HACKINBO

Winter 2016 Edition

Information Security In an Agile Environment

Bologna
29 Ottobre 2016

Welcome

- **Giacomo Collini**
  Director of Information Security @ King.com

Chi Sono

2002–2006

TELECOM ITALIA

CAD IT INFORMATION TECHNOLOGY ®

2006–2012

PartyPoker World's Largest Poker Room

bwin .com

2014–…

King

2002–2006

2006–2012

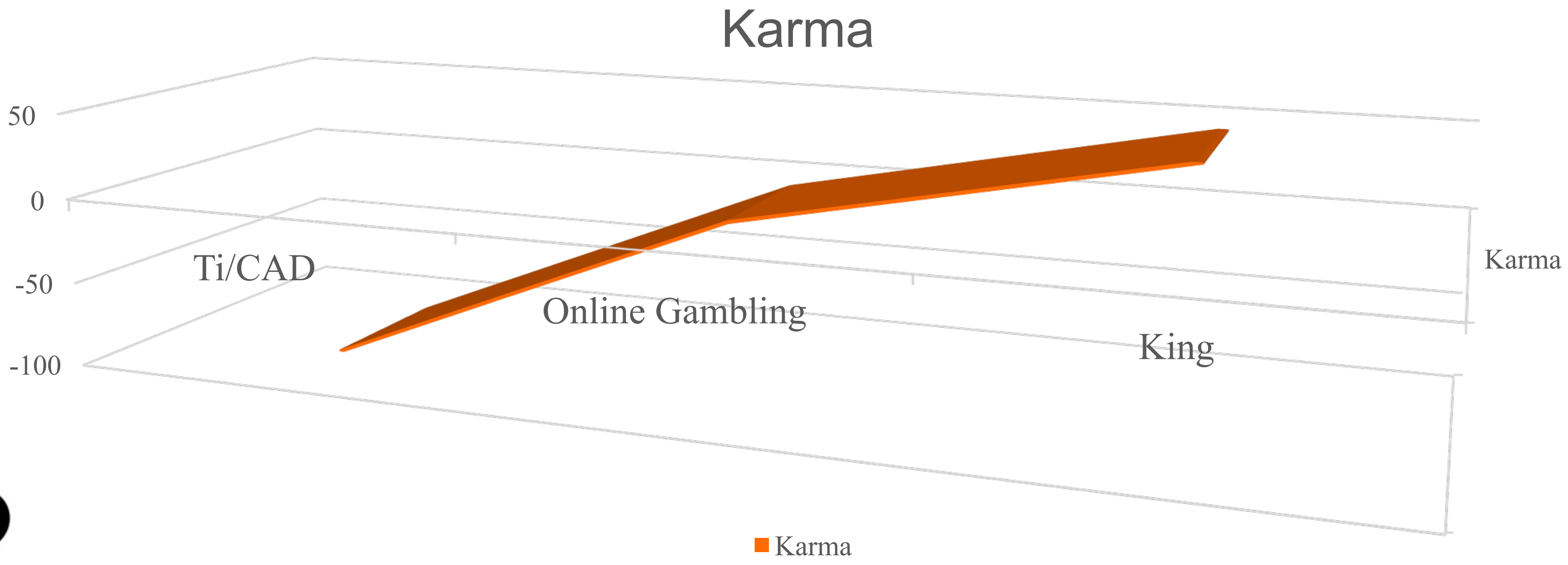
2014–…

TELECOM ITALIA CAD IT INFORMATION TECHNOLOGY

PartyPoker World's Largest Poker Room

bwin.com

King



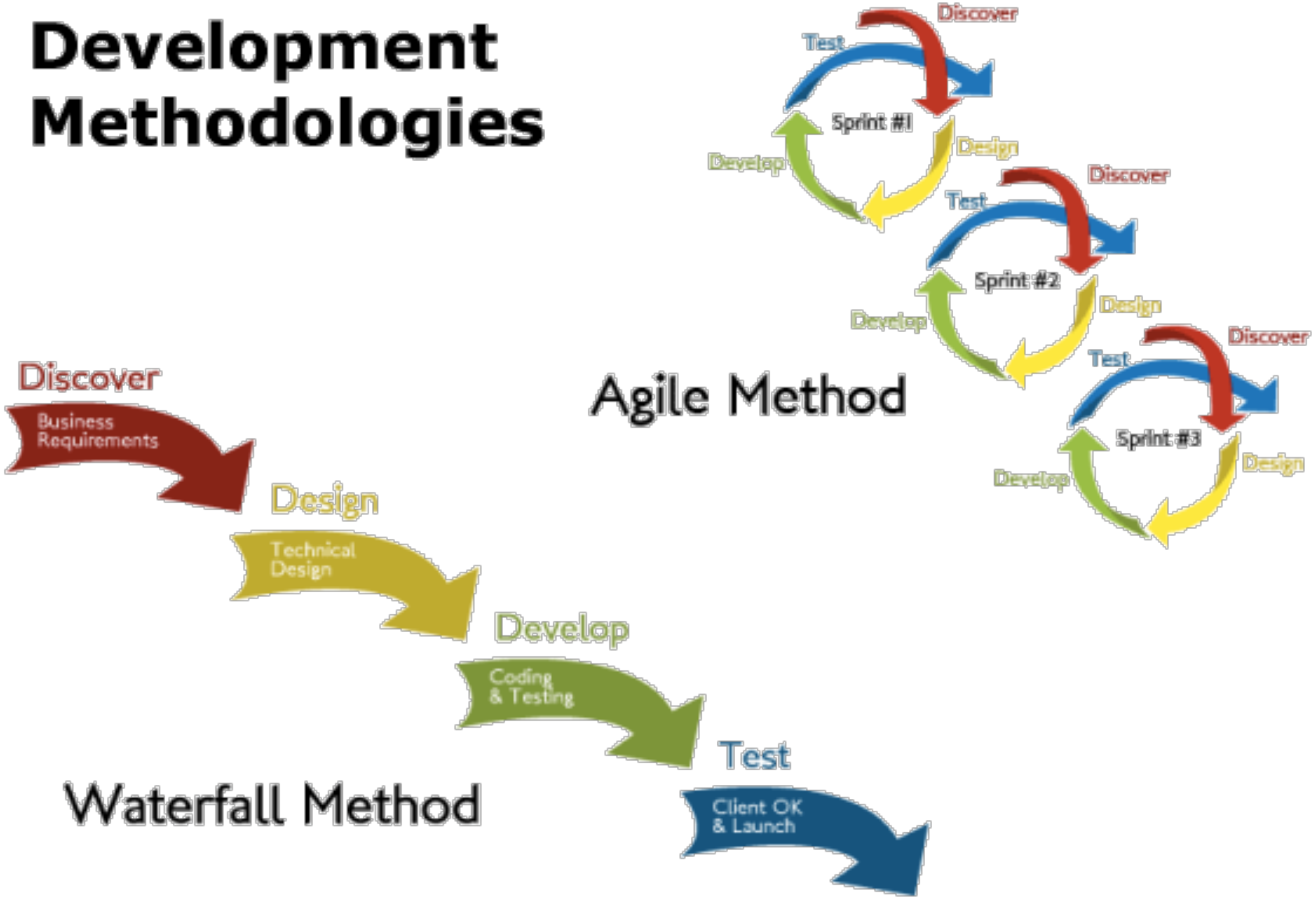
