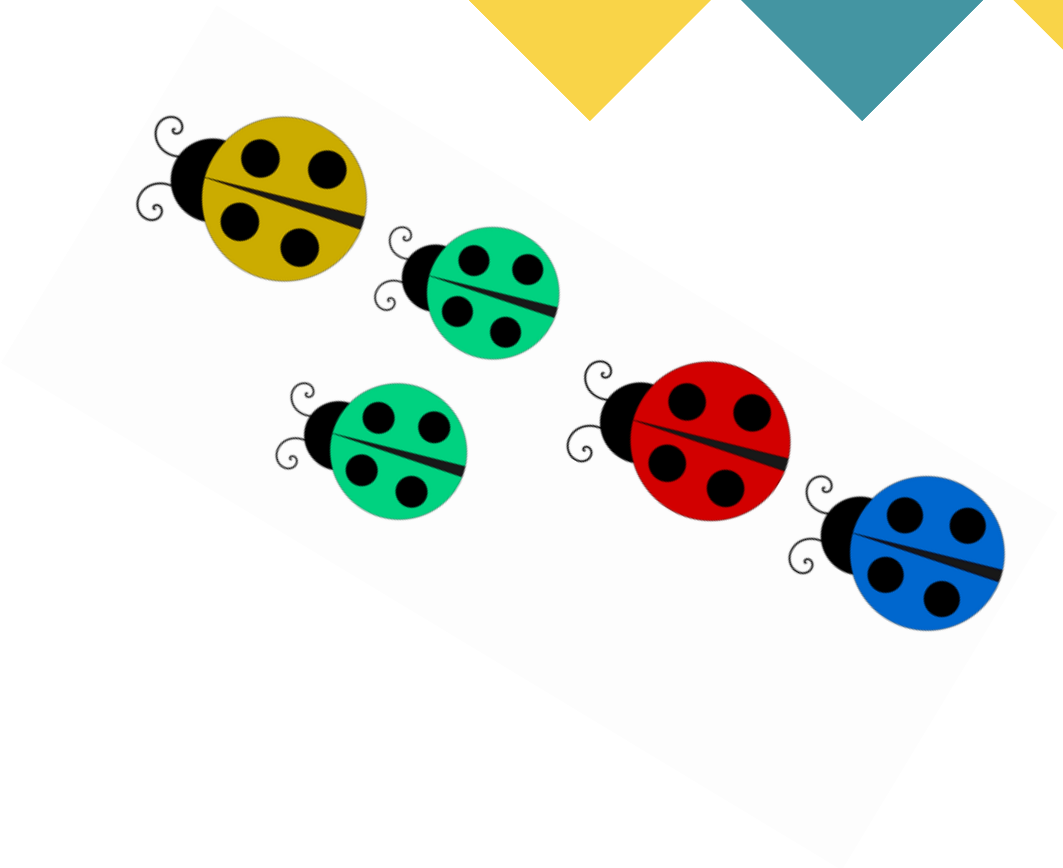
One Bug
Two Bug
Red Bug
Blue Bug

BSides Dublin 2025

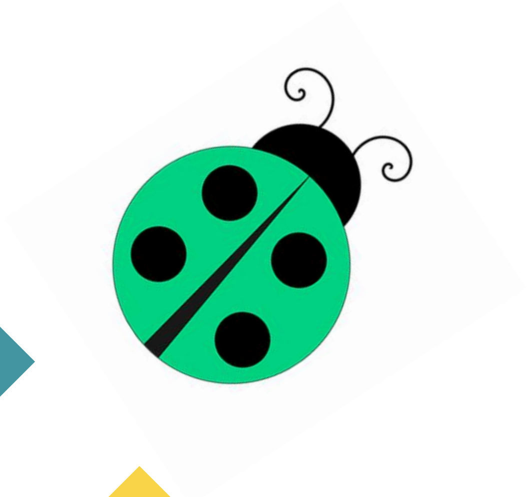
Agenda

- Introduction
- Problem Statement
- Solution – program & tooling
- Example
- Reusable framework

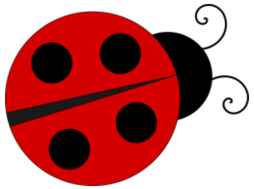


WhoamI? (x2)

