Welcome to the world of Cyber Threat Intelligence!

Andreas Sfakianakis - 30/06/2021

Image: EclecticIQ

whoami

CTI Lead EMEA @ S&P Global

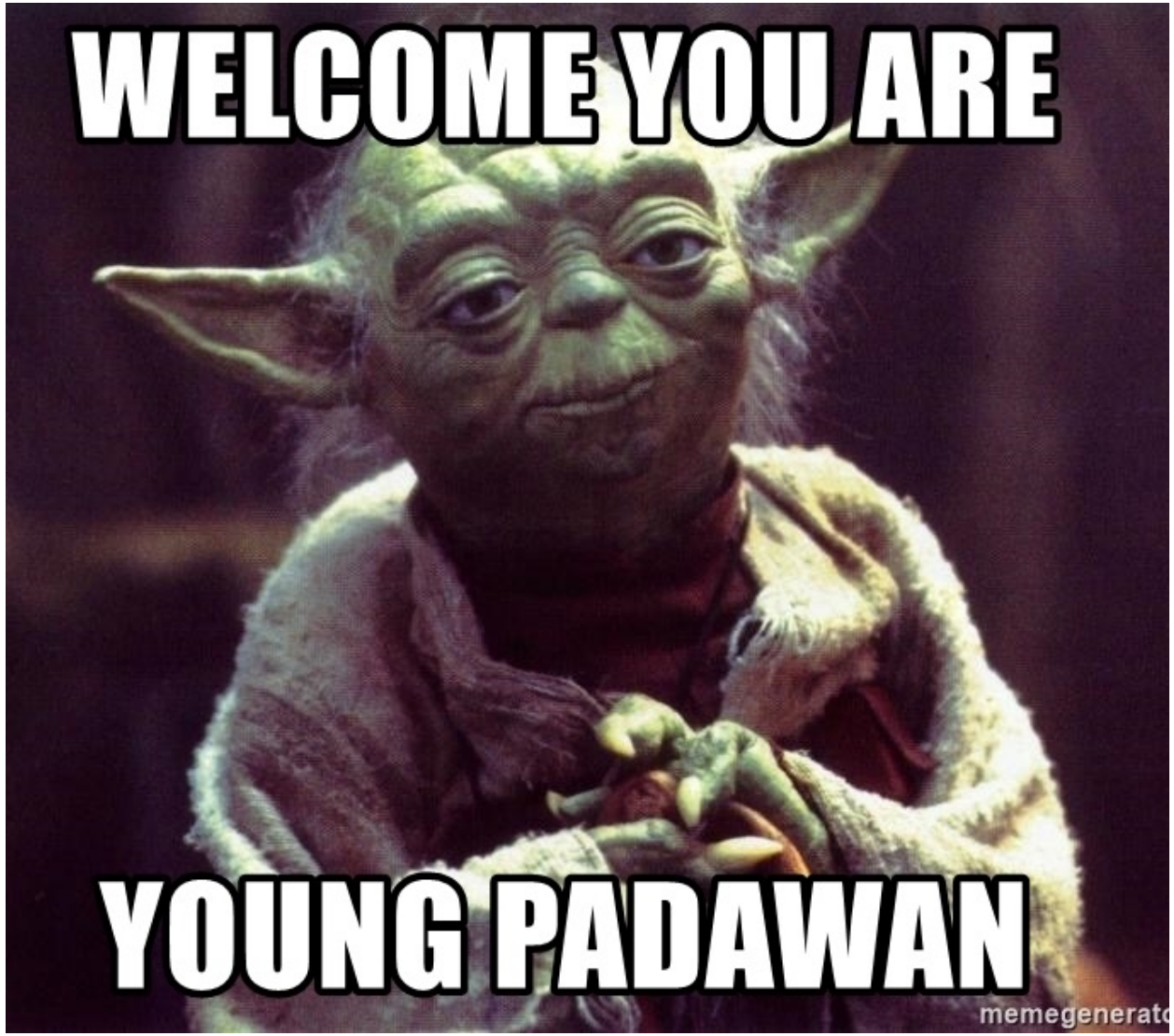
CTI @ Financial and Oil & Gas sectors

ENISA, FIRST.org, SANS, European Commission

Twitter: @asfakian Website: www.threatintel.eu

Outline

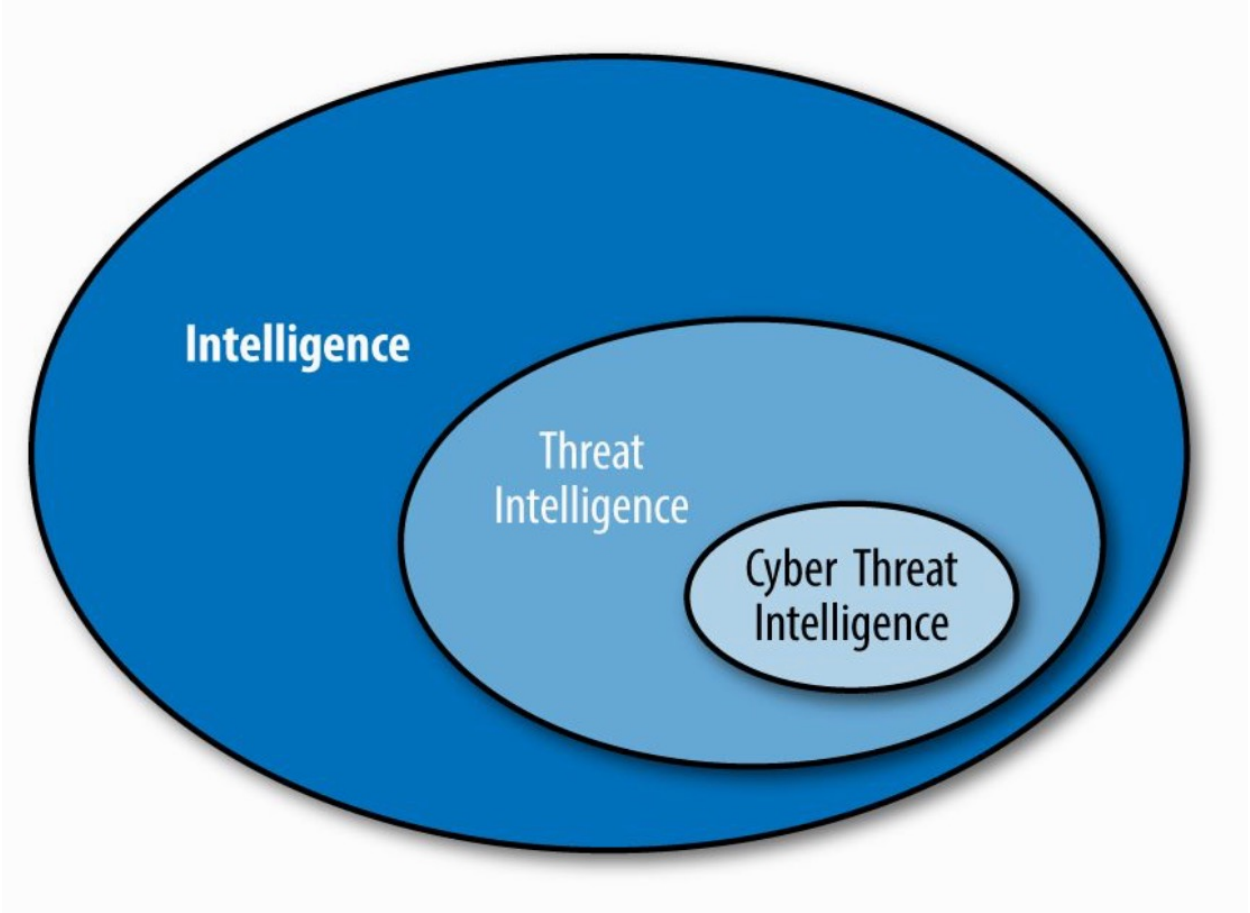
- Intro to CTI
- A view at the Threat Landscape
- CTI Analyst Skillset



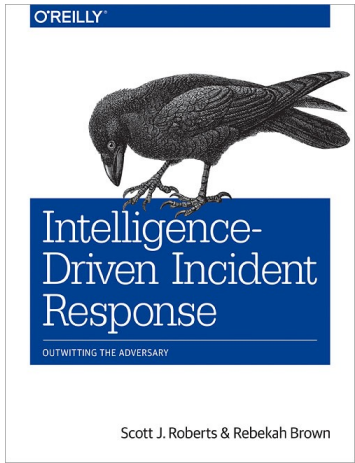
Intro to Cyber Threat Intelligence

Image:
Katie Nickels

From Intelligence to Cyber Threat Intelligence

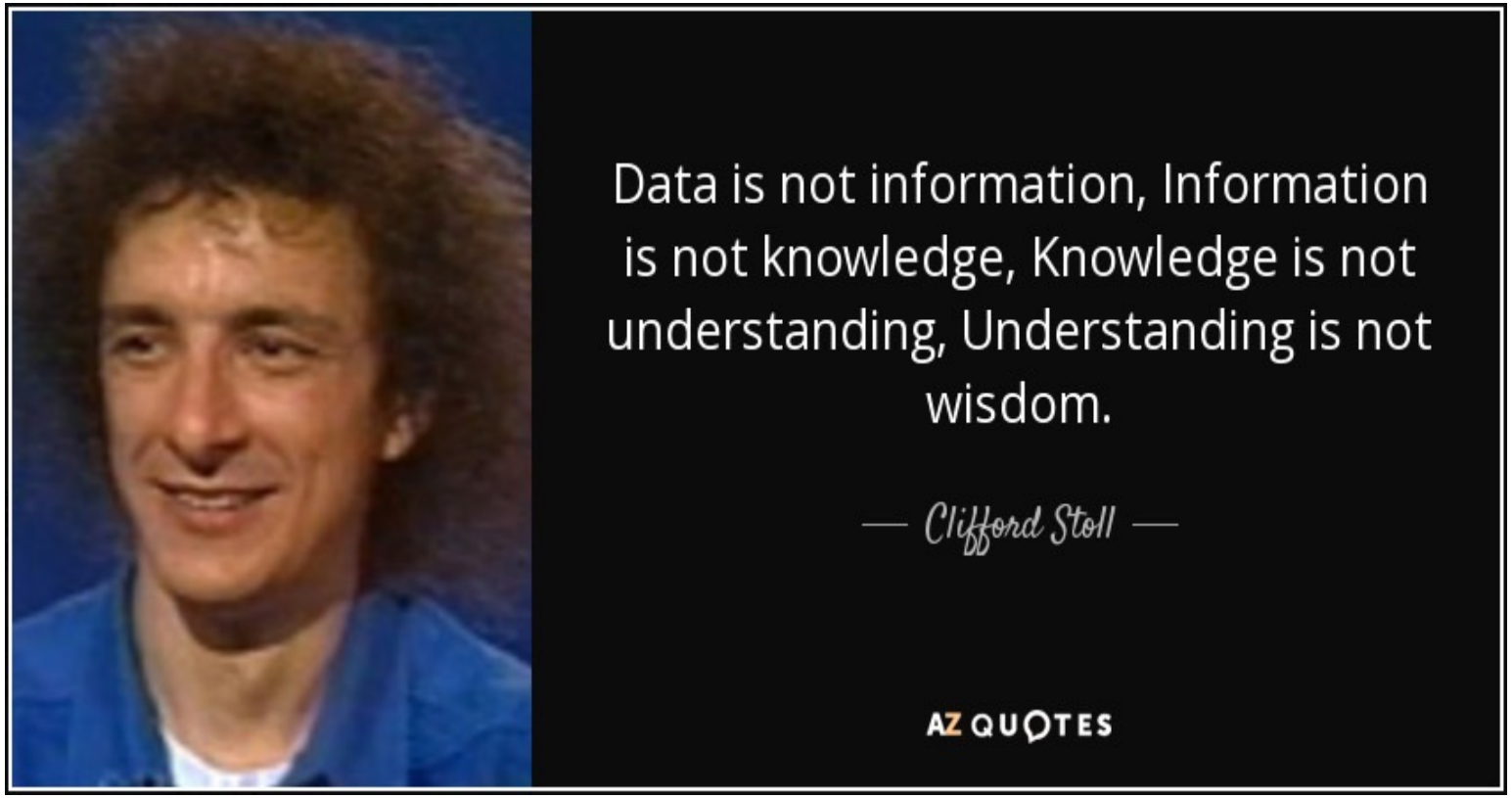


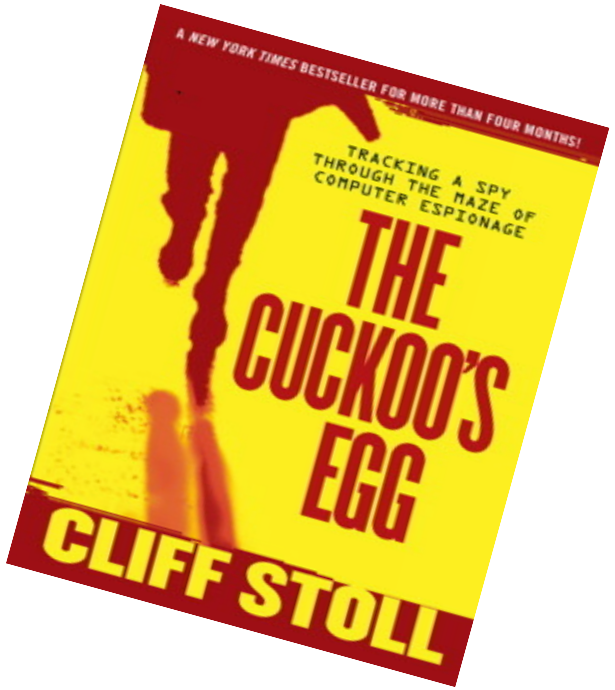
Reference:




How old is
Cyber Threat Intelligence?

When everything started in CTI!



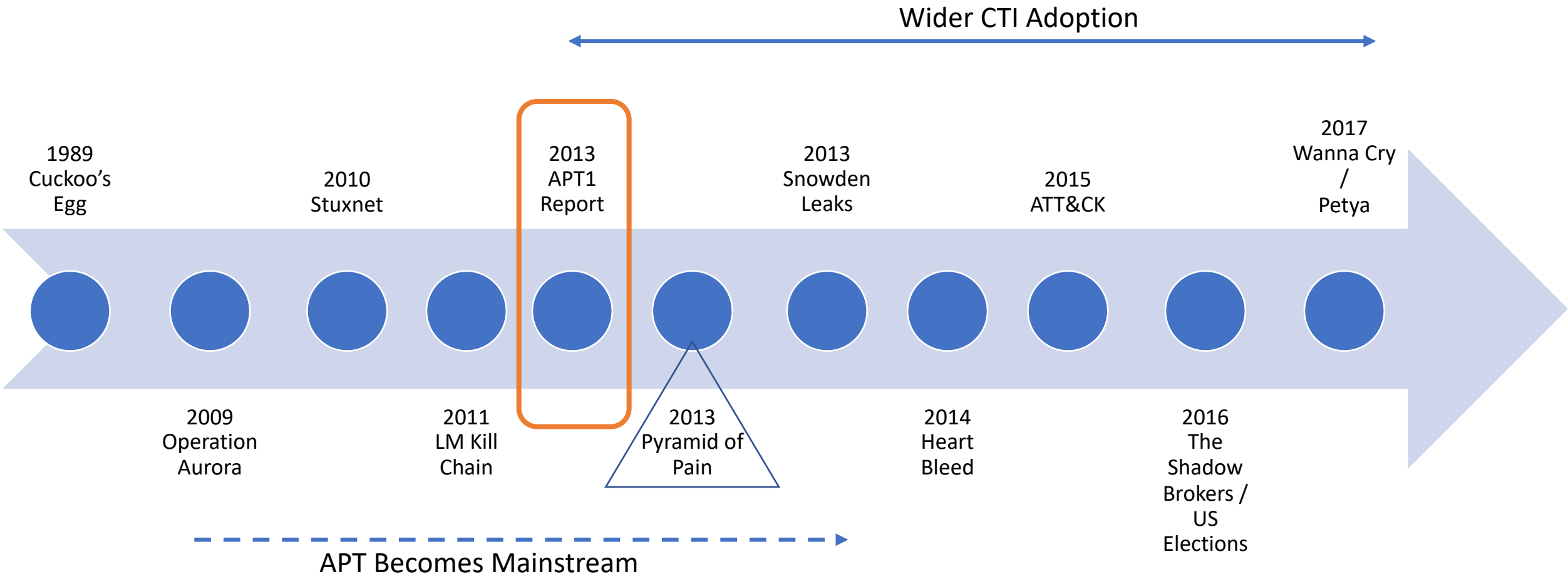


CTI, IR and SecOps

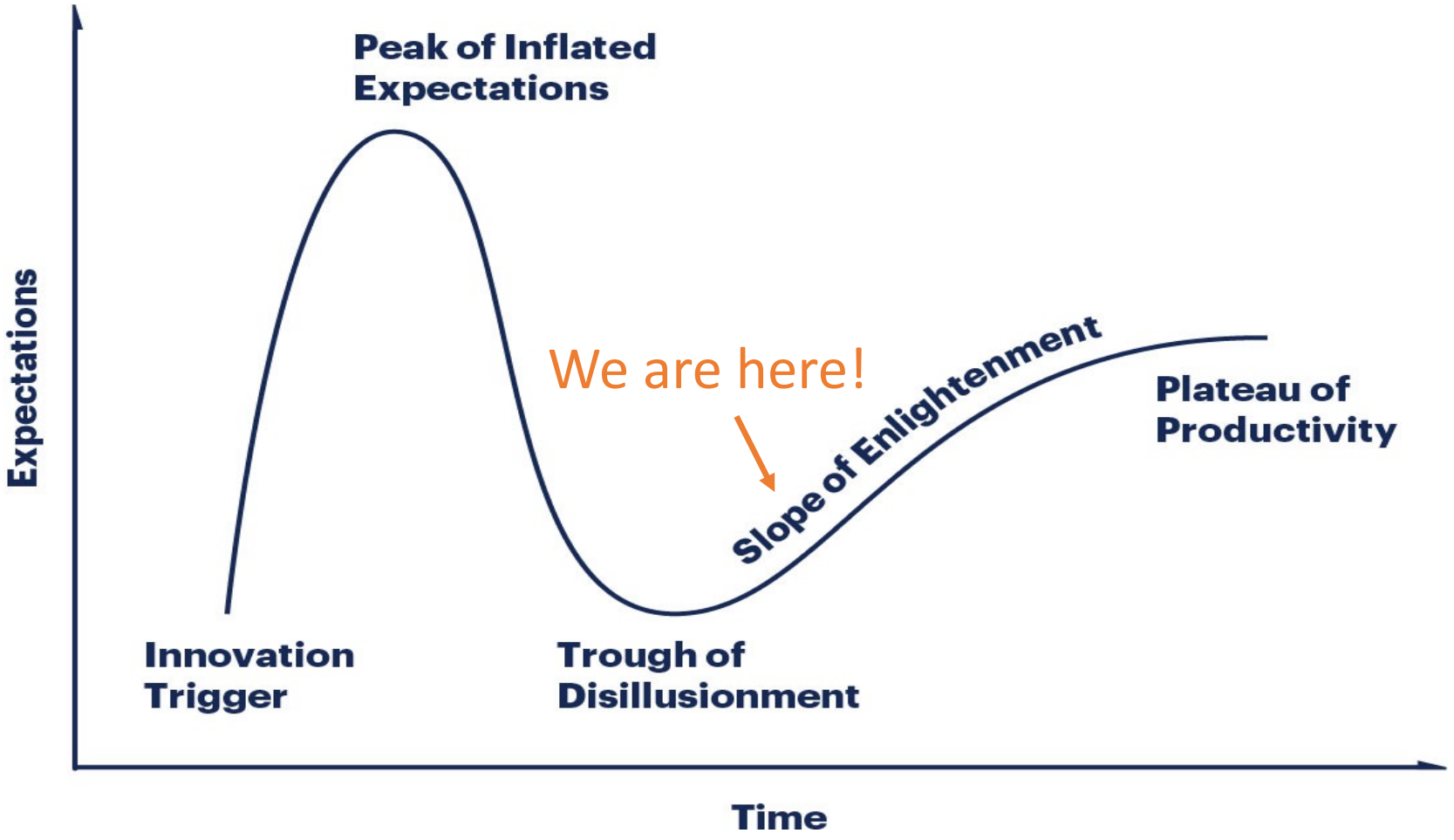
	CYBER THREAT INTELLIGENCE	INCIDENT RESPONSE	SECURITY OPERATIONS
Adoption	Early adoption phase	Mainstream since ~2010	Mainstream since ~2005
Focus	External threat monitoring	Security incidents and risk escalation	Notable security event monitoring
Best practices	Evolving best practices	Mature best practices	Mature best practices
Technology enablement	Evolving technology enablement	Mature technology enablement	Mature technology enablement

