# IT Track

## Hoe cyberaanvallers voorblijven in 2024

# Wolfgang Meert

Sales engineer CrowdStrike

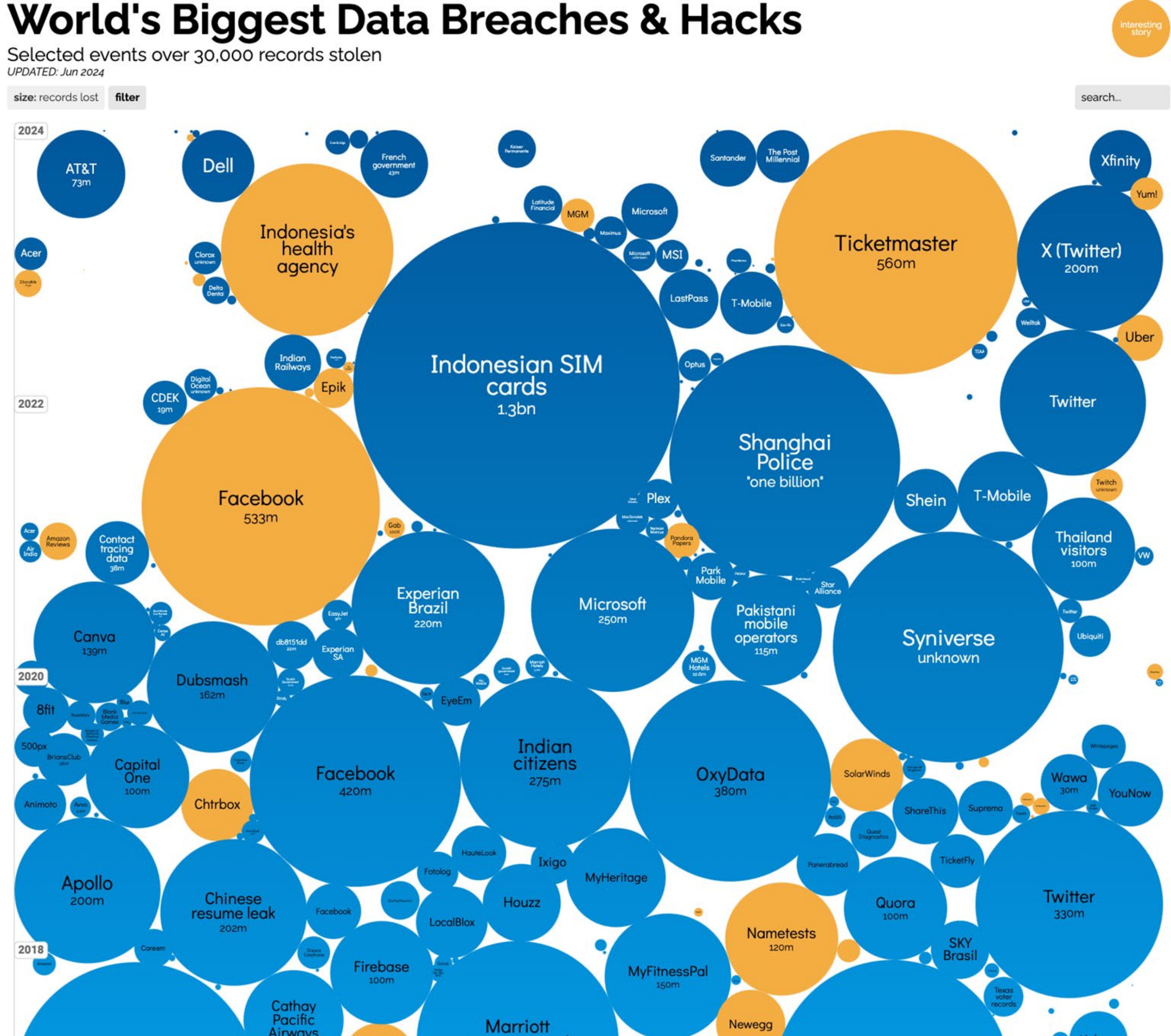
CROWDSTRIKE

# CrowdStrike 2024 Global Threat Report

Wolfgang Meert –Sales Engineer

# Agenda

- Threat Landscape
- Major Themes
- eCrime Landscape
- Recommendations



# World's Biggest Data Breaches & Hacks

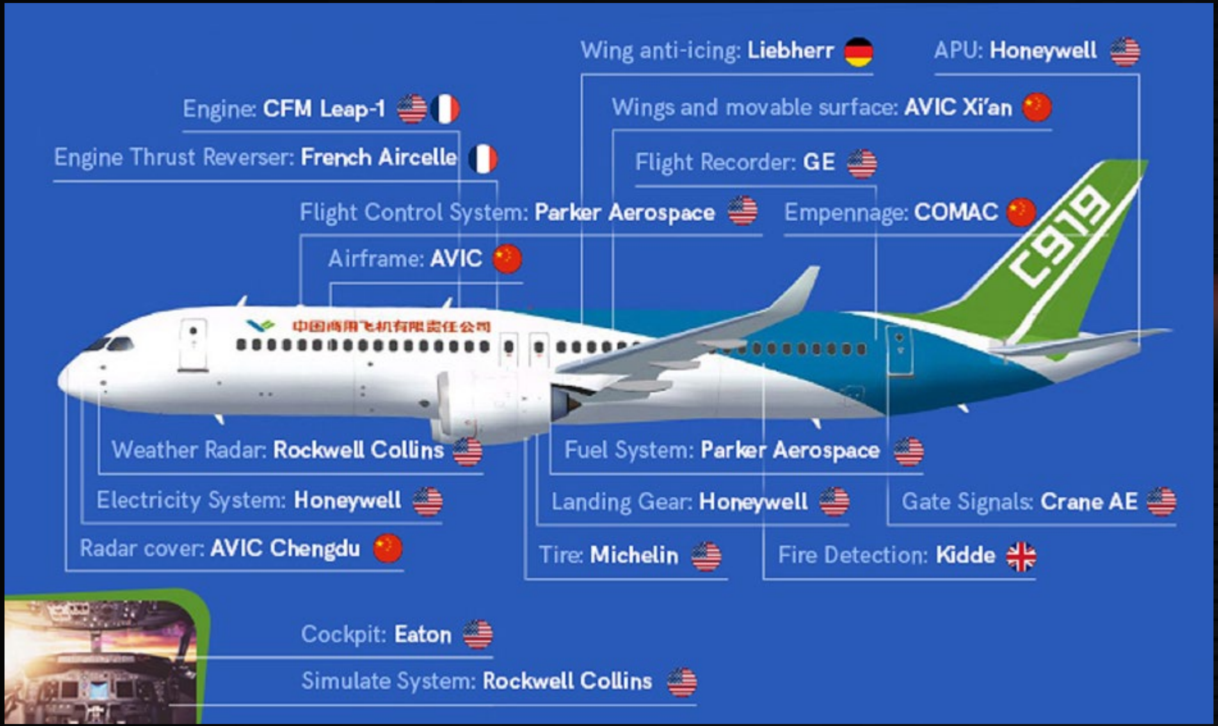
Selected events over 30,000 records stolen

*UPDATED: Jun 2024*

Source https://informationisbeautiful.net/

# We stop breaches

中国南方航空
CHINA SOUTHERN
C919
B-002L
COMAC C919



Wing anti-icing: **Liebherr** 🇩🇪

APU: **Honeywell** 🇺🇸

Engine: **CFM Leap-1** 🇺🇸 🇫🇷

Wings and movable surface: **AVIC Xi'an** 🇨🇳

Engine Thrust Reverser: **French Aircelle** 🇫🇷

Flight Recorder: **GE** 🇺🇸

Flight Control System: **Parker Aerospace** 🇺🇸

Empennage: **COMAC** 🇨🇳

