ALL DAY DEVOPS

NOVEMBER 6, 2019

Gert Jan van Halem

Compliance as Code

ADDO
ALL DAY DEVOPS

Gert Jan van Halem

CTO @ devoteam

gert.jan.van.halem@devoteam.com
#2019addo-devsecops

ADDO
ALL DAY DEVOPS

"In general, compliance means conforming to a rule, such as a specification, policy, standard or law."

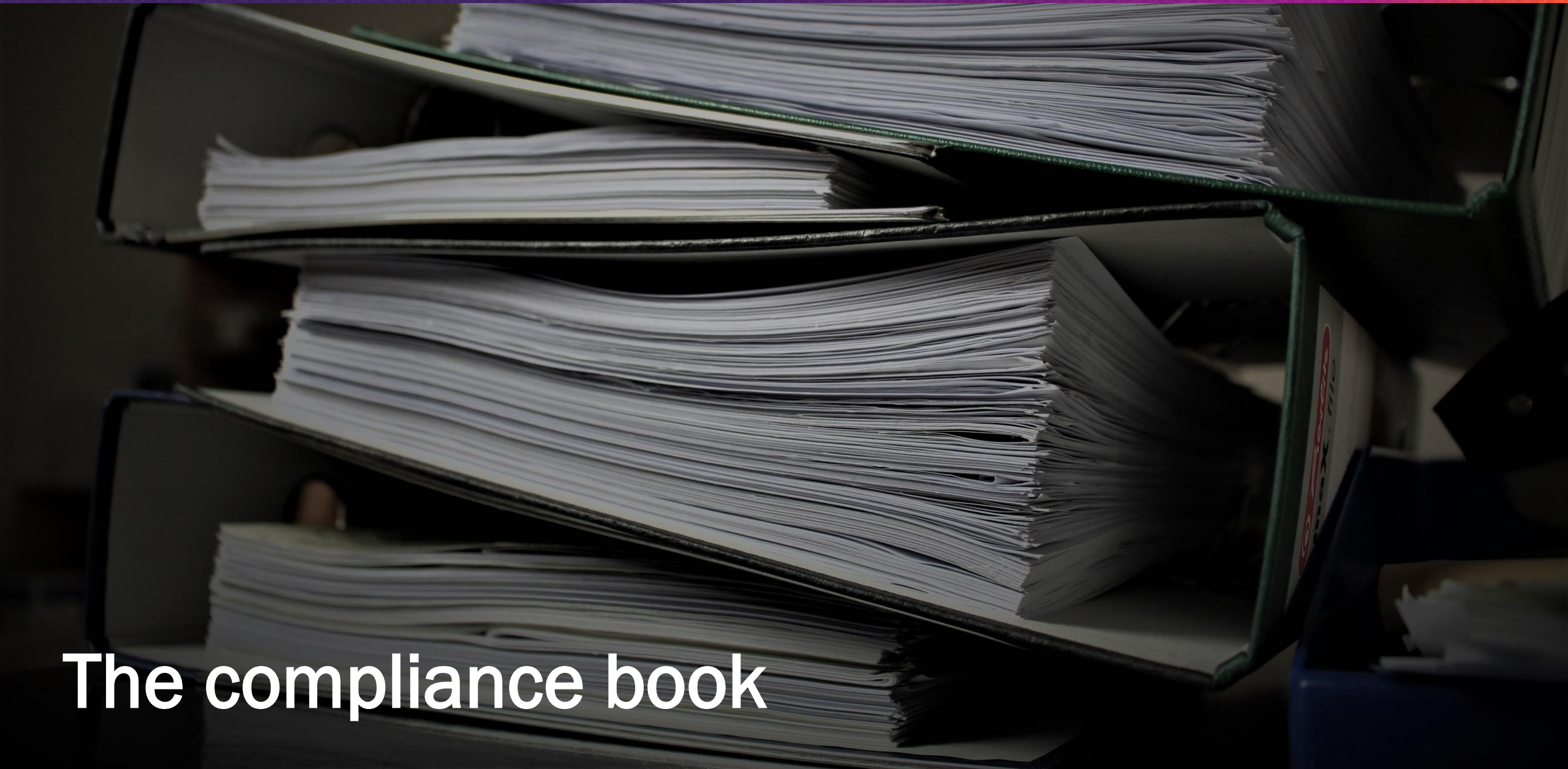
- Wikipedia

