CROWDSTRIKE

크라우드스트라이크
NO.1 엔드포인트 보안 플랫폼

한국IT진흥 2020

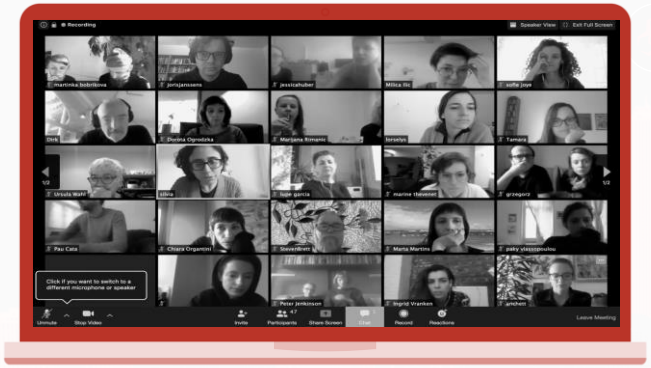
CROWDSTRIKE KOREA

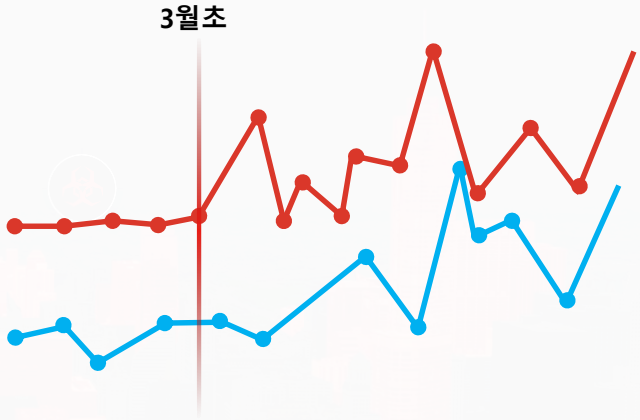
kitt 한국IT진흥

CROWDSTRIKE

kitt 한국IT진흥

COVID-19 이후에 생각해 봐야 할 것들





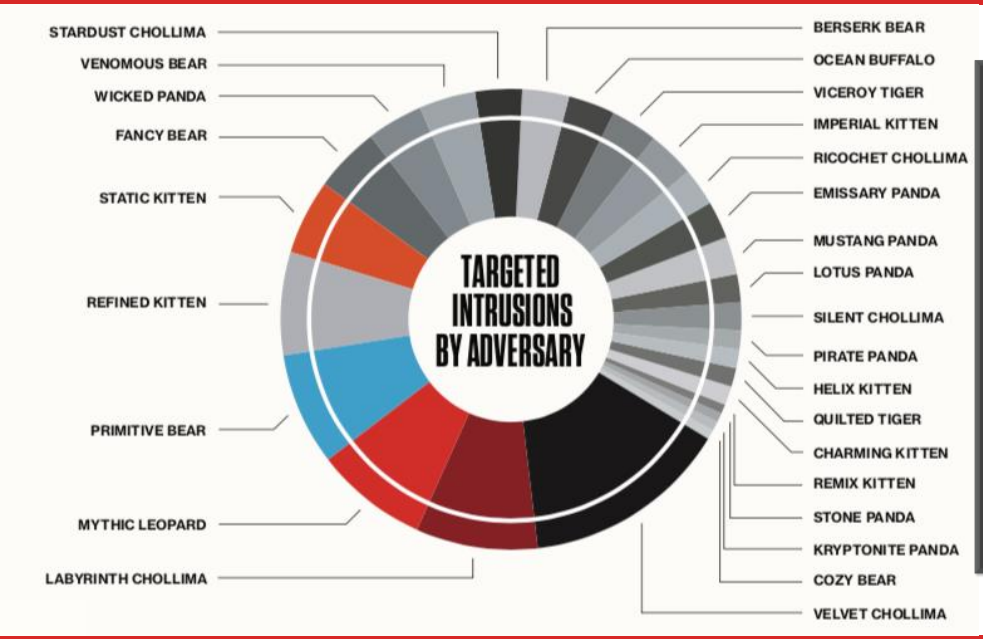
WORK FROM EVERYWHERE

클라우드를 통한 엔드포인트 보안 필요

CROWDSTRIKE

kitt 한국IT진흥

1분기 위협 인텔리전스 리포트



북한발 해킹 그룹 CHOLLIMA

Q1 기간 동안 50여 리포트 발간

CROWDSTRIKE

kitt 한국IT진흥

북한 정찰총국 3국(121부대)

WHAT?

