CROWDSTRIKE

Race against the machines and time

Robert Michalski

CEE SE Manager

You don’t have a **malware** problem,

you have an **adversary** problem.

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.

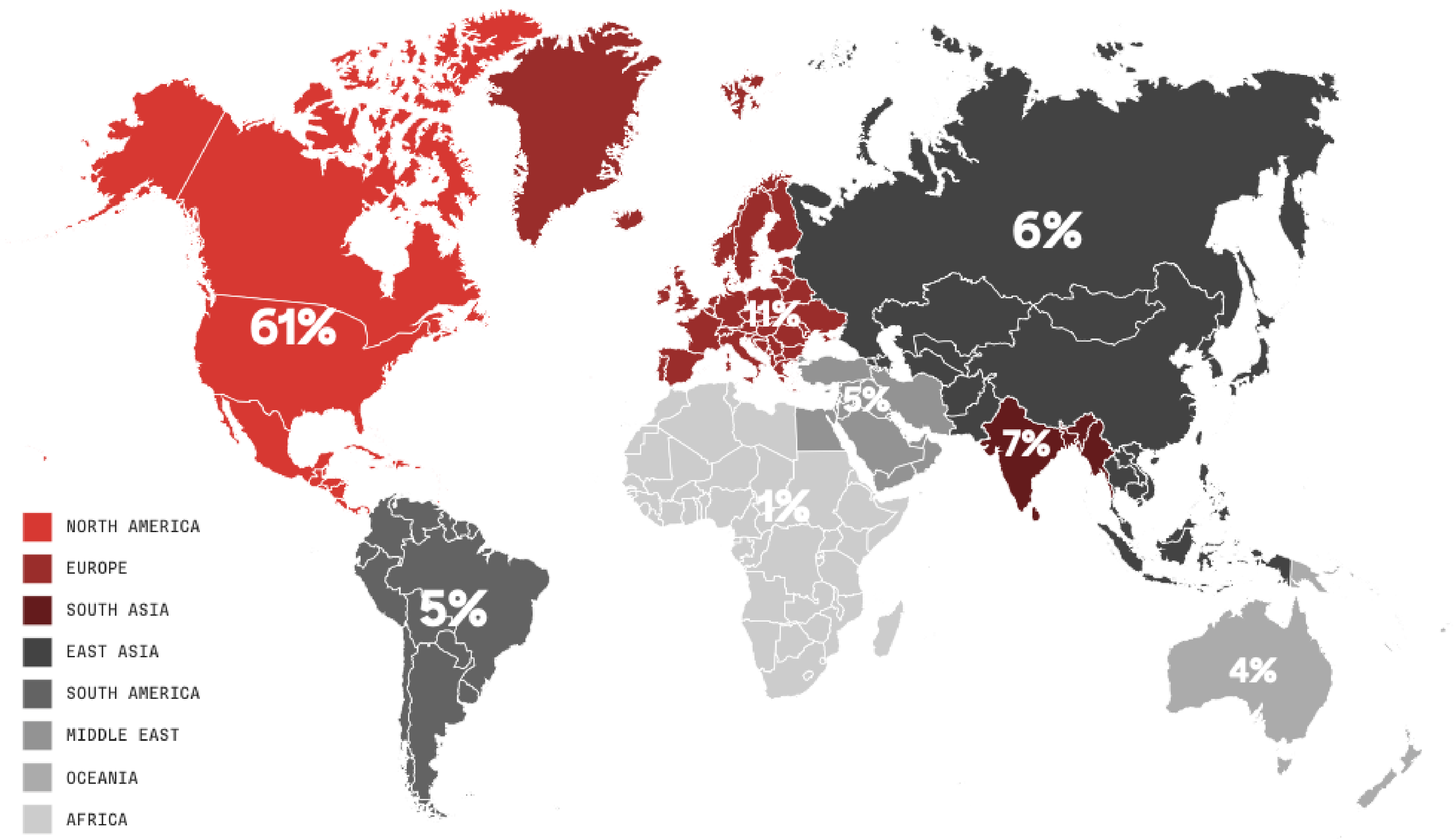
8'0"
7'5"
7'0"
6'5"
6'0"
5'5"
5'0"
4'5"
4'0"
3'5"
C.S. P.D. CROWDSTRIKE GOBLIN PANDA
C.S. P.D. CROWDSTRIKE COZY BEAR
C.S. P.D. CROWDSTRIKE STARDUST CHOLLIMA
C.S. P.D. CROWDSTRIKE HELIX KITTEN
C.S. P.D. CROWDSTRIKE DEEP PANDA
C.S. P.D. CROWDSTRIKE COBALT SPIDER
C.S. P.D. CROWDSTRIKE VENOMOUS BEAR

Malware Free Initial Access

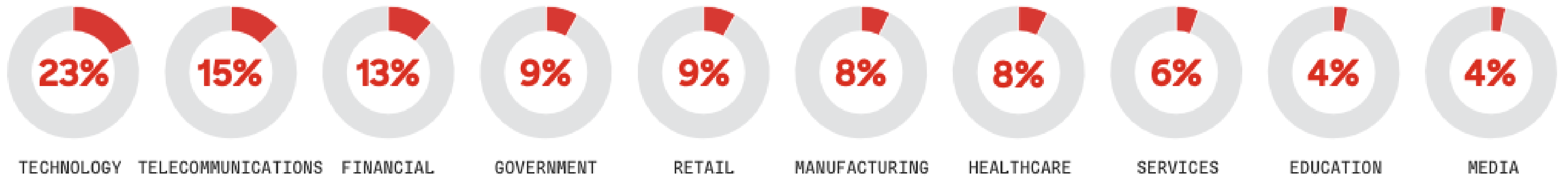
»

