الاتحاد الدولي للمصرفيين العرب
World Union of Arab Bankers

ANAT
SECURITY

Cybersecurity in Financial Services

Safeguarding Our Digital Future

Tony Chebli
ANAT SECURITY
CEO

Toni Chebli

Paris France

25 Years+ Industry Experience, CISSP, CMSA, CIISP authorized Trainer, PECB & TRECCERT Certified Trainer, PECB Certified Data Protection Officer, ISO/IEC 27001 Lead Auditor, ISO 27701 LI, ISO 27002 Lead Manager, PECB Cloud Manager, ISO 27005 Risk Manager and PECB Certified ISO/IEC 31000 Risk Manager and many more.

Expert Insights

Tony Chebli is a seasoned cybersecurity expert and the CEO of **ANAT SECURITY, a prominent cybersecurity firm based in Paris, France.**

With extensive experience in information security, he has established himself as a leader in the field, known for his commitment to protecting organizational assets and enhancing cybersecurity practices across various sectors.

Tony received the security award "CISO-100" (Chief Information Security Officer among the top 100 in the region) from the Middle East Security Awards (MESA) in Dubai, UAE, for three consecutive years.

He achieved PCI-DSS compliance for several institutions, including Credit Libanais (the first and still the only bank to be certified PCI-DSS in Lebanon), Netcommerce (an e-commerce site), IPN (a service provider), CCM (another service provider), and Credit International Bank in Senegal.

His experience in the field is extensive and has led him to perform the following:

- ISO 27001
- PCI-DSS
- ISO 42001
- ISO 31000
- ISO 27701
- GDPR

Agenda

I. Definition

II. The ugly truth

III. Adversary’s weapons

IV. Security news!

V. Security Facts!

VI. Real cases

VII. The cure

VIII. ANAT SECURITY

IX. Ask me anything

Definition

What is Cybersecurity?

Cybersecurity protects the bank’s money, operations, and trust from digital threats.

- **Protects sensitive data**

Customer information, financial records, and transactions.

- **Secures critical banking systems**

Core banking, payments, digital channels, and third parties

- **Ensures business continuity**

Prevents service disruption and operational outages.

- **Manages cyber incidents**

Detects attacks early, limits impact, and enables fast recovery.

