TRAINING SESSIONS

WELCOME

WHAT TO EXPECT (ON TRAINING)

- Learn by working with small, diverse teams
- 10-day, high-energy experience
- Facilitated collaboration between Developers and security professionals
- Practitioner led training sessions
- Creating solutions for real world problems

WHAT WE EXPECT FROM YOU :)

- Participation
- Care deeply
- Mutual respect
- Objective distance
- Challenge directly
- Be Solution Focused

Summit == Openness

Sessions will be video recorded, sometimes live streamed as well, and will later be shared on social media (i.e YouTube, Twitter, Linkedin).

If you do not want to be identified, please take personal precautions (such as not activating your video, using N/A as your name during the session).

Everything created at the Summit is released under a CC or Open Source license

RESPECT

We are all here to collaborate on topics we have chosen as a community, no-one should be discriminated or harassed based on their race, gender, age, religion, appearance, inexperience, or anything else.

We are all expected to preserve a certain level of professionalism and respect.

If you feel any kind of abusive behaviour against yourself or anyone else during the summit, please report to one of the organisers as soon as you can; so that it can be handled and prevented from future occurrence.

SHARE YOUR VIEWS

#OSS2020

slack

OSS Slack Invite Link

AND LEARN :)

OPEN SECURITY SUMMIT

ALL SESSIONS AT
OPEN SECURITY SUMMIT 2020
WILL BE RECORDED AND SHARED
WITH THE PUBLIC ☺

All materials will be published under a CC or open source license

OPEN SECURITY SUMMIT

Supported by OWASP

Goher Mohammad

Head of InfoSec @ L&Q

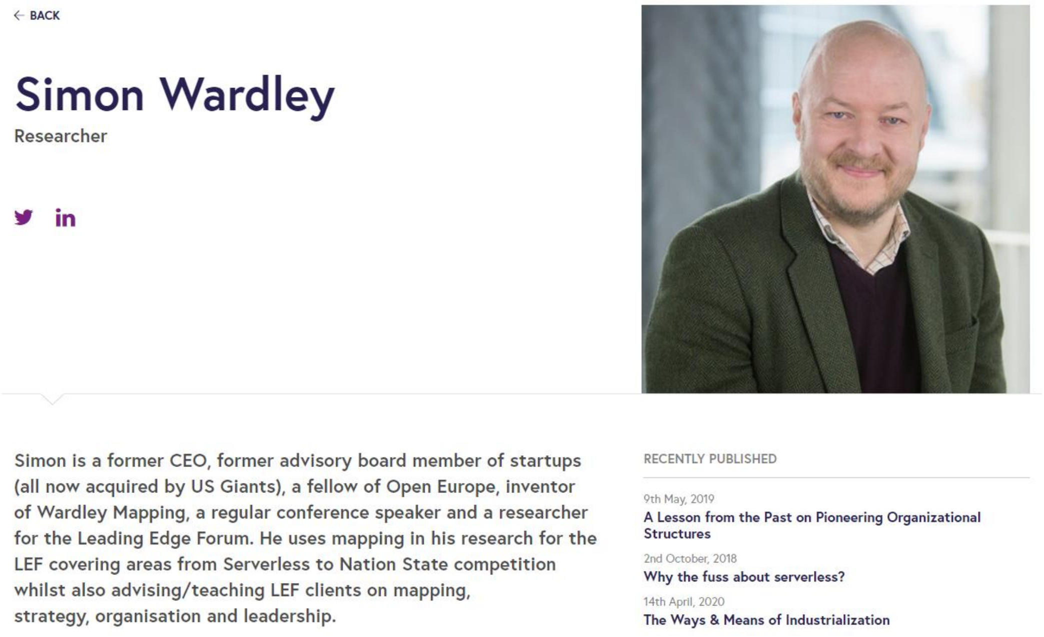
Background:
Finance
Media
Fintech
E-Commerce

Rules of engagement

- Open and honest
- Allow others to speak
- There is no wrong or right so don’t be shy to speak
- Its interactive
- Questions in the chat or reaction preferred

What is Wardley Mapping?

Brainchild of Simon Wardley



← BACK

Simon Wardley

Researcher

in

Simon is a former CEO, former advisory board member of startups (all now acquired by US Giants), a fellow of Open Europe, inventor of Wardley Mapping, a regular conference speaker and a researcher for the Leading Edge Forum. He uses mapping in his research for the LEF covering areas from Serverless to Nation State competition whilst also advising/teaching LEF clients on mapping, strategy, organisation and leadership.

RECENTLY PUBLISHED

9th May, 2019
A Lesson from the Past on Pioneering Organizational Structures

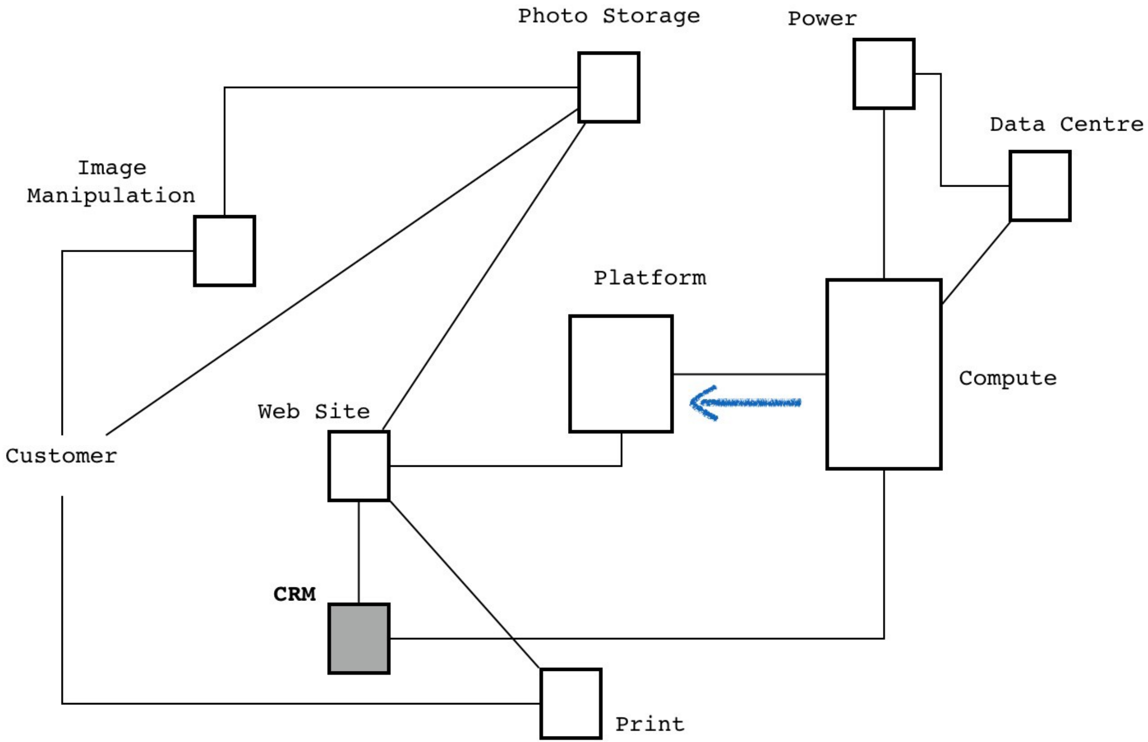
2nd October, 2018
Why the fuss about serverless?

14th April, 2020
The Ways & Means of Industrialization

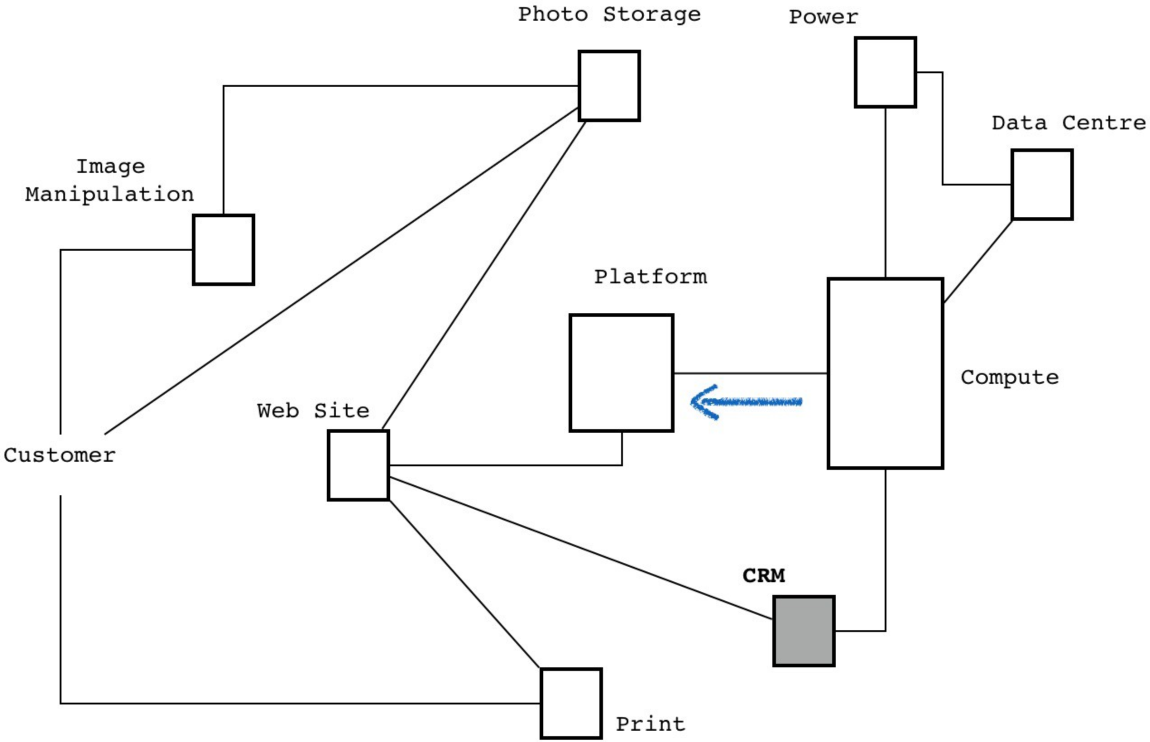
More information can be found here about Simon Wardley and Wardley Maps:

https://medium.com/wardleymaps

This is normally seen as ‘mapping’

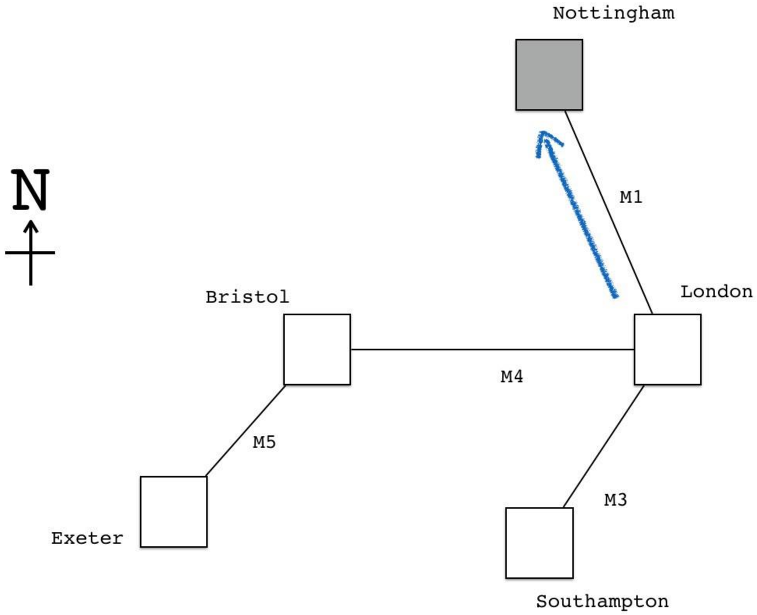


Has anything changed?

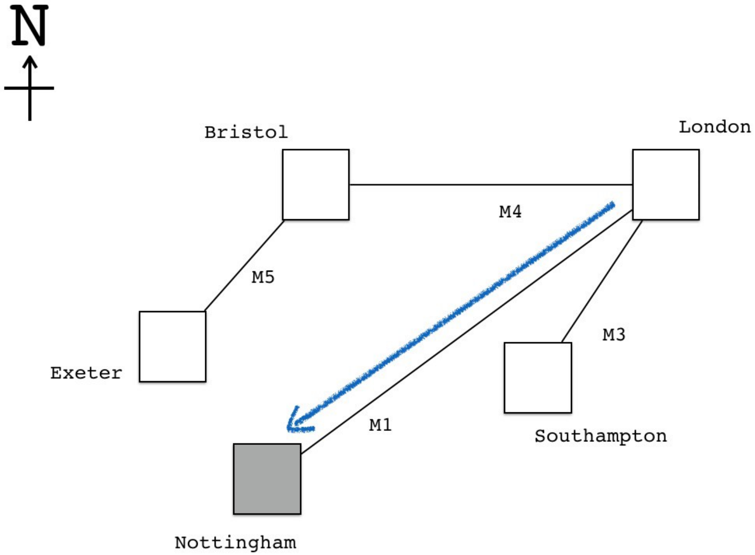


Basically it is a diagram!!

