Elevate Your Game with CrowdStrike and Bring AI Innovation to Your Cloud Detection and Response

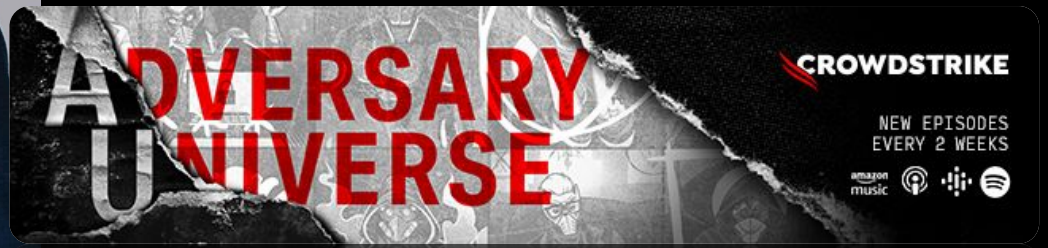
Cristian Rodriguez
Field CTO, Americas, CrowdStrike

CROWDSTRIKE

CRISTIAN RODRIGUEZ

FIELD CTO | AMERICAS

- 20+ years in Cyber
  - CrowdStrike - 10 Years
    - MSSP
    - Global Enterprise
    - Public Sector
    - Healthcare



CROWDSTRIKE

Cloud Threat Landscape

Cloud Attacks Are Leveraging:

- Compromised Identities / Theft of Valid Credentials
- Credential Reset
- MFA Bypass
- Abuse of Public-Facing Applications
- Exploitation of Misconfigurations

To Achieve:

Access to Data

For data extortion or destruction, IP theft, espionage

Access to Compute Resources

For resource hijacking, crypto-mining operations

Access to Other Targets

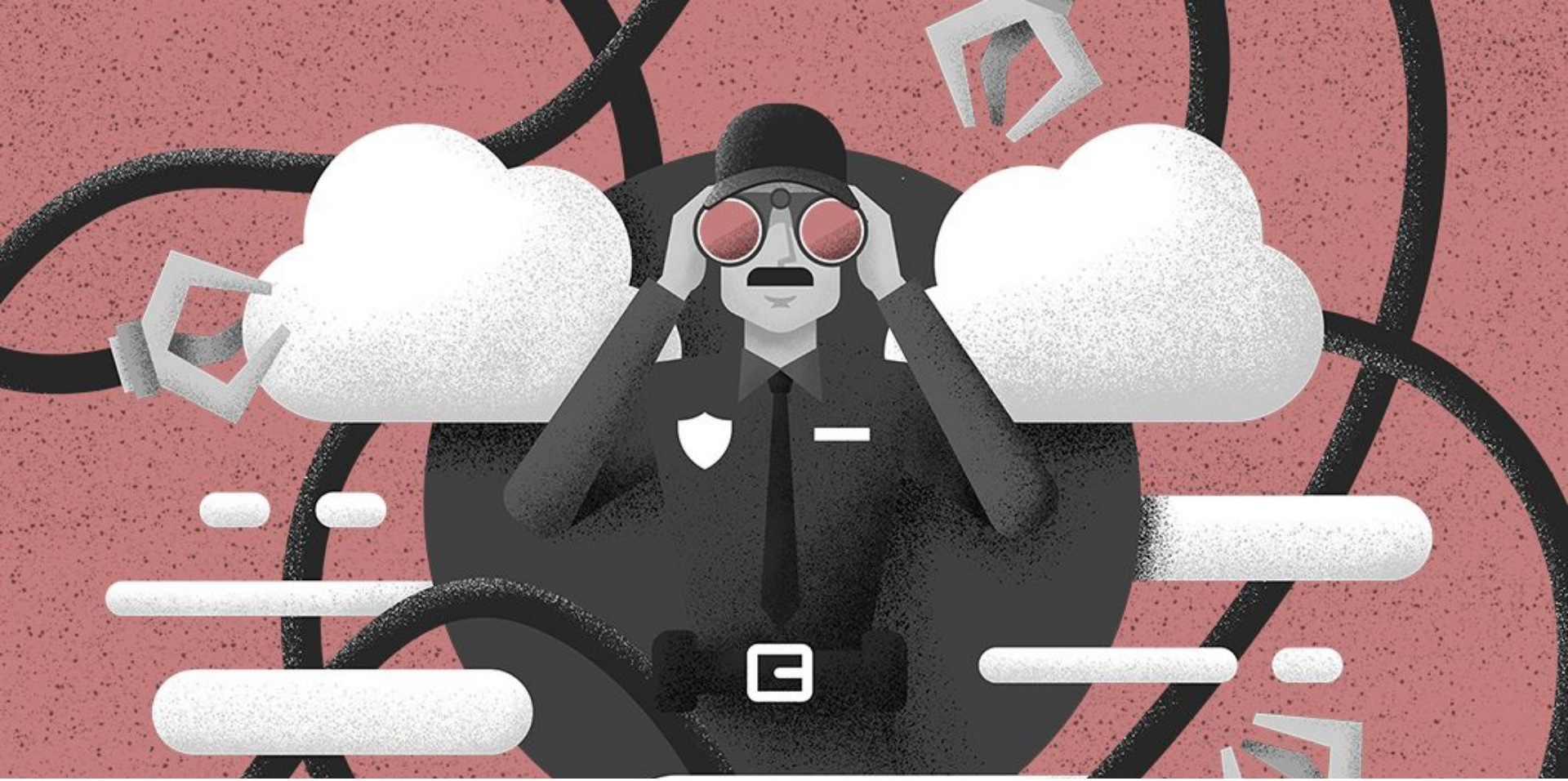
For moving laterally, maintaining stealth, identifying resources (including access to other organizations)

