CYBERSEC 2021
臺灣資安大會

ORGANIZED BY iThome

TRUST:redefined

信 任 重 構

MAY 4-6 臺北南港展覽二館

IaC Security

Spearker: ChangYu Wu

Date: 5/6 10:45 - 11:15

Room: 7F 701G

樂屋網 www.rakuya.com.tw

TRUST: redefined

Rakuya International Info. Co. Ltd
MIS Manager

Goal:
Break down departmental barriers to shorten development cycles.

Increase deployment frequency, and enhance the success rate and reliability of each release.

Why security is so difficult ?

- Traditionally, security is as an afterthought.
- Too many secure issues come from unhealthy environment architecture.
- Fix critical bugs or secure issues would delay the release date.
- Development unit look upon security as obstacle and burden.
- Security unit think development unit is irresponsible and release vulnerable code.

Good solution

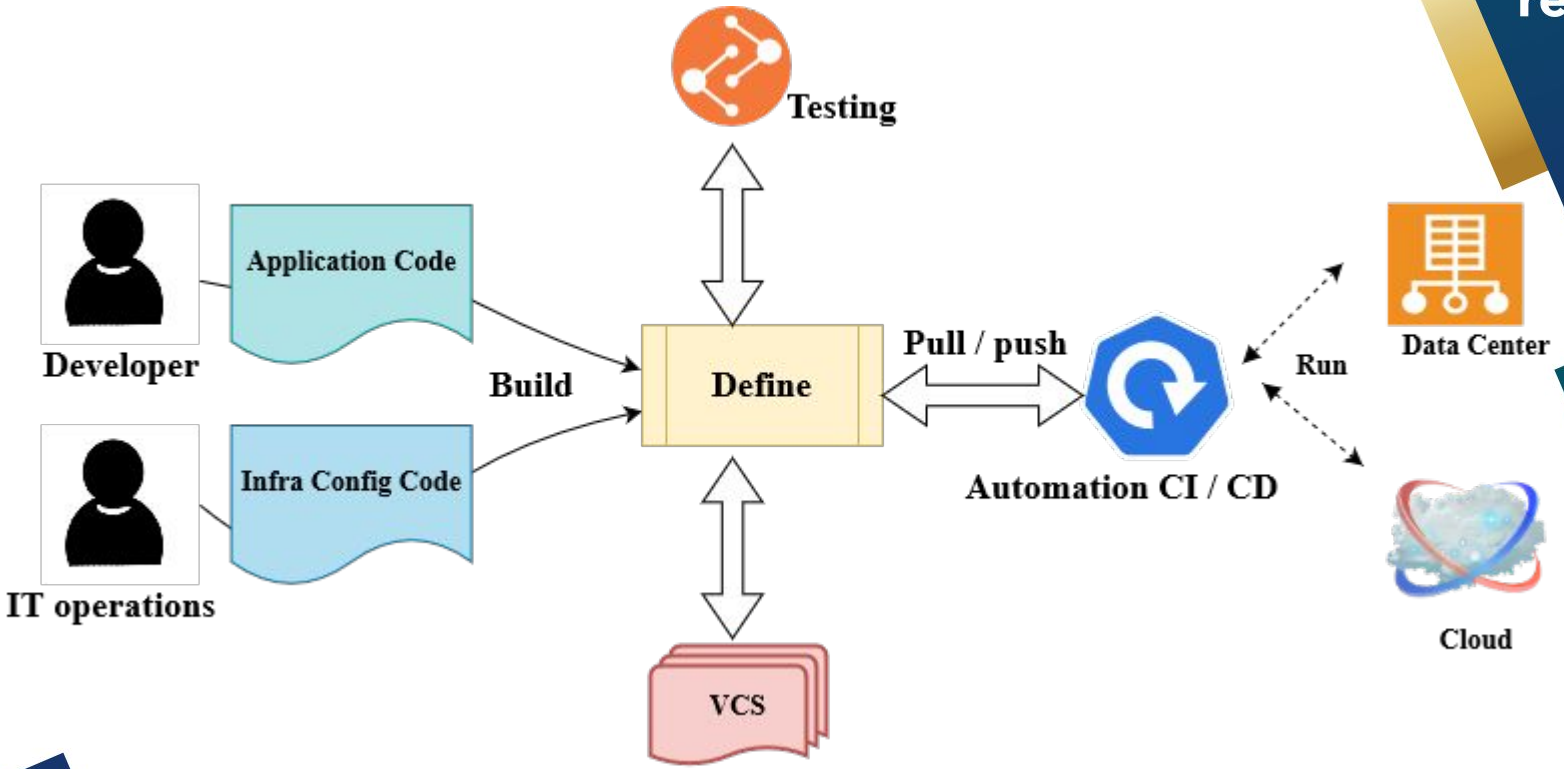
IaC Security

Infrastructure as Code (IaC)