Is this a map?

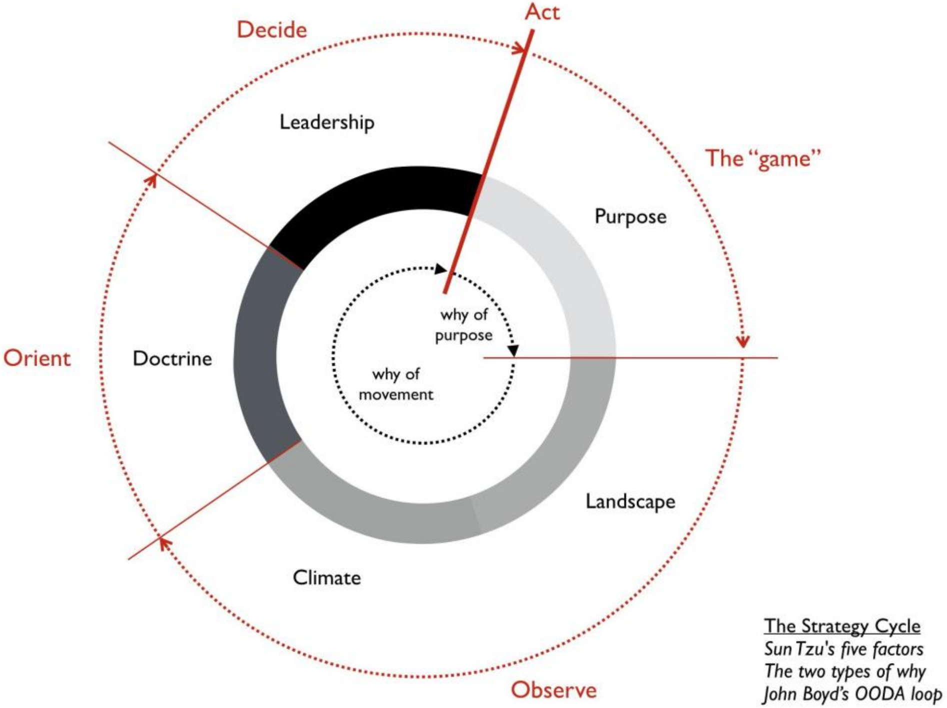


Changing Nottingham changes the meaning of the map!



..but it is a map that’s meaningful!!

‘True’ Mapping allows Strategy, Visibility and Direction



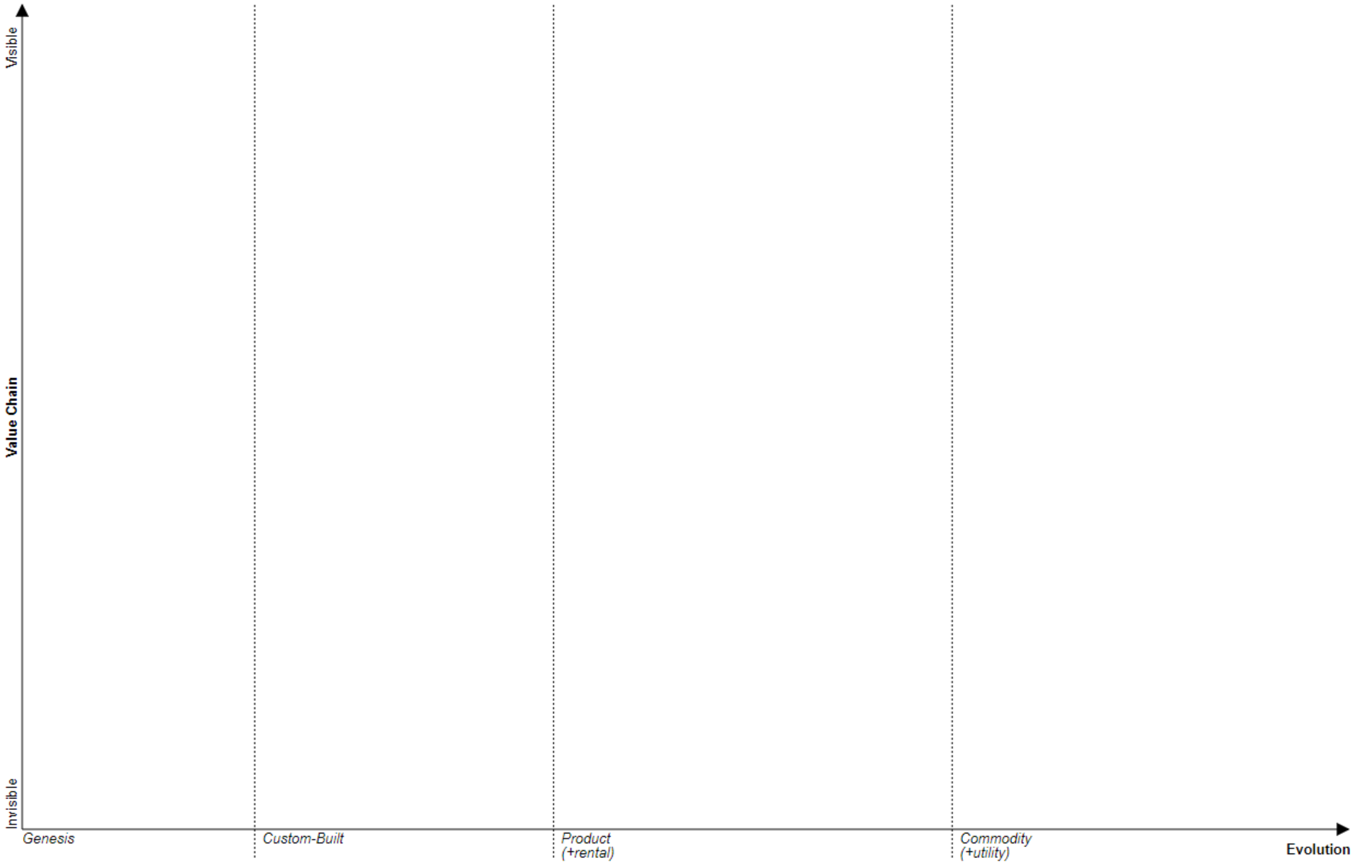
The Strategy Cycle

Sun Tzu's five factors

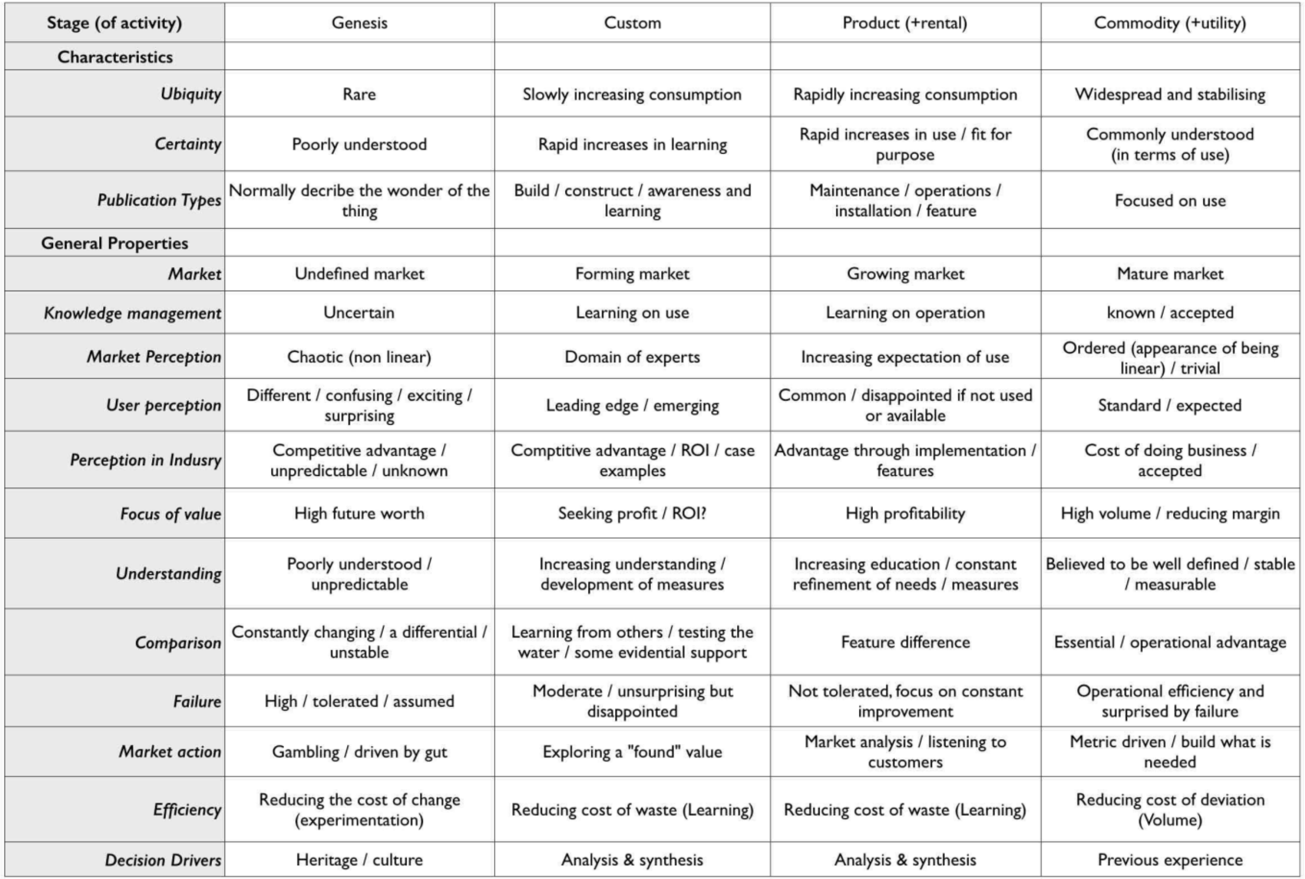
The two types of why

John Boyd’s OODA loop

This is a ‘Wardley Map’

