Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Why the Cyber Resilience Act?

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

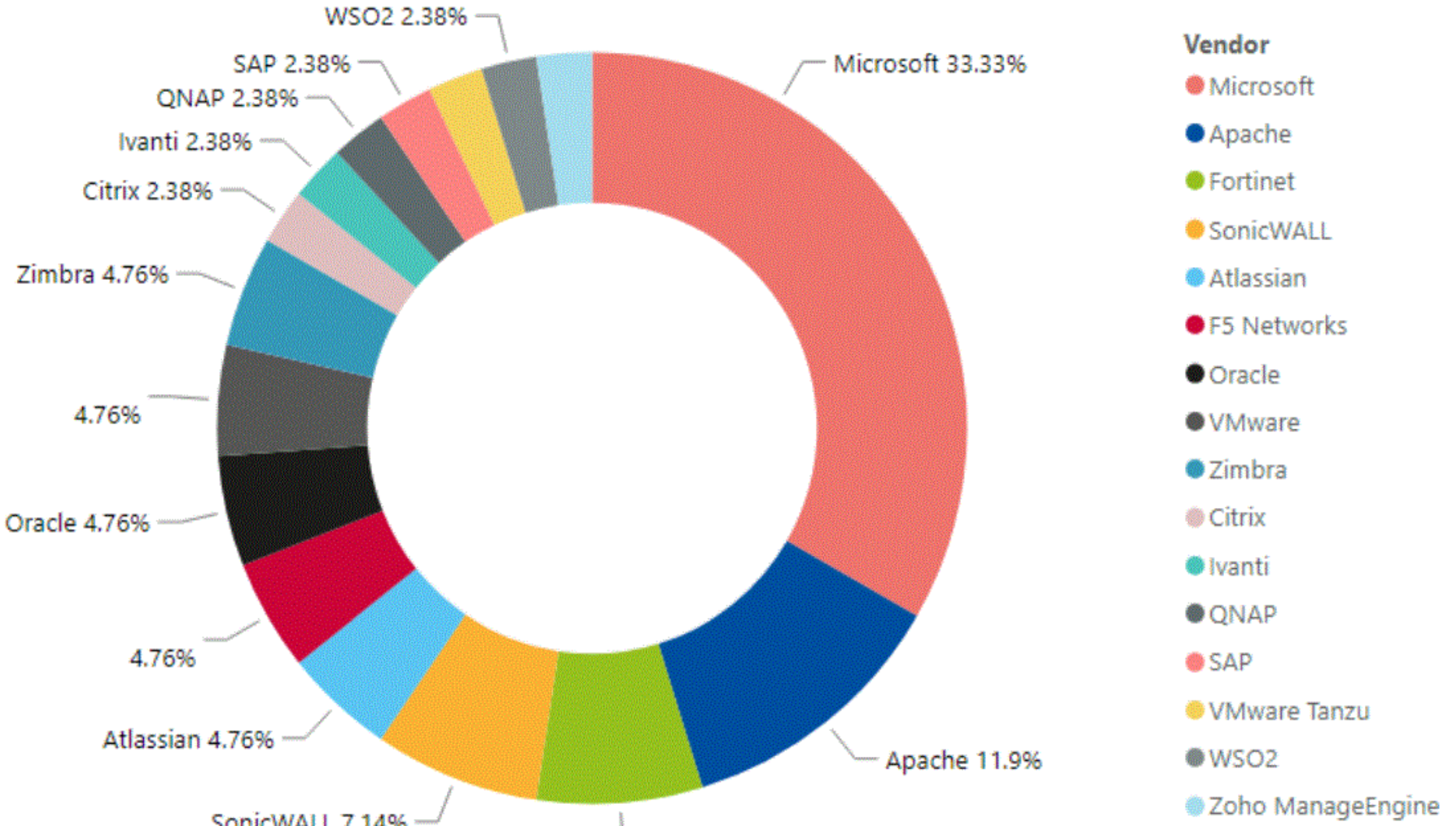
Digital Single Market challenges

- Europe’s increasing reliance on connected hardware and software across sectors and borders.
- Fragmented cybersecurity requirements hinder consistency, trust, and cross-border trade.

