CYFIRMA

DECODING THREATS

THE VALUE OF PREDICTIVE INTELLIGENCE

EXTERNAL THREAT LANDSCAPE MANAGEMENT

2022

CYFIRMA AT A GLANCE

TRAILBLAZING EXTERNAL THREAT LANDSCAPE MANAGEMENT PLATFORM COMPANY

Founded in 2017 by ex-government intelligence head and CISO

AI/ML enabled, cloud native SaaS products – DeCYFIR and DeTCT

Won multiple renowned awards garnering global industry recognition

Established player in Japan; displaced larger competitors at Fortune 100 customers

Referenceable Fortune 500 clients

Digital Hearts, ecbeing, Mitsubishi Corporation, NEC, NTT DATA INTELLILINK Corporation, TOSHIBA, TOPPAN, ZUELLIG PHARMA

Trusted Partnerships

aws partner network, isv accelerate, Digital Hearts, NEC, NTT DATA INTELLILINK Corporation, PRIANTO, Inflow Information Integrity

Backed by Marquee Investors

Goldman Sachs, ZODIUS, Z3Partners

5	**>100**	**1.4mn+**	**145+**	**25+**	**~USD 2bn**
Region Presence (Singapore, Japan, India, US, EU)	GB Data analyzed every 8 hours	Threats analyzed and prioritized[1]	Predictive Advisory Release[2]	Clients avoided financial, reputational & productivity damage[1]	Tangible & Intangible losses avoided[1]

WHY ARE WE DOING WHAT WE ARE DOING

ONCE UPON A TIME…

Understand the identified threat actors, campaigns, and target assets that could affect your customer and the industry they are operating in, to take corrective actions well before the threat and risk is realised.

REACTIVE	PROACTIVE	PREDICTIVE

Every now has a history
▪ The concept of Cyber Security has its heritage from the 1970s, something that has became increasingly visible since the 1990s.
▪ Simple methods have grown into sophisticated methods to attack and defence.
	Today's mindset may help you
	▪ The "you have been breached" mindset is a common agreement.
	▪ Security Controls allow you to secure your organisation
	  ▪ Using privileges with an automated management.
	  ▪ Structure the infrastructure more precisely by network segregation and air gapped networks .
	  ▪ Implement endpoint security.
	  ▪ Identify the common security parameters: Identities and their access permissions.
		The future always starts today
		▪ The change of infrastructure perimeters, e.g. by SaaS, PaaS and basic cloud adoption leads to more complex security challenges.
		▪ Interoperability across multiple organisations lead to exposure towards the cybersecurity threats and risks.

Security Vendors, Specialized organizations such as country CIRT / Internet News	OSINT, Threat Intelligence Vendors, Professional Researchers	**CYFIRMA' S ETLM, THREAT DISCOVERY AND PREDICTIVE CYBER INTELLIGENCE**

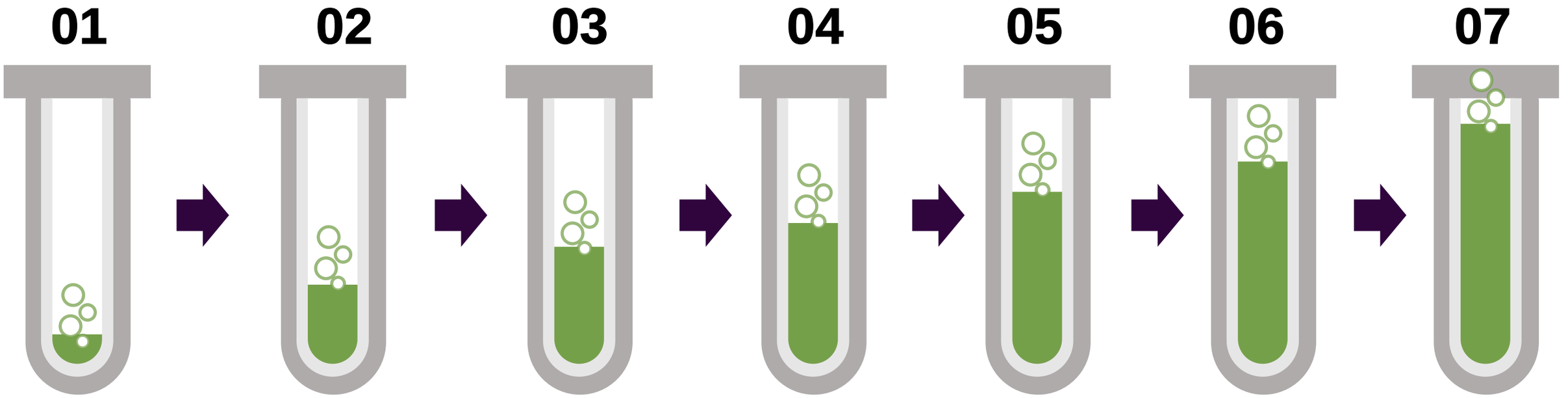
A secure "inside" does not prevent you from risks and threats from the "outside"

