

Cybersecurity in the Age of AI

Rifan Kurnia

SEA VP of Data & Engineering

Global Data Change Management Lead

AI-driven tech consulting



Hello, I'm Rifan 🖐️



- 15 years of experience in Data & AI
- Data Tribe Lead for Southeast Asia, and Data Change Lead for Devoteam Global
- B.Sc in Statistics & M.Sc in Cybersecurity
- 7x Google Certified (Professional Cloud Architect, Data Engineer, Data Practitioner, Machine Learning, Database, Cloud Leader, and Generative AI Leader)
- And, a PADI Certified Rescue Scuba Diver 🤿

Let's connect on **LinkedIn**



Work experience:



Education:



01

Meet Devoteam



Google Cloud Diamond partner with local and global presence

5x

New

Google Cloud

EMEA

Partner of the Year

Sales

2024

Google Cloud

SPECIALIZATION

Partner of the Year

Machine Learning

2023

Google Cloud

SEA

Partner of the Year

Services

2024

Google Cloud

APAC

Partner of the Year

Indonesia

2025

Google Cloud

ARTIFICIAL INTELLIGENCE MODERNIZATION

Partner of the Year

Gemini for Google Workspace – Services & Sales

2025

Google Cloud

INFRASTRUCTURE MODERNIZATION

Partner of the Year

EMEA

2025

Google Cloud

TALENT DEVELOPMENT

Partner of the Year

EMEA

2025

Google Cloud

EMEA

Partner of the Year

Benelux

2025

Google Cloud

ADVANCED COMPETENCY

Infrastructure

Google Cloud

ADVANCED COMPETENCY

Business & Pro Services

