Cyber Security in Travel

Bertrand Alberola
Head of Tech Services Portfolio

April 29th, 2024

"My message to companies that think they haven't been attacked is: **'You're not looking hard enough'**"

UK Department for Science, Innovation and Technology

It's how travel works more securely

Cybercrime global impact

$10.5Tn

Cybercrime Worldwide annual cost by 2025
(3tn $ in 2015)
(INTZ, 2020)[2]

+15% avg growth/y
+60% extortion groups

Sophistication & Professionalization of cybercriminals "Cybercrime as a Service"

(CyberSecurity report, 2022)[1]

93%

of company networks can be accessed by cybercriminals
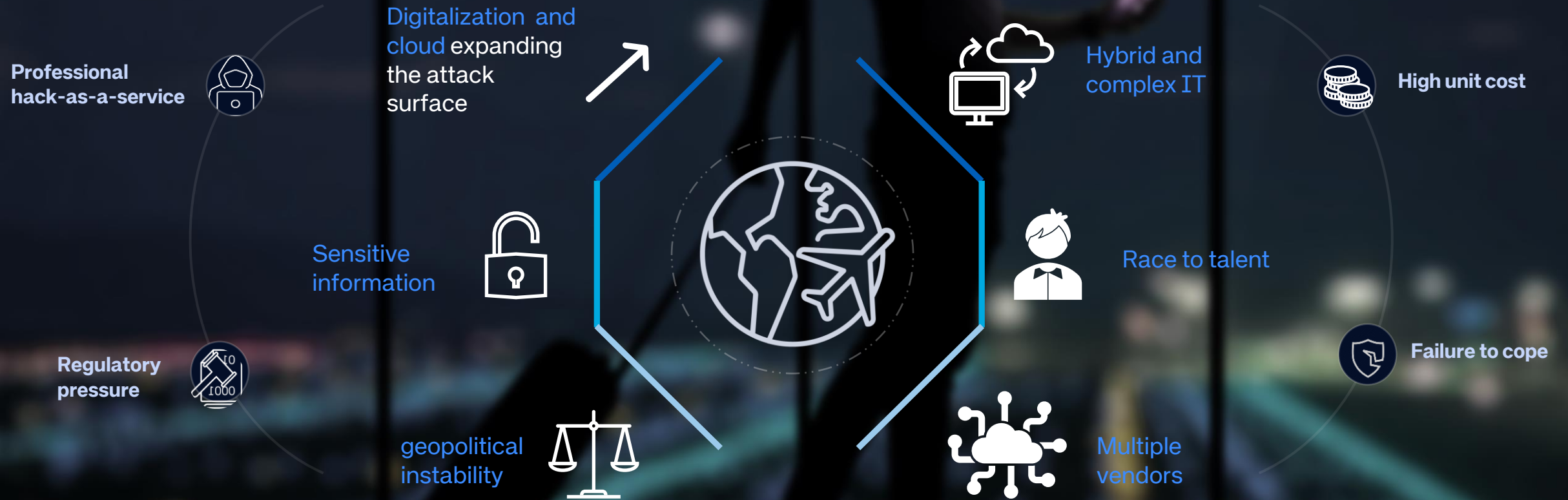*(betanews, 2020)[4]*

+358%

Increase of malware attacks compared to 2019
(Global Risks Report, 2022)[5]

