How to Write a Cybersecurity Whitepaper

That People Actually Read

Whitepaper Submissions

ISAUnited

ISAUnited
Technical Research Center
A Division of Applied Cyber Sciences

A short, practical guide for practitioners who want to turn engineering work into a clear, persuasive whitepaper.

Most cybersecurity pros are builders, breakers, and fixers—not writers. That is okay. A solid whitepaper is just your engineering work told in a clean, useful story: why the problem matters, what you tried, what worked, what did not, and what others can reuse tomorrow. This guide shows you a simple path to get there—without academic jargon or marketing fluff.

What a Whitepaper Is (and Is Not)

A whitepaper is a practitioner's narrative that turns hard-earned lessons into repeatable guidance. It is practical, evidence-aware, and action-oriented. It explains the problem, shows your design decisions, and proves your approach with reasoning, references, or artifacts (logs, configs, tests, diagrams). It is not a press release, a sales deck, or a research paper.
A research paper contributes new knowledge with formal methodology, original data, and peer-verifiable results. If your work does not include original study design and analysis, you are

likely writing a whitepaper. ISAUnited publishes both. If you plan to submit a research paper, contact us via the site's Contact section first so we can route it to the research review pathway.

A Simple, Reusable Structure

Use this as your backbone. Each section should be short, concrete, and written for a busy engineer or decision-maker.

1) The Situation – What is happening in the wild, and why it matters now. State the stakes in one paragraph.

2) The Gap – What current practices miss. Name the risk plainly (exposure, fragility, blind spot).

3) The Approach – Your design, framework, or method. Explain it like you would to a peer on a whiteboard.

4) Evidence – How you know it works: tests, logs, simulations, metrics, or comparisons.

5) Implementation Notes – What to do first, where it breaks, and how to avoid common mistakes.

6) Outcomes – What improved (latency, coverage, resilience, MTTR) and what to measure next.

7) Call to Action – A clear next step: pilot, workshop, or adoption checklist.

Three Common Flavors (Pick One, Blend Two)

- Technical: You are explaining a concrete mechanism or concept—say, Component Integrity Engineering (CIE) or an adversary-aware segmentation pattern. Keep the narrative tight: problem → mechanism → validation → how to reuse.
- Problem–Solution: You found a nasty gap (for example, lateral movement through unmanaged identities) and built a fix. Walk the reader from pain to remedy, then prove it with results or artifacts.
- Framework/Methodology: You are standardizing how to do something—like Adversary-Centric Defensive Architecture (ACDA). Define roles, steps, decision points, and checkpoints so others can execute consistently.

Real Examples

- **Technical Whitepaper**
  - Use it when: explaining a concrete mechanism, concept, or innovation.
  - Why it helps: establishes technical authority and speeds adoption with clear how-to detail.
  - Example: Component Integrity Engineering (CIE) concept brief.
- **Research-Backed Whitepaper**
  - Use it when: presenting findings supported by data (studies, benchmarks, experiments).
  - Why it helps: lends credibility for standards, funding, or policy decisions.
  - Example: Effectiveness of AI-driven cyber defense models.
- **Industry Trends & Forecasting**
  - Use it when: analyzing emerging risks, market shifts, or near-term predictions.
  - Why it helps: attracts decision-makers seeking strategic timing and direction.
  - Example: Post-quantum impacts on enterprise cybersecurity.
- **Problem–Solution Whitepaper**
  - Use it when: a specific gap/pain needs a structured, repeatable fix.
  - Why it helps: positions you as a practical problem-solver with measurable outcomes.
  - Example: Adversary-Centric Defensive Architecture (ACDA) for external attack surfaces.
- **Call to Action (Change Advocacy)**
  - Use it when: pushing industry practices, policy shifts, or adoption of new norms.
  - Why it helps: mobilizes communities and stakeholders around a clear next step.
  - Example: Professional licensing for cybersecurity engineers.
- **Comparative Analysis**
  - Use it when: choosing between technologies, frameworks, or approaches.
  - Why it helps: clarifies trade-offs and drives informed adoption.

    - Example: Defensible Standards vs. NIST/ISO in enterprise programs.
- **Framework & Methodology**
    - Use it when: defining a structured way to design, implement, or govern.
    - Why it helps: enables consistent execution and auditability across teams.
    - Example: ISAUnited Cybersecurity Design Model (CDM).
- **Thought Leadership**
    - Use it when: shaping direction with big-picture, forward-leaning ideas.
    - Why it helps: builds reputation and opens doors for collaboration.
    - Example: Why cybersecurity needs systems engineering.
- **Regulatory & Compliance**
    - Use it when: interpreting new rules, mapping controls, or guiding attestations.
    - Why it helps: reduces risk, rework, and penalties through clarity.
    - Example: Aligning Defensible Standards with global regulations.
- **Case Study**
    - Use it when: documenting a real-world implementation and results.
    - Why it helps: proves value with outcomes others can replicate.
    - Example: Fortune 500 rollout of Defensible Architecture.

Voice and Readability (Write Like You Talk to a Peer)

Write in plain language. Prefer verbs like validate, instrument, isolate, correlate, and measure. Short paragraphs. Active voice. If a sentence has more than one idea, split it. Replace vague claims with a one-line proof (metric, log, or test).

Ready to Publish?

Submit your whitepaper. If you are an institute member, please use the ISAUnited TRC portal. If a non-member, email to research@isaunited.org. For research papers with original study methods and new datasets, reach out via the Contact section first. If you want a quick gut-check on scope or structure, include a one-paragraph summary, and we will point you to the right review path.