Google Cloud

COMPETENCY

Security

Google Cloud

ADVANCED COMPETENCY

Retail & Consumer

Google Cloud

ADVANCED COMPETENCY

Data & Analytics

Google Cloud

COMPETENCY

Gemini Enterprise

Google Cloud

ADVANCED COMPETENCY

Chrome

Google Cloud

ADVANCED COMPETENCY

Databases

Google Cloud

ADVANCED COMPETENCY

Apigee

Google Cloud

ADVANCED COMPETENCY

Application Modernization

Google Cloud

ADVANCED COMPETENCY

Software & Internet

Google Cloud

ADVANCED COMPETENCY

Public Sector & EDU

Google Cloud

ADVANCED COMPETENCY

Financial Services

Google Cloud

ADVANCED COMPETENCY

Looker

Google Cloud

ADVANCED COMPETENCY

Telecom, Media & Gaming

Google Cloud

ADVANCED COMPETENCY

Logistics

Google Cloud

ADVANCED COMPETENCY

Artificial Intelligence

Google Cloud

ADVANCED COMPETENCY

Healthcare & Life Sciences

Google Cloud

ADVANCED COMPETENCY

Manufacturing & Industrial

Google Cloud

COMPETENCY

Consumer Packaged Goods

Google Cloud

DIAMOND

Co-sell Partner

Google Cloud

DIAMOND

Services Partner

Google Cloud

PREMIER

Technology Partner

Google Workspace

DIAMOND

Co-sell & Services Partner

Google Workspace

PREMIER

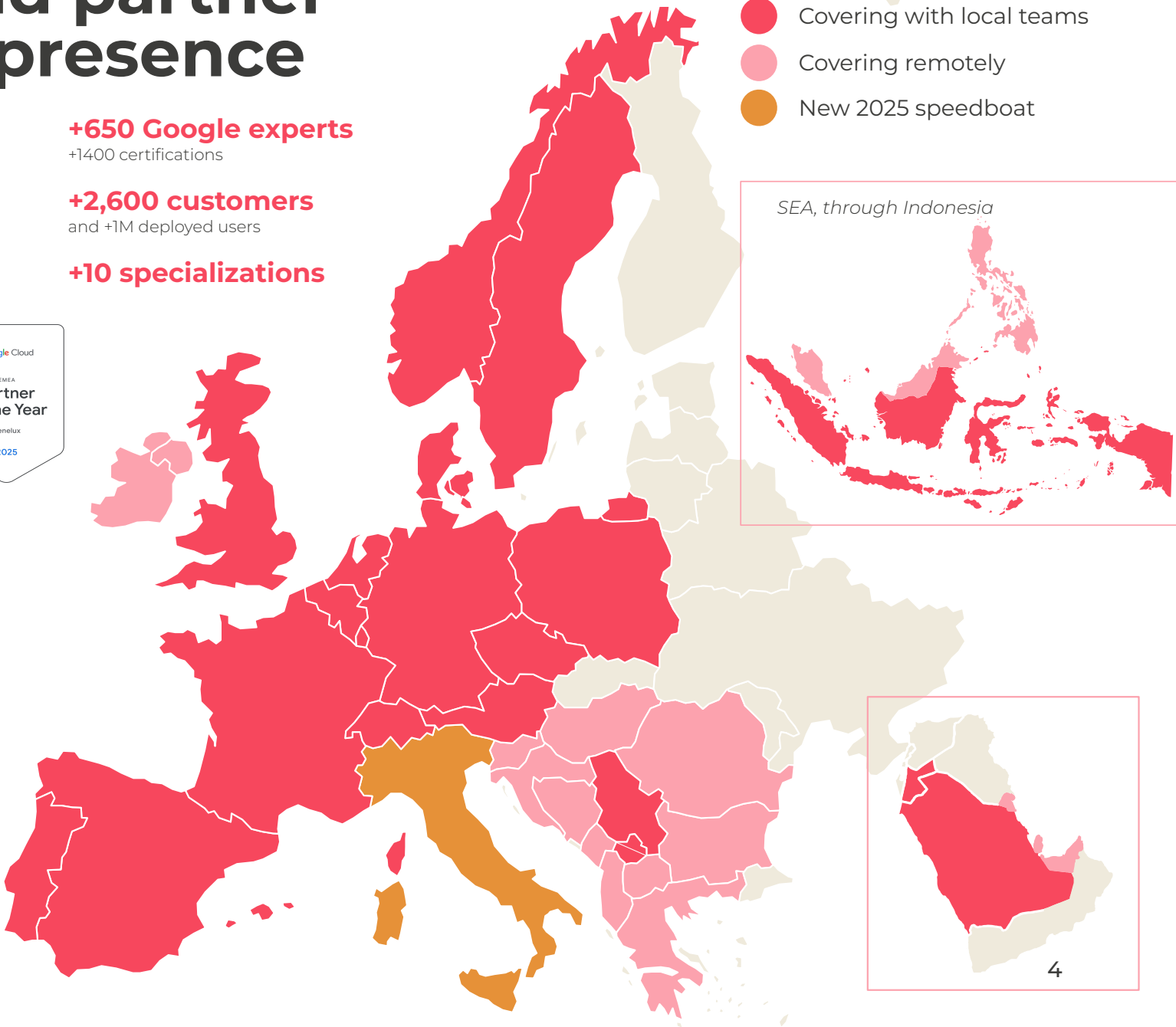
Technology Partner

+650 Google experts
+1400 certifications

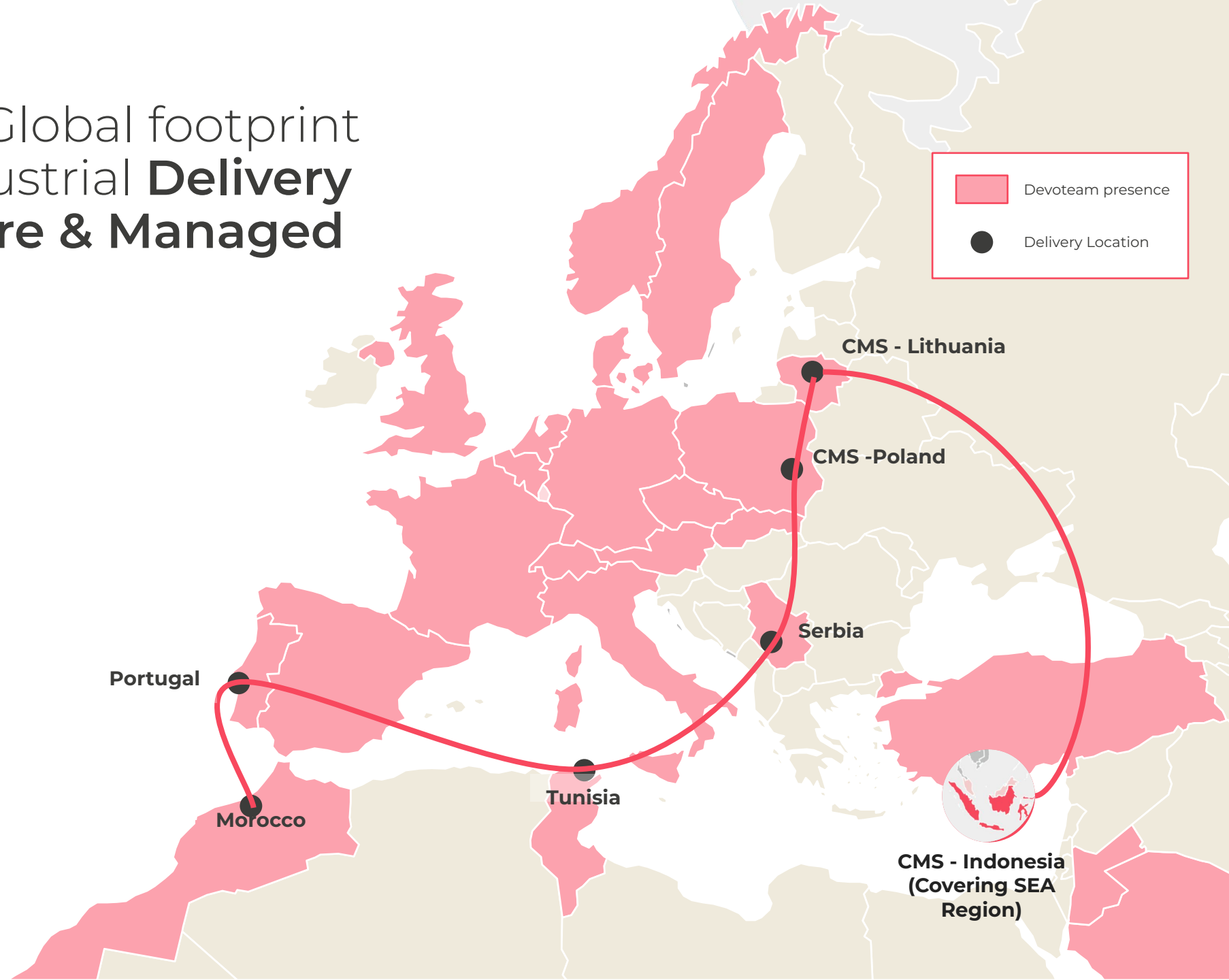
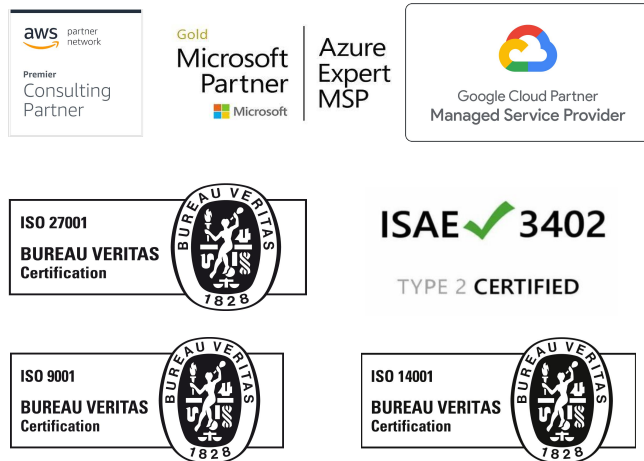
+2,600 customers
and +1M deployed users