About King

- FY 2015
  - Revenues: 2Bn$
  - 499m MAU
- +12 Locations, 2000+ Employees, >50% Developers
- 10+ Security team

- 2016: Acquired by Activision|Blizzard for 5.9Bn$
- Currently operating as an independent unit of A|B

Cosa e’ Agile

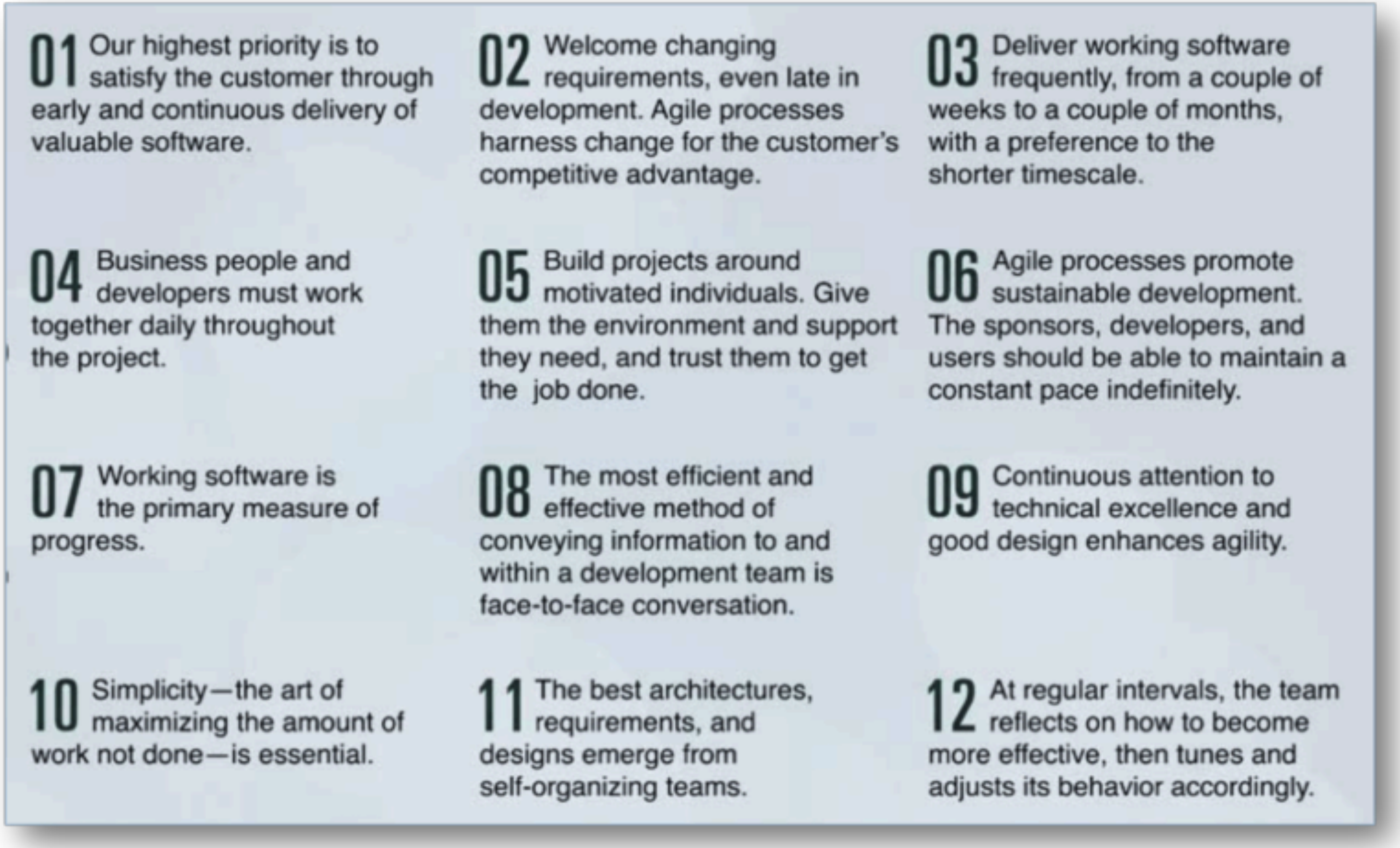
Development Methodologies



Agile - Disclaimer

- Agile Manifesto
- Am I believer?

- Iterative approach
- Short feedback
- Fail Fast
- Ready to Pivot
- No Dependencies
- Empowerment



01 Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.

