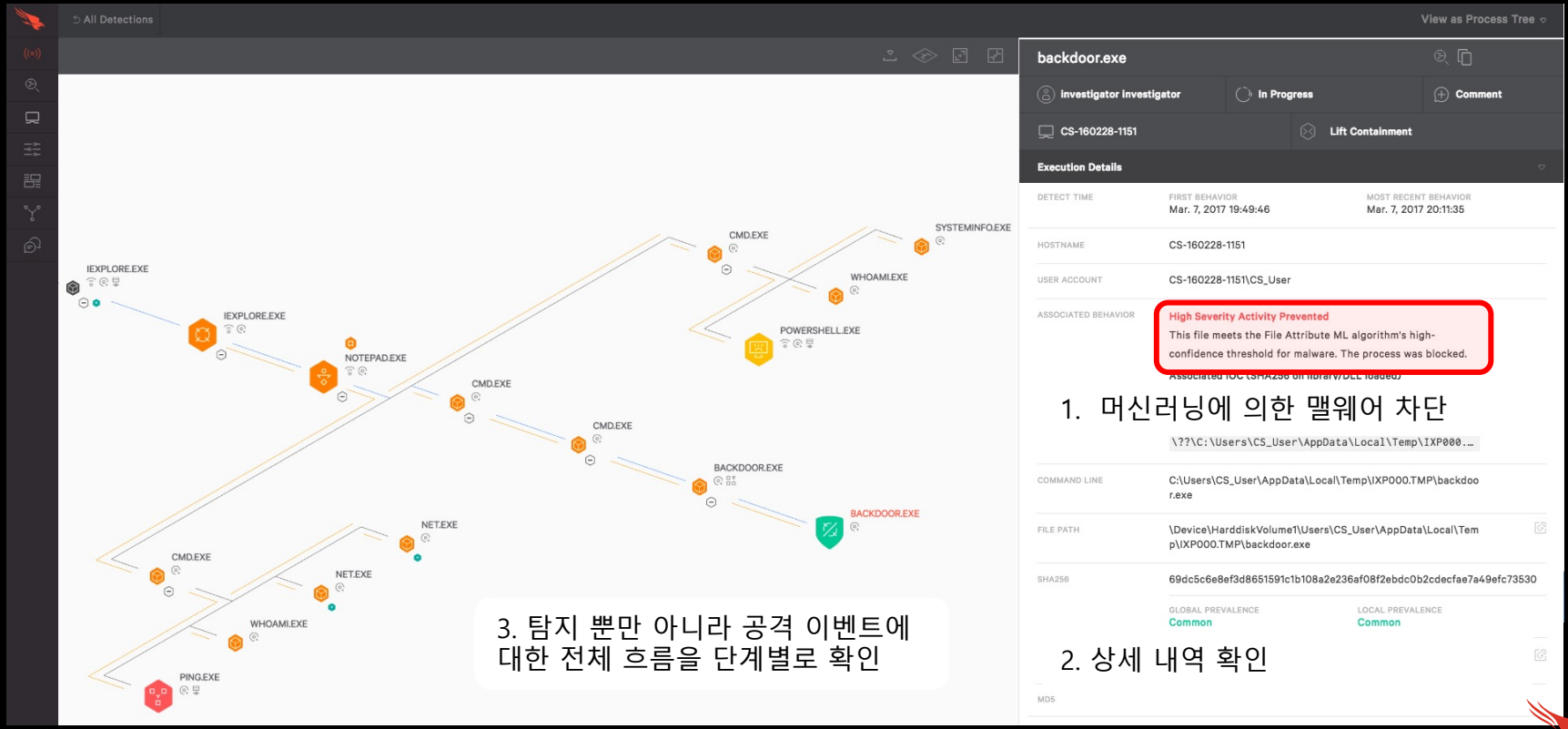
AV comparatives APPROVED Business Security DEC 2019

