FORTRA

Digital Risk Protection: Contributing to your Modern Security Operations

Anirudh Chand

Director, Solutions Engineering APJ

FORTRA

Agenda

1. Digital Risk Protection: Definition and Examples
2. Building a Successful DRP Program: Process and Challenges
3. DRP Best Practices
4. About Phishlabs

The Fortra Portfolio

Infrastructure Protection & Data Security

Vulnerability Management
- Vulnerability Management
- Web Application Scanning
- Application Security Testing

Data Protection
- Data Classification
- Digital Rights Management
- Endpoint DLP

Secure File Transfer
- Managed File Transfer
- EDI
- File Acceleration

Offensive Security
- Automated Pen Testing
- Adversary Simulations
- Red Team Operations

Digital Risk Protection
- Account Takeover Protection
- Social Media Protection

Email Security
- Brand Protection
- BEC
- Secure Email Gateway

Intelligence & Automation

Threat Research & Intelligence

Automation
- Robotic Process Automation
- Workload Automation
- Automated Remediation

Centralized Analytics

FORTRA

GONE PHISHING TOURNAMENT®

The 2023 Gone Phishing Tournament: Results and Recommendations

Co-sponsored by

Microsoft

2023 Gone Phishing Tournament (GPT) Summary

Methodology, simulation details, and a record-setting global reach

The Gone Phishing Tournament™ (GPT) is a **free annual cyber security training event** that helps organizations strengthen security awareness with accurate phishing benchmarking data.

The insights generated empower security leaders to **better understand high-risk areas**, **compare phishing performance** to their peers, and **establish data-driven awareness goals**

31

Number of languages the 2023 template was made available in, the most ever for the GPT

1.37M

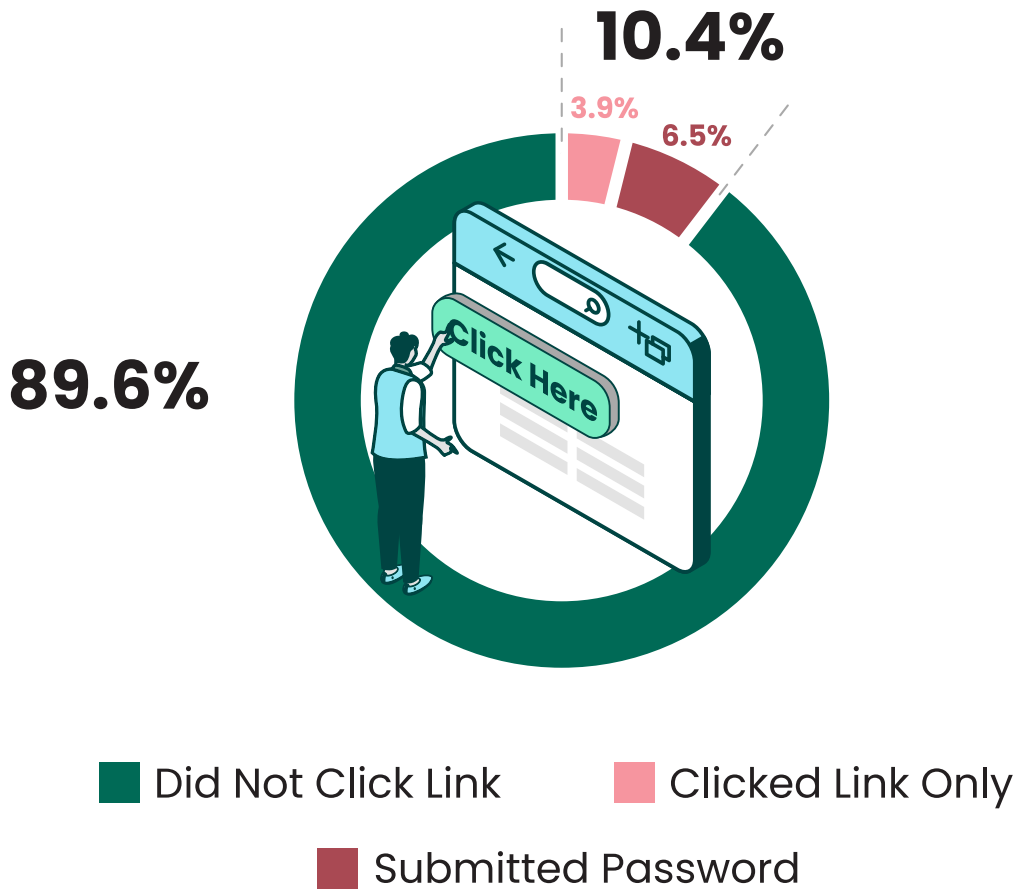
Participating global end users, as 10% YoY increase from a record-setting 2022.

>275

Participating organizations, setting another GPT participation record

Overall Results

- **10.4% of all simulation email recipients clicked the phishing link** (a 3.4 percentage point increase compared to the 2022 event)
- **6.5% of all recipients submitted their password** in the form embedded in the simulation webpage (3.5 percentage point increase)
- **62.3% of simulation clickers compromised their credentials** during the simulation