02 Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.

03 Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.

04 Business people and developers must work together daily throughout the project.

05 Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.

06 Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.

07 Working software is the primary measure of progress.

08 The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.

09 Continuous attention to technical excellence and good design enhances agility.

10 Simplicity—the art of maximizing the amount of work not done—is essential.

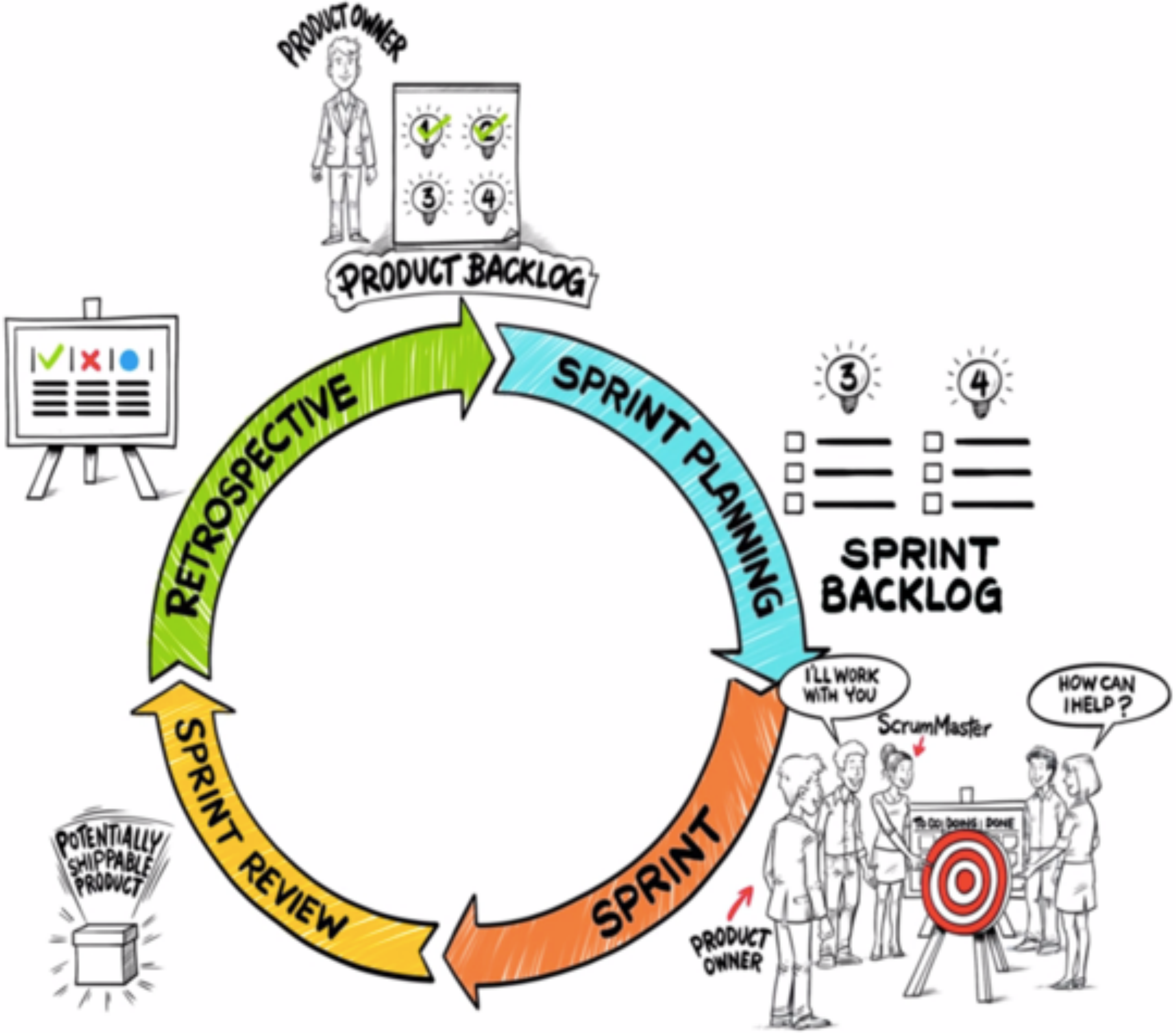
11 The best architectures, requirements, and designs emerge from self-organizing teams.

12 At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan

What is Agile

- Iterative approach
- Short feedback
- Fail Fast
- Ready to Pivot
- No Dependencies
- Empowerment



Fail Fast: Not suitable for everybody

Agile & Security

How Agile practices impact Security

Domain	Impact
Risk Management	None
Capital Planning	None
Resource Management	Medium
Policy Management	High
Data Management	Low
Incident Management	Medium
Disaster Recovery	Medium
Threat Intelligence	Low
Security Awareness	Low

Domain	Impact
App. Security Testing	High
Vendor Management	Medium
Asset Management	Medium
Physical Security	Medium
Data Management	Medium
Identity and Access	None
Change Control	High
Vulnerability Mgmt.	High
Systems Standards	High

Policies, Standards and Guidelines

PROBLEMS:

- Policy Based approach won’t work or won’t be sufficient
- Agile suggests external dependencies to be reduced to a minimum

