



# Anatomy of

## A DevOps Tool Chain Attack

Presented by Alex Dow – Chief Innovations Officer  
BSides Ottawa 2022  
November 28<sup>th</sup>, 2022

**CONFIDENTIAL**  
[www.miraisecurity.com](http://www.miraisecurity.com)  
© Mirai Security Inc. All rights reserved.

# Speaking of Penetration Testing....

**WHATEVER  
YOU GROW  
WILL SAVE  
A BRO**



**MOVEMBER.COM**  
SIGN UP OR DONATE



**SAVE A BRO!**

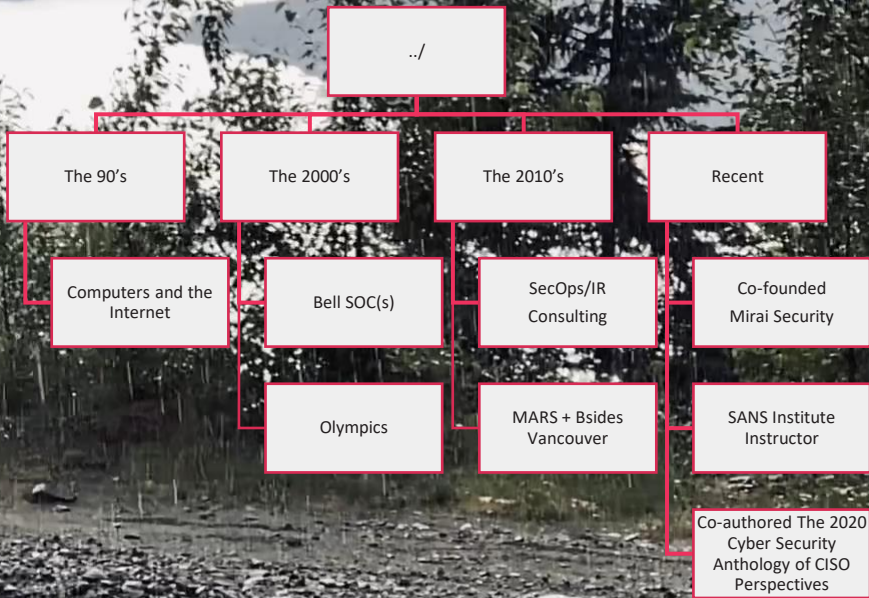


**CONFIDENTIAL**

[www.miraisecurity.com](http://www.miraisecurity.com)

© Mirai Security Inc. All rights reserved.

# \$ jqtree ~/.history





# The Tower of Babel



# The Race to Digital Transform

---

- The Race to Modernize
  - Changing Culture
  - Adopting Bleeding Edge Technologies
  - Moving Critical Business Assets
- 





# Innovation Bias: ɪnˈə-vāˈshən bīˈəs

- Culture
- Proliferation of DevOps
- Security Team's Invite is in the Mail
- Enterprise Risk Blind Spot

# Attackers are Digitally Transforming

4 minute read · April 19, 2021 4:51 PM PDT · Last Updated 2 years ago

## Codecov hackers breached hundreds of restricted customer sites - sources

By Joseph Menn and Raphael Satter

### Researcher hacks over 35 tech firms in novel supply chain attack



By [Ax Sharma](#)

### The SolarWinds cyberattack: The hack, the victims, and what we know

## Jenkins warns of security holes in these 25 plugins

Relax, most of the vulnerabilities so far have, er, no fix

[Thomas Claburn](#)

Thu 30 Jun 2022

## 80% of Software Codebases Contain at Least One Vulnerability

Open source code continues its steady takeover of codebases, and organizations have made slight gains in eliminating out-of-date and vulnerable components.



**Robert Lemos**

Contributing Writer, Dark Reading

April 12, 2022





# The Anatomy of a DevOps Tool Chain Attack

---



# The Client

## The Who

- Breaking Rocks Mining Co.
- Growth through Acquisition
- Vertically Integrated

## The Why

- Digital Transformation Initiative
- Things are going live, has anyone talked to security?

