But I want all the shiny things... How to align offensive security with your maturity and threat models

Me

Cofounder/Commercial Director @ Tanto Security

Worked with customers on a lot of offensive security engagements

I have seen good and bad uses of Offensive Security

I know a little… but still learning all the time

This talk is for people earlier in the journey but wanting to understand the full spectrum that can be provided under the banner of Offensive Security Services

What’s the challenge?

Organisations can struggle to identify which offensive security services are most suited for their circumstances.

The Goal & Key Takeaway

The Goal

- Pragmatic Approach
- Understanding of Maturity
- Application of appropriate Threat Models

Key Takeaway

- Match services to level of maturity and threat model
- Closely align services to overall objectives
- Ensure value for money

What is Offensive Security

Offensive security is the **proactive approach to securing networks and systems from attacks** by actively seeking out vulnerabilities and weaknesses.

Can include:

- Threat Intel
- Vulnerability Scans
- Penetration Testing
- Assumed Breach
- Bug Bounties
- Code/Config Reviews
- Red Team
- Purple Team

Threat Models 101

Threat modelling is analysing representations of a system to highlight concerns about security and privacy characteristics.

If you have never done Threat Modelling before start with:

- Threat Modelling Manifesto - https://www.threatmodelingmanifesto.org/

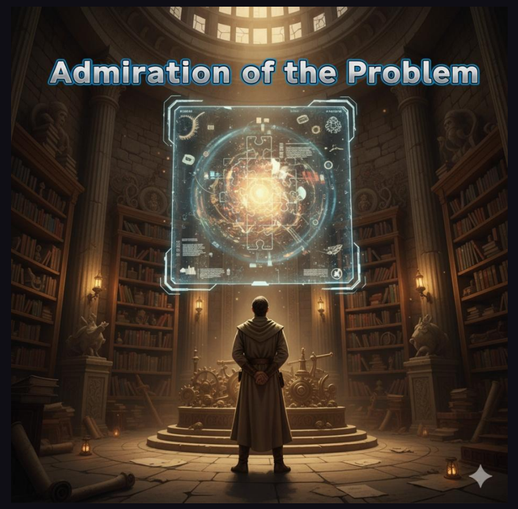
- Fast, Cheap + Good Whitepaper – Adam Shostack - https://shostack.org/blog/fast-cheap-good/

Fast, Cheap + Good Whitepaper

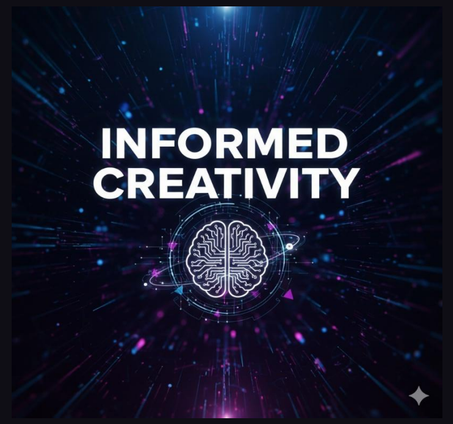
- It is possible to find approaches that are **fast, cheap, and good enough** to be valuable
- Shows the value of ‘lightweight’ models
- Presents 9 Fast Cheap and Good Approaches

Threat Modelling Manifesto

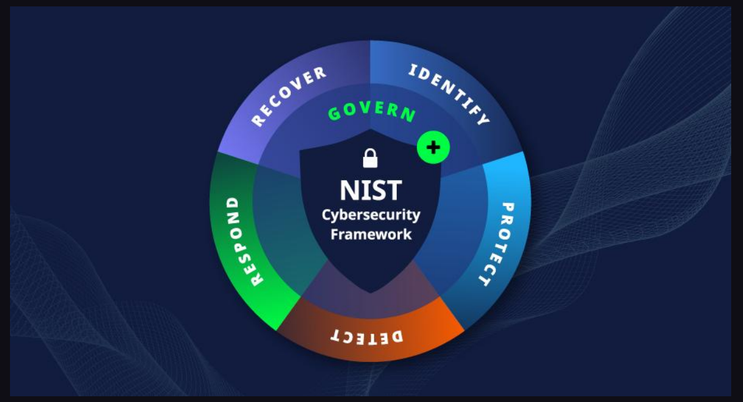
Threat Modelling Manifesto – Bad Patterns