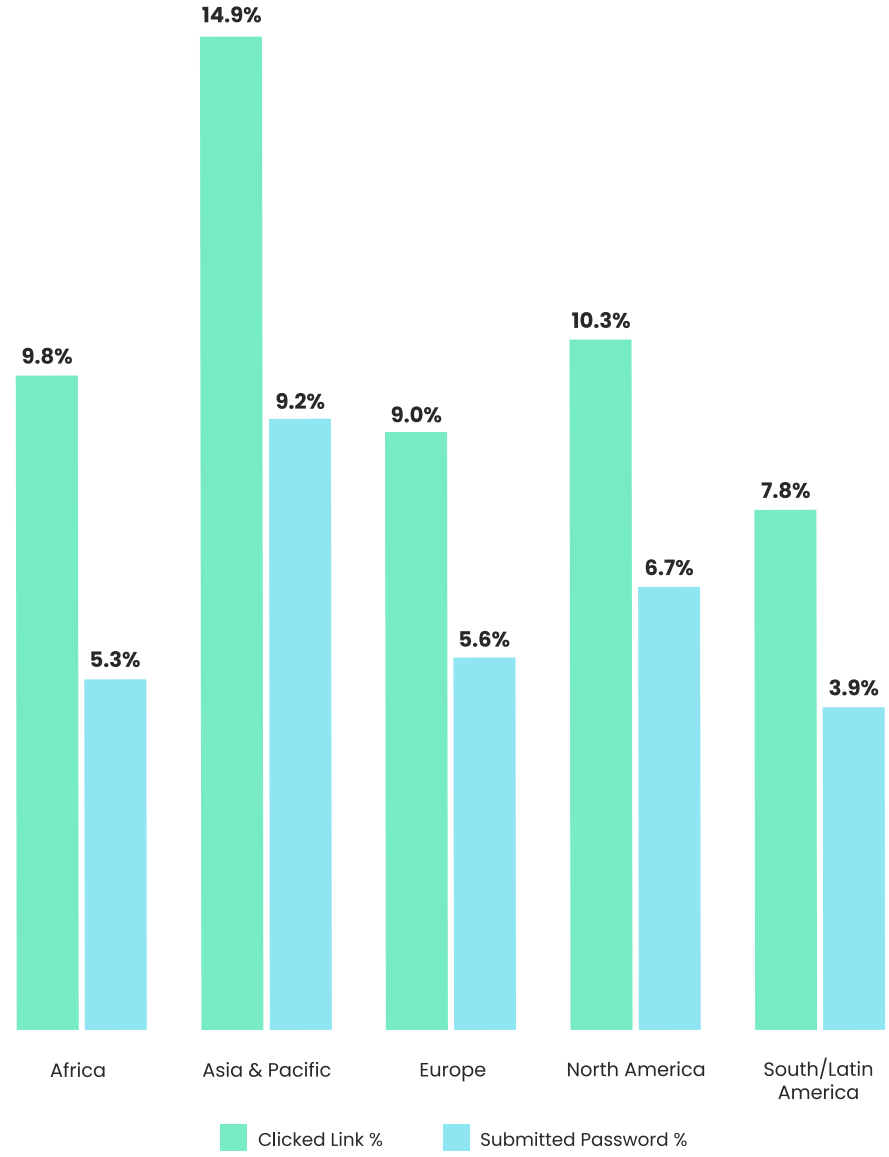
Overall Results

Had this been a real-world phishing attack …

- **Cyber criminals would have collected nearly 90,000 passwords** that secure business accounts
- This data could have been used for:
  - Account Takeovers (ATO)
  - Business Email Compromise (BEC)
  - Credential stuffing
  - Many other malicious activities

Results by region (%)

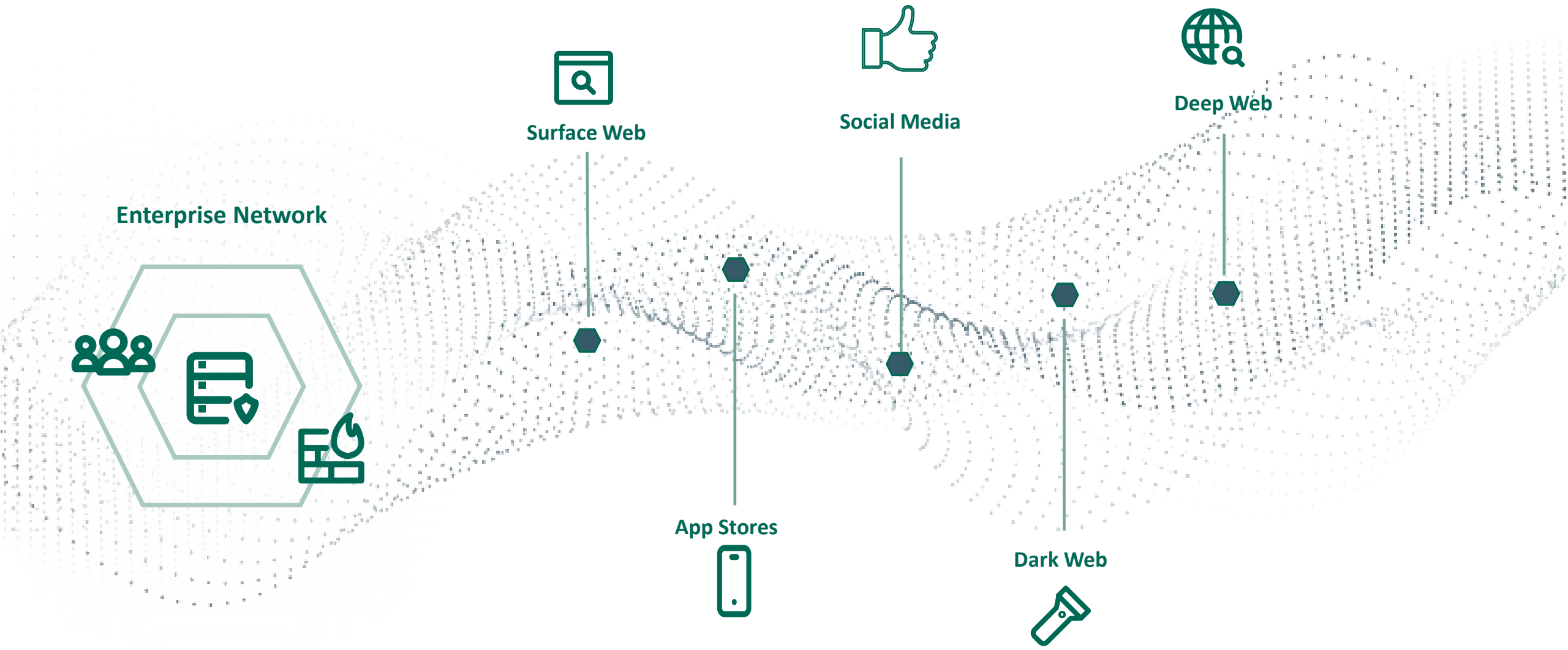
- **South/Latin America** performed the best of all participating regions (7.8% click rate, 3.9% password submission rate)
- **The Asia & Pacific region** finished with the highest click rate (14.9%) and password submission rate (9.2%)
- **North America** posted the highest clicker-to-password-submission rate (over 65%)



What is Digital Risk Protection (DRP)?

DRP is an operational process that combines intelligence, detection, and response to mitigate attacks across the external digital risk landscape.

What is Digital Risk Protection?



