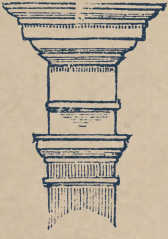


# WEEKLY DIGEST

## GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 17 MAY – 23 MAY 2026





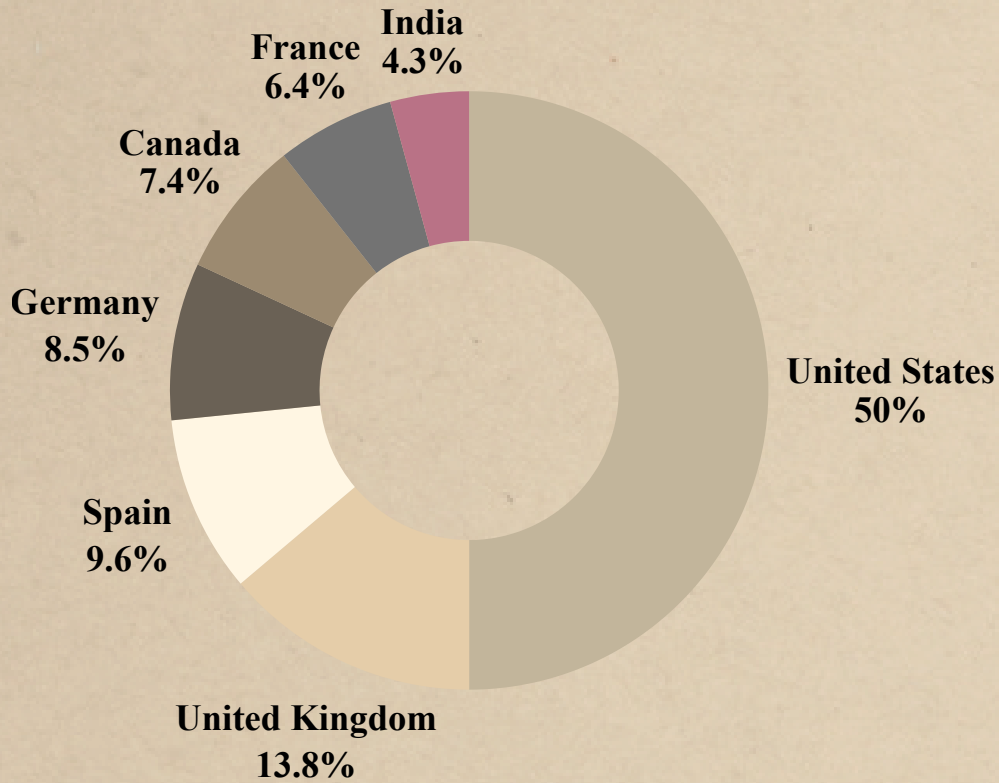
# GLOBAL DATA BREACH REPORT

\* REPORTING PERIOD: 17 MAY - 23 MAY 2026

## Overview

This weekly report provides an overview of global data breach activity linked to threat groups. It focuses on exposure patterns, threat actor activity, and key trends observed across industries and geographies.

## Geographic Distribution

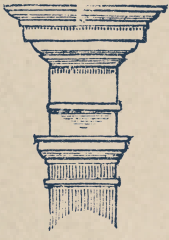


## Key Highlights

- The majority of incidents were associated with ransomware and data extortion operations, underscoring the continued activity of financially motivated threat actors.
- Groups such as **Qilin**, **Nova**, **Akira**, and **APT73** were repeatedly identified, indicating sustained and coordinated cyberattack campaigns.