Threat Modelling Manifesto – Good Patterns



Security Standards



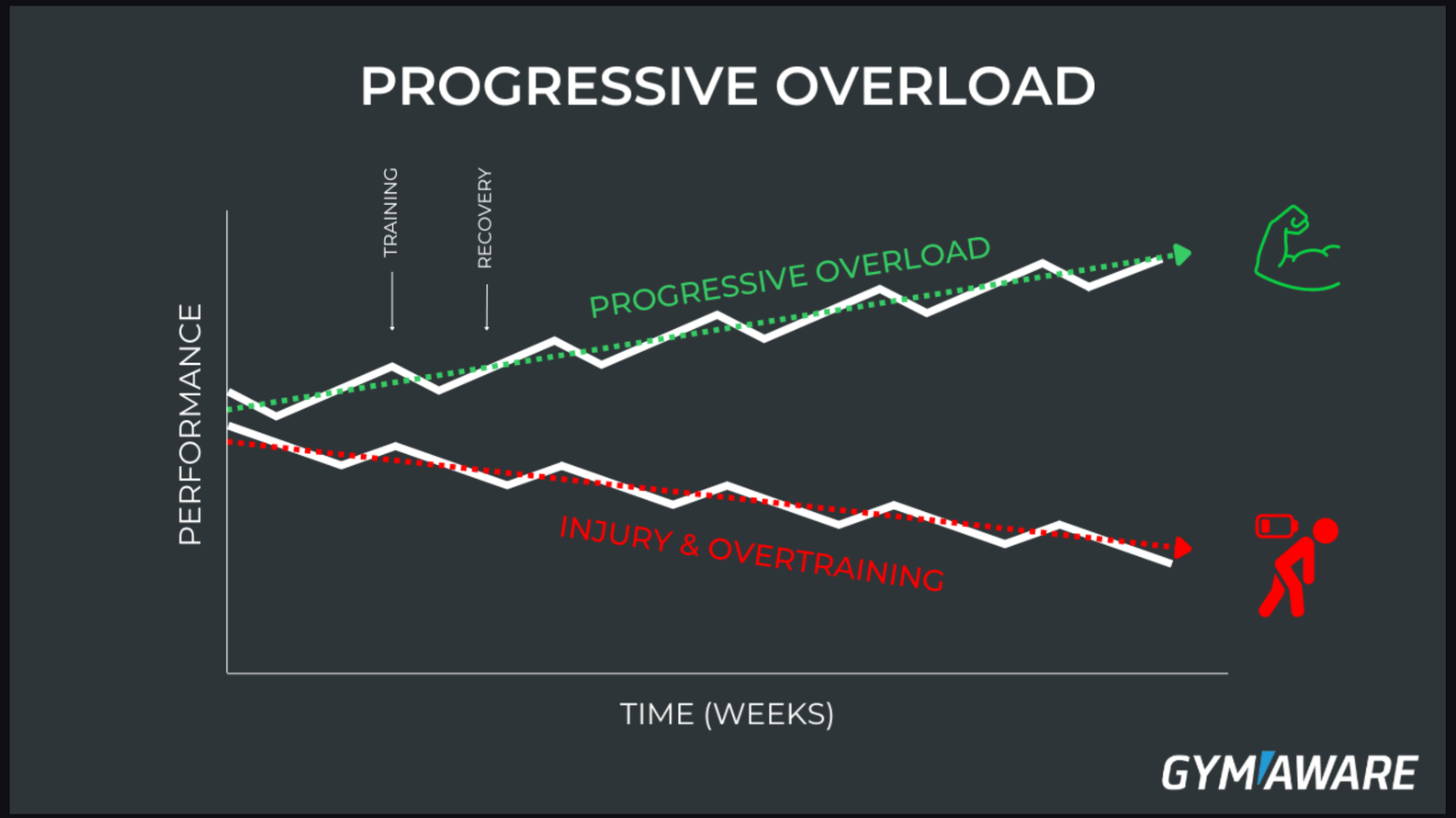
SOC 2