ADDO
ALL DAY DEVOPS


What happened?
FX

ADDO
ALL DAY DEVOPS

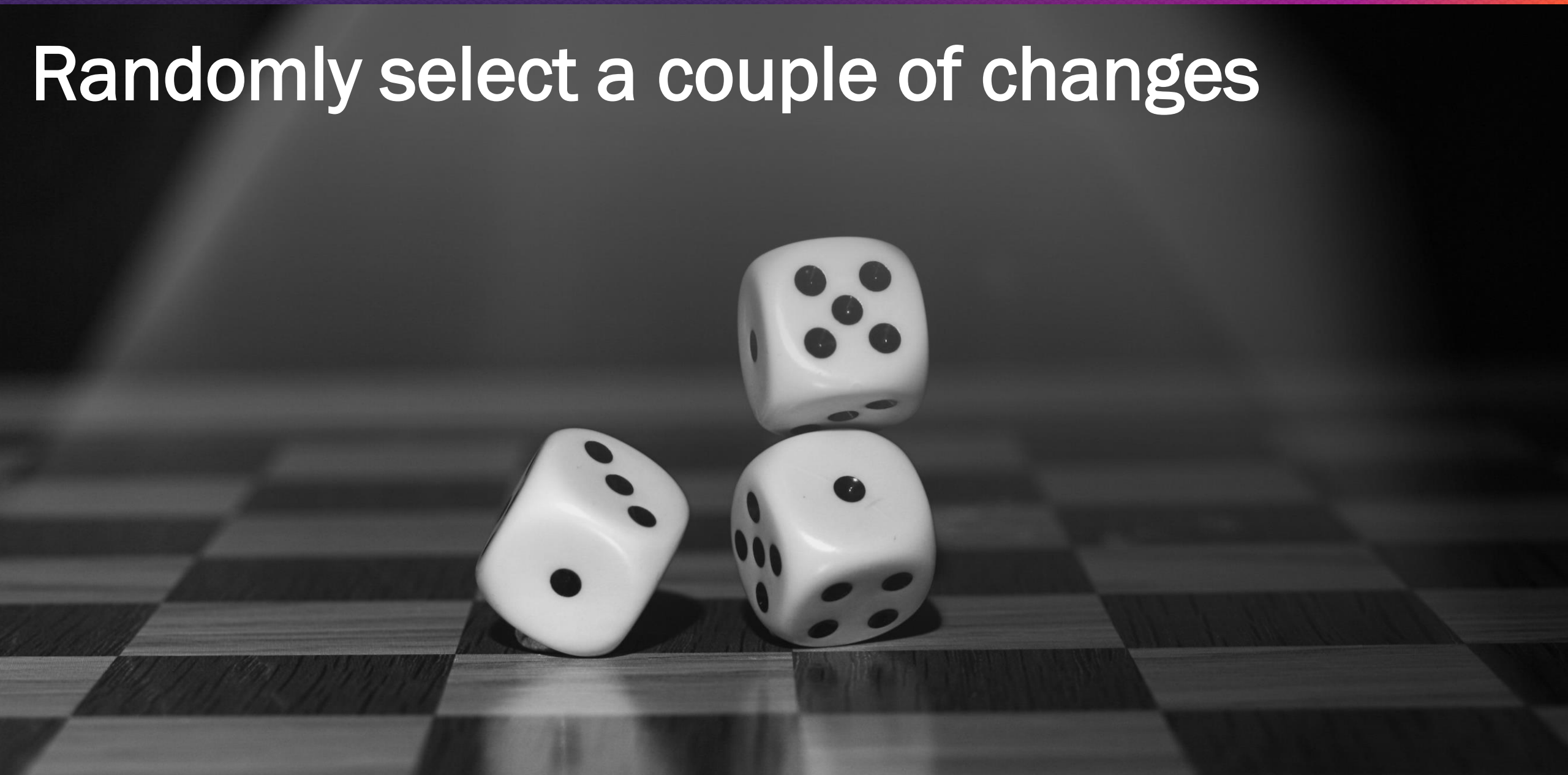
ADDO
ALL DAY DEVOPS



The compliance book

ADDO
ALL DAY DEVOPS

Randomly select a couple of changes



ADDO
ALL DAY DEVOPS

Walkthrough meeting

ADDO
ALL DAY DEVOPS

What it feels like...

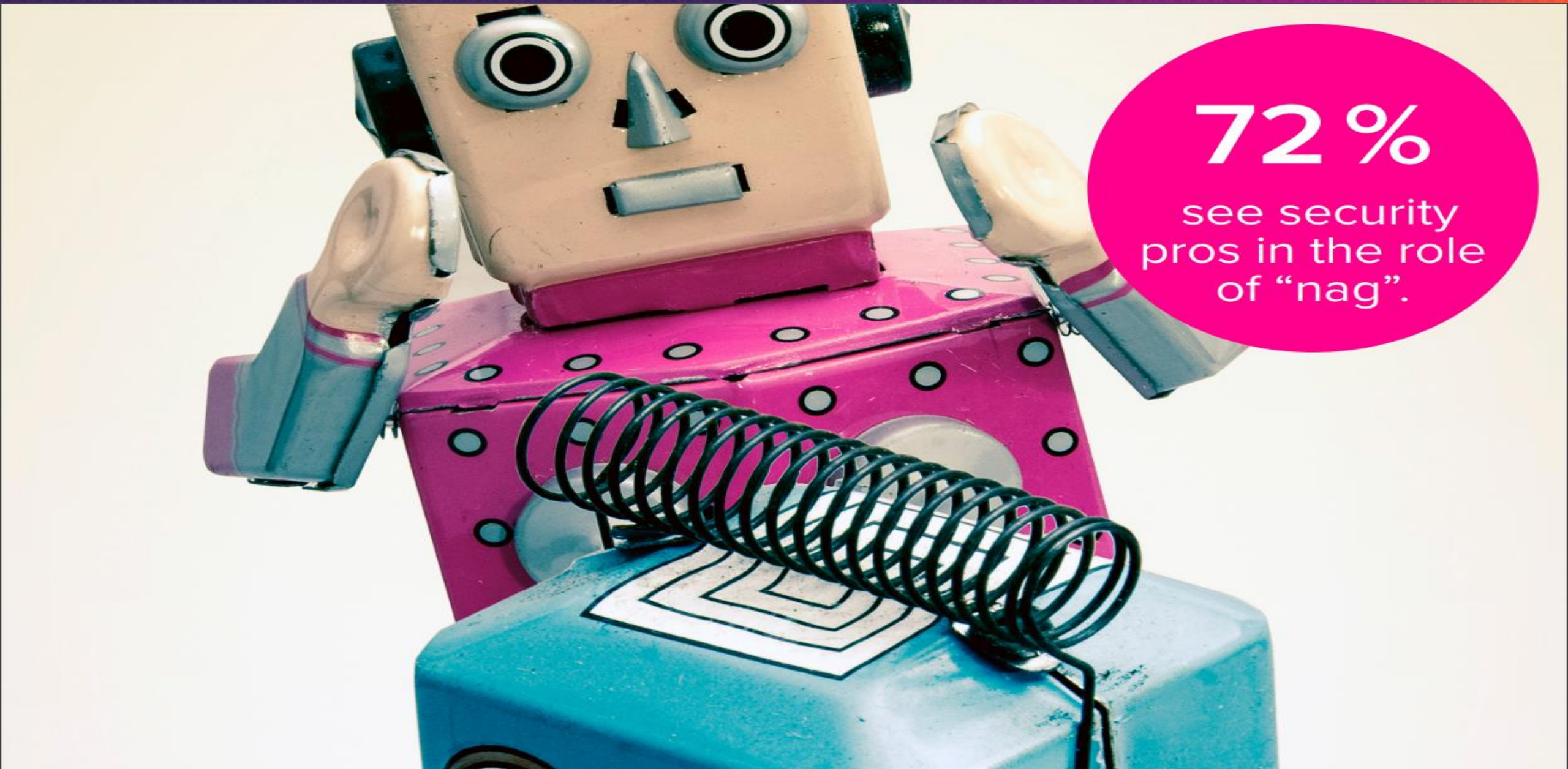
And then we made it worse...

