Attacchi Cross-Domain
Superare la Frammentazione per una Difesa Unificata

Luca Bechelli| Comitato Direttivo, *Clusit*
Alberto Greco | Team Lead Sales Engineering, *CrowdStrike*

Luca Bechelli

COMITATO DIRETTIVO

PARTNER @P4I – GRUPPO DIGITAL360

Alberto Greco
Team Lead Sales Engineering, *CrowdStrike*

L'inizio in CrowdStrike avviene nel gennaio 2022 con lo scopo di seguire il team dedicato al mercato enterprise e mid-market. Il ruolo principale è agire da punto di congiunzione tra le esigenze di business dei clienti e le soluzioni tecnologiche di CrowdStrike: dall'endpoint al cloud, dal mondo identity alla threat intelligence, dall'XDR all'IT Operations. A questo si aggiunge il ruolo di Team Lead per il team tech sales in Italia.

In passato Sales Engineer Enterprise per l'intero portfolio Palo Alto Networks, Sales Engineer in Forcepoint con focus sulla network security, technical trainer Fortinet in Exclusive Networks, network e security specialist in Sinergy e, prima ancora, network security specialist in Thales Alenia Space.

Convinto sostenitore della frase "Se non lo sai spiegare in modo semplice, non l'hai capito abbastanza bene" e che una diffusione della cultura CyberSec ad ogni livello sia fondamentale per una piena consapevolezza delle problematiche e, ancor più, delle opportunità che ne derivano.

Cloud Control Plane Is a Prime Target

The cloud control plane is the **backbone of cloud operations**, serving as a command center to manage, secure and optimize cloud environments.

A compromised control plane gives adversaries **broad access and control** over the entire cloud environment, making it a prime target.

SCATTERED SPIDER

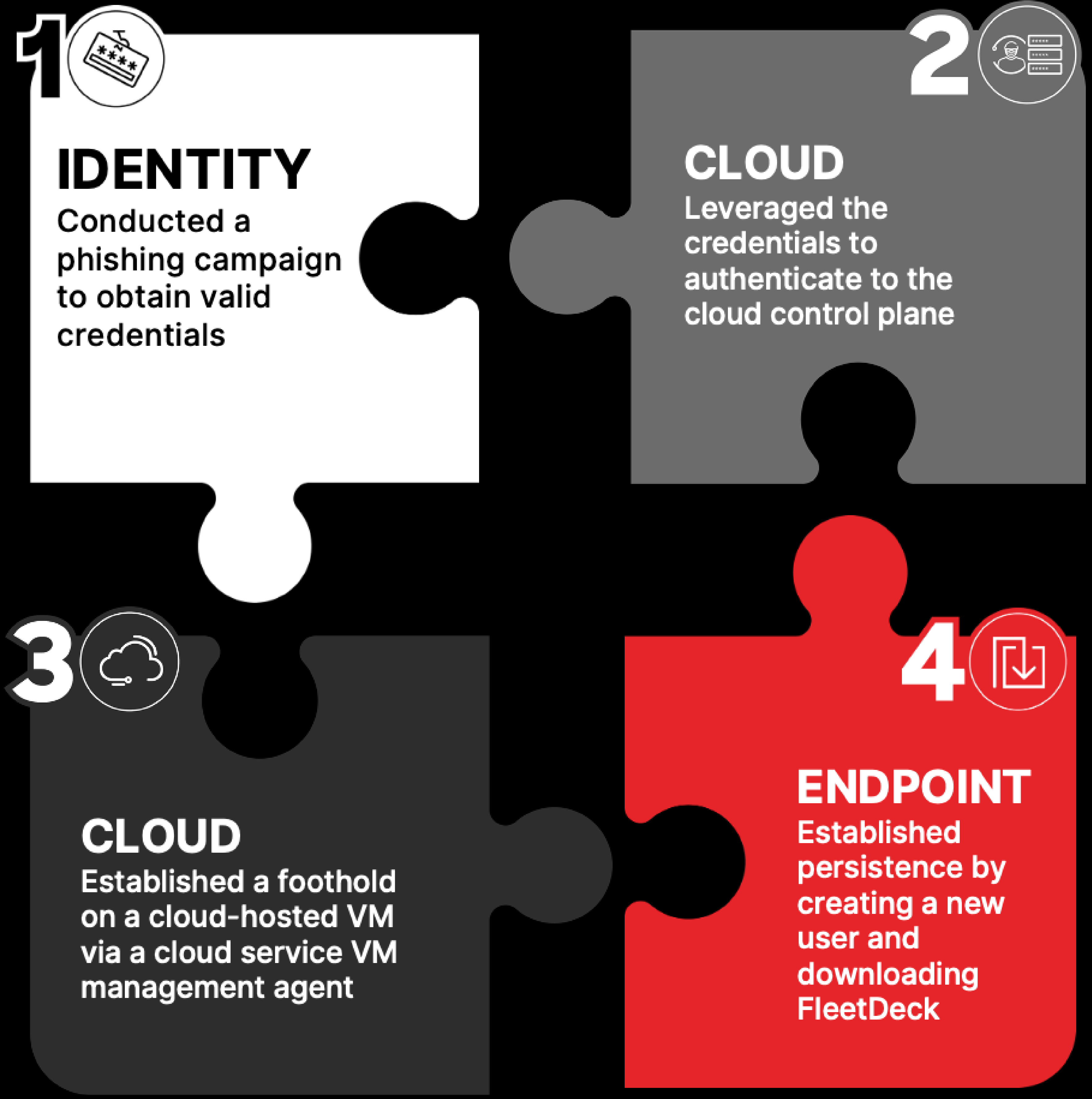
Financially motivated actor; successfully abuses all major cloud service providers

