Security as a MVP

Josh Bressers
Elastic Product Security
@joshbressers
Our Challenge

I’LL JUST PUT THIS OVER HERE... WITH THE REST OF THE FIRE.
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

How do you do, fellow kids?
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

- A4:2017-XML External Entities (XXE) [NEW]
- A7:2017-Cross-Site Scripting (XSS) [A3:2013]
- A8:2017-Insecure Deserialization [NEW]
- A10:2017-Insufficient Logging&Monitoring [NEW]
DevOps MVP Fairy
● 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
● 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