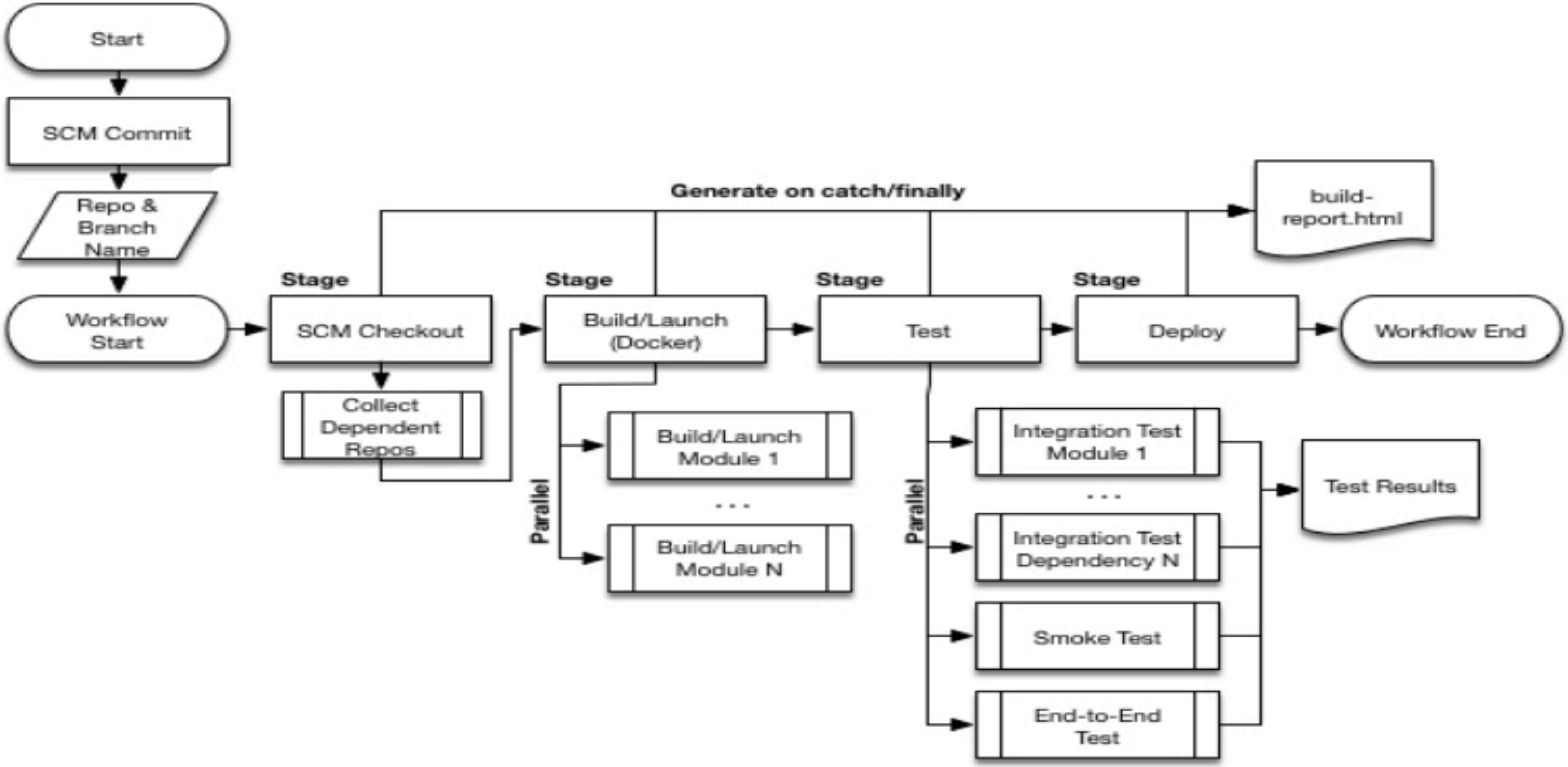
MITIGATION:

- Security to become a customer advocate
- Work with Product Owners and Team Leads
- Implement patterns that makes sense

Secure SDLC

- Probably the, most impacted domain
- Embed Security in the Quality Program (if there is any)
- Work with Lead Developers and Product Owners
- Find your champions
- Embed controls in the CI Loop