Common Threat Vectors

Unauthorized mobile apps

Brand infringement

Look-alike domains

Malicious emails

Invoice scams

Website traffic redirection

Vishing/SMiShing

Stolen credentials

BEC

Executive impersonation

Social spoofing

Fake social profiles

Phishing sites

Banking trojans

False brand association

Crimeware

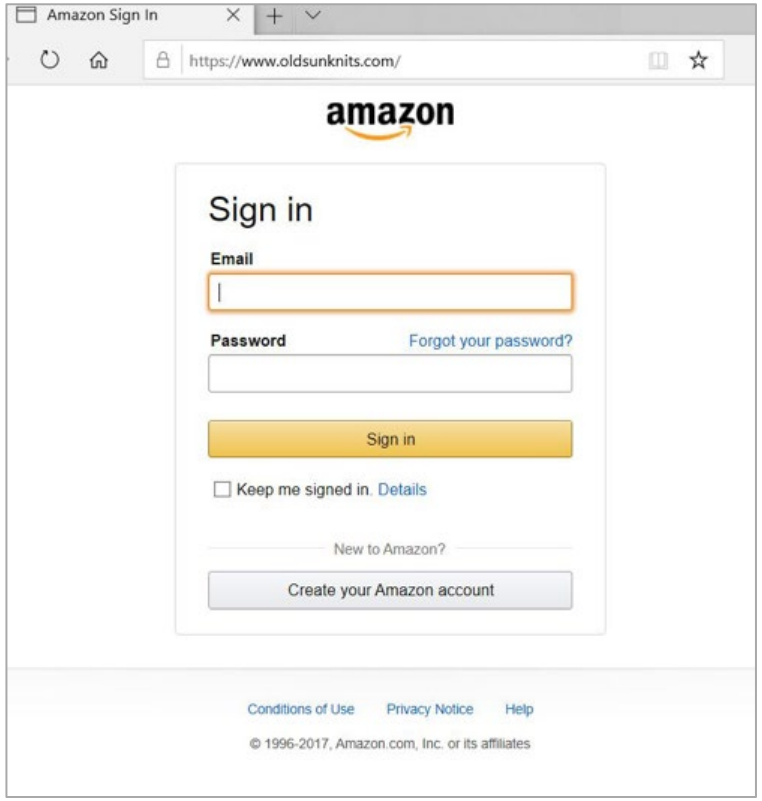
Dark web

Leaked data

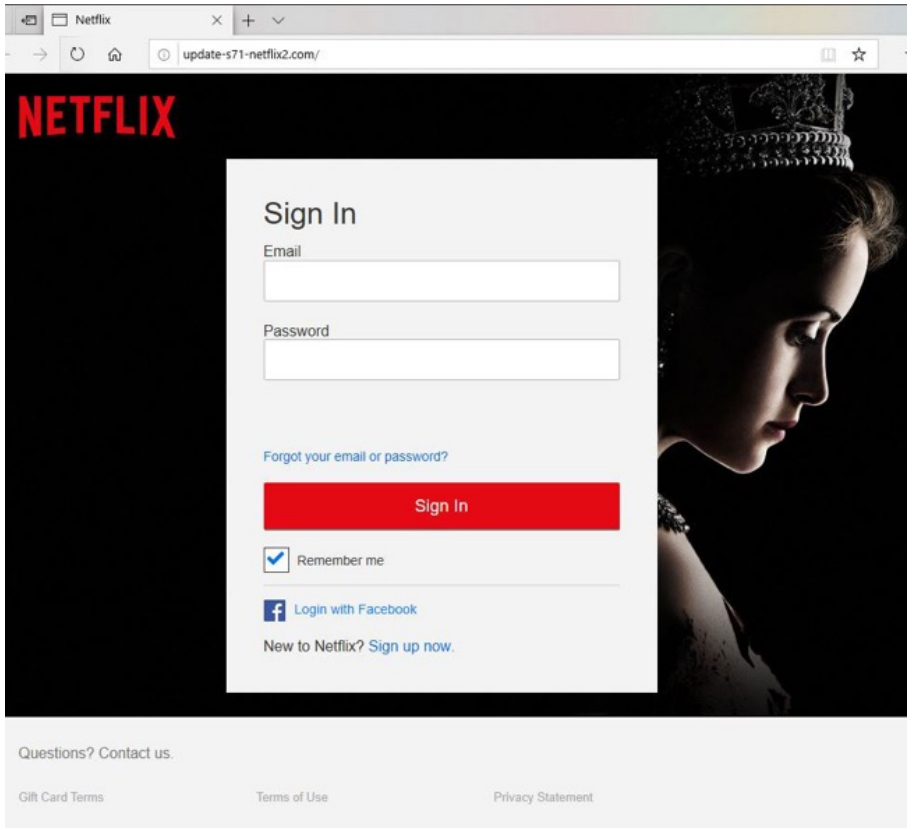
Digital Risk Protection : Common Threat Vectors

- Credential Theft Phishing
  - Vishing
  - Spear Phishing
  - Mishing
- Lookalike or Imposter Domains
- Social Media Threats
- Mobile Application Clones
- Counterfeiting
- Leaked Credentials
- Stolen Credentials for Sale

Credential Theft Phishing

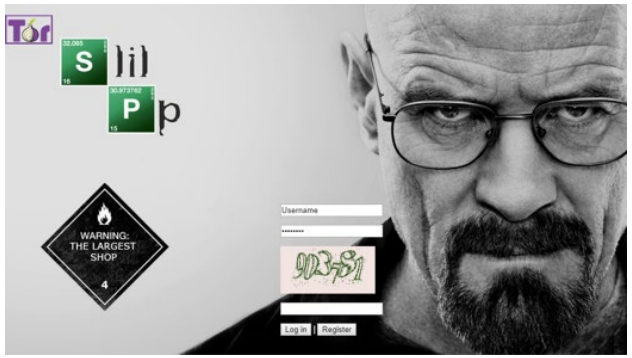


https://www.oldsunknits.com/

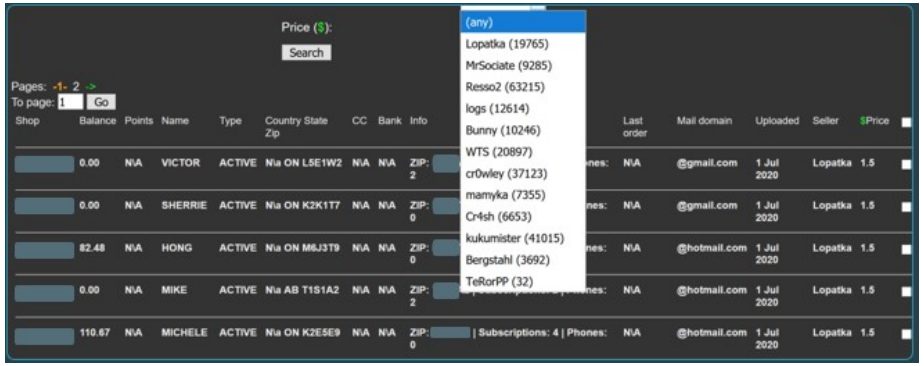


http://update-s71-netflix2.com/

Stolen Credentials for Sale



Dark Web Marketplace



Vendor list and customer account numbers for sale

Credential Theft Phishing - Useful Discovery Tools

- **https://github.com/mitchellkrogza/Phishing.Database**
- **Phishtank: https://phishtank.org/**
- **Openphish: https://openphish.com/**
- **URLScan: https://urlscan.io/search**

