The 7 Habits of Highly Mature Products

Inspired by The 7 Habits of Highly Effective People
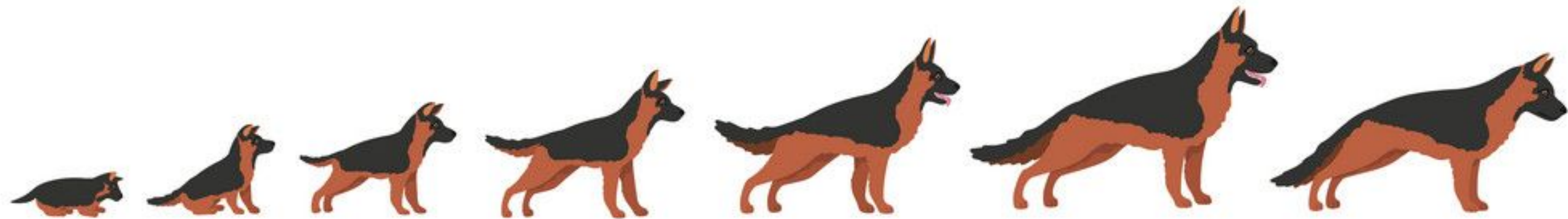
Jamie Ooi

AISA

whoami

- Chief Operating Officer, elttam
  Security Testing Partner of Australia's Top Technology Teams

- Director (Pacific), Trustwave SpiderLabs

- Various technical security consulting roles

- Embedded electronics engineer - automotive

- Ornithologist and botanist

- Guest lecture, sessional teacher, mentor at Swinburne University of Technology
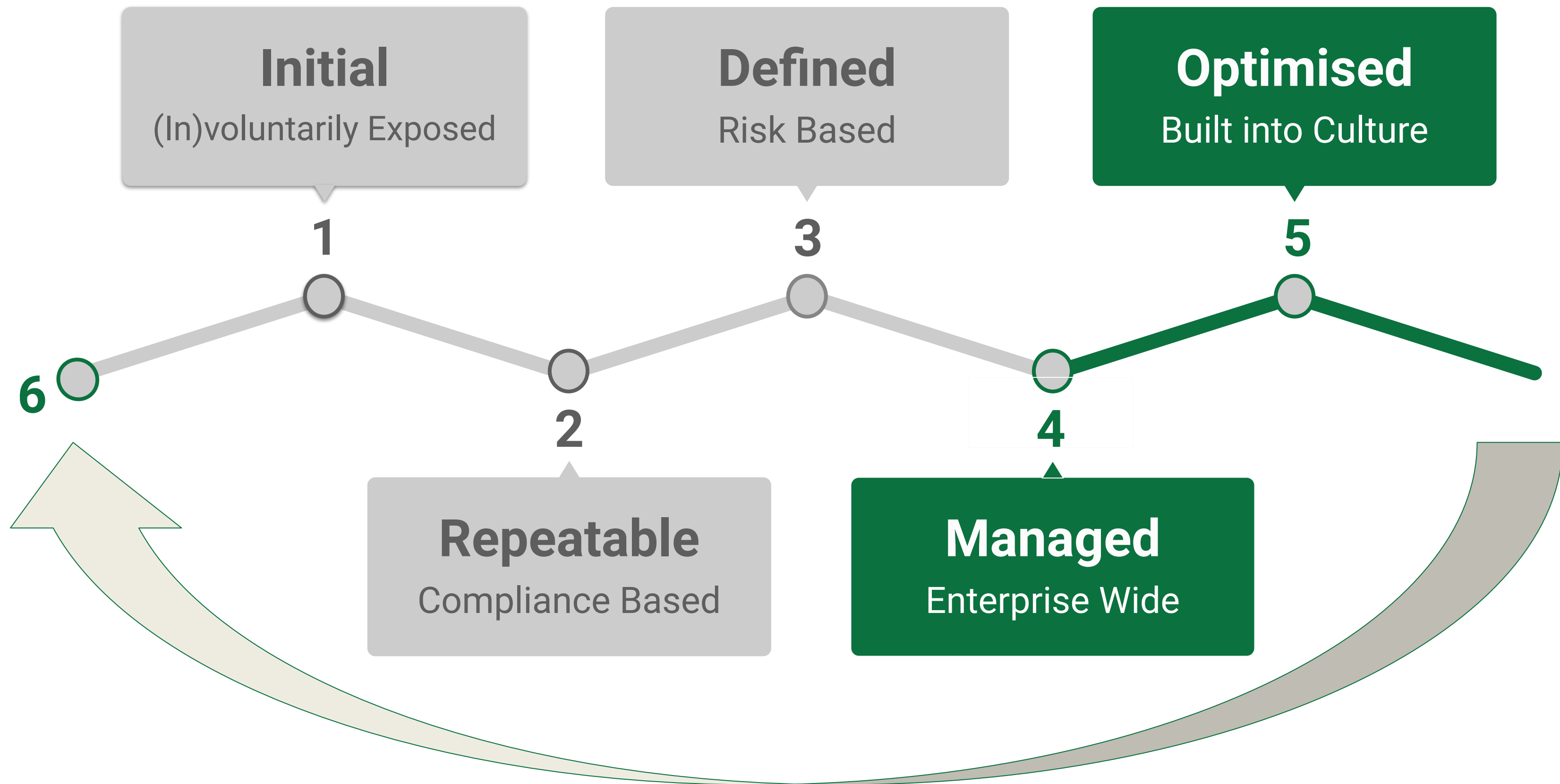
Connect with me on LinkedIn: https://www.linkedin.com/in/jamie-ooi-15297b98/

