SAINT

Systemic Analyser in Network Threats

Presented by: Christopher Hemmens

MANDAT INTERNATIONAL

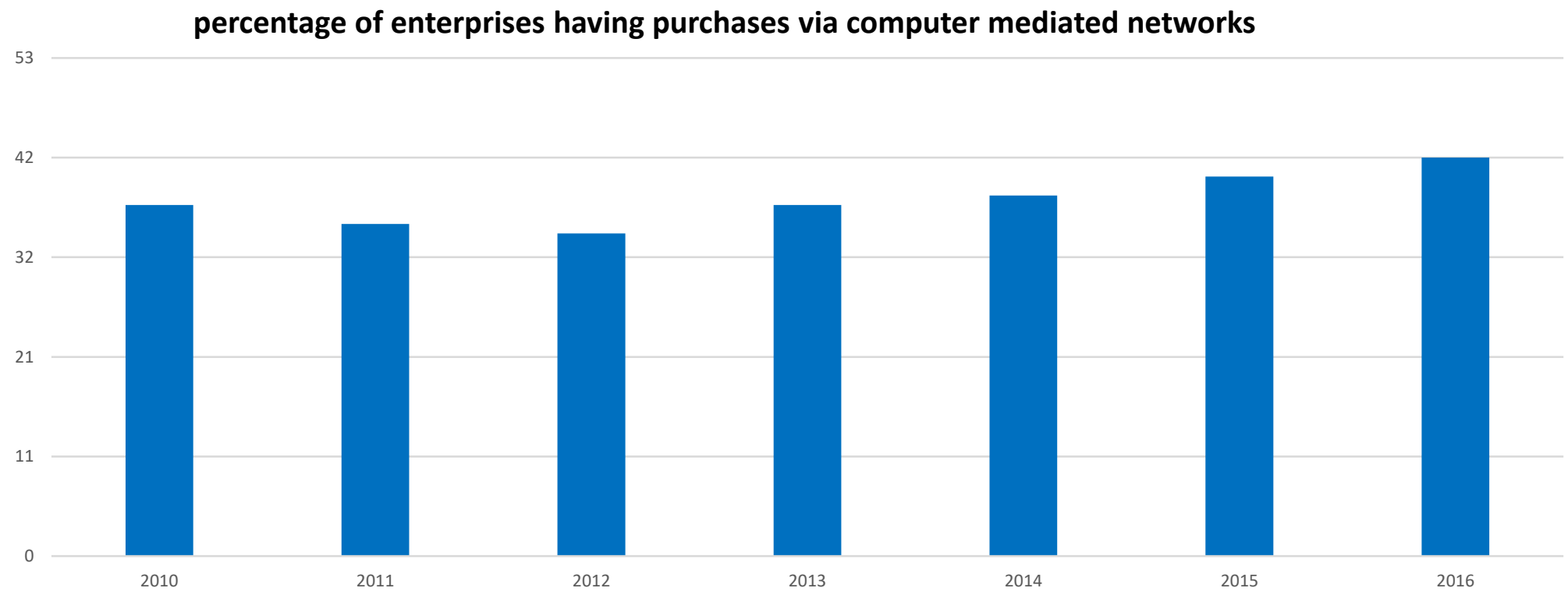
This work is performed within the SAINT Project (Systemic Analyser in Network Threats),
with the support of the European Commission and the Horizon 2020 Program, under Grant Agreement No 740829.

Objectives

- Identify relevant cybersecurity metrics and employ digital epidemiological methods
- Identify market opportunities and potential business models
- Forecast future costs and benefits for cybersecurity solutions
- Develop strategic business models for information regarding cyberattacks and privacy and for cybersecurity services
- Validate framework methodologies and analytic models
- Communicate with stakeholders and the public
- Monitor and identify social, economic, sustainability, ethical, legal, and privacy aspects and risks