CYFIRMA
DECODING THREATS

WHY ARE WE DOING WHAT WE ARE DOING

IDENTIFYING TARGETED INTELLIGENCE TO PREVENT ATTACKS

The Kill Chain



Reconnaissance
Scanning the environment or harvesting information from various sources

Weaponization
Pairing malicious code with an exploit to create a weapon (Piece of Malware

Delivery
Transmission of weapon/malware to target (e.g. via email, intrusion, spoofing, phishing etc.)

Exploitation
Once delivered, the weapon/malware code is triggered upon an action. This in turn exploits the vulnerability.

Installation
The weapon installs malware on the system

Command & Control
A command channel for remote manipulation of the victim

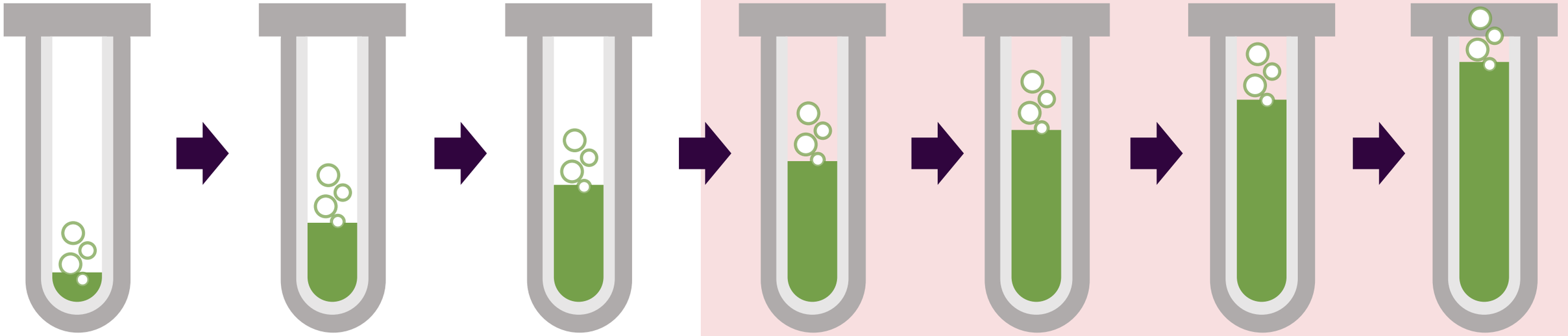
Action on objectives
With hands on access the attacker and achieve their objective

CYFIRMA
DECODING THREATS

WHY ARE WE DOING WHAT WE ARE DOING

IDENTIFYING TARGETED INTELLIGENCE TO PREVENT ATTACKS

The Kill Chain



01 Reconnaissance
Scanning the environment or harvesting information from various sources

02 Weaponization
Pairing malicious code with an exploit to create a weapon (Piece of Malware

03 Delivery
Transmission of weapon/malware to target (e.g. via email, intrusion, spoofing, phishing etc.)

04 Exploitation
Once delivered, the weapon/malware code is triggered upon an action. This in turn exploits the vulnerability.

