



CROWDSTRIKE

크라우드스트라이크

NO.1 엔드포인트 보안 플랫폼

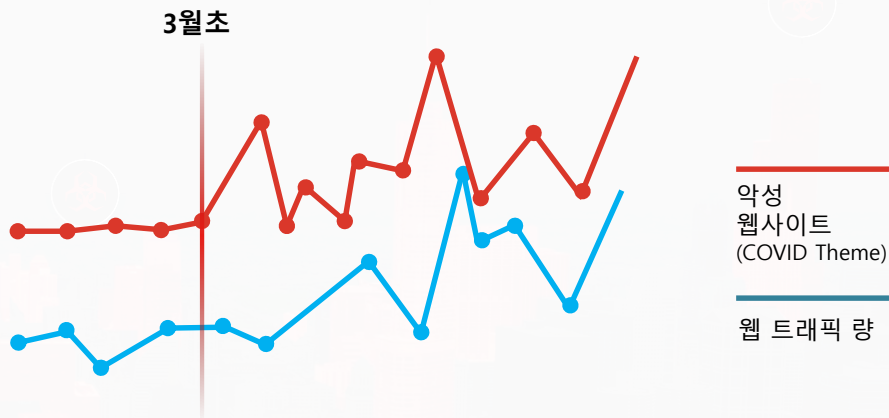
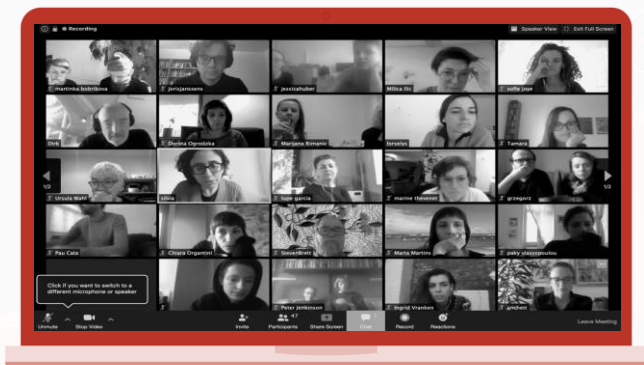
한국IT진흥 2020