From a compliance perspective at least

ADDO
ALL DAY DEVOPS

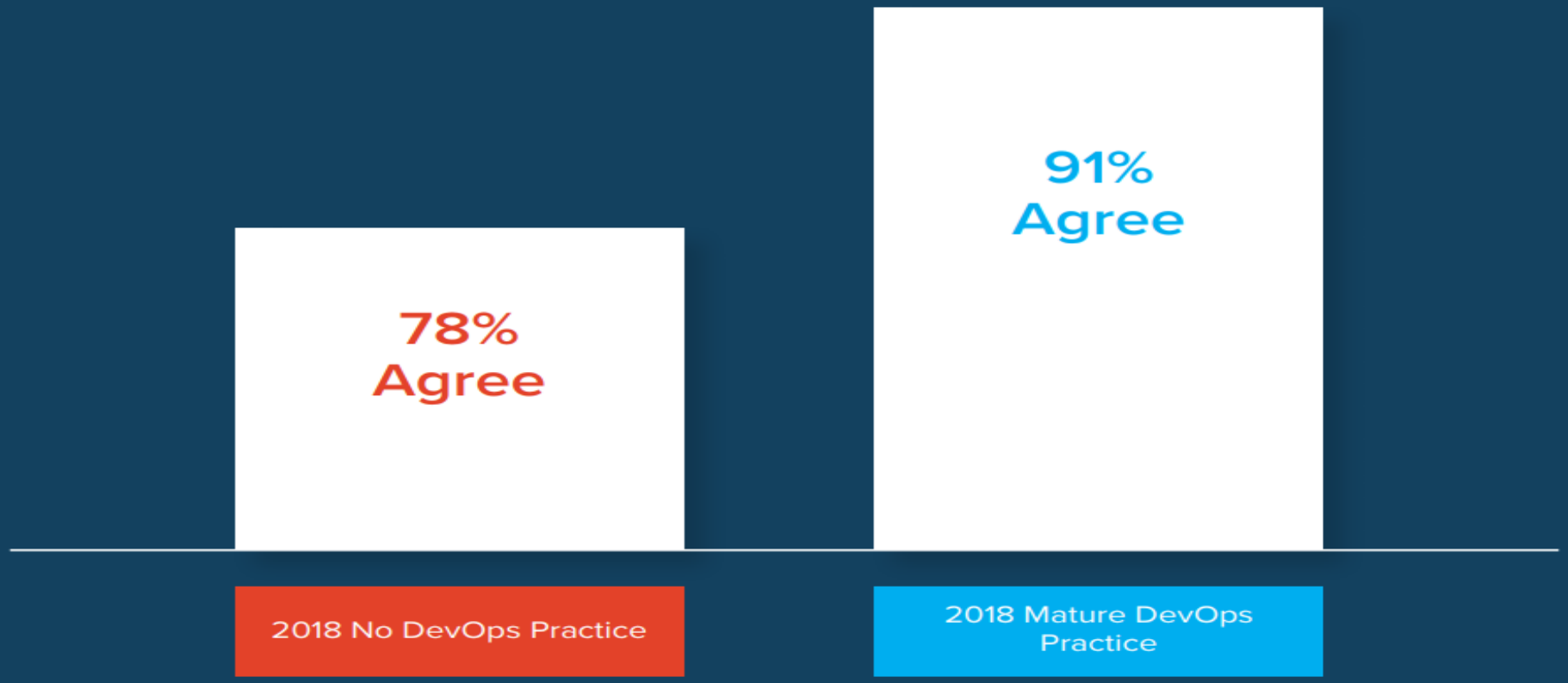
Autonomous teams

ADDO
ALL DAY DEVOPS


72%
see security pros in the role of “nag”.