75%	2023
71%	2022
62%	2021
51%	2020
40%	2019

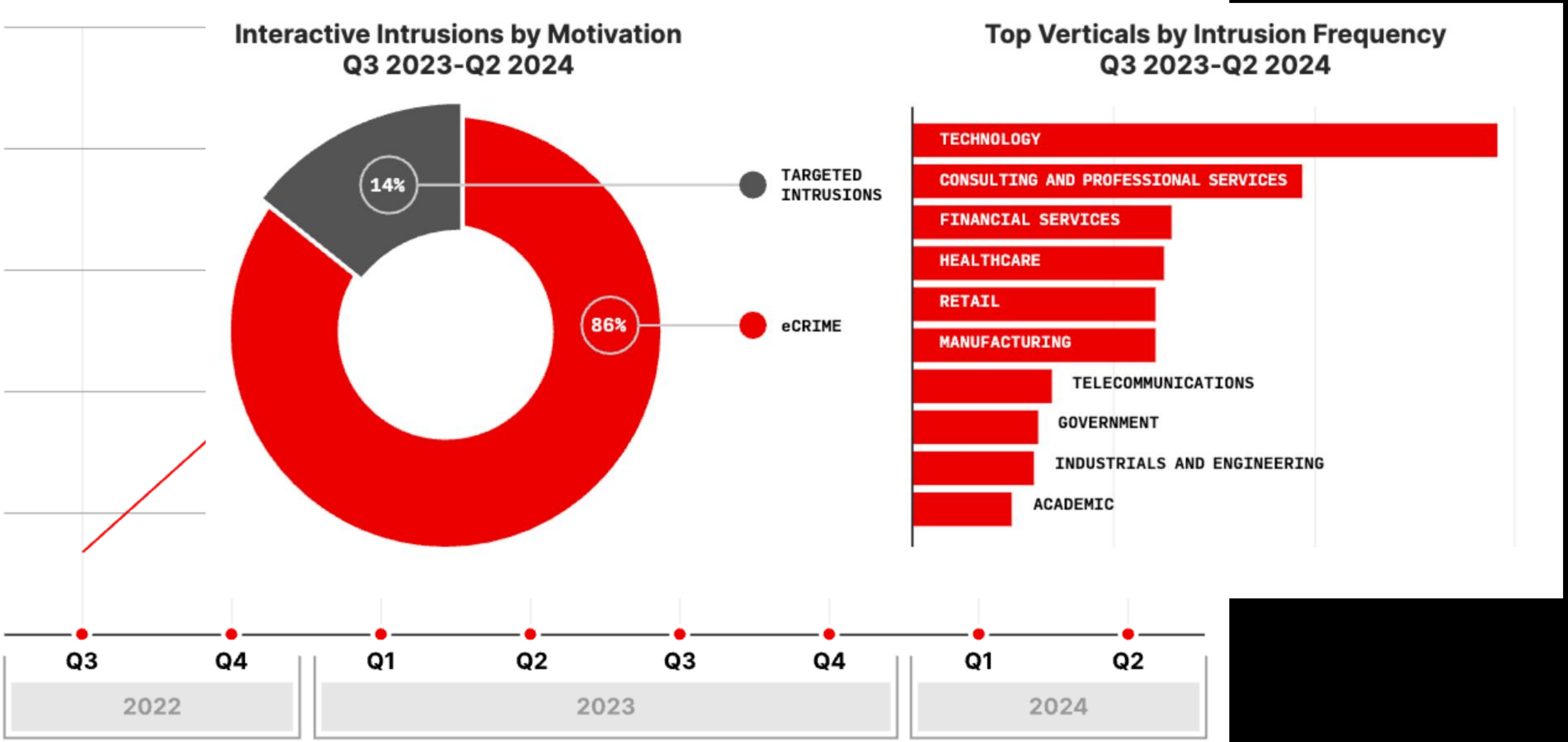
Interactive Intrusions by Region



Interactive Intrusions by Industry

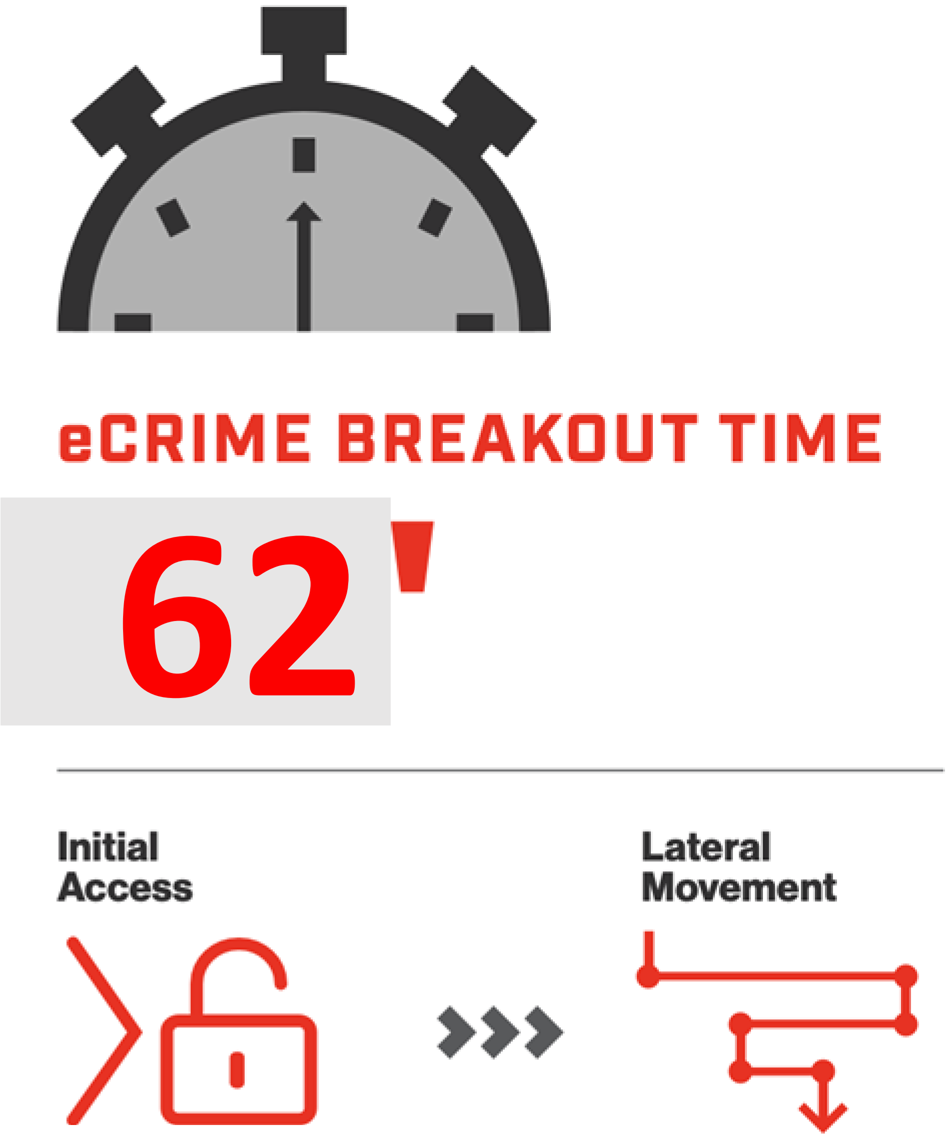


Interactive Intrusions Over Time | Q3 2022-Q2 2024



Interactive Intrusions by Motivation
Q3 2023-Q2 2024

Top Verticals by Intrusion Frequency
Q3 2023-Q2 2024



eCRIME BREAKOUT TIME

62'

