


# Unlocking a Secure Future via Test-Driven Delivery

The Long Con

Oley V., November 2023

# why do I listen

- My journey began with MS-DOS, FreeBSD 3.1, and Debian Potato
- Before I knew that it was a journey my first pet was a knockoff of ZX80
- I have MSc in info sec from 💙💛 and a few info sec certs
- As a teenager I got inspired by  to try that “info sec” of theirs
- Now I work as an AVP Enterprise Security Architect

# why does he talk about it

An idea haunted me after a question during my 2018 B-sides talk

Can

- a security state of solutions, before deployment, be evaluated
- via test driven approach and will
- the community be interested in contributing

?

# are you reinventing the wheel

- I wasn't able to find anything that is actively developing (7 years ago...)

site github.com test driven architecture

Canada (en) Safe search: moderate Any time

https://github.com > topics > test-driven-development  
**test-driven-development · GitHub Topics · GitHub**  
Add this topic to your repo. To associate your repository with the test-driven-development topic, visit your repo's landing page and select "manage topics." GitHub is where people build software. More than 100 million people use GitHub to discover, fork, and contribute to over 330 million projects.

https://github.com > topics > test-driven-design  
**test-driven-design · GitHub Topics · GitHub**  
GitHub is where people build software. More than 94 million people use GitHub to discover, fork, and contribute to over 330 million projects. ... Add a description, image, and links to the test-driven-design topic page so that developers can more easily learn about it. Curate this topic. Add this topic to your...

https://microsoft.github.io > code-with-engineering-playbook > automated-testing > unit-testing > ...  
**Test-Driven Development Example - Code With Engineering Playbook**  
Test-Driven Development Example With this method, rather than writing all your tests up front, you write one test at a time and then switch to write the system code that would make that test pass. It's important to write the bare minimum of code necessary even if it is not actually "correct".

https://github.com > bayeslife > test-driven-architecture  
**GitHub - bayeslife/test-driven-architecture**  
Solution Overview A page containing a table with badges that call out to Invoke tests relevant to infrastructure specific to a solution. Representation The solution is to be represented as: an **architecture**: in terms of environments, connected zones, virtual and physical interface components,...

bayeslife / test-driven-architecture

Code Issues Pull requests Actions Projects Security Insights

test-driven-architecture (Public) Watch 1 Fork 0 Star 0

master 1 branch 0 tags Go to file Add file Code

bayeslife Updated 1765395 on Feb 28, 2017 11 commits

client	Updated	7 years ago
features	Updated	7 years ago
mock	Updated	7 years ago
src	Updated	7 years ago
.gitignore	Updated	7 years ago

About  
No description, website, or topics provided.  
Readme  
Activity  
0 stars  
1 watching  
0 forks  
Report repository

# what is the test driven delivery

- Tests that can be easily written and edited by humans
  - there are frameworks that can help to create tests (e.g. NIST SP 800-53, OWASP)
- Tests that can be easily interpreted and evaluated by machines
- Tests that can be executed anywhere(ish)
- Tests that are driving architecture and design aka requirements
- Results that can answer “Is it secure?”
- Results that can drive the risk based decision making

# what does it solve for

## Initial Compromise

- Unpatched vulnerabilities
- Security misconfigurations
- Weak, leaked, and stolen credentials
- Social engineering
- Insider threats

Where did you get those ideas?