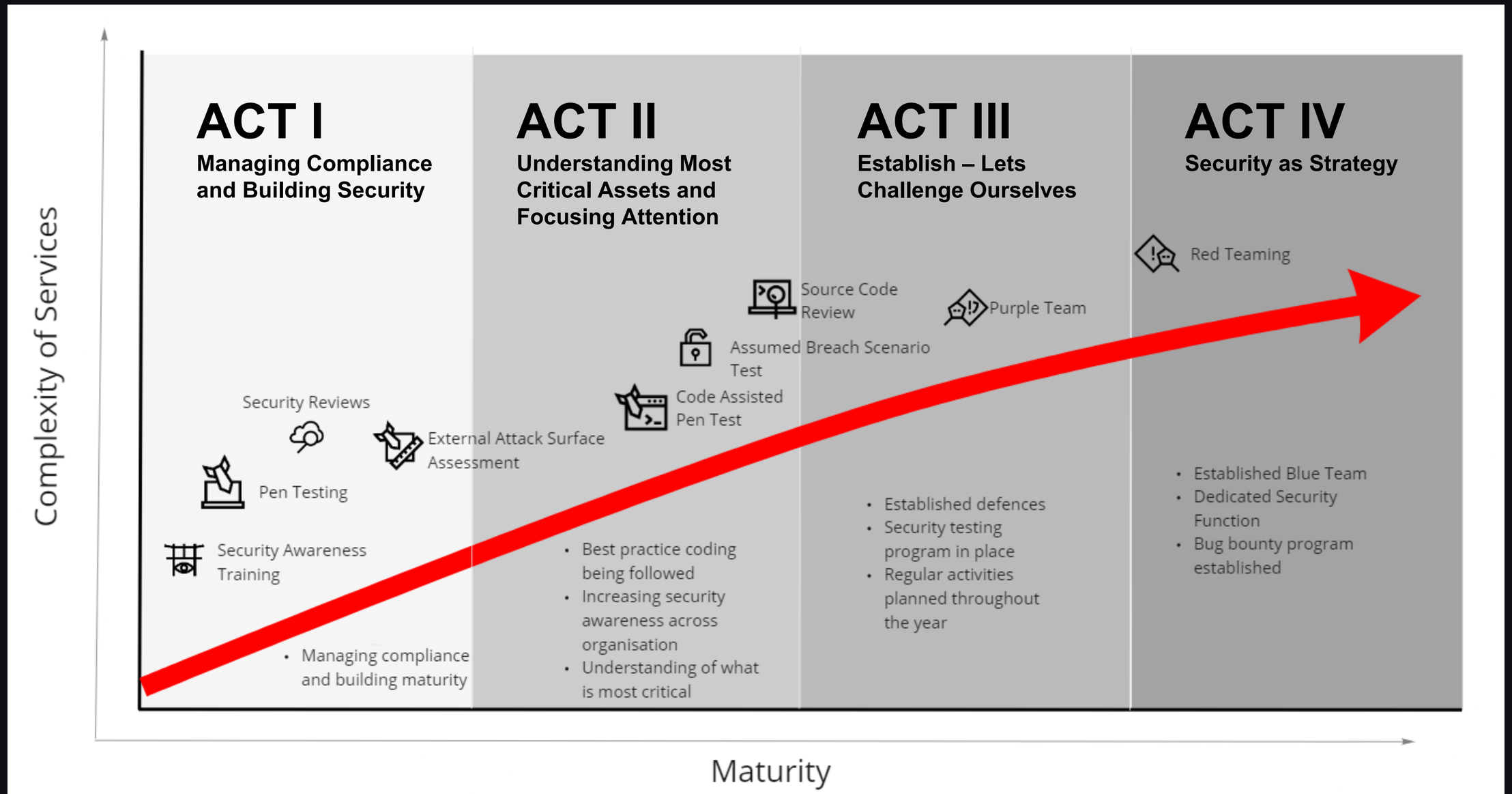
Australian Government
Australian Signals Directorate
ACSC
Australian
Cyber Security Centre
Essential 8

