CROWDSTRIKE

Pivoting is Easy When You’re Prepared

Modern Solutions & Success Stories

TINA THORSTENSON

Quick Bio

TINA THORSTENSON

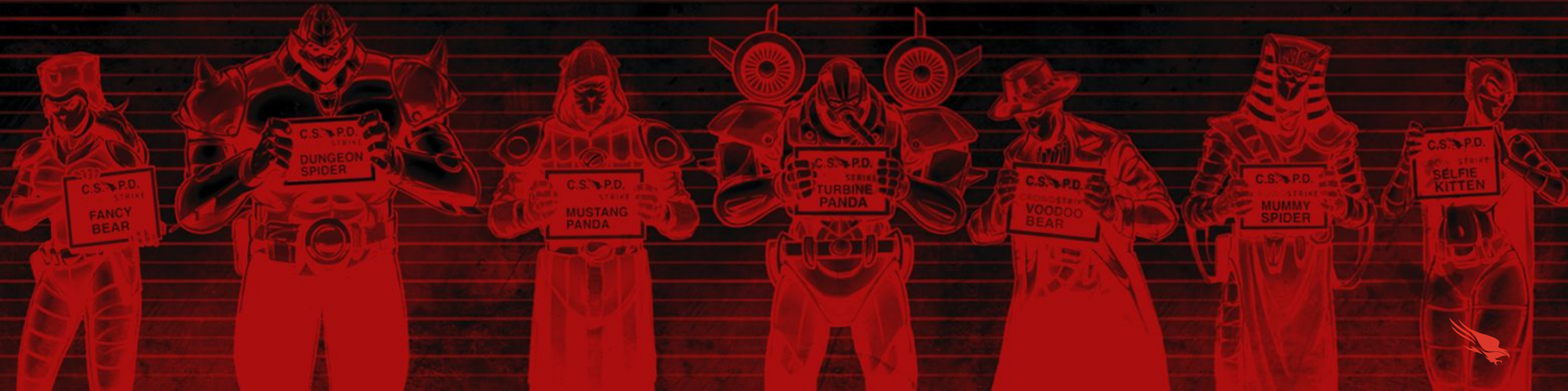
VP, INDUSTRY BUSINESS UNIT
& EXECUTIVE STRATEGIST

Tina Thorstenson leads a unit within CrowdStrike that provides strategic advisory services related to enterprise cybersecurity solutions. Tina has spent 30+ years running IT and security programs and 11 years holding the title of CISO.

Just prior to joining CrowdStrike, she most recently served as the Deputy CIO & Chief Information Security Officer for Arizona State University.

AGENDA

- SECURITY THEMES
- EXECUTIVE SUMMARY
- THE ADVERSARY OPERATIONS LIFECYCLE
- CYBER CRIME
- NATION-STATE REVIEW
- THE WAY FORWARD