CROWDSTRIKE

Adversaries are learning cloud to better **monetize** their access

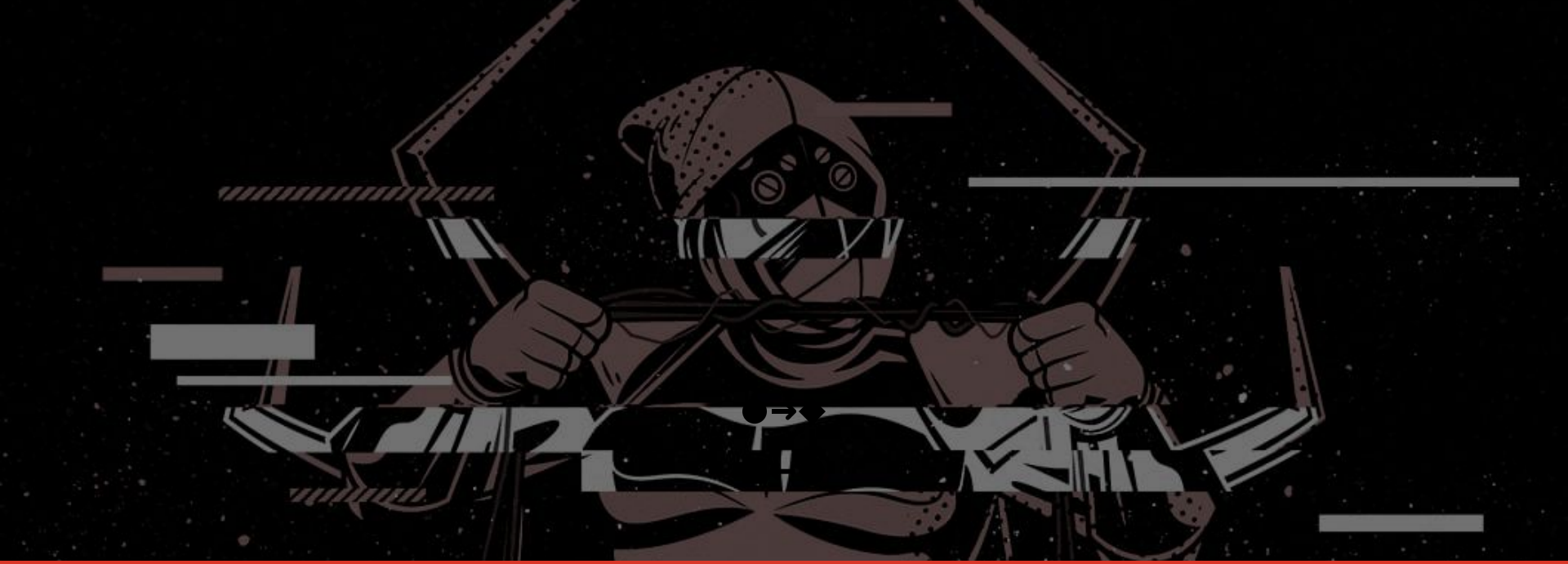

Opportunistic
Resource Hijacking
for…
CRYPTO

They are exploring new TTPs to achieve their objectives



We can learn the most from what has already happened in

CROWDSTRIKE



CLOUD-AGNOSTIC ACTOR

Treats a Cloud Workload simply as another computer

Playbooks are primarily ransomware focused on the host and network layer.

CLOUD-CONSCIOUS ACTOR

Understands the relationship between the CSP's control plane, services, and workload.

Actively attempts to abuse the services of the Cloud Service Provider while having the victim pay for it