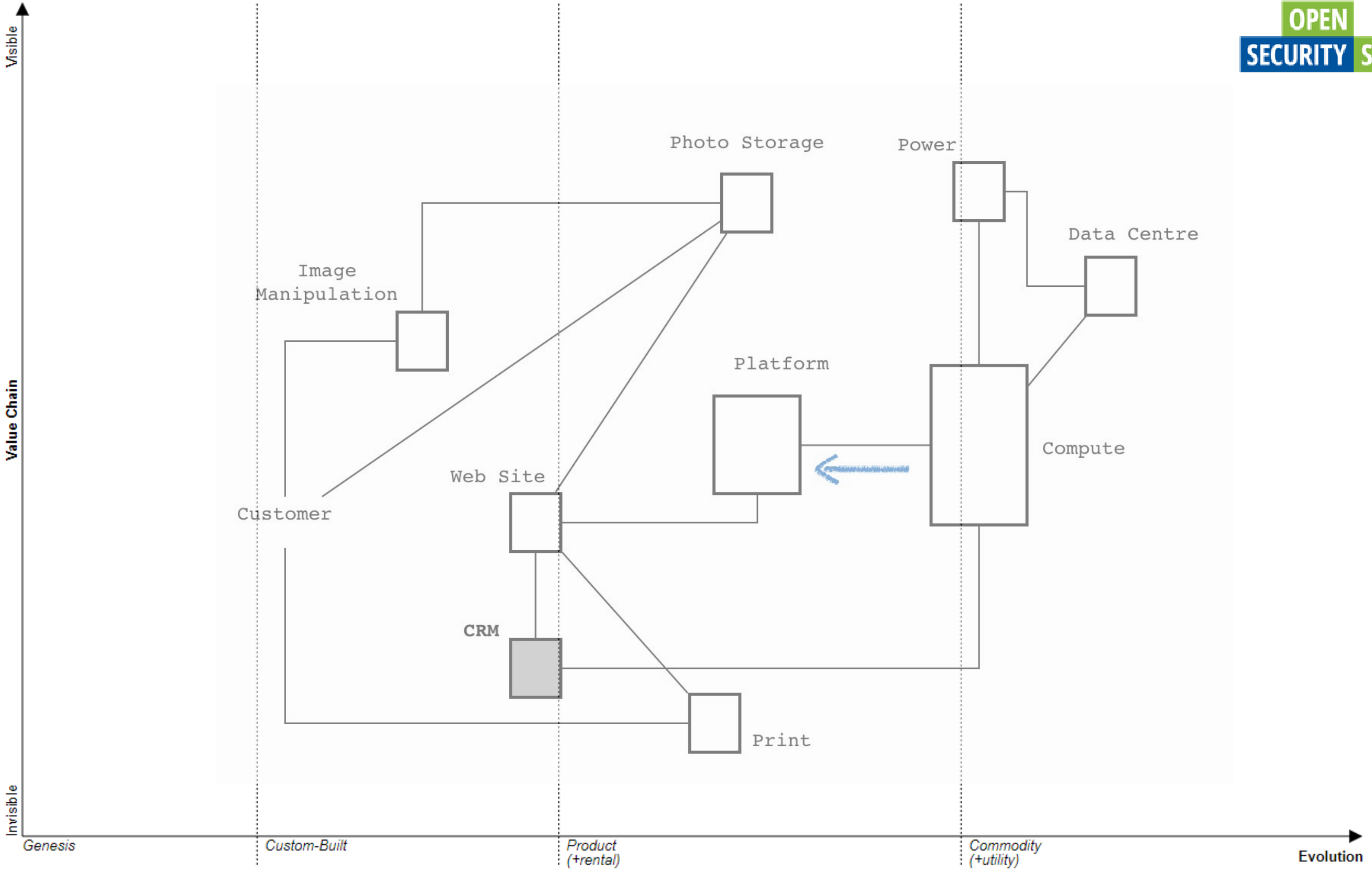


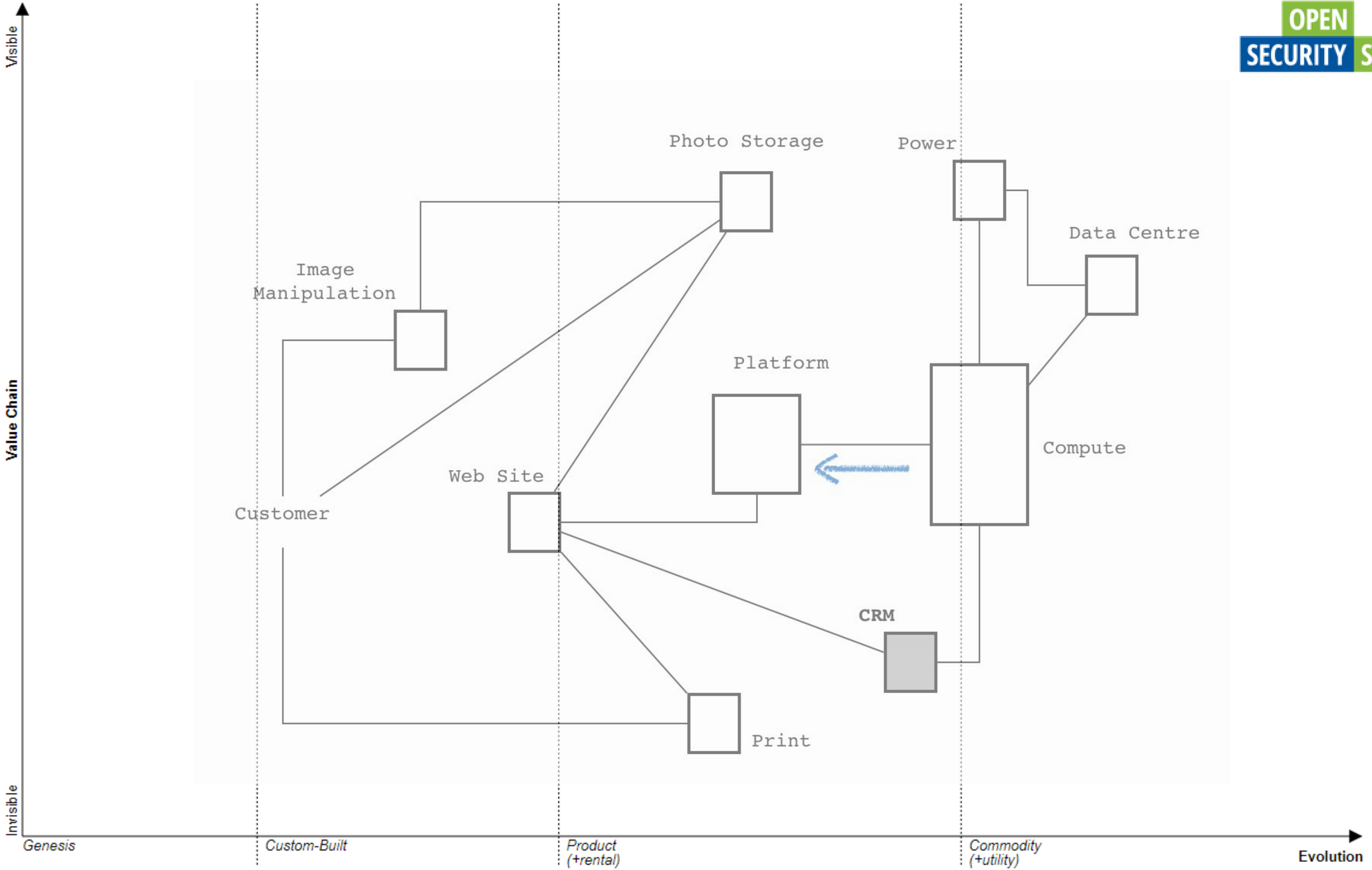
Evolution cheat sheet



Stage (of activity)	Genesis	Custom	Product (+rental)	Commodity (+utility)
Characteristics				
Ubiquity	Rare	Slowly increasing consumption	Rapidly increasing consumption	Widespread and stabilising
Certainty	Poorly understood	Rapid increases in learning	Rapid increases in use / fit for purpose	Commonly understood (in terms of use)
Publication Types	Normally decribe the wonder of the thing	Build / construct / awareness and learning	Maintenance / operations / installation / feature	Focused on use
General Properties				
Market	Undefined market	Forming market	Growing market	Mature market
Knowledge management	Uncertain	Learning on use	Learning on operation	known / accepted
Market Perception	Chaotic (non linear)	Domain of experts	Increasing expectation of use	Ordered (appearance of being linear) / trivial
User perception	Different / confusing / exciting / surprising	Leading edge / emerging	Common / disappointed if not used or available	Standard / expected
Perception in Indusry	Competitive advantage / unpredictable / unknown	Comptitive advantage / ROI / case examples	Advantage through implementation / features	Cost of doing business / accepted
Focus of value	High future worth	Seeking profit / ROI?	High profitability	High volume / reducing margin
Understanding	Poorly understood / unpredictable	Increasing understanding / development of measures	Increasing education / constant refinement of needs / measures	Believed to be well defined / stable / measurable
Comparison	Constantly changing / a differential / unstable	Learning from others / testing the water / some evidential support	Feature difference	Essential / operational advantage
Failure	High / tolerated / assumed	Moderate / unsurprising but disappointed	Not tolerated, focus on constant improvement	Operational efficiency and surprised by failure
Market action	Gambling / driven by gut	Exploring a "found" value	Market analysis / listening to customers	Metric driven / build what is needed
Efficiency	Reducing the cost of change (experimentation)	Reducing cost of waste (Learning)	Reducing cost of waste (Learning)	Reducing cost of deviation (Volume)
Decision Drivers	Heritage / culture	Analysis & synthesis	Analysis & synthesis	Previous experience

Previous diagram now mapped

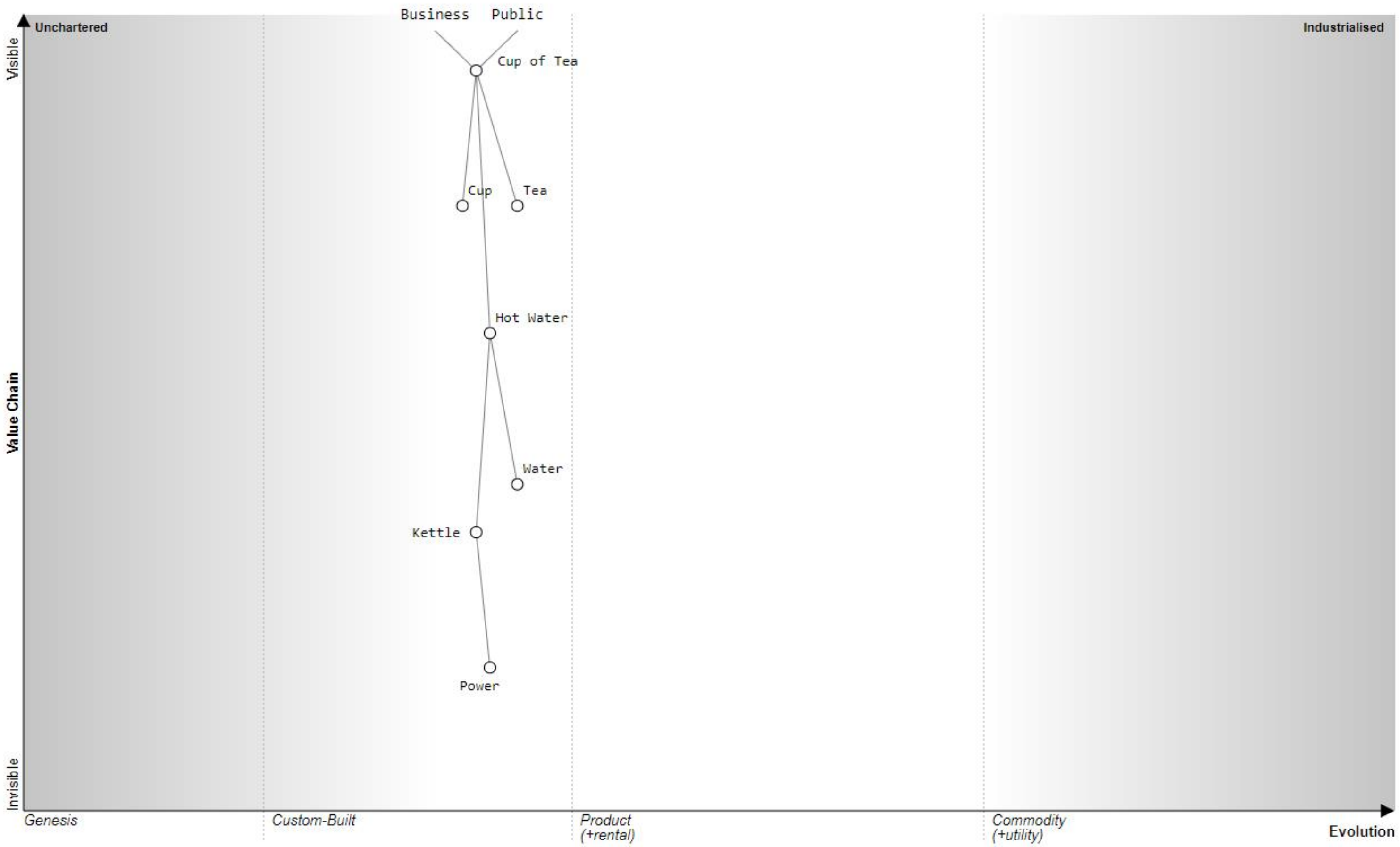

Visible
Value Chain
Invisible
Photo Storage
Power
Data Centre
Image Manipulation
Platform
Compute
Web Site
Customer
CRM
Print
Genesis
Custom-Built
Product (+rental)
Commodity (+utility)
Evolution


Visible
Value Chain
Invisible
Photo Storage
Power
Data Centre
Image Manipulation
Platform
Compute
Web Site
Customer
CRM
Print
Genesis
Custom-Built
Product (+rental)
Commodity (+utility)
Evolution

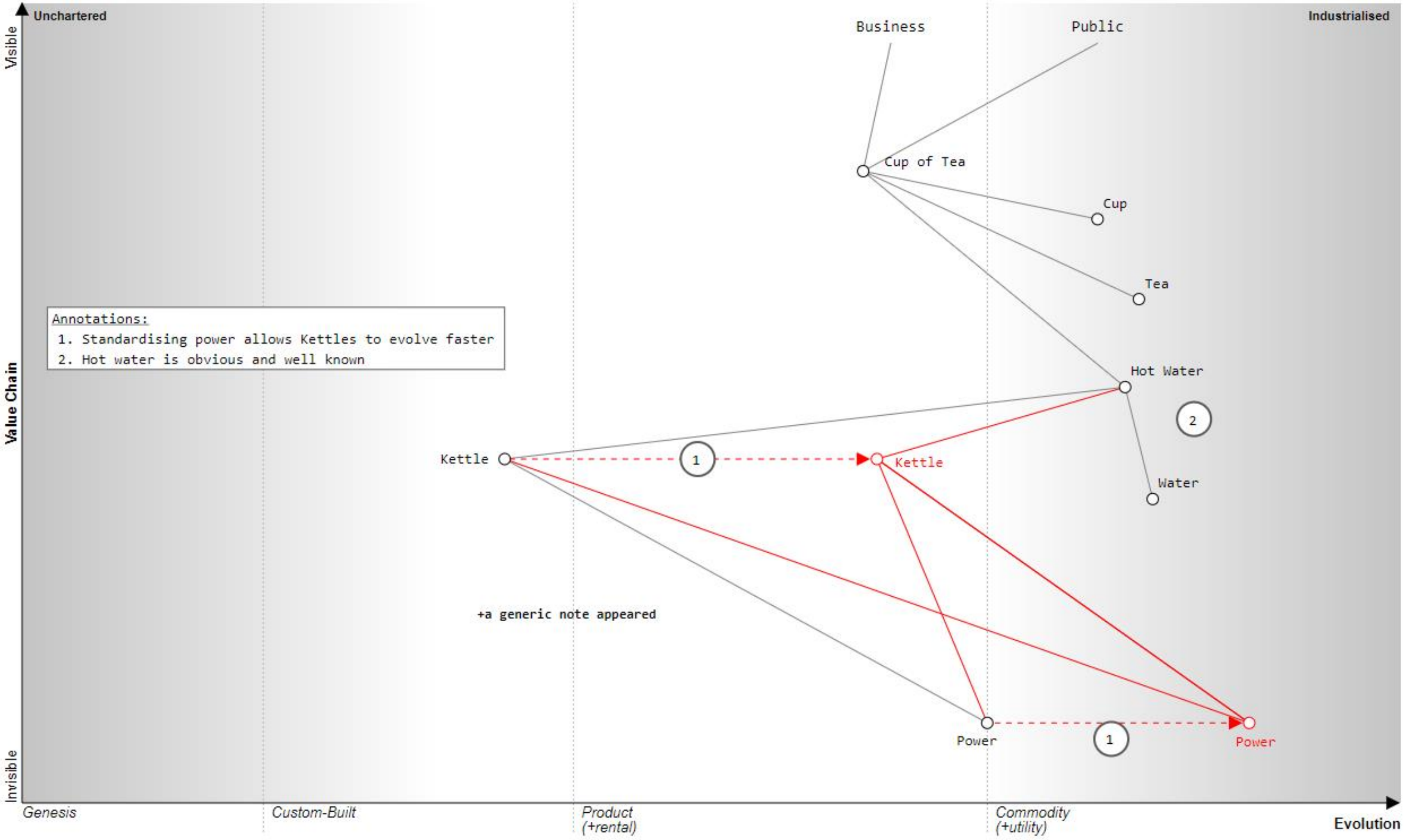
Meaning of map completely changes and becomes useful

How can this be applied?