- Leveraged a federated identity provider (IdP) to establish persistence with a federated domain in Entra ID, initially relying on AADInternals Azure AD backdoor; later added a federated IdP to a victim's Okta tenant
- Accessed credentials stored in cloud-hosted secrets manager and HashiCorp Vault, then located a DC inside a victim's Azure tenant, copied the disks and created a new adversary-controlled VM where the adversary mounted the DC disk copies. From those disks, the adversary dumped the Active Directory database NTDS.dit
- Used access to a victim's M365 environment to search SharePoint Online for VPN setup instructions. Logged on to the VPN and moved laterally to on-premises servers. Used cloud-hosted VMs to move laterally from the cloud control plane to computer instances
- Leveraged the open-source S3 Browser to exfiltrate data to an external adversary-controlled cloud storage repository

CROWDSTRIKE

SCATTERED SPIDER Cross-Domain Attack

Having full insight into telemetry spanning endpoint, identity and cloud environments is a force multiplier to hunt cross-domain attacks



1 **IDENTITY**
Conducted a phishing campaign to obtain valid credentials

2 **CLOUD**
Leveraged the credentials to authenticate to the cloud control plane

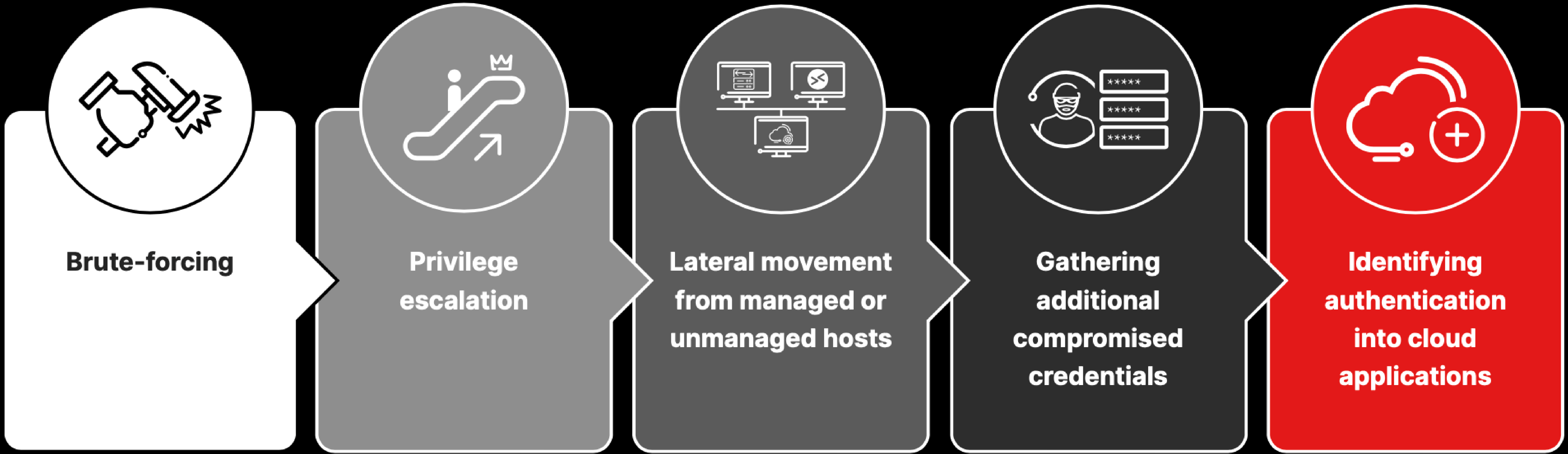
3 **CLOUD**
Established a foothold on a cloud-hosted VM via a cloud service VM management agent

4 **ENDPOINT**
Established persistence by creating a new user and downloading FleetDeck

Stealthy Adversaries Exploit Legitimate Credentials to Gain Access

Surge in access broker advertisements

142% in healthcare and 152% in consulting and professional services



Brute-forcing

Privilege escalation

Lateral movement from managed or unmanaged hosts

Gathering additional compromised credentials

Identifying authentication into cloud applications

FAMOUS CHOLLIMA

FAMOUS CHOLLIMA has been active since at least 2018. The adversary primarily conducts operations to illicitly obtain freelance or full-time equivalent (FTE) work to earn a salary that can be funnelled to North Korea.

Insider threats can lead to data theft, regulatory penalties and damaged trust.

Adversary groups like Democratic People's Republic of Korea (DPRK)-nexus FAMOUS CHOLLIMA use insiders to steal information for harmful operations.