SSRF In the Cloud

- Attacker exploits SSRF tricking the EC2 instance into requesting credentials from IMDS
- IMDS returns credentials
- EC2 instance forwards credentials to attacker

→ SSRF Repeatedly observed as initial access vector

→ In 2022, exploiting public facing applications almost as common as having valid

CROWDSTRIKE

Scattered Spider Cloud TTPs

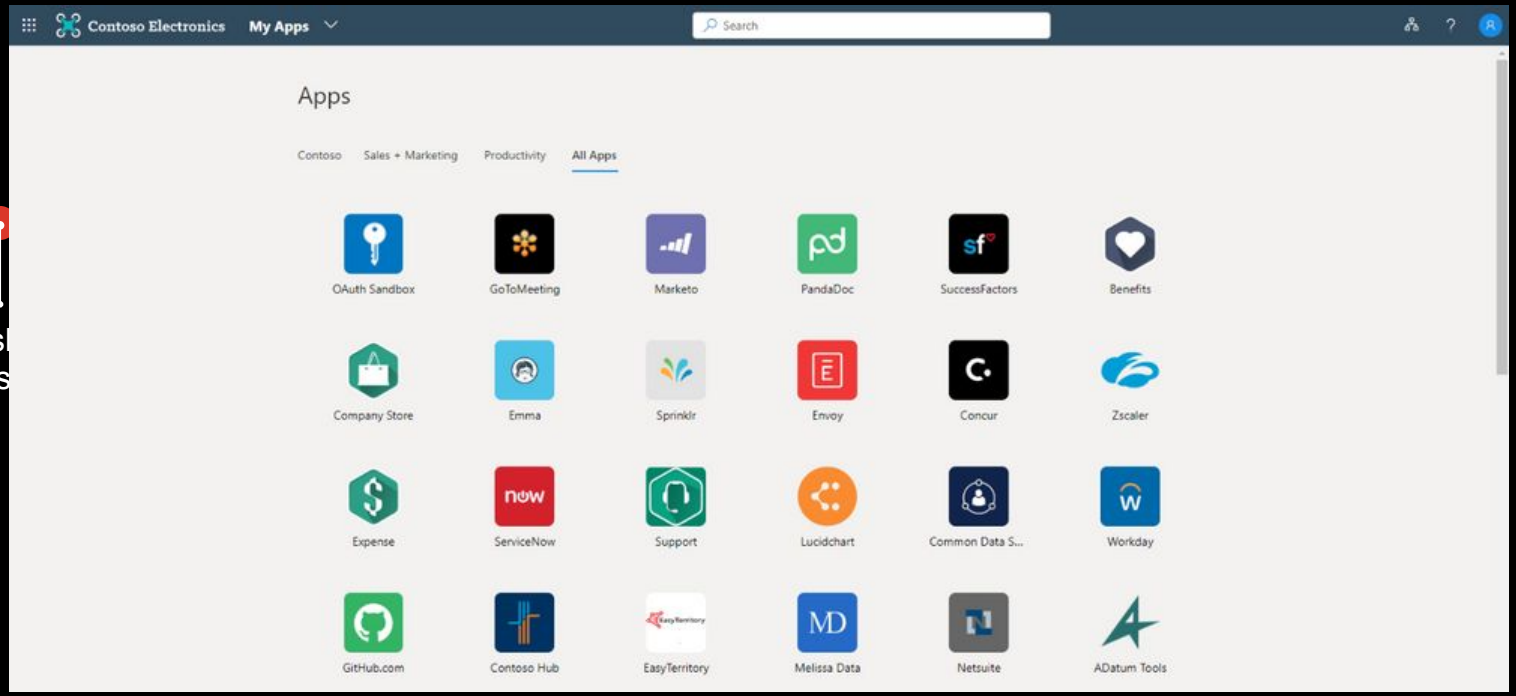
- Data Staging for Exfiltration
- Deployment of Cloud Virtual Machines
- Cloud Native Persistence Mechanisms
- Discovery of connections between cloud environment and on premises