- Lea Snyder
  - Principal Security Engineer
  - Security Community – speaker & organizer
- Patrick Fitzgerald
  - Principal Security Engineering Manager
- Why this talk



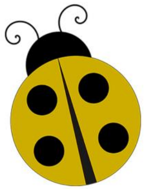
Problem Statement



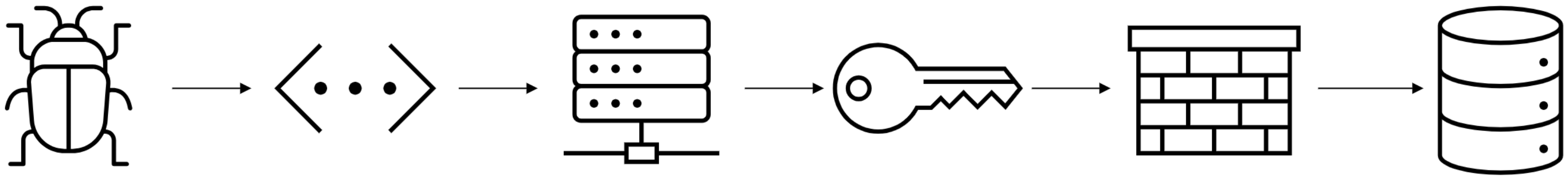
Have you ever found a bug (or two) and wondering where the others might be hiding?

Variant Analysis

- What are we trying to solve?
- Why is it hard? Are we thinking about this wrong?
- Exposure staring you in the face but you’re not seeing it (Example: security boundary violations)
- Gathering and sharing evidence (or thanks for fixing everything, now show me you are sure)



- “Defenders think in lists. Attackers think in graphs” – John Lambert, Microsoft CVP
- What is Breach Path Analysis?
- What isn’t it?
- How do we use it

