The DevSecOps Playbook

from a Practitioner's Perspective

Shannon Lietz (@devsecops)

<me />

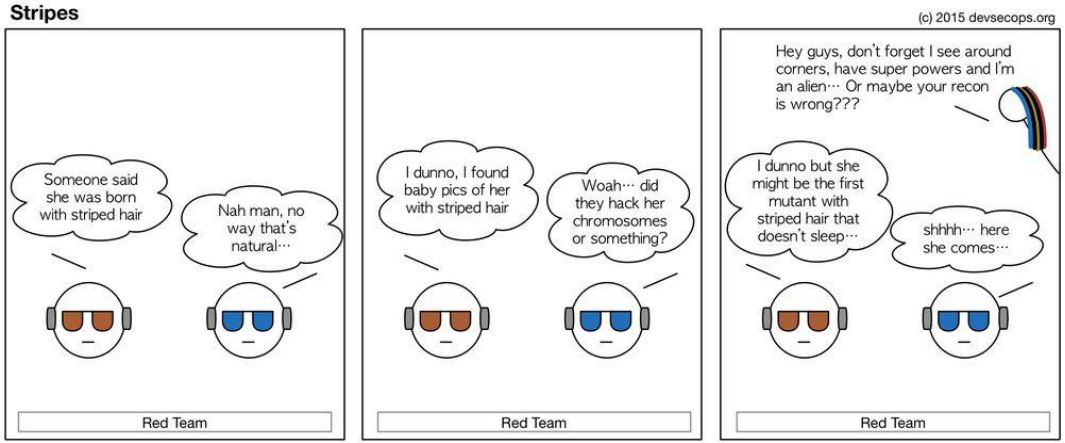
SAFER
SOFTWARE
SOONER

1984 1989 1996 2001 2011 PRESENT

DEVELOPER
SECURITY
OPERATIONS
"DEVSECOPS"
"RUGGED"

Take Responsibility.
Give Credit.

@seniorstoryteller

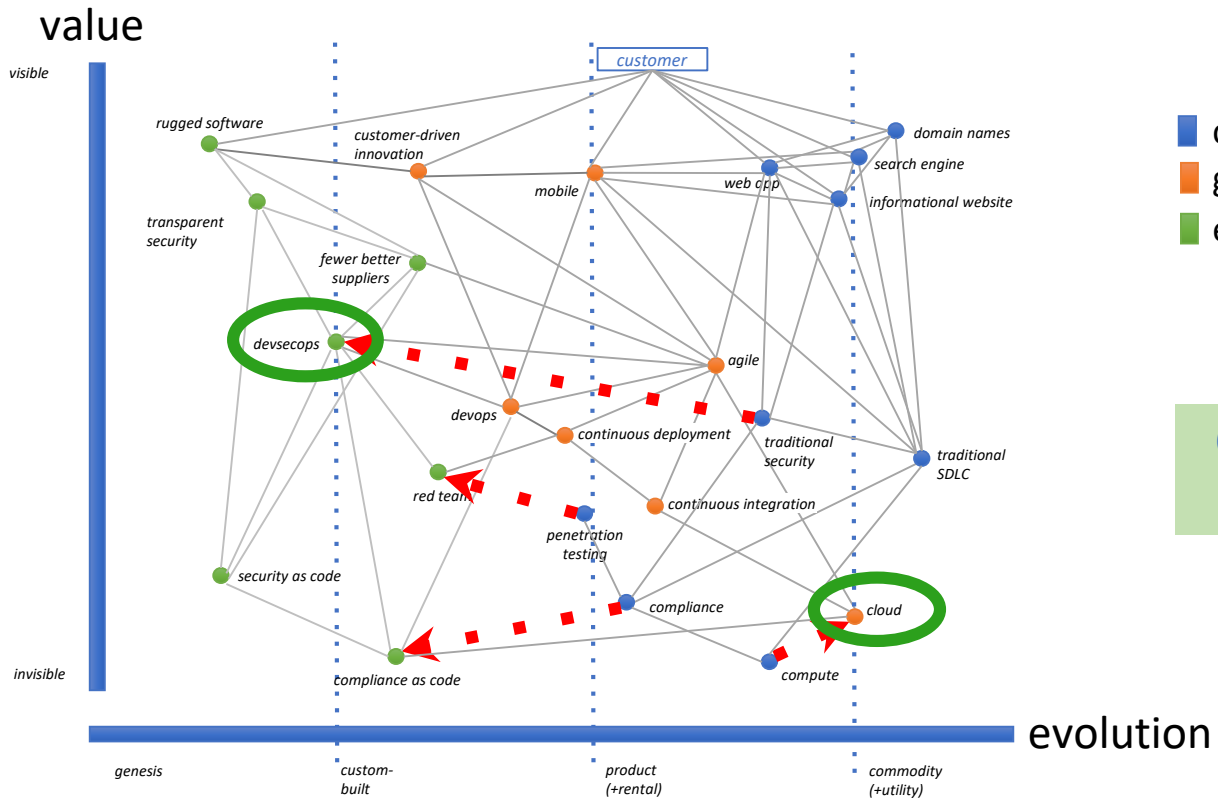


DEVSECOPS
-- FOUNDER --

HACKERGIRL
https://hackergirl.io

All Day DevOps

Why change?



- commodity bound
- growth
- emerging

Catching up takes commitment

First things first… Mindshare...

Leaning in over Always Saying “No”

Data & Security Science over Fear, Uncertainty and Doubt

Open Contribution & Collaboration over Security-Only Requirements

Consumable Security Services with APIs over Mandated Security Controls & Paperwork

Business Driven Security Scores over Rubber Stamp Security

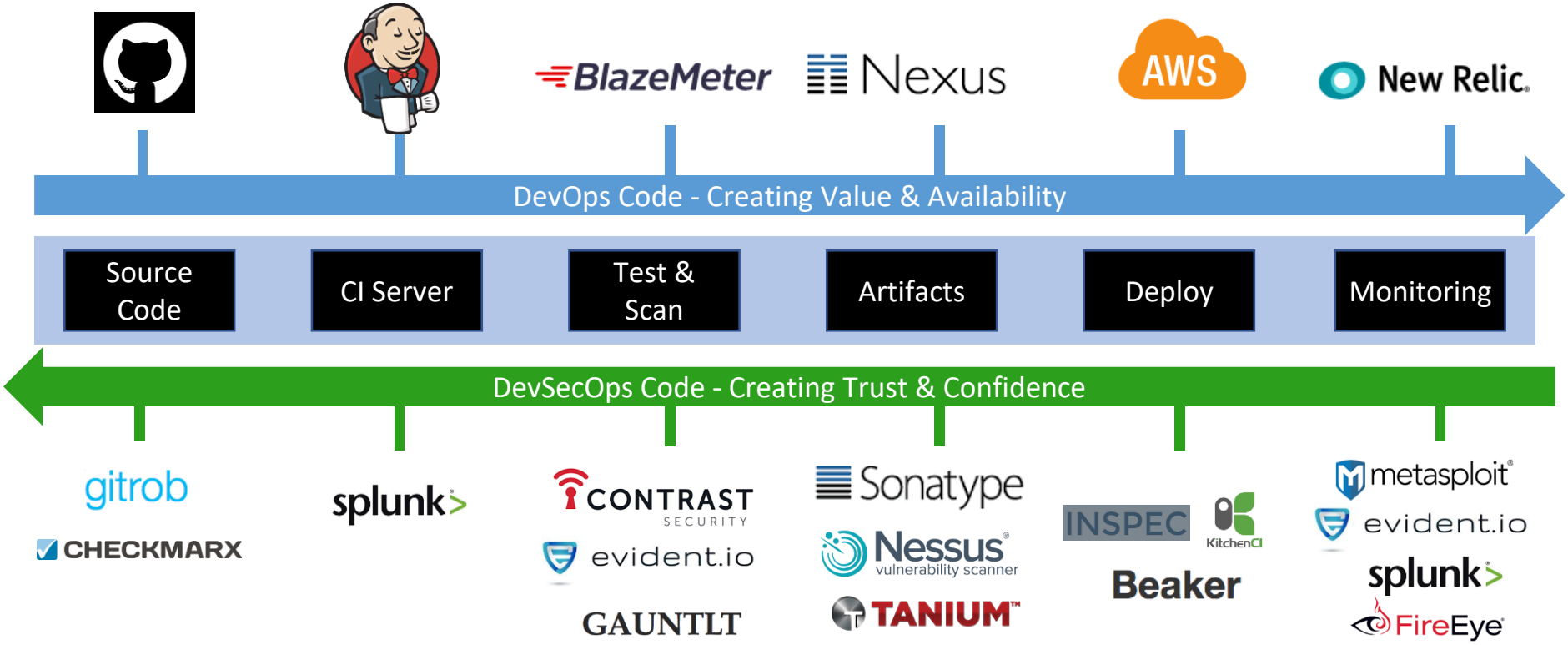
Red & Blue Team Exploit Testing over Relying on Scans & Theoretical Vulnerabilities