Attack Case : SSRF Exploitation Leads to Data Exfil & Ransom

CROWDSTRIKE

Attack Case: SCATTERED SPIDER's Lateral Movement between Cloud and On-Premise

Smish
Mess



CROWDSTRIKE

Accesses SharePoint

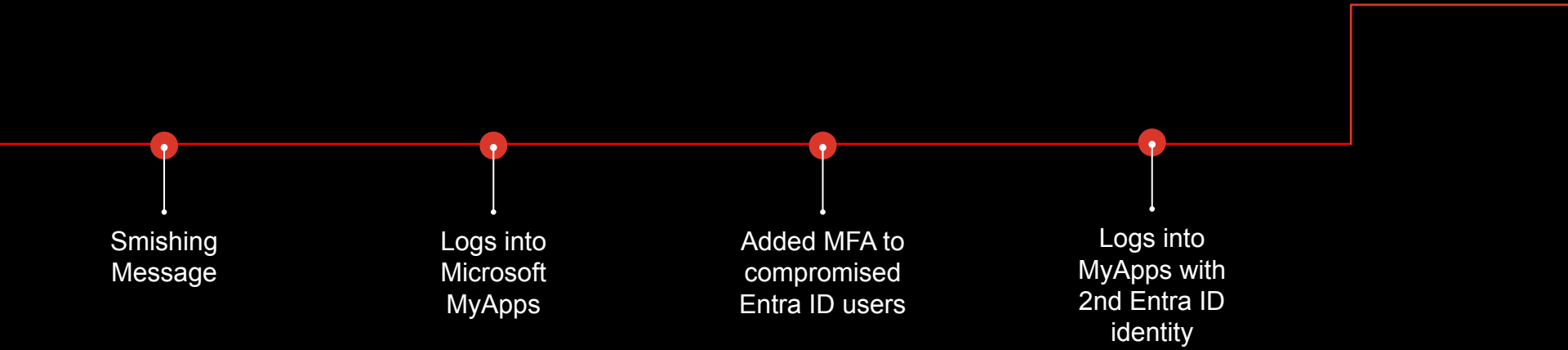
Found VPN Setup documentation

Logs into VPN

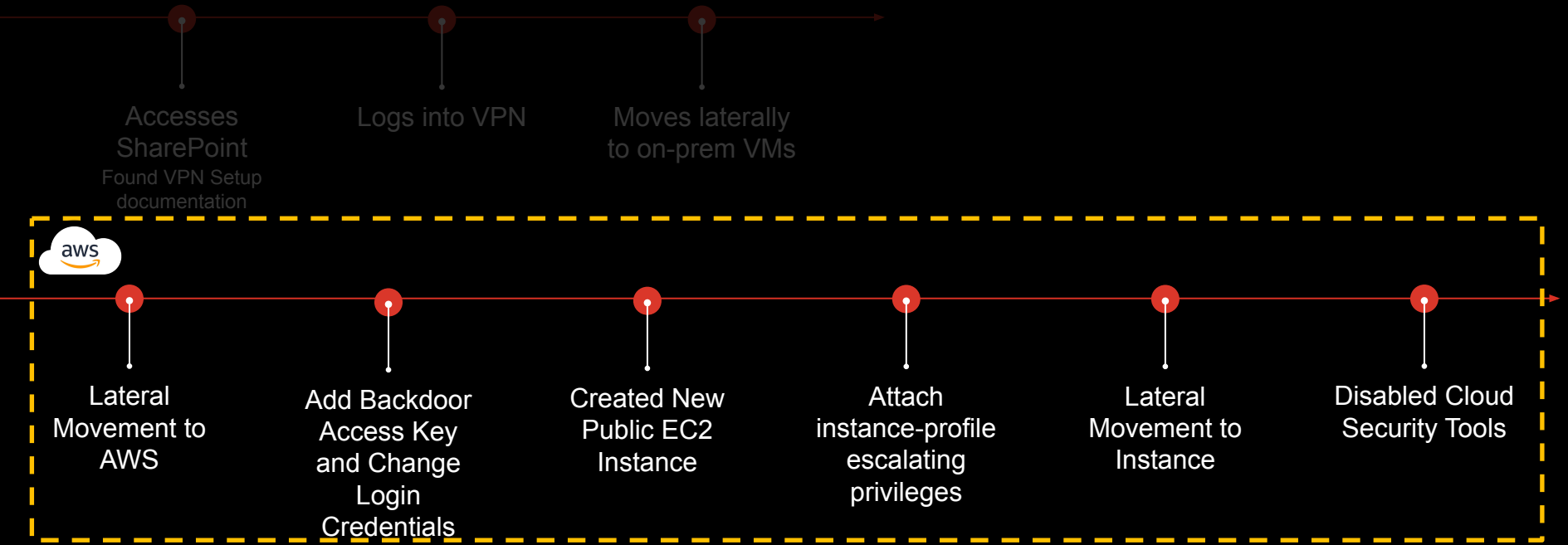
Moves laterally to on-prem VMs

CROWDSTRIKE

Case 3: SCATTERED SPIDER’s Lateral Movement between Cloud and On-Premise



CROWDSTRIKE



CROWDSTRIKE

ADVERSARIES CONTINUE TO DEVELOP CLOUD-CONSCIOUSNESS

75%