Reference: EclecticIQ

Timeline of important events in CTI history



CTI Hype Cycle



Reference:

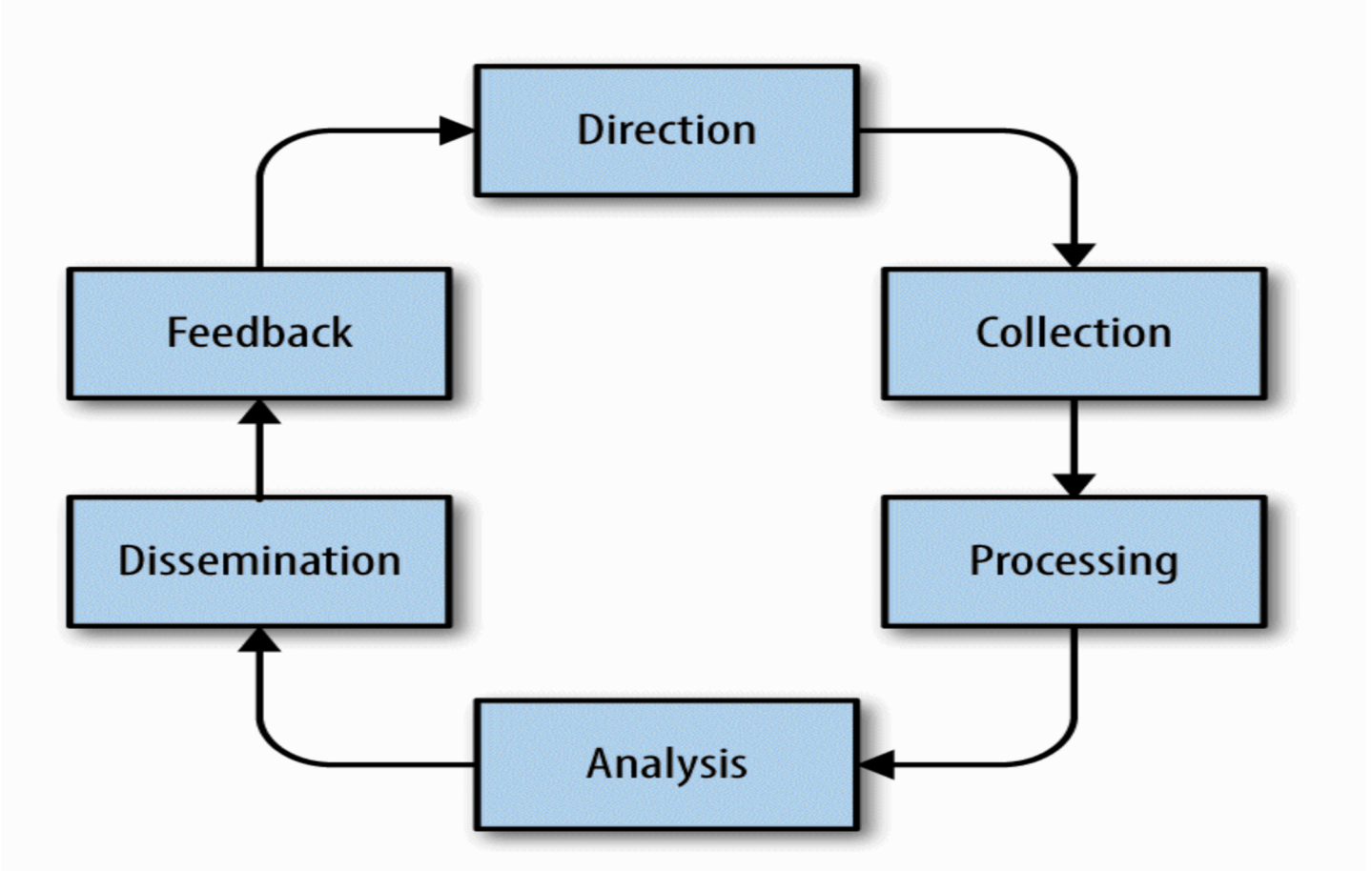
Gartner


How would you
consume or generate
(cyber threat) intelligence?

Reference:
Joe Slowik

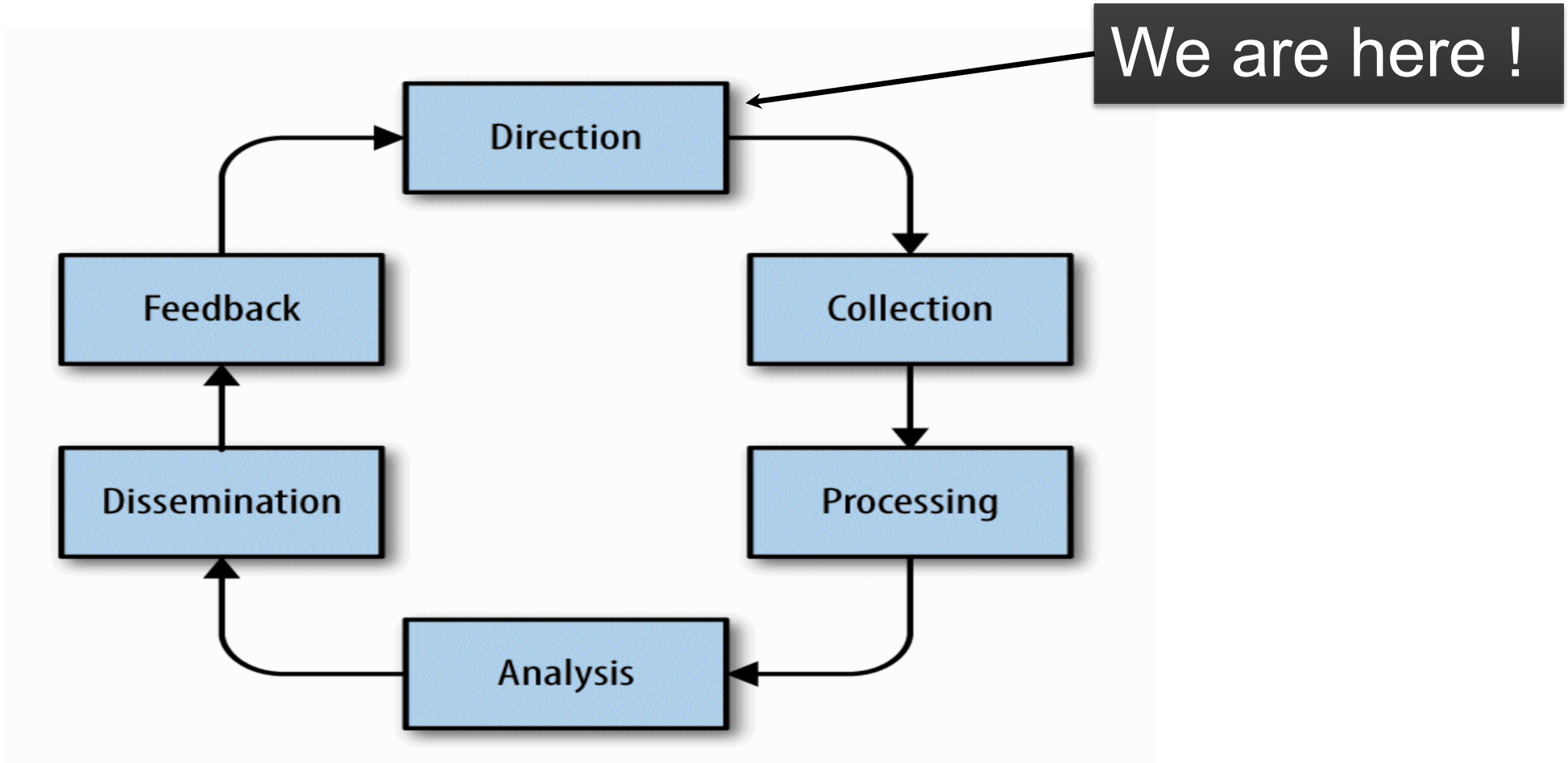
Repeat after me

Let me introduce you to the intelligence cycle



All models are wrong, but some are useful (especially within corporate environments)

Intelligence Direction



Questions to be answered

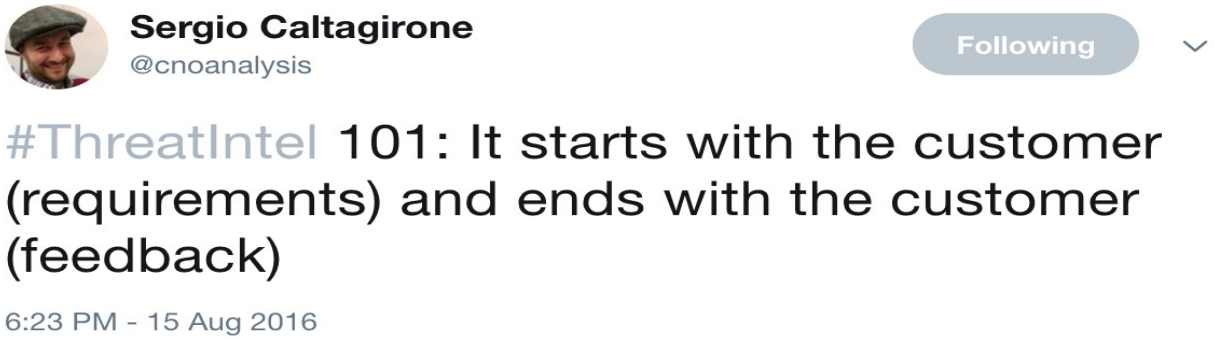
- Does your org need a CTI function? Why do you need intelligence?
- How do you identify which threats are relevant to your organisation?
- How do you prioritize to which threats to spend time on?
- Has your CTI team identified and connected with its stakeholders?
- How does your analysis bring value to the CyberDefence and your organisation?

“CTI teams should not do intelligence for intelligence’s sake; it costs money and time”

Intelligence Requirements

- Intelligence requirements are enduring questions that consumers of intelligence need answers to.

- Answer critical questions intelligence customers care about (not what YOU care about).



Reference: Sergio Caltagirone

CTI Focus and Stakeholders

Tactical Intelligence

- Security Engineering
- SOC Team

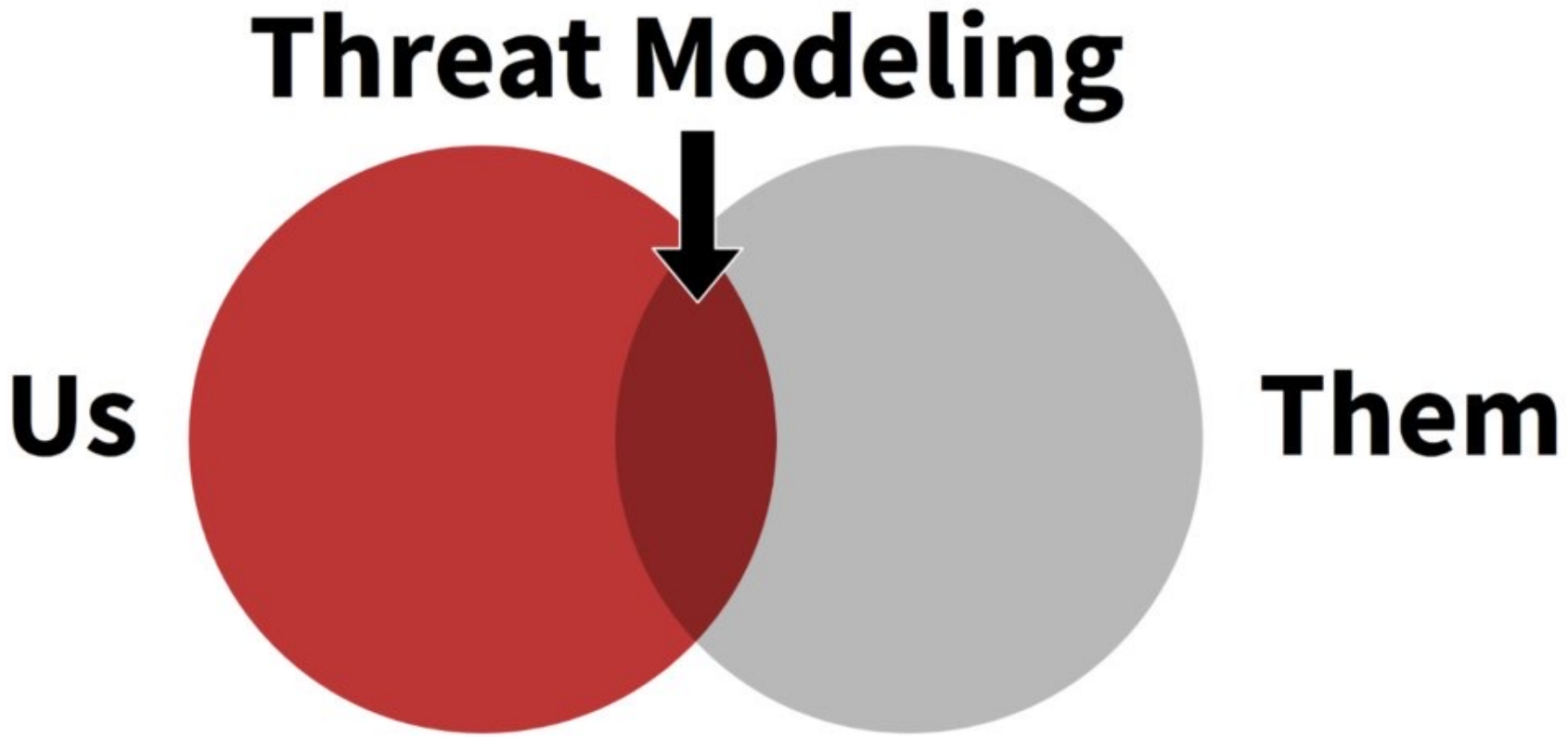
Operational Intelligence

- Incident Responders
- Threat Hunters
- Vulnerability Management
- Red Team
- Fraud Team
- Sys Admins
- IT Managers

Strategic Intelligence

- C-Suite / Executives
- Group Security
- Risk Managers
- Business Stakeholders
- Regional Stakeholders
- IT Architects

https://www.youtube.com/watch?v=kGqnCR6XOhQ

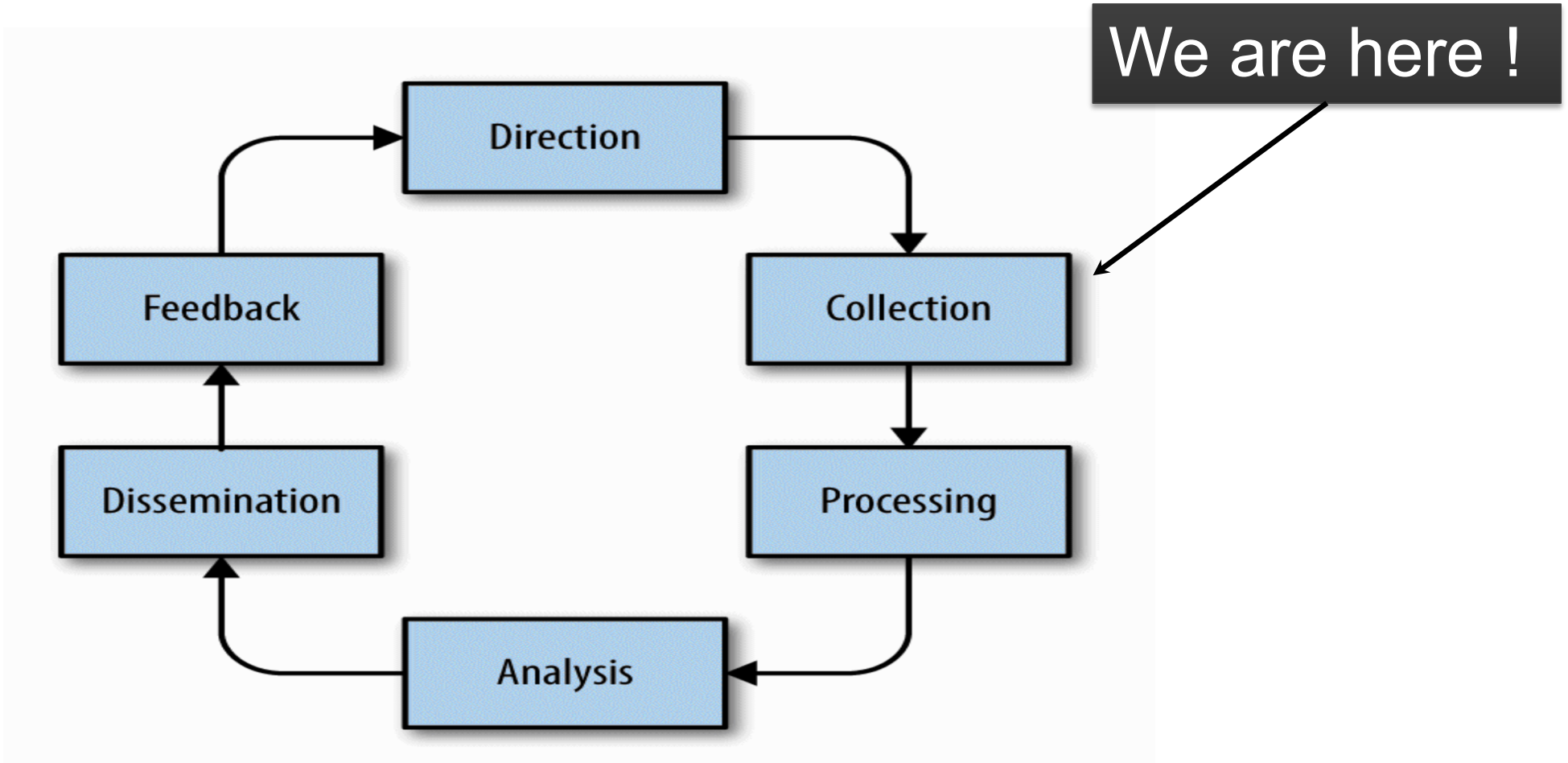


Reference:
Katie Nickels

Simple Threat Model

Reference: SANS

Intelligence Collection




Where would you go to collect data for cyber threat intelligence?