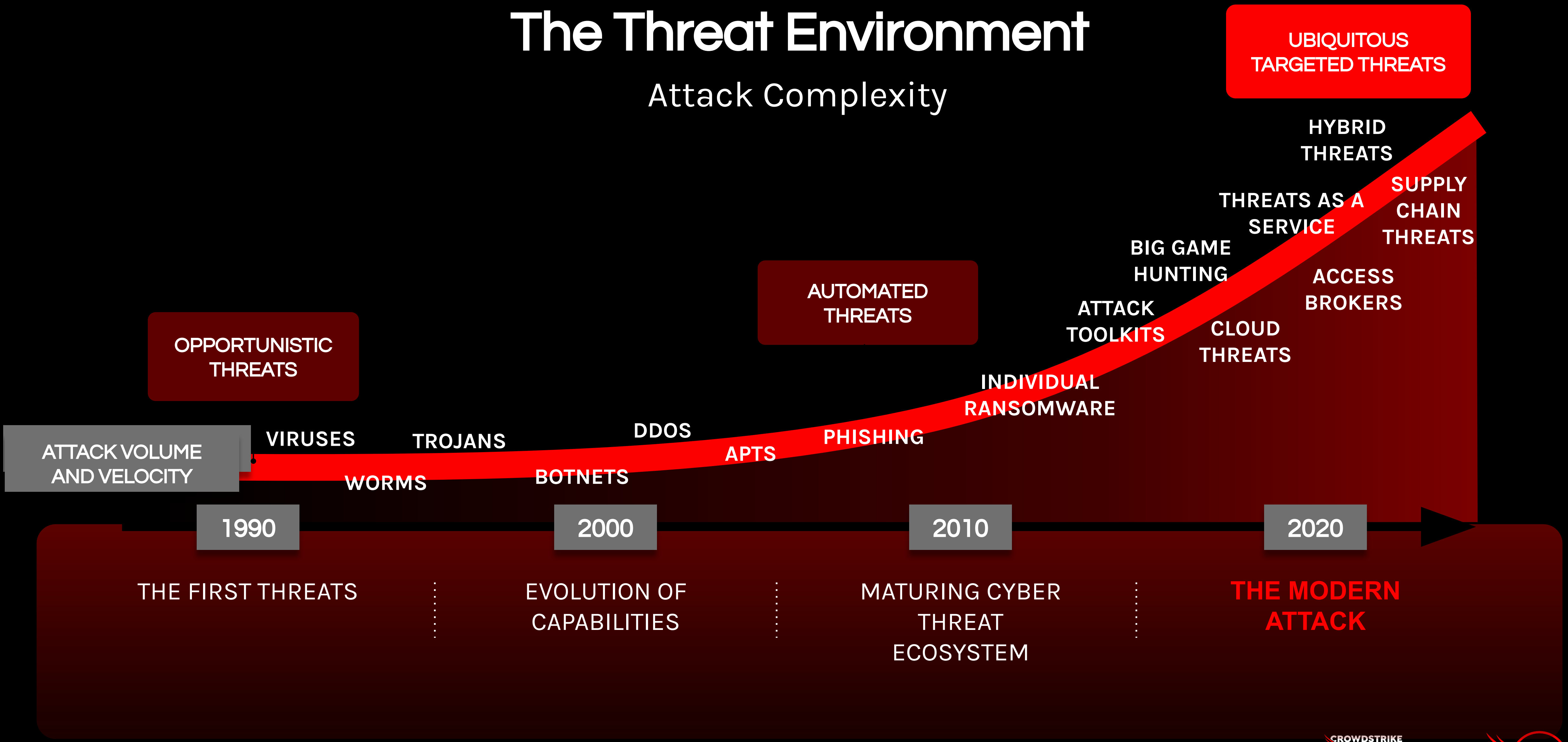
Today's Security Themes

Attack Sophistication

Innovation While Maintaining Siloed Security Solutions

Skill Shortages

The Threat Environment



Attack Complexity

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

ACCESS BROKERS

HYBRID THREATS

SUPPLY CHAIN THREATS

1990 — THE FIRST THREATS

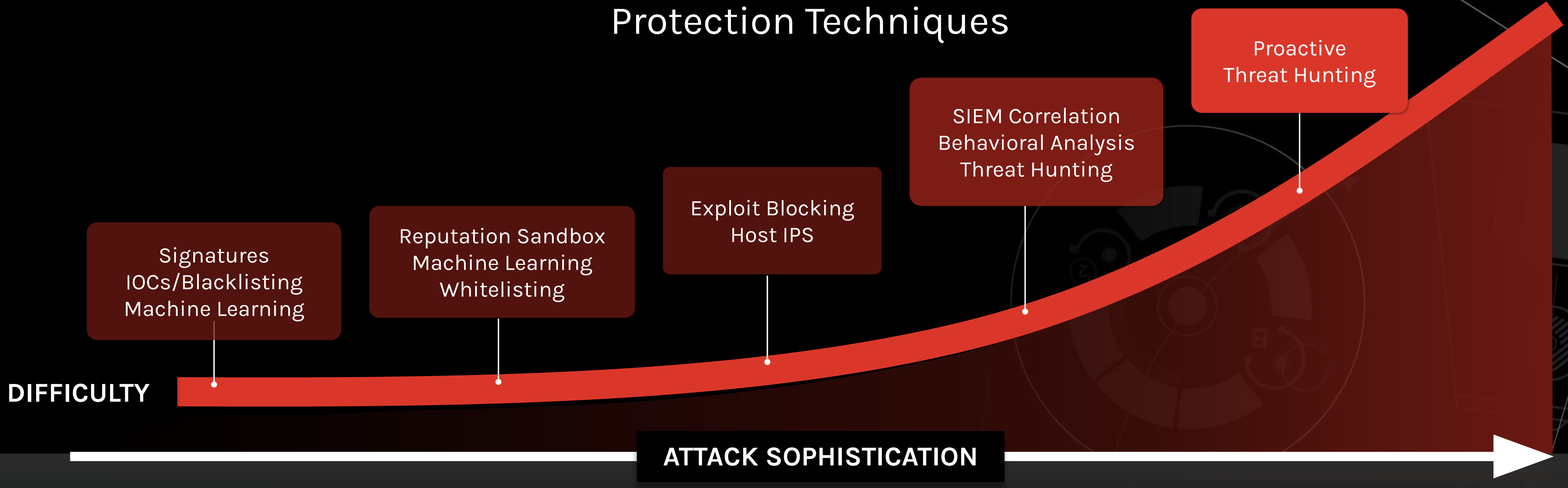
2000 — EVOLUTION OF CAPABILITIES

2010 — MATURING CYBER THREAT ECOSYSTEM

2020 — THE MODERN ATTACK

The Threat Environment

Protection Techniques



Signatures
IOCs/Blacklisting
Machine Learning

Reputation Sandbox
Machine Learning
Whitelisting

Exploit Blocking
Host IPS

SIEM Correlation
Behavioral Analysis
Threat Hunting

Proactive
Threat Hunting

FILE BASED MALWARE

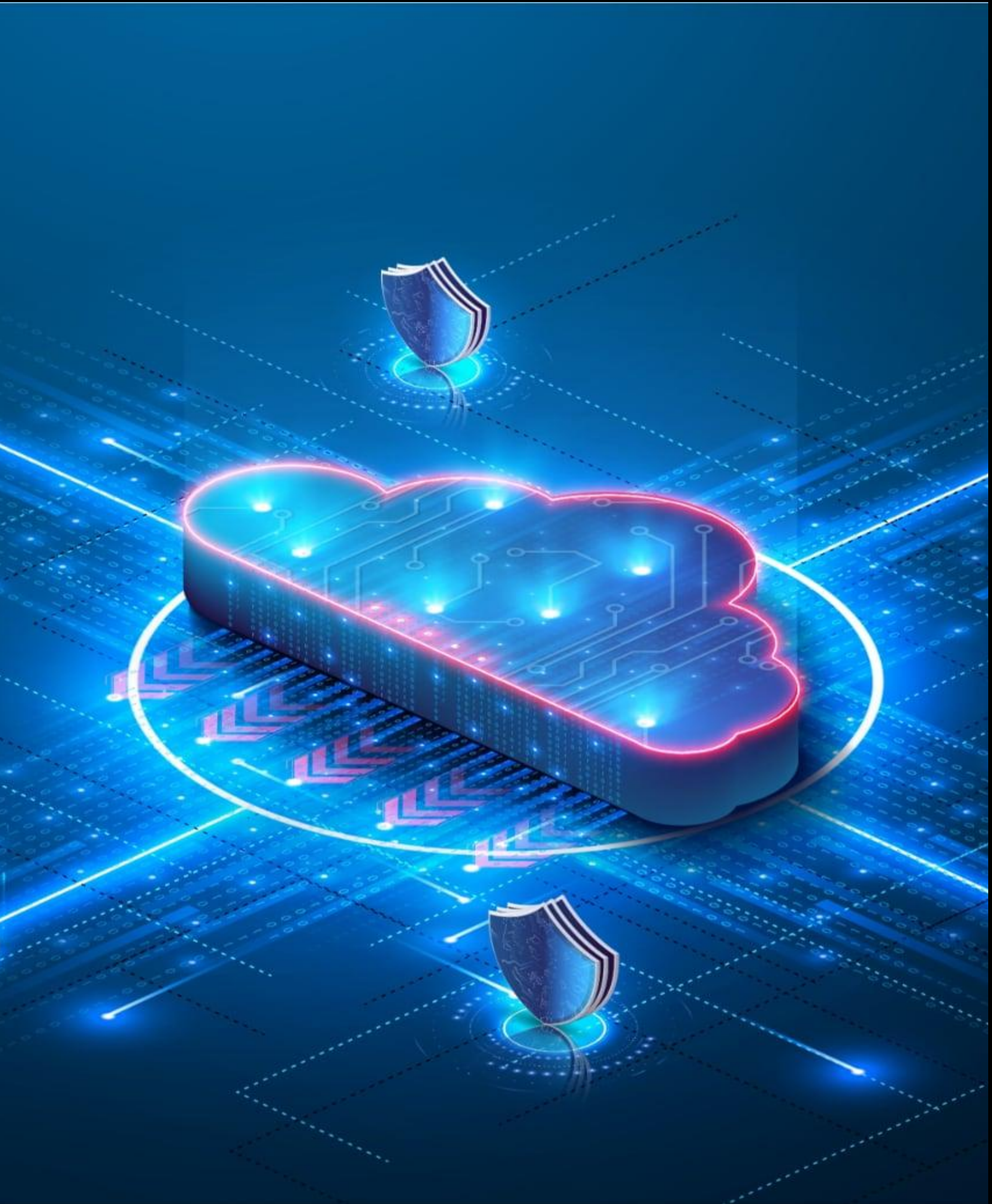
- Malware
- Zero-Day Malware

FILELESS AND EXPLOITS

- Exploitation of vulnerabilities
- Zero-Day Malware
- Credential Theft

LIVE ATTACKER/INSIDER

- Living off the land
- Hands-on keyboard



Cloud-Based Data

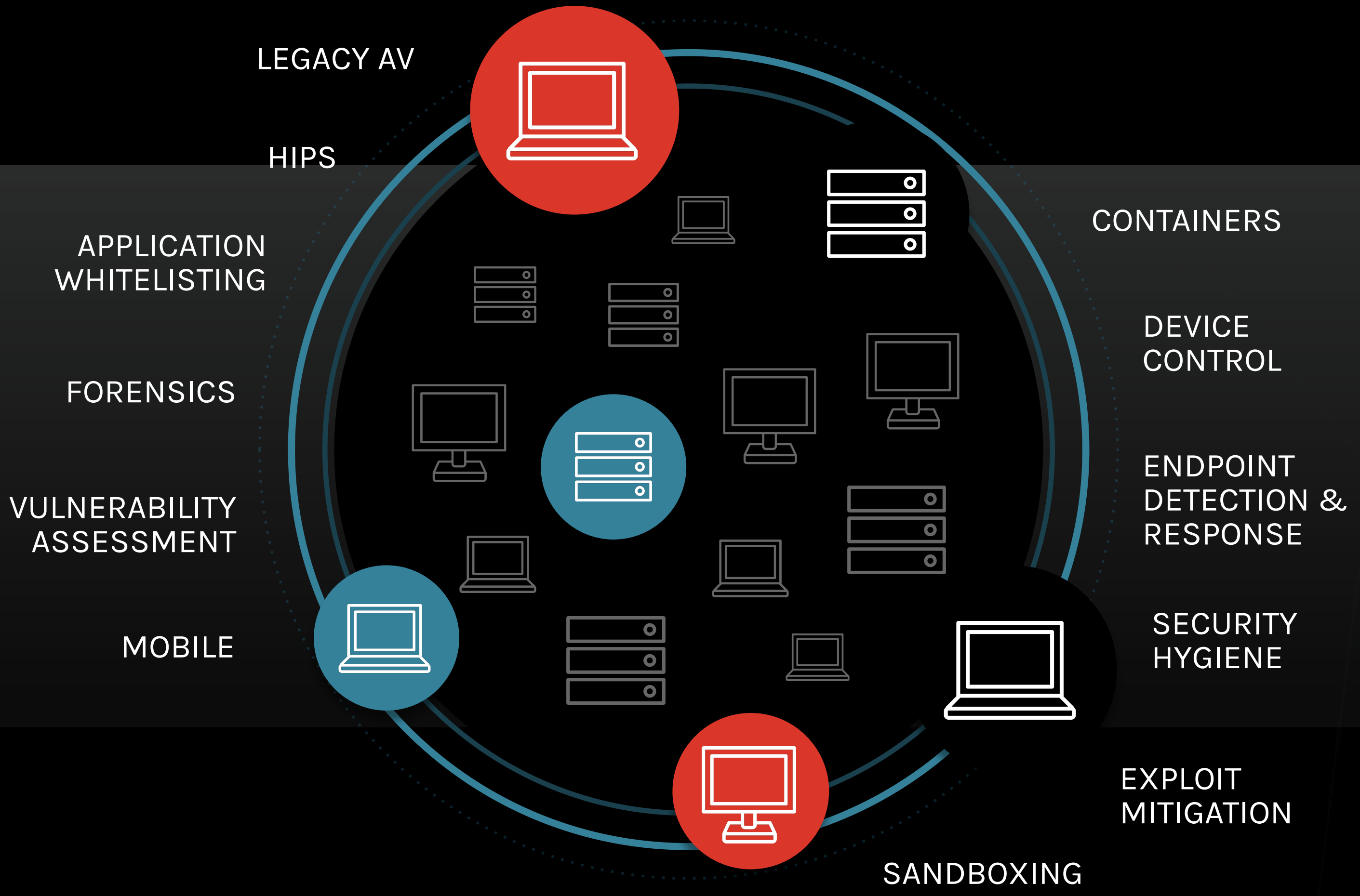
Recent Trends

CLOUD ADOPTION CONTINUES TO RISE IN PREVALENCE AND ORGANIZATIONS CONTINUE TO **MOVE SENSITIVE**, ON-PREM INFRASTRUCTURE **EXTERNALLY**

CONSISTENT MIS-MANAGEMENT & EXTENSIVE TECHNOLOGY **VULNERABILITIES** MAKE CLOUD AN ATTRACTIVE TARGET

COMMON CLOUD HOSTED ENVIRONMENTS SUCH AS **EMAIL SERVICES** AND **ACTIVE DIRECTORY** SERVE AS JUMPING OFF POINTS FOR ADVERSARIES

Solution Complexity

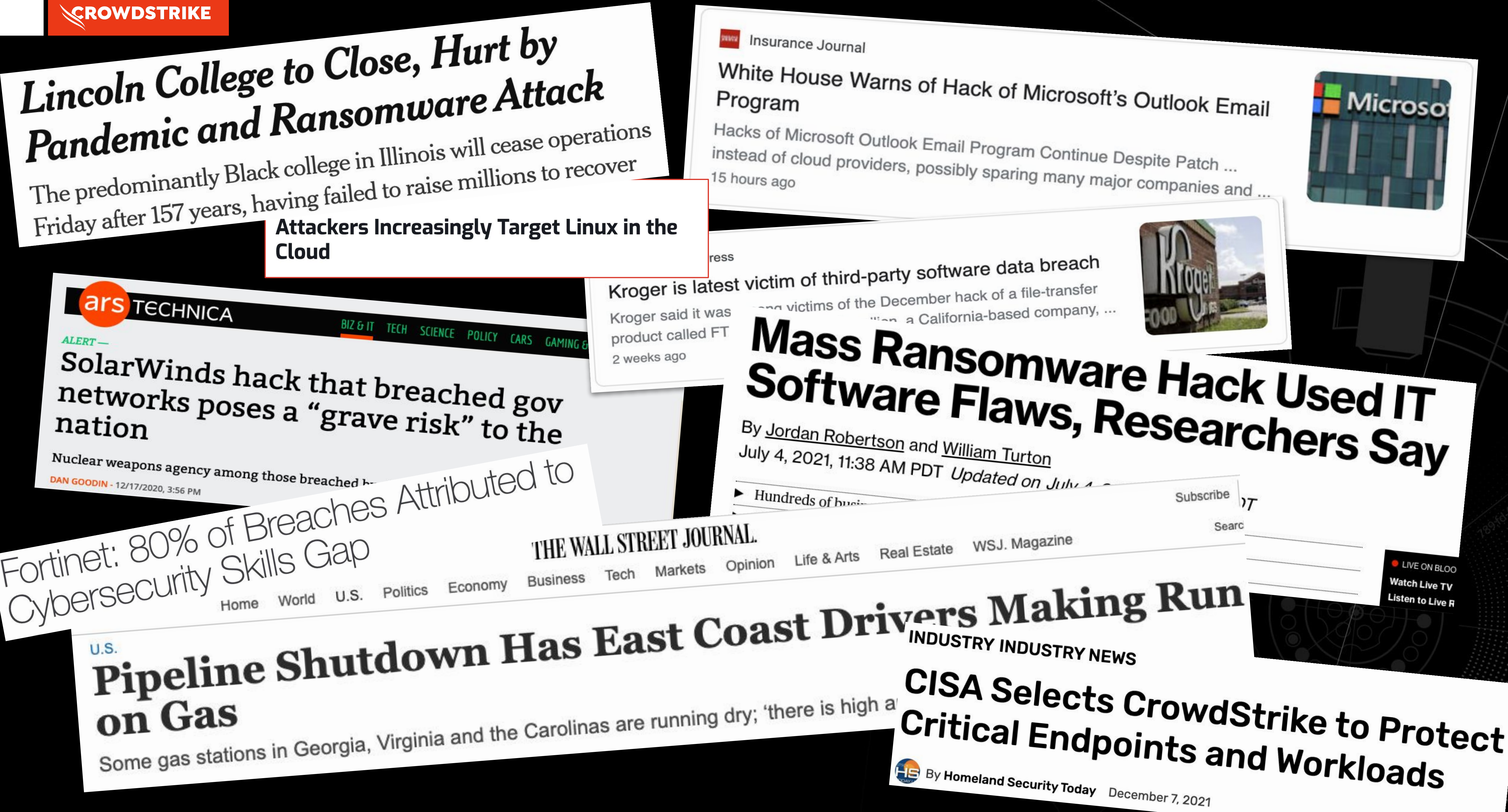


COSTLY TO DEPLOY

DIFFICULT TO MAINTAIN

POOR USER EXPERIENCE

MINIMAL SECURITY EFFECTIVENESS



Lincoln College to Close, Hurt by Pandemic and Ransomware Attack

The predominantly Black college in Illinois will cease operations Friday after 157 years, having failed to raise millions to recover

Attackers Increasingly Target Linux in the Cloud

Insurance Journal

White House Warns of Hack of Microsoft's Outlook Email Program

Hacks of Microsoft Outlook Email Program Continue Despite Patch ... instead of cloud providers, possibly sparing many major companies and ...

15 hours ago

ress

Kroger is latest victim of third-party software data breach

Kroger said it was ... victims of the December hack of a file-transfer product called FT... a California-based company, ...

2 weeks ago

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING &

ALERT —

SolarWinds hack that breached gov networks poses a "grave risk" to the nation

Nuclear weapons agency among those breached b...

DAN GOODIN - 12/17/2020, 3:56 PM

Mass Ransomware Hack Used IT Software Flaws, Researchers Say

By Jordan Robertson and William Turton

July 4, 2021, 11:38 AM PDT Updated on July 4, 2... DT

- Hundreds of busi...

LIVE ON BLOO

Watch Live TV

Listen to Live R

Fortinet: 80% of Breaches Attributed to Cybersecurity Skills Gap

THE WALL STREET JOURNAL.

