CROWDSTRIKE

In the Cross-Hairs:
Protecting the Public’s Data

Public Sector Threat Brief - Q3 2023
Matt Singleton, CrowdStrike

CROWDSTRIKE

MATT SINGLETON

Executive Strategist

HIGHER ED GOVERNMENT CONSULTING

- **25+ years:** Innovating at the intersection of security, education & digital transformation
- **State Government:** Former Chief Information Security Officer for the State of Oklahoma; Chief Operations Officer for the state's IT division; State Chief Information Officer for Education
- **Higher Education:** Developed cybersecurity strategy and program for the University of Oklahoma system; Led innovation arm of OU IT; Professor of Cybersecurity
- **Education:** M.P.S. – Applied Intelligence, specializing in Cyber Intel, Homeland Security & Counterterrorism from Georgetown University; B.A. – Administrative Leadership from the University Of Oklahoma
- **Thought Leadership:** Momentum, National Association of State Technology Directors; Hunt, Bourne and Ryan are Amateurs, Threatday

AGENDA

The Global Threat Landscape

Public Sector Specific Threats

The Way Forward

GLOBAL THREAT LANDSCAPE

- Volume/Speed/Sophistication of Attacks
- Adversaries
- Top Current Threats
  - Third-Party Software
  - Cloud Exploitation
  - Access Brokers/Identity

