NIS2 als Chance – Verteidigung gegen Ransomware- & KI-Angriffe

Philip Scheidl, Sales Engineer

NIS 2 - are you ready?

- Artikel 21, (1): "… geeignete und verhältnismäßige **technische**, operative und organisatorische **Maßnahmen** ergreifen…"
- Artikel 21, (2), a): "Konzepte in Bezug auf **Risikoanalyse und Sicherheit für Informationssysteme**"
- Artikel 21, (2), b): "Bewältigung von Sicherheitsvorfällen"
- Artikel 21, (2), e): "**Sicherheit der Lieferkette**…"
- Artikel 21, (2), f): "Konzepte und Verfahren zur **Bewertung der Wirksamkeit von Risikomanagementmaßnahmen**…"
- Artikel 21, (3): "Die spezifischen Schwachstellen der **einzelnen unmittelbaren Anbieter und Dienstanbieter** […] berücksichtigen"

UNDERSTANDING
THE THREAT LANDSCAPE

Motivations

NATION STATE

ECRIME

HACKTIVISM

Nation State Goals

CHINA

ECONOMIC ESPIONAGE
INTELLIGENCE COLLECTION

North Korea

CURRENCY GENERATION
ECONOMIC ESPIONAGE

IRAN

GEOPOLITICAL CAMPAIGNS
TELECOM FOCUSED

RUSSIA

INFORMATION OPERATIONS
CRITICAL INFRASTRUCTURE

Sophisticated & Symbiotic E-Crime Ecosystem

SERVICES

CAPABILITIES ENABLING CYBER CRIMINAL ACTIVITY

DISTRIBUTION

VEHICLES LEVERAGED FOR DELIVERING TO VICTIMS

MONETIZATION

CAPITALIZING ON SUCCESSFUL EXECUTION

(Generative) AI

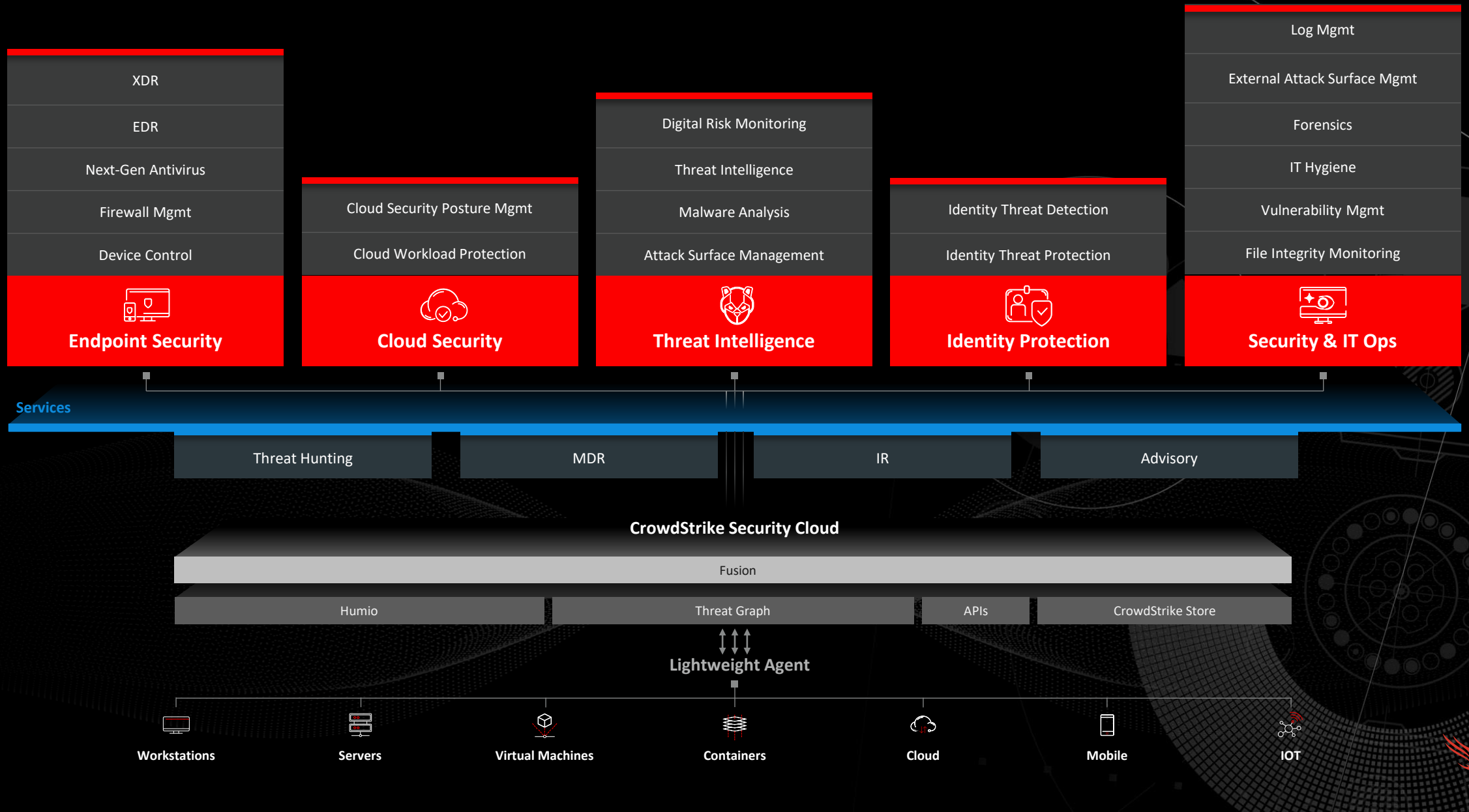
- Social Engineering
- Malware Variants
- Faster Coding
- Deep Fakes

UNDERSTANDING & DEFEND

YOUR ENTERPRISE

CROWDSTRIKE

THE FALCON PLATFORM



DELIVERED VIA ONE AGENT
THAT REPLACES DOZENS OF POINT PRODUCTS

Falcon Agent

Prevent • Predict • Detect • Respond

- **Lightweight**
- **Zero reboots**
- **Superior user experience**

Endpoints

Workstations | Mobile | Servers | IOT

Clouds

Data Centers | Workloads | Containers

Red Hat · Google Cloud · Microsoft Azure · ORACLE · amazon web services · aws · docker