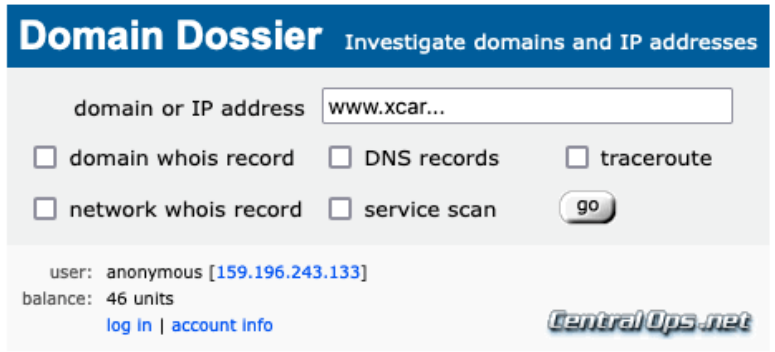
hXXp://ayrus707.github.io/Netflix-Clone.github.io

hXXps://telegramsoft.cn/

hXXp://nextmediaa.online/walmart

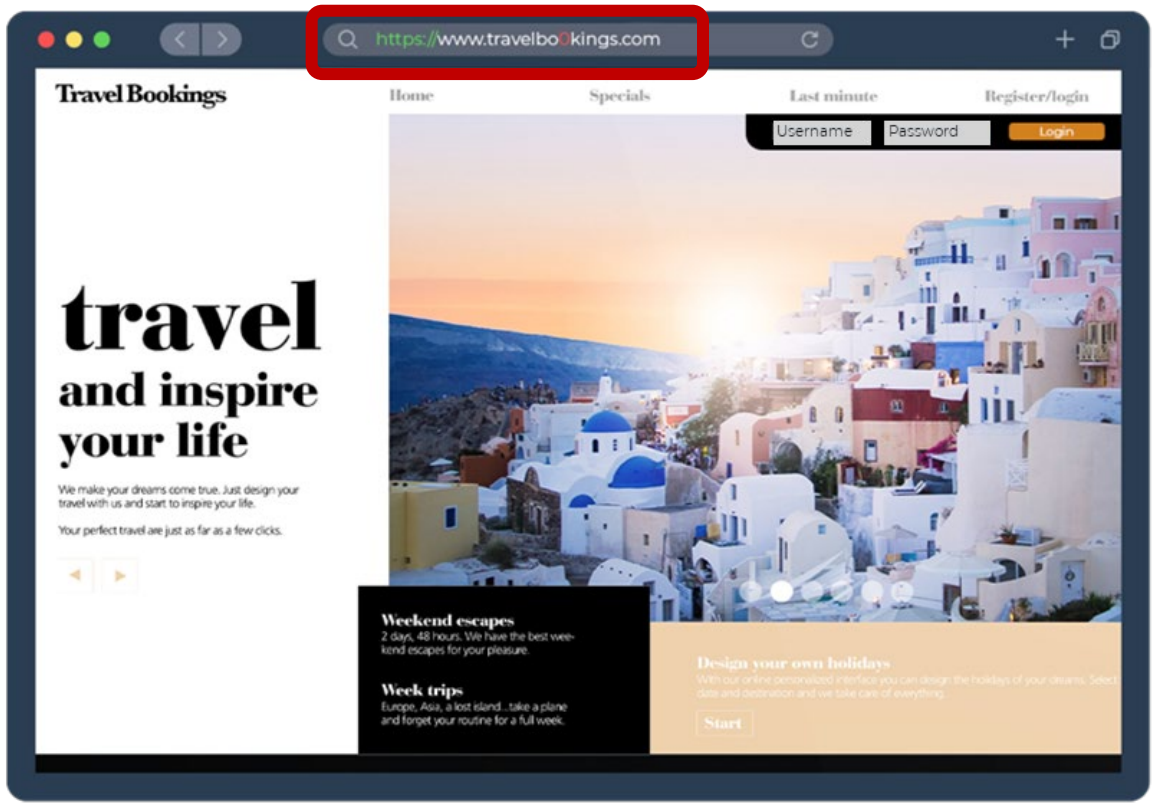
Helpful (free) URL, IP and Domain Analysis Tools

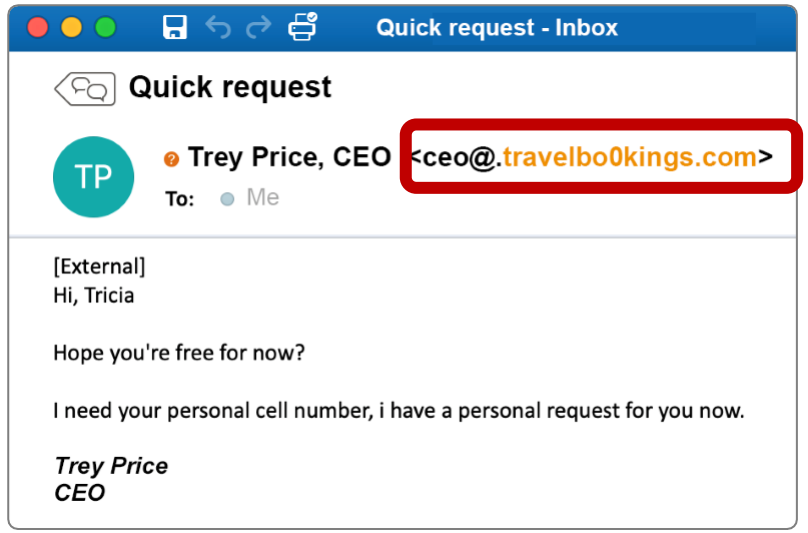
- Domain Dossier - WHOIS
- https://www.archive.org – Historical Screenshots
- https://wheregoes.com/ - Redirect Tracer
- User Agent Switcher / VPN - For detection evasion.
- Open Multiple URLs browser plugin.



