

Reducing Your Attack Surface Is No Longer Optional

Anant Shrivastava
Founder
Cyfinoid Research

About Cyfinoid

- Research focused cyber security firm
- Major focus areas as of now
 - Software Supply Chain
 - Web Applications
 - Cloud Security

<https://cyfinoid.com/>

Anant Shrivastava

- Chief researcher @ Cyfinoid Research
- 15+ yrs of corporate exposure
- **Speaker / Trainer:** BlackHat, Defcon, c0c0n, nullcon & more
- **Project Lead:**
 - Code Vigilant (code review project)
 - Hacking Archives of India
- (@anantshri on social platforms) <https://anantshri.info>

How Developers use to write code

A developer uses a **Chrome extension** to manipulate AI prompts, which are then fed into **Visual Studio Code** through a set of AI-driven code completion **extensions**. The resulting code is committed to **GitHub**, where a set of **GitHub Actions** automatically run analysis and tests. The code is then containerized into a **Docker image**, deployed on **Kubernetes**, running inside an **EC2 instance**, built from a specific **AMI**.

How developers now write code

A developer uses an **autonomous AI agent** to write code by providing them a one liner prompt and **full access to the command line**. The resulting code is committed to **GitHub**, where a set of **GitHub Actions** automatically run analysis and tests. The code is then containerized into a **Docker image**, deployed on **Kubernetes**, running inside an **EC2 instance**, built from a specific **AMI**.

Things we all need to worry about

Your **Biz Dev / HR / Finance person** gets an idea, **downloads cursor/windsurf/AI IDE**, **pays** for 1 month of **subscription by personal card**. Uses the IDE to **develop the application**.

Does **deployment per AI recommendation** in **personal vercel / railway or likes**. Either get admin to **CNAME to a url** or just make a **url available as direct url** in documentation.

Attack Surface

The attack surface is the total sum of all reachable ways an adversary can interact with your system : intentionally or unintentionally.

- **Code** you write (endpoints, APIs, binaries)
- **Configurations** you expose (network ports, IAM roles, CI/CD runners)
- **Data** you store, process, or leak (logs, backups, analytics feeds)
- **Identities** that can authenticate or impersonate (users, tokens, service accounts)
- **Dependencies and integrations** you inherit (open-source, SaaS, AI models, APIs)

Current way of handling things

- Patch after compromise
- Add another scanner
- Deploy more layers
- Buy another dashboard
- Monitor more alerts

Reality of Modern World

- AI has lowered the barrier for attackers.
- Supply chains are opaque and unmanageable.
- Cloud and CI/CD systems now control everything.
- Misconfigurations at abstraction layers bypass traditional defenses.

"AI is a multiplier. If you're a +1 programmer, it can make you a +10. But if you're at -1, you're just amplifying bad decisions at scale."

<https://blog.anantshri.info/a-rational-survival-guide-to-vibe-coding-with-ai>

AI Effect

Speed negates the need for efficiency

- Faster development turnaround
- More feature requests
- Lesser testing time allocated
- More bugs in the system
- More bugs fixed coz of AI
- Cycle repeats

AI hallucinating package names

 www.darkreading.com/application-security/ai-code-tools-widely-hallucinate-packages



DARKREADING

Cybersecurity Topics ▼

World ▼

The Edge

DR Technology

The analysis showed 21.7% of the package names that open source AI models recommended or referenced in response to specific coding-related inputs were hallucinations — meaning no such packages existed in npm or PyPI repositories. With commercial AI models, the problem was somewhat more limited in scope, as 5.2% of the package names were hallucinations.

<https://www.darkreading.com/application-security/ai-code-tools-widely-hallucinate-packages>

<https://arxiv.org/pdf/2406.10279>

AI for Defensive Purposes

>   www.darpa.mil/news/2025/aixcc-results

Teams' AI-driven systems find, patch real-world cyber vulnerabilities; available open source for broad adoption