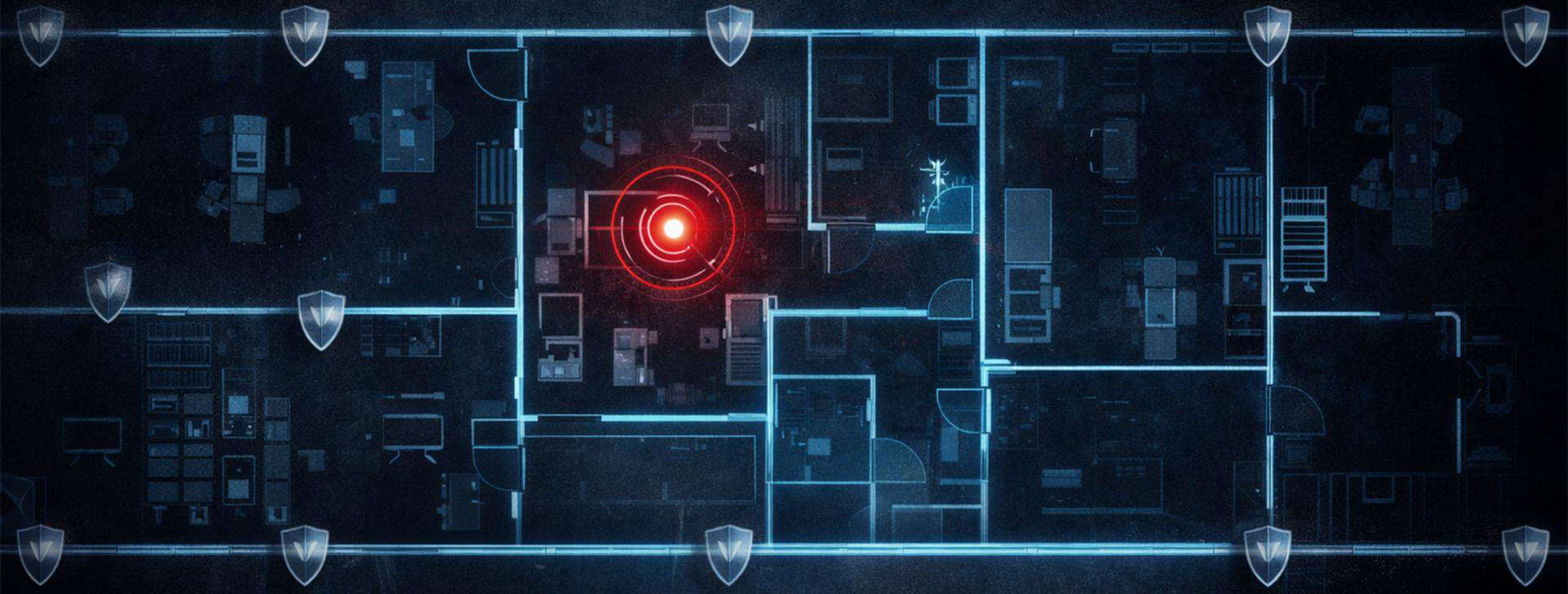
- **Why It Matters**

Financial losses

Regulatory penalties

Customer trust & reputation

The Ugly Truth



Adversary's Weapons

Phishing	Malware	Ransomware
DDOS	APTs	Cloud
IoT	Insider Threats	AI

Vulnerabilities

- API weaknesses
- Password fatigue
- Third-party access
- DDoS susceptibility
- Improper storage of sensitive data
- Legacy systems
- Phishable users
- Cloud misconfigurations
- Authentication weaknesses
- Mobile banking app vulnerabilities
- Lack of encryption

Threats

- Mobile banking threats
- Phishing scams
- Trojan
- Mobile malware
- Ransomware
- Insider threats
- Third-party risks
- Password attacks
- Cloud threats
- DDoS attacks
- Emerging technologies
- AI

Security News

- Comparitech reported in 2024 that over 70% of German companies were subject to a successful cyberattack within 12 months
- Almost Half of Boards Lack a Real Understanding of Cyber Threats according to PwC's Global CEO Survey and Deloitte's Cybersecurity Reports.
- A 2025 study by Strategy & Global Business Unit of PwC revealed that nine out of ten organizations surveyed reported a shortage of cybersecurity specialists
- More than 50 Billion Devices are Vulnerable to Cyberattacks
- IoT: Hacker’s Wonderland in the Enterprise

Security News

- Lack of Skills Still Hampers the Ability to Deliver Cybersecurity
- EU General Data Protection Regulation (GDPR) is Forcing Firms to Report Breaches
- Ransomware incidents have surged by approximately 30% in 2024, signaling a persistent and growing trend in cyber threats.
- Errors related to misconfigurations of cloud storage remain a critical issue, contributing to 15% of data breaches in 2024.
- Human error continues to play a significant role, with 85% of breaches in 2024 involving some aspect of the human element, underscoring the need for enhanced training and awareness

References: Cybersecurity & Infrastructure Security Agency (CISA), Verizon Data Breach Investigations Report (DBIR), Cybersecurity Ventures

Security Facts!

Ransomware

- 2024 Ransomware was involved in 32% of breaches.
- 2025 Ransomware increased to 44% of breaches.
- 2024 The median ransom was **$150,000**.
- 2025 The median ransom decreased to **$115,000** (though not an increase, it reflects a trend that organizations are not paying as much).

Human Elements

- 2024 Approximately 61% of breaches involved human elements.
- 2025 This number slightly decreased to around 60%.

Security Facts!

Privileges misuse

2025

- Privilege misuse accounted for 825 incidents, with 757 confirmed data disclosures.
- The majority of privilege misuse cases were caused by internal actors (90%), with a small percentage attributed to partners (10%) and external actors (3%).
- Personal data (72%), internal data (36%), and other types were commonly targeted.