Imposter Domains

microskoft.com	microspft.com
microgsoft.com	microsift.com
micrpsoft.com	micreosoft.com
microslft.com	microsofrt.com





Domain Registration Data

New Domain Sources:

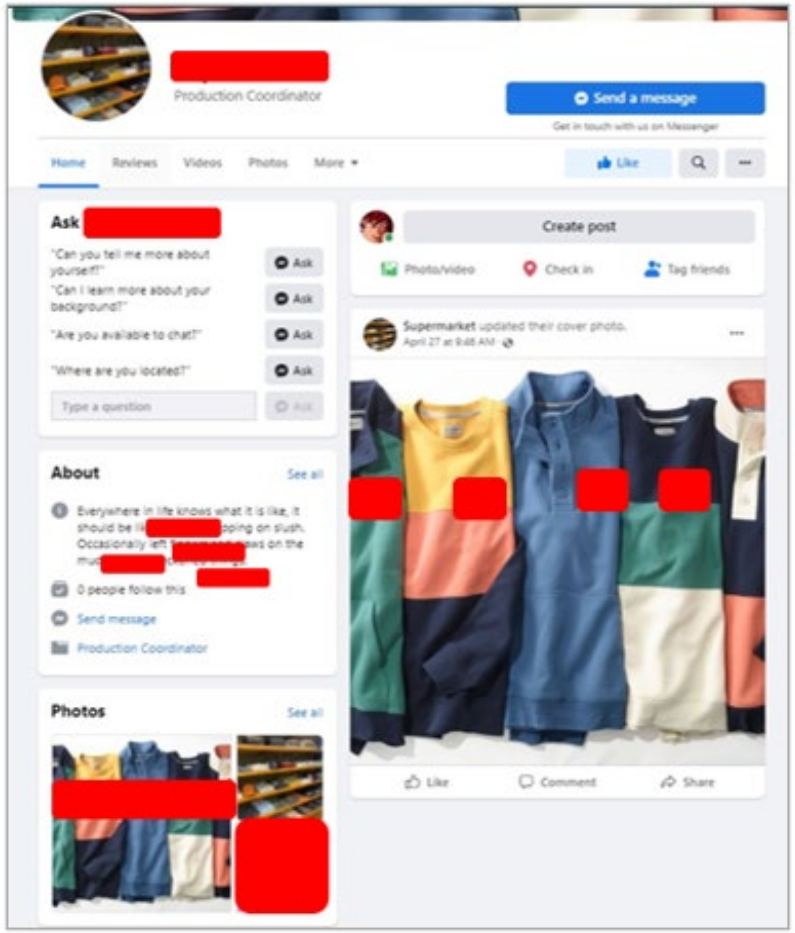
- Registry Zone Files
- SSL Certs
- DNS Queries
- ISACs

DNSlytics

DNSTWISTER

Free applications that can be used to discover look alike domains.

Social Media Impersonations… or unauthorised affiliations



Social Search Tactics

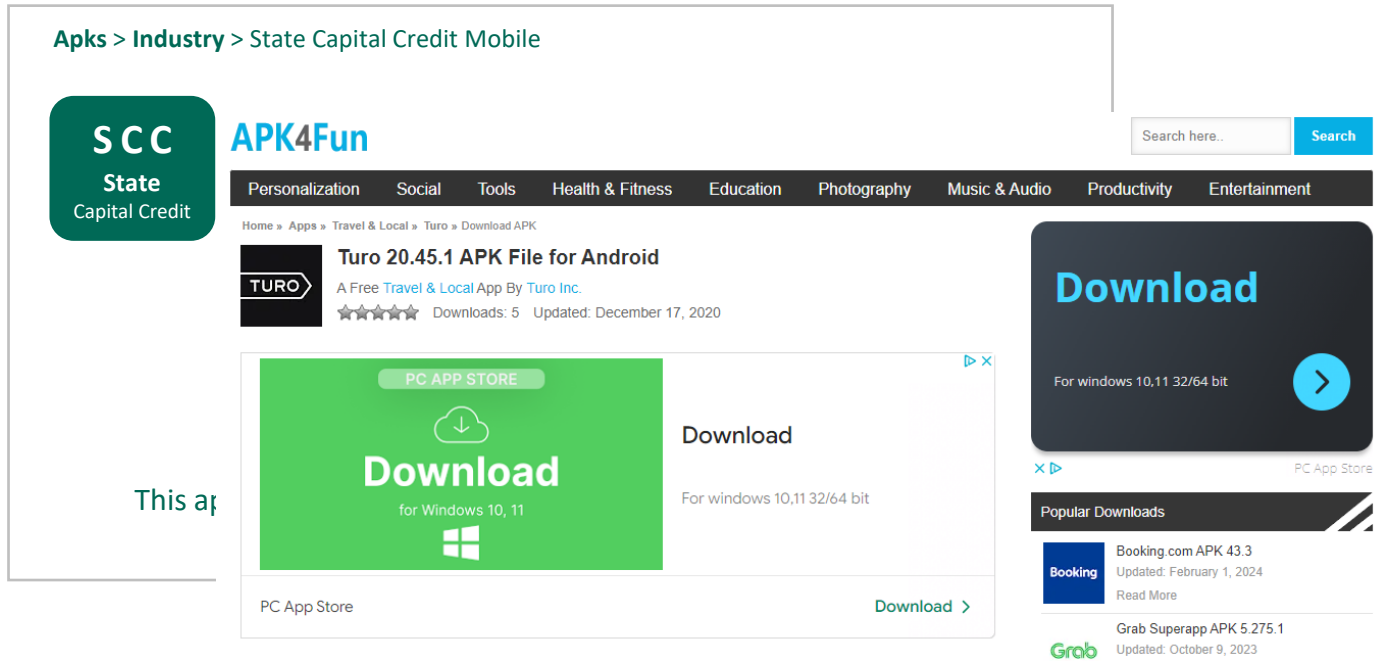
- In-platform searching (brand, keyword, person)
- Search engine “site” searching
  - https://www.social-searcher.com/
  - https://awario.com/
- http://sydex.net/ (Executive Impersonations)

Rogue Application Clones

Apk Versions available: 13.13.1, 13.7.1, 13.4.6, 13.4.5, 13.1.2, 13.1.0, 13.0.5, 12.2.5, 12.2.2, 11.2.1, 11.0.3

13.19.7	June 3, 2019
13.13.1	February 22, 2019
13.7.1	August 19, 2018
13.4.6	July 7, 2018
13.4.5	May 12, 2018
13.1.2	March 2, 2018
13.1.0	January 16, 2018
13.0.5	November 9, 2017
12.2.5	March 4, 2017
12.2.2	February 15, 2017
11.2.1	April 7, 2016
11.0.3	December 2, 2015