Airframe: **AVIC** 🇨🇳

Weather Radar: **Rockwell Collins** 🇺🇸

Fuel System: **Parker Aerospace** 🇺🇸

Electricity System: **Honeywell** 🇺🇸

Landing Gear: **Honeywell** 🇺🇸

Gate Signals: **Crane AE** 🇺🇸

Radar cover: **AVIC Chengdu** 🇨🇳

Tire: **Michelin** 🇺🇸

Fire Detection: **Kidde** 🇬🇧

Cockpit: **Eaton** 🇺🇸

Simulate System: **Rockwell Collins** 🇺🇸

## 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

## 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

## 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

## ACTIVIST

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

# 2024 Threat Landscape

+34

232

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

110%

Cloud-conscious cases increased by **110% YoY**

$$$

84%

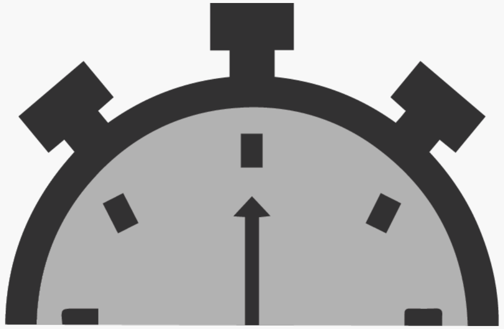
**84%** of adversary-attributed cloud-conscious intrusions were focused on eCrime

