



Hello, We are

Aegis

December 2023



Cyber Resilience in Today's World

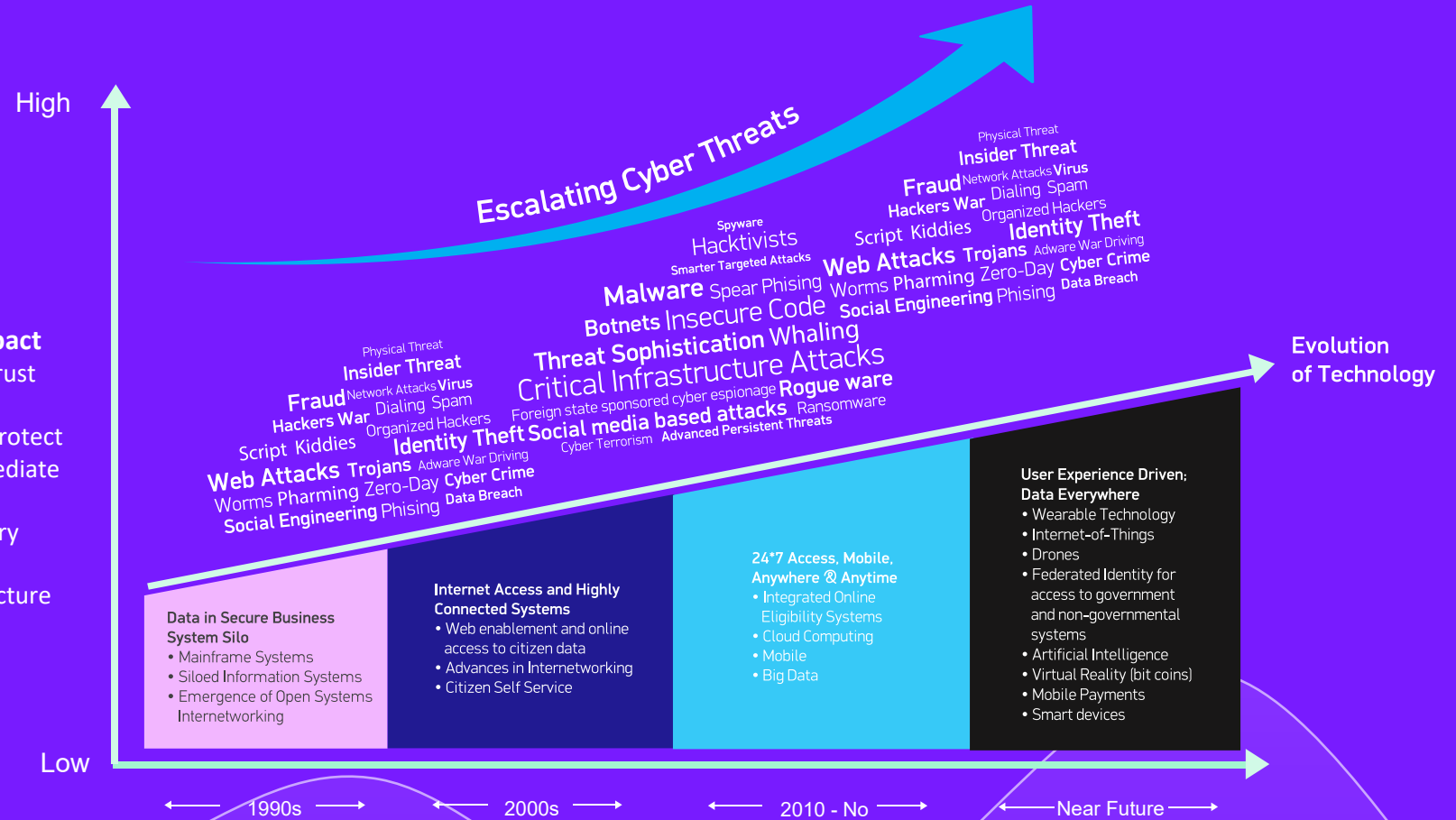
Are security tools & services enough?



Changing Threat Landscape

Increasing Business Impact

- Citizen Trust Impact
- Cost to protect and remediate
- Legal / Regulatory
- Critical Infrastructure



01 

SUPPLY CHAIN ATTACKS

The compromise of third party software and managed services.