- 5 개의 천리마 그룹들이 공동 목표를 향해 긴밀히 협력 중

SILENT
C2

VELVET
SIGINT

RICOCHE
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

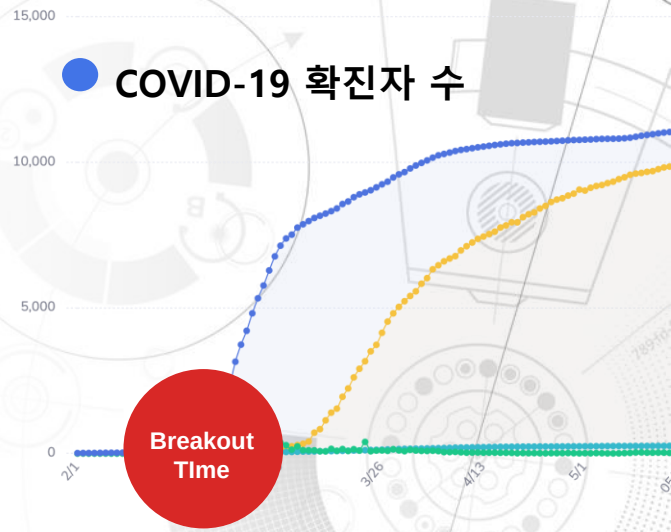
CROWDSTRIKE

kitt 한국IT진흥

SURVIVAL OF THE FASTEST

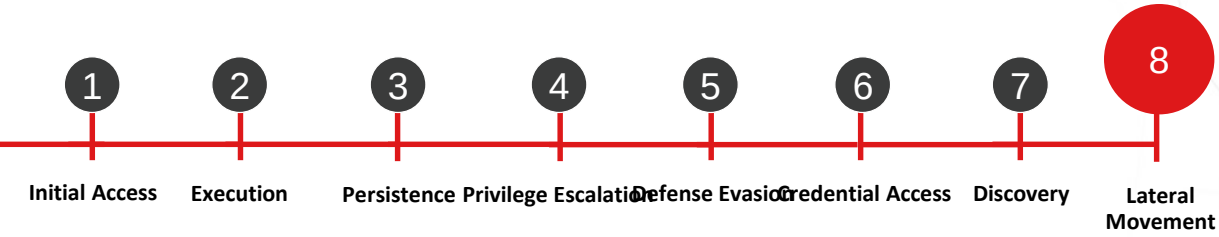
BREAKOUT TIME

MITRE ATT&CK PHASE



SURVIVAL OF THE FASTEST

BREAKOUT TIME



MITRE ATT&CK PHASE

BEAR **00:18:49**

CHOLLIMA **02:20:14**

PANDA **04:00:26**

KITTEN **05:09:04**

SPIDER **09:42:23**

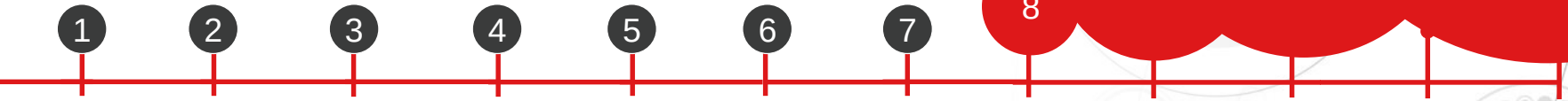
CROWDSTRIKE

kitt 한국IT진흥

SURVIVAL OF THE FASTEST

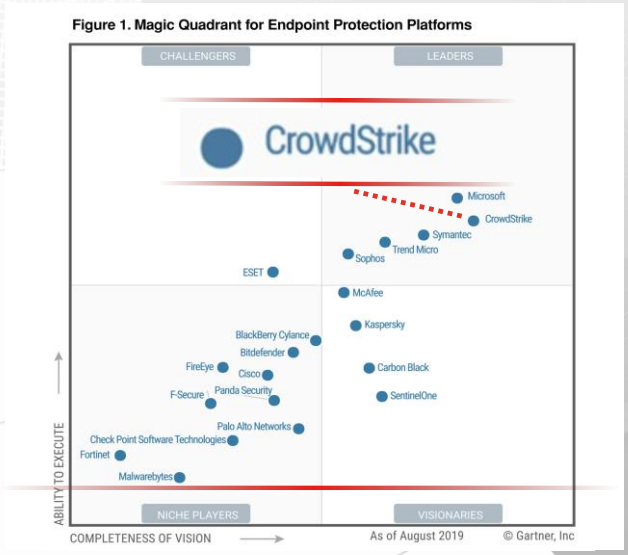
TO STAY AHEAD YOU MUST:

DETECT IN	INVESTIGATE IN	RESPOND IN
1min	10min	60min



WE STOP BREACHES

CROWDSTRIKE COMPANY



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, 트랜드마이크로를
뛰어넘음

CROWDSTRIKE가 제공하는 주요 세가지

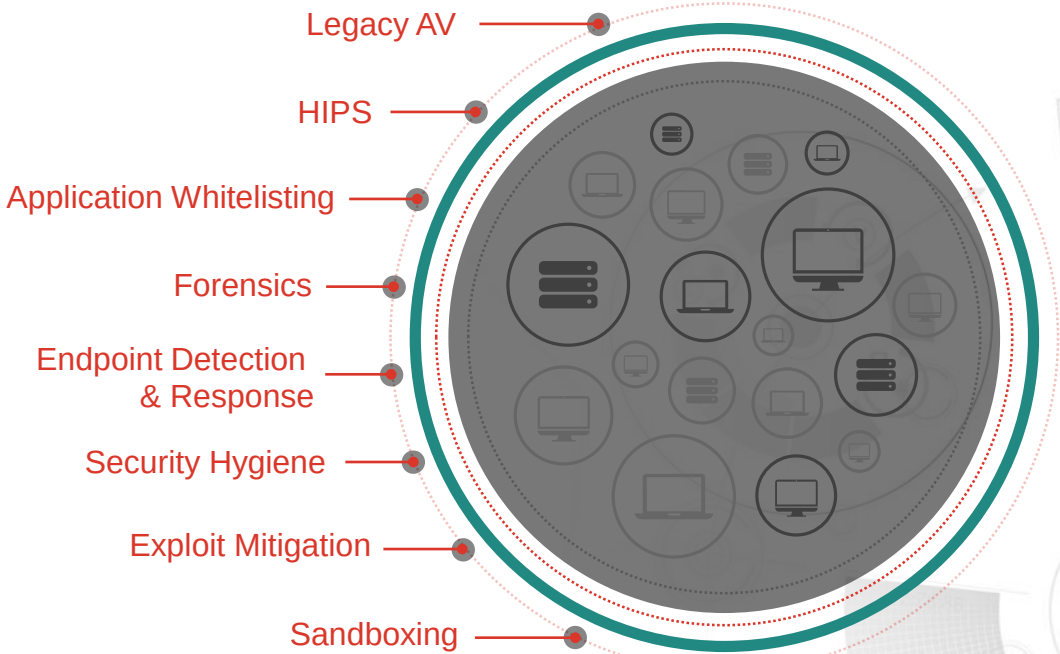
향상된 보호기능
TECHNOLOGY

스마트한 보안
INTELLIGENCE

더 높은 가치
EXPERTISE

PROBLEM: AGENT BLOAT + SIGNATURES

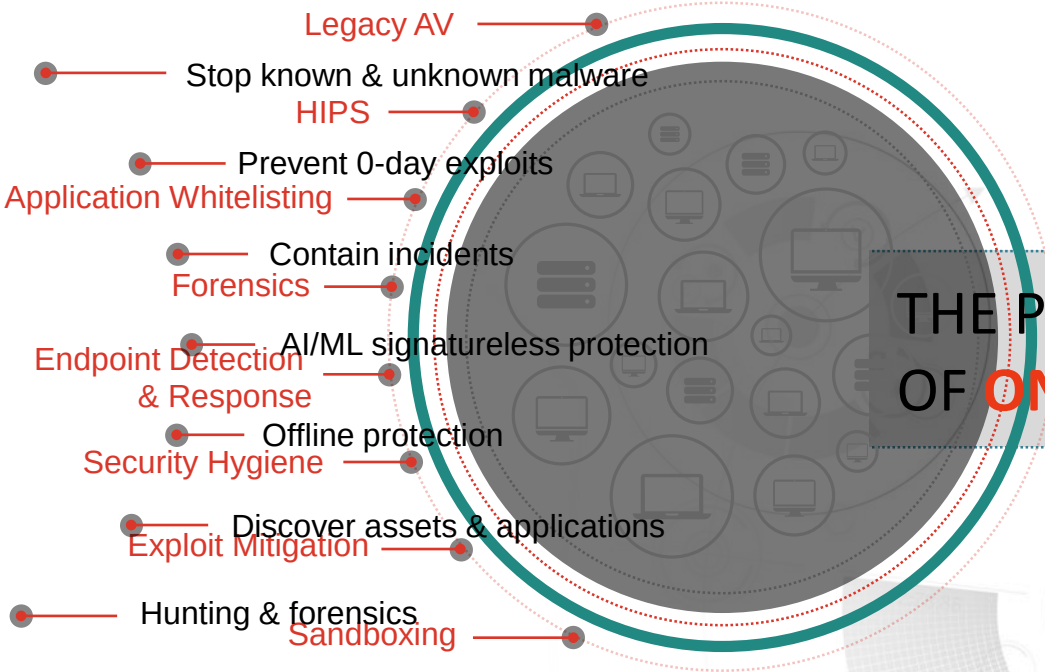
LEGACY SOLUTIONS



SOLUTION: REDUCE AGENT COMPLEXITY

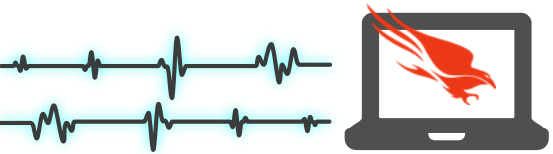
LEGACY SOLUTIONS

SINGLE LIGHTWEIGHT AGENT



THE POWER OF ONE