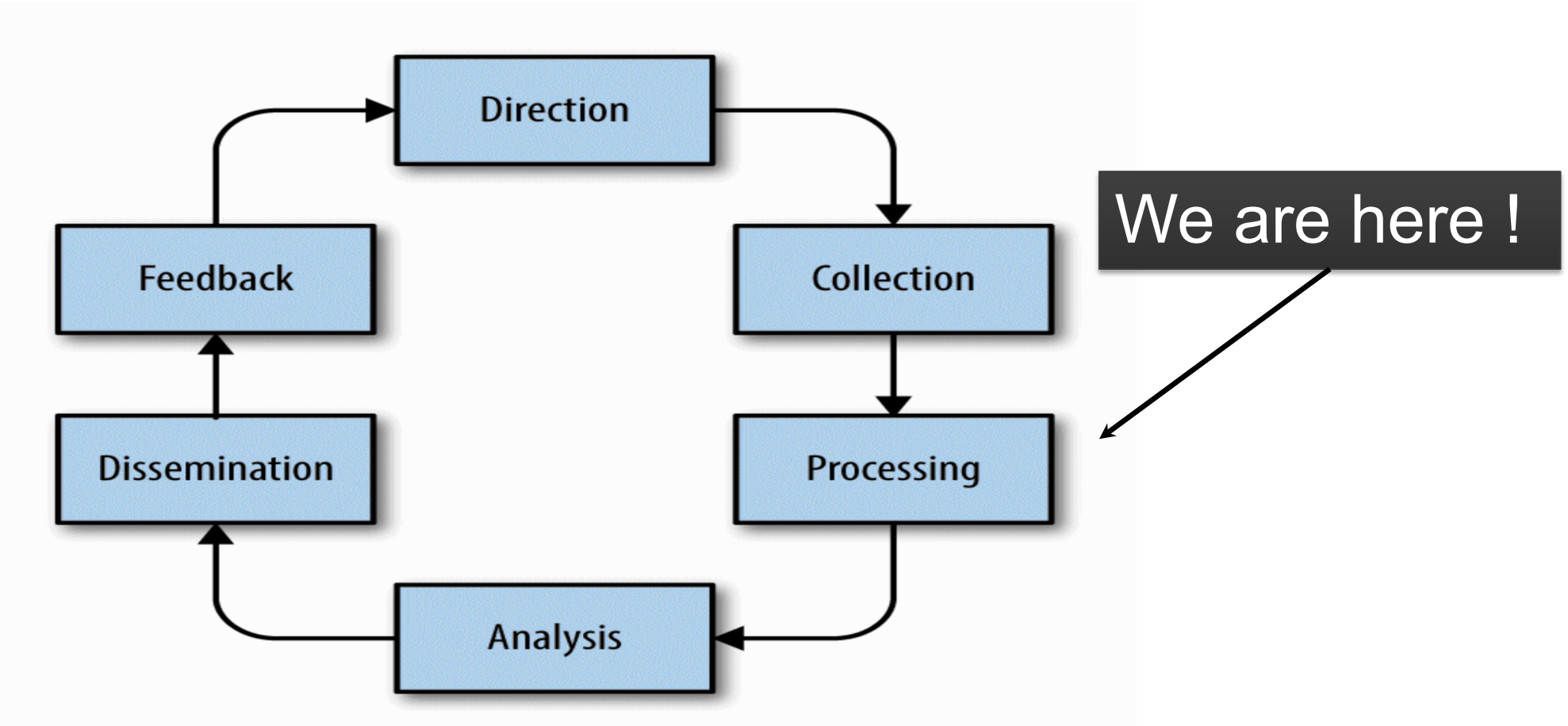
Intelligence Collection Sources

- Internal Security Incident Data
  - (Listen to your enemy, for God is talking. ~ Jewish Proverb)
- Internal Log Data Lake
- Internal Stakeholders
  - Corporate Security/Business
- Vendor Reports
- Sharing Communities, ISACs
- Governmental Sources
- OSINT
- Paid IOC Feeds

https://medium.com/@sroberts/intelligence-collection-priorities-a80fa3ed73cd

Reference:
Scott J Roberts

Intelligence Processing

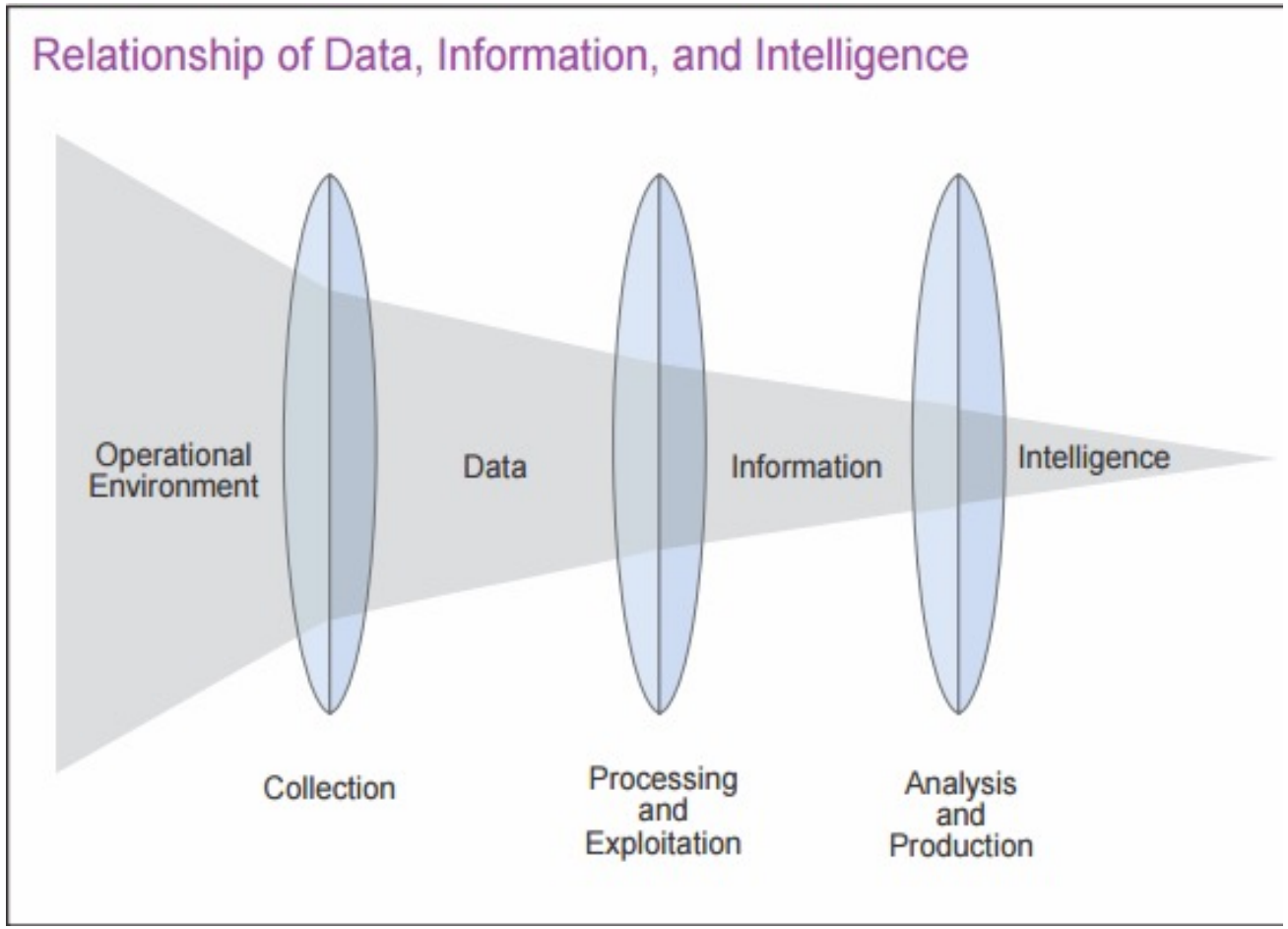


Data versus Intelligence

- Data is a piece of information, a fact, or a statistic.
  Data is something that describes something that is.

- Intelligence is derived from a process of collecting, processing, and analyzing data.

- The difference between data and true intelligence is ***analysis***.