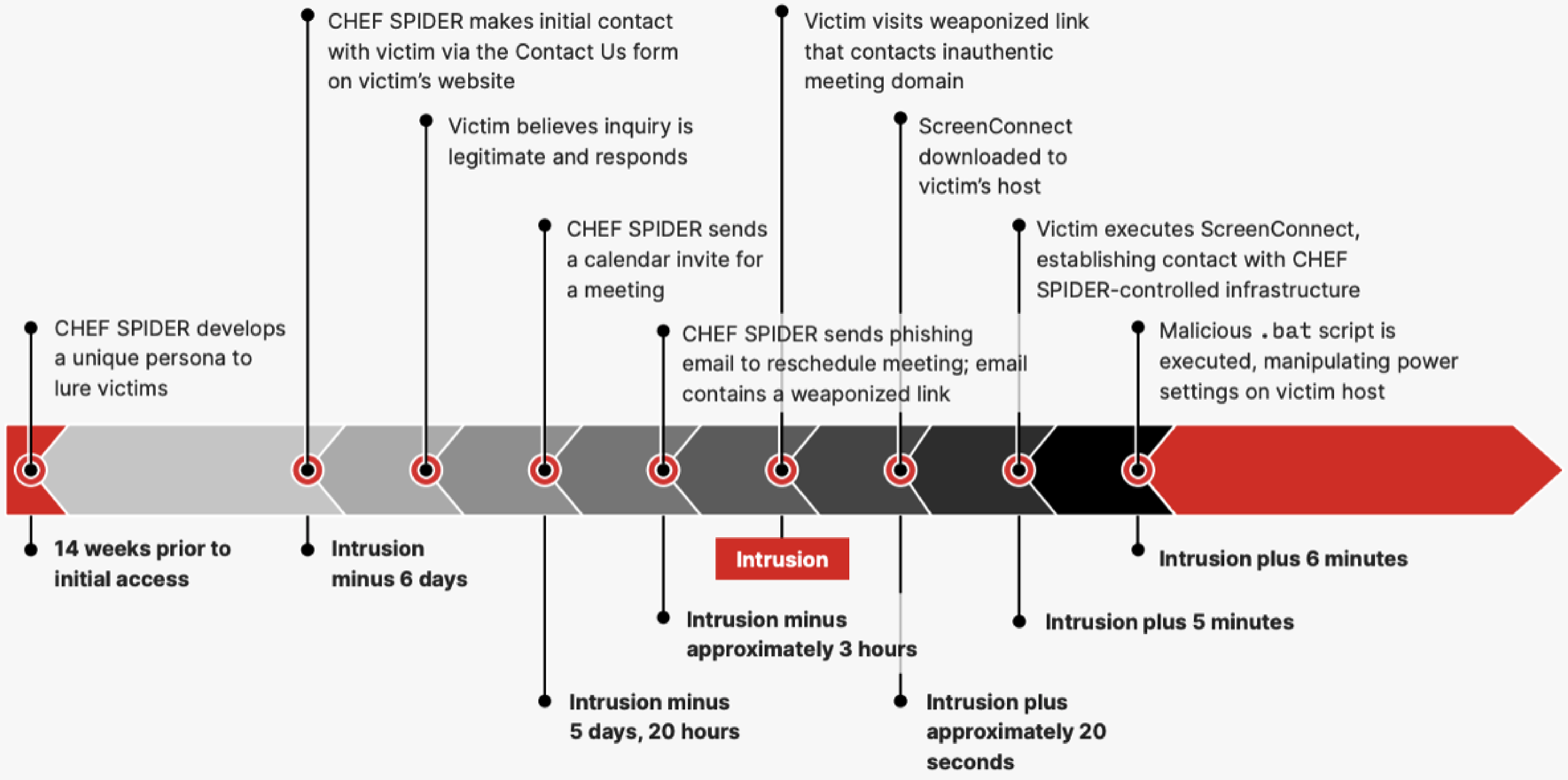
The CrowdStrike OverWatch team recently uncovered FAMOUS CHOLLIMA insiders applying to or working at more than 150 organizations and confirmed that data theft occurred in 50% of service engagements, illustrating how insiders pose serious risks to reputation and finances.

How Falcon Adversary OverWatch Hunts Down Insider Threats

1. **Global Telemetry and Detection**: correlates telemetry from multiple customer environments to identify patterns missed by individual organizations
2. **Advanced Monitoring**: conducts real-time monitoring and behavioural analysis to catch insider threats early
3. **Speed and Collaboration**: uses AI-powered detections to identify adversaries in minutes and partners with law enforcement to dismantle insider networks

