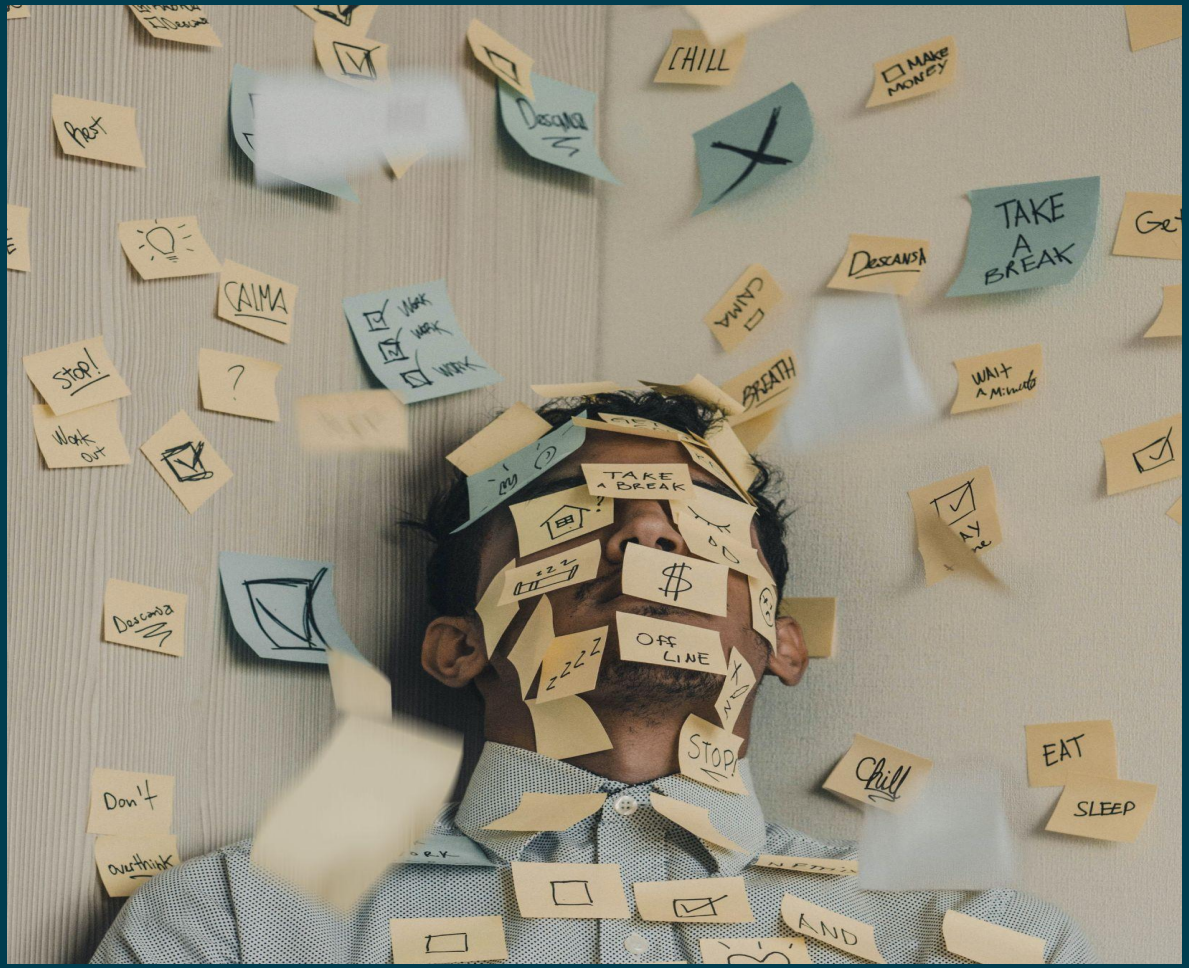
Organizational Change Through The Power Of Why - DevSec Ops Enablement