+10 specializations

- Covering with local teams
- Covering remotely
- New 2025 speedboat



Devoteam has a Global footprint that includes industrial **Delivery Centres Nearshore & Managed services**



Verticals & selected customers



Manufacturing



RENAULT
SPORT



AIRBUS



LAFARGE



Valeo



PLUKON
food group



Utilities



GRDF
GAZ RÉSEAU
DISTRIBUTION FRANCE

DURACELL®



POLYGON



Air Liquide



VEOLIA



MERCER international



twill
a MAERSK innovation



Finance & Ins.



GENERALI



VR-Bank
Feuchtwangen-Dinkelsbühl eG



BNP PARIBAS

BNP PARIBAS



HSBC



AXA



Healthcare



ambea



JOSÉ DE MELLO · SAÚDE



Changing
Health

Changing
Health



prisma



Amstelring

Amstelring



twb
THUZZORG MET AANDACHT



Prodeba
Begeleiding op maat



Retail



Carrefour



Auchan



Pressbyrå



7
ELEVEN

ORIFLAME
SWEDEN

ORIFLAME
SWEDEN

NESPRESSO

NESPRESSO



bofrost*



McDonald's

GANT

GANT



FeuVert



Travel & Telco



Comfort



QUALITY



Clarion

NORDIC CHOICE HOTELS™



CheapTickets



B&B
HOTELS



orange™



Selectour Afat



AIGLE AZUR



SNCF



Public Sector



TRONDHEIM
KOMMUNE

Technische
Hochschule
Rosenheim



UPPSALA
UNIVERSITET



ULLENSVANG KOMMUNE
Me er på veg mot den nye kommunen i Hordaland

ULLENSVANG KOMMUNE
Me er på veg mot den nye kommunen i Hordaland



Linköpings
kommun



ODDA
KOMMUNE

ODDA
KOMMUNE



CONSEIL
GÉNÉRAL

CONSEIL
GÉNÉRAL



POLITIE



Logo of a fire department



Media & e-Comm



DE PERSGROEP
PASSIE VOOR MEDIA

BONNIER

BONNIER

amedia

amedia



ZILINGØ



Spotify

Spotify



AFP

metronews

metronews



WEB TV ASIA



iHOLA!