Travel is a high target for sophisticated attacks

Why Travel is a high target

Root causes

Professional hack-as-a-service

Digitalization and cloud expanding the attack surface

Sensitive information

Regulatory pressure

geopolitical instability

Hybrid and complex IT

High unit cost

Race to talent

Failure to cope

Multiple vendors

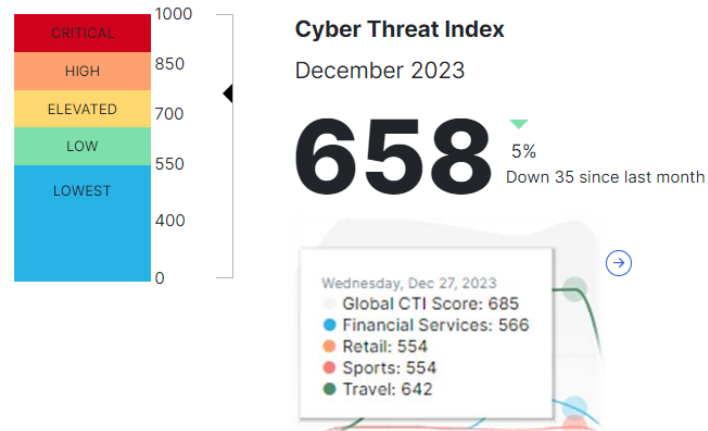It's how travel works more securely

aMaDEUS

Travel is a key target for cybercriminals

Cybercriminals are increasingly taking advantage of vulnerabilities within the travel industry, given the substantial value and sensitivity of the data stored for each traveler.
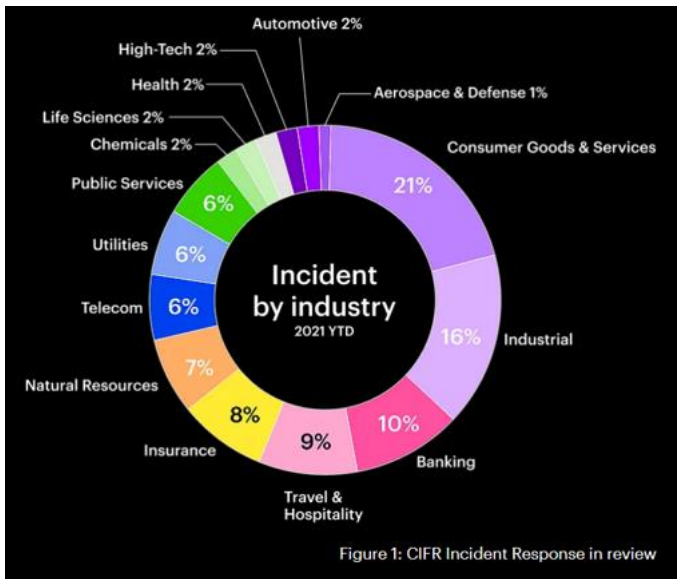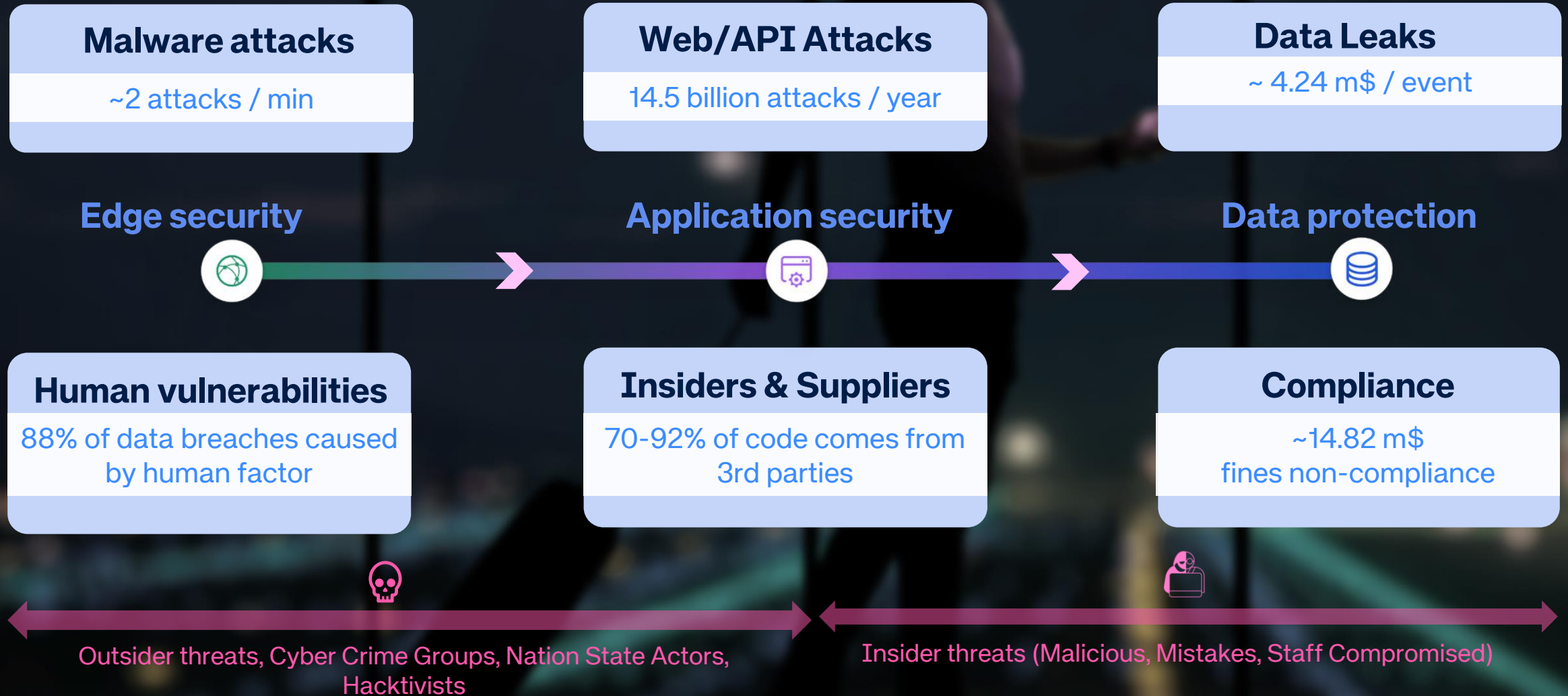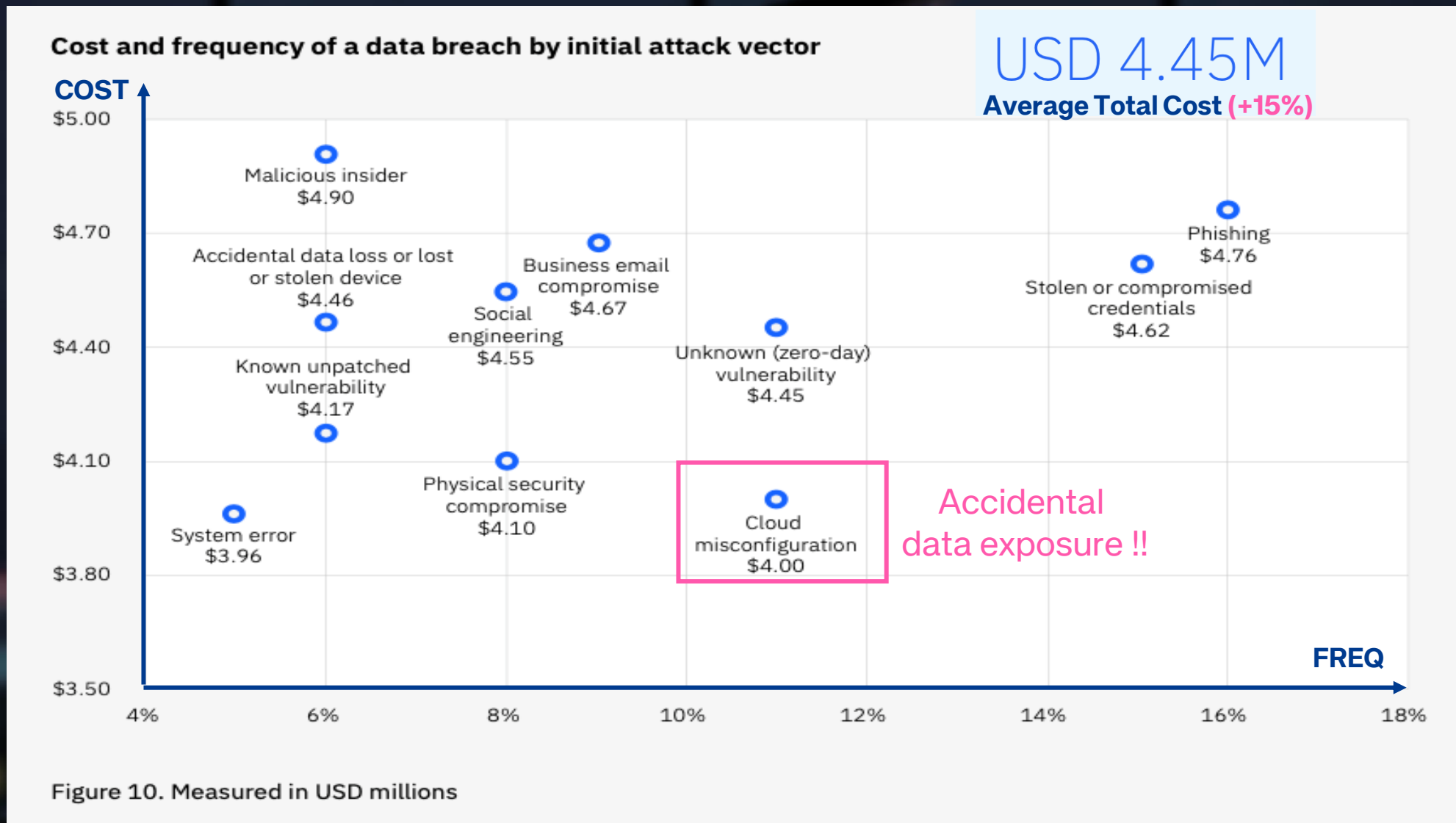

