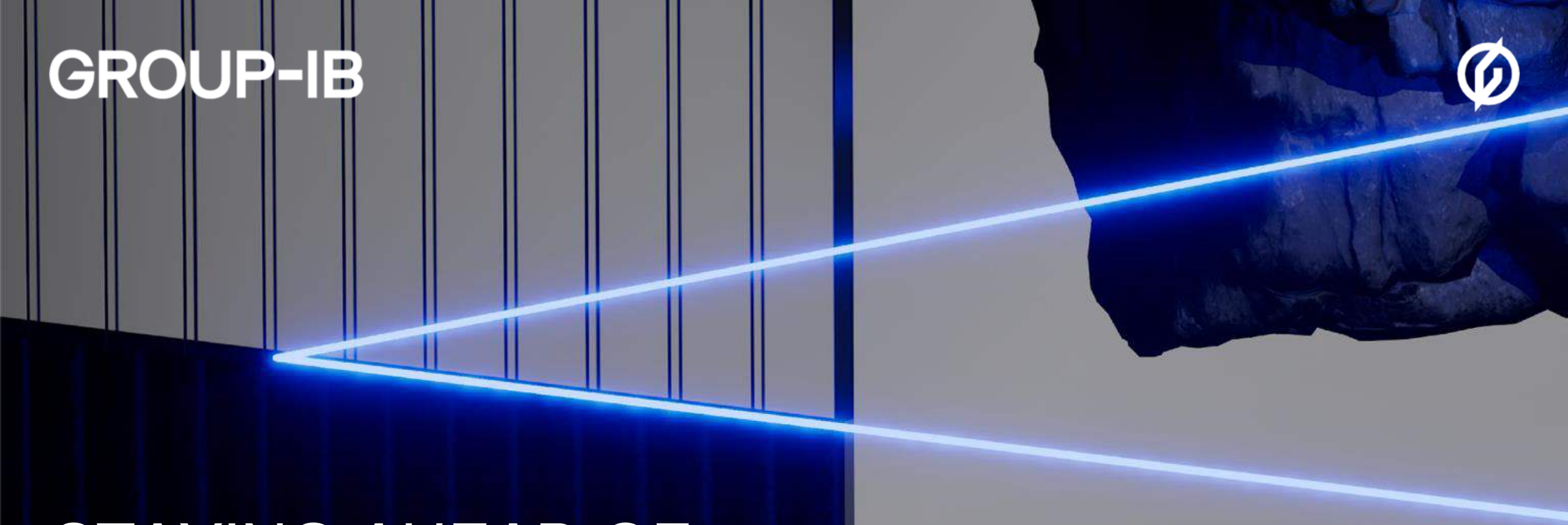
GROUP-IB



STAYING AHEAD OF THREAT ACTORS

19TH JANUARY 2022

INTRODUCTION

Security teams are tasked with defending their organization from incoming attacks, but in the rapidly evolving cyber landscape how can they stay ahead of threat actors?

Implementing a robust security strategy could be the difference that prevents a costly data breach, unmitigated fraud and unnecessary expenditure.

About me

Alexandra Wells
Threat Intelligence & Attribution
Group-IB

AGENDA

Part 1: Using your **threat landscape** to build **security strategy**

- Filtering data to focus on relevant information
- Attributing attacks provides actionable intelligence
- Threat landscapes answer critical strategic questions

Part 2: How to use **threat intelligence** to understand your **threat landscape**

- What is threat intelligence
- How threat intelligence is sourced and disseminated
- Use cases for threat intelligence insights

Part 3: Building your **business case** using the **security strategy**

- How analysts build business cases
- Creating your own business case
- Doing nothing is also a choice

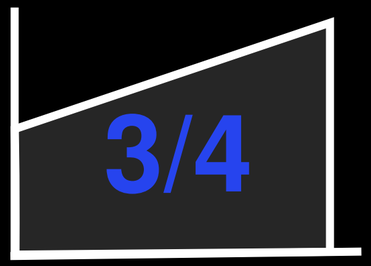
PART 1: USING THE THREAT LANDSCAPE TO BUILD A SECURITY STRATEGY

TRADITIONAL SECURITY HAS A FLAW

“Know the enemy and know yourself in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal.”

