

CROWDSTRIKE 특징점

엔드포인트 시큐리티 리더

베스핀글로벌

문의 / zerotrust@bespinglobal.com

AUTOMATED HUNTING ENGINE THREAT GRAPH

클라우드스트라이크 플랫폼의 핵심 요소인 Threat Graph는 매주 7조개 이상의 엔드포인트 텔레메트리 정보를 실시간으로 수집하며 이를 기반으로 머신러닝 알고리즘이 최적화되며, 분당 1,350억개의 악의적인 행동에 대한 결정과 170개 이상의 공격그룹을 추적하는데 사용됩니다.
그 결과 한 해 동안 약 90,000건의 침해를 막을 수 있었습니다.

135 MILLION
IOA DECISIONS/MIN

7 TRILLION
EVENTS/WEEK

170
ADVERSARIES TRACKED

ENRICHED
DATA

ACTIONABLE
INSIGHTS

ANALYZED
DATA

PREVENT
THREATS

HUNT
PROACTIVELY

INVESTIGATE
FASTER

90,000

POTENTIAL BREACHES STOPPED



외부 평가 사이버 보안 리더로써 검증된 크라우드스트라이크

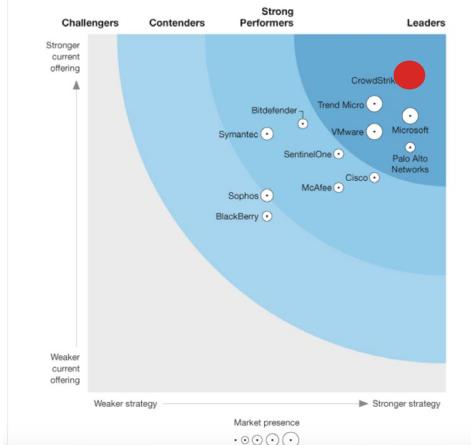
엔드포인트 시큐리티
EPP/EDR 리더 기업

"Leader" – 2021 Gartner
Magic Quadrant for Endpoint
Protection Platforms

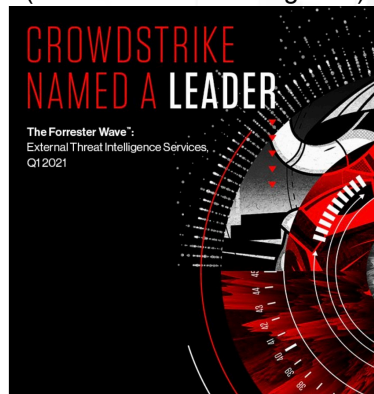


위협 인텔리전스
161 APT 공격 그룹

"Leader" - 2021
Forrester Wave for Endpoint
Security Software As A Service



"Leader" - 2021
Forrester Wave for ETI
(External Threat Intelligence)



글로벌 전문가
IR/CA/MDR 리더 기업

"Leader" - 2021
Forrester Wave for MDR



외부 평가 엔드포인트 시큐리티 리더로써 검증된 기술력



A LEADER

Gartner®

FORRESTER®



A CUSTOMER CHOICE

“Not very often one finds a vendor that has a great end to end team like CrowdStrike”