THREE PRIMARY METRICS FOR MEASURING THE ADVERSARY

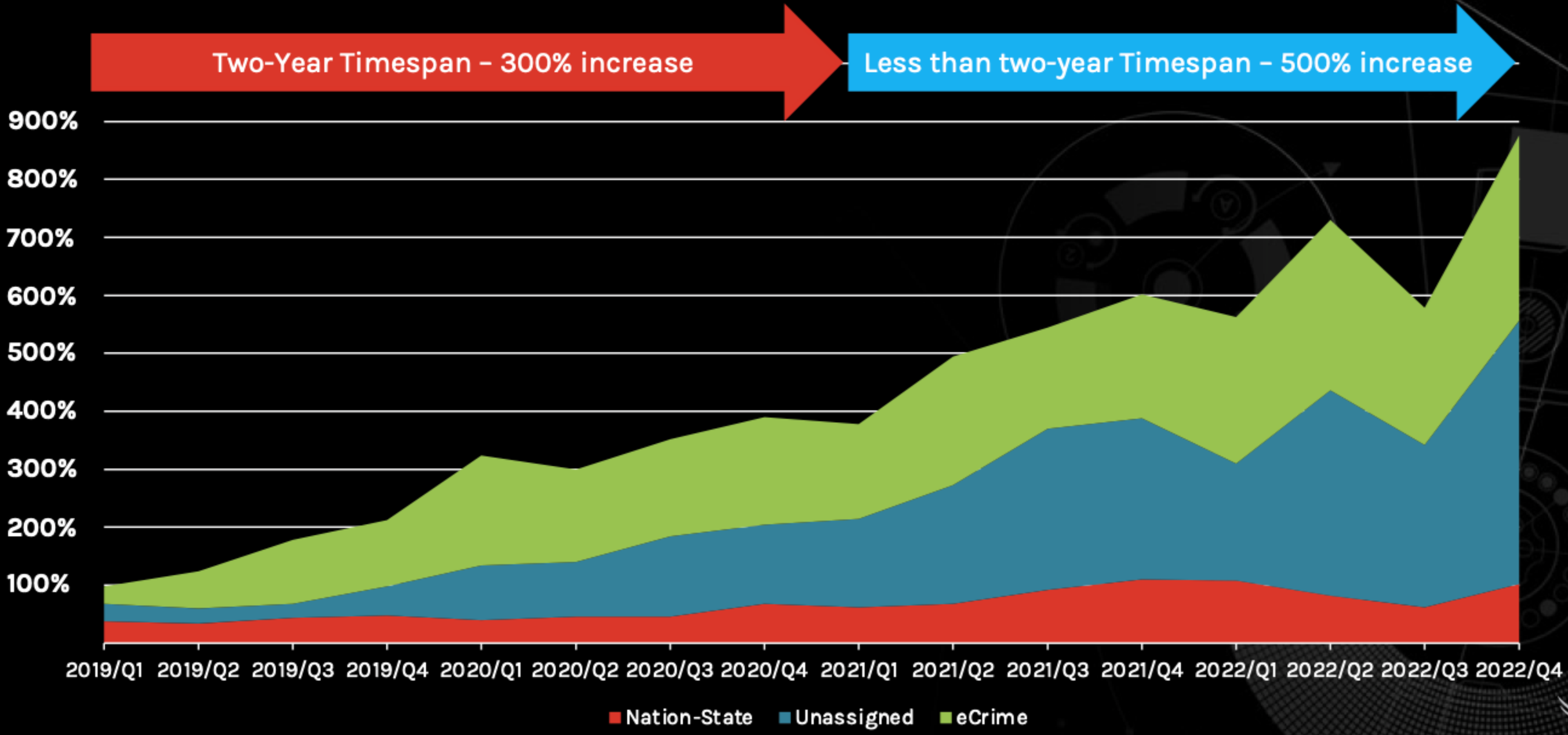
Volume

Speed

Sophistication

Volume Speed Sophistication

CROWDSTRIKE DISTINCT & SOPHISTICATED INTRUSION TELEMETRY



Two-Year Timespan – 300% increase

Less than two-year Timespan – 500% increase

eCrime Breakout Time

79 min

Every Second Counts

Adversaries are getting faster, defenders must accelerate

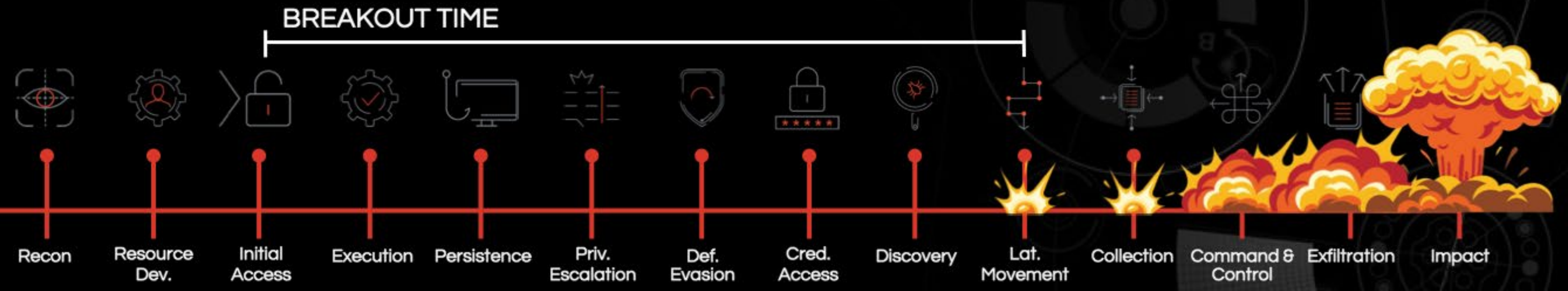
Breakout time has dropped from **9 hours and 42 min** in 2018 to only **79 min in 2023**

THE NECESSITY OF SPEED

Survival of the Fastest

TO STAY AHEAD YOU MUST:

DETECT IN	INVESTIGATE IN	RESPOND IN
1min	10min	60min



BREAKOUT TIME

Recon

Resource Dev.

Initial Access

Execution

Persistence

Priv. Escalation

Def. Evasion

Cred. Access

Discovery

Lat. Movement

Collection

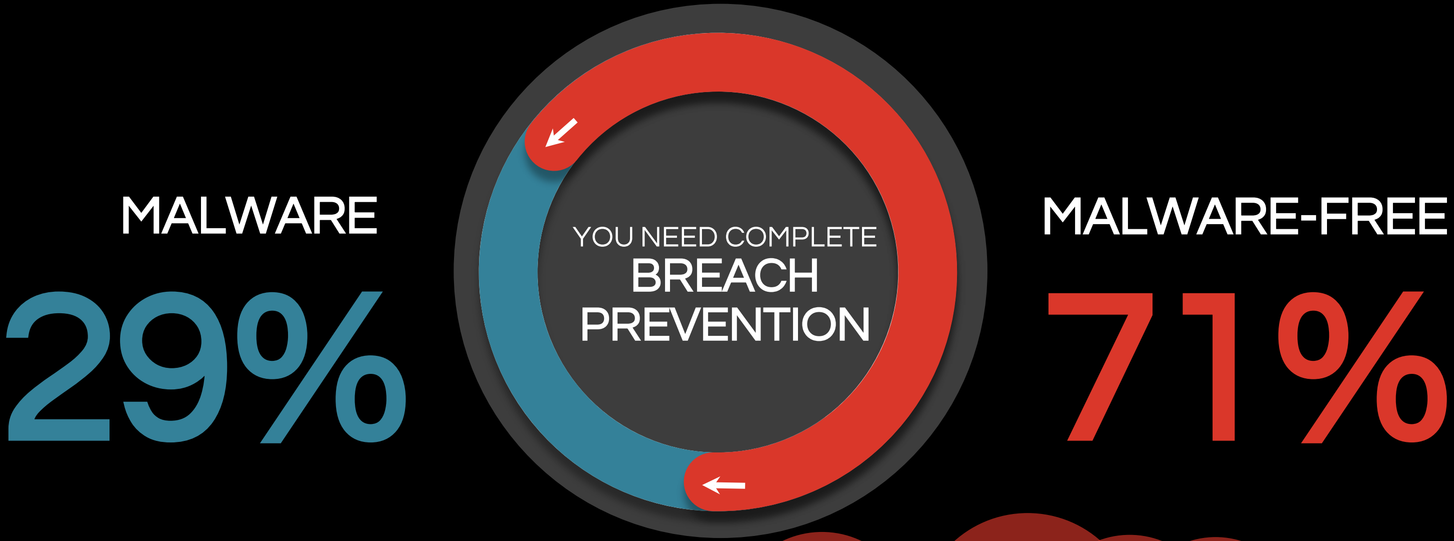
Command & Control

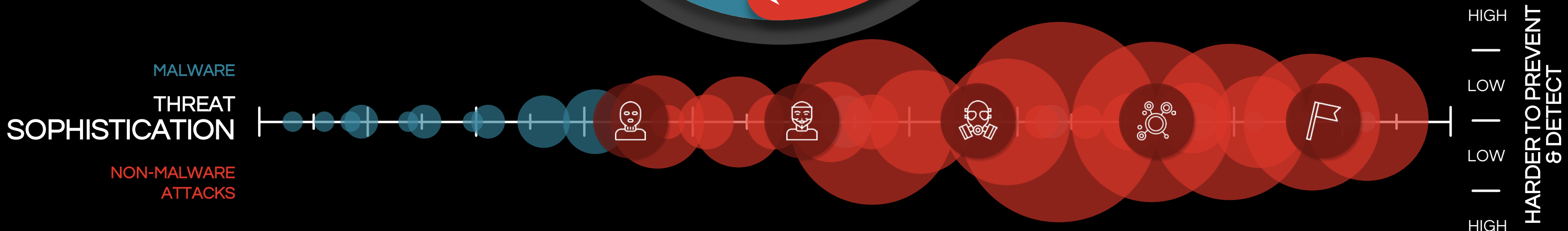
Exfiltration

Impact

MITRE ATT&CK PHASE

Complexity: Malware versus Malware-Free Attacks





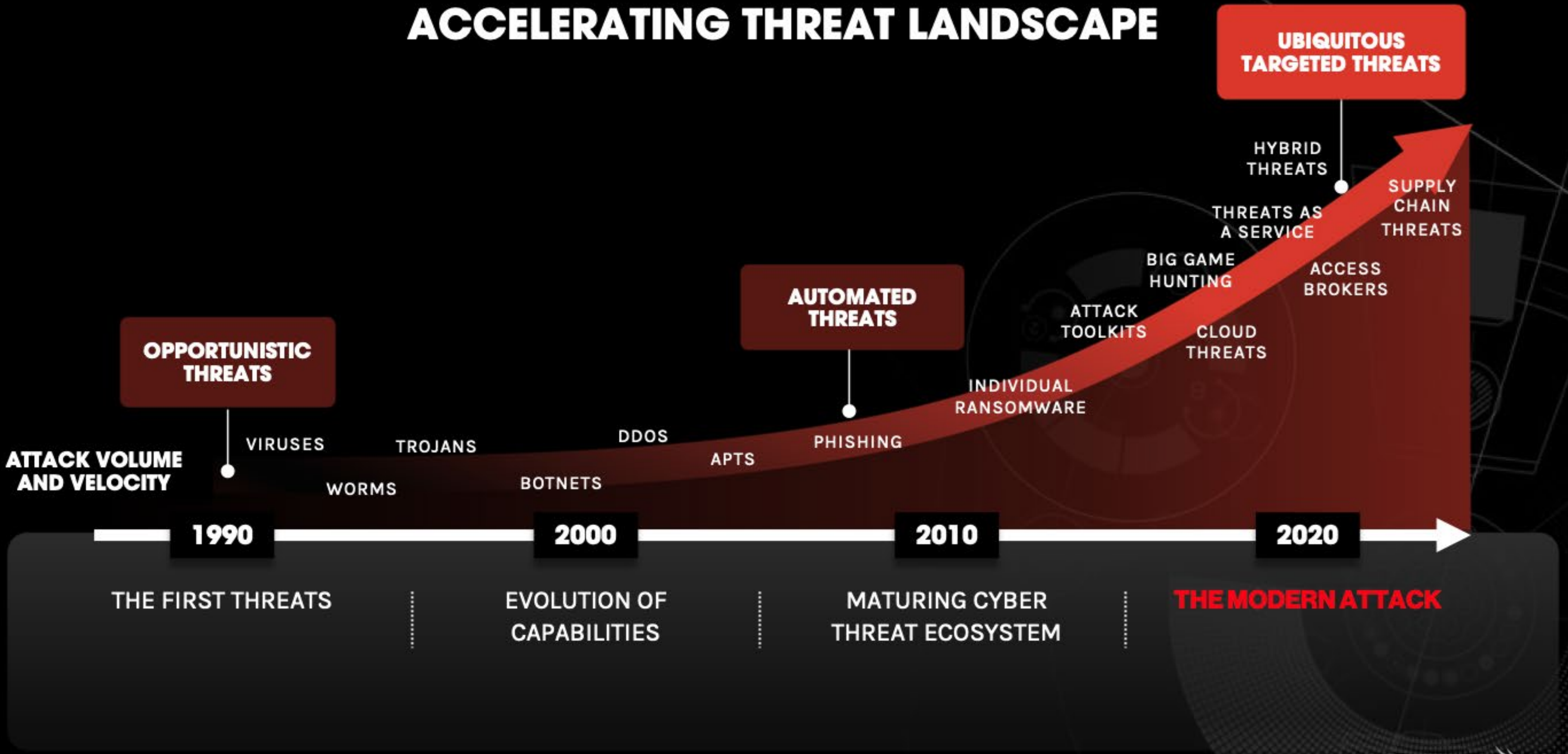
https://www.crowdstrike.com/resources/reports/overwatch-threat-hunting-report/

CROWDSTRIKE

CROWDSTRIKE

Volume Speed Sophistication

ACCELERATING THREAT LANDSCAPE



UBIQUITOUS TARGETED THREATS

AUTOMATED THREATS

OPPORTUNISTIC THREATS

ATTACK VOLUME AND VELOCITY

VIRUSES

WORMS

TROJANS

BOTNETS

DDOS

APTS

PHISHING

INDIVIDUAL RANSOMWARE

ATTACK TOOLKITS

BIG GAME HUNTING

CLOUD THREATS

THREATS AS A SERVICE

HYBRID THREATS

ACCESS BROKERS

SUPPLY CHAIN THREATS

1990 | 2000 | 2010 | 2020

THE FIRST THREATS

EVOLUTION OF CAPABILITIES

MATURING CYBER THREAT ECOSYSTEM

THE MODERN ATTACK

ADVERSARIES TRACKED BY CROWDSTRIKE

STATE-SPONSORED

Cryptonym: Panda, Bear, Kitten, Chollima...

Motive: Geopolitical or financial gain
Method: disruption, espionage, or manipulation

CRIMINAL

Cryptonym: Spider

Motive: Financial gain
Method: Fraud, data theft, extortion, etc.

HACKTIVIST / TERRORIST

Cryptonym: Jackal

Motive: Attention
Method: disruption or disclosure

CROWDSTRIKE

TOP CURRENT TRENDS

3rd PARTY SOFTWARE VULNERABILITIES

CLOUD-BASED ATTACKS

IDENTITY-BASED BYPASS

CrowdStrike 2023 Cloud Risk Report

Cloud exploitation is on the rise

95%

increase in cloud exploitation

3x

increase in cases involving cloud-conscious adversaries

Adversaries sharpening cloud TTPs

COZY BEAR:
uses malicious tools to modify cloud services

SCATTERED SPIDER:
deployed ransomware from a cloud staging env.

LABYRINTH CHOLLIMA:
uses cloud resources to deliver documents with malicious macros

COSMIC WOLF:
Targets victim data stored within cloud environments

Identity is a key cloud access point

Valid accounts are used to gain initial access in **43%** of cloud-based intrusions

In **67%** of cloud security instances. roles have elevated privileges beyond what was required

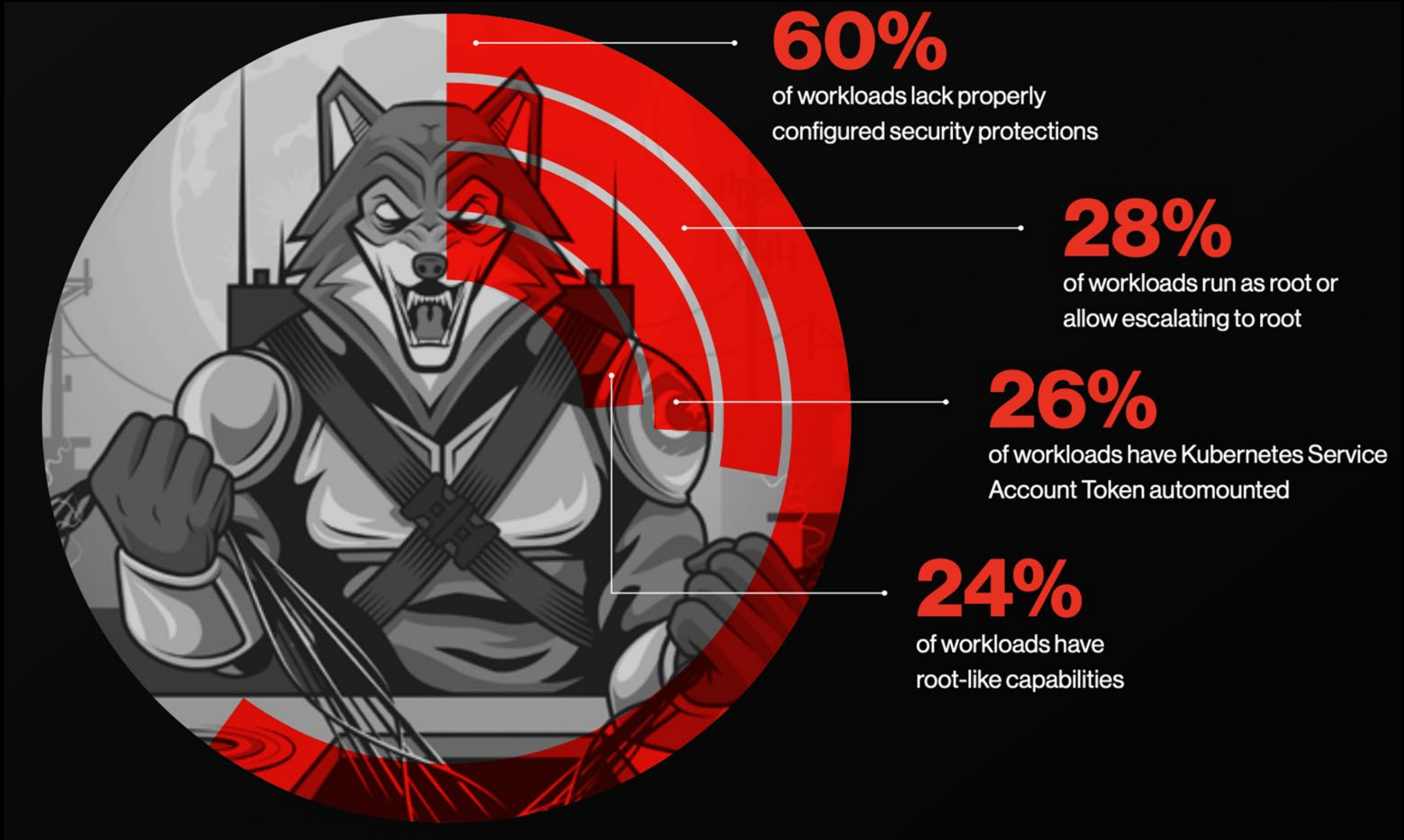
CROWDSTRIKE

A Growing Threat: Insecure Configurations

Human error drives cloud risk

99%

Of cloud security failures are the customer's fault
- Gartner



60% of workloads lack properly configured security protections

28% of workloads run as root or allow escalating to root

26% of workloads have Kubernetes Service Account Token automounted

24% of workloads have root-like capabilities

IDENTITY IS A PRIMARY ACCESS MECHANISM FOR THE ADVERSARY

80%

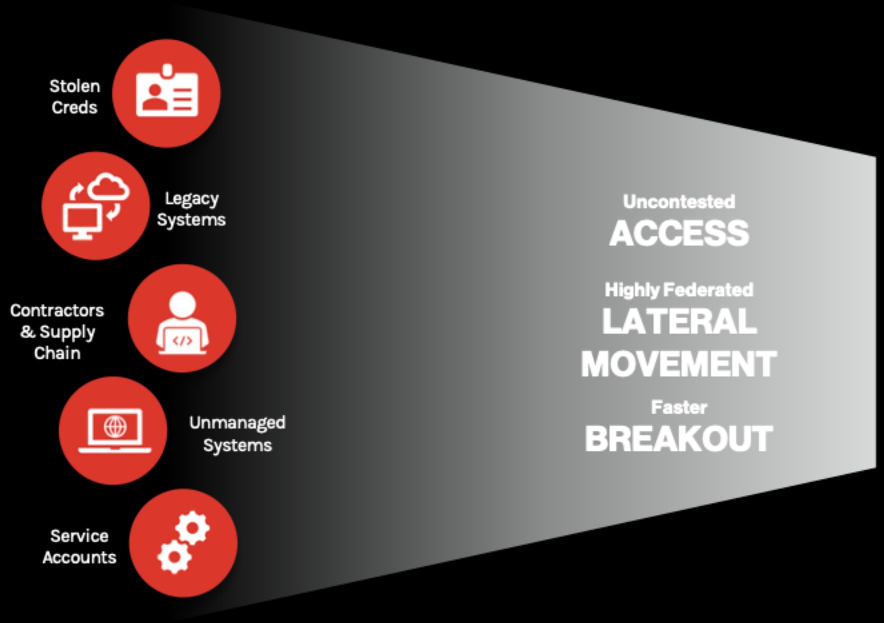
of data breaches have a connection to compromised privileged credentials

- Forrester Research

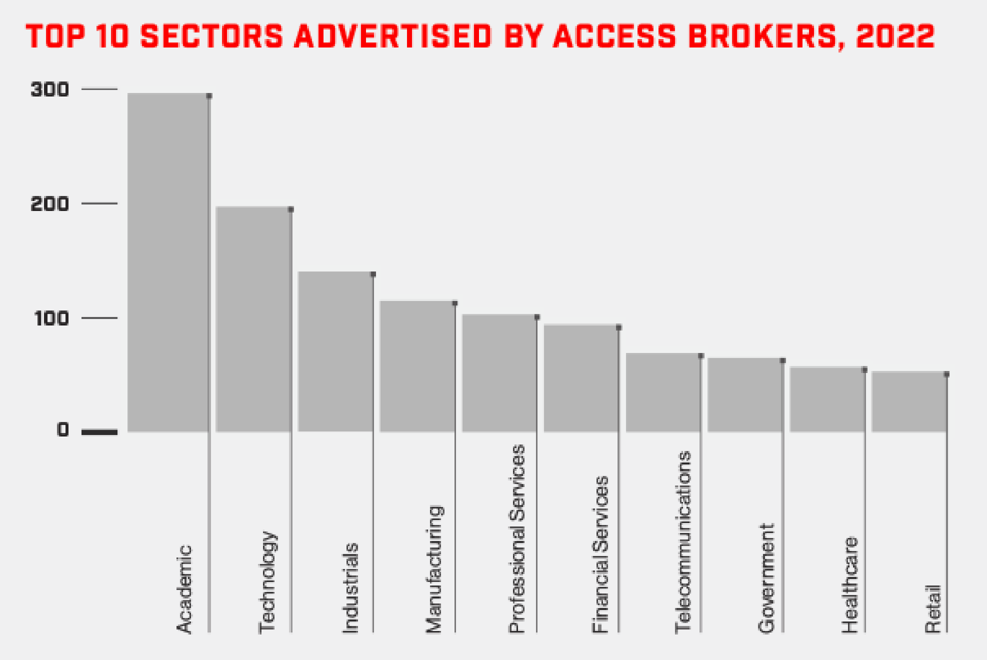
Breaches from stolen/compromised credentials took the longest to detect:

250 days

- Cost of a Breach Report, 2021



Access Broker Boom



Acceleration of demand

Popularity of services increasing with more than 2,500 advertisements – a 112% increase from 2021

Buy a la carte or in bulk

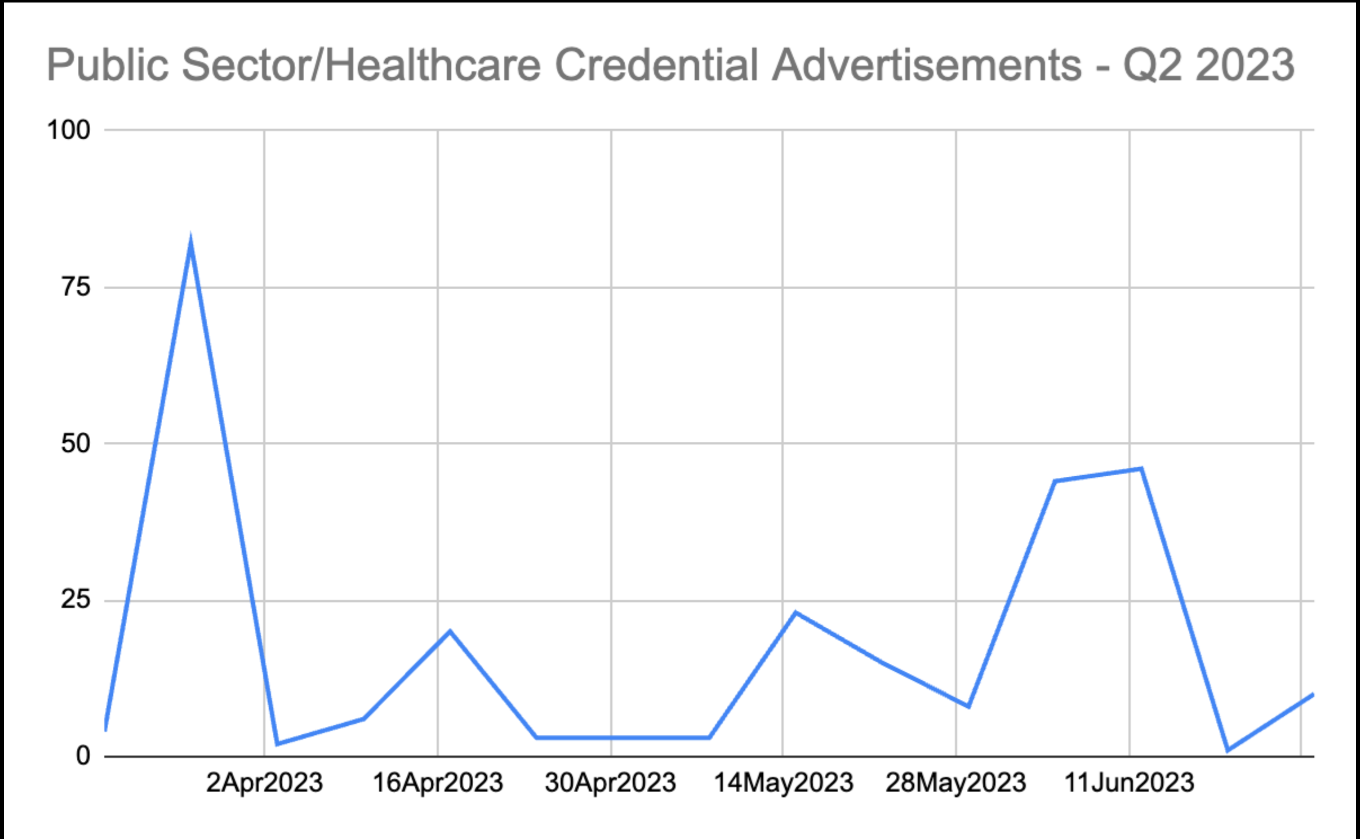
Several brokers will sell in bulk as others will use a "one-access, one-auction" technique.

Access methods remain consistent

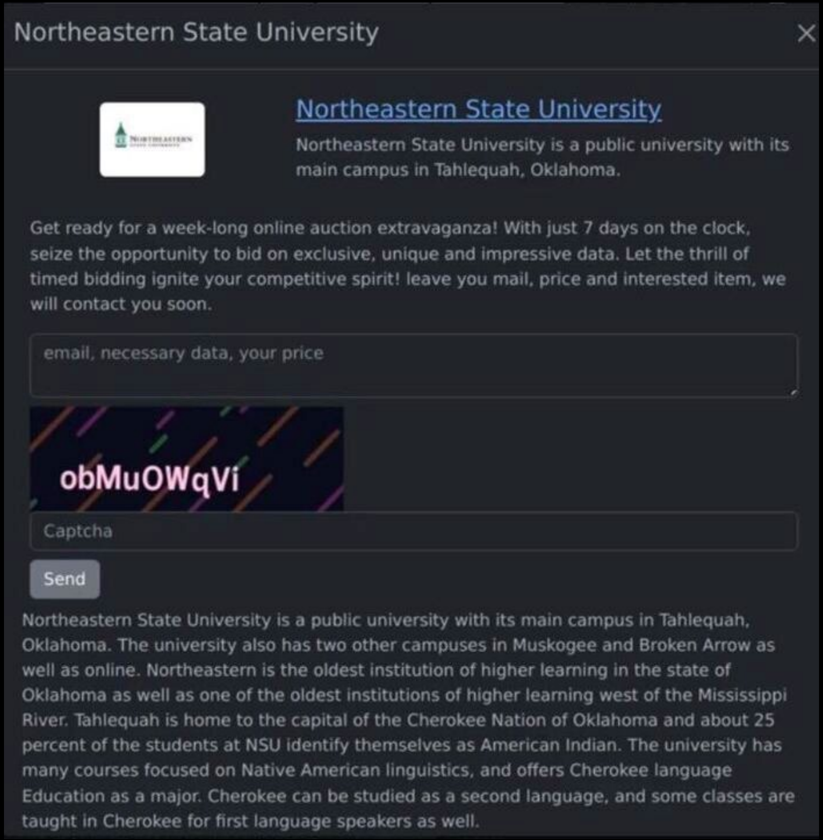
Abuse of compromised credentials obtained by information stealers or purchased in log shops on the dark web

> "80% of all breaches use compromised identities and 50% of organizations have experienced an Active Directory (AD) attack in the last two years."

PUBLIC SECTOR CREDENTIAL ADVERTISEMENTS - Q2 2023



DARK WEB ADVERTISEMENT



Northeastern State University
×
obMuOWqVi
email, necessary data, your price
Captcha
Send

Northeastern State University

Northeastern State University is a public university with its main campus in Tahlequah, Oklahoma.

Get ready for a week-long online auction extravaganza! With just 7 days on the clock, seize the opportunity to bid on exclusive, unique and impressive data. Let the thrill of timed bidding ignite your competitive spirit! leave you mail, price and interested item, we will contact you soon.

Northeastern State University is a public university with its main campus in Tahlequah, Oklahoma. The university also has two other campuses in Muskogee and Broken Arrow as well as online. Northeastern is the oldest institution of higher learning in the state of Oklahoma as well as one of the oldest institutions of higher learning west of the Mississippi River. Tahlequah is home to the capital of the Cherokee Nation of Oklahoma and about 25 percent of the students at NSU identify themselves as American Indian. The university has many courses focused on Native American linguistics, and offers Cherokee language Education as a major. Cherokee can be studied as a second language, and some classes are taught in Cherokee for first language speakers as well.

CROWDSTRIKE

PUBLIC SECTOR SPECIFIC THREATS

- Why Public Sector?
- The Growing Cyber Threat
- Denial of Service
- Ransomware & Data Extortion
- Third-Party Tools

WHY PUBLIC SECTOR?

- Large user base
- Public Safety implications
- Diverse end points
- High-profile
- Numerous stakeholders
- Federated IT/Cybersecurity models
- Under-resourced

PUBLIC SECTOR - ADVERSARY MOTIVATIONS

Nation State	eCrime	Hacktivist
14	17	4

CROWDSTRIKE

PUBLIC SECTOR - NATION STATE TRENDS

CHINA

3

DPRK (North Korea)

3

RUSSIA

4

IRAN

4

POTENTIAL DISRUPTIVE IMPACTS

TARGET: OPERATIONAL TECHNOLOGY INDUSTRY-SPECIFIC TOOLS

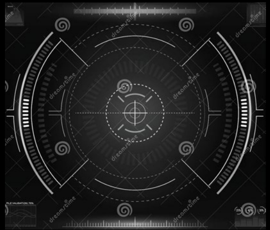
TARGET: INTELLECTUAL PROPERTY

MISSION CRITICAL

TARGET: MISSION CRITICAL APPLICATIONS

TARGET: PHYSICAL SAFETY/SECURITY SYSTEMS

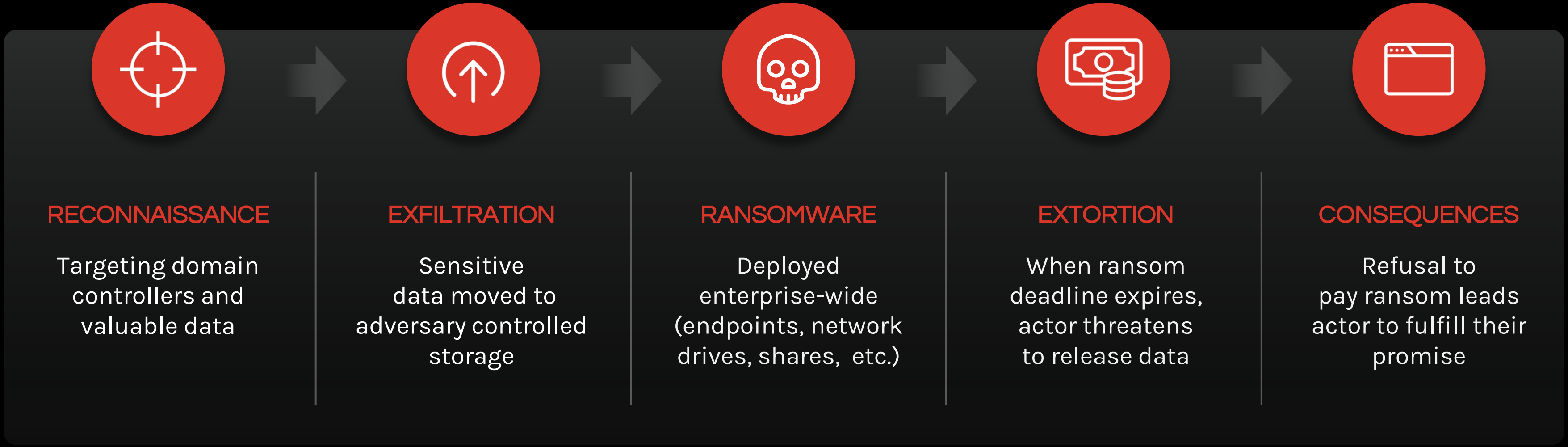
TARGET: PERSONALLY IDENTIFIABLE INFORMATION (PII)



TARGET: WEAPONIZABLE RESOURCES

CURRENT TREND: RANSOMWARE + DATA EXTORTION

Data extortion forces you to choose between the consequences of data leaks or the consequences of ransomware.



RECONNAISSANCE

Targeting domain controllers and valuable data

EXFILTRATION

Sensitive data moved to adversary controlled storage

RANSOMWARE

Deployed enterprise-wide (endpoints, network drives, shares, etc.)

EXTORTION

When ransom deadline expires, actor threatens to release data

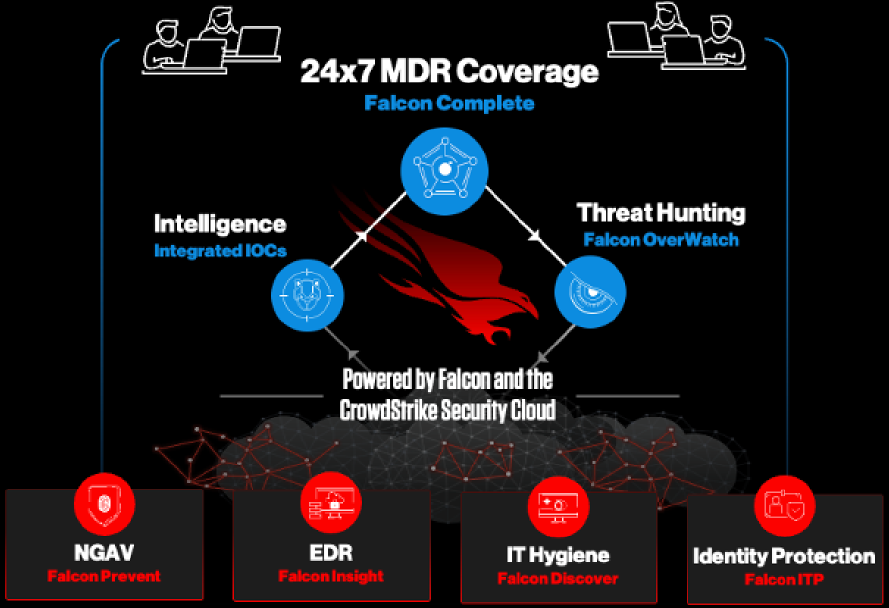
CONSEQUENCES

Refusal to pay ransom leads actor to fulfill their promise

THE WAY FORWARD

- Where We Need to Be
- CrowdStrike Recommendations
- Call to Action

WHERE WE NEED TO BE



- Dedicated 24 x 7 coverage t0 Prevent, Predict, Detect, Respond
- Complete visibility of our environment and risks
- Complementing state-provided security controls
- Reduced risk and increased productivity

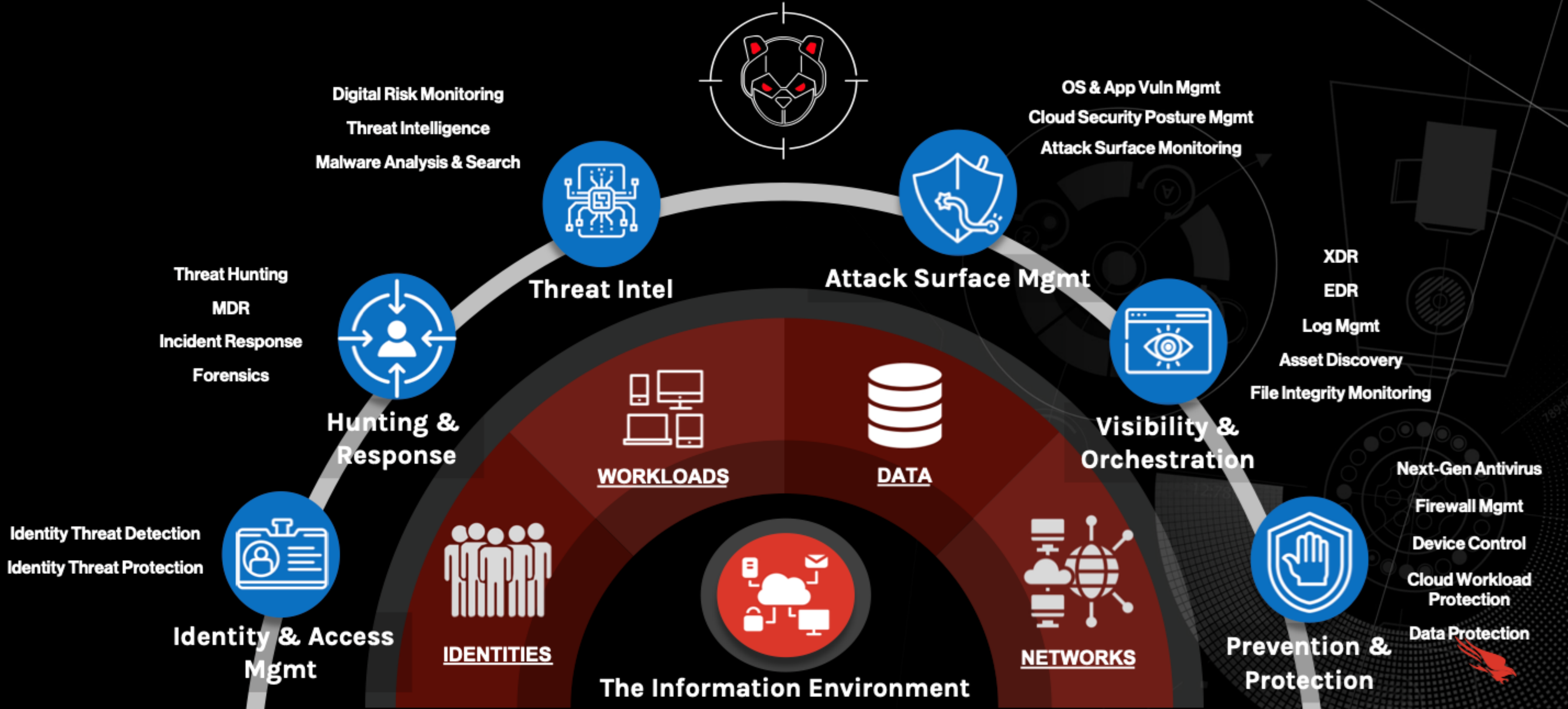
CrowdStrike Recommendations

- Join the MS-ISAC.
- Leverage free MS-ISAC services.*
- Engage in regional ISACs/ISAOs.
- Work with state organizations on the SLCGP.
- Participate in Whole-of-State strategies.
- Engage CrowdStrike RSM.
  - Conduct a free AD Assessment.
  - Conduct a free Cloud Security Assessment.

CROWDSTRIKE

*https://www.cisecurity.org/ms-isac/services

CALL TO ACTION: PROTECT THE INFORMATION ENVIRONMENT FROM THE ADVERSARY THROUGH A COMPREHENSIVE CYBERSECURITY STRATEGY



Identity & Access Mgmt
- Identity Threat Detection
- Identity Threat Protection

Hunting & Response
- Threat Hunting
- MDR
- Incident Response
- Forensics

Threat Intel
- Digital Risk Monitoring
- Threat Intelligence
- Malware Analysis & Search

Attack Surface Mgmt
- OS & App Vuln Mgmt
- Cloud Security Posture Mgmt
- Attack Surface Monitoring

Visibility & Orchestration
- XDR
- EDR
- Log Mgmt
- Asset Discovery
- File Integrity Monitoring

Prevention & Protection
- Next-Gen Antivirus
- Firewall Mgmt
- Device Control
- Cloud Workload Protection
- Data Protection

The Information Environment
- IDENTITIES
- WORKLOADS
- DATA
- NETWORKS

Matt.singleton@crowdstrike.com
www.linkedin.com/in/themattman