Tea Shop


Business
Public
Cup of Tea
Cup
Tea
Hot Water
Water
Kettle
Power
Unchartered
Industrialised
Visible
Value Chain
Invisible
Genesis
Custom-Built
Product
(+rental)
Commodity
(+utility)
Evolution

Tea Shop

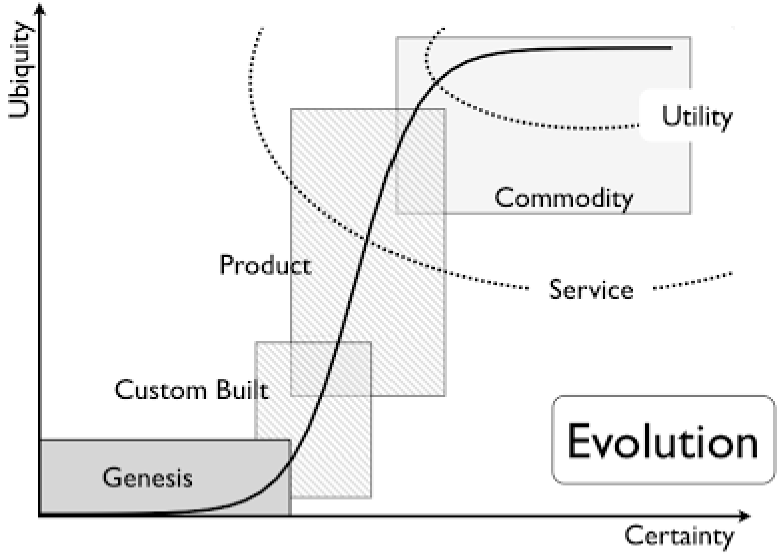


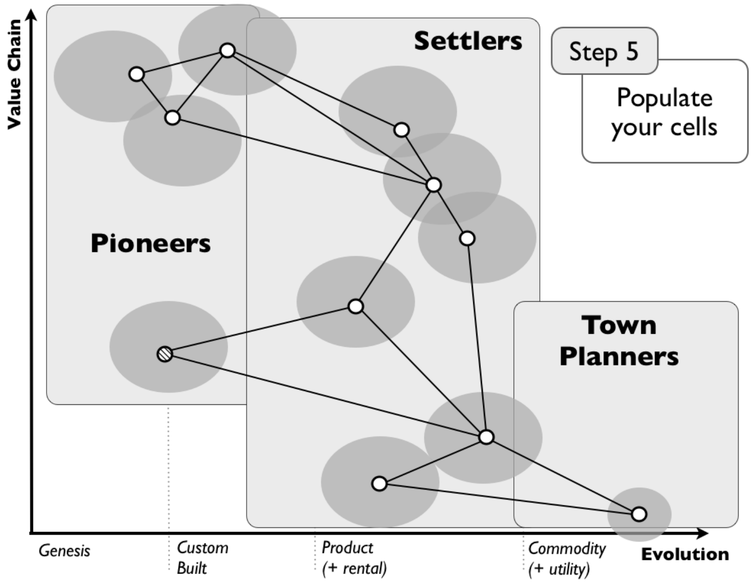
Annotations:

1. Standardising power allows Kettles to evolve faster
2. Hot water is obvious and well known

+a generic note appeared

Context to populate a Wardley Map

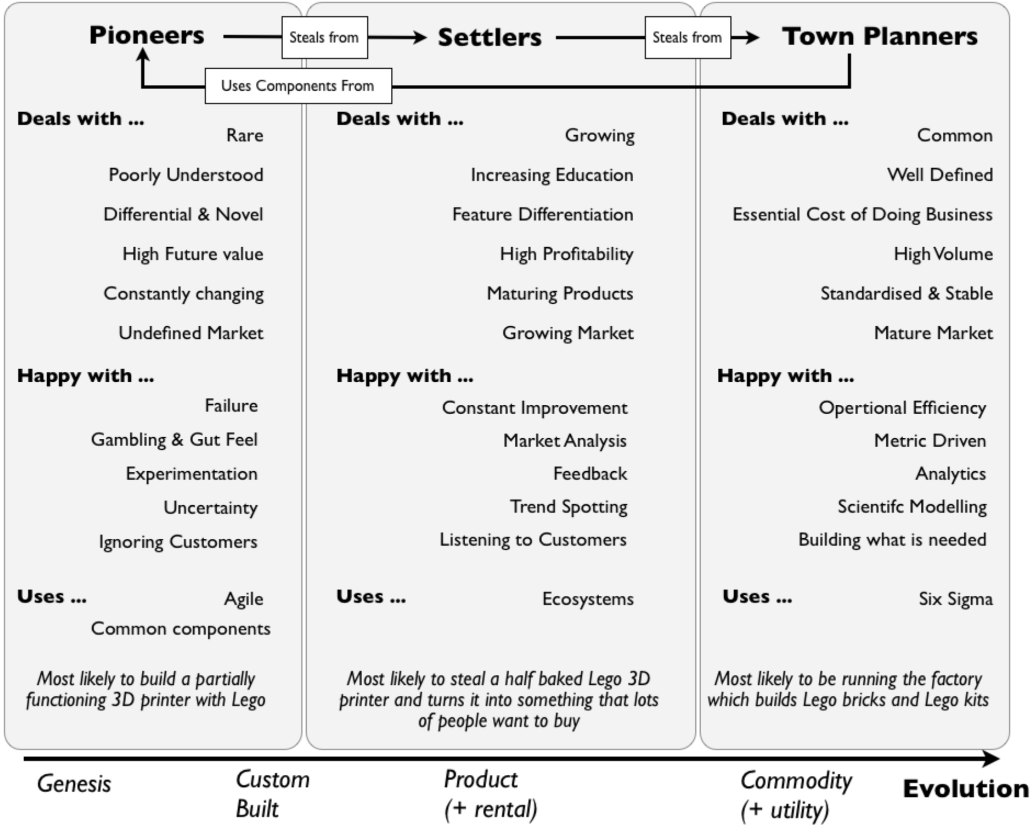




Step 5

Populate your cells

What are Pioneers, Settlers and Town Planners?



Pioneers	Settlers	Town Planners
Deals with ...	**Deals with ...**	**Deals with ...**
Rare	Growing	Common
Poorly Understood	Increasing Education	Well Defined
Differential & Novel	Feature Differentiation	Essential Cost of Doing Business
High Future value	High Profitability	High Volume
Constantly changing	Maturing Products	Standardised & Stable
Undefined Market	Growing Market	Mature Market
Happy with ...	**Happy with ...**	**Happy with ...**
Failure	Constant Improvement	Opertional Efficiency
Gambling & Gut Feel	Market Analysis	Metric Driven
Experimentation	Feedback	Analytics
Uncertainty	Trend Spotting	Scientifc Modelling
Ignoring Customers	Listening to Customers	Building what is needed
Uses ...	**Uses ...**	**Uses ...**
Agile Common components	Ecosystems	Six Sigma
Most likely to build a partially functioning 3D printer with Lego	*Most likely to steal a half baked Lego 3D printer and turns it into something that lots of people want to buy*	*Most likely to be running the factory which builds Lego bricks and Lego kits*

Create your own!