HIGHEST SCORE OF 4.9/5 IN BOTH EDR AND ENDPOINT PROTECTION PLATFORMS



VALIDATED

MITRE

AV

comparatives

SE Labs

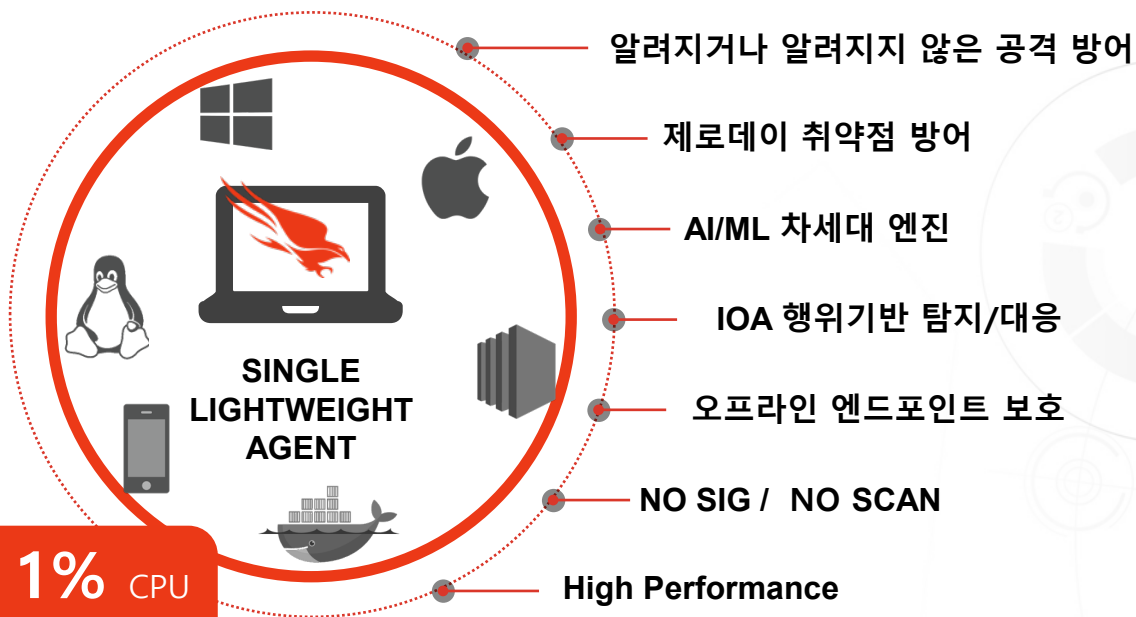
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and 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. GARTNER is a registered trademark and the GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge 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 Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology, they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. Gartner Peer Insights 'Voice of the Customer' Endpoint Detection and Response Solutions, 28 February 2019 and Gartner Peer Insights 'Voice of the Customer' Endpoint Protection Platforms, 10 December 2019



CROWDSTRIKE 기술 특징점



기술 강점 단일 경량화 에이전트 (Single Lightweight Agent)