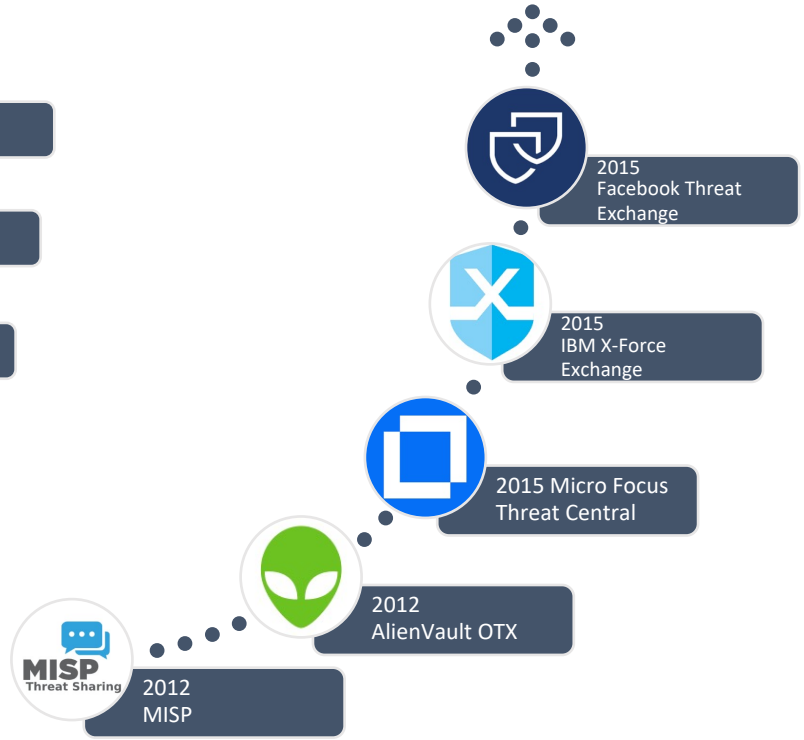


Reference: DoD

Threat Intelligence Platforms

Open Source

Commercial

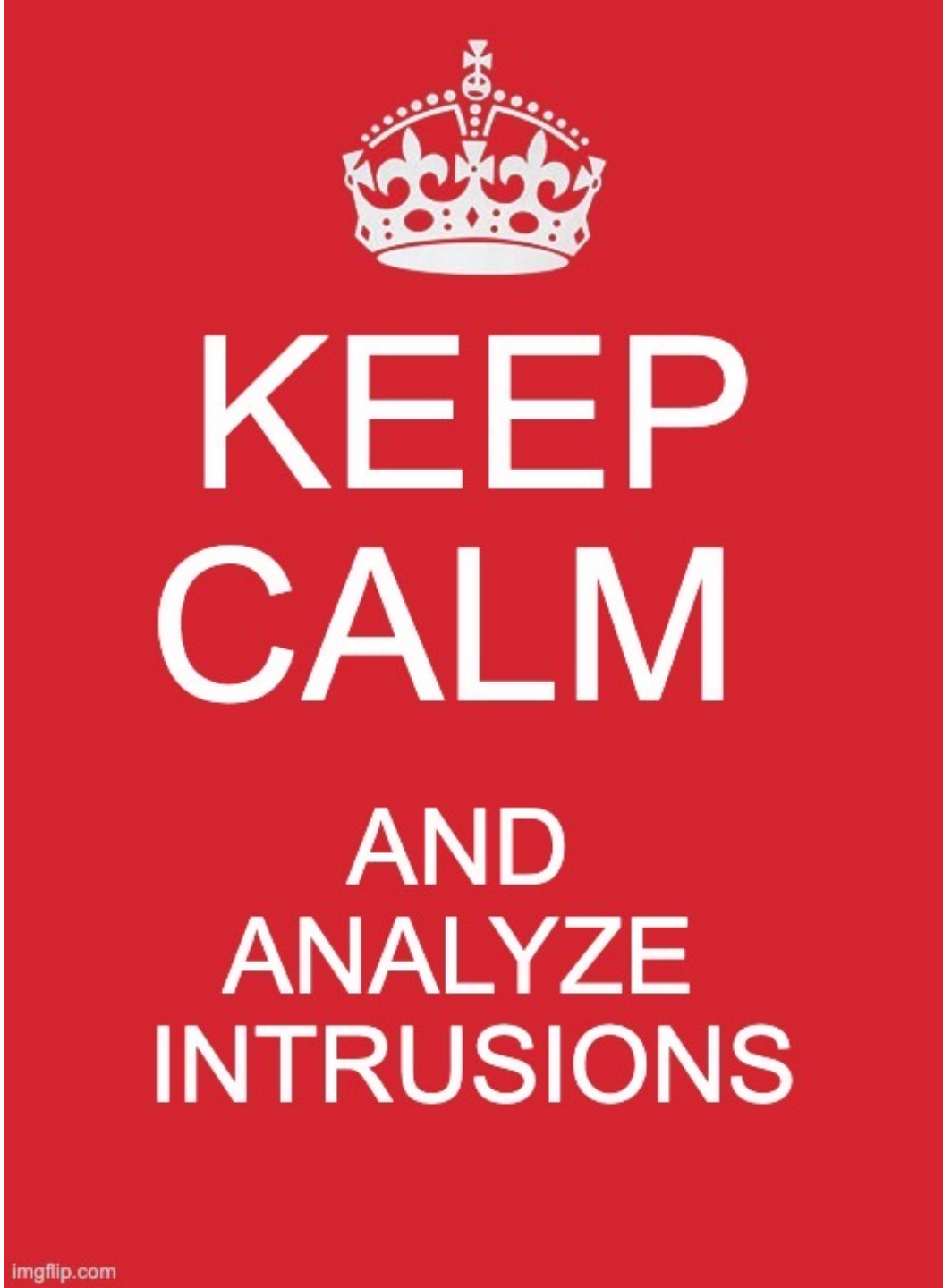


Community Exchange Platforms

The Analyst’s Dream: Data Into Buckets

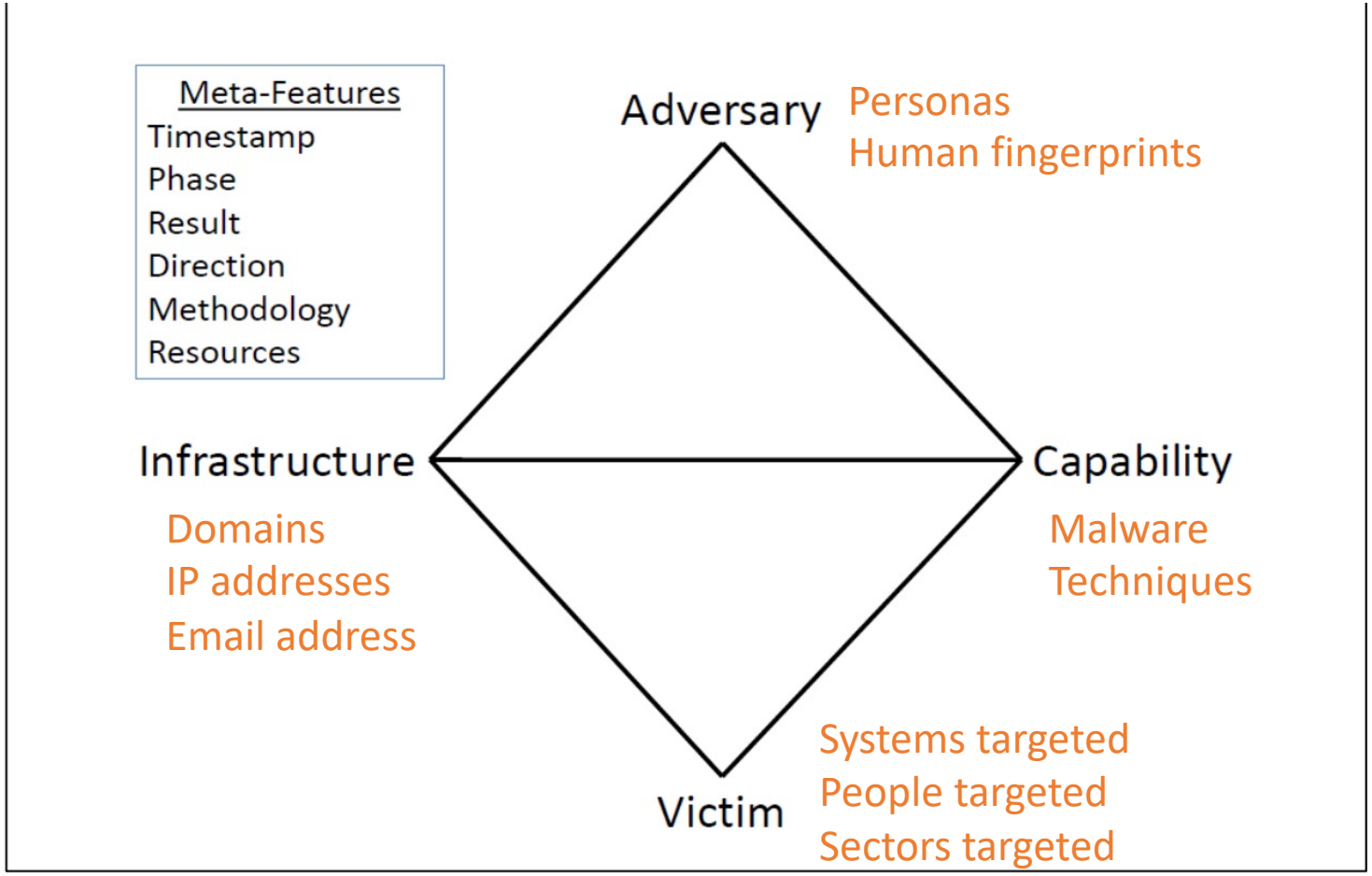
Intrusion Analysis Frameworks 101

- Kill Chain
- Diamond Model
- ATT&CK Framework



Reference:
Original: Hutchins, Cloppert, Amin
Graphic: SANS CTI Poster

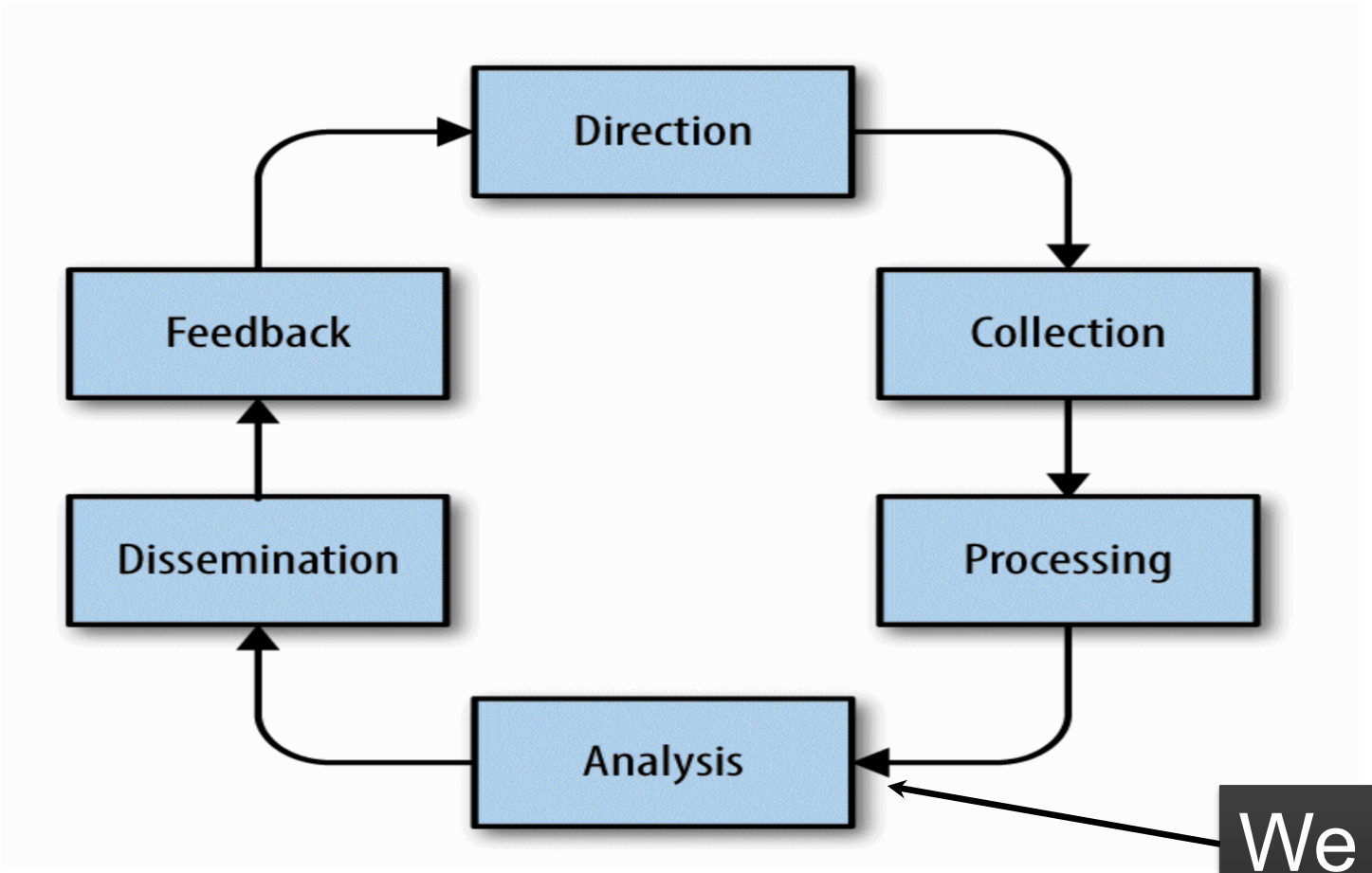
Diamond Model of Intrusion Analysis



Reference: Caltagirone, Pendergast, Betz

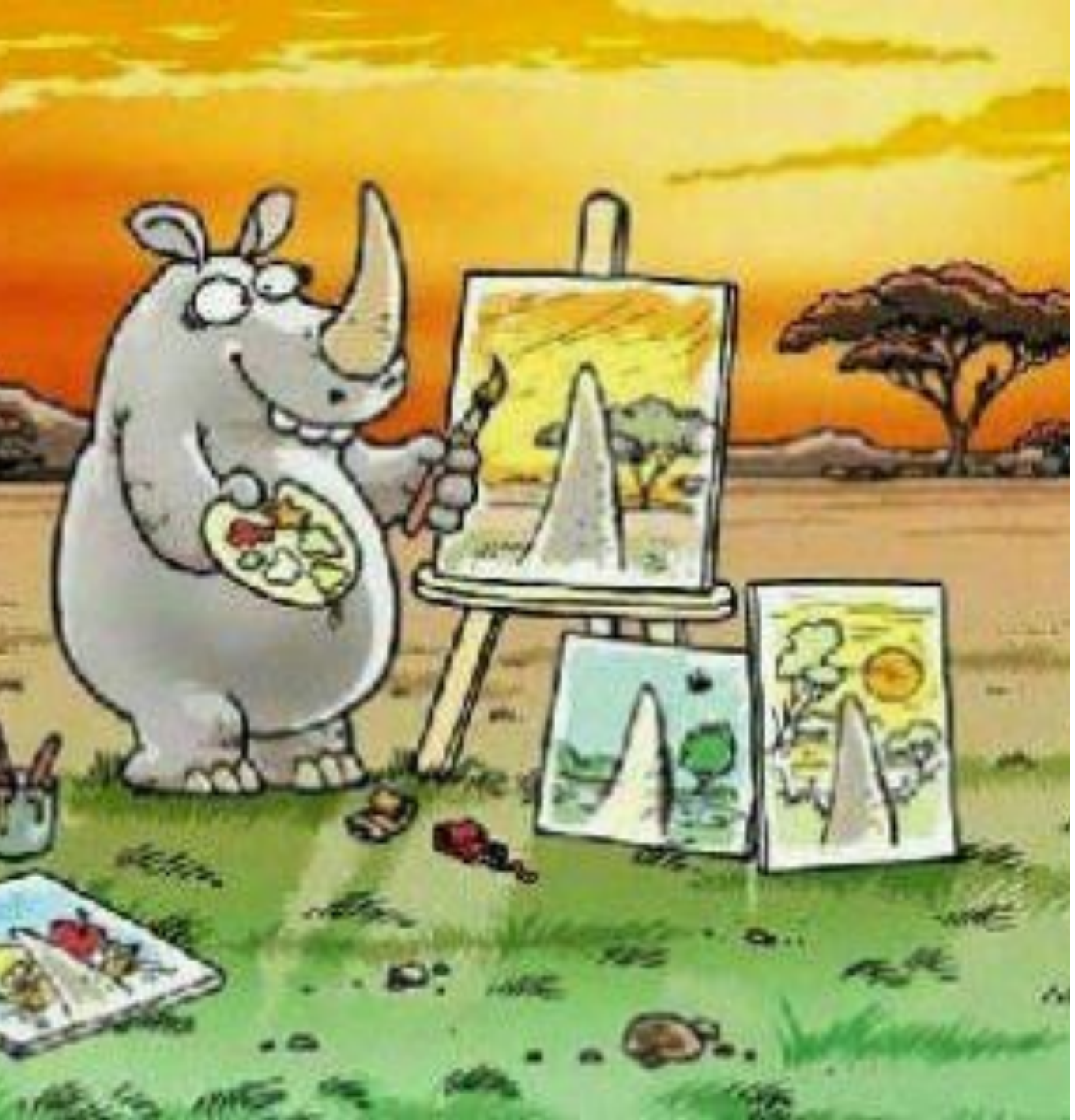
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Email Collection (3)	Non-Standard Port
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (1)	Remote Access Software
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry		Screen Capture	Traffic Signaling (1)
				Modify Authentication Process (3)		Remote System Discovery		Video Capture	Web Service (3)
				Modify Cloud Compute		Software Discovery (1)			
						System Information Discovery			

Intelligence Analysis



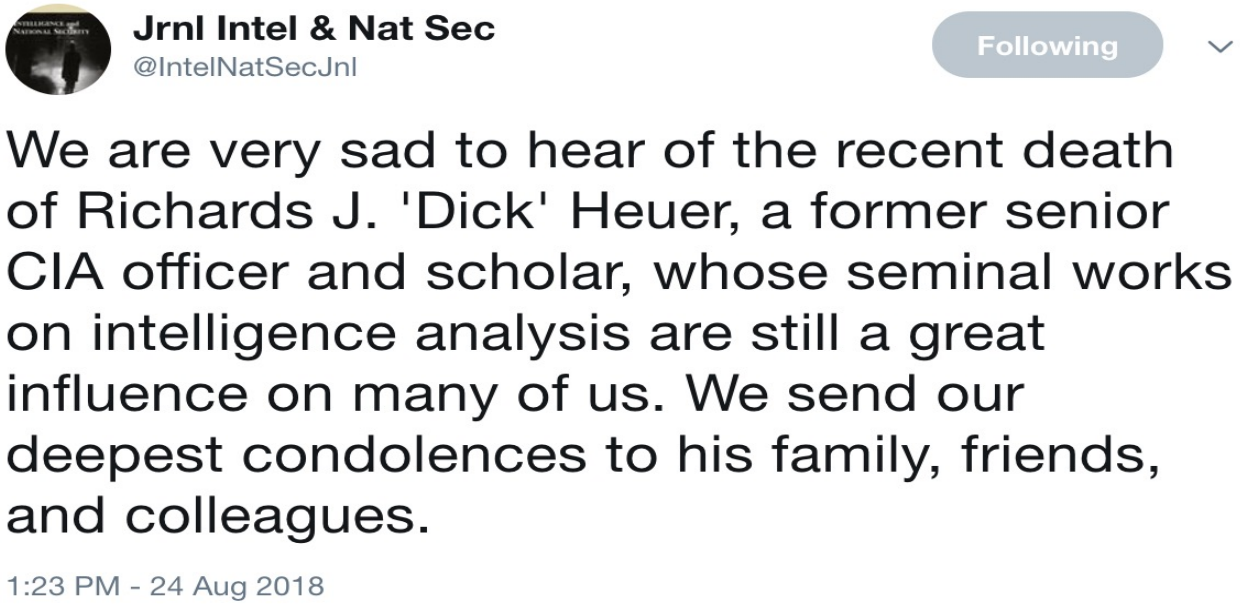

PARIS
IN THE
THE SPRING
ONCE
IN A
A LIFETIME
BIRD
IN THE
THE HAND

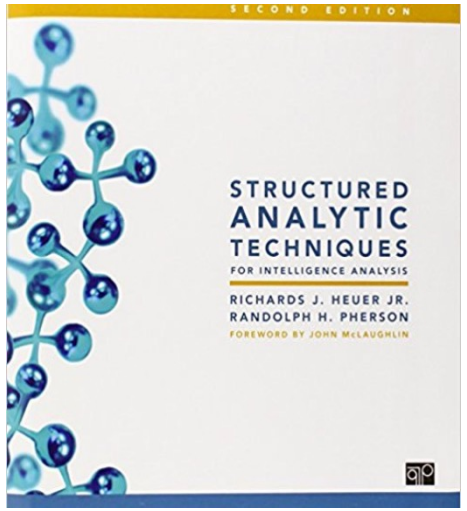
Figure 1

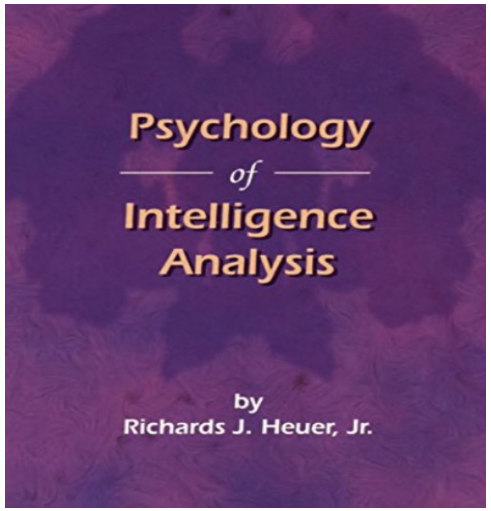


Cognitive Biases

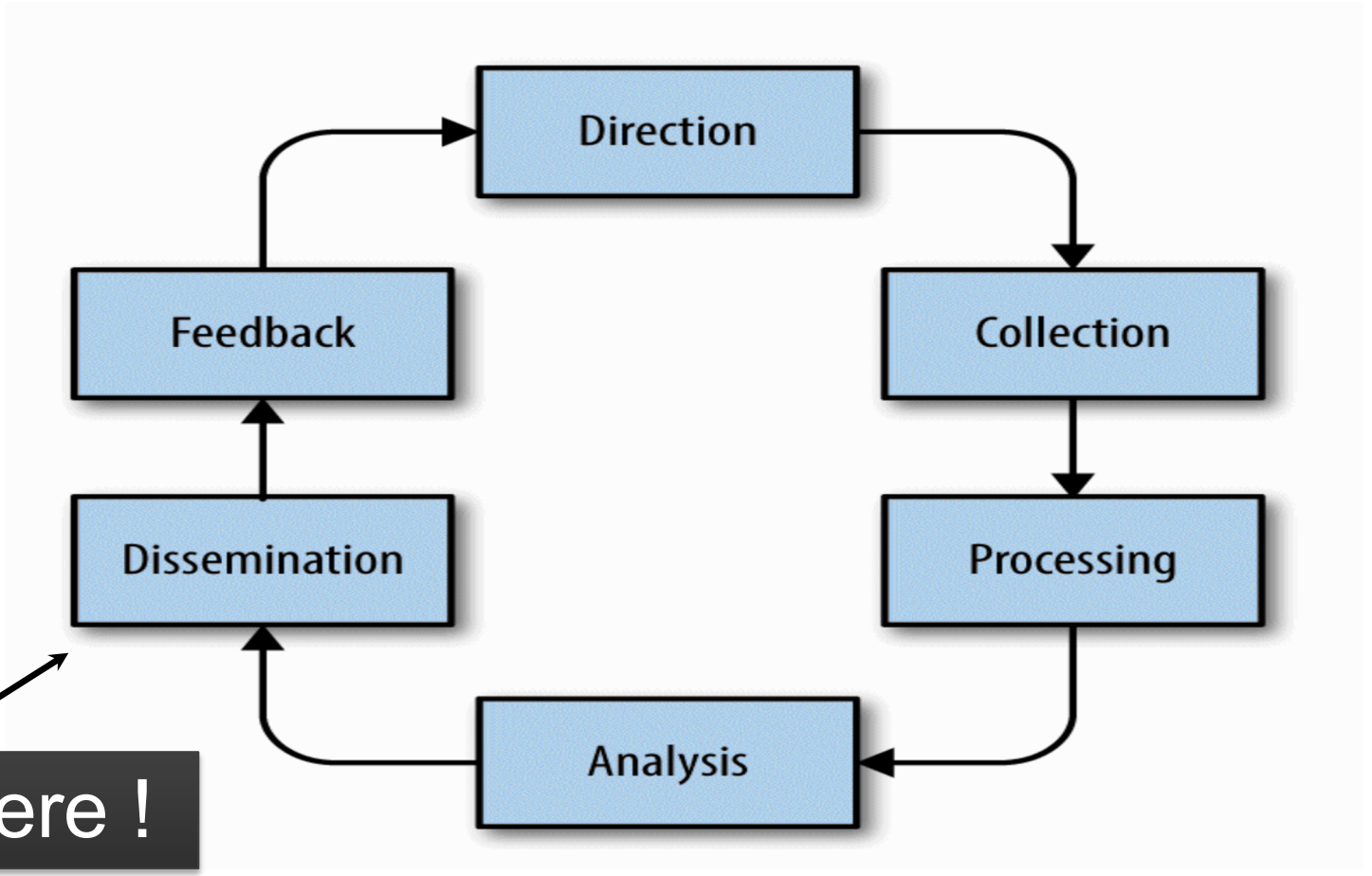
Overcoming Biases







Intelligence Dissemination



We are here !


Collection
Analysis
?
ACTION


THANKS FOR THIS
THREAT INTEL REPORT
YOU'RE GONNA
TAKE ACTION, RIGHT?
YOU'RE GONNA
TAKE ACTION, RIGHT?
imgflip.com

THREAT INTELLIGENCE

LEVELS

	Audience	Deliverable
Strategic *Who and why?*	BOD; Executive Leadership; Security Leadership	Business context; strategic impact; risk management -M & A -Brand reputation -Compliance
Operational *How and where?*	Security Leadership; Incident Response; Threat Hunters	Support to remediation, hunting, detection; budget decisions; collection management - Prioritize and budget security operations
Tactical *What?*	Security Operations; Network Defenders; Incident Response; Automation	Technical indicator ingest; threat behavior analytics (TBA) -Malware analysis -Automated tools & processes

Reference:
Amy Bejtlich


What about intelligence tradecraft in reporting?

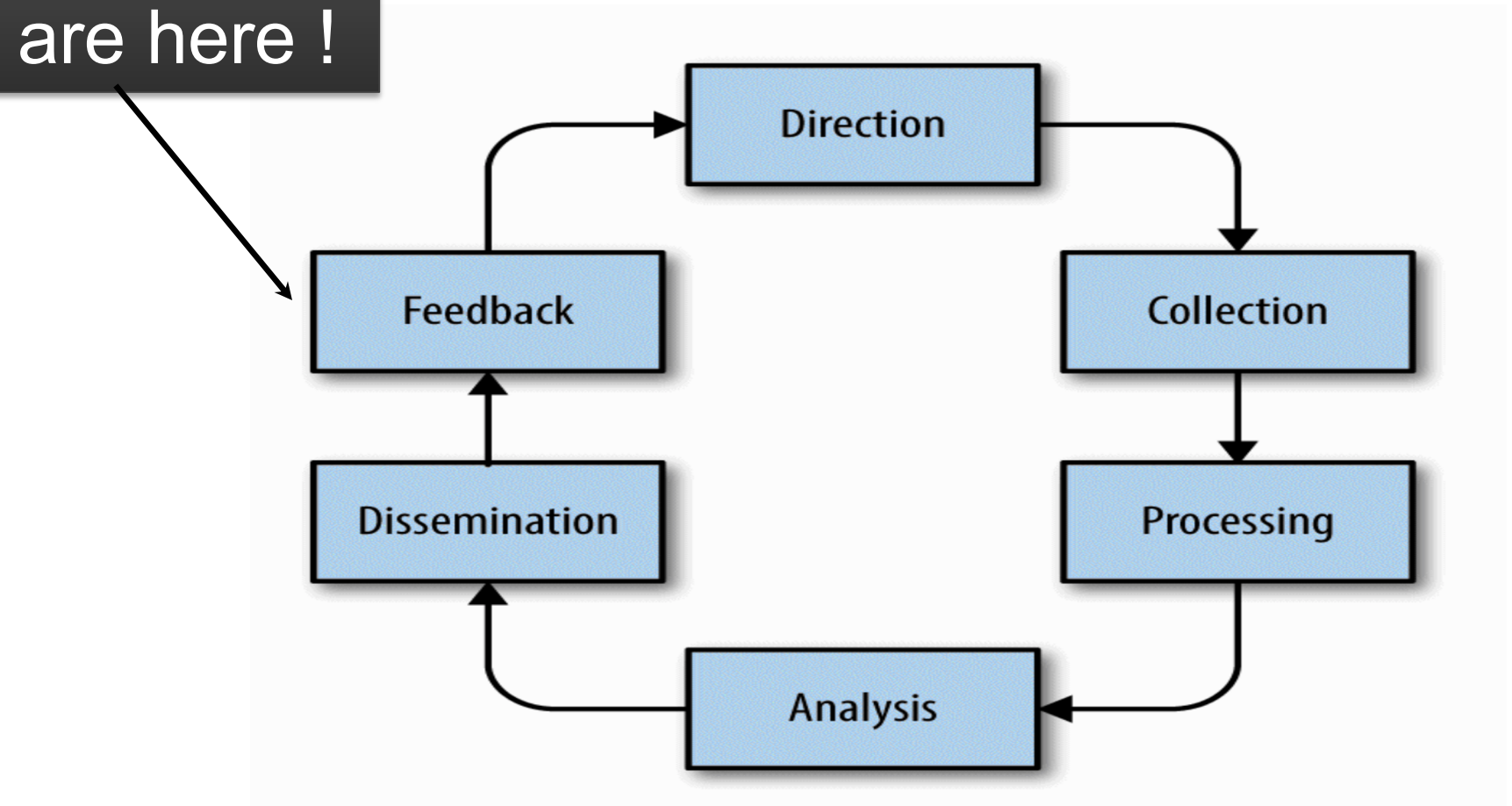
Sample Report Structure

Report Structure

- Title
- Executive Summary (BLUF)
- What?
- So what?
- What next?
- References
- Appendix
  - Indicators (machine readable?)
  - Tradecraft used

Intelligence Feedback

We are here !