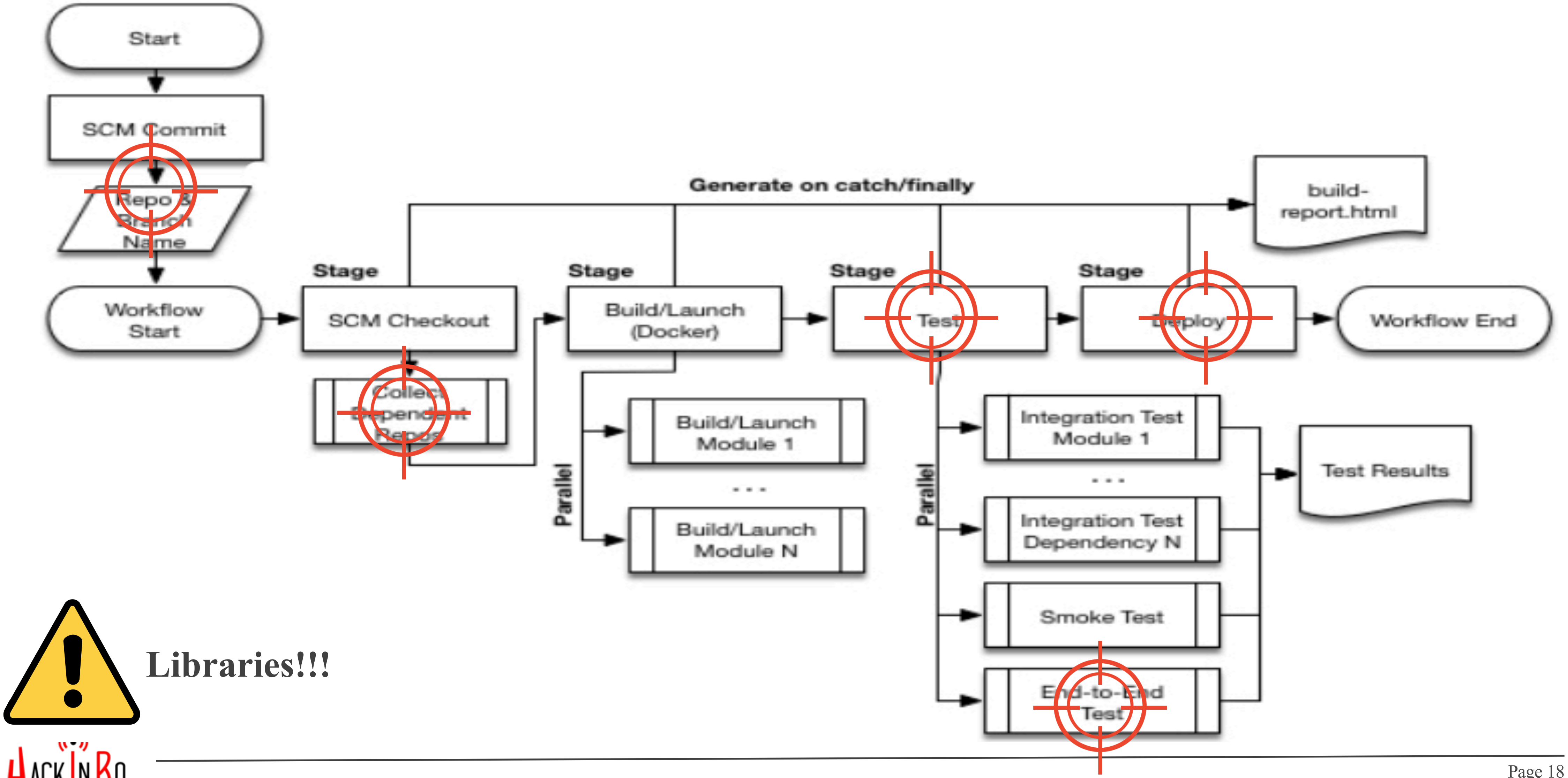
Secure SDLC



Start
SCM Commit
Repo & Branch Name
Workflow Start
Generate on catch/finally
build-report.html
Stage
SCM Checkout
Collect Dependent Repos
Stage
Build/Launch (Docker)
Parallel
Build/Launch Module 1
. . .
Build/Launch Module N
Stage
Test
Parallel
Integration Test Module 1
. . .
Integration Test Dependency N
Smoke Test
End-to-End Test
Test Results
Stage
Deploy
Workflow End

Agile Security

Secure SDLC



Libraries!!!

Empower your colleagues

- People are a big part of the equation, Security Awareness must be at the centre of our strategy
- Bring people to your side, explain why some controls are needed
- Many vulnerabilities are reported by people and not tools

Never waste people's time!

Agile & Friends

- Keep them out of privileged network

- Adopt some sort of MDM

- Strategy must be data driven rather than device driven

salesforce
Google Apps
workday

amazon
web services
Azure

Services **VS** **Platforms**

AND THEN WE TOLD THEM
THEIR PERIMETER WAS SECURE!
memegenerator.net

Identity Management

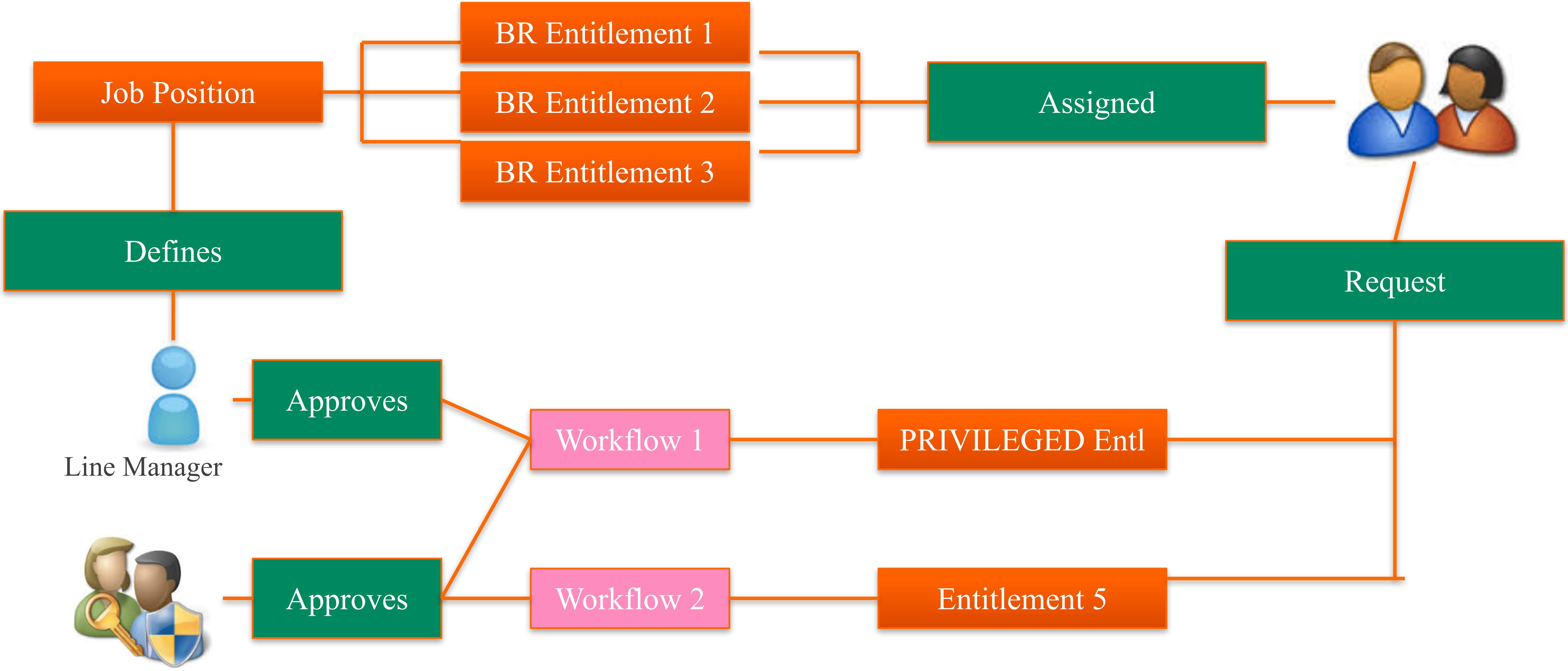
What we wanted to build and How did we built it