1% CPU
50MB MEM

THE POWER
OF ONE



기술 강점 단일 경량화 에이전트의 신속한 배포



No infrastructure
setup



No fine-tuning,
rule writing



Install the
Falcon Agent



Verify the
installation



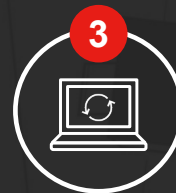
No reboot



No signatures
updates



No scan



Instant
visibility

Financial Institution

77,000 AGENTS
1 DAY

Ecommerce Chain

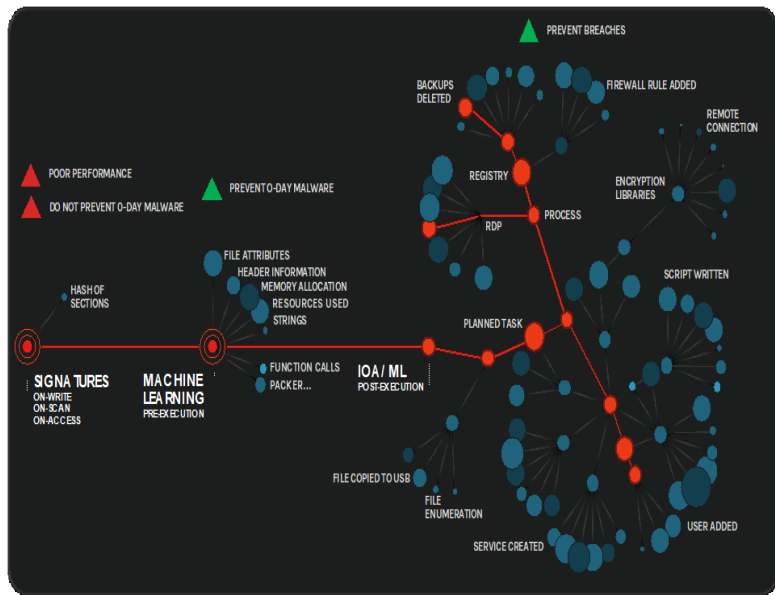
20,000 AGENTS
5 DAYS

**1 LIGHTWEIGHT
AGENT**

**1%
CPU**



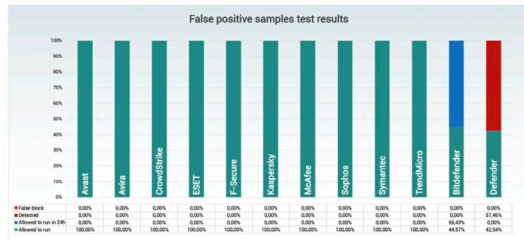
기술 강점 시그니처 없이 머신러닝을 통한 차세대 방어



INTERACTION RATINGS		
Product	None (allowed)	None (blocked)
CrowdStrike Falcon	100	0
ESET Endpoint Security	100	0
FireEye Endpoint Security	100	0
Kaspersky Endpoint Security	100	0
Sophos Intercept X	100	0
Broadcom Endpoint Security Enterprise Edition	99	1
McAfee Endpoint Security	99	1
SentinelOne	98	2
Microsoft Defender Antivirus (enterprise)	90	10

False positive samples test results

The table below shows the initial detection rates of the security products for 1032 false positive samples. This table is sorted by smallest amount of failures.



Usability

Impact of the security software on the usability of the whole computer (lower values indicate better results)

	Industry average	June
False detections of legitimate software as malware during a system scan 463,152 samples used	0	0
False warnings concerning certain actions carried out whilst installing and using legitimate software 60 samples used	0	0
Usability Score	6.0/6.0	

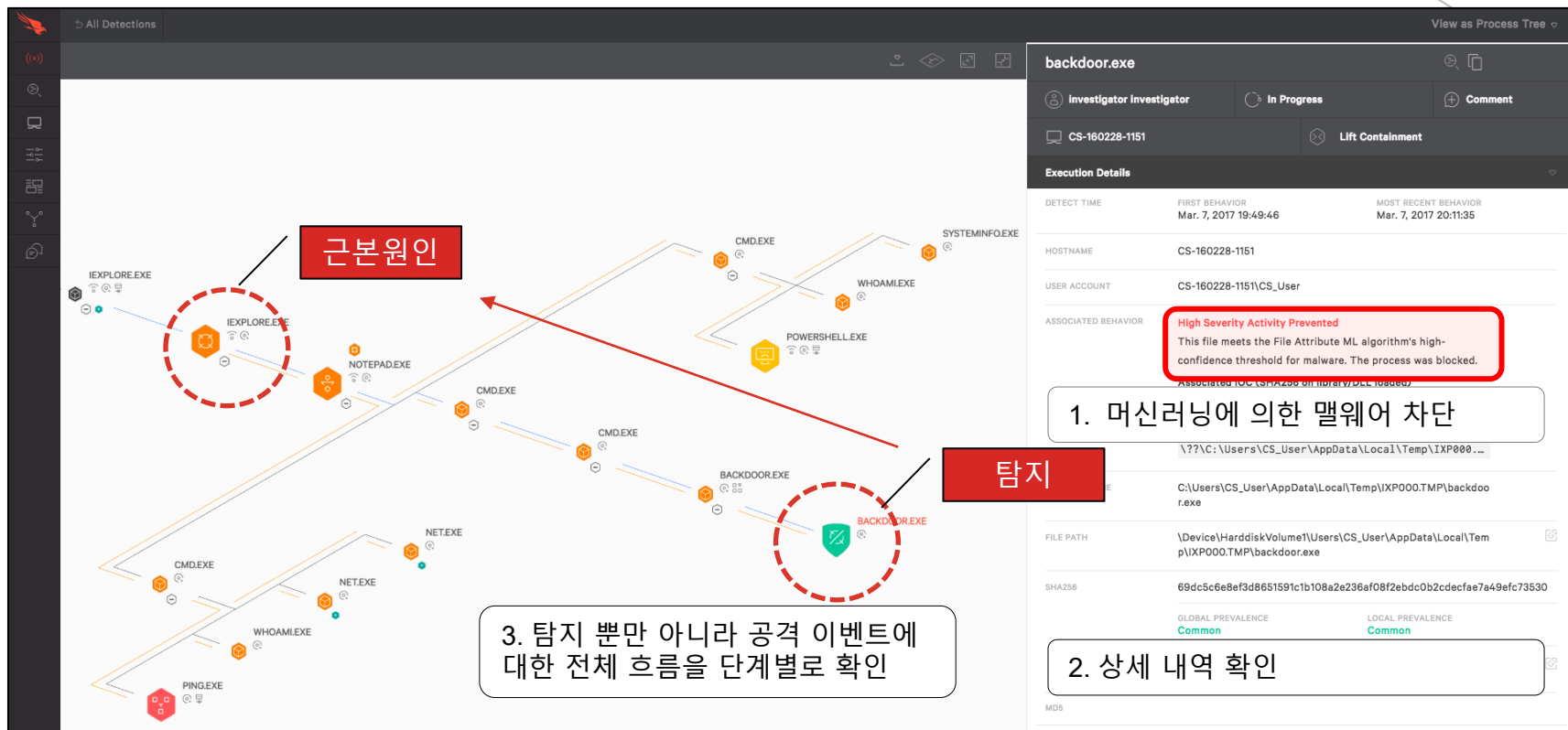
	Blocked	User dependent	Compromised	PROTECTION RATE (Blocked % + (User dependent %)/2)*	False Alarms
BitDefender	1163	-	-	100%	2
McAfee	1163	-	-	100%	4
Trend Micro	1163	-	-	100%	32
Kaspersky Lab	1161	-	2	99.8%	1
Avast	1160	-	3	99.7%	1
VIPRE	1159	-	4	99.7%	1
ESET	1156	-	7	99.4%	0
Emsisoft	1155	-	8	99.3%	0
Endgame	1151	-	12	99.0%	1
Panda	1150	-	13	98.9%	11
CrowdStrike	1149	-	14	98.8%	0
Microsoft	1132	31	-	98.7%	11
eScan	1142	-	21	98.2%	1
Fortinet	1142	-	21	98.2%	4
Saint Security	1065	-	98	91.6%	12
FireEye	1021	-	142	87.8%	0