CROWDSTRIKE KOREA



COVID-19 이후에 생각해 봐야 할 것들

BREACHES ARE EVERYWHERE

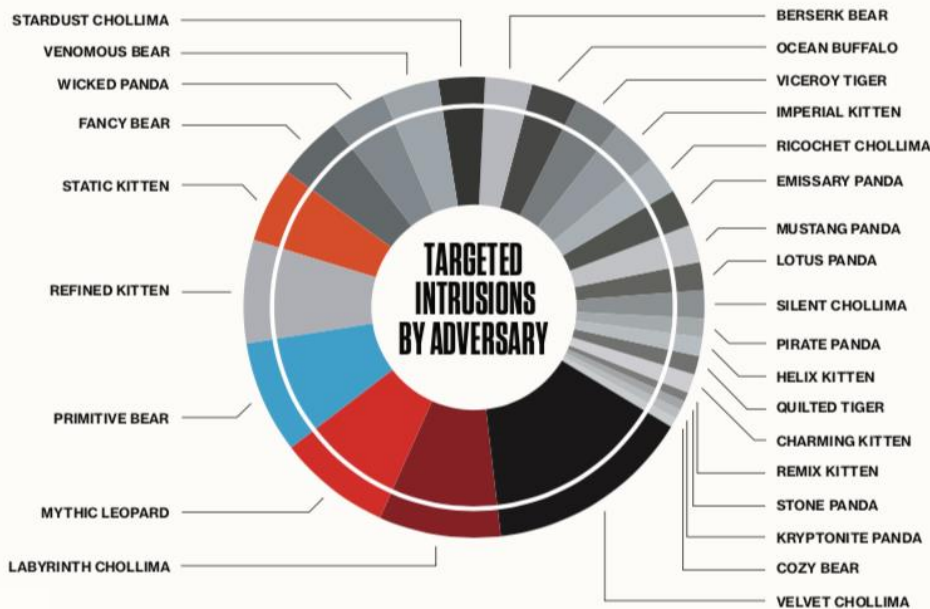


WORK FROM EVERYWHERE

클라우드를 통한 엔드포인트 보안 필요



1분기 위협 인텔리전스 리포트



북한발 해킹 그룹 CHOLLIMA

Q1 기간 동안 50여 리포트 발간

LABYRINTH CHOLLIMA: COVID-19 LURE DOCUMENT
DELIVERING XCRAT TARGETS SOUTH KOREANS

PUBLISHED 15 JUNE 2020

CROWDSTRIKE GLOBAL INTELLIGENCE TEAM
web: WWW.CROWDSTRIKE.COM | twitter: @CROWDSTRIKE

FOR INFORMATION AND PROFESSIONAL USE ONLY. NOT TO BE REPRODUCED OR DISTRIBUTED TO THIRD PARTIES. © COPYRIGHT 2020

This report is provided for situational awareness and network defense purposes only. DO NOT conduct searches on, communicate with, or engage any individual, organization, or network address identified in this report. Doing so may put you or your employer at risk and jeopardize any ongoing investigation efforts.



북한 정찰총국 3국(121부대)



WHAT?

- 5 개의 천리마 그룹들이 공동 목표를 향해 긴밀히 협력 중



SILENT
C2



VELVET
SIGINT



RICOCHET
T
HUMINT



STARDUST
HUMINT



LABYRINTH
ACCESS



SO WHAT?

- 북한은 정교한 다각적인 사이버 작전 능력을 보유하고 있다. 북한은 매우 영리하다 - 흔적(Artifact) 을 거의 남기지 않는다



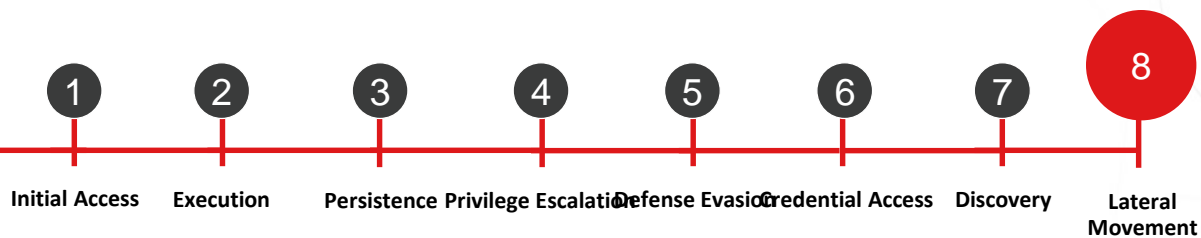
WHAT NEXT?

