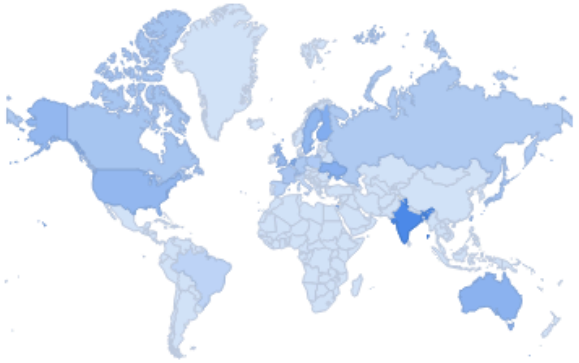
DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK ONE / LESSON ONE

What's Happening in the World?

- DEVOPS
- PUBLIC CLOUD
- AGILE
- SCRUM
- LEAN
- LOW-CODE
- NO-CODE
- NO OPS
- …



Region | City

India	100
Israel	99
Finland	58
Ukraine	57
Netherlands	56
Australia	52
Sweden	48

View change over time

https://www.google.com/trends/

A History Lesson – Google Trends Research

- *Several years after the Agile Manifesto, **DevOps.com** was registered in **2004***
- *Google searches for "DevOps" started to rise in **2010***
- *Major influences:*
  - *Saving your Infrastructure from DevOps / Chicago Tribune*
  - *DevOps: A Culture Shift, Not a Technology / Information Week*
  - *DevOps: A Sharder's Tale from Etsy*
  - *DevOps.com articles*
- *RuggedSoftware.org was registered in **2010***
- *As of **2013**, DevSecOps is on the map…*

Who's doing Enterprise DevOps?

…

What's the business benefit?

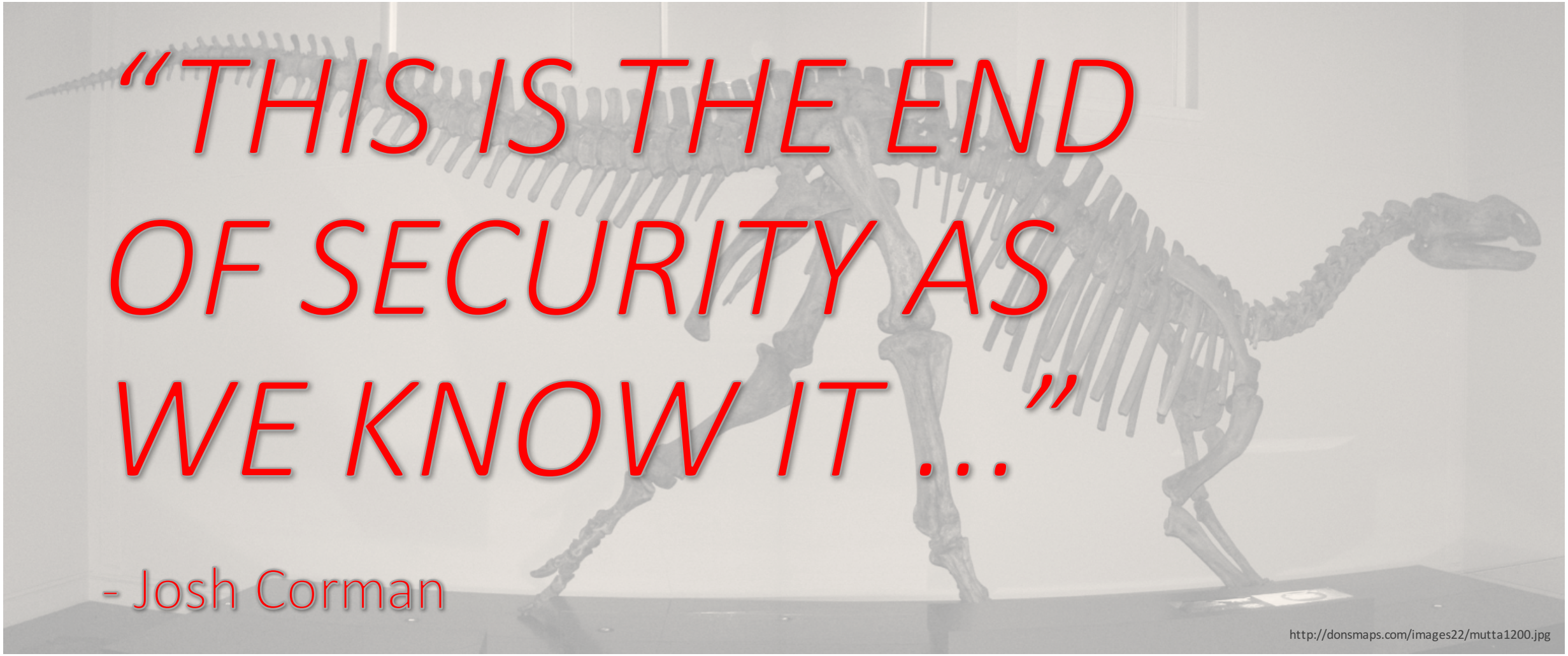
*Business strategy is achieved with the collaboration of all departments and providers in service to the customer who requires better, faster, cheaper, **secure** products and services.*

What Hinders Secure Innovation?

1. Manual processes & meeting culture
2. Point in time assessments
3. Friction for friction's sake
4. Contextual misunderstandings
5. Decisions being made outside of value creation
6. Late constraints and requirements
7. Big commitments, big teams, and big failures
8. Fear of failure, lack of learning
9. Lack of inspiration
10. Management and political interference (approvals, exceptions)

…

Say What??!!