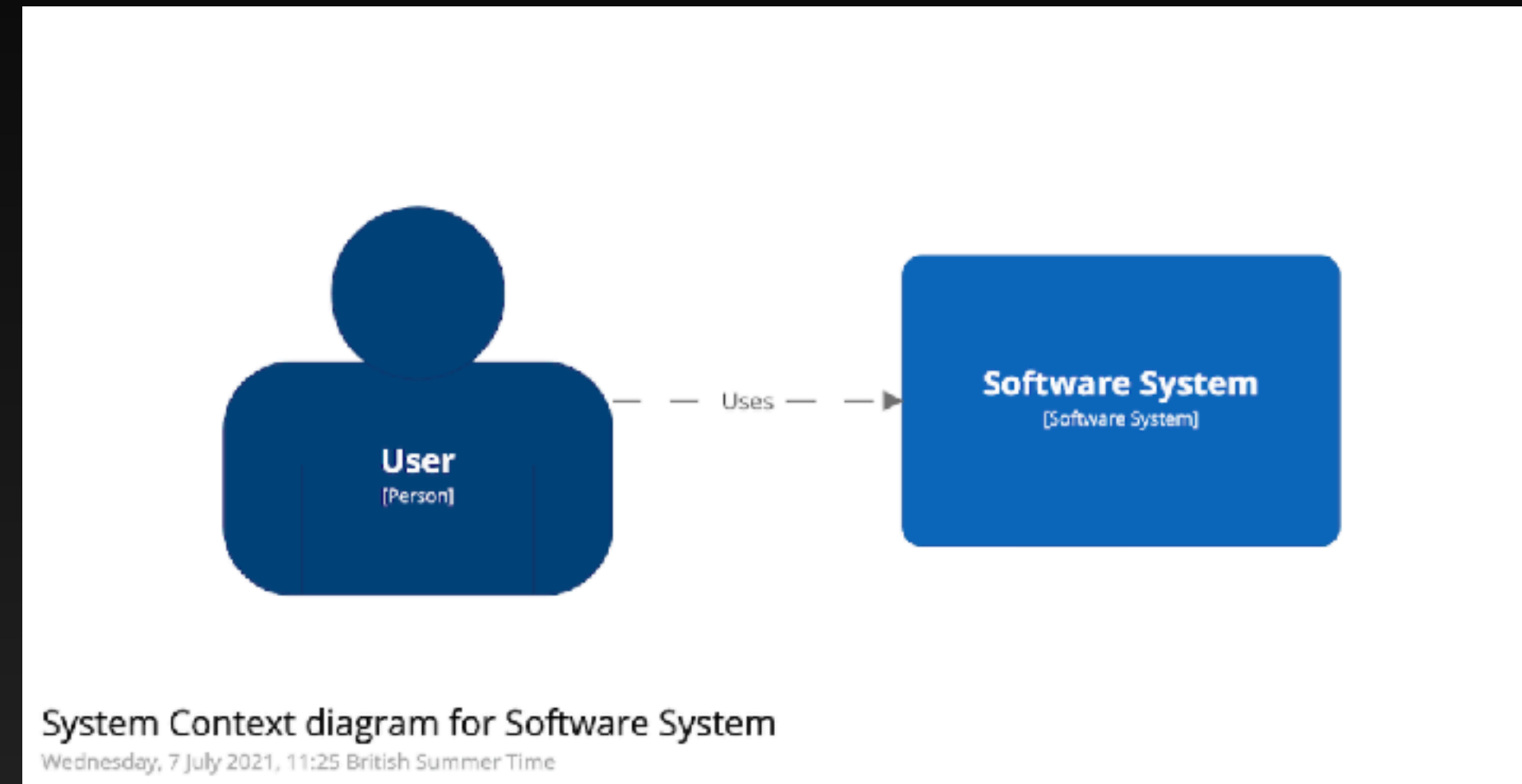
\*Mandiant: <https://www.mandiant.com/resources/insights/targeted-attack-lifecycle>

\*Kaspersky: <https://usa.kaspersky.com/blog/most-common-initial-attack-vectors/25557/>