Initial Access

Lateral Movement

Adversaries Increasing in Speed and Precision

Defenders must act quickly

To contain the threat and minimize cost and damage, defenders must respond within the breakout time

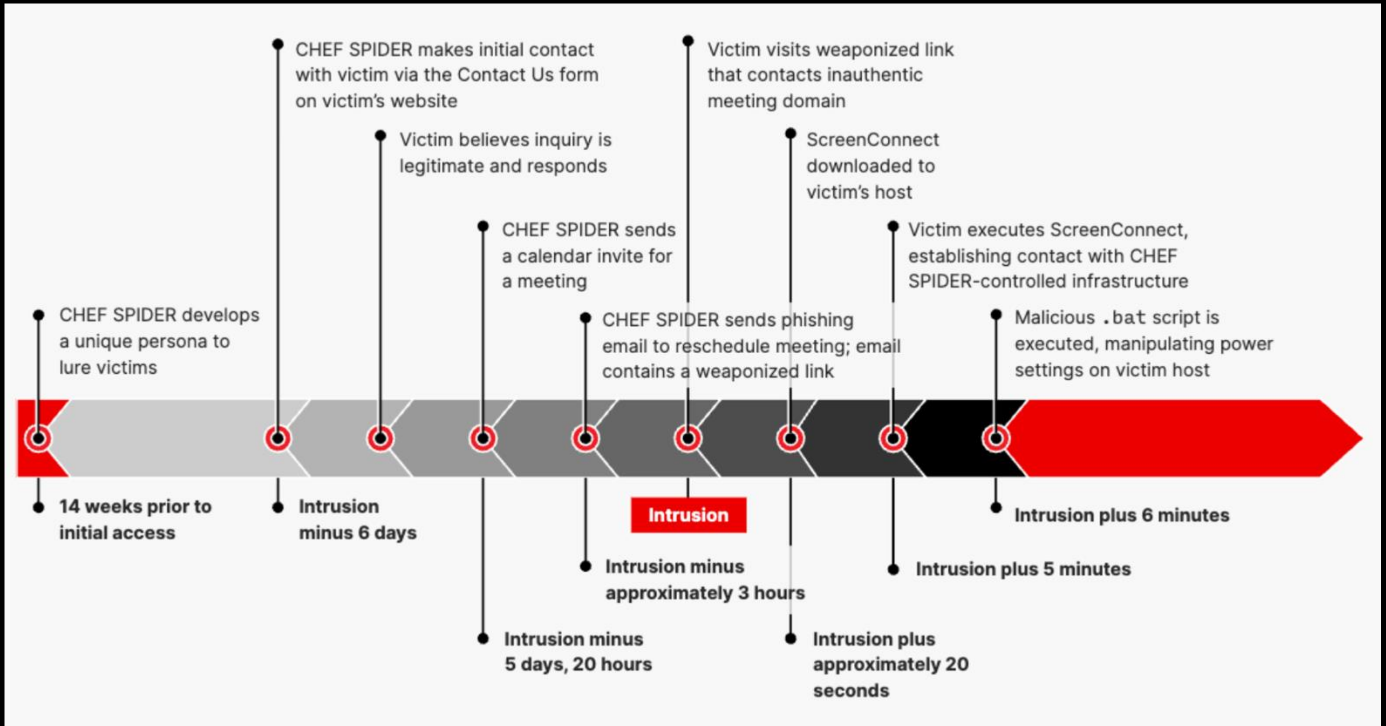
They weaponize YOUR tools and accounts

Adversaries use valid accounts and tools to move laterally, making it nearly impossible to detect abnormal activity and a potential breach

Fastest breakout time: 2 min, 7 sec

Nearly all security teams are not equipped to respond in less than 2 minutes

How about some real examples Robert?



CHEF SPIDER develops a unique persona to lure victims

14 weeks prior to initial access

CHEF SPIDER makes initial contact with victim via the Contact Us form on victim's website

Intrusion minus 6 days

Victim believes inquiry is legitimate and responds

CHEF SPIDER sends a calendar invite for a meeting

Intrusion minus 5 days, 20 hours

CHEF SPIDER sends phishing email to reschedule meeting; email contains a weaponized link