CIFR, 2021 report - Accenture

Cyber Threat Index | Cyber Security Statistics & Trends | Imperva

Travel remains one of the top industries suffering from cybercriminals

Travel Cybersecurity Risks

Malware attacks

~2 attacks / min

Web/API Attacks

14.5 billion attacks / year

Data Leaks

~ 4.24 m$ / event

Edge security

Application security

Data protection

Human vulnerabilities

88% of data breaches caused by human factor

Insiders & Suppliers

70-92% of code comes from 3rd parties

Compliance

~14.82 m$ fines non-compliance

Outsider threats, Cyber Crime Groups, Nation State Actors, Hacktivists

Insider threats (Malicious, Mistakes, Staff Compromised)

IBM Report – Cost of a Data Breach (2023)

Cost and frequency of a data breach by initial attack vector

USD 4.45M
Average Total Cost (+15%)

COST

$5.00

Malicious insider
$4.90

$4.70

Accidental data loss or lost
or stolen device
$4.46

Business email
compromise
$4.67

Social
engineering
$4.55

Phishing
$4.76

Stolen or compromised
credentials
$4.62

$4.40

Known unpatched
vulnerability
$4.17

Unknown (zero-day)
vulnerability
$4.45

$4.10

Physical security
compromise
$4.10

Accidental
data exposure !!