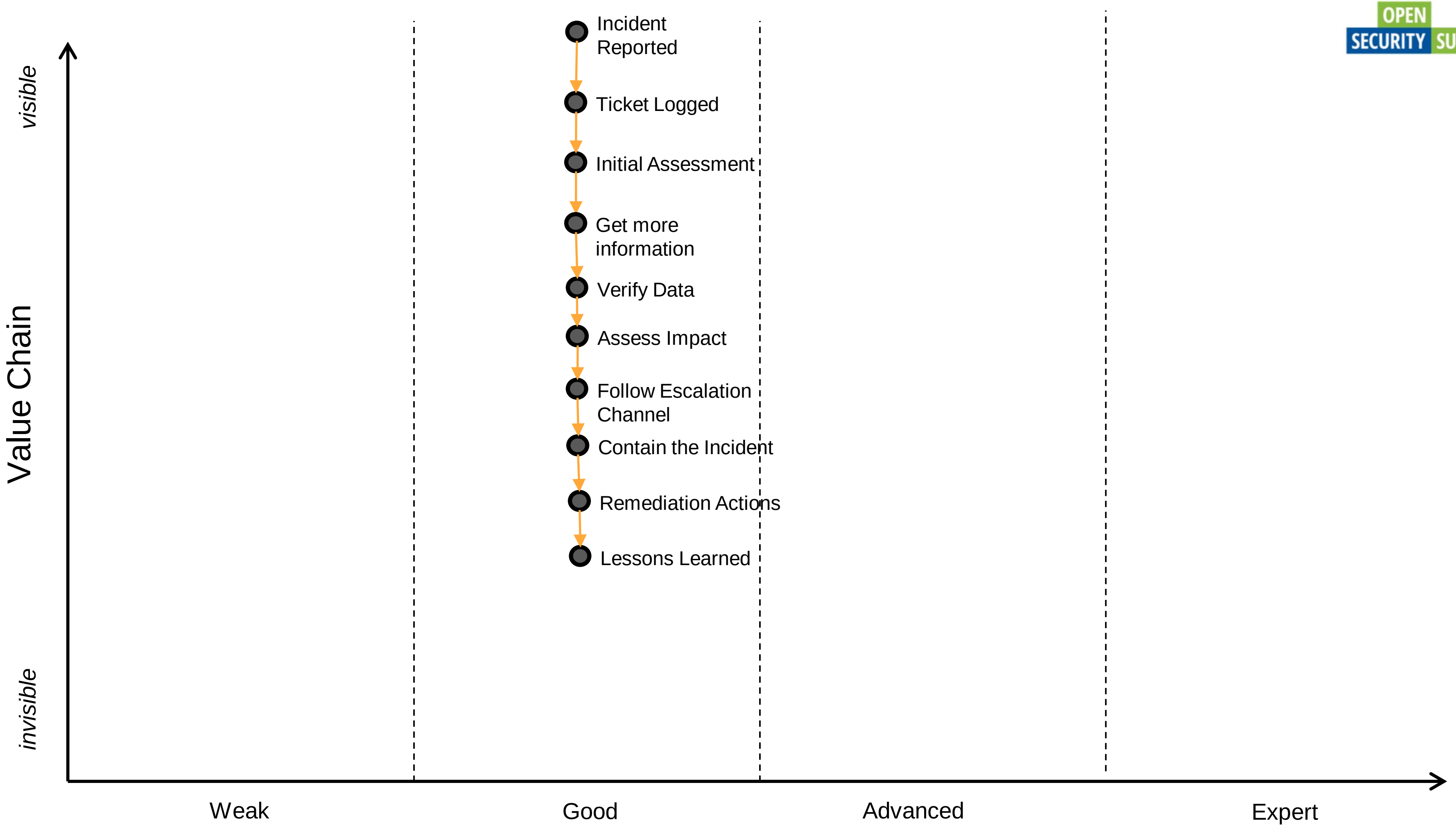
Create your own Wardley Map! - Exercise

Map out making Strawberry Milkshake

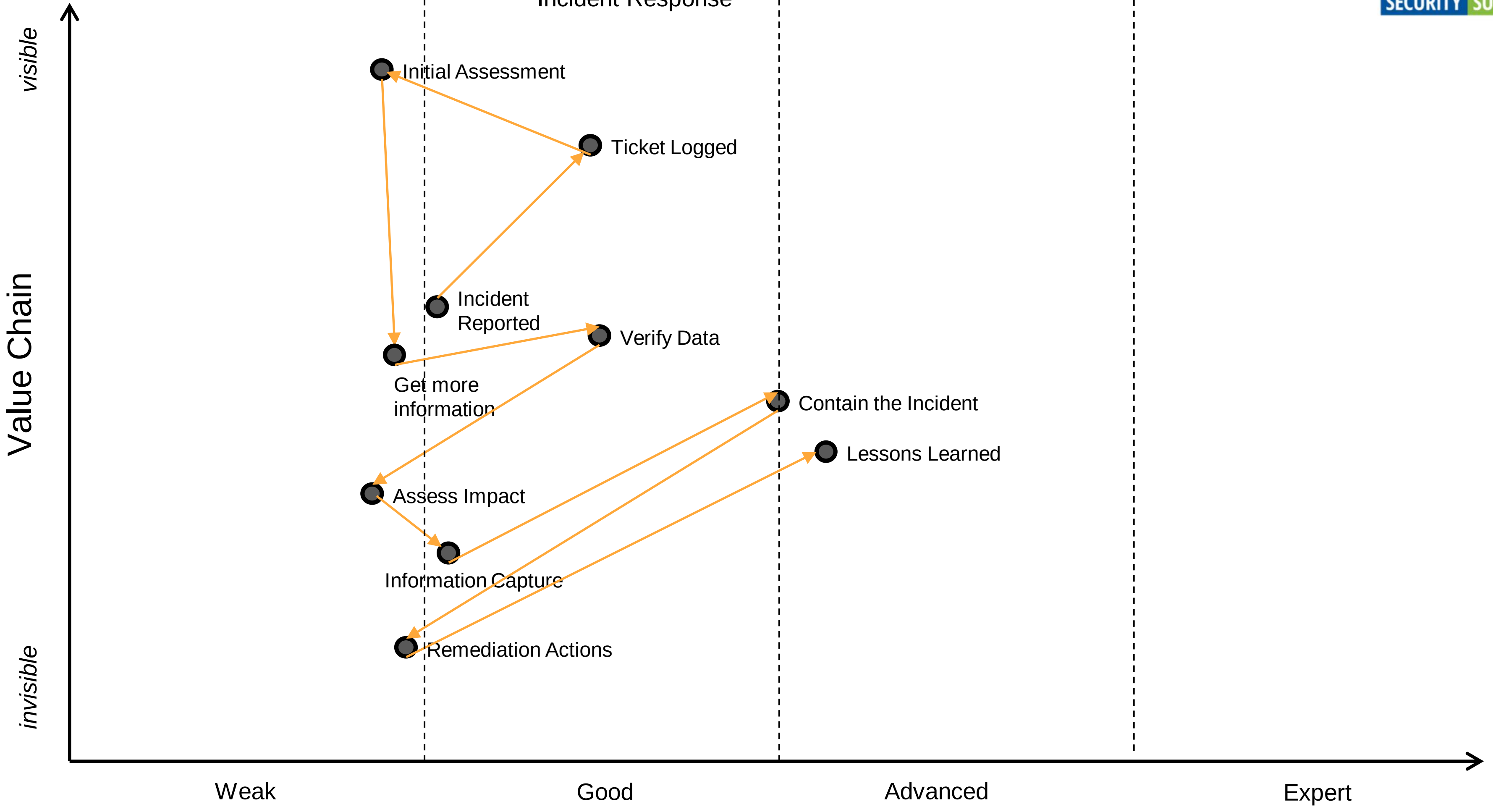
Go to:

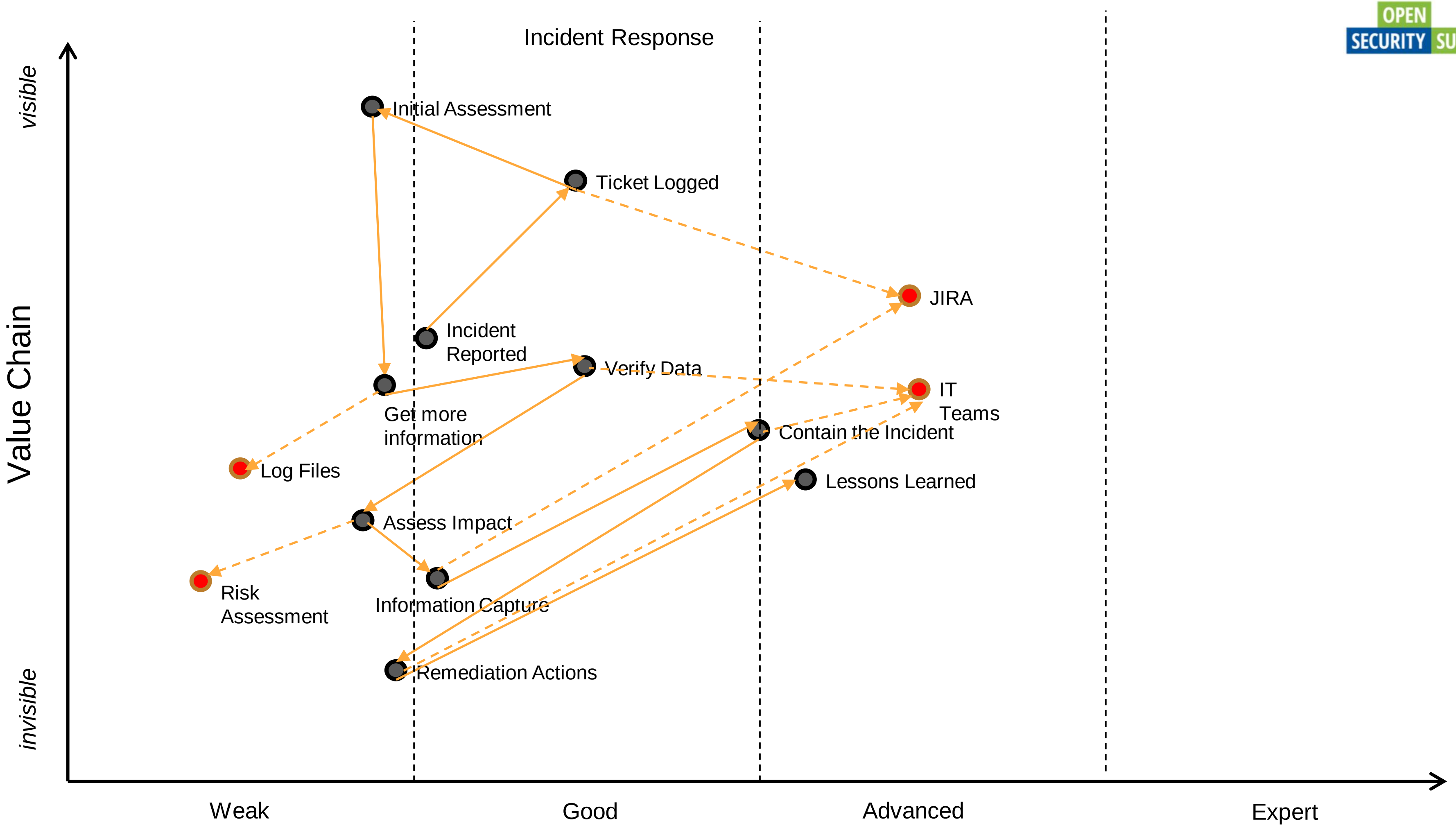
https://onlinewardleymaps.com/

A real life example in security


visible
Value Chain
invisible
Incident Reported
Ticket Logged
Initial Assessment
Get more information
Verify Data
Assess Impact
Follow Escalation Channel
Contain the Incident
Remediation Actions
Lessons Learned
Weak
Good
Advanced
Expert