Identities

Active Directory | User Accounts | 3rd Parties

CROWDSTRIKE

XDR @ CROWDSTRIKE

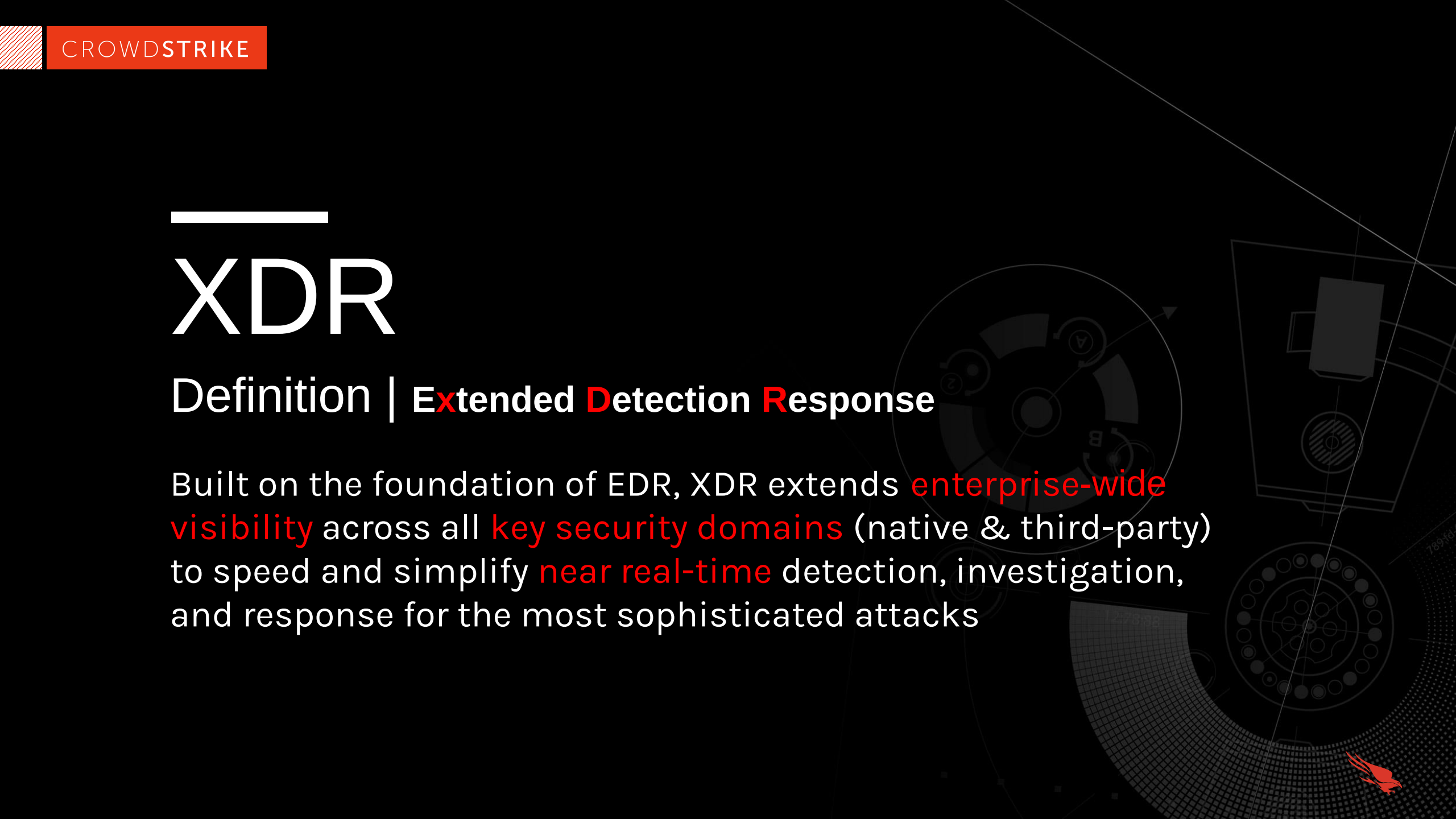
ENTERPRISE-WIDE VISIBILITY ACROSS ALL KEY SECURITY DOMAINS

CROWDSTRIKE

XDR

Definition | **Extended Detection Response**

Built on the foundation of EDR, XDR extends enterprise-wide visibility across all key security domains (native & third-party) to speed and simplify near real-time detection, investigation, and response for the most sophisticated attacks



CROWDSTRIKE

UNIFY SIGNALS TO FIND THE MOST SOPHISTICATED ATTACKS ACROSS THE ENTERPRISE

Ingest

Endpoint

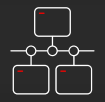
Identity

Cloud

Web

CASB

Email



Network

Firewall

Analyze

Parse

Normalize

Map to Schema

Enrich with telemetry & threat intel

Advanced analytics

Correlate

Action

Identify: Custom & CrowdStrike created detections

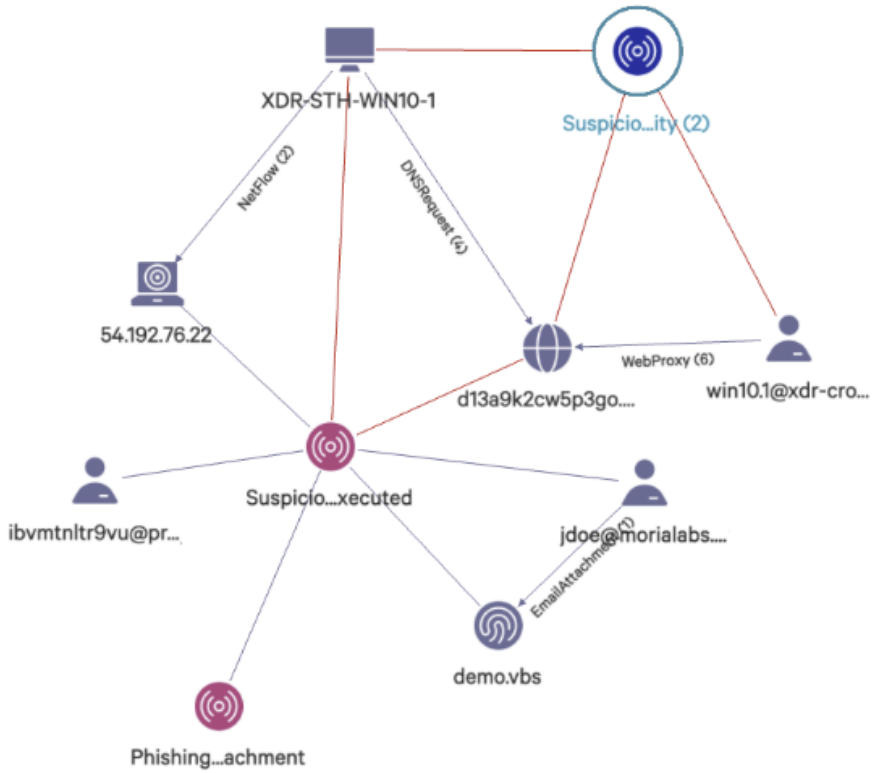
Orient: Native cross-domain graph explorer

Hunt: Unified cross-domain investigations

Respond: Surgical response for native & third-party tools

Automate: Native SOAR automates repetitive tasks

CROWDSTRIKE



Suspicious Web Proxy Allowed Activity (2)

Web indicator

Event time
Oct. 27, 2022 03:18:51

Log source
Zscaler

Tactic & technique
Command and Control via Application Layer Protocol

Domain
Web

Description
Suspicious allowed web proxy activity observed.

