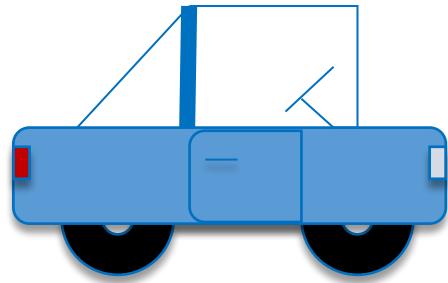
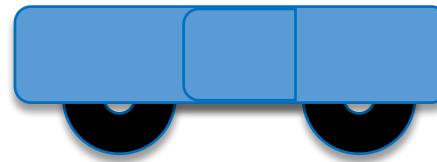


<- SHIFTING SECURITY TO THE LEFT

A DEVSECOPS JOURNEY

SHANNON LIETZ (@devsecops)

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

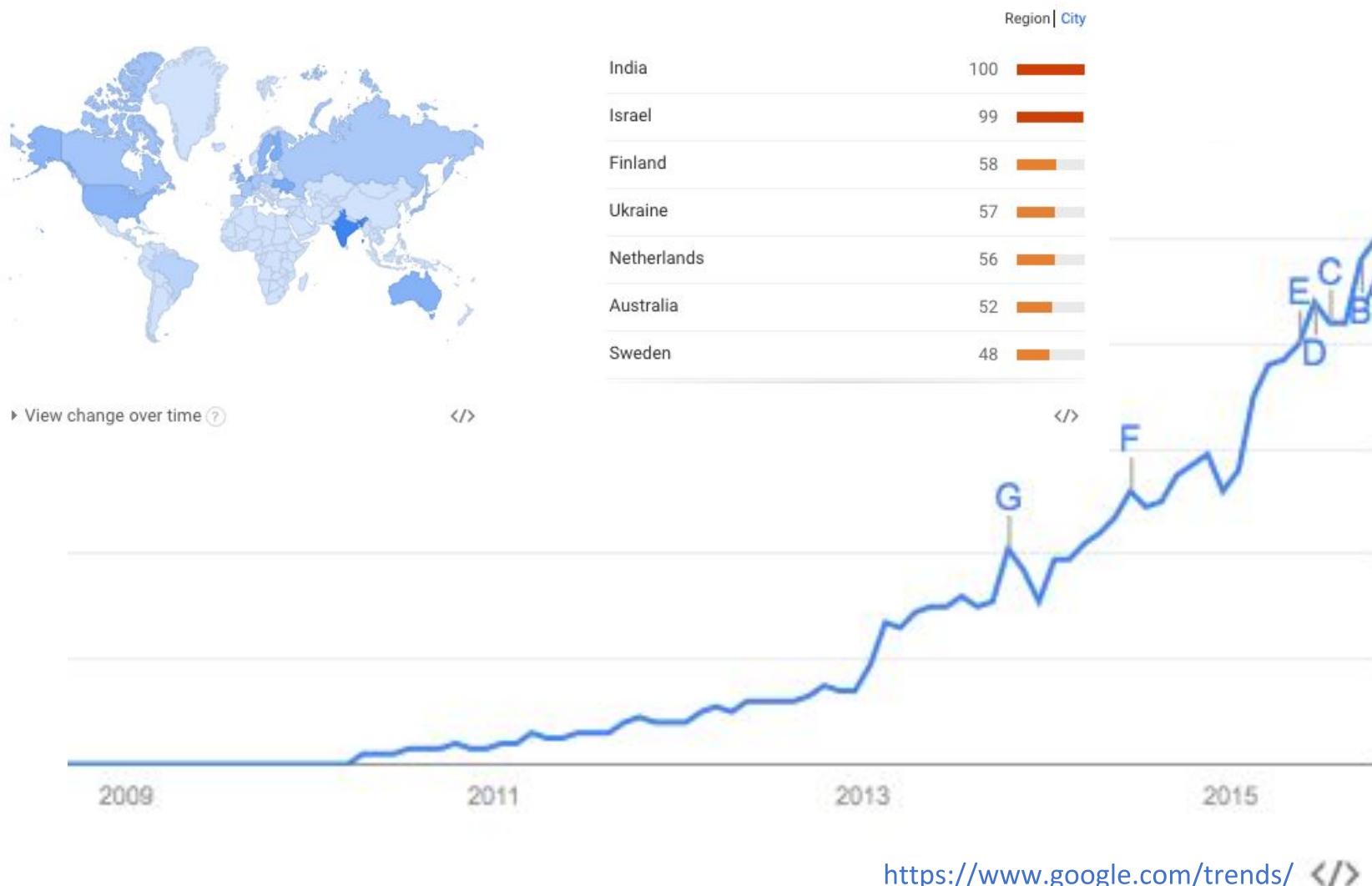
This Same Process Applied to Software...



BANG
HEAD
HERE

Now Trending...

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



GLOBAL CALL FOR CHANGE...

Who's doing Enterprise DevOps?



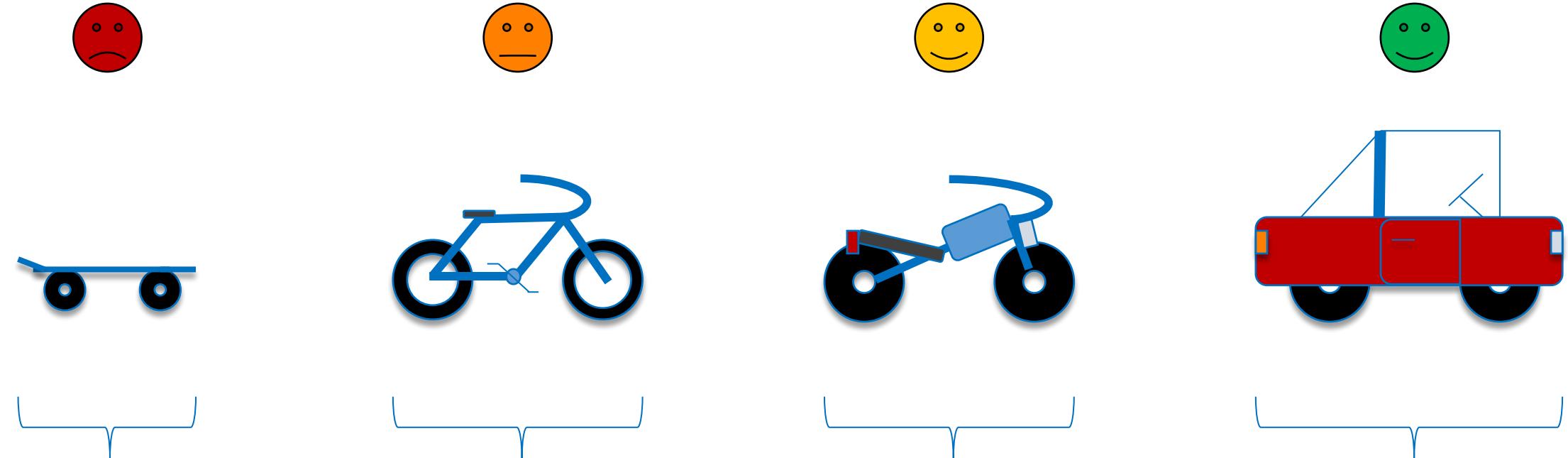
intuit.