**Most Targeted Sector: Manufacturing**  
**Ransomware-linked breaches: 87.8%**

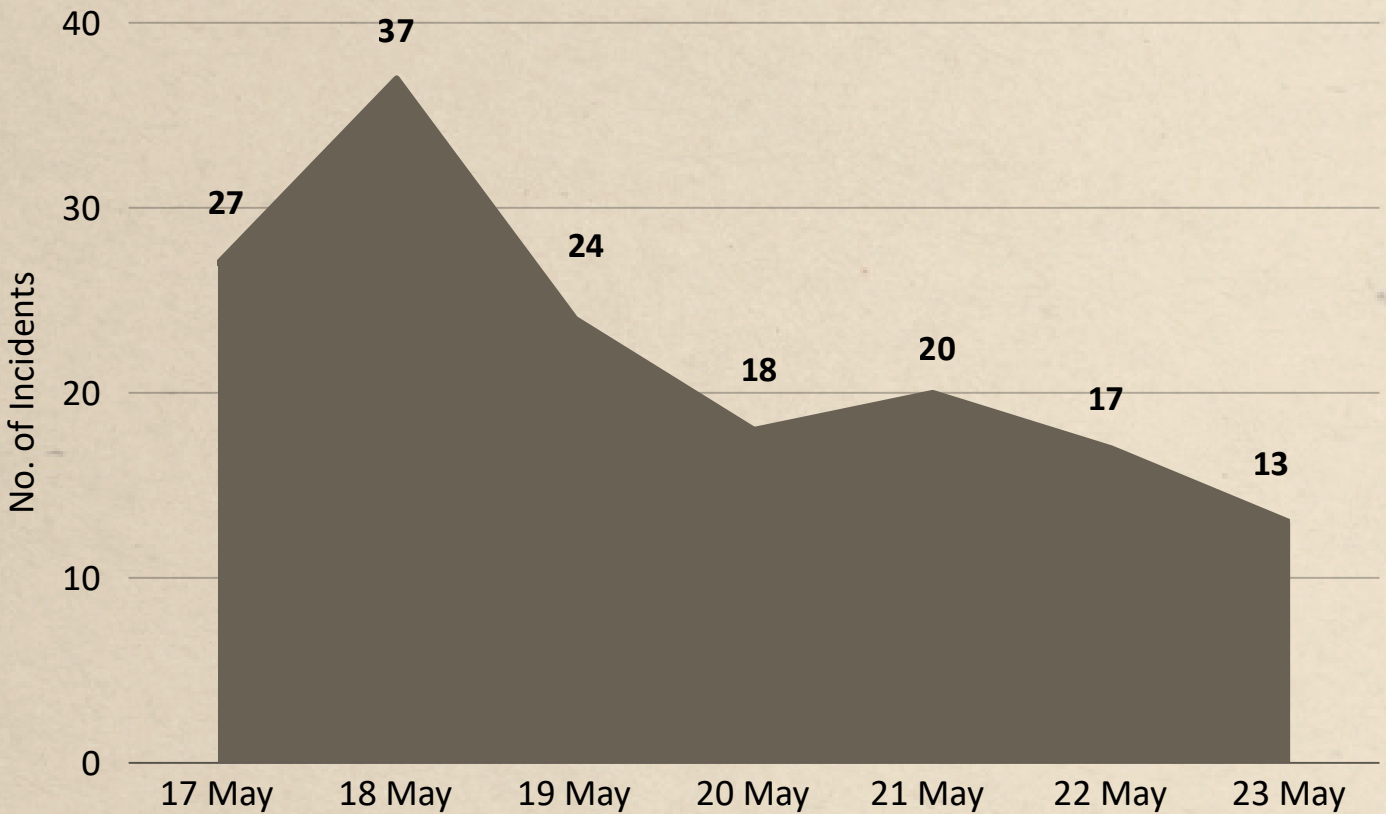
**Total Breaches Observed: 156**  
**Countries Affected: 40**