System error
$3.96

Cloud
misconfiguration
$4.00

$3.80

FREQ

$3.50

4%   6%   8%   10%   12%   14%   16%   18%

Figure 10. Measured in USD millions

Ransomware Payments Exceed $1 Billion in 2023 hitting a new record

Top 50 ransomware strains by median payment size and payment frequency

Note: Bubble size denotes total 2023 ransom inflows
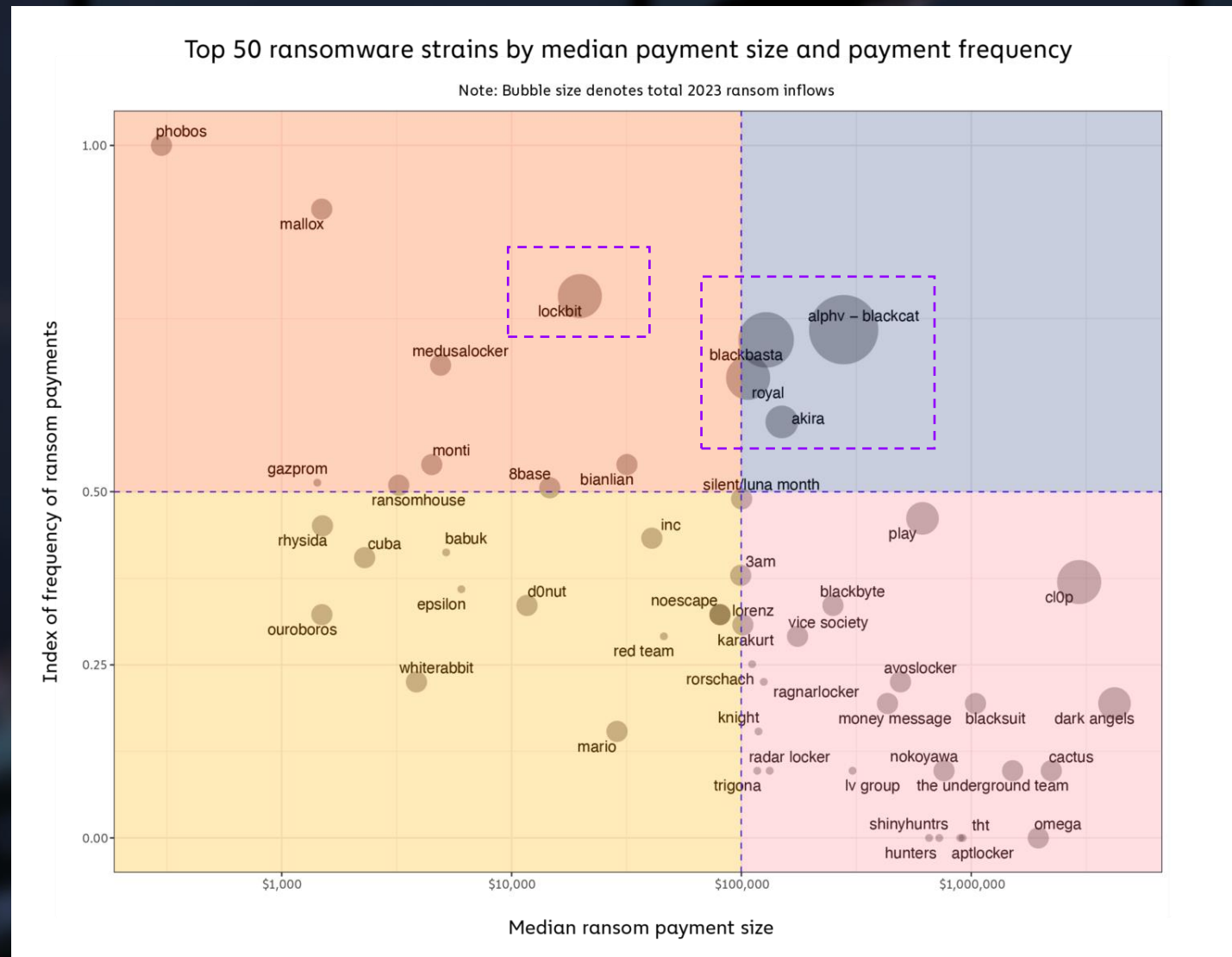
Cyber Threat is evolving