Subscribe

Searc

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

U.S.

Pipeline Shutdown Has East Coast Drivers Making Run on Gas

Some gas stations in Georgia, Virginia and the Carolinas are running dry; 'there is high a...

INDUSTRY INDUSTRY NEWS

CISA Selects CrowdStrike to Protect Critical Endpoints and Workloads

By Homeland Security Today December 7, 2021

Executive Summary

A Global Perspective on Adversarial Trends

Power of the Security Cloud

180+
Adversaries Tracked

1+ Trillion
Events/Day

135+ Million
Indicators of Attack Decisions/Min

1.5+ Billion
Containers Protected/Day

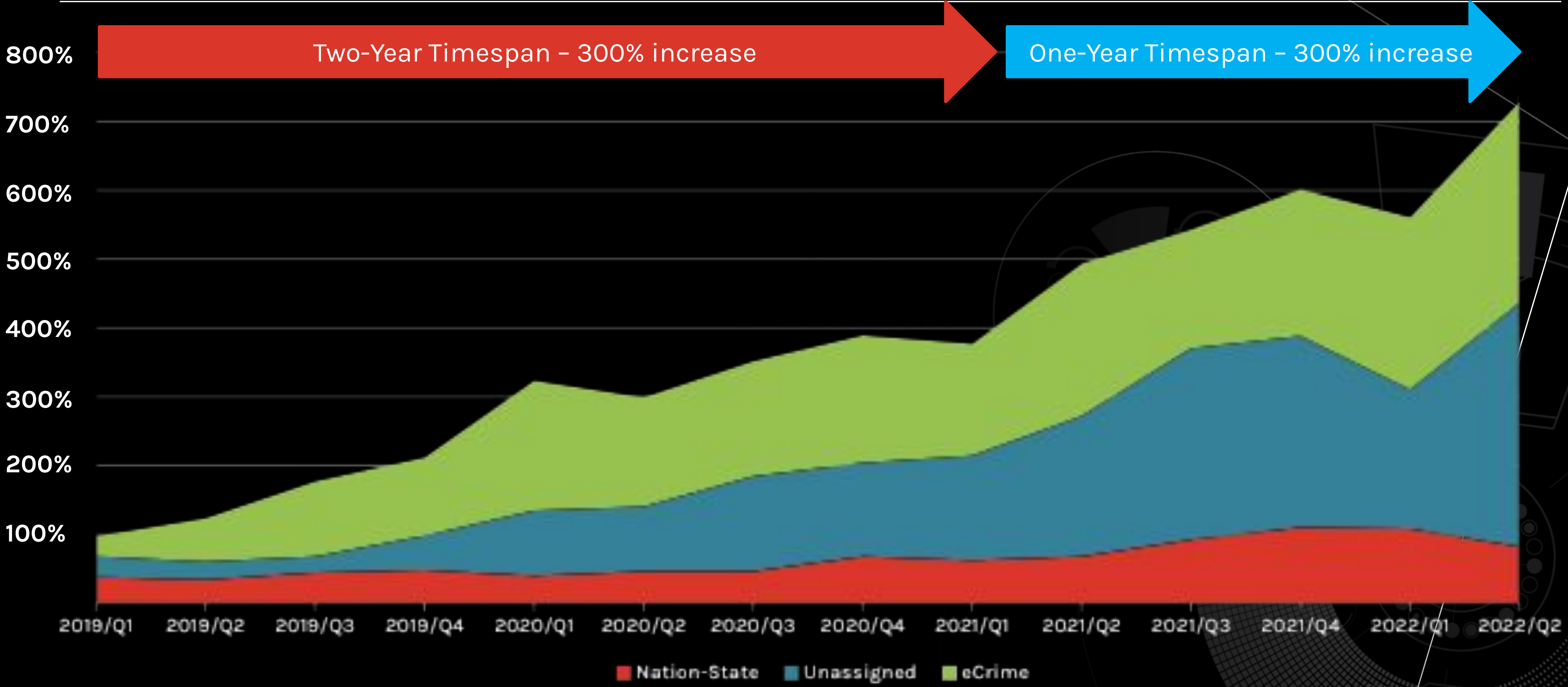
CrowdStrike Security Cloud

Asset Graph
IT Asset Context

Threat Graph
Threat Intelligence

Intel Graph
Adversary Data

CrowdStrike Distinct & Sophisticated Intrusion Telemetry



Two-Year Timespan – 300% increase

One-Year Timespan – 300% increase

eCrime Adversary Average Breakout Time

2018

9H 42M

2022

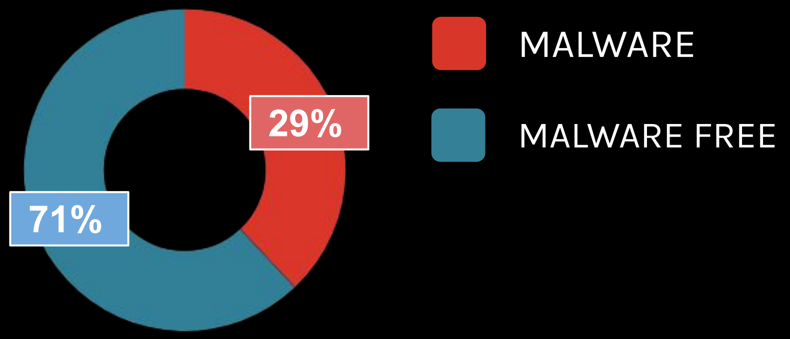
1H 24M

Components of the Advanced Modern Attack

ECRIME ADVERSARY EXPEDITED BREAKOUT TIME

2018	9H 42M
2022	1H 24M
2021 INFOSEC TEAM REMEDIATION TIMELINE	*162H*

2022 MALWARE vs MALWARE FREE ATTACKS



2018

- Malware: 60%
- Malware-Free: 40%

CROWDSTRIKE ADVERSARY UNIVERSE WORLD TOUR 22

CROWDSTRIKE

[redacted]

2022 Global Threat Hunting Report
Top 5 Findings

Top industries targeted by interactive intrusion activity included tech, telecom, healthcare, manufacturing and academia

50% increase in interactive intrusion activity

1 hr and 24 minutes, average eCrime adversary breakout time

71 % of attacks were malware-free

180+ adversaries tracked

Adversary Motivations

Nation State

eCrime

Hacktivist

CRIMINAL

- Alchemist Spider
- Aviator Spider
- Bitwise Spider
- Carbon Spider
- Chariot Spider
- Clockwork Spider
- Cyborg Spider
- Doppel Spider
- Feral Spider
- Graceful Spider
- Hidden Spider
- Hive Spider
- Indrik Spider
- Knockout Spider
- Lunar Spider
- Mallard Spider
- Mummy Spider
- Narwhal Spider
- Night Spider
- Outbreak Spider
- Outlaw Spider
- Percussion Spider
- Pinchy Spider
- Prophet Spider
- Salty Spider
- Samba Spider
- Scully Spider
- Slippy Spider

CHINA

- Aquatic Panda
- Circuit Panda
- Emissary Panda
- Karma Panda
- Kryptonite Panda
- Mustang Panda
- Octane Panda
- Pirate Panda
- Puzzle Panda
- Shattered Panda
- Sunrise Panda
- Vixen Panda
- Wicked Panda

NORTH KOREA

- Labyrinth Chollima
- Ricochet Chollima
- Silent Chollima
- Stardust Chollima
- Velvet Chollima

IRAN

- Charming Kitten
- Chrono Kitten
- Haywire Kitten
- Imperial Kitten
- Nemesis Kitten
- Pioneer Kitten
- Refined Kitten
- Spectral Kitten
- Static Kitten
- Tracer Kitten

INDIA

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

RUSSIA

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

PAKISTAN

- **Mythic Leopard**
- **Fringe Leopard**

VIETNAM

Ocean Buffalo

SOUTH KOREA

Shadow Crane

SYRIA

Deadeye Hawk

COLOMBIA

Galactic Ocelot

TURKEY

Cosmic Wolf

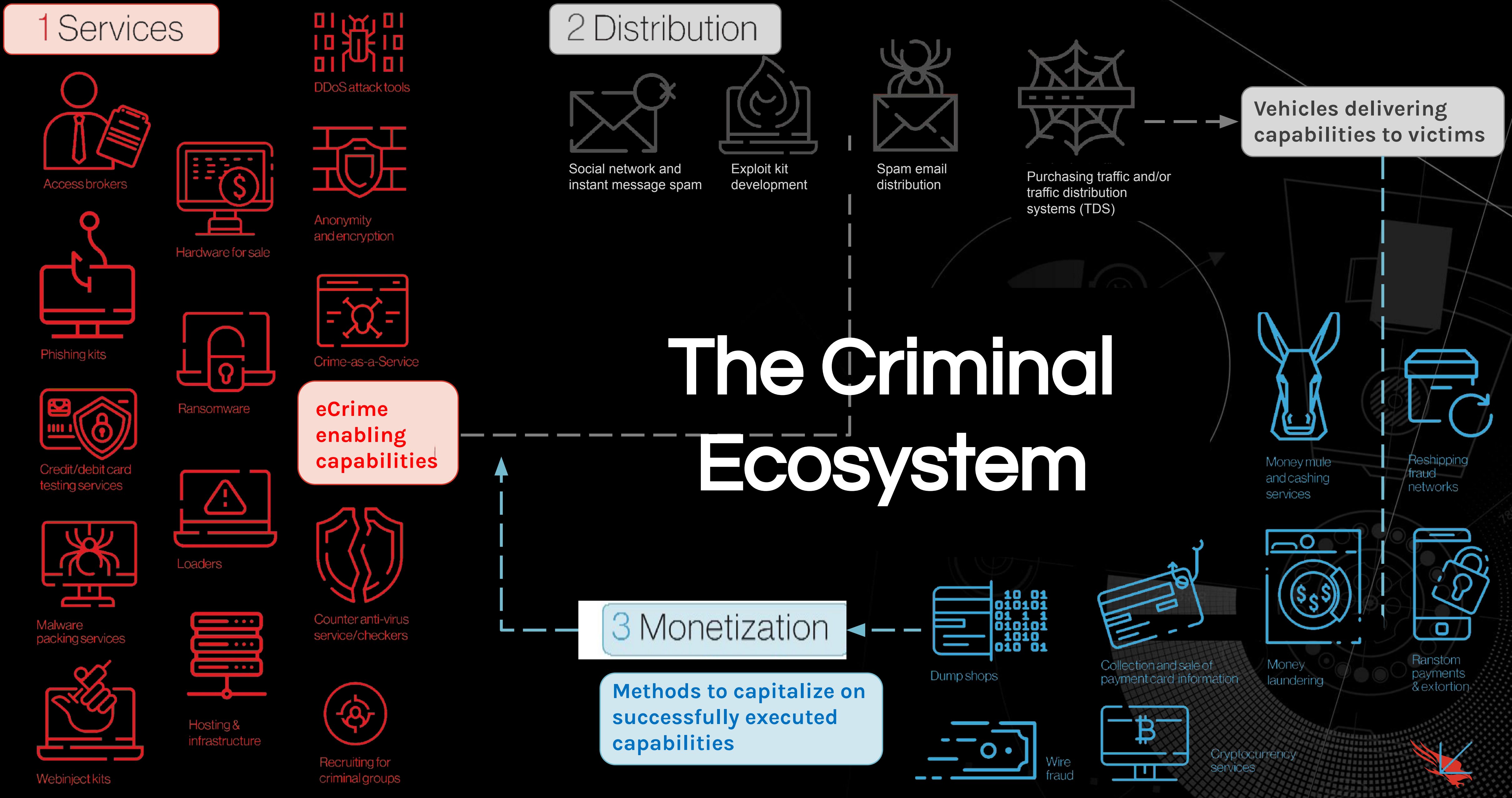
ACTIVIST

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

CROWDSTRIKE

TLP AMBER

The Criminal Ecosystem



1 Services

Access brokers

Hardware for sale

DDoS attack tools

Anonymity and encryption

Phishing kits

Ransomware

Crime-as-a-Service

Credit/debit card testing services

Loaders

Counter anti-virus service/checkers

Malware packing services

Hosting & infrastructure

Recruiting for criminal groups

Webinject kits

eCrime enabling capabilities

2 Distribution

Social network and instant message spam

Exploit kit development

Spam email distribution

Purchasing traffic and/or traffic distribution systems (TDS)

Vehicles delivering capabilities to victims

3 Monetization

Methods to capitalize on successfully executed capabilities

Money mule and cashing services

Reshipping fraud networks

Dump shops

Collection and sale of payment card information

Money laundering

Ranstom payments & extortion

Wire fraud

Cryptocurrency services

The Adversary Operations Lifecycle

How Advanced Adversaries Engage in Operations

The Adversary Operations Lifecycle

Access Operations

How Adversaries gain access

- VALID CREDENTIALS
- SUPPLY CHAIN COMPROMISE
- 0-DAY EXPLOITATION
- MFA BYPASS

Post Exploitation

How Adversaries remain stealthy

- LIVING OFF THE LAND

Target Environments

What Adversaries are attacking

- DOMAIN CONTROLLERS
- CLOUD WORKLOADS
- EMAIL & DATA SERVERS
- DOWNSTREAM ACCESS

Access Operations

How Adversaries Gain Access

The Problem

“YOU DON’T HAVE A MALWARE PROBLEM. YOU HAVE AN ADVERSARY PROBLEM”

“Attackers don’t break in, they log in.”