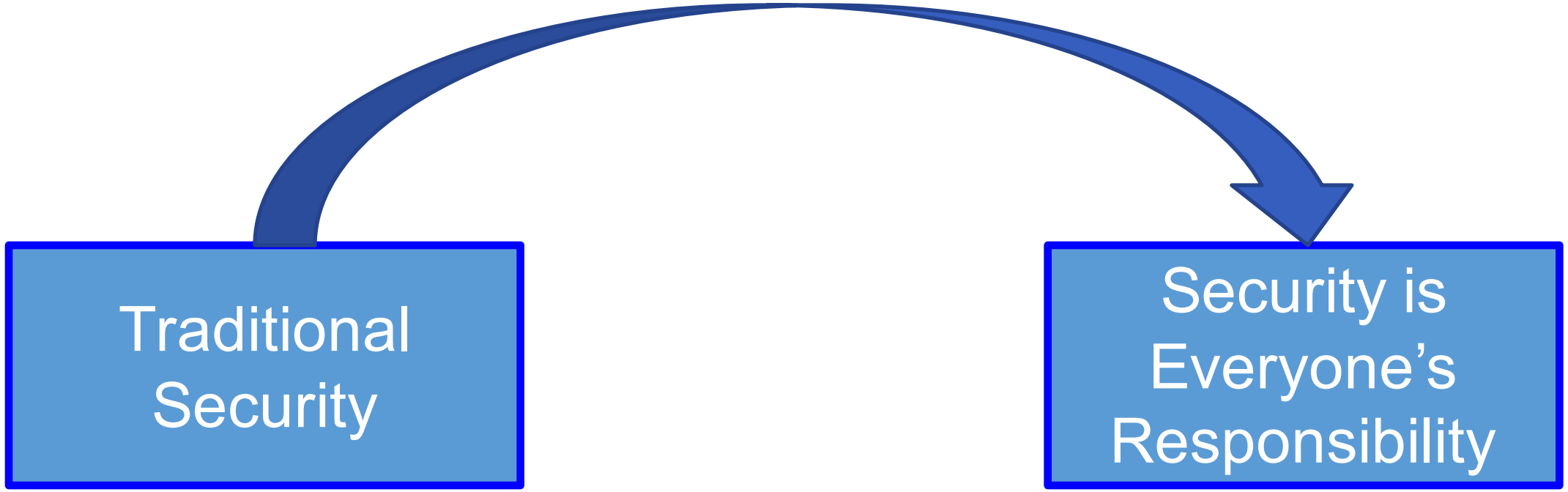


The Need for Change

- **Innovation** is a competitive advantage
- **Cloud** has leveled the playing field
- Demand for **Customer centric** product development
- Continuous delivery of features and changes
- New generation of workers desire collaboration
- **Speed and scale** are necessary to handle demand
- **Integration** over invention to speed up results
- Security breaches are on the rise
- People desire to work with **greater autonomy**...
- **Continuous Learning**... How can I do better? & better?