Advanced automated attacks

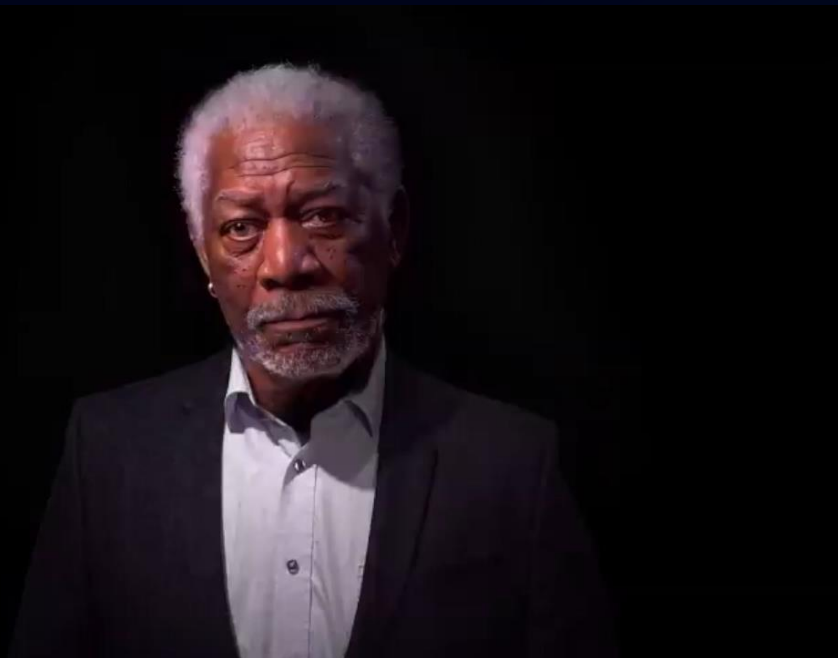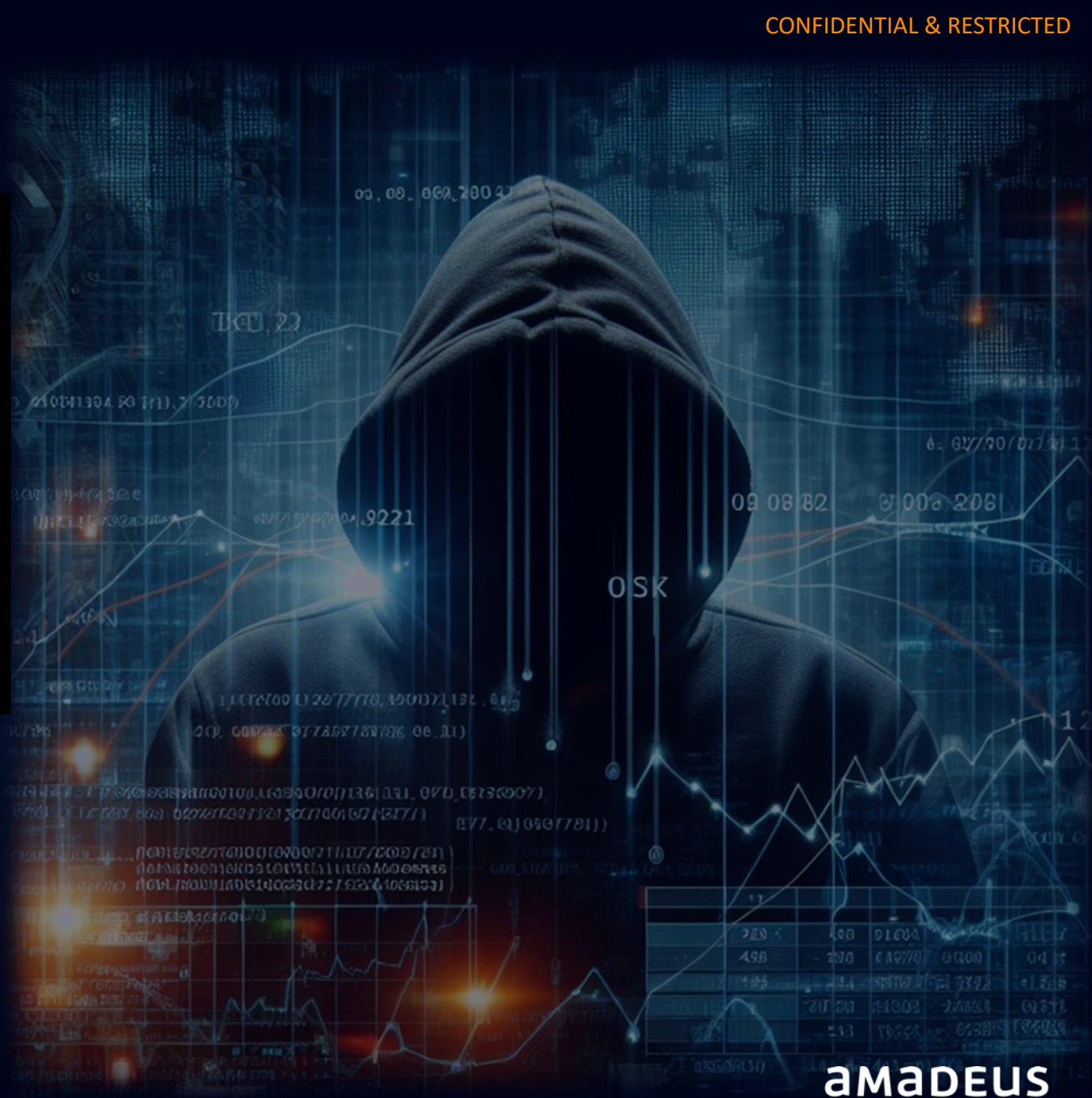Shift to functional abuse & business-logic attacks