CROWDSTRIKE

Remote Monitoring and Management Tool Exploit



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

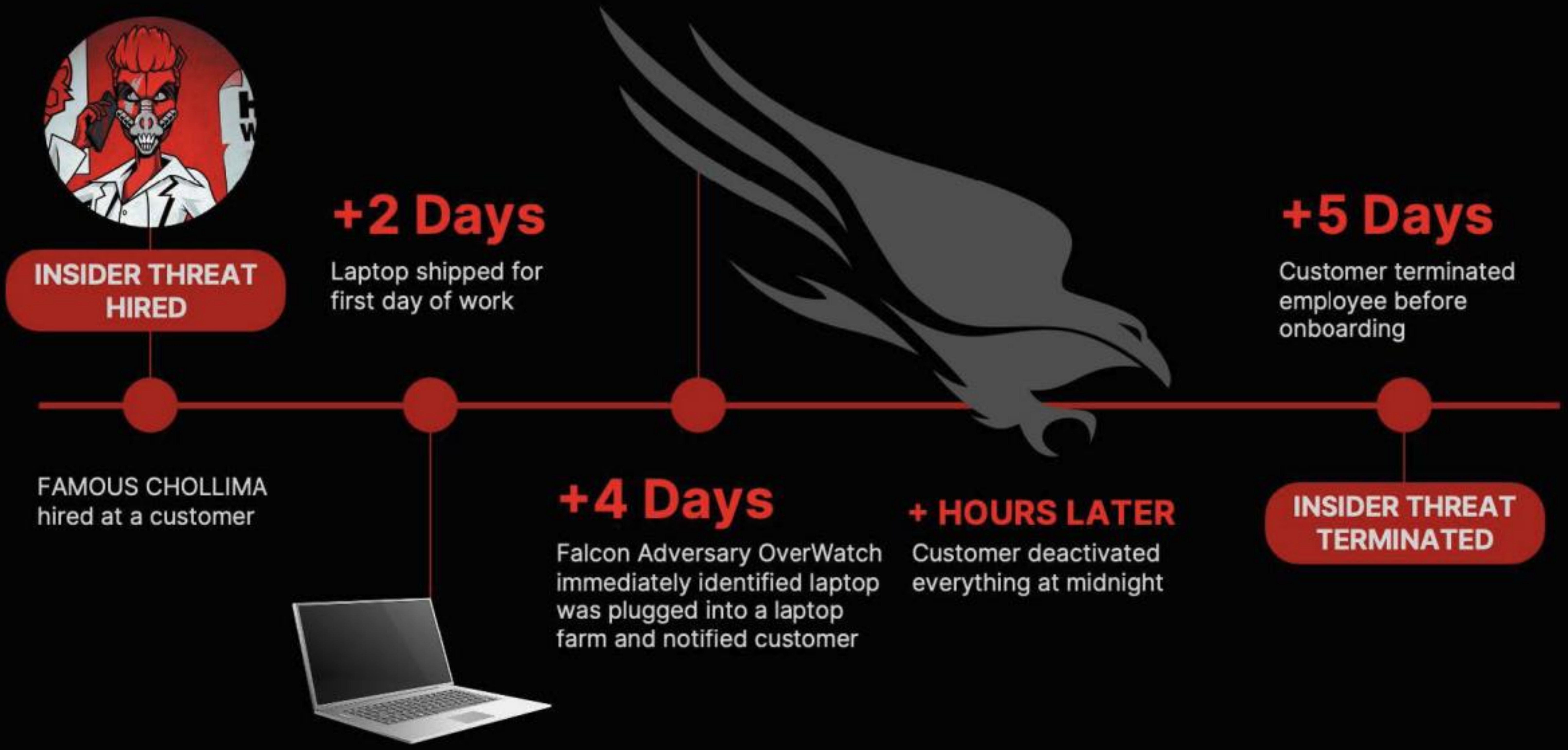
70% increase in adversaries exploiting legitimate RMM tools

156% increase in ConnectWise ScreenConnect usage, becoming the most exploited RMM tool

Top 5 RMM tools:

1. ConnectWise ScreenConnect
2. AnyDesk
3. TeamViewer
4. Atera Agent
5. Splashtop

CROWDSTRIKE



INSIDER THREAT HIRED

FAMOUS CHOLLIMA
hired at a customer

+2 Days

Laptop shipped for
first day of work

+4 Days

Falcon Adversary OverWatch immediately identified laptop was plugged into a laptop farm and notified customer