Intrusion minus approximately 3 hours

Victim visits weaponized link that contacts inauthentic meeting domain

Intrusion

ScreenConnect downloaded to victim's host

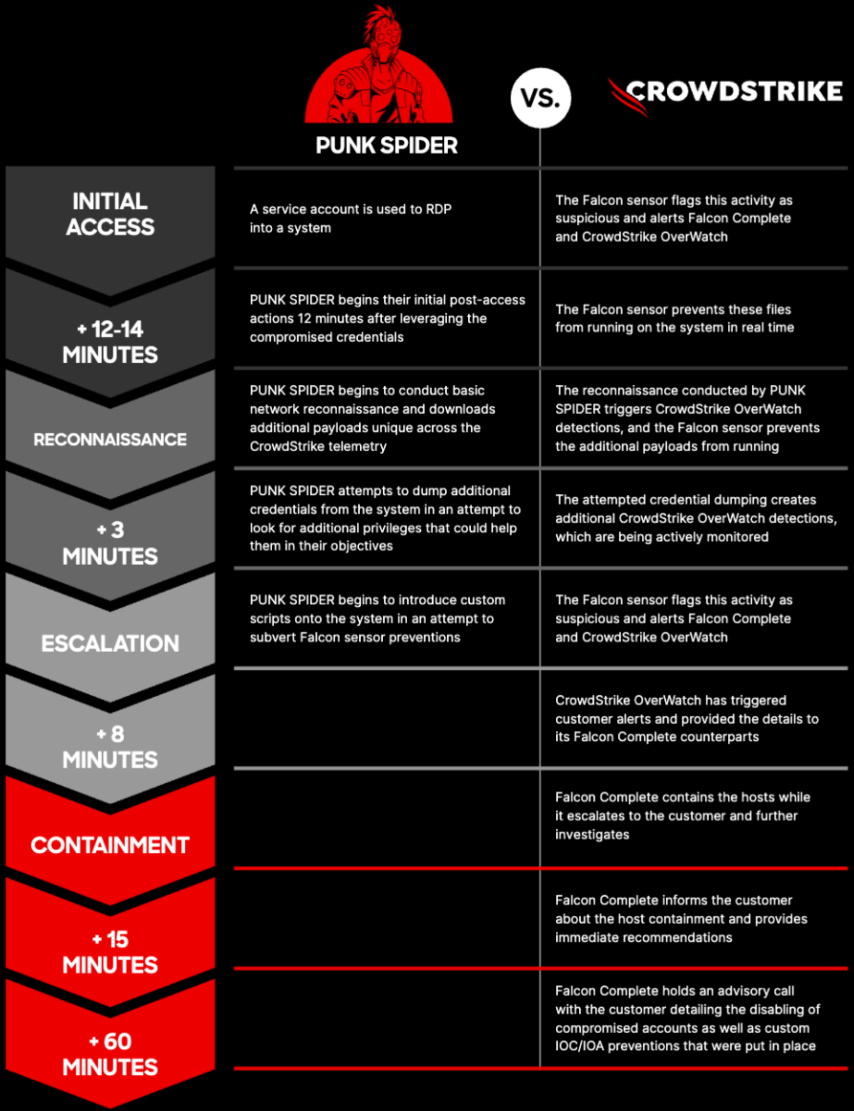
Intrusion plus approximately 20 seconds

Victim executes ScreenConnect, establishing contact with CHEF SPIDER-controlled infrastructure

Intrusion plus 5 minutes

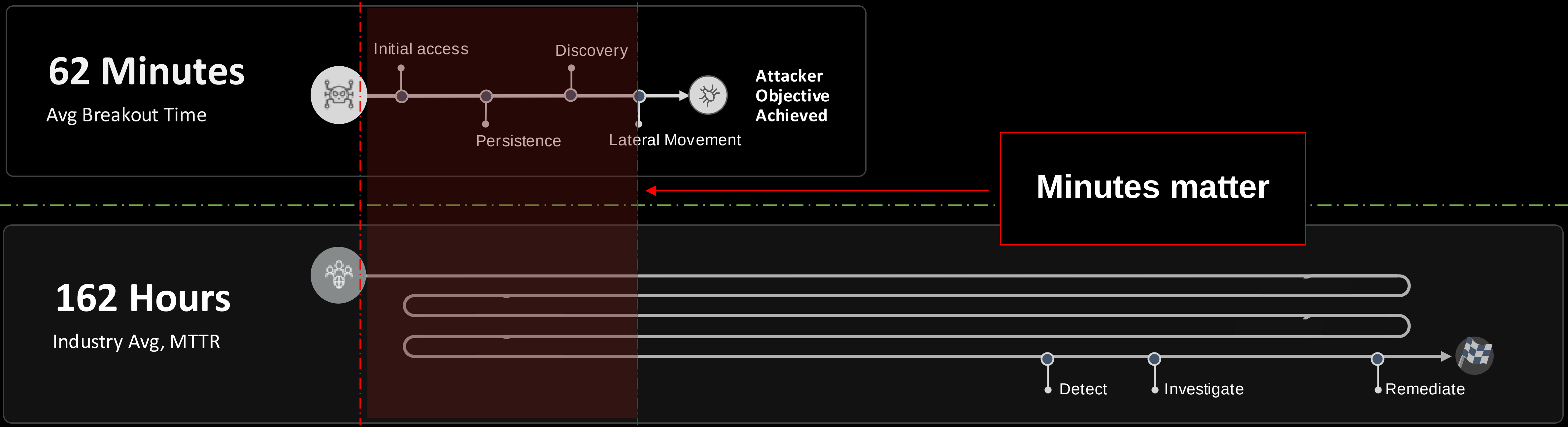
Malicious .bat script is executed, manipulating power settings on victim host

Intrusion plus 6 minutes



	PUNK SPIDER	VS. CROWDSTRIKE
INITIAL ACCESS	A service account is used to RDP into a system	The Falcon sensor flags this activity as suspicious and alerts Falcon Complete and CrowdStrike OverWatch
+ 12-14 MINUTES	PUNK SPIDER begins their initial post-access actions 12 minutes after leveraging the compromised credentials	The Falcon sensor prevents these files from running on the system in real time
RECONNAISSANCE	PUNK SPIDER begins to conduct basic network reconnaissance and downloads additional payloads unique across the CrowdStrike telemetry	The reconnaissance conducted by PUNK SPIDER triggers CrowdStrike OverWatch detections, and the Falcon sensor prevents the additional payloads from running
+ 3 MINUTES	PUNK SPIDER attempts to dump additional credentials from the system in an attempt to look for additional privileges that could help them in their objectives	The attempted credential dumping creates additional CrowdStrike OverWatch detections, which are being actively monitored
ESCALATION	PUNK SPIDER begins to introduce custom scripts onto the system in an attempt to subvert Falcon sensor preventions	The Falcon sensor flags this activity as suspicious and alerts Falcon Complete and CrowdStrike OverWatch
+ 8 MINUTES		CrowdStrike OverWatch has triggered customer alerts and provided the details to its Falcon Complete counterparts
CONTAINMENT		Falcon Complete contains the hosts while it escalates to the customer and further investigates
+ 15 MINUTES		Falcon Complete informs the customer about the host containment and provides immediate recommendations
+ 60 MINUTES		Falcon Complete holds an advisory call with the customer detailing the disabling of compromised accounts as well as custom IOC/IOA preventions that were put in place