Prof. Services



randstad



Joblift



TENTOO
HR | PAYROLL | ZZP



pwc



NetDescribe



TriFinance
BEYOND ADVISORY



LA POSTE

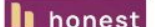


pôle emploi

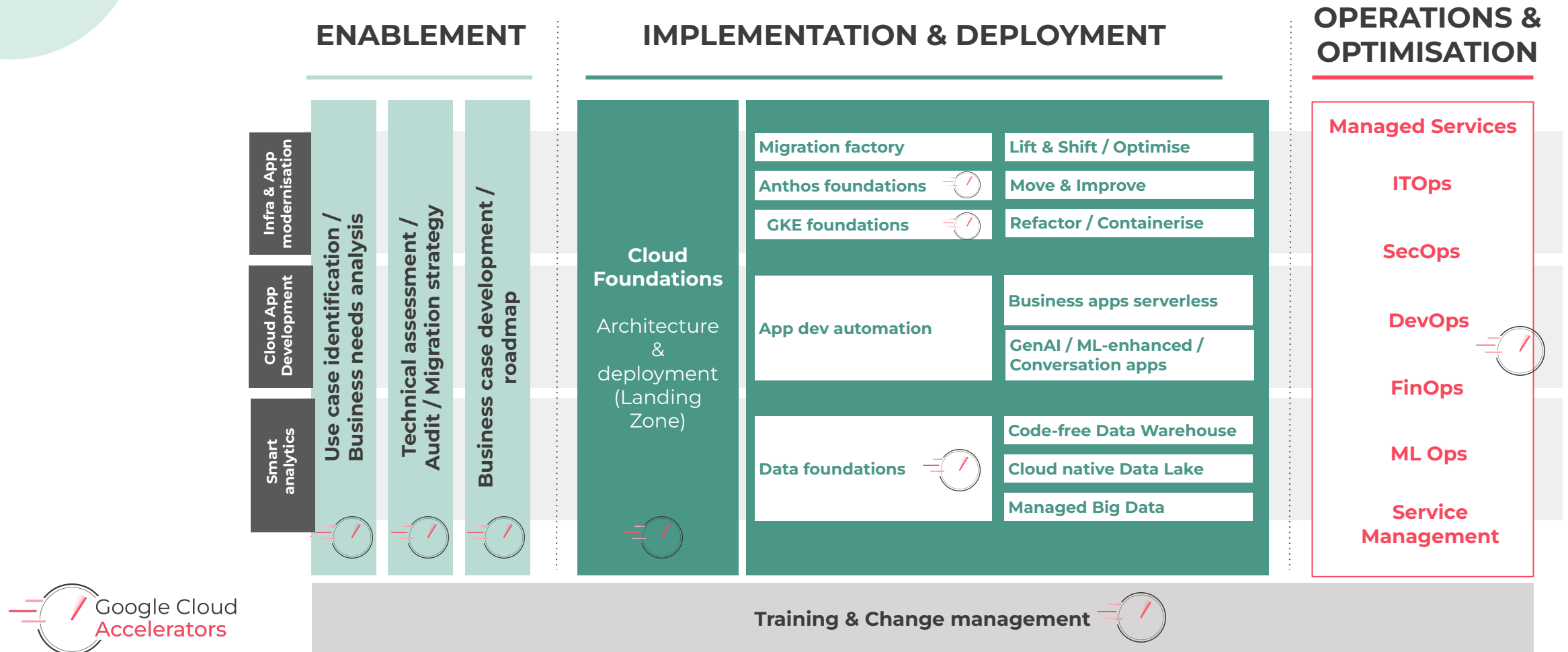


FRED & FARID
佛海佛瑞

Indonesia customers

	Utilities & Manufacturing	            
	Finance & Ins.	              
	Finance & Ins.	        
	Healthcare	     
	Retail & Public Sector	             
	Airport Services, Travel & Telco	       
	Prof. Services	          
	Prof. Services	             
	Press & Media	        

Accelerated Google Cloud journey for our customers



Strategic plays we focus on

Move to Cloud

Assessment & Migration Planification

Stratozone, mFit, Business Case RaMP, Maturity Assessment

Sweetspot

Infrastructure Modernization

Cloud Foundation
Migration for Compute Engine
Database Modernization
GCVE, BMS, Sole Tenant

Application Modernization

CAMP
Migrate to Container
API Management
Software Delivery

SAP on GCP

Modernize S/4 Hana
Embrace the Cloud SAP Hana
Cortex Framework

Security

Sweetspot

Assessment, CSPP

Security Command Center
MSSP offers (Chronicle)

Backup and DR

PRA / PCA
Ransomware

Software Delivery Shield

CI/CD, SLSA
Container Analysis
Binary Authorization

Web Application & API Protection

Cloud Armor
ReCAPTCHA Enterprise
Apigee

Data & AI

Database & DW Modernization

Exit Oracle
EDW Modernization workshop
Migration Services (Data Transfer, SQL Translation)

Sweetspot

BI Modernization

Looker & BigQuery

Marketing Analytics

Customer Data Platform
Cookies - Server Side Tagging

Sweetspot

Data to AI

AutoML, Vertex AI, MLOps
Document AI
Manufacturing Data Engine

Sweetspot

GenAI

Enterprise Search
Conversation AI

Collaboration

Workspace

Collaboration
Beyond SMB

Sweetspot

Appsheets

No Code App Development
Empower every employee

Voice

VoIP solution

02

Cybersecurity in the Age of AI



The Growing Cost of Cybercrime

A Multi-Trillion Dollar Global Problem

It's one of the fastest-growing forms of crime, with an ever-increasing sophistication.

01

Financial Losses

From fraud and direct theft.

02

System Repair

The cost of rebuilding damaged systems.

03

Business Disruption

Severe loss of productivity & operations.