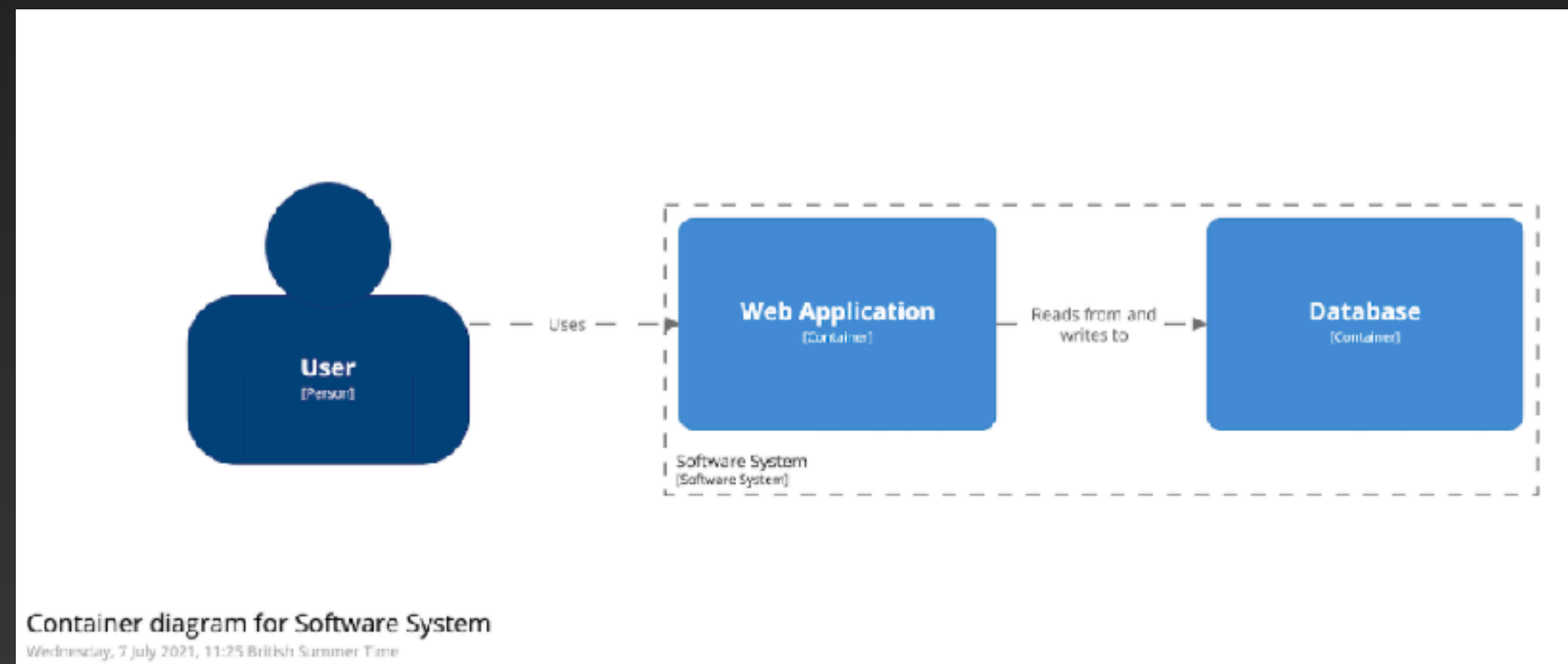
\*Cybersecurity Threats, Malware Trends, and Strategies, Tim Rains

# can we do everything as code

```
workspace {  
  model {  
    user = person "User"  
    softwareSystem = softwareSystem "Software System" {  
      webapp = container "Web Application" {  
        user -> this "Uses"  
      }  
      container "Database" {  
        webapp -> this "Reads from and writes to"  
      }  
    }  
  }  
}
```



```
views  
systemContext softwareSystem {  
  include *  
  autolayout lr  
}  
  
container softwareSystem {  
  include *  
  autolayout lr  
}
```



# how could we do it



- C4 and structurizr <https://structurizr.com/>
- Gherkin <https://cucumber.io/blog/bdd/gherkin-rules/>
- Open Policy Agent <https://www.openpolicyagent.org/>
- Your choice of CI/CD; it is Jenkins for this purpose
- Your choice of IaC, PaC; it is Terraform for this purpose



# are you in

- code and data driven decisions **via human friendly code**
- executed via Test Driven Delivery **orchestration with the existing tools**
- OSS community support **to exhaust the test cases beyond any framework**