ISO
27001
Information Security
Management

PCI

Challenge but don’t overwhelm – Training your Security

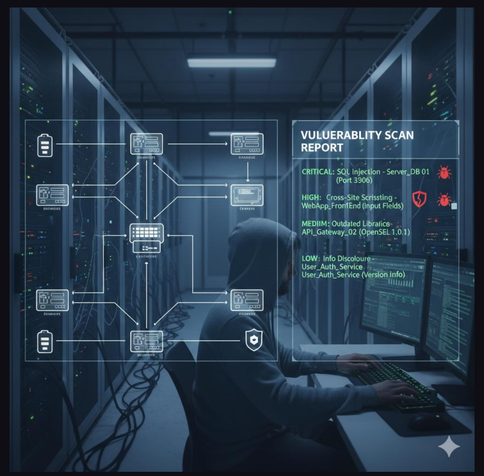



ACT I
Managing Compliance and Building Security
ACT II
Understanding Most Critical Assets and Focusing Attention
ACT III
Establish – Lets Challenge Ourselves
ACT IV
Security as Strategy
Complexity of Services
Maturity
Red Teaming
Source Code Review
Purple Team
Assumed Breach Scenario Test
Code Assisted Pen Test
Security Reviews
External Attack Surface Assessment
Pen Testing
