Disrupting Advanced Persistent Cybercrime

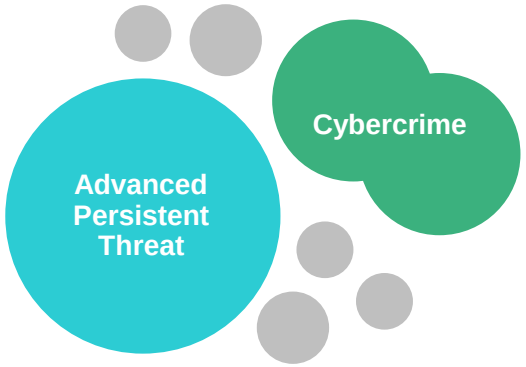
Derek Manky

Chief Security Strategist & Global VP Threat Intelligence

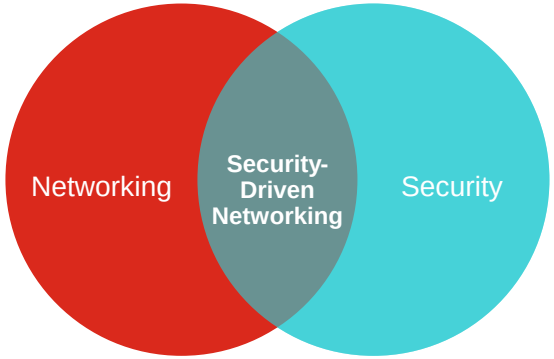
The Converging Threat Landscape

Reduced Complexity and Rapid Response

THREAT LANDSCAPE

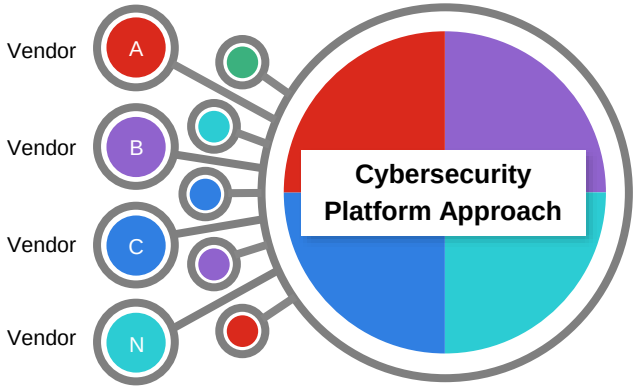


CONVERGENCE OF NETWORKING AND SECURITY



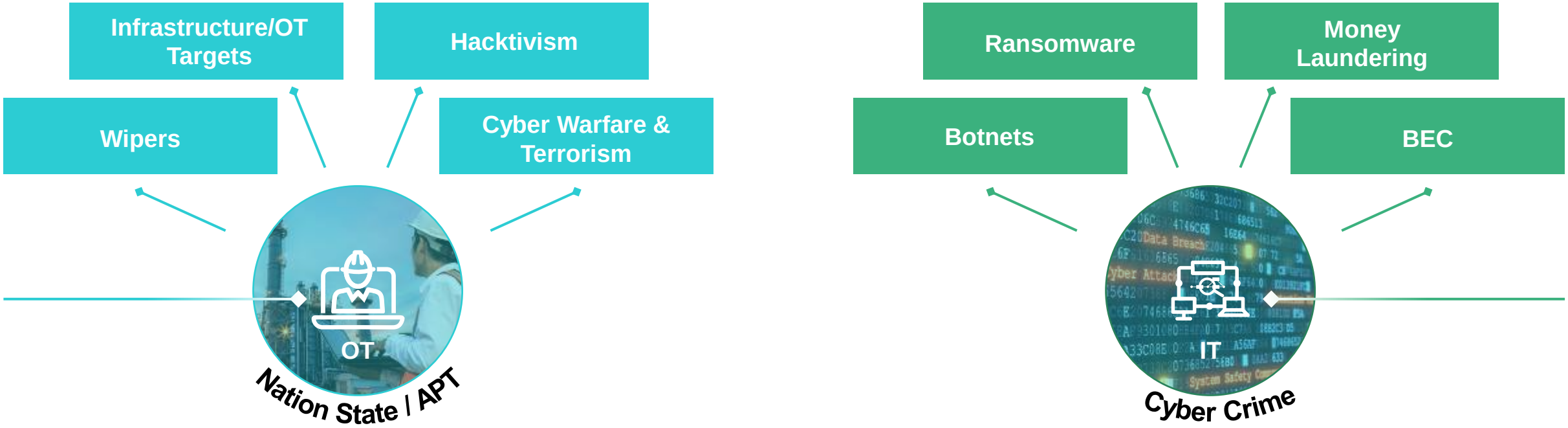
Proof points: Gartner Enterprise Networking Market Forecast