Incident Response

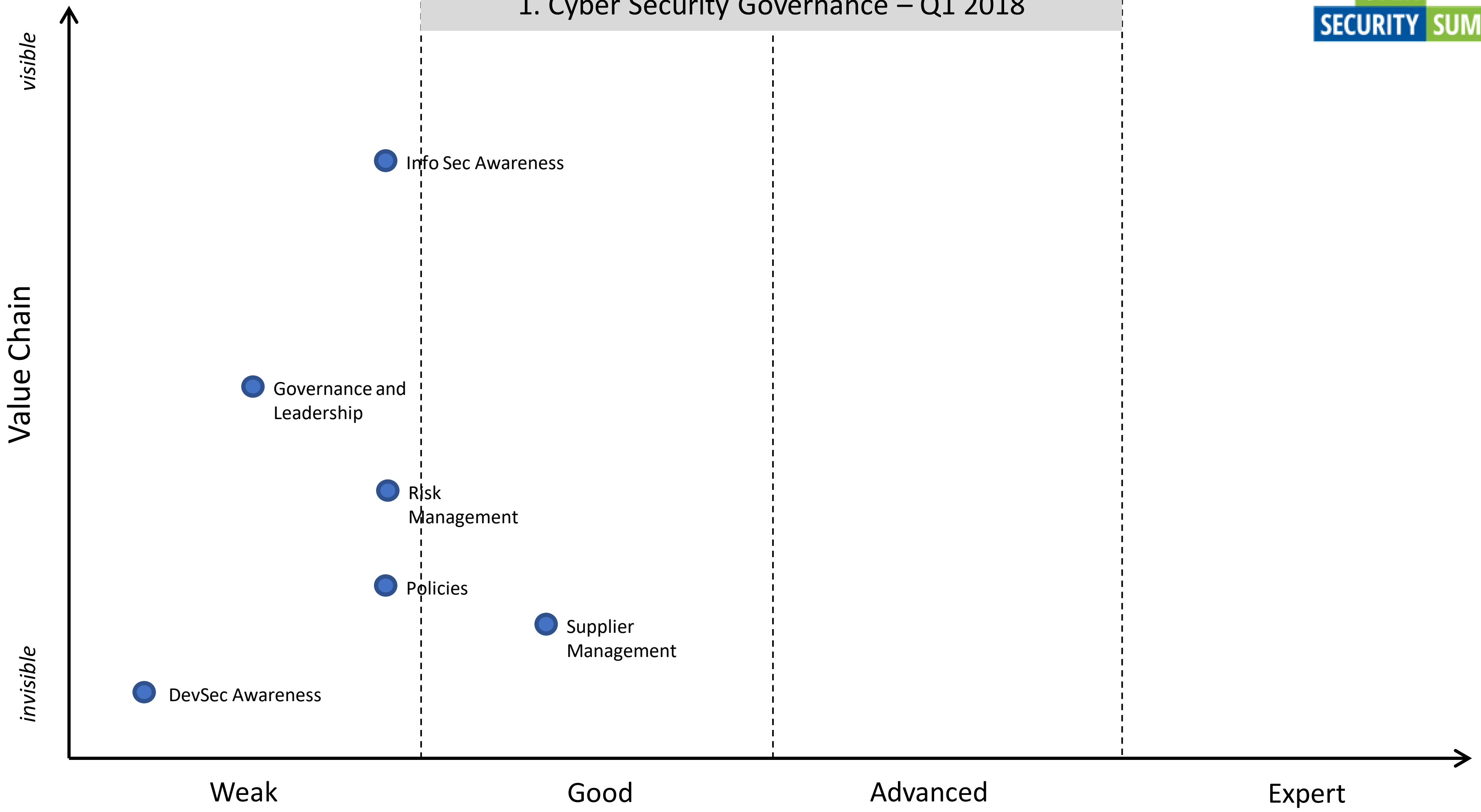




OPEN SECURITY SUMMIT

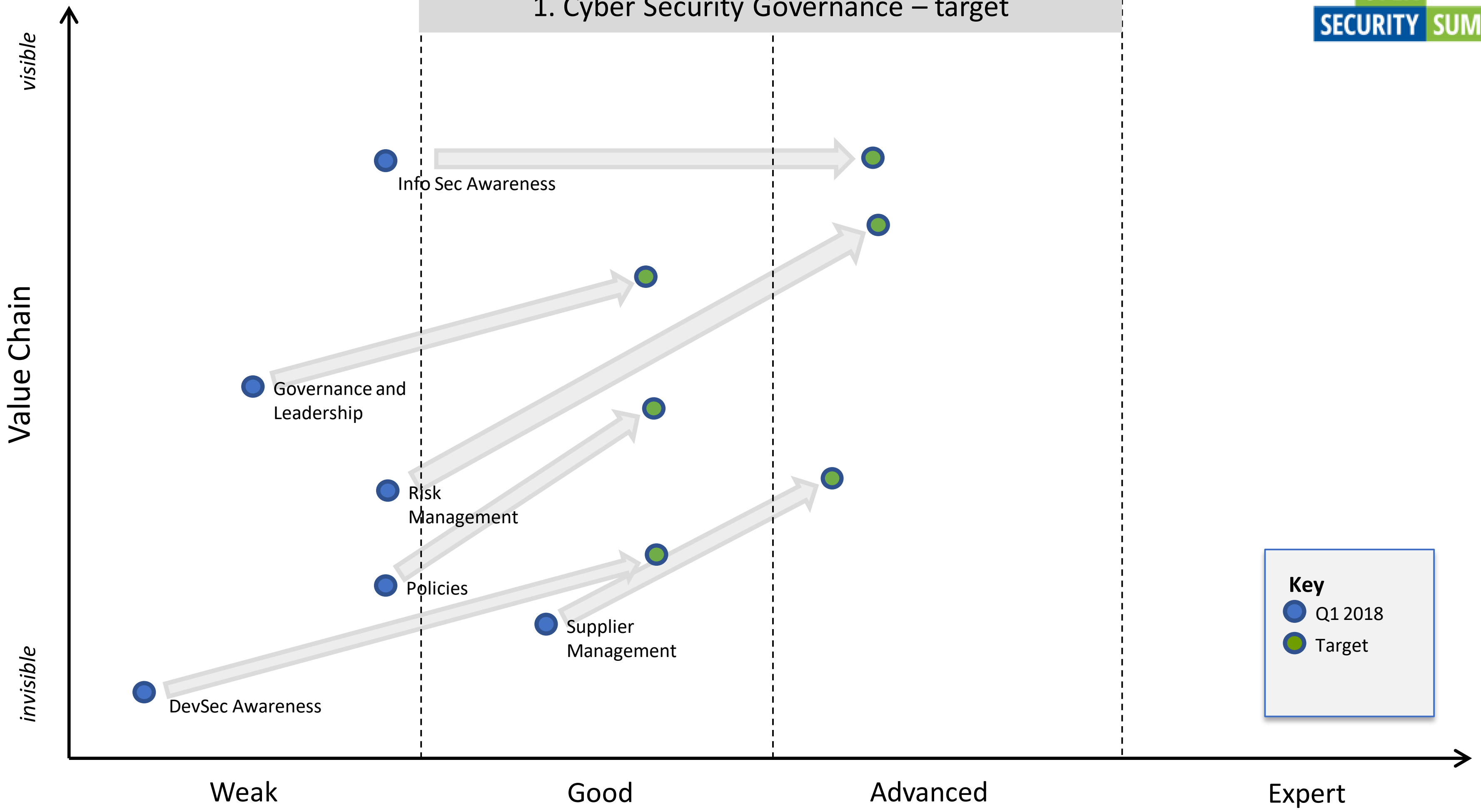
Roadmap Mapping - Example

1. Cyber Security Governance – Q1 2018



OPEN SECURITY SUMMIT

1. Cyber Security Governance – target



1. Cyber Security Governance – Status of work

Infosec Awareness

- Security Champion programme
- Review and improvement of online training
- Security awareness weeks

Supplier Management

- 3rd party questionnaire and review
- Embed process in tender process
- Retrospective review of current contracts
- Policy creation, review and implementation

Policies

- Policy alignment to ISMS Standard
- Policy creation, review and implementation
- Policy approval and implementation

1. Cyber Security Governance - cont

Governance and Leadership

- Roles and responsibilities defined
- Infosec steering committee established
- Hierarchy of risk ownership

Risk Management

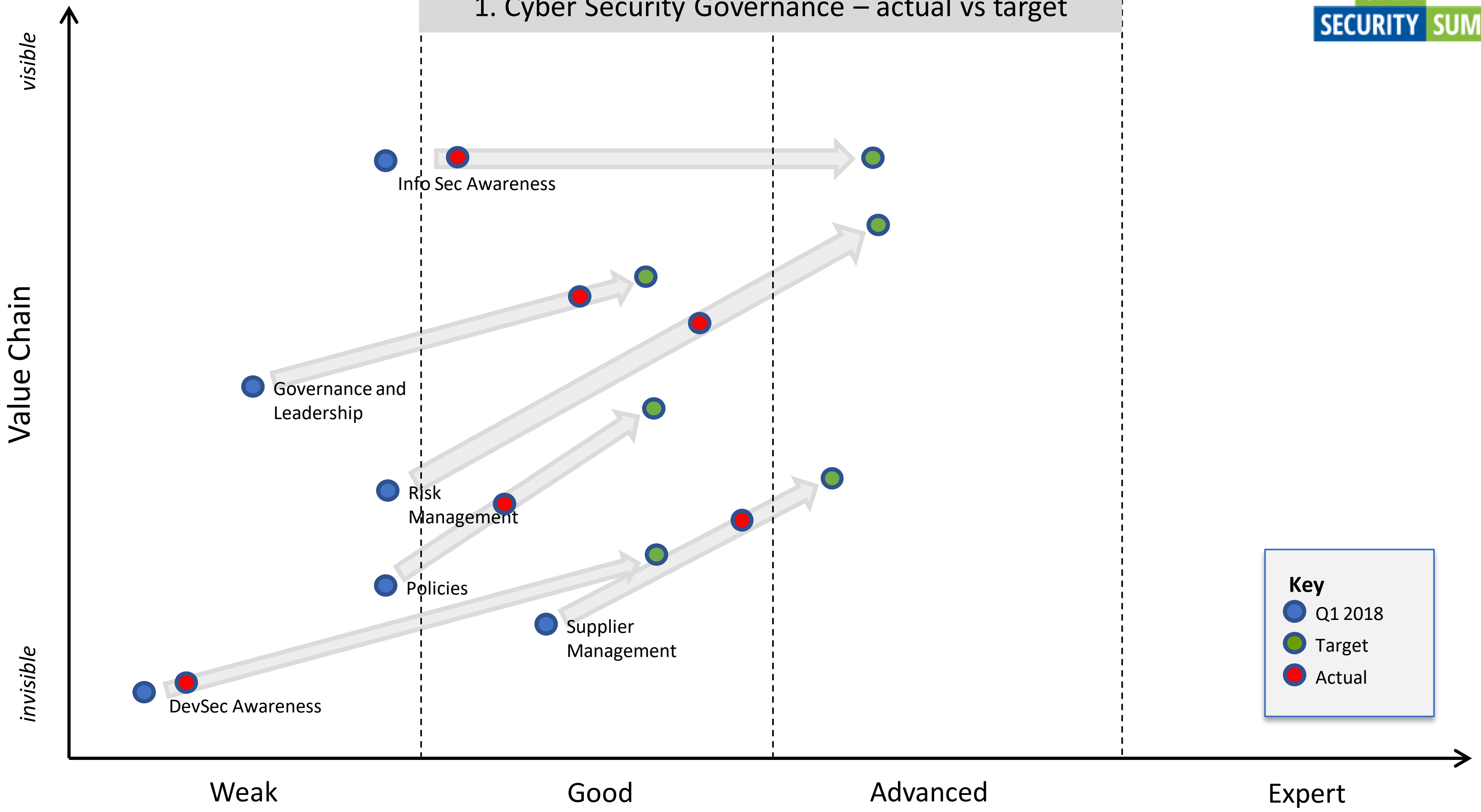
- Mature Technology risk appetite based on ERM
- Define and embed capture process with scalability
- Set up Risk and Incident committee with regular cadence

Dev Sec Awareness

- Training module to be defined and setup in e-learning module
- Security champion programme integration
- Developer training embedding best practice SDLC

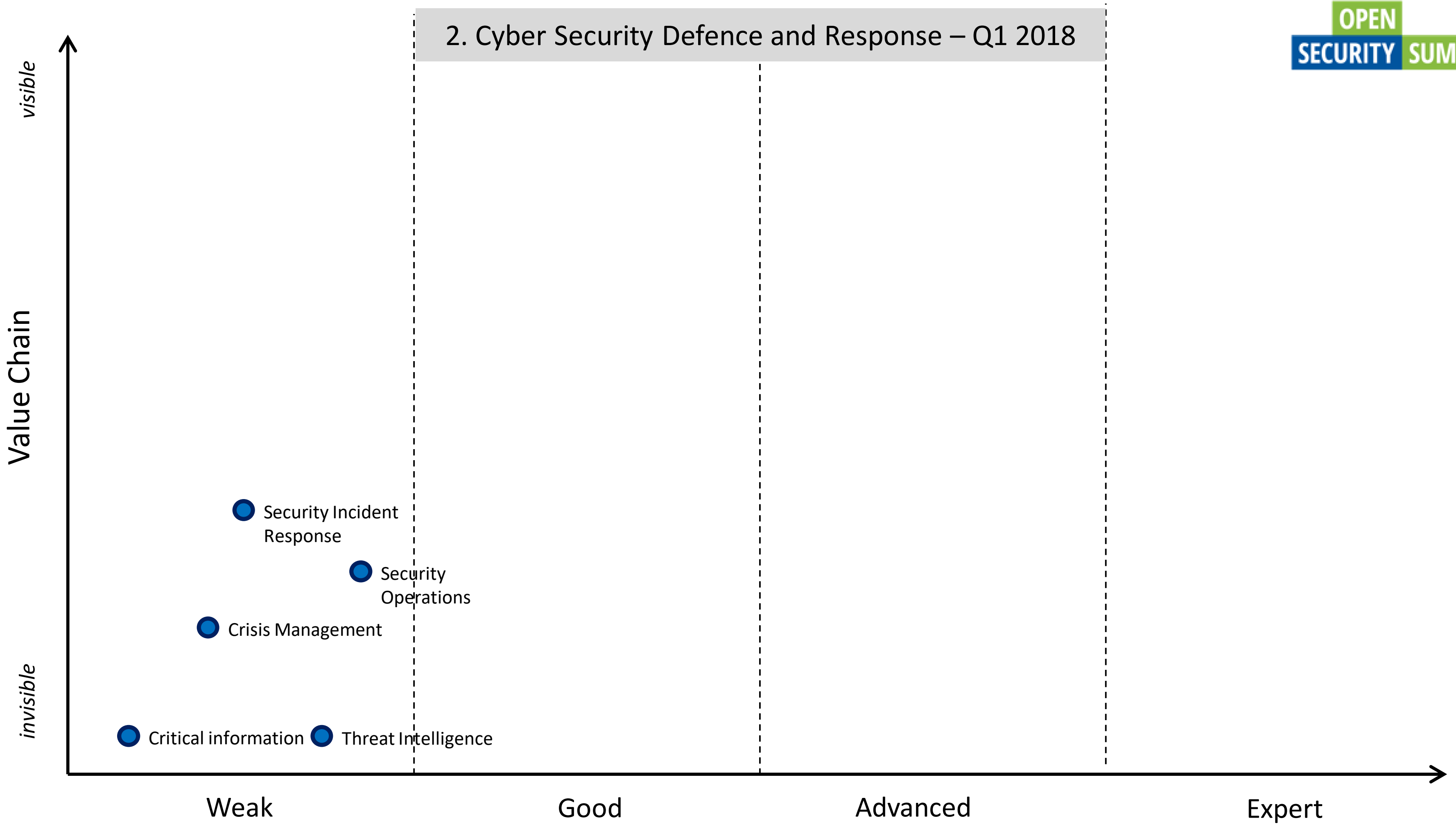
OPEN SECURITY SUMMIT

1. Cyber Security Governance – actual vs target

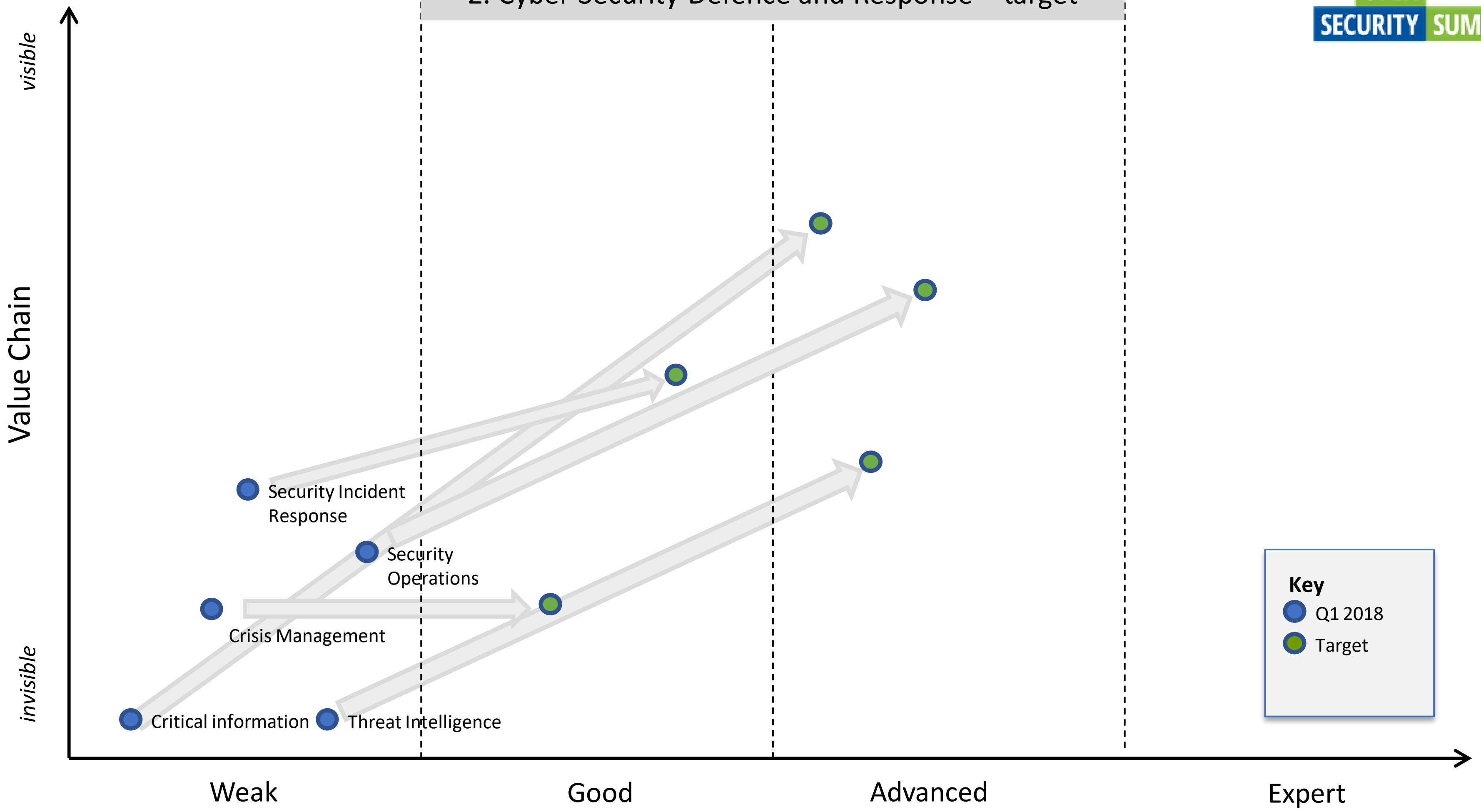


2. Cyber Security Defence and Response – Q1 2018

OPEN SECURITY SUMMIT



2. Cyber Security Defence and Response – target



2. Cyber Security Defence and Response – Status of work

Security Incident Response

- Build process for Incident Response via playbook
- Define PoC for frontline, triage and resolution

