CYBERSECURITY ROMANIA
- BUCHAREST TALKS
4 IUNIE 2019

BISS

Cat & Mouse / On who's money?

Bogdan TOPORAN | BISS

Threats are real

- 2009-2012 / CITADEL ZEUS (man-in-the browser/ target: bank & customer)
- 2014 -2016 / DYRE TROJAN (man-in-the browser /credentials harvesting from banking websites / target: bank & customer)
- 2016-2018 / COBALT STRIKE (Hybrid / target: bank users)

- ONLINE BANKING FRAUD
- MOBILE BANKING FRAUD
- CYBER THREATS / RANSOM
- BANKING MALWARE
- PHISHING AND ROBOTS
- SKIMMING
- SOCIAL ENGINEERING
- IDENTITY THEFT

The Cyber Reality is changing

Increased Threats From the Outside

- Increasing Alert Volume
- Time-sensitive attacks
- Multi-Vector Attacks
- Non-malware Attacks

- Skill Shortage
- Increased Regulation

Growing Challenges from Within

- Converging attack surface
- Connected Infrastructure

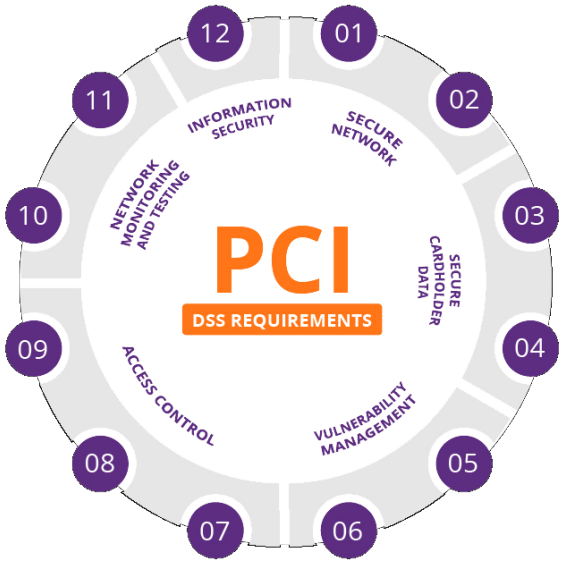
In target

networks, apps, devices, users, regulations

- Networks are more complex, heterogenous and **interconnected**
- Applications do not provide **security by design**
- User devices, apps and data are **multiplying** every day.
- Compliance is always a **concern**
- Regulations are also **multiplying**

- Lack of Network **visibility**
- Application security is a **must**
- Who knows and **who controls** the user?
- ISO 27k, PCI-DSS, GDPR, **NISD, PSD2**

Regulation drivers



User authentication

- Banks chose MFA (costs)
- SMS delivered OTP
- SMS token providers focus on availability and speed, not security
- “Online Banking Credentials That Use SMS For Authentication Of Users Are Being Systematically Hacked”
  - As far back as 2014 systemic vulnerabilities on the SS7 protocol for SMS
  - SS7, first designed in the 1980s, is riddled with serious vulnerabilities that undermine the privacy of the world’s billions of cellular customers
  - These vulnerabilities continue to exist
- The flaw in the Signaling System 7, enables data theft, eavesdropping, text interception, and even location tracking.

- With many bank accounts secured by multi-factor authentication that depends on smartphones, the security of everything smartphone-related might well need reassessment.

User & Customer focus

✓Gartner's security layers

LAYER 4
Multiple channel protection - all gathered data / evaluated in context of all covered channels.