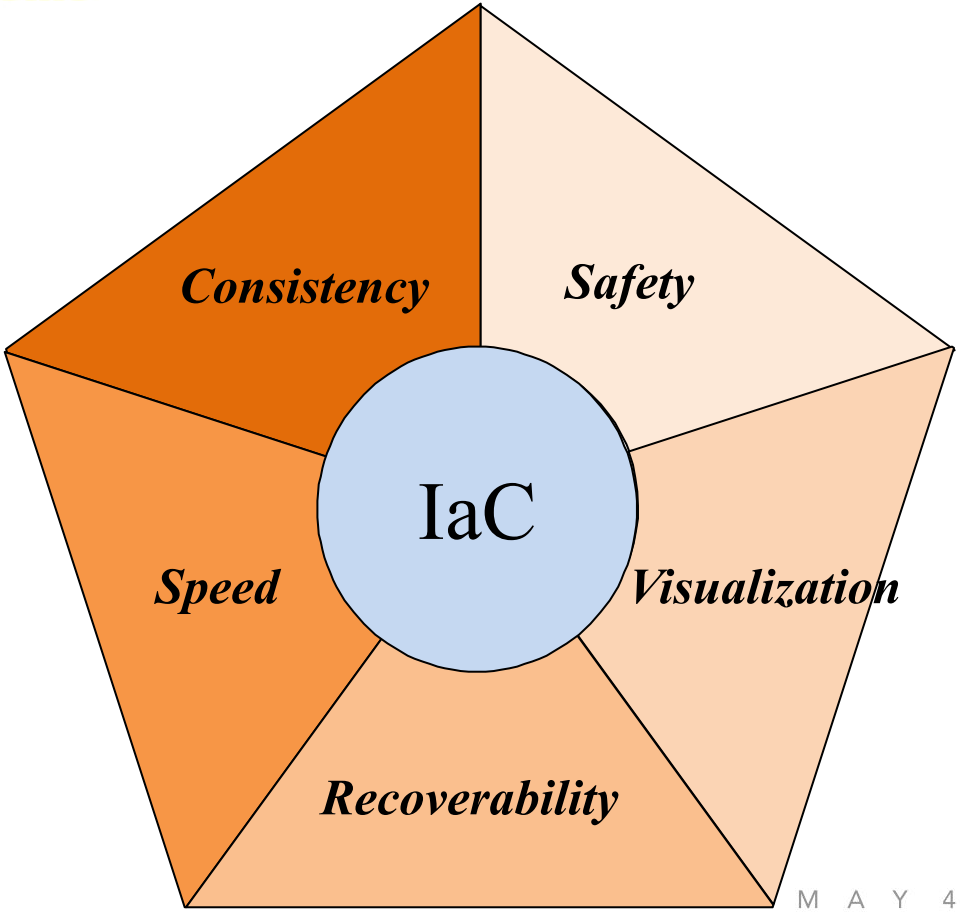
Infrastructure as Code is the process of provisioning and configuring an environment (Data center/Cloud) through code instead of manually setting up the required devices and systems.

- Definition files (Specification / Configuration)
- Everything codified
- Version control systems (VCS)
- Continuous Integration / Continuous Delivery (CI/CD)

Workflow (IaC)



Benefit (IaC)



Automation fear spiral (IaC)

source: infrastructure-as-code.com

Security as Code

Security Starts and Ends with Developers

Strengthen security (ex. System configuration settings)

- Security risks
- Implementing Security as Code
  - Security testing
  - Vulnerability testing
  - User and data access policies
- Continuous Workflow

Security risks

Templates	Credential management	The Communication Channels	User Access Management / privilege-related
Images / ISO Packaging Repository Code language Framework Third-party software Cloud instance images	Password Secure Shell Keys	Master-node architecture	Principle of least privileg(PoLP)