CONSOLIDATION OF SECURITY POINT PRODUCT VENDORS



Proof point: Gartner Cybersecurity MESH Architecture

Advanced Persistent Cybercrime



PRE-ATT&CK

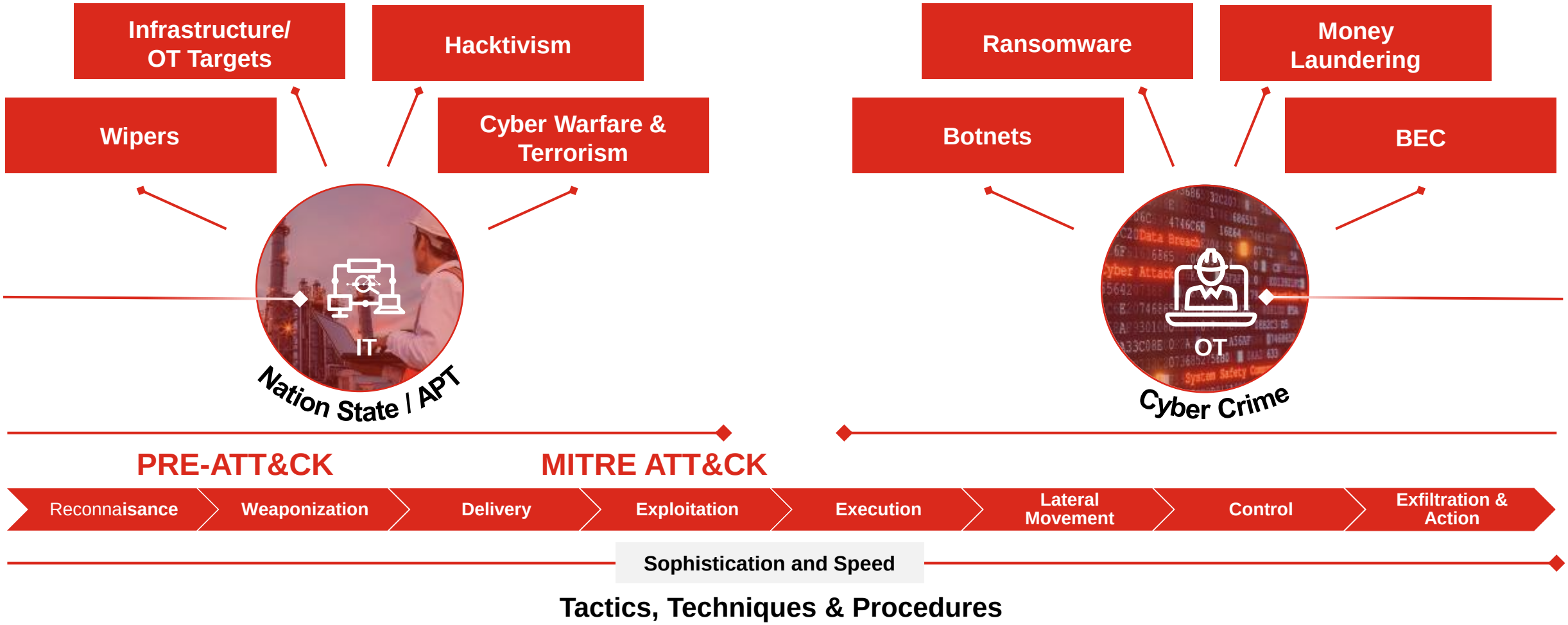
MITRE ATT&CK

Reconnaissance | Weaponization | Delivery | Exploitation | Execution | Lateral Movement | Control | Exfiltration & Action