Older versions available for download

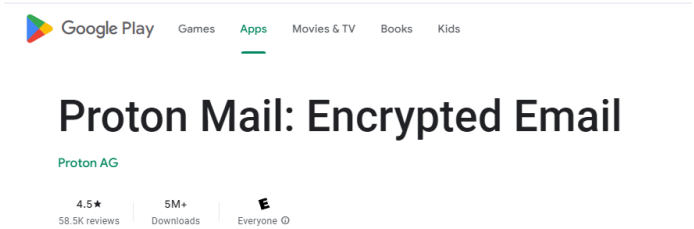


Concerns:

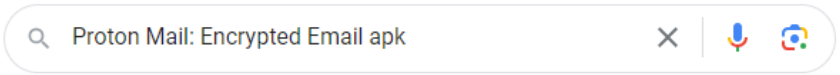
Cloned Applications
Previous Versions
Unwanted Applications/Ads

Mobile Apps Search Tactics

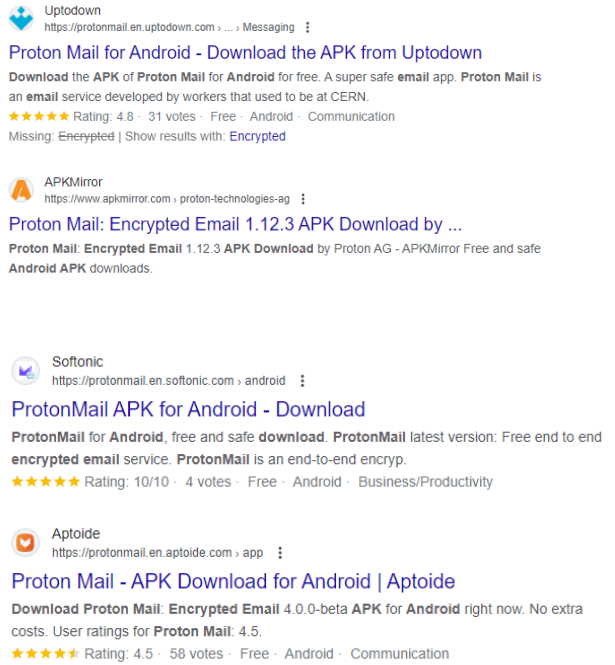
1.



2.



3.



Search Engine Operators

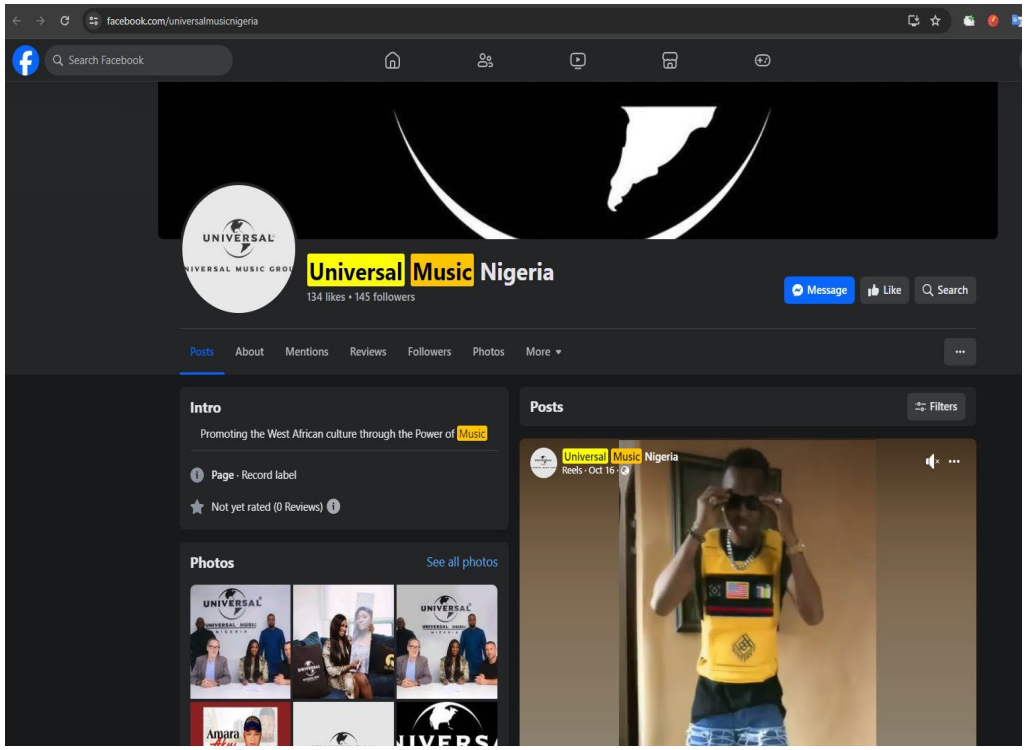
- Dorking/Hacking
- Site Searching
  - site:targetsite.com <keyword>
- URL Searching
  - inurl:<keyword/brand>
- Open / Surface Web

About Keywords

hXXps://a-thiele.eu/postnord/nord/nord/login/account.php

Types of Keywords

- Brand
- Person/Individual.
- Threat.
- Industry
- Combinations



Common Challenges

Lack of Visibility

Insufficient intelligence across digital channels.

Too Much Noise

Volume of data is overwhelming.