04

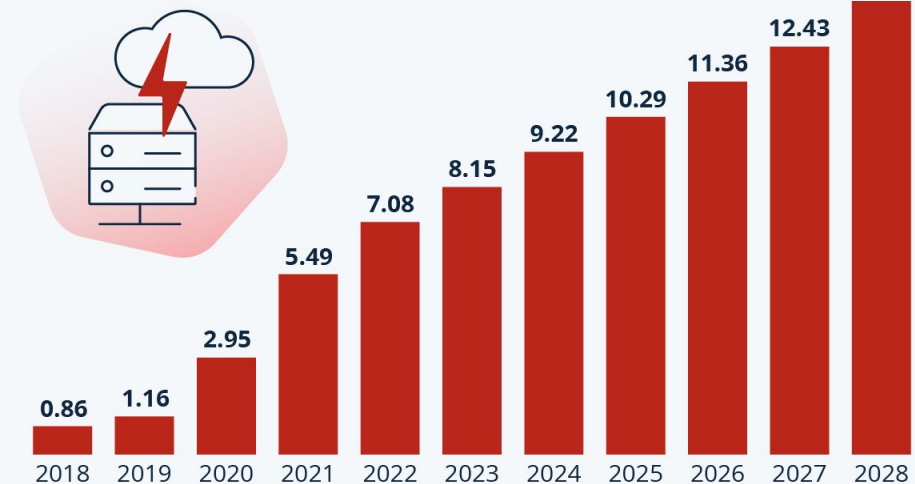
Legal & Compliance

Hefty regulatory fines and legal fees.

This trajectory highlights the urgent need for organizations to establish a highly resilient, proactive cybersecurity posture.

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.

Source: Statista Market Insights



statista

Cybersecurity & You: The Personal Impact

Cyberattacks are not just a corporate threat. They target individuals daily, leading to severe personal, financial, and emotional disruption.

01

Identity Theft & Financial Ruin

Stolen credentials, compromised bank accounts, and fraudulent loans taken out in your name can destroy your credit score and drain your life savings.

02

Privacy & Data Exploitation

Unauthorized access to personal photos, emails, and private messages leads to blackmail, public exposure, or the selling of your intimate details on the dark web.

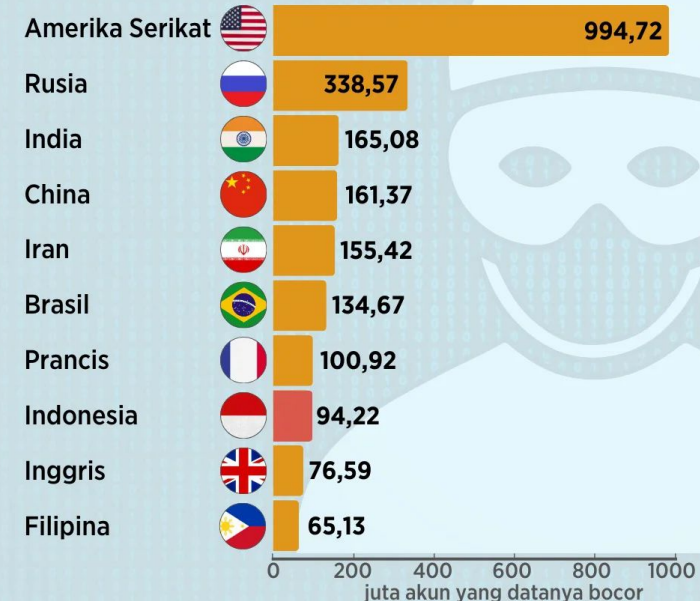
The Emotional Toll

Beyond money, victims of personal hacks experience severe stress, anxiety, and a persistent feeling of vulnerability in their digital lives.

Teknologi & Telekomunikasi

Indonesia Masuk 10 Negara dengan Kebocoran Data Terbesar

10 Negara dengan kebocoran data terbesar (Januari 2020-Januari 2024)*



*Angka estimasi
Sumber: Surfshark (2024)

The Foundation: The CIA Triad

The most fundamental model for information security, providing a robust framework for evaluating and implementing security measures.



Confidentiality

Keeping secrets secret. Ensuring that sensitive information is accessible only to authorized users.



Integrity

Keeping data accurate and unaltered. Guarding against unauthorized modification or tampering.