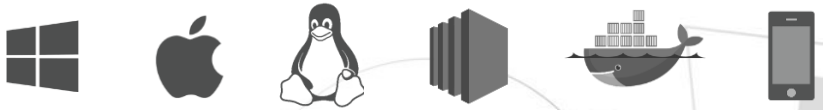
SOLUTION: REDUCE AGENT COMPLEXITY



1% CPU
40MB MEM

SINGLE LIGHTWEIGHT AGENT

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

CROWDSTRIKE

kitt 한국IT진흥

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**

CROWDSTRIKE

kitt 한국IT진흥

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

CROWDSTRIKE

kitt 한국IT진흥

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

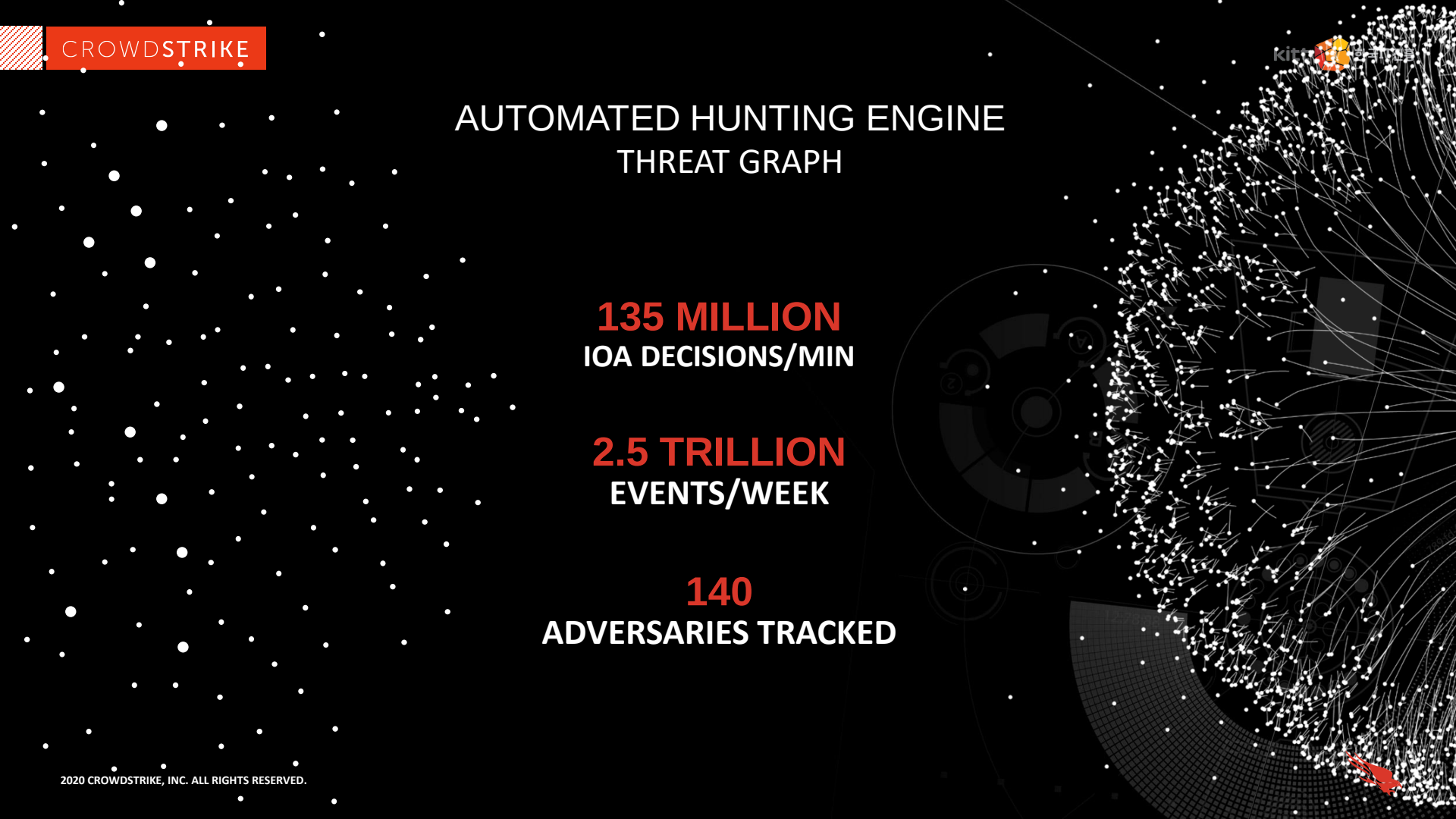
CROWDSTRIKE

AUTOMATED HUNTING ENGINE
THREAT GRAPH

135 MILLION
IOA DECISIONS/MIN

2.5 TRILLION