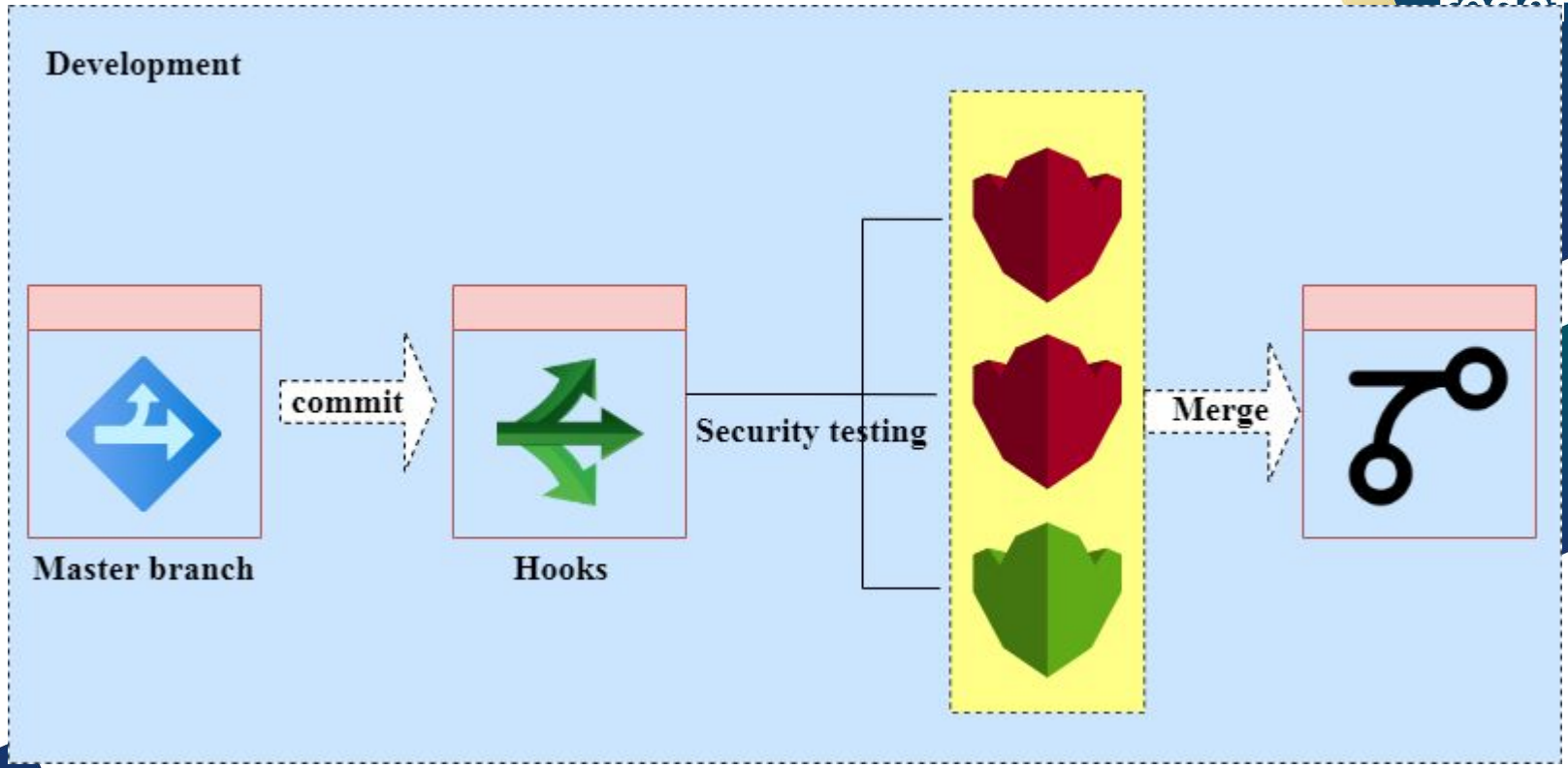
Security risks (other)

Unlabeled resources	Configuration drift
Untagged assets	Snowflake servers
Data Transmissions	**Audit Logs**
Cyber-attacks are multiplying	Identifying potential threats Proactive Continuous Monitoring