05 Installation
The weapon installs malware on the system

06 Command & Control
A command channel for remote manipulation of the victim

07 Action on objectives
With hands on access the attacker and achieve their objective

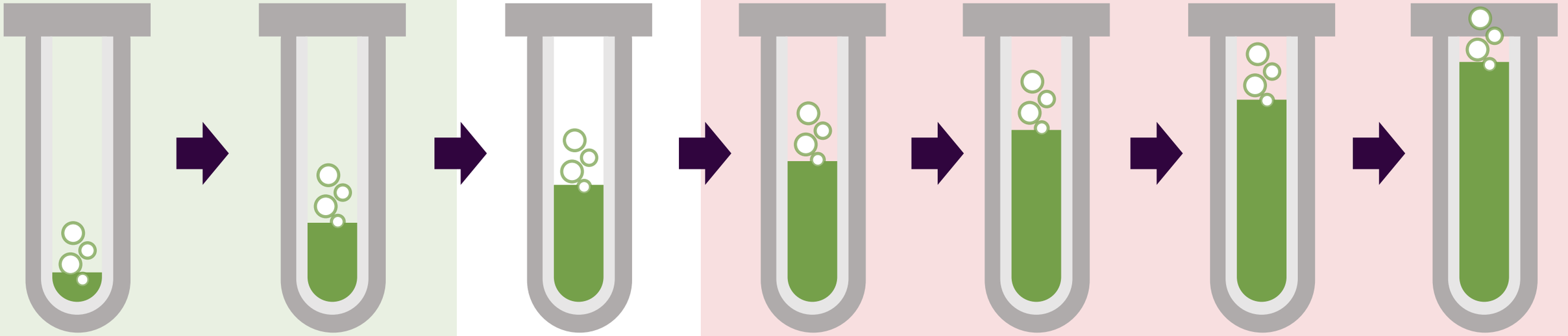
Traditional Approaches to react against identified Cyber Threats

CYFIRMA
DECODING THREATS

WHY ARE WE DOING WHAT WE ARE DOING

IDENTIFYING TARGETED INTELLIGENCE TO PREVENT ATTACKS

The Kill Chain



01 Reconnaissance
Scanning the environment or harvesting information from various sources

02 Weaponization
Pairing malicious code with an exploit to create a weapon (Piece of Malware

03 Delivery
Transmission of weapon/malware to target (e.g. via email, intrusion, spoofing, phishing etc.)

04 Exploitation
Once delivered, the weapon/malware code is triggered upon an action. This in turn exploits the vulnerability.

05 Installation
The weapon installs malware on the system

06 Command & Control
A command channel for remote manipulation of the victim

07 Action on objectives
With hands on access the attacker and achieve their objective

CYFIRMAS unique value of predictive Intelligence

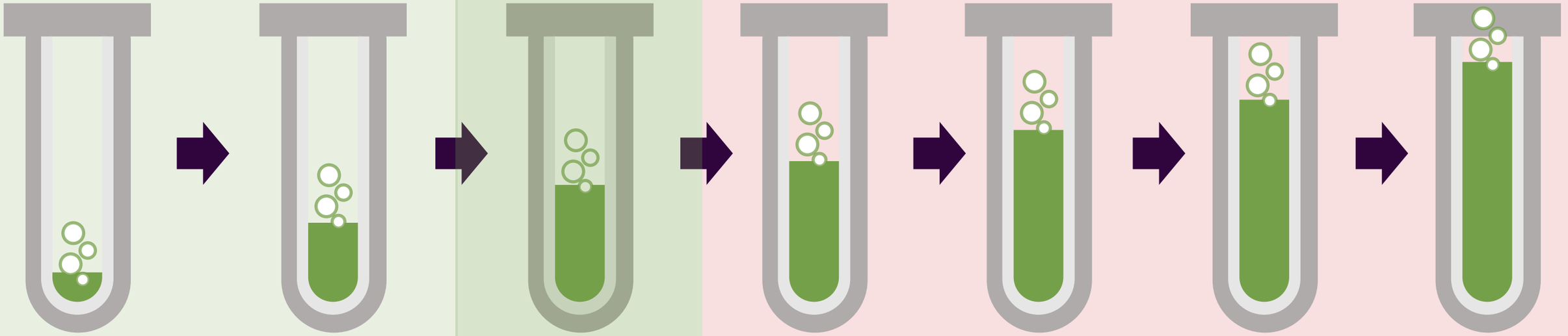
Traditional Approaches to react against identified Cyber Threats

CYFIRMA
DECODING THREATS

WHY ARE WE DOING WHAT WE ARE DOING

IDENTIFYING TARGETED INTELLIGENCE TO PREVENT ATTACKS

The Kill Chain



01 Reconnaissance
Scanning the environment or harvesting information from various sources

02 Weaponization
Pairing malicious code with an exploit to create a weapon (Piece of Malware

03 Delivery
Transmission of weapon/malware to target (e.g. via email, intrusion, spoofing, phishing etc.)

04 Exploitation
Once delivered, the weapon/malware code is triggered upon an action. This in turn exploits the vulnerability.