Source IP
172.17.0.26

Destination IP
18.65.229.61

Action
Allowed

ApplicationClass
General Browsing

ApplicationName
General Browsing

ContentType
Other

DataDomain
Web

EventID
95

HTTPRequestMethod
CONNECT

HTTPResponseCode
200

MalwareCategory
None

MalwareClass
None

Product
XDR

Protocol
HTTP_PROXY

Reason
Allowed

RefererURL
None

RemoteAddressIP4
18.65.229.61

RemoteHostname
d13a9k2cw5p3go.cloudfront.net

CROWDSTRIKE

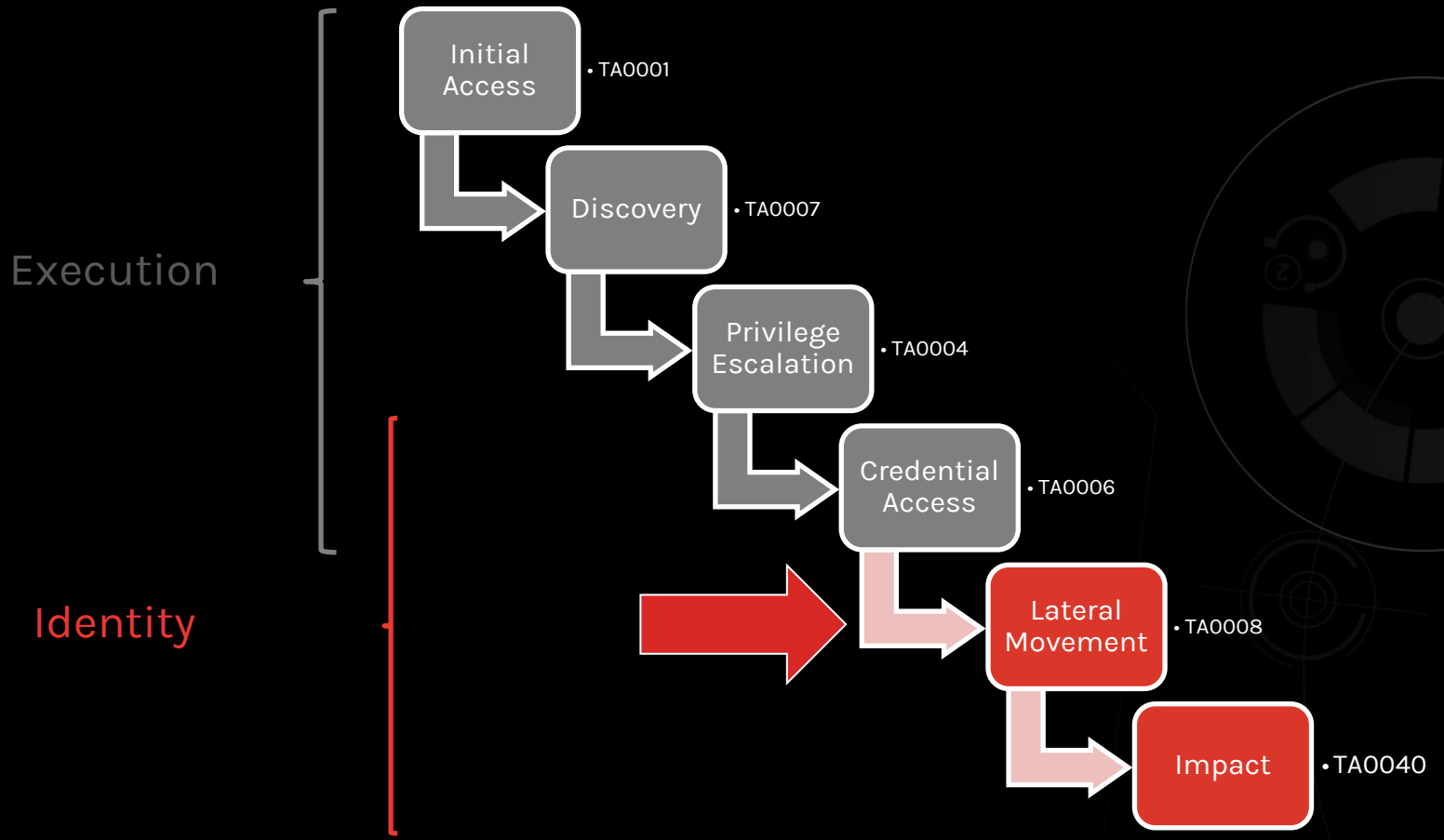
RANSOMWARE & NIS2 – IDENTITIES

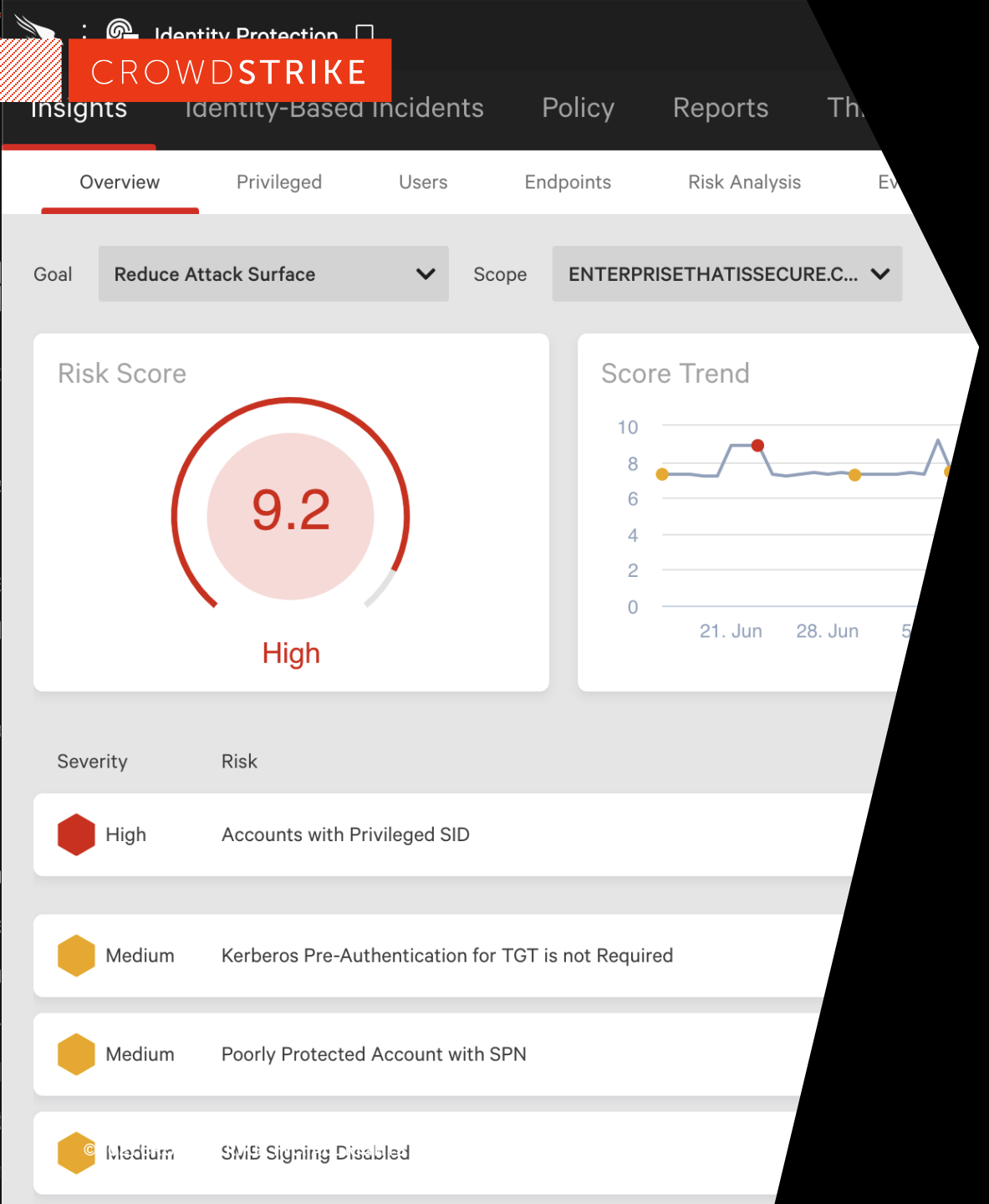
“80% OF DATA BREACHES HAVE A CONNECTION TO COMPROMISED PRIVILEGED CREDENTIALS”