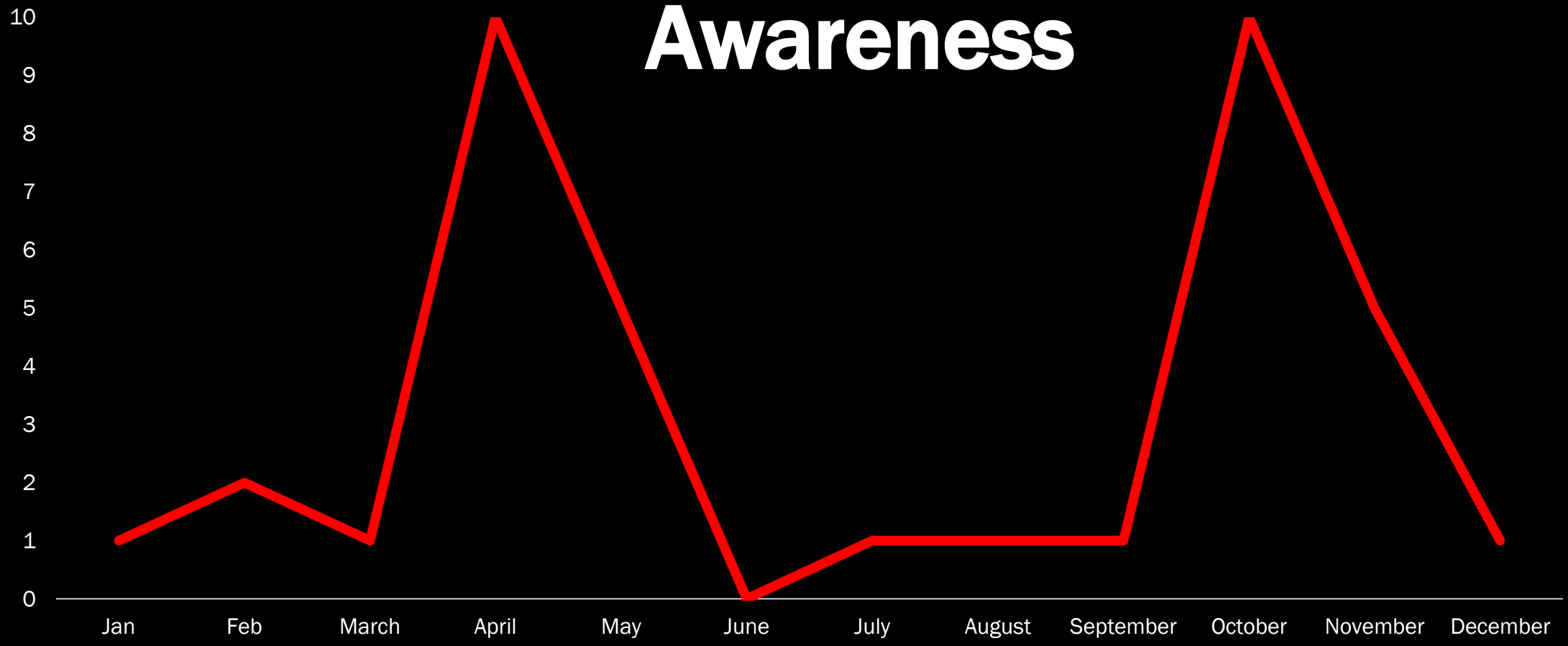
ADDO
ALL DAY DEVOPS

Security is part of everyone's role.