02 

ADVANCED DISINFORMATION

Deepfake attack for political or monetary gains.

03 

DIGITAL SURVEILLANCE

Facial recognition and biometric data targeted by criminal groups.

04 

CYBER-PSYCHICAL HUMAN ERRORS

The fast retrofit of industrial systems lead to security issues.

05 

IOT-ENABLED ADVANCED ATTACKS

Sophisticated attacks tailored from IOT data abuse.

06 

SPACE-BASED INFRASTRUCTURE

The public-private infrastructure model is weakly secure.

07 

ADVANCED HYBRID THREAT

The combination of physical, offline and online attacks.

08 


SKILL SHORTAGE

Lack of understanding and competencies increase the gap to fight cybercriminals.

09 

TELCO AS SINGLE POINT OF FAILURE

Telco, connecting everything, can be weaponized by adversaries

10 

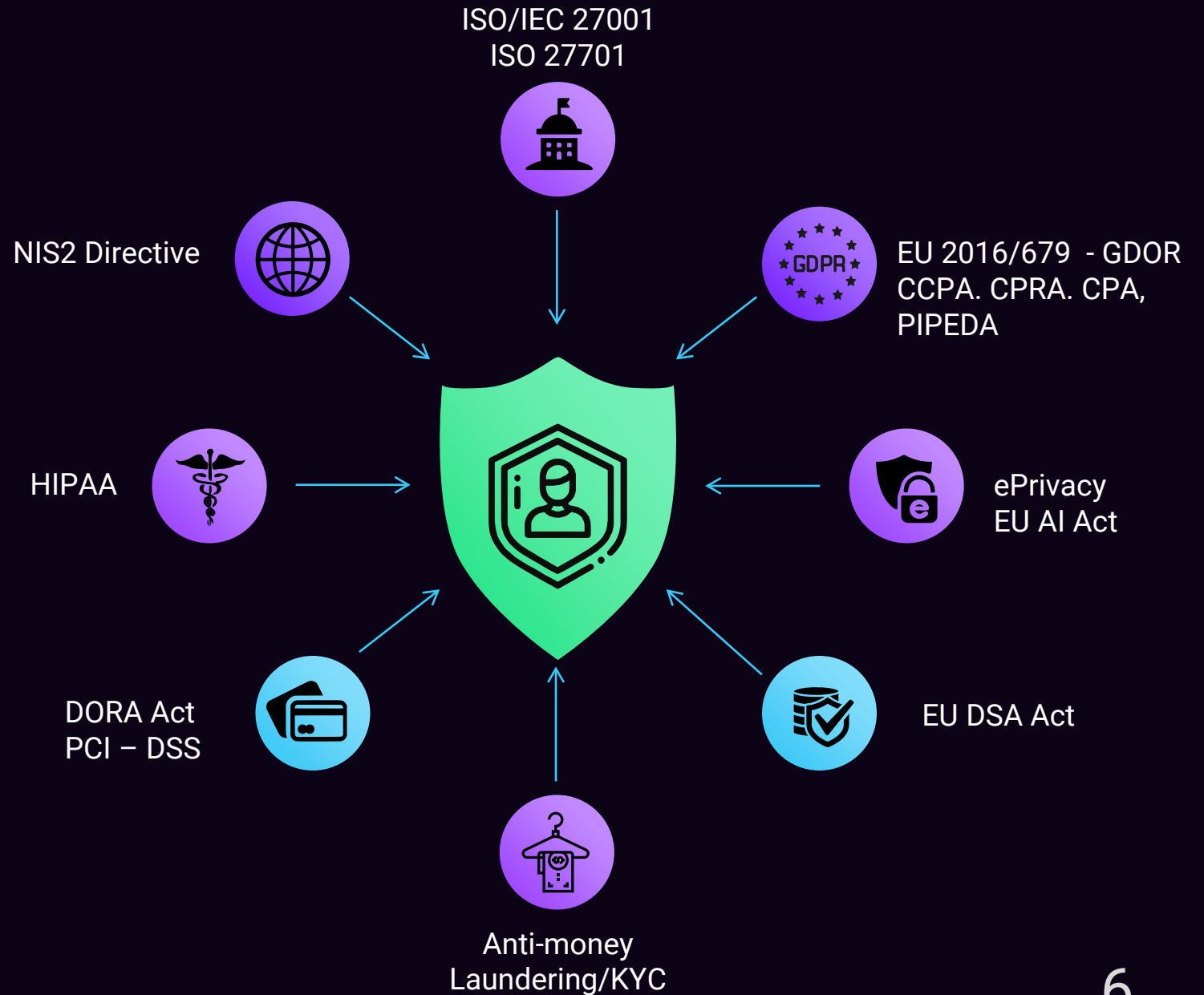
ARTIFICIAL INTELLIGENCE ABUSE

Manipulation of AI to enhance malicious operations.

Top 10 Cyber Threats by 2030



Evolving Regulatory Environment





REGULATION (EU) 2019/881 on Cybersecurity Act (CSA)

Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.

Directive NIS2 (EU) 2022/2555

Sets cybersecurity measures on entities falling under critical infrastructure sectors

DORA (Digital Operational Resilience Act) – Financial sector Regulation (EU) 2022/2554

Ensures that financial entities in EU remain resilient through a severe operational disruption

Cyber Resilience Act (proposal)

Use of EU cybersecurity certifications and rules to ensure more secure hardware and software products.



RED - radio equipment directive 2014/53/EUEN

Establishes a framework for placing radio equipment on market and subjects certain categories of radio equipment to increased level of cybersecurity, personal data protection and privacy.

Directive CER (EU) 2022/2557 (Resilience of critical entities)

strengthens the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage.

Directive (EU) 2019/1937 on Whistle-blower Reports of violations of NIS requirements

Regulation (EU) 2021/887 ECCC (Network of National Coordination Centres)
Boosts research excellence and the competitiveness of the Union in the field of cybersecurity.

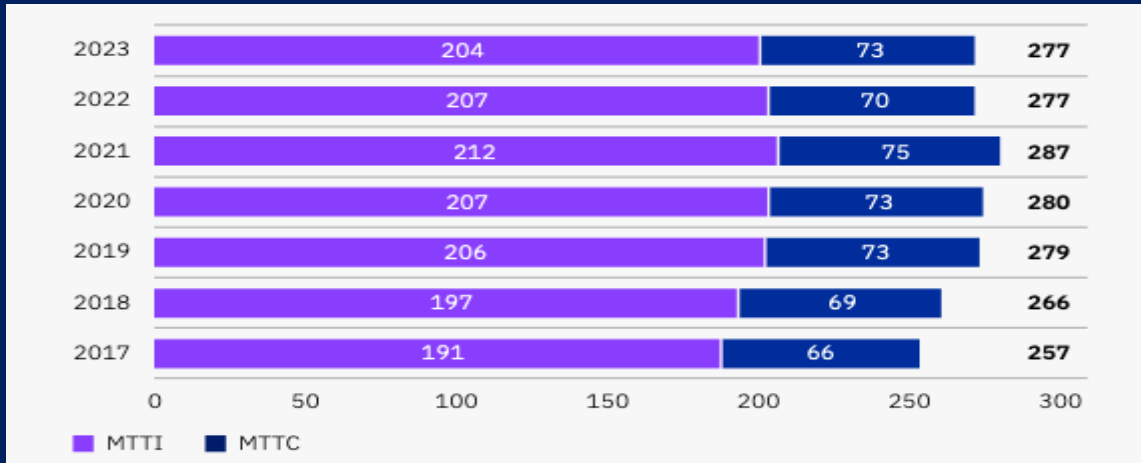
Cyber Security Regulations in EU



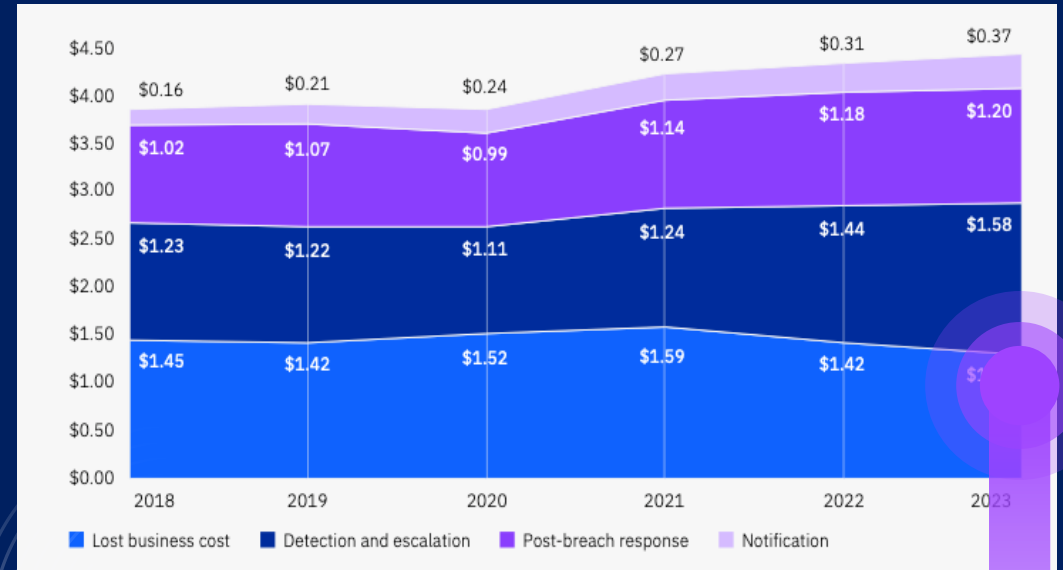
Total cost of a data breach (USD)



Per-record cost of a data breach (USD)

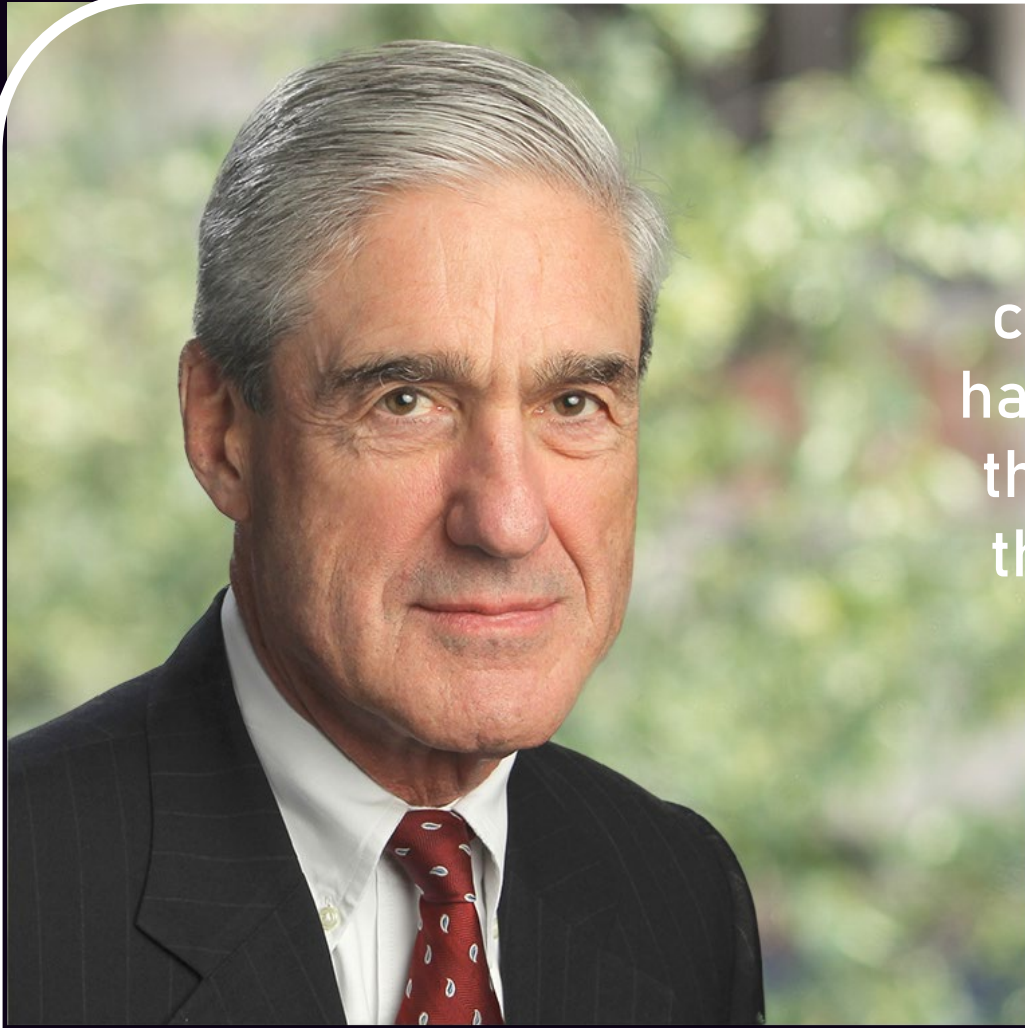


Time to identify and contain the breach (days)



Cost of a data breach divided into four cost segments (USD Millions)

Data Breach Cost



There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.