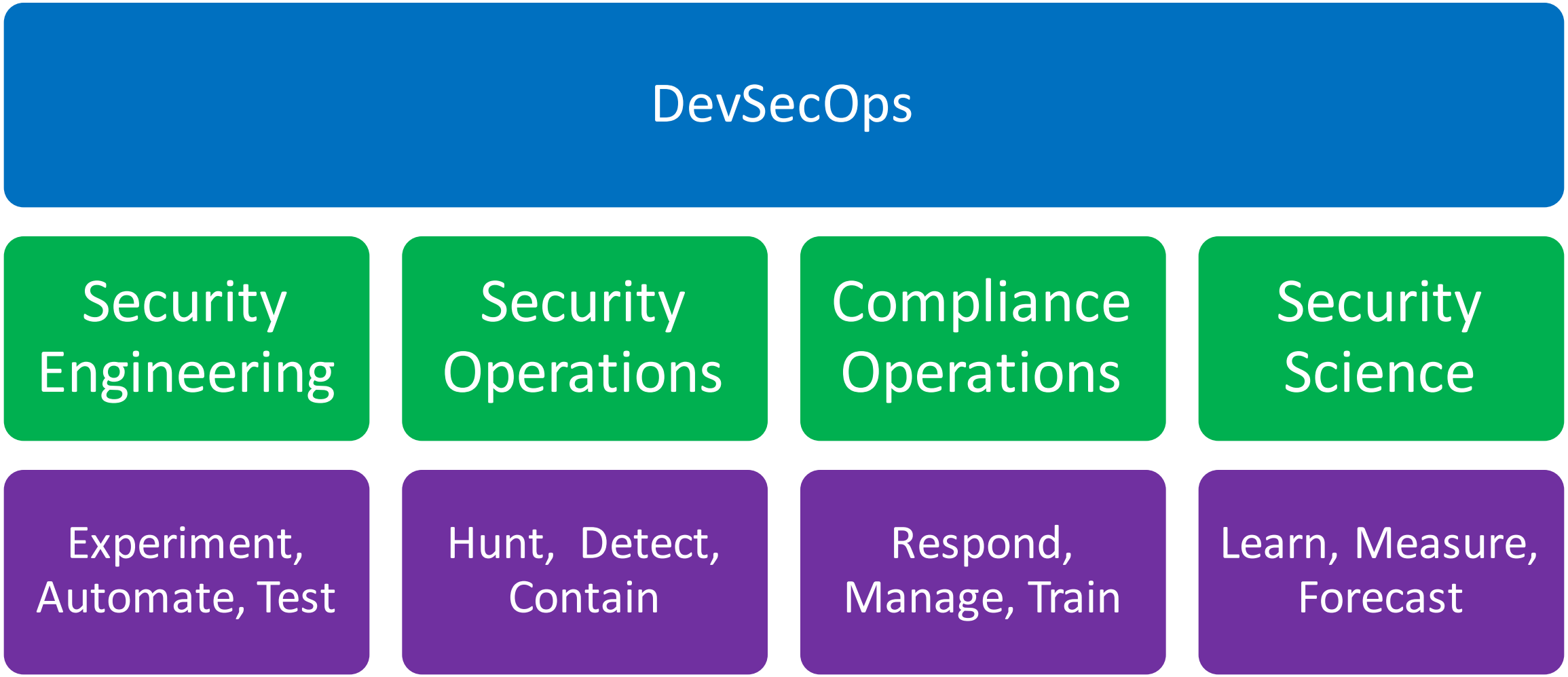
commons.wikimedia.org

Culture Hacking



DEVSECOPS

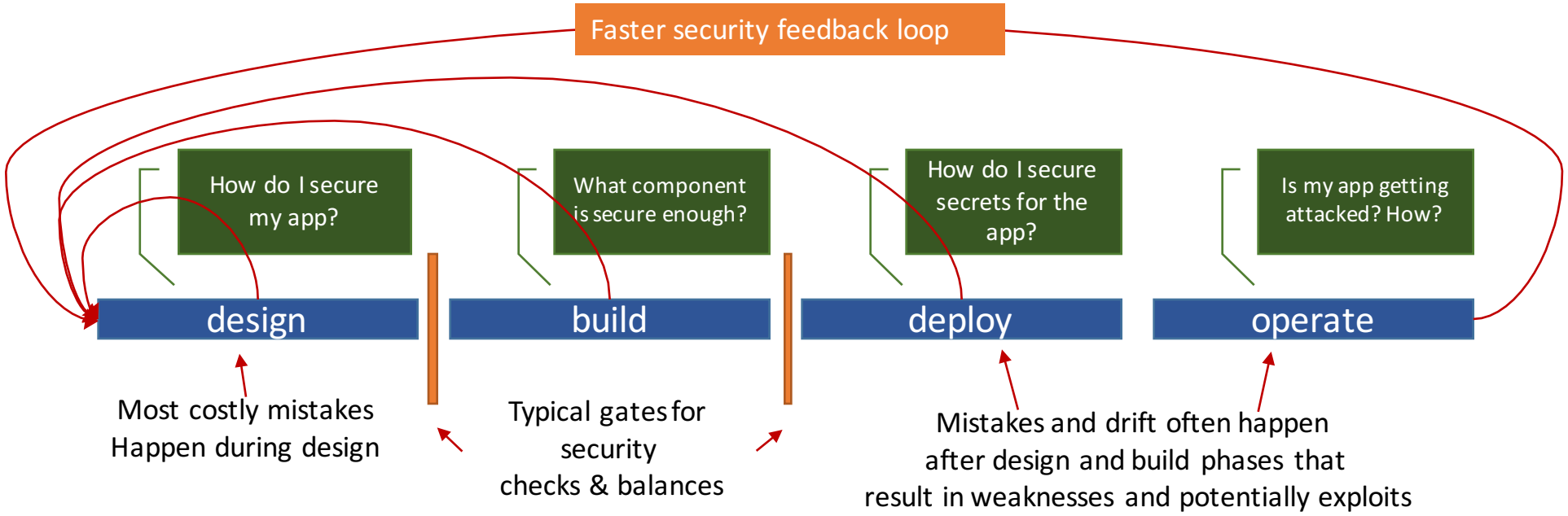
The Art of DevSecOps



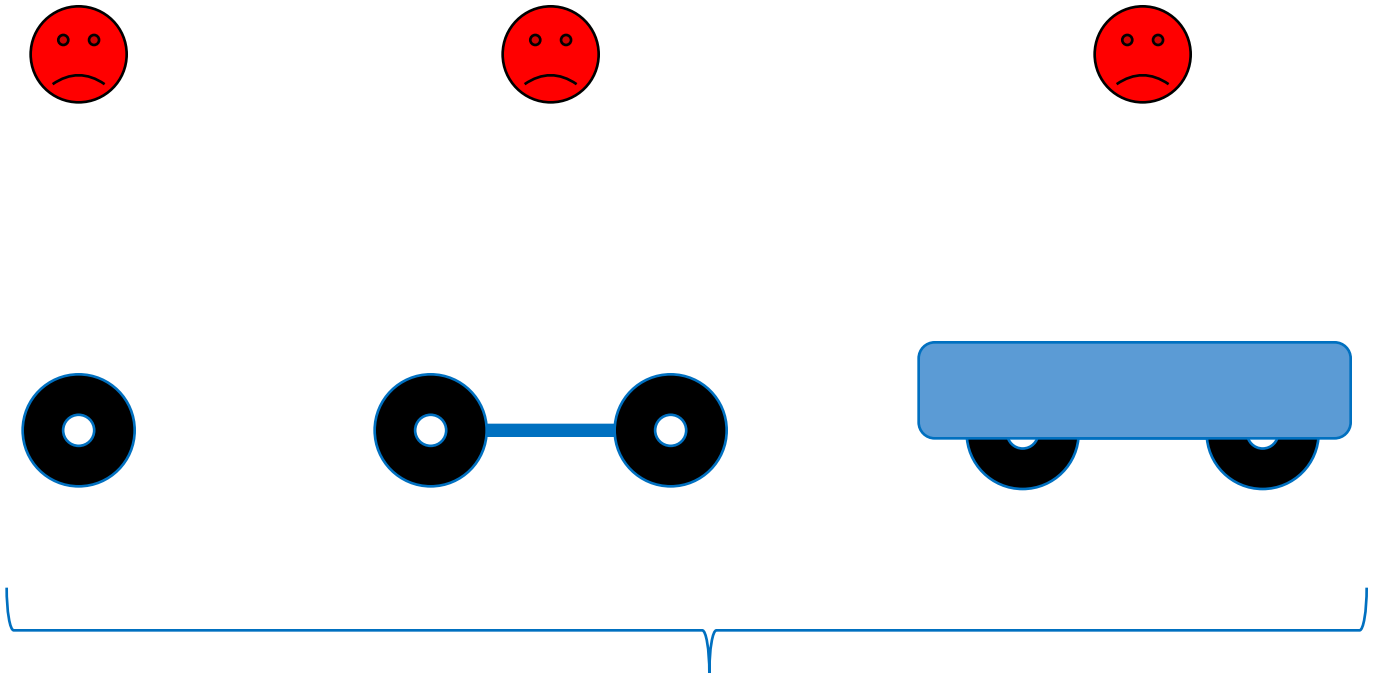
The Secure Software Supply Chain

- Gating processes are not Deming-like
- Security is a design constraint
- Decisions made by engineering teams

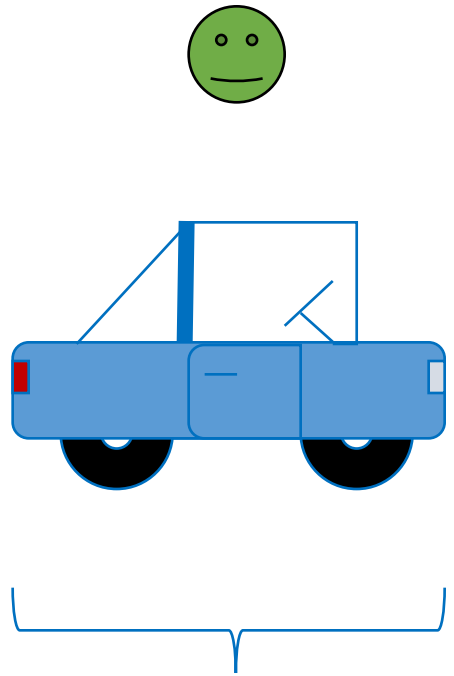
- Hard to avoid business catastrophes by applying one-size-fits-all strategies
- Security defects is more like a security “recall”



From a Traditional Supply Chain…



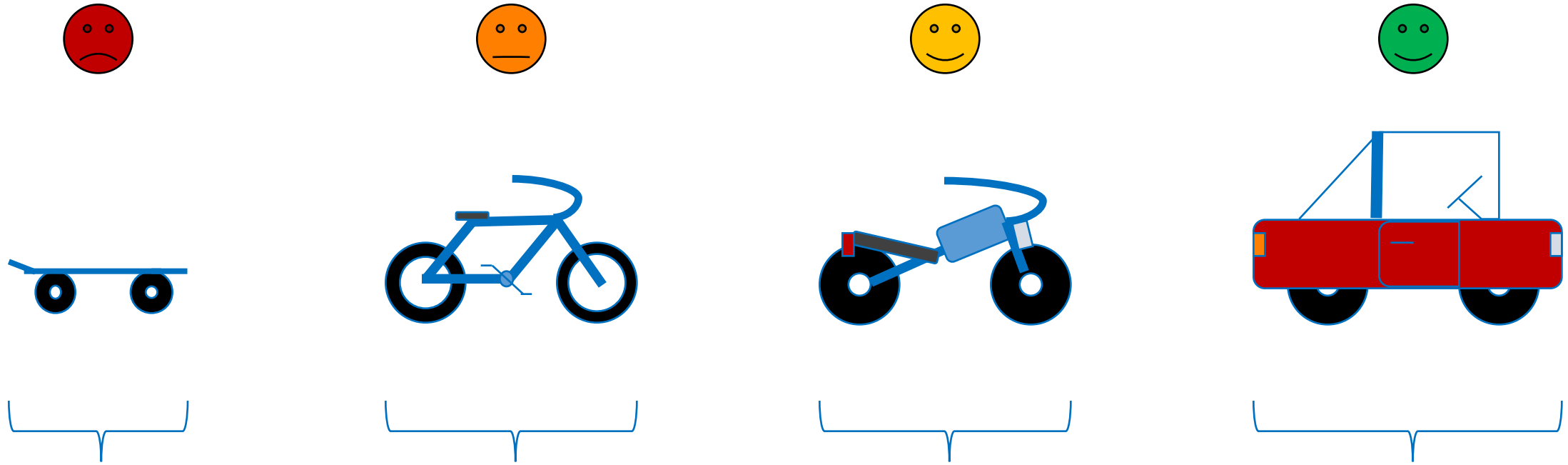
When will you solve my problem?!!



