

# DEVSECOPS

The Good, Bad, and Ugly

DevOps TW Meetup #28

# WHOIS

## I am Anderson Lin

MaiCoin Cyber Security Engineer  
AWS Certified All-5 + Sec specialty

 4ndersonLin

# AGENDA

- Security and DevOps
- The Good
- The Bad
- The Ugly

SECURITY AND DEVOPS



**Security**



**DevOps**

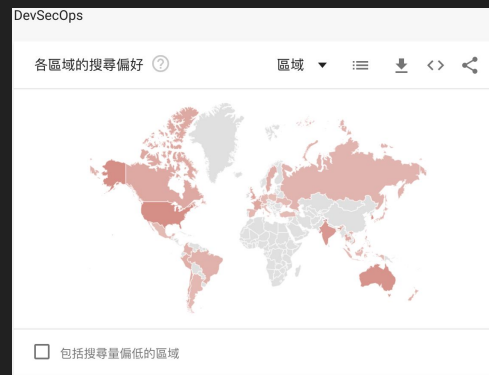
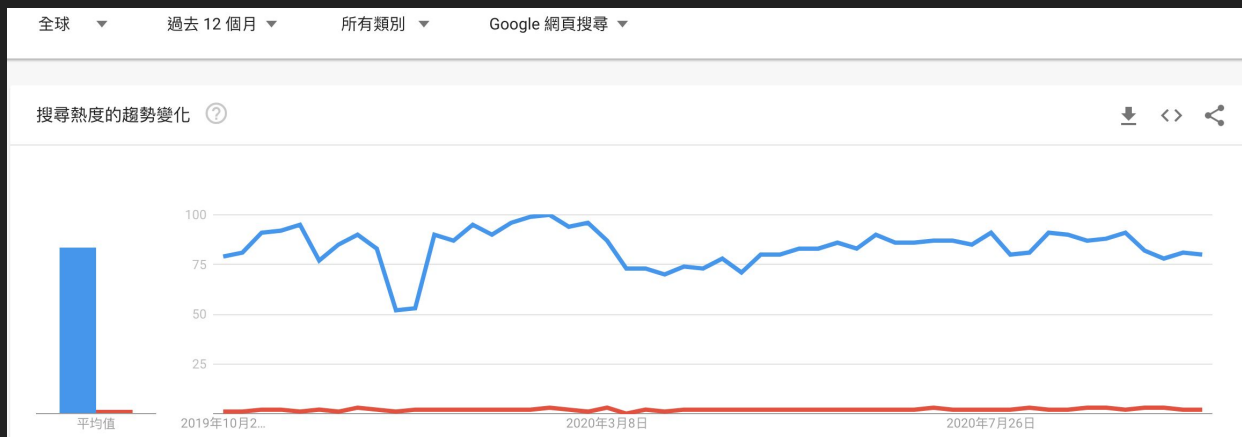
# REALITY

Maybe we still need some **security**:

- Business about **money** and sensitive **data**
- Company **policy**
- Local **law** and regulation issue