Cyber threats escalate

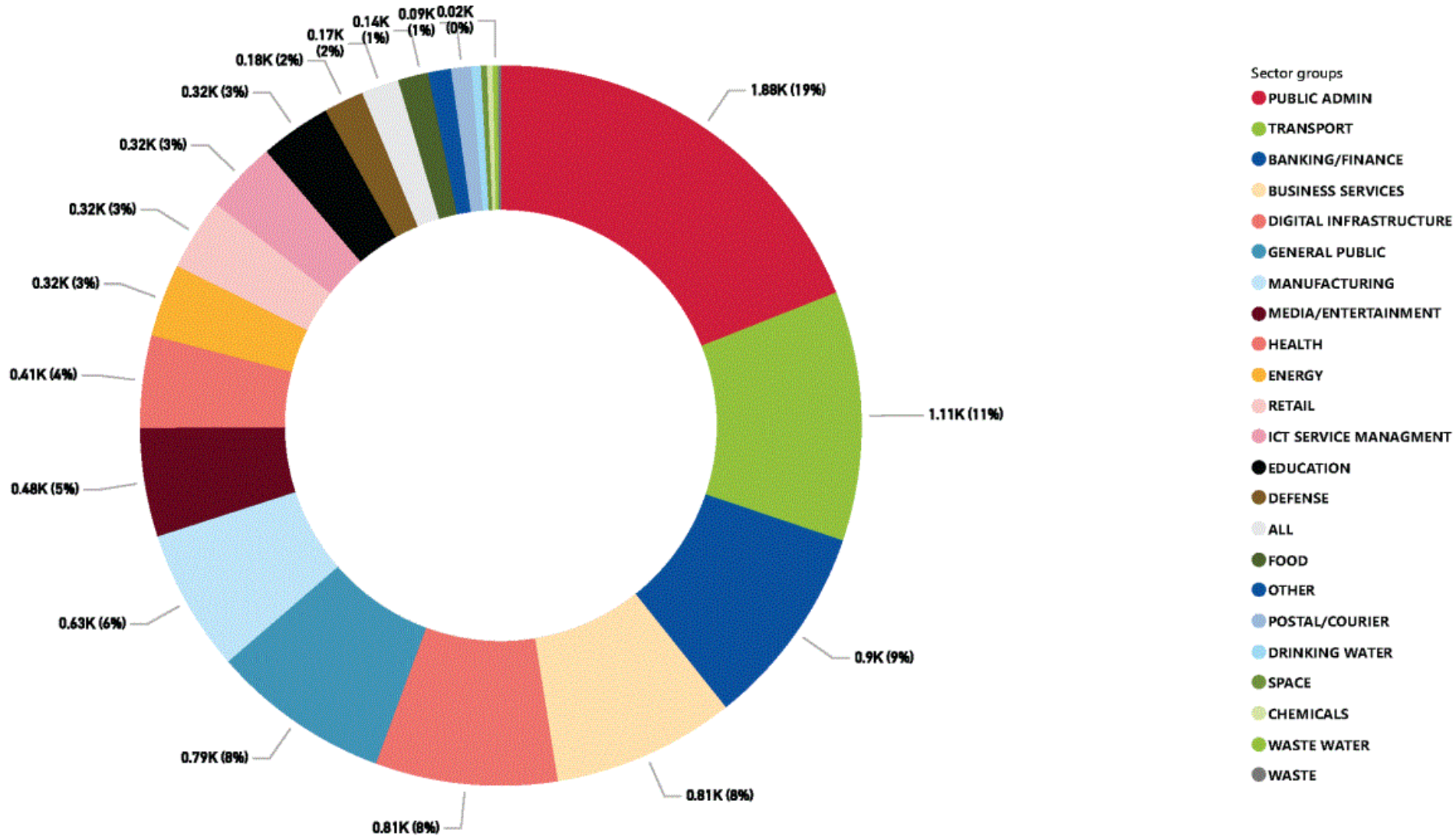
- ENISA's **Threat Landscape 2024** identifies seven prime threat types in the EU: ransomware, malware, social engineering, threats against data, denial of service, information manipulation, and supply chain attacks.
- The rise of state-sponsored and disruptive attacks: "Disruptive digital attacks…have doubled from Q4 2023 to Q1 2024."