# The Mission

## Scenario

- Dev laptop was compromised by phishing attack
- Devs cred are read-only
- Pentester has little knowledge of the environment

## Objectives

- ✓ Privilege Escalation
- ✓ Lateral Movement
- ✓ Data Access/Exfil
- ✓ OSS Supply Chain Attack
- ✓ Avoid Detection



# OSINT and External Reconnaissance



## Social Engineering Prep/Tech Stack Identification

- LinkedIn
- Job Postings
- Stackoverflow Posts



## Low Hanging Fruit

- Exposed DB/S3/Blob
- Exposed web or API interfaces
- Exposed DevOps Tools



## Digital Exhaust

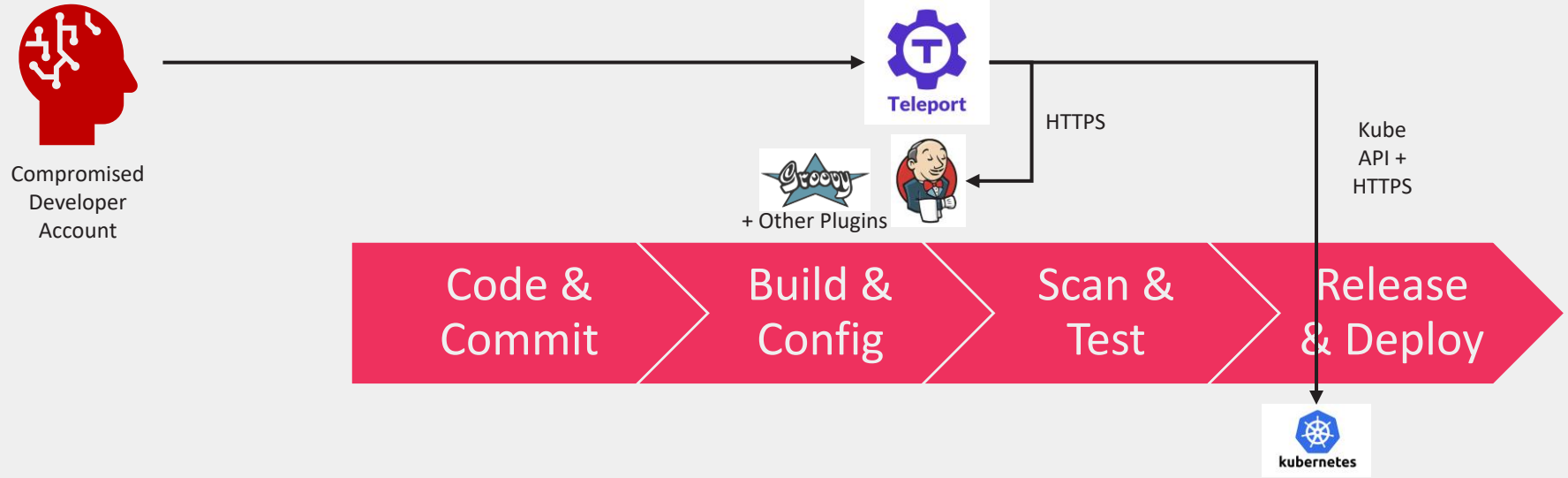
- Accidental Commits:  
SSH keys, certs, .env  
files, creds, scrips, API  
keys, build server  
configs



