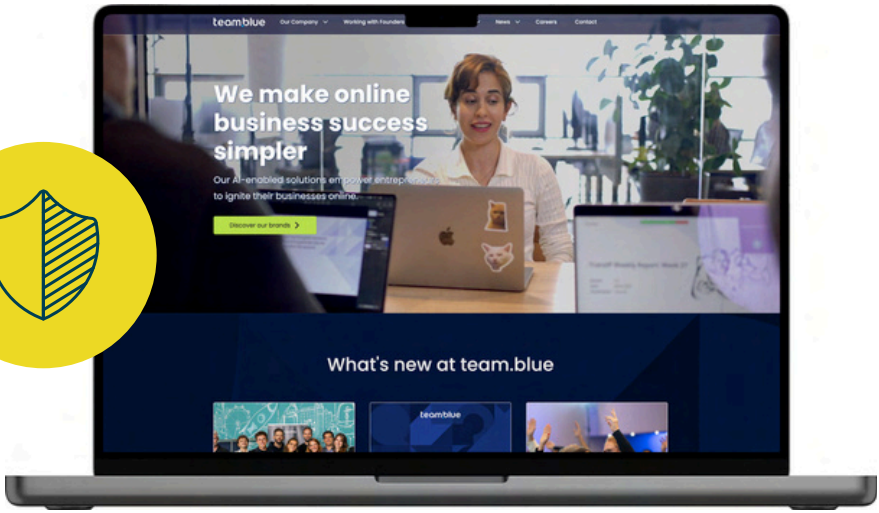
team.blue



CASE STUDY

From 50% Manual Work to 50% More Time:

How **team.blue** Automated Brand Protection Across 60+ Brands

netcraft

team.blue Overview:

Summary: team.blue is a European digital-services group (domains, hosting, email, cloud, and adjacent tools) serving **~3.3M SMB customers through 60+ brands across 22 countries**, with **3,600+ employees**. You'll recognize some of their brands like: Combell, TransIP, LCN.com, Shoptet, and more.

Use Cases:

- Phishing and Phishing URL Mail detection and rapid takedown/disruption across all brands.
- Centralized, standardized phishing reporting via portal/API and shared Slack workflows.
- Ingests Netcraft reporting to take down malicious sites they host.

> "Security is at the core of our business, and trust is the foundation of every customer relationship. We work proactively so our clients feel confident and protected at all times."
>
> — Emil Stahl, Security Lead

Challenge:

Multiple brands across geos:
With ~60 brands in 22 European countries, their fast-growing portfolio experienced campaigns surge, pause, and reappear.

Costly and slow manual takedowns:
Security team members spent up to 50% of their time in remediation of phishing campaigns targeting team.blue.

> "My Monday mornings were spent sending takedown emails, hoping they get actioned; it's not the most exciting way to start your work week." —Emil Stahl, Security Lead

Brand and support impact:
Ticket spikes and negative public reviews increased when victims associated losses with team.blue's brands. An increase in Denmark targeted attacks increased consumer liability (the first case was ~USD $1,200 equivalent), amplifying frustration and reputational risk.

> "The nature of our business is security, and trust is really important with our customers, being able to get in front of that and ensure they can feel safe with no concerns is really important to us." —Shelby Torrence, Marketing Director

Inconsistent internal reporting:
Across countries and brands, some teams are highly targeted and savvy; others are hit only a few times a year and unaware of the right reporting path.

Slow response to threats:
team.blue teams were unable to disrupt threats fast enough, recognizing that the value of disruption is directly tied to the speed at which an attack is addressed.

Netcraft Reported

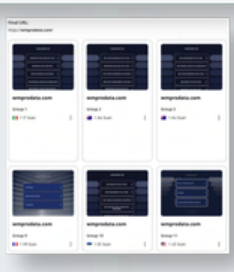
Available for: **3 hours Final**

Outage: **13 hours**

Phishing URL: **https://wmprodata.com**

Hosting Provider: **Amazon**

Automatically checking the attack status across geos through our proxy network



Solution:

Group-widerollout of Netcraft takedown & disruption:

- Coverage for all brands.
- Easy reporting via portal and API (including forwarding phishing emails).

Operational integration:

- Creation of an internal #phishing channel to funnel threat campaigns and intelligence.
- Developer-built tooling that flags spikes and enables one-click reports to Netcraft's API.

> "Now we can open Netcraft on a Monday and see that phishing logs started for a phishing attack reported by a customer on Saturday night. Before, we just had the data, but now we can use that data to be more proactive to kill the phishing campaign before it reaches our customers."
> —Emil Stahl, Security Lead

Provider leverage:

- Netcraft's strong relationships with registrar/hosting providers, including many that have direct integrations and kill-switches available.
- Rapid browser blocking as an initial disruption mechanism.

> "We recognize that some hosts will ignore everyone's requests, which isn't on Netcraft, but in most cases, Netcraft's kill switches and relationships with providers and blocking with browsers happen really fast. It's nice for us to know that when we report something, it gets actioned and addressed quickly."
> —Emil Stahl, Security Lead

Enablement & customer education:

- Brand-level FAQs (e.g., "report to phishing@...") to route signals centrally.
- Standardized, uniform reporting processes across all regions.

Impact:

Timesavings: Security and ops teams focus on acquisitions and customer requests instead of chasing abuse. The burden of alerts on weekends is reduced.

Faster disruption: Incidents are addressed in the critical first hour, limiting spread and minimizing follow-on tickets.

Brand protection:

- Fewer negative experiences escalate when campaigns are disrupted early.
- Clearer messaging to customers on how to report suspicious emails.

Attacker displacement: Observed shift of attacker focus to a major competitor after Netcraft go-live.

Better signal utilization:

- More customer-reported phish ingested (thanks to FAQs and shared mailboxes)
- Turning ad-hoc data into actionable takedowns

> "It just works. After implementing Netcraft, we observed that the threat actor group started targeting our main competitor with the same phishing kit. An increase of attacks started against them the same time we saw a decrease."
>
> — Emil Stahl, Security Lead

Key Results:

50% reduction

Up to 50% reduction in individual time spent on manual takedowns for key security staff.

~60 brands in 22 countries

Group-wide coverage: Rollout across **~60 brands in 22 countries** via a single service and API.

Operational responsiveness: Early disruption is achieved more consistently, reducing the window of victimization; support tickets are reported where the API/automation is in place.

Observed attacker pivot away from team.blue brands toward a competitor post-deployment.

Why Netcraft?

Proven accuracy & low false positives:team.blue had long received Netcraft's infrastructure abuse reports and knew the quality first-hand.

Speed via relationships & automation: Registrar/host APIs, kill-switches, and established contacts accelerate takedowns and browser blocks.

Scalable for Mergers & Acquisitions: For a business consistently taking on new brands, a single platform and process that onboards new brands quickly and uniformly is essential.

> "It's more like a partnership since we have the same interest in combating cybercrime" —team.blue

netcraft

Connect with Netcraft today for greater speed and global reach at scale.