Use of Generative AI

- 15% of employees accessed generative AI systems on corporate devices, raising concerns about corporate data leakage.
- A significant portion of these users accessed GenAI platforms using non-corporate emails (72%) or corporate emails without security measures (17%).

Capital One Data Breach Using AI

The 2024 Capital One data breach.

Capital One is a major financial institution operating as a bank holding company, providing:

- Credit Cards: to millions of customers.
- Consumer banking products including checking and savings accounts.
- Lending services, such as personal loans and auto loans.

Incident Overview

Nature of the incident

The breach involved exploiting a misconfigured web application firewall, allowing the attacker to access sensitive data**.**

Attack Method

A weakness in the configuration of a web application security mechanism allowed the attacker to bypass intended protections and access internal data resources.

Use of Automation and AI Techniques

- Automation and AI-assisted techniques were used to accelerate the attack process
- Large volumes of data were rapidly queried, filtered, and analyzed
- Sensitive information was identified and extracted more efficiently than through manual methods

Capital One Data Breach Using AI

Key Facts and Impact

Data Compromised

Personal information of over 100 million customers, including names, addresses, credit-related data, and identification details.

Motivation

The incident was financially motivated to exploit stolen data for fraud, identity theft, or illicit resale.

Detection and Response

- The breach was identified in early 2019, leading to law-enforcement intervention.
- The institution faced regulatory scrutiny, financial penalties, and reputational impact.

Consequences

- Demonstrates how automation and AI can increase the speed, scale, and impact of cyber attacks.
- Highlights the necessity for strong security governance, including configuration management, access controls, and continuous monitoring to mitigate AI-enabled threats.

AI Threats in the Middle East

Incident Overview- APT34 (OilRig)- a state-linked cyber espionage group

Attack Type

APT34 conducted targeted cyber campaigns against financial institutions and critical infrastructure organizations across the Middle East, leveraging advanced automation and AI-assisted techniques.

Attack Methodology

Phishing Campaigns

- AI-assisted phishing campaigns designed to appear legitimate by impersonating trusted individuals or well-known organizations.

Credential Harvesting

- Credential harvesting, enabling unauthorized access to internal banking and operational systems once users were compromised

Targeted Institutions

- Financial institutions
- Oil and gas companies,
- telecommunications providers

Across multiple Middle Eastern countries.

AI Threats in the Middle East

Consequences

Financial and Operational Impact

Potential for significant financial losses, service disruption, and operational instability across targeted sectors.

Increased Sophistication

The use of AI and automation demonstrates the growing sophistication of cyber threats, reducing the effectiveness of traditional, perimeter-based defenses.

Countermeasures

Enhanced Phishing Awareness Training

Implement structured awareness programs to help employees recognize, avoid, and report phishing and social-engineering attempts.

Strong Security Infrastructure

Deploy strong authentication mechanisms and centralized monitoring capabilities to detect, investigate, and contain cyber threats.

AI-Based Threat Detection

Leverage AI-driven analytics to identify anomalies and suspicious behavior early, enabling faster and more effective responses.

Bangladesh Bank heist case

Incident Overview – Bangladesh Bank (SWIFT)

Context

The Central Bank of Bangladesh used the SWIFT interbank messaging system for international financial transactions.

Attack Method

Bank employees were targeted through a phishing campaign, leading to the compromise of SWIFT credentials.

Exploitation

Stolen credentials were used to submit fraudulent SWIFT payment messages to the Federal Reserve Bank of New York

Impact

- Dozens of unauthorized transfer requests totaling nearly USD 1 billion were initiated.
- While most transactions were blocked, approximately USD 81 million was successfully transferred and lost.