- THREAT ACTOR PROFILING
- CAMPAIGN TRACKING

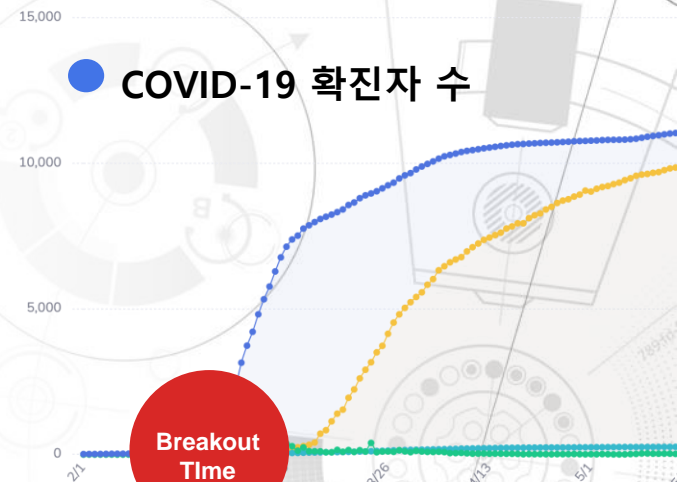


SURVIVAL OF THE FASTEST

BREAKOUT TIME

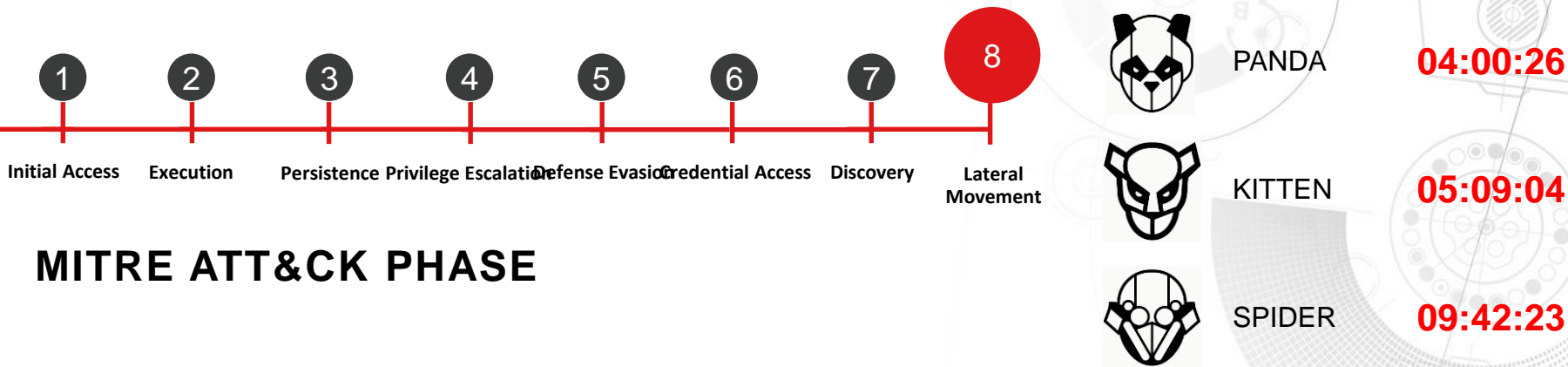


MITRE ATT&CK PHASE



SURVIVAL OF THE FASTEST

BREAKOUT TIME



SURVIVAL OF THE FASTEST

TO STAY AHEAD
YOU MUST:

DETECT IN

1min

INVESTIGATE IN

10min

RESPOND IN

60min

1

2

3

4

5

6

7

8



WE STOP BREACHES



CROWDSTRIKE COMPANY

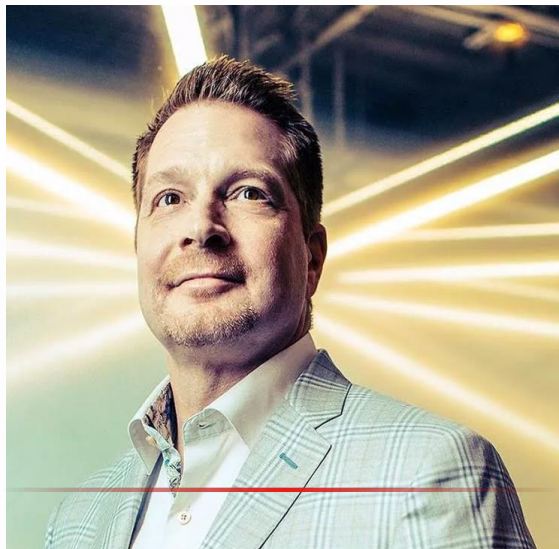


Figure 1. Magic Quadrant for Endpoint Protection Platforms



Gartner Magic Quadrant for Endpoint Protection Platforms, August 2019

설립일 : 2011년
CEO : George Kurtz
(원래 McAfee 사의 CTO)
매출액 : 연간100% 증가

2019년 6월 IPO (NASDAQ)
상장 첫날 종료 시점의
시가총액은 114억 달러(약14조)까지 상승

2018년 Visionary에서
2019년 Leader로 급부상
30년 이상의 시만택, 맥아피, 트렌드마이크로를
뛰어넘음



CROWDSTRIKE가 제공하는 주요 세가지



향상된 보호기능
TECHNOLOGY



스마트한 보안
INTELLIGENCE

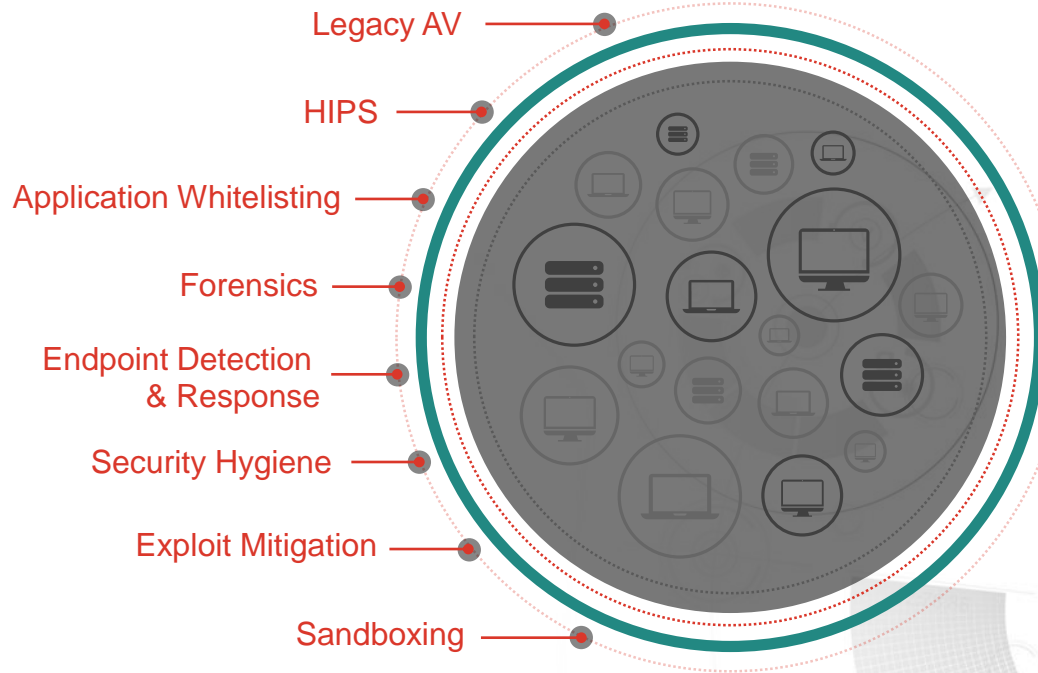


더 높은 가치
EXPERTISE



PROBLEM: AGENT BLOAT + SIGNATURES

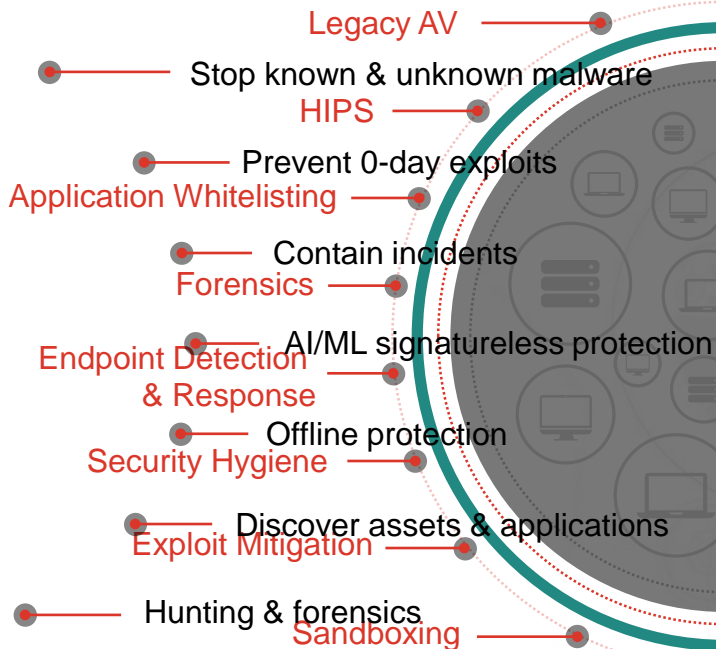
LEGACY SOLUTIONS



SOLUTION: REDUCE AGENT COMPLEXITY

LEGACY
SOLUTIONS

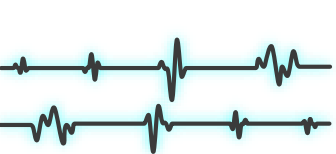

SINGLE
LIGHTWEIGHT
AGENT



THE POWER
OF **ONE**



SOLUTION: REDUCE AGENT COMPLEXITY



**SINGLE
LIGHTWEIGHT
AGENT**

1% CPU
40MB MEM

MULTI OS



PREVENTION

머신 러닝

취약점 차단

IOA(Indicators Of Attack)

DETECTION & RESPONSE

실시간 수집

빠른 검색

실시간 대응

위협 헌팅

IT HYGENE & VULNERABILITY 관리

자산 관리

사용자 관리

어플리케이션 관리/취약점 관리





CLOUD-NATIVE PLATFORM



클라우드 모듈

- 신속한 구현
- 대량 검색 능력
- 확장성 용이



Threat Graph

- 파워풀한 AI
- 클라우드 기반 위협 헌팅 엔진



단일화된 경량 에이전트

- 성능 저하없이 모든 워크로드 보호
- Windows, Mac, Linux, iOS, Android, Cloud workload, Container