Sophistication and Speed

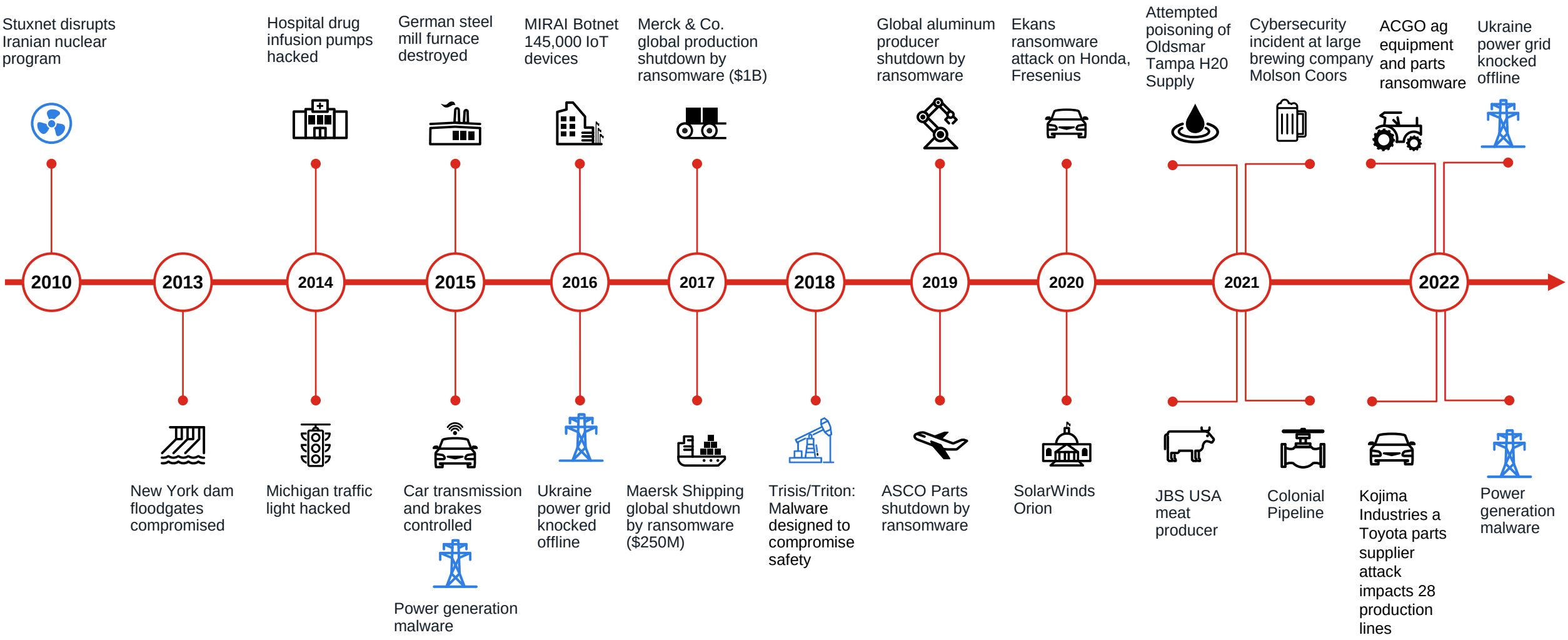
Tactics, Techniques & Procedures

Advanced Persistent Cybercrime



OT Infrastructure Attacks Are Getting Worse

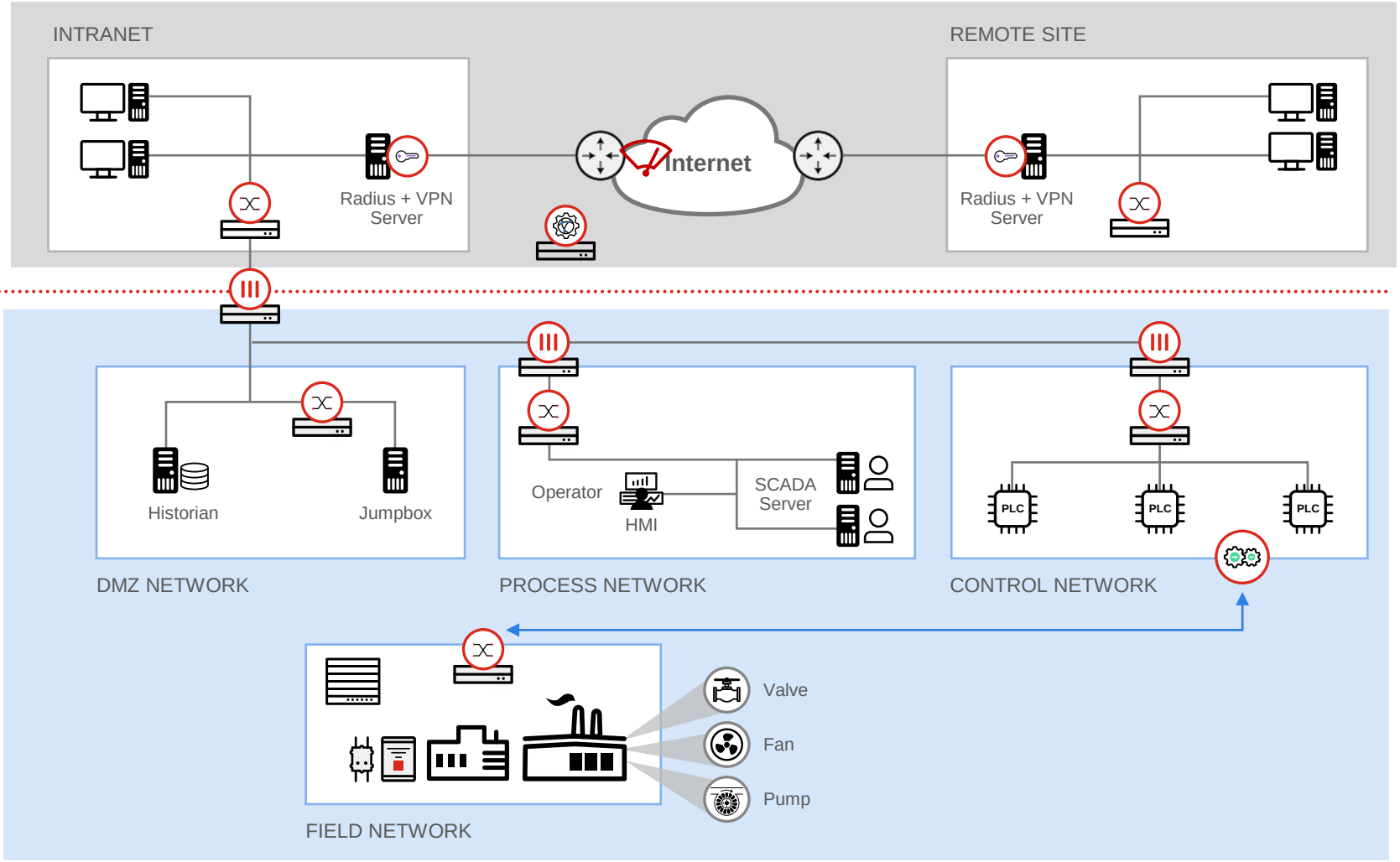
Attacks are increasing in frequency and impact