75%

Cloud environment intrusions increased by **75% YoY**

76%

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



## eCRIME BREAKOUT TIME

## 62’

Initial
Access
Lateral
Movement

Sen

# 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

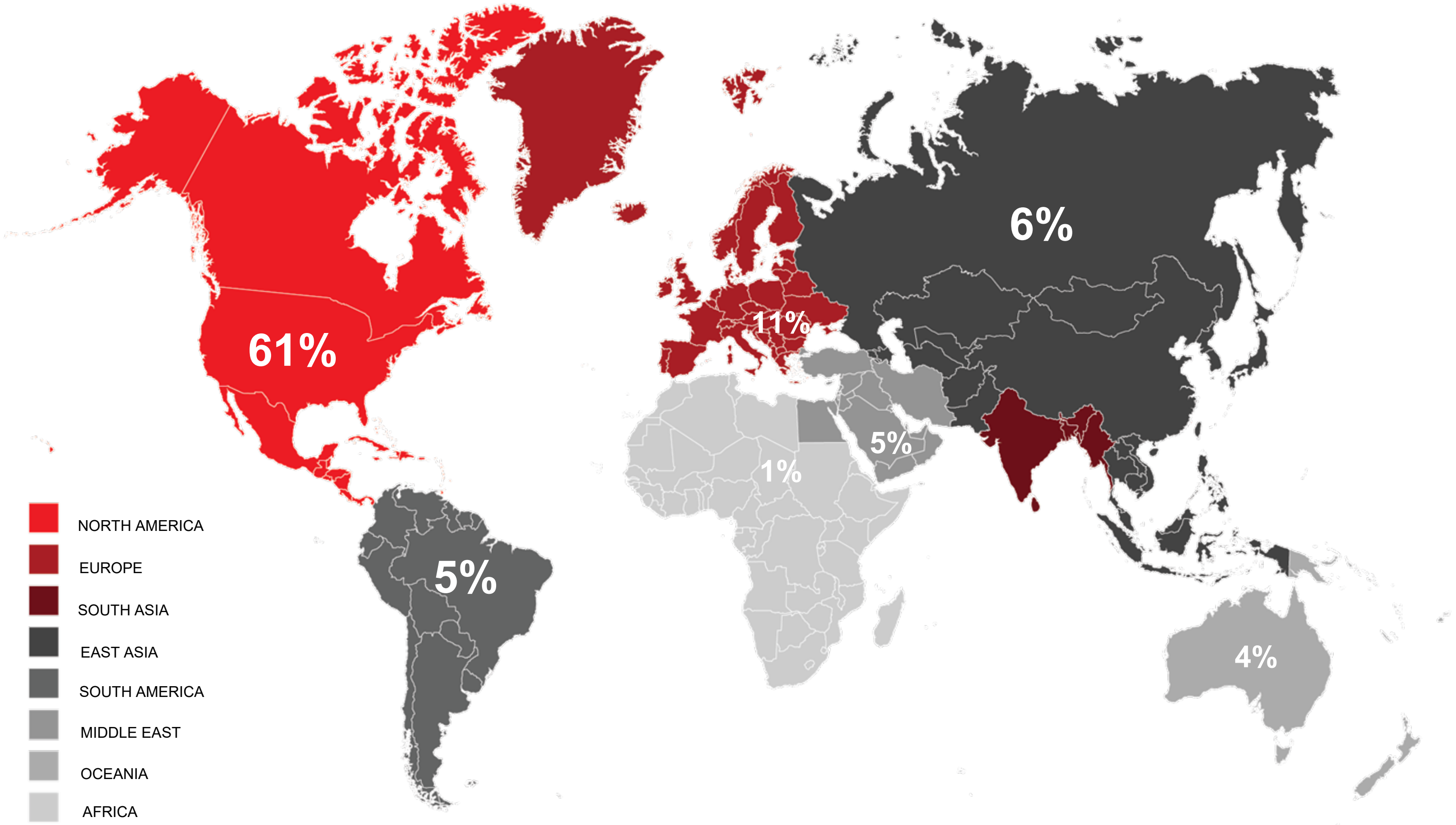
CROWDSTRIKE

# Malware -Free Initial Access

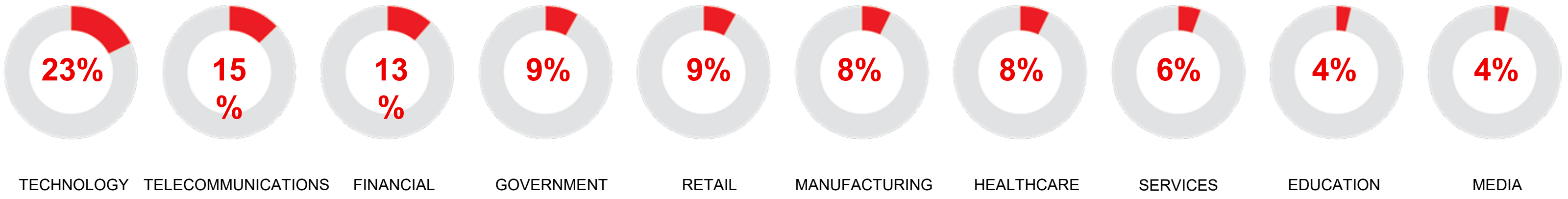
»