## Get *SMRT*!

- Youtube
- Latest cheat sheets
- Disclosure sites

# Active Reconnaissance

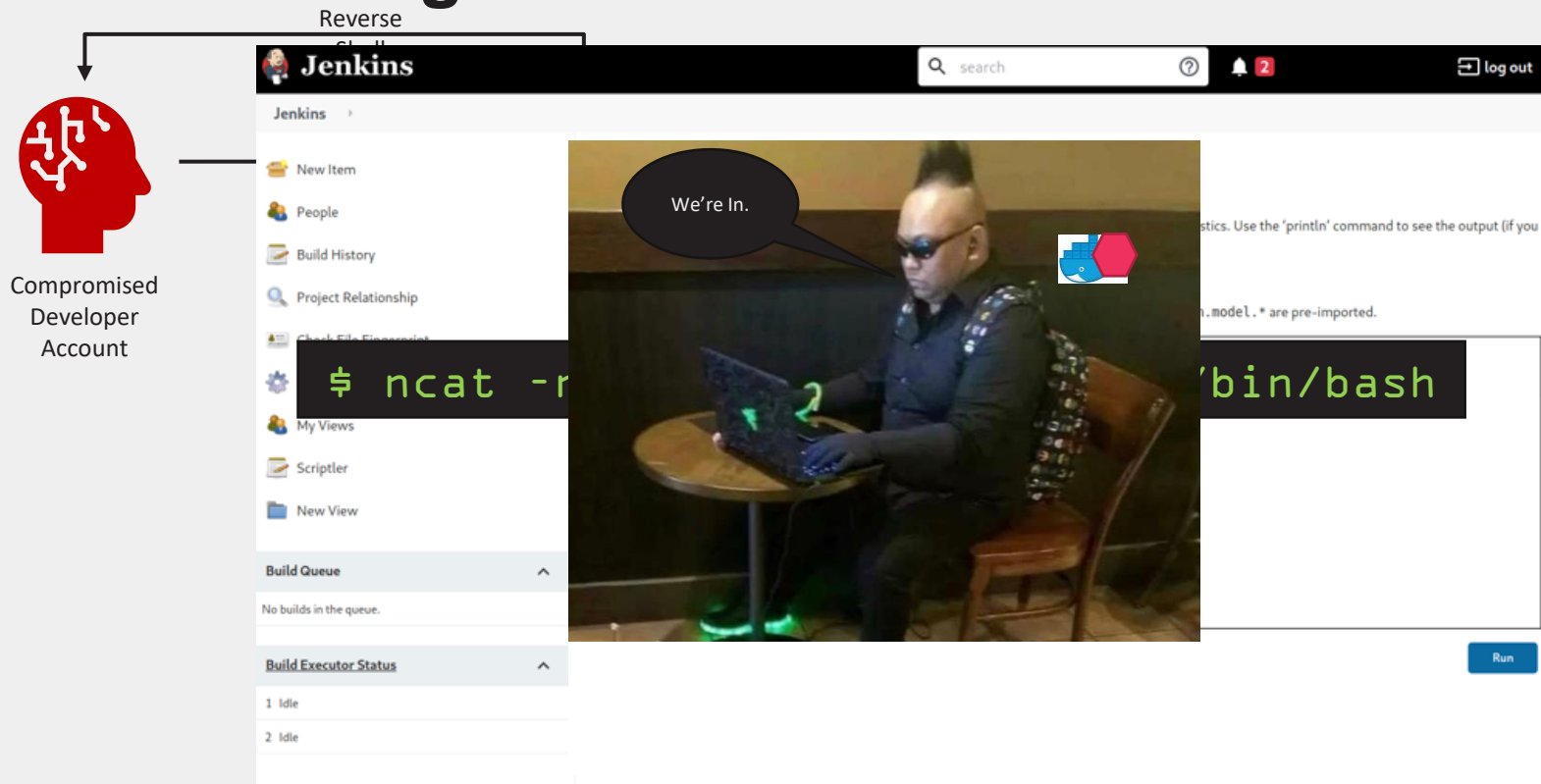




# Establishing an Initial Foothold

Reverse

Compromised Developer Account



Jenkins

New Item

People

Build History

Project Relationship

Check File Dependencies

My Views

Scriptler

New View

Build Queue

No builds in the queue.