매주 7조개의 엔드포인트 텔레메트리를 기반으로 최적화된 머신러닝 기반의 차세대 백신

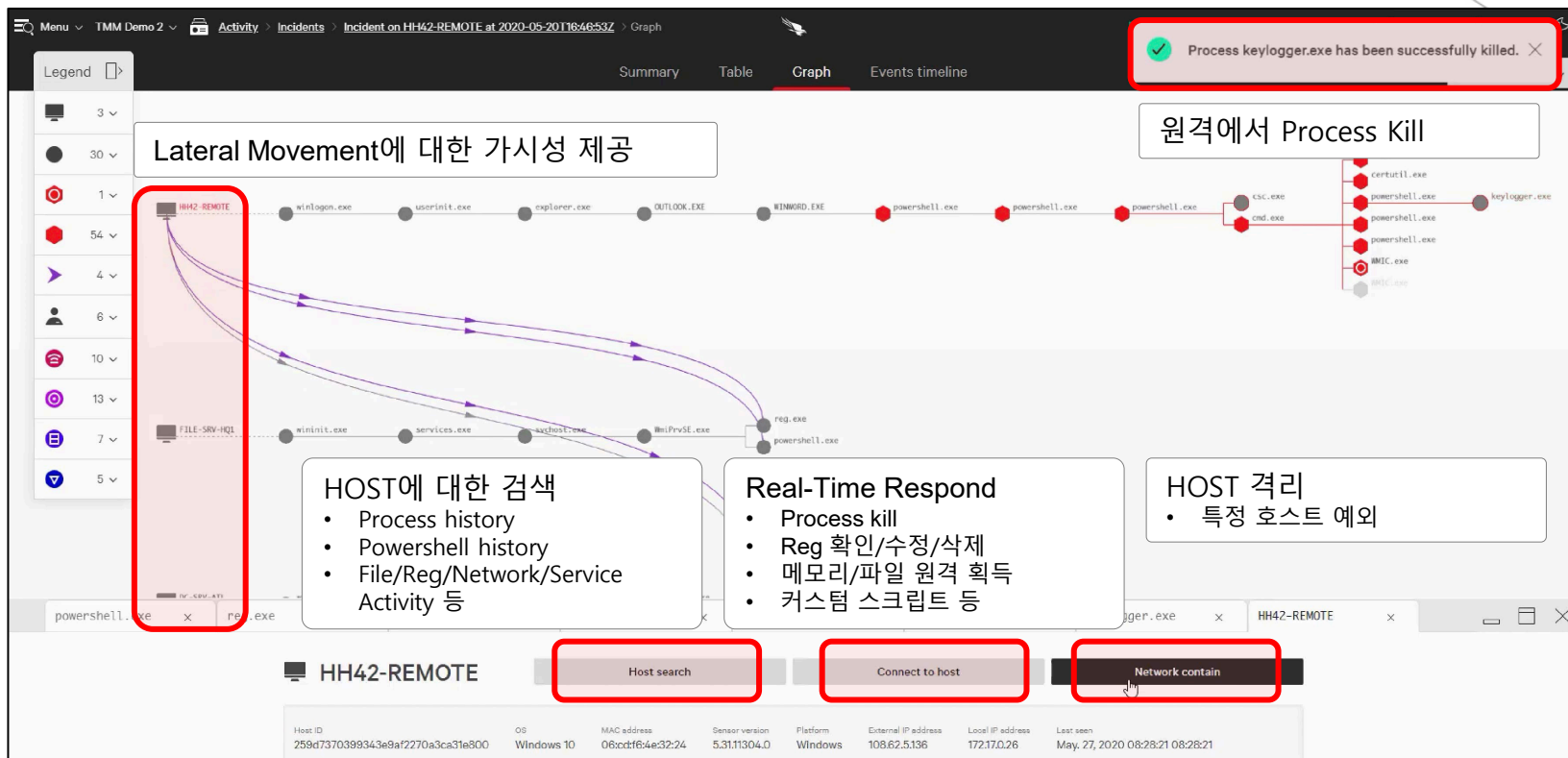
AV 테스트 결과 높은 정탐율과 함께 제로에 가까운 오탐율로 높은 성능의 차세대 백신을 입증