24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident

Shared Threat Intelligence over Keeping Info to Ourselves

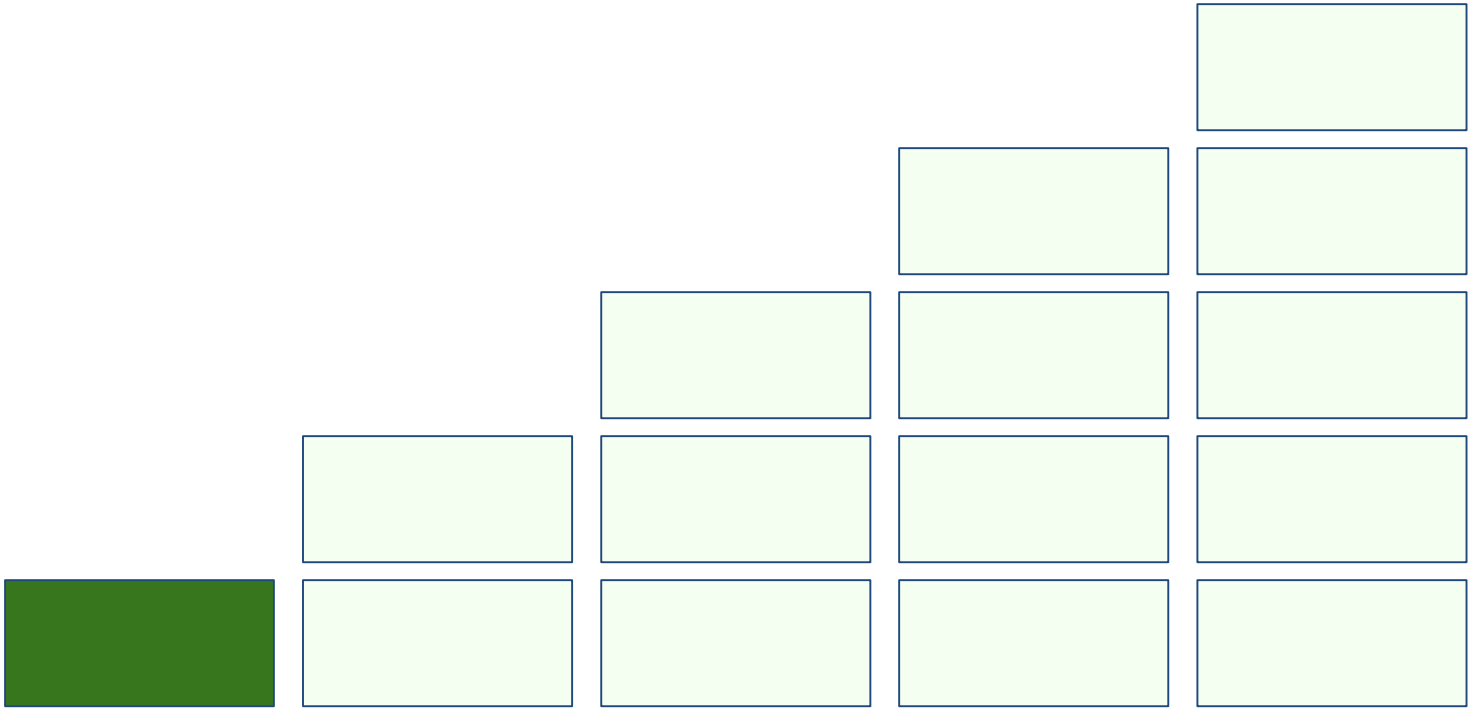
Compliance Operations over Clipboards & Checklists

How hard could it be?




BANG
HEAD
HERE

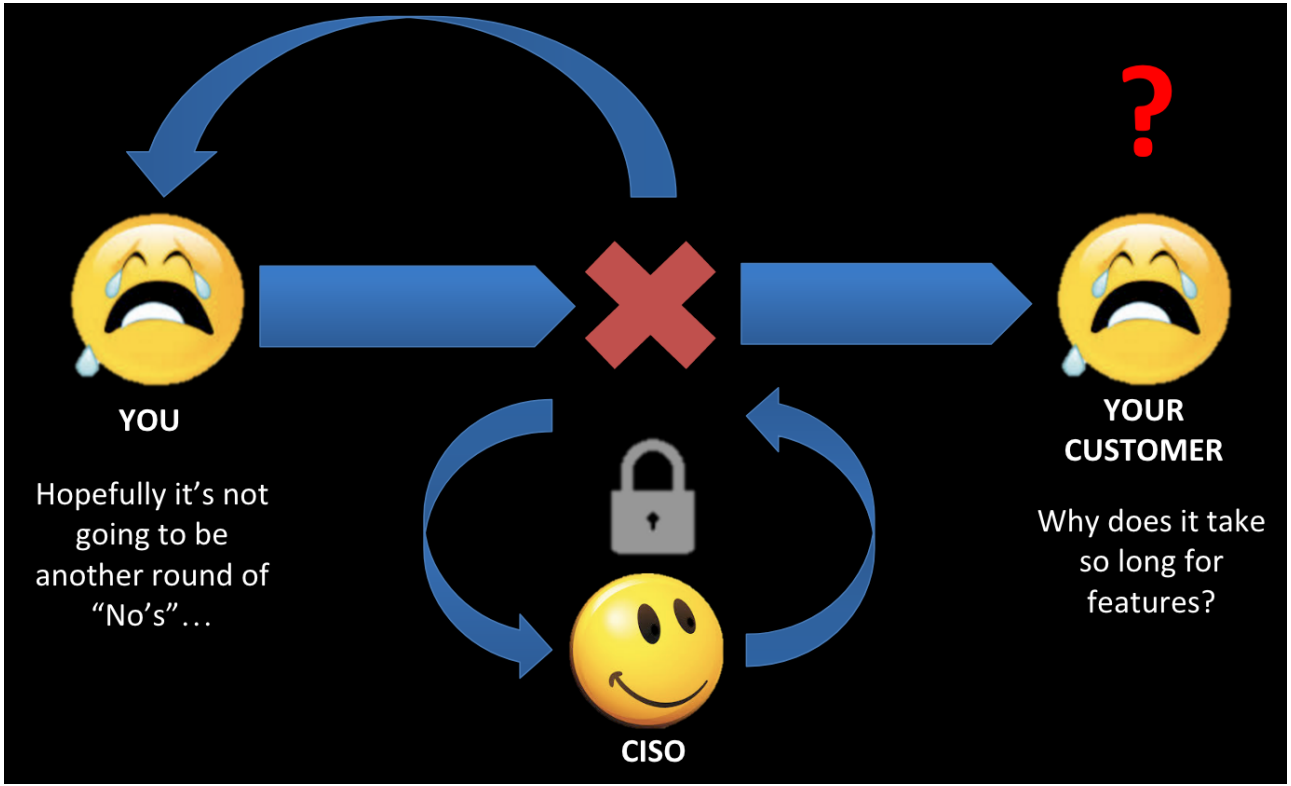
In the Beginning...