Figure 18: 2022 Top routinely exploited vulnerabilities by Vendors (2023 version hasn't been published)



Economic impact

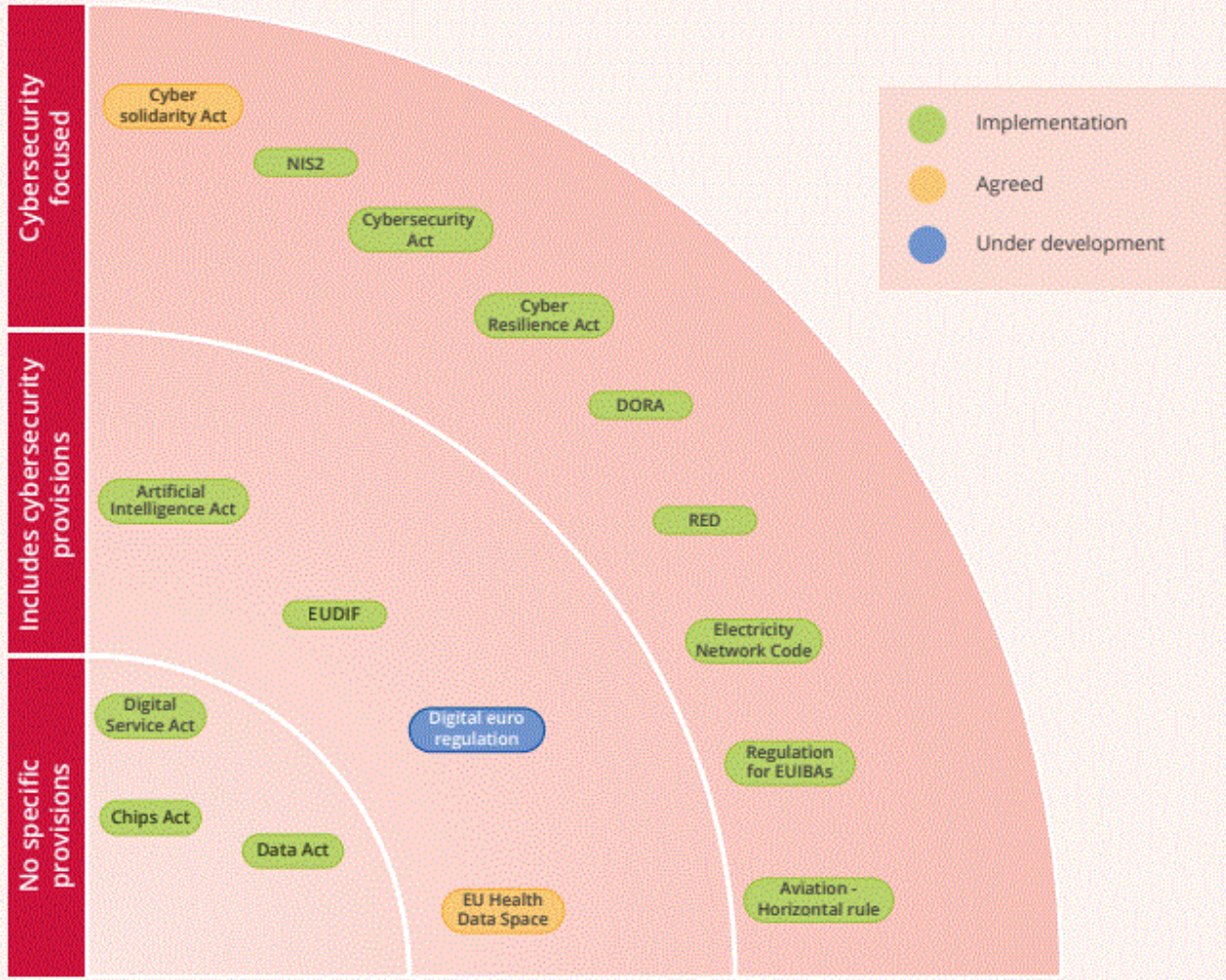
- Cybercrime’s global cost estimated at **€5.5 trillion by 2021** — highlighting the urgency for preventive regulation.