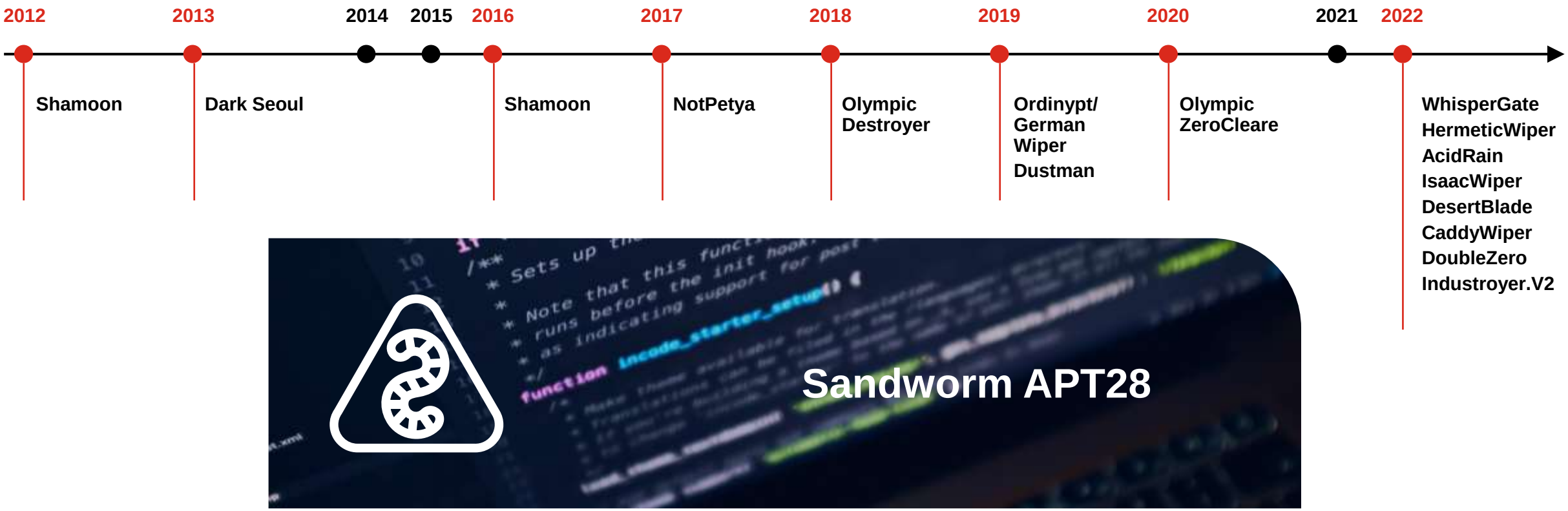
Advanced Persistent Cybercrime

Information Technology (IT)

Operational Technology (OT)



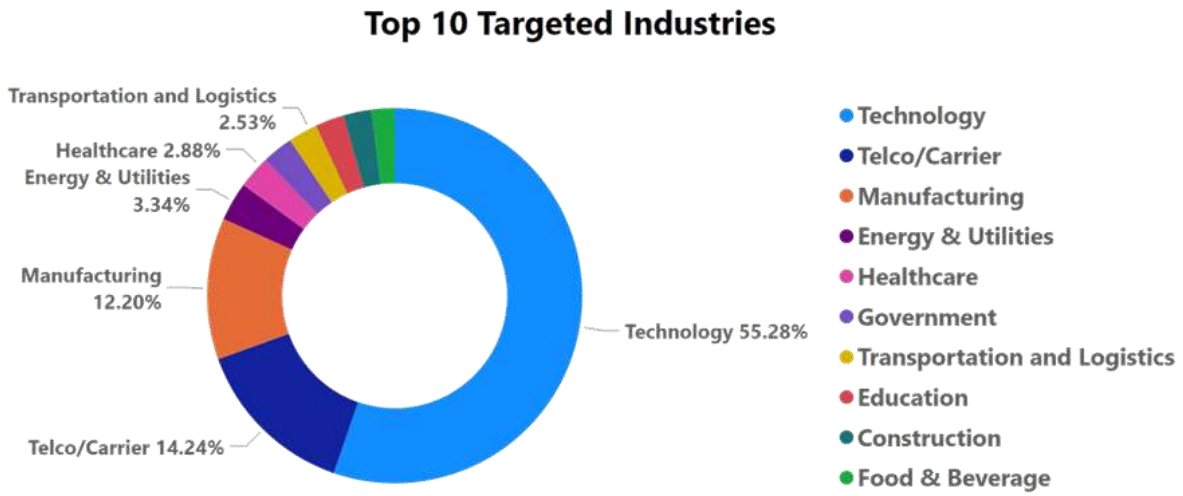
Wiper Malware Timeline

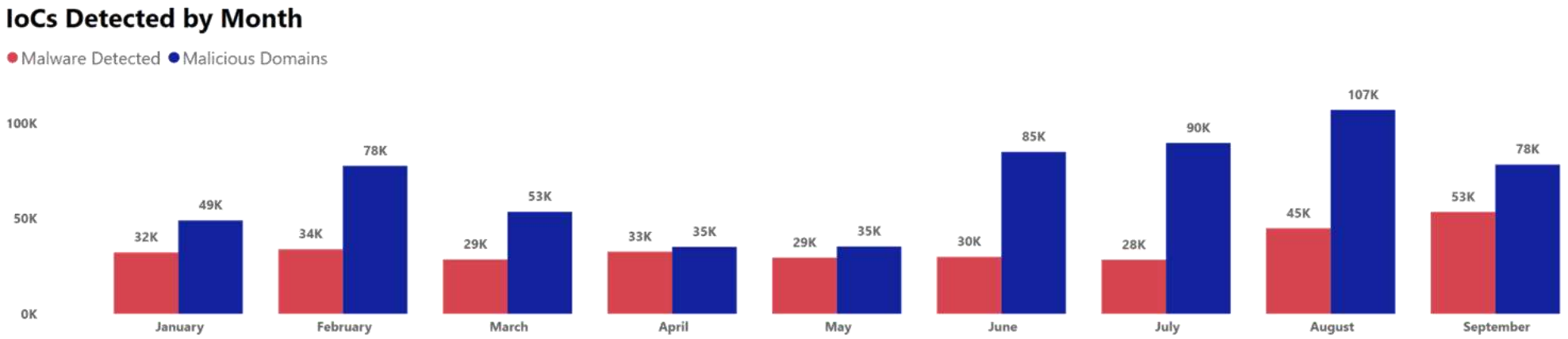


Sandworm – OT & IT Convergence (APC)