RESIP Proxies

Sophisticated AI-based cyberattacks

amadeus

Social Engineering is evolving

Can not trust what you see!
Digital image manipulation with deep fake

aMaDEUS

AI Deepfake Teams Meeting Results in Over $25 Million Loss

February 6, 2024

The Hong Kong branch of a multinational company has lost $25.6 million (HK$200 million) after scammers using deepfake technology posed as the firm's chief financial officer (CFO) in a video conference call and ordered money transfers

aMaDEUS

https://microtime.com/ai-deepfake-teams-meeting-results-in-over-25-million-loss/

The path to Cyber-resiliency

Cyber security strategy based on business risks

Protect from fast-evolving threats

Defense-in-Depth

CYBER-ATTACK

RESILIENCY

Zero Trust Approach

Constantly review your cyber security capability

Rely on a network of experts & partners

aMaDEUS

Amadeus Cyber

Prevent adversary's success.
Continue delivering expected outcome.

Amadeus. It's how travel works more securely.

13

Leading Cybersecurity in Aviation & Travel

Covering all assets with dedicated expertise

400+

K+

184

90

81

137

1M+

30

22

Front ends

Web interfaces & APIs

People & Social Networks

Assets

Core Systems
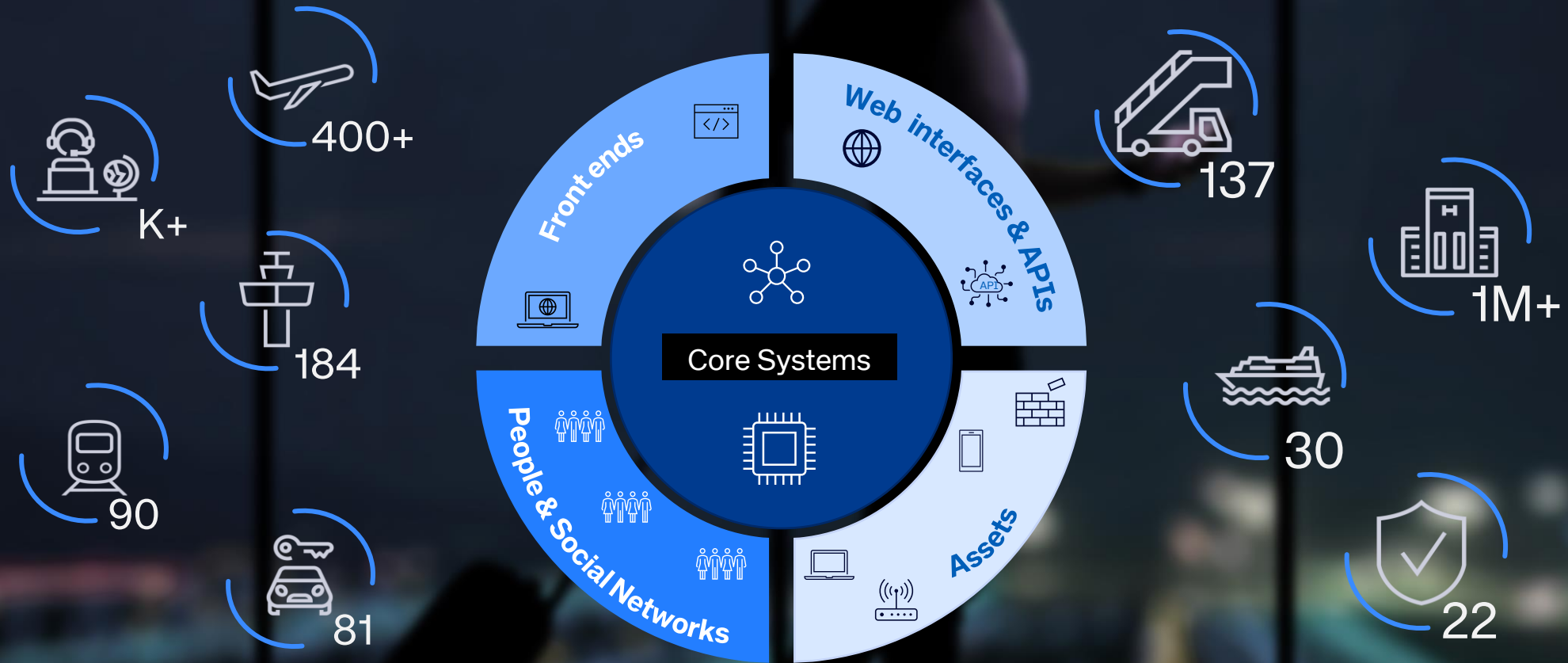
Amadeus sustainable investment