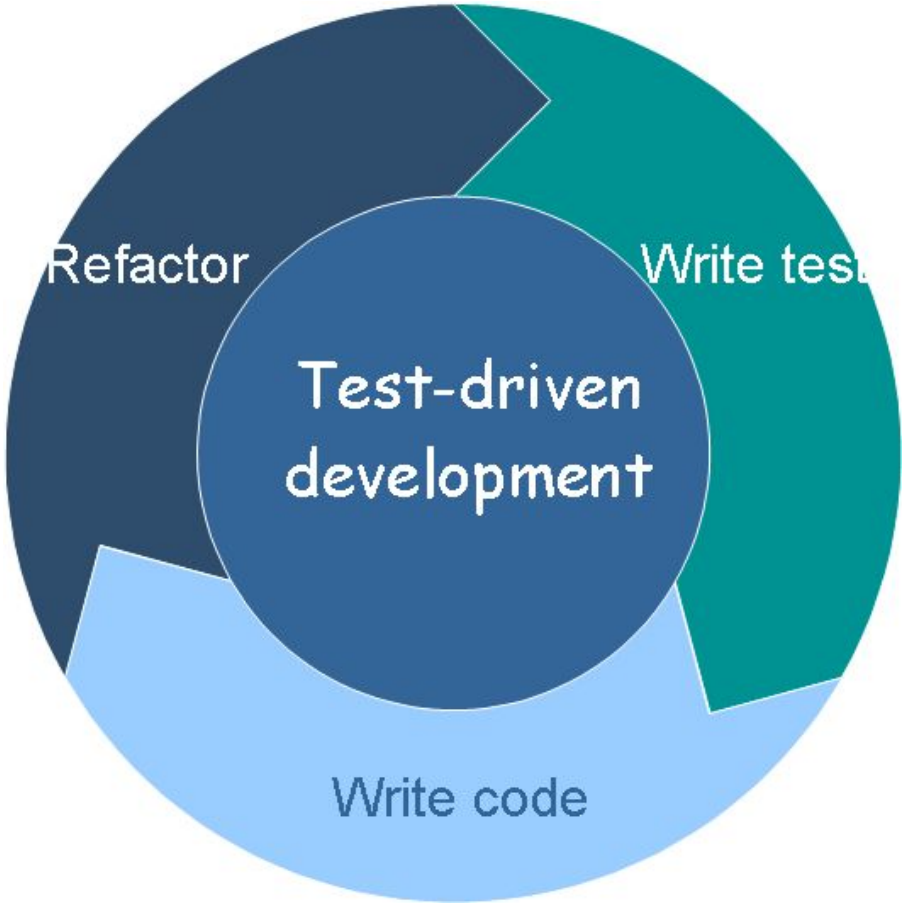
Note:

Unauthorised users、Data leakage、Unauthorised access to critical resources、Increased attack surface.

Security testing



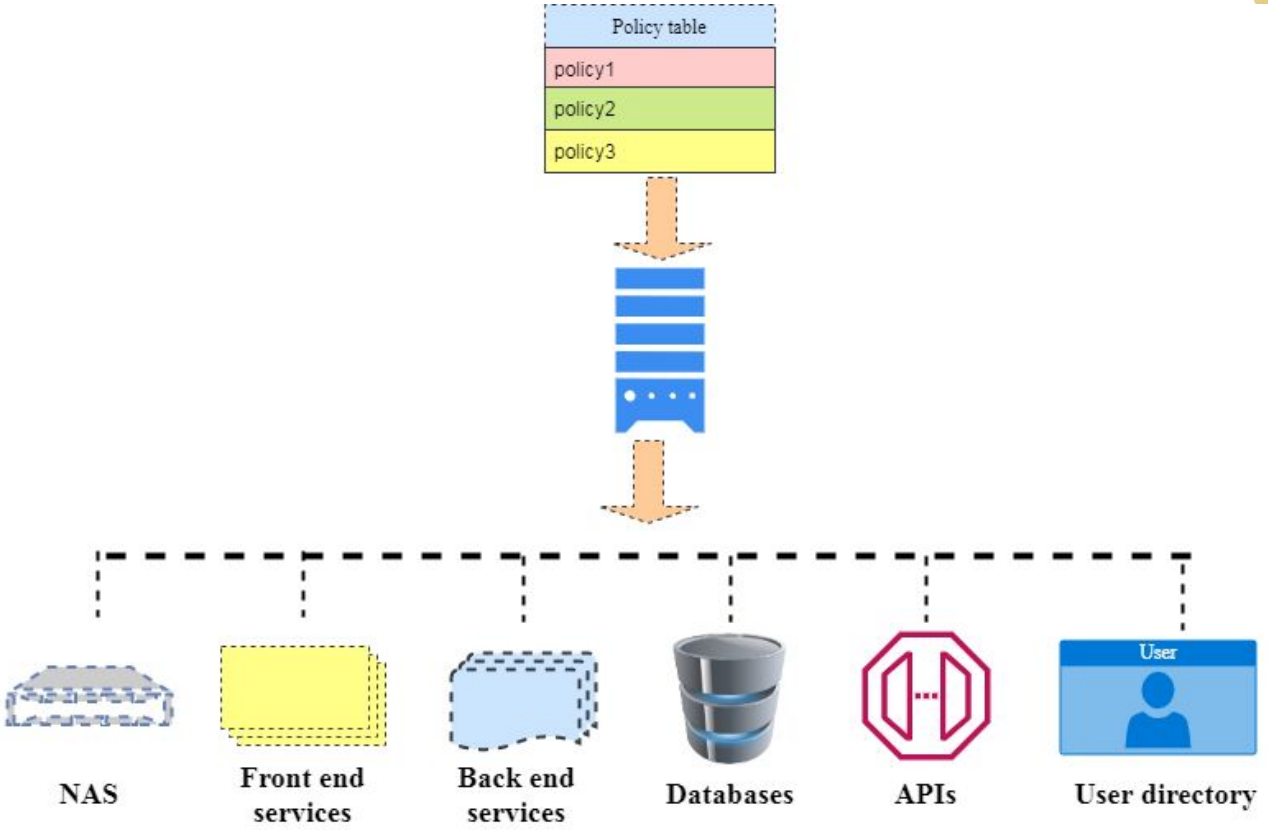
Test-Driven Development (TDD)