Bangladesh Bank heist case

Root Cause Analysis – Bangladesh Bank (2016)

Security Weaknesses Identified

- Insufficient network segmentation, allowing attackers to move laterally within critical systems
- Inadequate logging and monitoring, limiting visibility over suspicious activity and delaying detection
- Weak authentication and oversight controls over SWIFT operations, including limited use of multi-factor authentication:

Outcome

- These combined weaknesses enabled attackers to evade detection for an extended period and execute large-scale fraudulent transactions.

Accenture security breach case

Incident Overview – Accenture (2021)

Context

- Accenture is a global professional services firm providing technology and consulting services to financial institutions worldwide.

Nature of the Incident

- In 2021, malicious actors compromised Accenture’s systems, resulting in unauthorized access to customer banking data.

Data Impact

- Exposed information included transaction records, authentication credentials, and customers’ personal data.

Accenture security breach case

Root Cause Analysis – Accenture (2021)

Initial Compromise

Unauthorized access was traced to a compromised credential exposed online, suggesting password reuse or successful phishing.

Lateral Movement

Once inside the environment, attackers were able to move laterally within internal systems, gaining access to sensitive customer banking data.

Control Weaknesses

Insufficient internal network segmentation enabled attackers to access data related to multiple banking clients managed by Accenture as a service provider.

Outcome

The incident impacted more than two dozen banks, highlighting the concentration risk associated with large third-party service providers.

Big Bank in Qatar Data Breach (2025)

Nature of the Incident

A large data archive (approximately 1.4–1.5 GB) containing customer banking information was unlawfully disclosed online, making it publicly accessible.

Data Exposed

- Bank account details
- Authentication Information (passwords and PINS)
- Payment card data
- Contact details (phone numbers and email addresses)
- Transaction records and other personal identifiers.

Root cause analysis

Application Security Weakness

The breach resulted from an SQL injection vulnerability in a web application, allowing unauthorized access to backend databases.

Data Protection Failures

Sensitive information was reportedly stored in unencrypted or insufficiently protected formats, increasing the severity and usability of the stolen data.

A Bank in Qatar Data Breach (2025)

Attribution

- Some reports attributed the incident to a hacker group claiming Turkish affiliations; however, definitive attribution and motives remain unconfirmed.
- Suggested motivations ranged from reputational damage and hacktivism rather than direct financial gain.

Consequences and Impact

- Privacy & Identity Risk

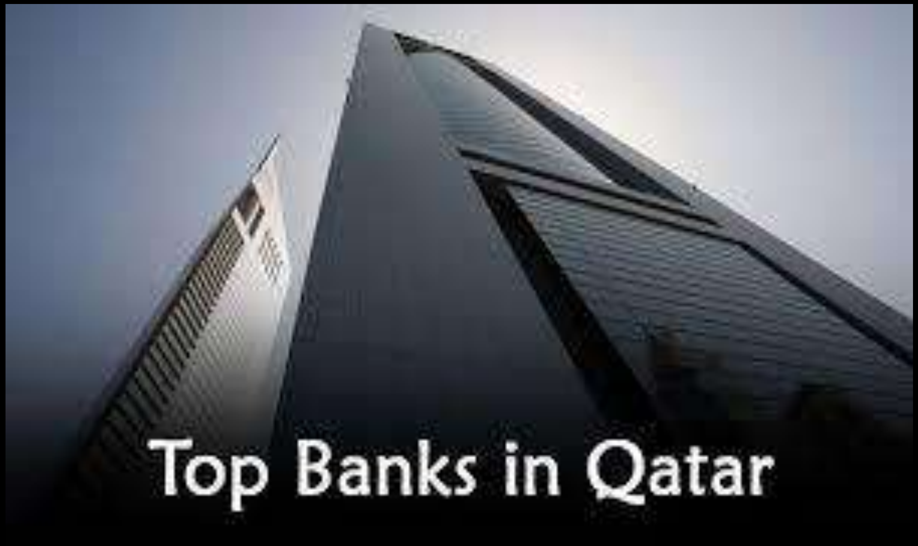
Exposure of authentication credentials and personal data increased the risk of identity theft, phishing, and unauthorized access to other services.