EVENTS/WEEK

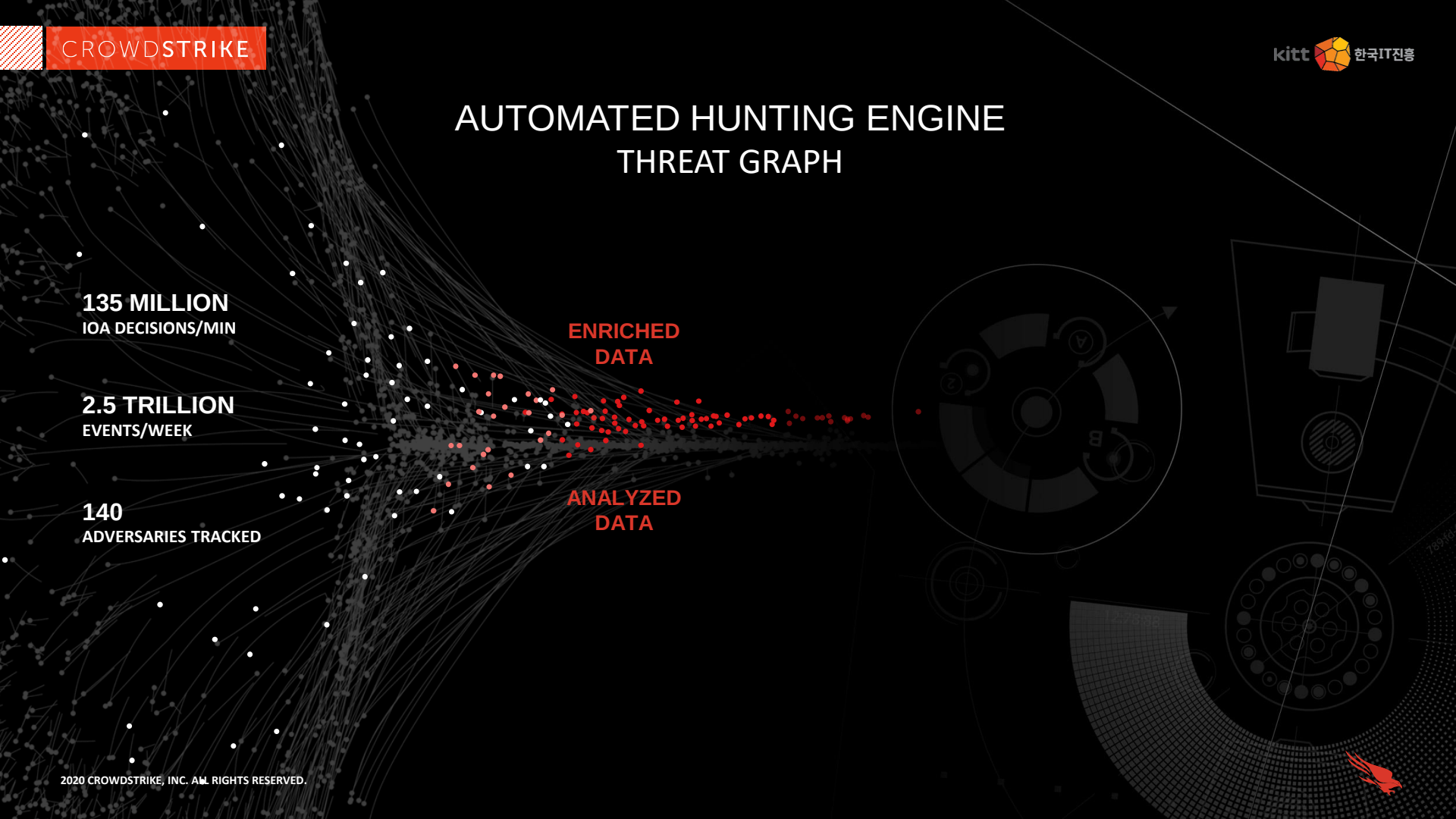
140
ADVERSARIES TRACKED



CROWDSTRIKE

kitt 한국IT진흥

AUTOMATED HUNTING ENGINE
THREAT GRAPH



CROWDSTRIKE

kitt 한국IT진흥

AUTOMATED HUNTING ENGINE
THREAT GRAPH

135 MILLION
IOA DECISIONS/MIN

2.5 TRILLION
EVENTS/WEEK

140
ADVERSARIES TRACKED

ENRICHED DATA

ACTIONABLE INSIGHTS

ANALYZED DATA

35,000

POTENTIAL BREACHES STOPPED

CROWDSTRIKE

kitt 한국IT진흥

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

CROWDSTRIKE

kitt 한국IT진흥

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)	