Agenda

1. The 7 stages of security maturity

2. The 7 observations of growing pains

3. The 7 habits to growing a highly mature product

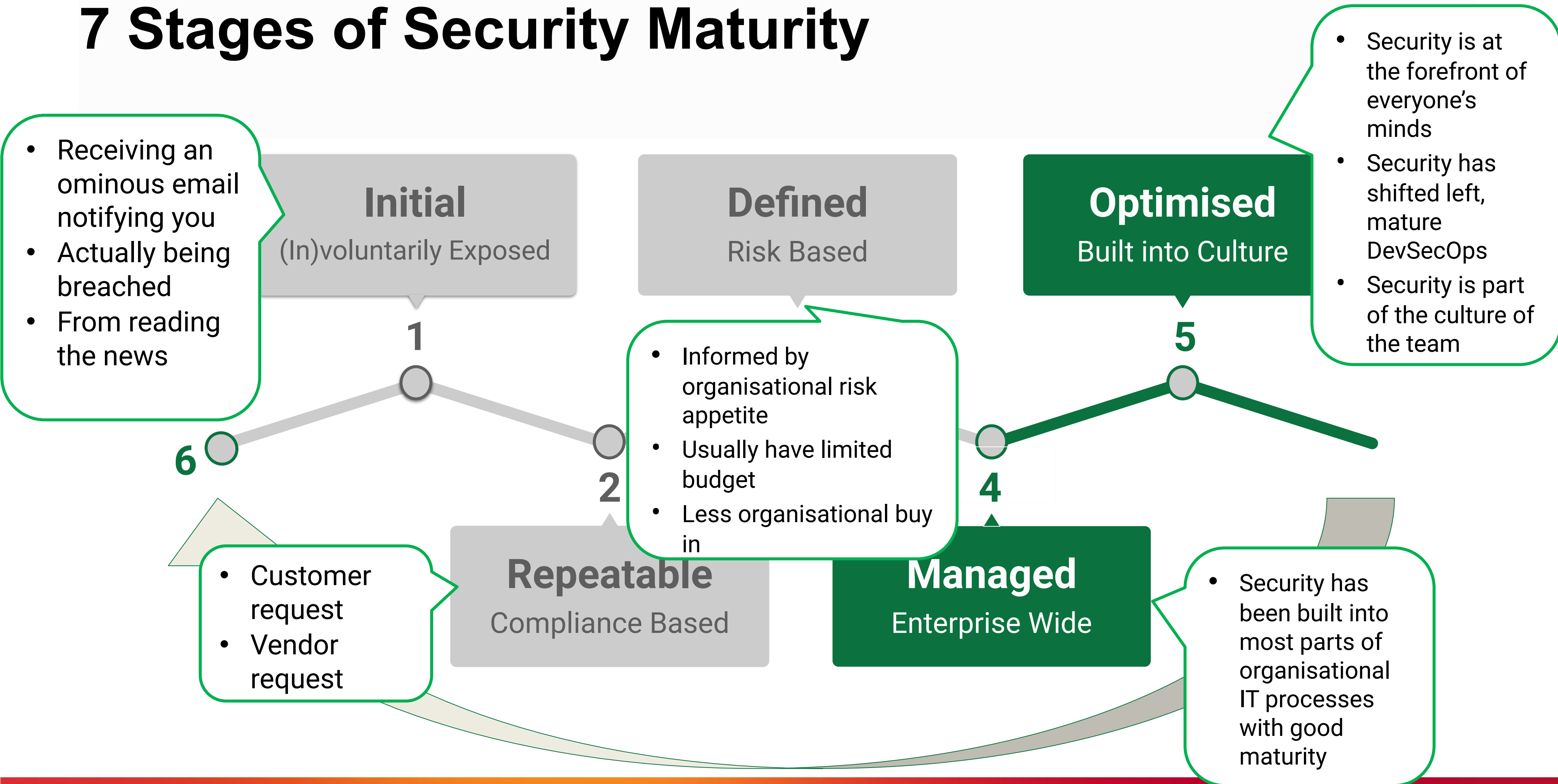# 7 Stages of Security Maturity
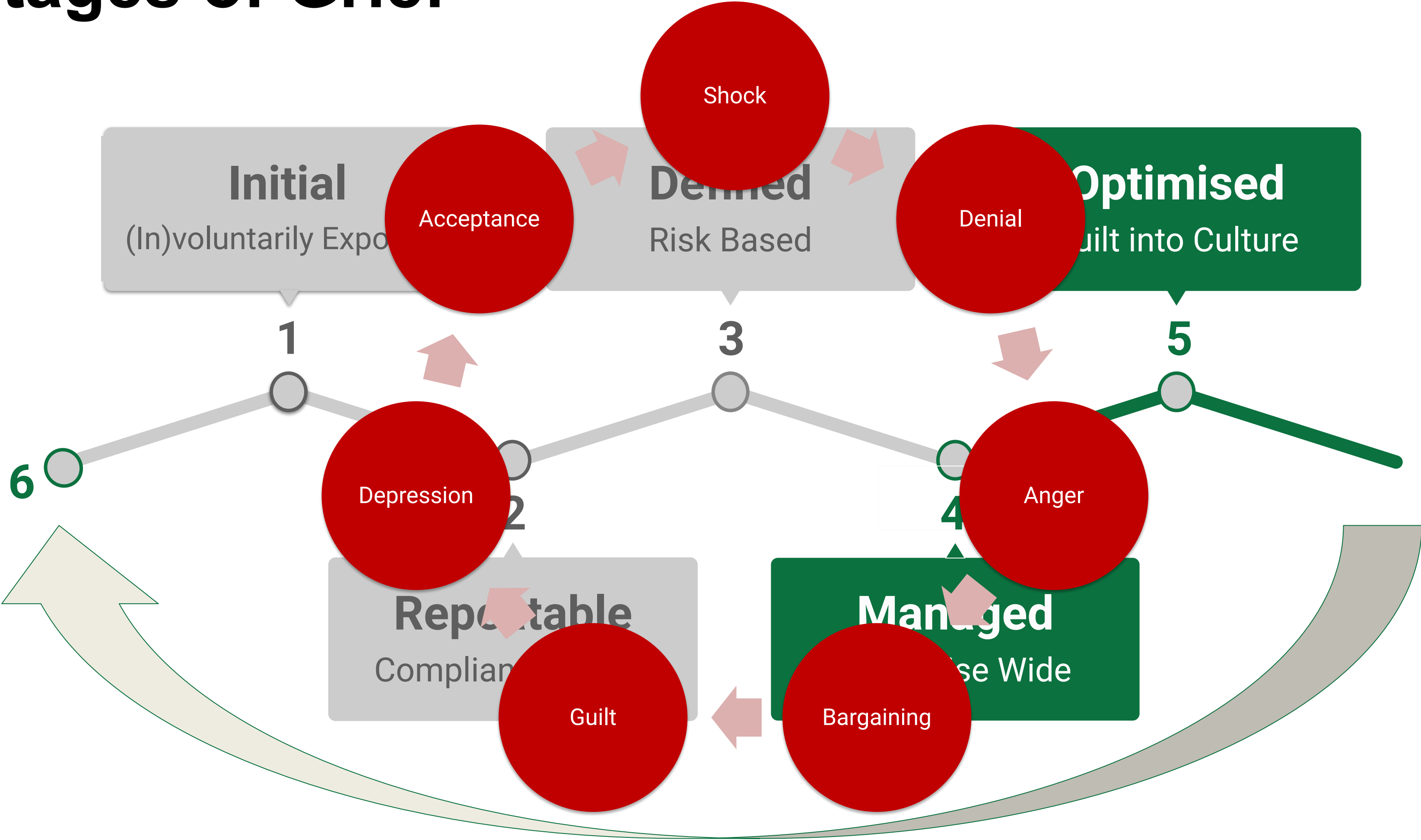Referenced from NIST CSF Maturity Model

