INETCO and Printec

Borica Bulgaria – Major Recent Success in 2022/2023

REAL-TIME MONITORING AND ALERTING CAPABILITIES

DETECTING INCIDENTS (PROACTIVITY vs REACTIVITY)

REAL-TIME STATISTICS AND DASHBOARDS

Major focus – Balkans and Central Europe

About INETCO

Key Offerings for small, mid and big-size entities

Payment Fraud Prevention & Cybersecurity Protection

Transaction Performance & Omnichannel Monitoring

Data Analytics & Fraud Analysis

Real Time and Scalable

How the INETCO Platform is Being Used

Category				
ATM Monitoring & Analytics	coast capital SAVINGS	BB&T	Santander	Ficohsa · Interbank
POS & Online Retail	Publix	Walmart	Moneris	Ficohsa · izipay
Multi-channel & Card Processing	AMERICAN EXPRESS	FIS	fiserv.	Banco de Bogotá · Grupo Promerica
Channel, Card & Analytics	mashreq	WOODFOREST NATIONAL BANK	izipay	BORICA BANK SERVICES
Payment Monitoring & Audit	Interswitch	BKM BANKALARARASI KART MERKEZİ	elo	
BI Analytics, Fraud & Cash Mgmt	BECU	e·global servicios electrónicos globales		
Fraud Detection & Prevention	Stanbic Bank A member of Standard Bank Group	LAFISE	ALTO	

ONE CASE: A multinational bank lost $19M in 3 hours and didn't know for several days

The Target Bank
- ➤ With over 8,000 ATMs, 40,000 POS devices, and millions of online transactions across the African continent
- ➤ lacked early detection and prevention of irregular transactions
- ➤ Did not have real-time end-to-end visibility into every transaction

The Attack
- ➤ Hackers installed malware that would automatically approve their transactions by bypassing the host
- ➤ Fraudsters took $19M in under 3 hours without the bank knowing about it until days later
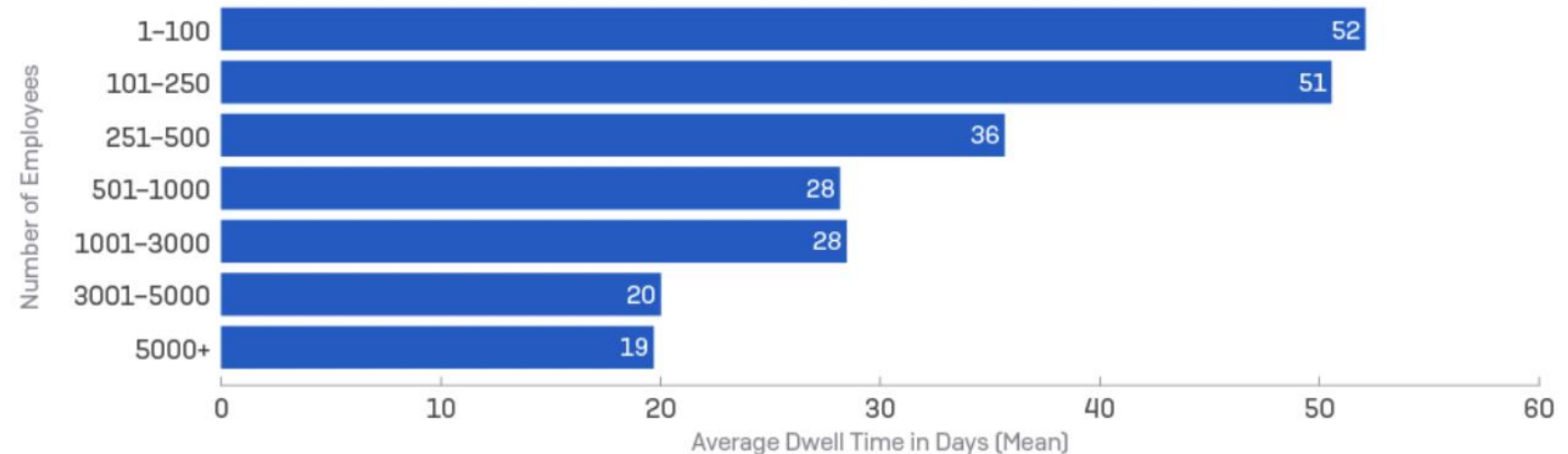- ➤ Highlights the banks inability to see the problem as it occurred and their inability to stop the problem

Time to detect compromise is high...

34

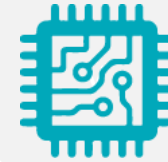Median number of days advanced attackers are on the network before being detected

Intruder Dwell Time by Company Size (Mean)

Number of Employees	Average Dwell Time in Days (Mean)
1–100	52
101–250	51
251–500	36
501–1000	28
1001–3000	28
3001–5000	20
5000+	19

AI Threats to Payment Systems

Spear Phishing and Social Engineering

Man-in-the-Middle Attacks

Distributed Denial of Service (DDoS) Attacks

Insider Fraud

Advanced Persistent Threats (APTs)

AI Dataset Poisoning and Adversarial Learning

INETCO®

Combining AI and Traditional Methods

6 Ways Adding AI Benefits Traditional Systems

Integrating AI with Tradition Fraud Prevention

While conventional methods often rely on static rules and manual analysis, AI brings dynamic capabilities such as machine learning, pattern recognition, anomaly detection, and real-time decision-making.

Data Aggregation

Implementing Machine Learning Models

Real-time Monitoring

Adaptive Risk Scoring

Automation and Orchestration

Continuous Learning and Improvement

INETCO BullzAI - Advanced Machine Learning and Analytics

Comprehensive monitoring

Proactive Threat Detection

Streamlined Incident Response

Regulatory Compliance

Scalable and Adaptable solution

Harnessing the power of AI

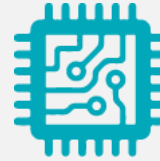**Continuous learning and adaptation**

Real-time Decision-Making

INETCO®

Key Takeaways

Importance of AI in Fraud Prevention and Cybersecurity for Payment Systems

Integration of AI with Traditional Fraud Prevention Methods

Working with INETCO BullzAI for Payment Fraud and Cyber Security

The Ever-Evolving Landscape of Digital Threats

The Need for Continuous Innovation in Cybersecurity for Payment Systems

Thank You

Continue the Conversation

🌐 www.inetco.com

in @carloslarranaga

✉ clarranaga@inetco.com