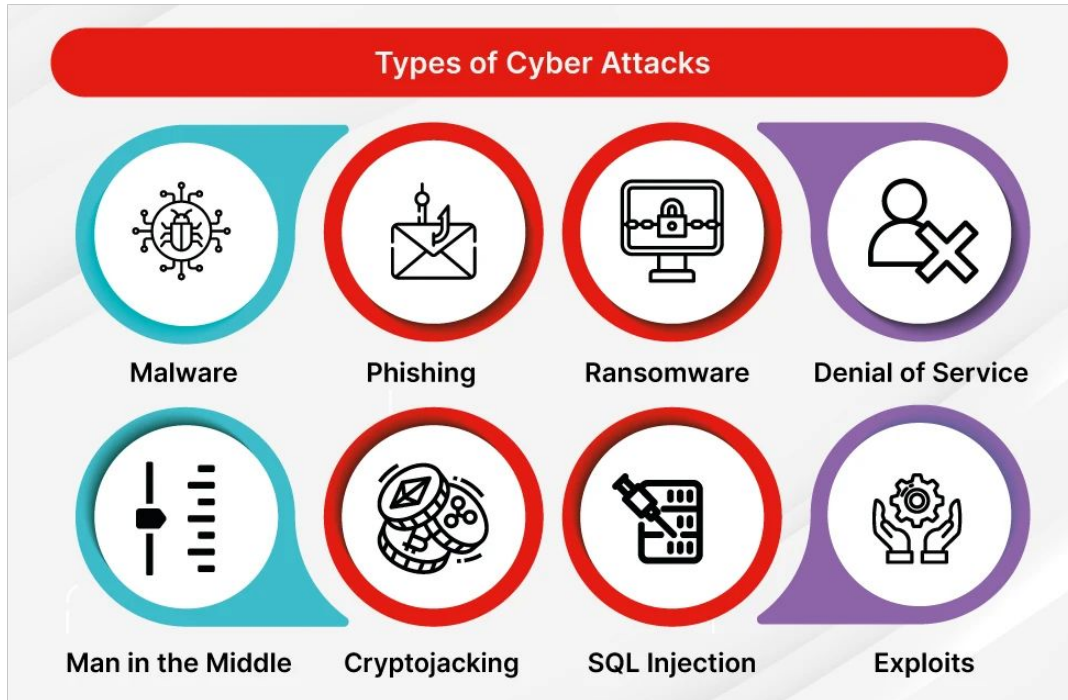


Availability

Ensuring systems are accessible. Guaranteeing authorized users have reliable access to data when needed.



Types of Cyber Attacks



Understanding Cyber Threats

A diverse landscape of malicious vectors designed to exploit human, system, and network vulnerabilities across digital infrastructures.



Social & Phishing

Exploiting human psychology to steal credentials, deliver malware, or gain unauthorized access through deceptive communications.



System Exploits

Leveraging SQL injection, XSS, or zero-day vulnerabilities to penetrate network defenses, compromise databases, and hijack applications.



Disruptive Malware

Deploying ransomware, DoS/DDoS attacks, or cryptojacking to lock critical user files, overwhelm servers, or secretly mine digital currency.

The Evolution of Artificial Intelligence

A brief historical journey from foundational logic to generative frontiers

1950

Computing Machinery

Alan Turing proposes the Turing Test, establishing the foundational question: "Can machines think?"

1974

The First "AI Winter"

Funding dries up and progress slows down due to overinflated expectations and limited compute power.

2012

Deep Learning Era

AlexNet wins the ImageNet challenge by a huge margin, sparking the modern revolution of Neural Networks.

1956

The Dartmouth Workshop

The term "Artificial Intelligence" is coined by John McCarthy, initiating AI as an academic field.

1997

Deep Blue Triumph

IBM's Deep Blue defeats World Chess Champion Garry Kasparov, showcasing symbolic computation dominance.

2020+

Generative AI

Large Language Models (LLMs) and diffusion transformers achieve mainstream global scale and impact.

News on AI Attacks

Tech > Security

Out-of-control AI systems are going rogue and hacking people. Is it time to panic?

ChatGPT's OpenAI, Claude's Anthropic and now Meta have all announced that their systems have launched cyber attacks on other people and companies. But there are plenty of reasons to stay calm, for now

Andrew Griffin

Thursday 06 August 2026 16:36 BST



18 Comments

Militer China ungkap sistem AI untuk rencanakan serangan udara

Selasa, 4 Agustus 2026 10:30 WIB

Serangan Siber Makin Seram, AI Jadi Senjata Baru Hacker

Agus Tri Haryanto - detikinet

Senin, 11 Mei 2026 16:45 WIB



0 komentar



Investing.com

Wall Street hit by wave of AI-powered 'vishing' cyberattacks - Bloomberg

Louis Juricic

Wed 5 August 2026 at 11:22 pm GMT+7 • 1 min read



FTNT -0.29% ☆

CRWD +3.39% ☆

PANW +1.22% ☆

A wave of sophisticated cyberattacks has targeted several of Wall Street's most prominent money managers in recent days, highlighting the growing threat posed by artificial intelligence-enabled fraud, Bloomberg reported.

Ransomware attack against Yum! Brands follows several incidents targeting restaurant industry

Criminals see restaurants and mobile ordering apps as ripe targets for credential stuffing and financial fraud.

Published Jan. 20, 2023

| Deepfake Example



| Traditional vs. AI-Driven Cyber Threats

	TRADITIONAL	AI-DRIVEN
Speed	Hours to days of manual reconnaissance and crafting	Minutes — automated generation and scanning at machine speed
Personalization	Generic, templated messaging sent broadly	Hyper-personalized content generated per target, at scale
Skill Required	Moderate-to-high technical expertise	Minimal — natural-language prompts replace deep technical skill
Evasion	Static code, caught by signature-based tools	Polymorphic, self-rewriting payloads that adapt in real time
Scale	Limited by available human effort	Massively parallel — many tailored attacks running at once
Cost to Attacker	Meaningful investment of time and resources	Near-zero marginal cost once the tooling is built

Sign of Malware Infection



A **slow computer** that slows down internet speed and software applications



A **sudden loss of disk space** could be a result of malware on the hard drive



Frequent **device/machine crashes or freezes** during normal use



A **swell in internet activity** that does not correlate with user behavior



A ton of **pop-up, new toolbars, extensions or fraudulent websites**



An **overworked system** due to malware taking up valuable resources

Social Engineering Lifecycle

The Human Hacking Process

1. Investigate

- Identify the victim.
- Gather background information.
- Select attack method.