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

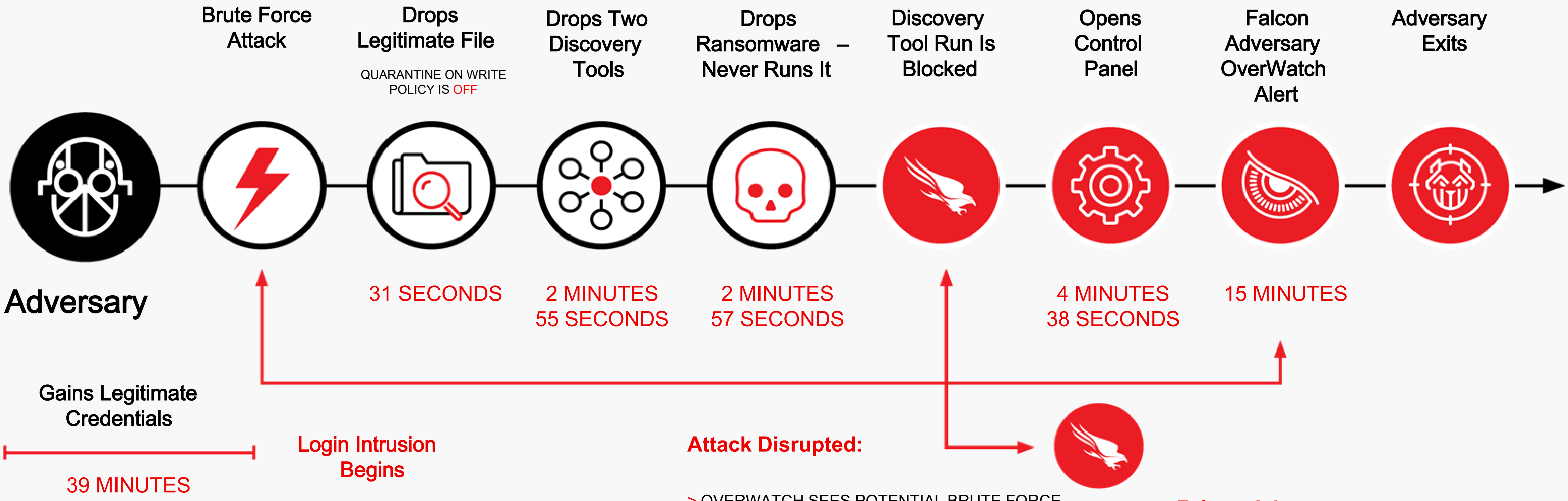
## Interactive Intrusions by Region



## Interactive Intrusions by Industry



# Identity Is the Critical Battleground



Adversary

Brute Force Attack

Drops Legitimate File

QUARANTINE ON WRITE POLICY IS OFF

31 SECONDS

Drops Two Discovery Tools

2 MINUTES 55 SECONDS

Drops Ransomware – Never Runs It

2 MINUTES 57 SECONDS

Discovery Tool Run Is Blocked

Opens Control Panel

4 MINUTES 38 SECONDS

Falcon Adversary OverWatch Alert

15 MINUTES

Adversary Exits

Gains Legitimate Credentials

39 MINUTES

Login Intrusion Begins

**Attack Disrupted:**

> OVERWATCH SEES POTENTIAL BRUTE FORCE

> OVERWATCH SEES SUSPICIOUS FILES DROPPED

> FALCON SENSOR BLOCKS AND QUARANTINES DISCOVERY TOOL

**Falcon Adversary OverWatch Response:**

> HOST NETWORK ISOLATED

> PASSWORD RESET

# 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

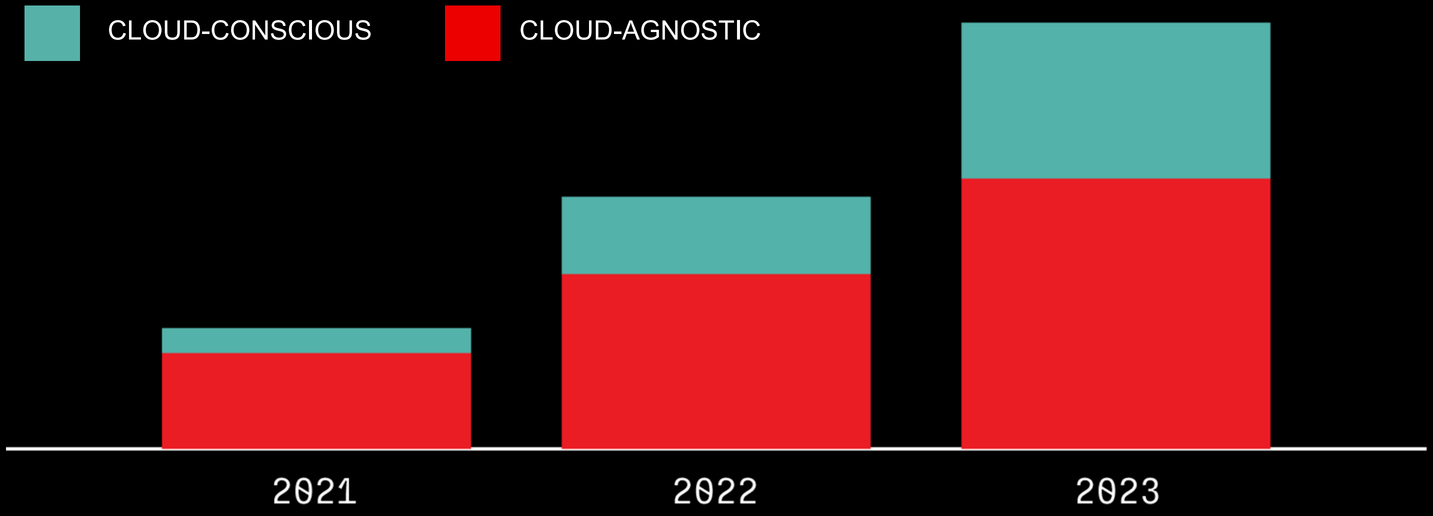
Conducted sophisticated social engineering campaigns