- Sun Tzu

WHAT WE HAVE ALL HEARD BEFORE

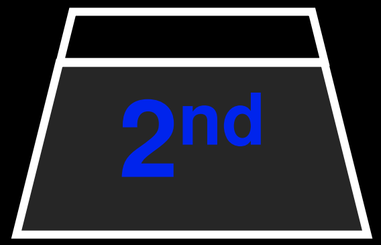


Over three quarters of CISOs say their organization experienced an increase in the number of cyber attacks in the past 12 months

VMware Global Security Insights Report 2021

It takes an average of 287 days to identify and contain a data breach, and an average of 341 for compromised credentials

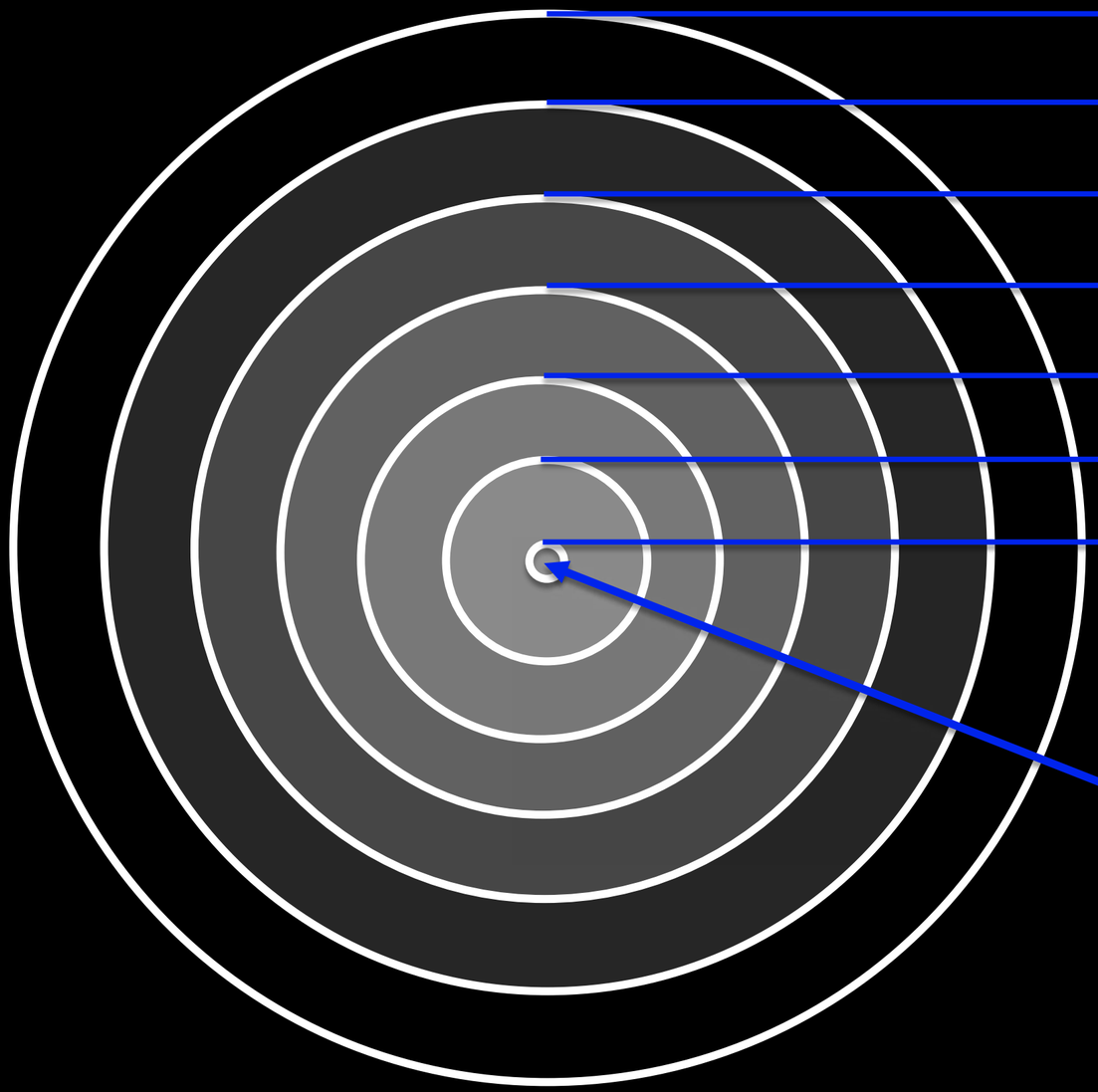
IBM Security Cost of a Data Breach Report 2021



Cyberattacks 2nd most concerning risk for doing business globally over the next 10 years

World Economic Forum - Global Risk Report (2020)

INFORMATION NEEDS TO BE FILTERED



All information

Geographic region

Industry

Organization size

Technology

Partners

Customers

Information we care about

EXAMPLE: LOCALISED INFORMATION

Ransomware

Europe suffered the **second most** ransomware attacks in 2021 of any region

Ransomware attacks on European organizations grew **84%** last year

The Netherlands is **ranked 11th globally**, for the number of ransomware attacks

Phishing

Europe is the most targeted region by phishing, receiving **36.2%** of all attacks