Best in class cybersecurity technology, vendor partnerships, research, awareness & training

Amadeus attack surface – #attacks per day

Covered Period: 1st Jan – 31st March 2024

14 network attacks
99.3 % blocked automatically
5 cases investigated by SOC

595 web attacks
96,8% blocked automatically
17 cases investigated by SOC

43K phishing emails reported by user
80% blocked automatically
98 cases investigated by SOC

13 malware attacks
88% blocked automatically
3 cases investigated by SOC

Network
112K IPs

Web & APIS
3.7K domains

Emails
33.5K mailboxes

Hosts
68.2K endpoints

Core Systems

2 fraud alerts
Investigated
by GSOC

CISO strategy relies on ...

Risks management

Informs >

< Reduces

Defense-in-depth approach

Drives >

< Supports

Security-by-design

Malware attacks

Web/DDoS attacks

Data leaks

Human vulnerabilities

Insiders & suppliers

Compliance

Anticipation

Prevention

Protection

Detection

Response

Align business and technology objectives.
Security-by-design for all applications and technology.

Amadeus Creation Platform

Amadeus Cloud Platform

outpayce
from amadeus

cytric easy
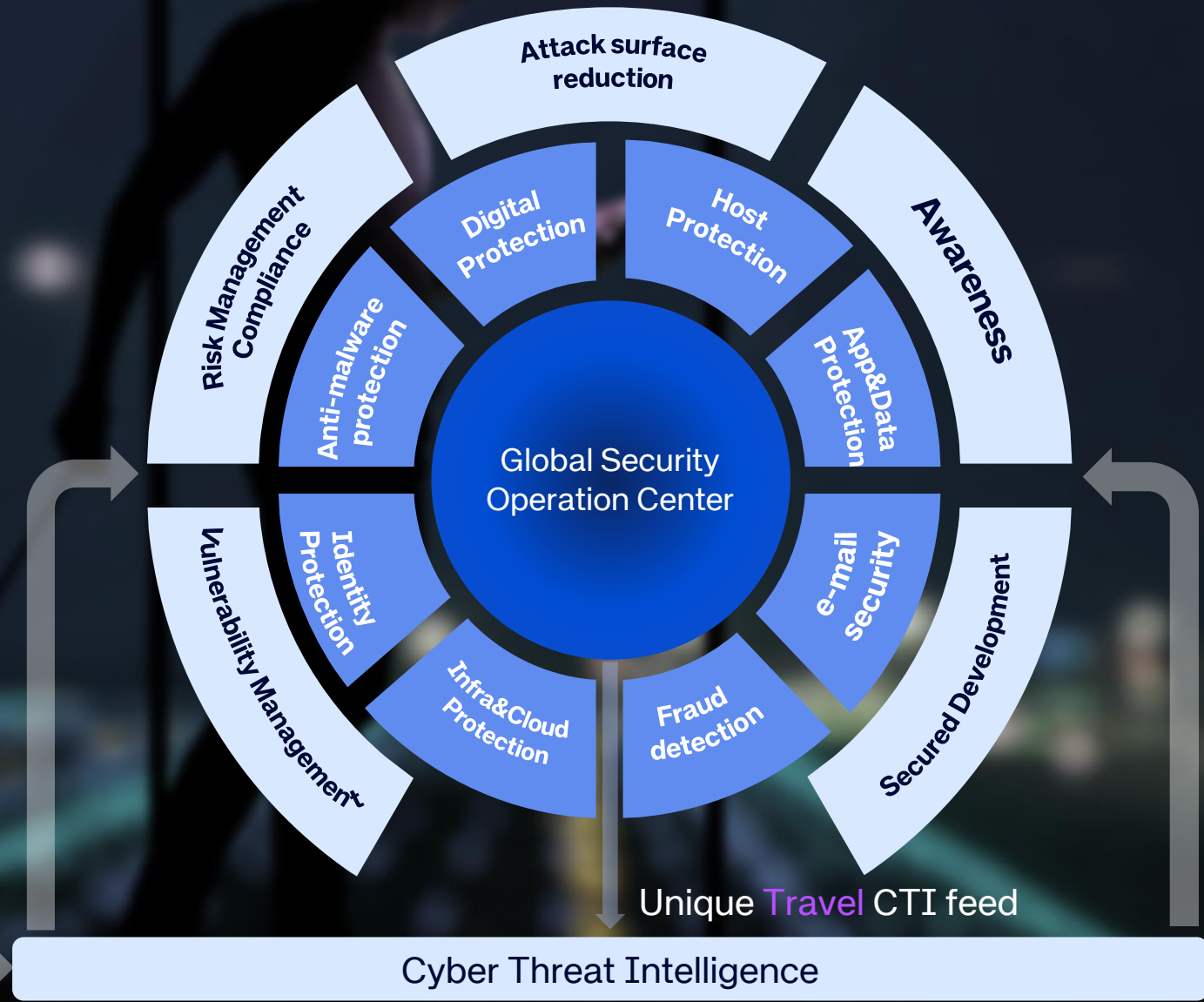
aMaDEUS
Global Security Operations