ADDO
ALL DAY DEVOPS

Awareness



ADDO
ALL DAY DEVOPS

ADDO
ALL DAY DEVOPS

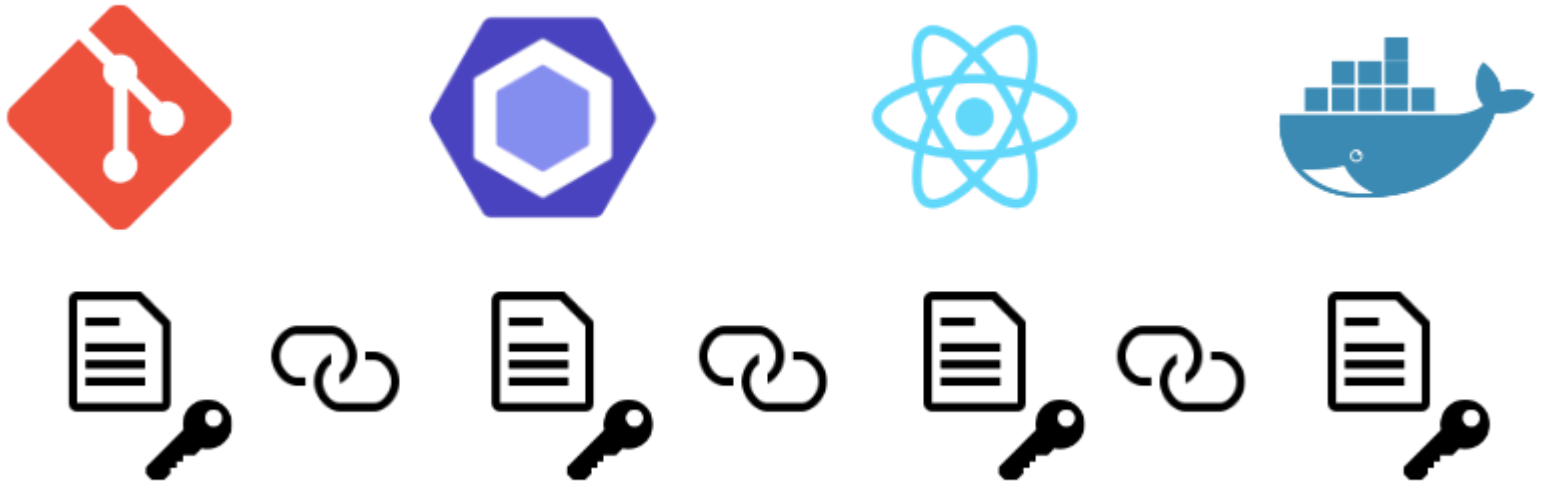
Shift it left


NJIT
New Jersey Institute of Technology


NYU

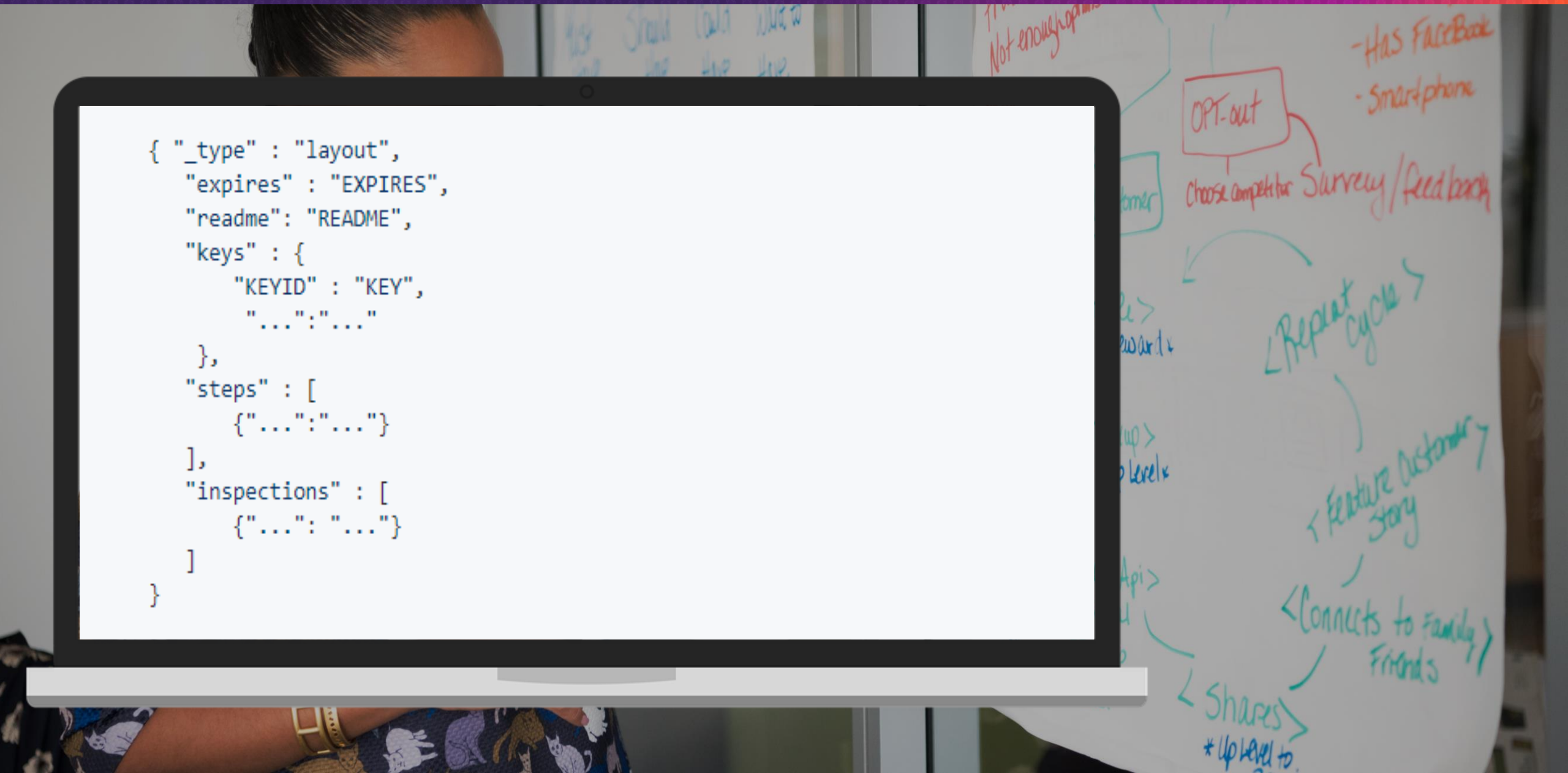
in-toto

A framework to secure the integrity of software supply chains