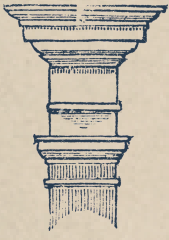
# GLOBAL DATA BREACH REPORT

\* REPORTING PERIOD: 17 MAY - 23 MAY 2026

## Breach Over time



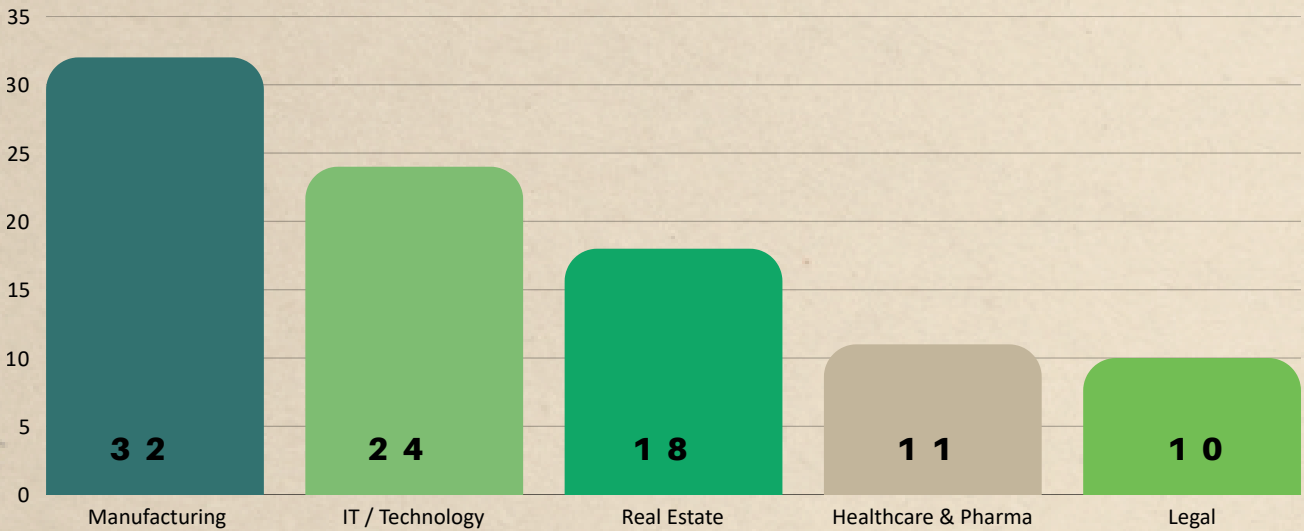
- Breach activity fluctuated throughout the period, with May 18 recording the highest spike at 37 reported incidents.
- A sharp rise was observed between May 17 and May 19, peaking at 27 incidents on May 17, indicating intensified disclosure or attack activity.
- May 23 reported the lowest number of incidents, with only 13 breaches observed.
- Overall, the trend reflects irregular but high-impact surges, followed by short periods of decline and stabilization.



# GLOBAL DATA BREACH REPORT

\* REPORTING PERIOD: 17 MAY - 23 MAY 2026

## Affected Sectors

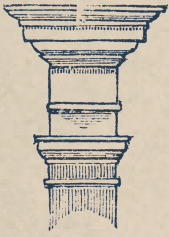


## Industry Highlights

- Manufacturing & Engineering: **32+ incidents** (highest targeted sector)
- IT / Technology: **24+ incidents** (high exposure due to digital infrastructure)
- Real State: **18+ incidents**
- Healthcare & Pharma: **11+ incidents**
- Finance / Legal / Insurance: **10+ incidents**