The Netherlands has **3,836 phishing** resources hosted in the country

Phishing-as-a-Service programs are being developed in the Netherlands

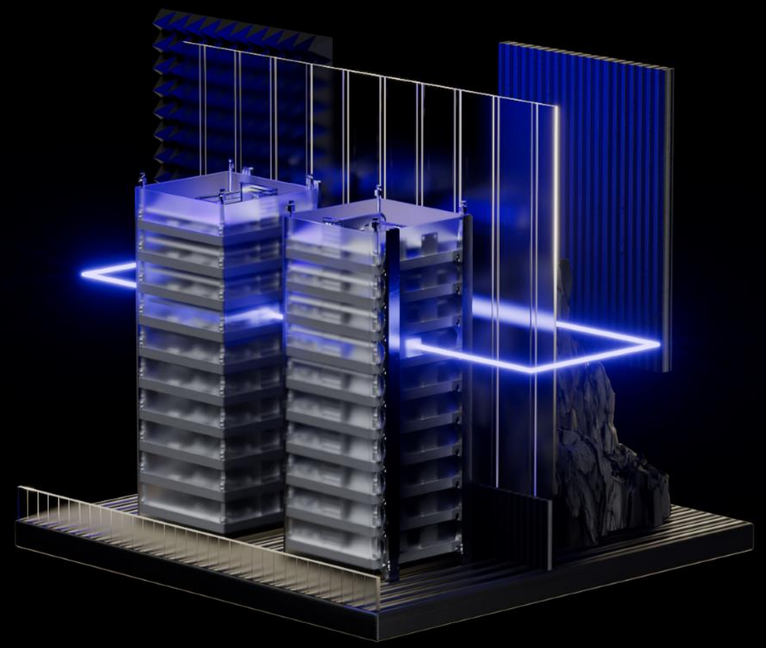
Source: Group-IB Hi-Tech Crime Reports 2021 Link 1 Link 2

ATTACKS DON’T COME FROM NOWHERE

Attacks are launched by threat actors

Threat actors have patterns and behaviours which we can use to our advantage.

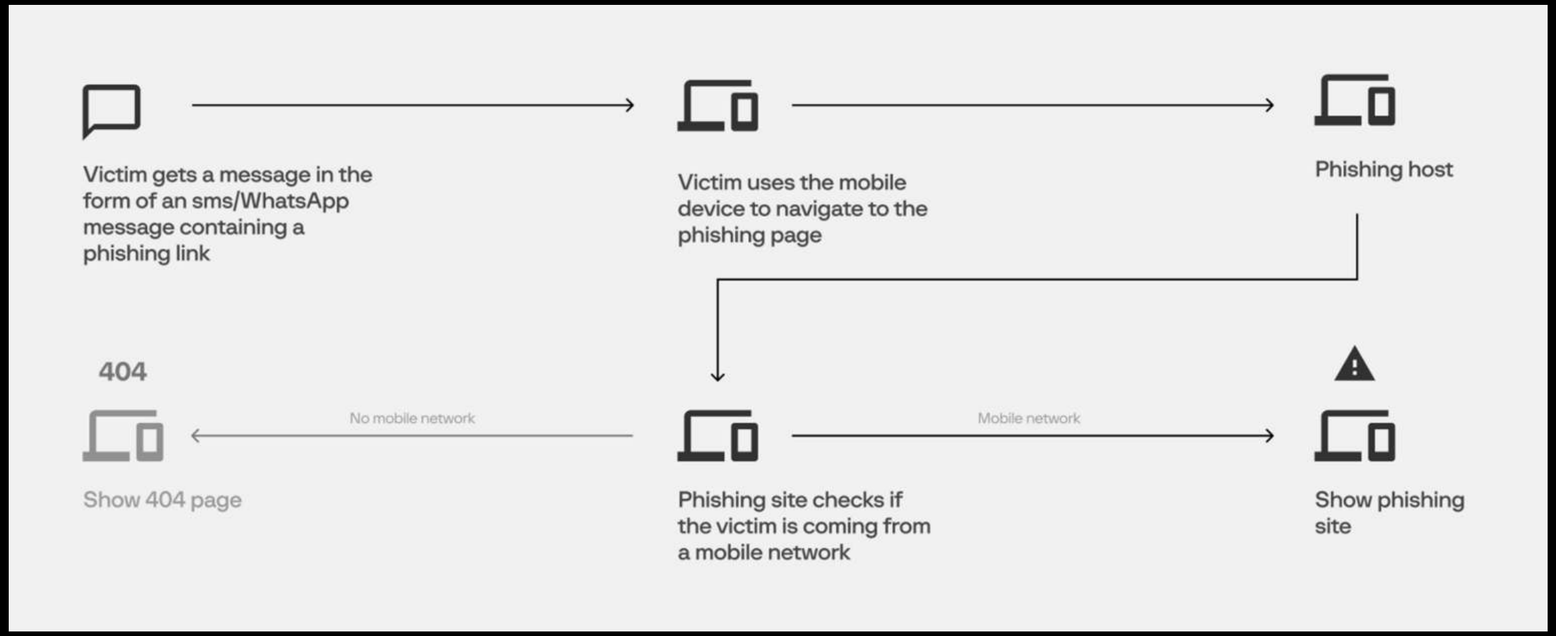
They will often reuse infrastructure they have developed, use techniques and procedures they have developed over time, and attack industries and regions that they are familiar with.