Initial
(In)voluntarily Exposed

Defined
Risk Based

Optimised
Built into Culture

1

3

5

6

2

4

Repeatable
Compliance Based

Managed
Enterprise Wide

7 Stages of Security Maturity

Receiving an ominous email notifying you — Receiving an ominous email notifying you; Actually being breached; From reading the news

Initial (In)voluntarily Exposed — 1

Defined Risk Based — 2
- Informed by organisational risk appetite
- Usually have limited budget
- Less organisational buy in

Optimised Built into Culture — 5
- Security is at the forefront of everyone's minds
- Security has shifted left, mature DevSecOps
- Security is part of the culture of the team

6
- Customer request
- Vendor request

Repeatable Compliance Based

Managed Enterprise Wide — 4
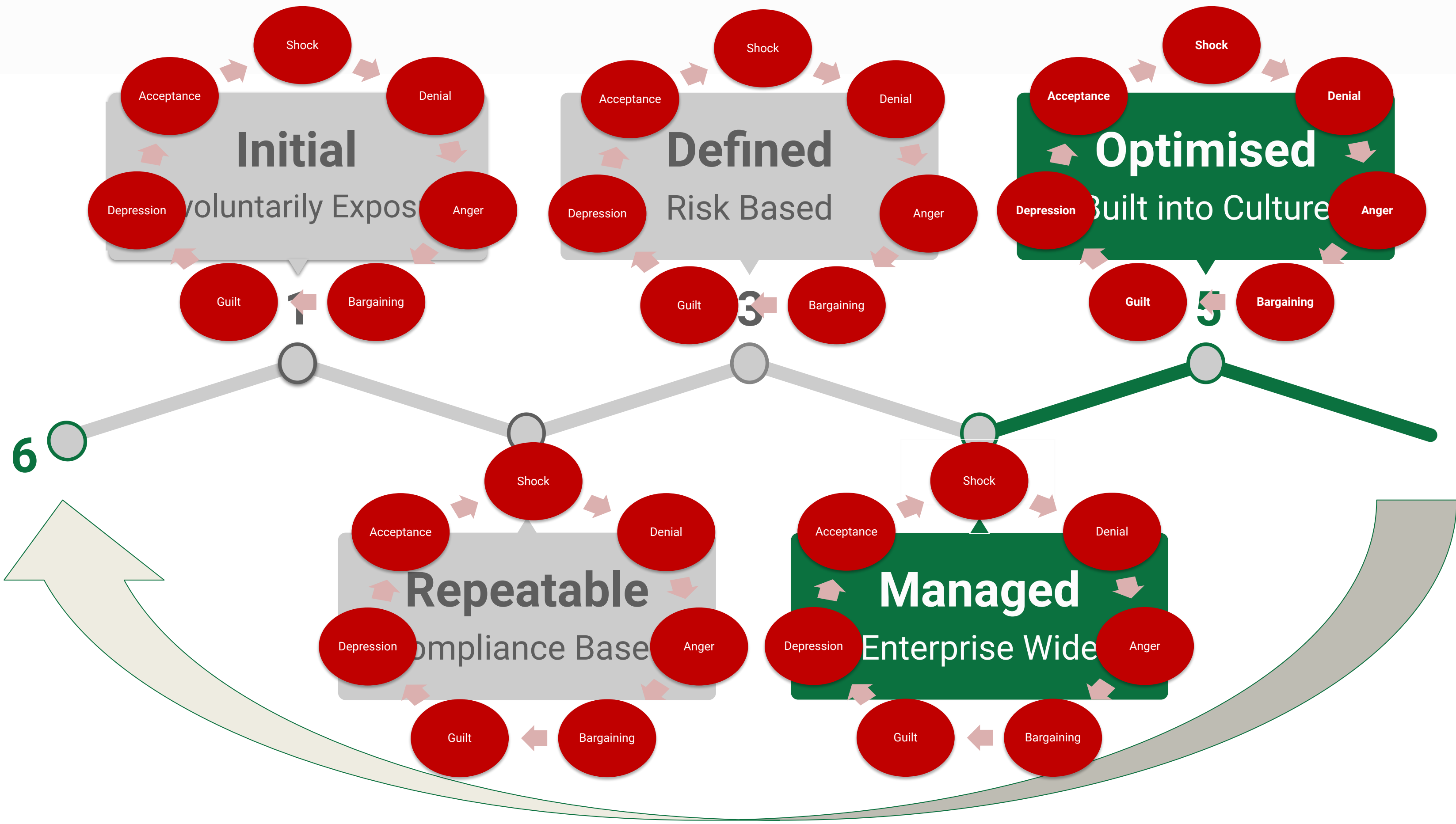- Security has been built into most parts of organisational IT processes with good maturity