05 Installation
The weapon installs malware on the system

06 Command & Control
A command channel for remote manipulation of the victim

07 Action on objectives
With hands on access the attacker and achieve their objective

CYFIRMAS unique value of predictive Intelligence

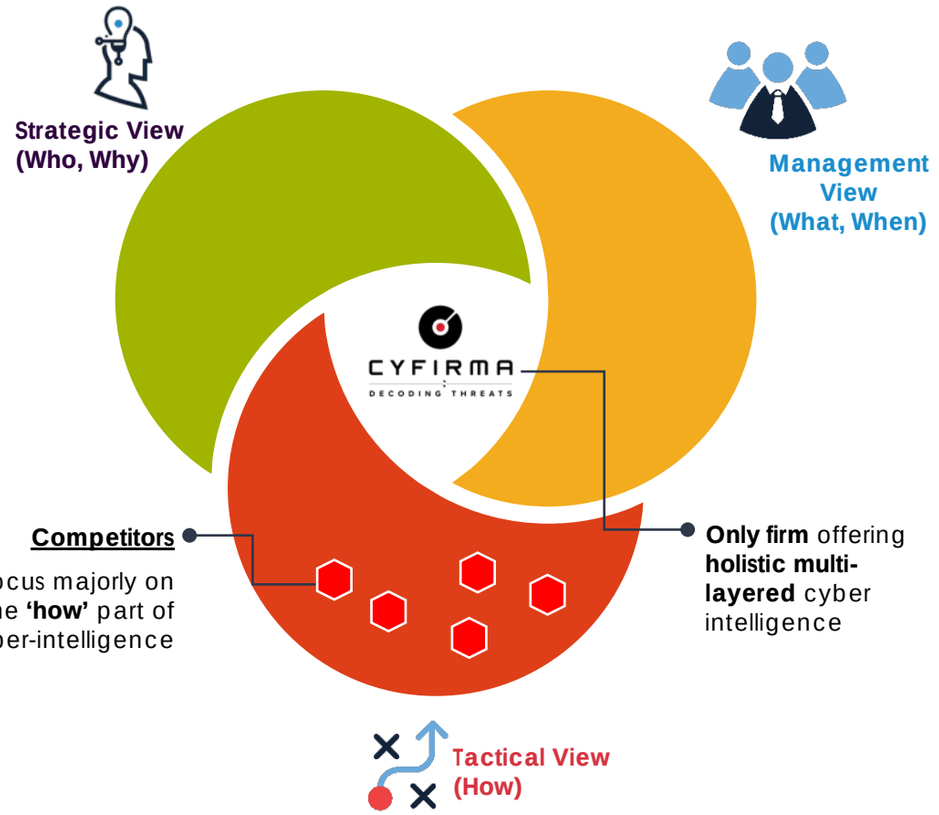
Traditional Approaches to react against identified Cyber Threats