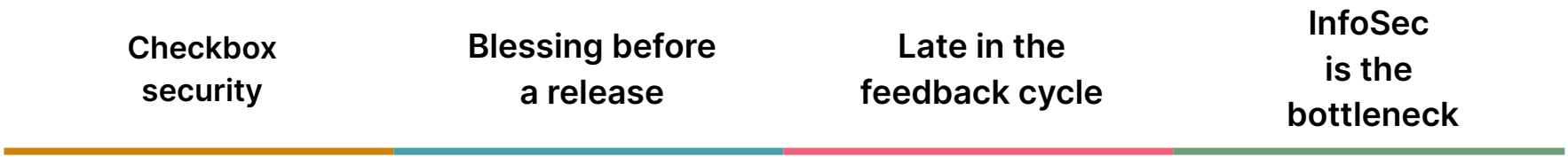
thoughtworks

Nazneen Rupawalla



SECURITY IS EVERYONE'S RESPONSIBILITY AND UNFORTUNATELY, IT'S EASIER SAID THAN DONE

Observations



Challenges

Ownership and accountability of secure development still falls onto InfoSec

Security literacy is currently not seen as everyone’s responsibility

Discussions with IT product teams felt like status call

Security roadmap not being able to be integrated by leads

What will it take to move the needle?

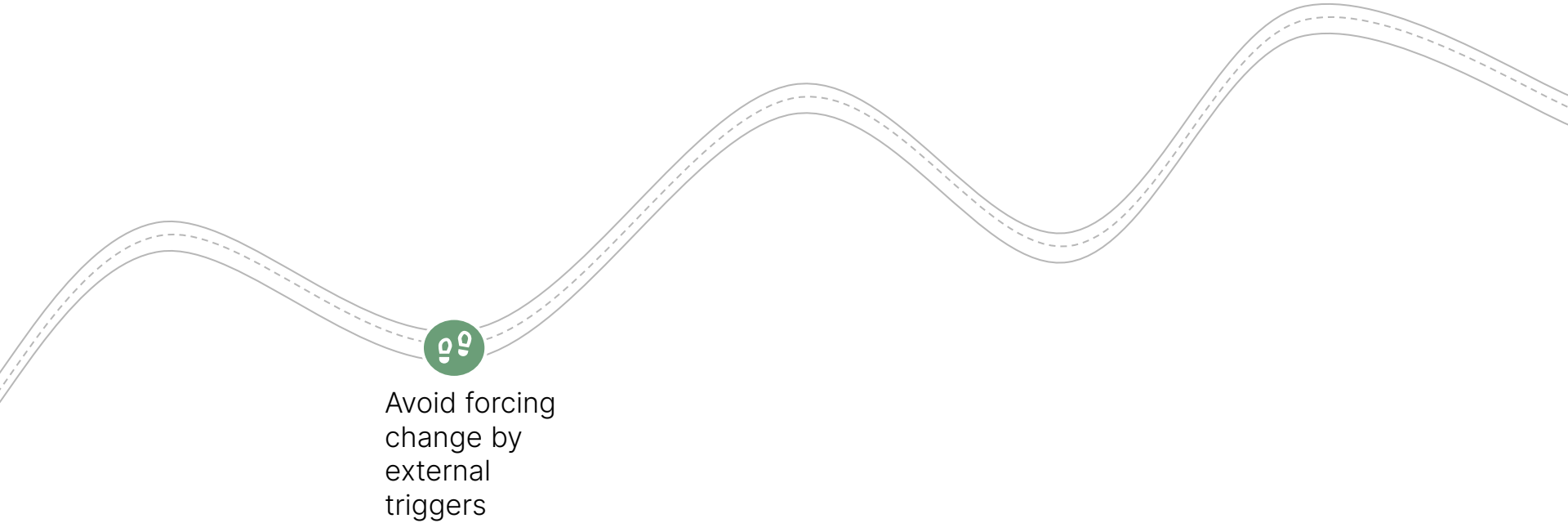
Security Journey

Insights

Self paced progress
and support

What will make the process effective for teams?

What are their current touch-points?