Response speed matters



62 Minutes

Avg Breakout Time

Initial access

Discovery

Persistence

Lateral Movement

Attacker Objective Achieved

Minutes matter

162 Hours

Industry Avg, MTTR

Detect

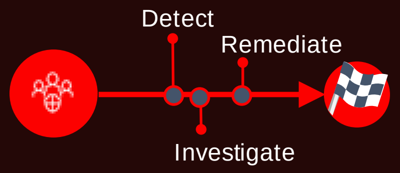
Investigate

Remediate

Beat the fastest adversary at unrivaled speed

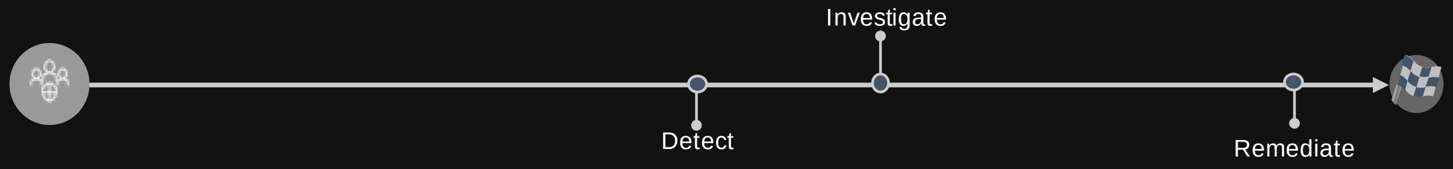
45 minutes

Falcon Complete's mean-time-to-remediate



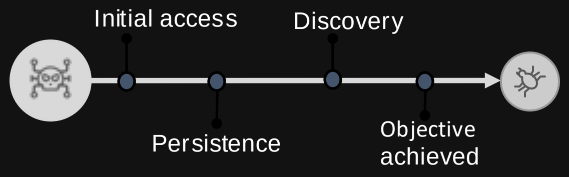
162 hours

Industry average MTTR



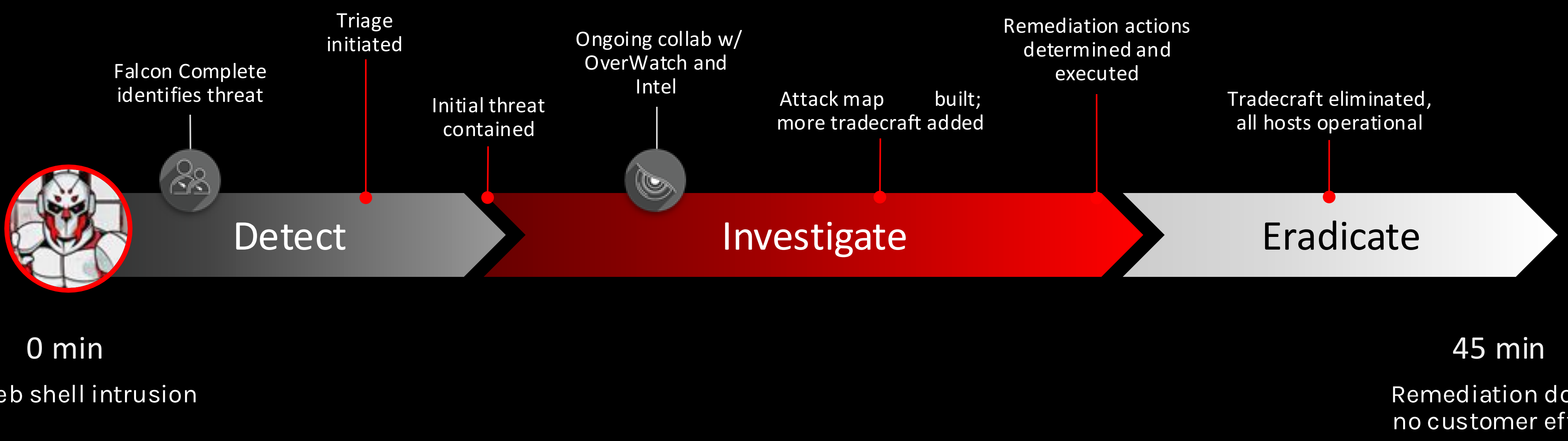
62 minutes

eCrime breakout time



Typical response timeline

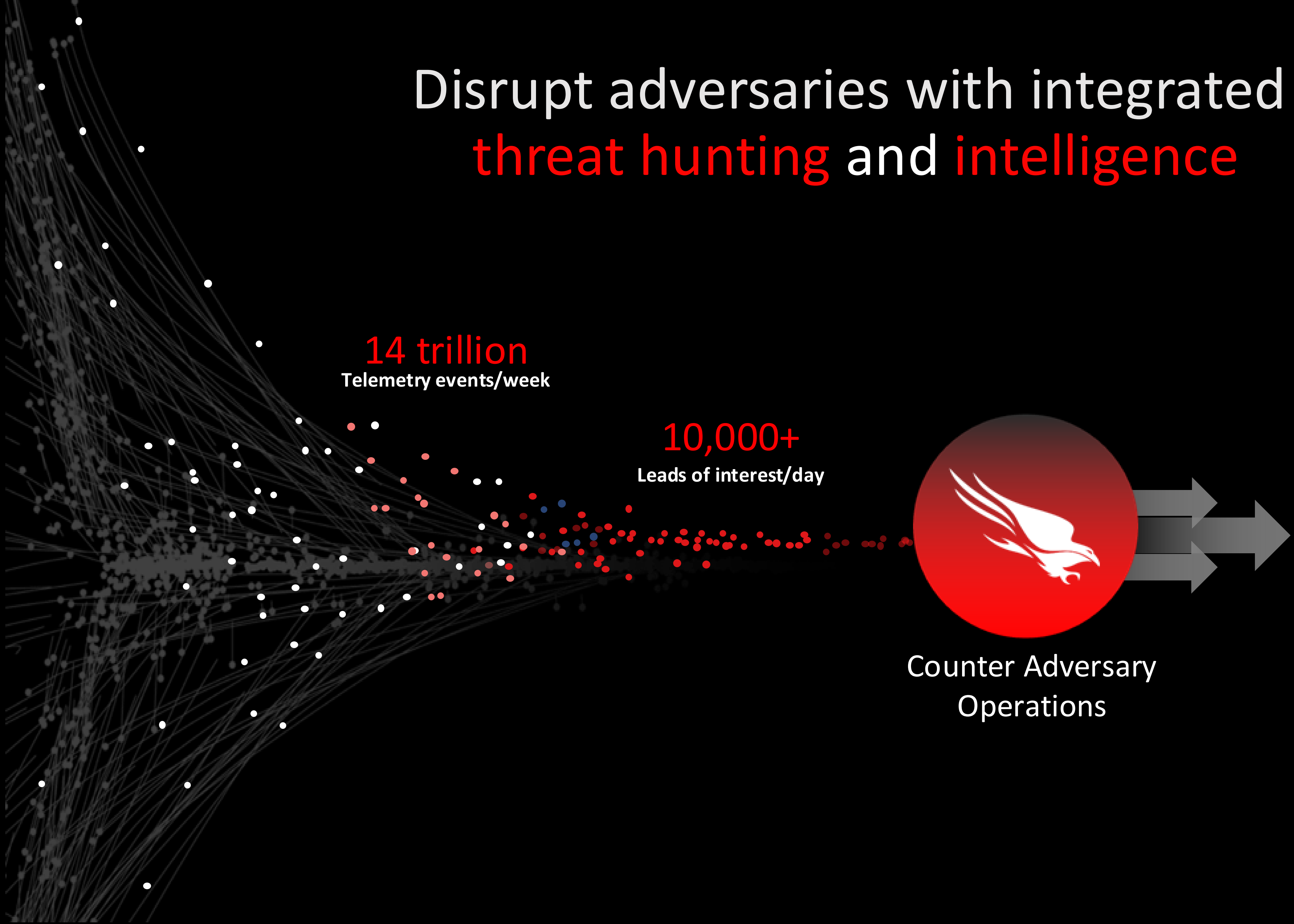
End-to-end delivery with full-cycle remediation