+ HOURS LATER

Customer deactivated everything at midnight

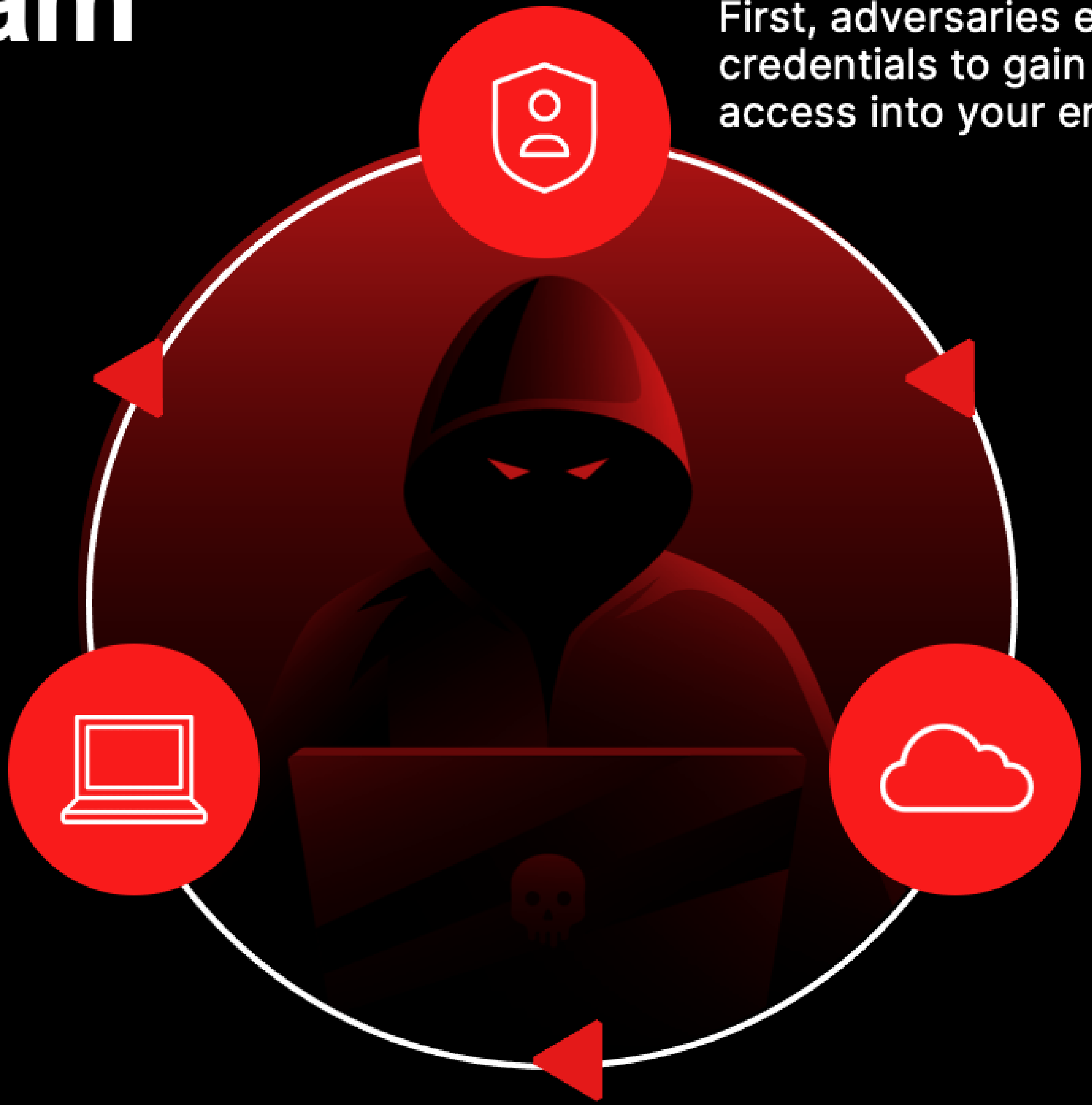
+5 Days

Customer terminated employee before onboarding

INSIDER THREAT TERMINATED

Cross-Domain Attacks Are Now Mainstream

Only a unified platform enables threat hunting to accelerate detection and response



Identity

First, adversaries exploit valid credentials to gain unauthorized access into your environment

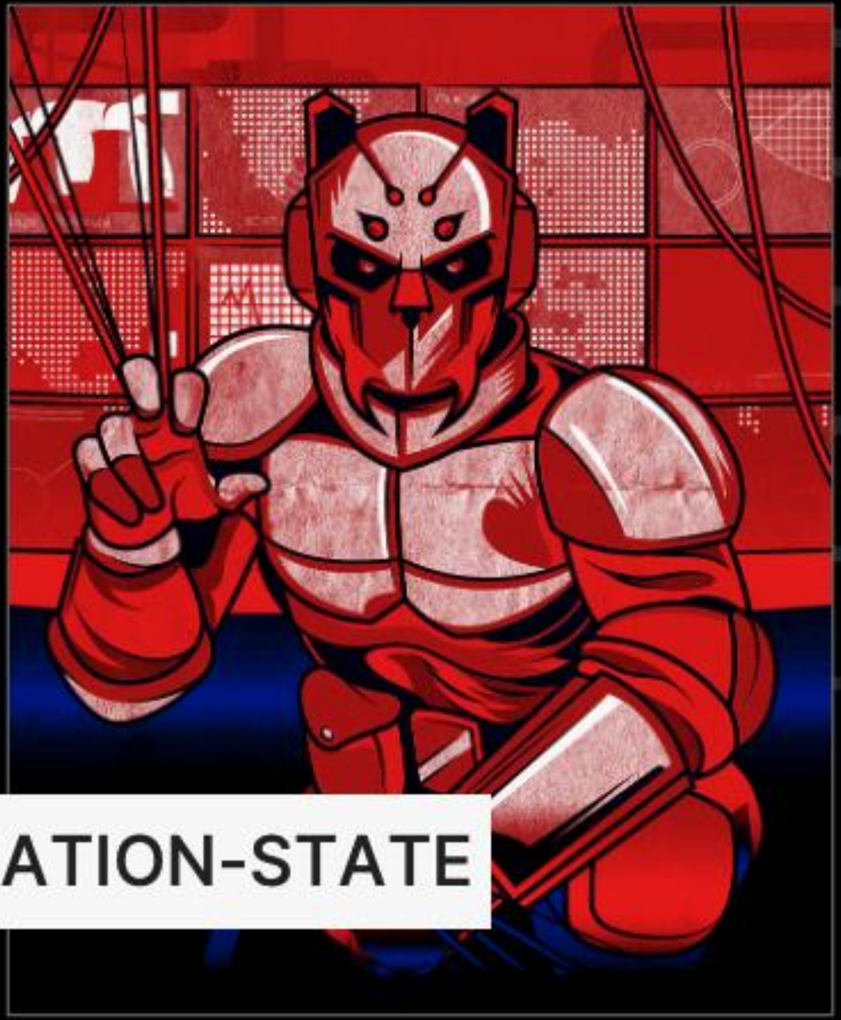
Cloud

Next, adversaries use legitimate commands to harvest credentials or further compromise cloud environment

Endpoint

Finally, adversaries move laterally to access high-value data or deploy ransomware for extortion

Threat Actor Motivation



NATION-STATE

eCRIME

HACKTIVISM

CRIMINAL

ALCHEMIST SPIDER
ALPHA SPIDER
AVIATOR SPIDER
BITWISE SPIDER
BLIND SPIDER
BRAIN SPIDER
CARBON SPIDER
CHARIOT SPIDER
CHAOTIC SPIDER
CHEF SPIDER
CLOCKWORK SPIDER
DEMON SPIDER
DONUT SPIDER
FROZEN SPIDER
GRACEFUL SPIDER
HAZARD SPIDER
HERMIT SPIDER
HIVE SPIDER
HOLIDAY SPIDER
HONEY SPIDER
INDRIK SPIDER
KNOCKOUT SPIDER
LILY SPIDER
LUNAR SPIDER
MALLARD SPIDER
MANGLED SPIDER
MASKED SPIDER
MONARCH SPIDER
MUMMY SPIDER
NARWHAL SPIDER
ODYSSEY SPIDER
OUTBREAK SPIDER
PERCUSSION SPIDER
PROPHET SPIDER
PUNK SPIDER
QUANTUM SPIDER
RECESS SPIDER
RICE SPIDER
ROYAL SPIDER
SALTY SPIDER
SAMBA SPIDER
SCATTERED SPIDER
SCULLY SPIDER
SHINING SPIDER
SLIPPY SPIDER
SMOKY SPIDER
SOLAR SPIDER
SPRITE SPIDER
TRAVELING SPIDER
TUNNEL SPIDER
VAMPIRE SPIDER
VENOM SPIDER
VETO SPIDER
WANDERING SPIDER
WIZARD SPIDER
VICE SPIDER