Identity Threat Detection and Response is Crucial

80%

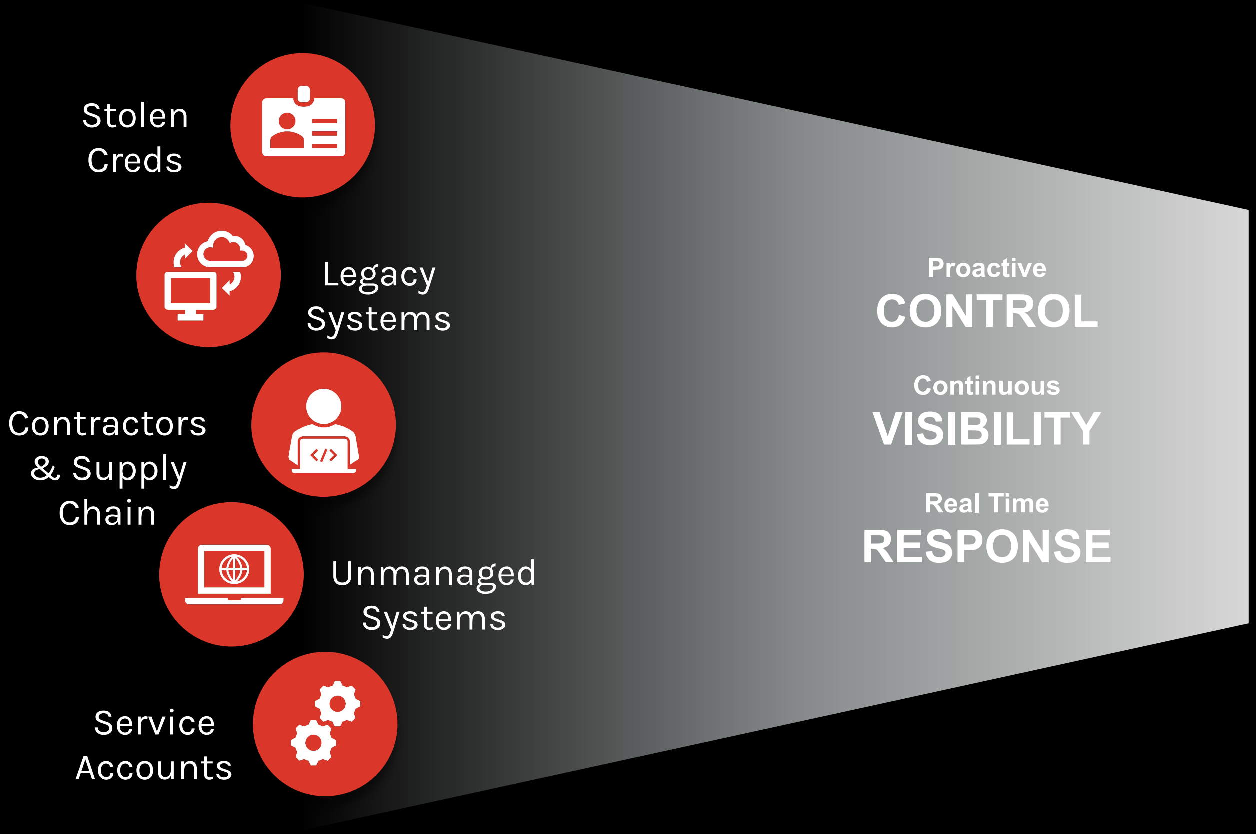
of data breaches have a connection to compromised privileged credentials

- Forrester Research

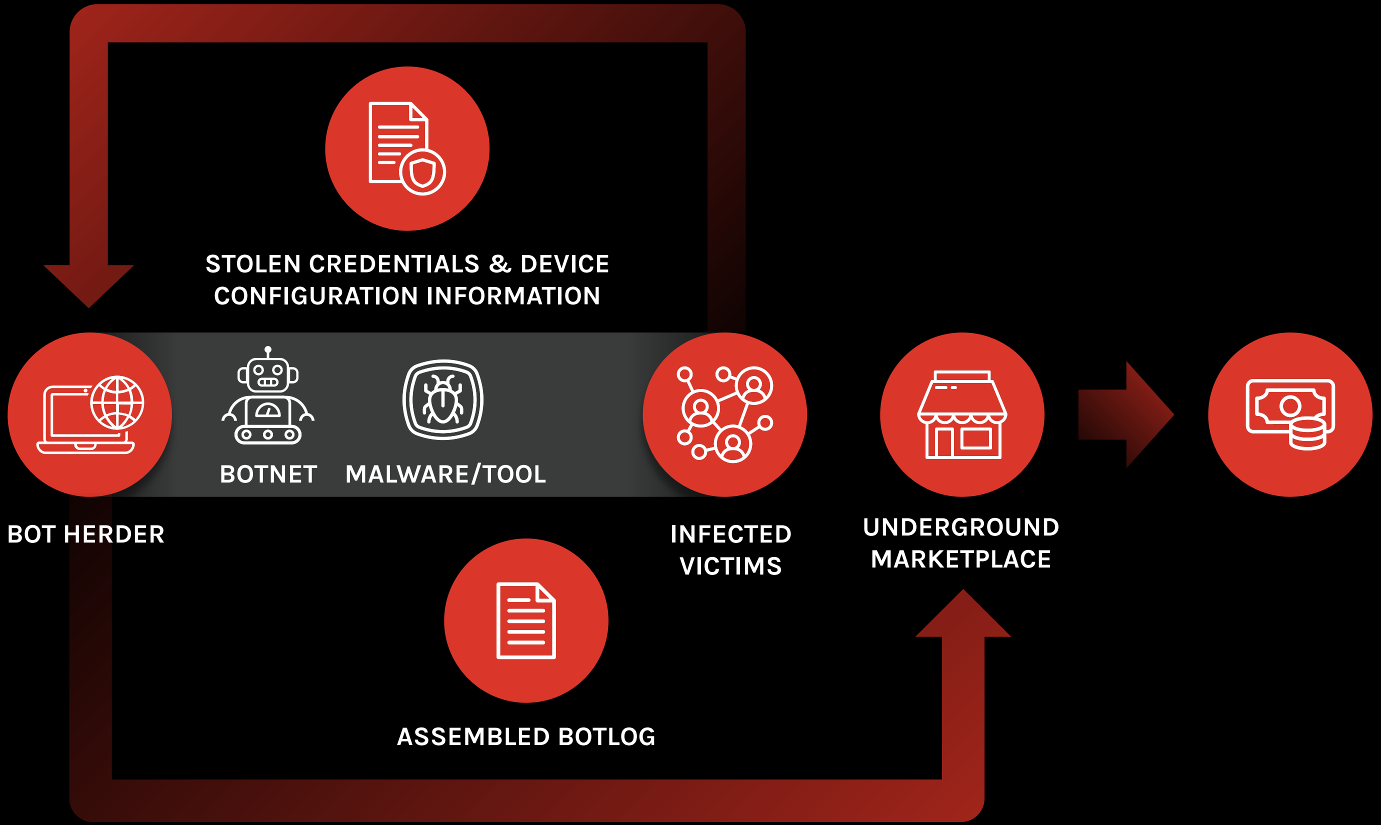
Breaches from stolen/compromised credentials took the longest to detect:

243 days

- IBM Cost of a Breach Report, 2022



Access brokers: vital role in the e-crime ecosystem



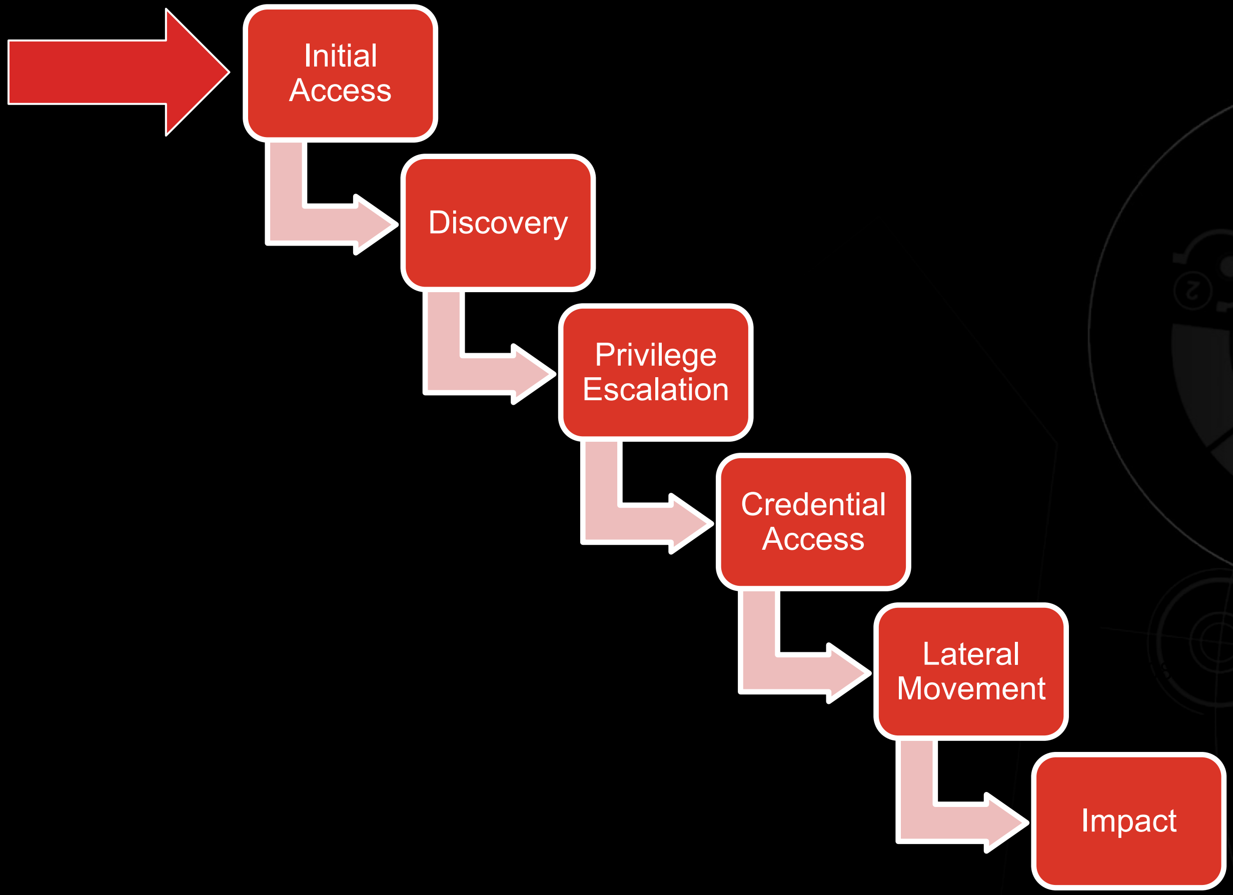
ACCESS BROKERS ARE THREAT ACTORS WITH A SIGNIFICANT HISTORY OF PROVIDING INITIAL ACCESS TO MULTIPLE ENTITIES