7 Stages of Grief

7 Observations of Growing Pains

7 Observations of Growing Pains

1. Uninformed comparison
2. Competing stakeholders and priorities (not well received)
3. Overwhelmed with choices, tooling, methodology, un/trusted sources / advisory
4. Not having the required skill set
5. Budget restrictions
6. 50 teams all working independently (500 people within also working independently)
7. Scapegoat sacrificial lamb

7 Habits to Growing a Highly Mature Product
3 Core Areas
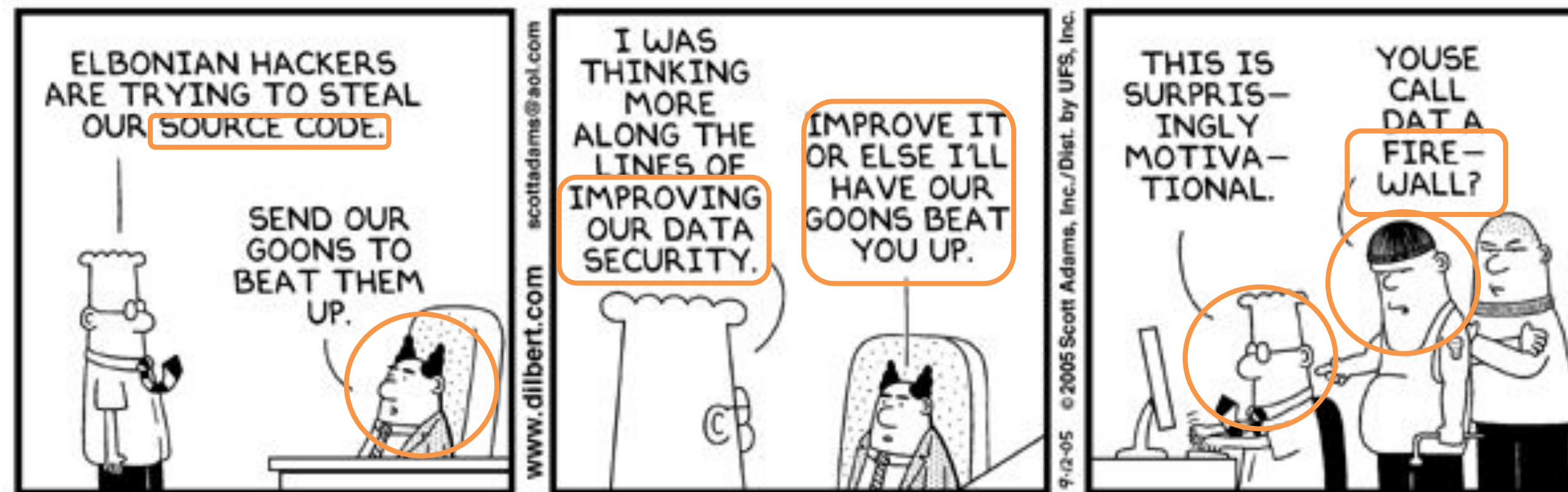
People

Process

Technology

Do this or else …

Source Code

Data Security

Firewall

The 7 Habits of Highly Mature Products

1. Quick Wins
2. Be Contextual
3. Templatise Everything
4. Shift Left, Rinse and Repeat
5. Cultivate Shared Responsibility
6. Monitor & Log
7. Right People in Right Seats