Can we discuss my feedback?
Did we pass the 98 point inspection?

Thanks to Henrik Kniberg

To a Customer Centric Supply Chain



Better than walking, for sure…
but not by much...

Can this be motorized
to go faster and for longer trips?

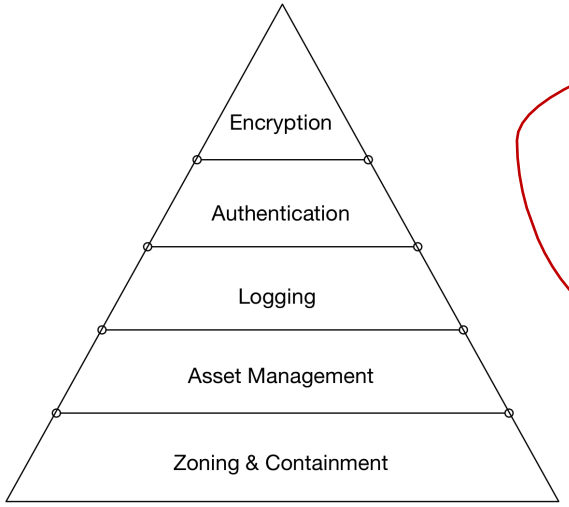
When can I bring my kids with me?
Does it come in Red?

Awesome!

Security must shift left with a Science Mindset like all other Ops…

Thanks to Henrik Kniberg

Shifting Security to the Left means built-in



Faster security feedback loop

How do I secure my app?

What component is secure enough?

How do I secure secrets for the app?

Is my app getting attacked? How?

design

build

deploy

operate

Most costly mistakes Happen during design

Typical gates for security checks & balances

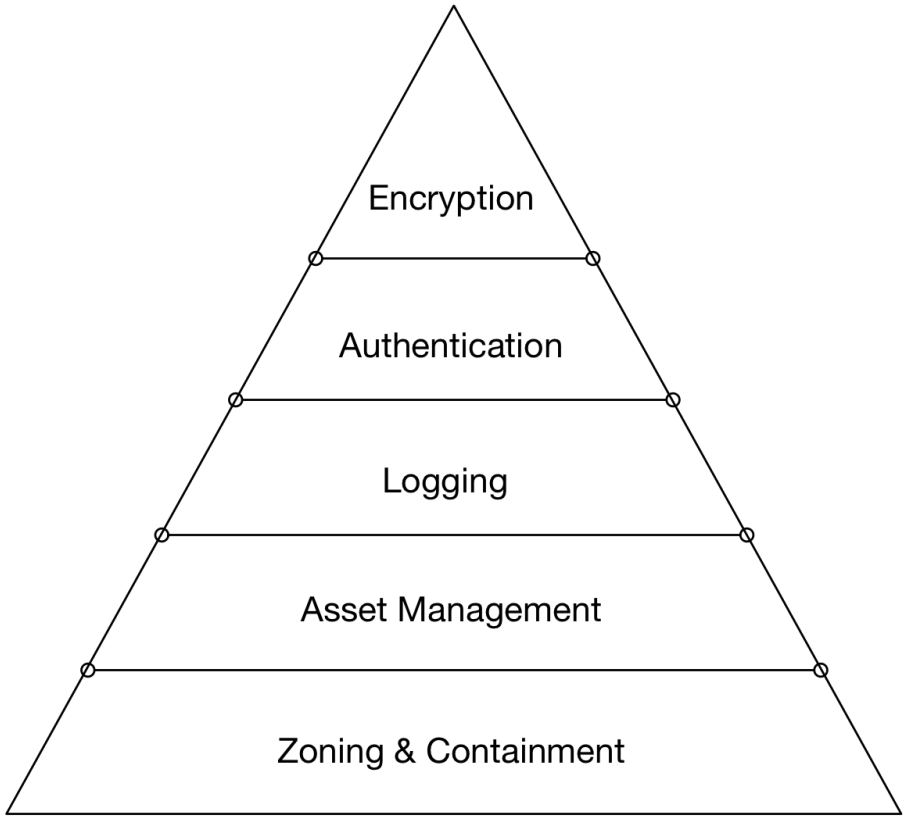
Mistakes and drift often happen after design and build phases that result in weaknesses and potentially exploits

Security is a Design Constraint

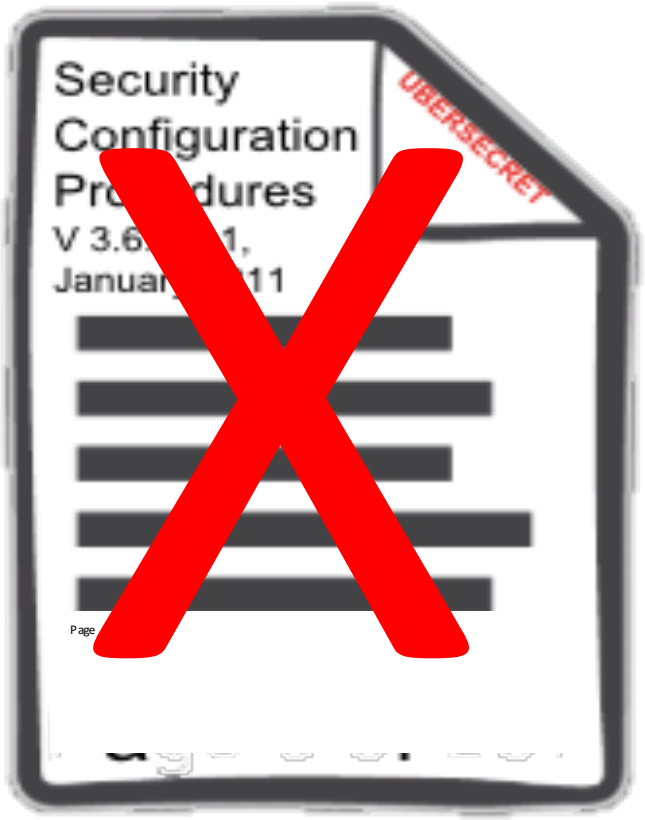
Security is and has always been a Design Constraint…

- Everyone knows Maslow…
- If you can remember 5 things, remember these ->

"Apps & data are as safe as where you put it, what's in it, how you inspect it, who talks to it, and how its protected…"



But Please No Checklists & Save the Trees!!

