AAM has a stable background in the industry and presence in the region

International team

- Budapest
- Sofia
- Belgrade
- Bucurest

25 Years of Excellence

- 65+ Countries
- 3500+ Successful Projects

Basic Pillars

Management Consulting

- Strategic project management and consulting
- Project & program management
- Enterprise Mobility
- Project audit and quality control
- Organizational operation and project culture development
- Business Process Management
- Management of tenders and European Union projects
- Selection and procurement

IT System development

- IT system and application development

IT Consulting & Management

- IT strategy and management
- Business applications
- Test management
- Migration coordination and roll-out management
- IT security, risk analysis and management

Information Security Consulting

- Information security frameworks, preparation for certification
- Mobile application security
- Data Leakage Prevention (DLP)
- BCP and DRP
- Log management (SIEM)
- Identity Management (IdM) / User administration
- GDPR, Data Protection

Public administration | Finance | Telco and media | Energy | Transport and industry | Health and education

AAM CONSULTING

Roles, which we often fill:

Program manager

Project manager

Business analyst

Process expert

Test manager

Data migration coordinator

IT security auditor

A D V A N C E T O G E T H E R

Social responsibility

AAM Management

Information Consulting Ltd.

AAM Core Values

AAM CONSULTING

Equal opportunities at AAM

At AAM one of our core values is Fairness and ethics.

We provide fair and unbiased treatment in the Workplace regarding salary, training opportunities, promotion and we highly value equity and diversity bringing unique perspectives and capabilities, enhancing business success.

The gender ratio in our company is around 50-50%

In the core management there is one lady, next to 5 gentlemen, but in the wider circle of leadership there are another 3 ladies.

The age of our colleagues is between 20 – 71 years old.

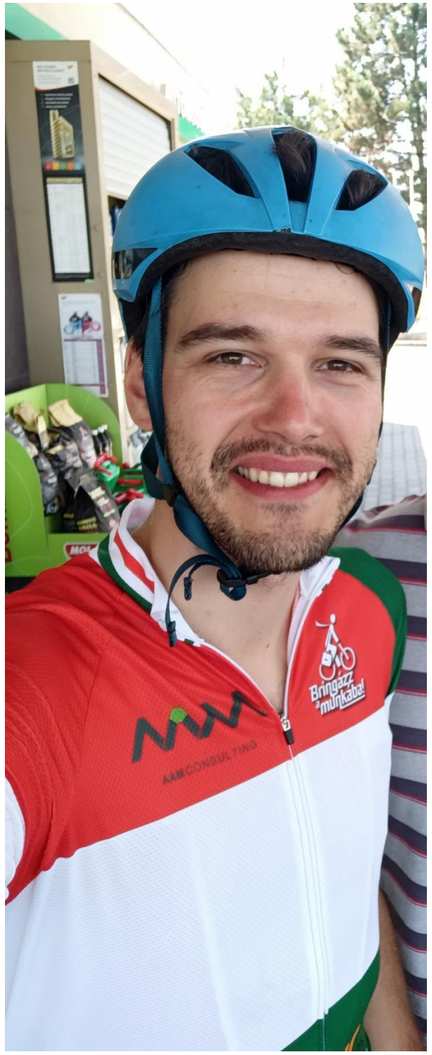
AAMCONSULTING

Environmental Sustainability at AAM

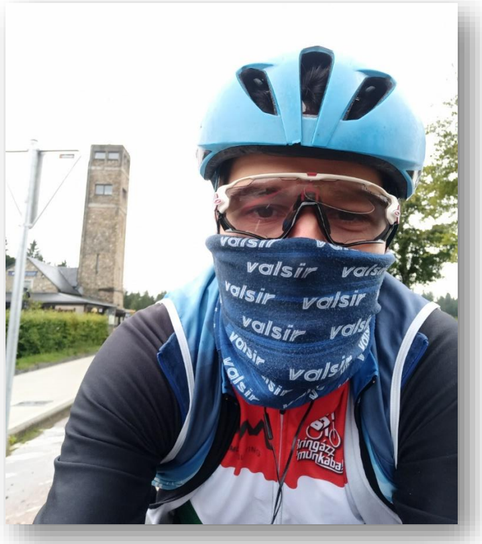
1. Implementing eco-friendly practices
2. Reducing carbon footprint
3. Conserving energy and water resources
4. Recycling and waste management programs
5. Providing a safe and healthy working environment

