

A hand holding a wooden gavel over a document, symbolizing law or enforcement. The background is dark and blurred, with a stack of papers and a keyboard visible. The text is overlaid on a dark blue rectangular background.

Hoe stealth een stap vooruit blijven met CrowdStrike?


NIS2-opvolgwebinars




wiki webinar
by **inetum**.
realdolmen

Praktische afspraken

- Vragen via chat
- Iedereen op mute
- Q&A na de presentatie
- Evaluatie met link naar de slides worden na de webinar doorgestuurd



inetum. 
realdolmen
Positive digital flow

 **CROWDSTRIKE**



CrowdStrike Inetum Webinar 26/03/24

Wolfgang Meert – Sales Engineer

© CrowdStrike, Inc. All rights reserved.





Agenda

- Threat Landscape
- Major Themes
- eCrime Landscape
- Recommendations
- The Falcon platform

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

NORTH KOREA

- Labyrinth 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

INDIA

- Hazy Tiger
- Outrider Tiger
- Quilted Tiger
- Razor Tiger
- Viceroy Tiger

EGYPT

- Watchful Sphinx

VIETNAM

- Ocean Buffalo

SOUTH KOREA

- Shadow Crane

SYRIA

- Deadeye Hawk

COLOMBIA

- Galactic Ocelot

TURKEY

- Cosmic Wolf

PAKISTAN

- Mythic Leopard
- Fringe Leopard

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

RUSSIA

- Berserk Bear
- Cozy Bear
- Ember Bear
- Fancy Bear
- Gossamer Bear
- Primitive Bear
- Venomous Bear
- Voodoo Bear

ACTIVIST

- Curious Jackal
- Frontline Jackal
- Intrepid Jackal
- Partisan Jackal
- Regal Jackal
- Renegade Jackal

2024 Threat Landscape



34 new adversaries tracked by CrowdStrike, raising the total to 232



Cloud-conscious cases increased by 110% YoY



84% of adversary-attributed cloud-conscious intrusions were focused on eCrime



Cloud environment intrusions increased by 75% YoY



76% YoY increase in victims named on eCrime dedicated leak sites



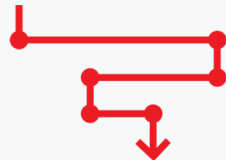
eCRIME BREAKOUT TIME

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

Malware-Free Initial Access »