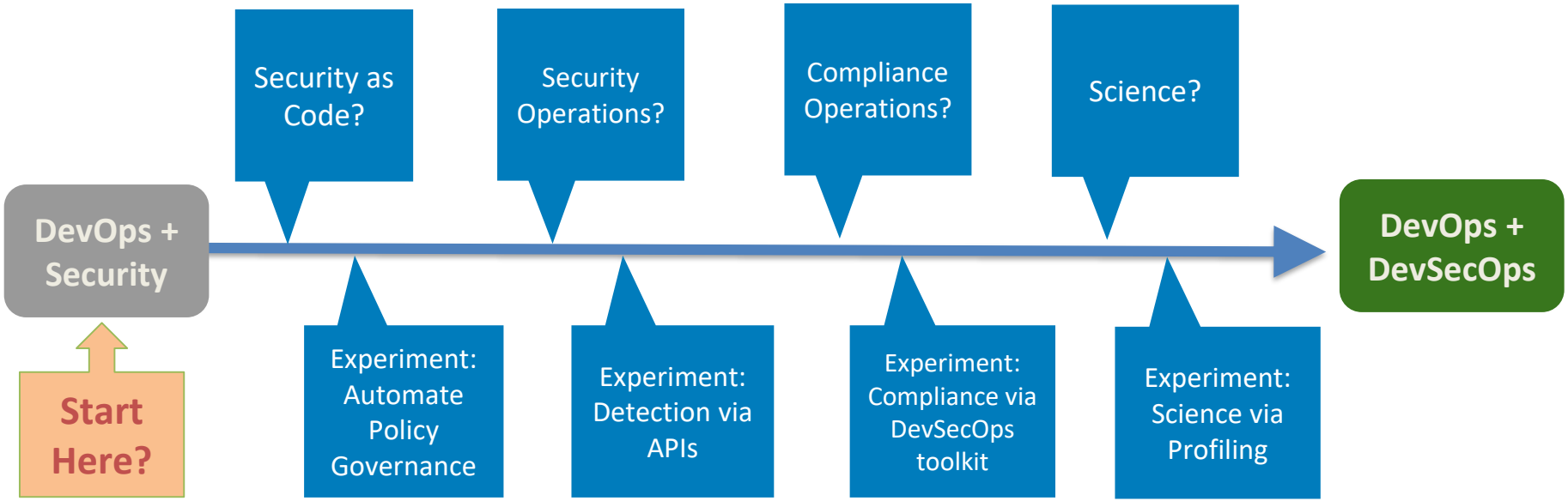
At Level 1, you are:

- Experiencing lots of friction with traditional process
- Finding it challenging to use checklists
- Worried about what needs to change
- Should invest in a few basic experiments
- Trying to figure out who to follow
- Red teaming...

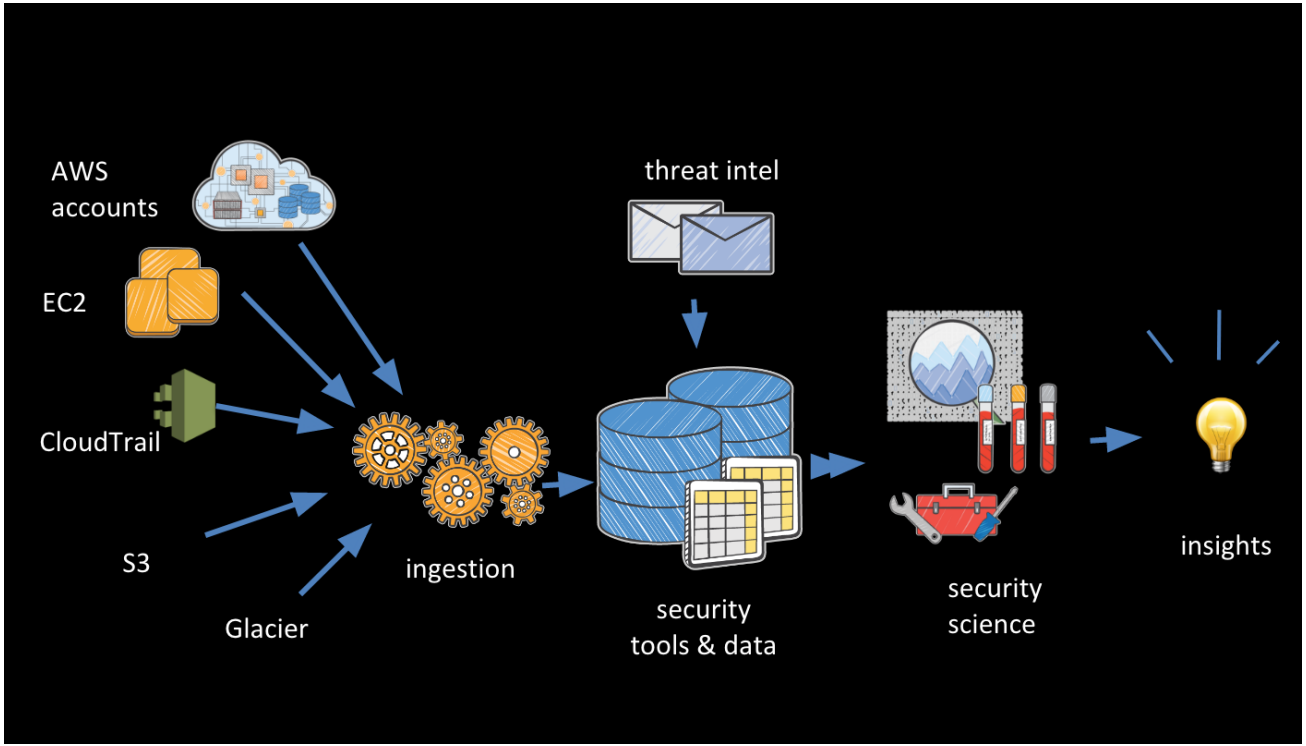
Losing faith in traditional security...



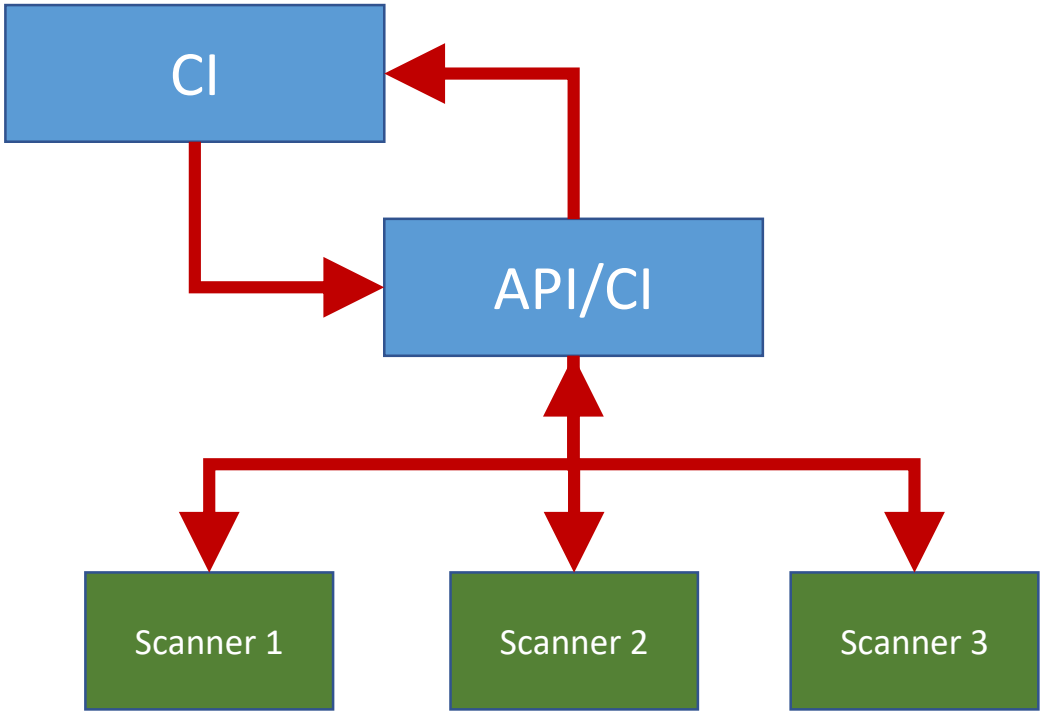
What are the changes?