BACKLOG	IN PROGRESS	COMPLETED
[IAM] Identity and access management	[Data] Data security and privacy	Threat Modelling
[Secrets Management] Secrets Handling		
[Secrets Management] Secrets Lifecycle management		
[Data] No production data in non production environment		
List of controls goes on..		

Milestone Release - Kickoff phase

Threat Assessment

Threat Modelling

Milestone Release - Kickoff phase

Secrets Management

Secrets Handling

Milestone Release - Kickoff phase

Secrets Management

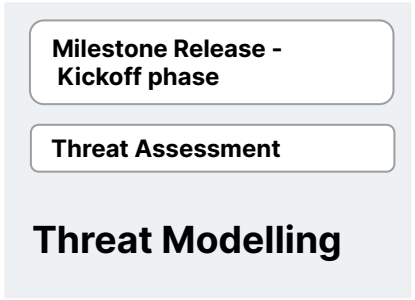
Secrets Handling

Why should effort be invested?

...
Recent breaches list due to secrets leakage
Common mistakes such as hard coding them in source code, littering them throughout configuration files and configuration management tools, and storing them in plaintext in version control.
...

How to implement this control?

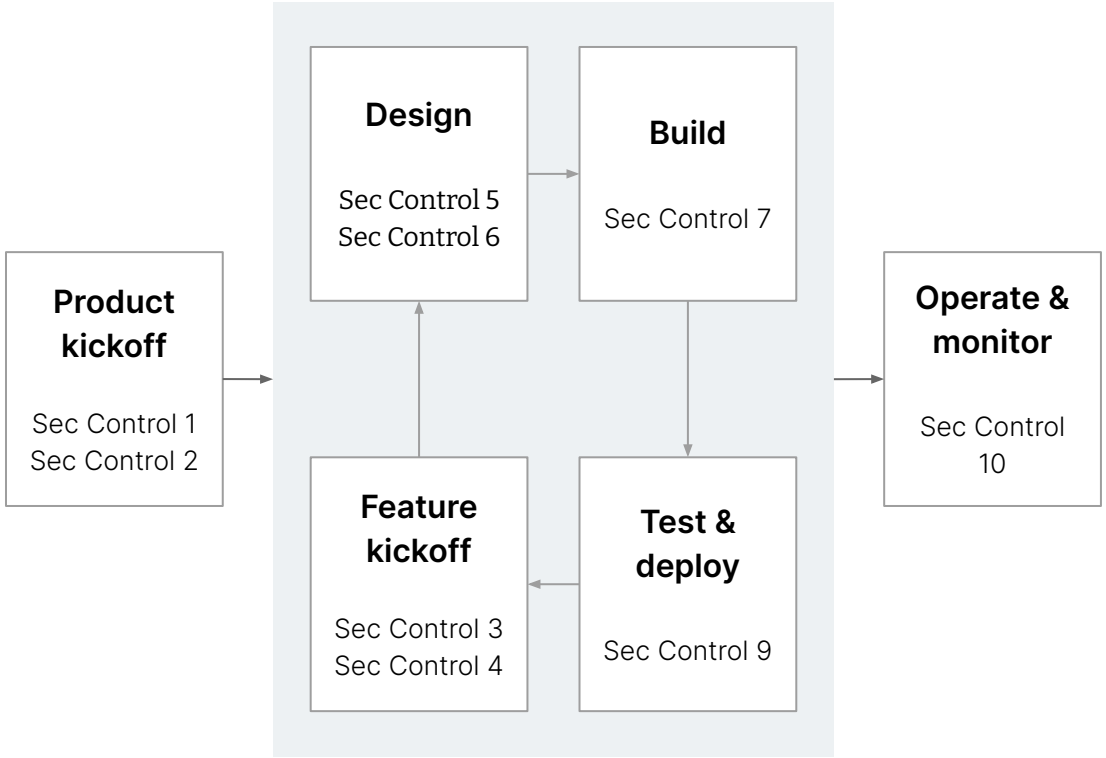
...
- Ensure a team password manager is in use.
- Ensure talisman is added as the pre-push hook to check for leakage
- Run trufflehog if talisman is yet not configured to check for secrets.
- Leverage existing secret management solutions.
- Do no re-use secrets for different environments, systems or services.
- Do not log any secrets in any logs, including CI/CD logs. - Ensure sensitive data is not exposed in the 'environment variables' section of AWS console for Lambda and ECS services
- Ensure secrets are not stored as plaintext in CI/CD solution
...