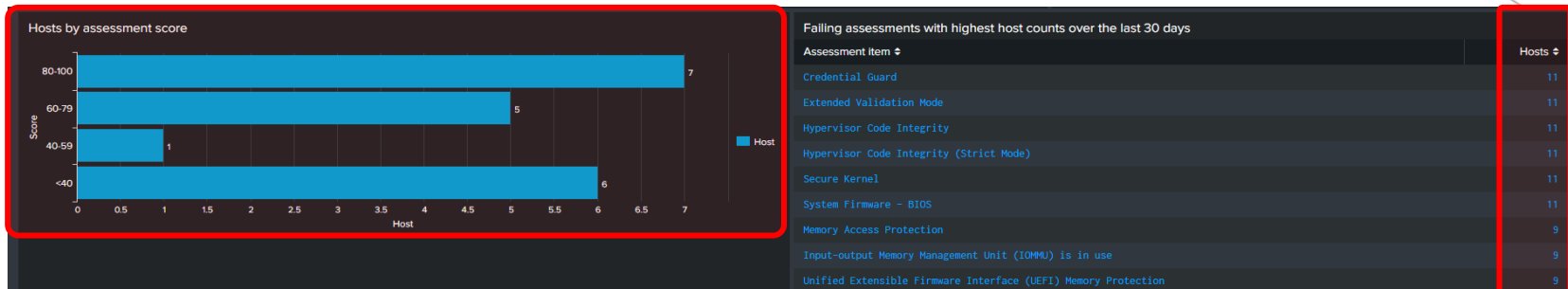
기술 강점 프로세스 트리를 통한 위협에 대한 가시성 확보



기술 강점 단순 탐지에서 벗어나 사고(INCIDENT) 뷰 제공



기술 강점 자산 평가 기능으로 보안 수준 가시성 확보



Assessment by host

Search by host ID or hostname: Score range: X Assessment:

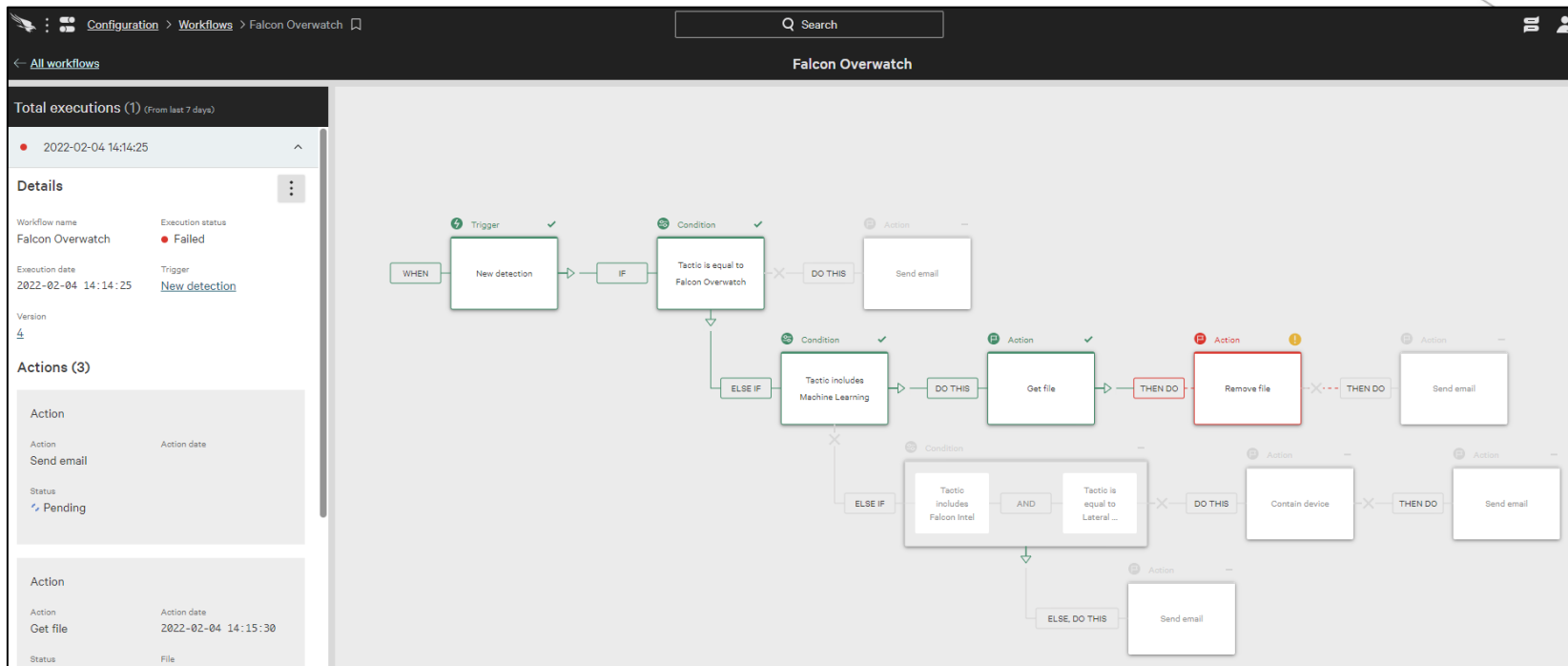
Displaying 6 of 19 hosts

Host ID	Hostname	Platform	Host type	Score version	Last updated	OS assessment	Sensor assessment	Overall assessment
8630231038c74817ad7fb18a80ba61a8	metanes-ui-Mac.local	macOS	Workstation	3.1.0	2022-01-12 07:23:16	64	25	39
81220a23a5324c0989af230360d595c5	CS-VLCI1H	Windows	Workstation	3.2.0	2022-02-03 04:50:37	51	27	36
0e5fd1cd2d71437cb8f9938e1cfec6ff	insungui-MacBook.local	macOS	Workstation	3.1.0	2022-01-25 06:39:27	57	25	36
1d486175ccee4225bb3cd6f8775962ec	DESKTOP-1NB16R9	Windows	Workstation	3.2.0	2022-01-28 01:12:34	54	21	33
8e9c1e2dabbd4e1c9f19c13a943c479f	WIN-N6MCCQ8CF5	Windows	Domain Controller	3.2.0	2022-01-28 01:01:53	47	21	30
3eb95e0e93a1487d85338e7a9d76ae78	crowdstrike3ul-Mac.local	macOS	Workstation	3.0.0	2022-01-07 00:08:25	72	19	24