- Reputation Impact

The involvement of high-profile individuals heightened public and regulatory concerns regarding the bank’s data protection practices.

- Sector-Wide Lesson

The incident underscored the critical need for secure application development, encryption of sensitive data, and timely vulnerability management across financial systems.



DDoS Attacks on UAE Financial Institutions

Incident Overview – Multi-Day DDoS Campaign (2024)

Nature of the Attack

- A sustained, high-volume Distributed Denial of Service (DDoS) campaign targeted a financial institution in the UAE.
- The attack persisted for more than six consecutive days, far exceeding typical short-duration DDoS incidents.

Attack Characteristics

- Multiple attack waves lasting 4 to 20 hours each.
- Average traffic volumes of approximately 4.5 million requests per second (RPS)
- During peak waves, legitimate traffic became a tiny fraction of all incoming requests, making normal banking services nearly impossible to reach.
- During peak periods, malicious traffic overwhelmed legitimate customer access, severely disrupting online banking services

Attribution

- The campaign was attributed to a hacktivist group, based on monitoring and analysis by Radware and related threat intelligence sources

Significance for Banks

- Demonstrates how financial institutions can be targeted continuously, not just through short, isolated attacks
- Highlights the vulnerability of customer-facing digital services during prolonged availability attacks

UAE Bank Voice-Cloning Attack

Incident Overview – AI-Driven Vishing Attack

Nature of the Incident

- Publicly reported analysis indicated that a UAE bank suffered losses of approximately USD 35 million following a sophisticated vishing (voice phishing) attack
- Attackers used AI-generated voice cloning to impersonate a senior bank executive and manipulate a branch manager into authorizing high-value transfers

Attack Method

- AI-cloned voices were used to impersonate executives, managers, or trusted authorities.
- Victims were pressured through urgent and credible scenarios (e.g., security incidents or regulatory requests) to approve transactions or share verification information

Emerging Trend (2025)

- Multiple incidents worldwide involved AI-generated audio deepfakes convincing bank staff to execute unauthorized transfers under time pressure

Consequences

Control Bypass

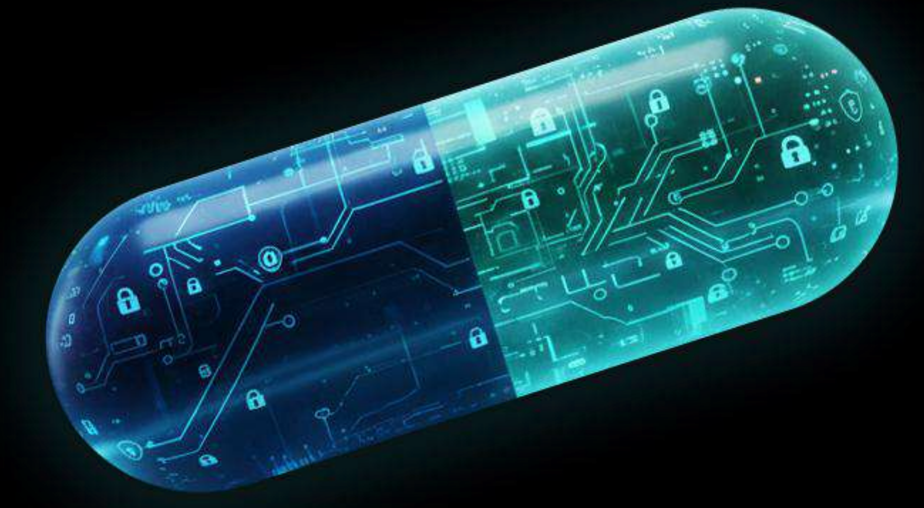
- Traditional voice-based identity verification was rendered ineffective

Financial Impact

- Resulted in significant unauthorized wire transfers, amounting to millions globally

Risk Amplification

- Demonstrated how AI significantly increases the credibility



The Medicine

Global Experts in Cybersecurity Excellence

Who We Are

ANAT

SECURITY

About ANAT Security

Founded

2024, Paris, France

Headquarters

Based in the heart of Paris, our headquarters reflect a strategic location — combining technological innovation with a truly global outlook.