- FORRESTER RESEARCH

CROWDSTRIKE

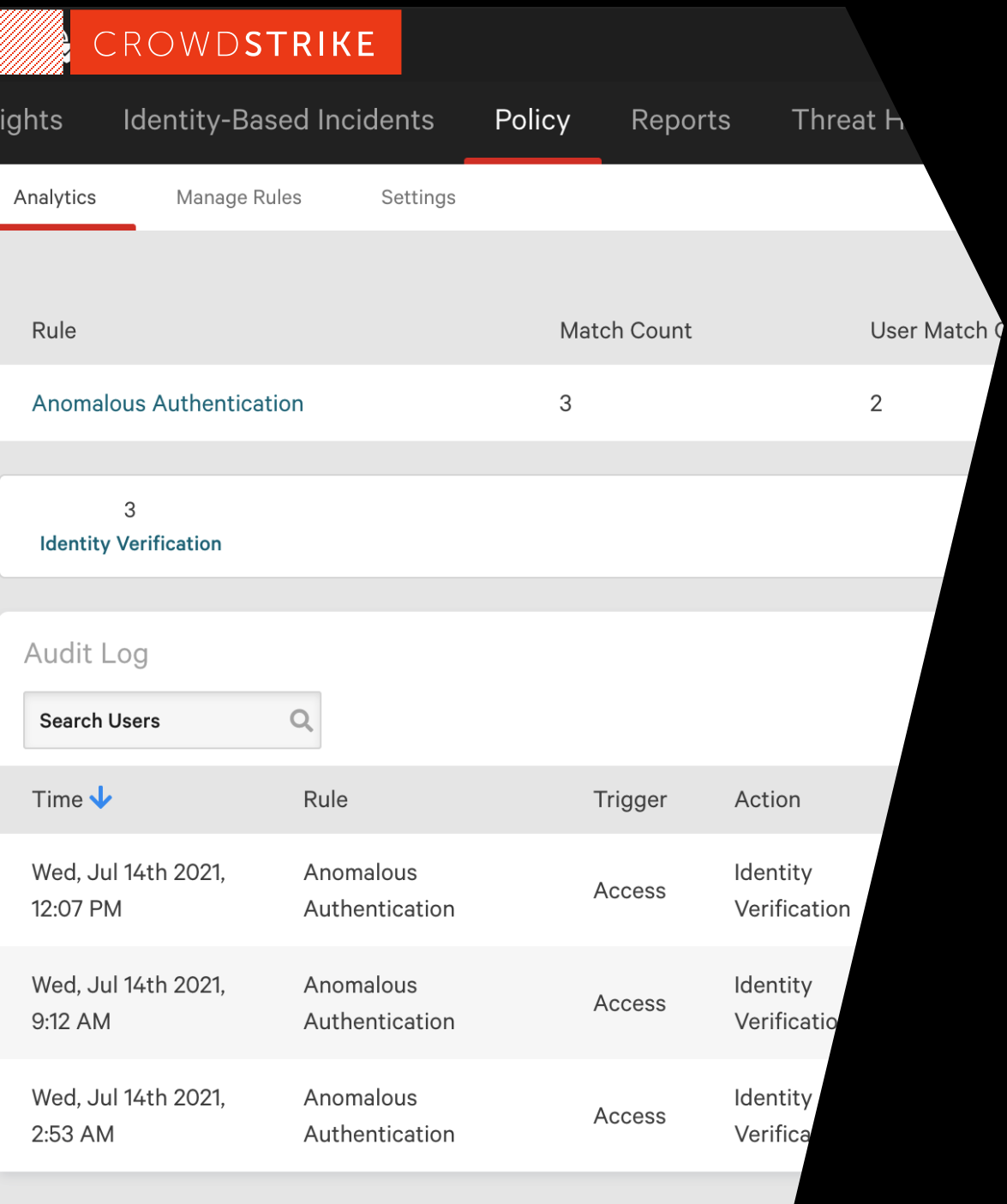
OFTEN, THEY ARE STARTING HERE





FALCON IDENTITY THREAT DETECTION

- Understand what privileged accounts exist
- Understand where privileged accounts are used
- Identify service accounts
- Identify stale accounts
- Assess the risk associated with accounts
- Assess risk associated with account usage
- Identity store stitching and correlation