THREAT INTELLIGENCE



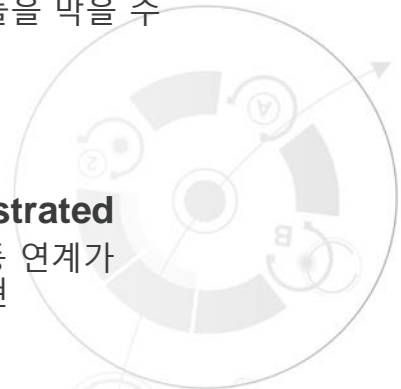
공격자에 대한 전문 정보 제공
그들을 알아야 그들을 막을 수 있습니다.



Automated and Orchestrated
엔드포인트 프로텍션과 자동 연계가 되어 빠른 조사 및 대응 구현



예측 가능한 파워
과거의 공격으로부터 학습하여 사전 대응 가능





WORLD-CLASS EXPERTISE



Managed Threat Hunting

24x7x365 연중 무휴 위협 헌팅을
통해 위협을 끊임없이 찾습니다.



Managed Endpoint Protection

관리, 대응의 전문성 제공



Services

사고 대응 및 전략적 자문 서비스 제공



CROWDSTRIKE FALCON



AUTOMATED HUNTING ENGINE THREAT GRAPH

135 MILLION
IOA DECISIONS/MIN

2.5 TRILLION
EVENTS/WEEK

140
ADVERSARIES TRACKED

AUTOMATED HUNTING ENGINE THREAT GRAPH

135 MILLION
IOA DECISIONS/MIN

2.5 TRILLION
EVENTS/WEEK

140
ADVERSARIES TRACKED

ENRICHED
DATA

ANALYZED
DATA



AUTOMATED HUNTING ENGINE THREAT GRAPH

135 MILLION
IOA DECISIONS/MIN

2.5 TRILLION
EVENTS/WEEK

140
ADVERSARIES TRACKED

ENRICHED
DATA

ACTIONABLE
INSIGHTS

ANALYZED
DATA

PREVENT
THREATS

HUNT
PROACTIVELY

INVESTIGATE
FASTER

35,000

POTENTIAL BREACHES STOPPED



NEXT-GEN AV FALCON PREVENT



CROWDSTRIKE FALCON
CERTIFIED AS LEGACY
AV REPLACEMENT

제공되는 가치

더 나은 보호기능 제공

침해사고 감소

사용자 생산성 향상

복잡성 제거

보안 효율성 제공





DW-SMILE Network Contain

Connect to Host

Execution Details

DETECT TIME	FIRST BEHAVIOR Feb. 22, 2019 10:51:24	MOST RECENT BEHAVIOR Feb. 22, 2019 10:55:16
HOSTNAME	DW-SMILE	
USER NAME	WORKGROUP\DW-SMILES	
SEVERITY	High	
OBJECTIVE	Contact Controlled Systems	
TACTIC & TECHNIQUE	Command and Control via Remote Access Tools	
SPECIFIC TO THIS DETECTION	A process launched that appears related to a remote administration tool (RAT). Review the process tree.	
SEVERITY	Low	
OBJECTIVE	Falcon Detection Method	
TACTIC & TECHNIQUE	Machine Learning via Sensor-based ML	
SPECIFIC TO THIS DETECTION	This file meets the machine learning-based on-sensor AV protection's low confidence threshold for malicious files.	
INDICATORS OF INTEREST	Associated IOC (SHA256 on library/DLL loaded) 742b47e8846b780329e58f767-735017368-cabe2282378f38949972a1	



ENDPOINT DETECTION AND RESPONSE FALCON INSIGHT



Record Everything

제공되는 가치

빠른 대응 시간 제공

SOC 프로세스 개선

치료 시간 단축

기술, 전문 지식 강화

위협 감소

보안 효율성 확보



POWERFUL RESPONSE AND REMEDIATION

COLLECT INFO



Processes



File System



Registry



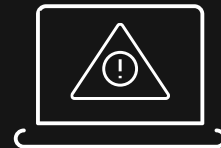
Network
Activities



Memory



OS Events



Kill
Process



Delete File
Blacklist File



Modify
Registry



Network
Quarantine



Custom
Scripts

TAKE ACTION



THREAT INTELLIGENCE

KNOW YOUR ADVERSARY

AT THE HEART OF EVERY ATTACK IS A HUMAN ADVERSARY.
FALCON INTELLIGENCE REVEALS THEIR MOTIVATION AND TRADECRAFT TO KEEP YOU ONE STEP AHEAD.