75% 2023

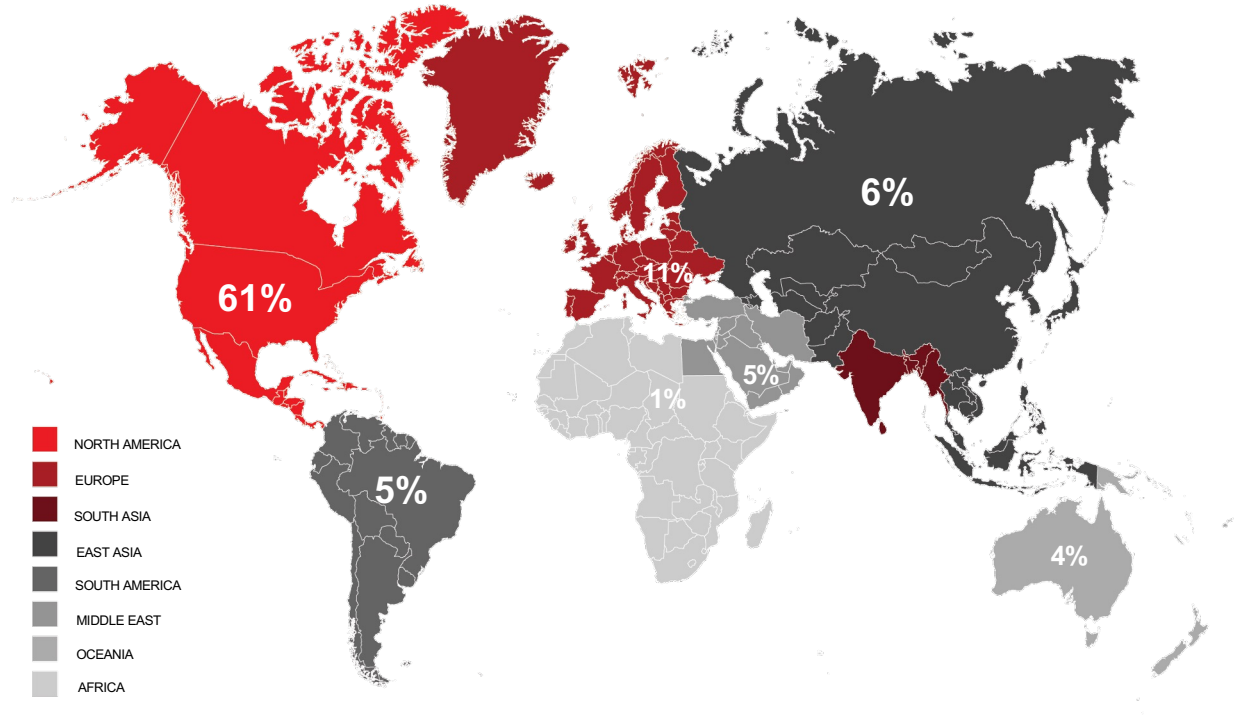
71% 2022

62% 2021

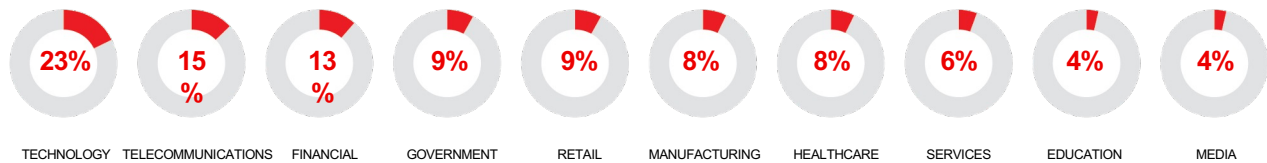
51% 2020

40% 2019

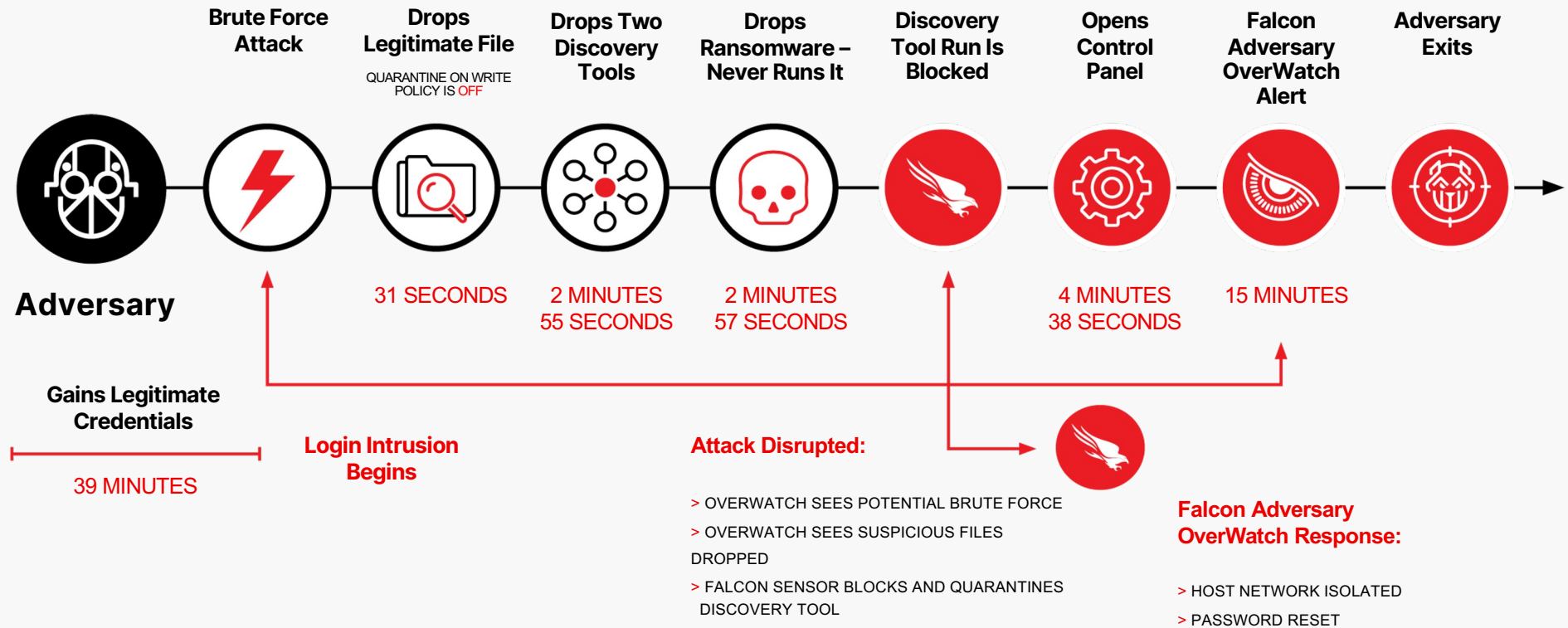
Interactive Intrusions by Region



Interactive Intrusions by Industry



Identity Is the **Critical** Battleground



CrowdStrike 2024 Global Threat Report



Main Theme

- » Identity-Based and Social Engineering Attacks
- » Adversaries Continue to Develop Cloud-Consciousness
- » Third-Party Relationship Exploitation
- » Vulnerability Landscape: "Under the Radar" Exploitation
- » 2023 Israel-Hamas Conflict Operations Focus on Disruption and Influence
- » Threats on the Horizon:
 - Generative AI Use in Adversary Operations
 - 2024 Worldwide Elections



IDENTITY-BASED AND

SOCIAL ENGINEERING ATTACKS



Adversaries expanded beyond valid accounts

Also targeted API keys and secrets, session cookies and tokens, one-time passwords and Kerberos tickets



COZY BEAR

Conducted regular credential phishing using Microsoft Teams messages to solicit multifactor authentication tokens for Microsoft 365 accounts



SCATTERED SPIDER

Conducted sophisticated social engineering campaigns



AS PREDICTED, CLOUD ENVIRONMENT INTRUSIONS INCREASED BY 75% FROM 2022 TO 2023 WITH CLOUD-CONSCIOUS CASES INCREASING BY 110% AND CLOUD-AGNOSTIC CASES INCREASING BY 60%

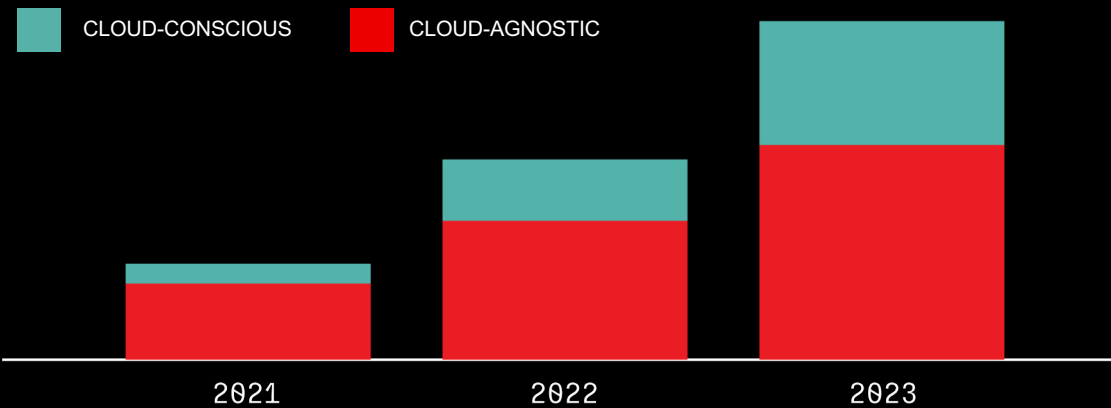
↑75%
IN CLOUD-CONSCIOUS CASES

eCRIME ADVERSARIES ACCOUNT FOR 84% OF ALL CLOUD-CONSCIOUS INTRUSIONS

ADVERSARIES CONTINUE

TO DEVELOP CLOUD-CONSCIOUSNESS

INCIDENTS IN THE CLOUD



▲ **110%** CLOUD-CONSCIOUS CASES

Actors are aware they gained access to a victim-owned cloud environment and use their access to abuse the victim-owned cloud service

▲ **60%** CLOUD-AGNOSTIC CASES

Actors either were not aware they had compromised a cloud environment or did not take advantage of cloud features

THIRD-PARTY

RELATIONSHIP EXPLOITATION



Yields a High Return on Investment

One compromised organization can lead to hundreds of thousands of follow-on targets



PANDA Adversaries

Consistently exploited trusted relations via supply chain and actor-on-the-side or actor-in-the-middle attacks