- Success Criteria
  - Automate as much as possible
  - Open Architecture → Support for Open protocol (SAML, openID, RESTful API)
  - Accommodate both Cloud and On-premises
  - Allow for exceptions and partially manual workflows
  - Contractors, Service Accounts, Privileged Accounts

How to do it (the Agile way)

- Identify your MVP
- Iterate
- Keep communication flowing

Entitlement management

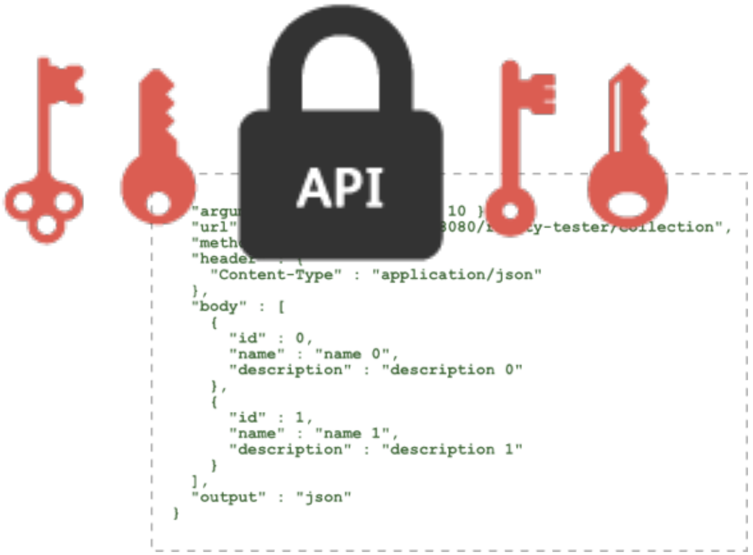


Automation

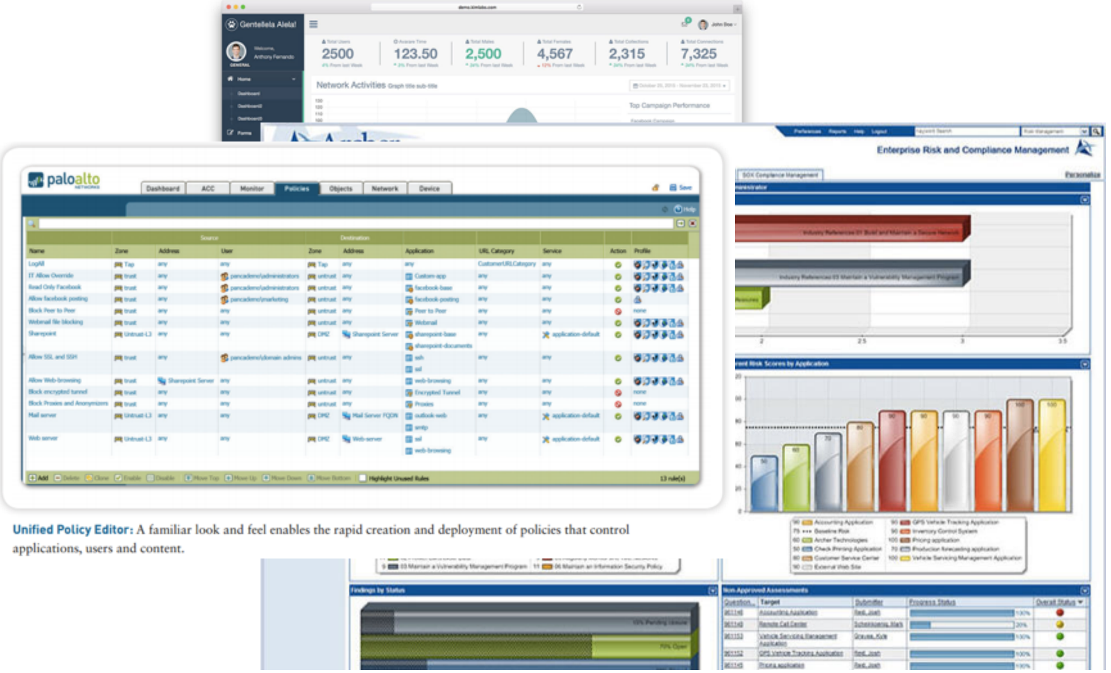
- Automation is key to optimize the output of your workflows, you cannot afford to not do it
  - SOC Operations
  - Incident Mitigation
  - Identity Management

- You need developers!