ACCESS BROKERS OFTEN PERFORM ADDITIONAL ROLES IN THE ECRIME ECOSYSTEM

LOGIN CREDENTIALS

DEVICE CONFIGURATION DATA

Threat actors don’t always start here



Initial Access

Discovery

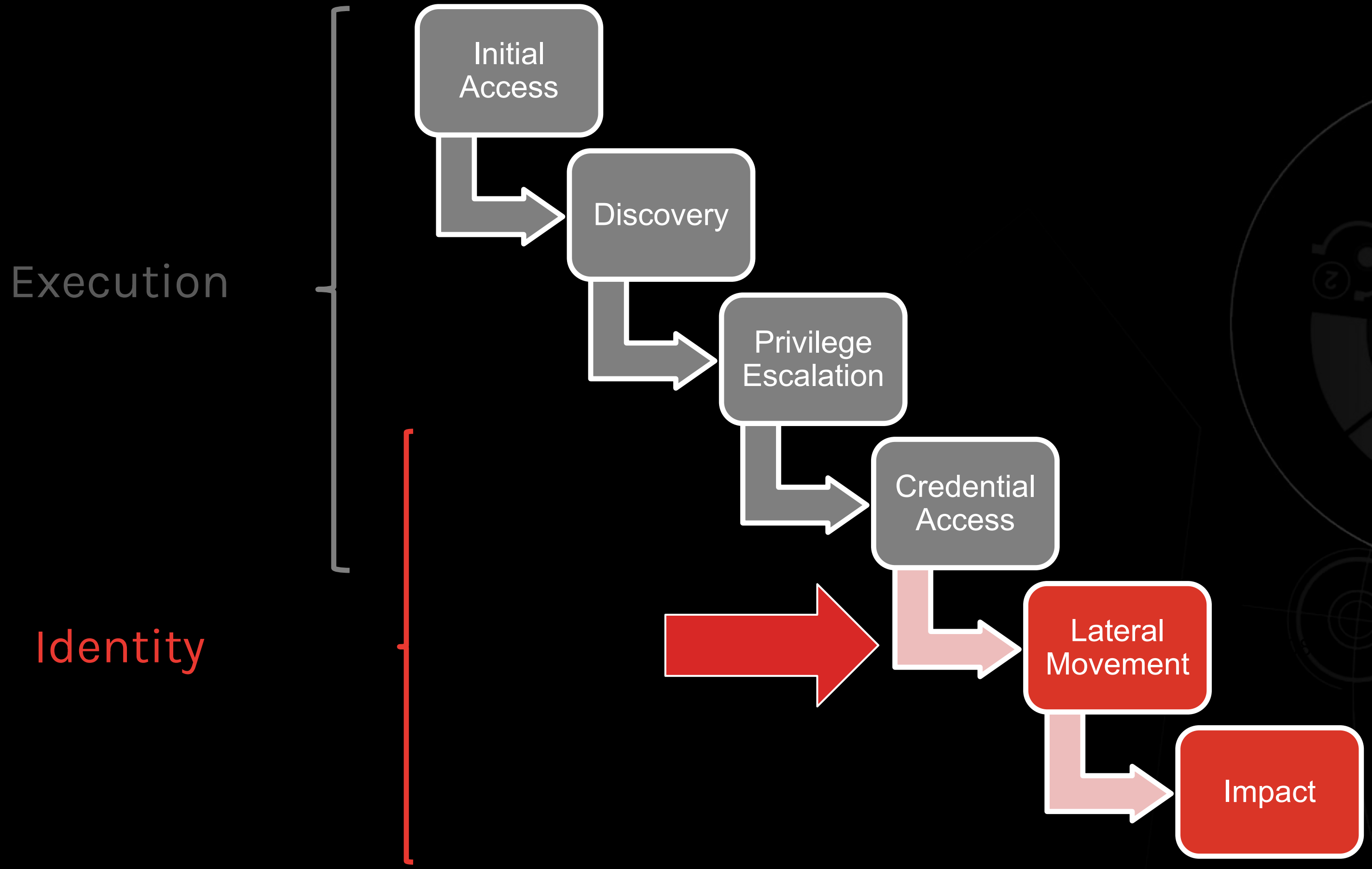
Privilege Escalation

Credential Access

Lateral Movement

Impact

Often, threat actors start here



Post Exploitation

How Adversaries Remain Stealthy

Living-Off-The-Land

Recent Trends

USES NATIVE TOOLS PRESENT ON THE TARGET SYSTEM TO ACCOMPLISH THE ADVERSARIES’ OBJECTIVE

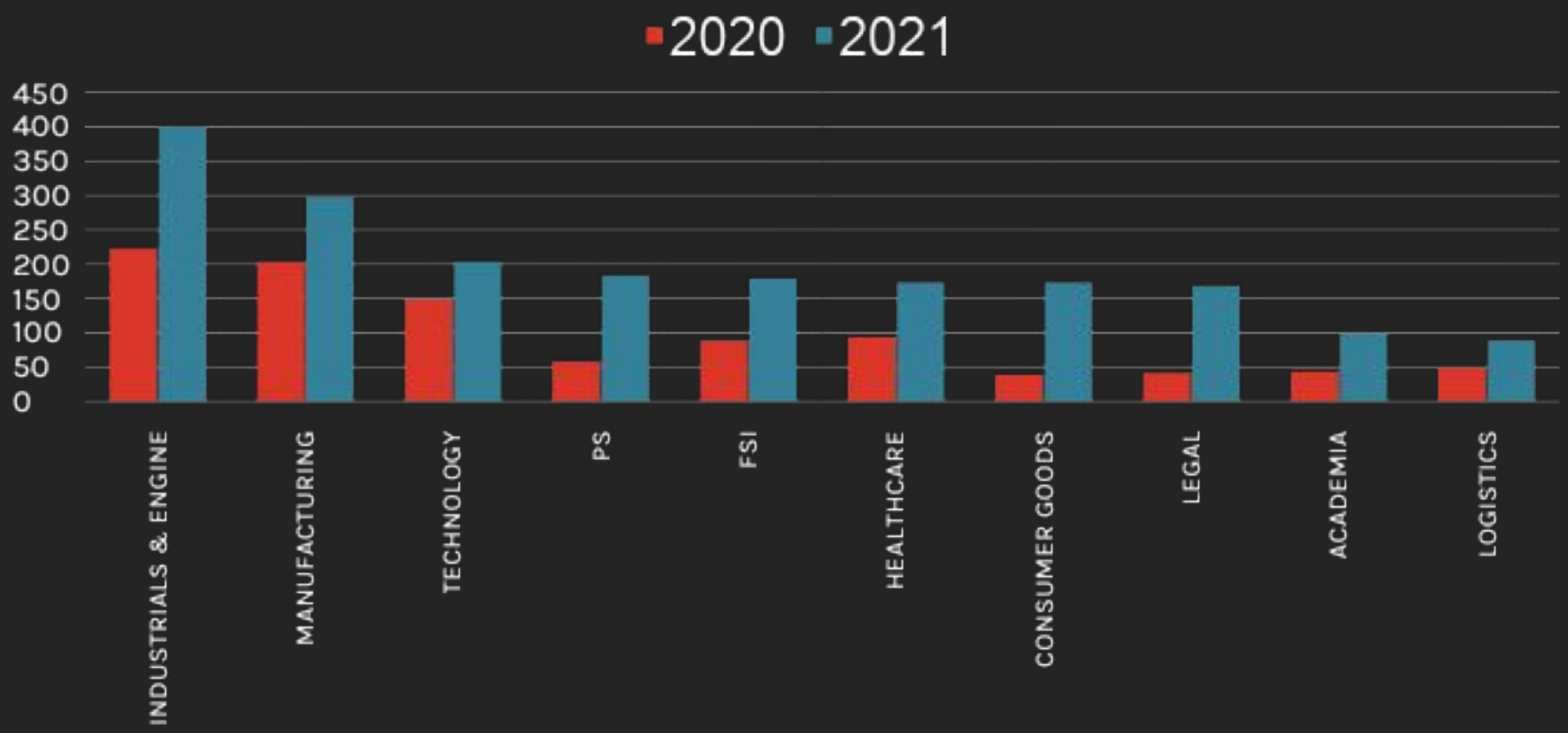
ENABLES ADVERSARIES TO BLEND IN TARGET NETWORK AND HIDE THEIR ACTIVITY IN LEGITIMATE PROCESSES

	TOP LIVING OFF THE LAND TOOLS	
	NATIVE TO IT ENVIRONMENTS	NOT NATIVE BUT COMMON AND LEGITIMATE
1	PSEXEC	MIMIKATZ
2	PROCDUMP	GMER
3	POWERSHELL	PROCESS HACKER
4	WMI	TEAMVIEWER
5	VBSCRIPT	PUTTY

Target Environments

What Adversaries Want

Comparison of Ransomware-Based Data Leaks



Industries most impacted by LockBit include Retail, Healthcare, Transportation and Logistics, Academia, Manufacturing, Professional Services, Telecom, and Tech

BITWISE SPIDER

BIG-GAME HUNTING RANSOMWARE

MOST PROLIFIC **RANSOMWARE** OPERATOR SINCE 2021

- ACTIVE SINCE SEP 2019, RESPONSIBLE FOR LOCKBIT & LOCKBIT 2.0 RANSOMWARE PLUS STEALBIT INFO STEALER
- GAINED POPULARITY WITH THE LAUNCH OF LOCKBIT 2.0 IN JUNE 2021 – AVERAGES 3-4 VICTIMS PER DAY, AND POSTS TO BITWISE SPIDER's DATA LEAK SITE
- VICTIMS COMPRISED 35 SECTORS ACROSS 74 COUNTRIES, BITWISE SPIDER AFFILIATES GAIN ACCESS BY BRUTE-FORCING INTERNET-FACING **RDP or VPN** SERVERS
- RELEASED UPDATE IN OCT 2021 WITH FEATURES TO ENCRYPT VMWARE ESXi SERVERS
- ANNOUNCED LOCKBIT 3.0 IN JUNE 2022 WITH TIERED OFFERING – CUSTOMIZATION FOR VIP AFFILIATES