Global Presence

Our roots in the Middle East have shaped our expertise in managing complex cybersecurity challenges. This foundation enables us to support clients across key international markets with agility and strategic insight.

Global Experts in Cybersecurity Excellence

Strategic Locations for Borderless Security

Why France and Paris?

- A global leader in cybersecurity and tech innovation.
- France plays a key role in cyber defense, advanced cryptography, and AI applied to cybersecurity. The country is home to leading clusters such as:
  - Campus Cyber
  - Government-backed initiatives like the France Cybersecurity Label
  - These make France a frontrunner in protecting digital infrastructures.
- A strong international R&D ecosystem:
  - Advanced labs dedicated to cybersecurity
  - Prestigious engineering schools
  - Ongoing collaboration between public and private sectors

France continues to accelerate innovation in cybersecurity, critical infrastructure resilience, and advanced threat behavior analysis.

Campus Cyber : https://campuscyber.fr
Label France Cybersecurity :https://www.francecybersecurity.fr

Global Experts in Cybersecurity Excellence

Strategic Locations for Borderless Security

Strategic Role in Europe

- Also, France plays a central role in shaping Europe’s digital landscape.
  - It contributes to the development of major data protection regulations (GDPR, NIS2, DORA, PCI-DSS*)
  - It helps define international cybersecurity standards

Strong Commitment to Digital Sovereignty:

- Through initiatives like France Cybersecurity and the promotion of European alternatives to non-EU tech solutions, France strengthens its technological autonomy and ensures the protection of both national and European infrastructures.

*PCI-DSS is not a European regulation but a private international standard developed by major payment providers like Visa and MasterCard. While not created by France or the EU, it is widely adopted by businesses operating in Europe and enforced through certified integration partners.
www.pcisecuritystandards.org/

Global Experts in Cybersecurity Excellence

Our Mission and Vision

Our vision

To transform cybersecurity across Europe, Africa, and the Middle East by strengthening organizational resilience against tomorrow's threats.

Our mission

To lead the cybersecurity landscape by helping define and implement the standards and regulations that safeguard our digital future.

Our values

- Integrity: We conduct our business with honesty and transparency, building lasting trust with our clients and partners
- Excellence: We pursue the highest standards in all our services, ensuring quality, reliability, and effectiveness.
- Collaboration: We foster teamwork and open communication, encouraging shared knowledge and collective success.
- Innovation: We embrace change and drive creative solutions to address evolving cybersecurity challenges.
- Client-Centricity: Our clients are at the core of everything we do; we tailor our solutions to their needs and objectives.

Global Experts in Cybersecurity Excellence

Leadership

A Team Built on Proven Expertise

Our Founders

Driven by a shared ambition to innovate and secure the digital world, our founders collectively bring more than 25 years of experience across key disciplines, including:

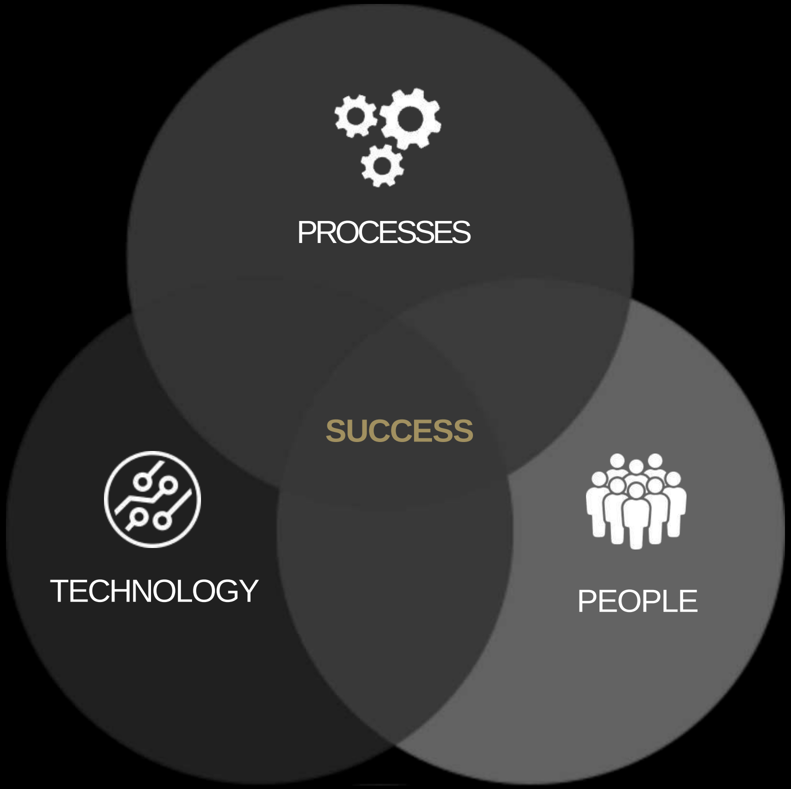
- Management and cybersecurity
- Information technologies
- Television broadcasting