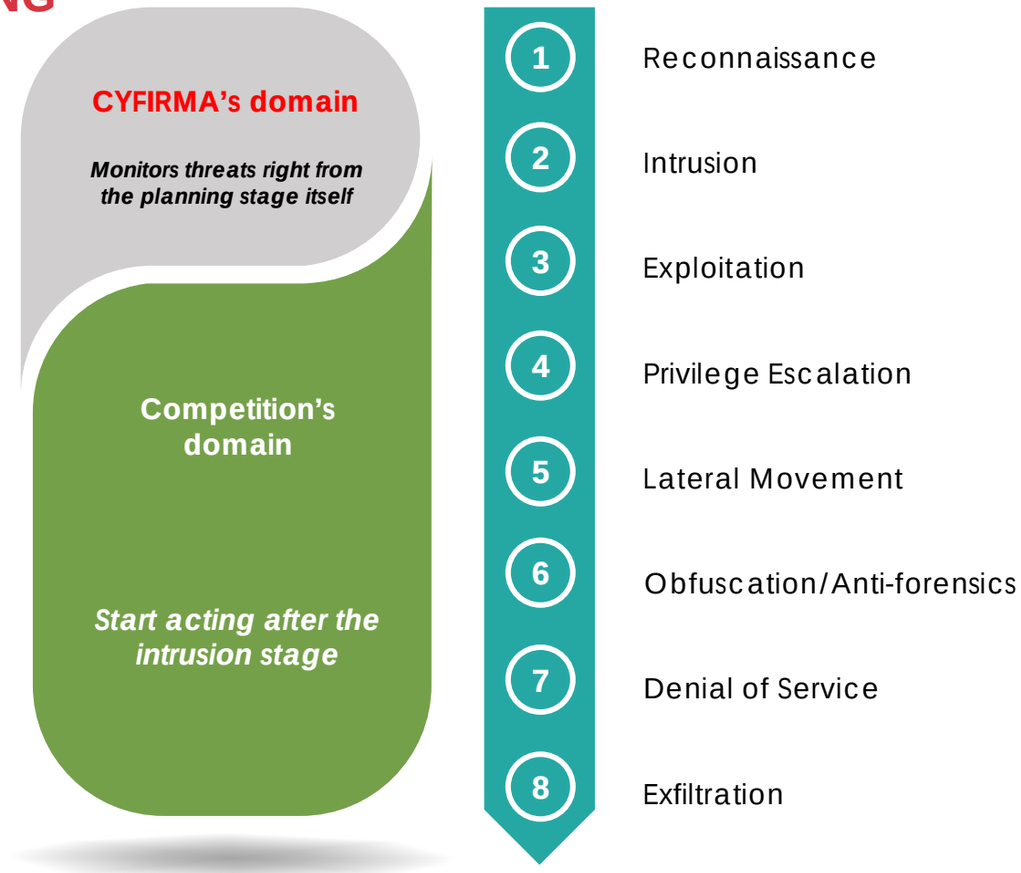
CYFIRMA
DECODING THREATS

COMPETITIVE LANDSCAPE (1/2)

MULTI-LAYERED CYBER INTELLIGENCE UNRAVELLING THREATS AT THE PLANNING STAGE ITSELF

COMPETITIVE POSITIONING





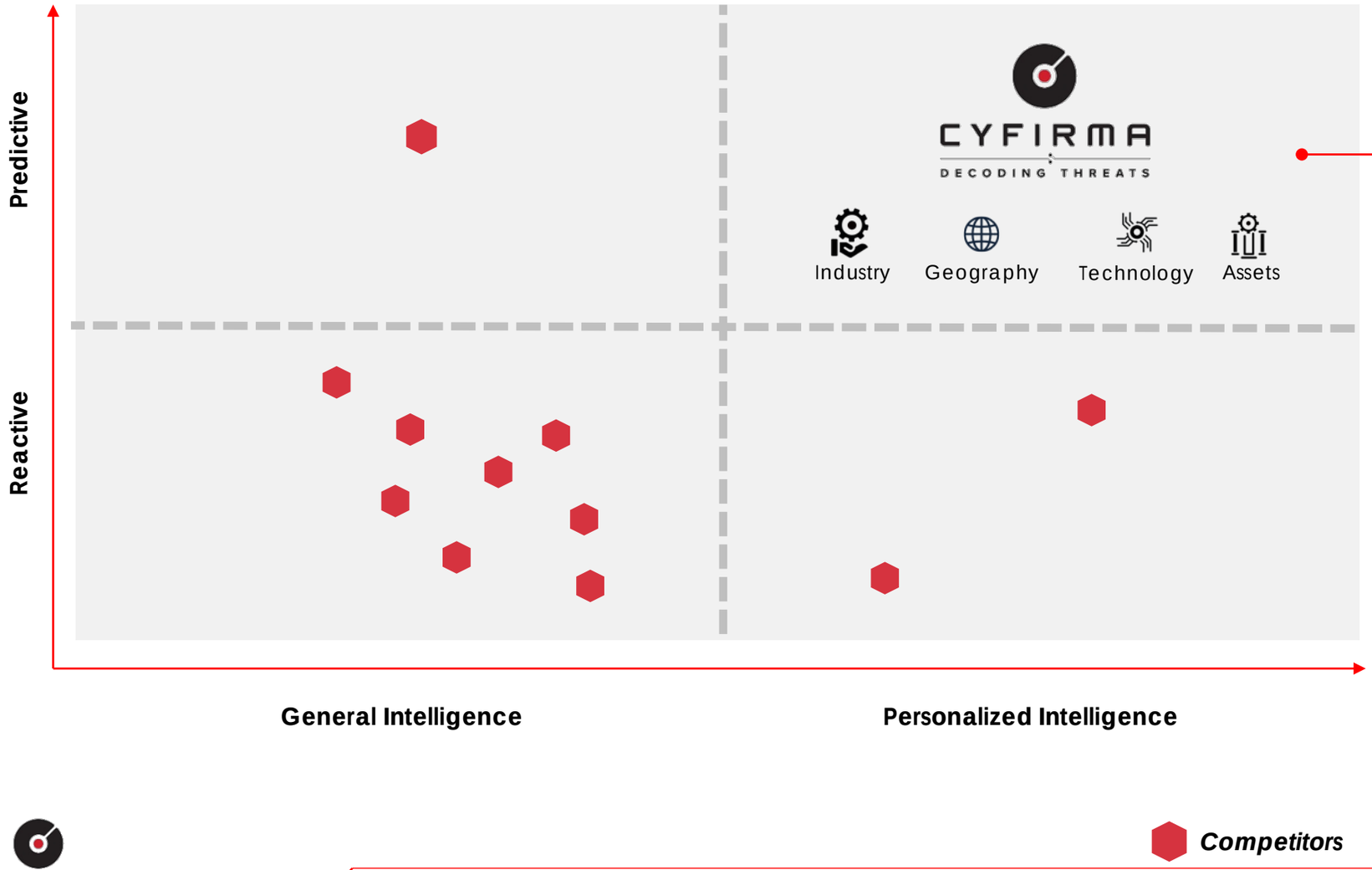
CYFIRMA offers clients comprehensive views of their external threat landscape