1.88K (19%)
1.11K (11%)
0.9K (9%)
0.81K (8%)
0.81K (8%)
0.79K (8%)
0.63K (6%)
0.48K (5%)
0.41K (4%)
0.32K (3%)
0.32K (3%)
0.32K (3%)
0.32K (3%)
0.18K (2%)
0.17K (2%)
0.14K (1%)
0.09K (1%)
0.02K (0%)
Sector groups
PUBLIC ADMIN
TRANSPORT
BANKING/FINANCE
BUSINESS SERVICES
DIGITAL INFRASTRUCTURE
GENERAL PUBLIC
MANUFACTURING
MEDIA/ENTERTAINMENT
HEALTH
ENERGY
RETAIL
ICT SERVICE MANAGMENT
EDUCATION
DEFENSE
ALL
FOOD
OTHER
POSTAL/COURIER
DRINKING WATER
SPACE
CHEMICALS
WASTE WATER
WASTE

EU’s Cybersecurity Response & Role of CRA

- **Gap in product-level regulation**:
- Existing frameworks like NIS2 and DORA focus on operational resilience and critical infrastructure.
- However, consumer and industrial products lacked harmonized cybersecurity standards — a gap CRA addresses directly
- **CRA builds on the Digital Single Market**:
- Ensures secure by design standards are embedded at product design and lifecycle.
- CE-marked products with digital elements gain trust and are immediately compliant market-wide.

EU legislative landscape



ENISA Data Spotlight — Rising Cyber Incidents

Telecom security incidents — 2024 snapshot

- **188 incidents** reported from 26 EU Member States and 2 EFTA countries — a **20.5% increase** over 2023's 156 incidents.
- Despite the rise in incidents, **user-hours lost decreased**, indicating improved response capabilities.