FALCON IDENTITY THREAT PROTECTION

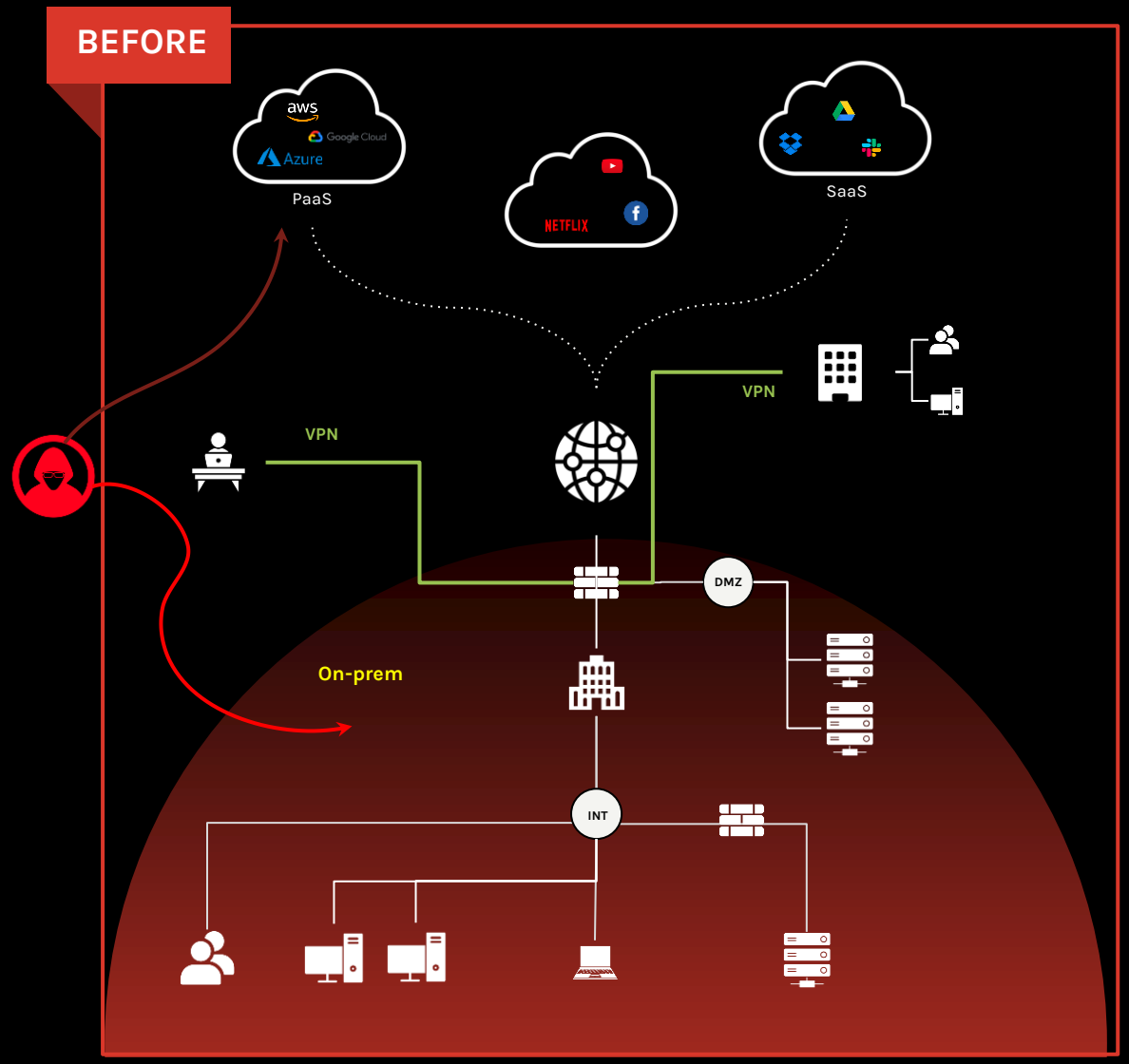
- Trust... and verify
- Automatically enforce conditional access on anomalous activity
- Create bespoke rules that allow, block, or challenge high-risk identity activity
- Integrate with current identity stores for a zero-friction end-user experience
- Stop adversaries in their tracks