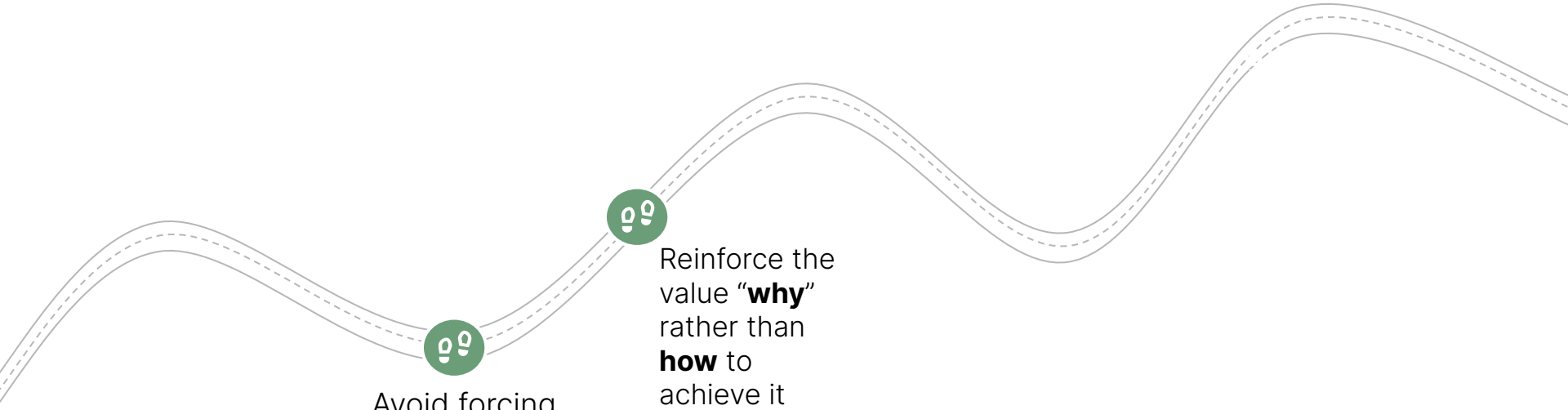
Spoofing - *On the Internet, nobody knows you*
Tampering - *Can the data overflow and become instructions?*
Repudiation - *If there's no evidence, it is easy to deny it happened*
Information disclosure - *Who else could be looking?*
Denial of service - *Could the service be taken down?*
Elevation of privilege - *How easy is it to circumvent protections?*

BACKLOG	IN PROGRESS	COMPLETED
[IAM] Identity and access management	[Data] Data security and privacy	Threat Modelling
[Secrets Management] Secrets Handling		
[Secrets Management] Secrets Lifecycle management		
[Data] No production data in non production environment		
List of controls goes on..		

Build Security In Cycle



What will make the process effective for teams?