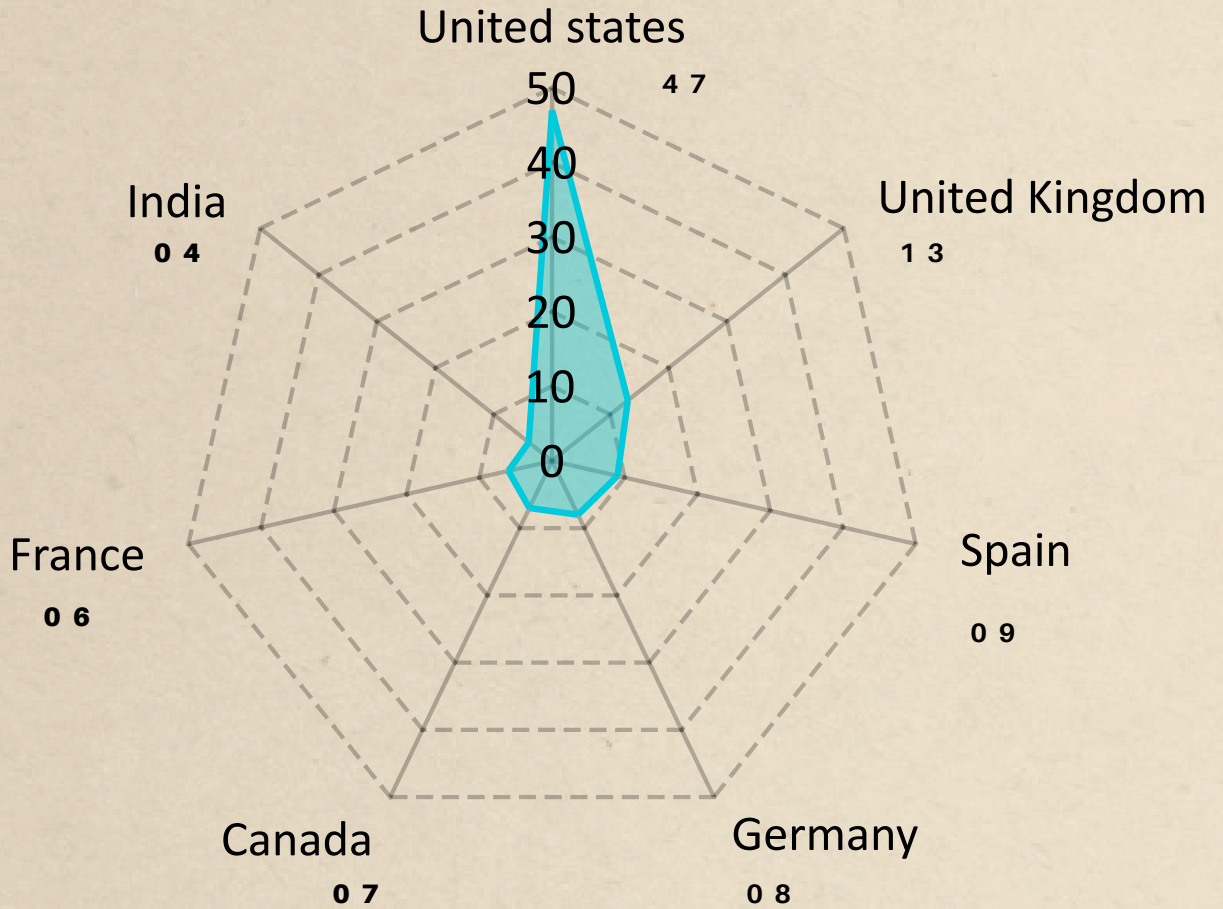
**Industries Insight:** Manufacturing and technology sectors remained the primary focus for threat actors, while construction, healthcare, and financial organizations also faced sustained targeting due to operational dependence and sensitive data exposure.



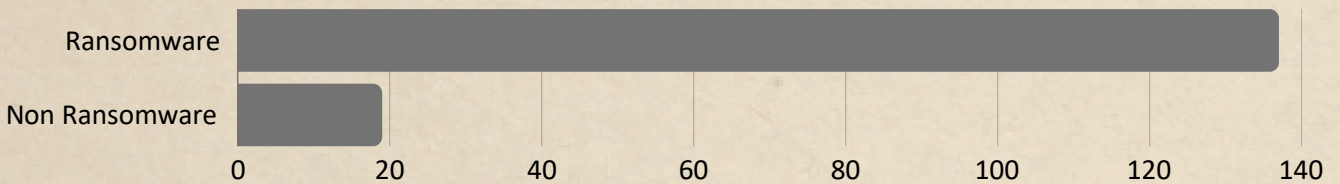
# GLOBAL DATA BREACH REPORT

\* REPORTING PERIOD: 17 MAY - 23 MAY 2026

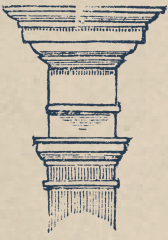
## Affected Countries



## Actor Distribution



Ransomware dominates the threat landscape with 137+ incidents, far outpacing 19 non-ransomware cases, making it the most prevalent and impactful attack type.



