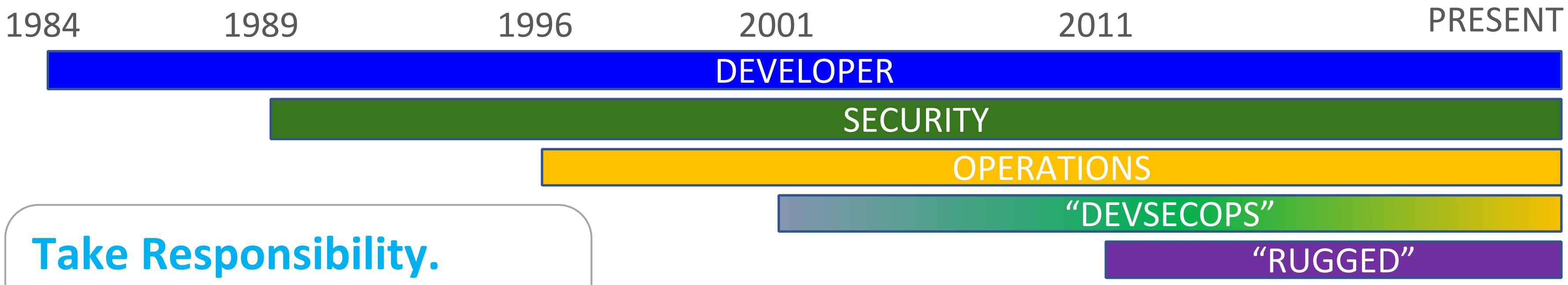
<me />

SAFER SOFTWARE SOONER

IANS

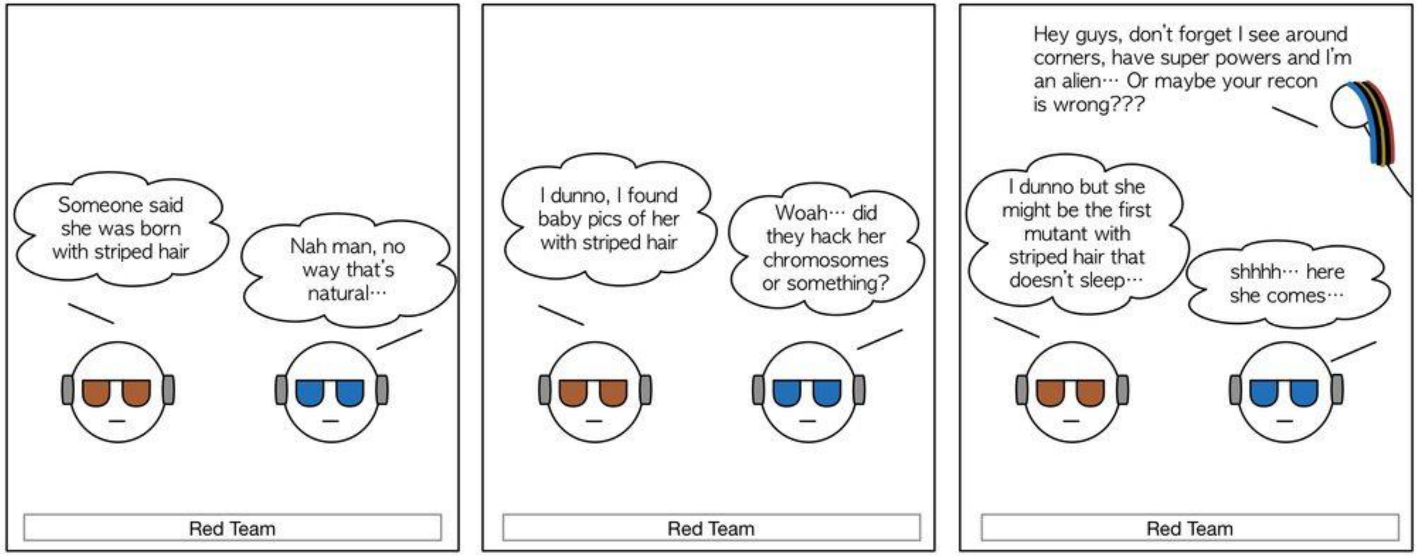


Take Responsibility.
Give Credit.

@seniorstoryteller

Stripes

(c) 2015 devsecops.org


Someone said she was born with striped hair
Nah man, no way that's natural···
Red Team
I dunno, I found baby pics of her with striped hair
Woah··· did they hack her chromosomes or something?
Red Team
Hey guys, don't forget I see around corners, have super powers and I'm an alien··· Or maybe your recon is wrong???
I dunno but she might be the first mutant with striped hair that doesn't sleep···
shhhh··· here she comes···
Red Team

DEVSECOPS

-- FOUNDER --

HACKERGIRL™

https://hackergirl.io

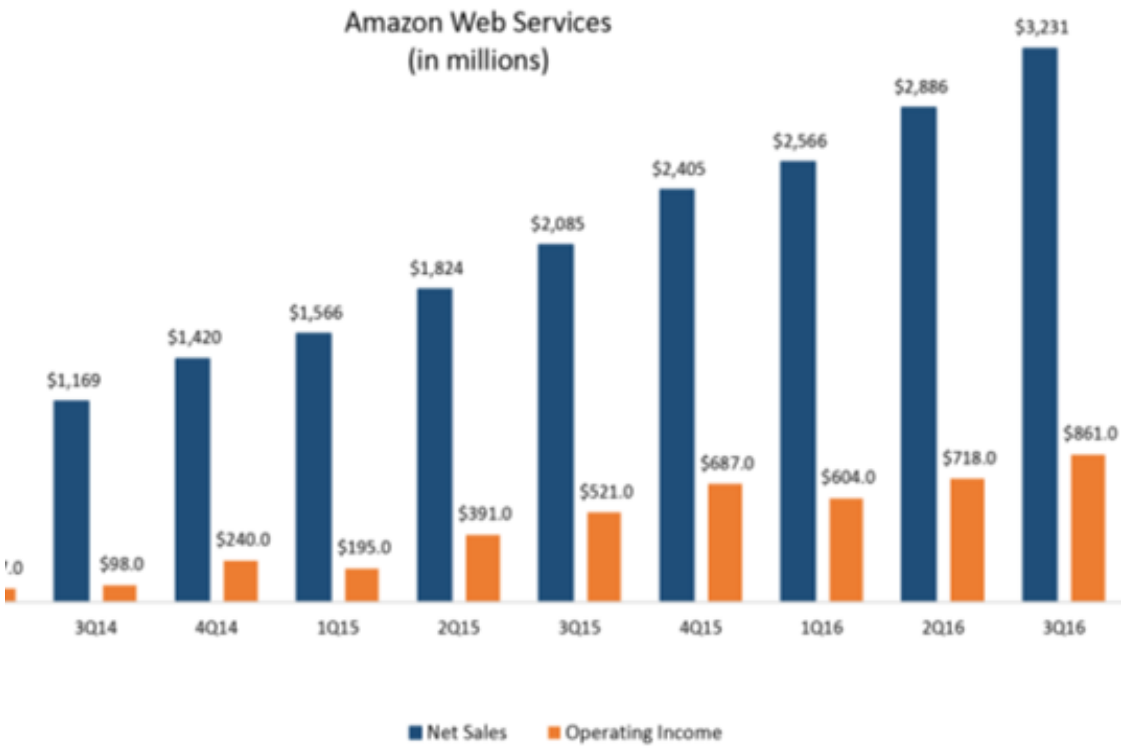
All Day DevOps

⍰

Your Level	Your Interest
⍰Beginner	Getting started
✣ Mid-Level	Making more progress
✷ Advanced	Efficiencies of Scale

Cloud growth is exponential!!

