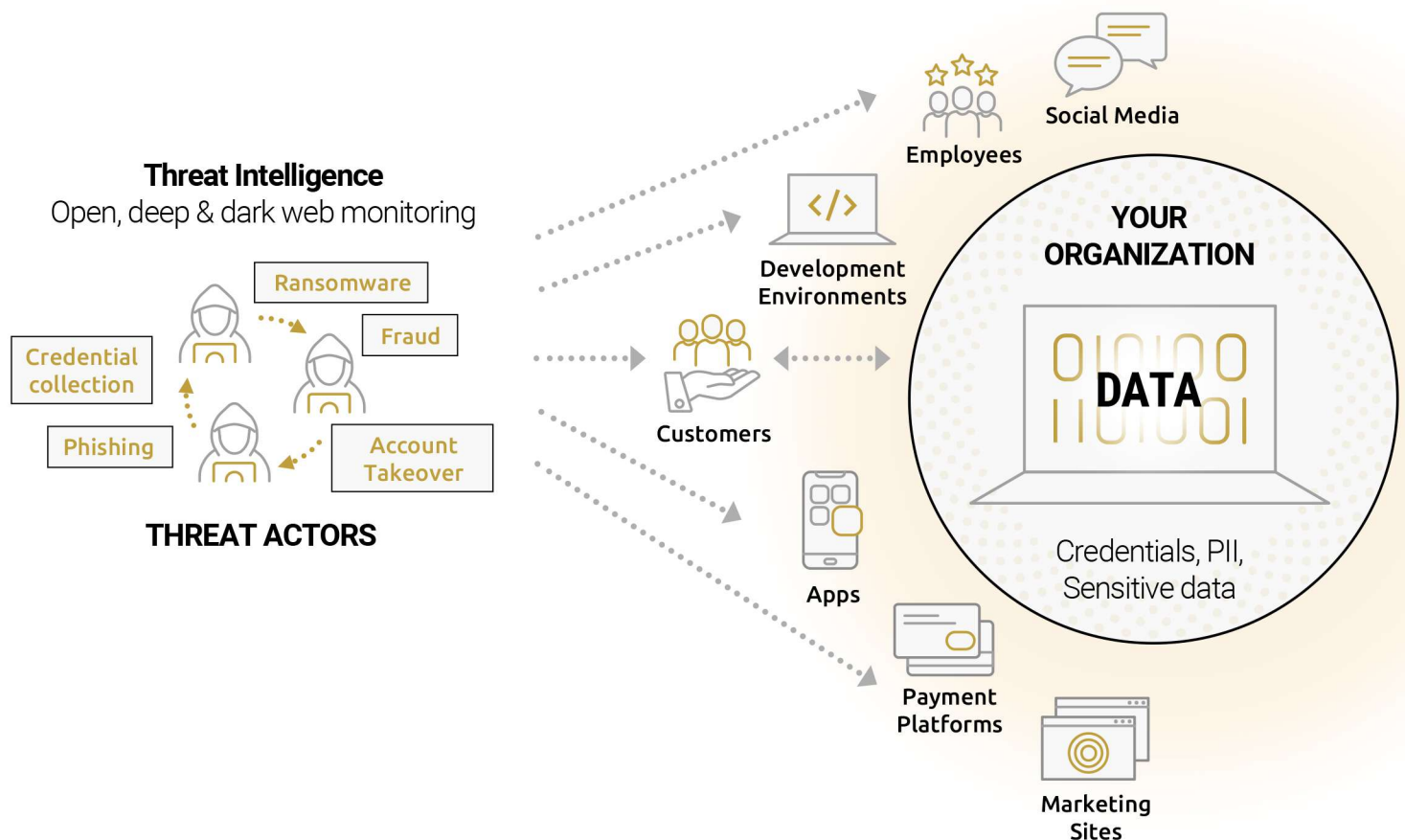# MANAGED SERVICE

Bespoke cyber intelligence services that fits your needs

VTCyber offers a managed Digital Risk Protection program providing access to our dedicated platform and a team of cyber threat analysts, augmenting any CTI program to a higher level of quality and performance. Partnership with VTCyber's analyst team includes day-to-day interaction with a dedicated analyst who becomes a member of your in-house team. Analysts are assigned based on their knowledge of industries and their intimate understanding of business needs. All raw intelligence items brought to light by our System are diligently verified, contextualized, and attributed to real risks by utilizing tremendous amounts of data collected from the open, deep, and dark web.

Our team of analysts is multilingual thus allowing an understanding of the threat actors in their respective language. In addition, the analyst's mastery of cybercriminal "lingo" and culture allows you to identify, verify, and mitigate those threats that will most likely come to fruition as attacks.
VTcyber provides a valuable human element when it comes to research, investigation, and threat intelligence operations. The Virtual HUMINT capabilities, i.e. live interaction with threat actors, enables deeper contextualization which is required for effective mitigation.

VT Cyber - Protection Beyond the Perimeter

Threat Intelligence
Open, deep & dark web monitoring

Ransomware

Fraud

Credential collection

Phishing

Account Takeover

THREAT ACTORS

Employees

Social Media

Development Environments

Customers

YOUR ORGANIZATION

DATA

Credentials, PII, Sensitive data

Apps

Payment Platforms

Marketing Sites

Contact Us

VT Cyber sp. z o.o.
www.vtcyber.pl
info@vtcyber.pl

We're in
Warsaw | Poland

VT Cyber Offering

Dedicated SaaS Platform
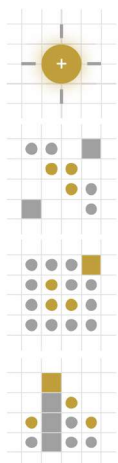
- Threat Intelligence
- Dark Web Monitoring
- Attack Surface Mapping
- Forensic Canvas
- Phishing Detection & Takedown

Managed Services

- Targeted Triaging & Monitoring
- Virtual HumINT Operations
- Deep Cyber Investigations
- Threat Landscape Analysis

Use cases / Packages	Categories
Exploitable ports	Attack Surface Monitoring & Vulnerabilities
Exposed company web interfaces	
Hijackable subdomains	
Email security issues	
CAA issues	
Open cloud storage	
Mail server blacklisted	
Executive impersonation in social media	Brand Abuse
Brand impersonation in social media	
Brand abuse websites detection	
Mobile apps impersonation	
Private access token	Data leakage & Compromise
Customer credentials exposed	
Customer payment cards exposed	
Employee credentials	
Source code disclosed	
Leaked documents (files and emails)	
Advanced sensitive information disclosure incl. PIIs, etc.	
Refund fraud services and tutorials	Fraud
Carding services and tutorials	
Advanced fraudulant activities	
Domain Squatting	Phishing
Phishing websites detection	
Phishing Beacon	
Advanced phishing detection incl. phishing kits, emails, etc.	
Credential Stuffing Tool Targeting Company	Attackware
Brute Force Tool Targeting Company	
Data Scraping Tool for Company Application	
Vulnerability Scanner Targeting Company	
Advanced attacks detection incl. attack prep, attack tools, scanners, etc.	

Contact Us

VT Cyber sp. z o.o.
www.vtcyber.pl
info@vtcyber.pl

We're in
Warsaw | Poland

VT Cyber :
Addressing a Variety of Business Risks

DIGITAL FOOTPRINT

Map the attack surface and identify vulnerable weaknesses

Exposed Web Interfaces • Hijackable Subdomains • Website Vulnerabilities • Exposed Cloud Storage • Exploitable Ports • Mail Servers in Blacklist • Server Connected to Botnet • Email Security Issues • Certificate Authority Issues

PHISHING

Identify & remediate phishing attack attempts before they impact

Phishing • Email • Phishing Kit • Phishing Website • Lookalike Domain • Phishing Target List

BRAND

Safeguard all facets of your online presence

Official Social Media Profile • Impersonation • Intellectual Property Infringement • Unauthorized Trading • Negative Sentiment • Fake Job Posting • Defacement

ATTACKWARE

Ensure ongoing and continuous visibility of threat actor's tools

Malicious File • Reconnaissance • Automated Attack Tool • Business Logic Bypass • Target List

FRAUD

Mitigate fraud to ultimately reduce your fraud rate

Refund Fraud • Carding • Coupon Fraud • Money Laundering • Victim Reports • Malicious Insider • Extortion

DATA & RANSOMWARE

Identify Leaked Information and Ransomware risk

Ransomware • Compromised PII • Compromised Access Token • Internal Information Disclosure • Malicious Insider • Compromised Payment Cards • Compromised Employee Credentials • Compromised Customer Credentials