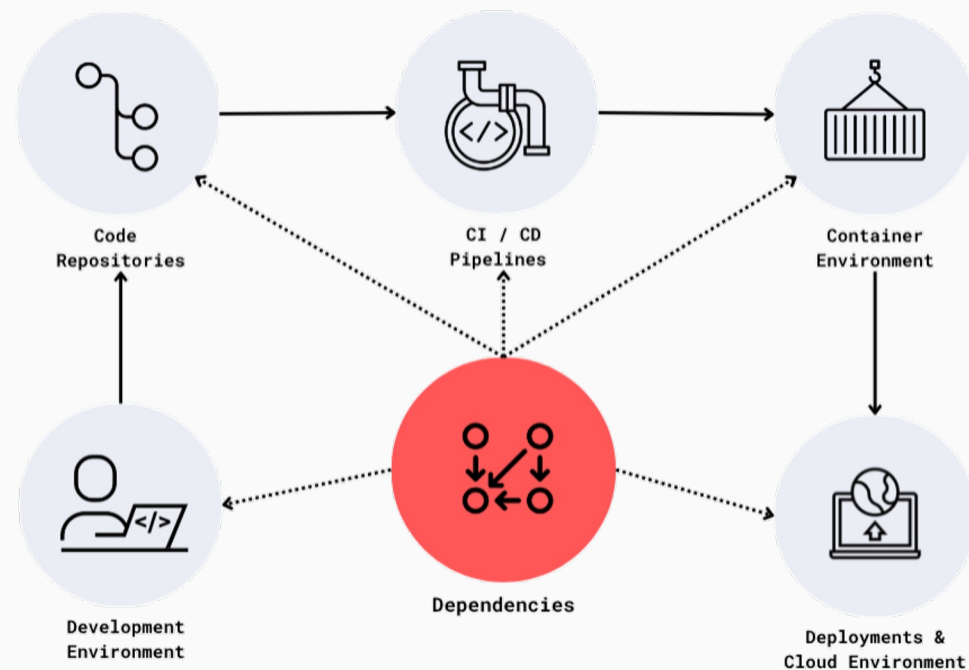
Aug 8, 2025

A cyber reasoning system (CRS) designed by Team Atlanta is the winner of the DARPA AI Cyber Challenge (AixCC), a two-year, first-of-its-kind competition in collaboration with the Advanced Research Projects Agency for Health (ARPA-H) and frontier labs. Competitors successfully demonstrated the ability of novel autonomous systems using AI to secure the open-source software that underlies critical infrastructure.

<https://www.darpa.mil/news/2025/aixcc-results>

Software Supply Chain

- We are about 80% dependent on others for all our software needs



Attack Surface Reduction

Lets try a different approach

Attack Surface Reduction Manifesto

- Build less. Expose less. Trust less.
- The Attack Surface Reduction (ASR) Manifesto is a philosophy-first approach to building resilient systems through subtraction, not accumulation.
- Rather than chasing visibility across growing complexity, we advocate for systems that are simpler, smaller, and inherently less attackable.

reducetheattacksurface.com

Attack Surface Reduction

- Minimal Footprint
- More wood behind fewer doors
- Less trust boundaries to exploit
- Actively reducing the attack surface

Areas of Reduction

- Software
- Identify and Access Management
- Infrastructure
- Data

Software Reduction

- **1. Minimize Features, APIs, and Endpoints**
- **2. Internal Reuse Over External Dependence**
- **3. Shrink Your Build and Toolchain**
- **4. Limit Codebase Blast Radius**
- **5. Hardening Through Simplicity**

IAM Reduction

- **1. Principle of Least Privilege**
- **2. Human Account Hygiene**
- **3. Service Identity Discipline**
- **4. Shadow Access Discovery**
- **5. Role Explosion Control**
- **6. Federated Identity Risks**
- **7. Secret Lifecycle ASR**
- **8. SaaS and Vendor Identity Exposure**

Infrastructure Reduction

- **1. Expose Nothing by Default**
- **2. Reduce Control Plane & Runtime Complexity**
- **3. Minimalism at the Image and Execution Level**
- **4. Prune Zombie Infra & Orphaned Services**
- **5. Reduce Lateral Movement Paths**
- **6. Runtime Cleanup & Reboot Culture**
- **7. Infrastructure-as-Code & Deployment Discipline**

Data Reduction

- **1. Collect Less Data by Default**
- **2. Reduce Data Retention**
- **3. Limit Data Propagation and Transformation**
- **4. Don't Over-Engineer Analytics**

How to convince management

- Quantifiable outcome (show me the \$\$\$\$\$)
- Reduced assets results in reduced cost for
 - Ongoing operation
 - ongoing security on assets (Compliance formalities)
 - electricity
 - data traffic
 - Any per device license cost
- For data : storage cost per mb is a good measure

What next?

- Explore your environment
- Identify non needed and non used entries
- Reduce the attack surface
- Revisit the manifesto @ reducetheattacksurface.com

Thanks for listening & open to Questions?

NAME **WEBSITE**

anant@cyfinoid.com

EMAIL



Trainings & Research

Web Application | Cloud | Supply Chain

Trainings

[Attacking Software Supply Chain](#) | [Attacking Cloud Environments](#)

Contact us at **contact@cyfinoid.com**