- Public Cloud adoption is accelerating at a rapid pace…
- Software defined environments allow scale to happen and more decisions to be made daily…
- More people can experiment, learn and fail at a rapid pace to solve for customer demand….
- Creativity is the next frontier…



http://www.geekwire.com/2016/study-aws-45-share-public-cloud-infrastructure-market-microsoft-google-ibm-combined/

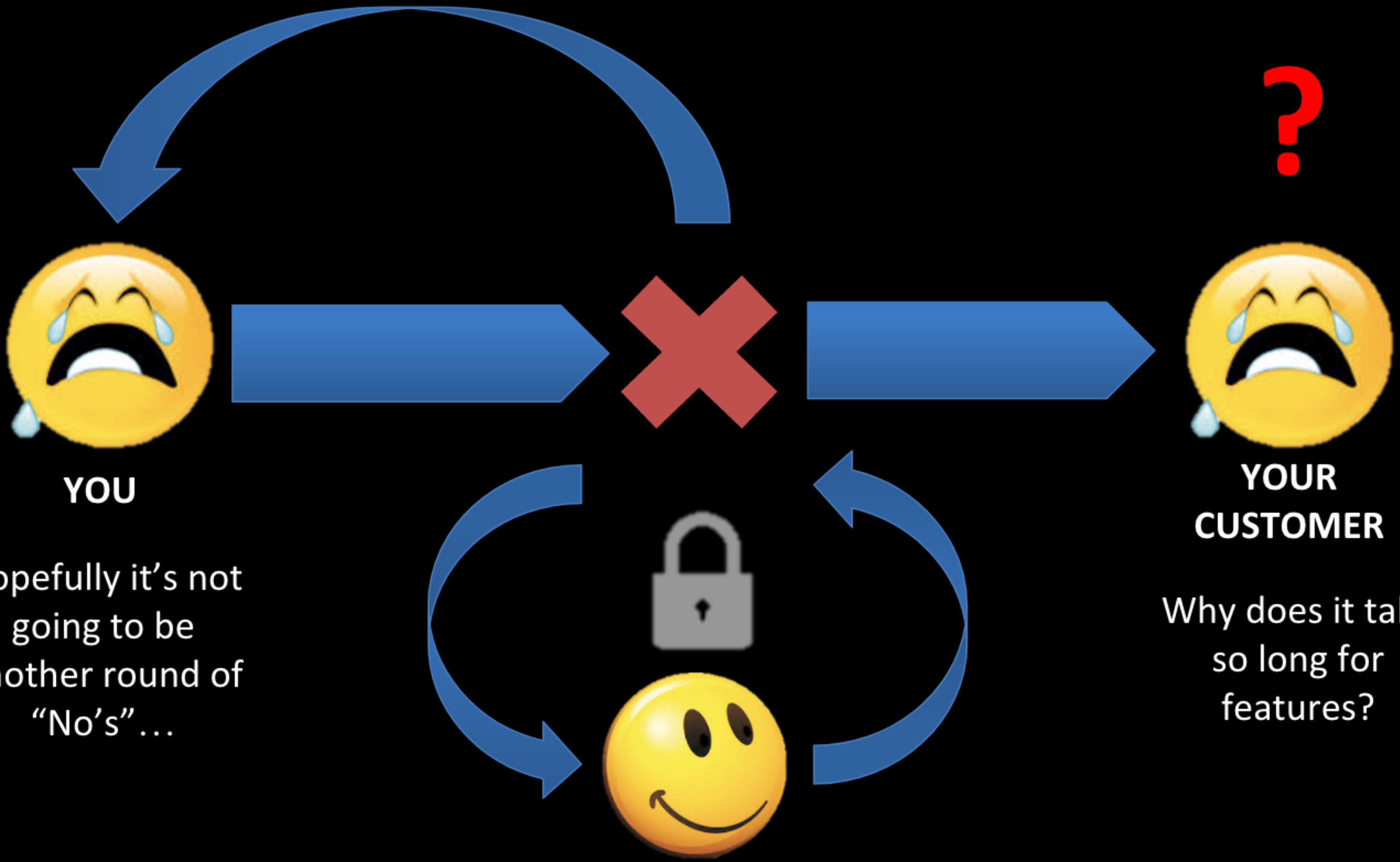
DevOps hiring is up ~2000% in last 5 years!

- Imagine solving the world’s problems faster by collaborating and taking responsibility.
- In connection with Cloud Computing, *DevOps is the cultural enabler* needed to scale creativity and innovation.
- With the goal of solving customer problems faster, no wonder DevOps is taking over.

~1500% increase
In 2 years

@petecheslock

Is bureaucracy getting in the way of Continuous Deployments and Real Security?