The 7 Habits of Highly Mature Products

1. Quick Wins (work smart not hard)

Goal: Achieve quick, impactful results with minimal resources

People

- Probably at Initial stages of security journey
- Lacks internal support, requires "ice breaking", and buy in
- Decisions are usually reactive
- Minimal resources available

Process

- Select top 3 high impact and low resource items, apply immediate mitigation; Repeat periodically until the next new lifecycle
- Raise security awareness in parallel while applying quick wins

Technology

- Must be achievable with the resources available
- Must be possible to achieve quickly
- Document, track progress of quick wins

The 7 Habits of Highly Mature Products

2. Be Contextual (why things are the way they are)

Goal: Align with business risks and objectives to inform decisions

People

- Security works across a few verticals
- Work collaboratively to understand context to meet shared objective

Process

- There is no such thing as one size fits all
- Too many choices can be overwhelming and cause indecision / inaction
- Understand and align with business context, risk appetite, objectives, goals, and priorities

Technology

- Understand technical environment setup and existing controls or tooling: why they are the way they are
- What is the best solution for your very unique environment for the available budget, at a strategic time

The 7 Habits of Highly Mature Products

3. Templatise Everything (also Standardise)

Goal: To de-hassle, reduce room for human error, and create sustainable scalable processes

People

- Remove opportunity for human error
- Reduce likelihood of compromise
- Make everyone's jobs easier

Process

- Align with "minimum viable security" / governing standards / benchmarks
- Test all templates / code / containers prior to use
- If it cannot be templatise it cannot be scaled, should you modify your approach

Technology

- Create a template for everything, where possible automate
- Use <everything> as code to create "Golden Images"
- Review, test and select the correct tooling as standard from the beginning

