ULTRARED

XTRA BY ULTRA RED: EXTEND CTEM TO UNCONTROLLED ATTACK SURFACE

The Rising Threat of Phishing and Brand Abuse

Phishing, impersonation, and brand abuse are escalating at an unprecedented rate — posing serious risks to organizations worldwide. In 2024 alone, phishing attacks surged by over 200%, highlighting the urgent need for proactive defense against one of today's fastest-growing cyber threats.

XTRA is a new capability within ULTRA RED's CTEM platform, built to strengthen your exposure management by extending visibility and control to unowned assets and domains — a critical blind spot in the modern threat landscape.

XTRA identifies and allows take-down of phishing attacks early in their lifecycle by detecting and classifying malicious domains, brand impersonation attempts, and other forms of digital fraud — before they can cause harm.

By allowing you to take down rogue or unowned assets impersonating your brand, XTRA expands the reach of your CTEM program. It makes your exposure management more comprehensive and resilient, protecting your organization from one of the most commonly exploited attack vectors.

KEY BENEFITS

Detect Unowned and Uncontrolled Assets
Uncover rogue domains and spoofed infrastructure beyond your environment's control.

Prevent Phishing Attacks Early On
Identify and shut down threats before they reach your users or infrastructure.

Take Down Impersonating Domains
Initiate domain takedown requests for spoofed assets targeting your brand.

Safeguard Your Brand Reputation
Prevent misuse of your brand in phishing and fraud attempts across the web.

Core Capabilities

Intent Classification
Distinguish between legitimate and malicious intent with high accuracy by analyzing behavioral patterns, hosting details, and metadata, helping prioritize which domains pose real threats.

Progression Tracking
Monitor how suspicious domains evolve over time — from initial registration to potential staging and launch — to identify phishing campaigns in their earliest stages.

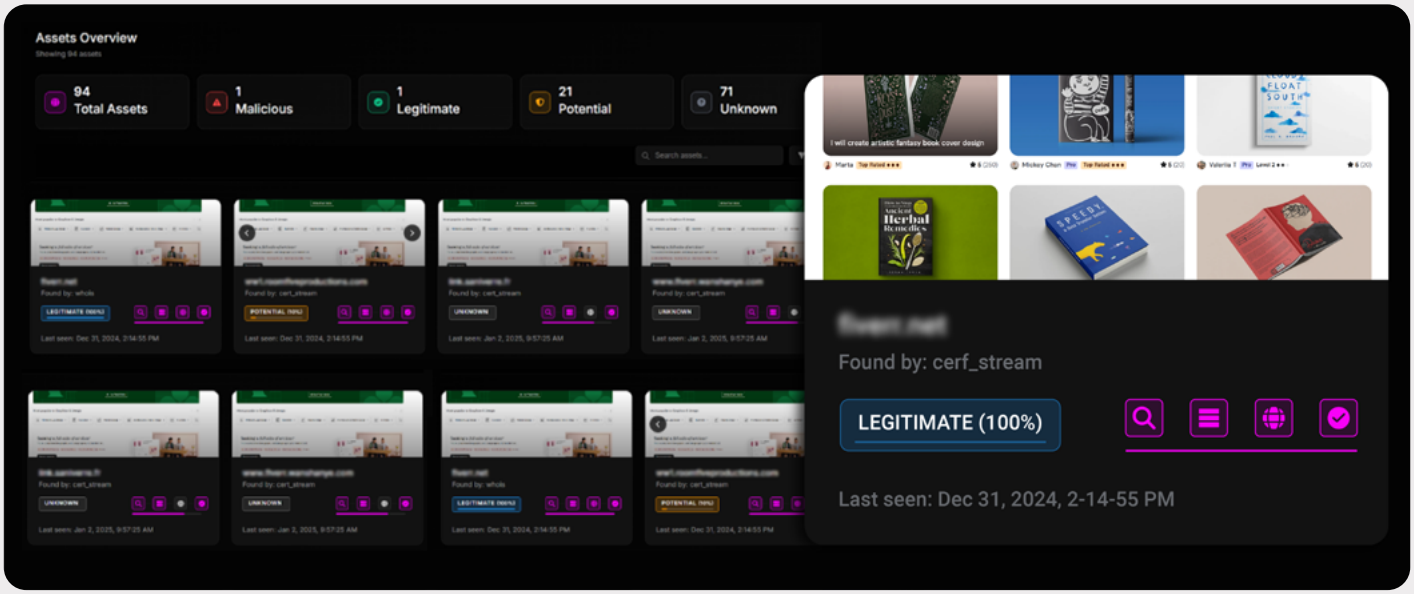
Similarity Analysis
Detect impersonation attempts using advanced similarity scoring that compares suspicious domains against your brand, domain names, and asset patterns, catching even subtle variations.

Easy Remediation
Request domain takedowns or secure lookalike domains through renewals or purchases. Actions are processed through automated pipelines, with each takedown billed separately.

XTRA: How It Works

Domain/ IP address

Discover unowned domains → **Analyze intent & similarity** → **Validate intent** → **Track progression** → **Take action**



XTRA findings: Instantly identify legitimate vs. malicious domains

Elevate Your CTEM Program with XTRA

XTRA by ULTRA RED extends your CTEM program beyond your owned assets, giving you the ability to detect, track, and take down malicious domains before they turn into active threats.

With intelligent intent classification, progression tracking, and built-in remediation actions, XTRA makes your exposure management more complete — helping you stay ahead of attackers while protecting your brand.

See XTRA in Action — Book Your Demo Today.

About ULTRA RED

ULTRA RED is a pioneer and leading provider of Continuous Threat Exposure Management (CTEM) solutions, built on a validation-first approach. Our CTEM platform enables security teams to confidently reduce threat exposure by continuously identifying, validating, and prioritizing gaps across the entire attack surface.
Learn more at www.ultrared.ai.

ULTRARED