EXAMPLE: ATTRIBUTED INTELLIGENCE

RUNLIR is a prolific phishing group in the Netherlands

- Use Smishing (phishing that uses mobile networks)
- Infrastructure was first discovered in March 2021, and includes 750 domains
- Their toolset includes:
  - BlackTDS (anti-bot)
  - Yalishanda (hosting service)
  - LogoKit (phishing kit)
  - uAdmin (phishing kit)



Example of one technique used by RUNLIR to avoid detection in the Netherlands

Source: Group-IB Hi-Tech Crime Reports 2021 Link

THE CHALLENGE

Every threat actor targets different victims and every threat actor uses different tactics, techniques and procedures (TTPs)

Which threat actors should I monitor?

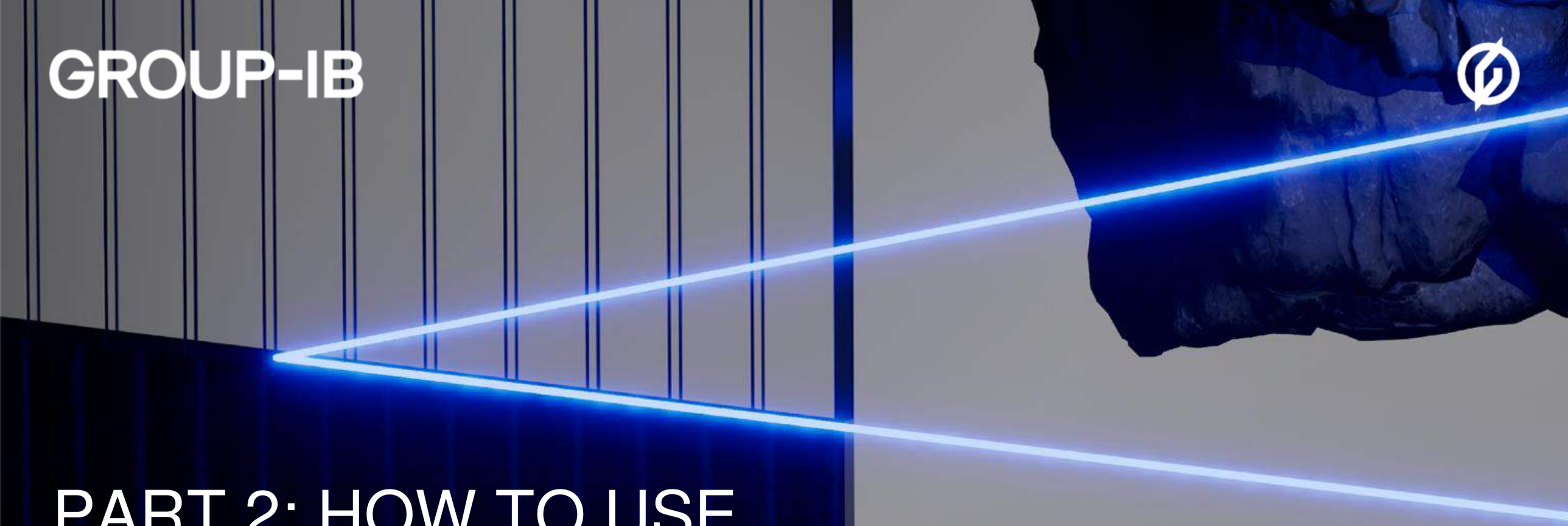
BUILDING A THREAT LANDSCAPE

Questions a threat landscape should seek to answer:

- Who are the threat actors targeting my organization?
- What are the threat actors' motives and objectives?
- Which assets and technologies are adversaries attacking?
- What are the emerging threats in my industry?
- Who poses a threat to the industry in different regions?
- Which adversaries have expressed interest in my organization in the past?

Answers can be found in threat intelligence

GROUP-IB



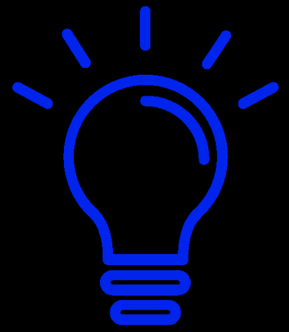
PART 2: HOW TO USE THREAT INTELLIGENCE TO UNDERSTAND THE THREAT LANDSCAPE

WHAT IS THREAT INTELLIGENCE?

“Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.”