Robert S. Mueller

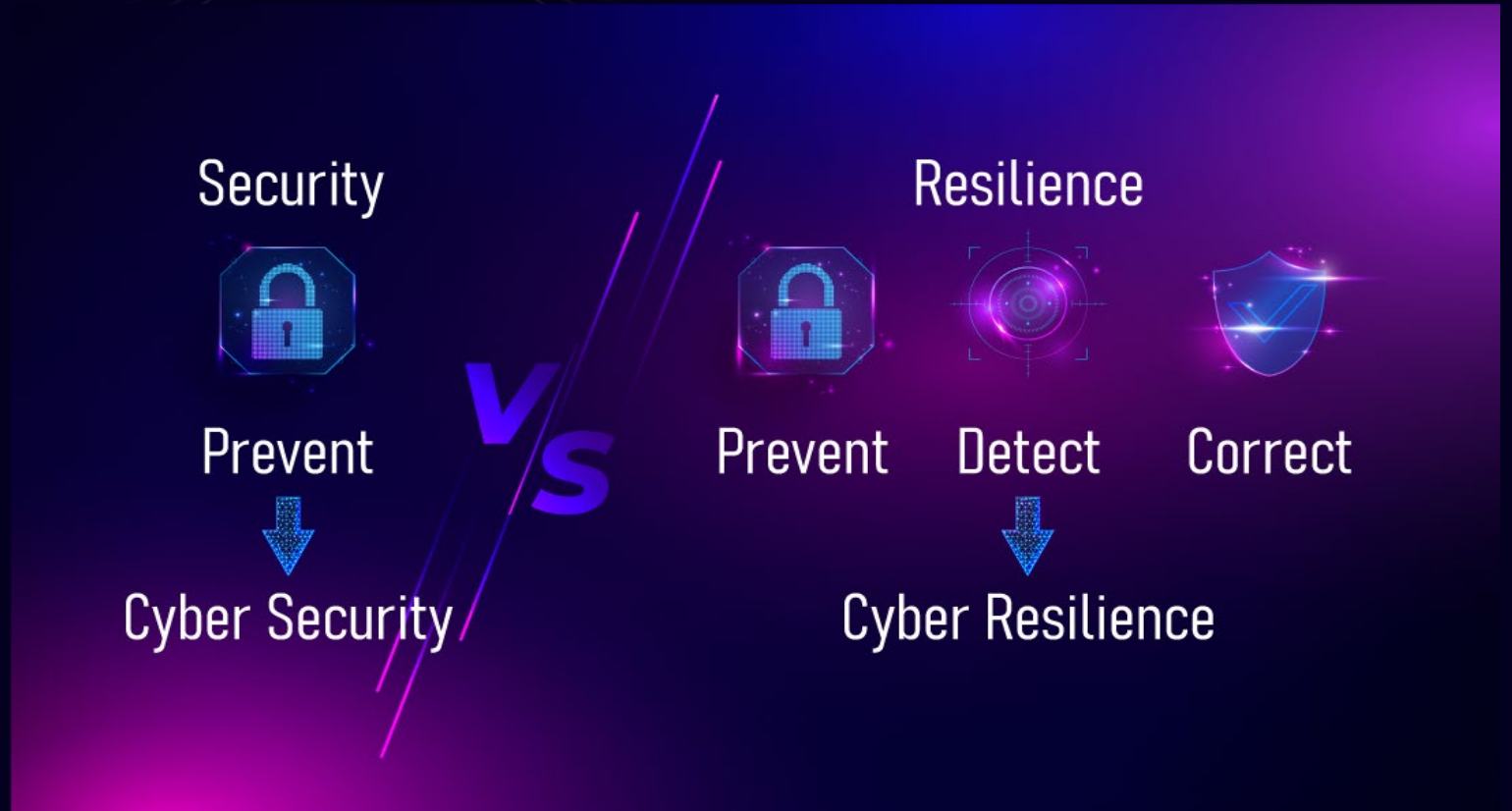


Cyber Security at its "Excellent"