YOU

Hopefully it's not going to be another round of "No's"…

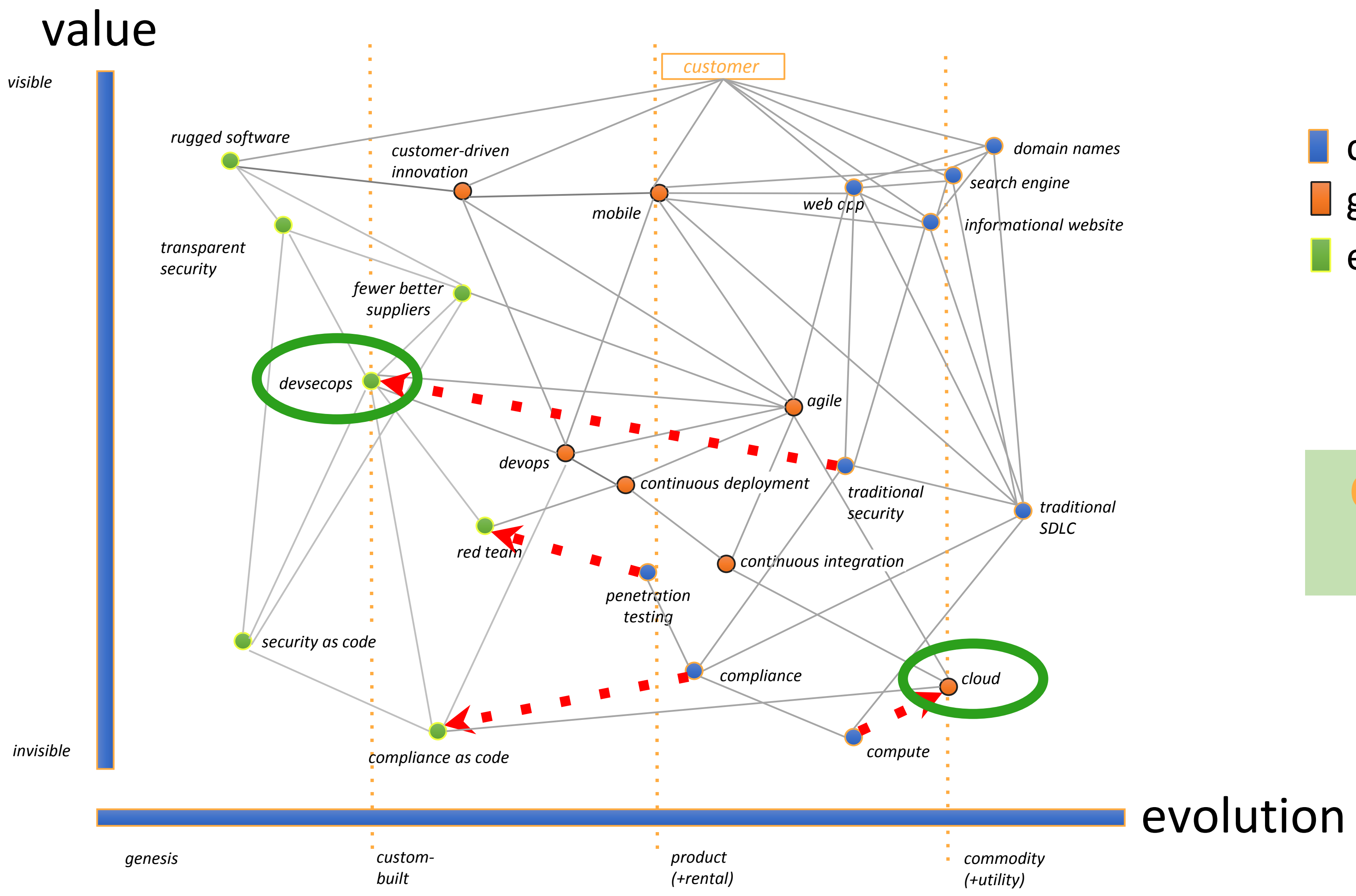
YOUR CUSTOMER

Why does it take so long for features?

CISO

BANG
HEAD
HERE

What’s Happening?



🟦 commodity bound

🟧 growth

🟩 emerging

Catching up takes commitment

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

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

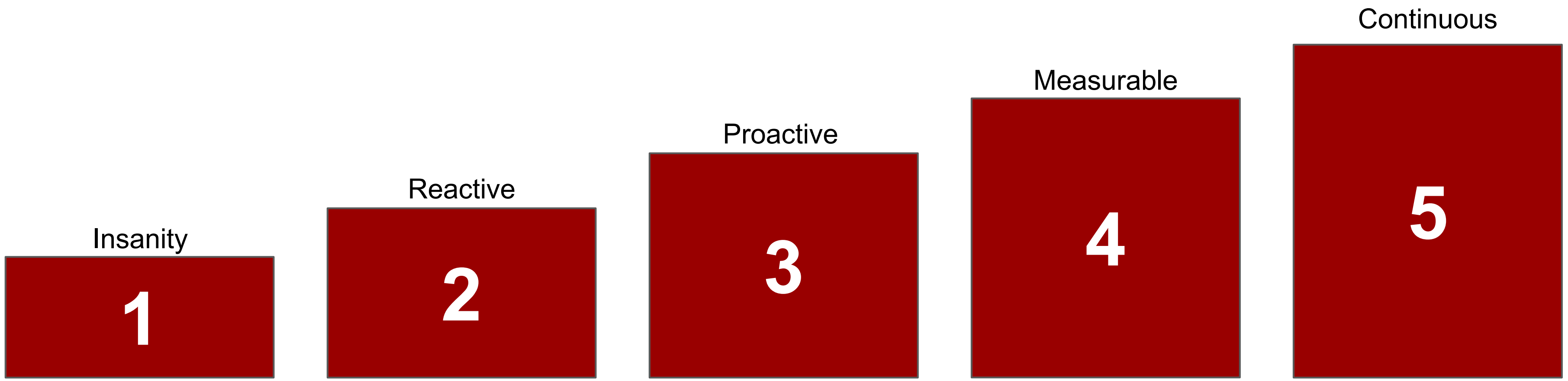
24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident

Shared Threat Intelligence over Keeping Info to Ourselves

Biggest Pitfalls...

1. Cloud is just a fad…
2. DevOps is fleeting…
3. We’re good with our traditional security program...
4. Mistakes are unacceptable!
5. We can find all security issues before launch...
6. Compliance gives us everything we need...
7. We’re under the radar…
8. Our penetration tests haven’t surfaced any of these issues…
9. Our company isn’t ready yet…
10. We’re a waterfall shop...

DevSecOps Maturity Model & Behaviors



Insanity 1

Reactive 2

Proactive 3

Measurable 4

Continuous 5

	Burp	**Crawl**	**Walk**	**Run**	**Fly**
Culture	Surprising with lots of Push Back	Full Awareness but Feeling Helpless	Integrated & Talked about by Execs; Feedback loop integrated	Measured by Execs	Context driven decisions
Skills	Skills developed outside of job function	Skills lining up with job functions	Skill development paired with job	Proactive skill development to meet roadmap demands	Knowledge evolves inline / Lessons savored
Program / Outcomes	Just getting by	Orderly Processes & Faster Reactions	Reduced number of Incidents	Measurable difference in attacks	Predictive & Proactive
Security Priorities	P0/Critical Waiting for Attackers	P0 and P1s Some Hygiene	P0 and P1s Compliance	Attack Surface driven & measured	Stay ahead of Bad guys