Getting Feedback

- Orally
- Written feedback
- SharePoint metrics
- Dissemination and feedback via corporate comms app
- Microsoft Forms
- Threat Intel Portal

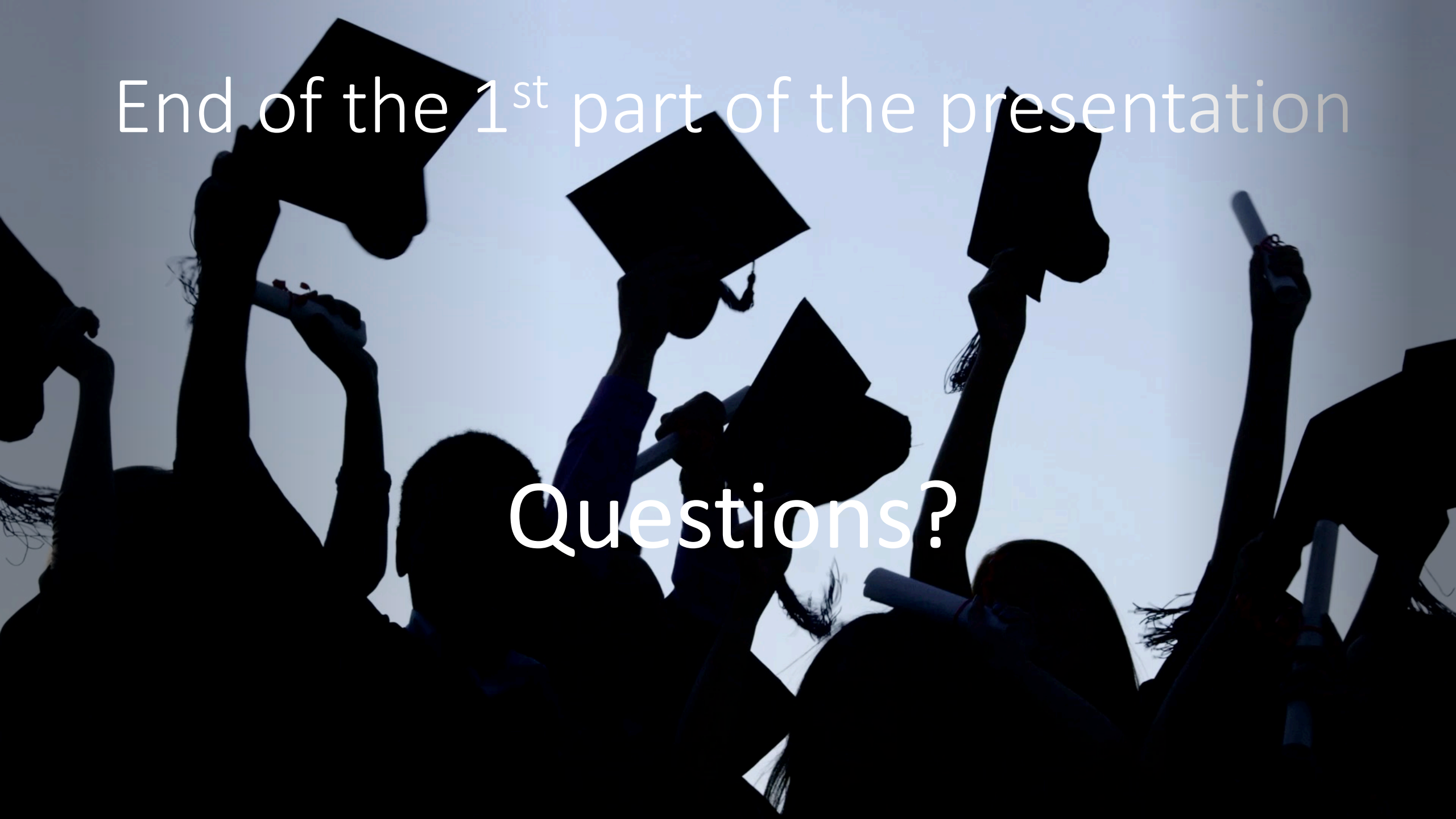
Wrapping up

From intelligence to CTI

Intelligence cycle

Basic CTI concepts and frameworks

End of the 1st part of the presentation



Questions?

A view at the Threat Landscape

CROWDSTRIKE


CAPABILITY
INTENT
THREAT
OPPORTUNITY

The human behind the keyboard


What is the top cyber threat nowadays for organisations?

@mikko
@mikko

Today, I was scheduled to have an interview with a journalist. The topic was the recent growth in ransomware attacks. The interview was just cancelled, because the publishing company itself was hit with a ransomware attack.

11:42 AM · Apr 26, 2021 · Twitter Web App

306 Retweets **37** Quote Tweets **1,629** Likes

MANDIANT

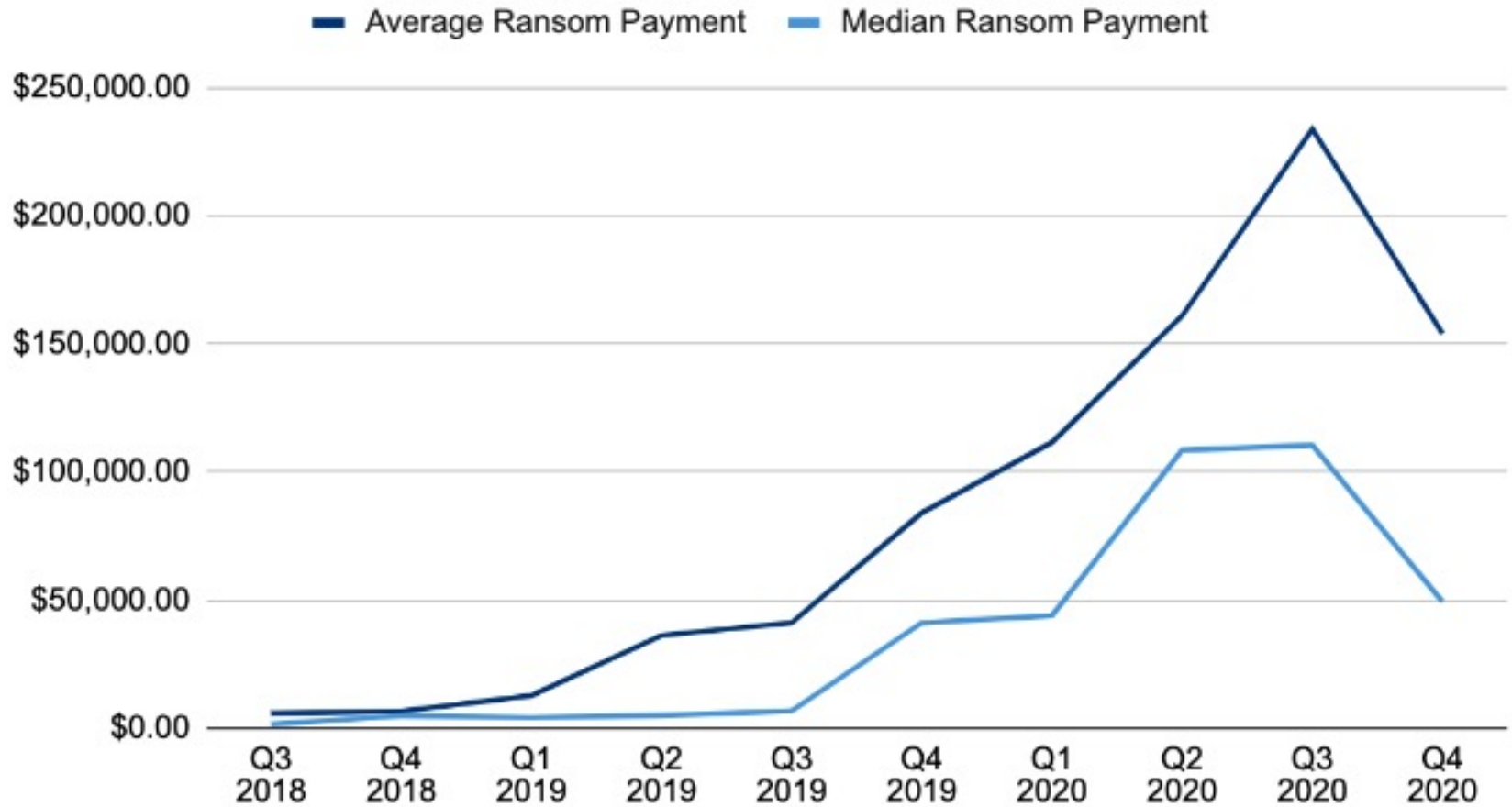
Evolution of Ransomware

Ransomware Trends

- Target is the whole organisation
- Data exfiltration before ransomware payload
- Public shaming sites
- Cold-calling victims
- Triple extortion
- Ransomware cartels
- Interconnected cybercrime ecosystem
- The role of insurance companies
- OFAC guidance on ransom payment

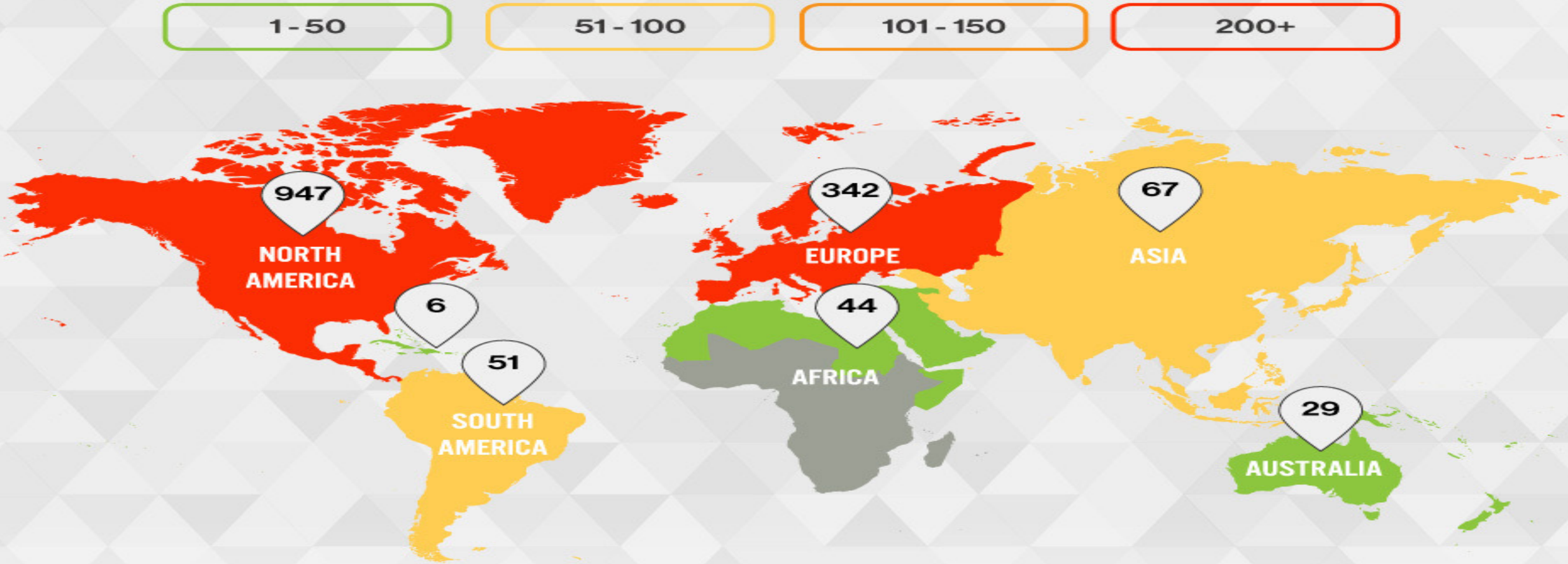

How much is the average ransom payment?

