Sound check script

Please read out loud

Hello, my name is _____ and I will be speaking during the session today.

I am testing my audio to confirm that the technical service providers can hear me clearly.

ICANN 84 ANNUAL GENERAL MEETING

Tech Day

Use of AI tools in abuse mitigation

25 October 2025

ICANN | ccNSO

SPEAK SLOWLY AND CLEARLY.

USE A HEADSET FOR BETTER AUDIO AND INTERPRETATION.

RAISE YOUR HAND IN ZOOM TO JOIN THE QUEUE.

ON SITE? PLEASE MUTE YOUR ZOOM AUDIO.

REMOTE? PLEASE TURN ON YOUR CAMERA WHEN SPEAKING.

SPEAKING IN A LANGUAGE OTHER THAN ENGLISH? LET US KNOW FOR INTERPRETATION.

Have a headset ready!

Participants could present, ask questions, or contribute in languages other than English.

Tech Day | DASC session on the use of AI tools in abuse mitigation

Monday, 27 October 2025 | 15:00-16:00 local, UTC +0

Session chair: Nick Wenban-Smith, .uk, Chair of the ccNSO Domain Name Abuse Standing Committee (DASC)

- Philip Struyf, .eu
- Jake Vincet, .uk
- Crystal Peterson, .us

ICANN | ccNSO

About the ccNSO DNS Abuse Standing Committee (DASC)

1. Share information, insights and practices
2. Raise understanding and awareness
3. Promote open and constructive dialogue
4. Assist ccTLD managers in their efforts to mitigate the impact of DNS Abuse

DASC does not formulate any policy or standards: out of scope of the ccNSO policy remit

DASC: resources and activities to date

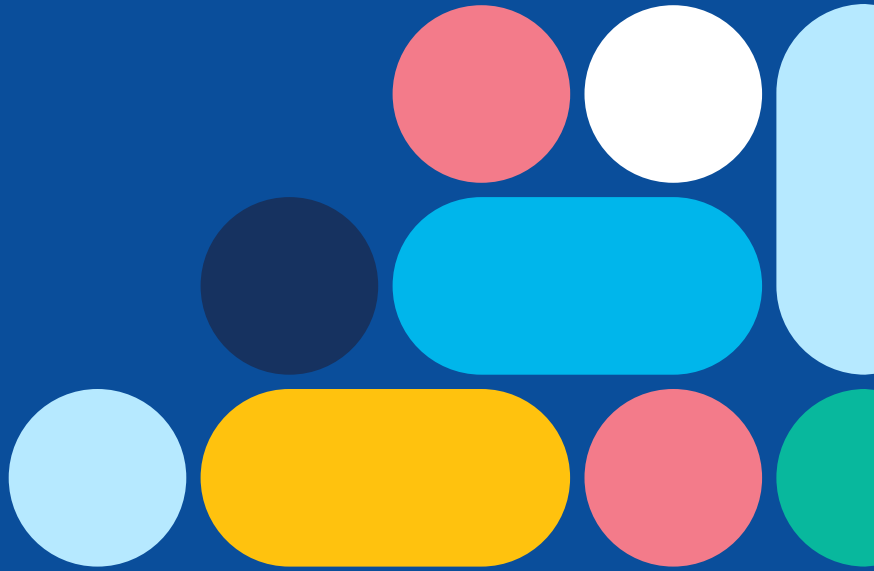
- Resources
  - DNS Abuse Library: https://icann-community.atlassian.net/wiki/x/JEJ2Bg
  - Dedicated email and contact list: https://icann-community.atlassian.net/wiki/x/JkR2Bg
- Understanding the landscape and how to best serve ccTLDs
  - Survey among ccTLDs 2022
  - Survey among ccTLDs 2024
- Sessions
  - Tools & measurements
  - Amendments to the gTLD Base Registry Agreement (Base RA) and gTLD Registrar Accreditation Agreement (RAA) to Modify DNS Abuse Contract: what do ccTLDs need to know?
  - The role of accurate domain name registration data in combating DNS abuse
  - Online scams and financial crime

AI-powered domain name abuse detection

ICANN84 – ccNSO Tech Day / DASC

.eu .ею .ευ

POWERED BY EURid



Agenda

- **Introduction**
- **Domain Name Abuse**
  - What are we facing ?
  - Why AI ?
- **Detection Tool: APEWS**
  - Current Implementation
    - Advantages
    - Limitations
  - Future Plans and Improvements
- **Q&A**

About EURid

EURid is the **registry manager** of the **.eu**, **.ею** (Cyrillic script) and **.ευ** (Greek script) country code top-level domain names by appointment of the European Commission, a role we fulfill since 2003.

At EURid, we envision a secure, trusted, and multilingual online environment that supports the European Digital Single Market by providing a **safe and reliable top-level domain** that is suitable for all official European scripts.

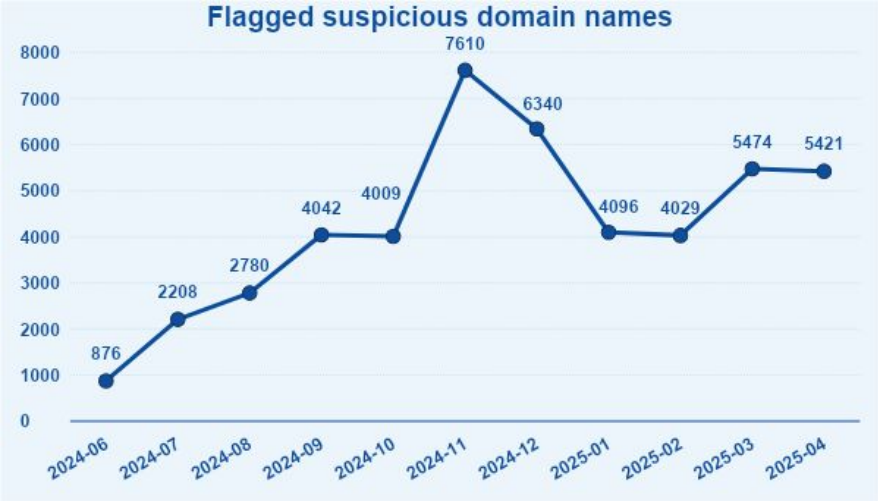
Explore our **timeline** for more info about our beginnings, growth and milestones: eurid.eu/en/about-eurid/timeline/

Statistics Q3 2025: eurid.eu/en/about-eurid/statistics/

- > 3.5 million domain names registered
- 500+ accredited registrars around the world

Our goal:

A safe and reliable .eu



.eu
POWERED BY EURid

Data Quality

Accurate data about domain name holders

- Key priority
- Legal Obligation (Concession contract, GDPR, NIS2)

Purpose

Assisting consumer protection and law-enforcement authorities, Identifying sources of spam, Safeguarding intellectual property rights, Addressing cyberattacks, Resolving technical network issues, …

Responsibilities

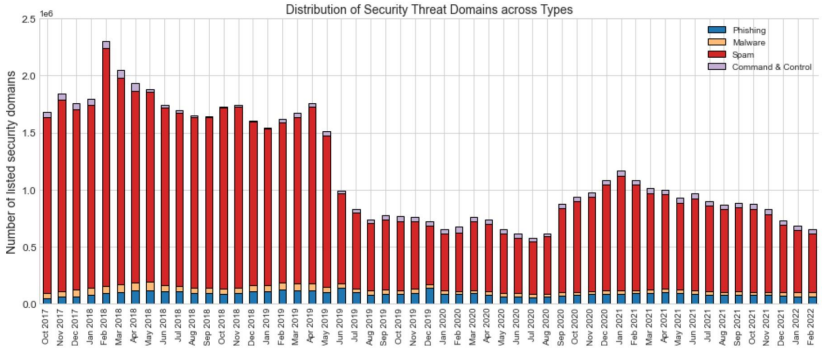
- Registrars are provisioning the data
- EURid is working closely with both registrars and registrants

WHOIS

- Some data are made publicly available via our WHOIS database
- CLI or web interface

What is threatening us?

DNS Abuse



Source: ICANN DNS Security Threat Mitigation Program – A Brief Review of DNS Abuse Trends

ICANN Definition (SSAC Report)

- **Malware** is malicious software, installed and/or executed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
- **Botnets** are collections of Internet-connected computers that have been infected with malware and can be commanded to perform activities under the control of a remote attacker.
- **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information, whether through sending fraudulent or 'look-alike' emails, or luring end-users to copycat websites.
- **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. Phishing differs from pharming in that pharming involves modifying DNS entries, while phishing tricks users into entering personal information.
- **Spam (as a delivery mechanism for other forms)** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content.

.eu
POWERED BY EURid

Short history (and future) of our abuse detection tool

APEWS on premise

- Integrated in .eu RP
- Addition of Rules
- Immediate suspension

APEWS aaS

- REST APIs
- Containerized
- Multi-TLD setup

APEWS: introduction of ML

- Collaboration with KUL
- Feedback: both external and internal
- Focus to limit the amount of false positives
- Dry-run → Delayed delegation

Manual Checks

- Detection of patterns in Spam-runs on D+1
- Workload
- Slow

APEWS

.eu POWERED BY EURid

Introduction of AI / ML

Development of a prediction system

- Collaboration with KU Leuven University
- Based on **registration (meta)data**
- Different predictor models
- Continuous training via external sources and feedback loop

Scientific Publications on our website (eurid.eu)

- Detection of Algorithmically Generated Domain Names used by Botnets: A Dual Arms Race
- Exploring the Ecosystem of Malicious Domain Registrations in the .eu TLD
- Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations.
- An Operational Solution for DNS Registries to Prevent Malicious Domain Registrations

.eu POWERED BY EURid

Table 1: Featureset used for reputation-based classification (*'Cla'* column) and similarity-based clustering (*'Clu'* column).

Feature	Type	Cla	Clu	New?
domain_length	Ord	✓	✓	[9]
domain_digits	Ord	✓		[3]
domain_max_digit_len	Ord	✓		✓
domain_max_digit_offset	Ord	✓		✓
domain_max_hex_len	Ord	✓		✓
domain_max_hex_offset	Ord	✓		✓
hour_of_registration	Ord	✓		[9]
registrant_country_code	Categ.	✓	✓	✓
registrant_address_score	Cont.	✓	✓	✓
registrar_reputation_pct	Cont.	✓		✓
nameservers_reputation_pct	Cont.	✓		✓
email_provider_reputation_pct	Cont.	✓		✓
phone_number_reputation_pct	Cont.	✓		✓
registrar_reputation_pct_14d	Cont.	✓		✓
nameservers_reputation_pct_14d	Cont.	✓		✓
email_provider_reputation_pct_14d	Cont.	✓		✓
phone_number_reputation_pct_14d	Cont.	✓		✓
registrar_reputation_pct_30d	Cont.	✓		✓
nameservers_reputation_pct_30d	Cont.	✓		✓
email_provider_reputation_pct_30d	Cont.	✓		✓
phone_number_reputation_pct_30d	Cont.	✓		✓
registrar_reputation_pct_60d	Cont.	✓		✓
nameservers_reputation_pct_60d	Cont.	✓		✓
email_provider_reputation_pct_60d	Cont.	✓		✓
phone_number_reputation_pct_60d	Cont.	✓		✓
registrar	Categ.	✓	✓	[1, 5]
email_prov	Categ.	✓	✓	✓
registrant_street	String		✓	✓
registrant_phone	String		✓	✓
registrant_email_account	String		✓	✓
registrant_name	String		✓	✓
registrant_city	String		✓	✓
registrant_postcode	String		✓	✓
registrant_state_province	String		✓	✓
randomness	Cont.		✓	✓
seconds_since_last_reg	Categ.		✓	✓
nameservers_domains	Categ.		✓	[5]
nameservers_locations	Categ.		✓	✓

Introduction of AI / ML

Development of a prediction system

- Collaboration with KU Leuven University
- Based on registration (meta)data
- Different **predictor models**
- Continuous training via external sources and feedback loop

Scientific Publications on our website (eurid.eu)

- Detection of Algorithmically Generated Domain Names used by Botnets: A Dual Arms Race
- Exploring the Ecosystem of Malicious Domain Registrations in the .eu TLD
- Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations.
- An Operational Solution for DNS Registries to Prevent Malicious Domain Registrations

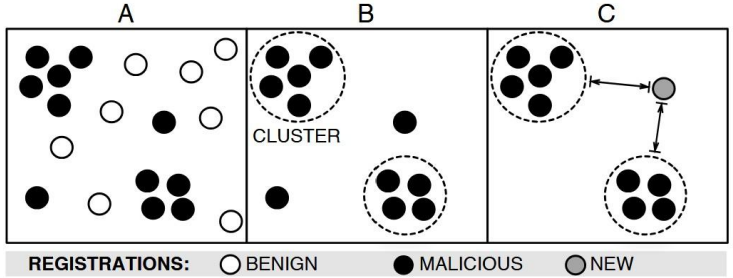


Figure 3: The three phases of the similarity-based prediction process. Malicious registrations in the training set are grouped together in clusters. Afterwards, new registrations can be compared to those clusters to predict their association with malicious activities.