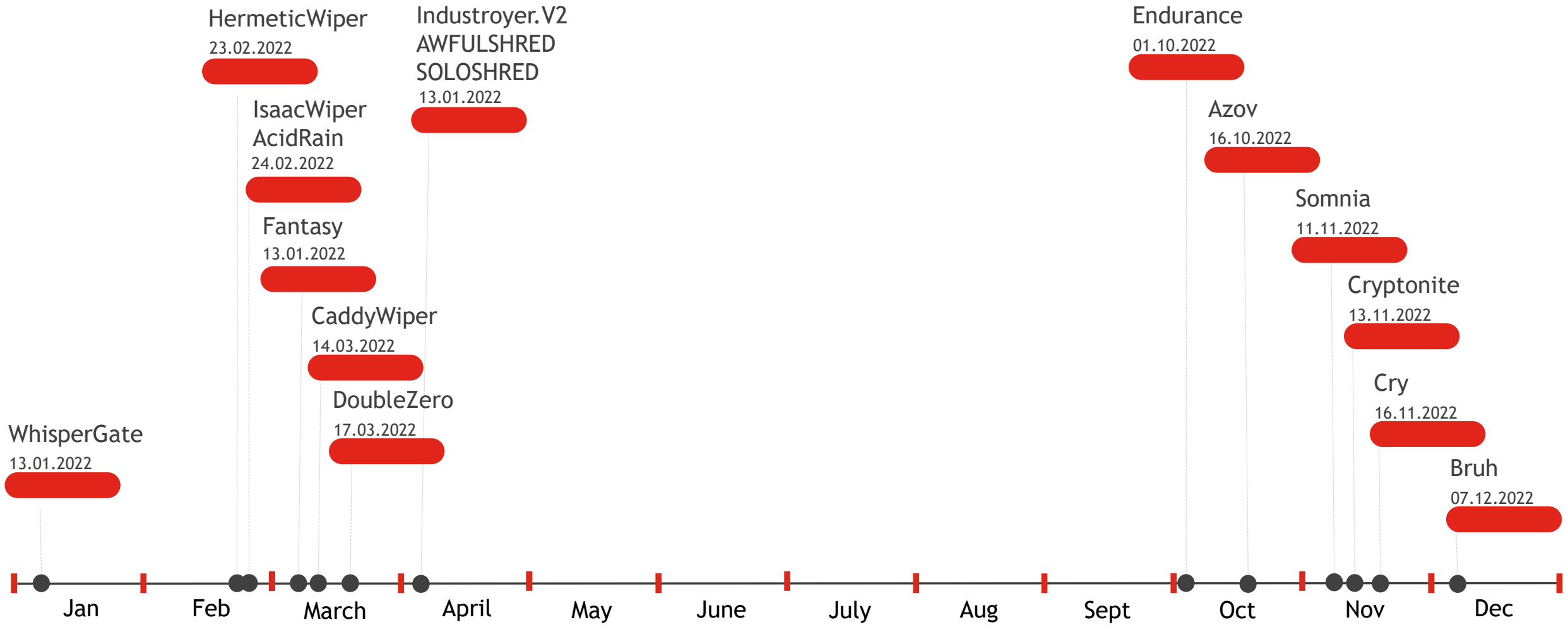
Total Detections

313K 610K



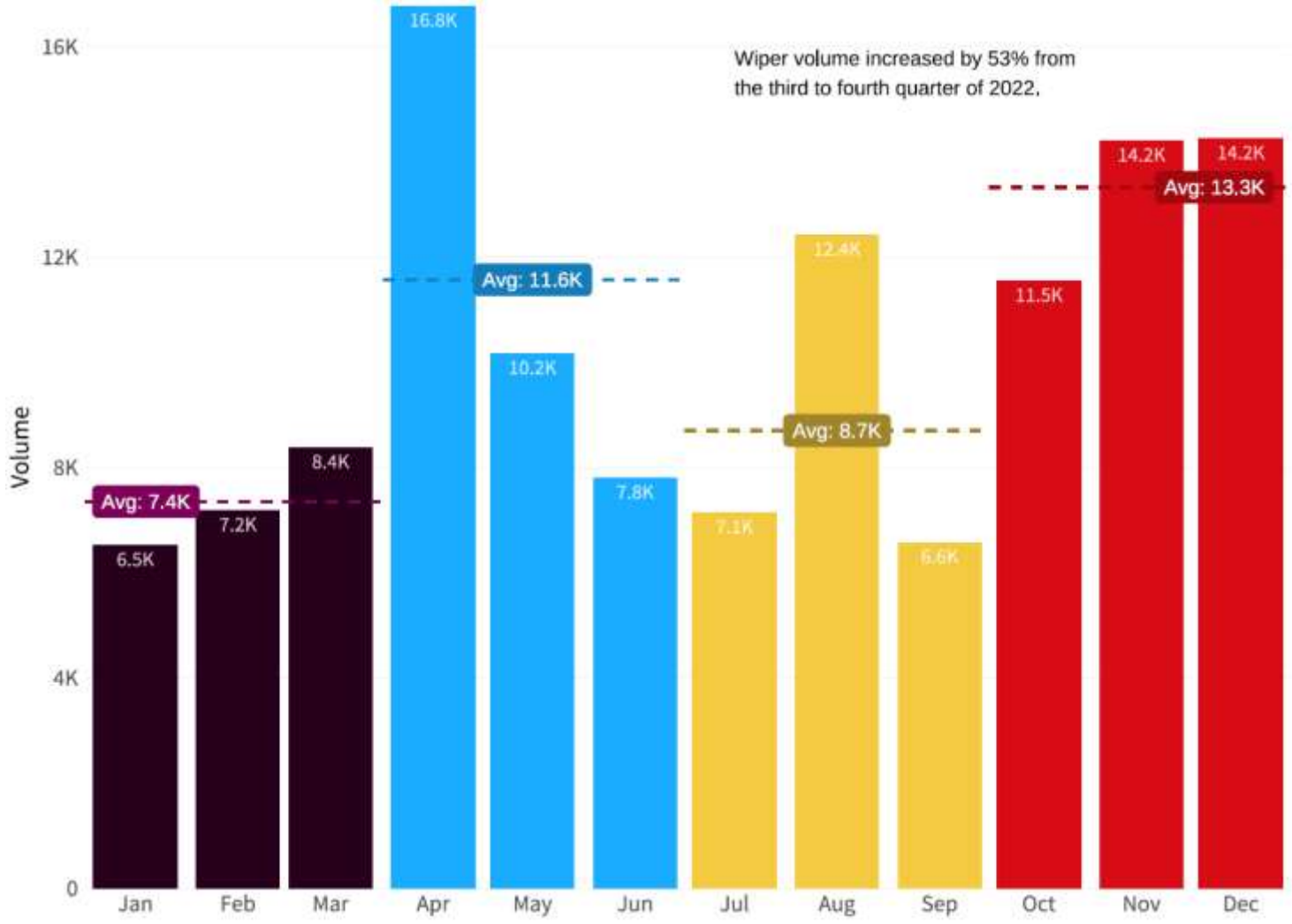


Wiper Attacks 2022 First Appearance



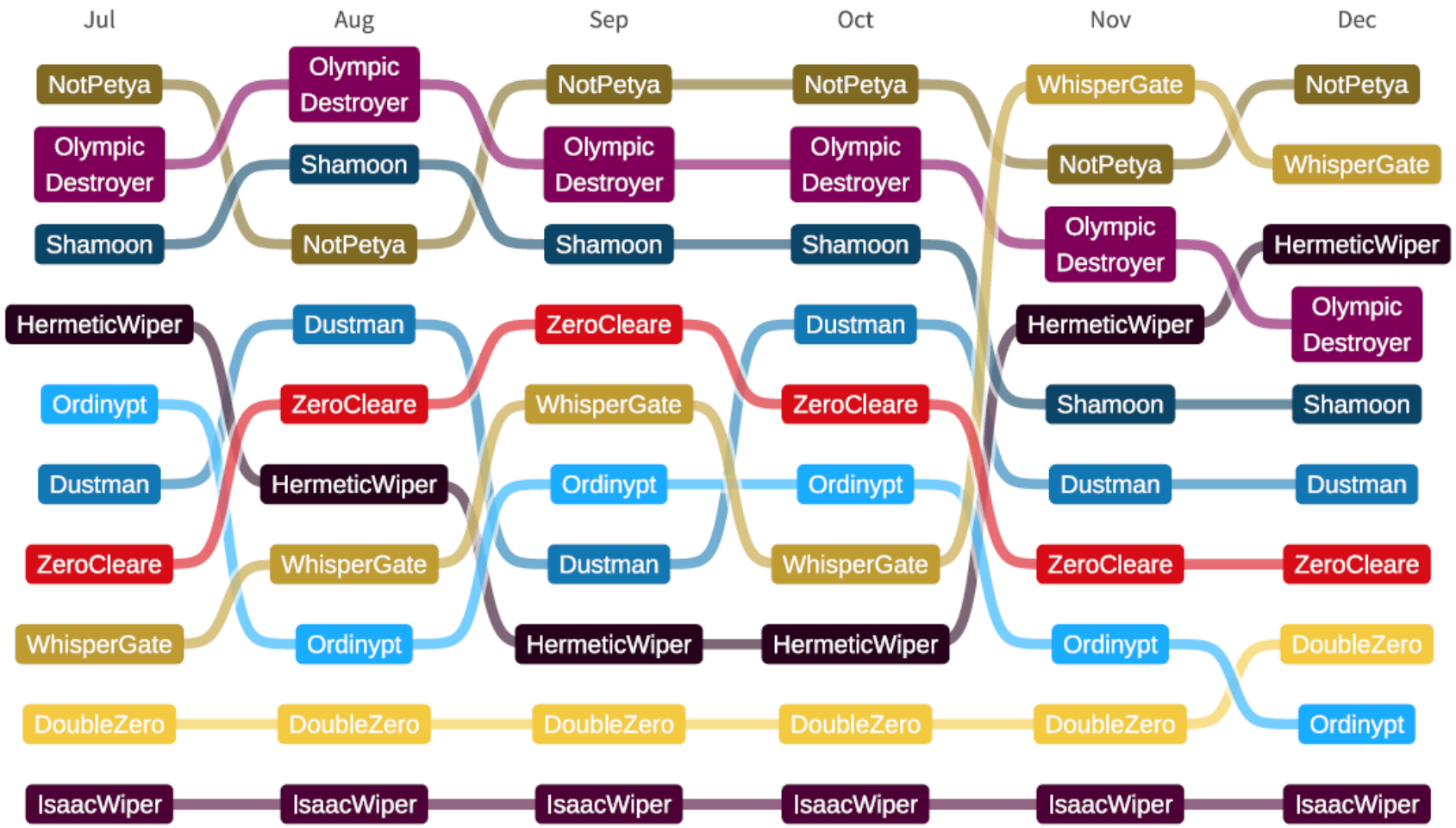
Wiper – Growth 53% Q3 vs. Q4 2022

Jan-Dec 2022 Wiper Growth Tracking



Wiper - Ranking

Jul-Dec 2022 Top Wiper Families in the Wild



Wiper – Global Spread

Jul-Dec 2022 Regional Prevalence of Wiper Families

	Africa	Asia	Europe	N. America	S. America
WhisperGate	75%	62%	74%	44%	71%
NotPetya		92%	74%	56%	71%
HermeticWiper	25%	85%	73%	44%	57%
Shamoon	25%	69%	62%	56%	43%
DoubleZero	50%	46%	64%	22%	71%
IsaacWiper	25%	54%	54%	11%	57%
Dustman		62%	60%	22%	43%