LABYRINTH CHOLLIMA

Abused trusted relationships to infiltrate high-value targets for currency generation and espionage



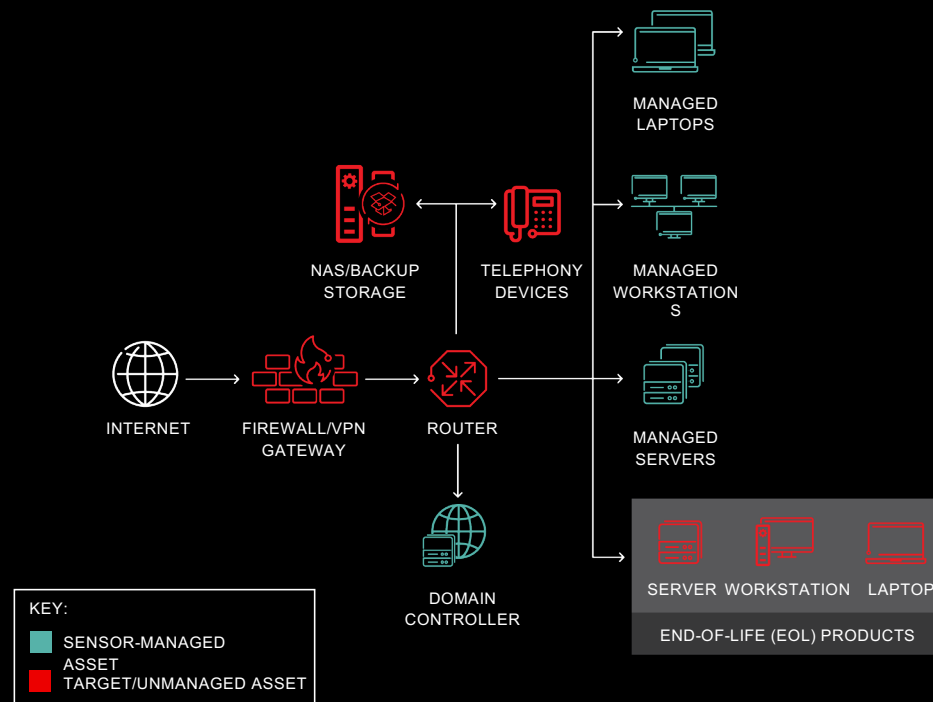
UNMANAGED NETWORK
APPLIANCES – PARTICULARLY
EDGE GATEWAY DEVICES –
REMAINED THE MOST ROUTINELY
OBSERVED INITIAL ACCESS
VECTOR FOR EXPLOITATION
DURING 2023



THREAT ACTORS ARE ACTIVELY
DEVELOPING EXPLOITS FOR EOL
PRODUCTS THAT CANNOT BE
PATCHED AND OFTEN DO NOT
ALLOW FOR MODERN SENSOR
DEPLOYMENT

VULNERABILITY LANDSCAPE:

“UNDER THE RADAR” EXPLOITATION





2023 ISRAEL-HAMAS CONFLICT:

CYBER OPERATIONS FOCUS ON

DISRUPTION AND INFLUENCE

Observed Activity



Campaigns designed to likely influence target populations and ones that deploy destructive wipers against Israeli or Israel-linked entities

Hamas Activity Not Observed



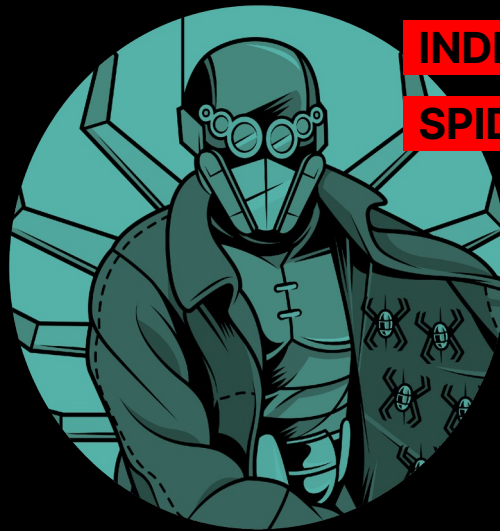
Likely due to unavailable resources or the degradation of internet and electricity-distribution infrastructure

Faketivists



Iranian adversaries operate inauthentic personas for disruption and information operations

THREATS ON THE 2024 HORIZON



**INDRIK
SPIDER**



**SCATTERED
SPIDER**



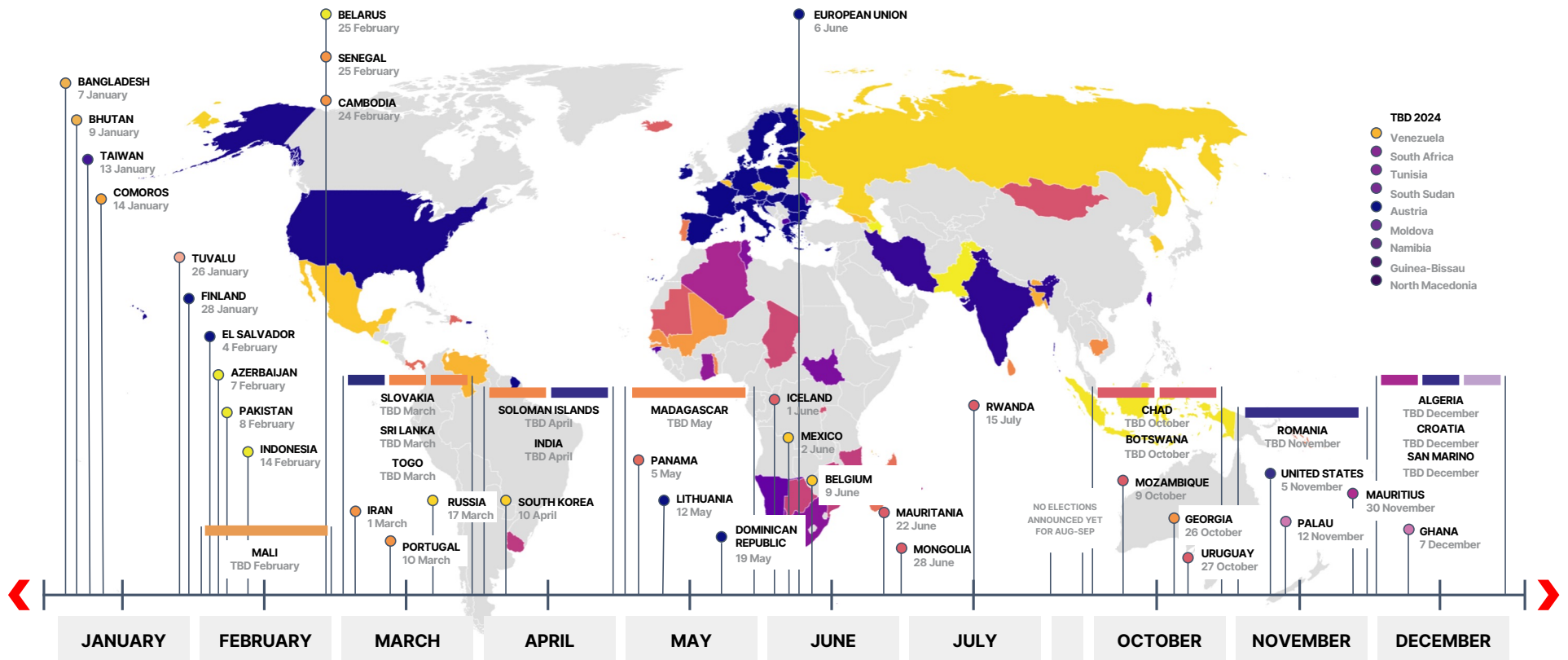
GENERATIVE AI HAS MASSIVELY DEMOCRATIZED COMPUTING TO IMPROVE ADVERSARY OPERATIONS. IT CAN ALSO POTENTIALLY LOWER THE ENTRY BARRIER TO THE THREAT LANDSCAPE FOR LESS SOPHISTICATED THREAT ACTORS.