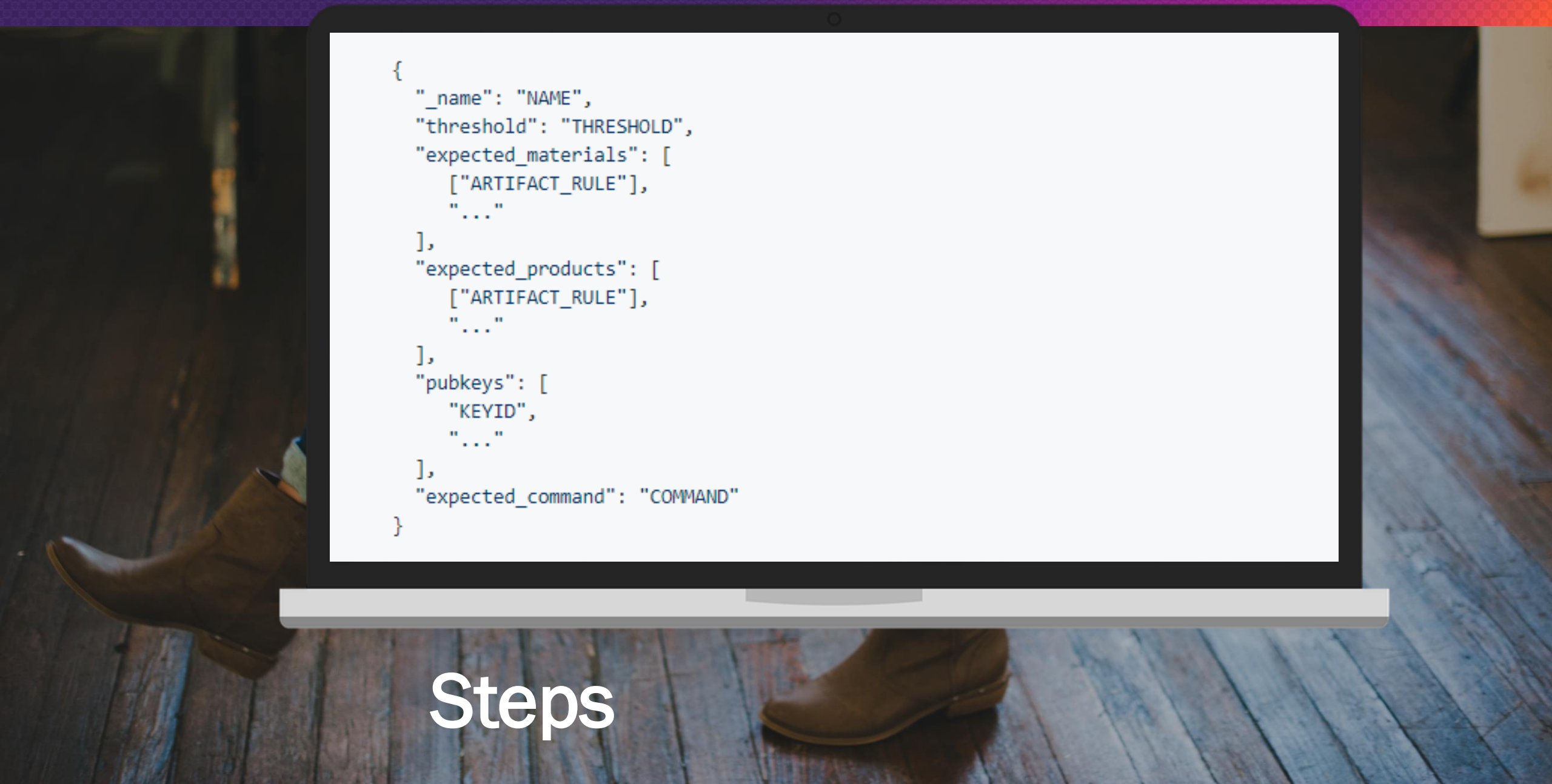


ADDO
ALL DAY DEVOPS

Layout



ADDO
ALL DAY DEVOPS

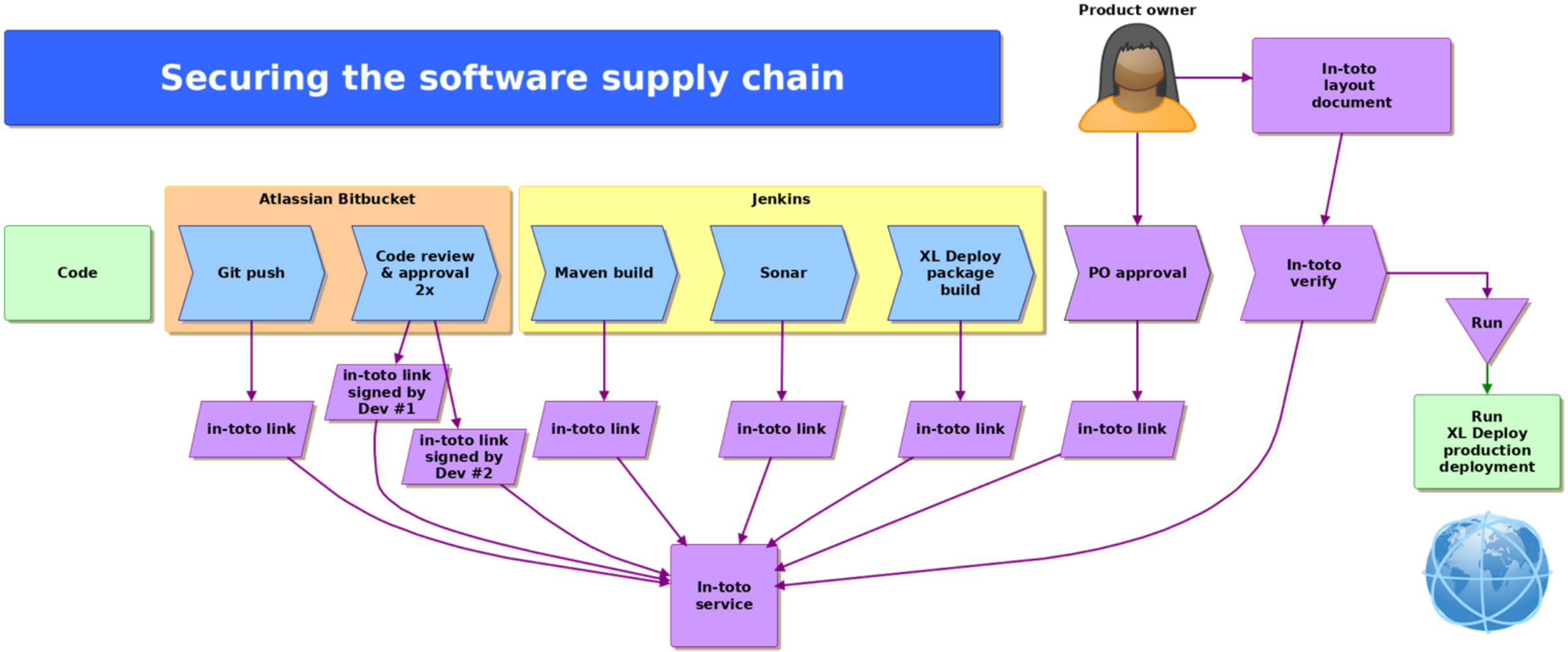


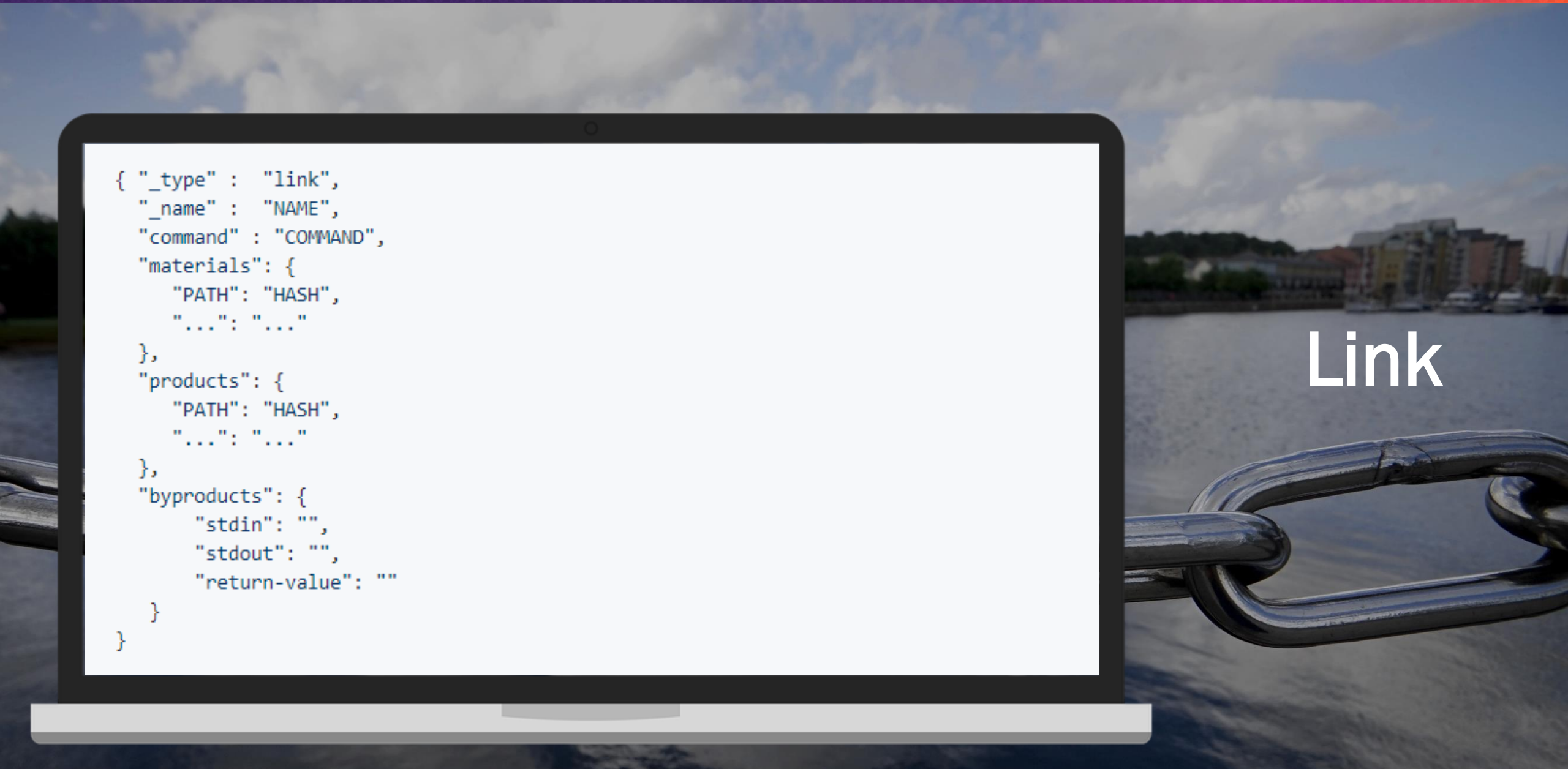
Steps

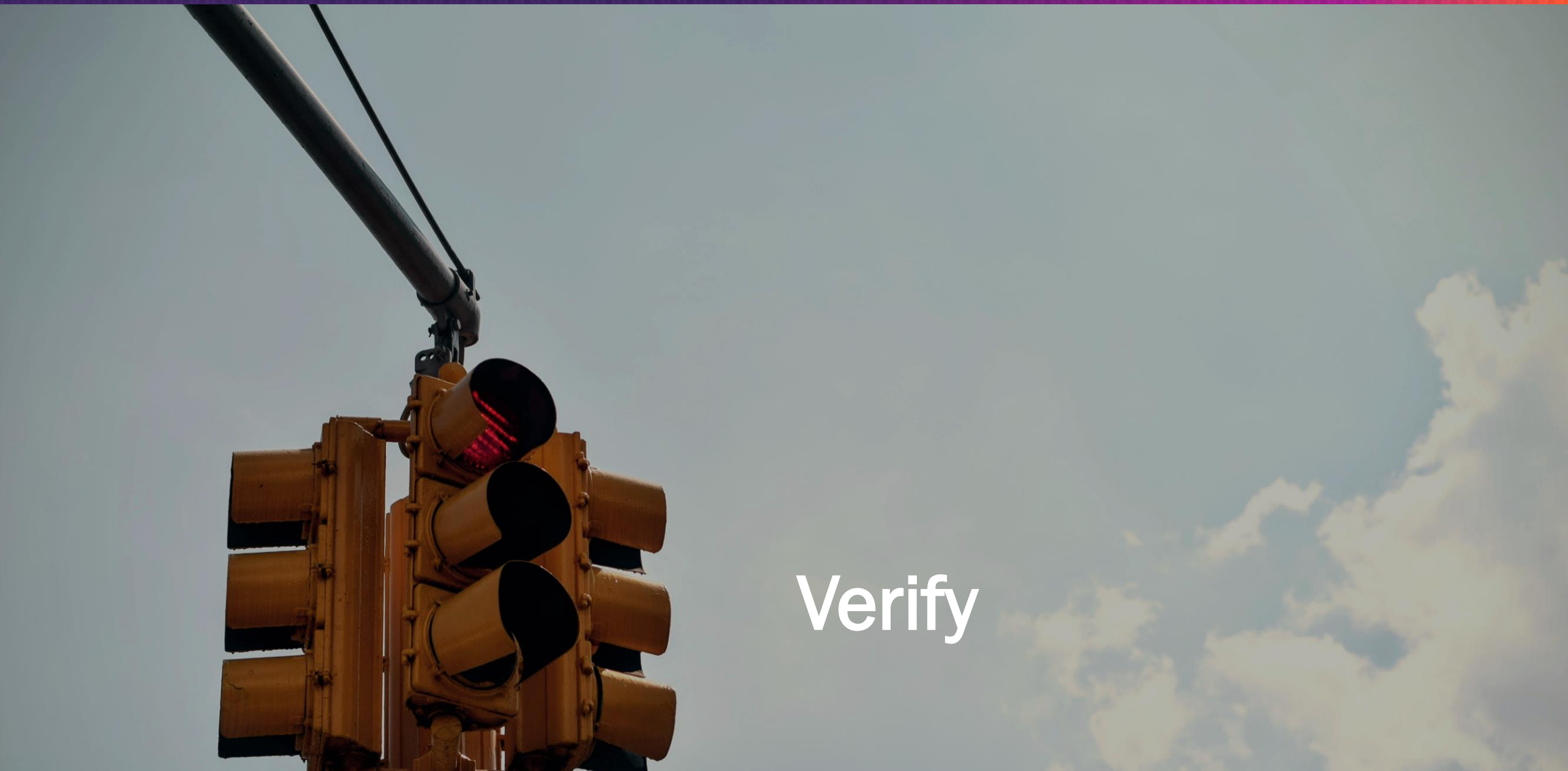
ADDO
ALL DAY DEVOPS

Inspect

Securing the software supply chain




{ "_type" : "link",
"_name" : "NAME",
"command" : "COMMAND",
"materials": {
"PATH": "HASH",
"...": "..."
},
"products": {
"PATH": "HASH",
"...": "..."
},
"byproducts": {
"stdin": "",
"stdout": "",
"return-value": ""
}
}
Link