- API vs Dashboards

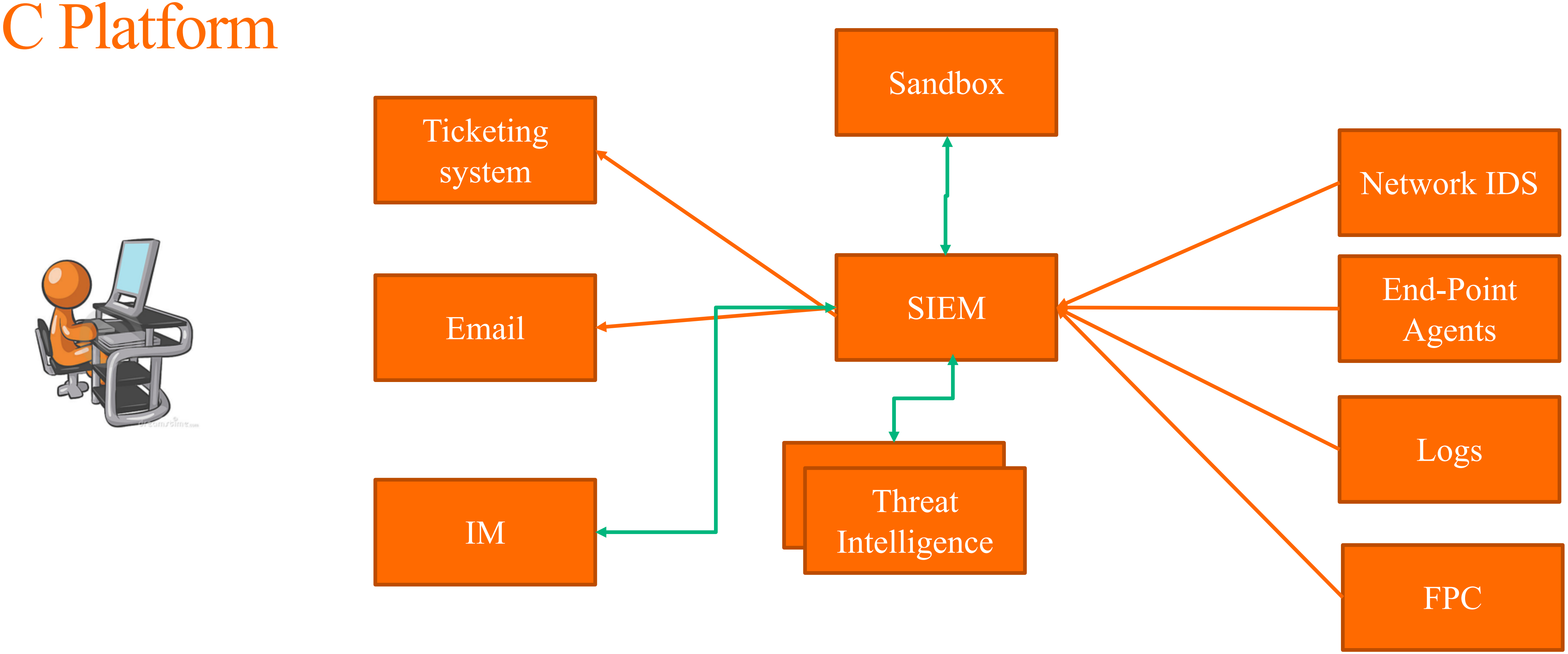


```
  "argu                          10 }
  "url"                         8080/i    y-tester/collection",
  "meth
  "header
    "Content-Type" : "application/json"
  },
  "body" : [
    {
      "id" : 0,
      "name" : "name 0",
      "description" : "description 0"
    },
    {
      "id" : 1,
      "name" : "name 1",
      "description" : "description 1"
    }
  ],
  "output" : "json"
}
```



Unified Policy Editor: A familiar look and feel enables the rapid creation and deployment of policies that control applications, users and content.

SOC Platform



The human factor

1) You have to increase awareness to make sure your colleagues are not weaponized by the enemy

2) You need to involve them to maximize their buy-in

3) You need to lead by example

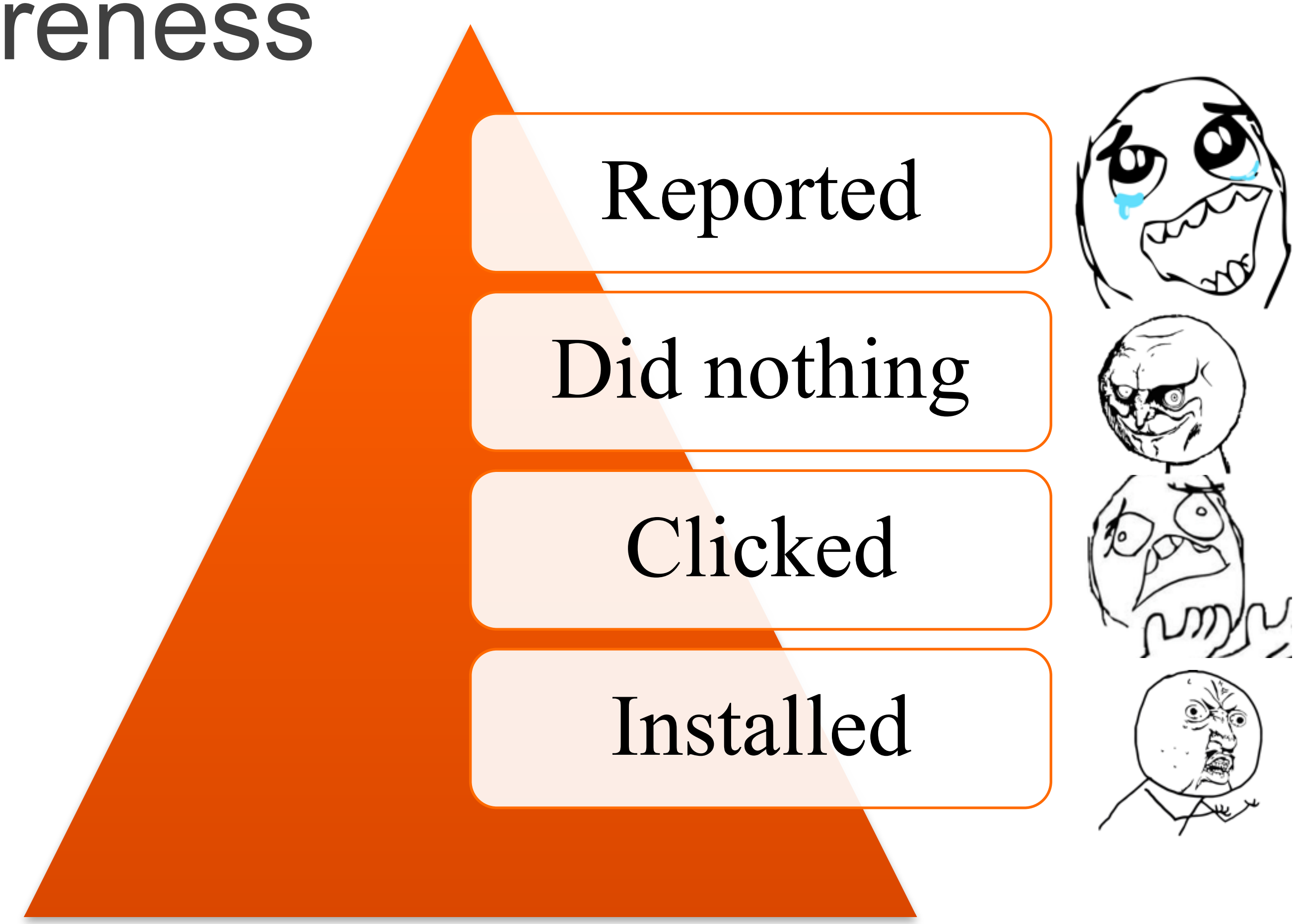
1) Establish a culture of mutual trust and respect