THREATS ON THE

2024 HORIZON



IN 2024, INDIVIDUALS FROM 55 COUNTRIES REPRESENTING MORE THAN 42% OF THE GLOBAL POPULATION WILL PARTICIPATE IN PRESIDENTIAL, PARLIAMENTARY AND/OR GENERAL ELECTIONS. THIS INCLUDES SEVEN OF THE 10 MOST POPULOUS COUNTRIES IN THE WORLD



eCrime Landscape

New Vulnerabilities with 9/10 CVSS3 Score

+6%

BGH Incidents Involving Data Leaks

+76%

Average Loader Cost

+169%

Average Crypter Cost

+250%

Average Stealer Cost

+286%

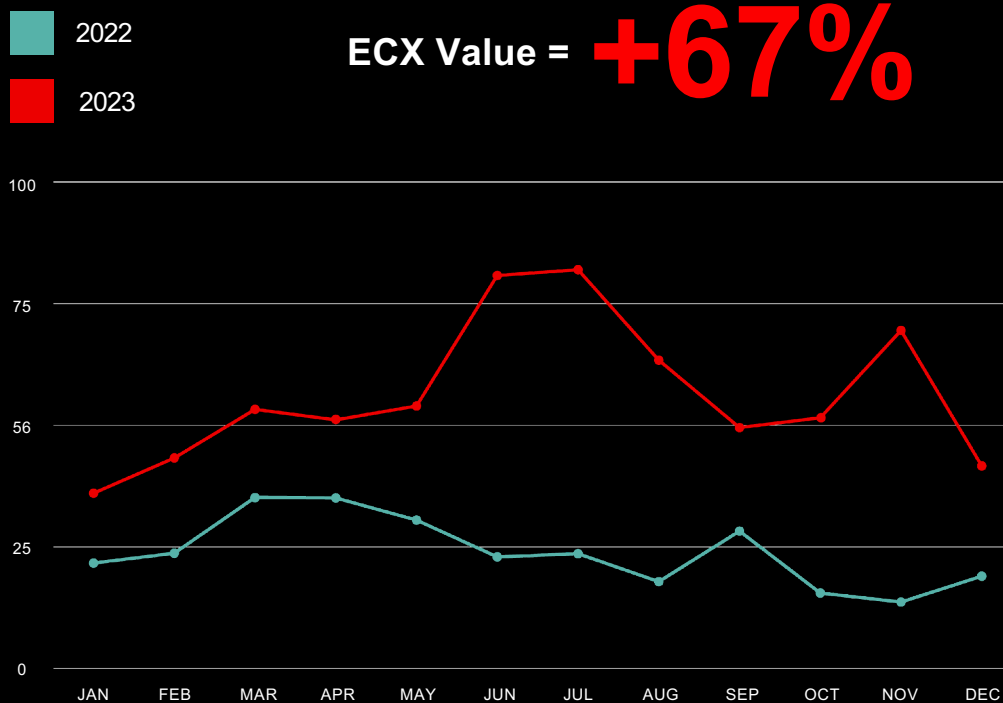
Average Ransom Demand

-27%

Identified Spam Emails

-15%

ECX Value = **+67%**



5 STEPS TO BE PREPARED

1 Identity Protection

2 Effective Cloud Security

3 Cross-Domain Threat Hunting

4 Speed: Outpace the Adversary

5 Practice Makes Perfect

CrowdStrike 2024 Global Threat Report



To get a deeper dive into the findings in the report, download your copy today!

[Download the Full Report](#)