NORTH KOREA

LABYRINTH CHOLLIMA
FAMOUS CHOLLIMA
RICOCHET CHOLLIMA
SILENT CHOLLIMA
STARDUST CHOLLIMA
VELVET CHOLLIMA

CHINA

AQUATIC PANDA
CASCADE PANDA
EMISSARY PANDA
ETHEREAL PANDA
JACKPOT PANDA
HORDE PANDA
KARMA PANDA
KRYPTONITE PANDA
LOTUS PANDA
MUSTANG PANDA
OVERCAST PANDA
PHANTOM PANDA
PIRATE PANDA
PUZZLE PANDA
SHATTERED PANDA
SUNRISE PANDA
VANGUARD PANDA
VAPOR PANDA
VERTIGO PANDA
VIXEN PANDA
WICKED PANDA

INDIA

HAZY TIGER
OUTRIDER TIGER
QUILTED TIGER
RAZOR TIGER
VICEROY TIGER

IRAN

BANISHED KITTEN
CHARMING KITTEN
CHRONO KITTEN
HAYWIRE KITTEN
IMPERIAL KITTEN
NEMESIS KITTEN
PIONEER KITTEN
REFINED KITTEN
SPECTRAL KITTEN
STATIC KITTEN
TRACER KITTEN
VENGEFUL KITTEN