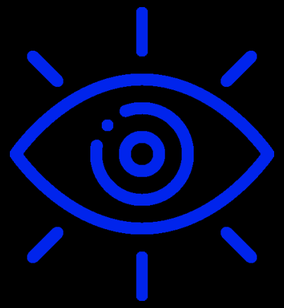
- Gartner

WHAT THE EXPERTS ARE SAYING



“The growing volume and complexity of attacks drive the demand for cybersecurity solutions as organizations recognize the importance of proactive and predictive defense for staying ahead of cyber adversaries”

Frost & Sullivan Frost Radar: Global Cyber Threat Intelligence Market, 2021*



“Cyber threat intelligence offers improved visibility into overall network threats and informs decision makers how to prioritize security around potential targets and threats”

Accenture Cyber Threat Intelligence Report (2021)

“Fewer than 1 in 3 organisations use available data and intelligence when making decisions. But those that had the best cybersecurity outcomes over the past two years are 18x more likely to say data and threat intel are integral to their operating model”

PwC - Digital Trust Insights (2022)

*Source: Link

SOURCES OF THREAT INTELLIGENCE

HUMAN INTELLIGENCE

- Malware reverse engineers
- Undercover dark web agents
- Hacker's communication channels

MALWARE INTELLIGENCE

- Malware emulators
- Malware configuration files extraction
- Detonation platform
- Public sandboxes

SENSOR NETWORK

- ISP-level sensors
- Honeypot network
- Spamtraps
- Sinkholing

DATA INTELLIGENCE

- Botnet and phishing C&C servers
- C&C servers of webskimmers
- Phishing admin panels
- Card shops

OPEN SOURCE INTELLIGENCE

- Paste sites
- Code repositories
- Vulnerabilities
- Social media
- URL sharing services

INVESTIGATIONS

- Collaboration with Interpol and Europol
- Regional law enforcement partners
- DFIR and audit teams

DISSEMINATING THREAT INTELLIGENCE

	Strategic	Operational	Tactical
Who it is for	• Security leaders • Executives	• Team leaders • SOC engineers	• Security analysts • Threat researchers
What format	• On-demand, and regular monthly and quarterly reports	• TTPs in MITRE ATT&CK matrix • Security integrations	• IoC database • Security integrations
How it is used	• Intelligence-driven risk management • Enable business growth • Maximize value of security investments	• Proactive threat mitigation • Identify and remove weaknesses • Automate workflows and improve efficiency	• Prioritize patching of vulnerabilities • Eliminate false positives • Reduce response time

USE CASE 1: RISK MANAGEMENT

Identifying and mitigating vulnerabilities

Challenge:

- It’s not feasible to patch every software application immediately
- Critical vulnerabilities can go unpatched for longer than necessary
- Threat actors can exploit unpatched applications

Solution:

- Threat intelligence enables organizations to anticipate threats
- Organizations can monitor how often vulnerabilities are exploited, whether their industry or software is being targeted, or exploits are discussed

Don’t try to patch everything; focus on vulnerabilities that are actually exploitable. Go beyond a bulk assessment of threats and use threat intelligence, attacker activity and internal asset criticality to provide a better view of real organizational risk

Gartner - The top 10 cybersecurity predictions for 2020-2021

USE CASE 2: ENABLE BUSINESS GROWTH

Enable growth with actionable intelligence

Challenge:

- Expanding into a new region/business line can attract new threat actors utilizing TTPs that the organization is unprepared for
- Digital transformation, particularly enabling customers and partners digitally, can expose business infrastructure

Solution:

- Threat intelligence allows security teams to investigate the threat actors targeting specific regions and industries
- Risk assessments of partners and technology can be conducted before services are implemented

By 2025, 40 percent of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from 10% today

Gartner – Press Release

USE CASE 3: MAXIMISE INVESTMENT VALUE

Lower the cost of cybersecurity

Challenge:

- Limited budget to spend on new and existing security services
- Many tools will provide a benefit, making it difficult to be selective about which to acquire

Solution:

- Threat intelligence helps organizations avoid unnecessary security investment and postpone unneeded upgrades
- Real-time intelligence allows organizations to tune their existing solutions to counter the attacks targeting them

Cybersecurity spending growth is slowing through 2023, while boards are starting to push back and ask what they have achieved after years of heavy cybersecurity spending

Gartner - Cybersecurity Must Be Treated as a Business Decision

PART 3: BUILDING A SECURITY BUSINESS CASE USING THREAT INTELLIGENCE

CASE STUDY

The Total Economic Impact analysis was created by Forrester Consulting to help organizations understand how to evaluate the value of Group-IB’s Threat Intelligence & Attribution.

The report can be used as a template to build security business cases for any organizations.