Ransom Payments By Quarter

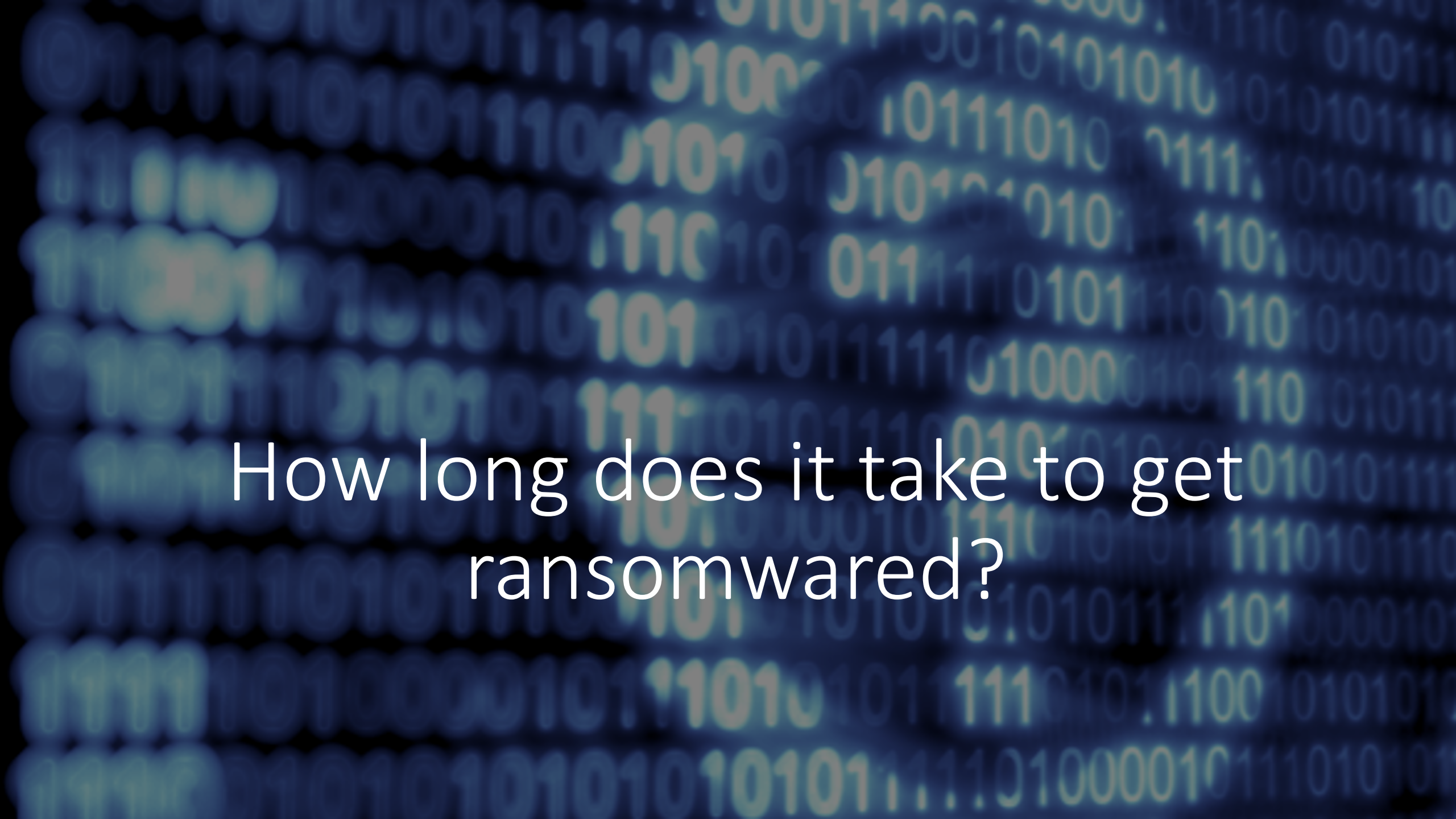


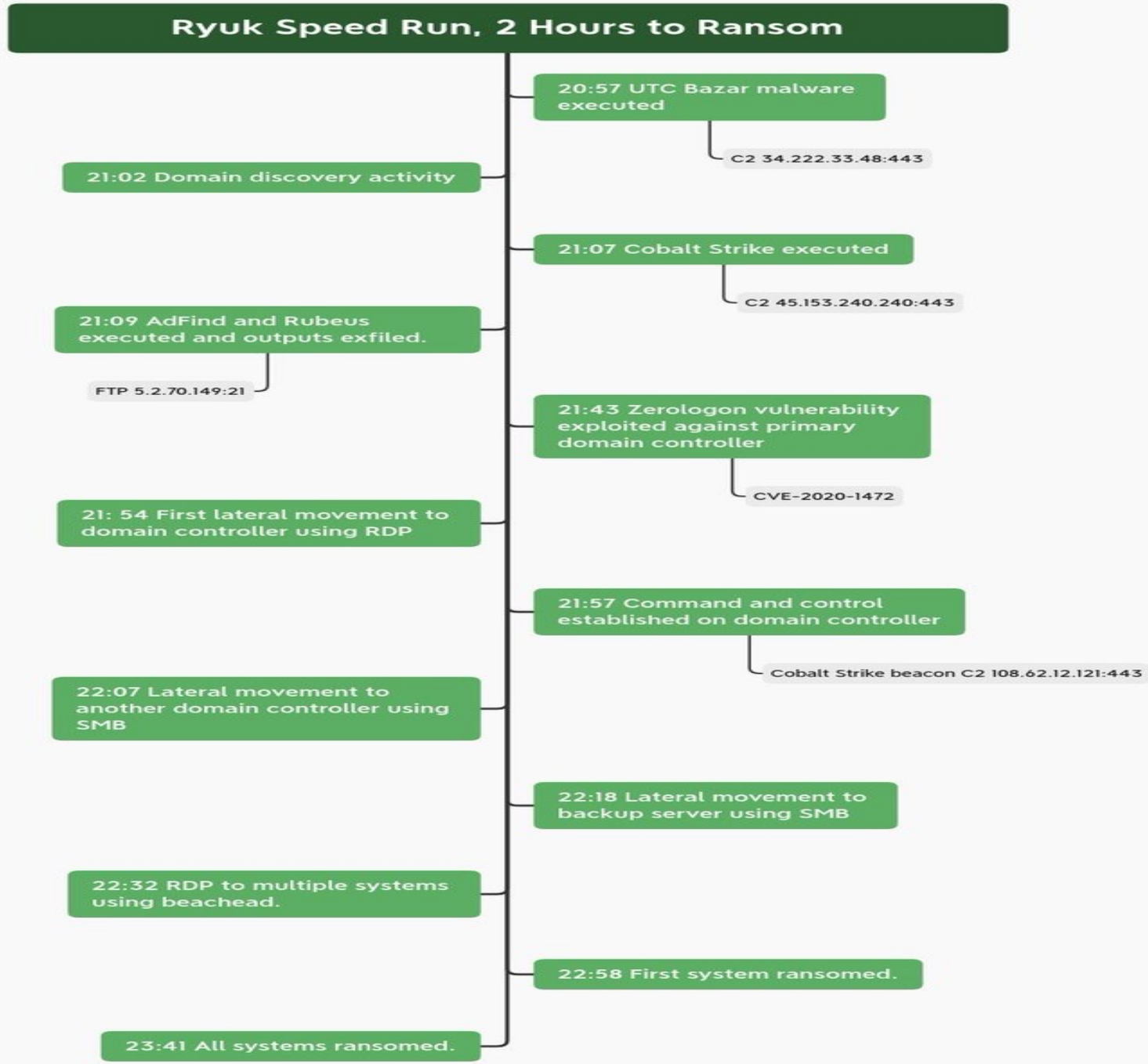
COVEWARE

Number of Ransomware Attacks That Used Data Extortion in 2020 By Continent



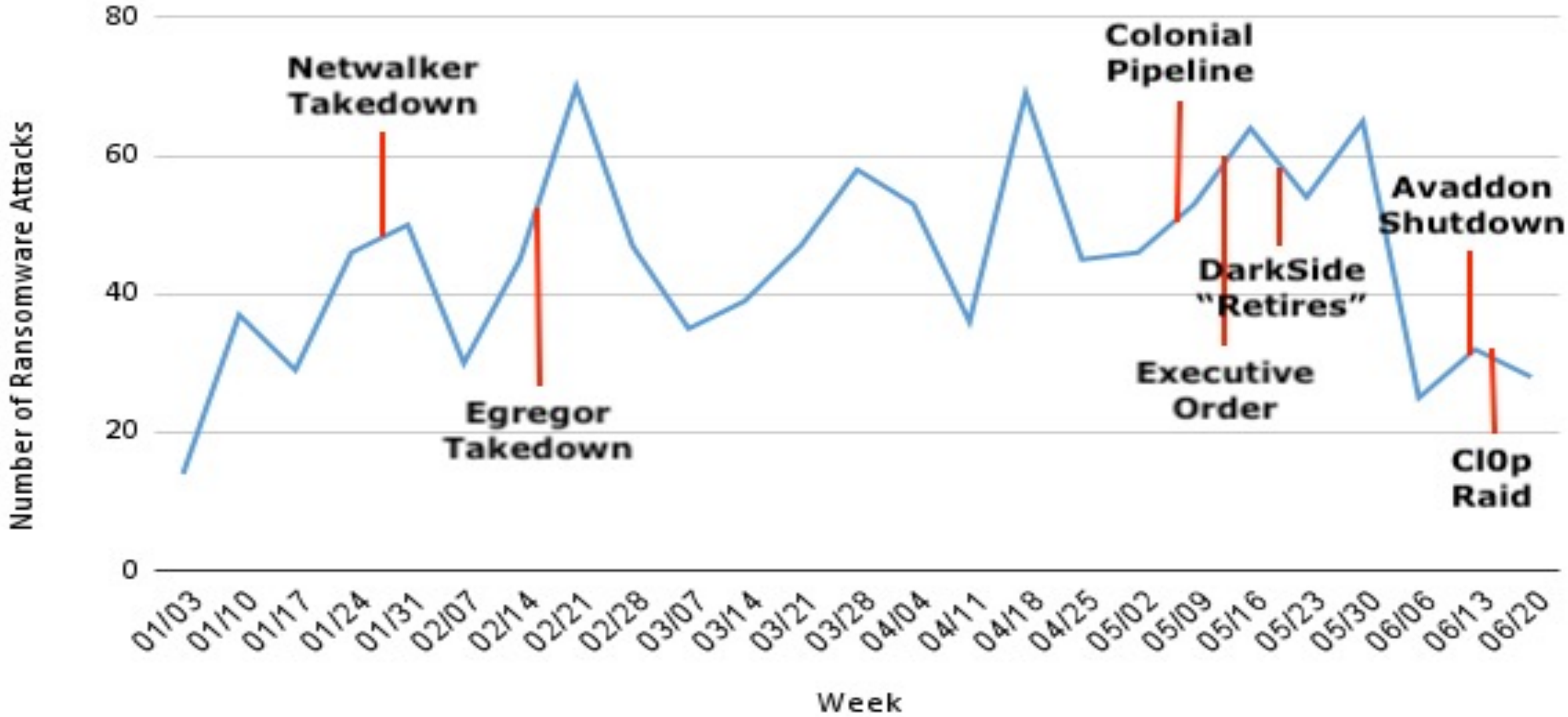
CROWDSTRIKE


How long does it take to get ransomwared?



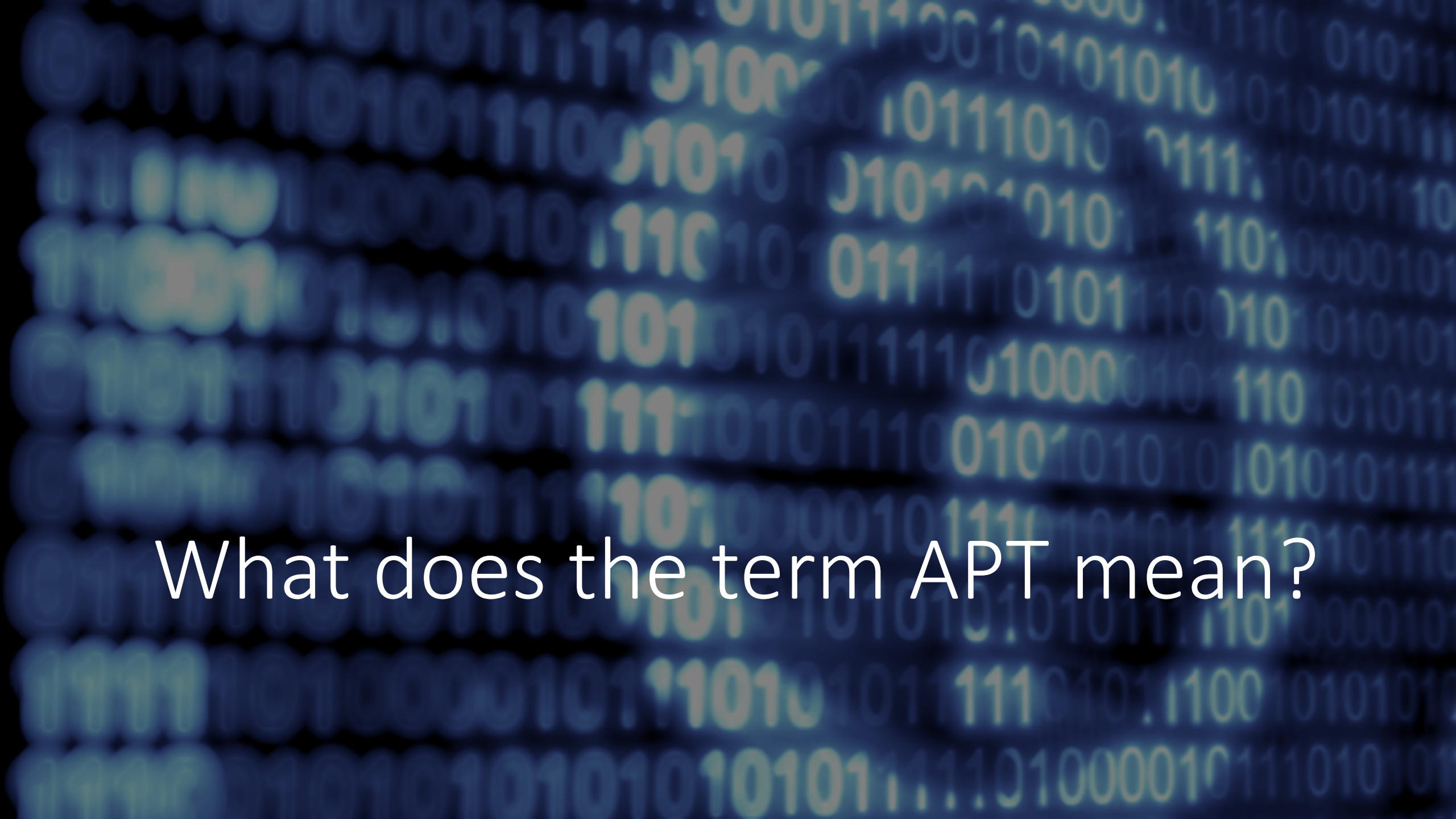
Reference:
DFIRReport

Ransomware Attacks per Week



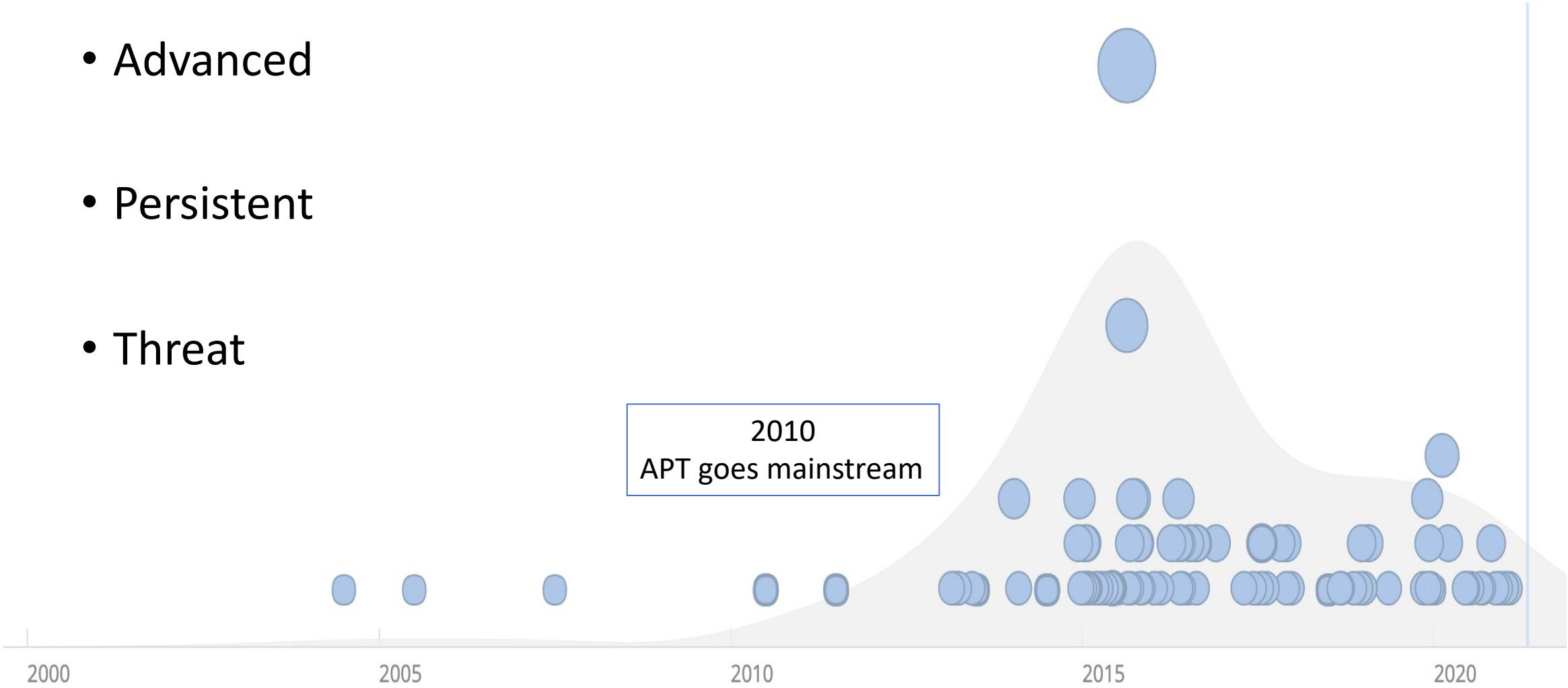

As a network defender, how can you detect and respond to ransomware?

State Sponsored Threat Groups


What does the term APT mean?