Avoid forcing change by external triggers

Reinforce the value “**why**” rather than **how** to achieve it

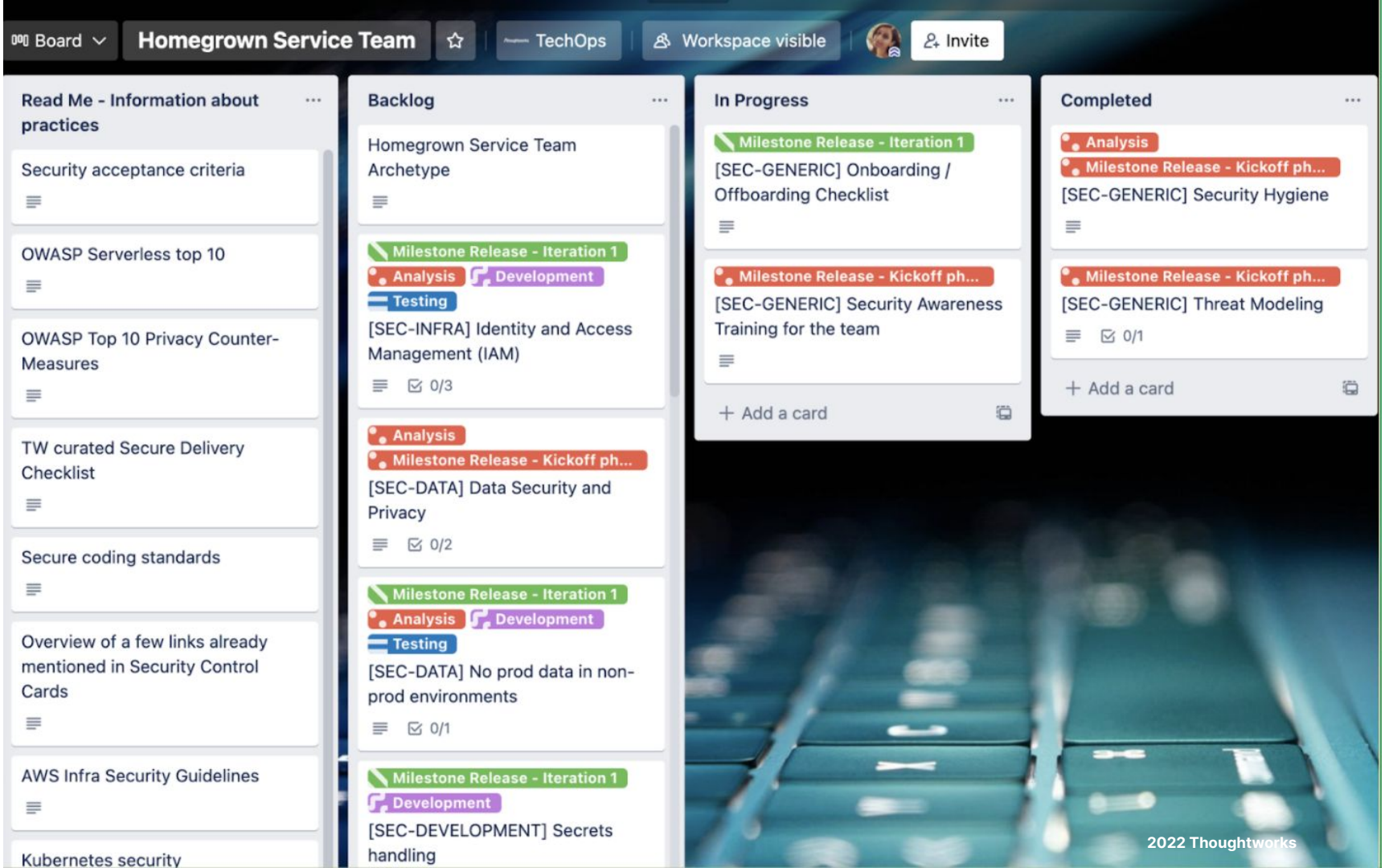
Supported the vision to seed the security program within IT