CYFIRMA provides early warning to clients on attacks at the planning stage*

CYFIRMA
DECODING THREATS

COMPETITIVE LANDSCAPE (2/2)

OFFERING PREDICTIVE & PERSONALIZED CYBER INTELLIGENCE



KEY DIFFERENTIATORS

Market leader and only player offering Cyber Intelligence that is:

- Predictive
- Personalized to – Organization's Assets / Geography / Industry / Technology
- Single pane of glass – complete view of threat landscape
- Multi-layered – S, M, T
- Cyber Intelligence combined with Attack Surface Discovery and Digital Risk protection
- Developed for CISOs, CROs, Security Ops team

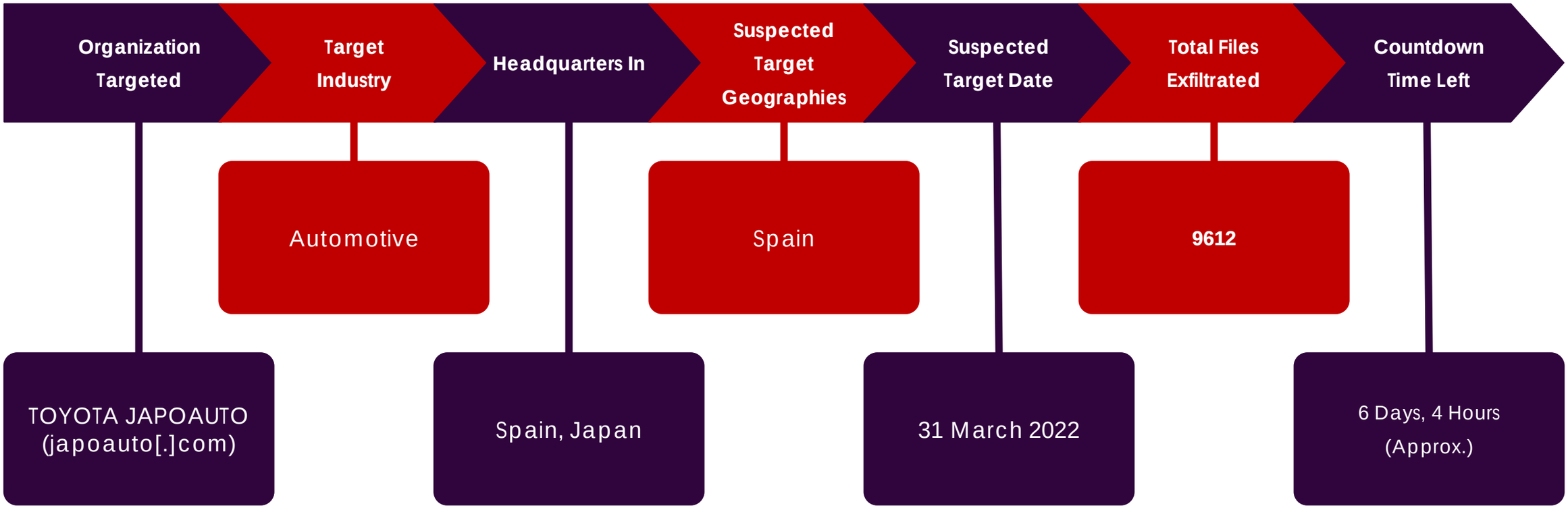
CISO – Chief Information Security Officer

CRO – Chief Risk Officer

PREDICTIVE INTELLIGNECE

A REAL LIFE EXAMPLE

LockBit2.0 Ransomware Targets TOYOTA JAPOAUTO



EXFILTRATED SENSITIVE INFORMATION COULD CONTAIN SENSITIVE DETAILS, PII, FII, CII AND MORE.