OS, Sensor 보안 평가 기능을 통해 자산의 보안 수준 가시성을 확보하고 안전한 자산인지 여부를 판단할 수 있는 Zero Trust Assessment 기능을 제공



기술 강점 Wokrflow 기반의 위협 자동 대응 체계



특정 트리거 및 복잡한 위협 시나리오에 대한 대응 체계를 자동화할 수 있는 기능을 제공




기술 강점 Threat Intelligence와의 결합으로 공격의 주체 파악


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
+Q		+Q	7 more	+Q	15 more	+Q

<input type="checkbox"/> Select All	<input type="checkbox"/> Update & Assign
-------------------------------------	--

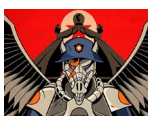
<input type="checkbox"/>		High	TACTIC & TECHNIQUE Machine Learning via Sensor-based ...	DETECT TIME Aug. 6, 2020 10:48:18
STONE PANDA Detected				
<input type="checkbox"/>		High +14 others	TACTIC & TECHNIQUE Execution via Exploitation for Client ...	DETECT TIME Aug. 6, 2020 10:44:33
VOLATILE KITTEN Detected				
<input type="checkbox"/>		High +5 others	TACTIC & TECHNIQUE Machine Learning via Cloud-based ML	DETECT TIME Aug. 6, 2020 10:35:47
<input type="checkbox"/>		High	TACTIC & TECHNIQUE Machine Learning via Sensor-based ...	DETECT TIME Aug. 6, 2020 10:34:23



**VELVET
SIGINT**



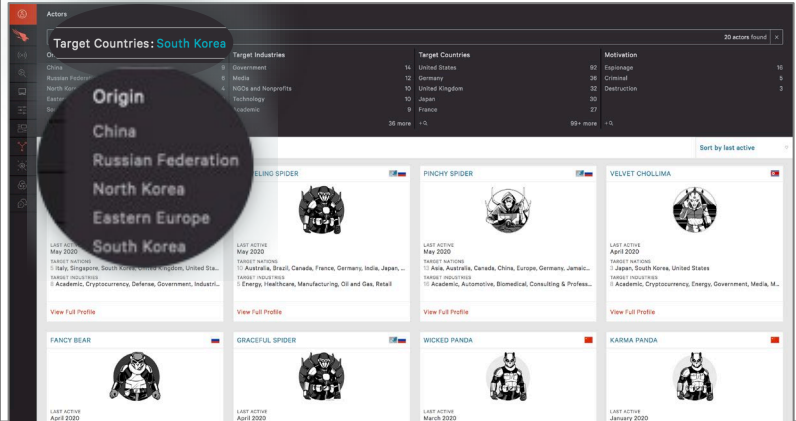
**RICOCHET
HUMINT**



**STARDUST
HUMINT**

ACTOR에 대한 정보 제공

- 타깃 국가 / 타깃 산업군
- 마지막 활동 시간
- 범죄 동기 / 범행 목적
- TTP (tactics, techniques and procedures)
- 엔드포인트와 자동 연계



어떤 공격 그룹이 어떤 목적(범행동기)를 가지고 어떤 기술/기법으로 침투 및 감염을 시키는지에 대한 인텔리전스 정보를 제공하므로 기업은 높은 우선순위 대응과 함께 예방차원의 대응을 같이 할 수 있음

기술 강점 글로벌 리더 전문가들에 의한 24x365 위협 헌팅

위협 헌팅팀(Overwatch) 전문가 사이버 위협 정보

대응 가이드 라인 제공

위협 헌팅팀(Overwatch) 전문가 코멘트 (플랫폼)

Specific to this detection: Rapid Response: The activity is likely malicious in nature. Investigate the process tree.

Command Line: reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CSFalconService" /f

2021 CROWDSTRIKE

WHY CROWDSTRIKE?



보다 나은 방어

Sophisticated technology
Built in threat intelligence
Deep human expertise

전문성 결합

Expert threat hunters
Fully managed
protection & remediation
Threat intelligence

복잡성 단순화

Consolidate agents
Simplify your architecture
Streamline operations

즉각적인 가치 실현

A true turnkey solution
Deploy in one day
No consulting
services required





감사합니다

crowdstrike.com