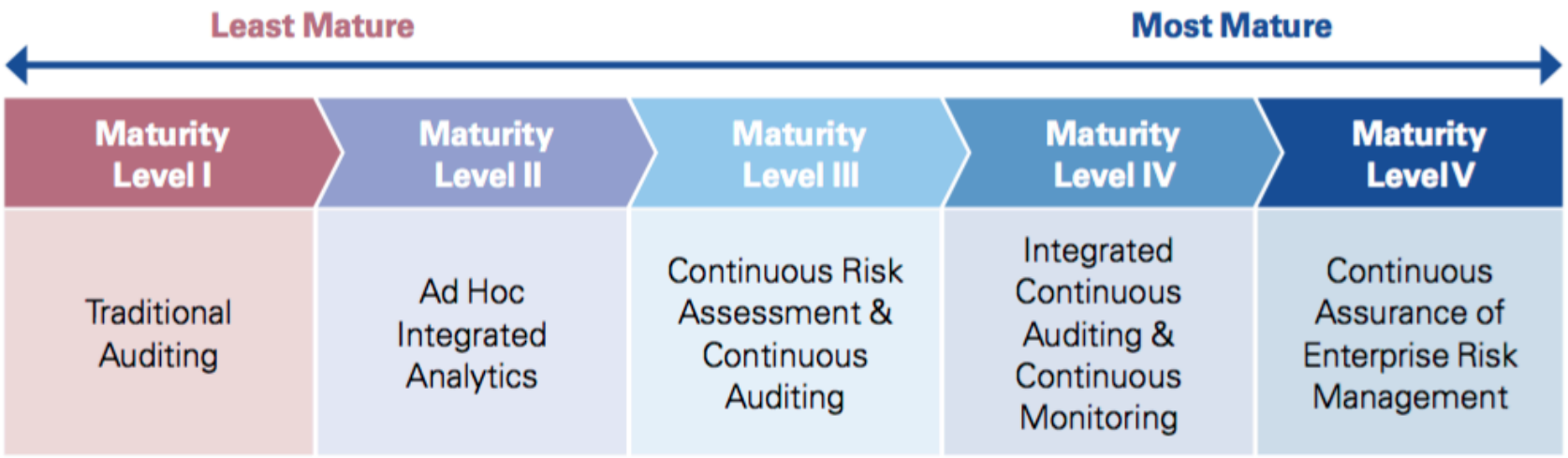


deforestation: https://www.flickr.com/photos/foreignoffice/3509228297

Security Governance Transparency via Continuous Improvement

An overview of maturity levels

The maturity model below represents the stages of maturity from the least mature state of traditional auditing through to the most mature state of continuous assurance of enterprise risk management.

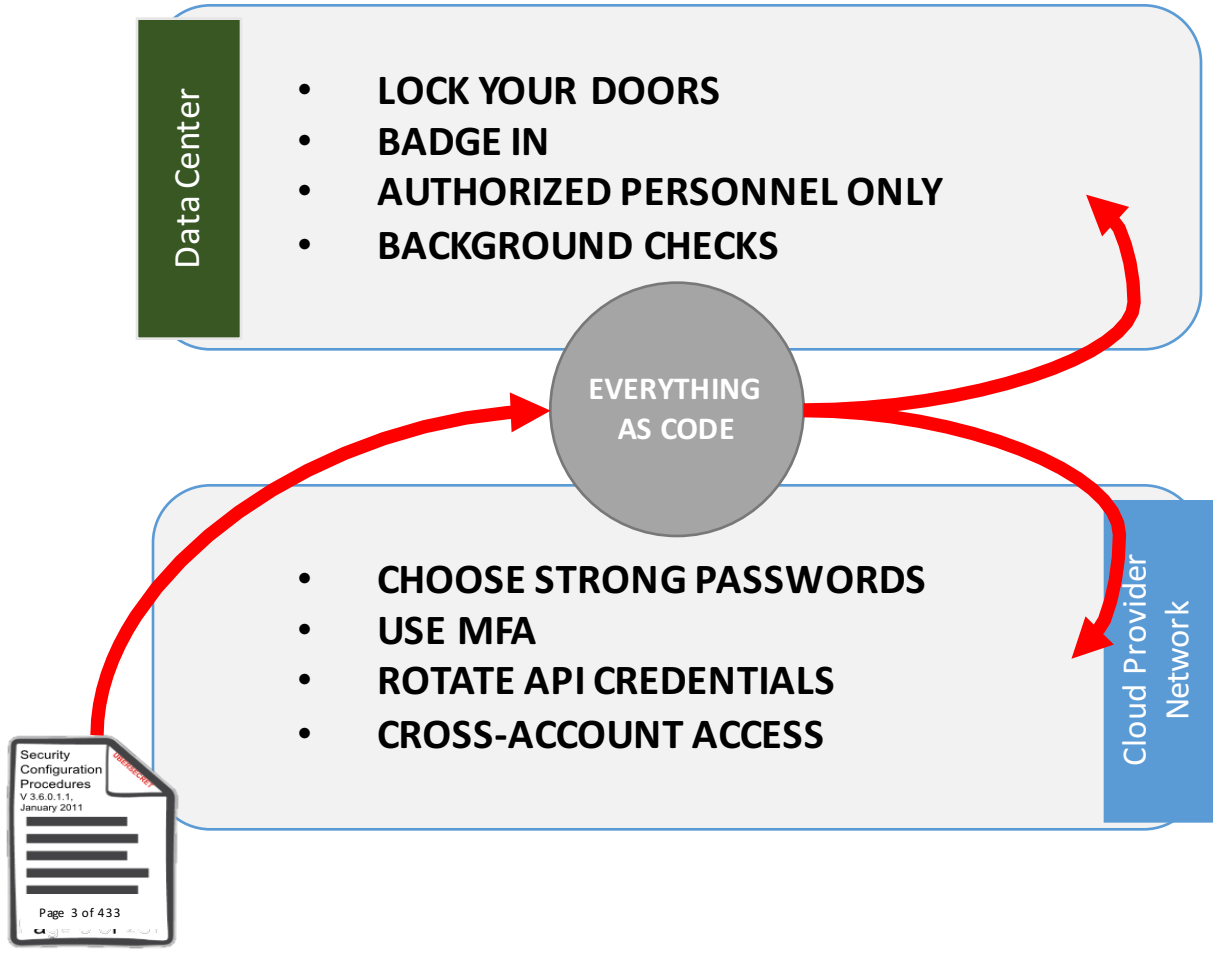


[1] Continuous Assurance is a progressive shift in audit practices towards the maximum possible degree of audit automation as a way of taking advantage of the technological basis of the modern entity in order to reduce audit costs and increase audit automation. Given the emphasis on the transformation of the entire system of auditing, the development of Continuous Assurance requires a fundamental rethink of all aspects of auditing, from the way in which data is made available to the auditor, to the kinds of tests the auditor conducts, how abnormalities are dealt with, what kinds of reports are issued, how often and to whom they are issued, and many other factors, the importance of some of which will only become apparent as Continuous Assurance is implemented.
"Continuous Assurance for the Now Economy", Rutgers Business School, February 2010.