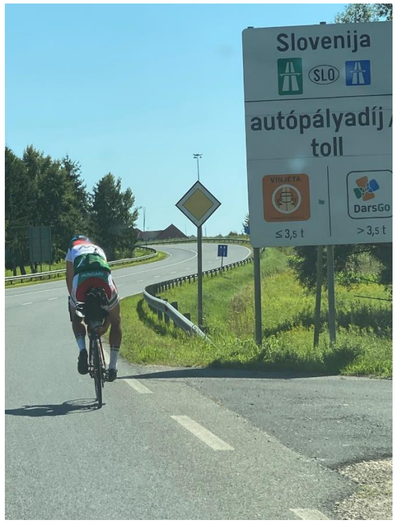
Environmental responsibility – AAM colleague Zoltán Ruttkay's WR attempt

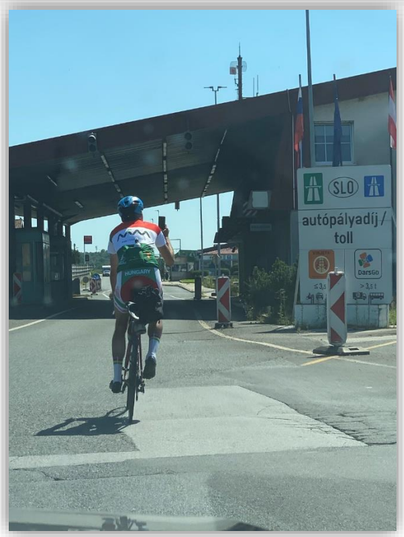
AAM CONSULTING



AAM's colleague Zoltán Ruttkay attempted a cycling world record crossing the most countries possible in a week. He started his ride through Europe in the Netherands and finished his journey in Romania!