»

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%

# ADVERSARIES CONTINUE TO DEVELOP CLOUD- CONSCIOUSNESS

## INCIDENTS IN THE CLOUD



↑75%

IN CLOUD-CONSCIOUS CASES

▲ 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

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

# 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

»

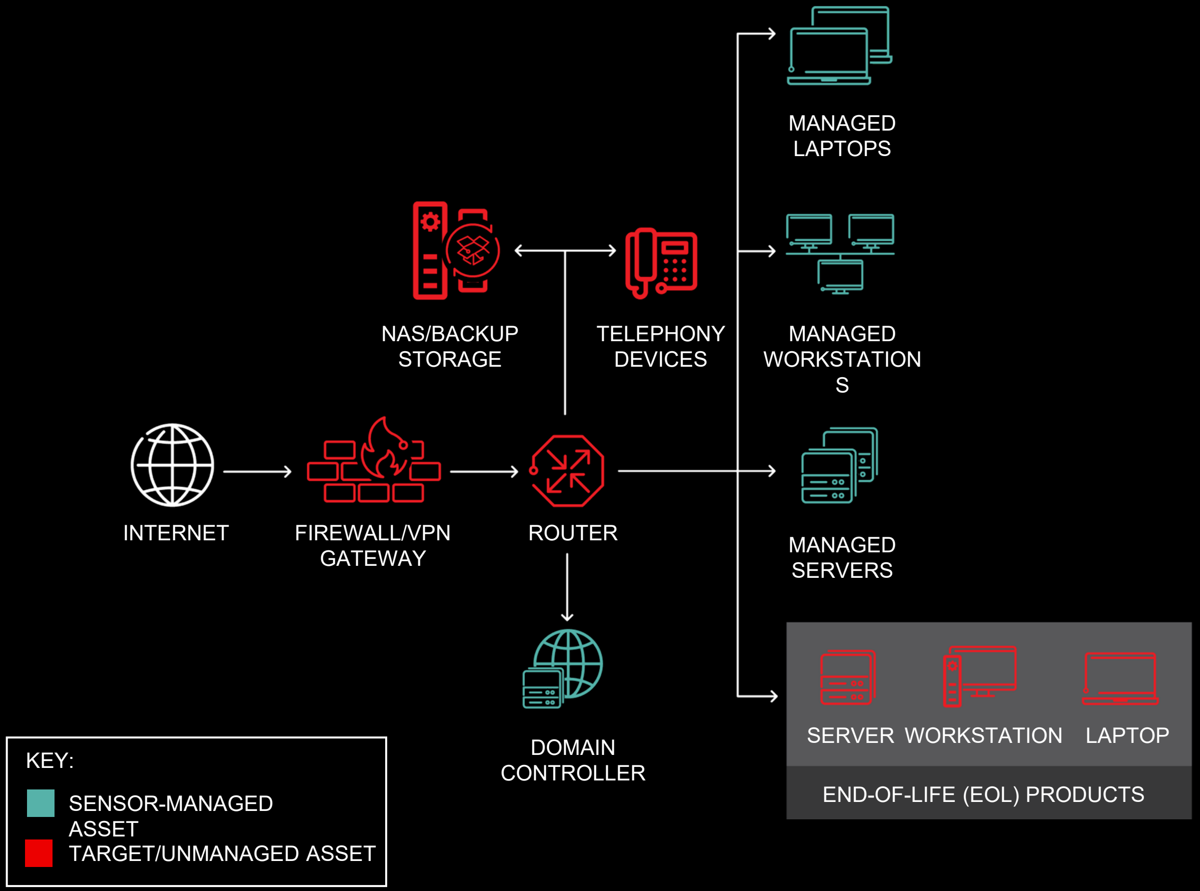
UNMANAGED NETWORK APPLIANCES – PARTICULARLY EDGE GATEWAY DEVICES – REMAINED THE MOST ROUTINELY OBSERVED INITIAL ACCESS VECTOR FOR EXPLOITATION DURING 2023

»

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



KEY:

🟩 SENSOR-MANAGED ASSET

🟥 TARGET/UNMANAGED ASSET

# 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

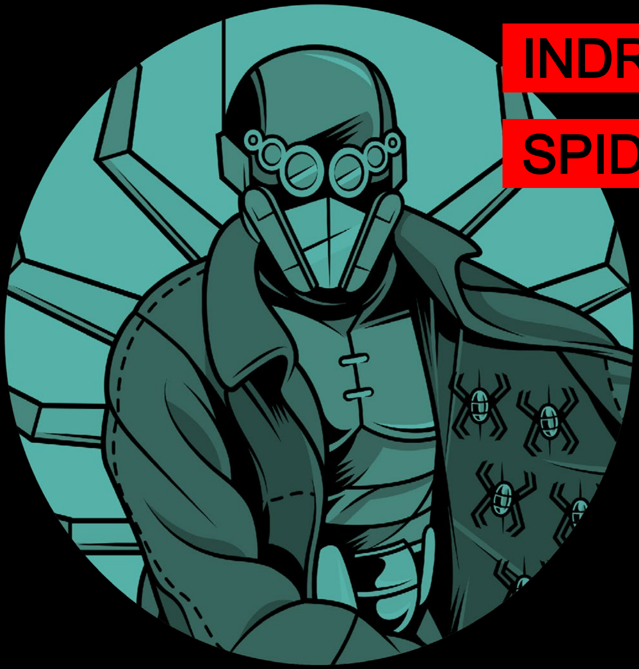
## Hamas Activity Not Observed

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



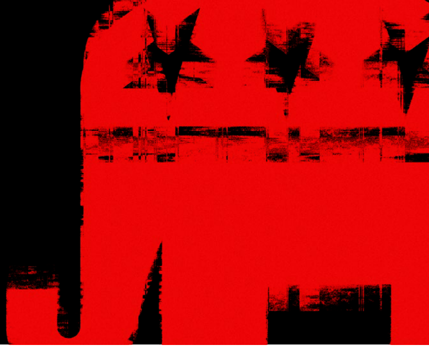
INDRIK SPIDER

SCATTERED SPIDER

»

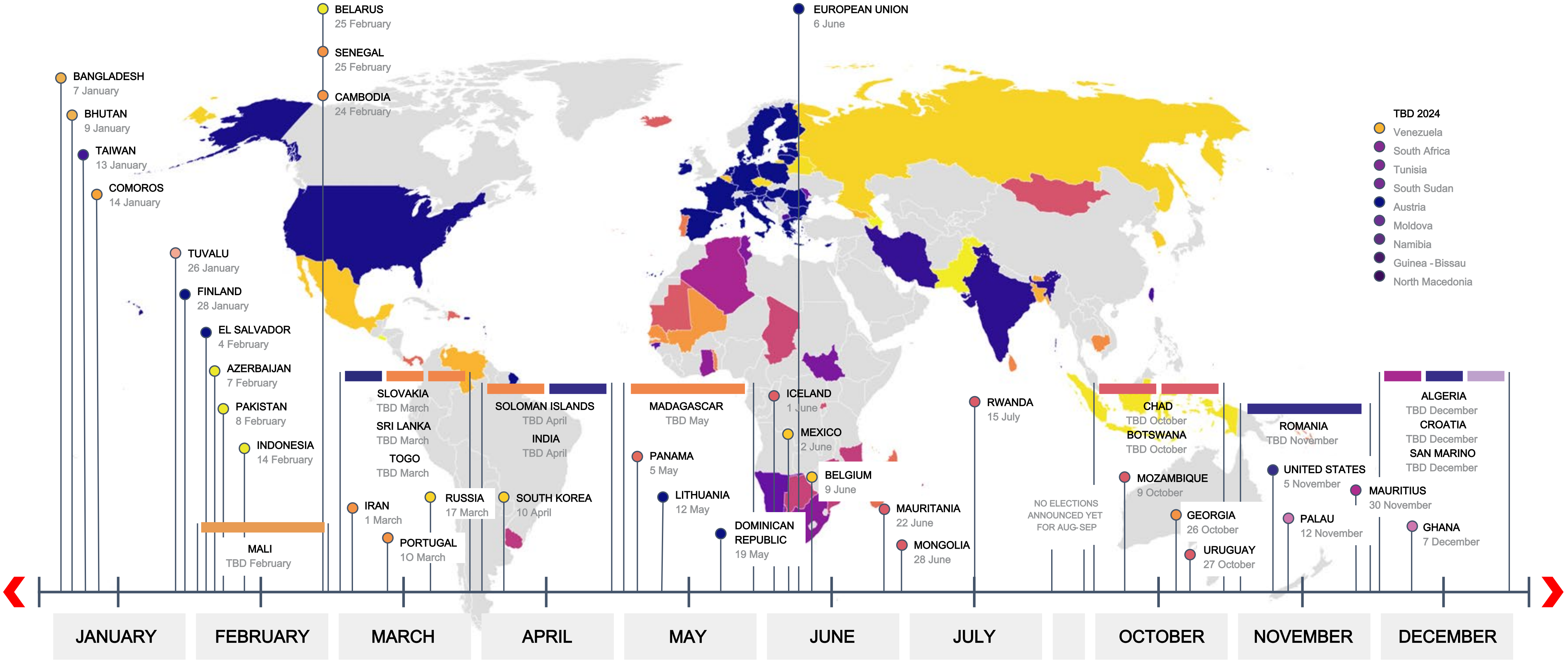
GENERATIVE AI HAS MASSIVELY DEMOCRATIZED COMPUTING TO IMPROVE ADVERSARY OPERATIONS. IT CAN ALSO POTENTIALLY LOWER THE ENTRY BARRIER TO THE THREAT LANDSCAPE FOR LESS SOPHISTICATED THREAT ACTORS.