Build Executor Status

1 Idle

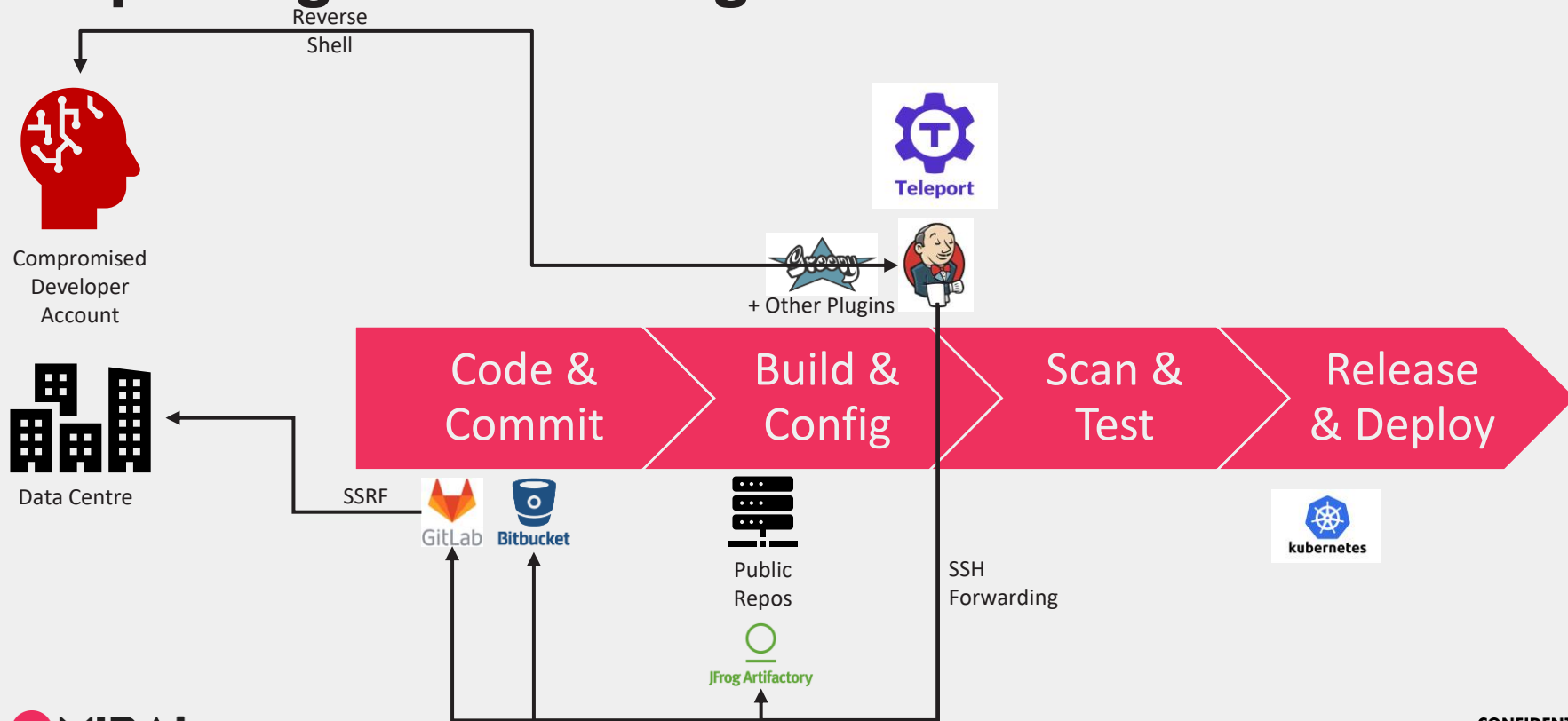
2 Idle

We're In.