1

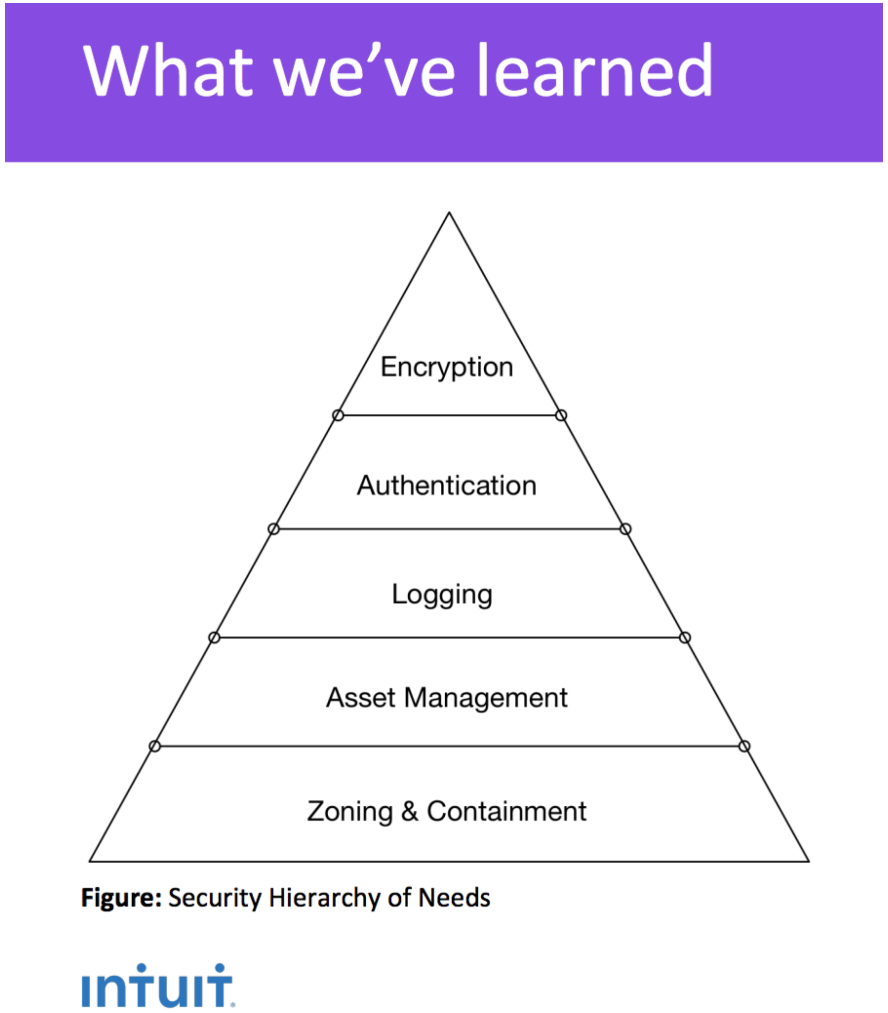
Security Hierarchy of Needs at RSA

https://published-prd.lanyonevents.com/published/rsaus17/sessionsFiles/4864/CSV-R10F-Securely-Moving-Data-to-the-Cloud-with-Confidence-and-Customer-Focus.pdf

- Security controls can be simplified for easier adoption and 80% protection using the *Security Hierarchy of Needs.*

- All of these categories are applicable to any environment.

- Simplifying provides an easier path to success in critical control categories.



What we've learned

Figure: Security Hierarchy of Needs

1

The Rise of Purple Teams at RSA

https://www.rsaconference.com/writable/presentations/file_upload/air-w02-the-rise-of-the-purple-team.pdf

- Prove it!

- Why not test like attackers do and get ahead of them?

- Finding problems and reporting has a serious advantage over simply complaining that nobody is listening...

DevSecOps Playbook at SANS

https://www.sans.org/reading-room/whitepapers/analyst/devsecops-playbook-36792

- DevSecOps Playbooks are everywhere and the community is vibrant

- Regardless of “how” you implement for your culture, use playbooks to learn but not follow to the letter...

- Don’t make the mistake of oversimplifying...

The Tao of Security Science at RSA

https://www.rsaconference.com/writable/presentations/file_upload/csv-w02-devsecops-the-tao-of-security-science.pdf

- Security science is at the heart of the change for DevSecOps.
- Finding ways to chip away at difficult issues is not insurmountable...
- Gathering data early and leveraging it to learn makes all the difference.

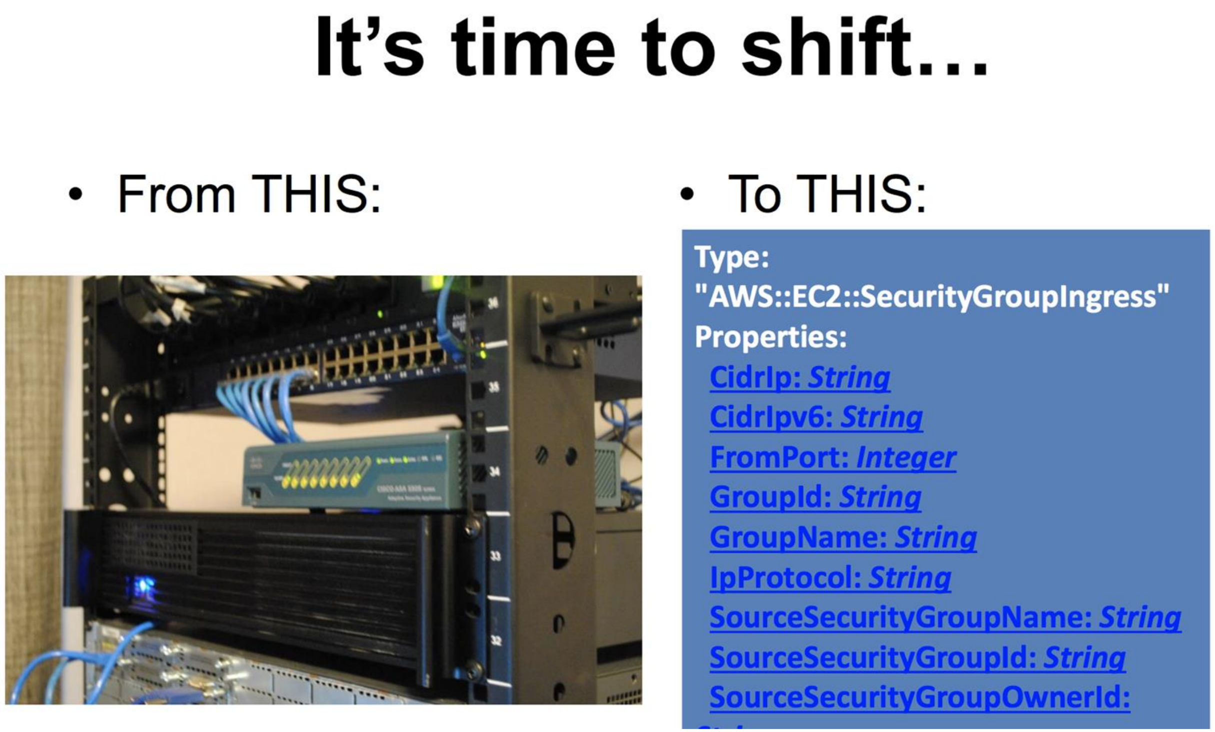
Which works better? DevSecOps?

“Nothing is more soft and yielding than water, yet for attacking the solid and the strong, nothing is better.” - **Tao Te Ching** (chapter 78)

Security as Code at SANS

https://www.sans.org/summit-archives/file/summit-archive-1493839170.pdf

- Security is migrating into code.
- It’s time to find the skills and know how to make security decisions with context.
- Don’t underestimate the simple mistakes...