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.

A Customer Centric Supply Chain is Born...



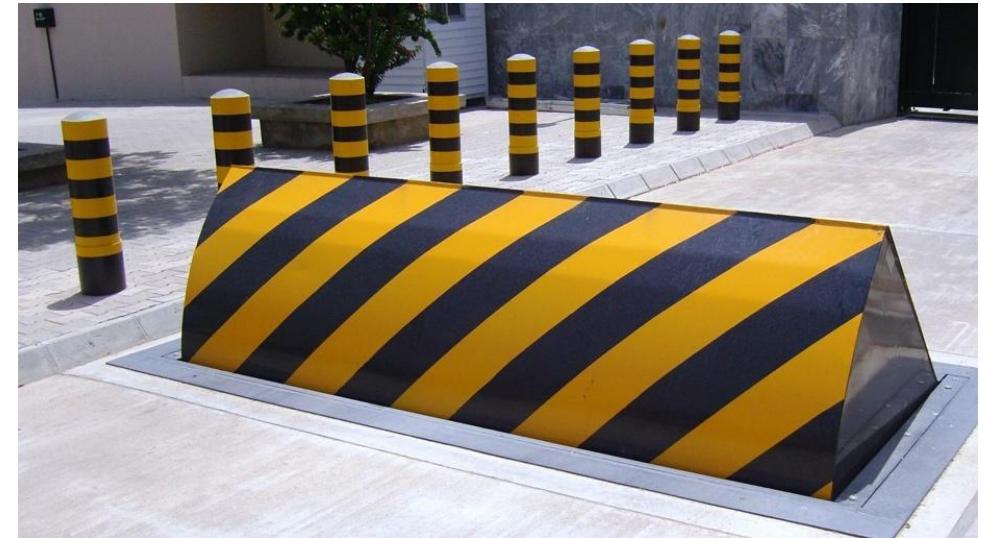
Security must shift left with a Science Mindset like all other Ops...

Thanks to Henrik Kniberg

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)
- ...

350. Centralization vs. De-centralization



Say What??!!

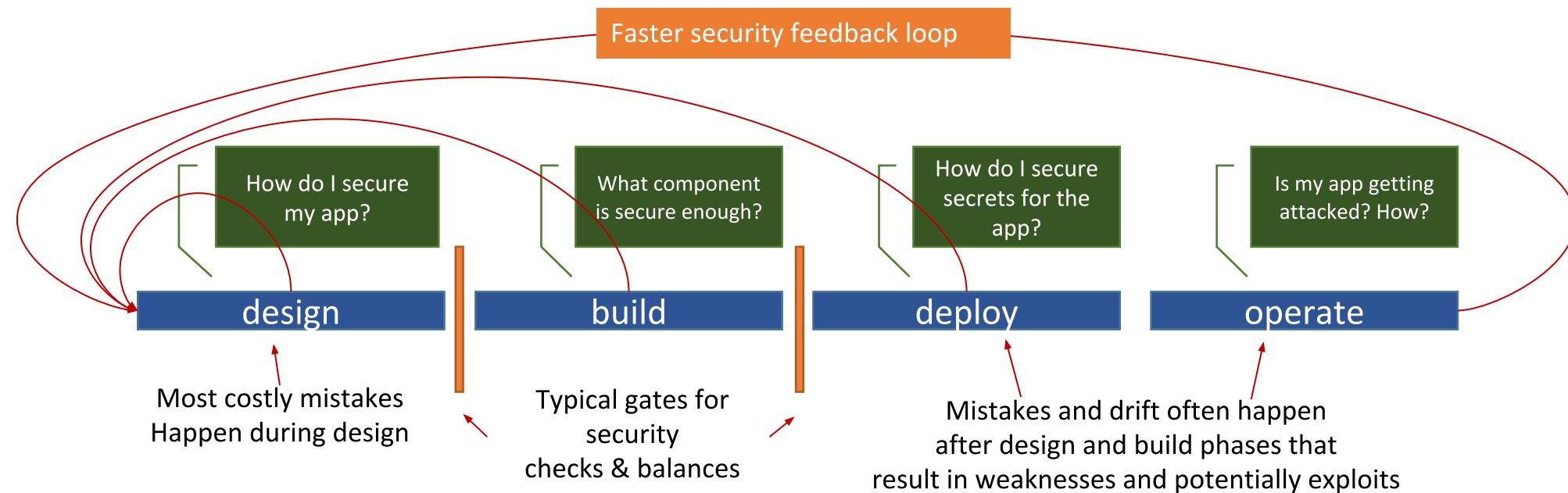
***“THIS IS THE END
OF SECURITY AS
WE KNOW IT...”***

- Josh Corman

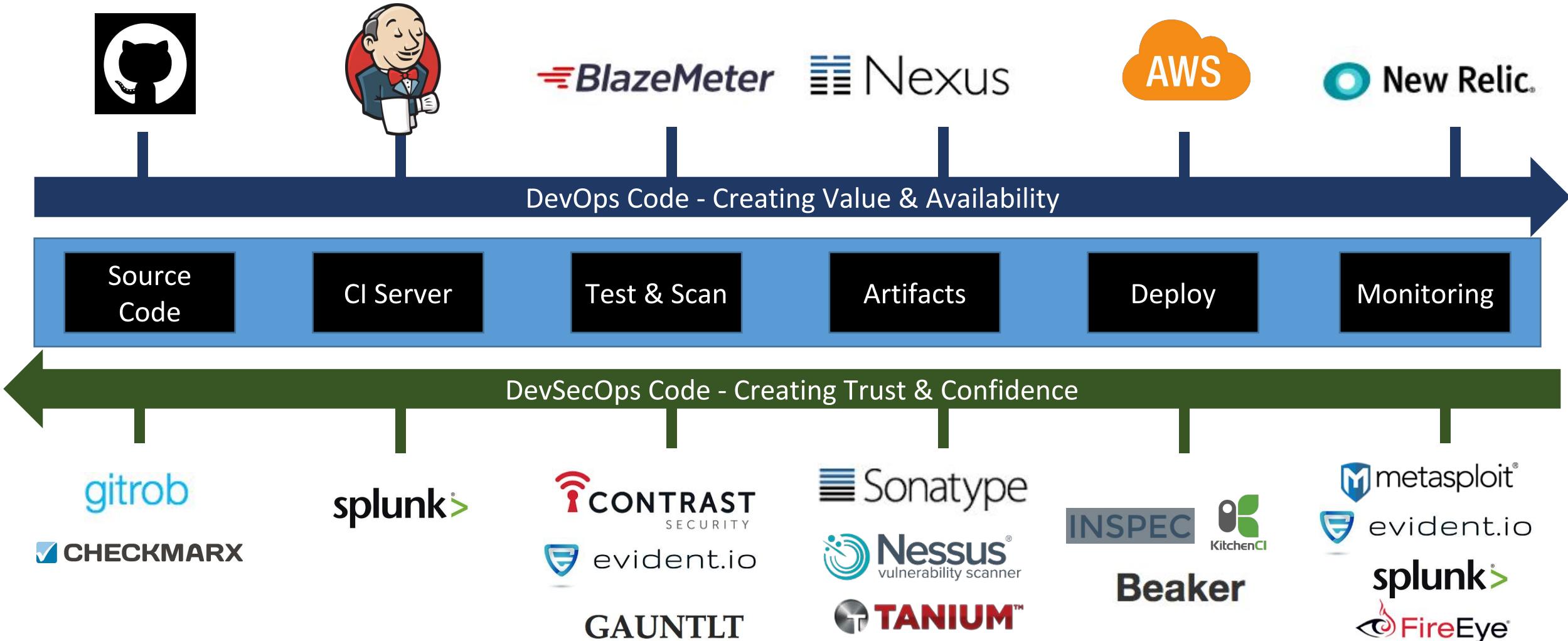
<http://donsmaps.com/images22/mutta1200.jpg>

Analyzing a Typical Secure Software Supply Chain

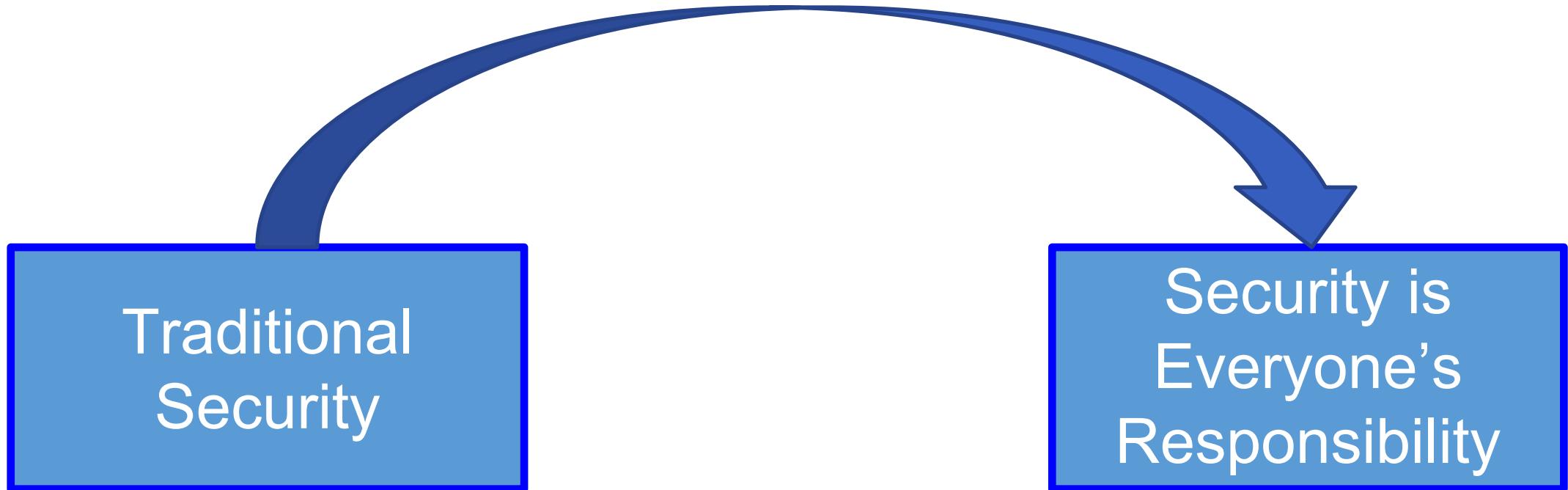
- Gating processes are not Deming-like
 - Security is a design constraint
 - Decisions made by engineering teams
- Hard to avoid business catastrophes by applying one-size-fits-all strategies
 - Security defects is more like a security “recall”



Example of Continuous Delivery + Security Pipeline



Culture Hacking



DEVSECOPS

The Art of DevSecOps

DevSecOps

Security
Engineering

Security
Operations

Compliance
Operations

Security
Science

Experiment,
Automate, Test

Hunt, Detect,
Contain

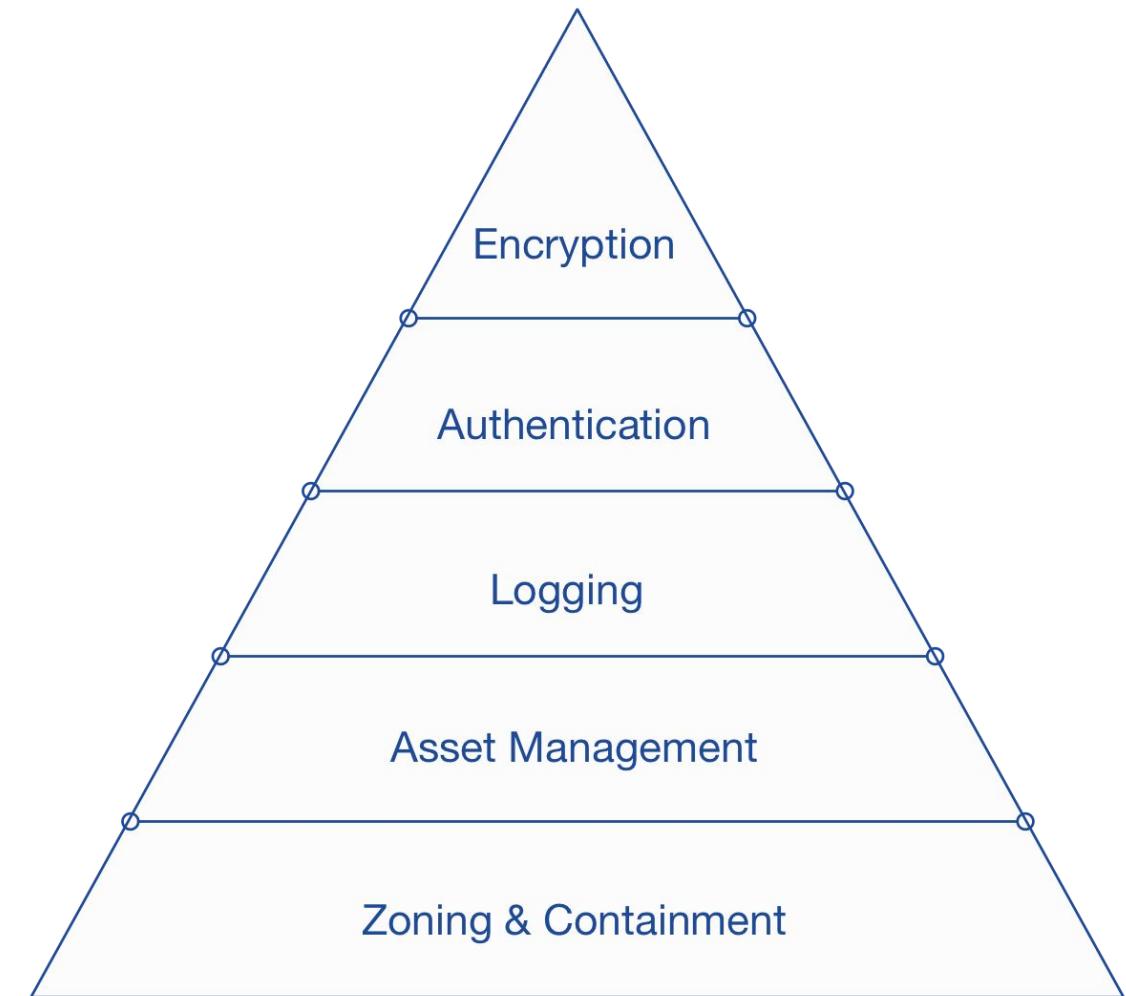
Respond,
Manage, Train

Learn, Measure,
Forecast

Security is and always has been a Design Constraint... It must get built-in to be effective...

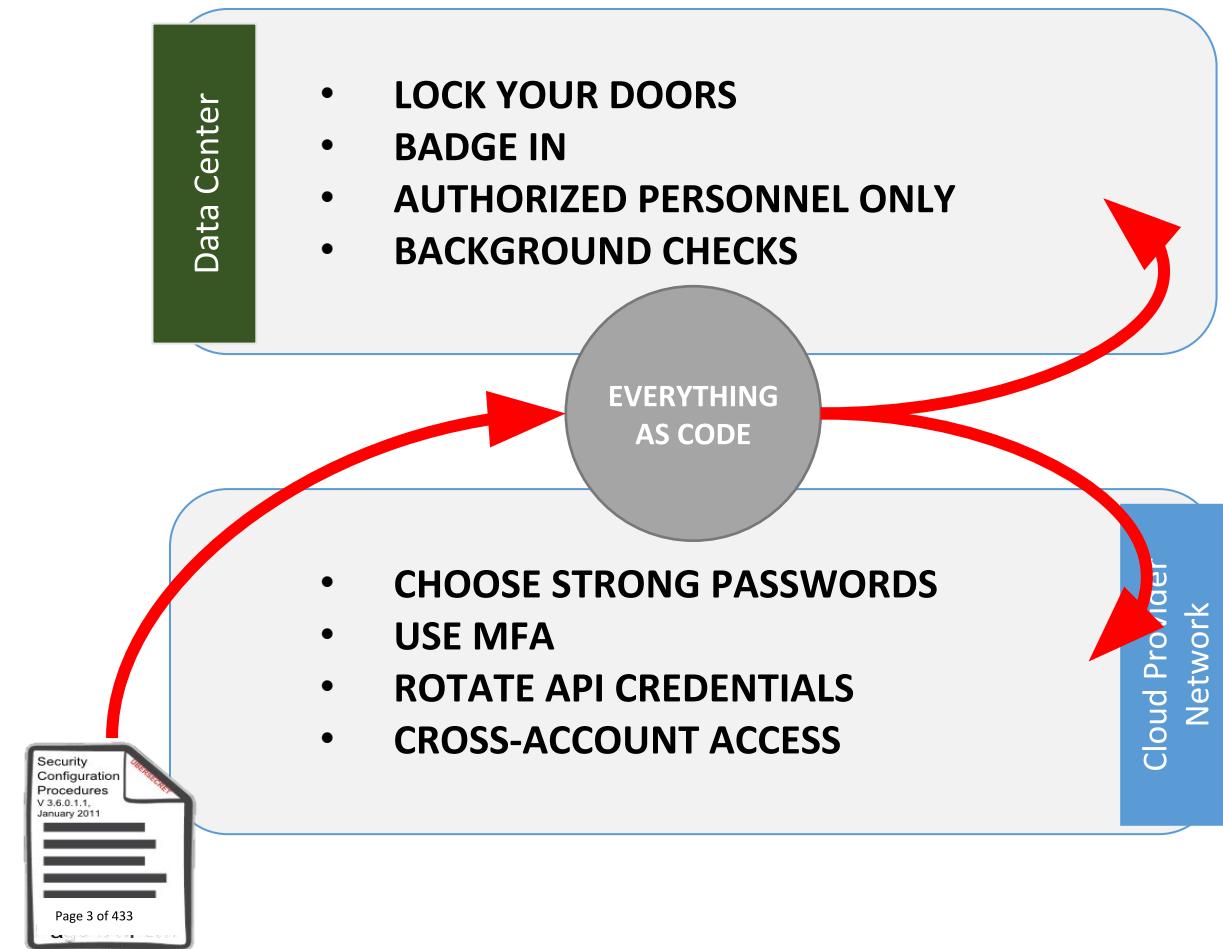
- Everyone knows Maslow...
- If you can remember 5 things, remember these ->

“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...”

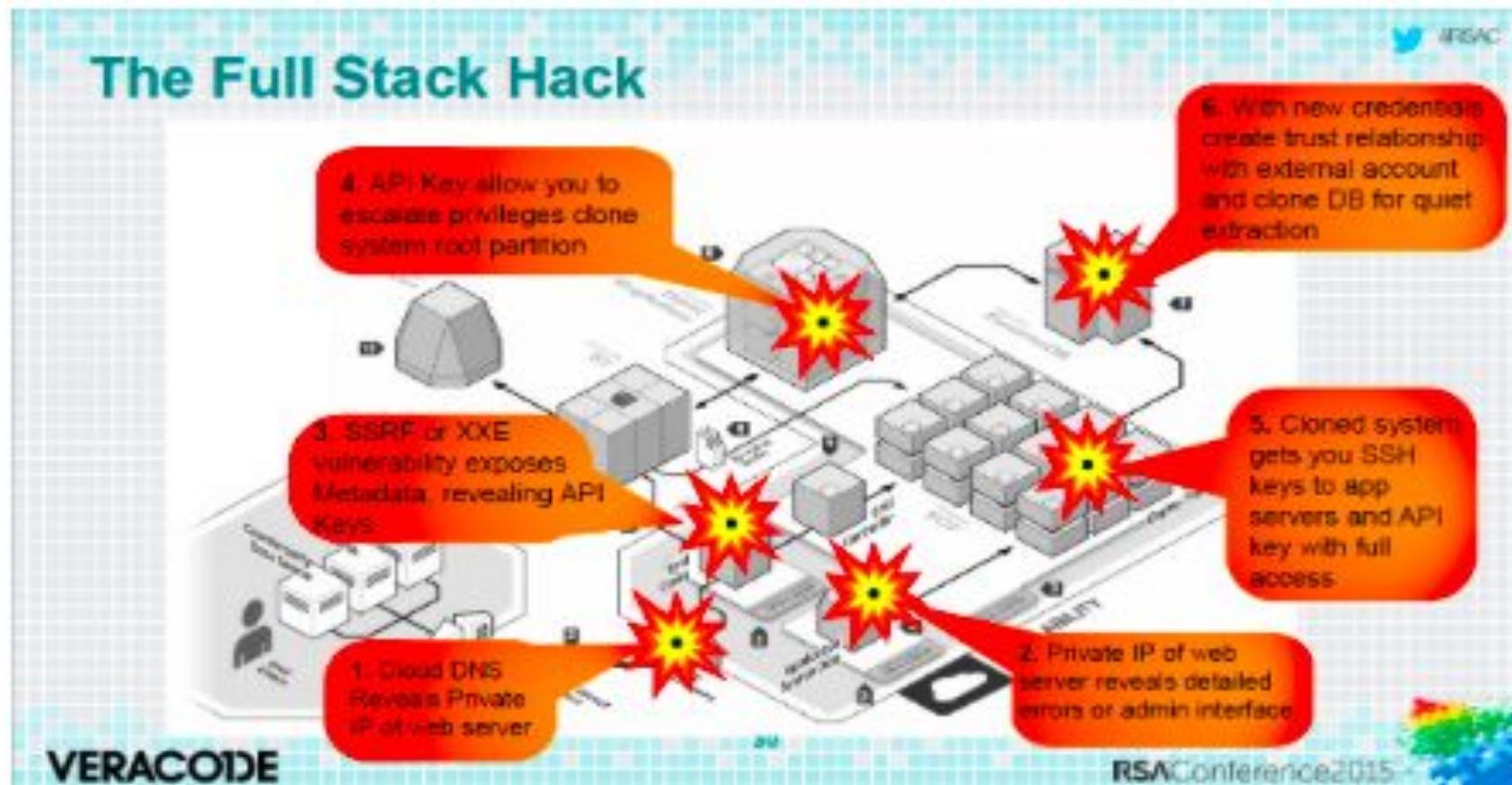


Security as Code / Everything as Code

- 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.



Red Team, Security Operations & Science



API KEY EXPOSURE -> 8 HRS

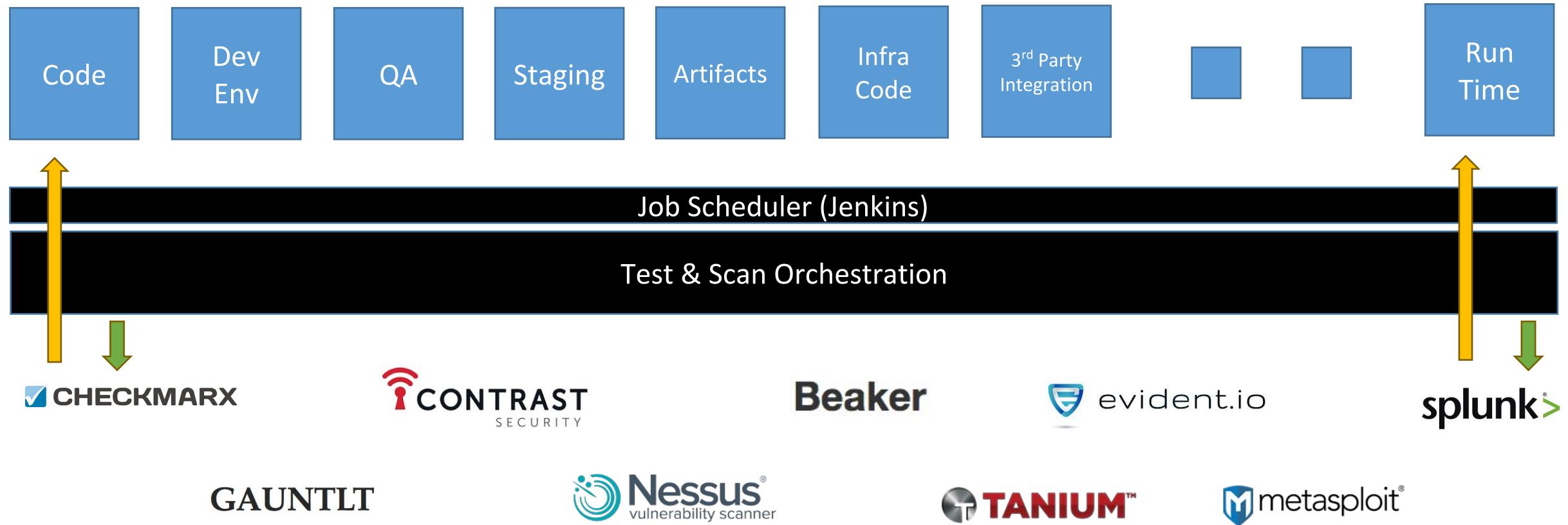
DEFAULT CONFIGS -> 24 HRS

SECURITY GROUPS -> 24 HRS

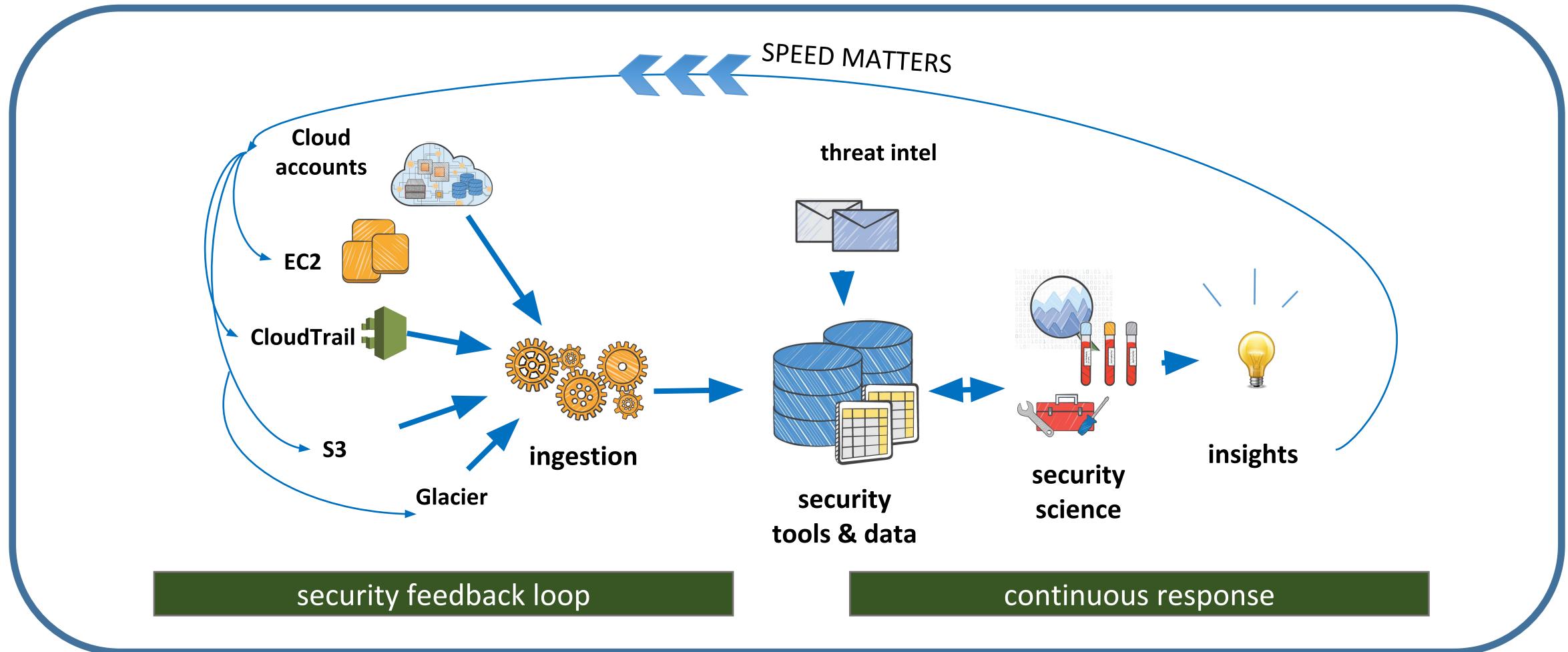
ESCALATION OF PRIVS -> 5 D

KNOWN VULN -> 8 HRS

Automated Testing and Inspection in CICD

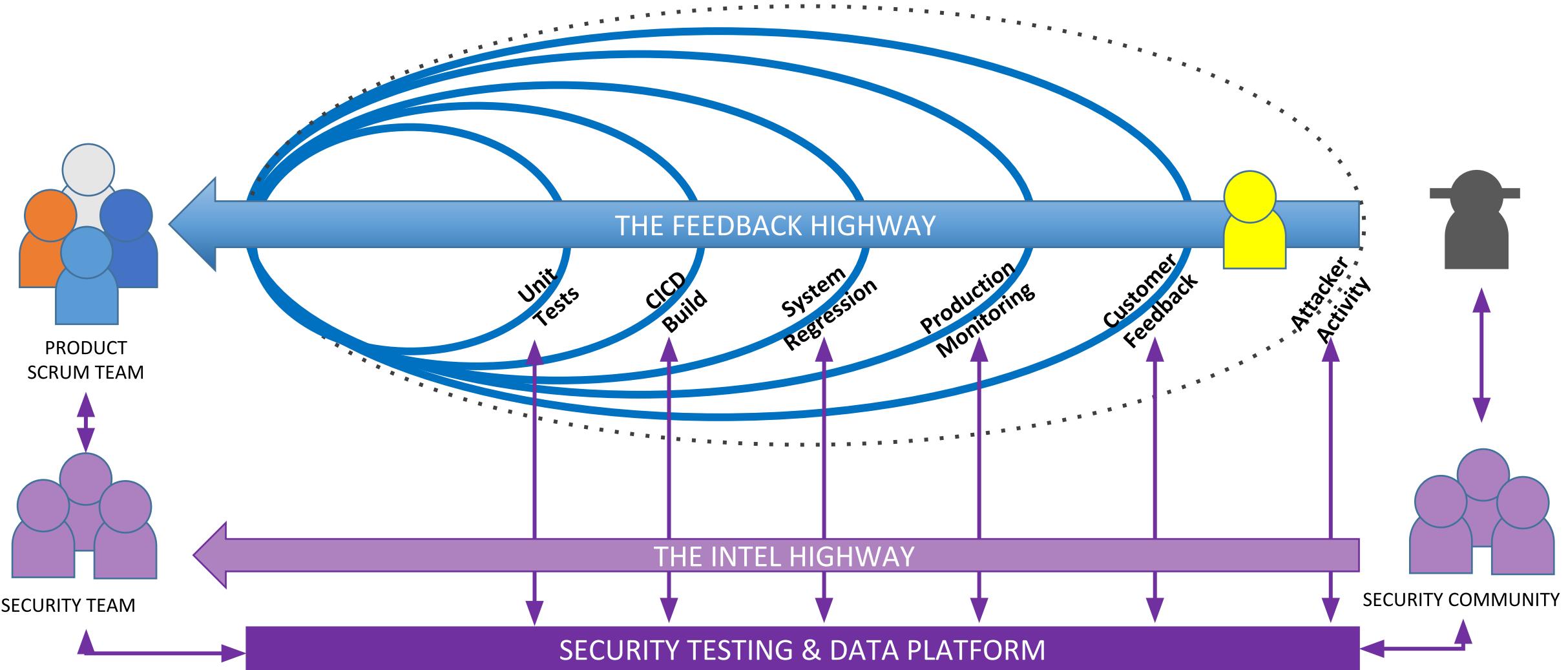


Continuous Security Engineering & Science

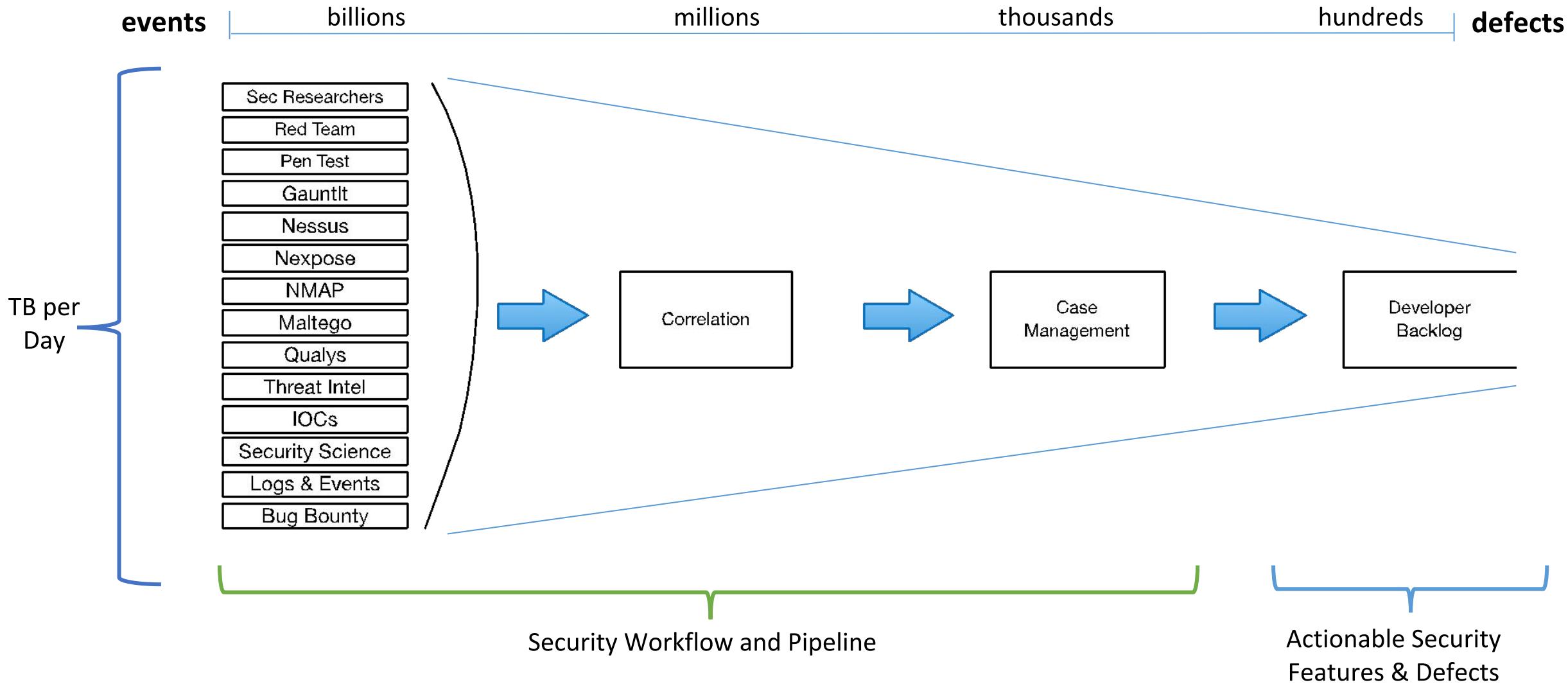


Monitor & Inspect Everything

Continuous Feedback



The Security Funnel – The Quest for High Fidelity Feedback



Security Decision Support

	On-Prem	Partial On-Prem	Outsource w/ No Indemnif.	Outsource w/ Part.Indemnif.	Outsource w/ Full Indemnif.	
Who is responsible?	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			

INTERNAL

```

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

```

Account Grade:

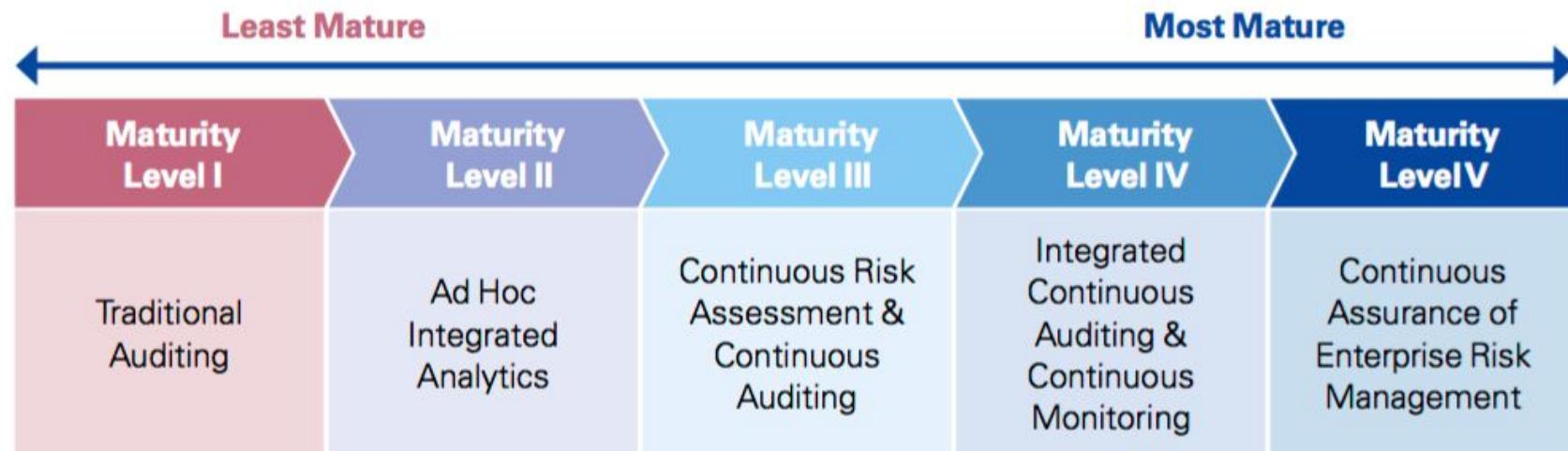
B

[Re-Grade Account?](#)

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.

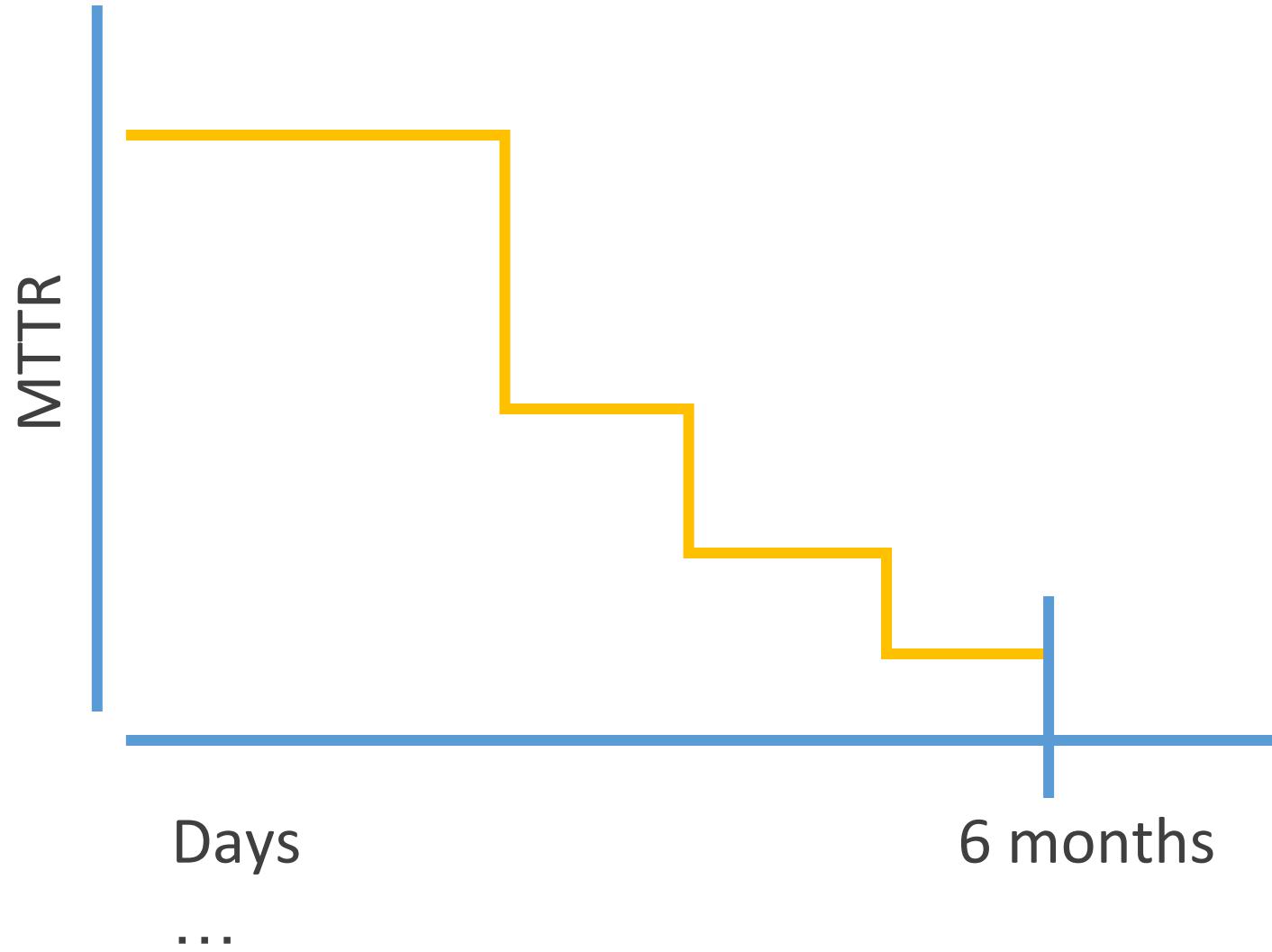


¹ Continuous Assurance is a progressive shift in audit practices towards the maximum possible degree of audit automation as a way of taking advantage of the technological basis of the modern entity in order to reduce audit costs and increase audit automation. Given the emphasis on the transformation 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 New Economy," Rutgers Business School, February 2010.

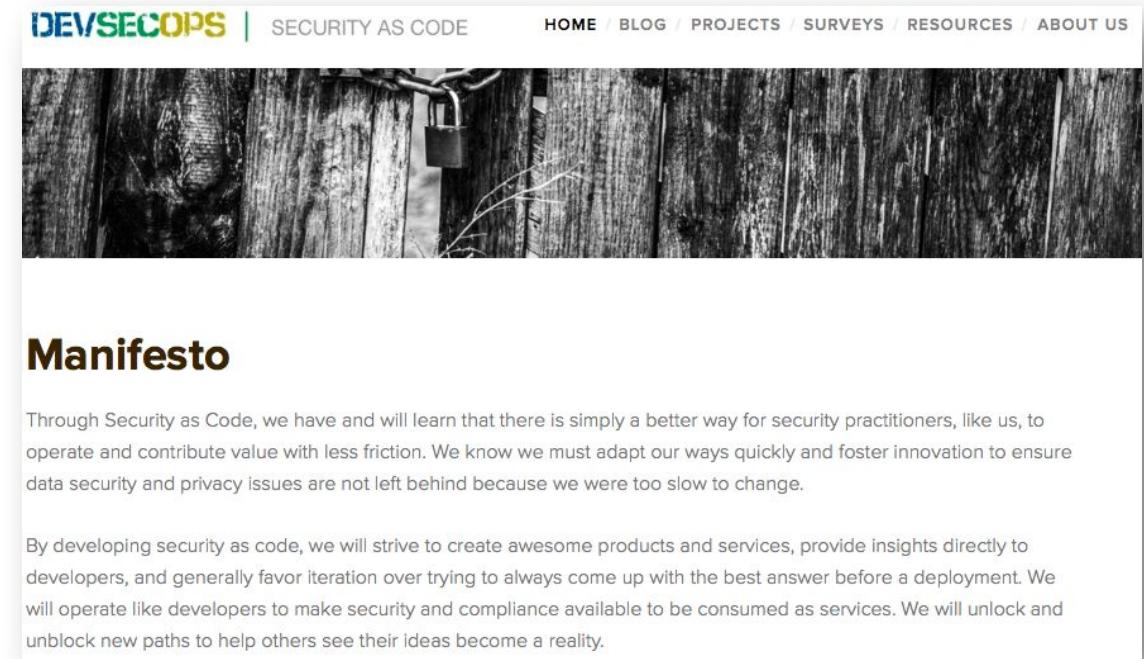
<https://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Transforming-Internal-Audit.pdf>

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
- ...



The screenshot shows the DEVSECOPS website. At the top, there is a navigation bar with links to HOME, BLOG, PROJECTS, SURVEYS, RESOURCES, and ABOUT US. Below the navigation bar is a large black and white photograph of a wooden fence with a padlock on it. To the left of the image, the word "DEVSECOPS" is written in its signature blue and green logo, followed by the text "SECURITY AS CODE". Below the image, the word "Manifesto" is centered in a bold, dark font. Underneath "Manifesto", there is a paragraph of text: "Through Security as Code, we have and will learn that there is simply a better way for security practitioners, like us, to operate and contribute value with less friction. We know we must adapt our ways quickly and foster innovation to ensure data security and privacy issues are not left behind because we were too slow to change." Another paragraph follows: "By developing security as code, we will strive to create awesome products and services, provide insights directly to developers, and generally favor iteration over trying to always come up with the best answer before a deployment. We will operate like developers to make security and compliance available to be consumed as services. We will unlock and unblock new paths to help others see their ideas become a reality."