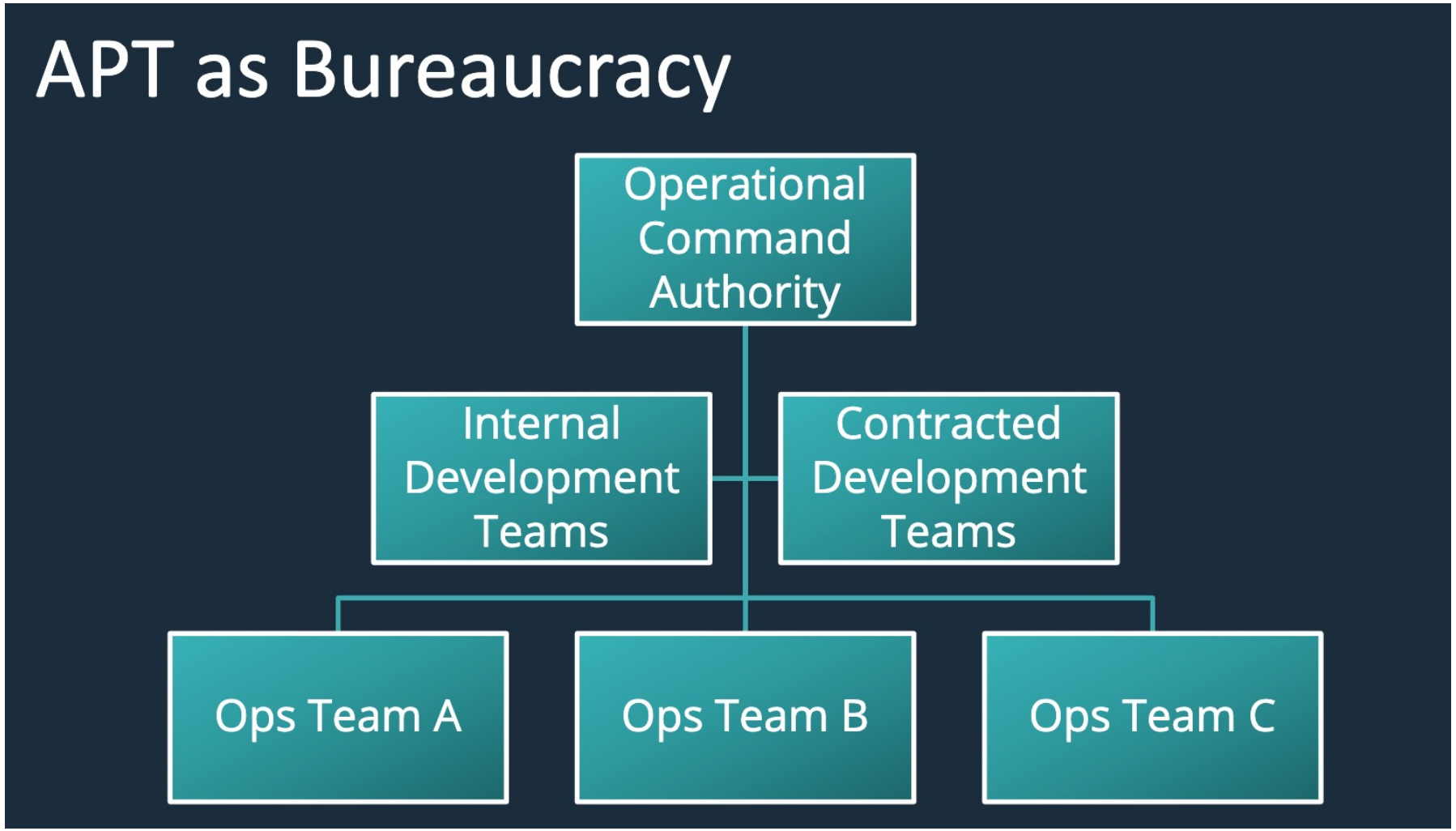
APT

- Advanced
- Persistent
- Threat



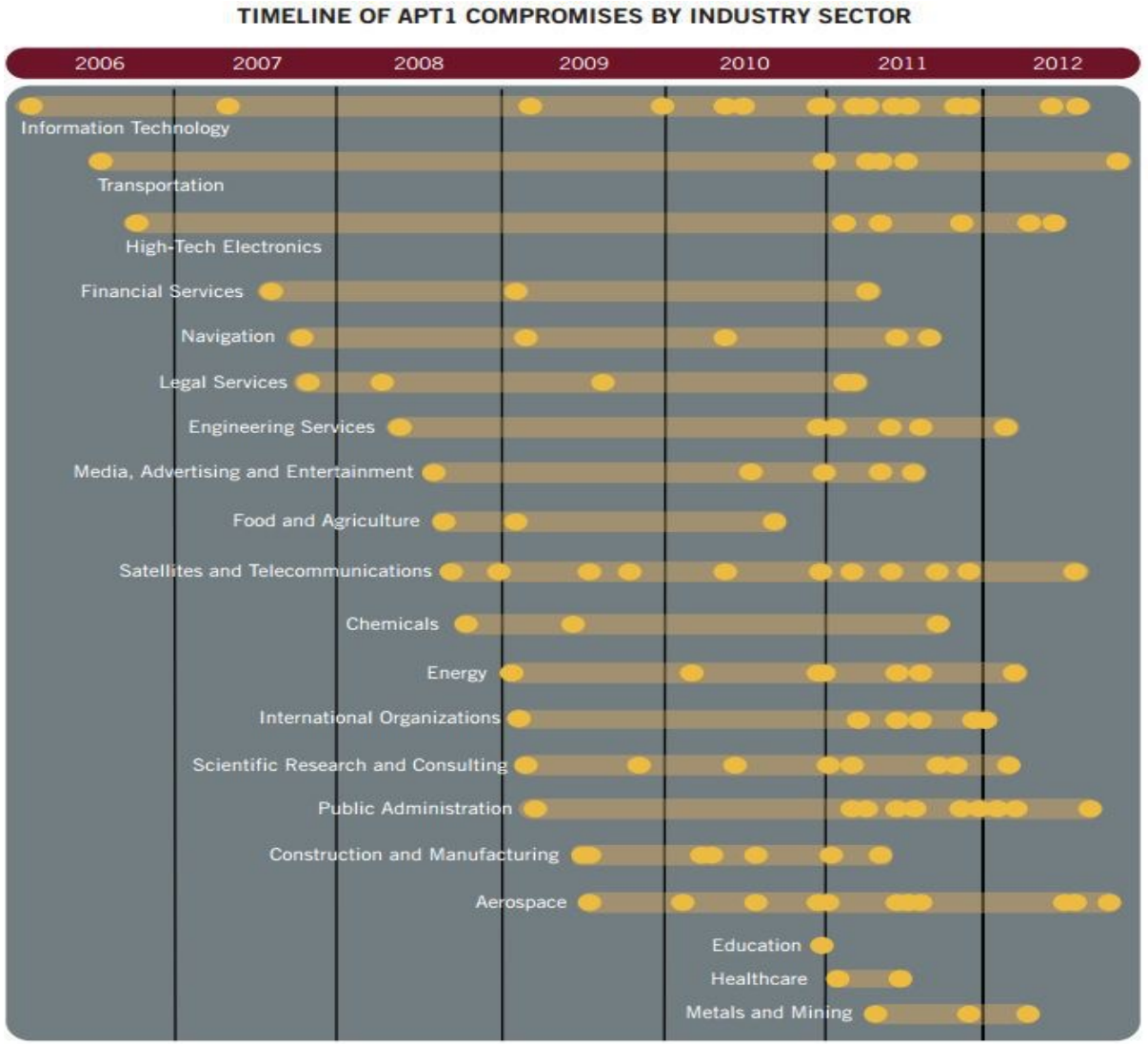
Reference: Recorded Future

Another way to look at APTs…

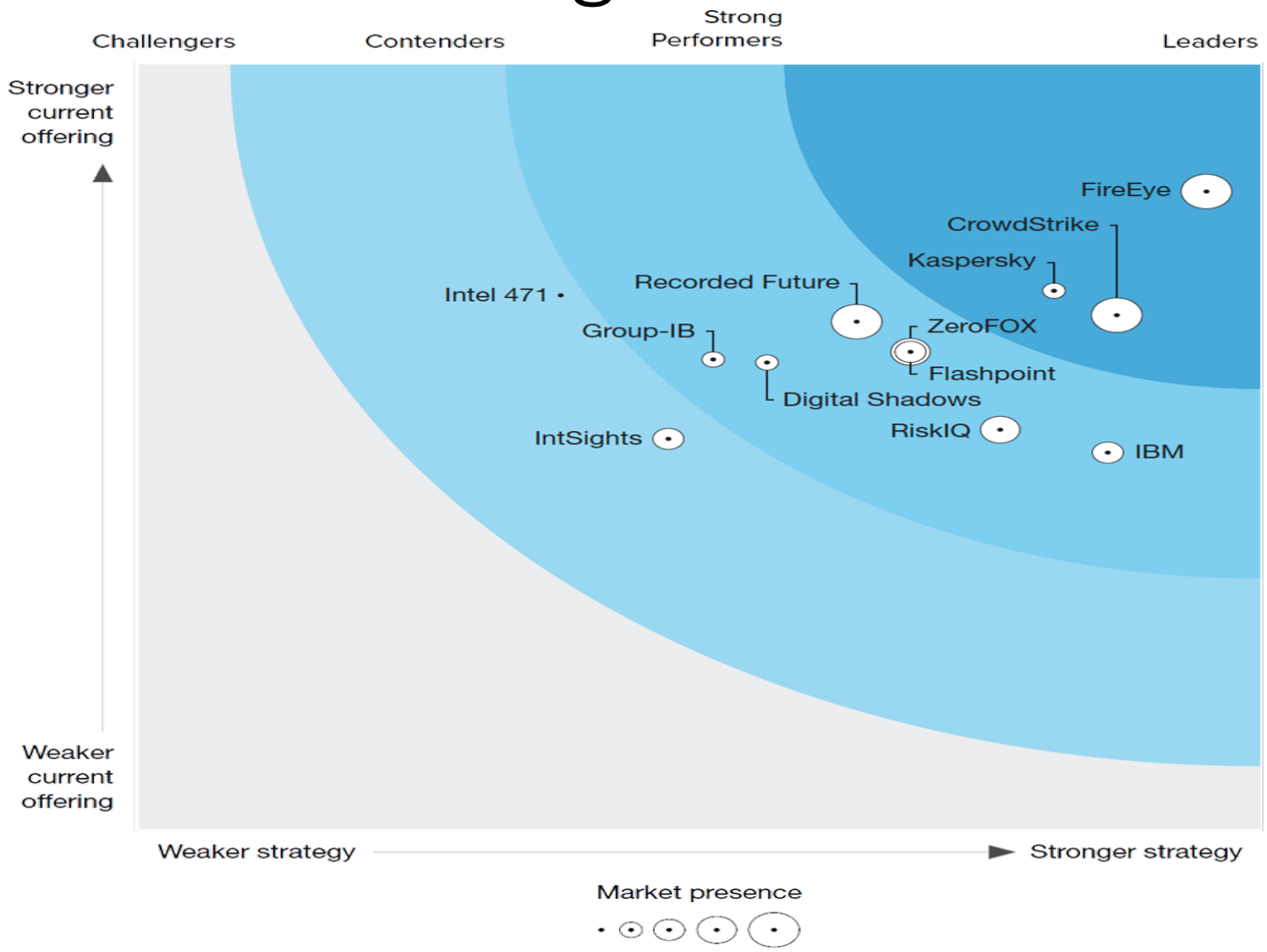


Source:
Joe Slowik

When everything started! (version 2)



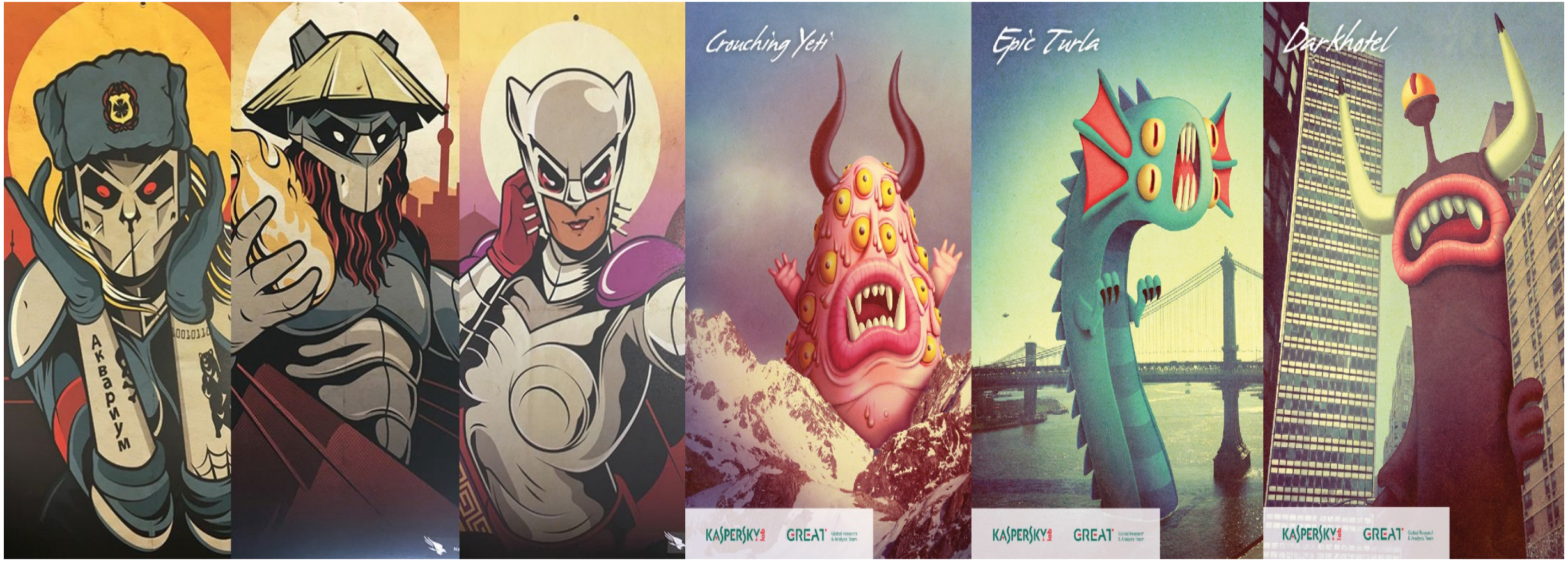
External Threat Intelligence Services Q1 2021



Source: Forrester


I SEE THREAT INTELLIGENCE REPORTS
SPACE RANGER
LIGHTYEAR
THREAT INTELLIGENCE REPORTS EVERYWHERE

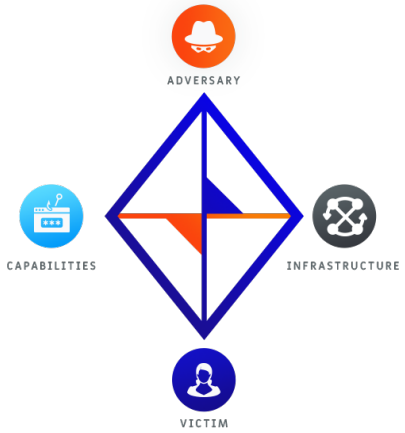
Bears, Pandas, Kittens and the rest



FireEye APT Groups

- FireEye's list of sophisticated actors and naming conventions looks like this:
  - APT0-27, 30/31, 40/41 = China
  - APT28/29 = Russia
  - APT32 = Vietnam
  - APT33/34/35/39 = Iran
  - APT36 = Pakistan
  - APT37/38 = North Korea

~2.5k UNC threat groups



FireEye

CrowdStrike APT Groups

CROWDSTRIKE

Adversary	Category or Nation-State
 SPIDER	ECRIME
 CHOLLIMA	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (NORTH KOREA)
 JACKAL	HACKTIVIST
 TIGER	INDIA
 KITTEN	IRAN
 LEOPARD	PAKISTAN
 PANDA	PEOPLE'S REPUBLIC OF CHINA
 BEAR	RUSSIAN FEDERATION
 CRANE	SOUTH KOREA
 BUFFALO	VIETNAM

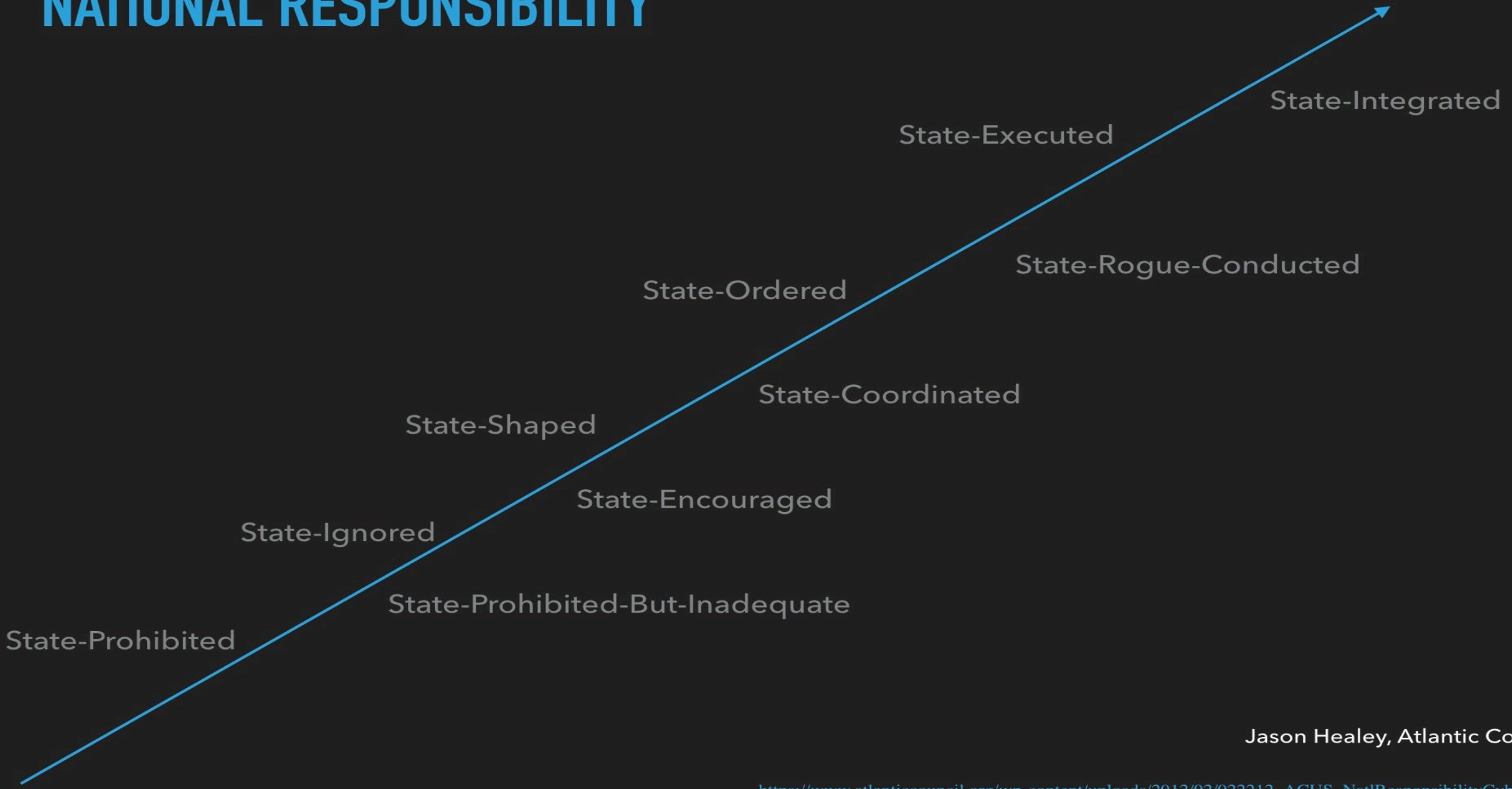
FireEye and CrowdStrike track APT groups from: China, Russia, Iran, N. Korea, Vietnam, Pakistan, India and S. Korea.

Why only groups from these states?

Reference:
Joe Slowik


How do governments do attribution?
What sources do they use?

NATIONAL RESPONSIBILITY



Jason Healey, Atlantic Council

https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF

On attribution

- Type of attribution
  - Person? Organisation? Country? Threat group?
- Technology enablement
- False flags
- Usage of open-source offensive tools

APT Research

'Slingshot' Campaign Outed by Kaspersky is U.S. Operation Targeting Terrorists: Report

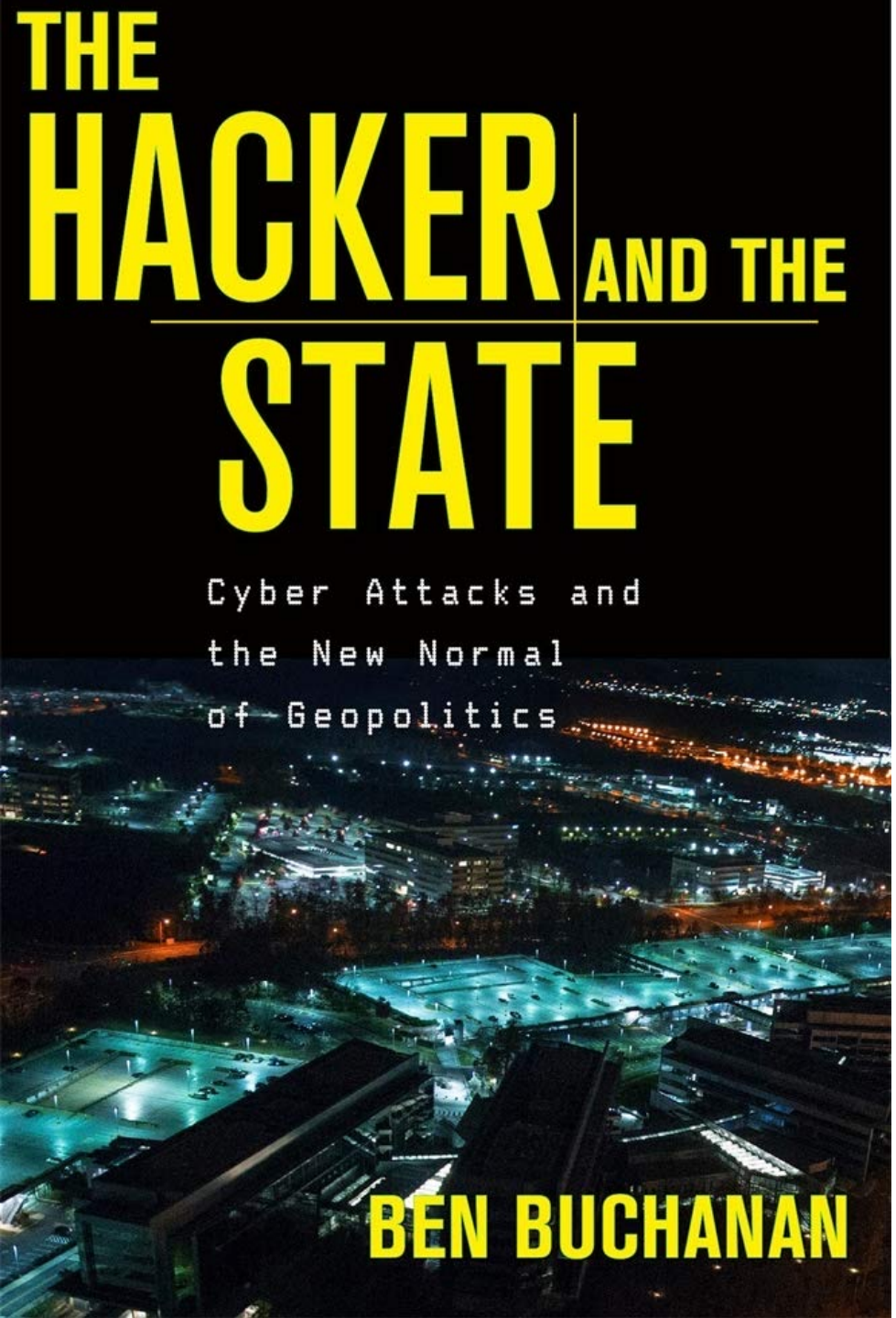
By Eduard Kovacs on March 21, 2018

Computing / Cybersecurity

Google's top security teams unilaterally shut down a counterterrorism operation

The decision to block an "expert" level cyberattack has caused controversy inside Google after it emerged that the hackers in question were working for a US ally.