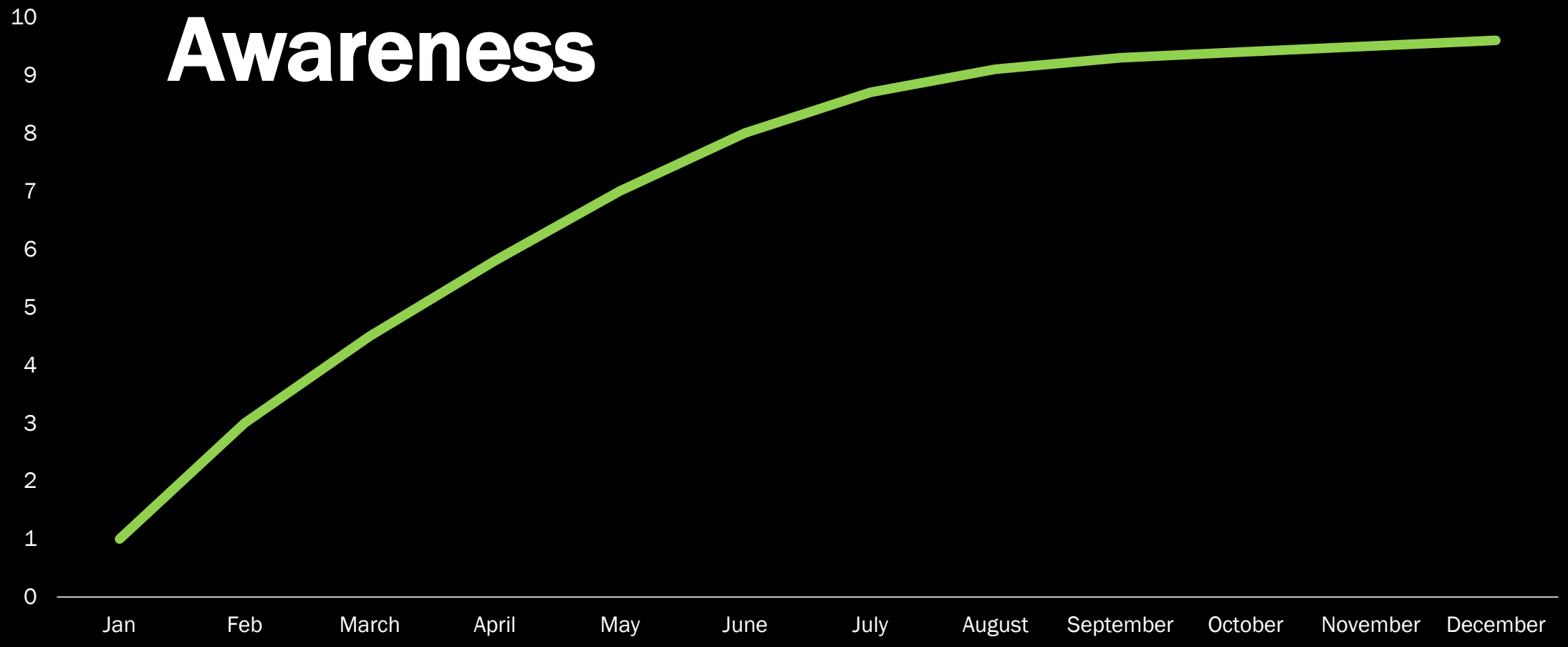


Verify

ADDO
ALL DAY DEVOPS

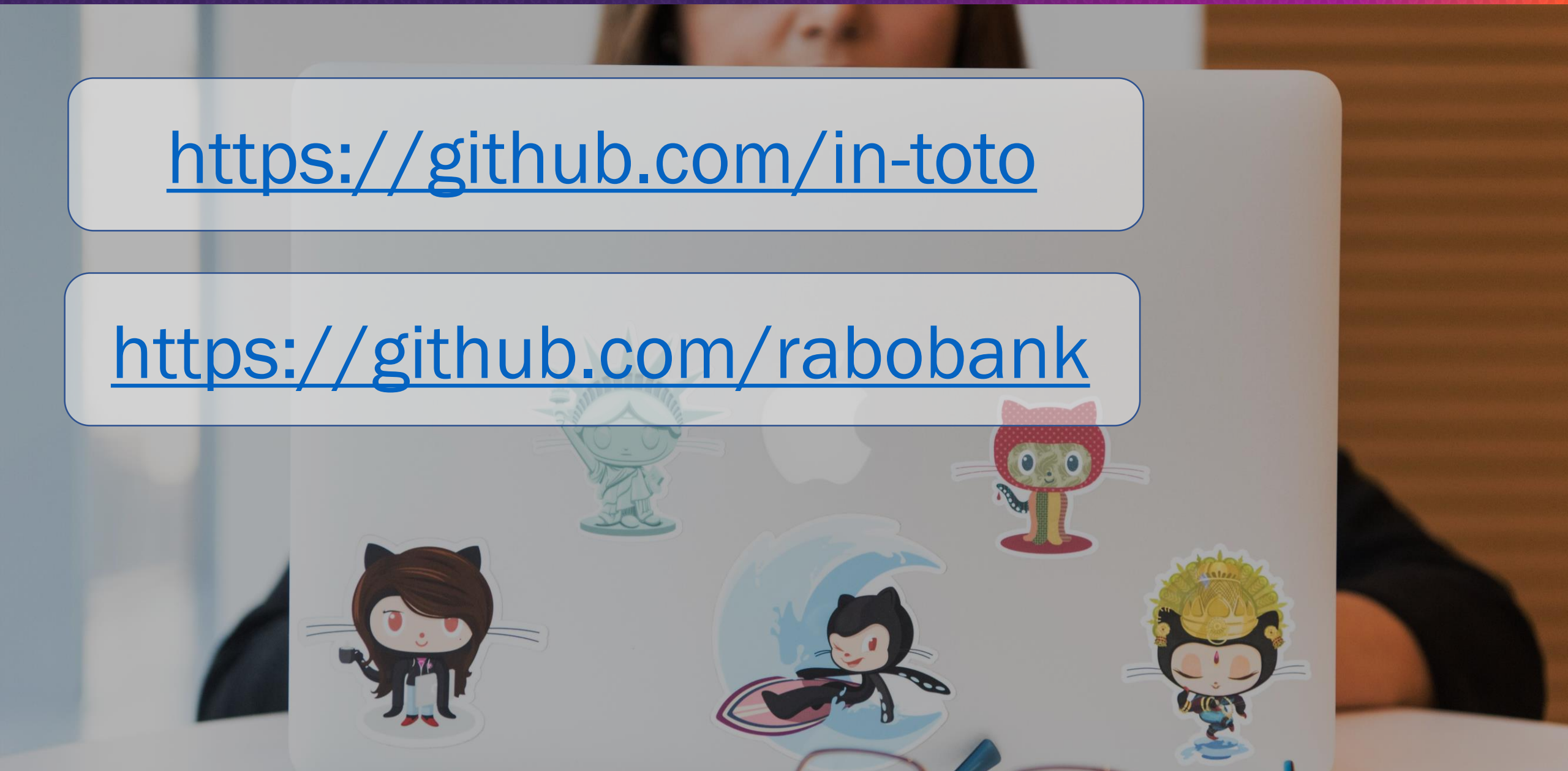
ADDO
ALL DAY DEVOPS

Awareness



https://github.com/in-toto

https://github.com/rabobank



Thanks

gert.jan.van.halem@devoteam.com

#2019addo-devsecops

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

StateFarm

GOLD SPONSORS

vmware

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XebiaLabs
Enterprise DevOps

cloudbees

Carnegie Mellon University
Software Engineering Institute

TIGERA

CONTINO

NowSecure

MEDIA SPONSORS

DZone
A DEVADA MEDIA PROPERTY

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire