CASE STUDY

ULTRARED

# BREAKING NEWS DOESN'T WAIT FOR THE NEXT PENTEST

## Continuous, Validated Exposure Management for Israel's Most-Read News Brand

**Organization:** ynet – Yedioth Ahronoth Group
**Industry:** Digital Media & Publishing
**Headquarters:** Rishon LeZion, Israel
**Founded:** 2000
**Website:** www.ynet.co.il

## BACKGROUND

ynet is the digital home of Yedioth Ahronoth and one of the most-visited websites in Israel. Online since 2000, it runs a 24/7 Hebrew newsroom alongside English, Russian and Spanish editions, lifestyle and local verticals, video and e-commerce.

Behind the homepage sits a footprint few organizations have to contend with: hundreds of domains and subdomains spanning news properties, election and sports microsites, campaign pages, commerce platforms, and a constant churn of staging environments. Twenty-five years of publishing leaves a long tail and every entry in it is still a door with ynet's name on it.

It is also a footprint under motivated attack. Israel was the most-targeted country worldwide for geopolitical cyberattacks in 2025: 1,881 attack claims, 12.2% of the global total (Radware). For groups seeking attention rather than extortion, a national news brand is one of the prime targets.

# CUSTOMER CHALLENGES

**Scale built over decades**

Two decades of publishing across microsites, campaign pages, and platforms – a digital footprint too large to map manually.

**Publishing faster than testing**

New properties go live in hours. An annual pen test describes an attack surface that no longer exists and misses the subdomain launched the next morning.

**Brand and trust as the target**

The worst case isn't data loss. It's a fabricated article on a ynet-branded address – a national story within minutes, and credibility a newsroom can't rebuild fast.

**Scanner noise, lean team**

Thousands of theoretical CVEs from version data, with no proof of exploitability. Triage consumed the whole week; system owners had no basis to touch live properties.

> We had plenty of vulnerability reports. The challenge was knowing which findings were real. If you're asking system owners to make changes in production, you need to prove why.
>
> **Ilan Norman, CISO at Ynet Group**

# THE YNET APPROACH: WHY ULTRA RED

ynet selected ULTRA RED for continuous, attacker's-eye visibility into its external attack surface - and to validate which exposures were genuinely exploitable. The deciding distinction: a platform that reports what might be vulnerable versus one that proves what is.

ULTRA RED executes real attack logic against discovered assets and surfaces a finding only once confirmed, with full proof-of-concept evidence - exact request, response and exploit path. That evidence turned conversations with system owners from debates about severity scores into decisions about demonstrated facts. Deployment required nothing: no agents, no appliances, no whitelisting.

**Proven exploitability, not theory**

Every exposure validated under real-world conditions before it reaches the team so a lean function remediates confirmed risk instead of triaging probability.

**Discovery at newsroom pace**

Continuous mapping of the full domain estate: a microsite launched for a breaking story is assessed as it appears, not in the next audit cycle.

**Zero deployment, zero risk**

Agentless and external, no installation, no changes to production. Critical where availability during peak news events is non-negotiable.

**One view of the brand family**

News, foreign-language editions, verticals and commerce assessed the way an attacker sees them: one perimeter, one brand.

# IMPLEMENTATION & RESULTS

ULTRA RED was deployed across ynet's full external footprint - news properties, verticals, foreign-language editions, commerce platforms and their surrounding staging environments - with continuous coverage from day one. Findings began surfacing within **hours** of onboarding.

**Continuous asset discovery**

A single, centralized view of all group assets – campaign sites, staging environments and subdomains – mapped in one place.

**Validated prioritization**

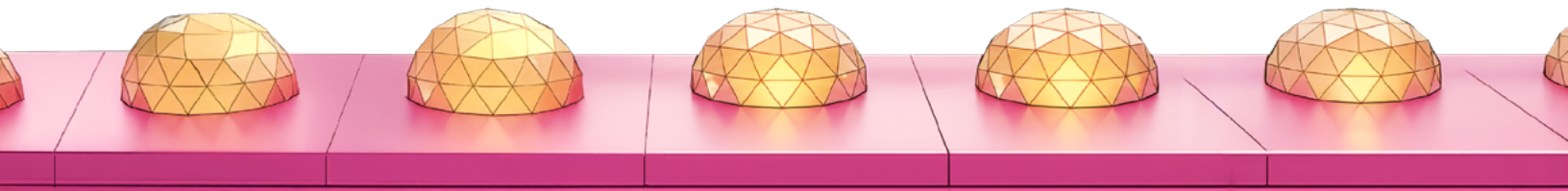
A ranked queue of confirmed-exploitable exposures instead of a CVE backlog. Validated findings remediated – mostly common web and configuration weaknesses, easy to miss at scale.

**Evidence-driven remediation**

Criticals move from detection to fix in **under 24 hours,** against a previous cycle of weeks. Proof-of-concept removed the reproduce-and-argue step entirely.

**Attack surface reduction**

Visibility became a decommissioning program: legacy assets retired and dangling DNS records removed – shrinking the perimeter, not just patching it.



# THE SUBDOMAIN THAT WASN'T THERE ANYMORE:

## Closing a Brand-Impersonation Risk Before Anyone Could Publish On It

Shortly after onboarding, ULTRA RED flagged a ynet.co.il subdomain created years earlier for a retired campaign. The campaign had ended. The content was gone. The DNS record was not - and it still pointed to a third-party resource that had since been released.

ULTRA RED validated it as a live subdomain takeover: the resource could be claimed by anyone, and whoever claimed it would control what a genuine, ynet-branded address served to the public. For a news organization that runs well past a defaced page — a fabricated article during an election, a phishing page on a domain readers already trust, malware under the country's most-read news brand. And because no breach of ynet's own infrastructure is required, no perimeter alarm would have sounded.

The finding arrived with proof-of-concept evidence that the takeover was viable. ynet removed the record the same day. The continuous DNS sweep that followed became the foundation of a permanent asset-lifecycle process.

> No one broke into anything. Someone had simply left a DNS record in place, and that was enough to publish content under our name. A typical scan wouldn't have caught it.
>
> **Ilan Norman, CISO at Ynet Group**

# LOOKING AHEAD: SECURITY AT THE SPEED OF THE NEWSROOM

- **DNS and asset lifecycle governance:** retiring domains and records when a campaign ends – decommissioning as part of the publishing workflow.
- **Pre-launch validation:** election hubs, tournament sites and event microsites validated as they go live.
- **Wider portfolio coverage:** extending continuous validation to additional Group properties, under a single attacker's-eye view.

### About ynet

ynet is the digital news platform of the Yedioth Ahronoth Group and one of the most-visited websites in Israel. Online since 2000, it operates a 24/7 Hebrew newsroom alongside English, Russian and Spanish editions, verticals, video and commerce. www.ynet.co.il

### About ULTRA RED

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