# GLOBAL DATA BREACH REPORT

\* REPORTING PERIOD: 17 MAY - 23 MAY 2026

## Venture Yours Breach Incident

On May 18, 2026, a US company Venture Yours suffered a significant data breach during the week, involving potentially sensitive information.

**Company Sector: PropTech / Vacation Rental Management**

**Threat Actor : zSenior**

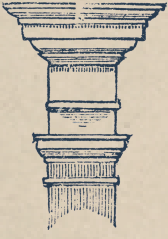
**Data Sold: 64 GB**



## Key Highlights

- **Data Exposure:** Approx 25.5M CSV records and 70K+ files reportedly leaked, including KYC documents, booking details, and customer PII
- **Threat Actor:** Linked to zSenior / BlavoForums
- **Threat Activity:** Shared on underground forum; exposed data allegedly includes driver licenses, rental agreements, emails, and phone numbers
- **Threat Level:** Critical non-ransomware breach with risks of identity theft, fraud, customer privacy violations, and unauthorized account misuse





# GLOBAL DATA BREACH REPORT

\* REPORTING PERIOD: 17 MAY - 23 MAY 2026

## WhatsApp LLC Breach Incident

On May 23, 2026, a USA company WhatsApp LLC suffered a significant data breach during the week, involving potentially sensitive information..

**Company Sector:** Technology

**Threat Actor :** NormalLeVrai


**Data Sold:** 3.78 GB

DATABASE: WHATSAPP.COM 3BILLION [LAST POST]  
By NormalLeVrai - 23-05-26, 09:05 PM

Pages (0): 1 2 Next »

23-05-26, 09:05 PM

**NormalLeVrai**



Banned

Posts: 45  
Threads: 43  
Joined: Apr 2026  
Reputation: 1 Month

WhatsApp is a cross-platform messaging application that allows users to send text messages, make voice and video calls, and share photos, videos and documents over the internet.

Data: ~3 Billion  
Sample:

Quote:

FNAME	LNAME	EMAIL	Cell	Whatsapp	Active	SMS	Delivered	Verified	Date	Address	City	State	Code	Country
George	McCormick	george.,1700@hotmail.co.uk	447816873120	447816873120	YES	18/08/2023	18	northgate	street	gloucester	gloucester	Gloucestershire	GL1 1SE	United Kingdom
Jeremy	Krantz	jeremykrantz@gmail.com	447540768317	447540768317	YES	18/08/2023	7	City East	Business Centre	Belfast	Antrim	BT4 1GW		United Kingdom
Mark	Diney	digitizationhd@gmail.com	447832826327	447832826327	YES	18/08/2023	2	Leicester Royal Infirmary		Leicester	Leicester	LE1 5WW		United Kingdom
Mr	Law	info@priorityrooms.com	447967713269	447967713269	YES	18/08/2023	8	ST. Peter's Court		London	London	NW4 2HG		United Kingdom
Dean	Burton	deburton@hotmail.co.uk	447903113057	447903113057	YES	18/08/2023	57	rotherham	S65 2UP					United Kingdom
George	Paterson	privacy@wzukltd.com	447739085465	447739085465	YES	18/08/2023	27	BURNBANK STRAITON	LOANHEAD	MIDLOTHIAN		EH209NE		United Kingdom
Steven	Leech	l6fche@btinternet.com	447545395738	447545395738	YES	18/08/2023	42	Newbery Close	Reading	Berkshire		RG316JN		United Kingdom
Simon	Blackham	simonblackham@yahoo.co.uk	447480245120	447480245120	YES	18/08/2023	unit 2	swansea	swansea	SAS 4HS				United Kingdom
Ben	Birns	ben.birns@goolemail.com	447827084283	447827084283	YES	18/08/2023	63a	Scott Road		Birmingham		XX B92 7LQ		United Kingdom
Simon	Lynes	simonboymac.com	447972446689	447972446689	YES	18/08/2023	7	Chantry Quarry		Guildford		ENG GU1 3AF		United Kingdom
Domains	Admin	admin@book.kraken.com	447789317956	447789317956	YES	18/08/2023	23	Bury Fields,		Guildford	Surrey	Guildford	GU2 4AZ	United Kingdom
Mark	Eusebe	mmarkusebe@gmail.com	447702867783	447702867783	YES	18/08/2023		Trevalla	Bradfield	Berkshire		RG7 6LG		United Kingdom
Steven	Lewis	slewis2079@gmail.com	447852921378	447852921378	YES	18/08/2023		Flat 3, 6 Glyn Street		New Bradwell	Milton Keynes	Buckinghamshire	MK13 0DD	United Kingdom
Ben	Treblcock	ben.treblcock@hotmail.co.uk	447967709790	447967709790	YES	18/08/2023	527	Ringwood Road		Ferndown	Dorset	BH22 9AQ		United Kingdom