# SOME INTERESTING DATA: THE TREND

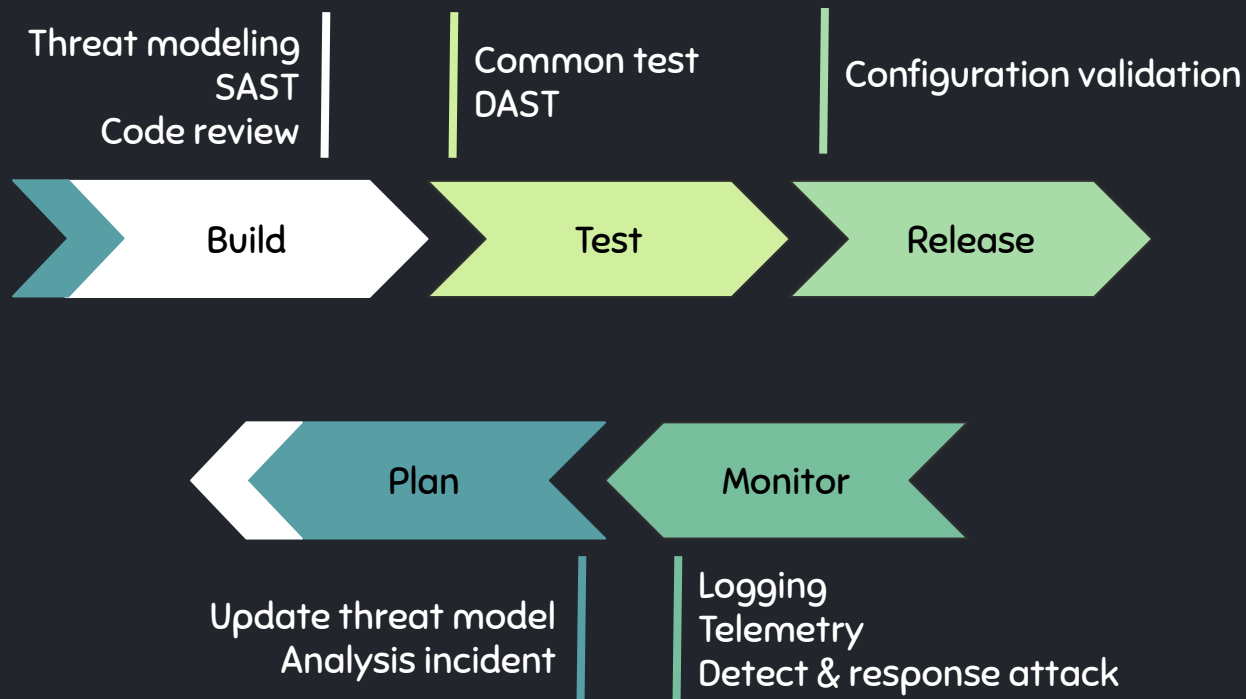




# DEVSECOPS

## THE OVERVIEW

# LIFE CYCLE OF DEVSECOPS



# DEVOPS PERIODIC TABLE

<div><div><div><div></div><div>AiOps/Analytics</div></div><div><div></div><div>Collaboration</div></div><div><div></div><div>Continuous Integration</div></div><div><div></div><div>Enterprise Agile Planning</div></div><div><div></div><div>Security</div></div><div><div></div><div>Testing</div></div></div><div><div><div></div><div>Artifact Repository</div></div><div><div></div><div>Configuration</div></div><div><div></div><div>Database Automation</div></div><div><div></div><div>ITSM/Issue Tracking</div></div><div><div></div><div>ServerLess/Pass</div></div><div><div></div><div>Value Stream Management</div></div></div><div><div><div></div><div>Cloud</div></div><div><div></div><div>Containers</div></div><div><div></div><div>Deployment</div></div><div><div></div><div>Release Orchestration</div></div><div><div></div><div>Source Control Management</div></div></div></div>																			
<div><div><div><div><div>1</div><div>En</div><div>Aja</div><div>Atlassian Jira Align</div></div><div><div>3</div><div>En</div><div>Daa</div><div>Digital.ai Agility</div></div><div><div>11</div><div>En</div><div>Pv</div><div>Planview</div></div></div><div><div><div>4</div><div>En</div><div>Tp</div><div>Targetprocess</div></div><div><div>12</div><div>En</div><div>Br</div><div>Broadcom Rally</div></div></div></div></div>										<div><div><div><div><div>2</div><div>Os</div><div>Gi</div><div>Git</div></div><div><div>10</div><div>Os</div><div>Gh</div><div>GitHub</div></div><div><div>18</div><div>Os</div><div>Gls</div><div>GitLab SCM</div></div></div><div><div><div>6</div><div>Os</div><div>Ow</div><div>OWASP ZAP</div></div><div><div>14</div><div>En</div><div>Sni</div><div>Sonatype Nexus IQ</div></div><div><div>32</div><div>En</div><div>Vc</div><div>Veracode</div></div></div><div><div><div>7</div><div>En</div><div>Dap</div><div>Digital.ai App Protection</div></div><div><div>15</div><div>En</div><div>Aq</div><div>Aqua Security</div></div><div><div>33</div><div>Os</div><div>Hv</div><div>HashiCorp Vault</div></div></div><div><div><div>8</div><div>En</div><div>Dar</div><div>Digital.ai Release</div></div><div><div>16</div><div>En</div><div>Cfr</div><div>CloudBees Flow</div></div><div><div>34</div><div>En</div><div>Ur</div><div>UrbanCode Release</div></div></div><div><div><div>9</div><div>En</div><div>Acp</div><div>AWS CodePipeline</div></div><div><div>17</div><div>En</div><div>Brl</div><div>BMC RLM</div></div><div><div>35</div><div>En</div><div>Al</div><div>AWS Lambda</div></div></div><div><div><div>5</div><div>En</div><div>Azp</div><div>Azure DevOps Pipelines</div></div><div><div>13</div><div>En</div><div>Dad</div><div>Digital.ai Deploy</div></div><div><div>31</div><div>En</div><div>Ud</div><div>UrbanCode Deploy</div></div></div><div><div><div>6</div><div>Os</div><div>Ow</div><div>OWASP ZAP</div></div><div><div>14</div><div>En</div><div>Sni</div><div>Sonatype Nexus IQ</div></div><div><div>32</div><div>En</div><div>Vc</div><div>Veracode</div></div></div><div><div><div>7</div><div>En</div><div>Dap</div><div>Digital.ai App Protection</div></div><div><div>15</div><div>En</div><div>Aq</div><div>Aqua Security</div></div><div><div>33</div><div>Os</div><div>Hv</div><div>HashiCorp Vault</div></div></div><div><div><div>8</div><div>En</div><div>Dar</div><div>Digital.ai