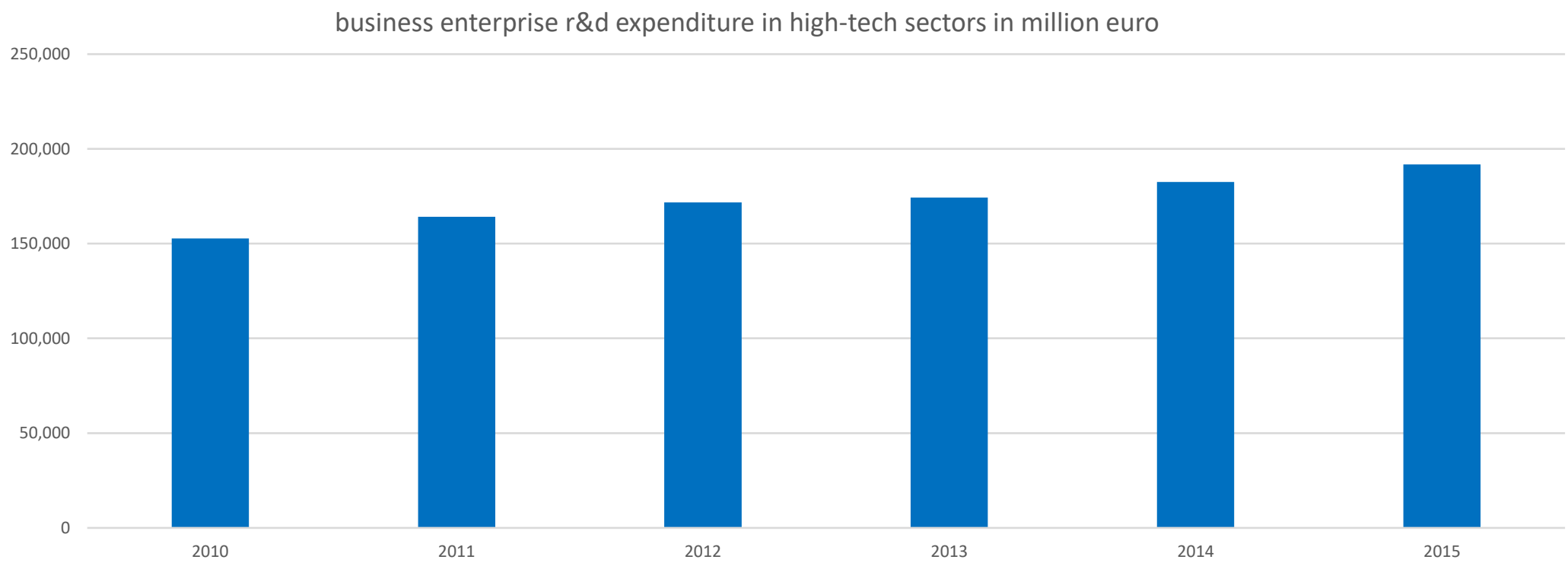
Relevant Field of Action

- **Relative Market Area Size**



Relevant Field of Action

- **Relative Market Area Size**



Outputs and challenges - Practical

Practical challenge = Application of Metrics of Cybersecurity - to - threat analysis – examples:

- Determine, Quantify & Rank ENISA's ETL - metrics
- Economic analysis
- OWASP Top 10 – Web Security - Vulnerabilities

ENISA's Top 15 Threats

Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	→	→
2. Web based attacks	→	→
3. Web application attacks	→	→
4. Denial of service	→	↑
5. Botnets	→	↓
6. Phishing	↓	↑
7. Spam	↑	↑
8. Ransomware	↓	↑
9. Insider threat (malicious, accidental)	↓	↓
10. Physical manipulation/damage/ theft/loss	→	↓
11. Exploit kits	→	↓
12. Data breaches	→	↓
13. Identity theft	↑	↓
14. Information leakage	→	↓
15. Cyber espionage	↑	→

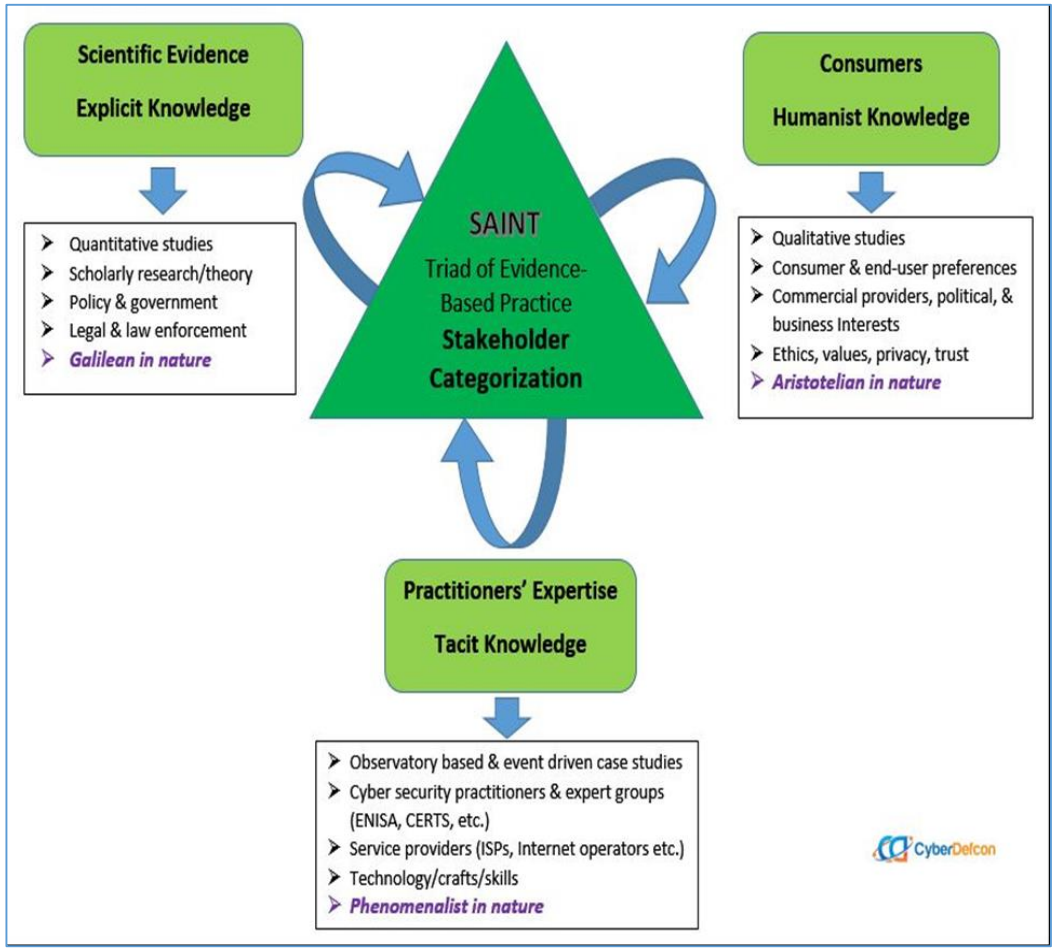
OWASP Top 10 (2017)