ADVANCE TOGETHER

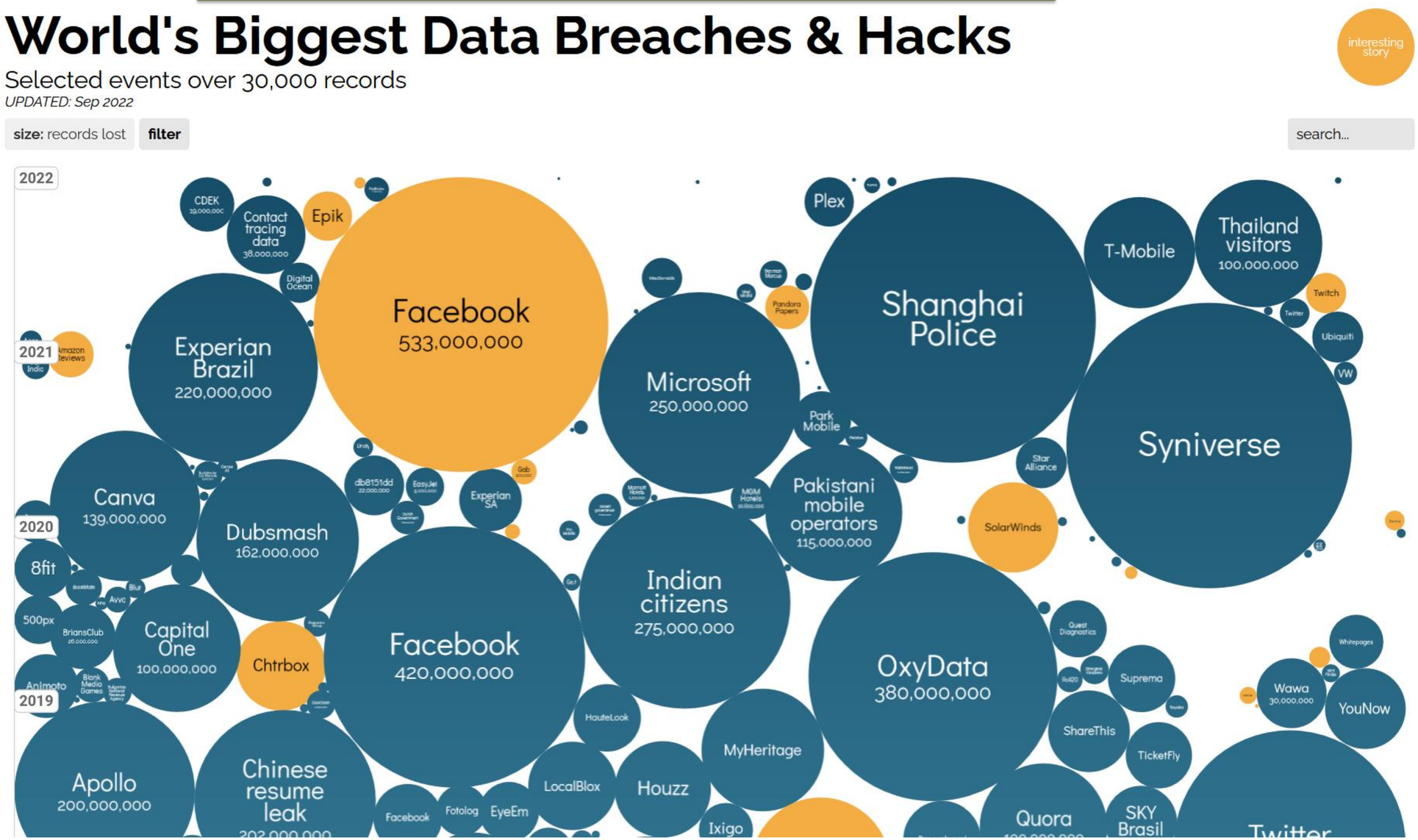
IT Security trends

Risk and Compliance

Gergely Nagy

2024. 01.10.