# 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



BANGLADESH
7 January

BHUTAN
9 January

TAIWAN
13 January

COMOROS
14 January

TUVALU
26 January

FINLAND
28 January

EL SALVADOR
4 February

AZERBAIJAN
7 February

PAKISTAN
8 February

INDONESIA
14 February

MALI
TBD February

CAMBODIA
24 February

SENEGAL
25 February

BELARUS
25 February

SLOVAKIA
TBD March

SRI LANKA
TBD March

TOGO
TBD March

IRAN
1 March

PORTUGAL
1O March

RUSSIA
17 March

SOLOMAN ISLANDS
TBD April

INDIA
TBD April

SOUTH KOREA
10 April

MADAGASCAR
TBD May

PANAMA
5 May

LITHUANIA
12 May

DOMINICAN REPUBLIC
19 May

ICELAND
1 June

MEXICO
2 June

EUROPEAN UNION
6 June

BELGIUM
9 June

MAURITANIA
22 June

MONGOLIA
28 June

RWANDA
15 July

NO ELECTIONS ANNOUNCED YET FOR AUG-SEP

CHAD
TBD October

BOTSWANA
TBD October

MOZAMBIQUE
9 October

GEORGIA
26 October

URUGUAY
27 October

ROMANIA
TBD November

UNITED STATES
5 November

PALAU
12 November

MAURITIUS
30 November

ALGERIA
TBD December

CROATIA
TBD December

SAN MARINO
TBD December

GHANA
7 December

TBD 2024
- ● Venezuela
- ● South Africa
- ● Tunisia
- ● South Sudan
- ● Austria
- ● Moldova
- ● Namibia
- ● Guinea -Bissau
- ● North Macedonia