CYBER RESILIENCE

Cyber Resilience is actually a mind shift






Cyber Resiliency Processes



Cyber Resiliency Strategy



Cyber Resiliency
Strategy need a
Cyber Security
Leader

3.999.964

+12.6% YoY*

NORTH AMERICA

521.827

+19.7%

EUROPE

347.761

+9.7%

ASIA-PACIFIC

2.670.316

+23.4%

LATIN AMERICA

348.259

-32.5%

MIDDLE EAST & AFRICA

111.801

-7.1%

*2023 gap includes 4 new countries - United Arab Emirates, Saudi Arabia, Nigeria and South Africa.
YoY growth are based on back estimates for those countries for 2022.

Lack of expertise



Speak Technical Jargon



Speak Business



Does he exist?



How to move forward?



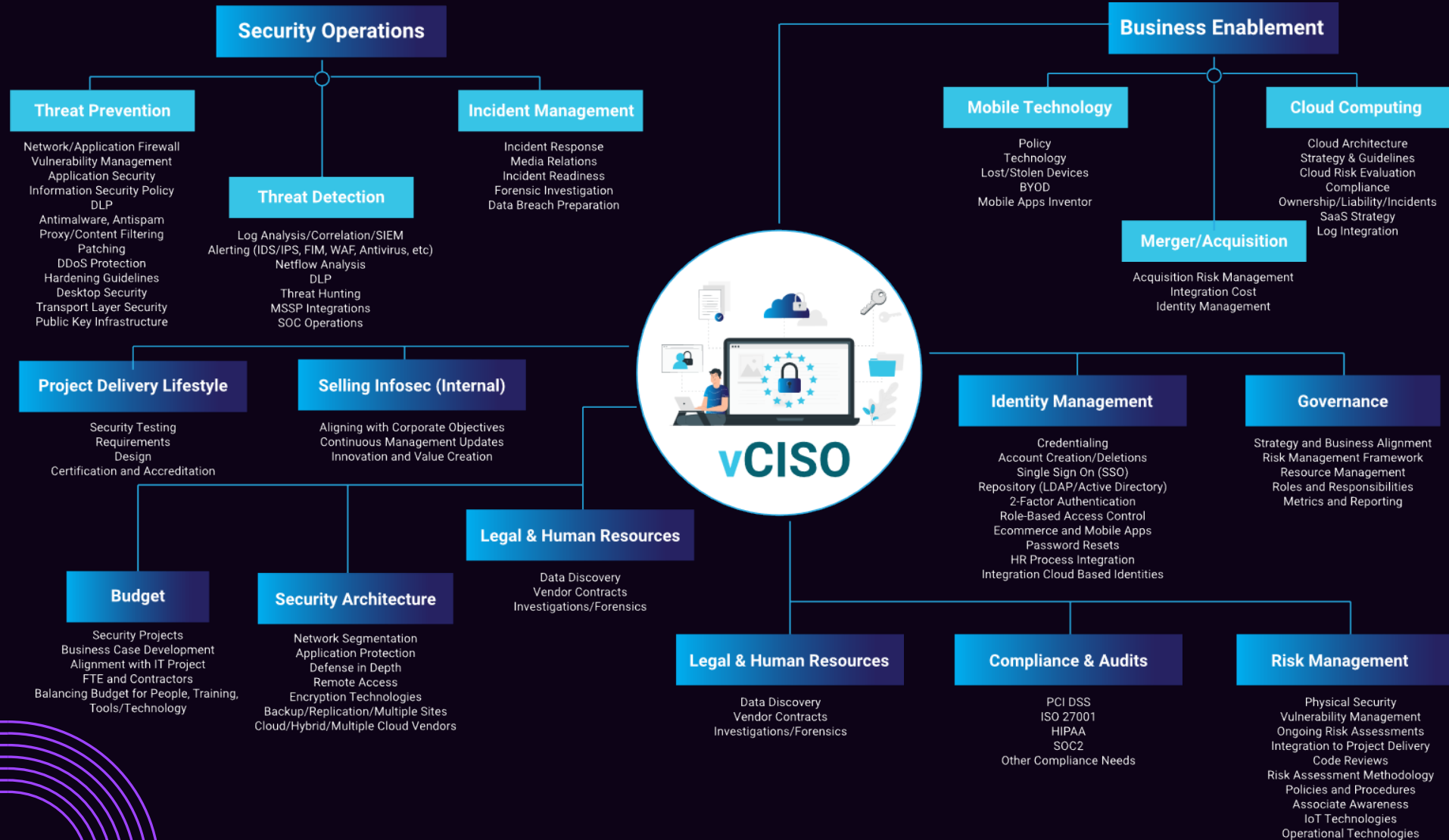
- Information security program leadership
- Security policy, process, procedure, guidelines & best practices development
- Governance and Compliance
- Aligning business strategy with security
- Security Point-of-Contact for All Issues
- Security architecture and design
- Planning Security assessments, penetration testing and risk assessments
- Security training and awareness
- Incident response planning
- Identity & Access Management
- Personnel Security and Training
- High-level cost estimates for budgetary purposes
- Project planning and execution