1 Initial Access
2 Execution
3 Persistence
4 Privilege Escalation
5 Defense Evasion
6 Credential Access
7 Discovery
8 Lateral Movement
9 Collection
10 Exfiltration
11 Command & Control

CROWDSTRIKE

kitt 한국IT진흥

ENDPOINT DETECTION AND RESPONSE

FALCON INSIGHT

Record Everything

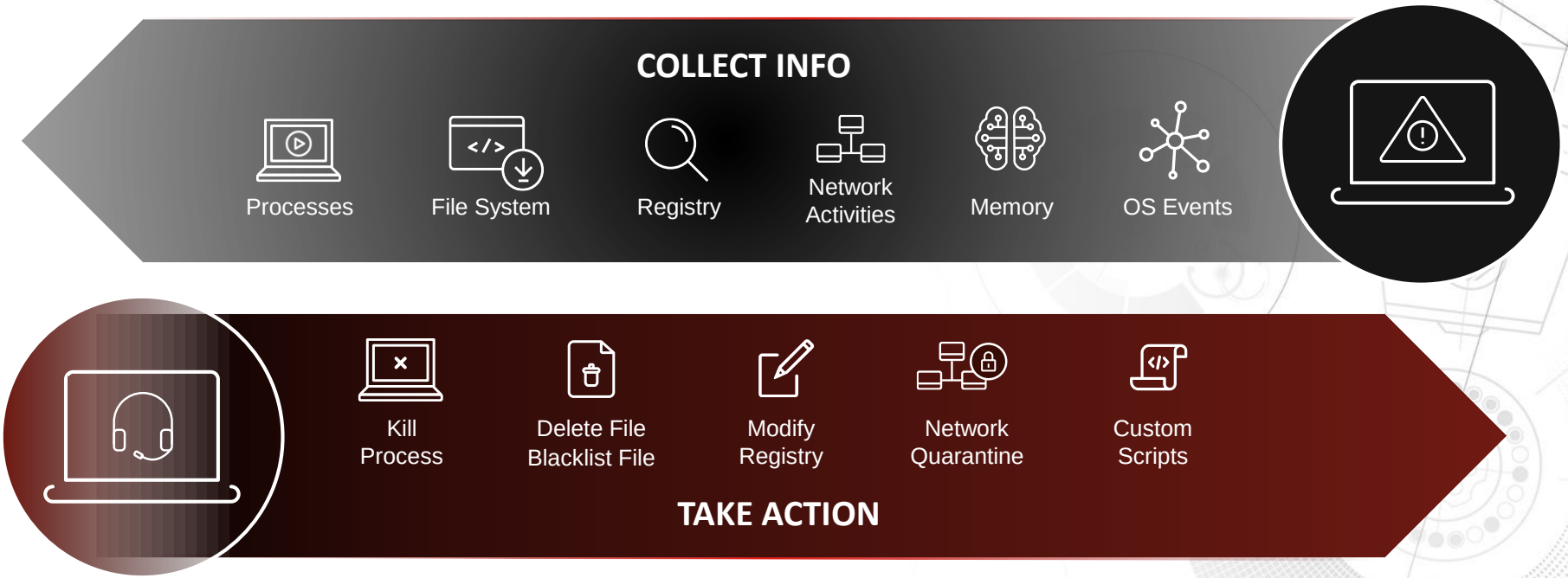
제공되는 가치

- 빠른 대응 시간 제공
- SOC 프로세스 개선
- 치료 시간 단축
- 기술, 전문 지식 강화
- 위협 감소
- 보안 효율성 확보

CROWDSTRIKE

kitt 한국IT진흥

POWERFUL RESPONSE AND REMEDIATION



CROWDSTRIKE

kitt 한국IT진흥

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.