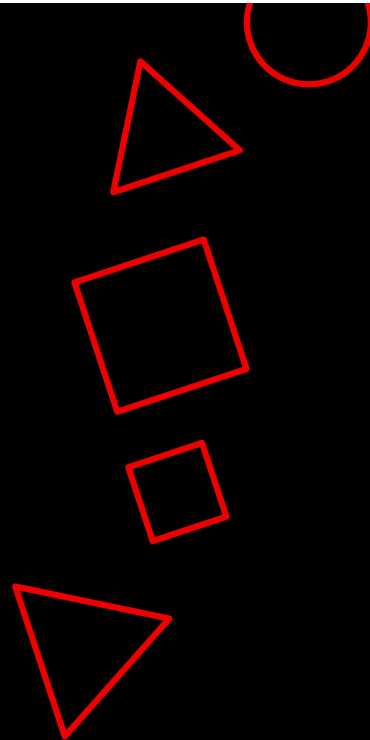


 **CROWDSTRIKE**

CUSTOMERS WANT MORE WITH LESS



MISSION-CRITICAL
Stop increasingly
sophisticated threats



FRAGMENTED
Too many point
products and agents

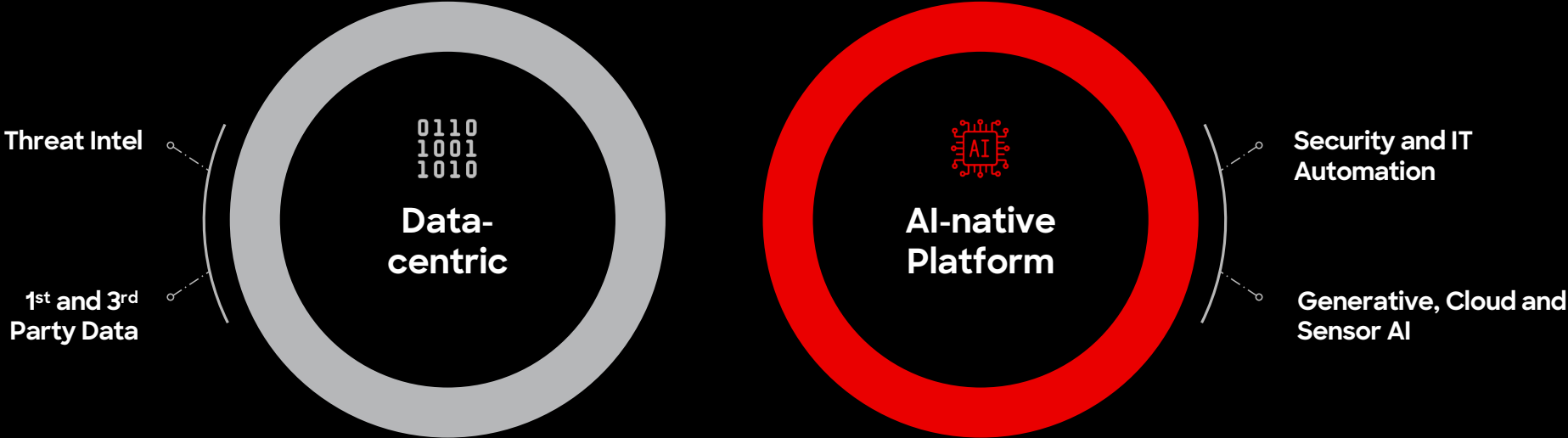


COSTLY
Relentlessly
rising expenses



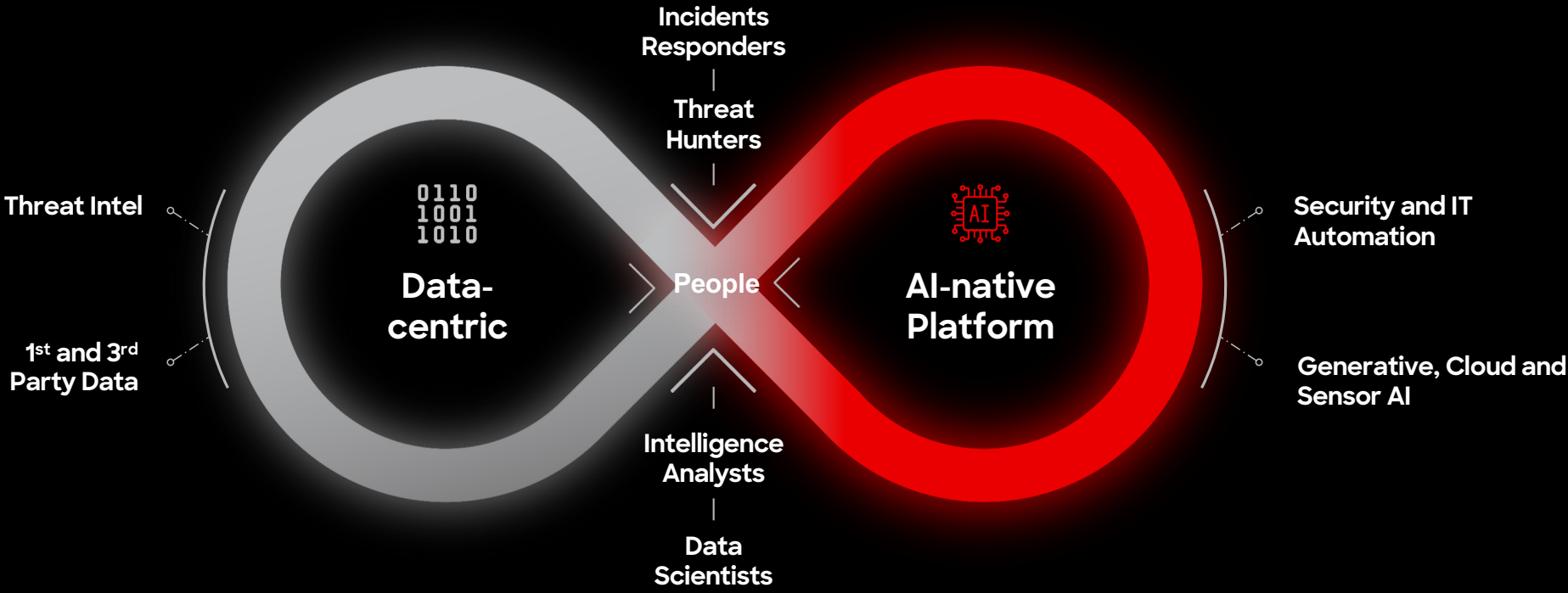


WE PIONEERED A DATA-CENTRIC PLATFORM APPROACH





WE PIONEERED A DATA-CENTRIC PLATFORM APPROACH





ALTERNATE APPROACHES FAIL TO STOP THE BREACH



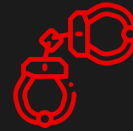
Legacy

Antiquated, reactive signature solutions fail to stop modern attacks



Imitators

Bolt-on point features fail to deliver a scalable data-centric platform



Lock-in

Multiple stitched “platforms” create protection gaps and impact scalability and usability



Monoculture

OS and cloud vendor dependence fails to reduce risk, and creates opportunity to exploit at scale