THREAT INTELLIGENCE AUTOMATION FALCON X



제공되는 가치

위협 조사 가속화

우선순위 기반 평가 / 빠른 대응 속도

IOC 확대 및 보호 극대화

OC, IR, CTI 협업

사고 예방



MANAGED THREAT HUNTING FALCON OVERWATCH

24/7 Proactive
Threat Hunting



Actionable Alerts
via Console
and Email



Prioritization



Guided
Response



제공되는 가치

끊임없는 전문 지식 확보

숨겨져 있는 정교한 위협을 보고/중재

Dwell time 감소

경고에 대한 피로 감소



REMIEDIATION REPORT

Incident Responders

- Investigate every alert and determine root cause
- Remote remediation
- **Remove of persistence mechanisms**
- **Stop active processes**
- **Adjust registry keys**
- Addressing the entire kill-chain
- Powered by our Falcon Platform

Incident Details

System_Hostname:

JoePC

Username:

Administrator

System_IP_Address:

192.168.10.106

Detection_Scenario:

Known Malware-Ursnif

Detection_Severity:

HIGH

Detection_Details:

<https://falcon.crowdstrike.com/activity/detections>

Date_of_Initial_Compromise:

20180611

Analysis_and_Remediation_Details:

The user fell victim to a phish which led to the installation of Ursnif malware.

Processes Stopped:

Markerscaler.exe

Quarantined Files:

C:\Users\Administrator\Downloads\Ballroom prices & Menu 2016\Emails Models.docx
 C:\Users\Administrator\AppData\Local\Temp\67406.exe
 C:\windows\SysWOW64\markerscaler.exe
 C:\ProgramData\KdbNNb.exe
 C:\Users\Administrator\AppData\Local\Temp\ouxlfcbtocvzpvvhvgtafmfdms.txt
 C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu32.dll
 C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu.exe
 C:\Users\Administrator\AppData\Local\Microsoft\Doetduo.wpq
 C:\windows\SysWOW64\g3lhvX8JQNMnRx.exe
 C:\windows\SysWOW64\ic4bNmqt.exe

Removed Regkey's

HKCU\Software\Microsoft\Windows\Currentversion\Run ychfmxl REG_SZ
 C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe "\$windowsupdate = \ C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu.exe";& \$windowsupdate"

Removed Scheduled Tasks related to the malware

125275F5-F470-4919-9A18-234F29DAB5C4
 cmd.exe/C:start/MINC:windows\system32\cscript.exe//E:javascrpt"C:\Users\Administrator\AppData\Local\Microsoft\doetdu.wpq"

44974F44-5BCA-4A51-9FC7-F91BAID74CE7
 C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe "\$windowsupdate = \ "C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu.exe"; & \$windowsupdate"

Recommended_Recovery_Tasks:

Reset Administrator password



FALCON PLATFORM PROTECTS ALL WORKLOADS



CLOUD SECURITY

ENDPOINT SECURITY

SECURITY & IT OPERATIONS

THREAT INTELLIGENCE

CROWDSTRIKE STORE

APIs

APIs

CROWDSTRIKE THREAT GRAPH

WINDOWS LINUX APPLE ANDROID iOS AWS GCP AZURE

WORKSTATIONS

SERVERS

DATACENTERS

MOBILE
FALCON FOR MOBILE

CLOUD / CONTAINERS
FALCON FOR AWS, AZURE, GCP

IOT

LIGHTWEIGHT AGENT



A PROVEN LEADER IN ENDPOINT PROTECTION



A LEADER

Gartner®

FORRESTER®

IDC



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 constitutes 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.



WHY CROWDSTRIKE?