CROWDSTRIKE

kitt 한국IT진흥

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

CROWDSTRIKE

kitt 한국IT진흥

MANAGED THREAT HUNTING
FALCON OVERWATCH

제공되는 가치

끊임없는 전문 지식 확보

숨겨져 있는 정교한 위협을 보고/중지

Dwell time 감소

경고에 대한 피로 감소

CROWDSTRIKE

kitt 한국IT진흥

REMEDIATION 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.dox
C:\Users\Administrator\AppData\Local\Temp\67406.exe
C:\windows\SysWOW64\markerscalar.exe
C:\ProgramData\KdbNNb.exe
C:\Users\Administrator\AppData\Local\Temp\ouxlfcbtocvpzpvhvgtsafmfds.txt
C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu32.dill
C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu.exe
C:\Users\Administrator\AppData\local\Microsoft\Doetduo.wqp
C:\windows\SysWOW64\g3lhVX8JQNMnRx.exe
C:\windows\SysWOW64\ic4bNmqtt.exe

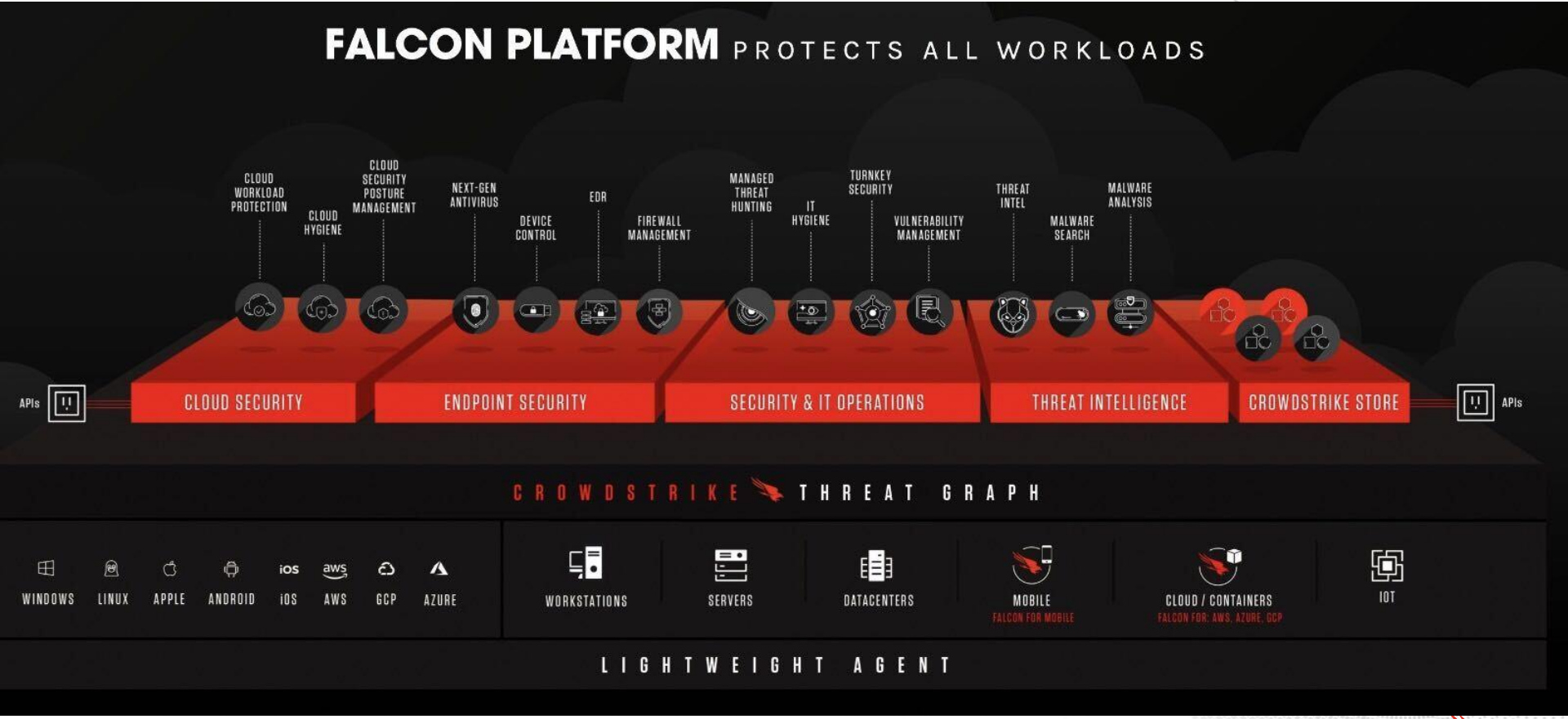
Removed Regkey's
HKCU\Software\Microsoft\Windows\Currentversion\Run ychfmxl REG_SZ C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe "$windowsupdate = \ C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu.exe\";& $windowsupdate"