CROWDSTRIKE BUILT CYBERSECURITY'S AI-NATIVE PLATFORM FOR THE XDR ERA

Sum of the Components is Greater Than the Parts

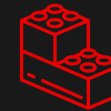
CROWDSTRIKE



Cloud Native
Architecture by
Design



Single Platform,
Console, Agent



Open,
Extensible

OTHERS



Stitched
Together
Products



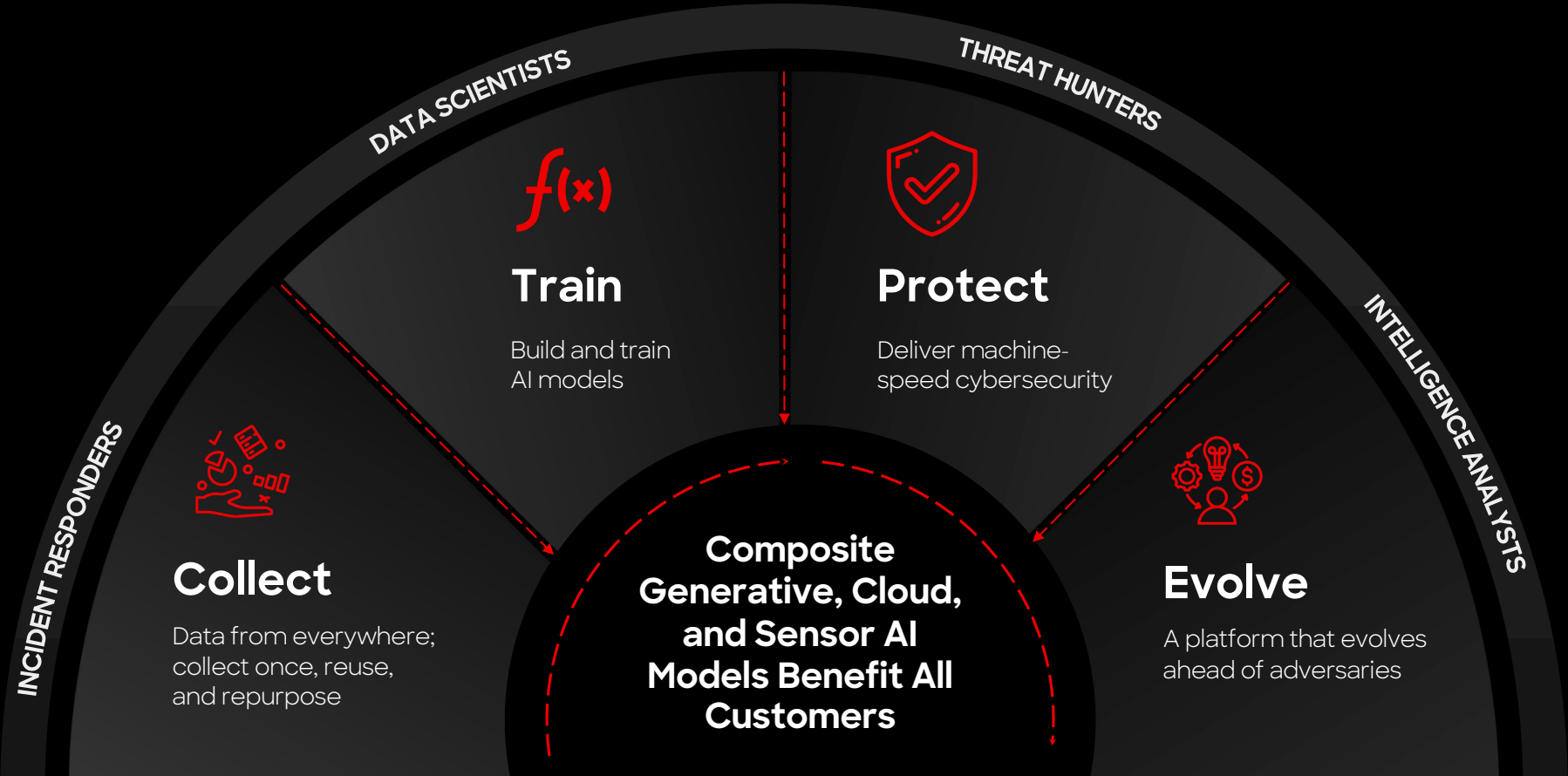
Many Platforms,
Consoles, Agents



Closed

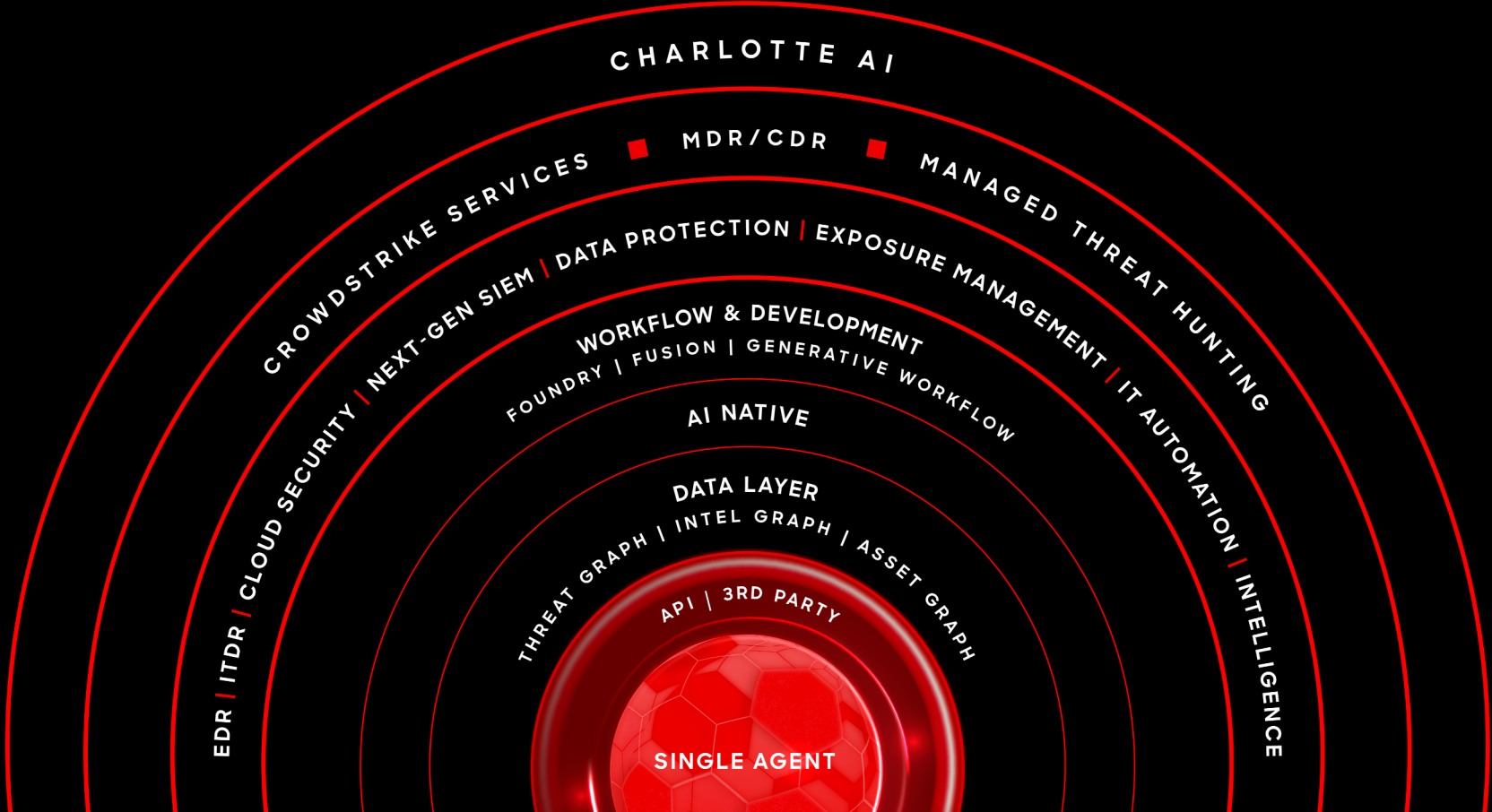


OUR DATA EXPERTISE CREATES A VIRTUOUS CYCLE, UNLOCKING THE POWER OF CRWD AI





CROWDSTRIKE'S FALCON XDR PLATFORM STOPS BREACHES





DATA COLLECTION IS AT OUR FOUNDATION, COLLECT ONCE, REUSE MANY

One Lightweight Agent Delivers All Capabilities, No Reboots Required

“CrowdStrike’s product benefits from the broad set of raw endpoint telemetry collected, mature and customizable EDR functionality, lightweight security agent, and app-store-like agent expansion capability.”





A DATA LAYER PUTS ALL OF THIS DATA IN CONTEXT

Threat Graph: Advanced AI and behavioral analysis techniques correlate trillions of events in real time to prevent advanced attacks

Intel Graph: Enriches all events with world-class adversary intelligence to understand and prioritize emerging attacks

Asset Graph: Comprehensive 360-degree visibility into all assets, managed and unmanaged, to minimize risk and simplify IT operations





AI NATIVE ARCHITECTURE FINDS THE SIGNALS IN THE NOISE

Machine Learning trained on the world's highest-fidelity security data

3x Improved vulnerability prioritization with EXPRT.AI