Defined the control

Shared the procedures in way anyone can pick from the team

Promoted a sense of accomplishment

Start of our journey of culture shift


Board
Homegrown Service Team
TechOps
Workspace visible
Invite
Read Me - Information about practices
Security acceptance criteria
OWASP Serverless top 10
OWASP Top 10 Privacy Counter-Measures
TW curated Secure Delivery Checklist
Secure coding standards
Overview of a few links already mentioned in Security Control Cards
AWS Infra Security Guidelines
Kubernetes security
Backlog
Homegrown Service Team Archetype
Milestone Release - Iteration 1
Analysis
Development
Testing
[SEC-INFRA] Identity and Access Management (IAM)
0/3
Analysis
Milestone Release - Kickoff ph...
[SEC-DATA] Data Security and Privacy
0/2
Milestone Release - Iteration 1
Analysis
Development
Testing
[SEC-DATA] No prod data in non-prod environments
0/1
Milestone Release - Iteration 1
Development
[SEC-DEVELOPMENT] Secrets handling
In Progress
Milestone Release - Iteration 1
[SEC-GENERIC] Onboarding / Offboarding Checklist
Milestone Release - Kickoff ph...
[SEC-GENERIC] Security Awareness Training for the team
Add a card
Completed
Analysis
Milestone Release - Kickoff ph...
[SEC-GENERIC] Security Hygiene
Milestone Release - Kickoff ph...
[SEC-GENERIC] Threat Modeling
0/1
Add a card
2022 Thoughtworks

Account 1

Team 1

CATEGORY	IN PROGRESS	COMPLETED
User and role management	**2**	**1**
Secrets Management	**1**	**0**
Data	**0**	**1**
Infrastructure	**0**	**1**

Team 2

CATEGORY	IN PROGRESS	COMPLETED
User and role management	**1**	**2**
Secrets Management	**1**	**0**
Data	**2**	**1**
Infrastructure	**1**	**0**

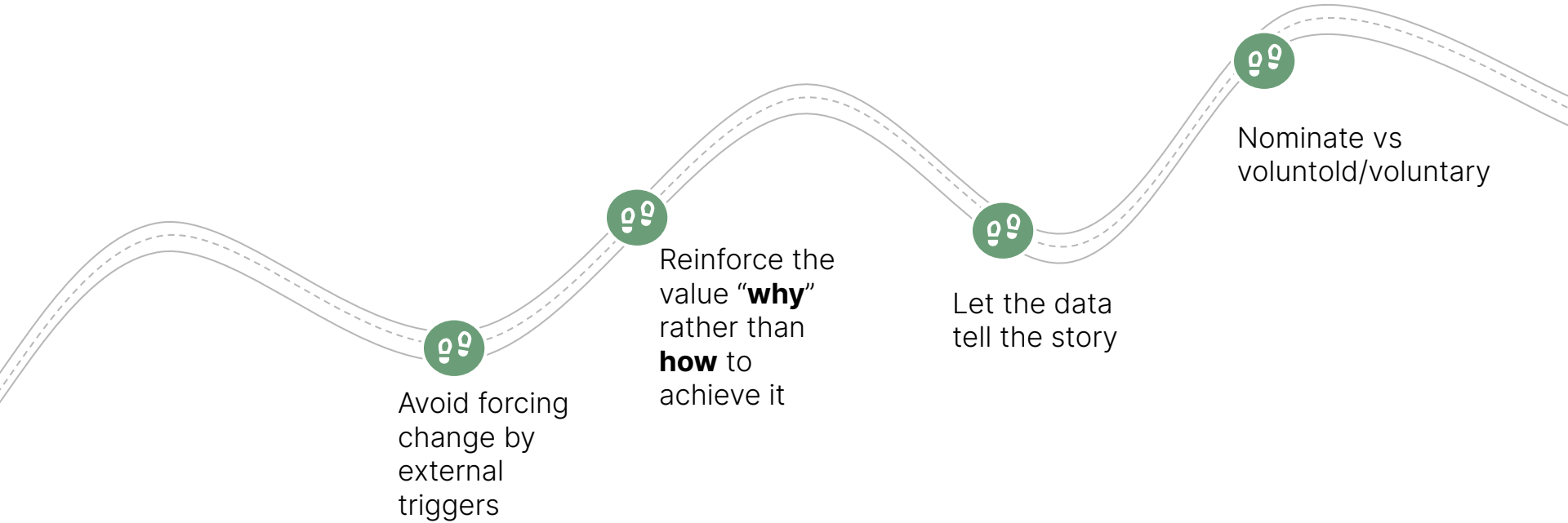
APPLICATION SECURITY MATURITY STAGES

Journey of the delivery teams to reduce security debt and achieve application & infrastructure security standards