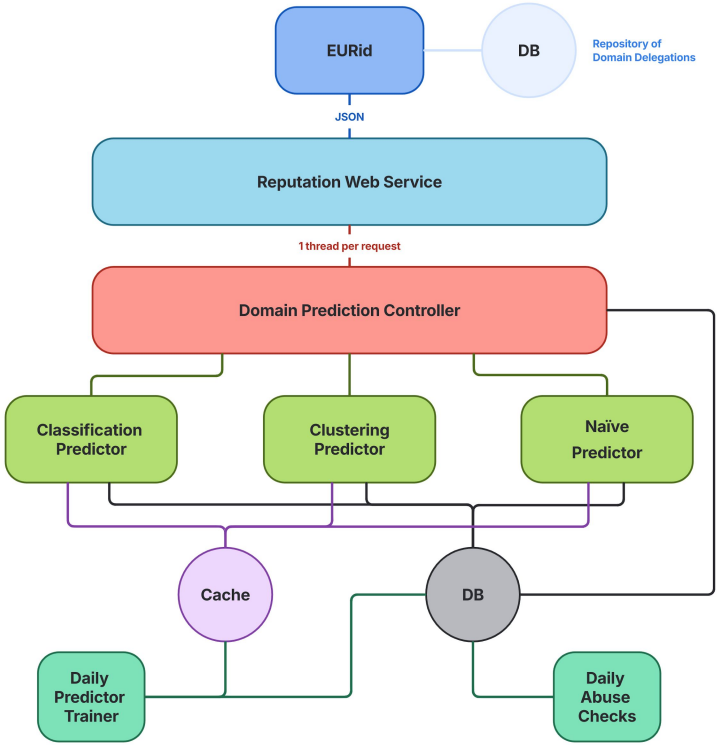
Introduction of AI / ML

Development of a prediction system

- Collaboration with KU Leuven University
- Based on registration (meta)data
- Different predictor models
- **Continuous training** via external sources and feedback loop

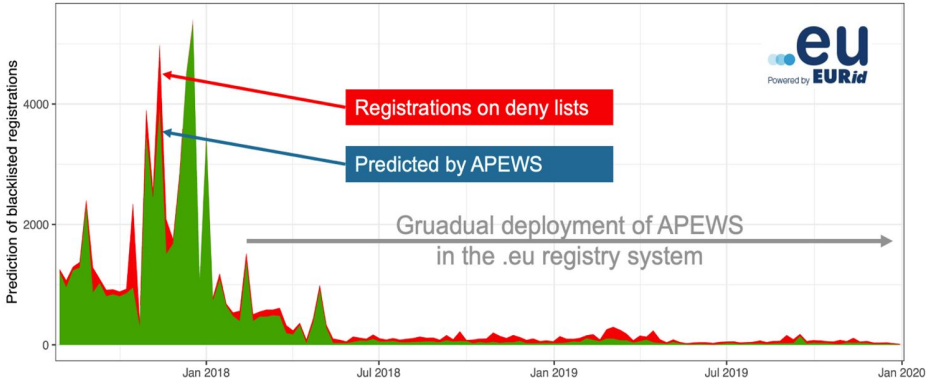
Scientific Publications on our website (eurid.eu)

- Detection of Algorithmically Generated Domain Names used by Botnets: A Dual Arms Race
- Exploring the Ecosystem of Malicious Domain Registrations in the .eu TLD
- Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations.
- An Operational Solution for DNS Registries to Prevent Malicious Domain Registrations



.eu POWERED BY EURid

Gradual Deployment



State of Play

Loop of Checks

- Each **check** can be enabled / disabled + assigned a **weight**
- Once **threshold** is reached, the **prediction** outcome will be 'malicious'

Addition of Rules

- Reduction of computational efforts
- Allows fast **tweaking of results**, independent of ML-training

Example: Keyword-related rules

- Covid-19 Pandemic
- War in Ukraine

Building block in a larger landscape

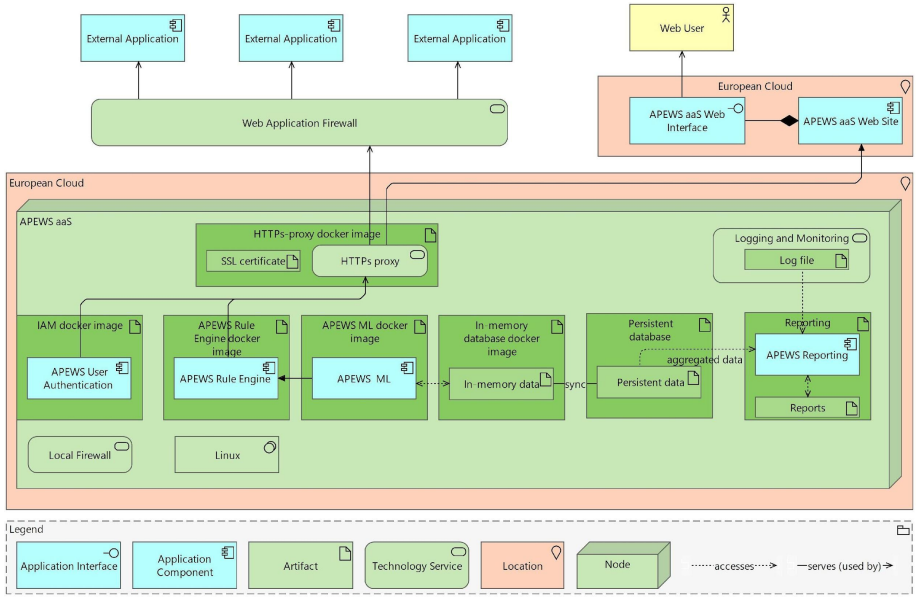
- Also **post-delegation checks**
- **Abuse Reports**: Problem of compromised servers / subdomains / …
- EURid is **content-neutral**, collaboration with 3rd parties (LEA, CERT, …)