Ineffective Mitigation

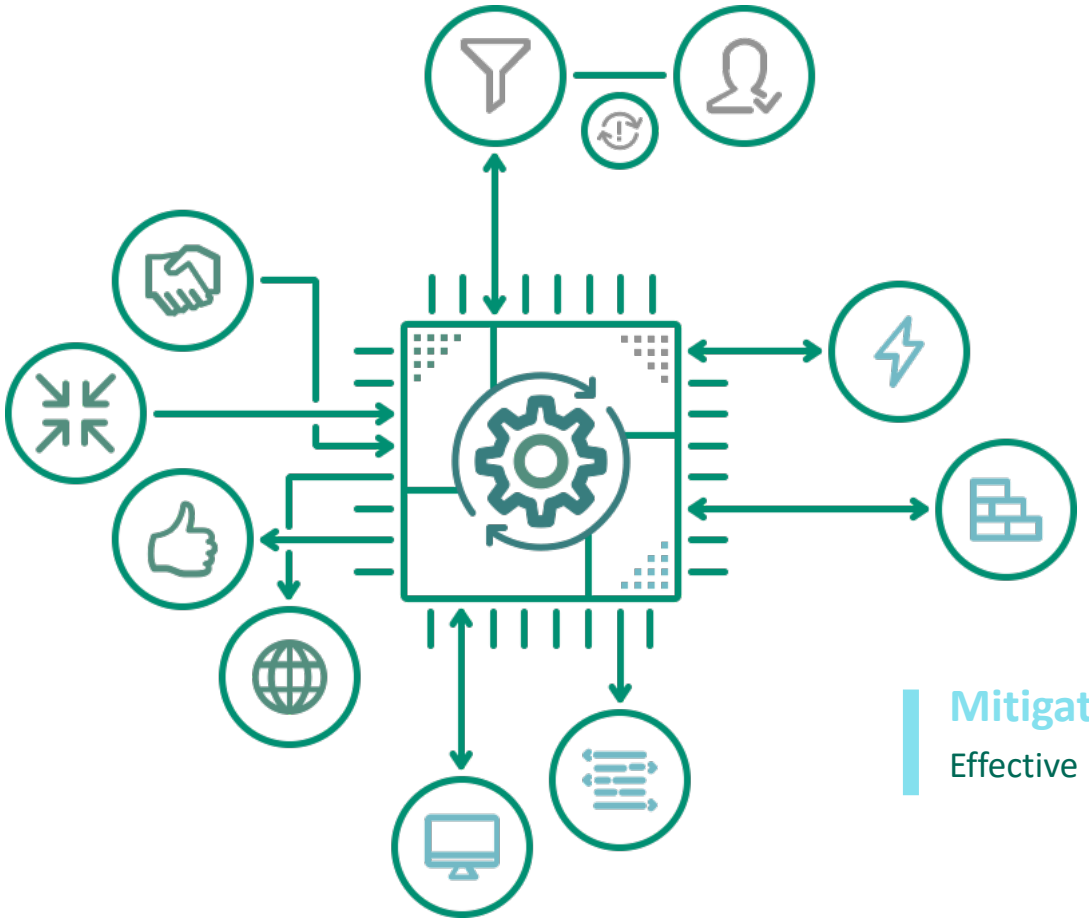
Slow, costly and often unsuccessful.

Limited Resources

Underestimated TCO: time, staff, and budget.