CROWDSTRIKE FALCON
CERTIFIED AS LEGACY
AV REPLACEMENT

제공되는 가치

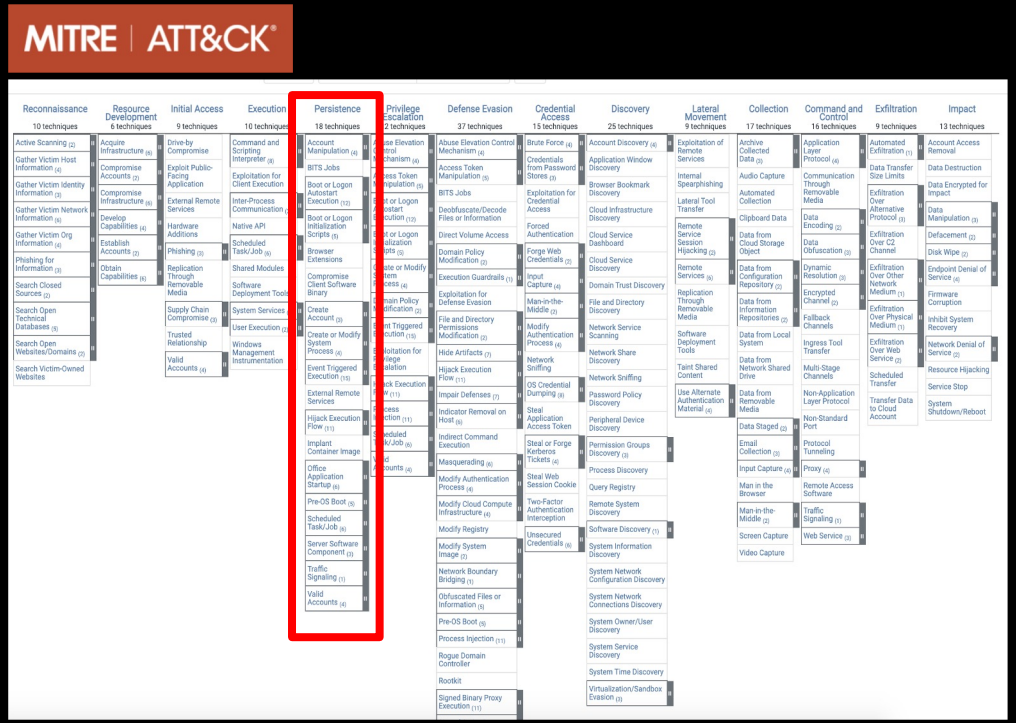
- 더 나은 보호기능 제공
- 침해사고 감소
- 사용자 생산성 향상
- 복잡성 제거
- 보안 효율성 제공