by **Patrick Howell O'Neill** March 26, 2021



Geopolitics and Cyber

- Adversary intent
- Geopolitical signaling
- Geopolitical shaping

Wrapping up

Ransomware threat

State sponsored threats

Threat group tracking & attribution

CTI Analyst Skillset

Computer Security

What my parents think I do

What my friends think I do

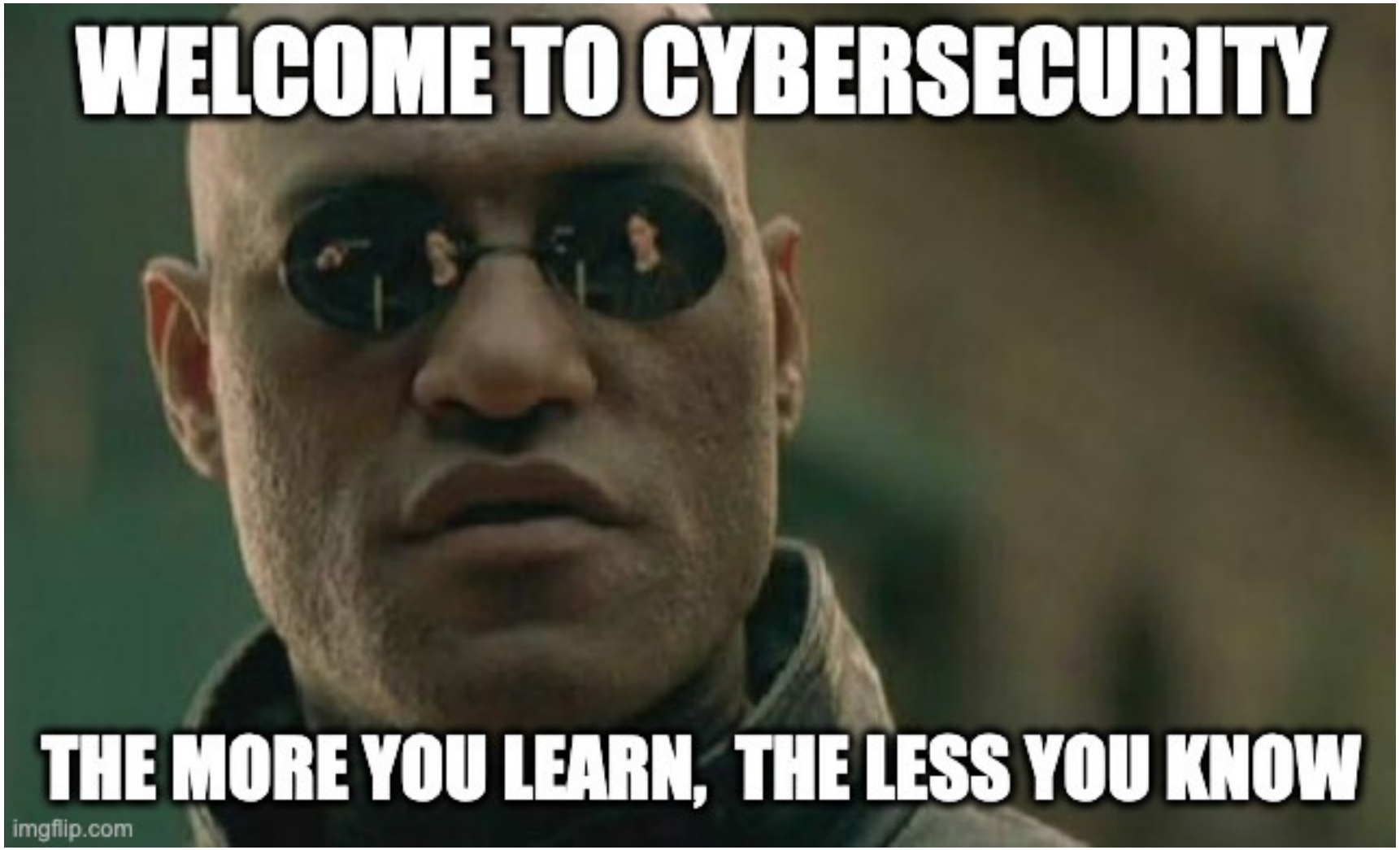
What my boss thinks I do

What my girlfriend thinks I do

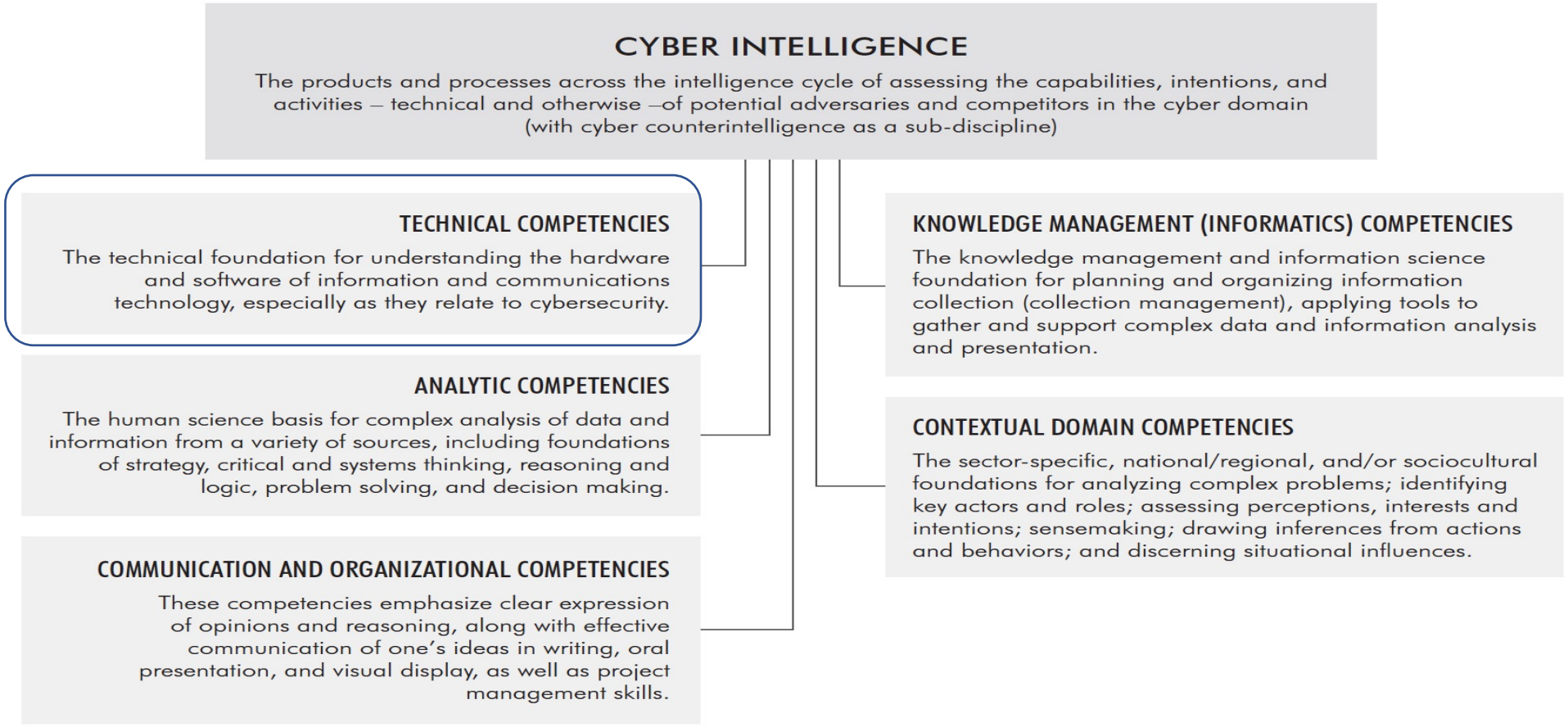
What the media thinks I do

What I actually do


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Cryptography
Security Engineering
Identity Management
Privileged Access Management
Identity & Access Management
Framework and Standard
COBIT
ISO/IEC
NIST
SANS/CSC
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Physical Security
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Source Code Scan
Blackbox
Whitebox
Data-Centric Risk Assessment
Data-Flow Map
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Data Leakage
Active Defense
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics


WELCOME TO CYBERSECURITY
THE MORE YOU LEARN, THE LESS YOU KNOW
imgflip.com

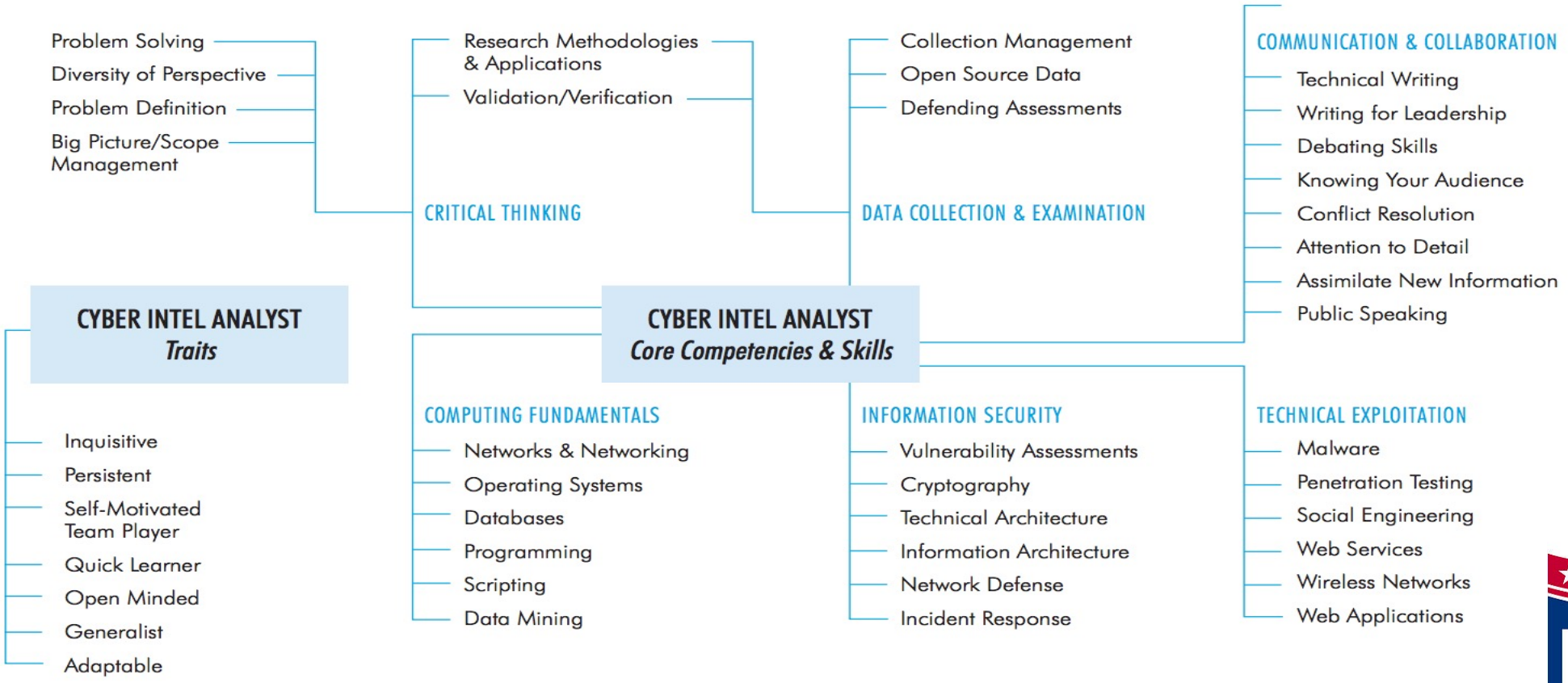
CTI Analyst Skillset



Reference:

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

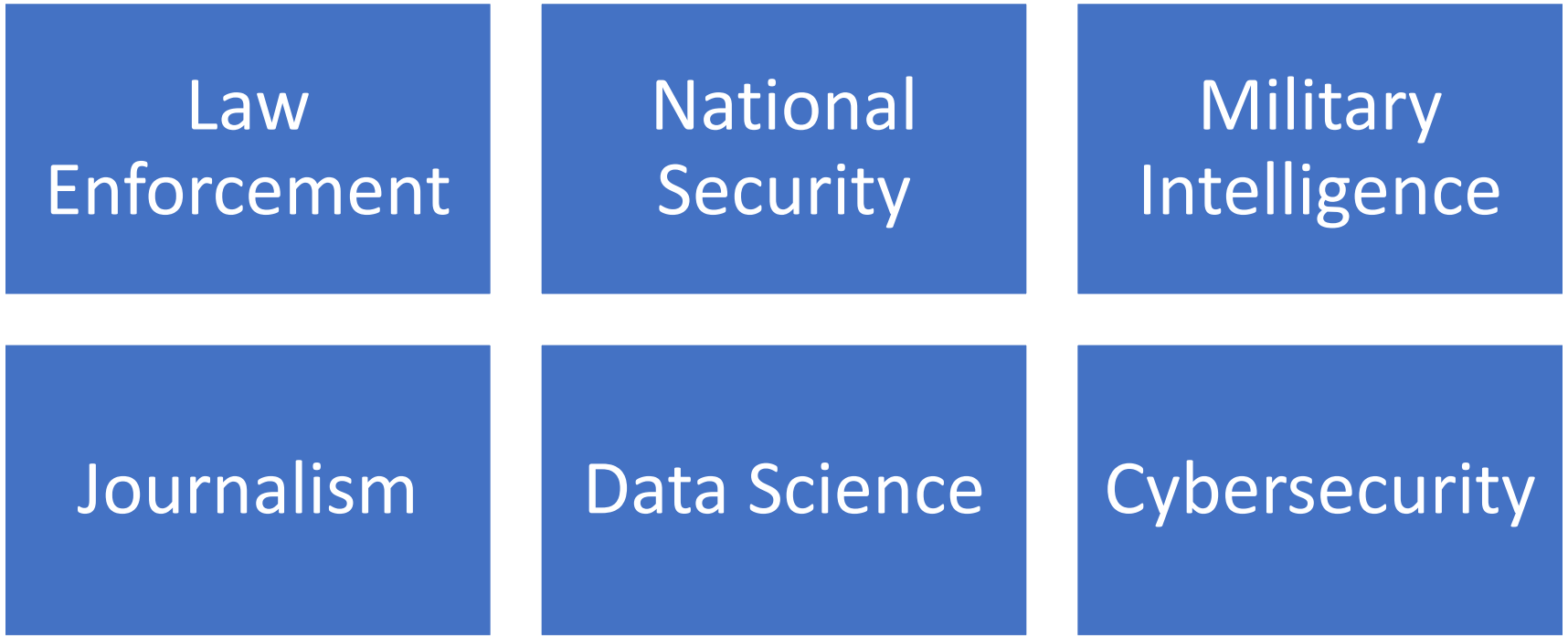
Cyber Threat Intel Analyst Tradecraft



Reference:

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Threat Intelligence Paths



Reference:
Amy Bejtlich

Maintaining External Situational Awareness

- RSS Aggregator (e.g., Feedly)
- Twitter
- ~~Nuzzel application~~
- Reddit
- Podcasts (e.g., CyberWire)
- Newsletter Team (e.g., TC Dragon News Bytes)
- Strategic sources (e.g., Economist, CFR, etc.)
- Weekly Summaries (e.g.This Week in 4n6)
- Threat Intelligence Reports
- ISACs
- Trust Groups (e.g., Slack channels, mailing lists)
- Threat Intelligence vendors

Maintaining Internal Situational Awareness

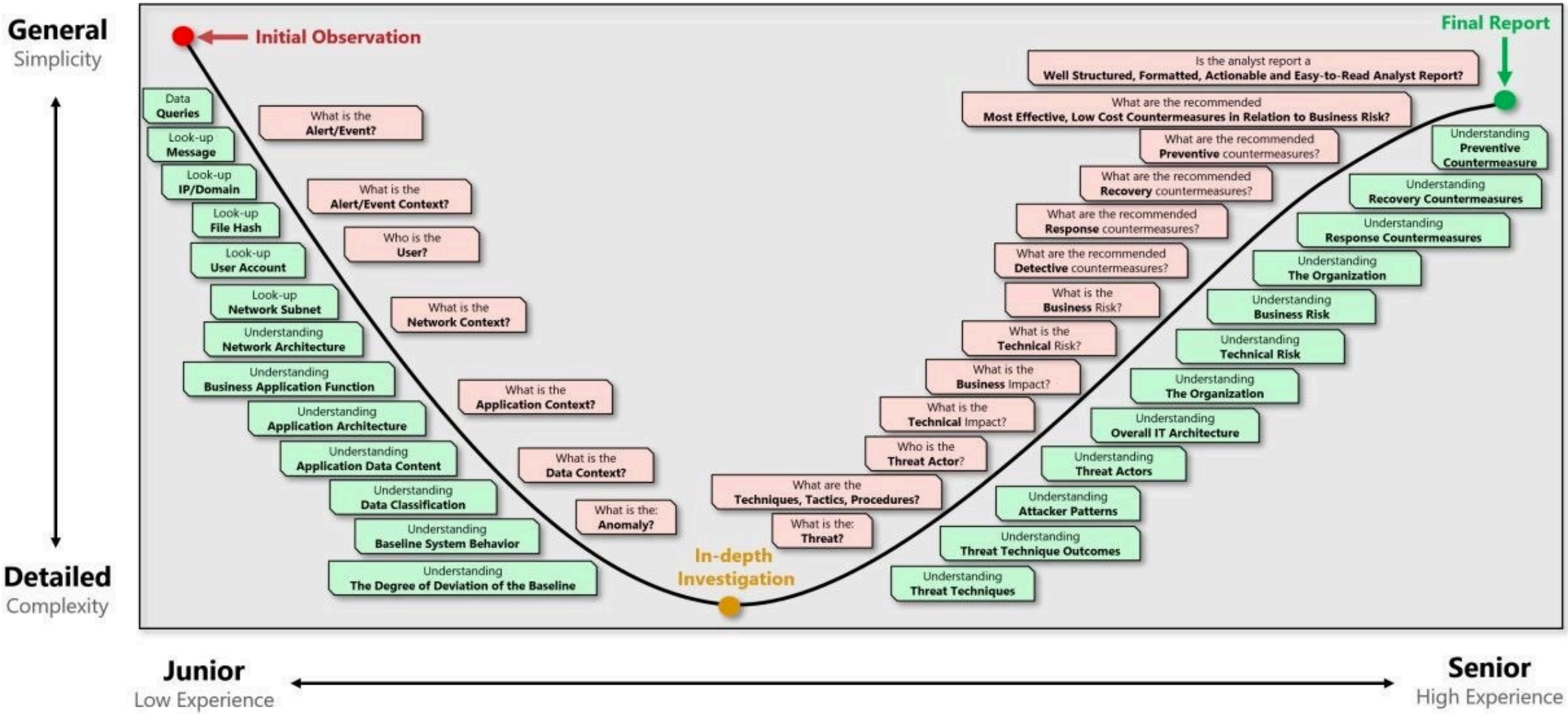
- Incident ticketing system
- Phishing campaigns
- Signature hits and alerts
- Failed intrusions
- Hunting/red team findings
- Business strategy
- Internal events

Continuous Education

- Self-initiated
- CTFs
- Academic programs
- Certifications
- Online training material
- Conferences
- Books
- Audiobooks

Cyber Security Analyst Maturity Curve

*"A senior cyber security analyst should be able to reach the **simplicity at the far side of complexity** and to be able to communicate the cyber security risks, threats and related countermeasures **simply, effectively and actionable.**"*



If you gonna read 2 articles…

- A Cyber Threat Intelligence Self-Study Plan: Part 1
- FAQs on Getting Started in Cyber Threat Intelligence

https://medium.com/@likethecoins

Wrapping up

- Lifelong learner
- Be part of the community
- Build communication skills
- Evolve

Final Thoughts

- Remember the process of the intelligence cycle
- Discussion on the evolving cyber threat landscape: major cybercrime and state sponsored threats
- Diverse skillset of the CTI analyst

Thank you!

Andreas Sfakianakis

@asfakian

tilting at windmills

threatintel.eu