JANUARY | FEBRUARY | MARCH | APRIL | MAY | JUNE | JULY | OCTOBER | NOVEMBER | DECEMBER

# 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%**

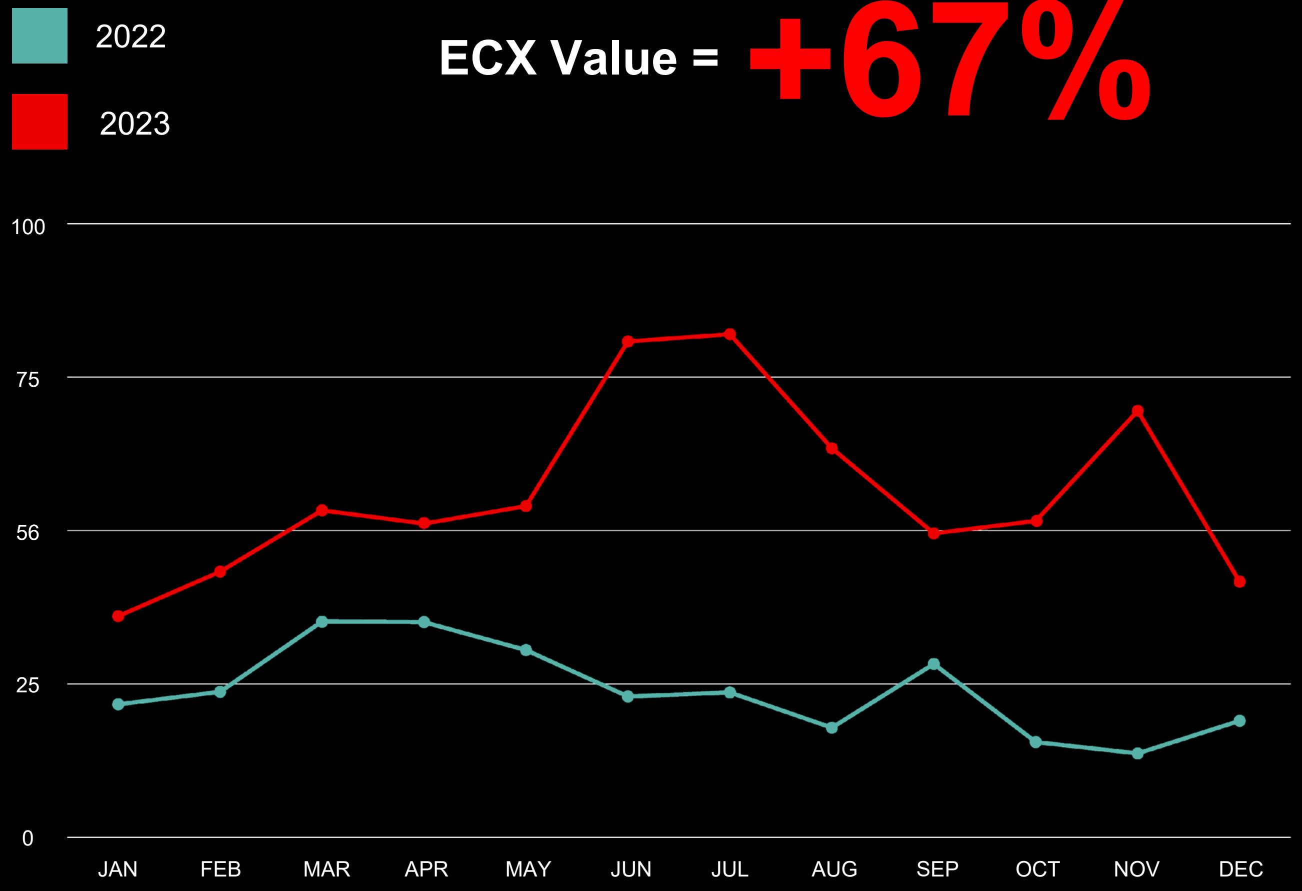
Average Ransom Demand

**-27%**

Identified Spam Emails

**-15%**

ECX Value = **+67%**



# 5 STEPS TO BE PREPARED

1 Identity Protection

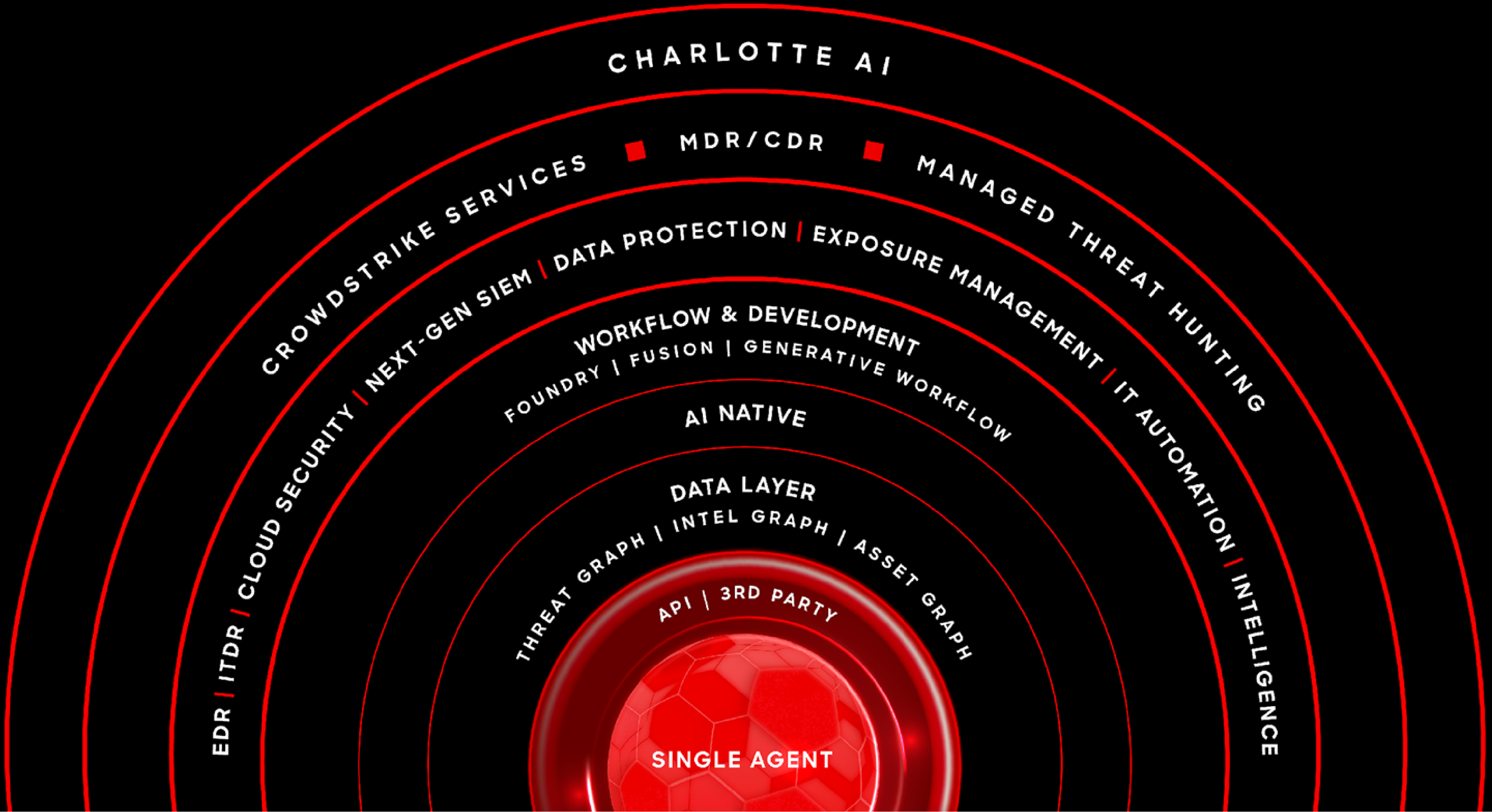
2 Effective Cloud Security

3 Cross - Domain Threat Hunting

4 Speed: Outpace the Adversary

5 Practice Makes Perfect

# CROWDSTRIKE’S FALCON XDR PLATFORM STOPS BREACHES


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

# 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

# Thank You