Release</div></div><div><div>16</div><div>En</div><div>Cfr</div><div>CloudBees Flow</div></div><div><div>34</div><div>En</div><div>Ur</div><div>UrbanCode Release</div></div></div><div><div><div>9</div><div>En</div><div>Acp</div><div>AWS CodePipeline</div></div><div><div>17</div><div>En</div><div>Brl</div><div>BMC RLM</div></div><div><div>35</div><div>En</div><div>Al</div><div>AWS Lambda</div></div></div><div><div><div>10</div><div>Os</div><div>Gh</div><div>GitHub</div></div><div><div>18</div><div>Os</div><div>Gls</div><div>GitLab SCM</div></div><div><div>36</div><div>Fm</div><div>Abb</div><div>Atlassian Bitbucket</div></div></div><div><div><div>5</div><div>En</div><div>Azp</div><div>Azure DevOps Pipelines</div></div><div><div>13</div><div>En</div><div>Dad</div><div>Digital.ai Deploy</div></div><div><div>31</div><div>En</div><div>Ud</div><div>UrbanCode Deploy</div></div></div><div><div><div>6</div><div>Os</div><div>Ow</div><div>OWASP ZAP</div></div><div><div>14</div><div>En</div><div>Sni</div><div>Sonatype Nexus IQ</div></div><div><div>32</div><div>En</div><div>Vc</div><div>Veracode</div></div></div><div><div><div>7</div><div>En</div><div>Dap</div><div>Digital.ai App Protection</div></div><div><div>15</div><div>En</div><div>Aq</div><div>Aqua Security</div></div><div><div>33</div><div>Os</div><div>Hv</div><div>HashiCorp Vault</div></div></div><div><div><div>8</div><div>En</div><div>Dar</div><div>Digital.ai Release</div></div><div><div>16</div><div>En</div><div>Cfr</div><div>CloudBees Flow</div></div><div><div>34</div><div>En</div><div>Ur</div><div>UrbanCode Release</div></div></div><div><div><div>9</div><div>En</div><div>Acp</div><div>AWS CodePipeline</div></div><div><div>17</div><div>En</div><div>Brl</div><div>BMC RLM</div></div><div><div>35</div><div>En</div><div>Al</div><div>AWS Lambda</div></div></div><div><div><div>10</div><div>Os</div><div>Gh</div><div>GitHub</div></div><div><div>18</div><div>Os</div><div>Gls</div><div>GitLab SCM</div></div><div><div>36</div><div>Fm</div><div>Abb</div><div>Atlassian Bitbucket</div></div></div><div><div><div>5</div><div>En</div><div>Azp</div><div>Azure DevOps Pipelines</div></div><div><div>13</div><div>En</div><div>Dad</div><div>Digital.ai Deploy</div></div><div><div>31</div><div>En</div><div>Ud</div><div>UrbanCode Deploy</div></div></div><div><div><div>6</div><div>Os</div><div>Ow</div><div>OWASP ZAP</div></div><div><div>14</div><div>En</div><div>Sni</div><div>Sonatype Nexus IQ</div></div><div><div>32</div><div>En</div><div>Vc</div><div>Veracode</div></div></div><div><div><div>7</div><div>En</div><div>Dap</div><div>Digital.ai App Protection</div></div><div><div>15</div><div>En</div><div>Aq</div><div>Aqua Security</div></div><div><div>33</div><div>Os</div><div>Hv</div><div>HashiCorp Vault</div></div></div><div><div><div>8</div><div>En</div><div>Dar</div><div>Digital.ai Release</div></div><div><div>16</div><div>En</div><div>Cfr</div><div>CloudBees Flow</div></div><div><div>34</div><div>En</div><div>Ur</div><div>UrbanCode Release</div></div></div><div><div><div>9</div><div>En</div><div>Acp</div><div>AWS CodePipeline</div></div><div><div>17</div><div>En</div><div>Brl</div><div>BMC RLM</div></div><div><div>35</div><div>En</div><div>Al</div><div>AWS Lambda</div></div></div><div><div><div>10</div><div>Os</div><div>Gh</div><div>GitHub</div></div><div><div>18</div><div>Os</div><div>Gls</div><div>GitLab SCM</div></div><div><div>36</div><div>Fm</div><div>Abb</div><div>Atlassian