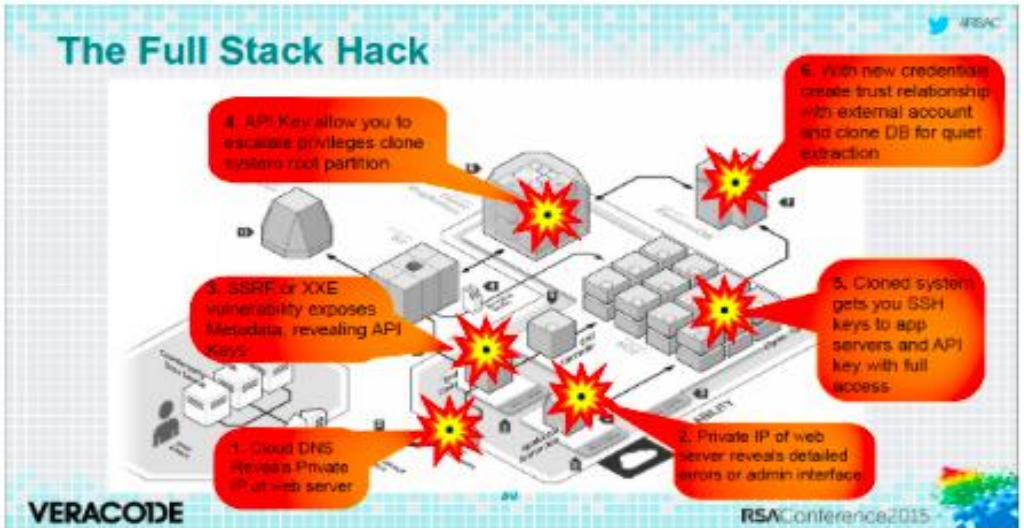
Attempting to use the cloud...



Investing in initial automation...



Woah… how do I communicate this?



API Key Exposure ->

8 hrs

Default Configs ->

24 Hrs

Security Groups ->

24 Hrs

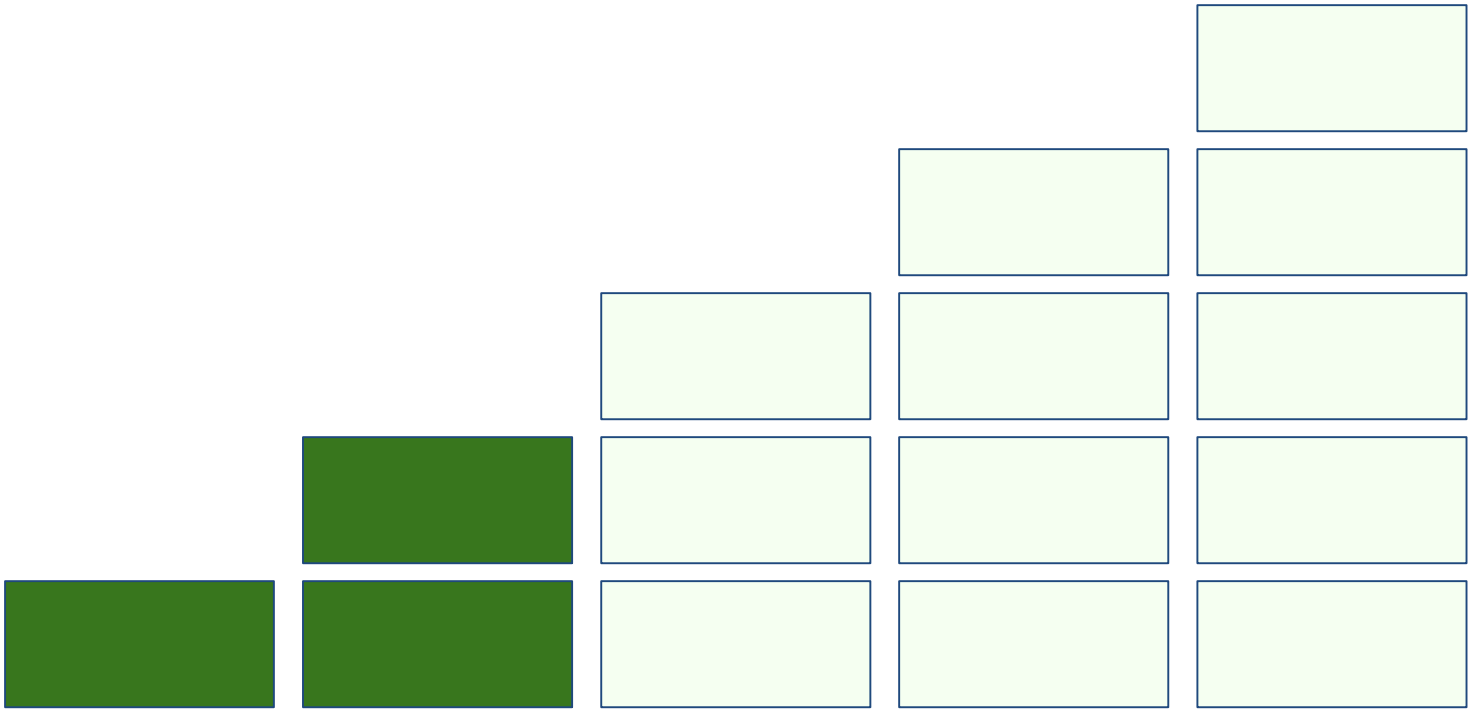
Escalation of Privs ->

5 D

Known Vuln ->

8 Hrs

Keep Calm… Be Manageable...



At Level 2, you are:

- Sorting out the lessons from initial experiments
- Assembling some ground rules for your org
- Aligning work against company objectives
- Identifying a strategy/roadmap
- Inventorying for skills on the team and needs
- Investing in upskilling talent base
- Increasing communication through dashboards

What is DevSecOps?

DevSecOps is the practice of developing safer software sooner by involving all needed parties in the creative process and practicing continuous improvement from high fidelity actionable feedback with context.

• IS

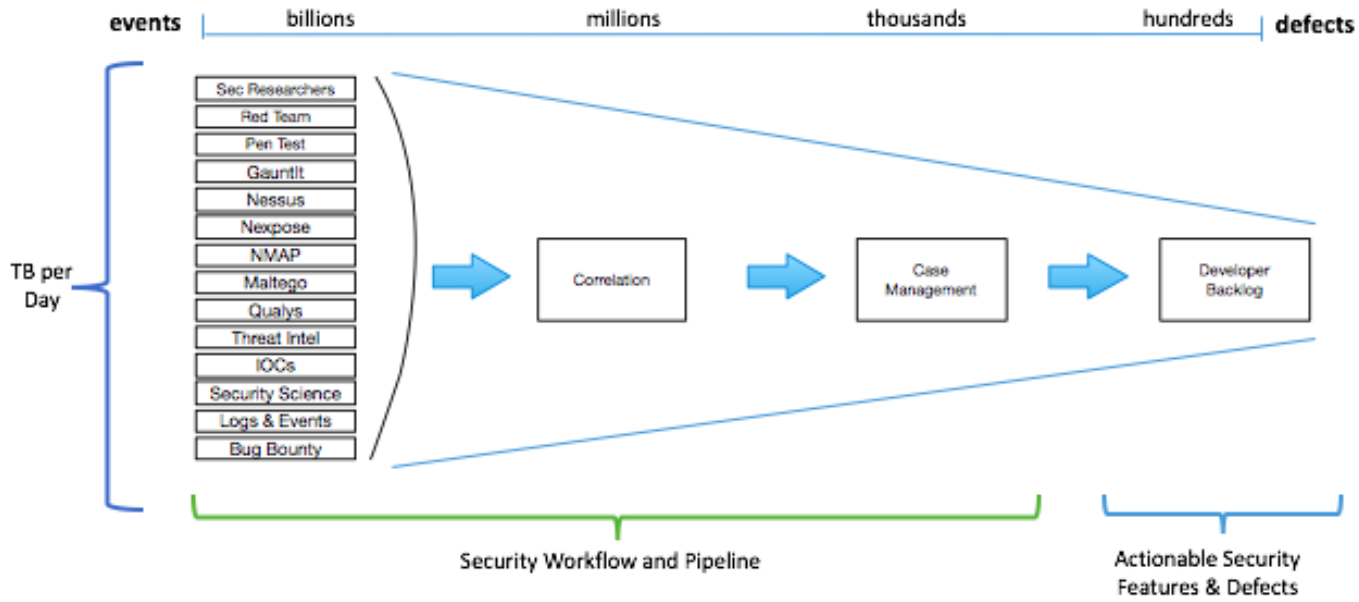
- A Mindset and Holistic Approach
- A Collection of Processes & Tools
- A Means of Building Security and Compliance into Software
- A Community Driven Effort
- A Strategy Driven by Learning and Experiments