Source: Link

CALCULATING THE TOTAL ECONOMIC IMPACT

Total cost of ownership doesn’t capture the full picture

Components of an effective business case:

1. IT impact – Total cost of ownership
2. Business impact – Return on investment
3. Risk – Uncertainty and requirements for success
4. Long term outcomes – Alignment with strategic goals

EVALUATING: IMPACT

Costs

Vendor
- Upfront technology costs
- Annual subscription costs

Implementation
- Deployment and integration
- Technology dependencies

Human
- Upfront training
- Ongoing management and support

Benefits

Gartner predicts that by 2024, 60% of CISOs will establish critical partnerships with key executives in sales, finance and marketing, up from less than 20% today

Gartner - Press Release

INCORPORATING: RISK AND OUTCOMES

Risk

On average, large IT projects run 45 percent over budget and 7 percent over time, while delivering 56 percent less value than predicted

McKinsey - Delivering large-scale IT projects on time, on budget, and on value

Long term outcomes

88% of board directors view cybersecurity as a business risk

Gartner - CIOs Need to Rebalance Accountability for Cybersecurity With Business Leaders

ORGANIZATIONAL PROFILE

Industry
- Financial services
- Investment banking

Size
- $10 billion in annual revenue
- 100,000 employees

Region
- Europe

Challenges
- Struggled to prevent fraud from occurring
- Fraud damaged customer experience
- Increasing cyber risks lead to complex business processes
- Unable to determine points of compromise
- Inefficient and slow remediation processes

Estimated cost of fraud to business:

20,000 payment cards compromised per year
$600 financial loss per payment card
12 million USD per year in losses per year

EXAMPLE: CALCULATING IMPACT

Case study sample

(Total amount of payment card fraud × Coefficient of activity prevented)	----►	(20,000 per year × 0.25)
×		×
(Average loss per card × Coefficient of loss prevented)	----►	($600 × 0.50)
×		×
Risk adjustment coefficient	----►	0.80
=		=
Mitigated damages	----►	**$1,200,000 per year**