Falcon Complete identifies threat
Triage initiated
Initial threat contained
Ongoing collab w/ OverWatch and Intel
Attack map built; more tradecraft added
Remediation actions determined and executed
Tradecraft eliminated, all hosts operational
Detect
Investigate
Eradicate
0 min
Web shell intrusion
45 min
Remediation done; no customer effort

MTTR

<45 minutes

Disrupt adversaries with integrated threat hunting and intelligence



14 trillion
Telemetry events/week

10,000+
Leads of interest/day

Counter Adversary Operations

240
Adversaries tracked daily

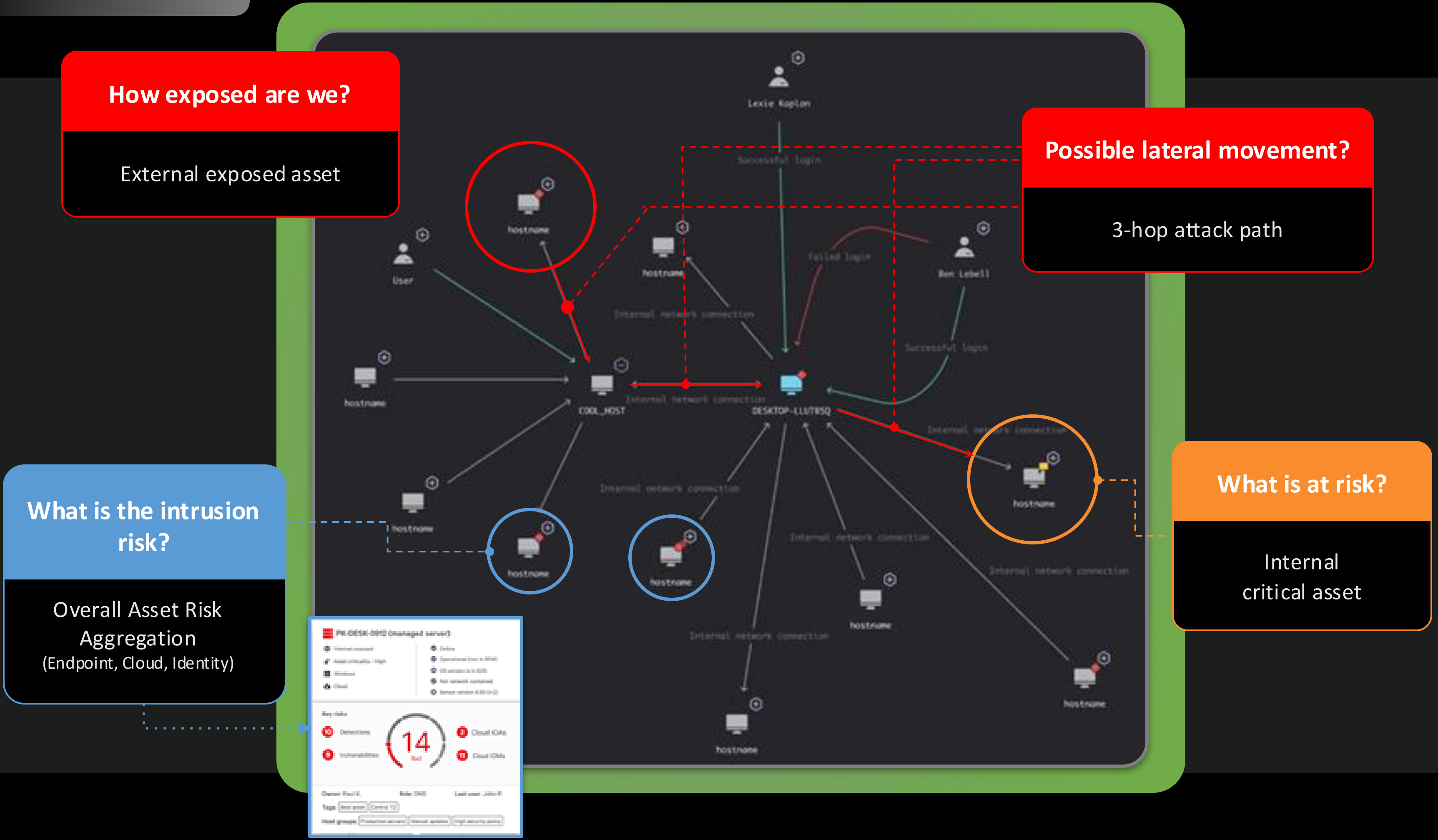
30% YoY

New hunting techniques

200k+
New IOCs published daily

CROWDSTRIKE

Prioritize



How exposed are we?

External exposed asset

Possible lateral movement?

3-hop attack path

What is at risk?

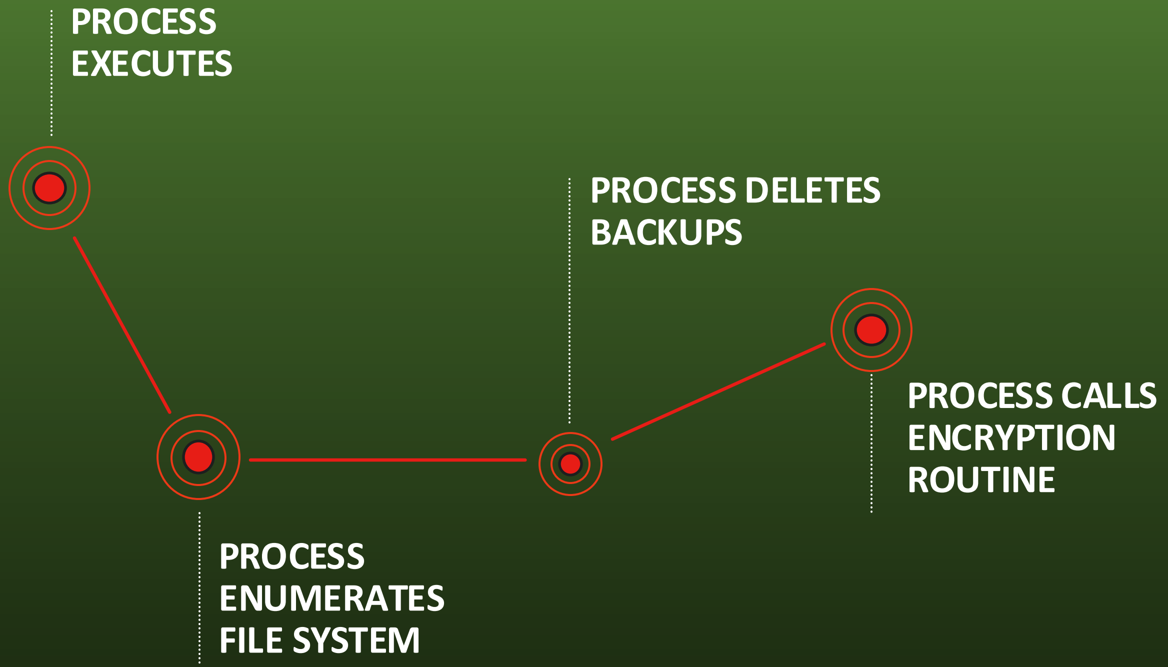
Internal critical asset

What is the intrusion risk?