FALCON PREVENT Malware 대응



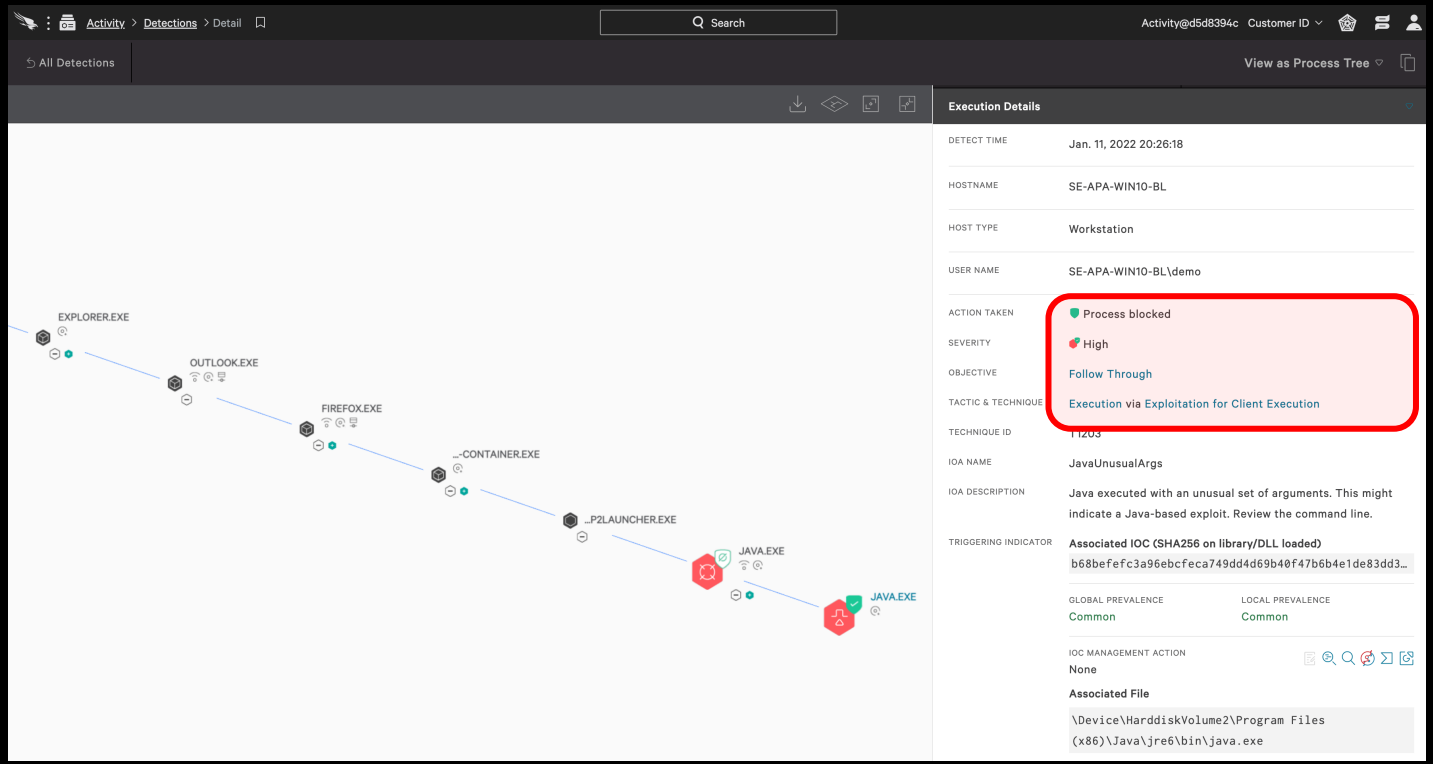
FALCON PREVENT File Less Attack 대응

SEVERITY	High
OBJECTIVE	Keep Access
TACTIC & TECHNIQUE	Persistence via Accessibility Features
TECHNIQUE ID	T1546.008
IOA NAME	RegWriteMagnifyBypass
IOA DESCRIPTION	A registry key was set to replace the magnify accessibility tool, which is often done by attackers to bypass the login screen.



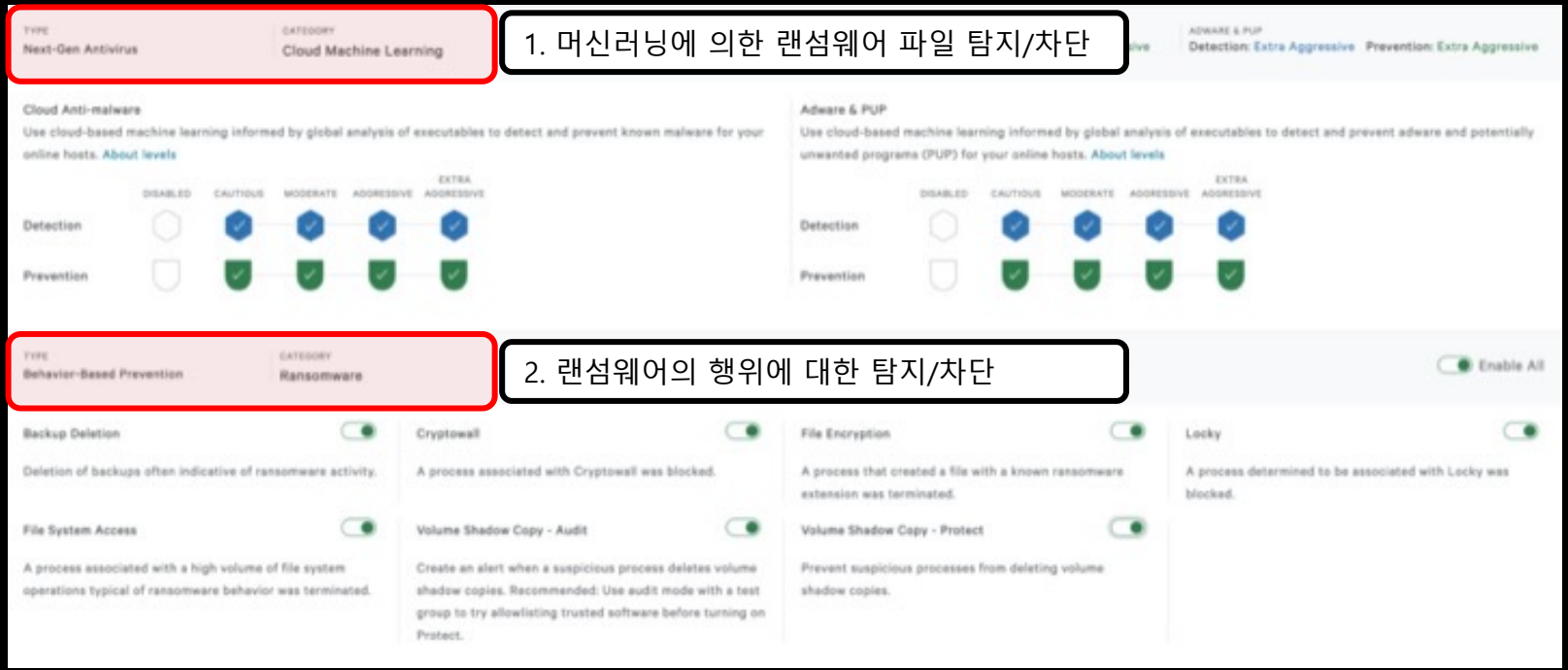
- 이상 행위 탐지(IOA)엔진 / File-less attack detect
- 탐지 시 보다 세분화된 Tactic/Technique 정보 제공
- MITRE ATT&CK TID / CrowdStrike TID로 구성
- Falcon 콘솔 또는 API를 통해 MITRE 데이터 수집 가능

