Transparency in Security

Security by Obscurity Doesn’t Work!

Paul Harrison

What Now?

Security by obscurity doesn’t work, if your posture sucks.. it sucks.

If implemented properly, security measures should be resilient and… doing their job?

Let’s talk about it!

Who am I anyways?

Paul Harrison (hi!)

Currently: Security Operations at Mattermost

Previously:

- Frontbridge Technologies (yep, that was 20 years ago)
- Microsoft
- Northfield IT
- GitLab
- Very Good Security

Mattermost

What do I do?

- Build security engineering and operations programs for Startups
- Advise and consult on security and compliance programs
- Advise on security feature design, implementation, and real-life use.

Anyways… Security!

Who has…

Who has run a bake-off (“vendor selection”) to buy a service or platform?

Or…

Tried to hire an engineer for a technical Security role?

Or considered applying for a technical Security role?

How about…

Tried to monitor DNS traffic from pods on a large, high-volume K8S cluster to spot DNS rebinding attacks?

(Seriously? Anyone?)

Or maybe?

Built alert enrichment pipelines to improve SnR and decrease remediation time of new incidents?

(Special Mention: Panther Labs, Tines)

OK… why?

Trying to help solve…

- Help people show off their successes, talk about their failures and frustrations.
- Improve hiring (both being hired, and hiring people!)
- Helping ramp the next generation of Security Engineers
- Growing the Security community
- Get new customers and simplify hiring vendors

And also..

Recording our knowledge, experiences, and mistakes on how we’ve managed to improve over time.

(Whether you use it or not is your own problem)

Make Security (yes, all of it) better, I don’t want my data to leak either!

Risk: Impact * Likelihood - right?

Common ground on risk profiles

Well-funded actors / APT <———> Randomware Gangs

High-volume confidential data <———> The next great recipe site

Talking about Security “things”

It’s about…

Be Humble

Imposter Syndrome & Anxiety

Not talking about Fight Club

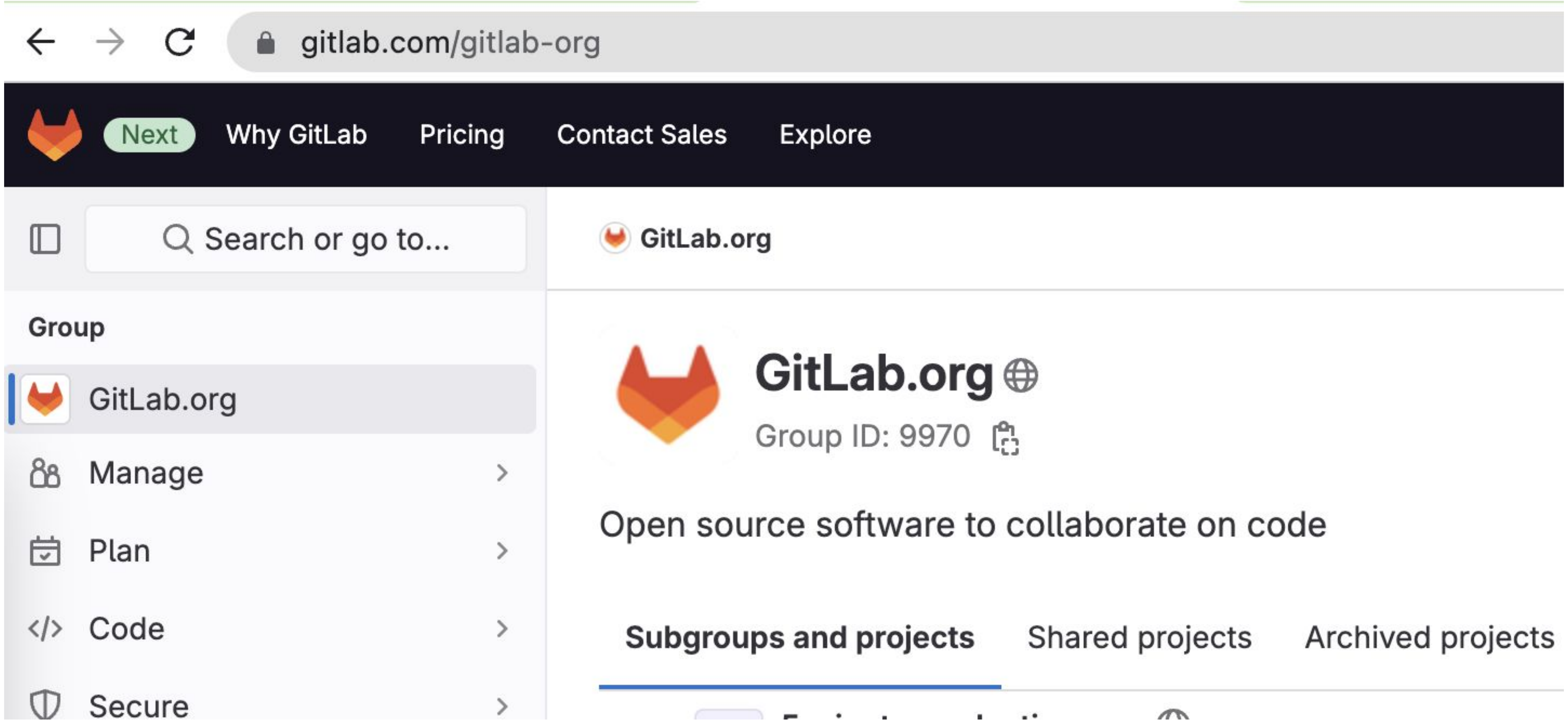
Being Humble

“Transparency is like an electric fence, sometimes you’ll get zapped by it”

Eric Johnson (Former CTO, GitLab)

Talk about mistakes

I deleted it, yep… all of it.



GitLab.org

Group ID: 9970

Open source software to collaborate on code

The Implication

You being seen as “a fraud” or an imposter* in your role

The company being ridiculed because of bad practices

Imposter Syndrome

It’s a thing.

- Talking openly about your mistakes, learnings, growth
- Everyone’s messy beginnings
- There’s only so many ways to build confidence
- Be willing to be a sponge!

(So much of this is fake it until you make it)

PMI + WMI

Poorly Managed Incompetence

V.S.

Well Managed Incompetence

Keep up & Pace of Change

Abstractions upon Abstractions

Speed our industry AND the industry we’re trying to protect is moving

Growth in technology and new layers on top of Kubernetes (which you’ll get to experience next from Mike!)

Hiring Pipelines

Challenge finding capable, interested, and resourceful engineers

Gaps in higher education

The need to hire and prepare junior engineers

Bad Actors

Increasing number and effectiveness well-funded bad actors

The cost of attack and risk against bad actors in many countries is decreasing (or not existent)

The Naysayers

Yes, the electric fence is real

- Bad actors monitoring public commits for security fixes or new vulnerabilities
- Being targeted by newly published exploits and/or 0days
- Sometimes your layered security model isn’t ***actually*** that layered
- Accidental leaks of confidential data

Lets Do This!

What now?

- Understand what data is ***actually*** confidential
- Write blog posts about challenges you’ve overcome and your successes!
- Come do a talk!
- Publicly document some issues and solutions (not just responding on stack-overflow to get points!)
- Ask people for help!

What’s Fun? (Maybe Scary?)

Canary Tokens & Honeypot Details

Questions?