Removed Scheduled Tasks related to the malware
125275F5-F470-4919-9A18-234F29DAB5C4
cmd.exe/C"start/MINC:\windows\system32\cscript.exe//E:javascript"C:\Users\Administrator\AppData\Local\Microsoft\doetdu.wpq""

44974F44-5BCA-4A51-9FC7-F91BA1D74CE7
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



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"

Gartner peerinsights customers' choice

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

VALIDATED

MITRE

AV comparatives

SE Labs

CROWDSTRIKE

kitt 한국IT진흥

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

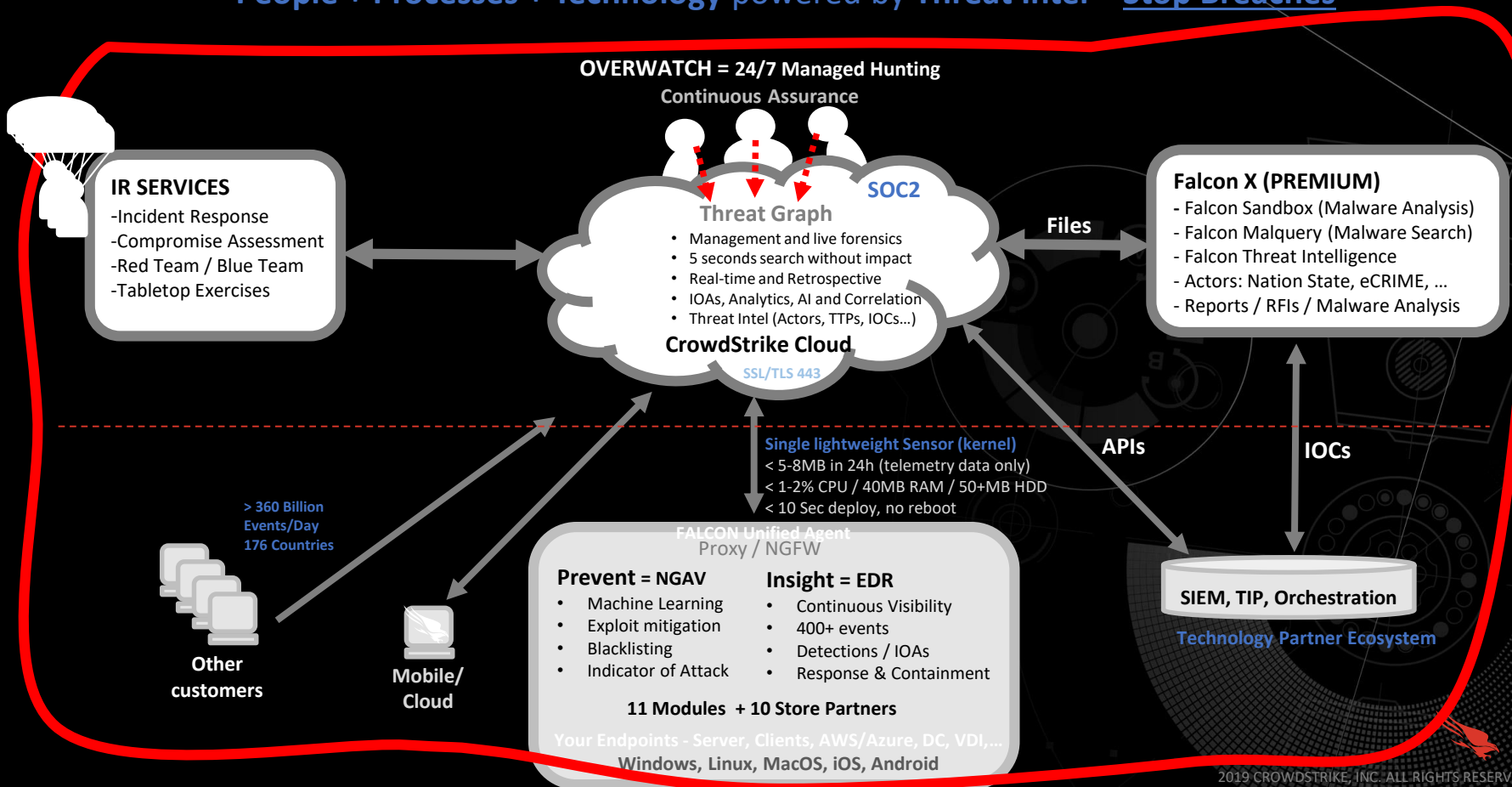
No consulting services required

CROWDSTRIKE

kitt 한국IT진흥

FALCON PLATFORM – Cloud Delivered Endpoint Protection

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




감사합니다
crowdstrike.com
kitt
한국IT진흥