Security Awareness Training
• Managing compliance and building maturity
• Best practice coding being followed
• Increasing security awareness across organisation
• Understanding of what is most critical
• Established defences
• Security testing program in place
• Regular activities planned throughout the year
• Established Blue Team
• Dedicated Security Function
• Bug bounty program established

Act I – Managing Compliance and Building Maturity

Time for a little threat modelling:

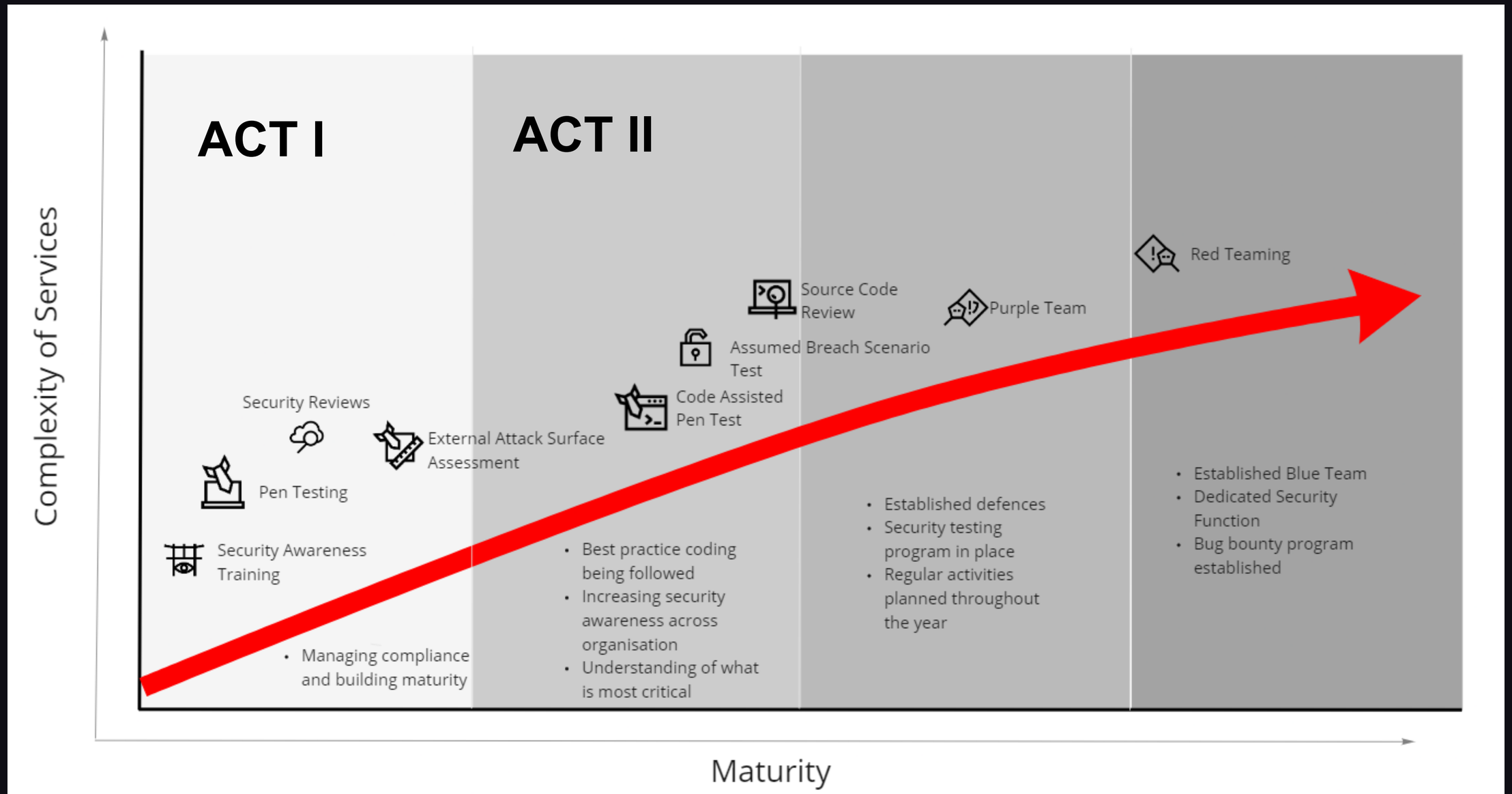
What could go wrong?