bin/bash

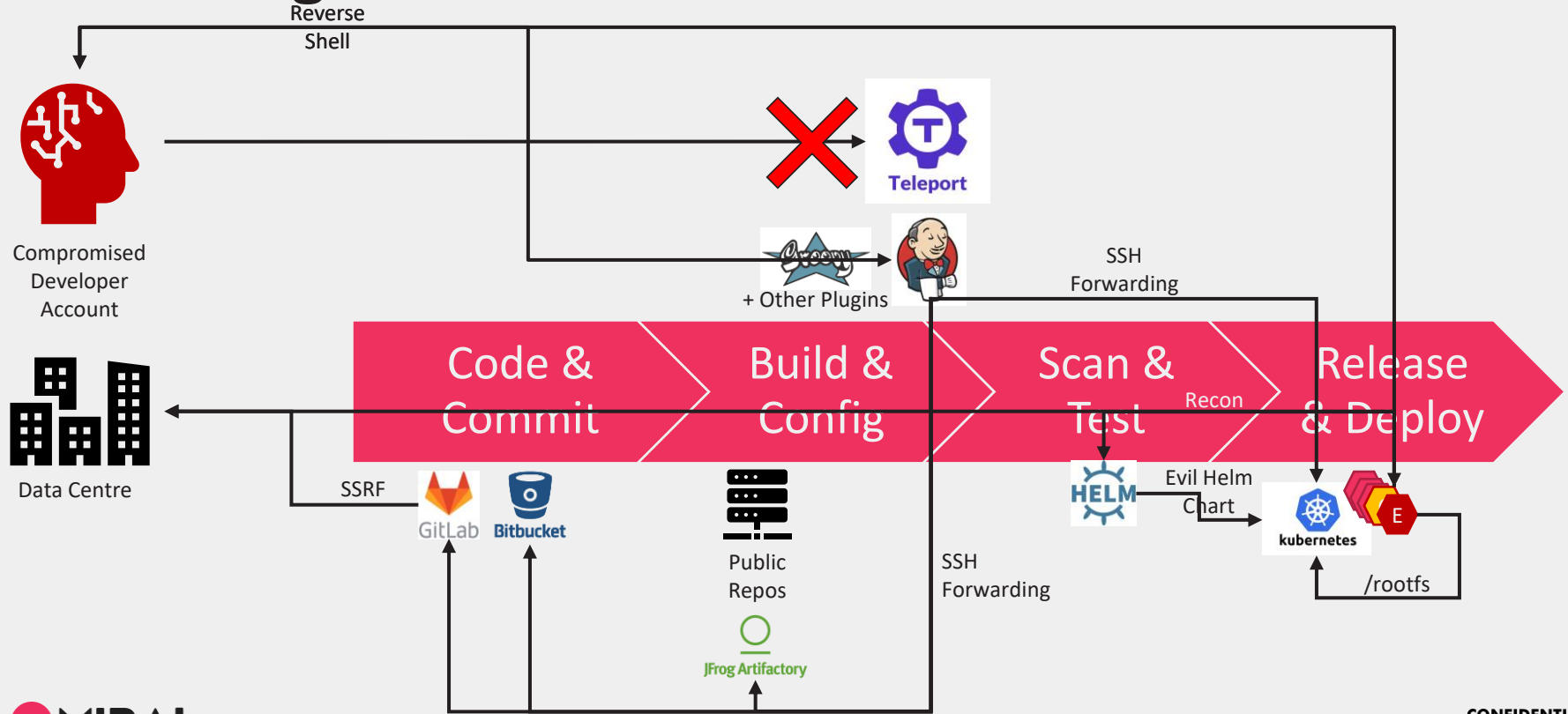
Run

# Exploring and Pivoting

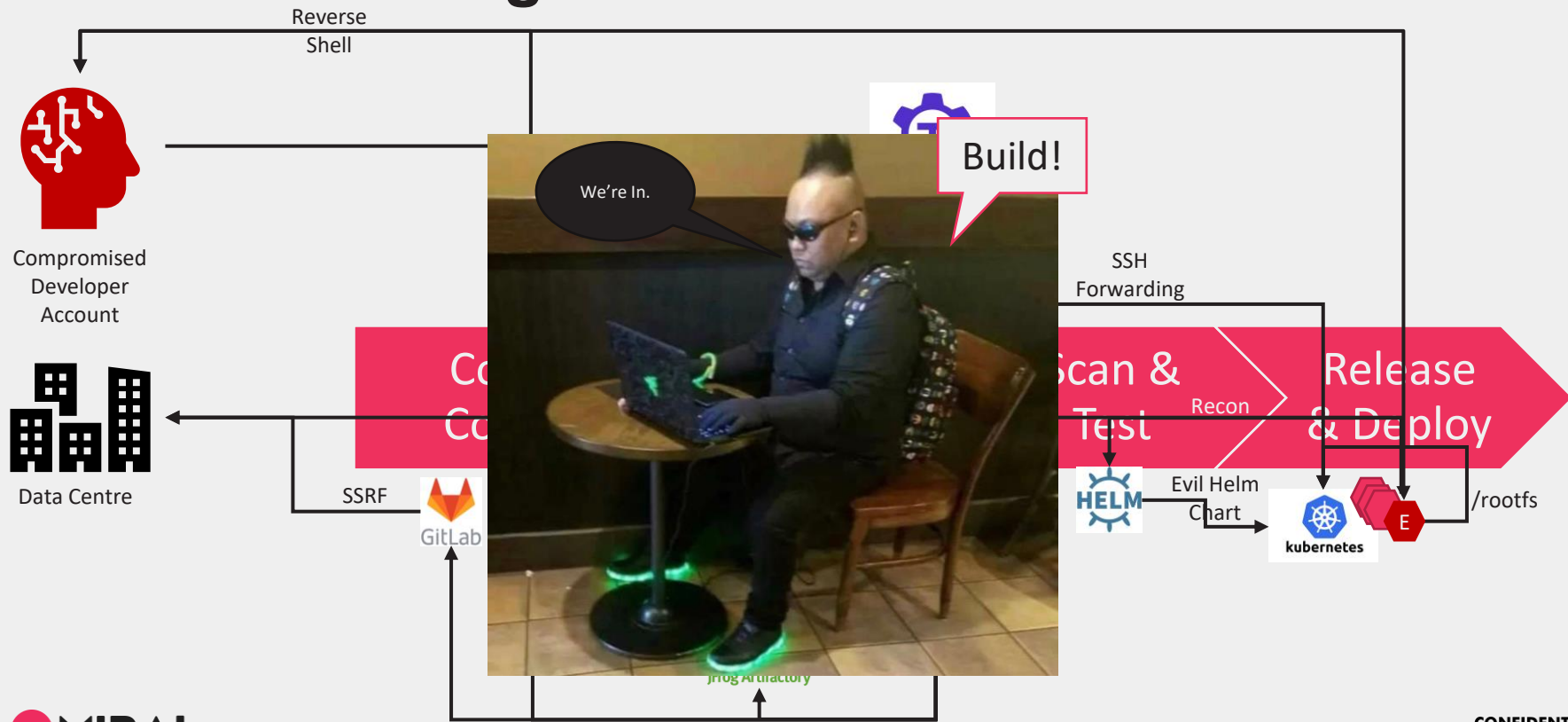




# Attacking Kubernetes



# Let's Take Things to 11



# Let's Debrief

Improve Security Culture

Shim Security into DevOps

Design with Security/Sustainability

Credential Management





# Put Engineering Back into Software Engineering

## Software Assurance Maturity Model

| Governance                                     | Design                                       | Implementation                          | Verification                                       | Operations                                |
|--|--|---|--|---|
| <b>Strategy &amp; Metrics</b>                  | <b>Threat Assessment</b>                     | <b>Secure Build</b>                     | <b>Architecture Assessment</b>                     | <b>Incident Management</b>                |
| Create & promote<br>Measure & improve          | Application risk profile<br>Threat modeling  | Build process<br>Software dependencies  | Architecture validation<br>Architecture compliance | Incident detection<br>Incident response   |
| <b>Policy &amp; Compliance</b>                 | <b>Security Requirements</b>                 | <b>Secure Deployment</b>                | <b>Requirements-driven Testing</b>                 | <b>Environment Management</b>             |
| Policy & standards<br>Compliance management    | Software requirements<br>Supplier security   | Deployment process<br>Secret management | Control verification<br>Misuse/abuse testing       | Configuration hardening<br>Patch & update |