Level 0	Level 1	Level 2	Level 3	Level 4
SECURITY PROCESS AND CONTROLS **UNORGANIZED AND REACTIVE**. PROCESS NOT DEFINED AND DOCUMENTED	**BASIC*** SECURITY PROCESSES AND CONTROLS ARE **IMPLEMENTED**. **PROACTIVE. REPEATABLE PROCESSES** PARTIALLY IN PLACE	**ALL** SECURITY PROCESSES AND CONTROLS ARE **IMPLEMENTED**. **PROACTIVE. REPEATABLE PROCESSES** PARTIALLY IN PLACE	**ALL** CONTROLS AND PROCESSES **REPEATABLE AND DEFINED**	CONTINUOUS MONITORING AND REMEDIATION
Team 1 Team 2	Team 3			

*Basic controls include: Security Awareness & Training, Threat Assessment, Security Incident Management, User and Role Management, Infrastructure, Secure Secrets Management, Data Security

What will make the process effective for teams?

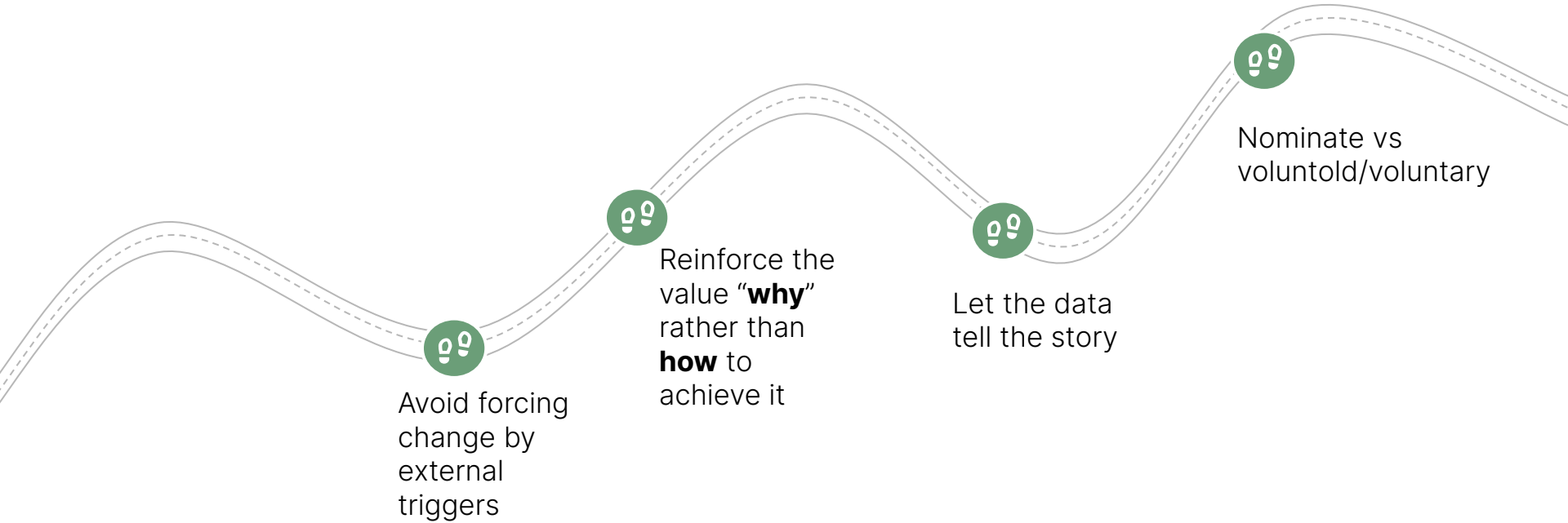


Nominations

Ownership

Community

What will make the process effective for teams?



Rollout Feedback

Some key reflections of our approach

1. Keep it human centric, collaborative
2. Use workflows that reduce friction
3. Follow hypothesis-driven development
4. **Make ourselves redundant**
5. Reinforce the power of why

My two part series **blog** with more details of the **impact-driven approach to security consulting**

about.me