CyberCrime

Data Leaks, Criminal Extortion, and Ransomware

Overarching eCrime Trends

EXTORTION & DATA LEAKS

LIVING OFF THE LAND

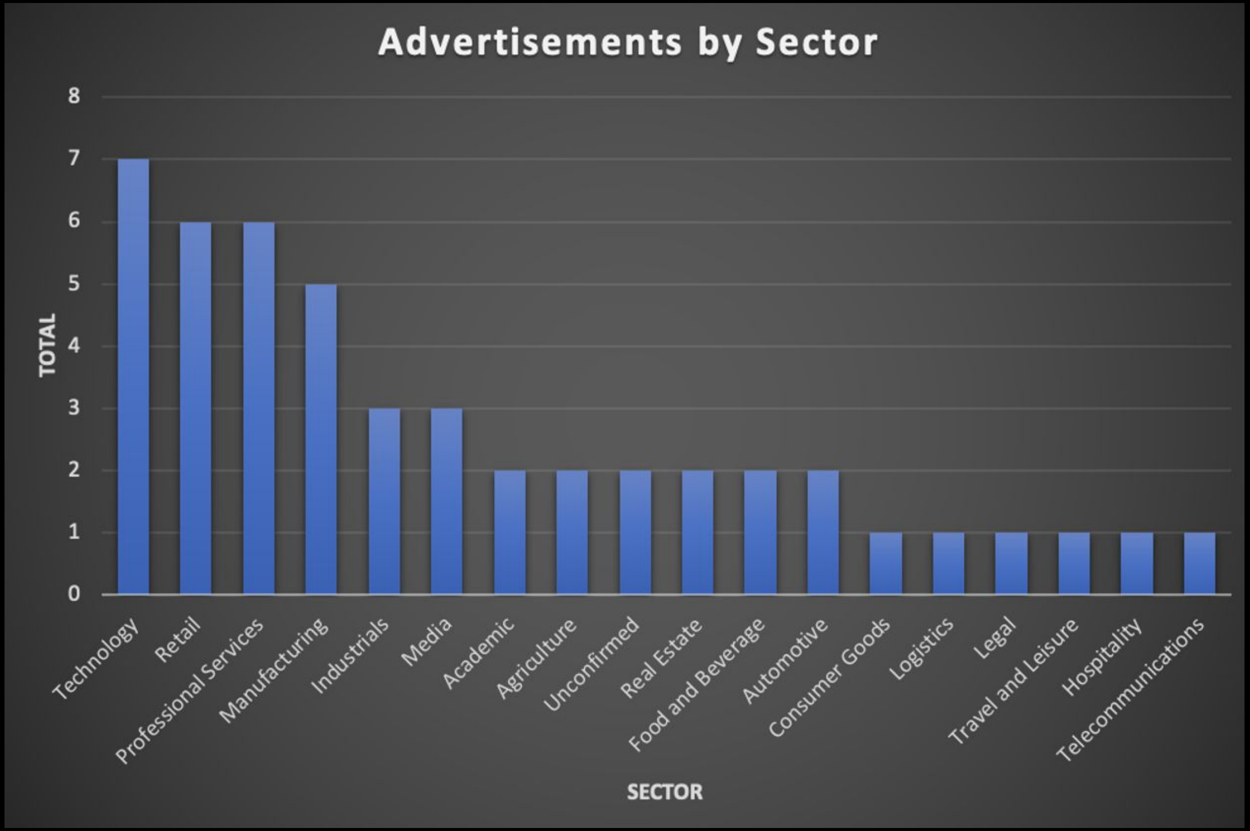
RANSOMWARE AS-A-SERVICE

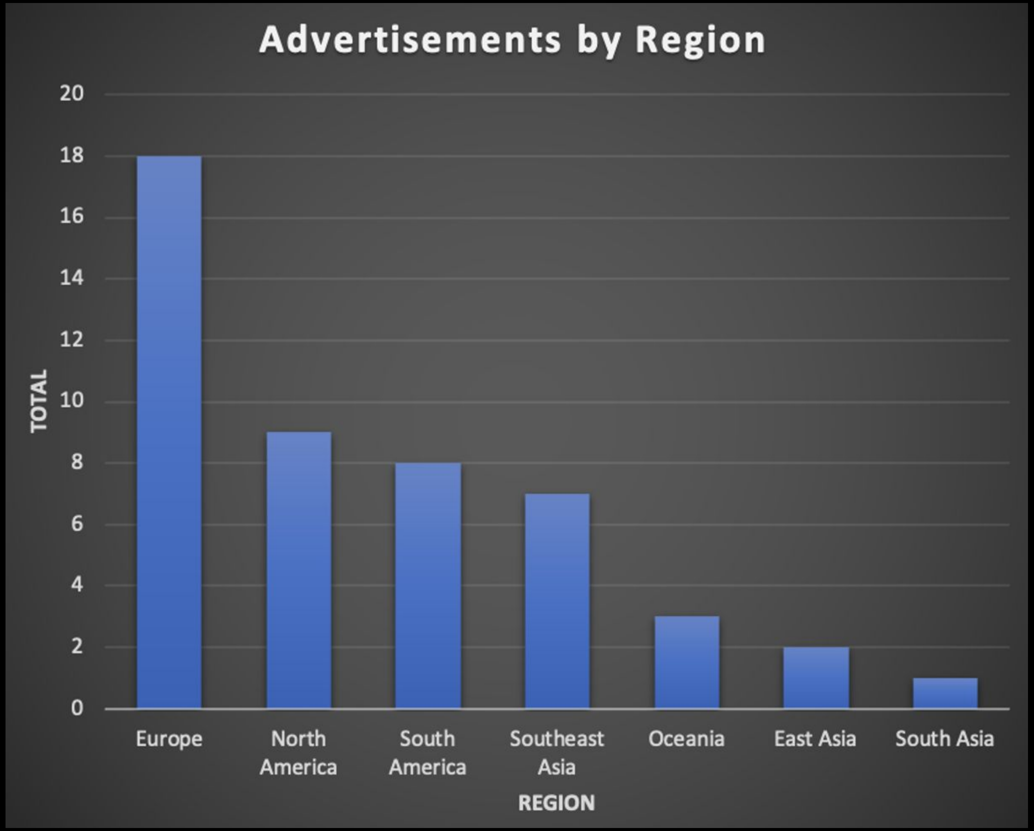
HIGH SOPHISTICATION

ACCESS BROKERS

ACCESS BROKER SEEKS COLLABORATIVE OPPORTUNITIES WITH RANSOMWARE OPERATORS; LIKELY TTPS EVIDENCED IN PREVIOUS FORUM ACTIVITIES

- An access broker who attempted to sell approximately 50 accesses has stated they wish to collaborate with ransomware operators on future intrusions.
- On 4 August 2022, an access broker posted to a popular eCrime forum, stating their desire for “joint work” as part of “a team” and offering to exchange knowledge and expertise.





Nation-State Review

Espionage, Destructive Attacks, & Advanced Attacks

NATION STATE TRENDS

CHINA

DPRK

IRAN

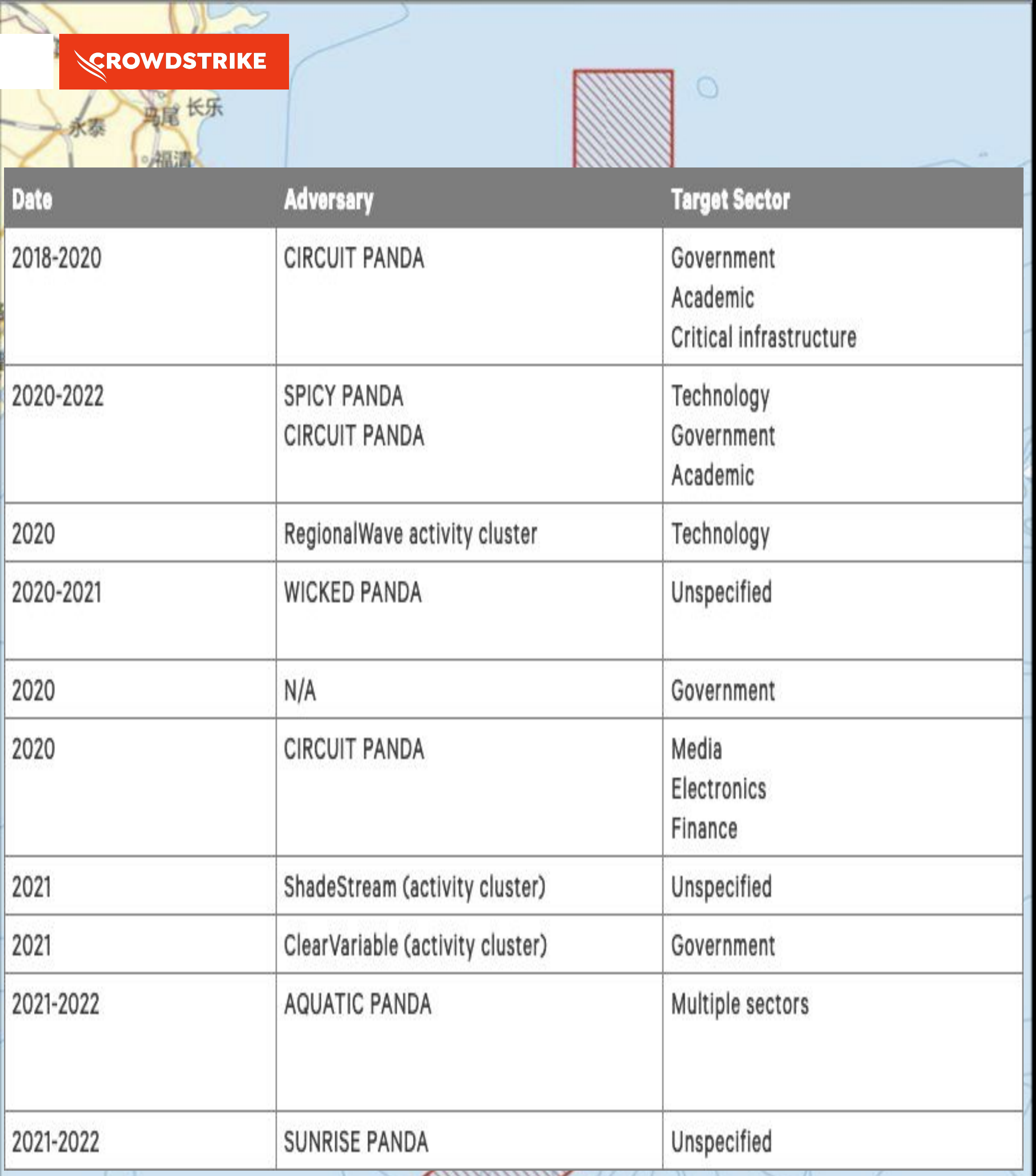
RUSSIA

Chinese Intrusion Activity

Acceleration over the past decade

DRIVEN BY THE STATE'S CORE INTERESTS

- CHINA STATE-NEXUS ADVERSARIES CONTINUE TO BE THE MOST ACTIVE NATION STATE GROUPS
- POLITICAL ESPIONAGE FOR GEOPOL INTELLIGENCE TO ACHIEVE REGIONAL PRIMACY AND GLOBAL INFLUENCE
- INDUSTRIAL ESPIONAGE & INTELLECTUAL PROPERTY THEFT TO ACHIEVE TECHNOLOGICAL SUPERIORITY
- INFLUENCE OPERATIONS & DOMESTIC SURVEILLANCE TO ENSURE REGIME STABILITY
- WHOLE-OF-SOCIETY ECOSYSTEM TO DEVELOP AND SUSTAIN A FORMIDABLE CYBER CAPABILITY



Date	Adversary	Target Sector
2018-2020	CIRCUIT PANDA	Government Academic Critical infrastructure
2020-2022	SPICY PANDA CIRCUIT PANDA	Technology Government Academic
2020	RegionalWave activity cluster	Technology
2020-2021	WICKED PANDA	Unspecified
2020	N/A	Government
2020	CIRCUIT PANDA	Media Electronics Finance
2021	ShadeStream (activity cluster)	Unspecified
2021	ClearVariable (activity cluster)	Government
2021-2022	AQUATIC PANDA	Multiple sectors
2021-2022	SUNRISE PANDA	Unspecified

Observed Chinese Targeting of Hong Kong and Taiwan, 2020-2022

U.S. HOUSE SPEAKER NANCY PELOSI ARRIVES IN TAIWAN; DDOS ATTACKS AGAINST TAIWANESE PRESIDENTIAL OFFICE CONFIRMED, CHINA PLANS MAJOR MILITARY EXERCISES AROUND ISLAND

A U.S. delegation led by House Speaker Nancy Pelosi landed in Taiwan on 2 August 2022, the first such visit in 25 years. In response, China's PLA Eastern Command announced it will commence military exercises in the sea east of Taiwan from 2 August 2022, and state media agency Xinhua separately declared the PLA will conduct live-fire drills encircling the island between 4-7 August 2022.