It’s time to shift…

- From THIS:
- To THIS:

Type: "AWS::EC2::SecurityGroupIngress"
Properties:
 CidrIp: *String*
 CidrIpv6: *String*
 FromPort: *Integer*
 GroupId: *String*
 GroupName: *String*
 IpProtocol: *String*
 SourceSecurityGroupName: *String*
 SourceSecurityGroupId: *String*
 SourceSecurityGroupOwnerId:

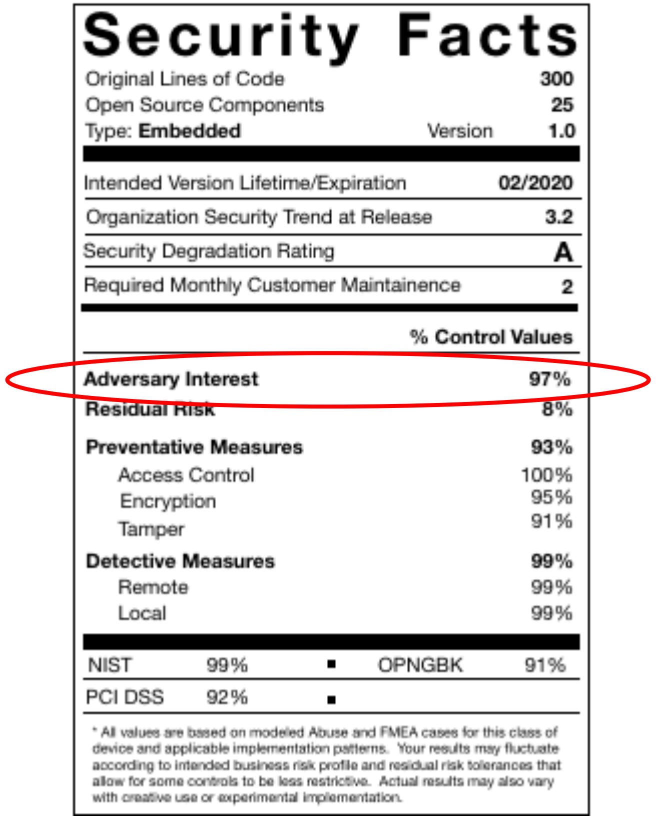
DevSecOps Symposium at IANS

https://www.iansresearch.com/events/seattle-symposium-devsecops

- Adversary interest and feedback loops are critical to prioritization...

- Given thousands of component parts, it’s important to trend your adversaries.

- P0 and P1s should never persist since security simply degrades over time.



Security Facts

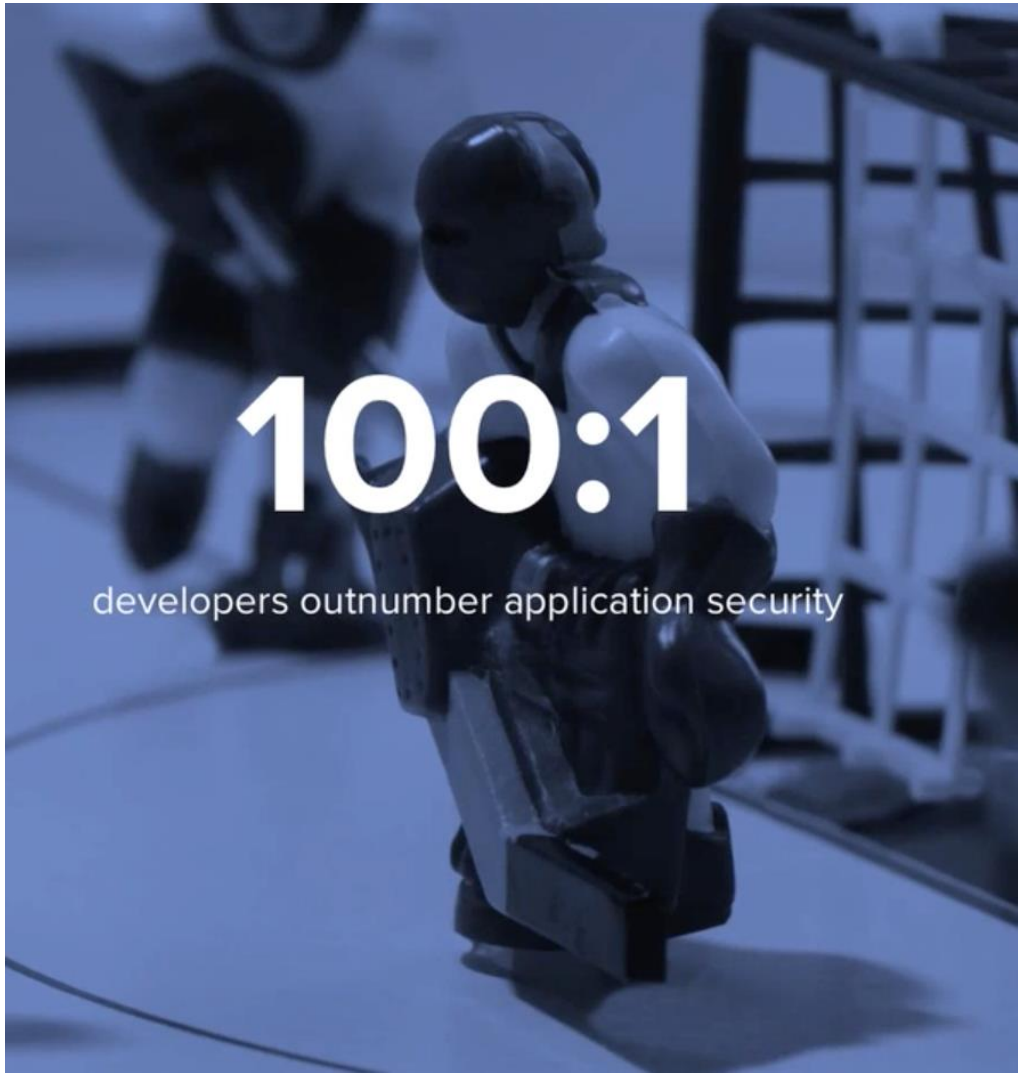
Original Lines of Code			300
Open Source Components			25
Type: **Embedded**		Version	1.0
Intended Version Lifetime/Expiration			02/2020
Organization Security Trend at Release			3.2
Security Degradation Rating			**A**
Required Monthly Customer Maintainence			2
			% Control Values
Adversary Interest			**97%**
Residual Risk			**8%**
Preventative Measures			**93%**
Access Control			100%
Encryption			95%
Tamper			91%
Detective Measures			**99%**
Remote			99%
Local			99%
NIST	99%	▪ OPNGBK	91%
PCI DSS	92%	▪	

* All values are based on modeled Abuse and FMEA cases for this class of device and applicable implementation patterns. Your results may fluctuate according to intended business risk profile and residual risk tolerances that allow for some controls to be less restrictive. Actual results may also vary with creative use or experimental implementation.