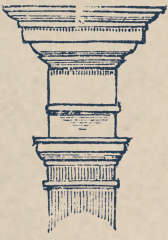
Enjoy your download: <https://anonfilesnew.com/MwMBITgx14/whatsapp.zip>

I also wanted to say goodbye, as this is my last message. As you may have noticed, my activity on the forums has decreased significantly lately, as I've decided to refocus on my personal life and my true priorities. I've greatly enjoyed the discussions and the time spent here, but it's time for me to move on. I now only accept private messages for interviews or media inquiries on Session. (I'm French, by the way.)

Thank you all for these moments.

## Key Highlights

- **Data Exposure:** Alleged leak claims exposure of approximately 3 billion WhatsApp-related records containing phone numbers, emails, and address details
- **Threat Actor:** Linked to NormalLeVrai
- **Threat Activity:** Shared on underground forum with downloadable archive references and sample records posted publicly
- **Threat Level:** Massive non-ransomware data exposure with high risks of phishing, spam campaigns, identity misuse, and large-scale social engineering attacks



# GLOBAL DATA BREACH REPORT

\* REPORTING PERIOD: 17 MAY - 23 MAY 2026

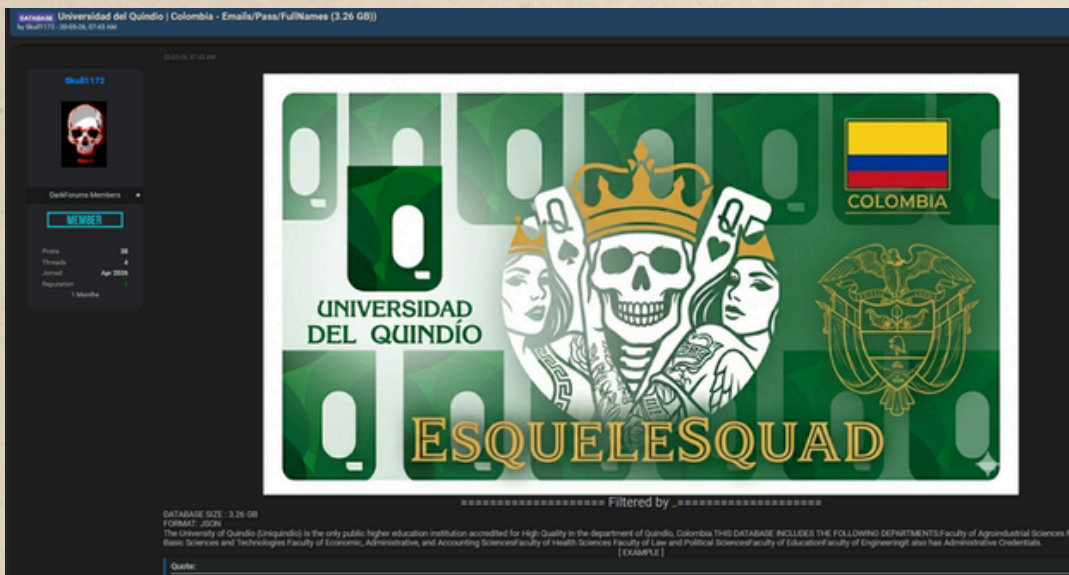
## Universidad del Quindío Breach Incident

On May 20, 2026, a Colombia company Universidad del Quindío suffered a significant data breach during the week, involving potentially sensitive information..