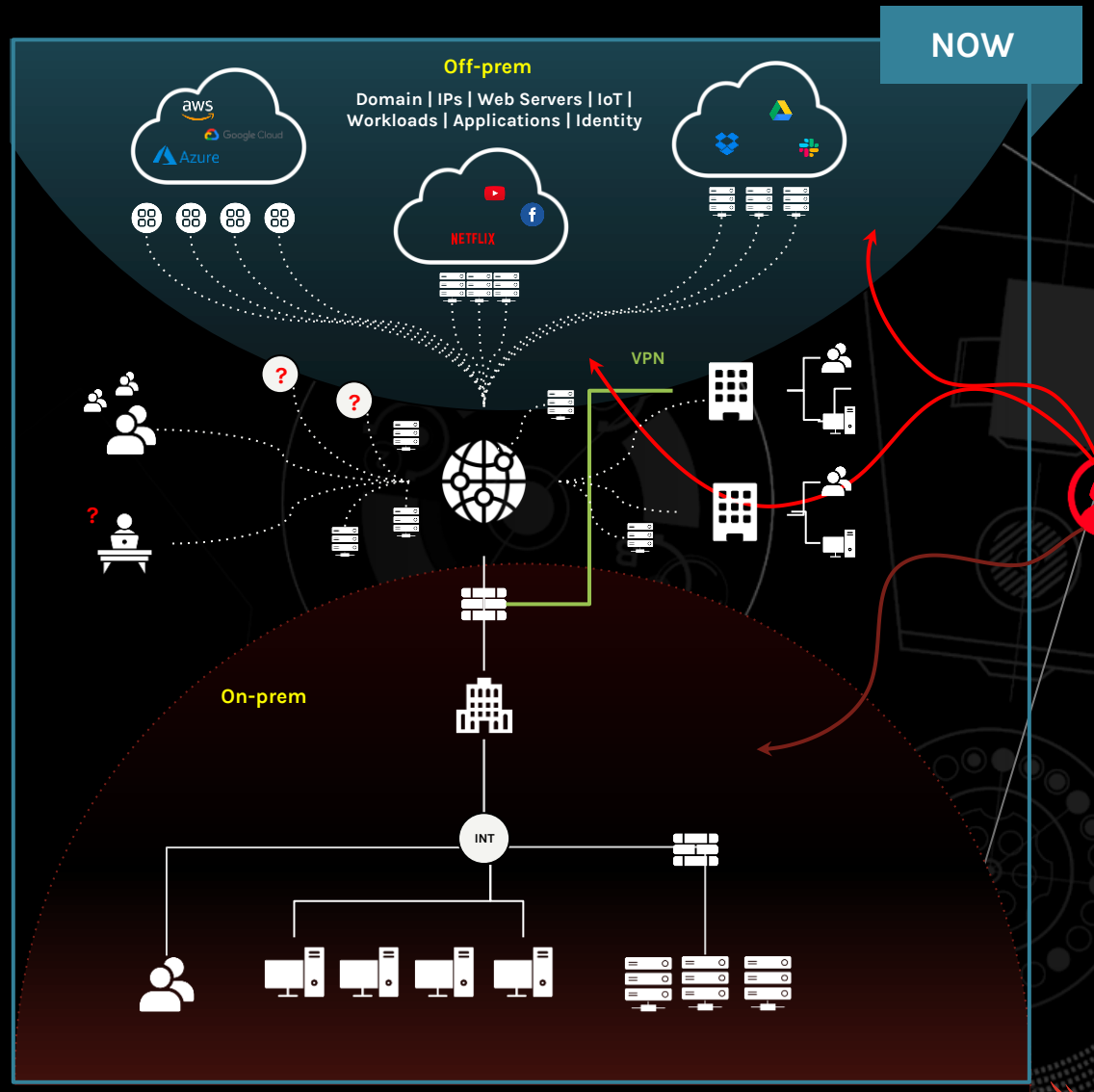
CROWDSTRIKE

EASM

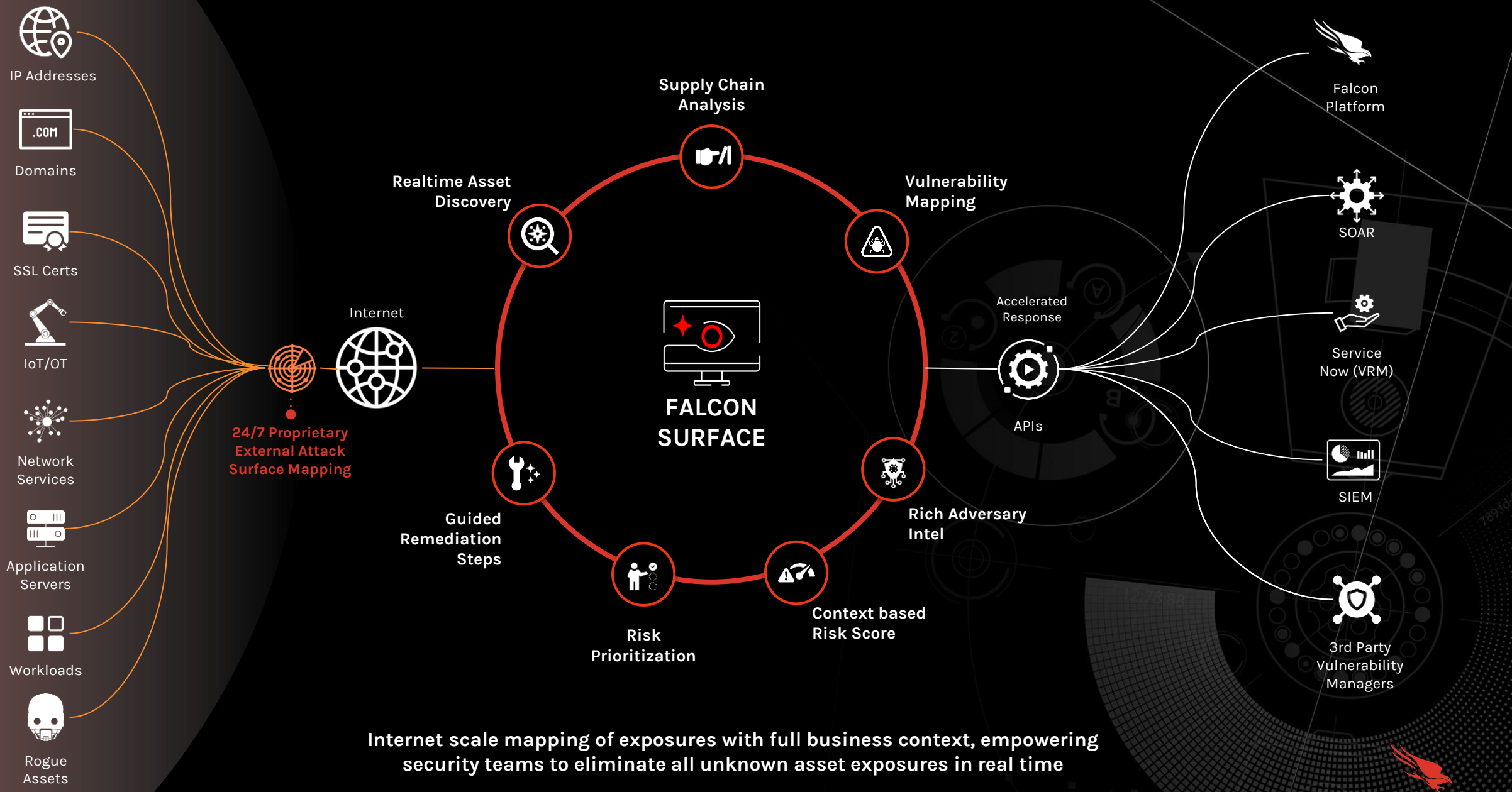
CROWDSTRIKE

Your digital footprint is becoming complex





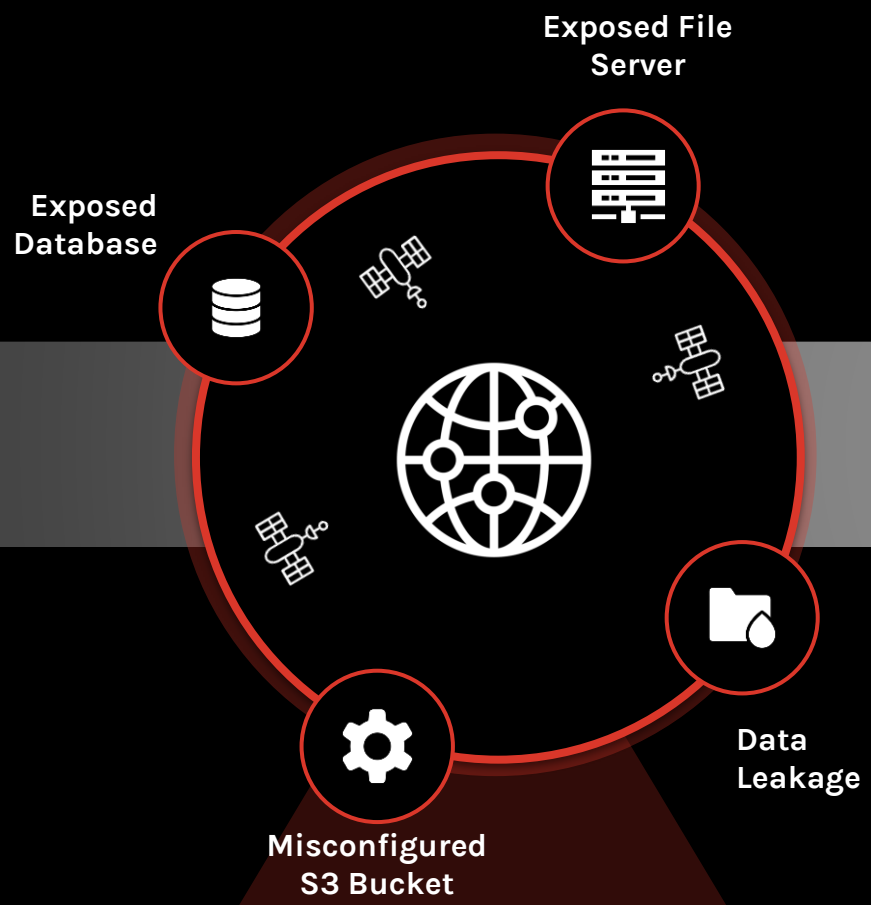
CROWDSTRIKE

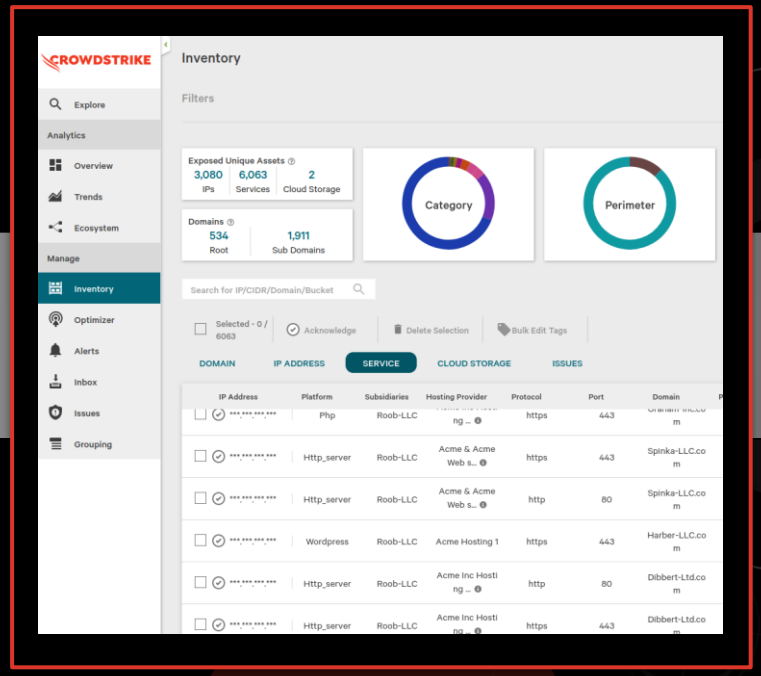


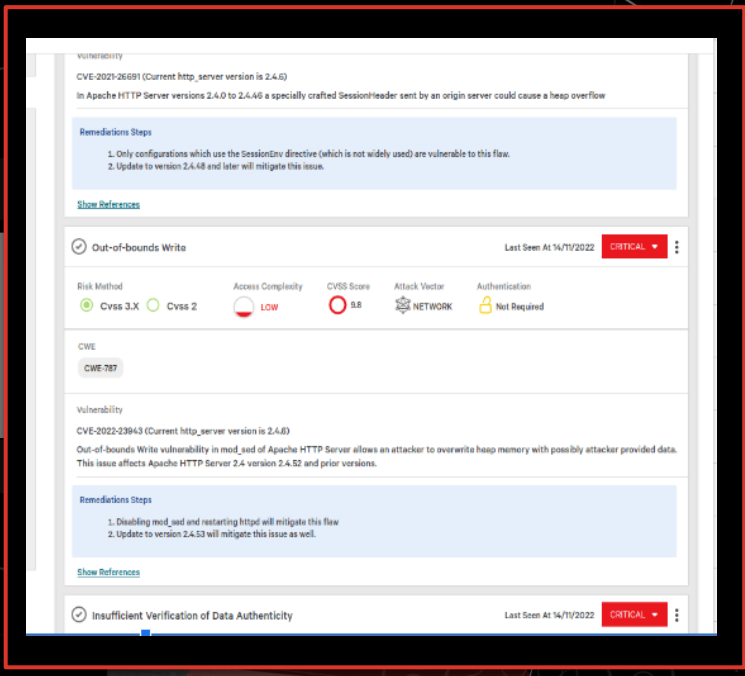
Internet scale mapping of exposures with full business context, empowering security teams to eliminate all unknown asset exposures in real time

CROWDSTRIKE

FALCON SURFACE MAPS THE WORLD'S INTERNET EXPOSURES IN REAL-TIME







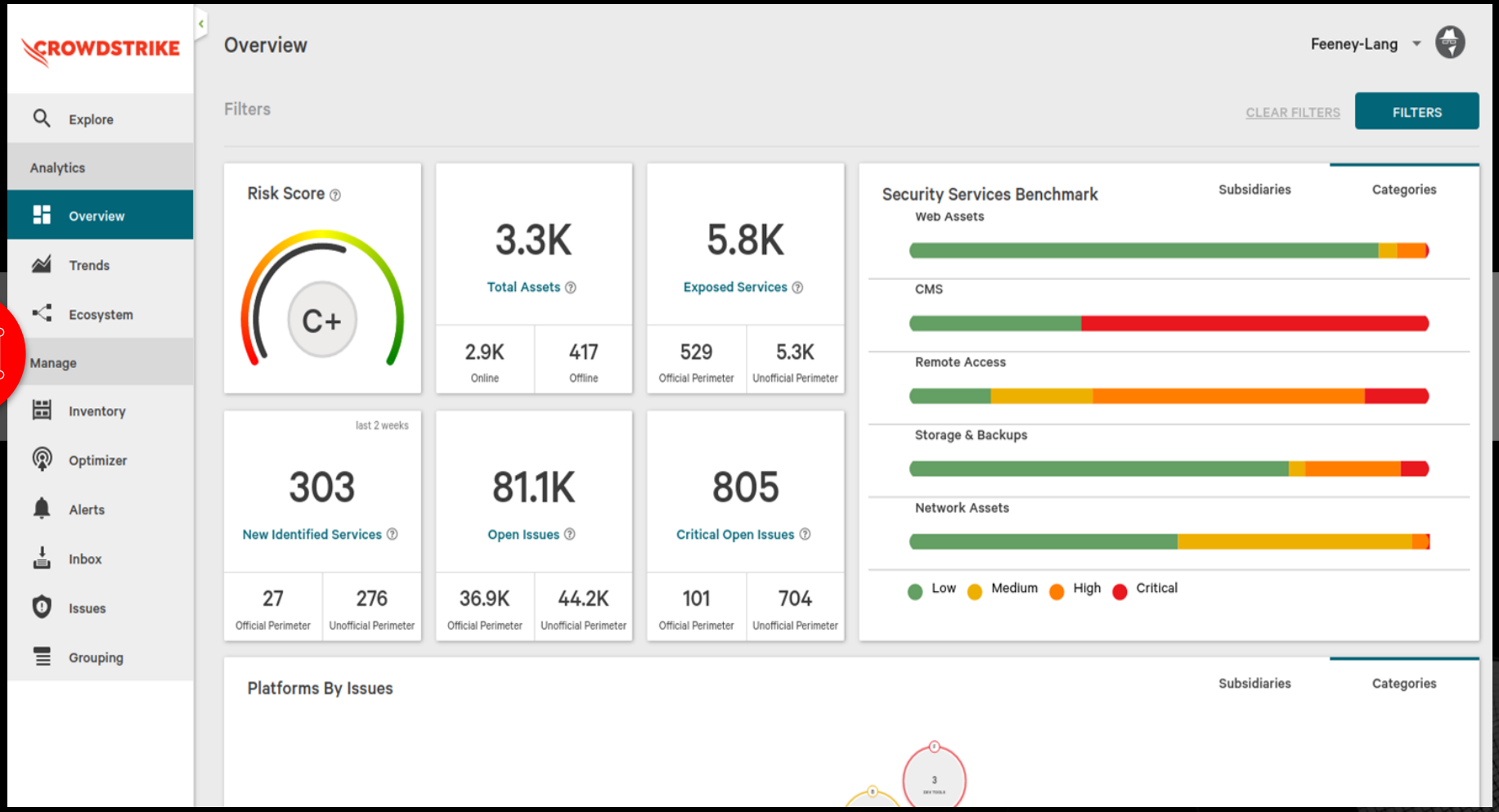
1. Scan the entire internet for exposed assets

2. Create exposed asset inventory and analyze security posture

3. Prioritize risk and generate guided remediation steps

CROWDSTRIKE

Do you know your external attack surface?