Increase in Cloud Exploitation in 2023

110%

Increase in Cloud-Conscious Threat Actors

84%

Of Adversary-Attributed Cloud-Conscious Intrusions Were Focused on eCrime

Source: CrowdStrike 2024 Global Threat Report

CROWDSTRIKE

HOW DOES AI FIT IN

PAIN

- Effective email phishing attacks
- Deep Fakes | Video & Voice
- Autonomous vulnerability exploitation
- Recursive attack cycle enforcement

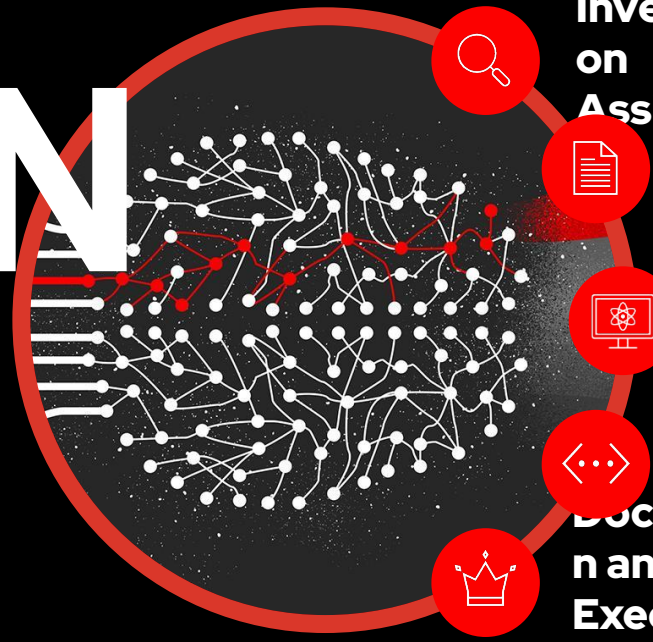
CROWDSTRIKE

TRADITIONAL SOC VS.
AI-AUGMENTED SOC

What would the AI Augmented SOC look like?