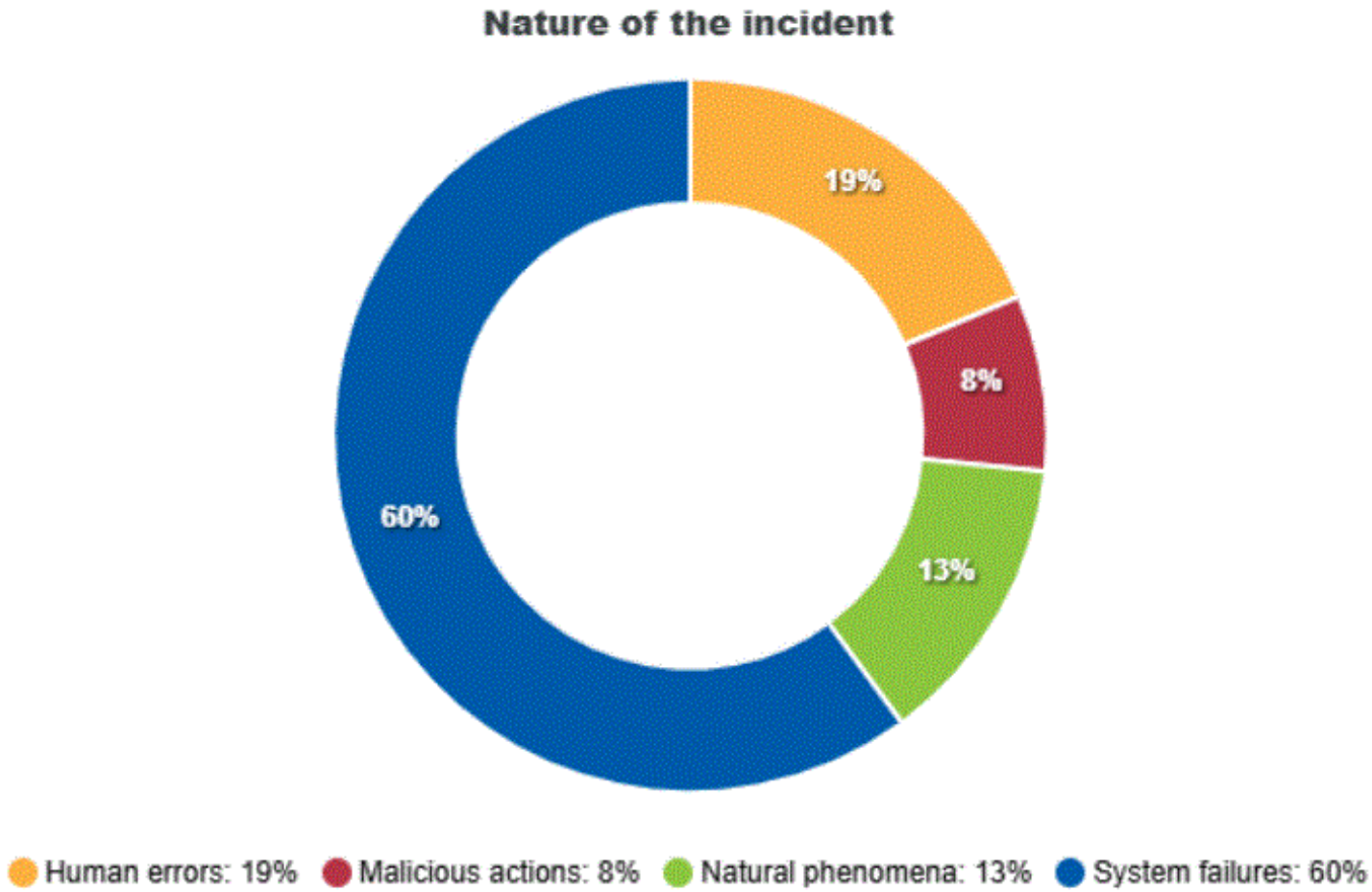


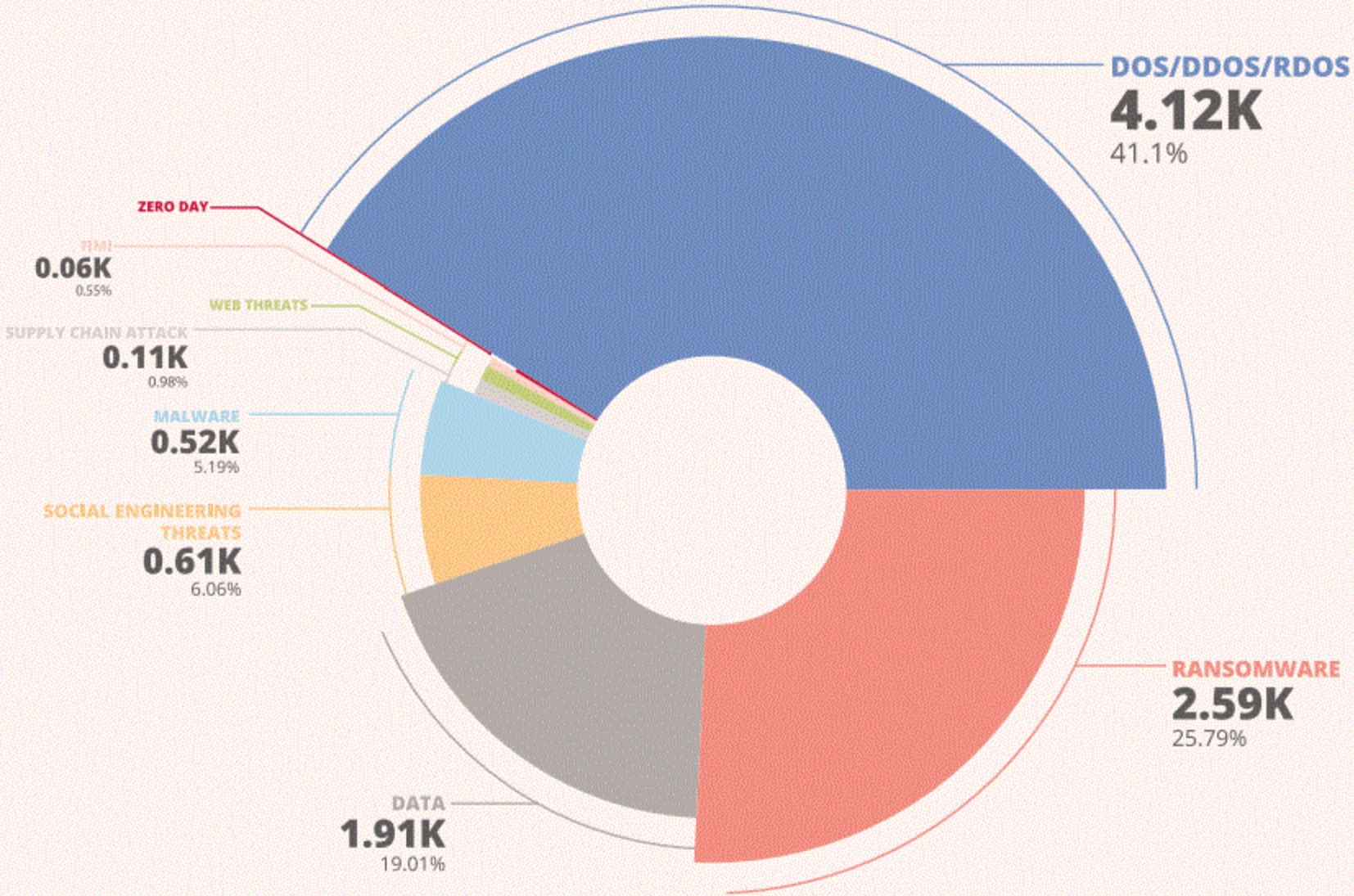
Figure 2: Root cause category

User hours lost per nature of incident

Threat Trends — 2023/2024

- The **ENISA Threat Landscape 2024** details sustained and evolving threats like ransomware and supply chain attacks, which target digital product vulnerabilities.

Incidents by threat type (July 2023 to June 2024)



Why CRA Matters — Bridging the Gap

- **Standardized cybersecurity across all EU products**: CRA mandates minimum security requirements, vulnerability reporting, and lifecycle obligations.
- **Supports Digital Single Market**: Reduces fragmentation, enables secure cross-border commerce, and reinforces EU digital sovereignty.
- **Data-driven justification**: Growing incidents and evolving threats underscore the urgency for regulation focused at the product level.
- Telecom incident rise (+20.5%) and ransomware dominance illustrate systemic risks.

Cybersecurity Threats for 2030

Publications

- ENISA Threat Landscape 2024 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024?utm_source=chatgpt.com#contentList
- Telecom Security Incidents 2024 https://www.enisa.europa.eu/publications/telecom-security-incidents-2024?utm_source=chatgpt.com#contentList
- ENISA Publications about Threat Landscape: https://www.enisa.europa.eu/publications?f[0]=topics%3A526#contentList

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
m.mitrev@dihtrakia.org