**Company Sector: Higher Education**

**Threat Actor : Skull1172**

**Data Sold: 3.26 GB**



## Key Highlights

- **Data Exposure:** Approx 3.26GB JSON database reportedly leaked, containing emails, passwords, full names, and administrative credential data
- **Threat Activity:** Alleged exposure impacts multiple academic departments and administrative systems of Universidad del Quindío
- **Threat Actor:** Linked to Skull1172 / EsqueleSquad
- **Threat Level:** High-risk academic data breach with potential for credential compromise, phishing attacks, and unauthorized institutional access



# About Castellum Labs

Based in Hyderabad, India with global customer base across India, US, Europe

Started by people with decades of product, services & deep tech experience

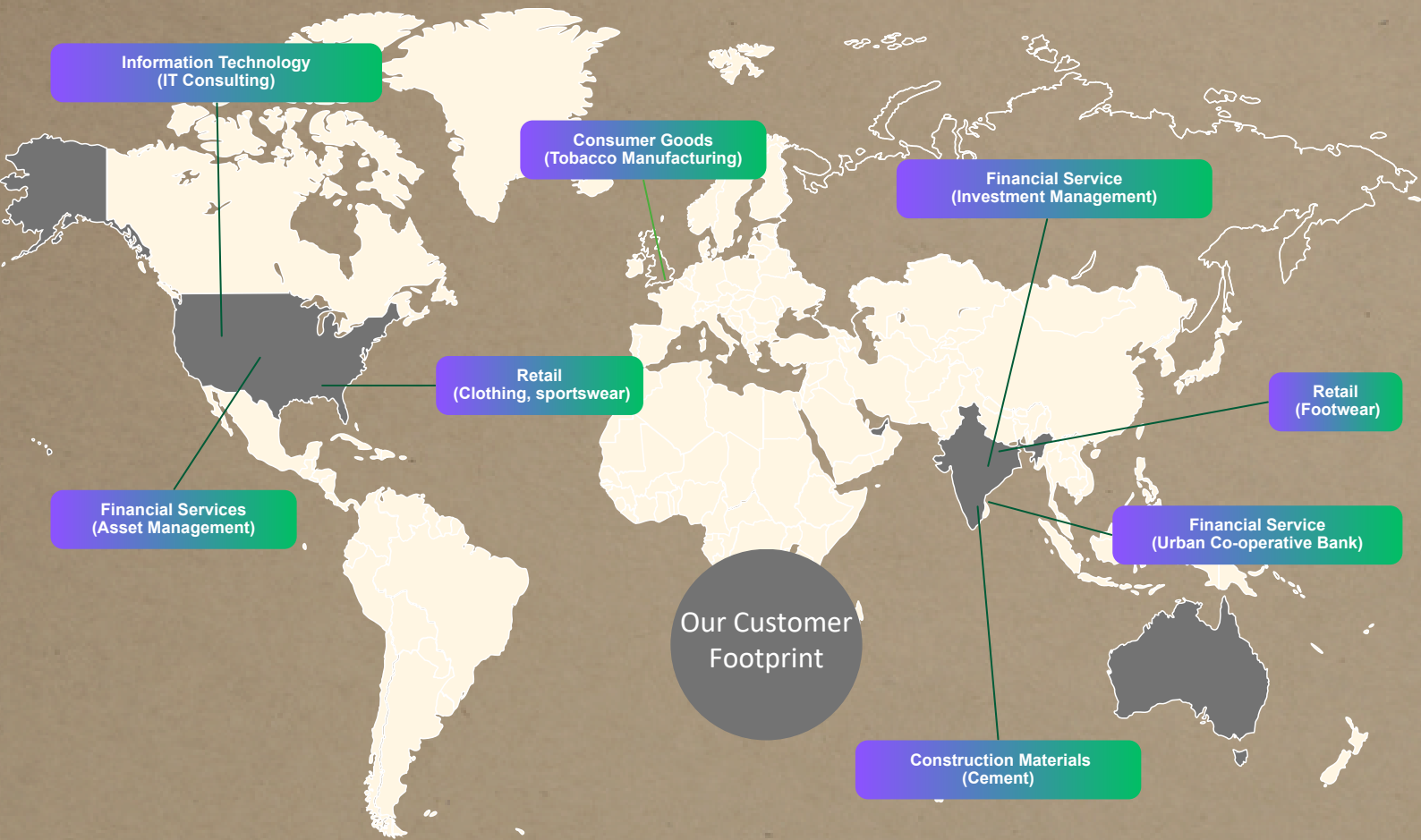
Value + Impact from Day One, No Installation & No Deployment