IS NOT

- A One-Size-Fits-All Approach
- A Single Tool or Method
- Just a means of adding Security into Continuous Delivery
- Invented by Vendors
- A Strategy Driven by Perfection and Compliance

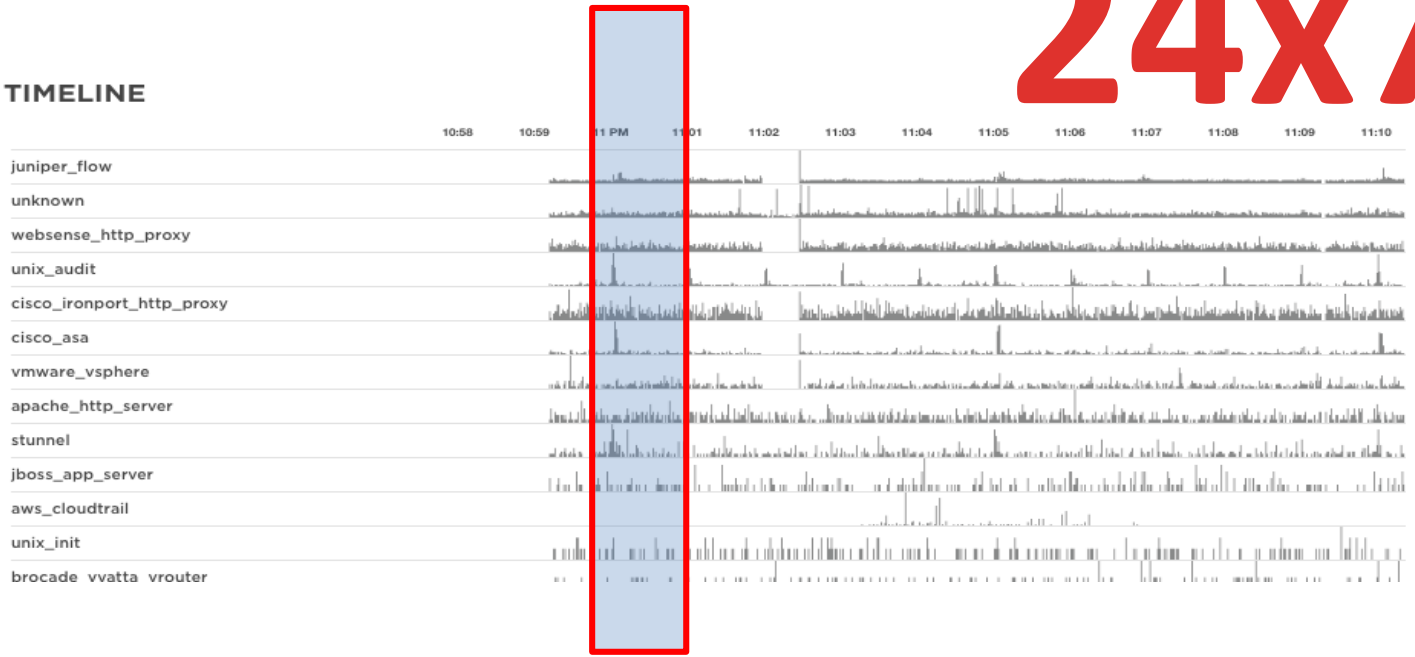
Shares concepts with Rugged Software, Rugged DevOps, SecDevOps, DevOpsSec, DevOps

Assembling a baseline & roadmap



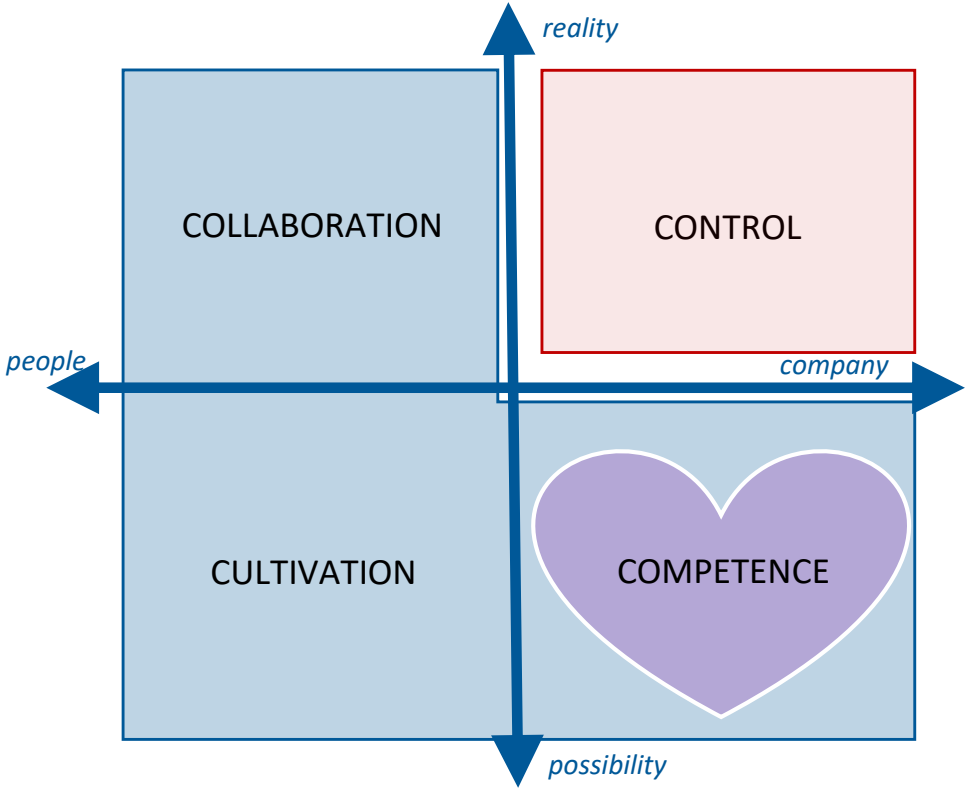
Finding new needs...

24x7



Where do I focus?

- **Management** has some firm requirements due to financial commitments and reporting
- **DevOps** and **Innovation** can easily live in 3 out of 4 boxes but hardly like Control
- **Security** practitioners tend to write policies and distrust everyone not them; rightfully so, 1% insider threat is a lot!