| <b>Education &amp; Guidance</b>                | <b>Secure Architecture</b>                   | <b>Defect Management</b>                | <b>Security Testing</b>                            | <b>Operational Management</b>             |
| Training & awareness<br>Organization & culture | Architecture design<br>Technology management | Defect tracking<br>Metrics & feedback   | Scalable baseline<br>Deep understanding            | Data protection<br>Legacy management      |

## Application Security Verification Standard

|  | Level 1 | Level 2 | Level 3 |
|--|---------|---------|---------|
| Architecture, Design and Threat Modeling |         | 41      | 42      |
| Authentication                           | 27      | 53      | 57      |
| Session Management                       | 12      | 18      | 20      |
| Access Control                           | 9       | 10      | 10      |
| Validation, Sanitization and Encoding    | 27      | 30      | 30      |
| Stored Cryptography                      | 1       | 13      | 16      |
| Error Handling and Logging               | 3       | 13      | 13      |
| Data Protection                          | 1       | 15      | 17      |
| Communications                           | 3       | 7       | 8       |
| Malicious Code                           | 3       | 5       | 10      |
| Business Logic                           | 5       | 8       | 8       |
| File and Resources                       | 11      | 15      | 15      |
| API and Web Services                     | 7       | 15      | 15      |
| Configuration                            | 16      | 24      | 25      |

Mo Money...



Thank You

Mirai Security Inc.  
Alex.Dow@miraisecurity.com  
1.877.745.2729  
www.miraisecurity.com

Mo Bros!