Crisis Management

- Review, update, define and approve BCP and DR processes
- Test BCP and DR processes on a regular basis

Critical Information

- Define and catalog critical assets with tracking
- Understand and track critical assets based on PII and confidential data flows

2. Cyber Security Defence and Response - cont

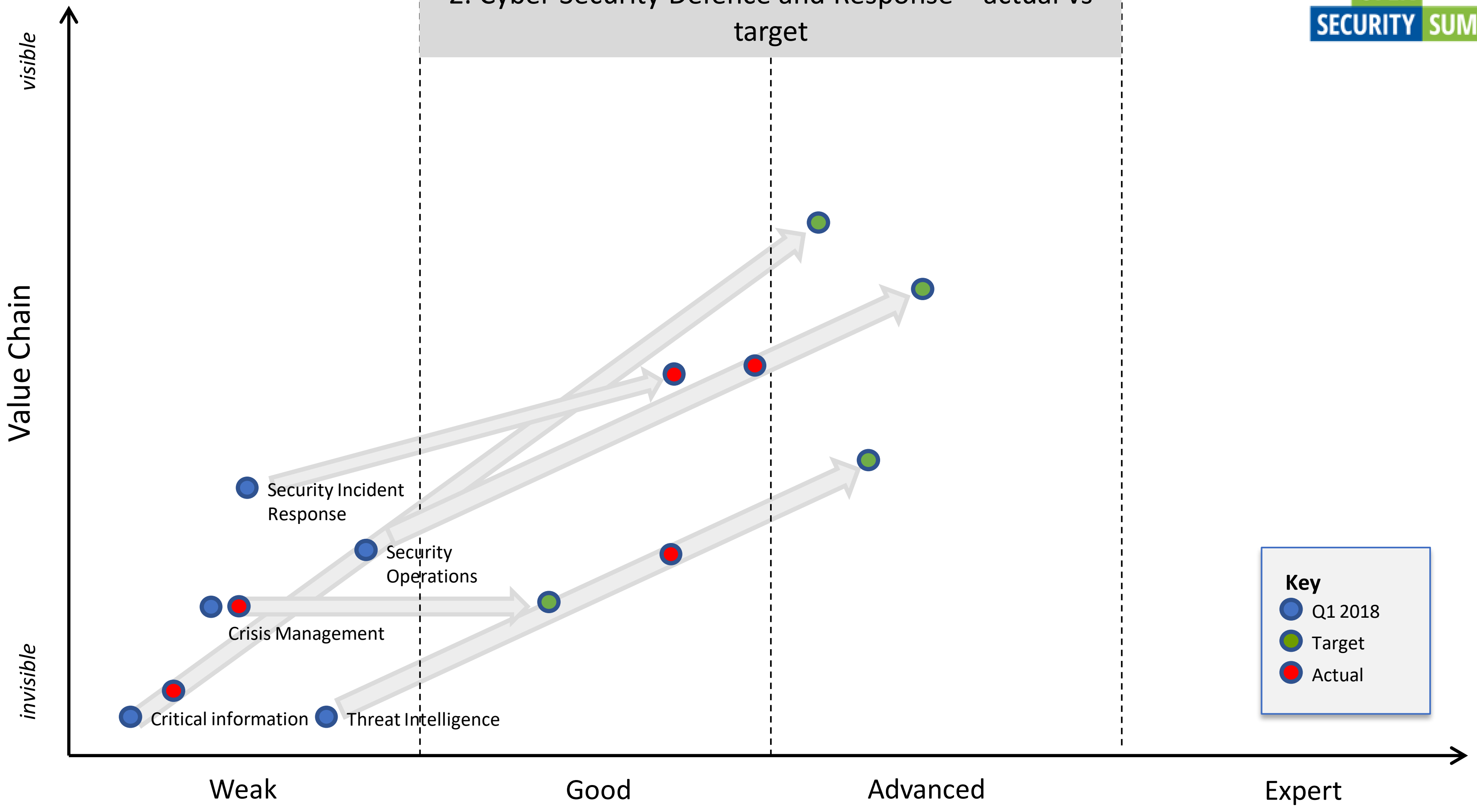
Threat Intelligence

- Proactive monitoring via SIEM and other monitoring tools
- Track and monitor trends and patterns via machine learning

Security Operations

- Set up SOC function and point of contact
- Establish first line assessment and triage of incidents
- Mature monitoring capability focussing on security and network

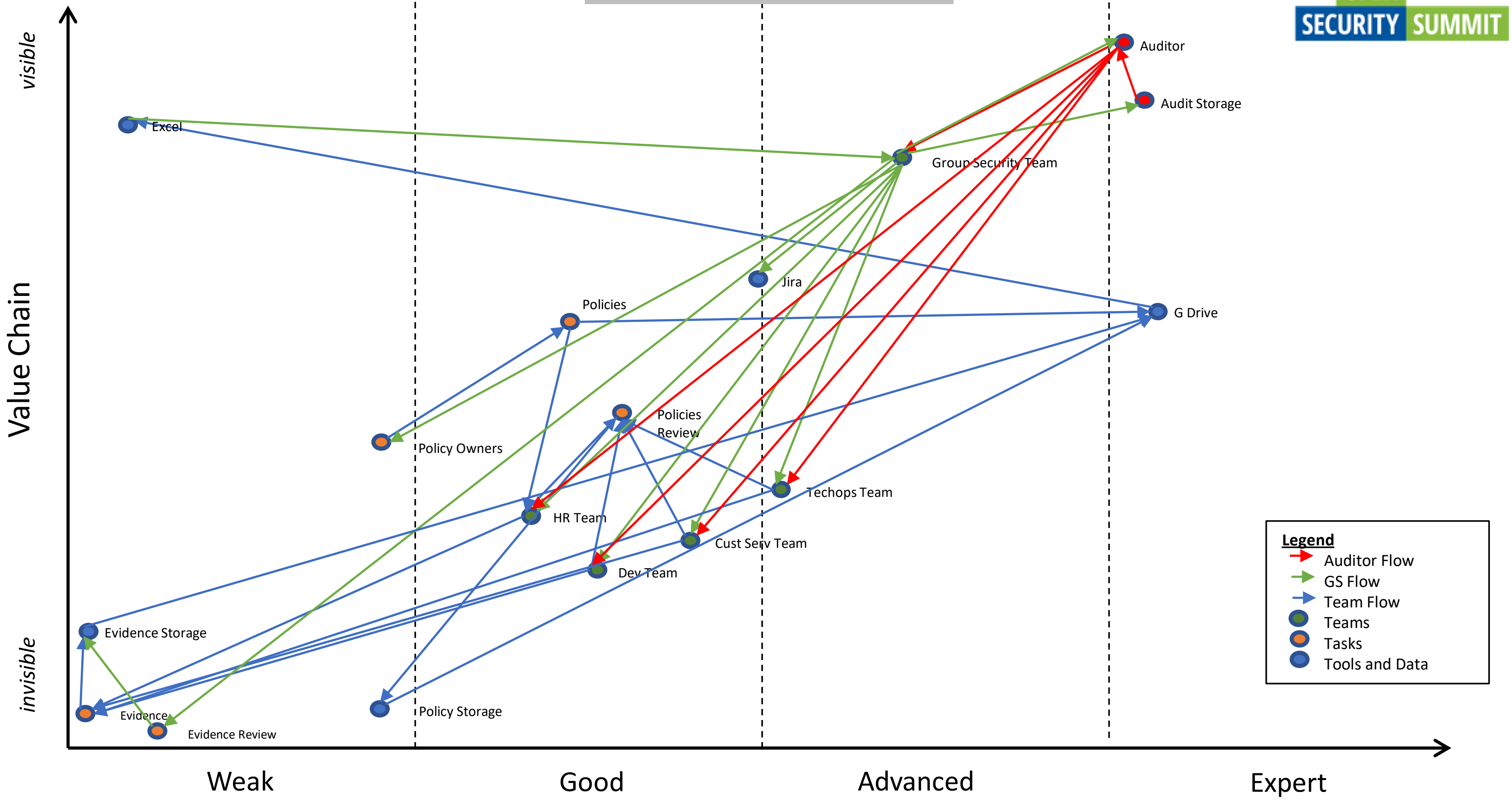
2. Cyber Security Defence and Response – actual vs target