Defense-in-Depth Strategy

NIST Cybersecurity Framework

Prevention | Protection | Detection | Response

Governance (2024)

External CTI feeds

ANSSI · Prävention Detektion Reaktion · incibe cert_

EATM-CERT · AVIATION ISAC · TF-CSIRT

Attack surface reduction

Risk Management Compliance

Awareness

Digital Protection

Host Protection

Anti-malware protection

App&Data Protection

Global Security Operation Center

Vulnerability Management

Identity Protection

e-mail security

Secured Development

Infra&Cloud Protection

Fraud detection

Unique Travel CTI feed

Cyber Threat Intelligence

"Rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him"

Sun Tzu, The Art of War

"It Only Takes One ... "

aMaDEUS Across

Skylight Cyber

Security Awareness Program

Not a training, it's company culture!

Part of you ADN

Embedding cybersecurity in company culture

Educate

Make cybersecurity a good habit

Simple & fun

Keep it simple, useful, recurrent and fun.

Prise

Always rewards the progress of team members.

aMaDEUS

Security Research & Innovation

Develop the next-gen tools for cyber security

Strengthen Amadeus cyber resilience across the IT continuum

Protect Amadeus against automated threats and distributed attacks

Advanced bot detection and mitigation

Functional abuse & Business logic attack detection

Enhance our fraud detection capabilities

Cyber Threat Intelligence (CTI) for Aviation & Travel

Enhanced malware behavior analysis sandbox

Advanced anti-malware capabilities

Situational awareness on Threat Actors behaviors and strategies

Use of AI / ML in cyber security

Collaborative research projects (EU)

RESCUE CONCORD Research proposals

aMaDEUS

Cybersecurity Services

Extending our reach to protect our customers

aMaDEUS
Global Security Operations

Amadeus. It's how travel works better.

Amadeus Cybersecurity Offer
Towards a consolidated view

Complexity

Gaps in coverage

Increased Attack Surface

Incident response & resolution

Increased Cost

Current protection state

Front ends

Web interfaces & APIs

Core Systems

People & Social Networks

Assets

Target protection state

Front ends

Web interfaces & APIs

Core Systems

People & Social Networks

Assets

Simplicity & Ease of Management

Integrated solutions & regularly assessed

Holistic view of security posture

Faster Incident Response

Scalability

MODULAR MANAGED SERVICES
Managing **Operations** through tailored solutions & travel expertise

Amadeus. It's how travel works more securely.

Amadeus, the right partner
Supporting our customers

Experts in Travel	**We come from experience**	**Our People**	**Reliable**
Industry leaders in Technology	Technical & Functional expertise	Proximity & Engagement	We deliver

Amadeus Cybersecurity Offer

Preventive & proactive solutions

ASSESS

- Black box Assessment
- Cybersecurity uplift
- Cyber strategy
- BAS & CART

PREPARE

- Digital Protection
- Host Protection
- Fraud Protection
- Asset Management
- Vulnerability Management
- Information Protection
- Infrastructure Security

OPERATE

- Cyber Threat Intelligence
- SOC Services
- Awareness Program
- Threat Management
- Penetration testing
- Cloud Security

RESOLVE

- Incident Response
- Incident Recovery
- Crisis Management
- Forensics
- Travel Cyberconsultancy

Customer support 24x7x365

Amadeus cybersecurity journey

It's how travel works more securely.

Define Strategy
Assess & understand risks

2 Digital Protection
Bots' risks..

1 Host Protection
Ransomware and Data leaks risks

4 CISO organization
Strategy & organization
Frameworks, policies & processes

3 Awareness Program
Phishing risk

6 CTI (Cyber Threat Intelligence)
Prevention processes

5 SOC
Central Datalake and cyber defense coordination

7 Protection components
New components to integrate with SOC (network, ...)

8 Independent assessments
Assess to evolve

9 Advanced travel specific features
Fraud, seat spinning, Residential IPs...)

Thank you