Recognition and Leadership

Recognized both individually and collectively as thought leaders in the cybersecurity domain, our leadership team distinguishes itself through visionary thinking and measurable impact. Acting as a driving force behind digital transformation and organizational resilience, they bring strategic insight and an innovative mindset to every challenge..

Anticipate, Protect, Secure

The Foundations of Effective Cybersecurity



A Holistic Approach to Optimal Protection

A comprehensive cybersecurity program relies on an integrated framework that brings together people, processes, and technology. This synergy is essential to proactively anticipate and counter cyber threats.

People

They form the first line of defense. This pillar emphasizes the creation of a strong security culture through awareness, education, and continuous training across the organization.

Processes

Processes involve the implementation of policies, procedures, and regulatory frameworks that structure and guide best practices in cybersecurity.

Technology

Technology plays a key role in the deployment and maintenance of a resilient infrastructure—enabling organizations to effectively defend against cyber threats.

A balanced approach across these three pillars ensures both the success and long-term sustainability of cybersecurity strategies.

Anticipate, Protect, Secure

A global approach to securing your infrastructure and data

Compliance & Risk Management

- Support throughout your regulatory compliance journey
- Guidance on aligning with ISO 27001, GDPR, NIS2, DORA and PCI-DSS requirements
- Includes audits, documentation support, and strategic compliance planning
- Assessment and implementation of cybersecurity policies tailored to each organization
- Advisory support to evaluate current practices and close security gaps
- Helps define governance, risk mitigation plans, and internal controls

ISO 27001

PCI DSS COMPLIANT

RGPD Règlement Général de la Protection des Données

Swift

NIS2

DORA Digital Operational Resilience Act

ANAT Security Solutions
Security Awareness

Building a culture of vigilance against cyber threats

What is security awareness?

- Understanding risks and best practices
- Ongoing training for employees

Why is it important?

- Reduces human error
- Strengthens the cybersecurity culture

ANAT Security Offering

- Embedding cybersecurity into daily routines to reduce human risk and raise awareness about common threats (phishing, social engineering, ransomware)
- Hands-on exercises and attack simulations to build reflexes
- Ongoing communication about emerging threats and best practices
- Full alignment with international security standards