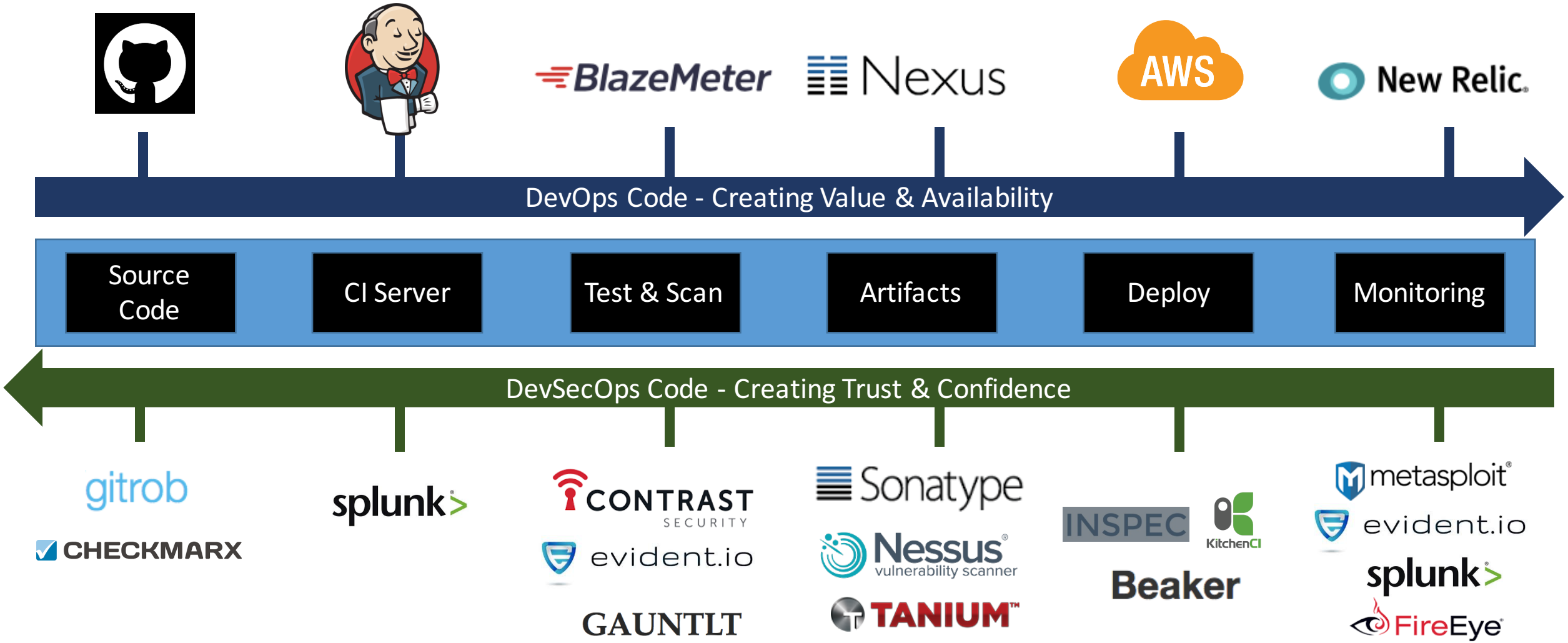
https://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Transforming-Internal-Audit.pdf

Security as Code / Everything as Code

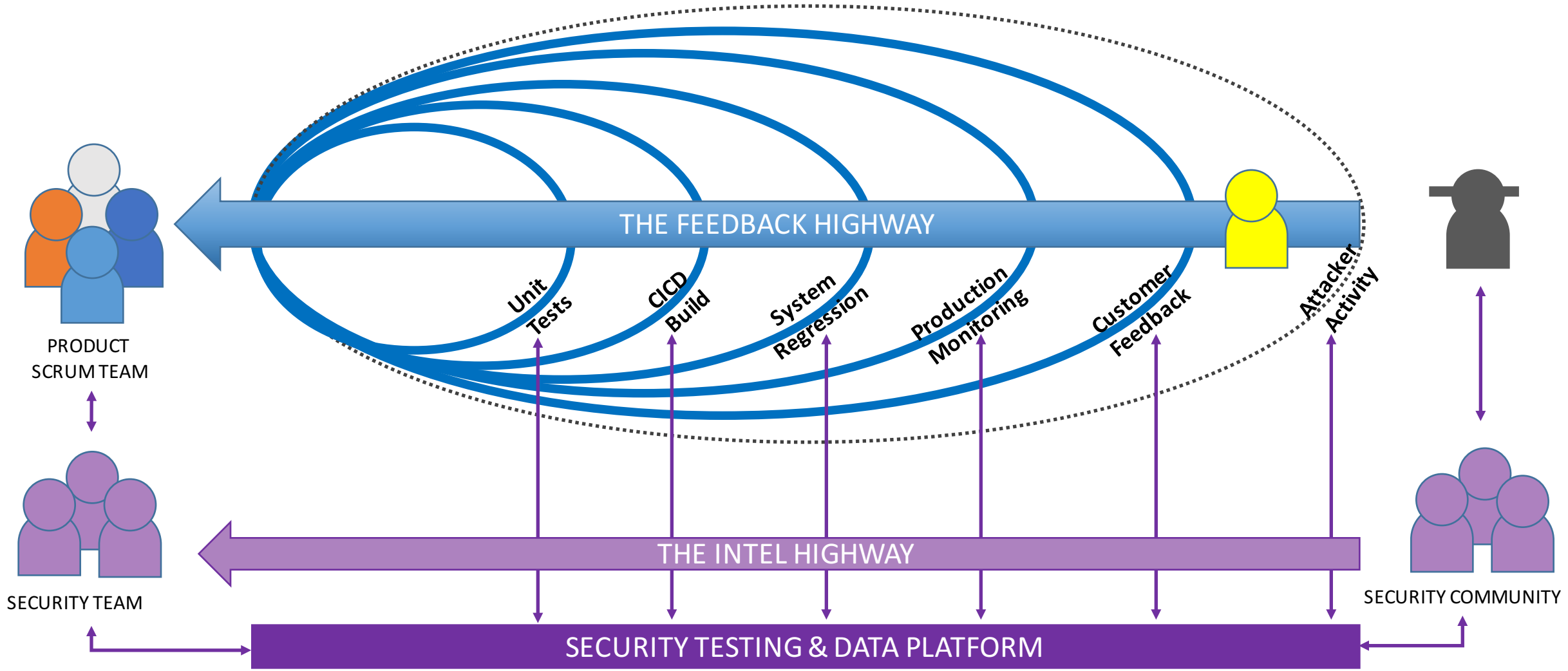
- Paper-resident policies do not stand up to constant cloud evolution and lessons learned.
- Translation from paper to code and back can lead to serious mistakes.
- Traditional security policies do not 1:1 translate to Full Stack deployments.