AegIS Cyber Security CISO as a Service / vCISO



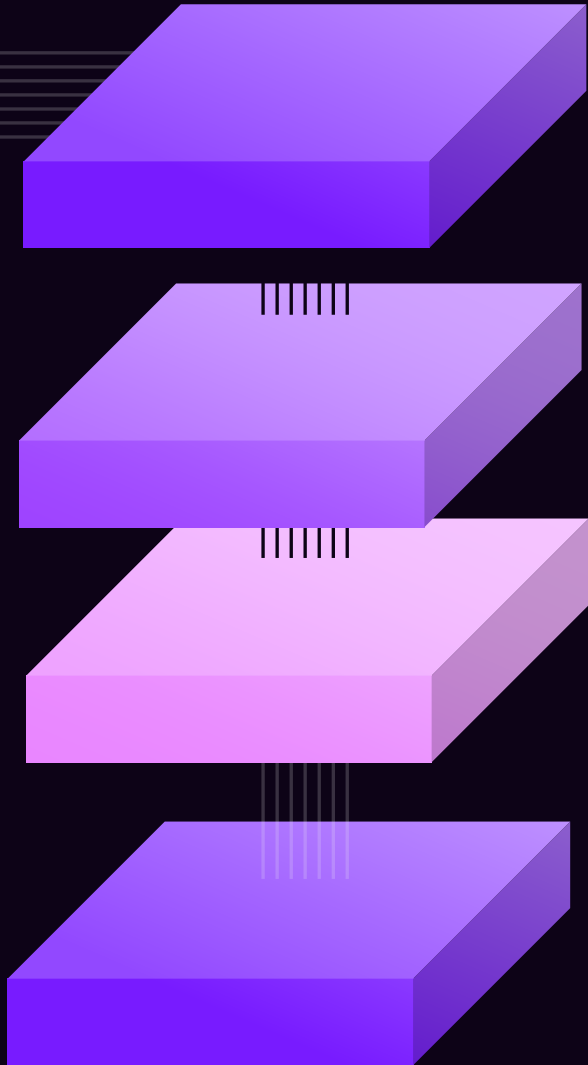


Overview & Responsibilities





vCISO Offering



Pay as you go model



Subscription model

- Bronze
- Gold
- Platinum



Project / Task based model



Custom offering model



Who We Are

- We are your strategic trusted advisor
- Our biggest aim is to empower companies to stand strong in the face of today's dynamic, sophisticated, and unrelenting cyber-attacks and maintain business continuity and financial stability
- Get all benefits of working with cyber security recognized professionals. We are always ahead of the curve in the cyber security industry.
- Forget about headaches caused by manual research through the industry. Just involve us in the project and spectate how magic goes on.

01

Recognized

Working with the best technology partners and customers. Our professionalism is confirmed by experts

02

Trusted

Chosen by world industries' leaders – Our clients include some of the most successful private equity companies worldwide. We protect companies, which are trusted by the whole world

03

Awarded

Awards that everyone would be proud of – Our team members have got numerous awards and recognitions for cybersecurity consulting and managed cybersecurity services in all of the top categories



Thank You



aegis-cs.eu



info@aegis-cs.eu