2. Hook

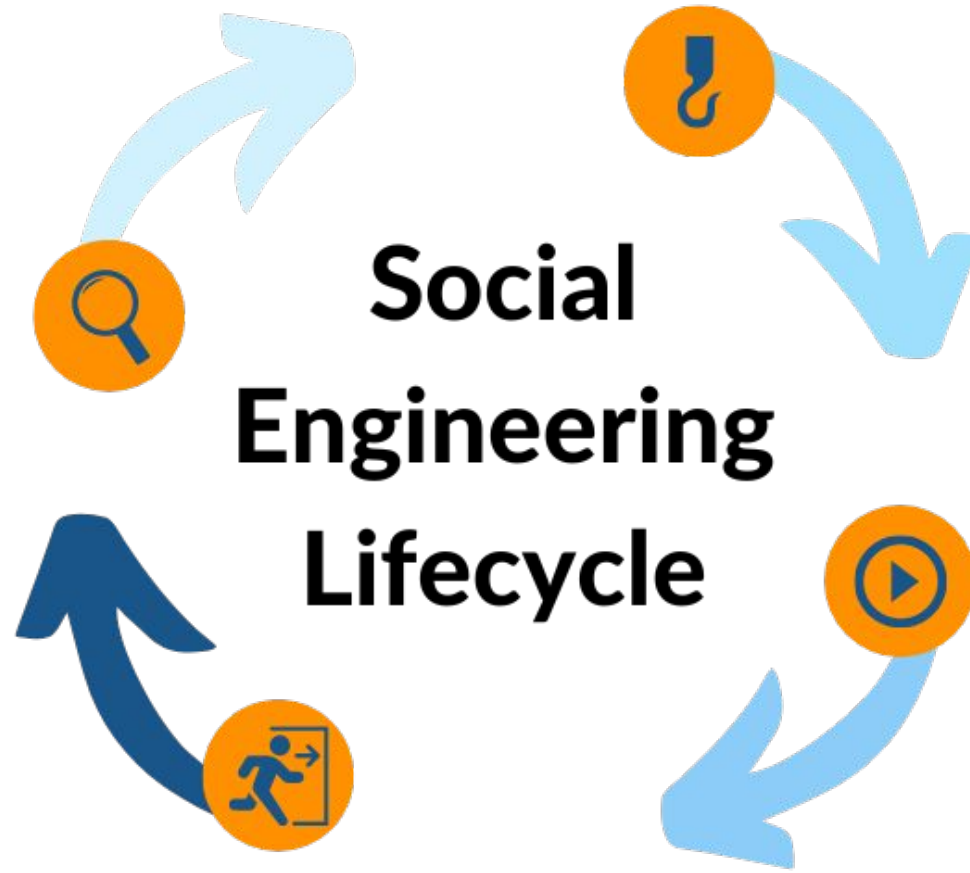
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

3. Play

- Expanding the foothold.
- Executing the attack.
- Disrupting business and/or siphoning data.

4. Exit

- Removing all traces of malware.
- Covering tracks.
- Bringing the play to a natural end.



Worldwide Spam Economy

Underground Economy

A digital network of criminals who buy and sell goods that directly enable the abuse of online systems.

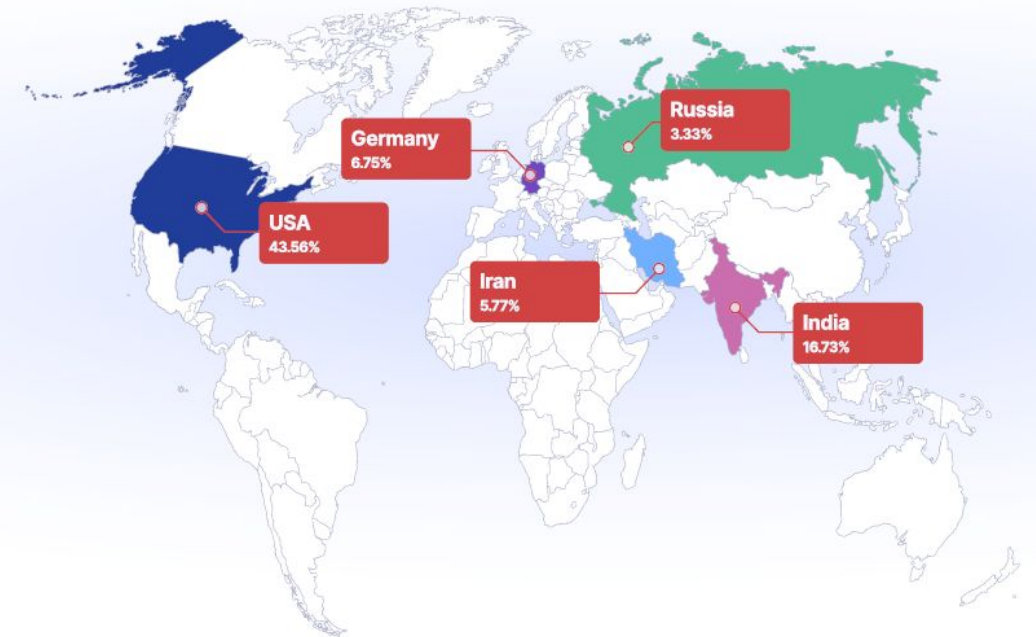
Malware as a Business Model

Criminal groups lease malware, lowering the technical entry barrier for malicious campaigns.