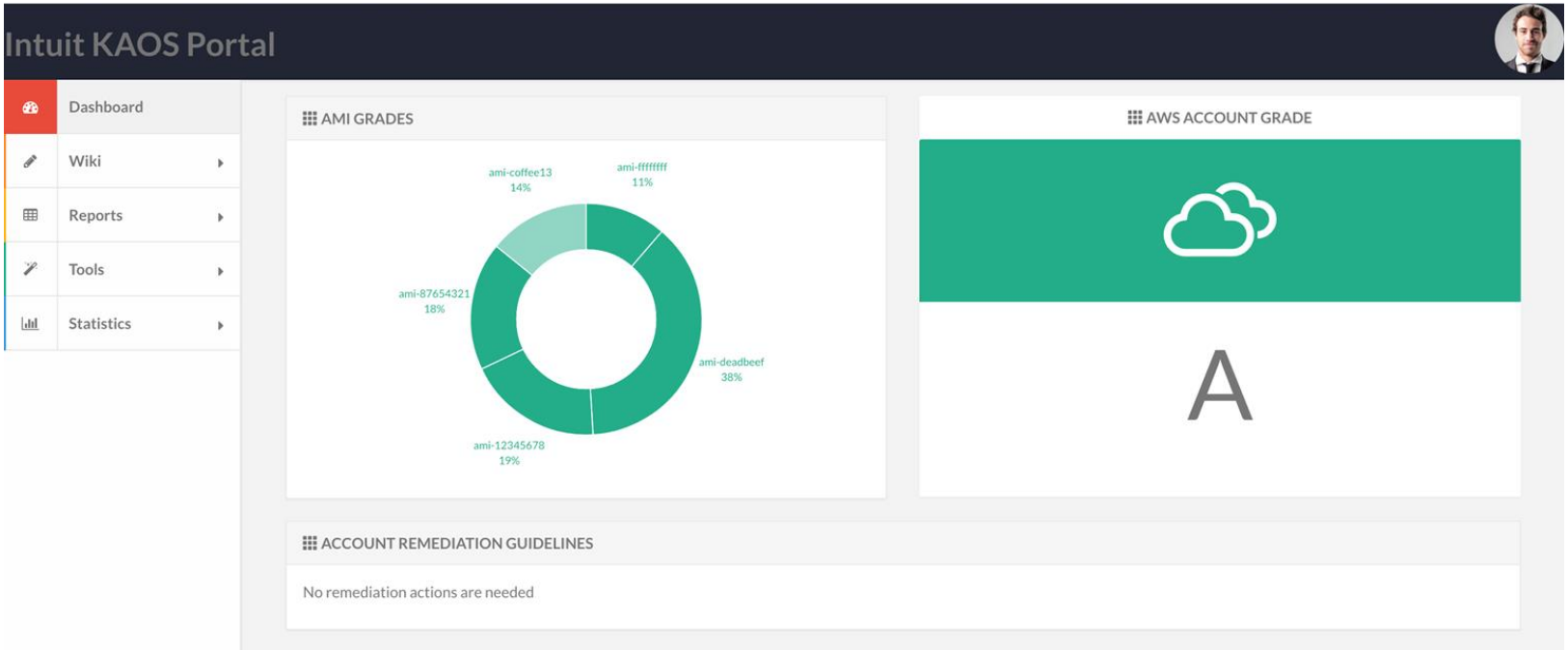
What skills do we need?

Developer		
Dev	Sec	Ops

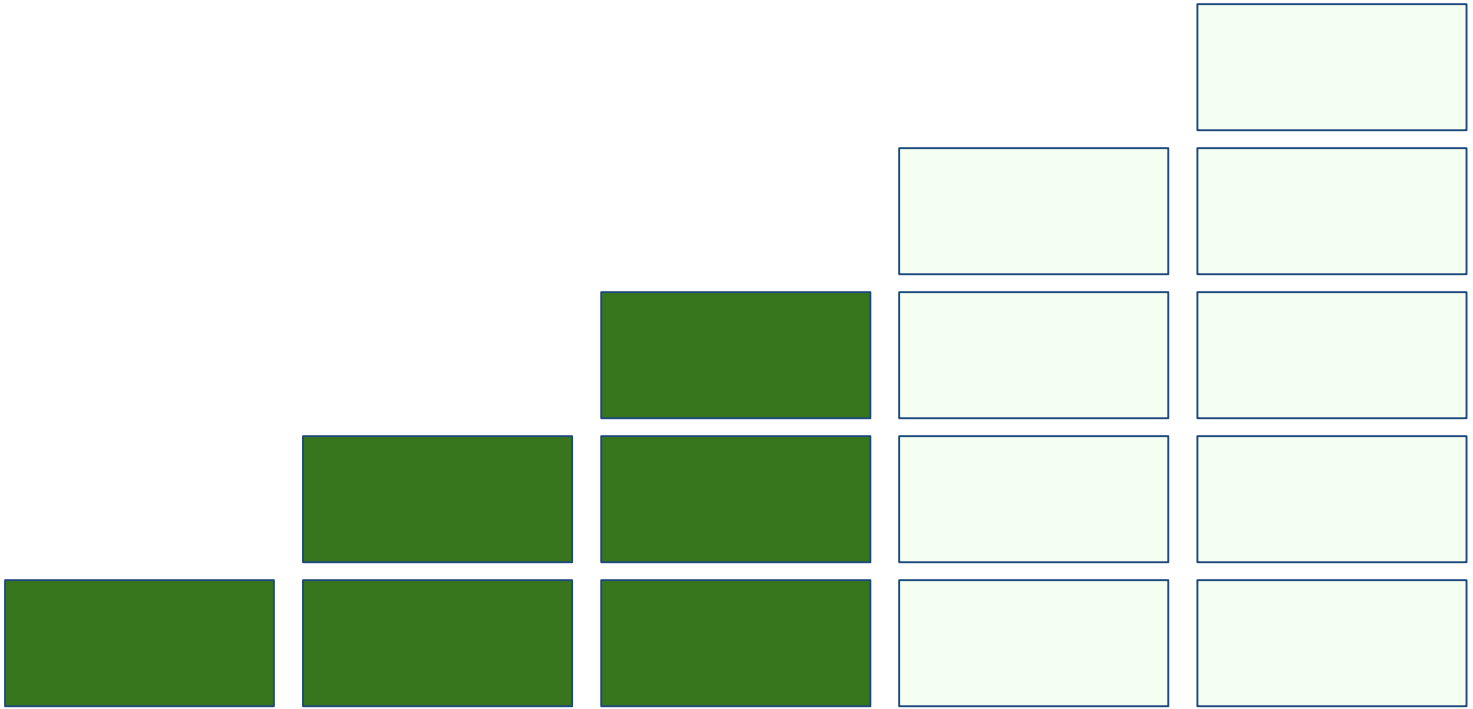
Sys Admin		
Dev	Sec	Ops

Security Engineer		
Dev	Sec	Ops

Building a Dashboard...



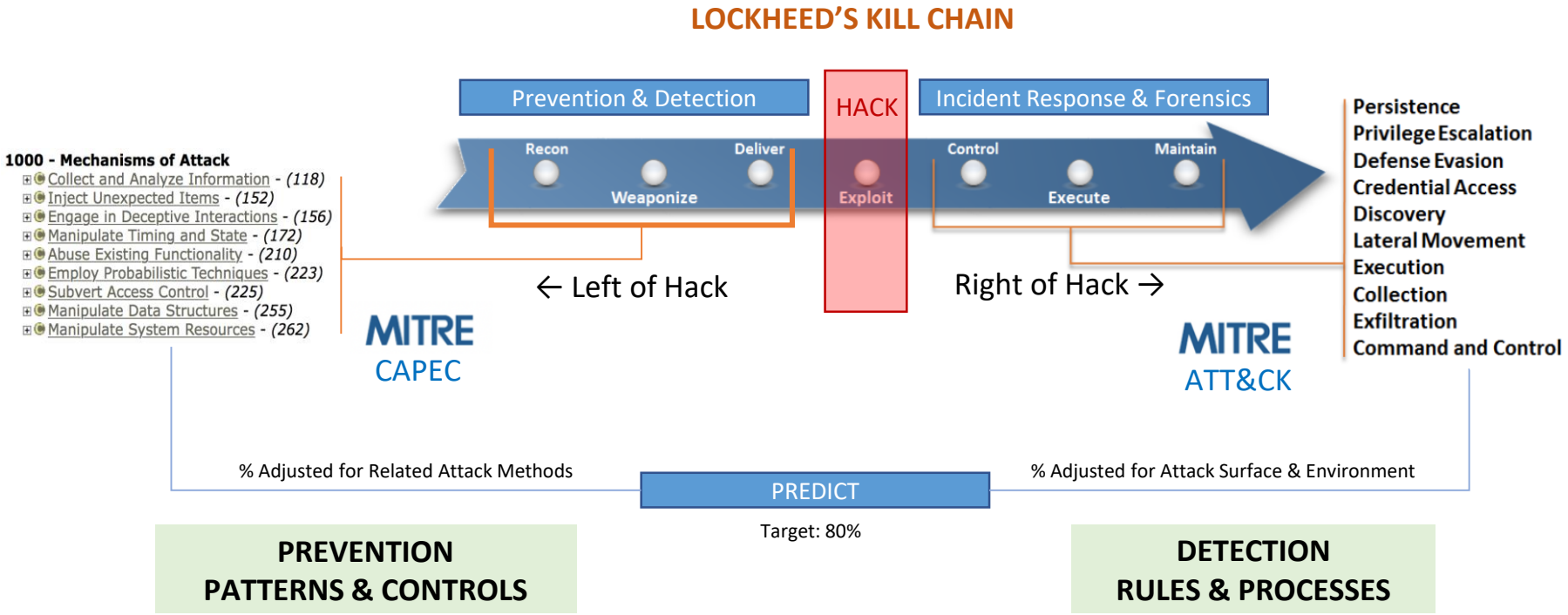
Worth being Consistent...