Building a Successful DRP Program

Collection
Gain Visibility



Curation
Reduce Noise,
Find Threats

Mitigation
Effective Mitigation

Collection

Centers of Excellence

Threat-Specific Sourcing

Web
Open, Dark, Deep, App Stores

Social Media
Social Networks, Paste Sites, Gripe Sites, Blogs

300+ Data Feeds
URLs, Passive DNS, SSL Certs, Email and SMS Spam, Malware

Client Feeds
3rd party feeds, Referrer Logs, Abuse Reports, Web Beacon

Unique Collection Technology and Techniques

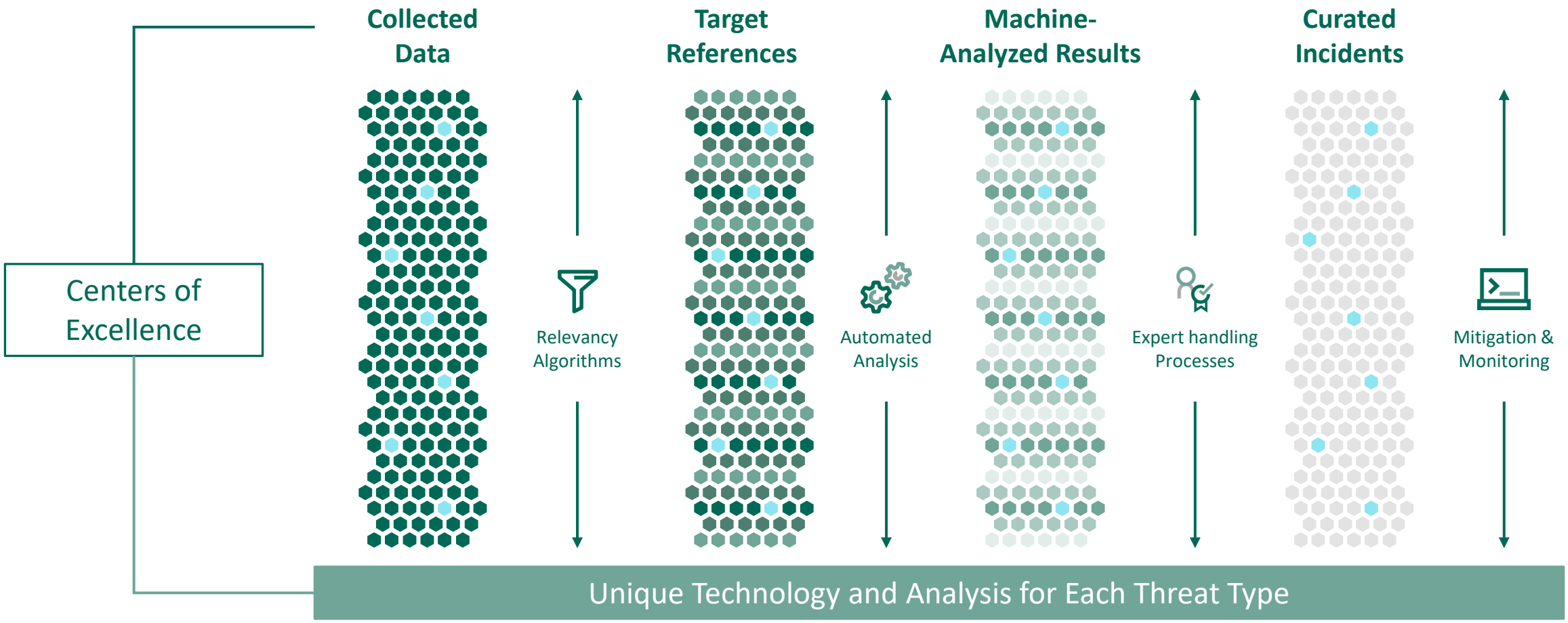
Parsing
Automated data ingestion

Crawling
Automated crawlers

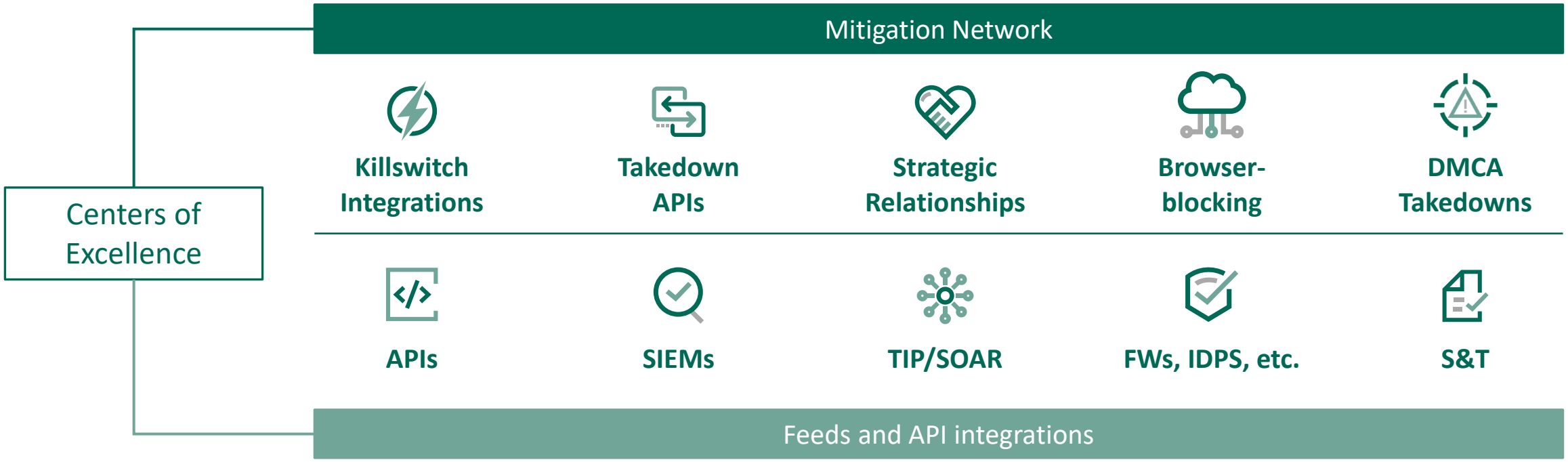
Anti-Evasion
Auto + analyst techniques to collect content

Pivoting
Auto + analyst methods for hunting related intel

Curation

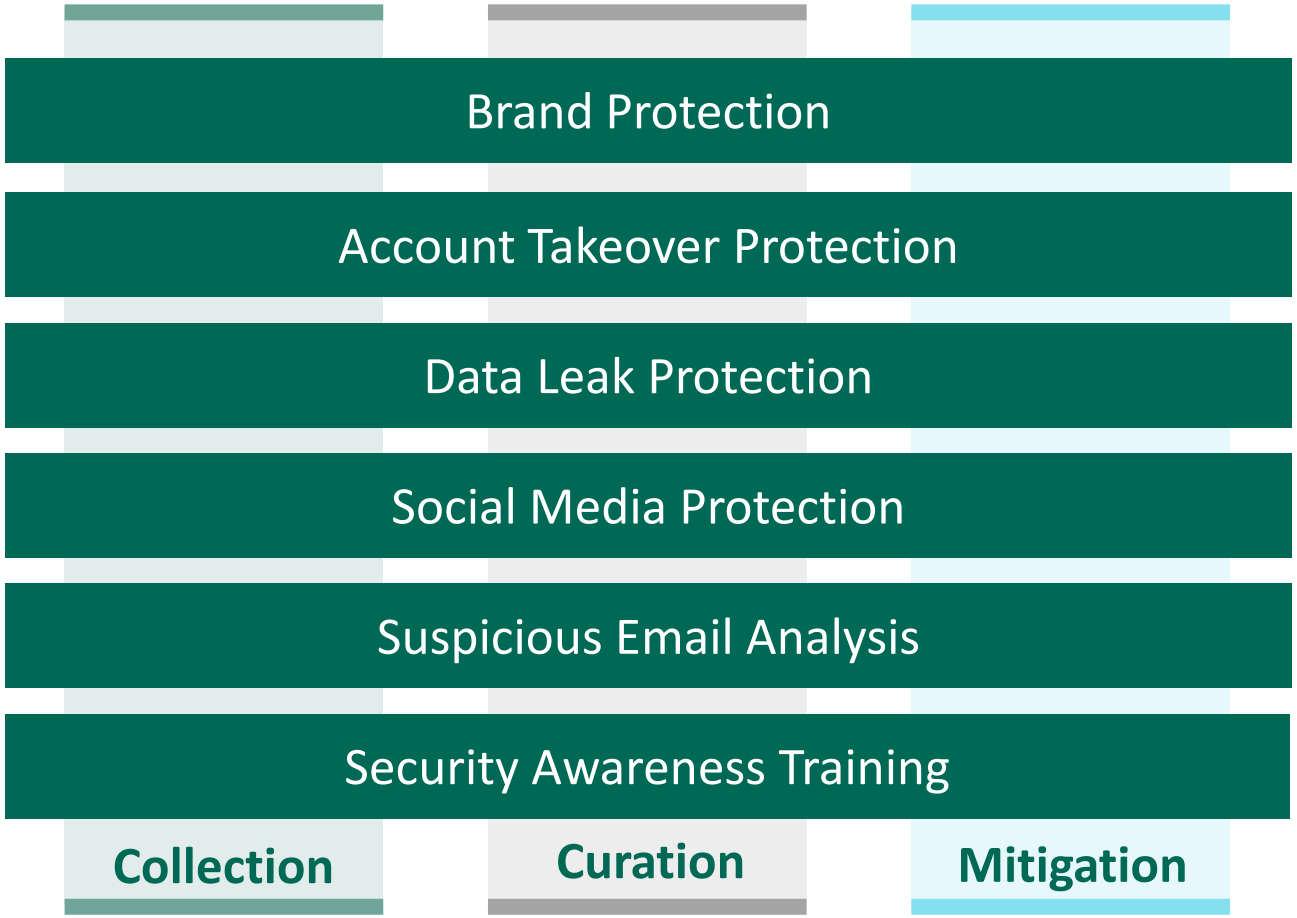

Centers of Excellence
Collected Data
Relevancy Algorithms
Target References
Automated Analysis
Machine-Analyzed Results
Expert handling Processes
Curated Incidents
Mitigation & Monitoring
Unique Technology and Analysis for Each Threat Type

Mitigation



> *Speed of take down for fraudulent sites is amazing*
>
> - Security Executive at Large Financial Institution

The Phishlabs Platform



CENTERS OF EXCELLENCE

Threat-Specific Technology
and Operations

Services

	Protects Brands and Customers	Protects Employees
Cred Theft Phishing	✓	
Open Web	✓	
Mobile App Stores	✓	
Crimeware	✓	
Social - Cyber	✓	
Social - Source Code	✓	
Social - Executive	✓	✓
Social - Physical	✓	✓
Domains	✓	✓
Dark Web	✓	✓
Suspicious Email Analysis		✓
MSOAR		✓

FORTRA

Questions.