Data Breaches and Hacks

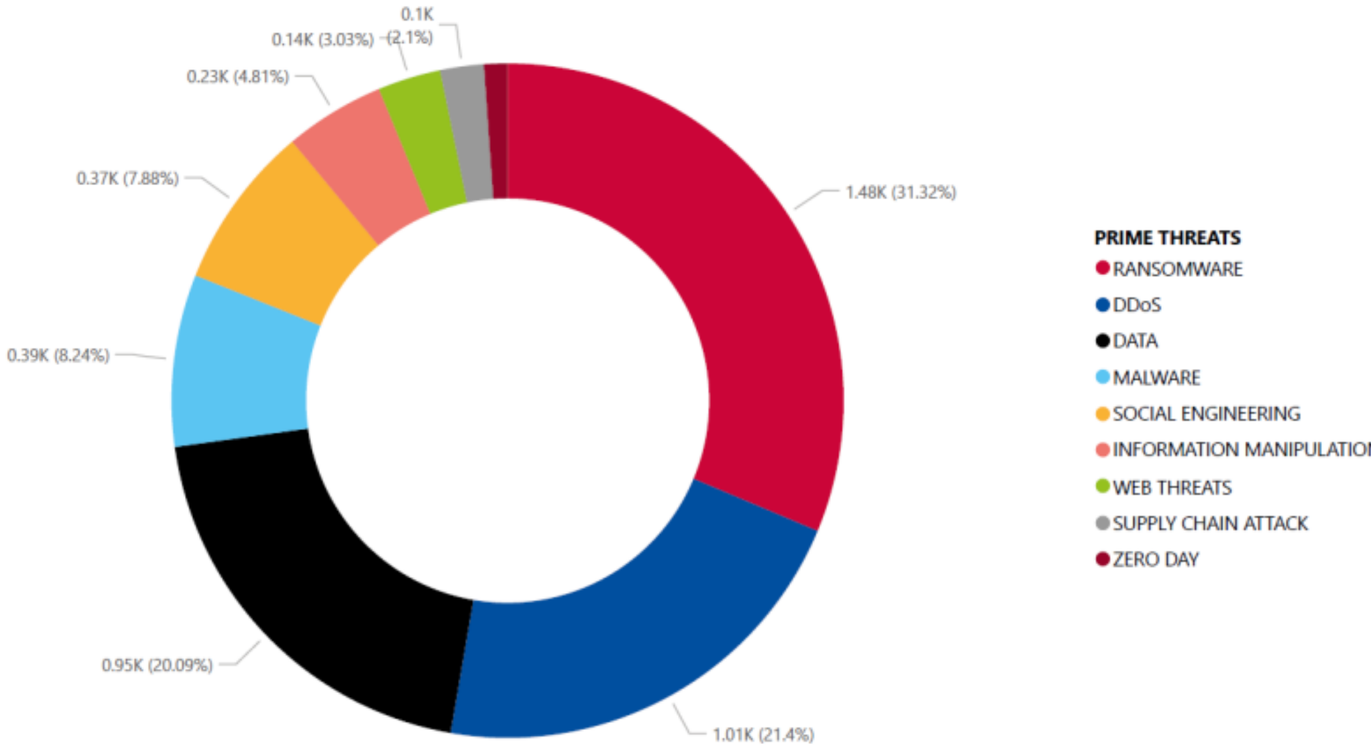


ADVANCE TOGETHER

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Threat landscape

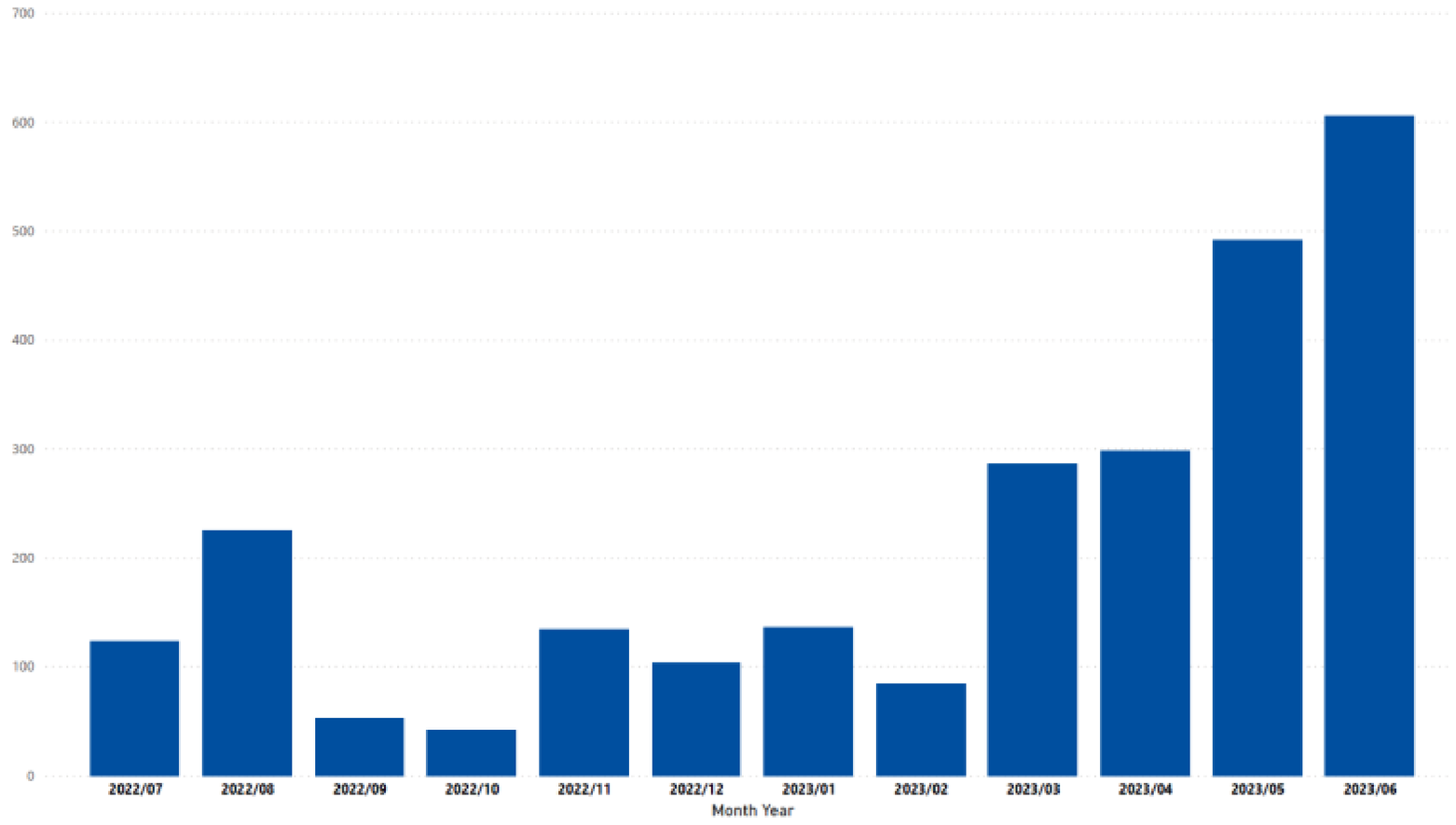
Figure 2: Breakdown of analysed incidents by threat type (July 2022 till June 2023)



Source: ENISA Threat Landscape 2023, 2023 October

Timeline of EU events (incidents per month)

Figure 4: Timeline of EU events (count of number of observed incidents per month)

