Shadow AI

The New Supply Chain Disruptor

Anant Shrivastava

Founder

Cyfinoid

About Cyfinoid

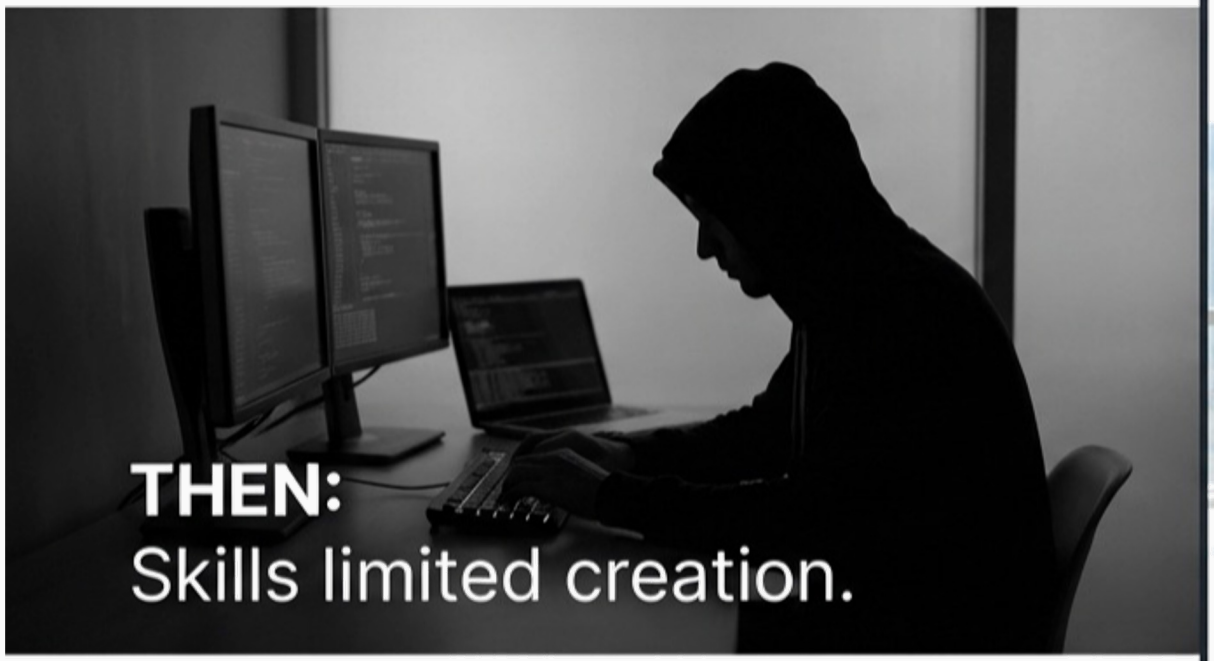
- Research focused cyber security firm
- Major focus areas as of now
  - Software Supply Chain
  - Cloud Security

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

World has changed



AI removed the requirement to be a developer.
Business teams now deploy production systems.

The flow we all need to know

1. The Idea

A non-technical employee has an idea for a business application.

2. Tool Acquisition

They download an AI IDE and pay with a personal card.

3. AI-Assisted Development

The employee uses the AI-powered tool to build the application.

4. Unsanctioned Deployment

Following AI recommendations, they deploy it to a personal cloud service.

5. Unofficial Launch

They share a direct URL or get an admin to link it.