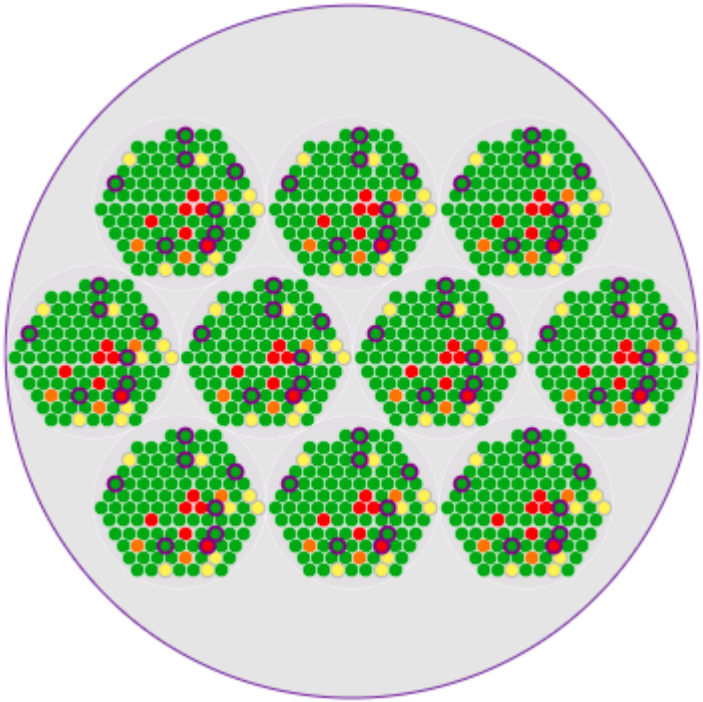
At Level 3, you are:

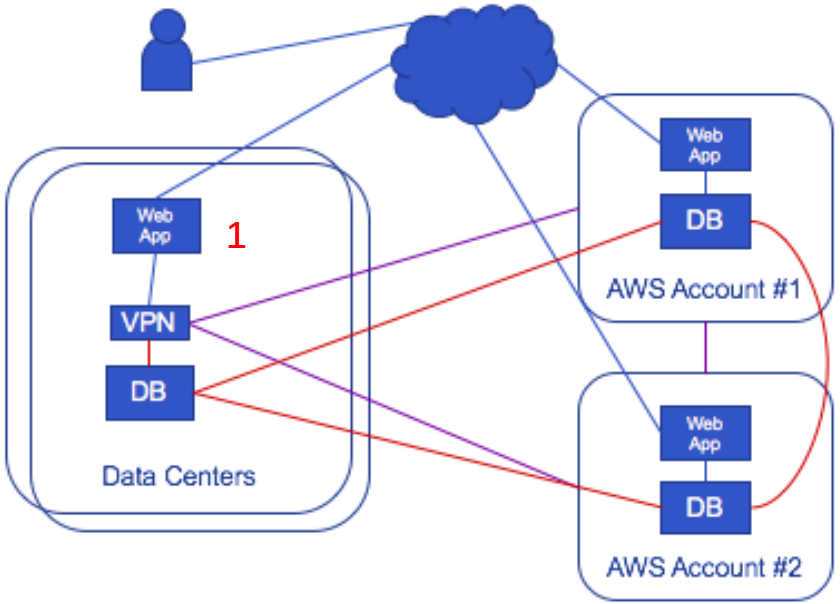
- Beginning to build up Organizing Principles
- Establishing better workflows and processes
- Expanding the initial team and distributing info
- Baselining against incoming data points
- Becoming more reliable

Bringing standards together...

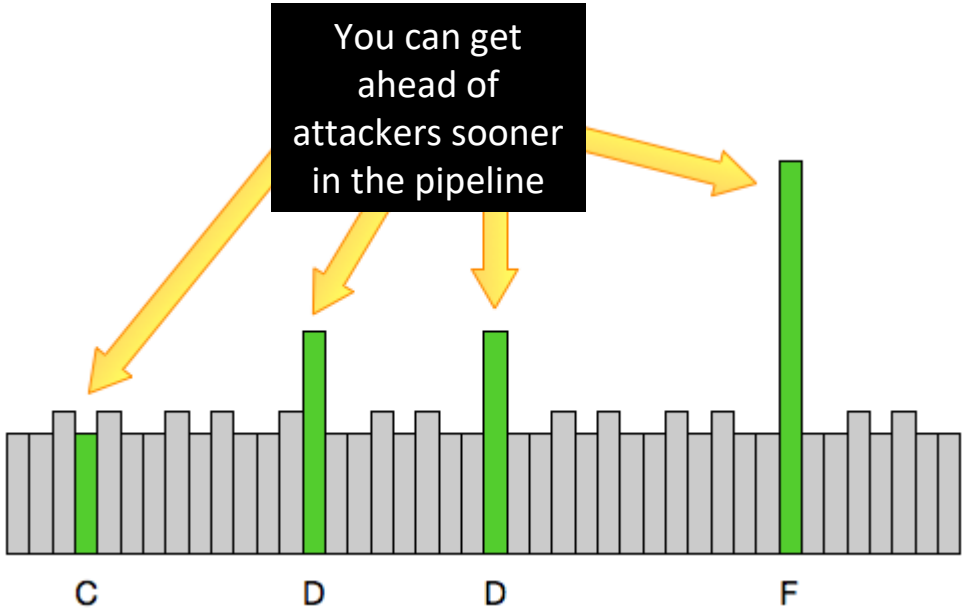


Gathering data points...

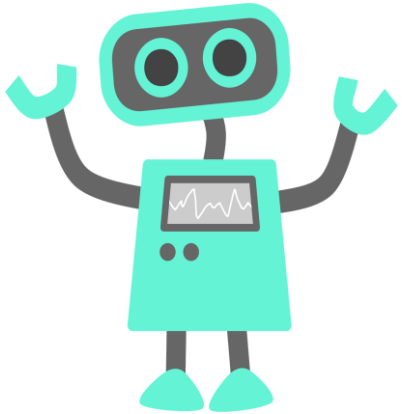


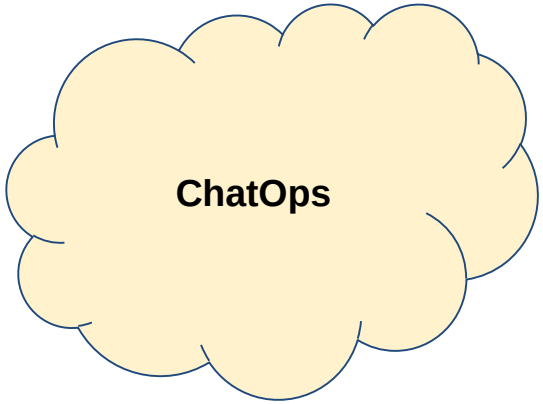


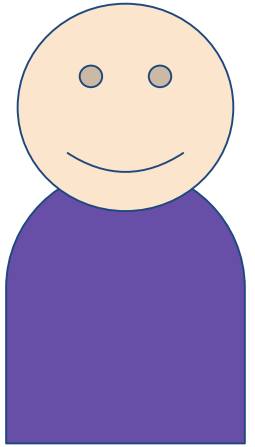
Looking for patterns...