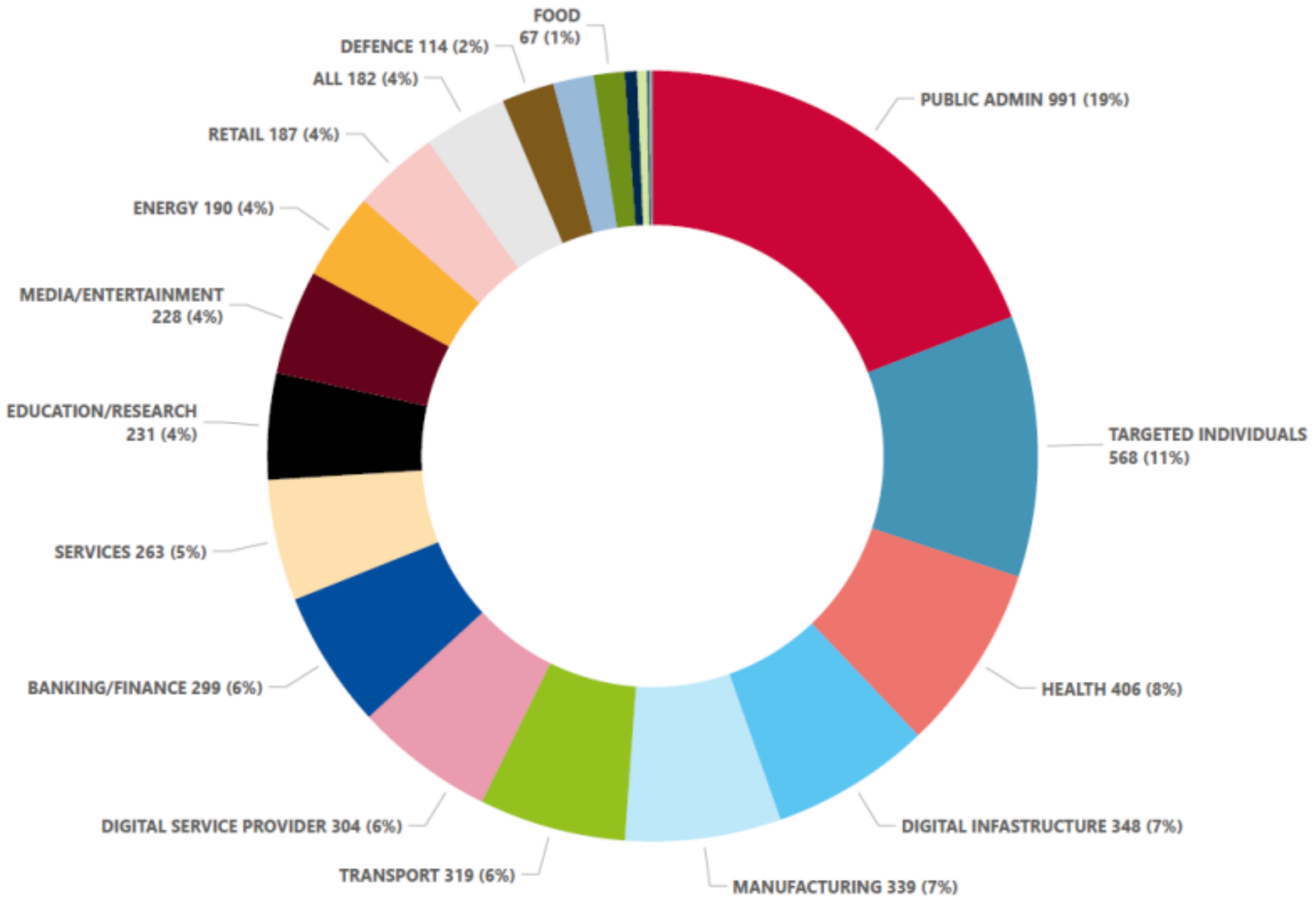


ADVANCE TOGETHER

Source: ENISA Threat Landscape 2023, 2023 October

Targeted sectors

Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)