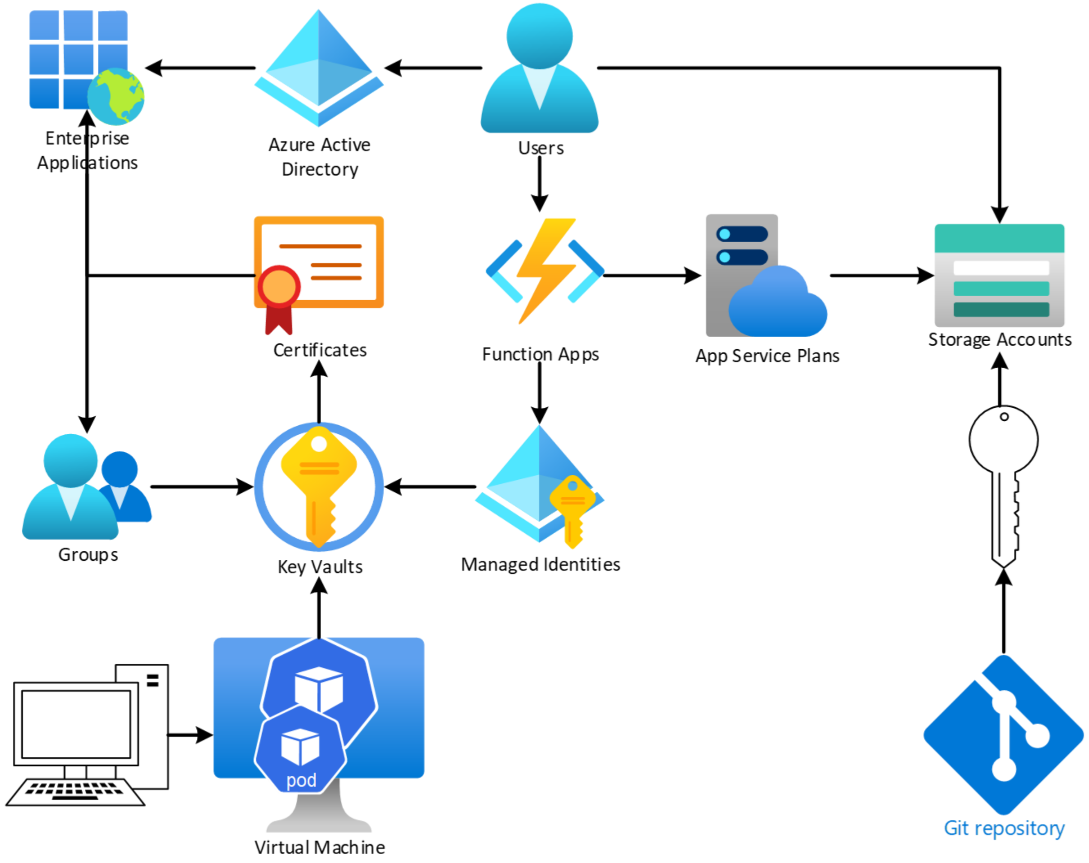


You need a map

https://github.com/JohnLaTwC/Shared/blob/master/Defenders%20think%20in%20lists.%20Attackers%20think%20in%20graphs.%20As%20long%20as%20this%20is%20true%2C%20attackers%20win.md

Let’s talk Graphs

- **Graphs** visualize collections of paths.
- This is the multiverse of possibilities, not actual threat actor activity.
- Security graphs help **blue teams** detect security risks that need to be mitigated.

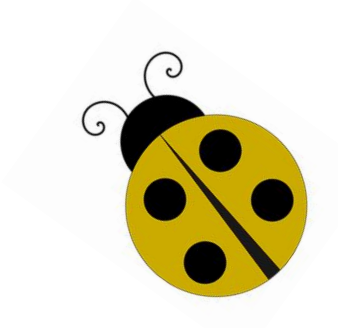


Wins

- Take anything and go beyond original scope to find MOAR, lots MOAR
- Quickly get actionable issues into the hands of developers
- Our goal: Prevent repeat breaches & limit the impact of novel breaches

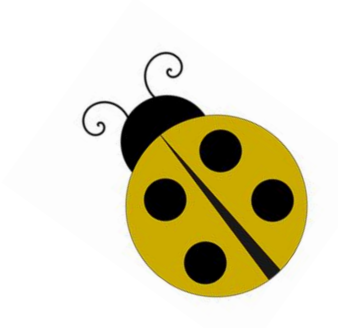
Framework

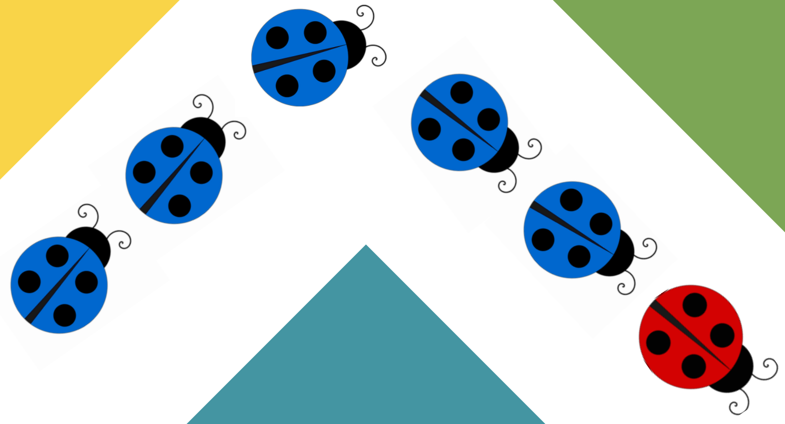
- Tips & Tricks for building your own Variant Analysis Program
  - Define what you want to solve first
  - Stand up related processes and governance in parallel
  - Celebrate the wins
  - Learn & iterate
- Avoid these pitfalls
  - Too easy to boil the ocean
  - Ignoring existing and gaps in processes



Framework (cont)

- Breach Path Analysis Tools: Buy or Build
  - Cloud Security Posture Management, Exposure Management, and Attack Path management tools exist!
  - You may have **unique business needs** or you have **regulatory requirements** or **security concerns** limiting third-party access.
  - Ontology (borrow ours): https://github.com/microsoft/security-graph-schemas





Question & Answers

Lea Snyder

https://www.linkedin.com/in/leasnyder/

Patrick Fitzgerald

https://www.linkedin.com/in/patrick-fitzgerald-msc-5299114/

Bug images:
Red: https://pixabay.com/vectors/ladybug-ladybird-nature-insect-bug-476344/
All others: https://pixabay.com/illustrations/ladybug-lady-bug-bug-insect-beetle-4994368/