EGYPT

WATCHFUL SPHINX

KAZAKHSTAN

COMRADE SAIGA

PAKISTAN

MYTHIC LEOPARD
FRINGE LEOPARD

RUSSIA

BERSERK BEAR
COZY BEAR
EMBER BEAR
FANCY BEAR
GOSSAMER BEAR
PRIMITIVE BEAR
VENOMOUS BEAR
VOODOO BEAR

VIETNAM

OCEAN BUFFALO

SOUTH KOREA

SHADOW CRANE

SYRIA

DEADEYE HAWK

COLOMBIA

GALACTIC OCELOT

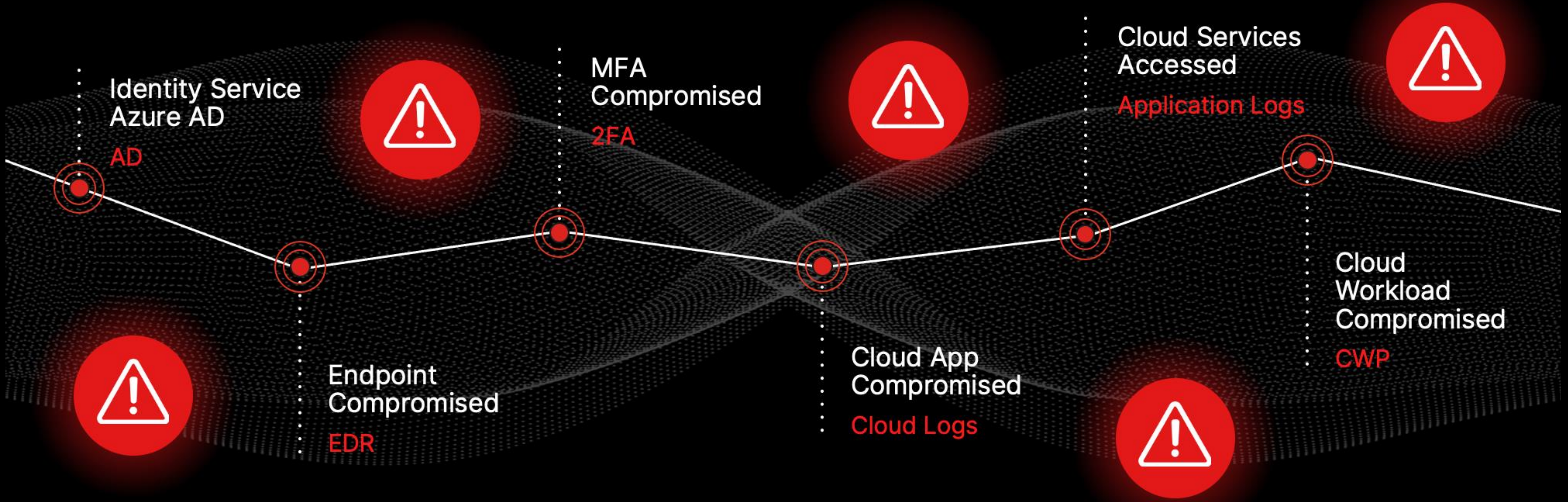
TURKEY

COSMIC WOLF

HACKTIVIST

CURIOUS JACKAL
FRONTLINE JACKAL
INTREPID JACKAL
PARTISAN JACKAL
REGAL JACKAL
RENEGADE JACKAL

The Nature of an Attack



Identity Service Azure AD

AD

Endpoint Compromised

EDR

MFA Compromised

2FA

Cloud App Compromised

Cloud Logs

Cloud Services Accessed

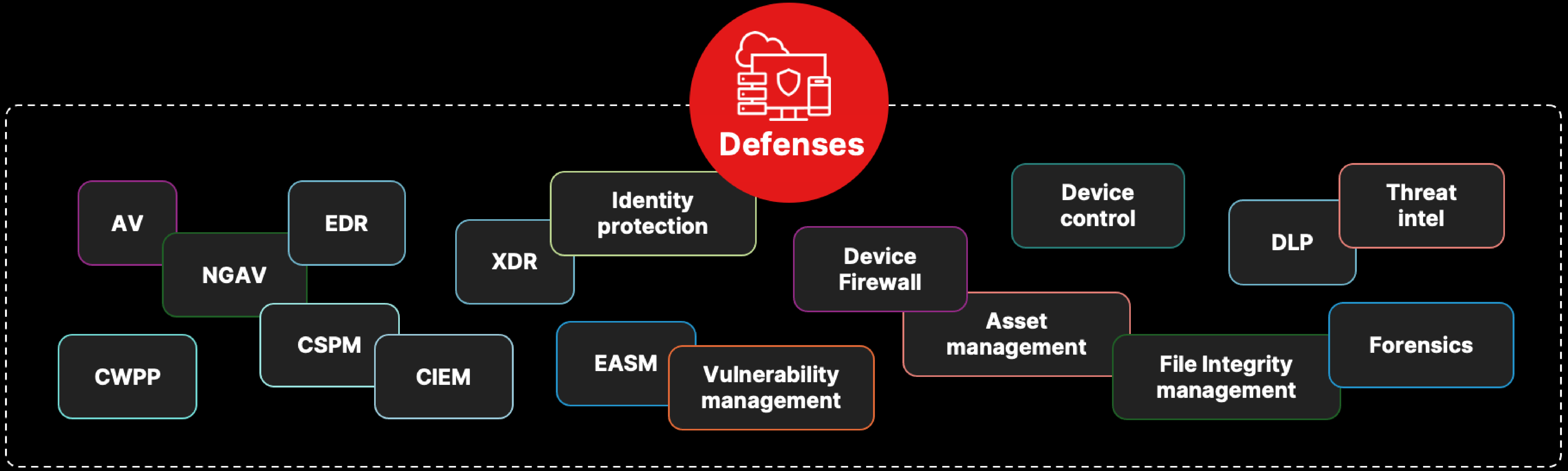
Application Logs

Cloud Workload Compromised

CWP

CROWDSTRIKE

Adversaries Live in the Gaps
Between Traditional Siloed Tools



Complexity

Alerts

Missed indicators

CROWDSTRIKE

What Is Cross Domain Threat Hunting?

Proactively searching for threats that have **bypassed initial security defenses.**

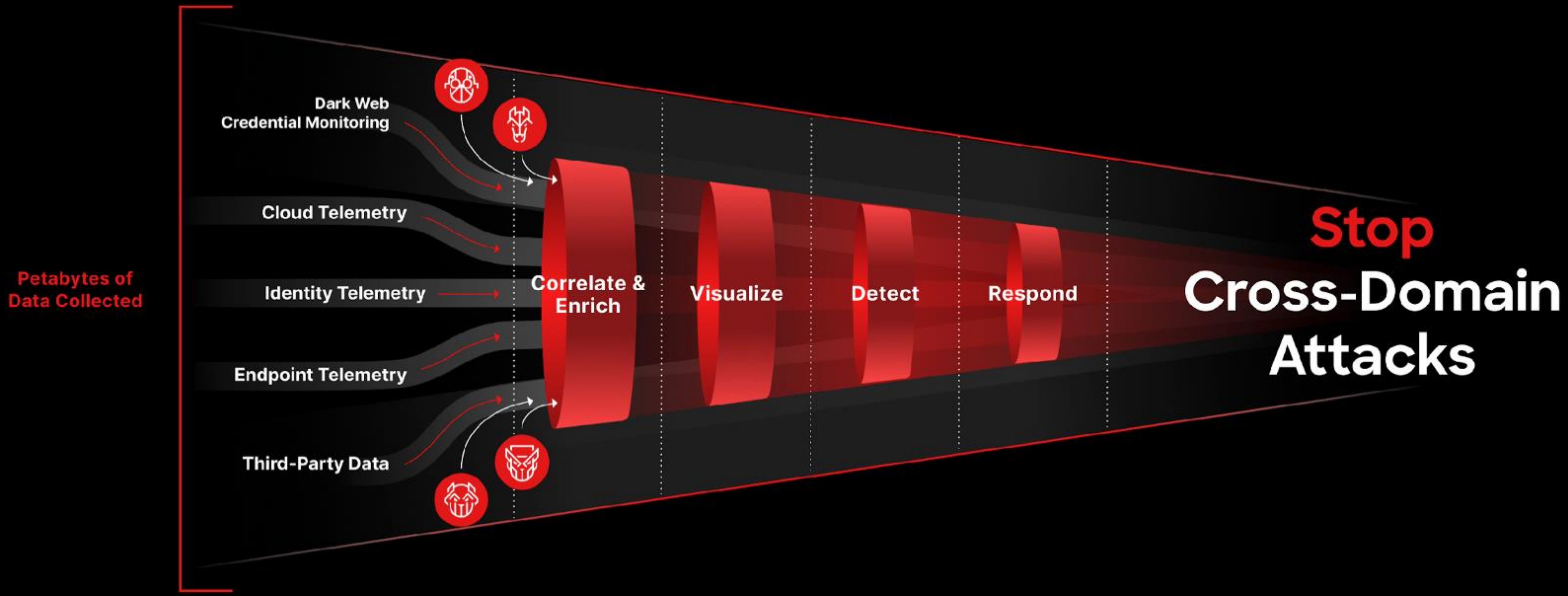
Adversaries can remain **hidden for months**, collecting sensitive data and credentials to enable lateral movement.