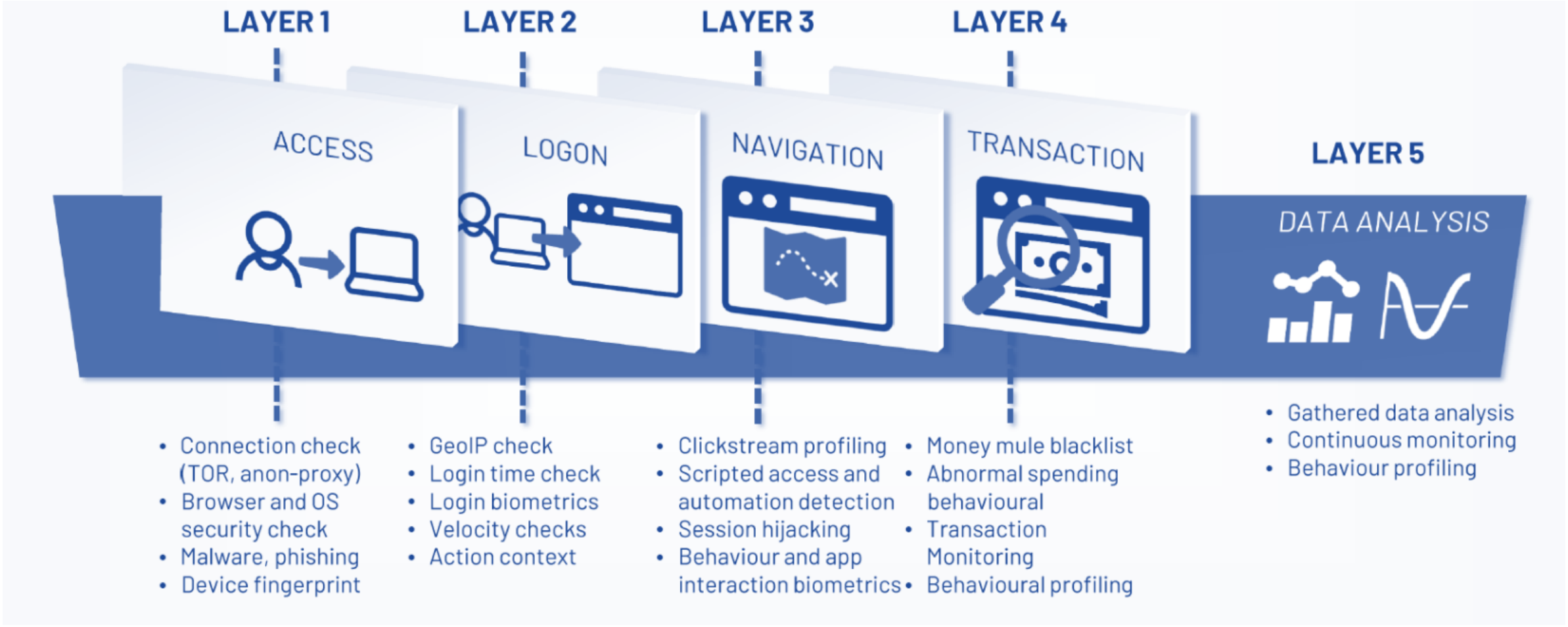
LAYER 2
Session protection - session monitoring and evaluation based on multiple inputs.

LAYER 5
Incorporate Global intelligence – enable shared intelligence / use for enhanced security across multiple entities.

LAYER 3
Channel protection – monitor every user's access /evaluate in context.

LAYER I
End-point protection - deep device monitoring and profiling.

A layered approach



Holistic approach

Customer protection with OTP over SMS is poor, and with PSD2 the liability shift will push all risks of weak security onto banks and payment service providers exposing them to systemic risks, which cannot be insured.

Strong Customer Authentication
- ✓ Possession
- ✓ Knowledge
- ✓ Inherence – Behavioural/biometry

Transaction Monitoring
- ✓ Real-time scoring
- ✓ Authentication element stolen
- ✓ Detection of Financial Malware
- ✓ Known fraudulent scenarios
- ✓ Amount of each payment

Screen Scraping
- ✓ Prohibited
- ✓ Must be Detectable

Transaction Risk Analysis
- ✓ Abnormal spending behavioral patterns
- ✓ Location of payer
- ✓ Location of payee's account
- ✓ Known fraud scenarios
- ✓ Unusual information about the device orsoftware
- ✓ Signs of malware infection

CYBERSECURITY ROMANIA
- BUCHAREST TALKS

4 IUNIE 2019

BISS

THANK YOU!

Bogdan TOPORAN | BISS