The 7 Habits of Highly Mature Products

4. Shift Left and Rinse and Repeat

Goal: Move security to the start of the DevOps / Product Lifecycle

People

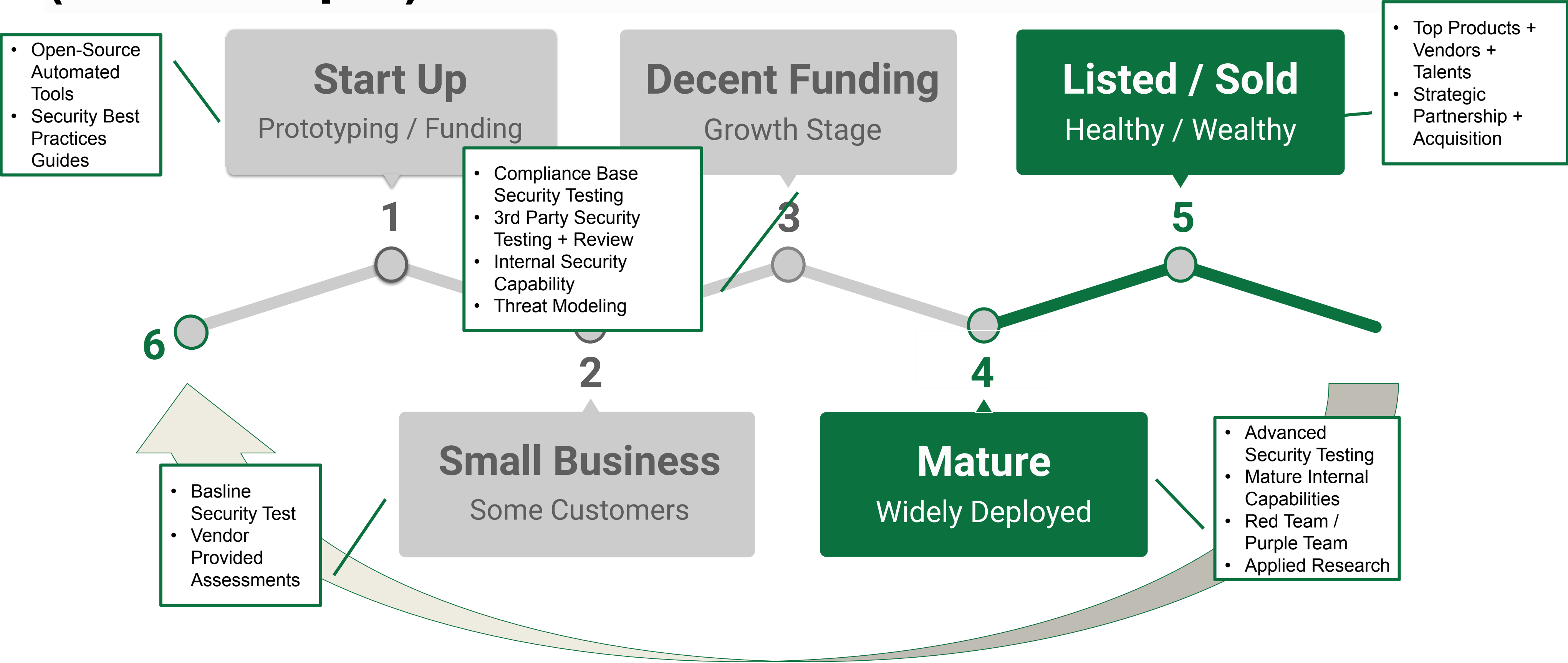- Work collaboratively from the start

Process

- Perform collaborative threat modeling
- Let your threat inform your decisions from the start

Technology

- Review and test everything, code, tools, standards, before introducing it into an existing / new environment

- Evaluate the security implementation, improve, repeat everywhere in product development lifecycle, organisational standards and processes where relevant

Vulnerability Management + Security Assurance (An Example)

Start Up
Prototyping / Funding

Decent Funding
Growth Stage

Listed / Sold
Healthy / Wealthy

Small Business
Some Customers

Mature
Widely Deployed

- Open-Source Automated Tools
- Security Best Practices Guides

- Compliance Base Security Testing
- 3rd Party Security Testing + Review
- Internal Security Capability
- Threat Modeling

- Top Products + Vendors + Talents
- Strategic Partnership + Acquisition

- Basline Security Test
- Vendor Provided Assessments

- Advanced Security Testing
- Mature Internal Capabilities
- Red Team / Purple Team
- Applied Research

1 2 3 4 5 6

The 7 Habits of Highly Mature Products

5. Cultivate Shared Responsibility

Goal: Have an inclusive, collaborative culture that encourages ownership

People

- Cultivate a shared responsibility culture where everyone is responsible for securing their own people, process and technology
- Promote a culture of collaboration - how can I help you achieve our shared goals

Process

- Include all relevant stakeholders in decision making, do not include people retrospectively;
- Encourage ownership of decision and accountability with formal authorisation processes

Technology

- Make use of collaborative platforms with Identity Access Management best practices to encourage accountability, traceability and ownership

The 7 Habits of Highly Mature Products

6. Monitor and Log (Everyone on the Same Page)

Goal: Traceability, visibility and accountability

People

- Foster a culture of shared responsibility where everyone is held accountable for their area of ownership and encourage collaboration

Process

- Have a centralise dashboard to quickly visualise to encourage transparency, track accountability and encourage sharing of resources

Technology

- Monitor and log all key processes, tasks and controls
- Automated, timely and up-to-date communication

The 7 Habits of Highly Mature Products

7. Right People in the Right Seats

> **Goal**: Ensure that the right skill sets are strategically available at the right places
> *This is how you will achieve the first 6 habits*

People

- Look internally, self evaluate and determine "success factors"
- Identify strengths and gaps
- Ensure that skill sets are allocated strategically and efficiently

Process

- Ensure that you have the right skill sets for the correct tasks, and provide regular and periodical training; Hiring, retaining, promoting and reallocating of people where required
- Identify strategic long term partnership to support you on your journey

Contact

Jamie Ooi
jamie@elttam.com