Overall Asset Risk Aggregation (Endpoint, Cloud, Identity)

- **Visualize intrusion** risk across endpoint, cloud and Identity assets
- **Understand lateral movement** through critical hosts and user accounts
- **Fine-tune policies** and respond with RTR (Real-Time Response) and Falcon® Fusion playbooks
- **Automatically unveil** internet exposures

Indicators of attack (IOA)


PROCESS EXECUTES
PROCESS ENUMERATES FILE SYSTEM
PROCESS DELETES BACKUPS
PROCESS CALLS ENCRYPTION ROUTINE

INDICATORS OF ATTACK

Code Execution, persistence, stealth, command control Lateral Movement

PROACTIVE INDICATORS OF ATTACK

VS

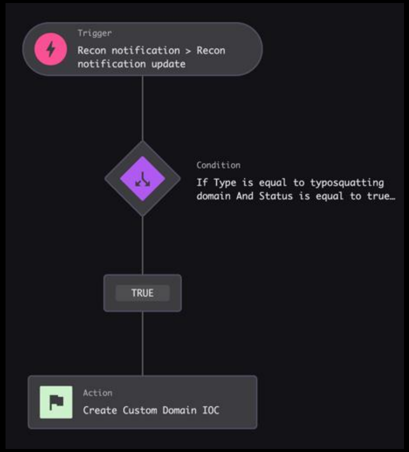
REACTIVE INDICATORS OF COMPROMISE

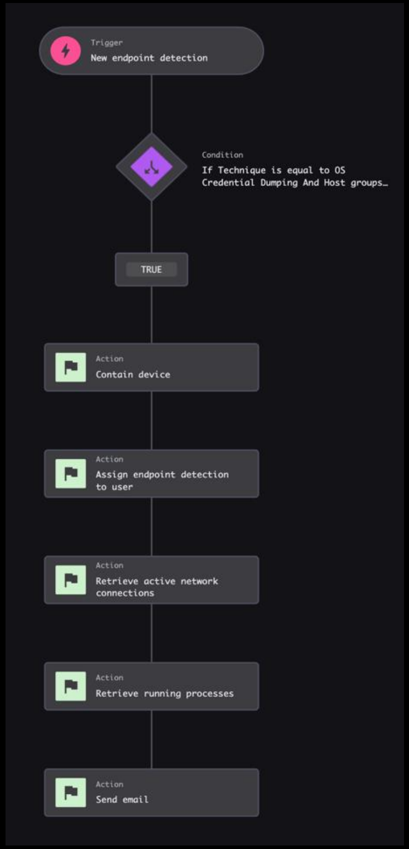
IOCs

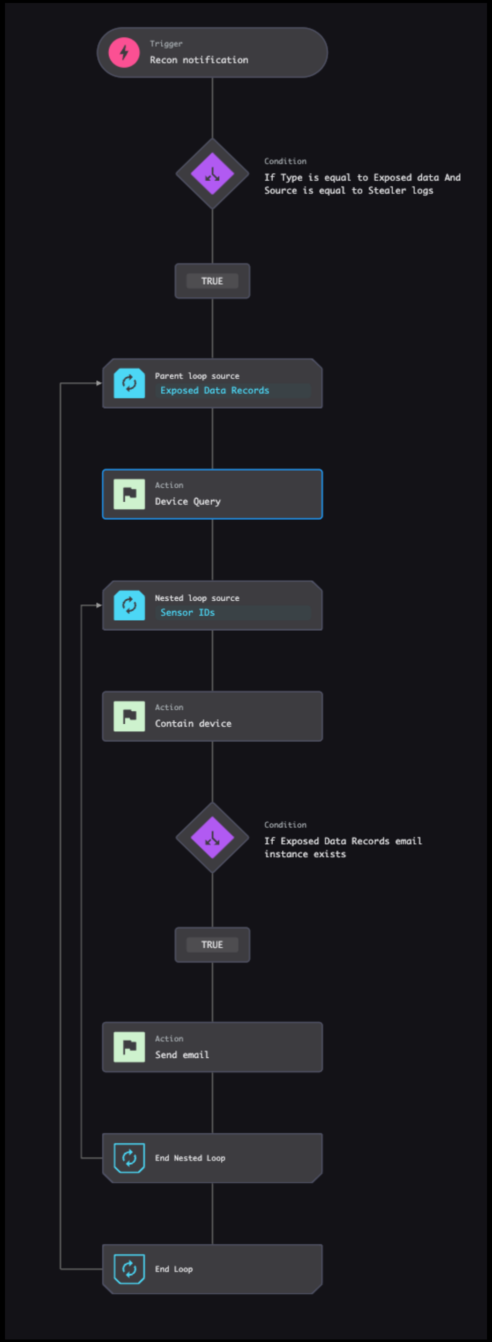
Malware, Signatures, Exploits, Vulnerabilities, IP Addresses

CROWDSTRIKE

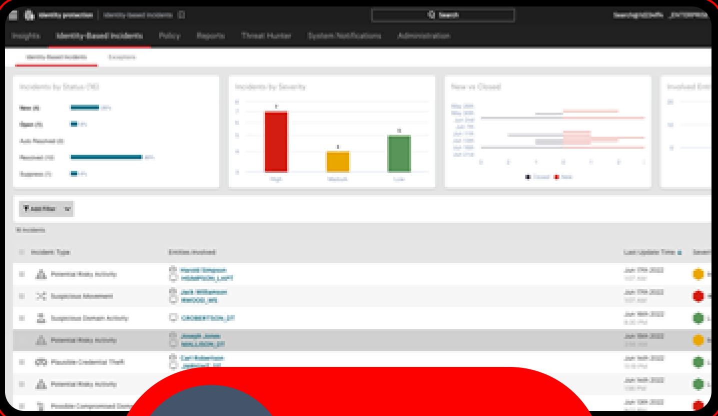
Platform based remediation with built in SOAR


Trigger
Recon notification > Recon notification update
Condition
If Type is equal to typosquatting domain And Status is equal to true…
TRUE
Action
Create Custom Domain IOC