ZeroCleare		62%	60%	22%	43%
Olympic Destroyer		54%	68%	22%	43%
Ordinypt		46%	59%	11%	43%
CaddyWiper	25%	15%	14%	22%	
WhisperKill		15%	12%	22%	
Azov			15%	11%	14%
AcidRain		15%		22%	

Disruption Efforts

Cybercrime Atlas

C4C CYBERCRIME ATLAS

EXPERT COMMUNITY

- ✓ 20+ Analysts contributed
- ✓ Weekly scrums
- ✓ 4 Levels of analysis

INTELLIGENCE KNOWLEDGE BASE

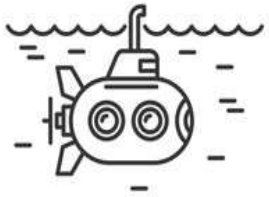
COLLABORATIVE PLATFORM

- 1+ Year POC on 13 Cybercrime Operations
- Over 800+ points of disruption identified on actors, 1000+ collective hours
- Positive connections between APT nation state and cyber crime groups discovered

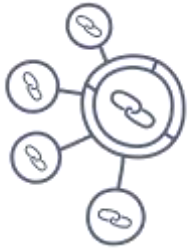
OPERATIONAL FRAMEWORK

Cybercrime Atlas: Analysis

Foundational research



Deep dive



Link analysis

Attribution & disruption prospects

1. Taxonomy

2. 3-4 Sample Threat Actors across 4 cybercrime Types:

- Ransomware
- Malware
- Business Email Compromise
- Card Fraud

- OSINT

WEF Cybercrime Atlas

EXPERT
COMMUNITY

INTELLIGENCE
KNOWLEDGE BASE

COLLABORATIVE
PLATFORM

OPERATIONAL
FRAMEWORK

PHASE 2 RECOMMENDATION / PREPARATION

- Continue to build PH1 Research and Analysis
- Prepare recommendations / Concept of operation for Phase 2
- Steering committee to design the foundation
- Iinitiating the incorporation process
- Building a community