FALCON PREVENT Exploit 대응



JAVA Exploit 탐지/차단

FALCON PREVENT Ransomware 대응



CROWDSTRIKE

FALCON PREVENT Threat Actor 대응 (APT, e-Crime)

Medium	3	Execution	28	Process Injection	23	Last	
Low	2	Credential Access	13	Command Line Interface	14	Last	
Informational	0	Post Exploit	13	Credential Dumping	13	Last	
+🔍		+🔍	7 more	+🔍	15 more	+🔍	

Select All | Update & Assign

High — TACTIC & TECHNIQUE: Machine Learning via Sensor-based ... — DETECT TIME: Aug. 6, 2020 10:48:18

STONE PANDA Detected

High +14 others — TACTIC & TECHNIQUE: Execution via Exploitation for Client ... — DETECT TIME: Aug. 6, 2020 10:44:33

VOLATILE KITTEN Detected

High +5 others — TACTIC & TECHNIQUE: Machine Learning via Cloud-based ML — DETECT TIME: Aug. 6, 2020 10:35:47

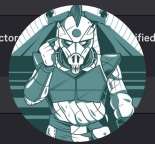
High — TACTIC & TECHNIQUE: Machine Learning via Sensor-based ... — DETECT TIME: Aug. 6, 2020 10:34:23

Customers

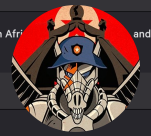
CrowdStrike Intelligence assesses with low confidence that GRACEFUL SPIDER likely operates internally.

Victims

GRACEFUL SPIDER has targeted companies in a variety of sector ...ified campaign ...zations in Afri... and Europe.


VELVET SIGINT


RICOCHET HUMINT


STARDUST HUMINT

Crimes

- Wire Fraud
- Accessing a computer without authorization for the purpose of commercial advantage and private financial gain
- Damaging a computer through the transmission of code and commands
- Conspiring to commit fraud and related activity in connection with computers
- Transmitting a demand in relation to damaging a protected computer

Monetization

- Ransom payments through cryptocurrency
- Extorting stolen data if ransom is not paid
- Monetary theft through wire fraud from victim accounts
- Likely selling payment card data via criminal marketplaces

Technical Tradecraft

GetAndGo Loader

- Distribution campaigns often use URL shorteners
- Use of HTML attachments containing links to direct victims to dropper documents hosted on filesharing-themed websites
- Use of IP address geolocation filtering on landing pages and tracking of victims through links to iplogger[.]org
- The macro extracts the GetAndGo loader dynamic link library (DLL) to the %APPDATA% folder, and the appropriate DLL is extracted based on whether the Operating System
- C2 beacon to domain that typically impersonates legitimate services/companies, followed by HTTPS traffic on TCP port 443 to corresponding IP address
- Self-signed SSL certificates
- C2 servers use DNSPod[.]com name servers

ACTOR에 대한 정보 제공

- 타깃 국가 / 타깃 산업군
- 마지막 활동 시간
- 범죄 동기 / 범행 목적
- Kill Chain
- 엔드포인트 플랫폼과 자동 연계


감사합니다
CROWDSTRIKE