Trigger
New endpoint detection
Condition
If Technique is equal to OS Credential Dumping And Host groups…
TRUE
Action
Contain device
Action
Assign endpoint detection to user
Action
Retrieve active network connections
Action
Retrieve running processes
Action
Send email

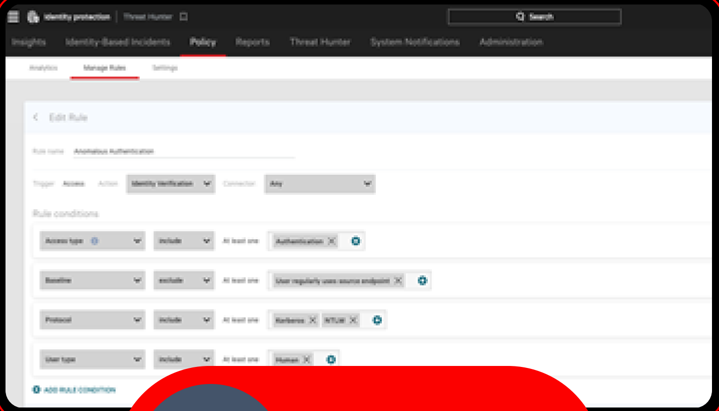


You don’t need to brake in, you can log in



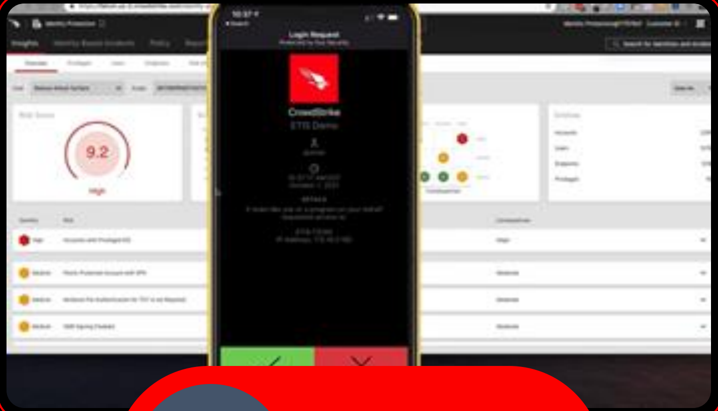
Enhanced
VISIBILITY

Get complete visibility into AD, baseline user behavior and anomalies



Realtime
PROTECTION

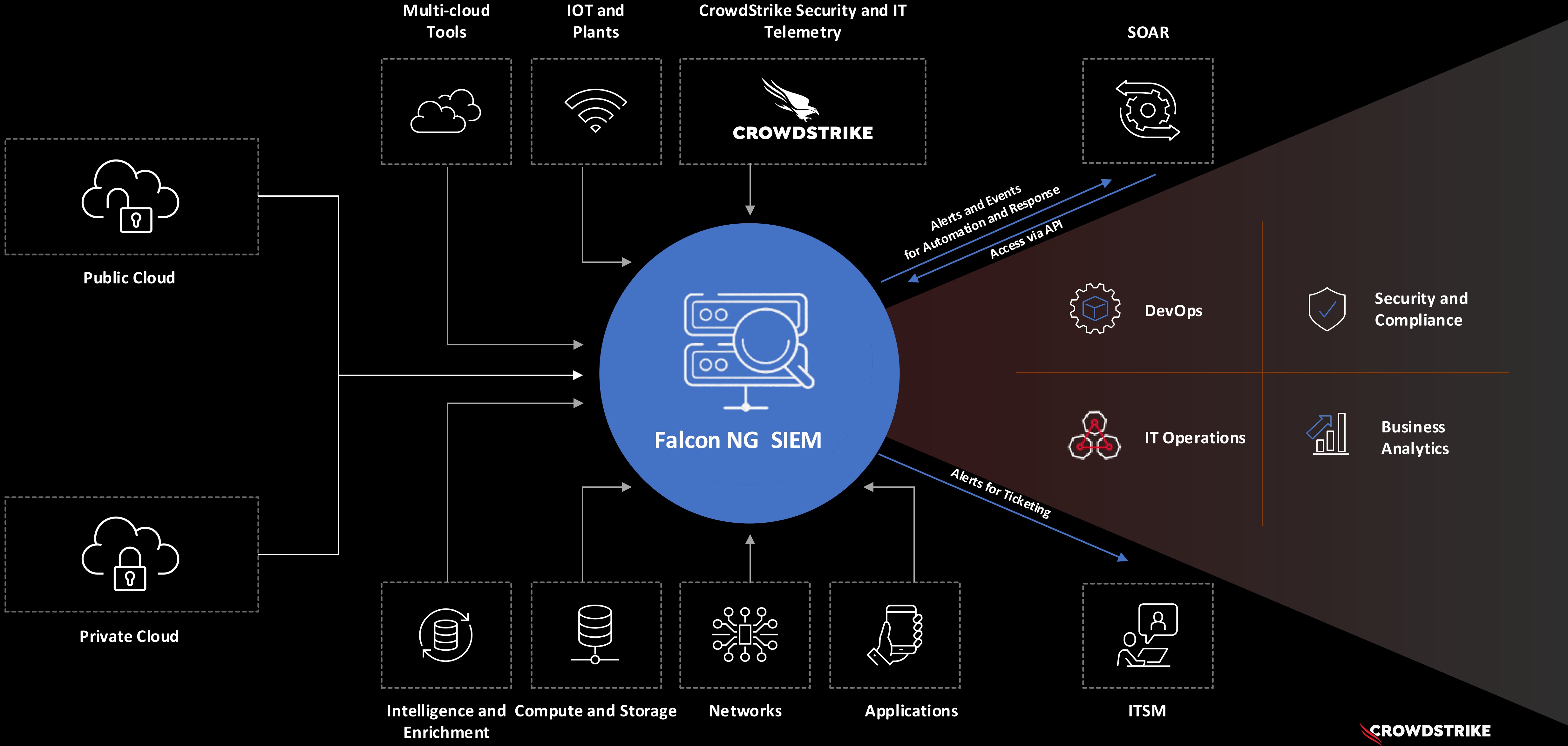
Detect and block identity-based threats in real-time across endpoint and identity



Risk-Based
RESPONSE

Add conditional access with MFA based on user behavior and changes in risk level

Data from your entire estate



CROWDSTRIKE

Ask any question to accelerate investigations

Which threat actors target my industry?

and get fast, actionable answers to stop threats quickly

Thank you.

Robert Michalski
CEE SE Manager
robert.michalski@crowdstrike.com