OWASP Top 10 – 2017 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities
A10 – Underprotected APIs (NEW)

- **1) Costs of Cybercrime**
- * The annual cost to the global economy from cybercrime is more than €300 billion Euros [6]
- * Cost of cybercrime for the EU 0.4% of its GDP = €13 billion / annum [7]
- Sample EU countries estimates for the cost of cybercrime :
- * Poland: € 377 million /annum
- * Germany: € 2.6 billion /annum
- * Cybercriminal revenues (estimate of the cybercrime market itself) €15 billion / annum [8]
- * Market for security products and services €50 billion / annum [9]
- **2) Examples of Cybercrime Metrics**
- * 3 Billion Users of the Internet (~39% world population) [10]
- * Over 200 billion emails processed / day [11]
- * 917.9 million Websites (variable) — 39 million / month added (4%) [10]
- * IP addresses - IPv4 = 4,294,967,296 (2¡^{32}) - IPv6 = 128-bits (2^{128}) [12]
- * 2.3 billion mobile-cellular subscriptions worldwide [13]
- * 1.4 million Browser user agents – bots [14]

- **3) Technical and Quantitative Metrics of Cybercrime Activity Indicators**
- * 85% of processed emails are spam [15]
- * 7% of all URLs malicious [16]
- * Public Block List count: 1,018,203,532 IP addresses [17]
- * 2,698,726,309 ids recorded from ‘known’ Data Breaches
- * 350 million+ in total identifiable malware [18]
- * 1 million+ measurable cyber-attacks (variable) [19]
- * 330 active Real-time Blackhole Lists (RBL & DNSBL) [20]
- * € 7.9 million is the average annualized cost of data breaches [21]
- * 10.4% net increase cost of data breaches over the past year [21]
- * 250,000 – 500,000 malicious binaries / day [22]
- * ~280 million malicious binaries collected [22]
- * 6 / 10 million unique IP's sink holed / day [22]
- * 900,000 malicious domains / day [22]
- * 500 of 52,000 ASNs worldwide (4%) account for hosting 85% of malicious activity [23]

To achieve workable practices for deriving cyber security metrics towards an empirical science

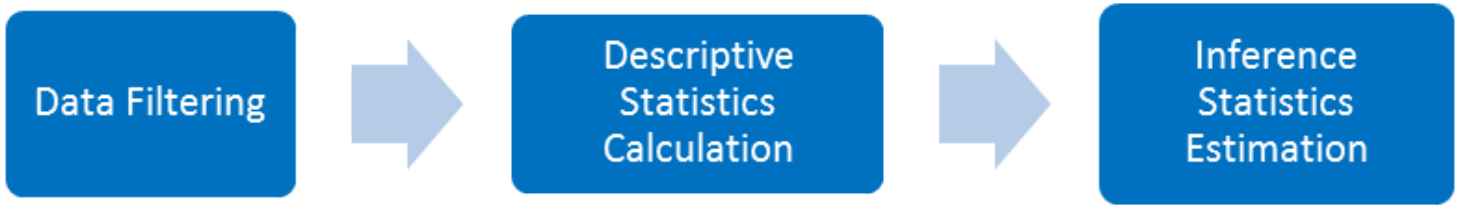


Its all about the data and the evidence!

- Digital Epidemiology and evidence based practice
- Use of the triad to enable & bring about disease prevention.
- A innovative paradigm from SAINT cyber security metrics for attack and threat **prevention**!
- Within SAINT –who and how we aim the surveys & gather knowledge from multiple data sources.

Work Methodology

- **Statistical Analysis Process**



- **Econometric Modelling Process**

Thank you

SAINT

This work is performed within the SAINT Project (Systemic Analyser in Network Threats),
with the support of the European Commission and the Horizon 2020 Program, under Grant Agreement No 740829.