FORTINET Microsoft Santander PayPal

ATLAS LAUNCH Davos 23

- January 15 2023

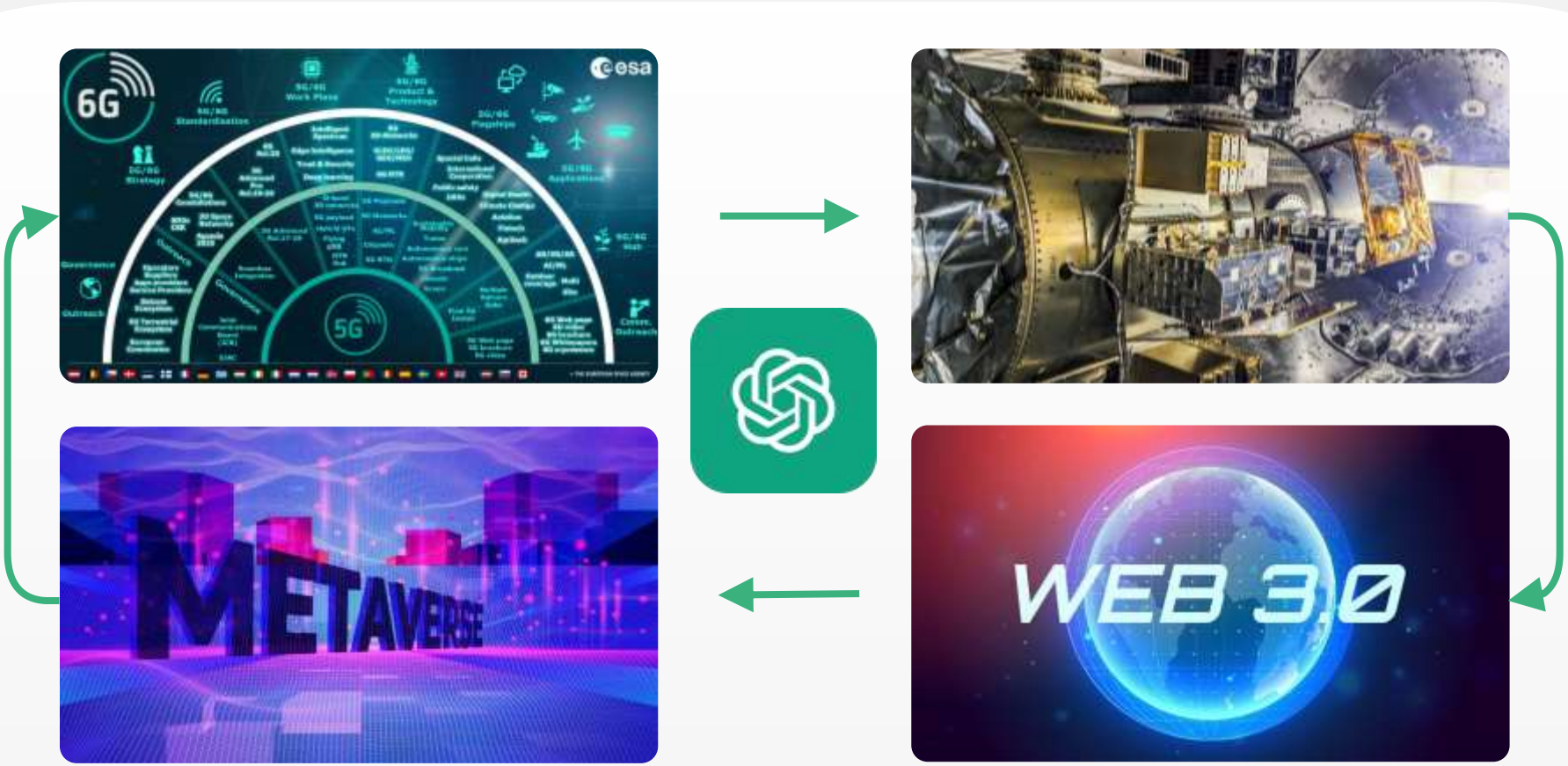
PHASE 1 PILOT
RESEARCH / ANALYSIS / IDENTIFICATION

- Map sample deep rather than broad
- Identify Linkages / Net New intelligence
- Develop / discover / define analytic process / techniques
- Conduct Stakeholder engagement / Define Requirements
- Develop / Articulate CybercrimeATLAS Terms of Reference
- Develop system requirements & use cases for PH2

ESTABLISHMENT and Transition to Operations

- Establish ATLAS Organization
- Securing commitments and fundings
- Operations and partnerships

A Converging Threat Landscape



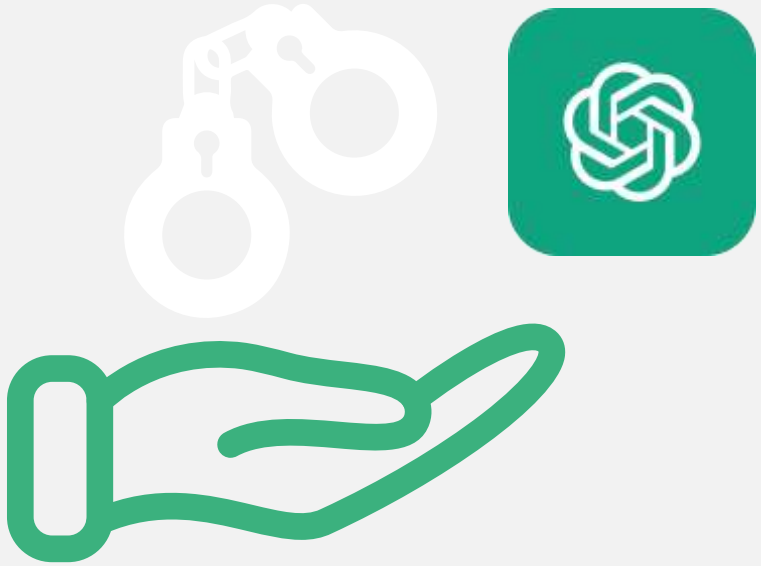
2023 PREDICTION:

The Growth of Wiper Malware

1. Wipers in combination with other attack vectors is one of the biggest emerging threats we're facing, allowing malware to replicate and spread quickly
2. Time to detection and the speed at which security teams can remediate is paramount
3. The commoditization of wipers give them the potential to impact networks at exponential scale.

2023 PREDICTION:

New Crime-as-a-Service (CaaS) Offerings



1. Threat Actors will take advantage of turnkey, subscription-based offerings
2. Seasoned Criminals will create and sell “as a service” attack portfolios
3. Attackers will leverage emerging attack vectors such as deepfakes
4. Influencers and those with a strong digital presence will be targeted
5. Reconnaissance as a Service: “Detectives” will gather intel, and RaaS offerings may include attack blueprints to ensure an effective attack


FORTINET