Behavioral AI and Custom LLMs

“CrowdStrike leads the industry with regards to the application of artificial intelligence/machine learning to endpoint security, as well as providing unparalleled prevention of malware and malware-free attacks on and off the network.”

FROST & SULLIVAN





WORKFLOW AND DEVELOPMENT TURN INSIGHTS INTO ACTION

Build your own workflows with Fusion

Build your own apps with Foundry

Do it all faster with Generative Workflow

Find new solutions on Marketplace





VALIDATED, TESTED AND CERTIFIED

Gartner

2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms



A Leader in the 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for the fourth consecutive time

FORRESTER



CrowdStrike named a Leader in the Forrester Wave for Cloud Workload Security, Q1 2024

Tested

MITRE

100% protection, visibility & analytic detection in Round 5 of MITRE Engenuity ATT&CK Evaluations: Enterprise

Highest detection coverage across all 16 vendors in 2023 MITRE ATT&CK evaluation for managed services



100% ransomware protection



100% legitimate accuracy rating

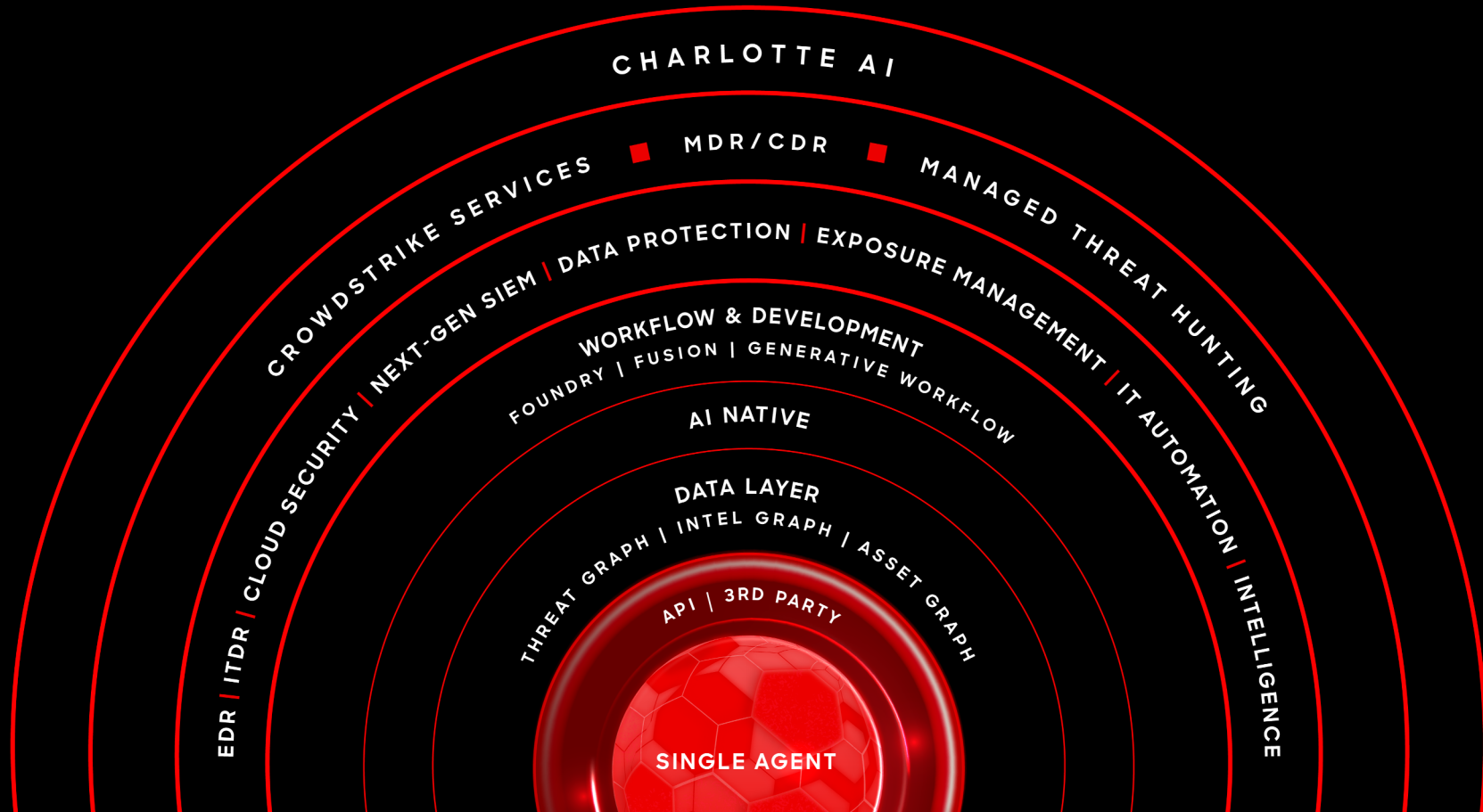


100% macOS malware protection

Certified



CROWDSTRIKE'S FALCON XDR PLATFORM STOPS BREACHES



A hand holding a wooden gavel over a stack of papers. A dark blue rectangular overlay is positioned in the center, containing the text 'Q&A' in white. The background is a blurred office setting. There are teal and red decorative squares in the corners.