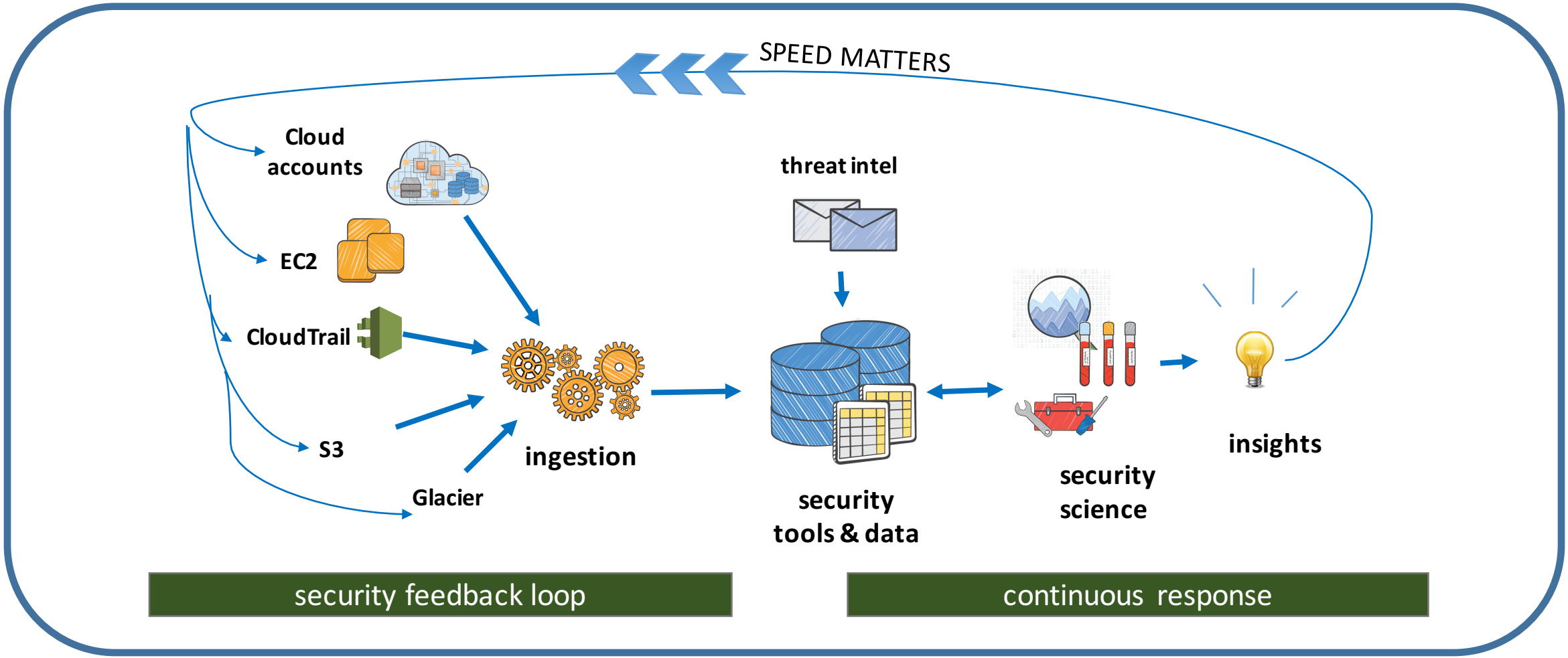
Example of Continuous Delivery + Security