DevSecOps Lessons at OWASP

https://vimeo.com/210478219

- Time to focus on component parts to get rid of exploitable attack surface.
- Supply chain issues must be measured to get better.
- Focusing on just the SDLC is not the sole essence of this challenge…



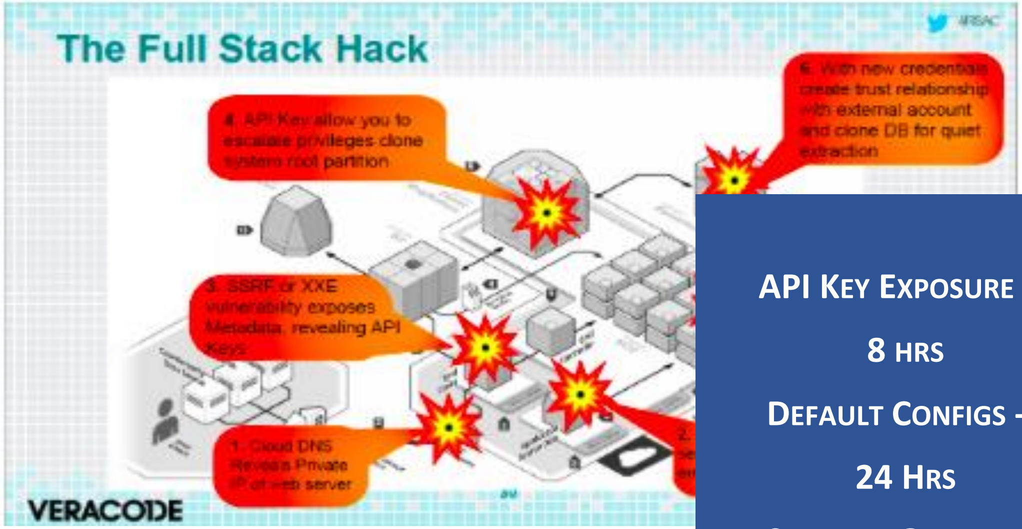
Full Stack Attack at RSA

https://www.rsaconference.com/writable/presentations/file_upload/csv-w03-_defending-the-cloud-from-the-full-stack-hack.pdf

- Attack Surface is what matters most...

- Attack Maps provide the basics faster than other methods.

- Measure and learn in order to stay ahead.


The Full Stack Hack
#RSAC
6. With new credentials create trust relationship with external account and clone DB for quiet extraction
4. API Key allow you to escalate privileges clone system root partition
3. SSRF or XXE vulnerability exposes Metadata, revealing API Keys
1. Cloud DNS Reveals Private IP of web server
2.
VERACODE