Limitations

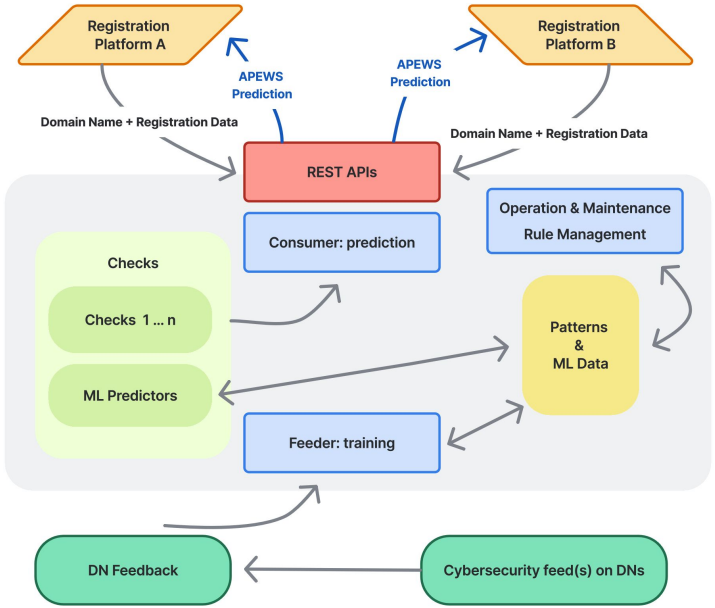
- **Dataset** is limited to .eu
- APEWS is **integrated** into the .eu registration platform
  - On-premise infrastructure
  - Message broker system

Current & Future Developments

- Expanding to a **multi-ccTLD** model
- **Anonymization** of data to be stored (ML)
- **Containerized** deployment on a **European Cloud**
- Communication via free and secure **REST-API's**



APEWS aaS – High Level Design



.eu POWERED BY EURid

One instance for all participating registries: Ensures centralized costs and unified approach.

Hosted on a European Public Cloud: Supports EU digital sovereignty and compliance with European data security standards.

Free and Secure REST APIs: Seamless and reliable integration for participating registries.

Self-Contained Database: Independent and efficient data storage for enhanced performance and scalability.

Machine Learning Training: Continuously improves abuse detection accuracy through collaborative data contributions.

Abuse Predictions: Report and Proactively mitigates DNS abuse threats with AI-powered predictions.

APEWS aaS - Roadmap

done

R&D and Product development

- Conduct research and develop the **core** DNS abuse prevention system.
  Establish **AI models** and define functional and non-functional requirements.

2025 - *done*

Lift & Shift + API Development

- **Transition** the system to a scalable cloud-based environment.
  Develop secure, free **REST APIs** for seamless integration with registries of all sizes.

2025 - *ongoing*

Open SaaS and test with registry community

- Launch the Software-as-a-Service (SaaS) **platform** for testing and feedback.
  Engage the registry **community** to ensure the system meets diverse operational needs.

2026 Onward

Enlarge community and improve model

- **Expand** the user base to include additional registries.
  Enhance the machine learning model with a broader dataset and refine based on feedback.

Powered by EURid

APEWS aaS - Integration Scenarios

The cost of integrating with APEWS as a Service for a registry would vary significantly depending on **two key factors**:

- The *technical architecture* of the registry's internal registration system
- The *desired level of integration* with APEWS.

To provide a clear overview, we outline **three possible integration scenarios**:

Scenario	Description	Advantages	Disadvantages	Cost / Effort
No Automation	Manual use of APEWS via web/Postman/scripts, no system integration.	• Minimal effort • No technical dependency	• Manual • Slow • Error-prone	1 – 5 Days
Limited Integration	Partial automation within registration flow, using common rules & feedback.	• Semi-automated • Shared rule set & feedback loop	• Some manual work • Limited flexibility	1 – 3 Months
Full Integration	Full bi-directional integration, custom rules, closed feedback loop.	• Fully automated • Registry-defined checks & reports	• High implementation effort • Possible internal changes	3 – 6 Months

Towards an AI powered European Shared Shield against Domain Name Abuse: apews.eu

General Inquiries
+32 (0)2 401 27 50
info@eurid.eu

eurid.eu

EURid vzw
Telecomlaan 9
1831 Diegem
+32 2 401 27 50

RPR Brussel – VAT
BE 0864.240.405

.eu .ею .ευ
POWERED BY EURid

Nominet's use of AI in DNS Abuse

Jake Vincet – Registry Policy Manager – Nominet .UK

Domain Watch

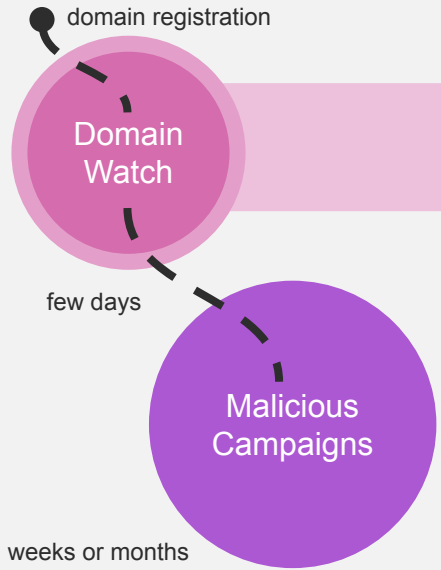
Domain Watch

An anti-phishing initiative to further increase the security of .UK and protect end users from malicious phishing activity

Designed to identify domains shortly after registration that are clearly deceptive

Mixture of rules and machine learning models that look for combinations of typos on key brands or keywords

Domain Watch



selfstorestorage.co.uk	3.7
greatoldbury.uk	1.6
owlconstruction.co.uk	0.2
28418232.co.uk	8.6
paypan.co.uk	9.5
golfballking.co.uk	8.8
evri-reschedule.uk	10
ring-a-roses.uk	4.2
psychics4you.uk	4.8
churchtower.uk	0.1
tax-gov.uk	10
team-down.co.uk	2.8
…	…

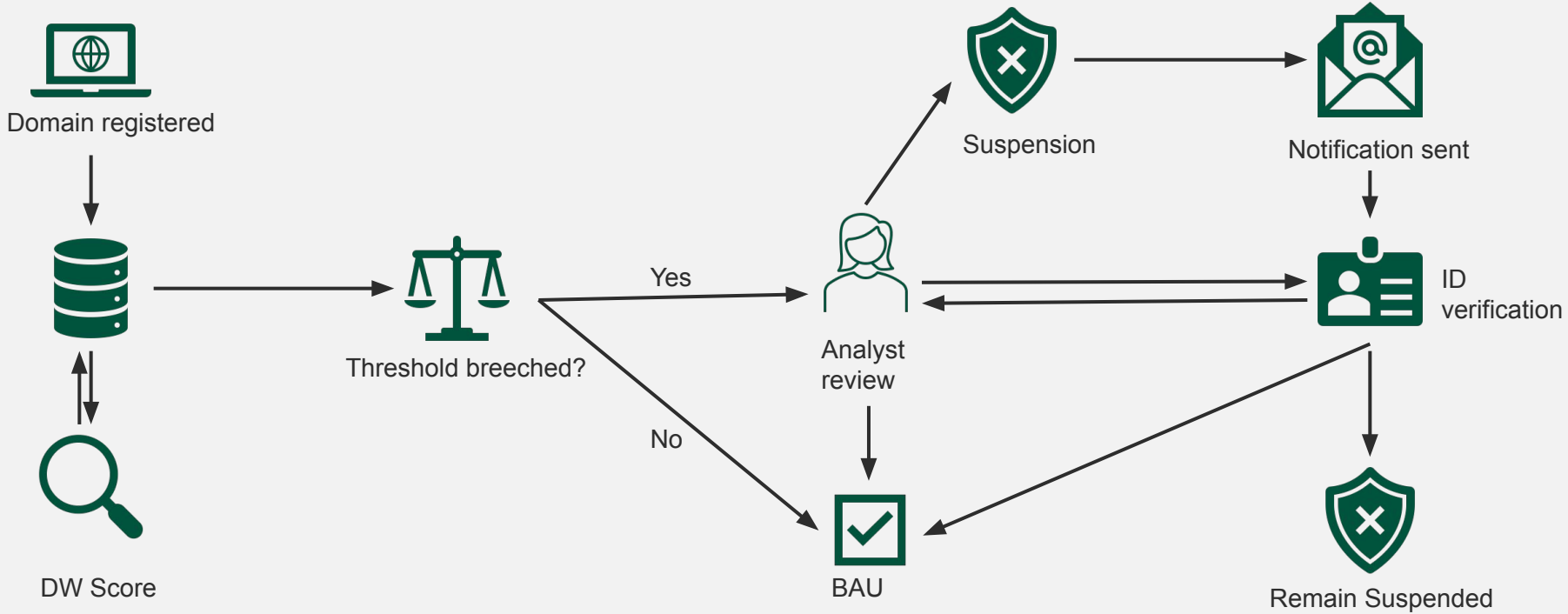
Every registered .UK domain is checked against the Domain Watch models

Score each domain using a mixture of rule-based and machine-learning models

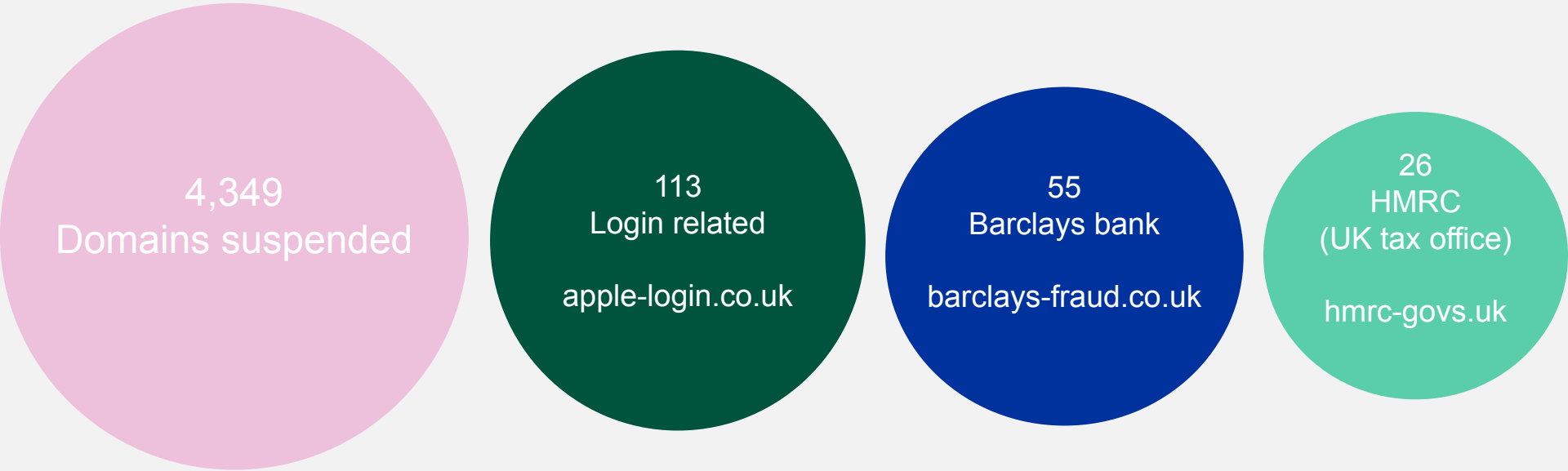
- **~20 domains a day flagged**
- **~50% suspended**
- **~10% of suspensions lifted**

All domains and scores are for demonstration only

Domain Watch Process



Domain Watch in Numbers

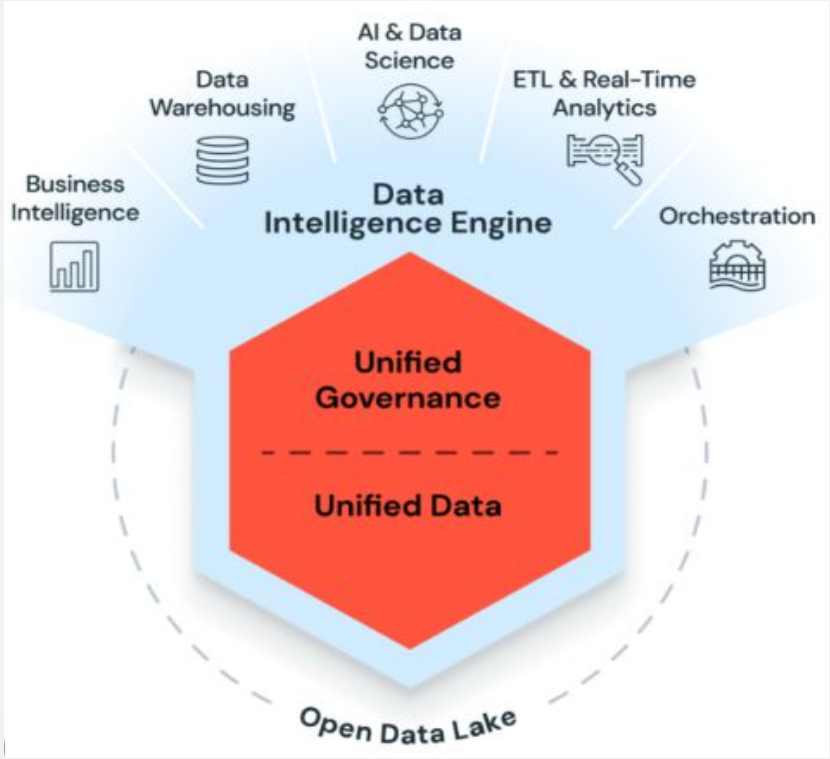


1 Nov 2023 - 31 Oct 2024

Genie

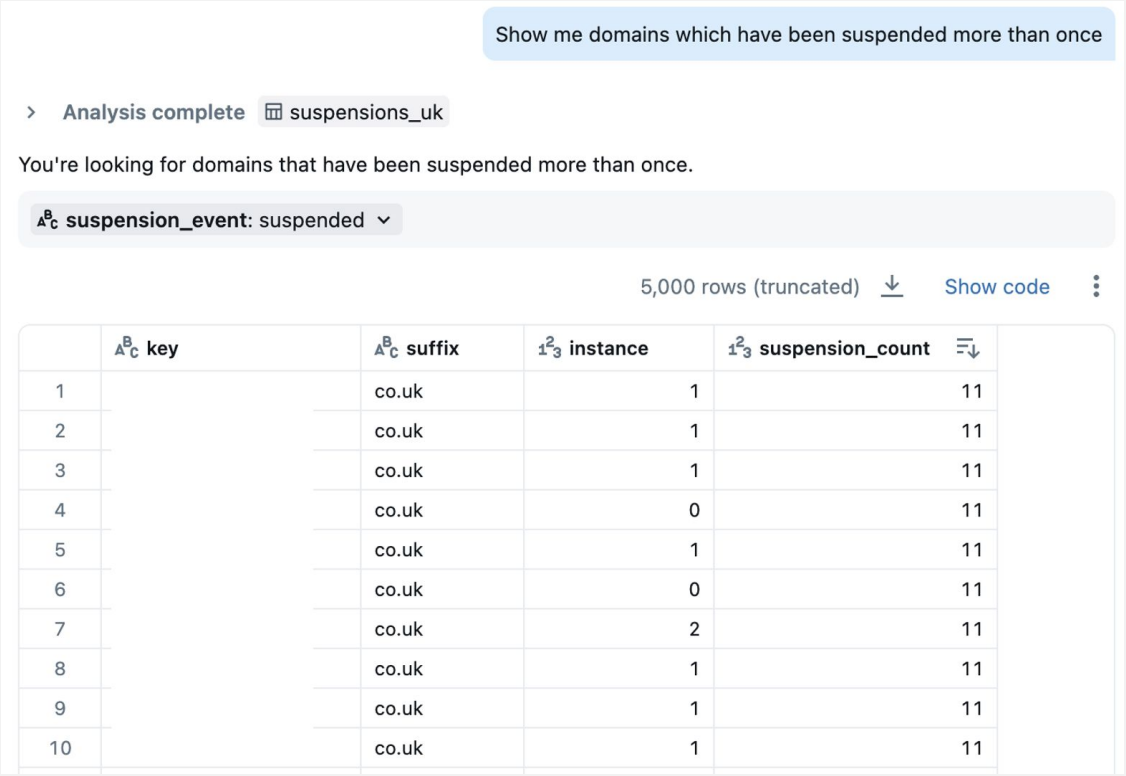
Genie

- Genie is an AI assistive feature of Databricks which is an analytics platform
- Our use of the tool is in its infancy, but we see use growing as we mature the capability
- Genie translates business questions into analytical queries
- Business users can query data which would have typically required SQL knowledge and database access



Genie – Basic use case

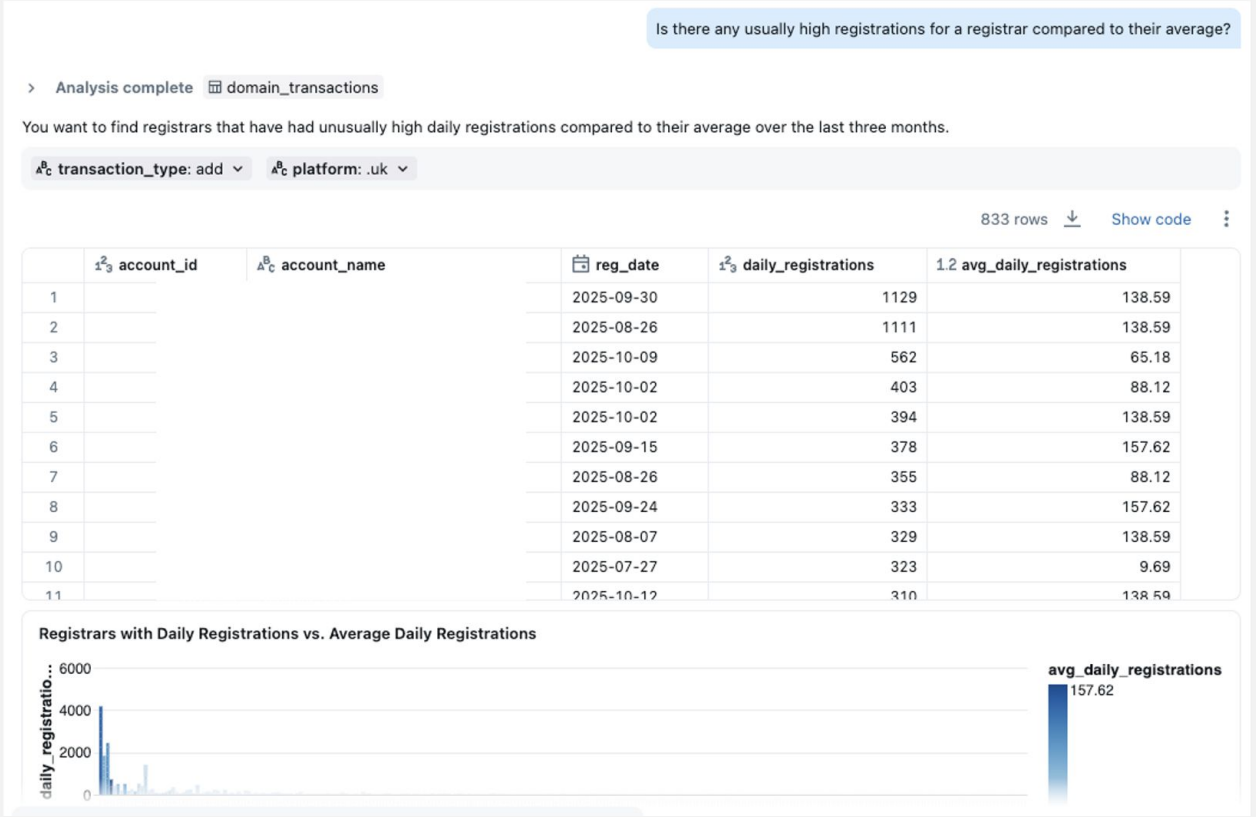
Could we do something with these domains to stop them being repeatedly suspended?



	key	suffix	instance	suspension_count
1		co.uk	1	11
2		co.uk	1	11
3		co.uk	1	11
4		co.uk	0	11
5		co.uk	1	11
6		co.uk	0	11
7		co.uk	2	11
8		co.uk	1	11
9		co.uk	1	11
10		co.uk	1	11

Genie

- Could we ask simple questions to look for spike and anomalies in registrations?
- Could we use it to pivot on registrant data for associated domain checks?



Collating Reports & Intelligence

Collate reports from a range of sources including MISP

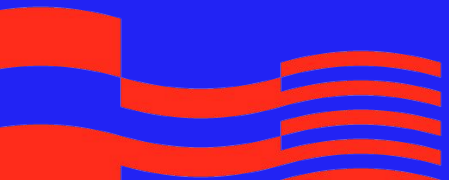
Use Genie to analyse the reports and extract key data at scale

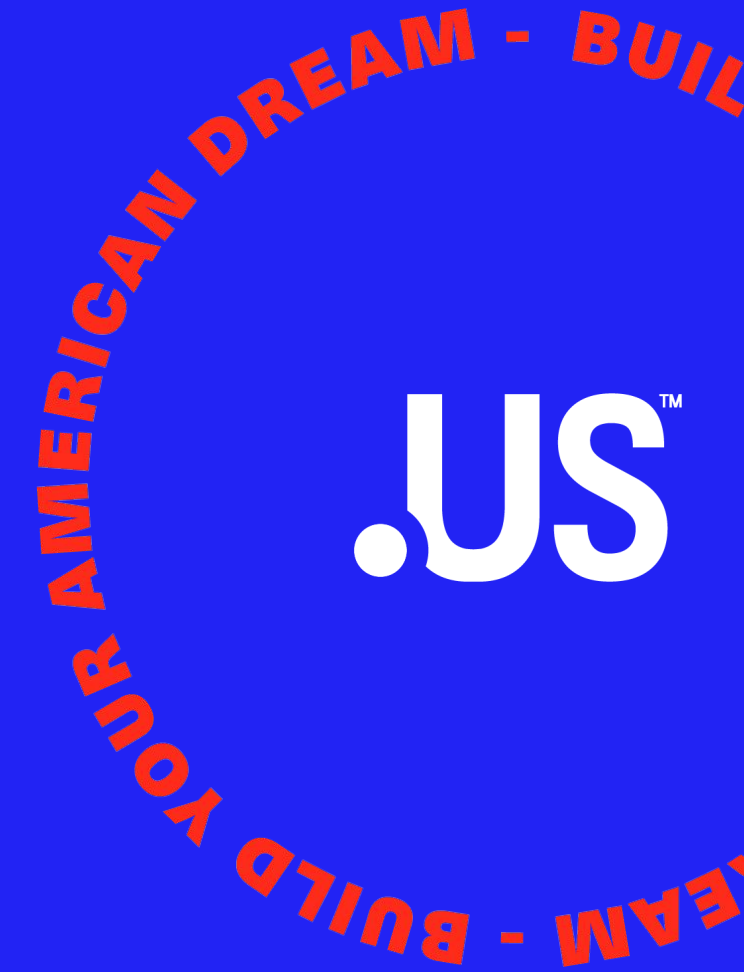
Produce findings in a human consumable format for action

Q&A

Preventative Measures for DNS Abuse in the usTLD

October 2025 – ICANN84





.US™

STATE OF THE DOMAIN

Domains Under Management

2.45M

Locality Domains Under Management

12.5k

+8.1%

DUM Growth Year Over Year

57.4%

Blended Renewal Rate

#10
TLD Ranking
Source: DomainState.com

#25
TLD Ranking
Source: DomainNameStat.com

**Stats as of 31 July 2025; Renewal rates as of April 2025*

.US™
Powered by GoDaddy Registry

PROACTIVE DOMAIN ABUSE BLOCKING

Combating DNS Abuse Before It Happens

Implementing capabilities to shift between reactive and proactive abuse prevention through AI-powered threat intelligence and cross-TLD pattern recognition

The Challenge - Current State of DNS Abuse Detection

Reactive Approach Challenges

- Abuse detected only after abusive activity
- Response times can expose users to risk
- A system that relies solely on reactive approaches creates a "whack-a-mole" cycle of enforcement

Cross-TLD Pattern Research Results

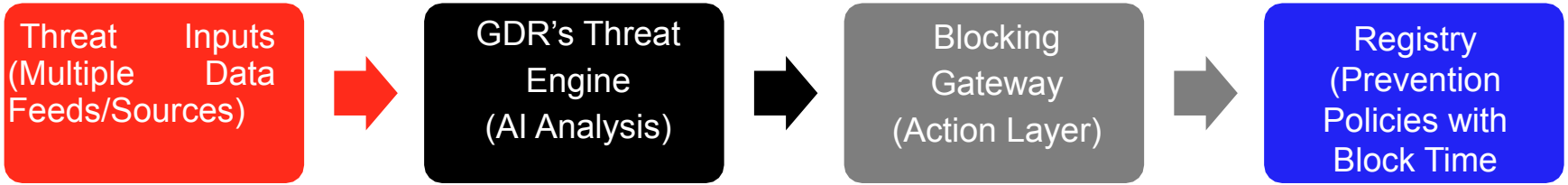
- Attackers often pivot between TLDs
- Weaknesses in cross-industry oversight enables exploitation of systems for DNS abuse
- Third parties weaponize TLD abuse

The Solution

Proactive Intelligence-Driven Prevention: Temporarily block domains identified as potential for malicious intent before registration using cross-TLD abuse patterns, AI analysis, and real-time threat intelligence to prevent DNS abuse with a TLD and protect the broader DNS ecosystem.

System Architecture - Multi-Layer Threat Analysis and Prevention

Data Flow



System Components

Historic Alert Integration (Threat Management Platform)

- Historical abuse records across GoDaddy TLDs provide baseline understanding of attack patterns

Threat Intelligence Feeds

- Real-time global abuse data integration with multiple providers

Cross-TLD Analysis

- Zone file analysis and bulk registration pattern detection across the TLD ecosystem

AI Threat Engine

- Fuzzy matching, ML behavioral analysis, and risk scoring with layered decision criteria

Blocking Gateway

- Interface providing automated blocking and appeals management

Impact Goals - Measurable Outcomes for TLD Security

Goal Metrics
(Upon initial proof of concept testing)

- **20%** Reduction in malicious domain registrations
- **20%** Known malicious strings blocked pre-registration
- **<5%** False positive rate for legitimate domains
- **75%** Faster abuse response time savings

Key Success Indicators

- Disruption of cross-TLD abuse migration
- Improved TLD reputation metrics
- Reduced downstream harm to users and brands
- Enhanced confidence with industry partners in abuse prevention within the TLD

Implementation Strategy - Phased Deployment

Phase 1: Proof of Concept [IN PROGRESS]

- Deploy targeting for the usTLD exclusively
- First focus is phishing pattern detection; then expand into other DNS abuse types
- Establish baseline metrics (*against goals*)
- Integrate threat intelligence feeds
- Develop appeals process

Phase 2: Optimization [Proposed]

- Refine AI models based on data
- Improve appeals processing
- Expand to additional abuse types
- Policy framework amendments
- Enhanced fuzzy matching

Phase 3: Product Expansion [Proposed]

- Deploy across additional GDR TLDs (gTLDs and ccTLDs)
- Cross-TLD intelligence sharing
- Commercial service development with Brand Safety Alliance
- Partnership integration
- Industry collaboration

Benefits for TLD Community - Raising Standards in DNS Security

Abuse Migration Disruption
Break the cycle of attackers moving between TLDs after enforcement occurs.
Outcome: Cross-TLD intelligence sharing prevents "Registry TLD shopping"

Enhanced Industry Reputation
Proactive measures improve overall trust in TLD operations
Outcome: Reduced negative publicity and security incidents

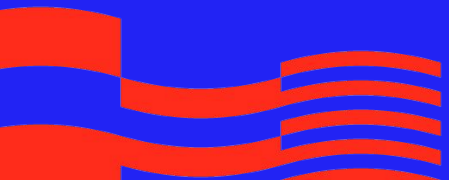
Cost-Effective Prevention
Preventing abuse can cost less than reactive cleanup and damage control
Outcome: Lower operational overheads for abuse responses

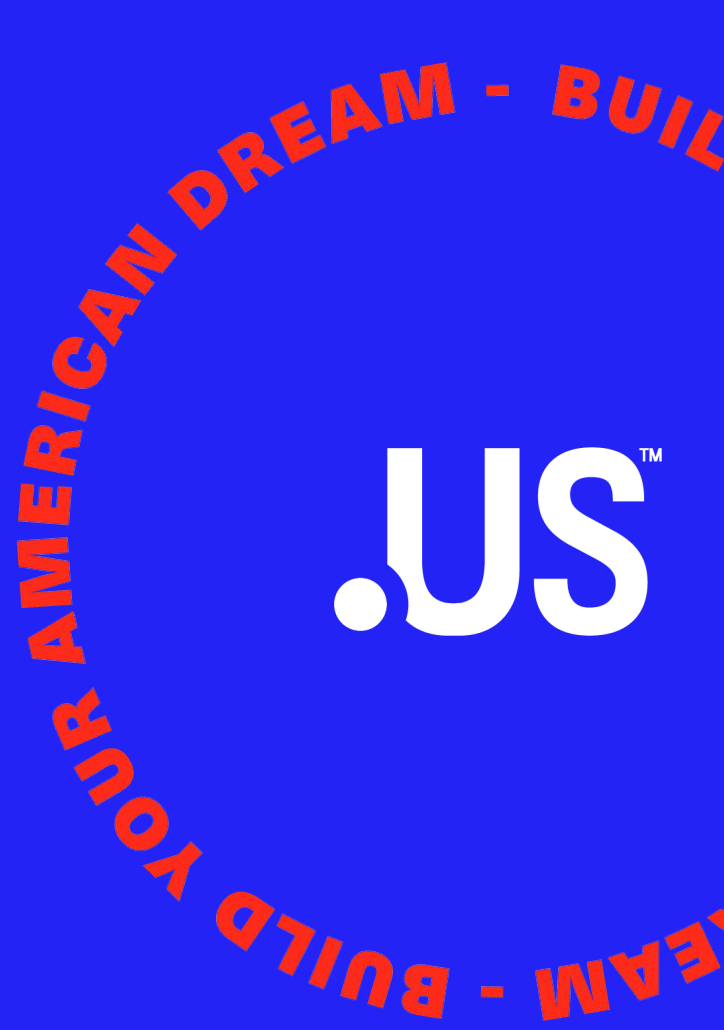
Collaborative Framework
Share threat intelligence and best practices across registry operators (and registrars)
Outcome: Industry-wide threat pattern recognition

Brand Protection Excellence
Proactive blocking enhances value proposition for
brand owners
Outcome: Higher brand confidence in TLD security measures

Regulatory Compliance
Demonstrate proactive responsibility to regulatory bodies
Outcome: Reduced regulatory pressure and oversight

QUESTIONS





.US™

Disclaimer

Definitions

We, us and our means any or all of the Registry Services, LLC group of companies, their related entities and their respective officers, employees, contractors or sub-contractors.

Disclaimer

This document has been produced by us and is only for the information of the particular person to whom it is provided (the Recipient). This document is subject to copyright and may contain privileged and/or confidential information. As such, this document (or any part of it) may not be reproduced, distributed or published without our prior written consent.

This document has been prepared and presented in good faith based on our own information and sources which are believed to be reliable. We assume no responsibility for the accuracy, reliability or completeness of the information contained in this document (except to the extent that liability under statute cannot be excluded).

Trademarks Notice

Any of our names, trademarks, service marks, logos, and icons appearing in this document may not be used in any manner by recipients of this document without our prior written consent. All rights conferred under law are reserved. All other trademarks contained within this document remain the property of their respective owners, and are used only to directly describe the products being provided by them or on their behalf. Their use in no way indicates any relationship between us and the owners of those other trademarks.

Forward Looking Statements

To the extent that the matters in this presentation include any forward-looking statements, such forward-looking statements are subject to risks and uncertainties. Actual results may differ materially from those contained in forward-looking statements as a result of many factors, including, but not limited to: the unpredictable nature of our rapidly evolving market; the effects of competition; technological, regulatory and legal developments; intellectual property litigation; developments in the economy, financial markets and credit markets, including as a result of the ongoing impact of the COVID-19 pandemic, continued escalation of geopolitical tensions and increasing interest rates and inflationary pressures. Any forward-looking statements are based on assumptions as of today, May 24, 2023, and except to the extent required by law, we undertake no obligation to update these statements because of new information or future events.

GoDaddy Registry

THANK YOU!

Crystal Peterson
Sr. Director, Registry Key Accounts &
Operations GoDaddy Registry

Thank you!