CYFIRMA
DECODING THREATS

PREDICTIVE INTELLIGNECE

A REAL LIFE EXAMPLE

What we know about LockBit 2.0 Ransomware

The ransomware is suspected to be **active since July 2021** and has targeted multiple organizations across industries and geographies.

For initial access into the system of the organization, the most common method used by the ransomware operators are **insider threats (offering monetary benefits to disgruntled employees)**, using RDP connections, vulnerabilities & exploits observed in public-facing servers, VPN servers, phishing emails, and drive-by downloads. They try to **gain access through StealBit Trojan, Metasploit Framework, and Cobalt Strike on domain admin accounts exploiting vulnerabilities such as CVE-2019-0708** (BlueKeep vulnerability).

Post gaining access, the ransomware group **carries out reconnaissance for sensitive information and active directory environment**. The operators appear to be **using the Double Extortion strategy** – demand ransom to **provide decryption keys for exfiltrated data** or **threaten** to **release the data in public** if the ransom is not paid. For this, they set up a count-down timer to make the ransom payments.

The ransomware operators are **believed to be Russian and offer Ransomware-as-a-Service (RaaS) model** and are suspected to be leveraged by Russian cybercriminals.

PREDICTIVE INTELLIGNECE

A REAL LIFE EXAMPLE

Based On Mitre Attack, Following Are The TTPs Used By Them

Sr.No	Tactics	Techniques
1	**TA0043: Reconnaissance**	T1595.001 : Active Scanning – scanning IP Blocks
2	**TA0042: Resource Development**	T1584.001 : Compromise Infrastructure - Domains
3	**TA001: Initial Access**	T1584.001 : Compromise Infrastructure - Domains
		T1190 : Exploit Public-Facing Application
4	**TA002: Execution**	T1059.001 : Command and Scripting Interpreter- PowerShell
		T1059.003 : Command and Scripting Interpreter- Windows Command Shell
		T1047:Windows Management Instrumentation
5	**TA003: Persistence**	T1547.001:Boot or Logon Autostart Execution Registry Run Key
6	**TA008: Lateral Movement**	T1021.002:Remote Services Remote Desktop Protocol
		T1570 : Lateral Tool Transfer
7	**TA0040: Impact**	T1486 : Data Encrypted For Impact
		T1490 : Inhabit System Recovery
		T1489 : Service Stop