2) Communicate and look for feedback

3) Try to enforce your vision in your area of influence

- Phishing is one of the cheapest vector for attackers to attempt
- Users must be trained according to their knowledge
- High sensitive users must be given special attention
- Phishing campaigns should be part of your Security Awareness Programme

Phishing Exercise results driven targeted awareness



Reported

Did nothing

Clicked

Installed

Useful Metrics

- Number of Security issues reported by colleagues
- Time to report a phishing attack
- End-point security events
- RT exercises result

Compliance

Compliance

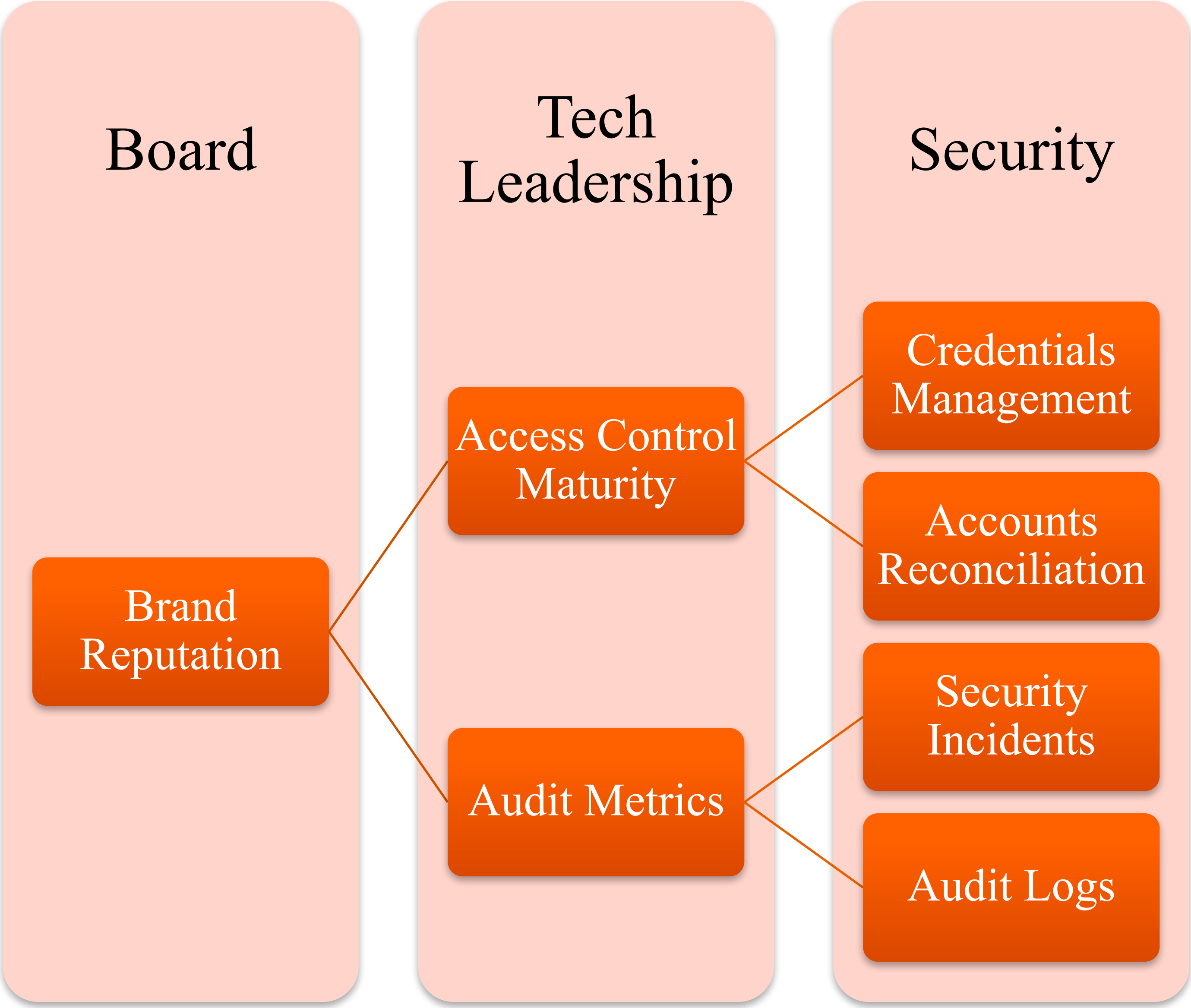
- Compliance != Security
- Compliance usually is decontextualized and based on not current/wrong assumptions.

- It can be helpful to drive Security, especially to drive un-popular controls
- If it’s finance driven it can be usually steered in an harmless way
- Standard like ISO have been risk based for a long time, some auditors don’t know thou

Risk Management

Risk Management

- Align to business opportunities and risk, monitor the context
- Identify major risks and worst case scenarios
- Map controls to risks and monitor per risk expenditure
- Define your technical vision: Prevent VS Be Prepared
- Balance technical controls with non-technical
- Change metrics and level of details depending on the audience
- Aim for relevant and meaningful metrics
- Analyse historic data



Board
Tech Leadership
Security
Brand Reputation
Access Control Maturity
Audit Metrics
Credentials Management
Accounts Reconciliation
Security Incidents
Audit Logs

KEEP
CALM
AND
BE
PREPARED

Thank you!