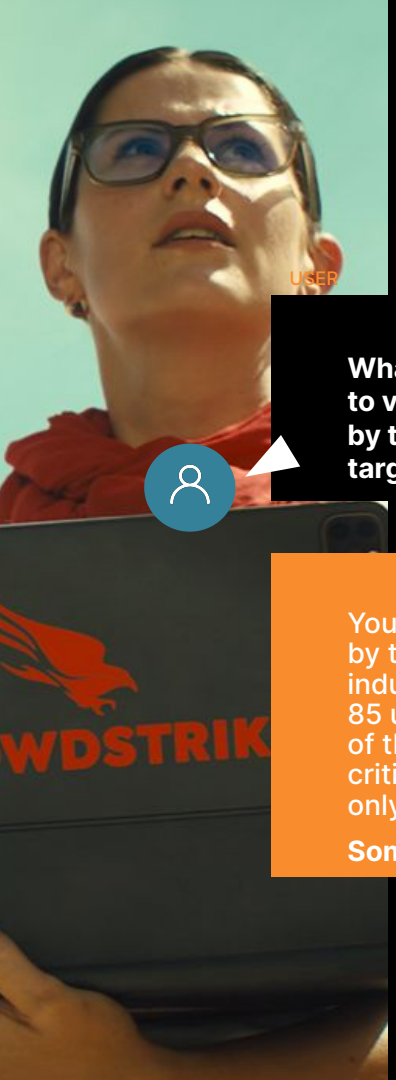
HOW DOES AI FIT IN

GAIN



- Investigation Assistance
- Intelligence Summarization
- Training and Onboarding
- Query Translation
- Documentation and Executive Reporting

CROWDSTRIKE



HOW DOES AI FIT IN

USER

What is my exposure to vulnerabilities used by threat actors who target my industry?

CHARLOTTE AI

Your exposure to vulnerabilities used by threat actors who target the industry technology is represented by 85 unique vulnerabilities. The majority of these vulnerabilities are rated as critical, with a count of 3031, while only two are rated as high.

Some key findings included.

