INTERNATIONAL SECURITY HUB

Editorial Standards

Connecting global security. Empowering human freedom.

Our purpose

International Security Hub (ISH) exists to make expert, verified security knowledge accessible to the people who need it - practitioners, businesses, and individuals navigating an increasingly hostile digital landscape. Every article, white paper, research piece, and event feature we publish is held to the same standard we would want as security professionals reading it ourselves: accurate, actionable, and honest about what is known versus assumed.

We publish under the belief that security is a right, not a privilege reserved for those who can afford it. Our editorial standards exist to protect that mission - because a knowledge hub is only as valuable as its credibility.

Core principles

1. Accuracy over speed.

We are not a breaking-news outlet. If a threat, breach, or vulnerability is still developing, we say so explicitly and update the piece rather than publish speculation dressed as fact.

2. Sourced and attributable.

Every technical claim, statistic, or finding must be traceable to a primary source - a vendor advisory, CVE record, academic paper, regulatory filing, or named practitioner. Anonymous sourcing is permitted only for matters of genuine personal risk (e.g., a SOC analyst discussing employer failures) and is disclosed as such to the reader.

3. Responsible disclosure, always.

ISH will never publish proof-of-concept exploit code, unpatched vulnerability details, or information that provides meaningful uplift to an attacker ahead of a vendor fix or coordinated disclosure timeline. We follow the disclosure norms of the security community we serve, not the news cycle.

4. Practitioner-grade, plain-language.

Content should be technically defensible enough that a SOC analyst or CISO respects it, and clear enough that a small business owner or individual without a security background can act on it. Technical terms are explained in plain language the first time they are used, not assumed.

5. Independence from vendors.

ISH does not accept payment for editorial coverage. Sponsored content, vendor-authored pieces, and paid placements are clearly labeled as such and are never mixed into the editorial review pipeline. Product reviews disclose whether ISH received free access, briefings, or compensation from the vendor.

6. No fear-mongering.

We report risk honestly, without inflating threat severity for engagement. Headlines reflect the content. “Critical” is reserved for things that are actually critical.

Content categories & standards

Category	Standard
News & Analysis	Fact-checked against primary sources; analysis clearly separated from reporting.
White Papers & Research	Peer-reviewed by at least one subject-matter expert outside the author's immediate team; methodology disclosed.
Reviews (tools, vendors, certifications)	Testing methodology disclosed; conflicts of interest stated up front.
Event & Community Coverage	Attributed to a named ISH contributor or verified attendee account.
Expert Features	Credentials verified before publication.

Sourcing & verification

- Primary sources (CVE/NVD, vendor security advisories, government CERTs, court filings, peer-reviewed research) are preferred over secondary reporting.
- Where a claim originates from another outlet, we verify against the original source before republishing framing or figures.
- Screenshots, breach data, or leaked material are only used when necessary to establish a factual claim, are redacted of personal data, and are never presented as an invitation to access the same material.
- Statistics carry their source, sample size, and date. "Studies show" without a citation does not run.

Author & contributor standards

- Contributors write within their demonstrated area of expertise. Bylines include relevant credentials or role context.
- Guest contributors disclose current employer and any financial interest relevant to the topic.
- AI-assisted drafting is permitted for structure and clarity; all technical claims are human-verified by the named author before submission.
- Plagiarism, in whole or in part, results in immediate removal and a permanent ban from contributing.

Review process

1. Technical review

A subject-matter expert checks claims, methodology, and framing.

2. Editorial review

Clarity, tone, and adherence to these standards.

3. Legal/ethical check

For anything touching disclosure timelines, ongoing incidents, or named individuals.

4. Publication

With author, date, and sources visible.

Time-sensitive pieces

Time-sensitive pieces (e.g., an active incident) may run with an initial technical review and a note that legal/ethical review is in progress, updated within 24 hours.

Corrections policy

Errors are corrected transparently. Every corrected article carries a visible correction note stating what changed and when. Material errors that affect the substance of a piece are corrected within 24 hours of verification; minor errors (typos, formatting) are fixed without a public note.

We do not silently edit published claims about ongoing incidents, active threat actors, or named organizations - updates are appended, not substituted.

What we will not publish

- Working exploit code or step-by-step attack instructions absent a patched, disclosed vulnerability.
- Personal data obtained from breaches, doxxing, or unauthorized access.
- Unverified claims about a named individual's or organization's security failures.
- Content that facilitates surveillance, stalking, or harassment.
- Undisclosed sponsored or vendor-authored content presented as independent editorial.

A note from the founder

I started in a Dutch healthcare SOC during COVID-19, as the third analyst onboarded into a team built almost overnight to protect Dutch residents' sensitive data under unprecedented strain. I have since worked municipal security operations, led ISO 27001 audits, run cyber resilience programs at enterprise scale, and served as Cybersecurity Officer for critical infrastructure, working with industrial control systems. What I learned across all of it is the same thing this hub is built on: good security knowledge is often locked behind paywalls, technical language, or organizations too large to share it freely.

International Security Hub is our answer to that. These standards are how we keep that answer honest.

- K. El Bouhmi
Founder, International Security Hub

Our editorial promise

Accurate. Actionable. Transparent about what is known, what is assumed, and what still needs verification.