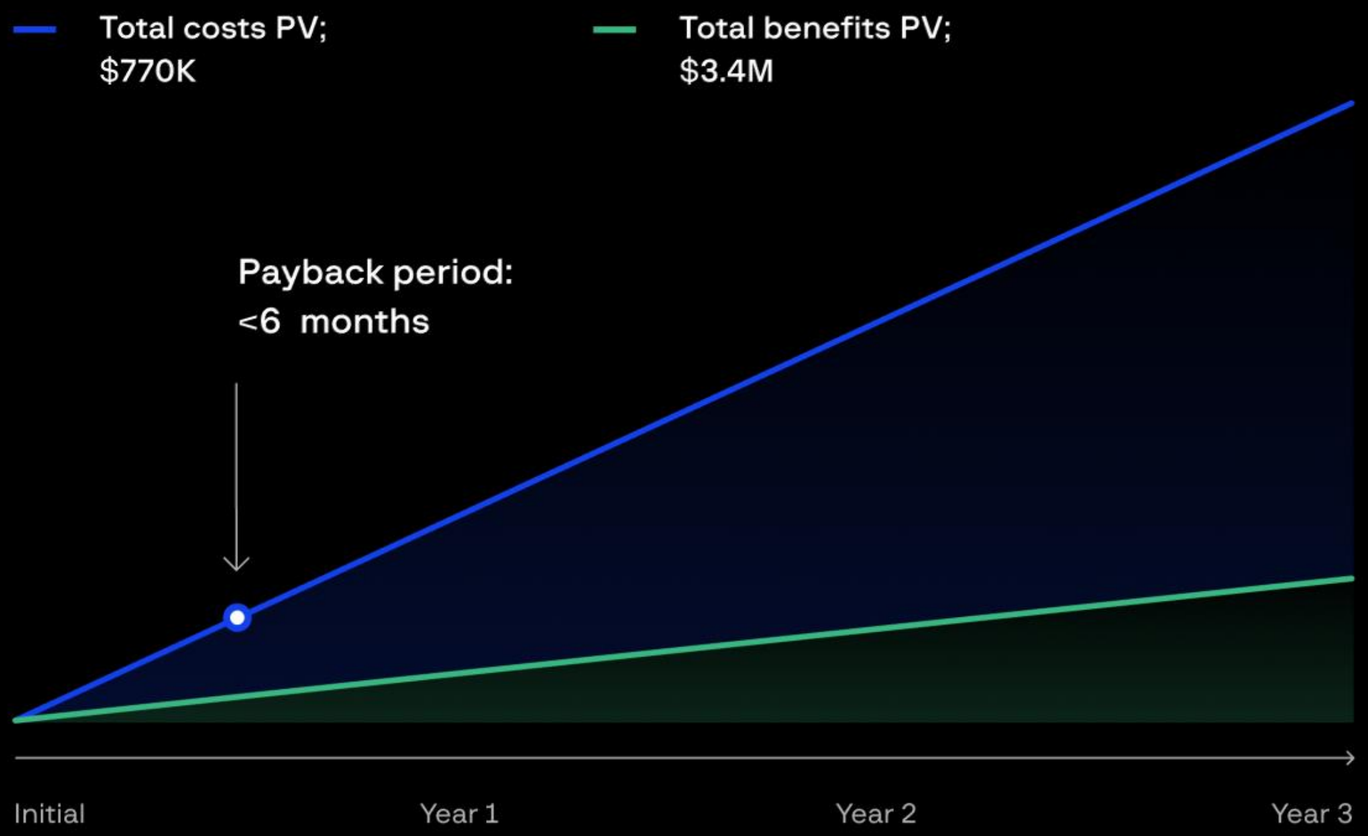
THE TOTAL ECONOMIC IMPACT

339%
Return on investment

$2.6 million
Net present value

+10%
Productivity in the security team

250 thousand
USD in opex savings



Source: Link

ADDITIONAL BENEFITS

Some benefits can not be easily quantified but are still valuable

For example:

- Better visibility into digital security threats
- Reduced cyber risks and potential reputational damage
- Time savings from reduced false incident investigations
- Improved the security team’s decision-making
- Increased collaboration
- Increased access to cyber threat intelligence

DOING NOTHING IS ALSO A CHOICE

Security business cases should be presented as A/B scenario choices not as yes/no decisions

The risks to a business from cyber threats change, historical events should not impact present day decision making

GROUP-IB

Summary

KEY POINTS

To have an effective security strategy you need to understand your threat landscape

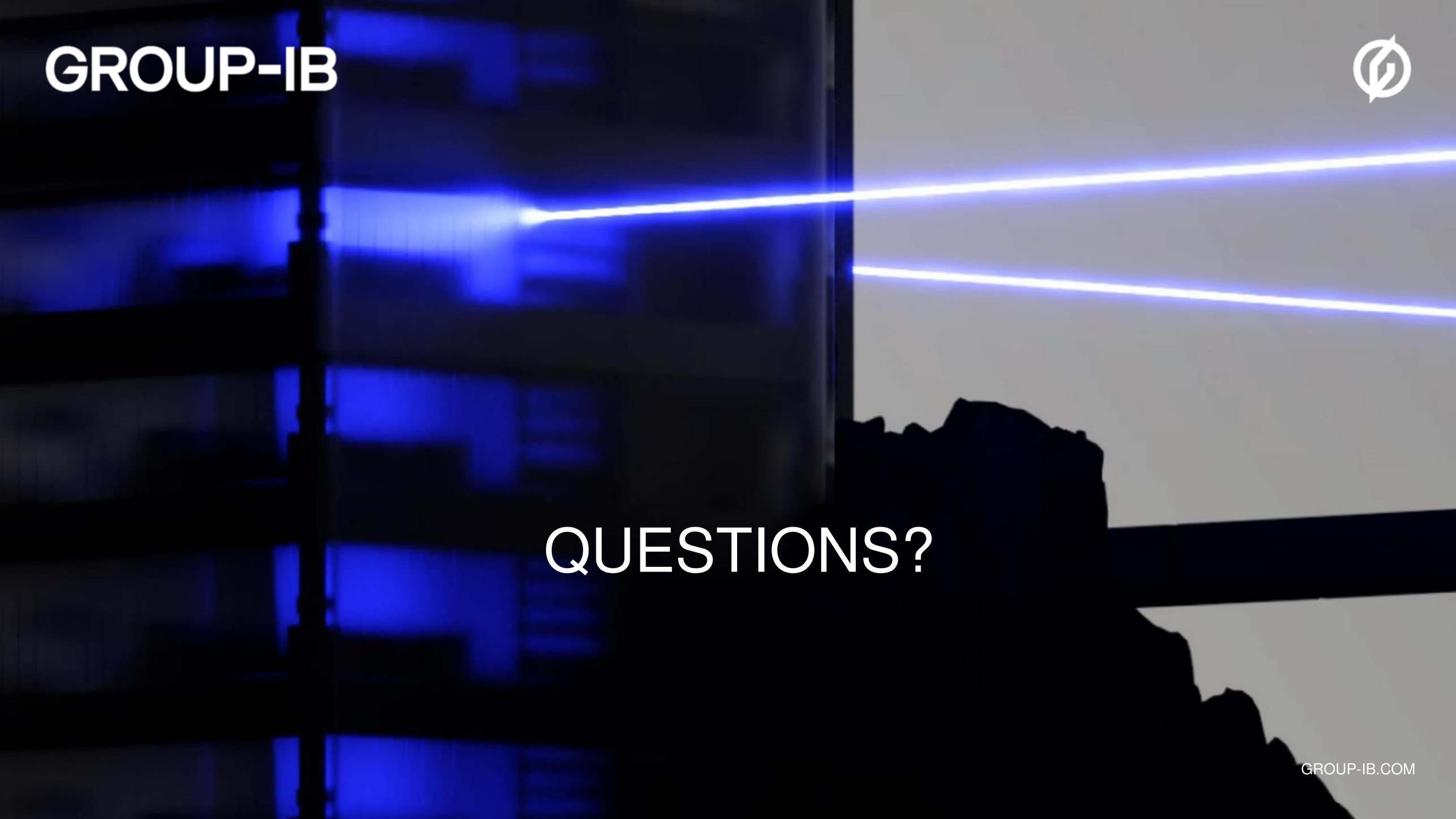
Build a detailed and up to date threat landscape using threat intelligence