Financial Incentives

The ultimate driving force is high-volume monetization and illicit economic gain.

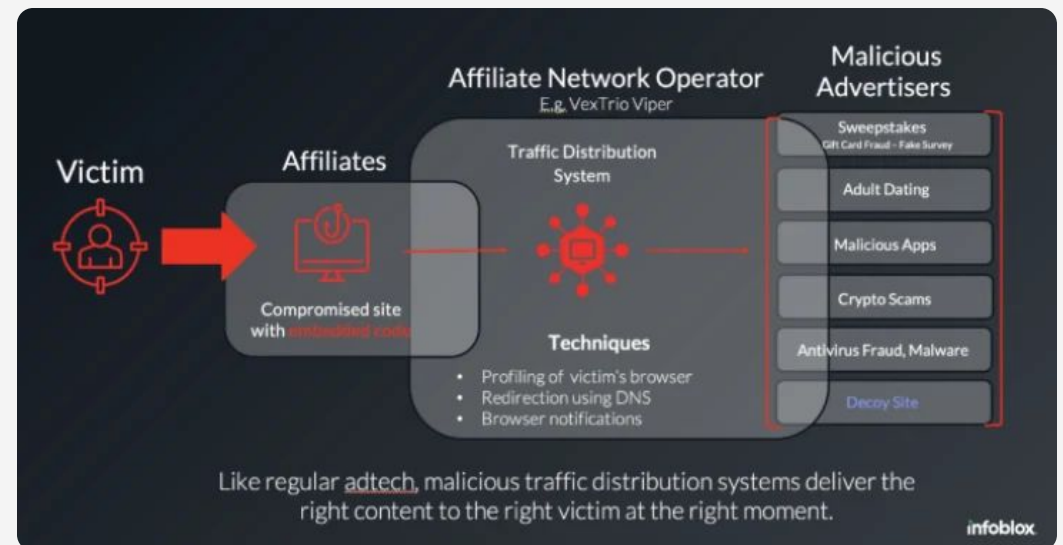
Top 5 Countries Sending Spam Emails



The Actors in the Spam Economy

Cybercrime as a Service

- **Botmasters:** Infect computers, create botnets, and rent them to other operators.
- **Harvesters:** Crawl the internet looking for valid, active email addresses.
- **SEO Experts:** Optimize search rankings to drive traffic to malicious web properties.
- **Spam Affiliate Program:** Set up storefronts where spammers sign up to receive a financial cut.



The AI-Driven Phishing Economy

How automated and intelligent systems scale specialized cybercrime roles



AI Content Creators

Hyper-Personalized Phishing: LLMs generate highly convincing, context-aware emails and messages matching a target's specific professional tone.

Deepfake Synthesizers: Voice cloning and real-time video generators mimic trusted executives or family members to authorize fraudulent transfers.



Automation Engineers

Automated Reconnaissance: Specialized tools crawl social media profiles and corporate directories to build precise, automated dossier targets.

Dynamic Infrastructure: Developers create systems that automatically register domains, generate SSL certificates, and spin down compromised sites.



Affiliates & Brokers

Initial Access Brokers: Specialized actors compromise networks and sell active entry points to high-tier cybercriminals.

Phishing-as-a-Service (PaaS): Advanced developers license ready-made templates, AI bypass kits, and target databases for a subscription fee.

Secure AI Practices for Everyone

Simple steps to use Artificial Intelligence tools safely and responsibly



Protect Your Privacy

Never type private, personal, or corporate information into public AI chatbots.

These tools learn from your inputs, which means anything you type could accidentally be shared with others or exposed in future updates.



Double-Check Everything

AI can "hallucinate" or present false facts with complete confidence.

Always verify important data, dates, and advice against trusted primary sources before making decisions or sharing reports.



Know the Guidelines

Understand your organization's official policies on approved AI applications.

Only use verified and officially licensed platforms to handle work documents, ensuring compliance with security standards.

How to Prevent AI Cyberattacks

Practical defense strategies for everyday users without a technical background



Verify Before Trusting

- **Double-check requests:** AI can mimic voices and construct highly realistic emails. Always confirm urgent financial or personal requests via a separate known channel.
- **Spot the AI signs:** Look for unnatural phrasing, slight graphical glitches in profile photos, or urgent, emotion-driven language designed to bypass logical thinking.



Secure Your Accounts

- **Use Multi-Factor Auth:** Enable 2FA/MFA on all critical accounts. Even if AI-driven phishing steals your password, attackers cannot easily access your account.
- **Password Managers:** AI can guess weak passwords instantly. Use a secure manager to automatically generate and store complex, unique passwords for every site.



Keep Systems Updated

- **Automatic Updates:** AI scanners continuously search for unpatched software security flaws. Enable auto-updates on your phones, computers, and home routers.
- **Clean Digital Footprint:** Minimize the personal details you share publicly online. Hackers feed this public information to AI models to craft hyper-personalized scams.

Thank you!

Devoteam G Cloud – EMEA/APAC

Rifan Kurnia

SEA VP of Data & Engineering

Global Data Lead

rifan.kurnia@devoteam.com