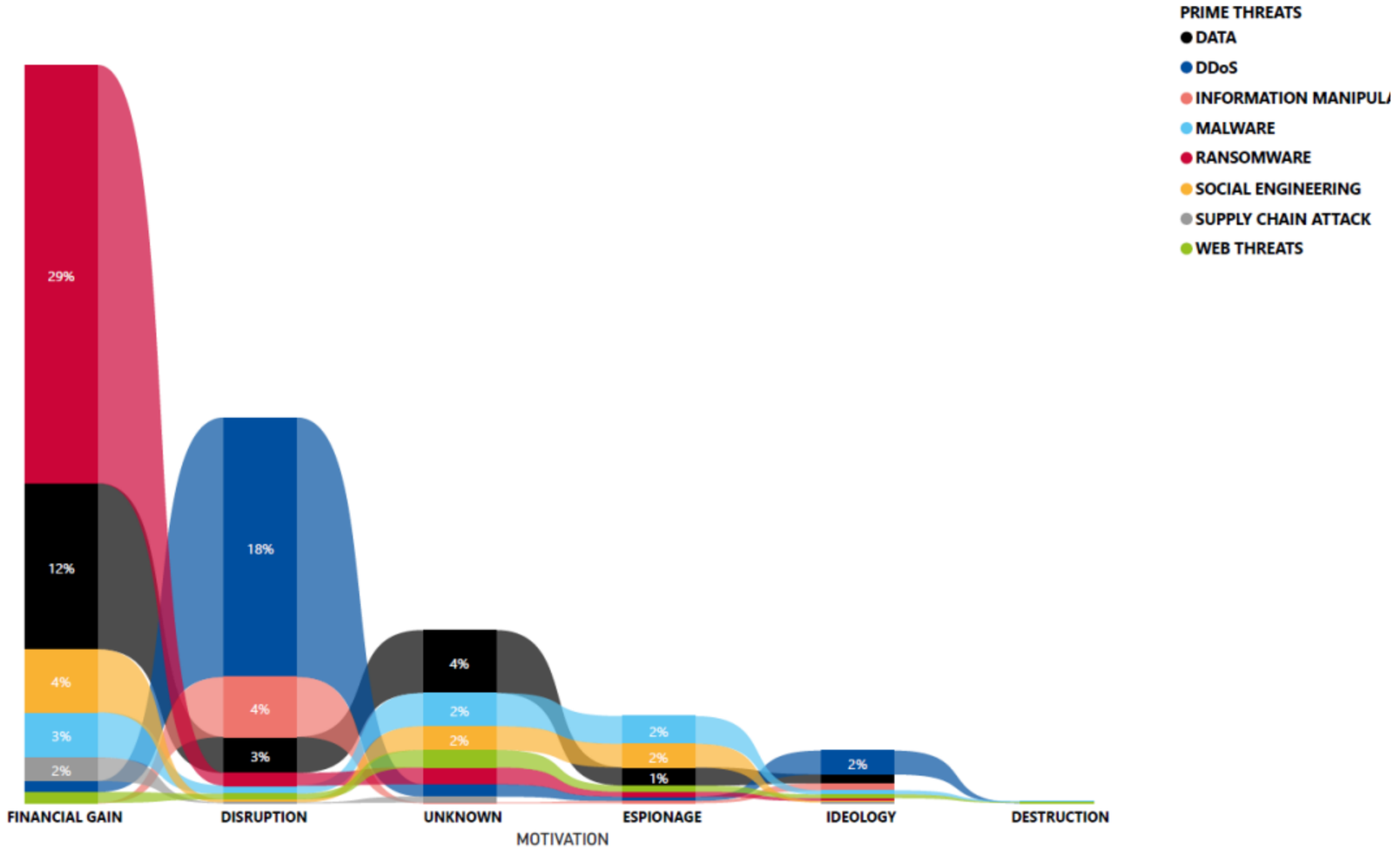


A D V A N C E T O G E T H E R

Source: ENISA Threat Landscape 2023, 2023 October

Motivation of attackers

Figure 10: Motivation of threat actors per threat category

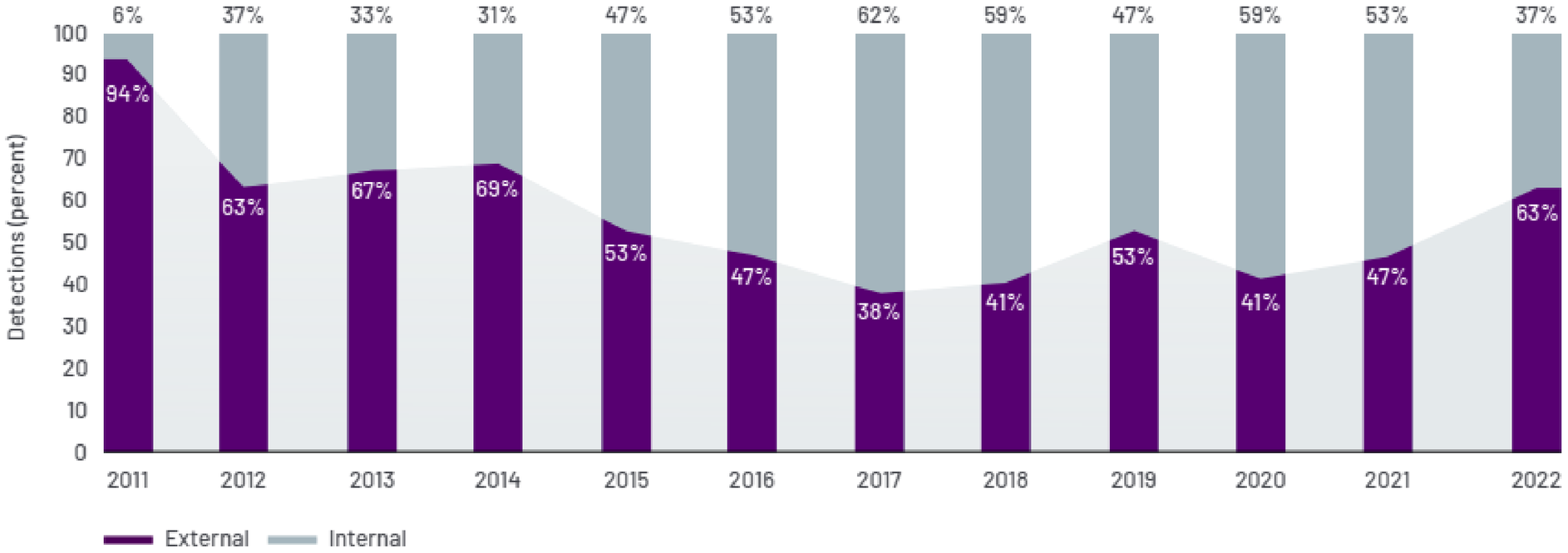


A D V A N C E T O G E T H E R

Source: ENISA Threat Landscape 2023, 2023 October

Detection Source

Detection by Source, 2011-2022



Internal detection is when an organization independently discovers it has been compromised.

External detection is when an outside entity informs an organization it has been compromised.

A D V A N C E T O G E T H E R

Source: M-Trends 2023 Mandiant Special Report

Trends

- **DDoS and ransomware rank the highest among the prime threats**, with social engineering, data related threats, information manipulation, supply chain, and malware following
- **Finanical gain has been the most common motivation of attackers**
- **Nearly all sectors have been targets of attacks**
- **A noticeable rise was observed in threat actors professionalizing their as-a-Service programs**, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extort them, advancing their illicit enterprises.
- **The Invasion of Ukraine:** Russia's invasion of Ukraine has evolved as nearly the sole driver of cyber threat activity from Russia
- **North Korean Financial Operations:** For years, North Korea has reportedly conducted various illicit financial activities to fund the regime.