Calculate the total economic impact of a projects to action your security strategy

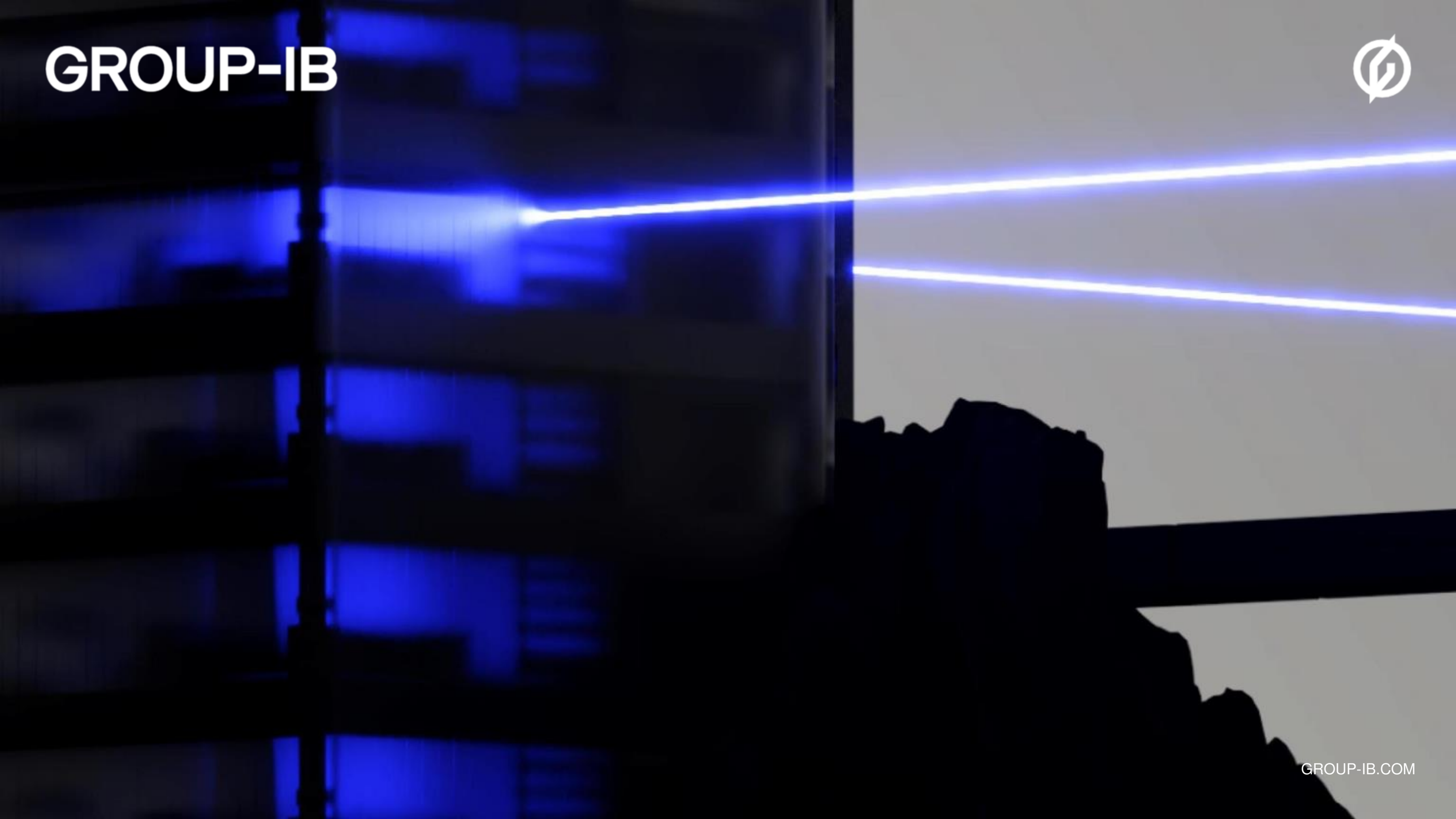
ONE LAST QUOTE

“It is only the enlightened ruler and the wise general who will use the highest intelligence of the army for the purposes of spying, and thereby they achieve great results.”

- Sun Tzu



QUESTIONS?


GROUP-IB