Cross Domain Threat Hunting uses data from Identity, Cloud Control Plane, Endpoint telemetry, and other domains such as IOT/ICT/OT.

5 Steps to Be Prepared

1. Protect Identities
2. Effective Cloud Security
3. Secure the Endpoint
4. Cross Domain Visibility & Hunting
5. Know the Adversary

Consolidating Cross-Domain Data



AI Powered Threat Hunting

ENRICHED DATA

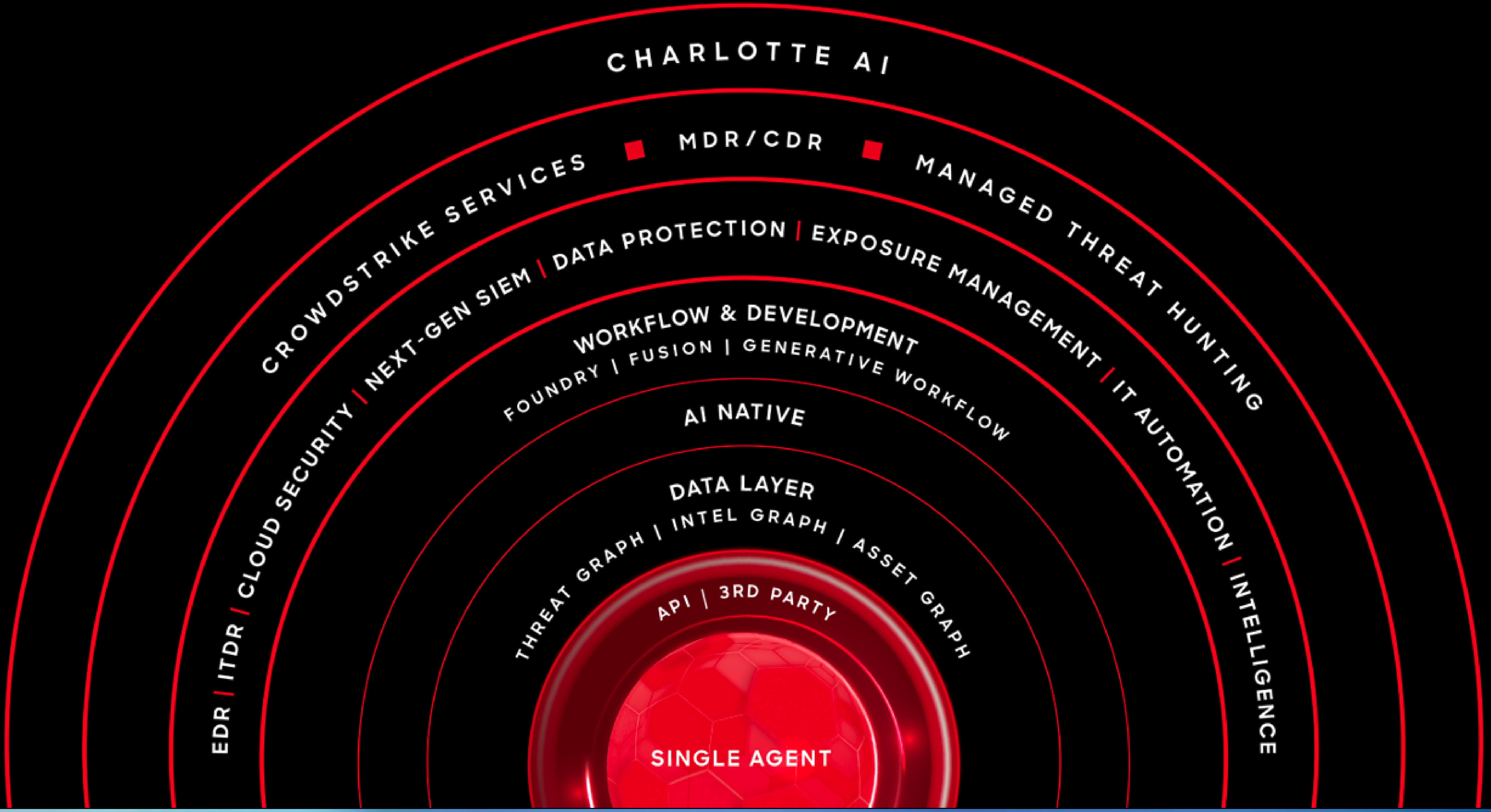
ANALYZED DATA

Endpoint

Identity

Cloud

CROWDSTRIKE’S FALCON PLATFORM AND SERVICES



CHARLOTTE AI

CROWDSTRIKE SERVICES ■ MDR/CDR ■ MANAGED THREAT HUNTING

EDR | ITDR | CLOUD SECURITY | NEXT-GEN SIEM | DATA PROTECTION | EXPOSURE MANAGEMENT | IT AUTOMATION | INTELLIGENCE

WORKFLOW & DEVELOPMENT

FOUNDRY | FUSION | GENERATIVE WORKFLOW

AI NATIVE

DATA LAYER

THREAT GRAPH | INTEL GRAPH | ASSET GRAPH

API | 3RD PARTY

SINGLE AGENT

Q&A

Contatti:

alberto.greco@crowdstrike.com

Vieni a trovarci al nostro stand!