Security as a MVP

...

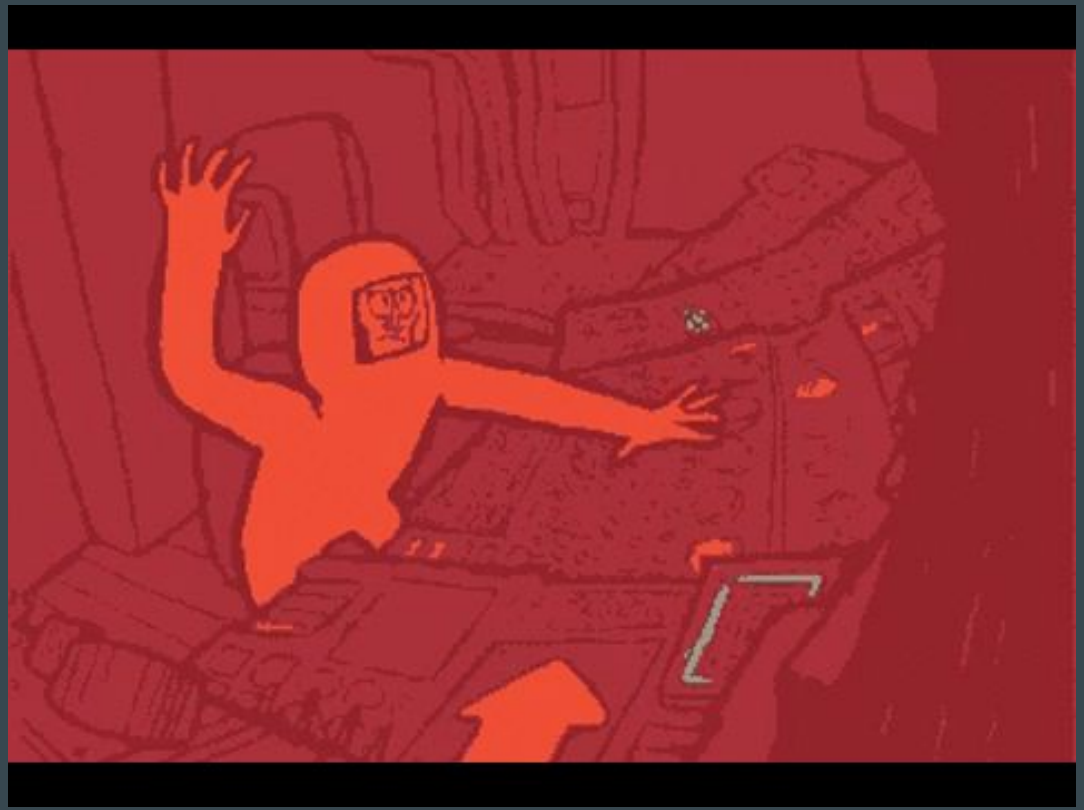
Josh Bressers
Elastic Product Security
@joshbressers
https://bit.ly/secmvp

Our Challenge

How did we get here?

First Open Source Won

Then DevOps Won



Now DevSecOps???

DevSecOps is dumb, it’s just DevOps

We still think about security the old way

What if it’s an MVP?

OWASP Top 10

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization
- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging&Monitoring

Everything old is new again

- A1:2017-Injection [A1:2013]
- A2:2017-Broken Authentication [A2:2013]
- A3:2017-Sensitive Data Exposure [A6:2013]
- A4:2017-XML External Entities (XXE) [NEW]
- A5:2017-Broken Access Control [A7:2013]
- A6:2017-Security Misconfiguration [A5:2013]
- A7:2017-Cross-Site Scripting (XSS) [A3:2013]
- A8:2017-Insecure Deserialization [NEW]
- A9:2017-Using Components with Known Vulnerabilities [A9:2013]
- A10:2017-Insufficient Logging&Monitoring [NEW]

DevOps MVP Fairy

~~OWASP Top 10~~

OWASP Top 3

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization
- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging&Monitoring

Use a framework for input and output

- A1:2017-Injection

- A4:2017-XML External Entities (XXE)

- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization

Use an auth library

- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure

- A5:2017-Broken Access Control

~~Dev~~Ops

- A6:2017-Security Misconfiguration

- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging&Monitoring

There is no magic

Perfect is impossible

Moving fast is the key

Questions?

...

Josh Bressers
Elastic Product Security
@joshbressers
https://bit.ly/secmvp