Bitbucket</div></div></div><div><div><div>5</div><div>En</div><div>Azp</div><div>Azure DevOps Pipelines</div></div><div><div>13</div><div>En</div><div>Dad</div><div>Digital.ai Deploy</div></div><div><div>31</div><div>En</div><div>Ud</div><div>UrbanCode Deploy</div></div></div><div><div><div>6</div><div>Os</div><div>Ow</div><div>OWASP ZAP</div></div><div><div>14</div><div>En</div><div>Sni</div><div>Sonatype Nexus IQ</div></div><div><div>32</div><div>En</div><div>Vc</div><div>Veracode</div></div></div><div><div><div>7</div><div>En</div><div>Dap</div><div>Digital.ai App Protection</div></div><div><div>15</div><div>En</div><div>Aq</div><div>Aqua Security</div></div><div><div>33</div><div>Os</div><div>Hv</div><div>HashiCorp Vault</div></div></div><div><div><div>8</div><div>En</div><div>Dar</div><div>Digital.ai Release</div></div><div><div>16</div><div>En</div><div>Cfr</div><div>CloudBees Flow</div></div><div><div>34</div><div>En</div><div>Ur</div><div>UrbanCode Release</div></div></div><div><div><div>9</div><div>En</div><div>Acp</div><div>AWS CodePipeline</div></div><div><div>17</div><div>En</div><div>Brl</div><div>BMC RLM</div></div><div><div>35</div><div>En</div><div>Al</div><div>AWS Lambda</div></div></div><div><div><div>10</div><div>Os</div><div>Gh</div><div>GitHub</div></div><div><div>18</div><div>Os</div><div>Gls</div><div>GitLab SCM</div></div><div><div>36</div><div>Fm</div><div>Abb</div><div>Atlassian Bitbucket</div></div></div><div><div><div>5</div><div>En</div><div>Azp</div><div>Azure DevOps Pipelines</div></div><div><div>13</div><div>En</div><div>Dad</div><div>Digital.ai Deploy</div></div><div><div>31</div><div>En</div><div>Ud</div><div>UrbanCode Deploy</div></div></div><div><div><div>6</div><div>Os</div><div>Ow</div><div>OWASP ZAP</div></div><div><div>14</div><div>En</div><div>Sni</div><div>Sonatype Nexus IQ</div></div><div><div>32</div><div>En</div><div>Vc</div><div>Veracode</div></div></div><div><div><div>7</div><div>En</div><div>Dap</div><div>Digital.ai App Protection</div></div><div><div>15</div><div>En</div><div>Aq</div><div>Aqua Security</div></div><div><div>33</div><div>Os</div><div>Hv</div><div>HashiCorp Vault</div></div></div><div><div><div>8</div><div>En</div><div>Dar</div><div>Digital.ai Release</div></div><div><div>16</div><div>En</div><div>Cfr</div><div>CloudBees Flow</div></div><div><div>34</div><div>En</div><div>Ur</div><div>UrbanCode Release</div></div></div><div><div><div>9</div><div>En</div><div>Acp</div><div>AWS CodePipeline</div></div><div><div>17</div><div>En</div><div>Brl</div><div>BMC RLM</div></div><div><div>35</div><div>En</div><div>Al</div><div>AWS Lambda</div></div></div><div><div><div>10</div><div>Os</div><div>Gh</div><div>GitHub</div></div><div><div>18</div><div>Os</div><div>Gls</div><div>GitLab SCM</div></div><div><div>36</div><div>Fm</div><div>Abb</div><div>Atlassian Bitbucket</div></div></div><div><div><div>5</div><div>En</div><div>Azp</div><div>Azure DevOps Pipelines</div></div><div><div>13</div><div>En</div><div>Dad</div><div>Digital.ai Deploy</div></div><div><div>31</div><div>En</div><div>Ud</div><div>UrbanCode Deploy</div></div></div><div><div><div>6</div><div>Os</div><div>Ow</div><div>OWASP ZAP</div></div><div><div>14</div><div>En</div><div>Sni</div><div>Sonatype Nexus IQ</div></div><div><div>32</div><div>En</div><div>Vc</div><div>Veracode</div></div></div><div><div><div>7</div><div>En</div><div>D</div></div></div></div></div>									