FALCON **SURFACE**

BOOK YOUR DEMO TODAY

CROWDSTRIKE

A PROVEN SECURITY LEADER

Leader In

Gartner • FORRESTER® • IDC

Validated

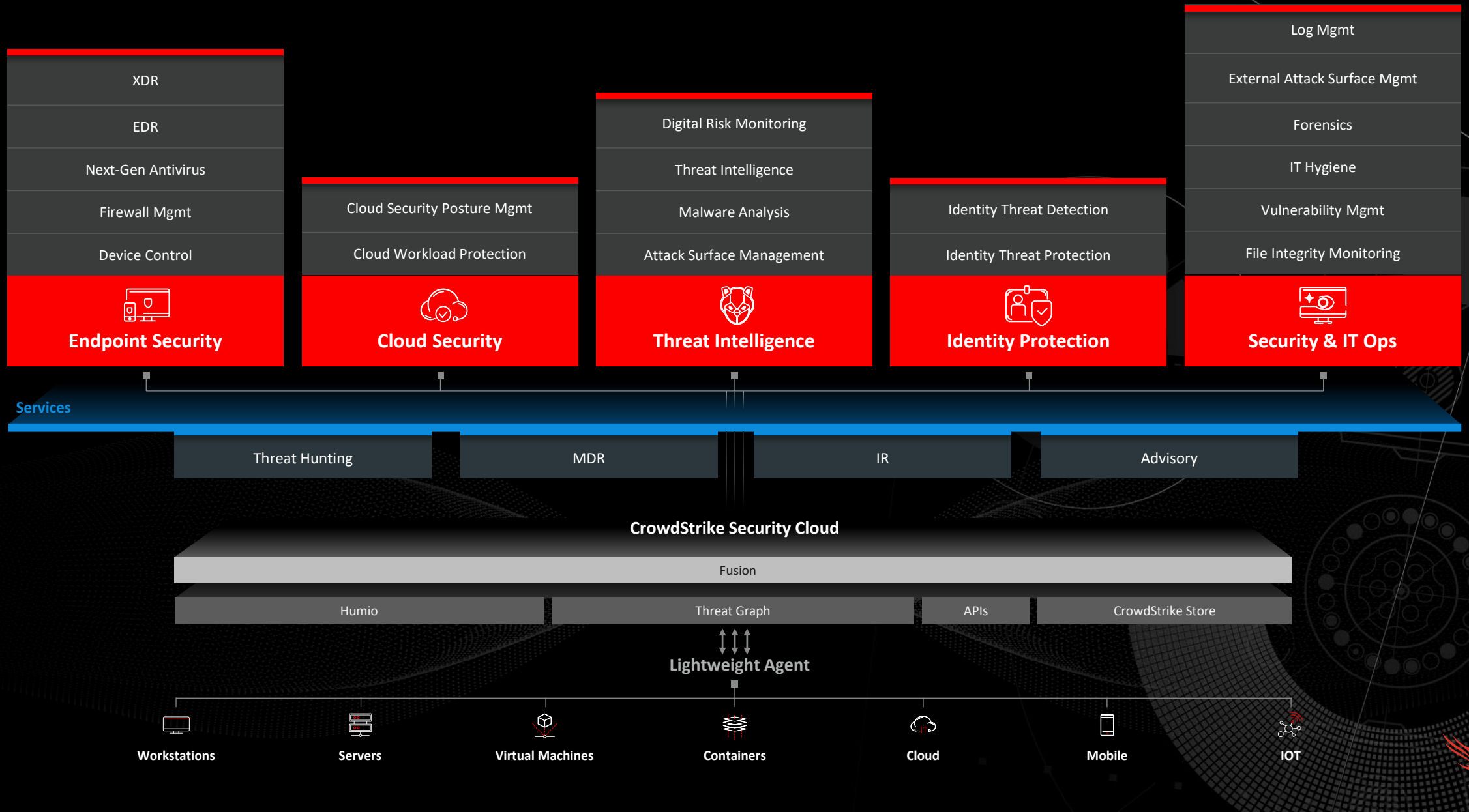
MITRE • AV comparatives • SE Labs

Compliance & Certifications

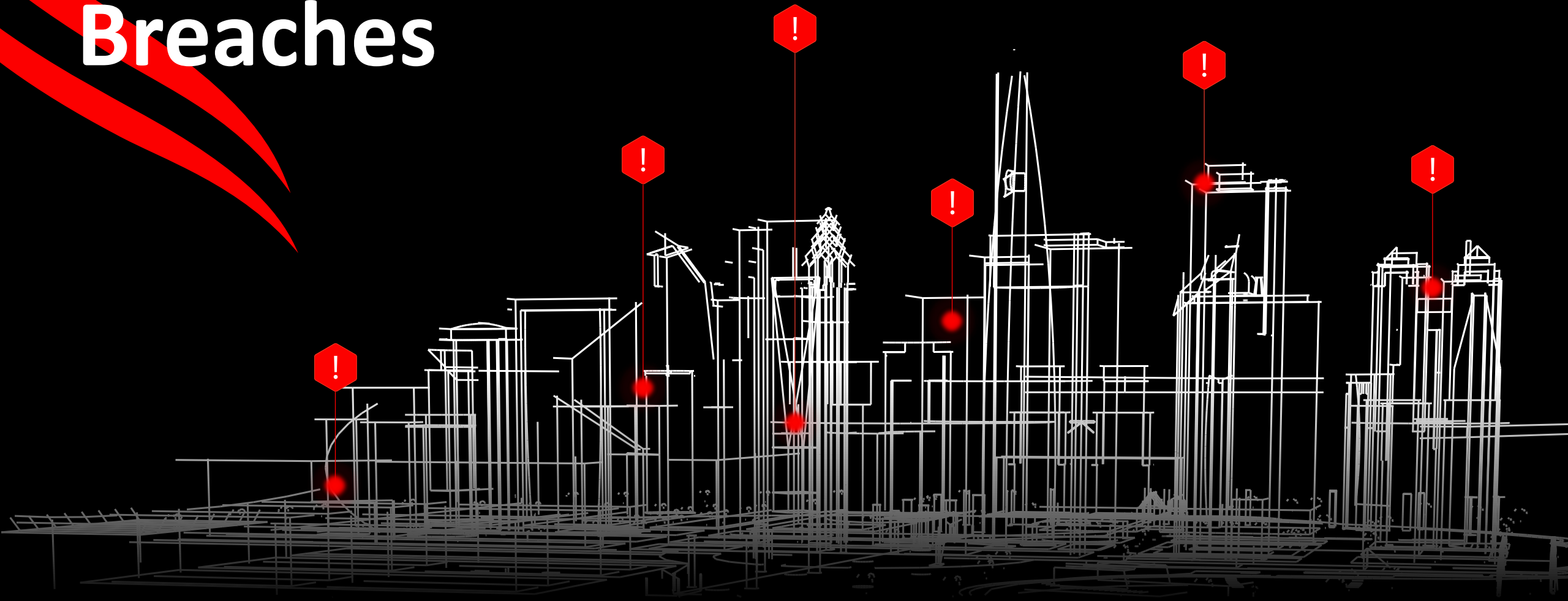
Privacy Shield Framework · FedRAMP · PCI · aws competency · amtso · FFIEC · Cyber Essentials Certified · CCN · STAR Level Two · CREST

CROWDSTRIKE

THE FALCON PLATFORM



We Stop Breaches



CROWDSTRIKE

THANK YOU