  The explosive growth of cryptocurrency is converging with aggressive and flexible North Korean cyber capabilities, making it natural that at least some North Korean threat groups would expand operations into this sector.
- **Social engineering attacks grew significantly in 2023 with Artificial Intelligence (AI)** and new types of techniques emerging, but phishing still remains the top attack vector.
- **Non-English phishing attacks** are becoming more refined with **Artificial Intelligence (AI) aided translation**

Sources: M-Trends 2023 Mandiant Special Report ENISA Threat Landscape 2023, other sources

EU Legislation- Cybersecurity

	DORA (Digital Operational Resilience Act)	NIS2 (Network and Information Systems Directive 2022/2555)	Cyber Resilience Act
Who does it apply to?	Financial sector	Certain Crtitical companies	Products with digital elements
Type	EU Act (Applies directly in all member states)	EU Directive (Local implementation is neccessary by each member state)	EU Act - Draft
Deadlines	2025 January	Local regulations will need to be created by 2024. october 17th (which will set the local deadline)	T + 24 month
Possible Sanctions	National authorities will determine sanctions	10M / 7M EUR Annual turnover 2% / 1,4 %	10M EUR 2% of annual turnover

Conclusion

Both the **threat landscape** and **compliance motivates** companies to **manage cybersecurity risks**

The **defense** against the threats **should be based on risk**

Many incidents are **no longer the sole problem of a single company** (supply chain, partner companies, etc…)