Continuous Feedback

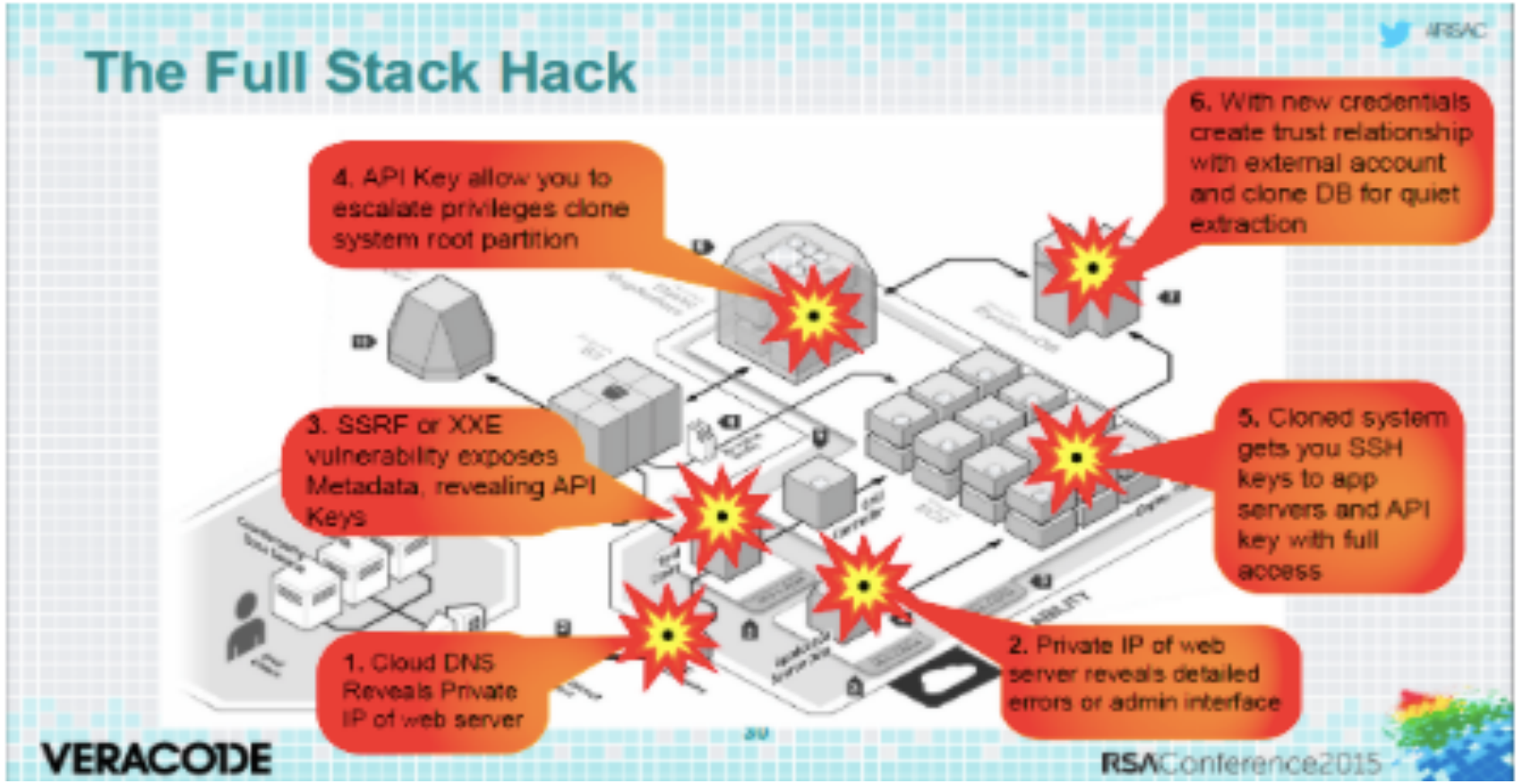


Continuous Security Engineering & Science



Monitor & Inspect Everything

Red Team, Security Operations & Science



API KEY EXPOSURE -> 8 HRS

DEFAULT CONFIGS -> 24 HRS

SECURITY GROUPS -> 24 HRS

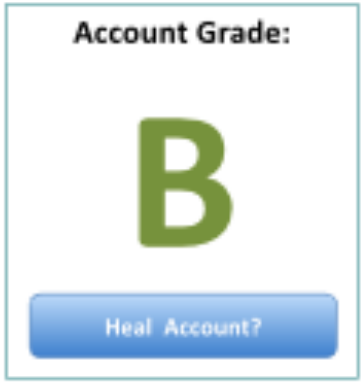
ESCALATION OF PRIVS -> 5 D

KNOWN VULN -> 8 HRS

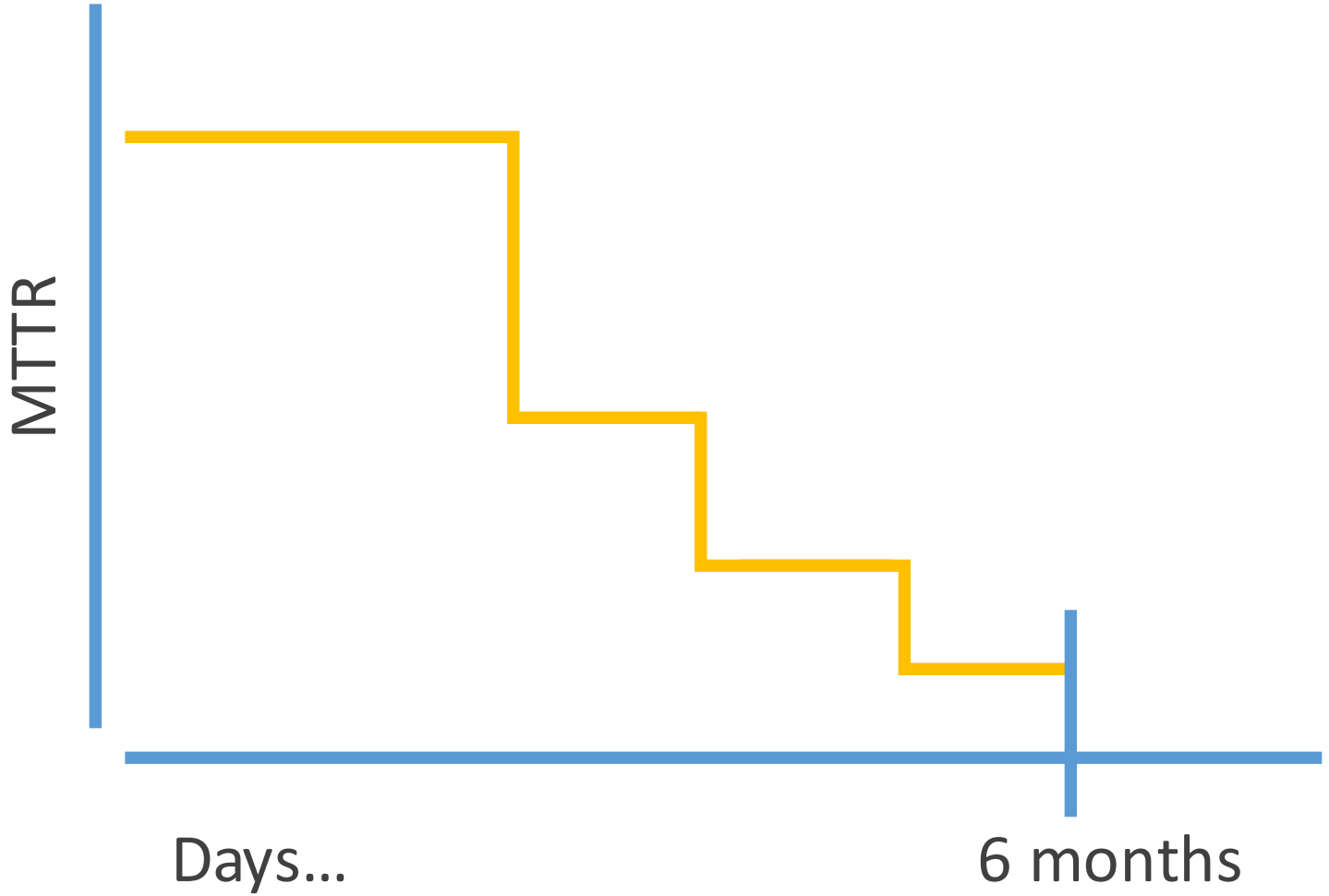
Security Decision Support

		On-Prem	Partial On-Prem	Outsource w/ No Indemnif.	Outsource w/ Part.Indemnif.	Outsource w/ Full Indemnif.
Who is responsible?	INTERNAL	You	You	You	You + Partner	Partner
Which minimal controls are needed?		Physical Security; Secure Handling & Disposal	File or Object Encryption for Sensitive Data; Physical Security; Secure Handling & Disposal	File or Object Encryption for Sensitive Data; Partner Security; SOC Attestation	File or Object Encryption for Sensitive Data; Partner Security;	Partner Security Controls; SOC Attestation
Where does data transit and get stored?		company "owned" data center or co-location	any compute & transit; data stored on-prem	public cloud; free services		
What are the innovation benefits?		reduced latency; search sensitive data	speed; reduced friction; search sensitive data	speed; reduced friction; evolving patterns; community		
What are the potential risks?		SQL Injection; Internal Threats; Mistakes; Phishing; Increased Friction; Slow	Latency; SQL Injection; Internal Threats; Mistakes; Phishing; Increased Friction; Slow	Inability to Search Sensitive Data; SQL Injection; Internal Threats; Mistakes; Phishing; Govt. Requests Unknown; Reduced Financial responsibility		

```
begin
  (iam.client.list_role_policies(:role_name => role)[:policy_names]\
      - roledb.list_policies(role)).each do |policy|
  log.warn("Deleting Policy \"#{policy}\", which is not part of the approved baseline.")
  if policydiff("{}",
   URI.decode(iam.client.get_role_policy(\
     :role_name => role,
     :policy_name => policy
   )[:policy_document]),
   {:argv => ARGV, :diff => options.diff})
  end
  options.dryrun ? nil : \
   iam.client.delete_role_policy(
     :role_name => role,
     :policy_name => policy
   )
```



This Could Be Your Mean Time to Resolution…



Get Involved and Join the Community

- devsecops.org
- @devsecops on Twitter
- DevSecOps on LinkedIn
- DevSecOps on Github
- RuggedSoftware.org
- Compliance at Velocity