Shadow's of all kind

Shadow IT

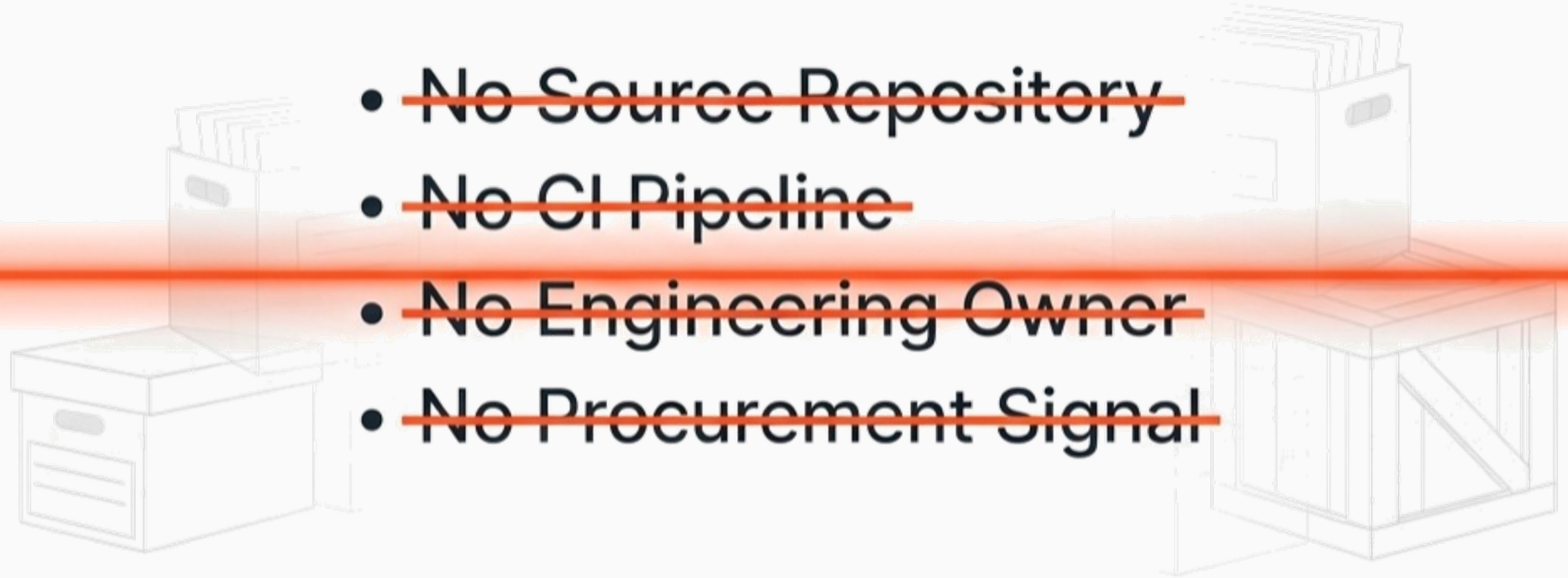
SaaS Tools,
File Sharing

Risk shifts from Data Leakage to Business Failure

Shadow AI

Workflow Automation,
Decision Support

Production



- ~~No Source Repository~~
- ~~No CI Pipeline~~
- ~~No Engineering Owner~~
- ~~No Procurement Signal~~

Traditional security tools (SCA, SBOM) fail because there is nothing to scan.

Current way of handling it

You cannot ban capability. Work routes around friction.

Inventory the systems

We stop trying to control the code and start tracking the intent.

Who built it? What data flows through it?

Old Inventory (Code)

New Inventory (Process)

Operational Loop

A Weekly Living Loop. Not a One-Time Audit.

Angles to Discover

Don't Spy. Listen to Signals.

DNS & Domains

OAuth & SSO

Reverse Proxy

External Apps

Shadow AI : Risk Classification

Data	Blast Radius	Control Maturity
Public	Internal	Customer/Regulated
Individual	Team	Org-wide
None	Partial	Strong

Explainable. Defensible.

Carrots and Sticks

Reward Visibility. Submission buys Support.

If you punish shadow AI, you create more shadow.
If you reward it, you gain visibility.

Incentive Loop

Build & Submit

Reward & Support

Harden & Maintain

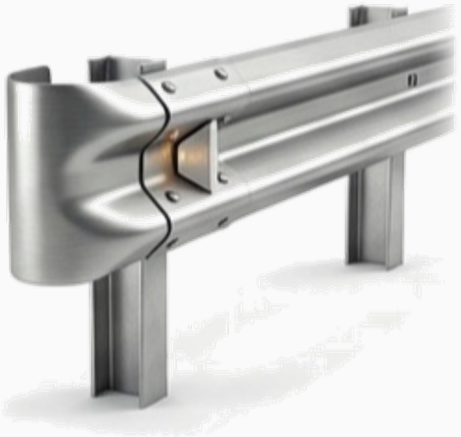
Submission buys Support.
Innovation flows in, Risk **flows out.**

Relook at your role

ENGINEERING

Hardening & Scale
Owns Maintenance

SECURITY



Guardrails & Acceleration
Defines Stances

Engineering doesn't police. Security doesn't block.

Thanks for listening & open to Questions?

Cyfinoid

Trainings & Research

Web Application | Cloud | Supply Chain

Trainings

Attacking Software Supply Chain | Attacking Cloud Environments

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