Services delivered by Global Cyber Capability Center using advance Platforms

Strong Handpicked Team of 50+ with (best of security talent globally)

Subscription & annual contract modeled services delivered globally

## 100's of Satisfied Customers Across the Globe!



# Cyber Security Portfolio

## Secure Cloud WL

Design Security for Cloud  
 Cloud Security Posture  
 DevOps Infra Security  
 Container Security  
 Kubernetes Security  
 Integrated S/W Security  
 Workload Hardening  
 Security Automation  
 Cloud Native Monitoring  
 Cloud Governance

**We create secure cloud environments, automate Cloud SecOps & manage it.**

## 24x7 Monitoring

MDR, 24x7 Monitoring  
 SOC as a Service  
 SIEM/SOC Design & Impl  
 SOC Team on Hire  
 Managed Incidents  
 IR Process Designs  
 IR Workshops  
 SOC Assessments  
 Threat Hunting Services  
 Forensic Services

**When it comes to SOC Monitoring & Response, we cover all aspects of it**

## Vuln Mgmt

Application Security  
 Network VAPT  
 Cloud VAPT  
 Controls & Config Audit  
 Program Design for VAPT  
 Managed Vuln Programs  
 VAPT Automations  
 Surface Assessments  
 Threat Intel for VAPT  
 DevSecOps

**Program designed VAPT Engagement to enhance protection & reduce attack surface**

## Threat Intel

Threat Intel Solutions  
 Darkweb Hunting  
 Deep Intel Reports  
 Threat Intel Integrations  
 Intelligence Automations  
 Threat Intel Curation  
 Vectored Searches  
 Data Hunting  
 Threat Intel Architecture  
 Adversary Tracking

**We take threat intel maintenance, keep, usage & application to next level.**

## Data & Privacy

Data Security Design  
 Data Sec Posture Assmnt  
 Data Sec Posture Mgmt  
 Encryption Design & Sol  
 Data Exfiltration Assmnt  
 Privacy Designing  
 Privacy Gap Assessment  
 Privacy Adoption Service  
 Privacy Automations  
 Privacy Compliances

**Data and privacy are two considerations, we design, implement it & run compliances**



## Unified View of Security ...

### #1 Orchestration & Automation

*Automated governance  
 SecOps automation  
 Automated response*

### #2 Attack Surface Reduction

*Inline AS detection  
 External AS validation  
 Continuous remediation*

### #3 Real Time Detection & Response

*Real time detection  
 Active threat hunting  
 Proactive responses*

### #4 Zero Trust Micro Architecture

*Zoning and isolations  
 Contextual runtime set  
 Transient access model*



## Castellum Labs



[www.castellumlabs.com](http://www.castellumlabs.com)



Castellum Labs



[reach@castellumlabs.com](mailto:reach@castellumlabs.com)



+91 7842046995