How ANAT Security Meets Your Needs

Strategic advisory services for robust cybersecurity frameworks

A Personalized Approach

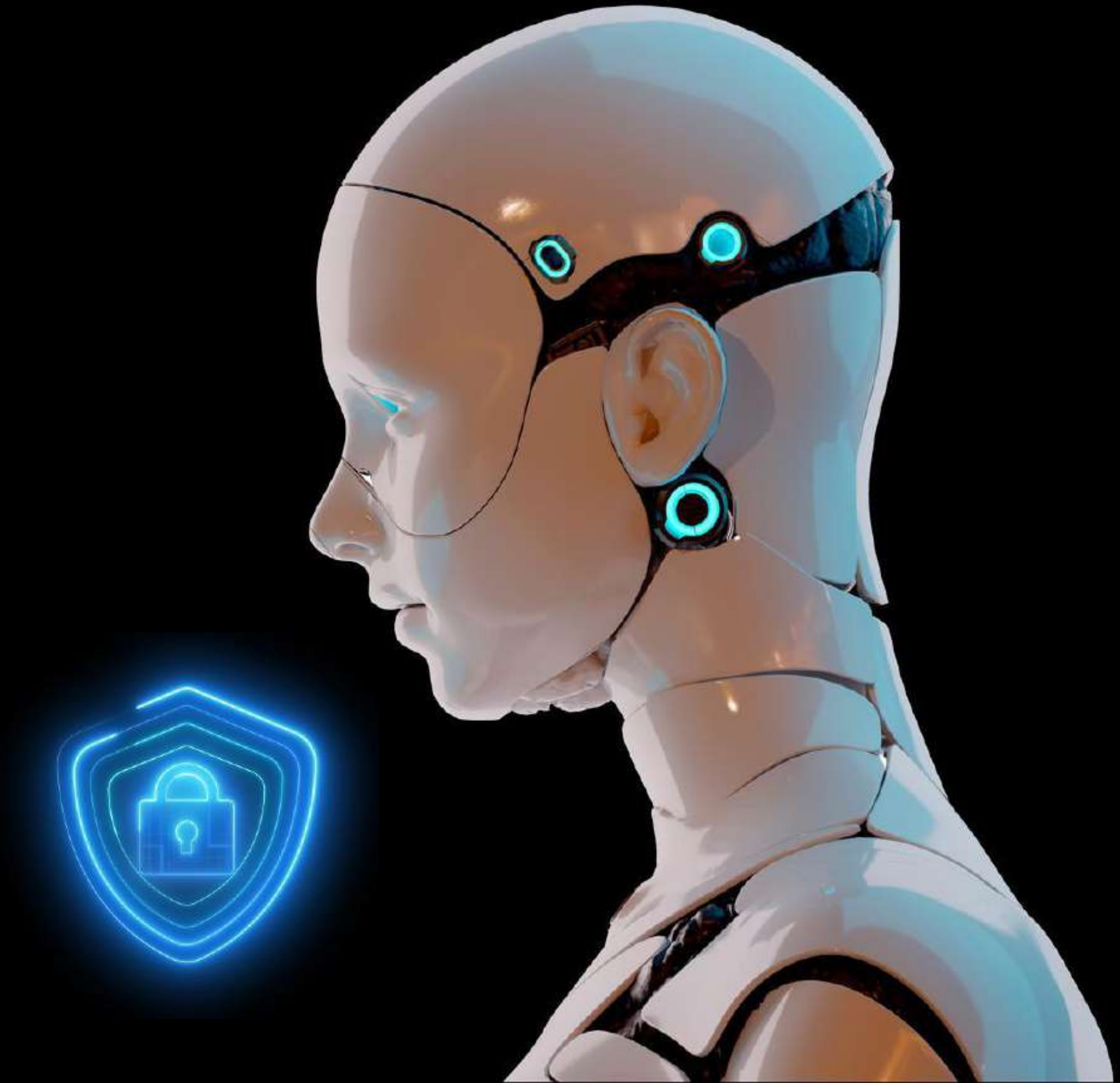
- ANAT Security tailors its consulting methodology to your business environment to provide a precise assessment of your cybersecurity posture.
- Our experts conduct structured interviews and documentation reviews to identify vulnerabilities and deliver actionable, risk-based recommendations.

Aligned with International Standards

- Our advisory services are based on globally recognized frameworks, including ISO 27001, PCI-DSS, NIST, NIS2, DORA, and GDPR.
- We help you document and align your internal processes to meet regulatory and contractual obligations.

Strategic Risk Anticipation

- By helping you anticipate threats, we support the development of strategic defenses against targeted attacks.
- Our consulting approach empowers your teams to make informed decisions and improve long-term cyber risk management..



Ask me anything