API Key Exposure ->

8 hrs

Default Configs ->

24 Hrs

Security Groups ->

24 Hrs

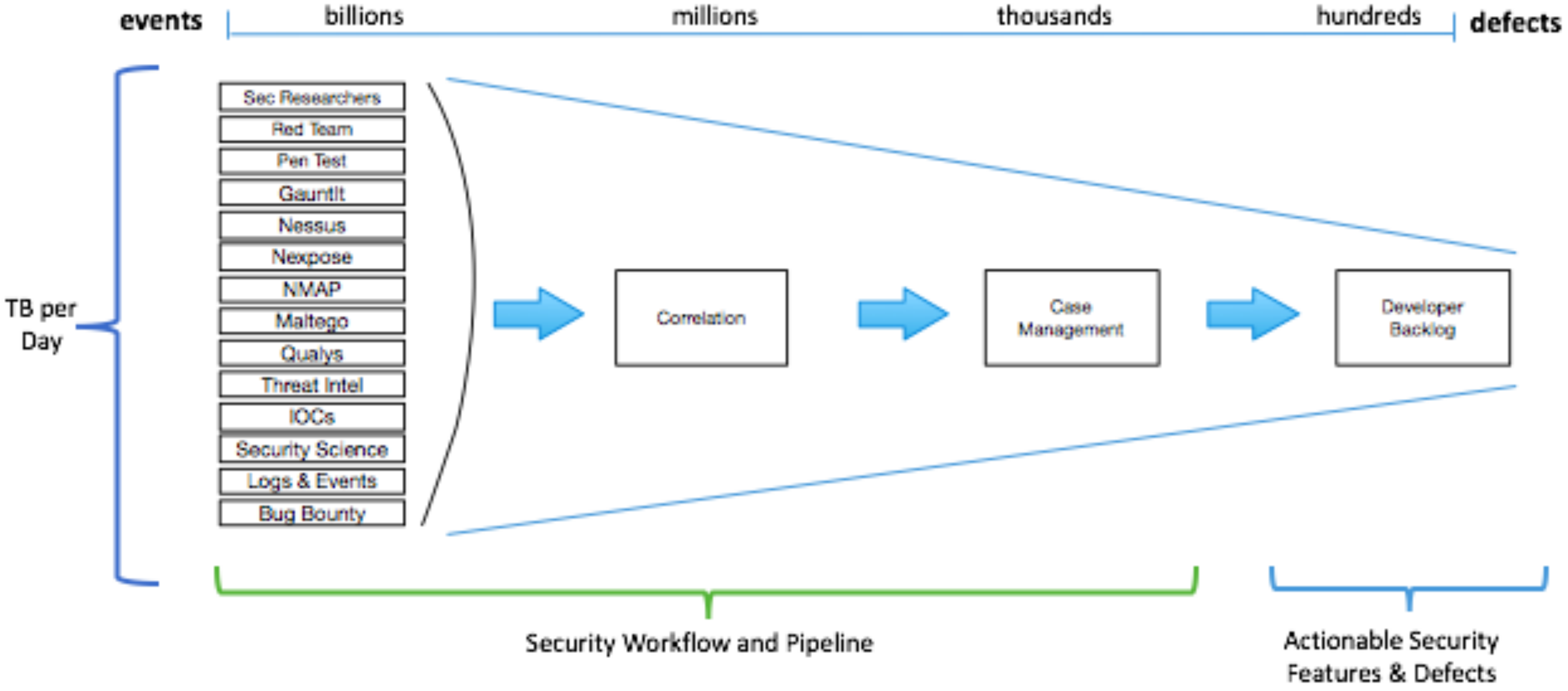
Escalation of Privs -> 5 D

Known Vuln ->

8 Hrs

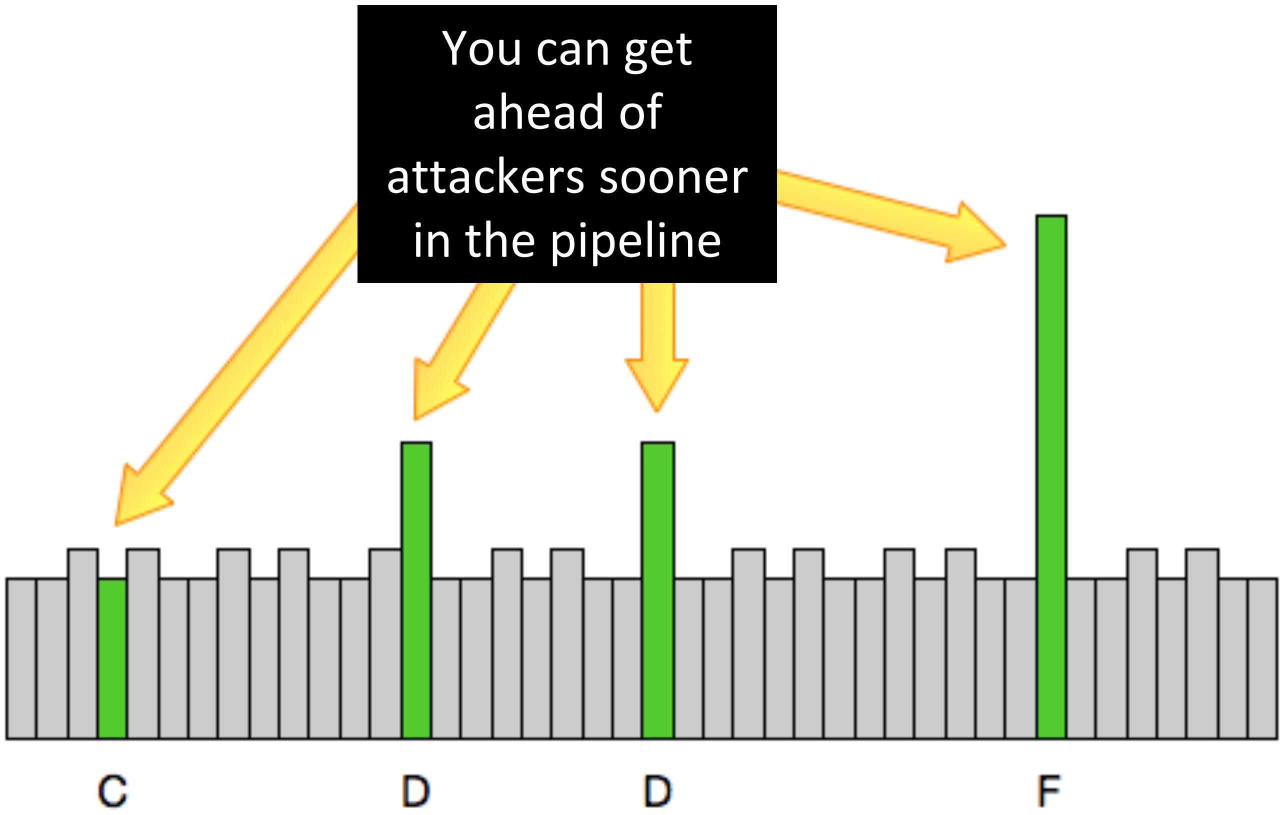
5

What’s the best way to organize around it?



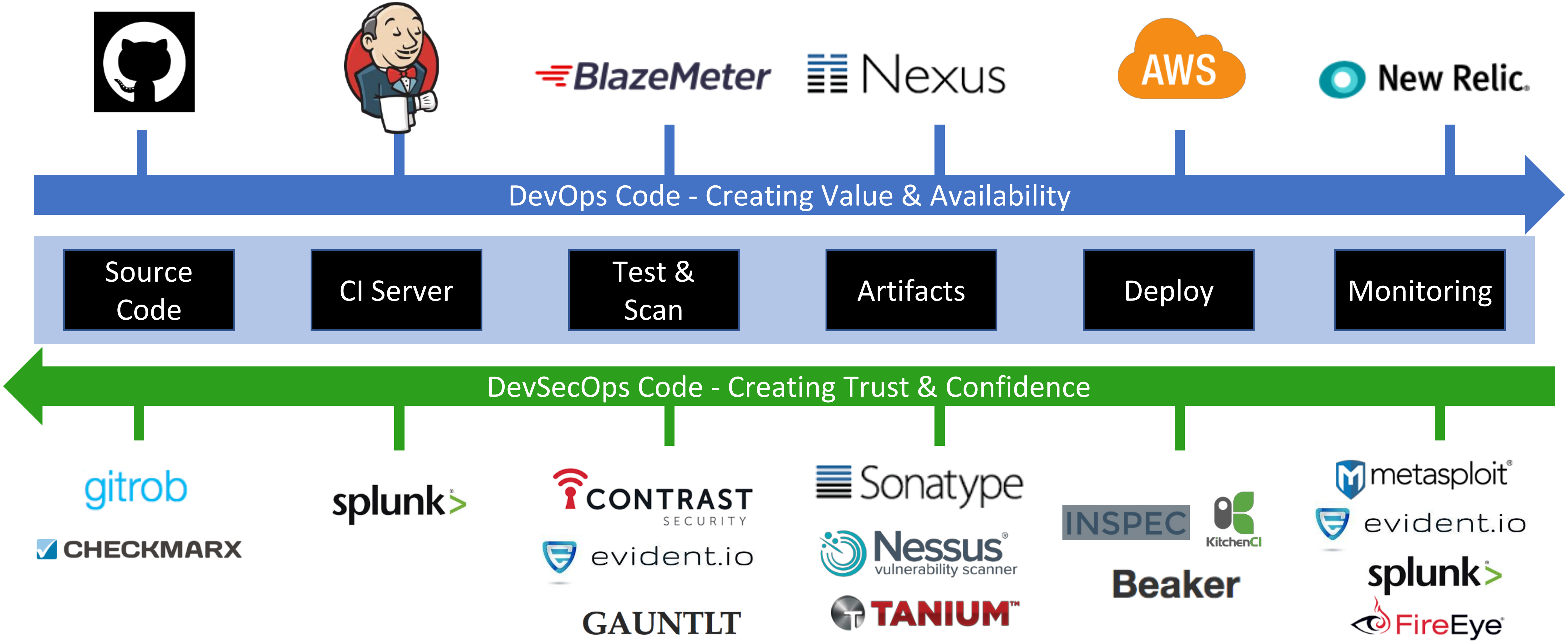
5

How will I know when I am doing it well?



You can get ahead of attackers sooner in the pipeline

How hard could it be?