Ref: <https://digital.ai/periodic-table-of-devops-tools>

# DIFFERENT VIEWPOINTS

DevSecOps:

- Dev
- Sec
- Ops

# DEVELOPER VIEWPOINT

## DevSecOps:

- Application static/dynamic testing in CI/CD
- Secure by design

# SECURITY VIEWPOINT

DevSecOps:

- Policy as code
- Vulnerability, Patch
- Response

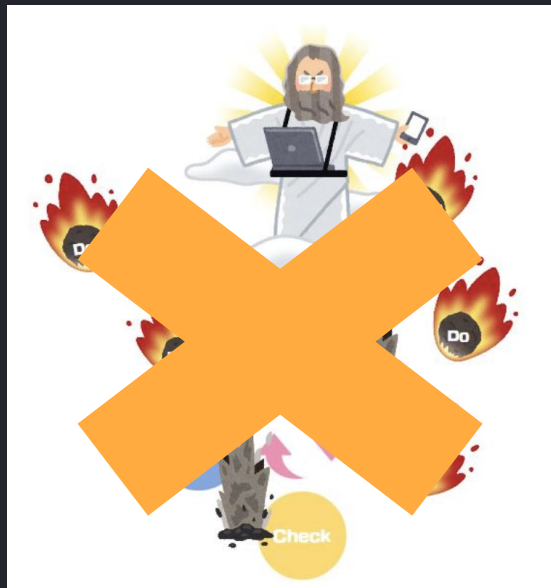
# OPS VIEWPOINT

DevSecOps:

- Reviewable infrastructure (Infra as code)
- Monitoring more items

## RECAP

- The life cycle
- From different viewpoint
  - Dev
  - Sec
  - Ops
  - ~~—Boss—~~



Ref: [https://eiki.hatenablog.jp/entry/meteo\\_fall](https://eiki.hatenablog.jp/entry/meteo_fall)



DEVSECOPS  
THE GOOD

# THE GOOD: LOW HANGING FRUIT

Secure by design

Left shift of testing

- Found and fix the vulnerability early

Reviewable infrastructure and policy

- IaC
- Pac

Monitoring makes response faster

# DEVSECOPS

## THE BAD

# THE BAD: SOMETIMES WE CAN SOLVE IT

Performance issue

Loss availability

Tools are good but people

- Threat modeling still need dev team's help
- Trust issue: when the red team coming

Vulnerability of sec tools

- Exploiting image scanners by matuzg

Overdesign

Ref:

<https://medium.com/@matuzg/testing-docker-cve-scanners-part-2-5-exploiting-cve-scanners-b37766f73005>

DEVSECOPS  
THE UGLY

# THE UGLY: THE HARDEST PART

Misunderstanding or Misconfiguration = Disaster

- "... \*\*\*-WAF-Role..." ~= 80M USD

New tools not stable...

- Falco: Dropped events #1403

More false positive alarm...

Security is always lagging...

Who will take the responsibility?

Ref: <https://github.com/falcosecurity/falco/issues/1403>

# SUMMARY

# SUMMARY

## DevSecOps

- The Good
- The Bad
- The Ugly

More than tool, process... the key is people and culture



以前的我：

DevOps



現在的我：

DevSecOps



# TAKE AWAY

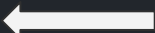
## Conference

- Blackhat
- Defcon
- DevSecCon
- DevSecOps days
- RSA

## DevSecOps youtube channel

- <https://www.youtube.com/channel/UCmzqpR98J4KtLj4K7RRRwEw>

## Tools collection

- <https://github.com/devsecops/awesome-devsecops>
- <https://github.com/4ndersonLin/awesome-cloud-security>  It's me! Please contribute!

# WE ARE HIRING



<https://github.com/MaiAmis/Careers>



THANKS!

Any questions?

You can find me at  
[4nderson.lin@pm.me](mailto:4nderson.lin@pm.me)