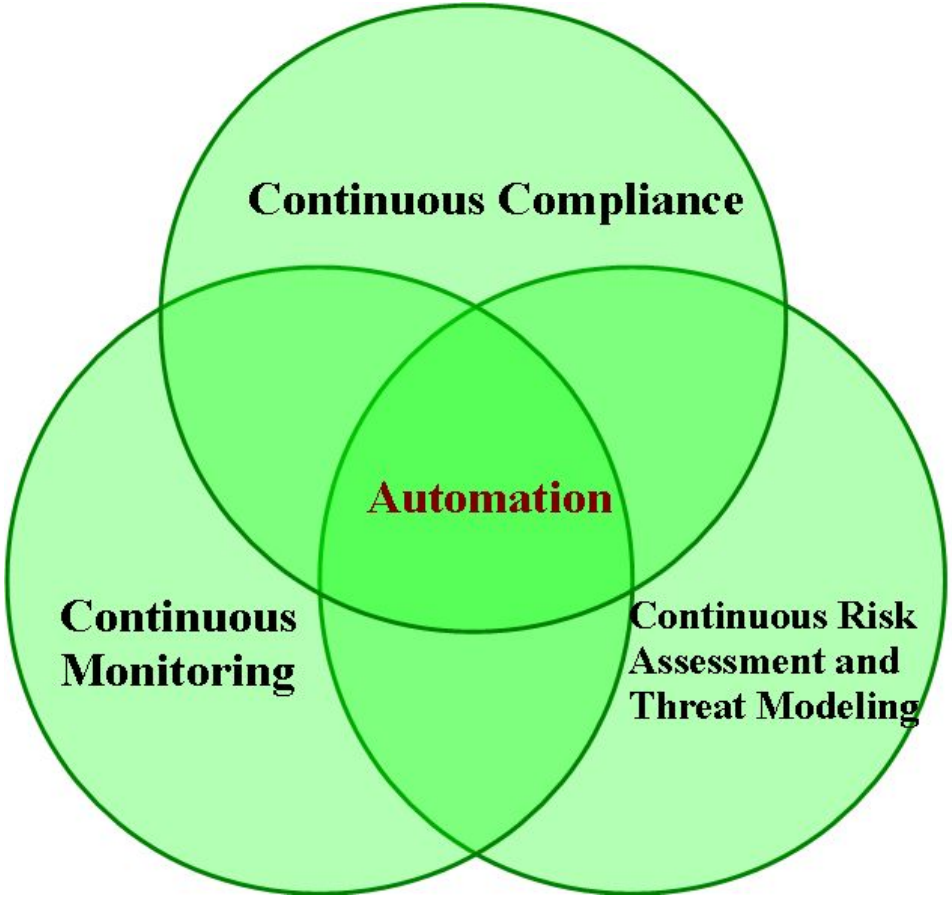
Vulnerability testing

Source code	Vulnerability scanning、Static code analysis
Infra code	Incorrect configuration 、Vulnerability package
App serivce	SQL injection、XSS、Wrong api call method
Network	Firewall configuration 、ACL

User and data access policy



Continuous Workflow



Popular IaC Tools

Conclusion

- IaC security is a concept about how to coding for secure strategy and inspect in development process.
- Enhance environmental security, transparency and consistency. Early deployment
- Find a best way to maintain security with agility.

TRUST:
redefined

Thank you

changyuwu@rakuya.com.tw