PCI Audit Mapping - Example

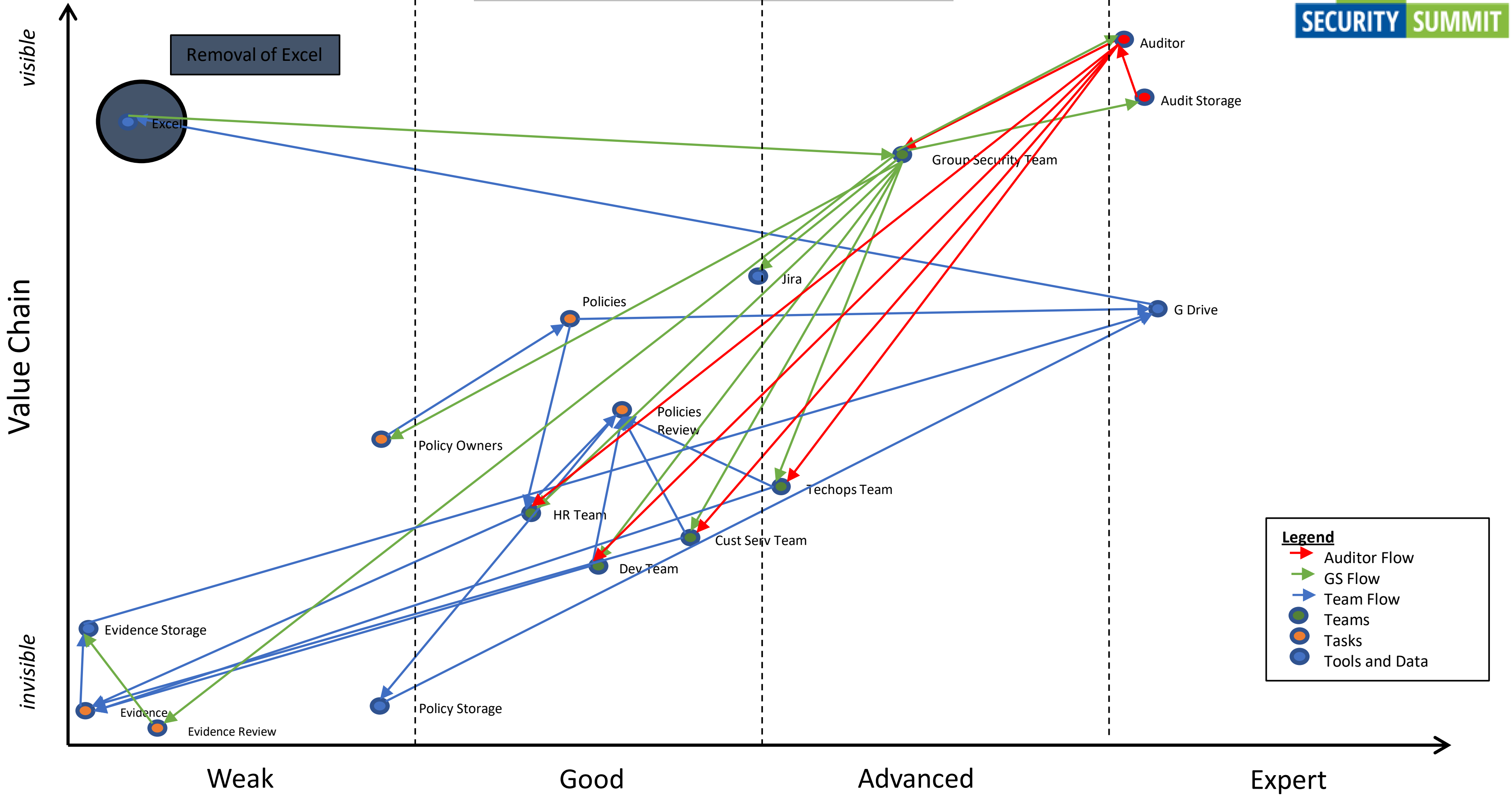
PCI Audit Before

OPEN SECURITY SUMMIT



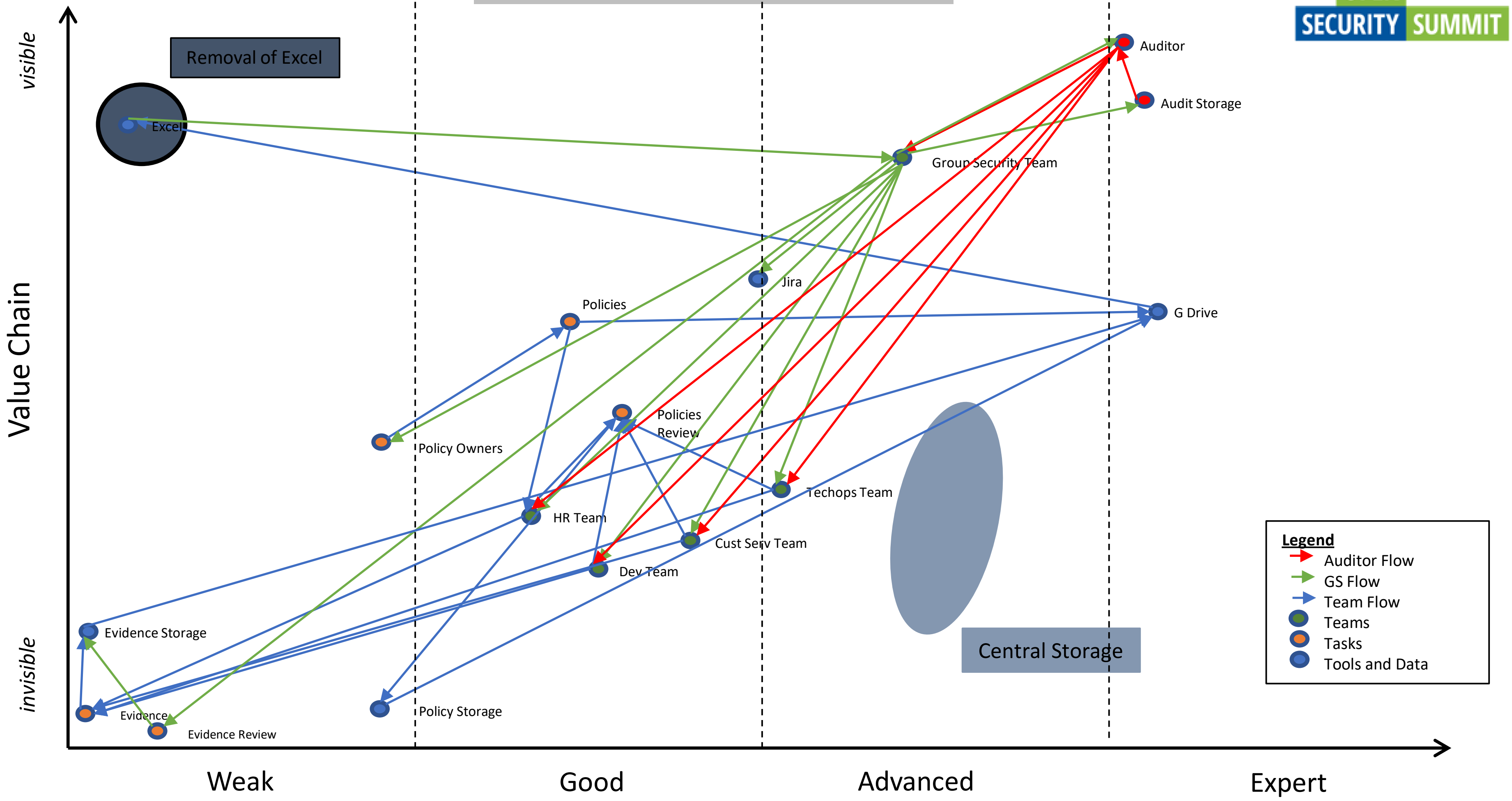
PCI Audit Process Maturity

OPEN SECURITY SUMMIT



PCI Audit Process Maturity

OPEN
SECURITY SUMMIT



Removal of Excel

Central Storage

visible

Value Chain

invisible

Weak

Good

Advanced

Expert

Excel

Auditor

Audit Storage

Group Security Team

Jira

Policies

G Drive

Policies Review

Policy Owners

Techops Team

HR Team

Cust Serv Team

Dev Team

Evidence Storage

Evidence

Evidence Review

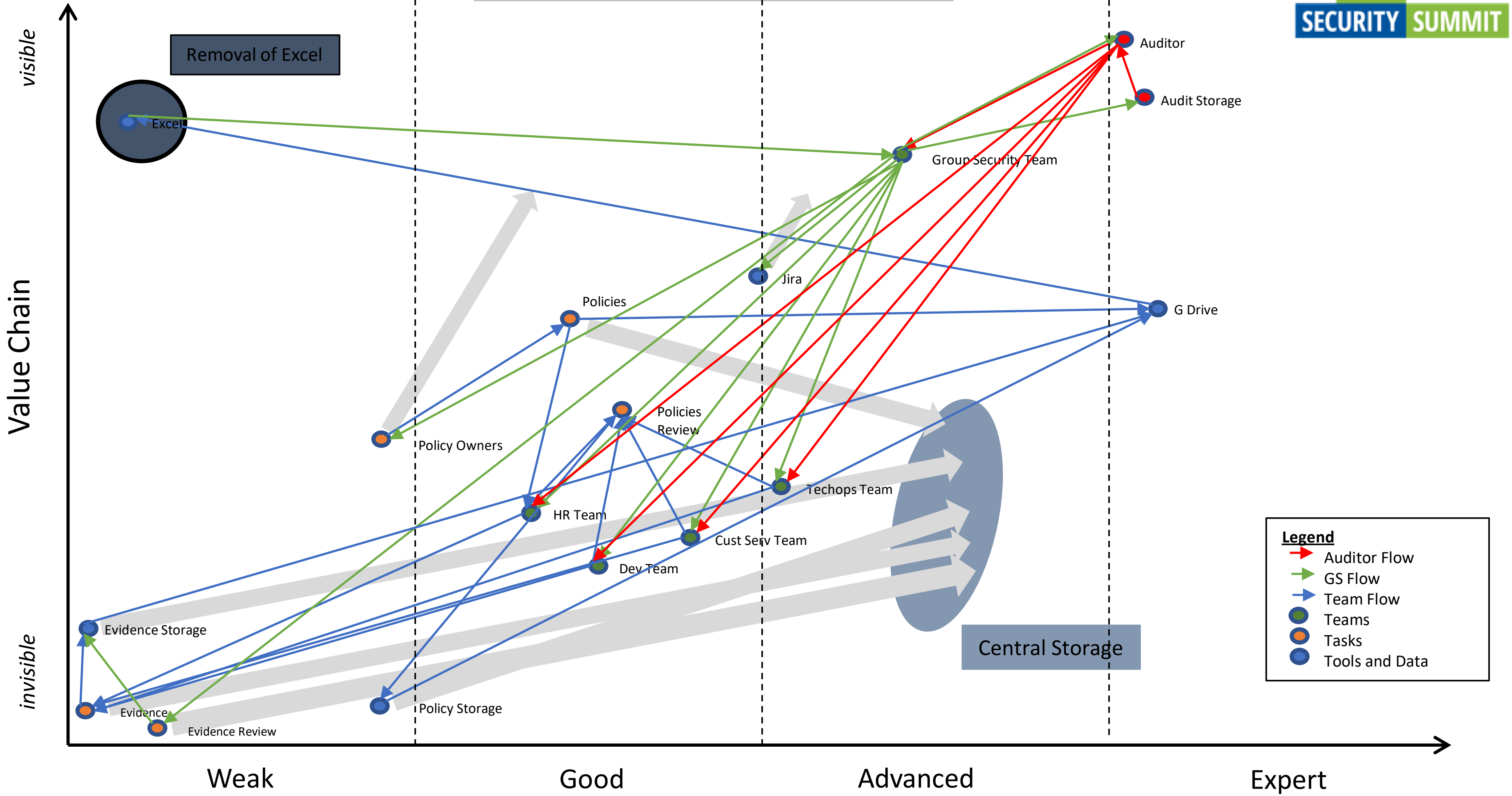
Policy Storage

Legend

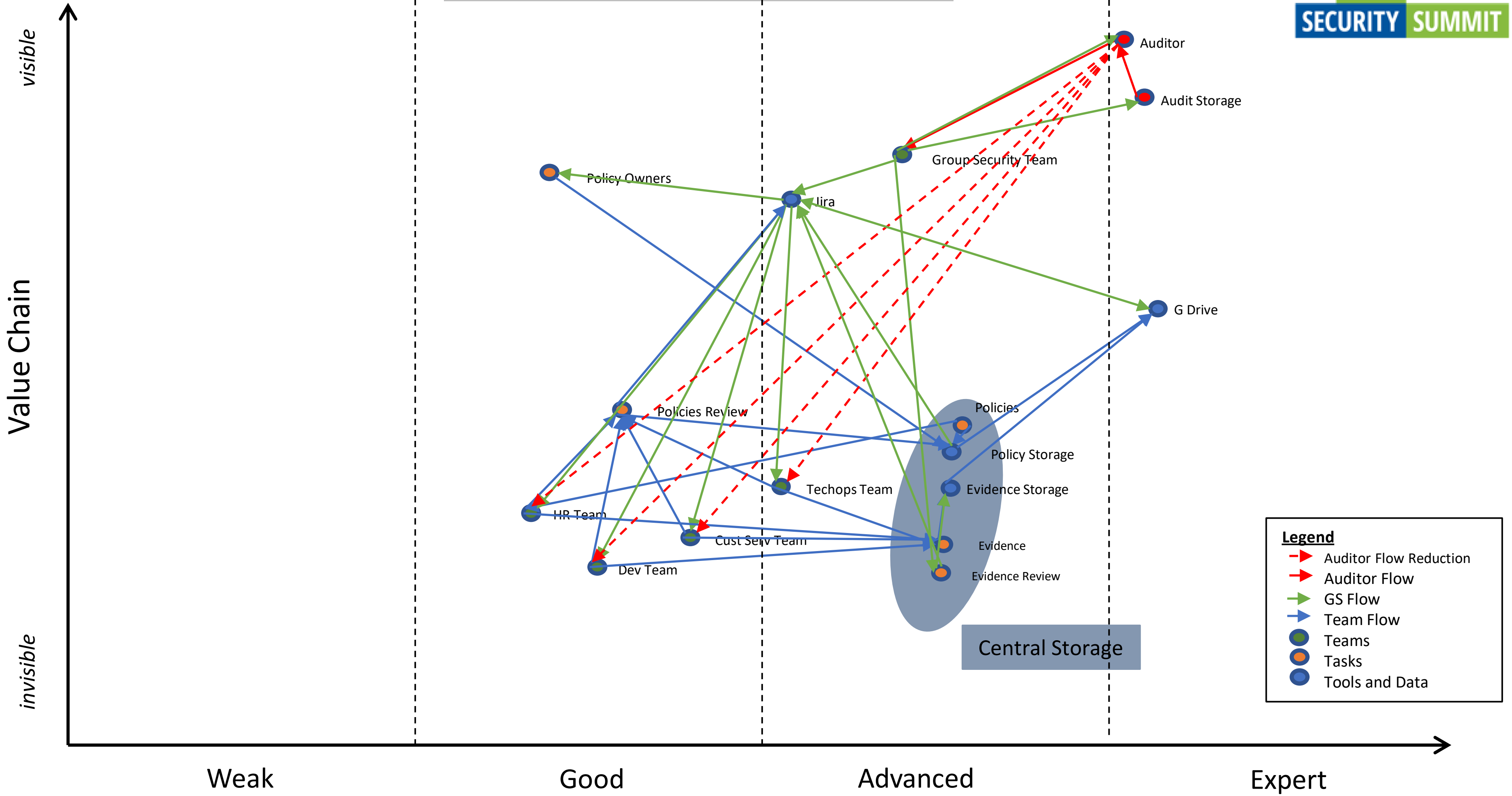
- Auditor Flow
- GS Flow
- Team Flow
- Teams
- Tasks
- Tools and Data

PCI Audit Process Maturity

OPEN SECURITY SUMMIT



PCI Audit New Process Used



Thank you