Security is an Awesome Product Feature

Mark Hahn
linkedin.com/in/markphahn

October 12, 2022
DevSecOps Days 2022 - Washington DC
https://resources.sei.cmu.edu/news-events/events/devsecops/

Mark Hahn
Director, Cloud Strategies, SRE and DevOps

Mark has 30+ years of experience as a Principal Architect delivering large-scale systems, including Wall Street trading systems, multinational retail payments systems and supply chain systems. Mark practices and coaches continuous delivery techniques that improve delivery timelines and increase system reliability, including Lean software development and continuous improvement.

Braking Down Security Podcast

“teams want to work on awesome features, not security, and they don't realize that security is an awesome feature”

-@noid

tcbtech.com/awesome

https://en.wiktionary.org/wiki/awesome

Etymology

From **awe** + **-some**; compare Old English eġeful (“fearful; inspiring awe”).

Adjective

awesome (comparative more awesome or awesomer, superlative most awesome or awesomest)

1. (dated) Causing awe or terror; inspiring wonder or excitement. [from 1590–1600.] *The waterfall in the middle of the rainforest was an awesome sight. The tsunami was awesome in its destructive power.*
2. (colloquial) Excellent, exciting, remarkable. *That was awesome!*

Describing Value

Teams need methods to evaluate the value and trade offs for security features:

- Relative Value
- Monetary Methods
- Checklists
- Frameworks

Relative Valuations

- Hard Requirements
  - Regulatory mandates
- Important Requirements
  - TLS and up to date cypher suites
  - OAuth2
  - Multi Factor Authentication
  - Encryption at rest
  - Correct Session Timeouts
- Nice to Haves
  - Application Firewall

Monetary Valuation

2022 IBM / Ponemon Data Breach Report

- Data Breach
  - $4.35 Million - average total cost of breach
  - $164 - average cost per record
- Regulations
  - €20 Million or 4% - minimum GDPR fine
  - $2,500 / consumer - CCPA Fine

https://www.ibm.com/reports/data-breach

Gartner: 12 Things to Get Right

1. Adapt the security testing tools and processes to the developers
2. Quit trying to eliminate all vulnerabilities during development
3. Identify and remove known open-source vulnerabilities
4. Don’t expect to use traditional dast/sast without changes
5. Train all developers on the basics of secure coding
6. Adopt a security champion model
7. Secure infrastructure with automation and infrastructure as code (IoC)
8. Implement strong version control on all code and components
9. Implement secrets management
10. Adopt an immutable infrastructure mindset
11. Rethink how service delivery incidents, including security, are handled
12. Use dynamic access provisioning for developers in DevSecOps

OWASP OpenSAMM Model

Governance	Design	Implementation	Verification	Operations
Strategy and Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy and Compliance	Security Requirements	Secure Deployment	Requirements-Driven Testing	Environment Management
Education and Guidance	Security Architecture	Defect Management	Security Testing	Operational Management

https://owaspsamm.org/

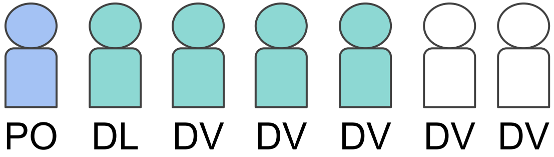
Agile Methods Empower Teams

Empowered teams can move fast and solve their own problems.

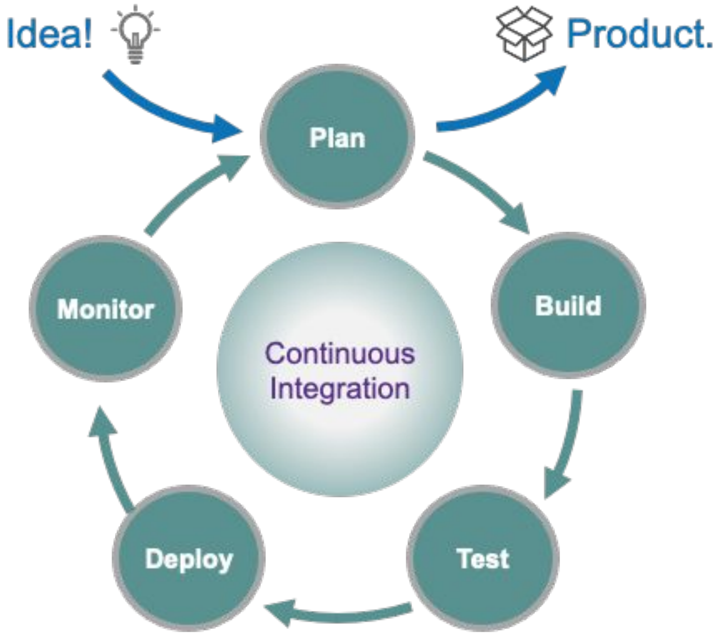
Empowered teams can collaborate with other teams directly without communication gaps.

Empowered teams can embrace security needs and prioritize security features for their product.

Cybersecurity is a Business Problem



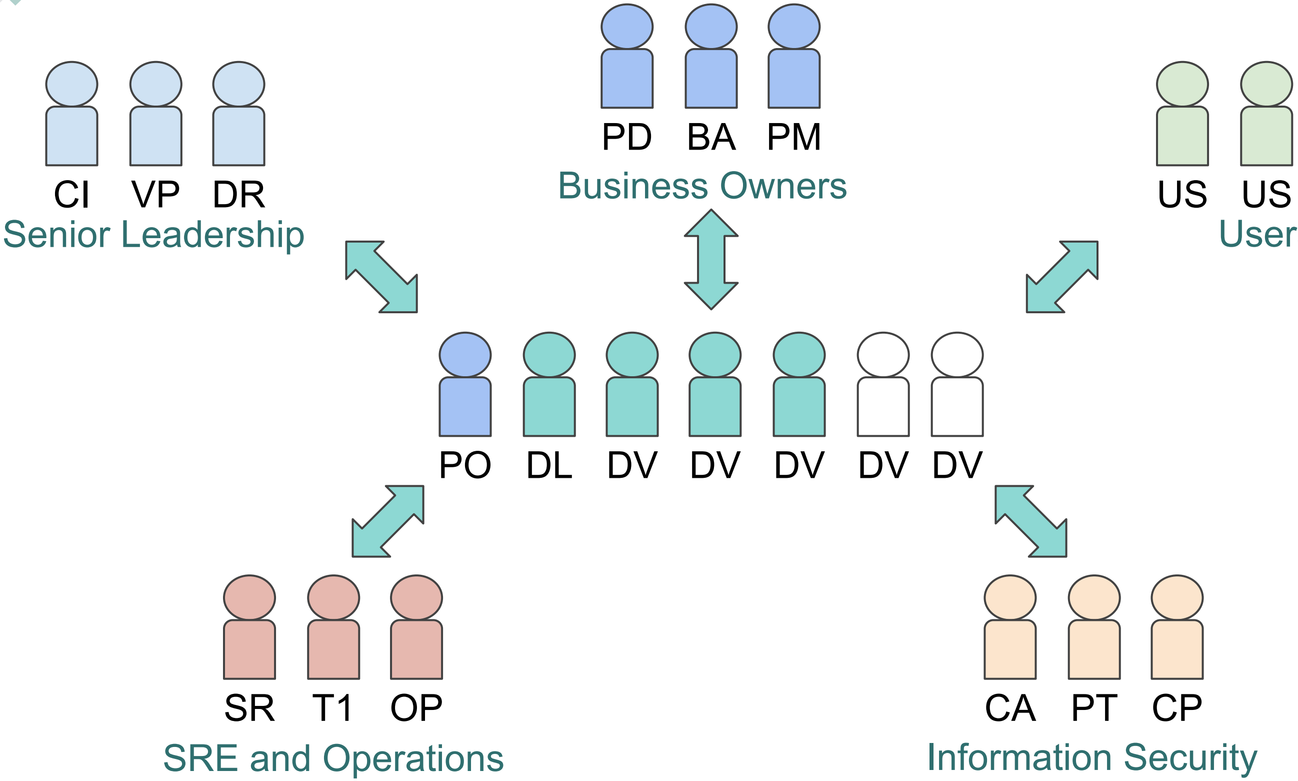
Empowered teams are responsible for all phases of software development.



Fire Doesn’t Innovate by Kip Boyle, ISBN-10: 1544513194

tcbtech.com/awesome

Business Value Chain



CI VP DR

Senior Leadership

PD BA PM

Business Owners

US US PU

Users

PO DL DV DV DV DV DV

SR T1 OP

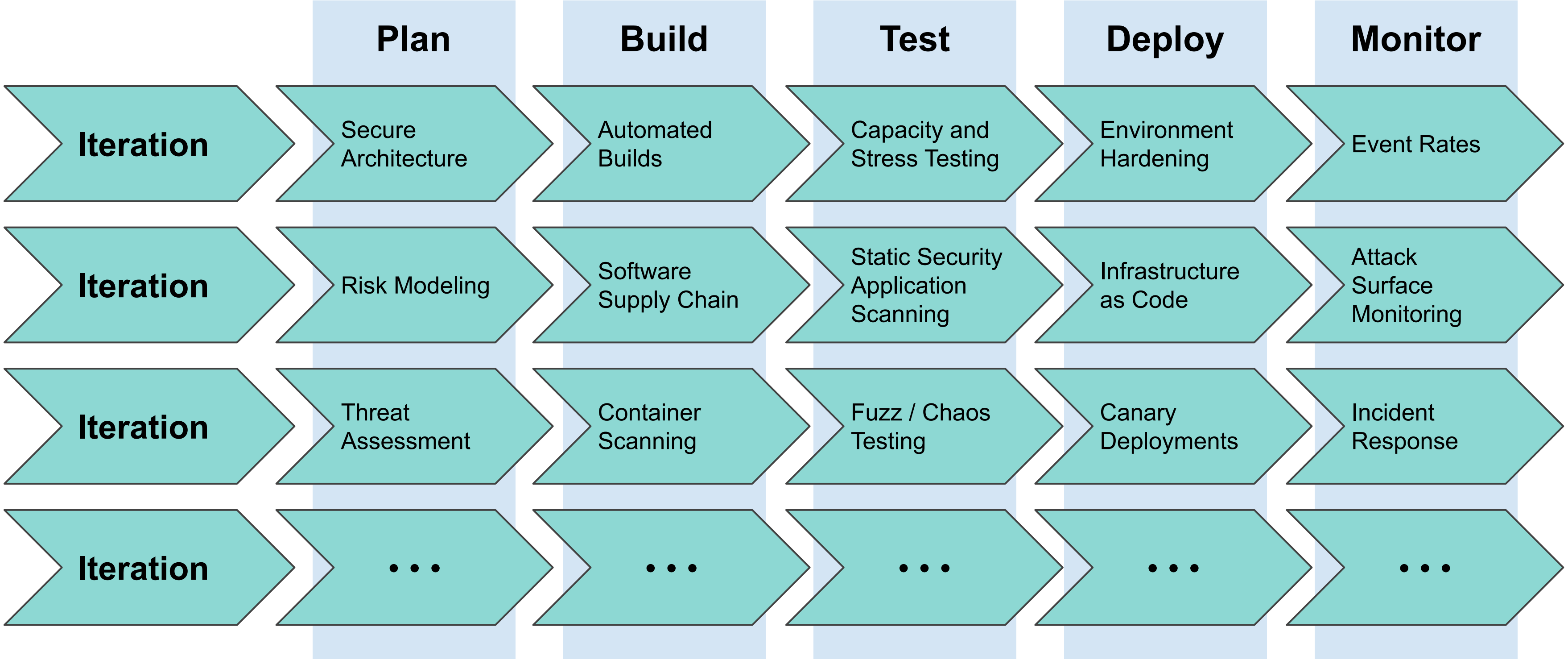
SRE and Operations

CA PT CP

Information Security

tcbtech.com/awesome

Iterative Approach



	Plan	Build	Test	Deploy	Monitor
Iteration	Secure Architecture	Automated Builds	Capacity and Stress Testing	Environment Hardening	Event Rates
Iteration	Risk Modeling	Software Supply Chain	Static Security Application Scanning	Infrastructure as Code	Attack Surface Monitoring
Iteration	Threat Assessment	Container Scanning	Fuzz / Chaos Testing	Canary Deployments	Incident Response
Iteration	• • •	• • •	• • •	• • •	• • •

tcbtech.com/awesome

Application Trust

- The business value of a system cannot be realized if the system is not trustworthy. To gain that trust information security requirements must be addressed.
- In many organizations, security features are added as requirements in a category called “non-functional requirements”.
- This category devalues these features. Product owners and development teams must value security aspects of the product as first-class features.

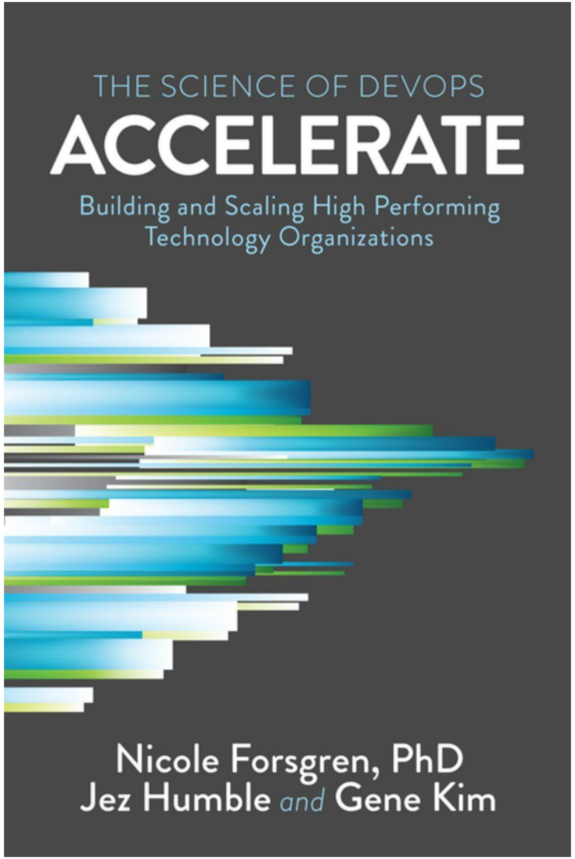
Security Culture

- Build a security culture
- Empower security champions
- Make small security steps at daily habit
- Learn to describe good security as return on investment
  - Not just risk avoided

https://owasp.org/www-project-security-culture/

Summary

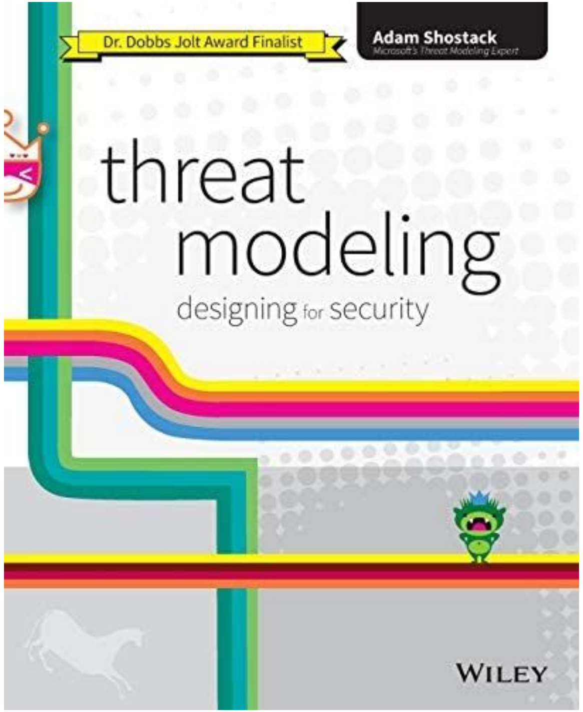
- Help your organization empower development teams.
- Pose security requirements as product requirements which bring value
- Search for developers who finds security interesting
- Work iteratively - don’t boil the ocean



DevOps Efficiency Matrix

https://devopsefficiency.com/

An open source tool for evaluating the effectiveness of your product delivery process


Dr. Dobbs Jolt Award Finalist
Adam Shostack
Microsoft's Threat Modeling Expert
threat modeling
designing for security
WILEY

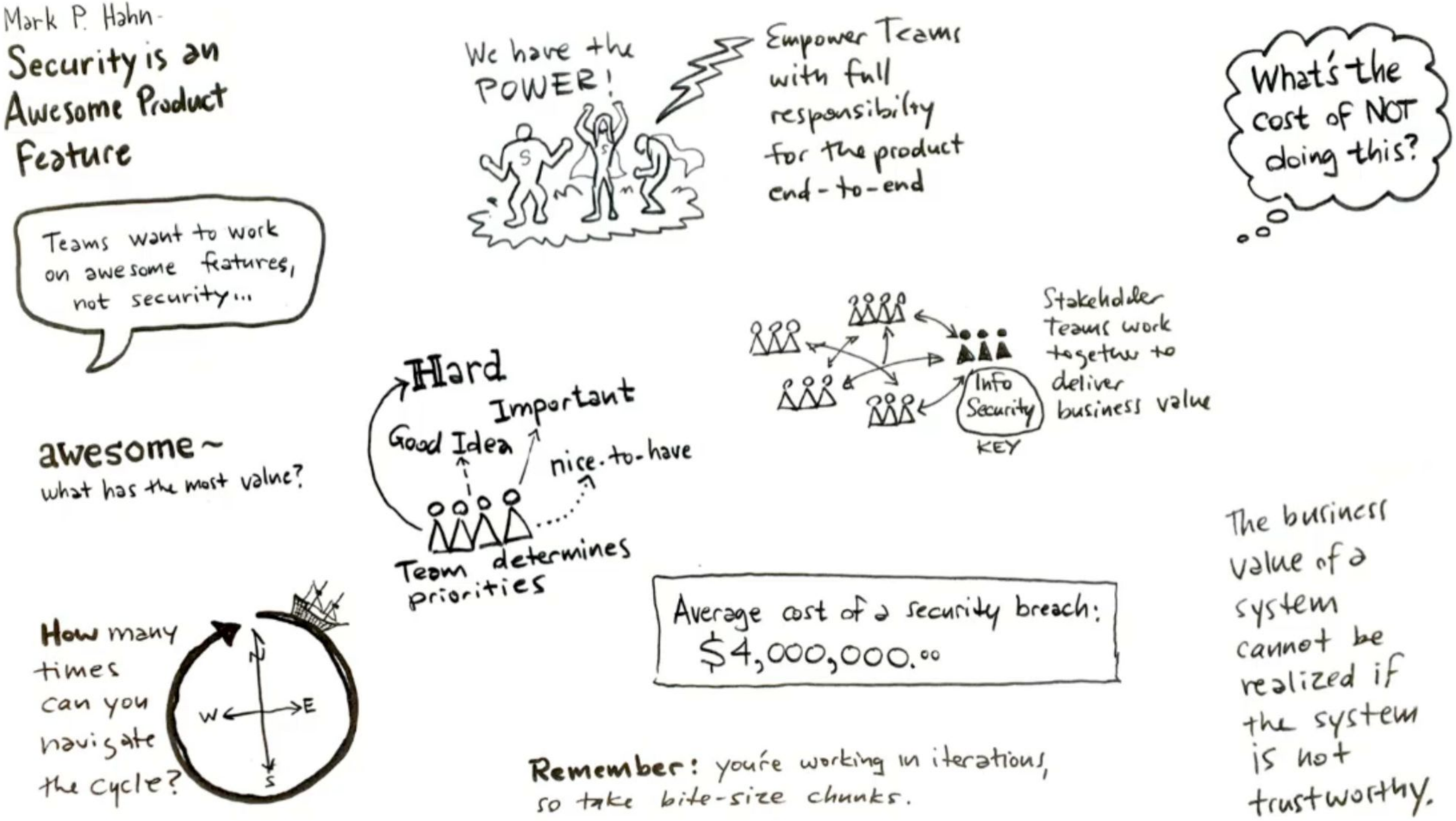
- Tools and a framework for structured thinking about what can go wrong.
- Jargon-free and accessible introduction to this essential skill.
- Techniques to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling.

Thank

You!

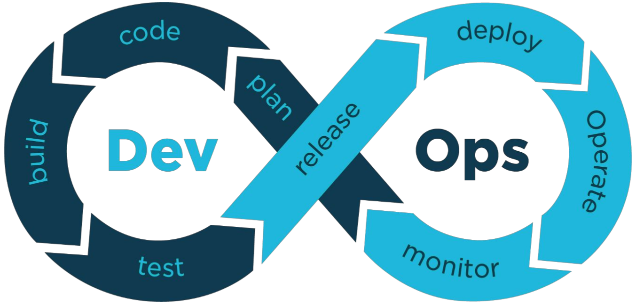
Mark Hahn

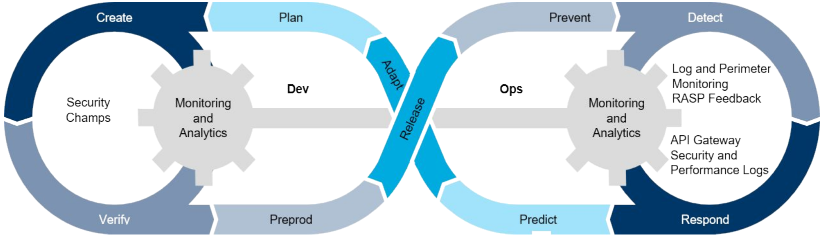
linkedin.com/in/markphahn

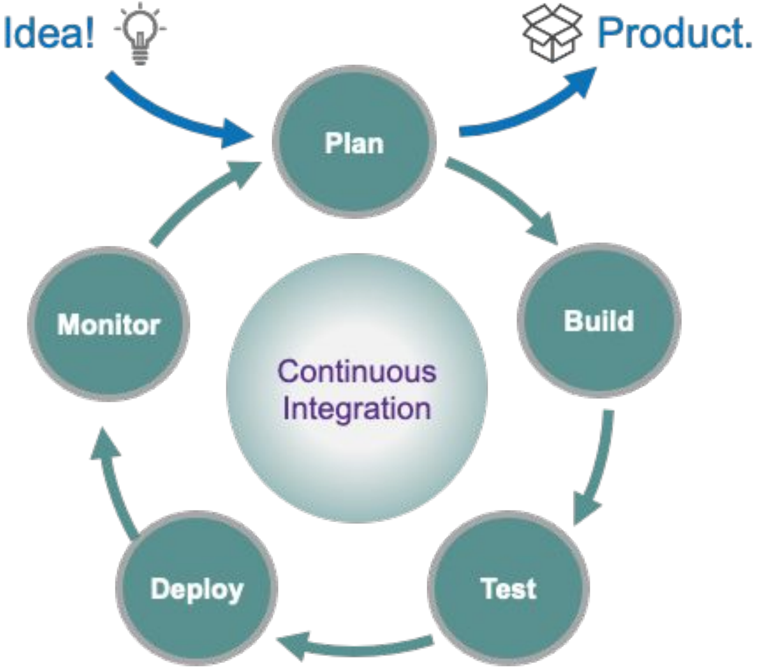

Mark P. Hahn
Security is an Awesome Product Feature
Teams want to work on awesome features, not security...
We have the POWER!
Empower Teams with full responsibility for the product end-to-end
What's the cost of NOT doing this?
Stakeholder Teams work together to deliver business value
Info Security
KEY
Hard
Important
Good Idea
nice-to-have
Team determines priorities
awesome ~
what has the most value?
How many times can you navigate the cycle?
N
W
E
S
Average cost of a security breach: $4,000,000.00
Remember: you're working in iterations, so take bite-size chunks.
The business value of a system cannot be realized if the system is not trustworthy.

tcbtech.com/awesome

Empowered Teams Drive Business Value







tcbtech.com/awesome