







# DEVOPS IS NOW MUCH MORE THAN... • Automated application code compile, package and test • Deploy to an artefact repository • That's CI (Continuous Integration) • On-demand deployment of those tested ready-to-run artefacts into target environments • That's CD (Continuous Deployment)







### WHICH MEANS WHAT FOR SECURITY?

- "Ops" staff (whether in-house or at service providers) as the gatekeepers to infrastructure and root access is no longer a sustainable practice.
- "Take a ticket and wait" for infrastructure resources creation is no longer a sustainable practice.
- Waiting for Ops to install and configure applications on that infrastructure is no longer a sustainable practice. (The cost of even large disposable infrastructure is almost always less than the cost of holding up a development team.)
- Root access to create infrastructure and then access that infrastructure to configure it
  must be eliminated. Indeed, "root" becomes a non-event in terms of access control for
  staff. There is nothing to access!

### WHICH MEANS WHAT FOR SECURITY?

- Only systems will have root-level access to other systems, if at all.
- No more shared root password for the Ops oppos!
- People configure what that root access will do via code and config files, to be run automatically.
- Trust thus shifts from who has root system access to who has access to the code that will run as root. Think about that!

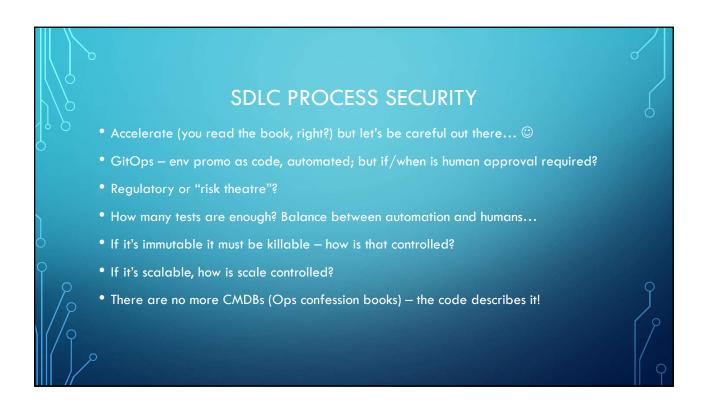




# SOURCE CODE AND ARTEFACT HANDLING • Supply chain integrity • Multi-level audit trail – repo, company, item, persons • If any one of these is found to have been compromised, need to know FAST if and where that code or artefact is running in my estate



# THE SURROUNDING LANDSCAPE • Logging integrity – immutable logs ideally • Metrics integrity – diversionary tactics by intruders • Tracing integrity – will it detect MITM net activity? • Policy control – what can do what and with whom • Access control – certificates, keys, etc • Zero trust networks – nothing to see here, move along...



# INCIDENT RESPONSE • Automated incident response/remediation – don't rely on it too much... • If it's immutable, no hot fixes! So, how fast can you replace that cow? • What checks are safe to skip for that? NFT? What else?