These military actions follow Beijing's ban of thousands of Taiwanese imports.

Taiwan's Presidential Office confirmed its website had been hit by a distributed denial-of-service (DDoS) attack at 5:15PM local time on 2 August 2022, hours before Pelosi's scheduled arrival. A government spokesperson confirmed the attack originated overseas, but did not specify if it came from China. The website was reportedly back online in 20 minutes.

The Way Forward

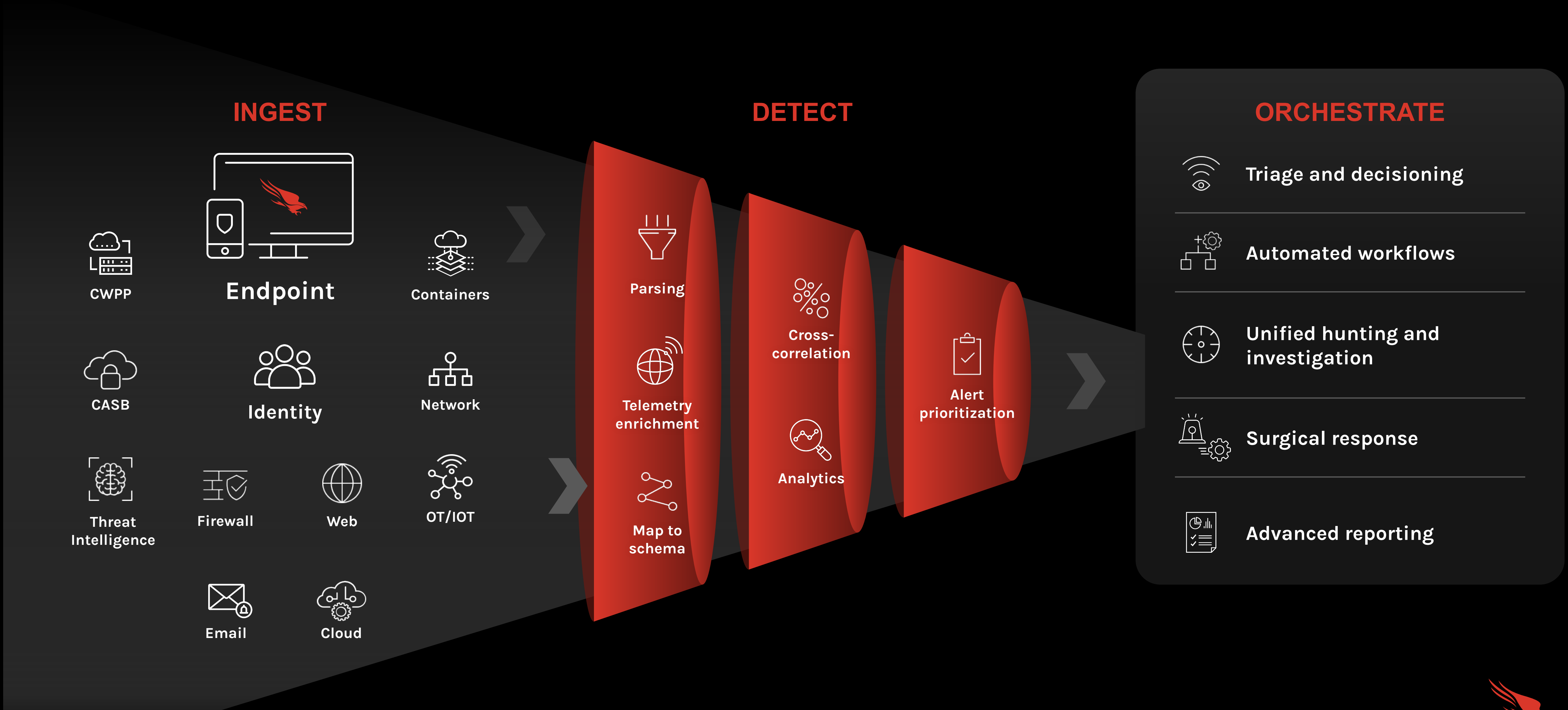
Innovative Protection Capabilities & Recommendations

Cyber Insurance Ready – Top 12 Controls

Controls Requested by Insurers:	AXA XL	AIG	Beazley	Coalition	CNA
MFA-Controlled Access	✓	✓	✓	✓	✓
Secured & Tested Backups	✓	✓	✓	✓	✓
Patched Systems & Applications	✓	✓	✓	✓	✓
Filtered Emails & Web Content	✓	✓	✓	✓	✓
Protected Privileged Accounts	✓	✓	✓	✓	✓
Protected Network	✓	✓	✓	✓	✓
Secured Endpoints	✓	✓	✓	✓	✓
Logged & Monitored Network	✓	✓	✓	✓	✓
Phishing-Aware Workforce	✓	✓	✓		✓
Managed Vulnerabilities	✓	✓	✓	✓	
Hardened Device Configuration	✓		✓	✓	
Prepared Incident Response	✓	✓			✓

CROWDSTRIKE

Falcon XDR A Platform Approach Extending Beyond The Endpoint



INGEST

CWPP

Endpoint

Containers

CASB

Identity

Network

Threat Intelligence

Firewall

Web

OT/IOT

Email

Cloud

DETECT

Parsing

Telemetry enrichment

Map to schema

Cross-correlation

Analytics

Alert prioritization

ORCHESTRATE

Triage and decisioning

Automated workflows

Unified hunting and investigation

Surgical response

Advanced reporting

CROWDSTRIKE

Falcon X Recon Intelligence

Digital Risk Monitoring

8+ BILLION
OBJECTS COLLECTED

1+ MILLION
UNIQUE SOURCES

500+ MILLION
DAILY SOCIAL MEDIA POSTS

55+ THOUSAND
UNIQUE DARK WEB SITES

42+ MILLION
INDICATORS OF COMPROMISE

OPEN WEB	SOCIAL MEDIA	MESSAGING APPS	CRIMINAL FORUMS	CRIMINAL MARKETS	ADVERSARY INFRASTRUCTURE
BLOGS, GITHUB, PASTEBIN, ETC	TWITTER, REDDIT, DISCORD, ETC	TELEGRAM, QQ, IRC, ETC	BLACKHAT, RAID, EXPLOIT, XSS, ETC	DARKMARKET, GENESIS, ETC	C2, BOTNETS, DDOS, ETC

Falcon Platform Coverage of Tradecraft

Top Adversary ATT&CK Tactics in 2022… Thus far

Actor Class	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
eCrime	Valid Accounts		Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping		Remote Services				
Targeted	Valid Accounts		Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping		Remote Services				

Identity

Actor Class	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
eCrime		Command and Scripting				OS Credential Dumping	System Owner/User Discovery		Archive Collected Data	Ingress Tool Transver	Exfiltration Over Alternative Protocol	Service Stop
Targeted		Command and Scripting				OS Credential Dumping	System Owner/User Discovery		Archive Collected Data	Ingress Tool Transver	Exfiltration Over Alternative Protocol	Service Stop

Endpoint

Actor Class	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
eCrime	Valid Accounts	Command and Scripting	Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping	System Owner/User Discovery	Remote Services	Archive Collected Data	Ingress Tool Transver	Exfiltration Over Alternative Protocol	Service Stop
Targeted	Valid Accounts	Command and Scripting	Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping	System Owner/User Discovery	Remote Services	Archive Collected Data	Ingress Tool Transver	Exfiltration Over Alternative Protocol	Service Stop

Identity
+
Endpoint

CROWDSTRIKE

TOP RECOMMENDATIONS

CULTURE OF CYBERSECURITY

Community awareness and practice are key to healthy cybersecurity; Engage your execs & board in a risk-based cyber program

ROLL IT OUT, TURN IT ON

Select tech partners who are strategic. Secure all of your tech infrastructure; Enable prevention capabilities, properly integrate

BE VIGILANT & READY TO ACT

Beyond technology, match defenders and adversaries 24x7x365, leveraging 1-10-60 rule

PROTECT YOUR IDENTITY

Use multi-factor for all accounts, protect service and admin accounts, adopt zero trust approach

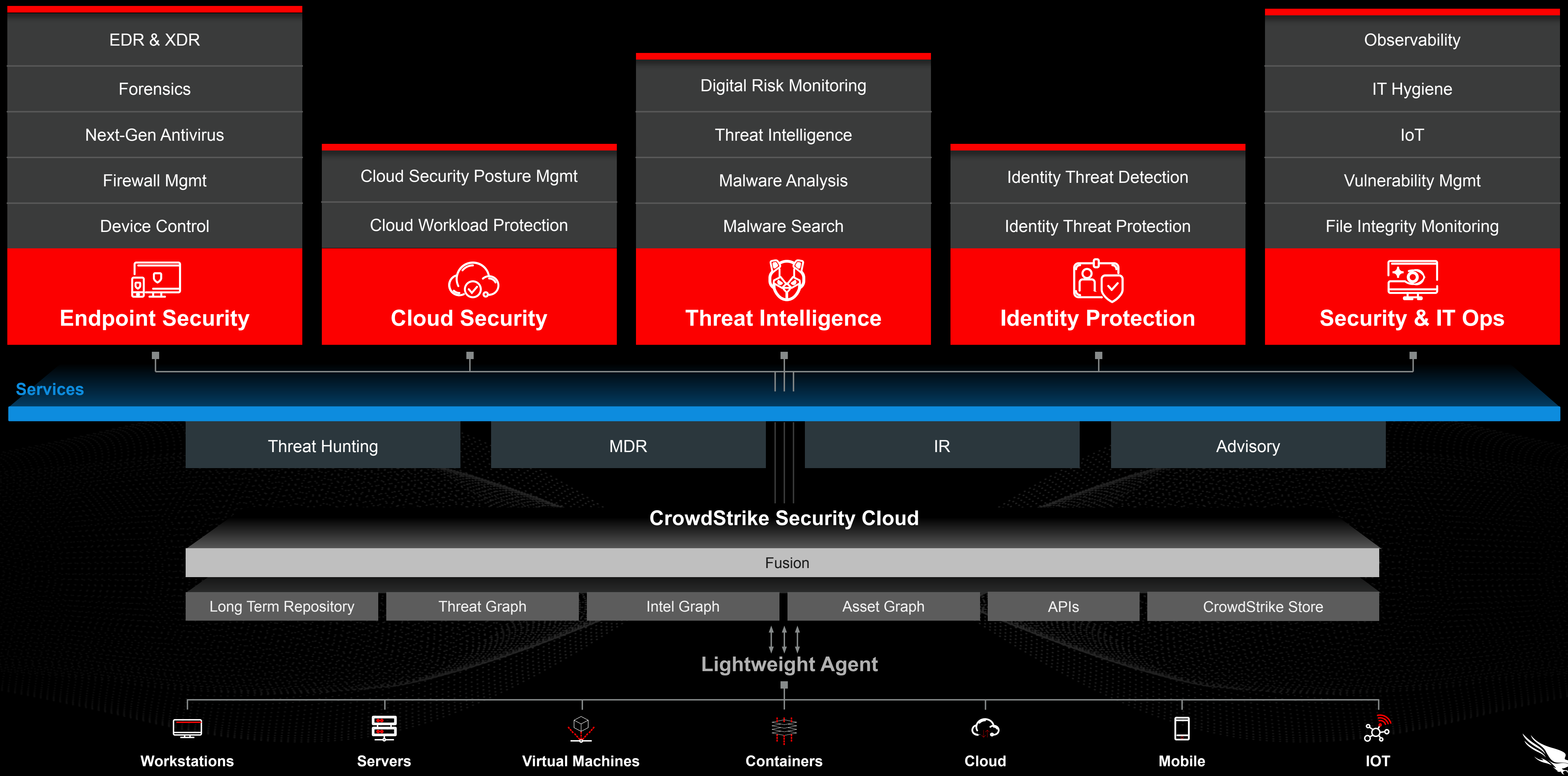
CONTROL REMOTE ACCESS

Refrain from exposing SMB and RDP ports to the internet, restrict remote access tools