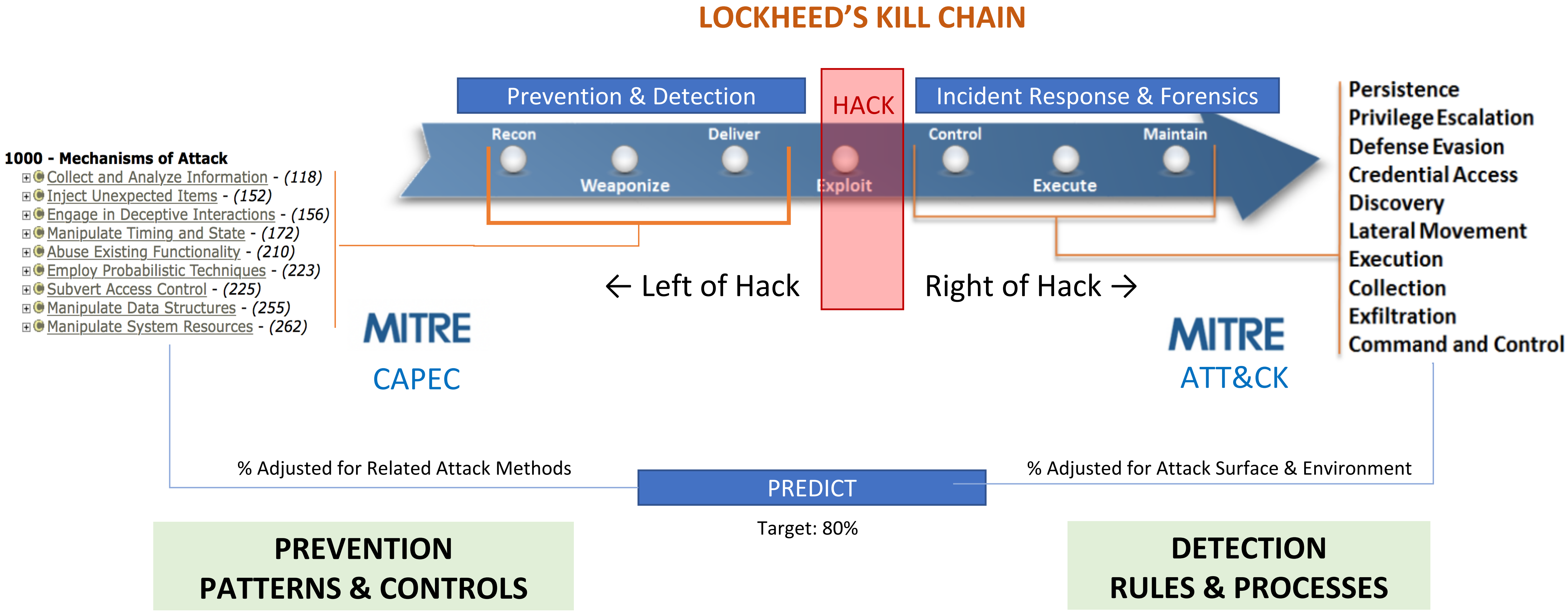


DevOps Code - Creating Value & Availability

Source Code | CI Server | Test & Scan | Artifacts | Deploy | Monitoring

DevSecOps Code - Creating Trust & Confidence

Is there some science behind all of this?

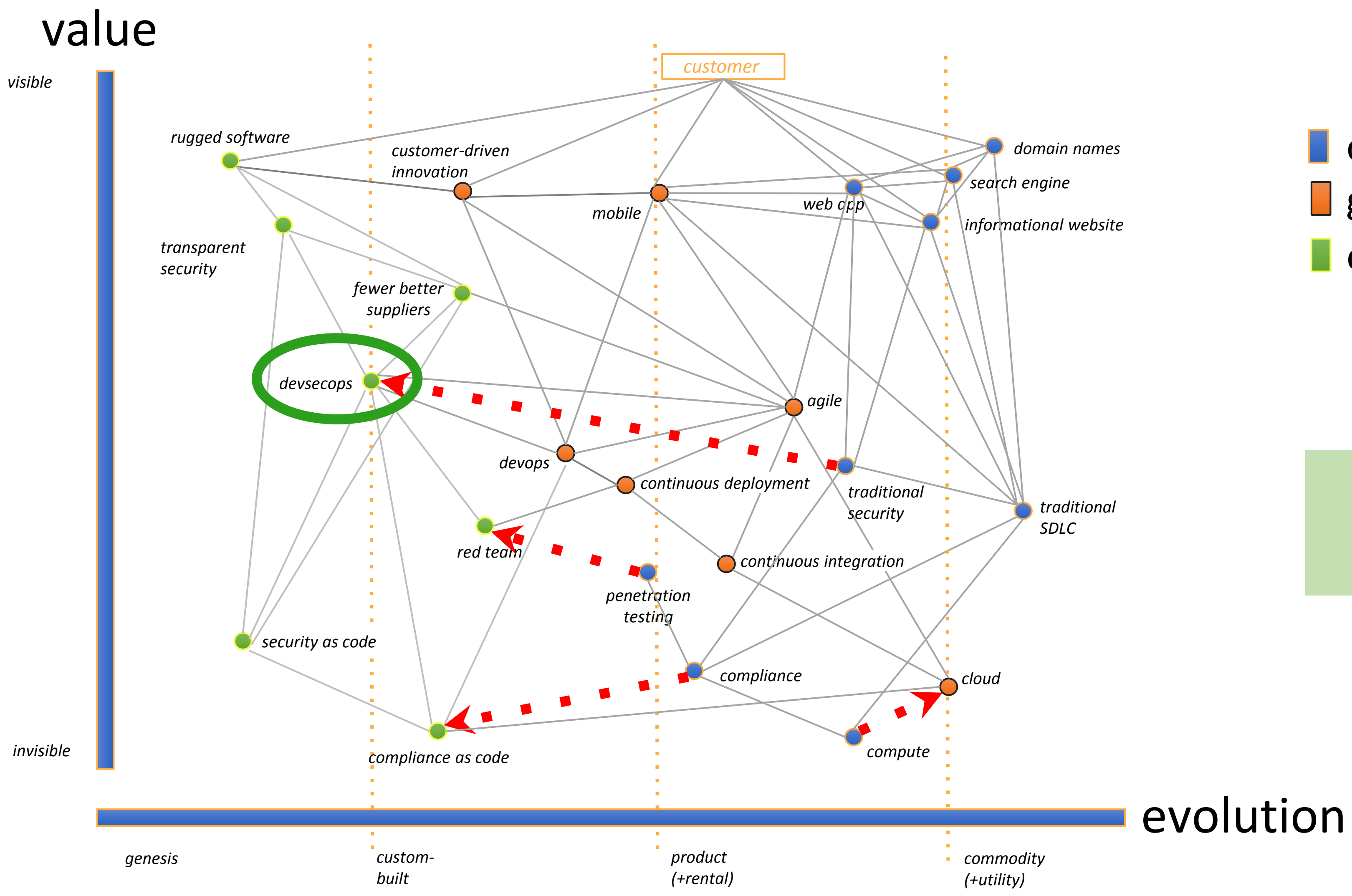


1000 - Mechanisms of Attack

- Collect and Analyze Information - *(118)*
- Inject Unexpected Items - *(152)*
- Engage in Deceptive Interactions - *(156)*
- Manipulate Timing and State - *(172)*
- Abuse Existing Functionality - *(210)*
- Employ Probabilistic Techniques - *(223)*
- Subvert Access Control - *(225)*
- Manipulate Data Structures - *(255)*
- Manipulate System Resources - *(262)*

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

With your help, Software Safer Sooner can be a reality...



🟦 commodity bound

🟧 growth

🟩 emerging

Catching up takes commitment