Act I – Managing Compliance and Building Maturity

- Customer requirements
- Compliance requirements
- Tie with high impact

- Security Awareness
- External Attack Surface Assessment
- Configuration Reviews
- Pen Testing on highest value assets


ACT I
ACT II
Complexity of Services
Maturity
Security Reviews
External Attack Surface Assessment
Pen Testing
Security Awareness Training
Code Assisted Pen Test
Assumed Breach Scenario Test
Source Code Review
Purple Team
Red Teaming
• Managing compliance and building maturity
• Best practice coding being followed
• Increasing security awareness across organisation
• Understanding of what is most critical
• Established defences
• Security testing program in place
• Regular activities planned throughout the year
• Established Blue Team
• Dedicated Security Function
• Bug bounty program established

Act II – Understand Most Critical Assets and Focus Attention

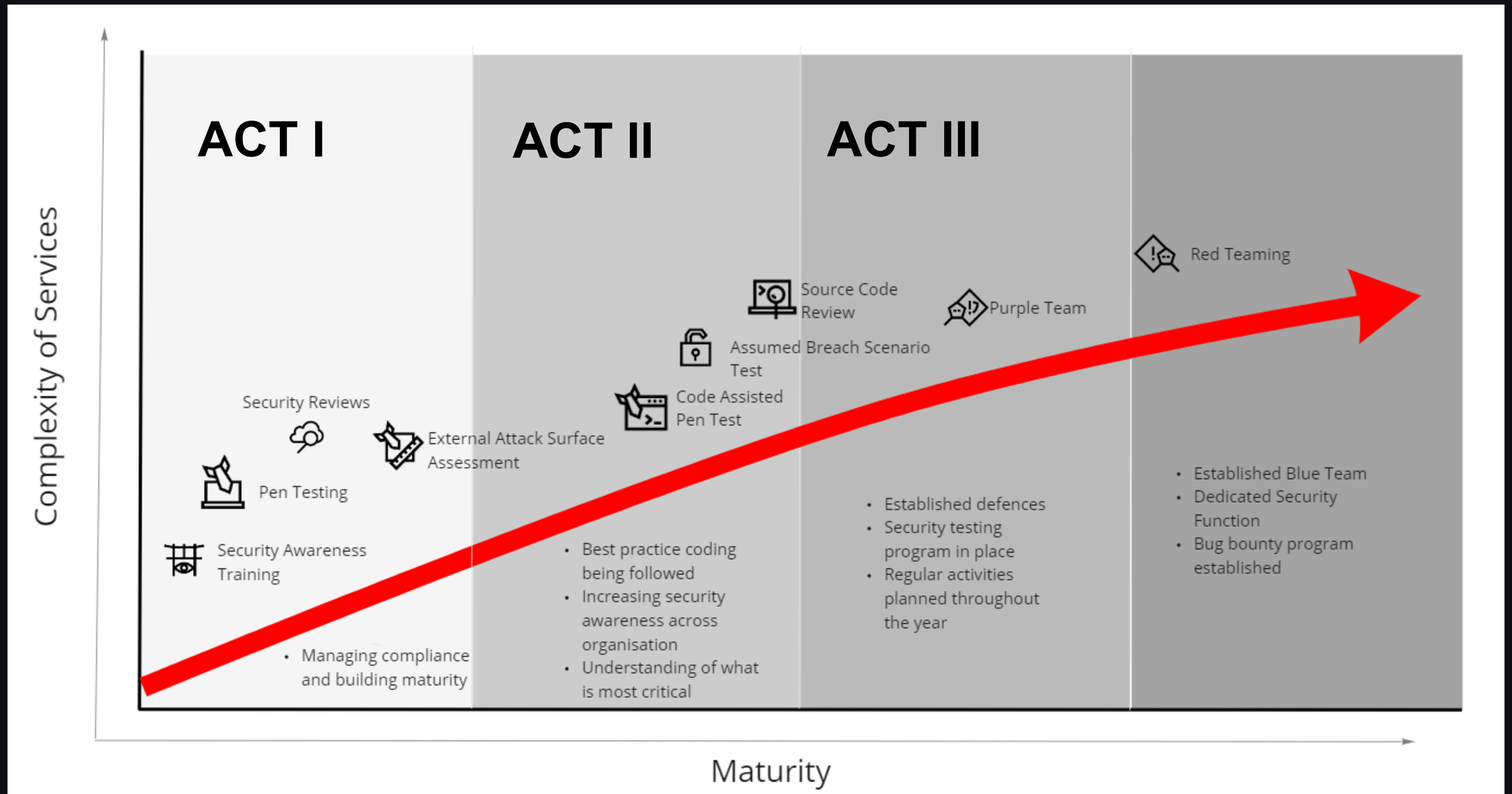
- Boxes are checked, lets start thinking a little deeper.
- Our Threat Model is getting constant input and this is shaping our strategy
- Keep up obligations to customers and compliance requirements
- But let’s start to think about deserves the most attention
- What is a ‘critical’ vulnerability in the context of your organisation

Act II – Understand Most Critical Assets and Focus Attention

- Code Assisted/White Box Penetration Testing

- Assumed Breach based on known threats

- Source Code Reviews

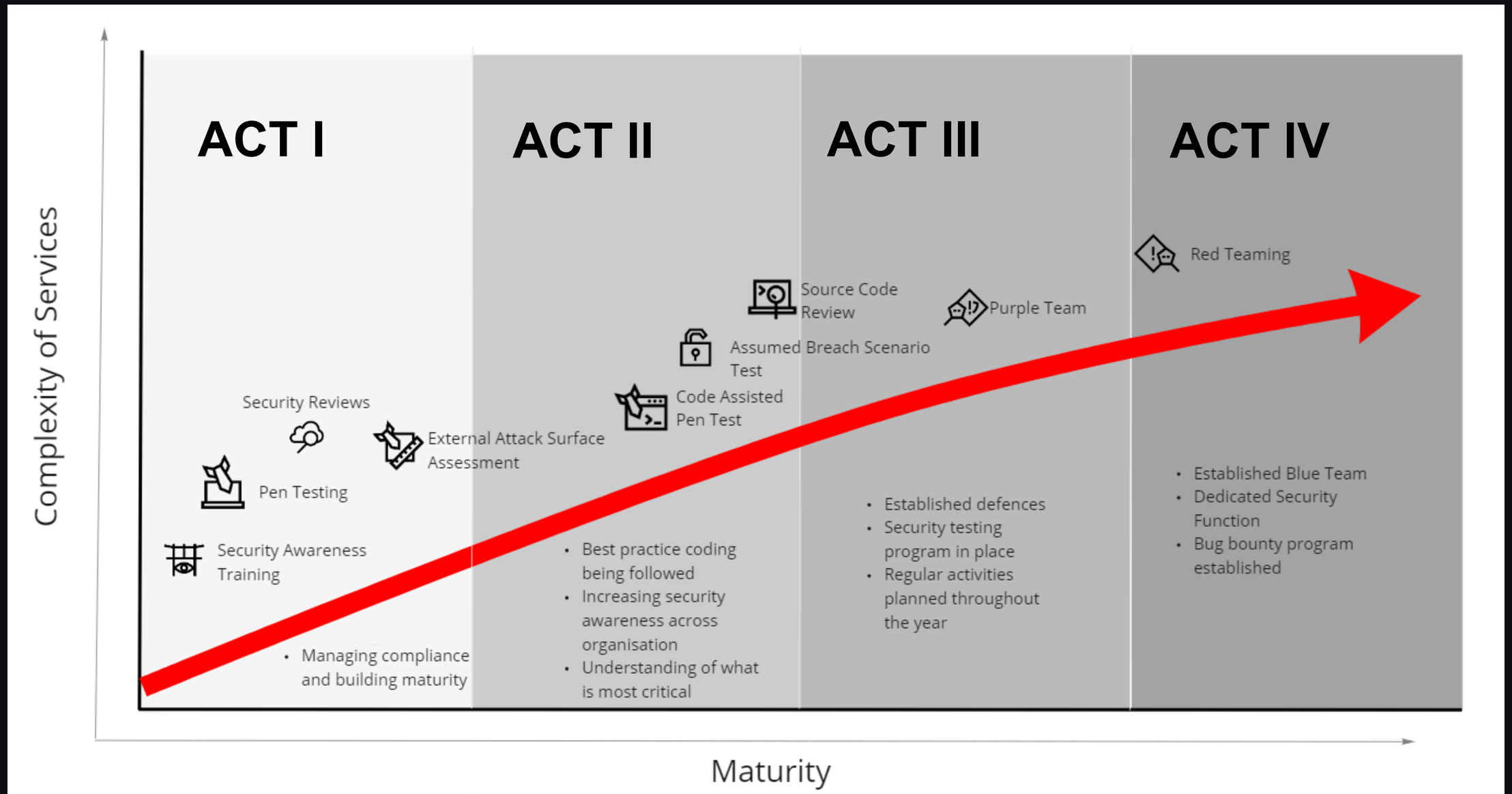

ACT I
ACT II
ACT III
Complexity of Services
Maturity
Security Reviews
External Attack Surface Assessment
Pen Testing
Security Awareness Training
Source Code Review
Purple Team
Red Teaming
Assumed Breach Scenario Test
Code Assisted Pen Test
• Managing compliance and building maturity
• Best practice coding being followed
• Increasing security awareness across organisation
• Understanding of what is most critical
• Established defences
• Security testing program in place
• Regular activities planned throughout the year
• Established Blue Team
• Dedicated Security Function
• Bug bounty program established

Act III – Established, lets challenge ourselves

- Our security strategy is well established
- The team is growing, and we are in a strong position
- Our defences are mature with internal capability complimented by third parties
- Activities are planned to ensure we can conduct them in the way we want

Act III – Established, lets challenge ourselves

- Established testing program
- Bug bounties
- Tabletop Exercises
- Purple Teaming


ACT I
ACT II
ACT III
ACT IV
Complexity of Services
Maturity
Security Reviews
External Attack Surface Assessment
Pen Testing
Security Awareness Training
Source Code Review
Purple Team
Assumed Breach Scenario Test
Code Assisted Pen Test
Red Teaming
• Managing compliance and building maturity
• Best practice coding being followed
• Increasing security awareness across organisation
• Understanding of what is most critical
• Established defences
• Security testing program in place
• Regular activities planned throughout the year
• Established Blue Team
• Dedicated Security Function
• Bug bounty program established

Act IV – Security as Strategy

- Entire organisation is buying into
- Evolve practices to up to date threats
- Bespoke capabilities
- Mature threat model

Multi layered approach to Offensive Security:

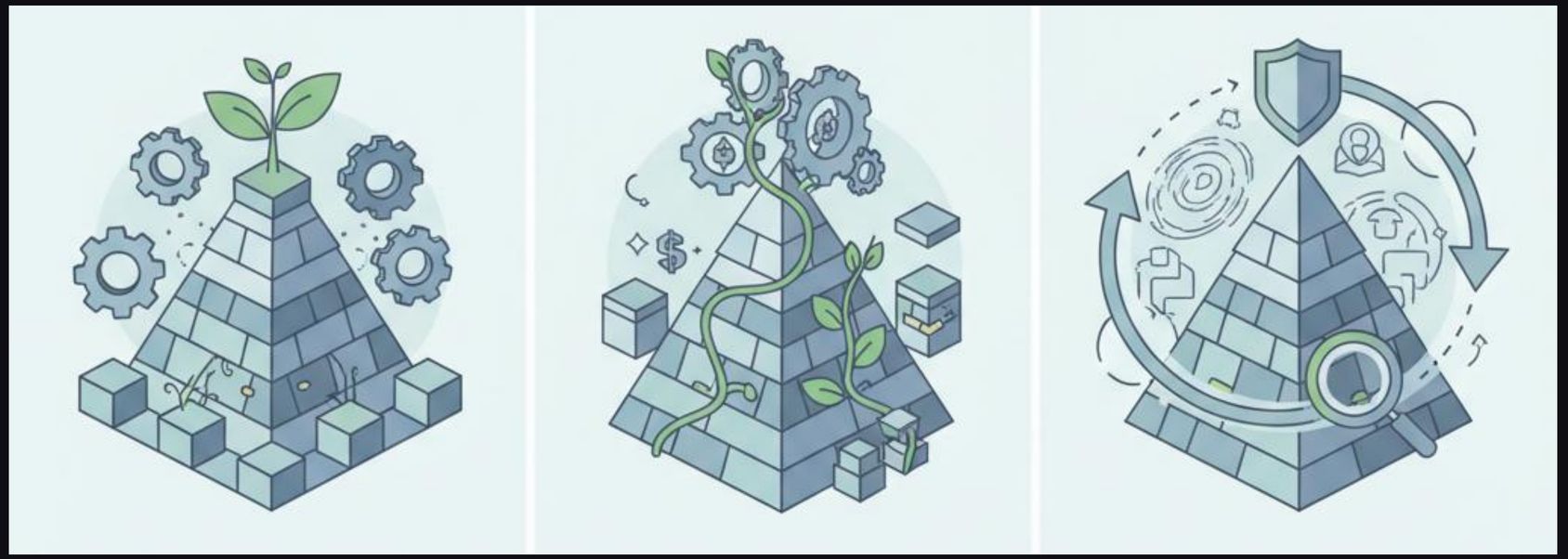
- In depth code assisted testing at least annually
- Regular bug bounty program
- Clear playbooks and threat models
- Objective based Red Teams based on real world threats and up to date Threat Intel

Stunt Hacking

How to get the most from every test

- Plan and engage early
- Find and work with trusted partners
  - Be clear about what is expected
  - Encourage continuous feedback
  - Work to have open lines of communication, before, during and after every engagement

Implementing an Effective Offensive Security Program



Start with Basics
Begin with foundational services

Develop Incrementally
Gradually increase complexity as you mature

Continuously Reassess
Regularly review and adjust as needed

Summary

- Understand various types of Offensive Security
- Know what suits your circumstances

- Pragmatic Approach
- Understanding of Maturity
- Application of appropriate Threat Models

- Know what will work best
- Get value for money

marco@tantosec.com

https://www.linkedin.com/in/marcocantarella1/

https://www.linkedin.com/company/tantosec

https://tantosec.com/blog