Investing in ChatOps...







Let’s be Measured...

At Level 4, you are:

- Consistency and standards are paying off
- L3 distributed functions are showing promise
- L1-L3 measurements have begun to align
- Investing in fine-grained measurement
- Building out benchmarks
- Obsessed with dashboards and progress

		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; SOC Attestation	Partner Security Controls; SOC Attestation
Where does data transit and get stored?		company "owned" data center or co-location				
What are the innovation benefits?		reduced latency; search sensitive data				
What are the potential risks?		SQL Injection; Internal Threats; Mistakes; Phishing; Increased Friction; Slow				

```
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
    )
```

Account Grade:

B

Heal Account?

Developing benchmarks...

Example companies working on the same journey:

Collaborating with Open Gradebook

#attacker

End Goal:

$$$ $$$ $$$ $$$




Methodology:

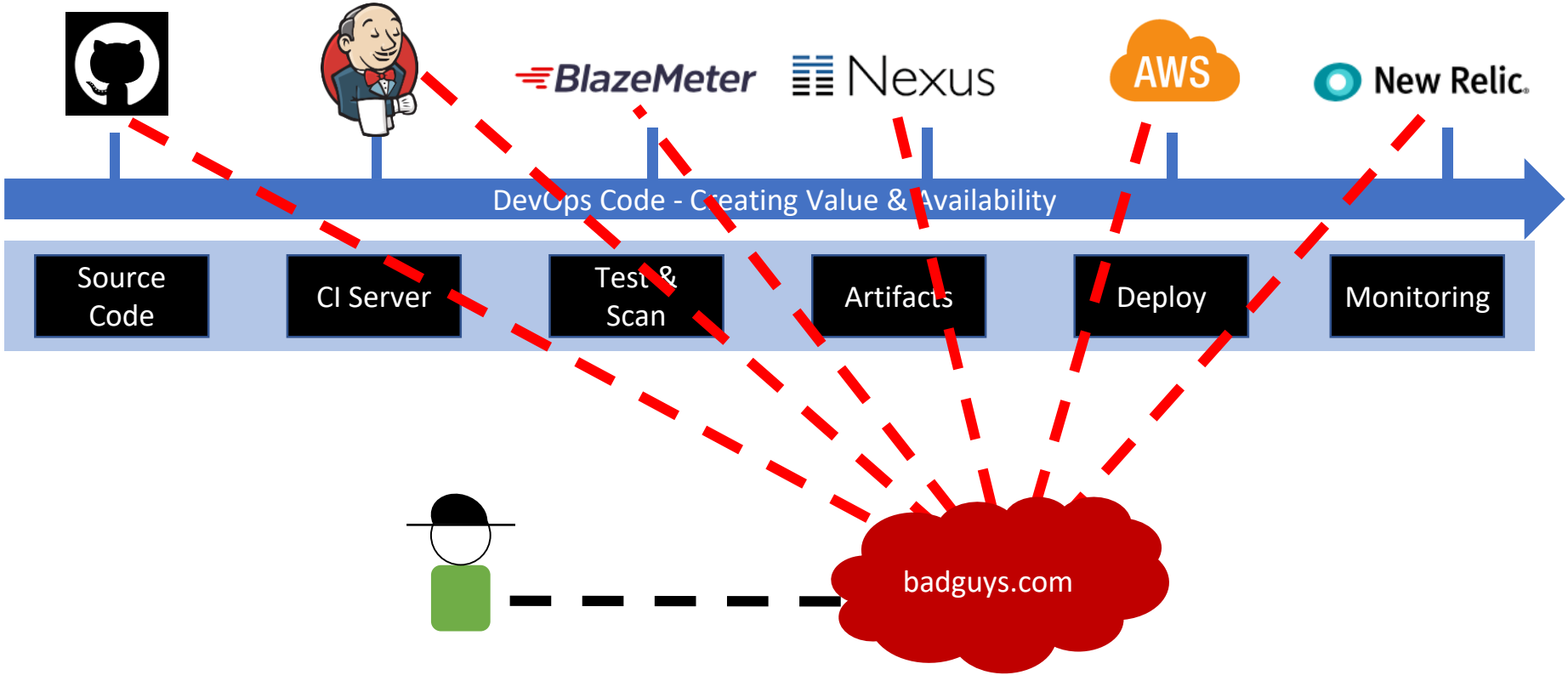
C1 Details	C2 Details	C3 Details	C4 Details	C5 Details	C6 Details	C7 Details
B10	C20	D30	F40	F50	F80	F100

Optimized DevSecOps...

At Level 5, you are:

- Finding ways to simplify for best effort
- Fluidly moving people into mission teams
- Constantly optimizing playbook
- Adversary obsessed...

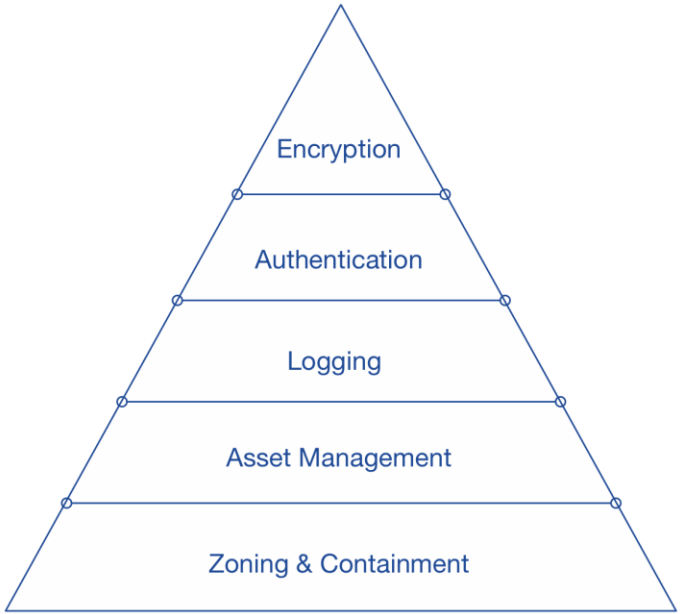
It’s all about getting rid of bad guys!



Simplifying...

- 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…"



Time for a Playbook...

n number of experiments to refine processes and automate where possible

Operating Model	Processes	Tooling
• Determine defect and feature flows for Security to funnel to distributed teams • Inventory work processes, guidelines, policies, experiments, data and tools • Identify groups, roles and skills required to support processes • Identify friction and measure speed of MTTR • Identify types of decisions • Identify metrics for measuring experiments and adapting processes	• Implement Code & Infrastructure Guidelines • Implement Rules Engineering Processes • Implement Security Defect Reporting • Implement Consulting and Requests Process • Implement Infrastructure Templates • Implement Red Team & SOC Processes • Implement Manual Staging Processes • Implement a Decisions Process • Implement an Escalation Process with clear stakeholders	• All systems should be run with API inspection available via a Security Fabric. (Systems without inspection require manual intervention.) • Implement Security Portal for feedback consolidation across security processes • Implement Case Management for Requests, Defects, and Incidents • Implement Testing framework • Implement Correlation engine • Implement foundational security controls • Integrate with core organizational systems

outcome

• Identified opportunities to develop capacity without increasing risk to too high a level • Inventory provides information for Decisions board to help with risk decisions	• Decisions board with clear escalation path by type of decision • Ability to Communicate and Train on initial processes	• Consistent Ins/Outs of Dynamic Work with standard templates • SDE helps with reducing manual efforts • Ability to build up capacity for Stage Two

Expected Issues: Communication changes, adaptation of skills, decisions processes, expectations, audits and risk guidelines mismatch

Consider helping with this content by:

1. Providing feedback
2. Asking for more details
3. Joining the community
4. Leaning in

Thank You to Our Sponsors

Join the community...

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