Q&A

A hand holding a wooden stamp over a document, with a dark blue overlay containing the text 'Next steps'. The background is a blurred office setting with a stack of papers and a keyboard. The text is centered in a white, bold, sans-serif font.

Next steps

How Inetum-Realdolmen can help



At Inetum-Realdolmen, we understand the importance of cybersecurity and the need to comply with regulatory frameworks such as NIS2

We provide tools and guidance to help you meet the minimum measures required by NIS2, such as risk assessments, security procedures, and incident response plans

Our team of cybersecurity experts can work with you to assess your current security posture and develop a customized security plan that meets your specific needs

You can have peace of mind knowing that your systems and data are protected by industry-leading security solutions.

CYBERSECURITY ACCELERATOR PROGRAM



Identify & Inspire

- Audit & Assessment
- Ethical hacking
- Roadmap
- Proof of Concept

Protect & Integrate

- Zero Trust implementation
 - Identities
 - Devices
 - Data
 - Applications
 - Networks & Infrastructure

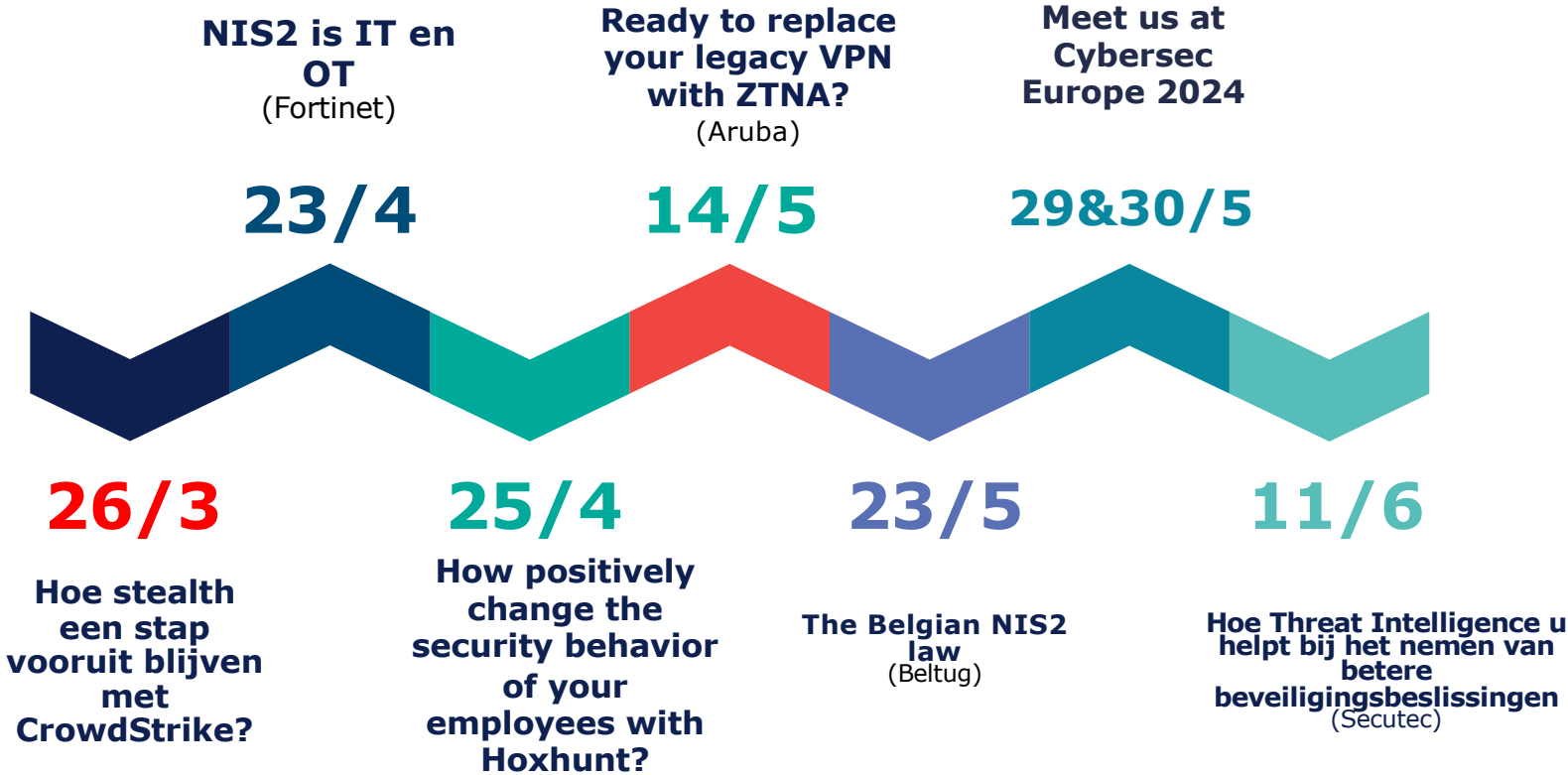
Detect & Operate

- Managed Security Services
- Vulnerability Management
- MDR Services

Respond & Optimize

- Incident Response
- Governance
- CISO as a Service
- User Awareness

Opvolgevents NIS2





Contacteer ons via:

- info@inetum-realdolmen.world
- Uw vertrouwde contactpersoon bij Inetum-Realdolmen

A close-up photograph of a hand holding a wooden-handled stamp over a document. The stamp has a brass base. The document is slightly out of focus. A dark blue rectangular box is overlaid on the image, containing the word 'Bedankt' in white text. The background is dark and blurred. There are teal and red decorative elements in the corners of the image.

Bedankt