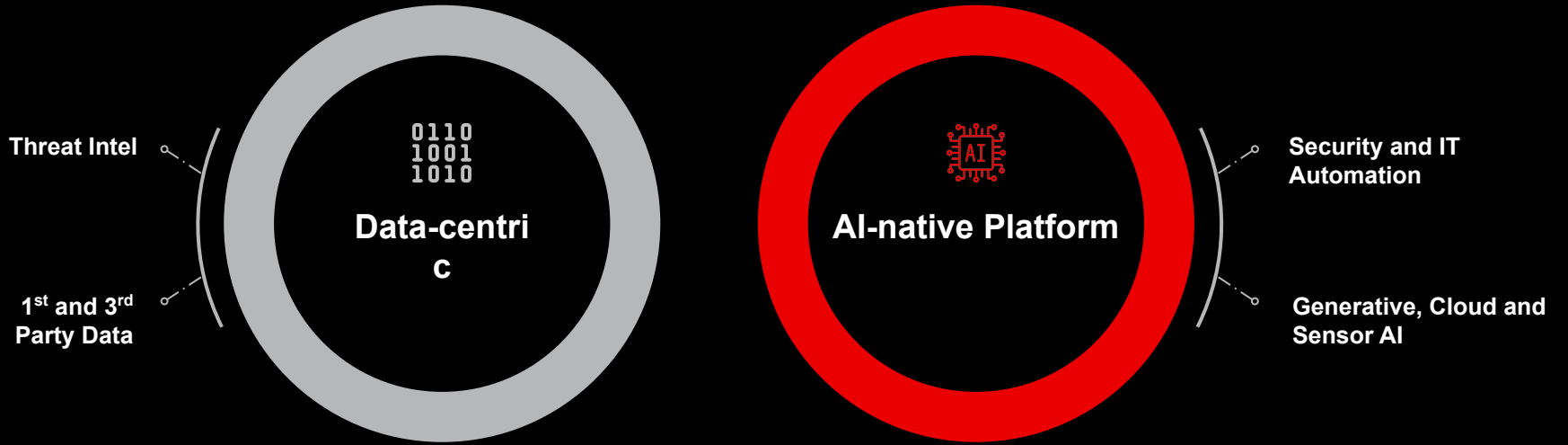
19s
query time

8
API calls

>30min
comparable analyst time for the same query

CROWDSTRIKE

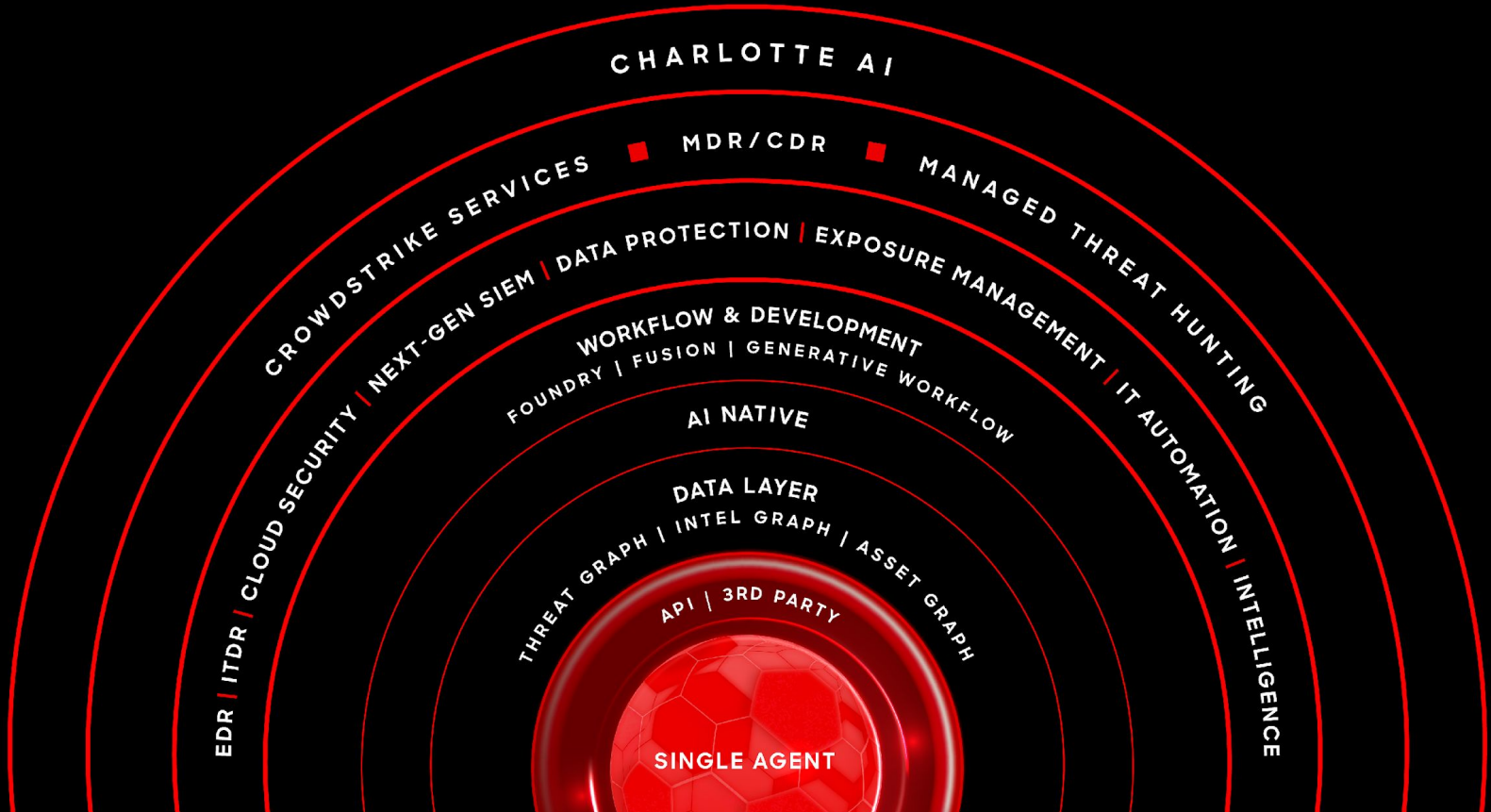
A DATA-CENTRIC PLATFORM APPROACH



CROWDSTRIKE


Thank you

CROWDSTRIKE'S FALCON XDR PLATFORM STOPS BREACHES



RIKE

Scattered Spider TTPs

- Targeted social-engineering
- Bypasses MFA via vishing, MFA notification fatigue, and likely SIM swapping
- Access to victims is primarily used for lateral movement to companies that are customers of the victim
- Changed monetization strategy in January 2023: First allegedly exfiltrating data for ransom, now BGH using the ransomware AlphV
- Novel cloud TTPs