Compliance mandates are also moving towards **ecosystem level requirements**

We believe **security** can be a **business enabler**

Our references in Bulgaria in the field of IT Security

AAM Bulgaria has build a reputation as IT Security Consultant in the Financial sector and beyond

Allianz

ОББ
Част от KBC Груп

банкаДСК
otp group

Fibank
Първа инвестиционна банка

БАЕЗ | BAEZ

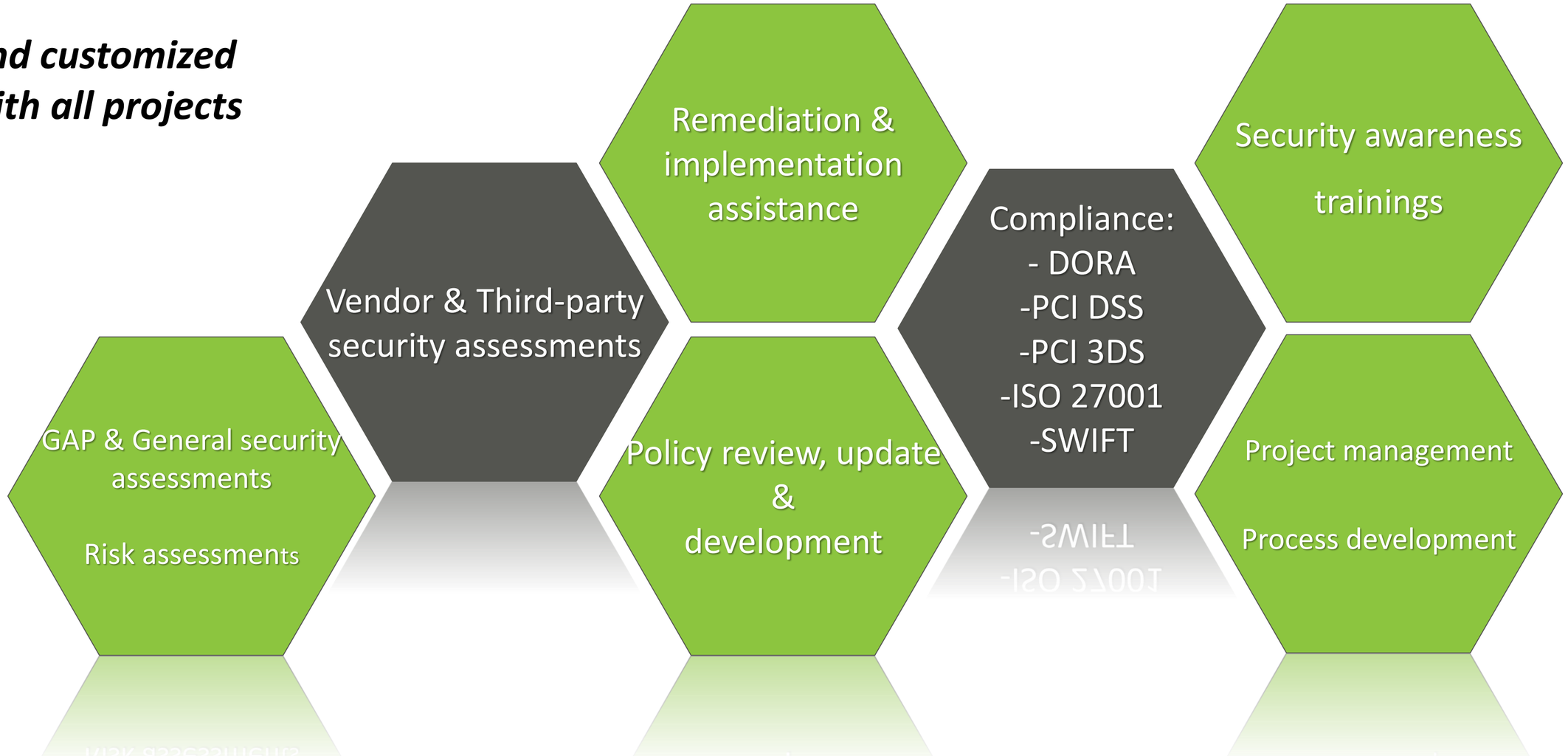
Райффайзен БАНК

DISCORDIA

ISACA
Sofia Chapter

Areas of competence and services that AAM can deliver

Flexibility and customized approach with all projects



Thank you for your attention!

https://aamconsulting.bg/

aam@aamconsulting.bg

ivo.nikolov@aamconsulting.bg

+359 883 22 54 77