CYFIRMA
DECODING THREATS

PREDICTIVE INTELLIGNECE

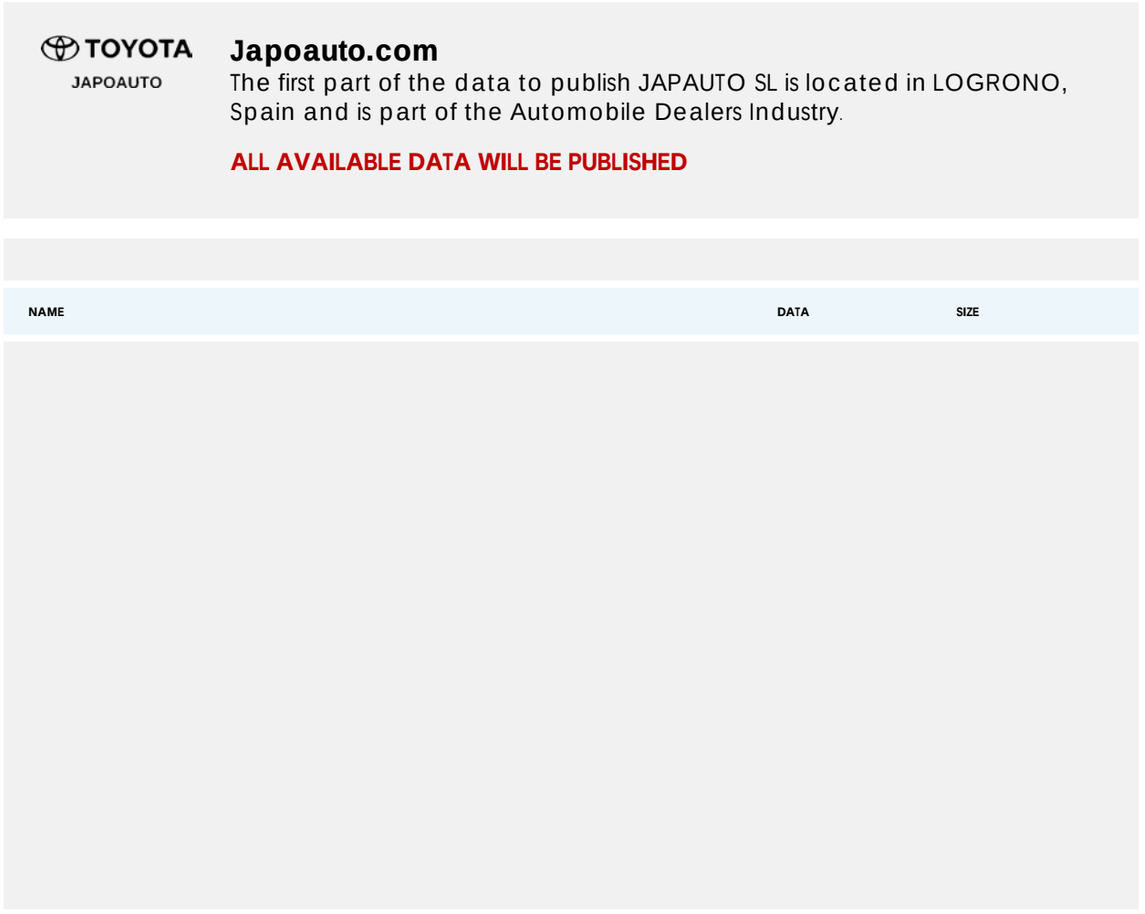
A REAL LIFE EXAMPLE

UNTIL FILES

6D 04: 13: 52

PUBLICATION

31 Mar, 2022 00:00:00



CYFIRMA
DECODING THREATS

OUR 6 PILLARS FOR PREDICTIVE INTELLIGENCE

SIX INTELLIGENCE VIEWS ON A UNIFIED PLATFORM TO MANAGE CYBER THREATS AND RISKS

1

ATTACK SURFACE DISCOVERY

Identify ‘doors’ and ‘windows’ into the organization

Business Outcome: Real-time continuous monitoring to identify shadow IT or porous systems which can be accessed by cybercriminals. **Awareness of attack surface will allow you to conduct a realistic cost-benefit analysis of each asset and decide how to shrink your attack surface.**

2

VULNERABILITY INTELLIGENCE

Keys to ‘doors’ and ‘windows’ that are available for cyber criminals to exploit

Business Outcome: Vulnerabilities are mapped to assets and associated exploits and ranked based on criticality. **This allows the business to optimize resources to focus on the most important and urgent gaps.**

3

BRAND INTELLIGENCE

Know when your brand is under attack

Business Outcome: Understand who, why and how your brand is being targeted, get complete view of brand infringement. **Protect the brand and retain customer loyalty by ensuring it is not being tarnished by corporate espionage, insider threats or other malicious bad actors.**

4

DIGITAL RISK PROTECTION

Clarity on digital profile, data leaks, breaches, and impersonations

Business Outcome: Unveil digital footprints and cases of impersonation and data leaks. Get near real-time alert on your data leaked in the wild. **With this knowledge, you can plug the gap and avert any further reputation and financial damage.**

5

SITUATIONAL AWARENESS

Gain control of evolving threat landscape by understanding emerging threats, mitigations and potential attack scenarios

Business Outcome: Quick view of cyberattack, incident and breach taking place in your industry, the technology you use, and the geography you operate in. **These insights and impact can guide important business decisions including cyber investments.**

6

CYBER-INTELLIGENCE

Predictive, personalized, multi-layered, contextualised intelligence dissects a cyberattack campaign to answer WHO, WHY, WHAT, WHEN, HOW of a cyberattack campaign in the making

Business Outcome: Get complete view and insights to your external threat landscape. **Keep the enemy at bay, receive early warning to fend off cyberattacks to avoid disruption that could threaten business.**

CYFIRMA
DECODING THREATS

CYFIRMA

DECODING THREATS

Japan | Singapore | India | USA | EU

THANK YOU

www.cyfirma.com
www.cyfirma.jp