PRACTICE GOOD HYGIENE

Control software, eliminating unneeded software, keep up-to-date with latest patches

The Falcon Platform



Endpoint Security
- EDR & XDR
- Forensics
- Next-Gen Antivirus
- Firewall Mgmt
- Device Control

Cloud Security
- Cloud Security Posture Mgmt
- Cloud Workload Protection

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

Identity Protection
- Identity Threat Detection
- Identity Threat Protection

Security & IT Ops
- Observability
- IT Hygiene
- IoT
- Vulnerability Mgmt
- File Integrity Monitoring

Services

- Threat Hunting
- MDR
- IR
- Advisory

CrowdStrike Security Cloud

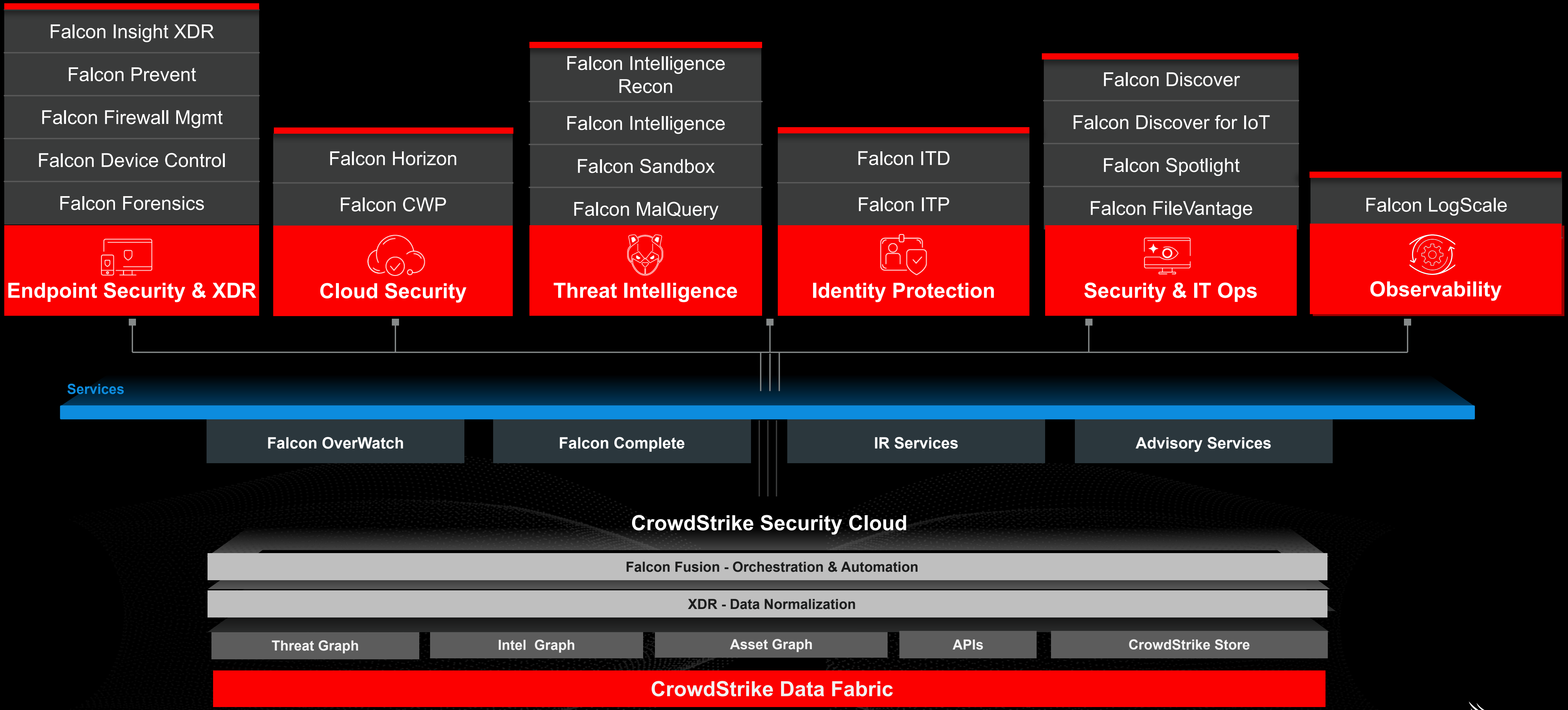
Fusion

- Long Term Repository
- Threat Graph
- Intel Graph
- Asset Graph
- APIs
- CrowdStrike Store

Lightweight Agent

- **Workstations**
- **Servers**
- **Virtual Machines**
- **Containers**
- **Cloud**
- **Mobile**
- **IOT**

The Falcon Platform



Endpoint Security & XDR
- Falcon Insight XDR
- Falcon Prevent
- Falcon Firewall Mgmt
- Falcon Device Control
- Falcon Forensics

Cloud Security
- Falcon Horizon
- Falcon CWP

Threat Intelligence
- Falcon Intelligence Recon
- Falcon Intelligence
- Falcon Sandbox
- Falcon MalQuery

Identity Protection
- Falcon ITD
- Falcon ITP

Security & IT Ops
- Falcon Discover
- Falcon Discover for IoT
- Falcon Spotlight
- Falcon FileVantage

Observability
- Falcon LogScale

Services
- Falcon OverWatch
- Falcon Complete
- IR Services
- Advisory Services

CrowdStrike Security Cloud

Falcon Fusion - Orchestration & Automation

XDR - Data Normalization

Threat Graph | Intel Graph | Asset Graph | APIs | CrowdStrike Store

CrowdStrike Data Fabric

Top Business Cases for Proactive Security

- 1) Real Time Response (EDR)
- 2) Immediate Remediation Reports (Falcon Complete Emails)
- 3) Corral Unmanaged Hardware and Software Assets (Discover > Unmanaged/Application Usage)
- 4) Get Authenticated Vulnerability Scans (Spotlight)
- 5) Executive-Level Key Metrics
- 6) Powerful Policies and Analytics (View Policies for RDP, Compromised PWs, Stale Accounts)
- 7) Stop Malicious Authentications (Challenge RDP, Force MFA on Compromised PWs, Block Stale Accounts)
- 8) Alert System Admins to Critical Issues (VIP Account Policies)
- 9) Track Down Behavior and Hygiene Issues (The Ghost Employee RDP)
- 10) Inspire Account and Password Cleanup (Policy Alerts > Create Reports)
- 11) Measure Cleanup Progress (Events Analysis)
- 12) Enforce Cleanup (New Policy for PW Reset or Block Stale Accounts)
- 13) Eliminate Attack Paths to Critical Accounts (Monitor > Attack Path)
- 14) Gain Awareness of Azure AD Incidents (Cred Scan/PW Spray Incidents)
- 15) Verify Lockouts are Actually Malicious
- 16) Correlate Endpoint and Identity Activity (EDR > ITP)

YOUR ABILITY TO DEFEAT ADVANCED CYBER THREATS RESTS ALMOST ENTIRELY ON YOUR UNDERSTANDING OF THE PROBLEM

CROWDSTRIKE

CrowdStrike’s Layered Defense

Zero Trust Strategy

SECURE AUTHENTICATION
IDENTITY PROTECTION

AUTHORIZATION
IDENTITY PROTECTION

VULNERABILITY MANAGEMENT
SPOTLIGHT

PREVENTION & VISIBILITY
PREVENT & INSIGHT

CLOUD SECURITY
CLOUD PROTECTION

DATA AGGREGATION & XDR
HUMIO

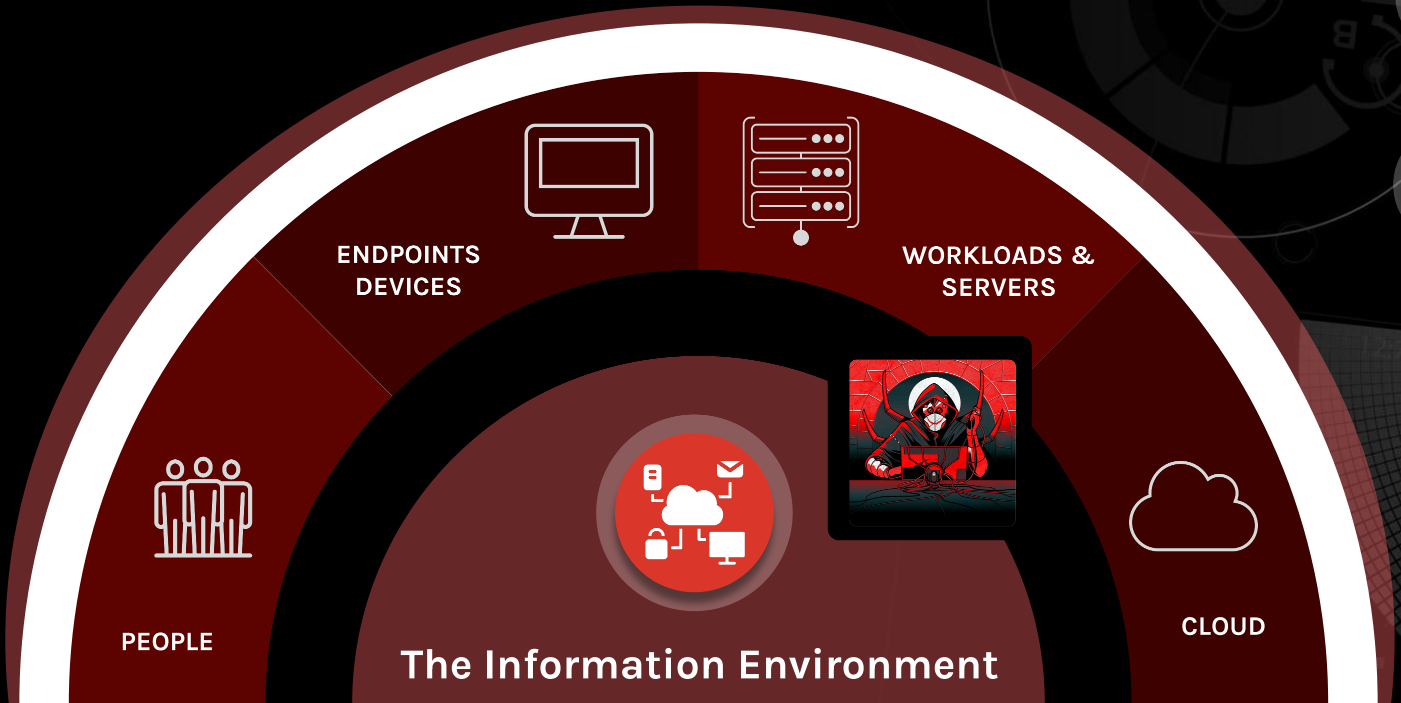
FILE INTEGRITY MONITORING
FILEVANTAGE

THREAT INTELLIGENCE
FALCON X

24/7/365 THREAT HUNTING
OVERWATCH

PROFESSIONAL SERVICES
CROWDSTRIKE SERVICES

MDR SERVICES
FALCON COMPLETE



CROWDSTRIKE

CROWDSTRIKE