IMPROVE YOUR PROTECTION

Sophisticated technology
Built in threat intelligence
Deep human expertise

GAIN EMBEDDED EXPERTISE

Expert threat hunters
Fully managed protection & remediation
Threat intelligence

REDUCE COMPLEXITY

Consolidate agents
Simplify your architecture
Streamline operations

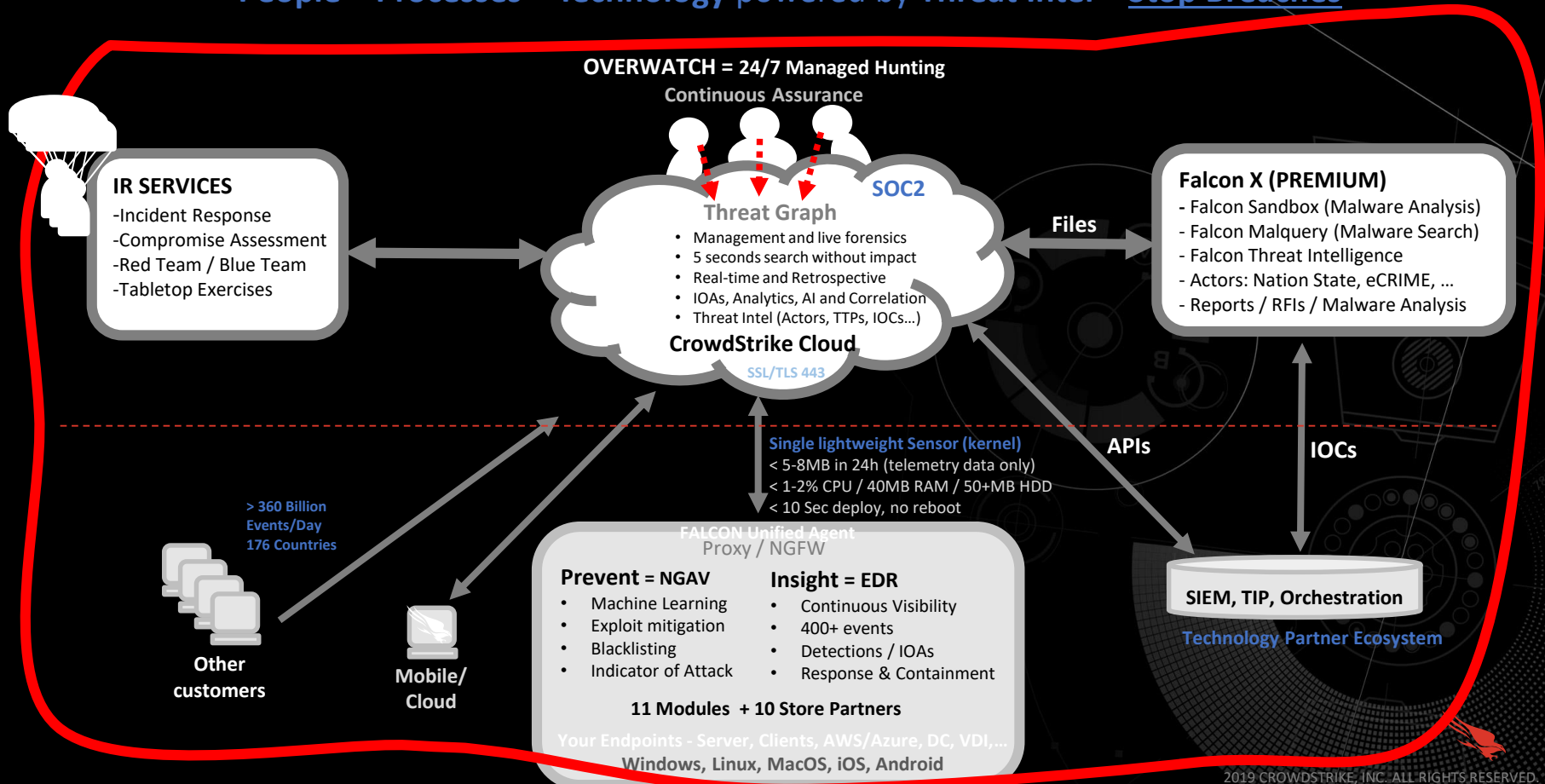
GET IMMEDIATE VALUE

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



FALCON PLATFORM – Cloud Delivered Endpoint Protection

People + Processes + Technology powered by Threat Intel = Stop Breaches





감사합니다

crowdstrike.com

kitt  한국IT진흥

