knowledge17

WORK at LIGHTSPEED™

Six Weeks to Security Operations – The AMP Story

DR. MARILYN K NELSON
PARTNER
KPMG Australia

RAHN WAKELEY
HEAD OF TECHNOLOGY – CYBER SECURITY
AMP

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Introductions
- The AMP Security Operations Story
- Lessons Learned
- Next Steps
- Key Take-Aways
- Questions & Answers

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



NAME: Marilyn Nelson, PhD

TITLE: Partner

FUNCTION: Global ServiceNow Practice Lead

COMPANY: KPMG Australia

EXPERIENCE: 31 years in Service Management Leadership, 12 years in ServiceNow implementations

EXPERTISE: ITSM, Governance, Risk Compliance, Security, HR, Configuration Management, Finance

ACHIEVEMENTS: Lead the first implementation of ServiceNow in 2005, successfully lead the delivery of 29 ServiceNow implementations, stepped foot on every continent except Antarctica (it's on my list) and lived in Panama, UK, Saudi Arabia, Singapore and Australia leading the worlds largest ServiceNow implementations to date

CURRENT PROJECTS: Custom build on ServiceNow platform for Tax lodgement, HR Case Management, and ITFM

© 2017 ServiceNow All Rights Reserved

My Company



NAME: KPMG

INDUSTRY: Finance, Higher Education, Healthcare, IT Services, Manufacturing, Government, Media, Telcom, FinTech

MARKET FOCUS: My area of KPMG focuses on providing Management Consulting, IT Operating Model, and ServiceNow Implementations

COMPANY'S PRIMARY PRODUCTS/SOLUTIONS: IT Operating Model, Organisational Transformations, ServiceNow Security Operations, HR Transformation on ServiceNow, Finance Transformations on ServiceNow

COMPANY-WIDE INITIATIVES: Cost efficiency, Regulatory Compliance, Speed of development/deployment/quality, Responsiveness to customers/partners/other teams

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



NAME: Rahn Wakeley

TITLE: Head of Technology

FUNCTION: Cyber Security

COMPANY: AMP

EXPERIENCE: 20 years experience in the IT industry, including 15 years' specialising in cyber security disciplines

EXPERTISE: Enterprise security governance, security architecture, security consulting & application security

ACHIEVEMENTS: Delivered ServiceNow security operations including a functional Cyber security service catalogue in 6 weeks

CURRENT PROJECTS: Driving process efficiencies and automation in Incident responce

© 2017 ServiceNow All Rights Reserved

My Company



NAME: AMP

INDUSTRY: Financial Services

MARKET FOCUS: Financial services company in Australia and New Zealand with superannuation and investment products, insurance, financial advice and banking products

COMPANY'S PRIMARY PRODUCTS/SOLUTIONS: Banking, Investment management, Financial planning and advice, Insurance and superannuation

COMPANY-WIDE INITIATIVES: Grow internationally, Create a customer-centred culture, Regulatory Compliance & risk management, Become more efficient by changing the way we work and use technology

© 2017 ServiceNow All Rights Reserved

Session Overview



Objectives

- Provide insight to the AMP ServiceNow Security Operations deployment



What You Will Learn

- Understand the environment and challenges facing AMP
- Learn about how KPMG deployed SecOps in six (6) weeks
- Gather key lessons related to Security Operations on the ServiceNow platform
- Discuss how the lessons may apply to you for your initiatives/projects

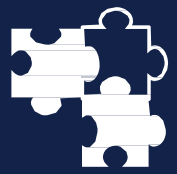
© 2017 ServiceNow All Rights Reserved

Context – Setting the stage

- Industry trends
  - Corporate reputation is critical and needs to be protected from cyber attacks
  - Growing customer expectations for data privacy of personal data
  - Regulatory hurdles, compliance needs (standards, audits)
- Competitive pressures
  - Increasing competition with specialized products – too many creating an influx of data but no real way to manage
- Corporate transformations
  - Legacy processes and infrastructures
  - Push for cloud
  - Push for analytics & standardisation
  - Desire for more Data driven decisioning
- Departmental/Project/Program drivers and goals
  - Push for Agile methodologies
  - Reduction in time to identify, analyse, and respond to vulnerabilities, security incidents, and threats

© 2017 ServiceNow All Rights Reserved

Challenges and Goals

PREVENT	IMPROVE	DETECT	RESPOND
			
Client was struggling with immature vulnerability response and security incident response processes	No tracking and auditing capability for approving of accepted vulnerabilities as well as re-opening vulnerabilities that have been marked as closed	Identifying relevant CI stakeholders and remediation of vulnerabilities would take up to 3 months which is a significant amount of time in the Cyber domain	Responding to security incidents was largely done inconsistently by multiple vendors with little or no oversight by the client
STRATEGY AND GOVERNANCE	TRANSFORMATION	CYBER DEFENSE	DIGITAL RESPONSE SERVICES

© 2017 ServiceNow All Rights Reserved

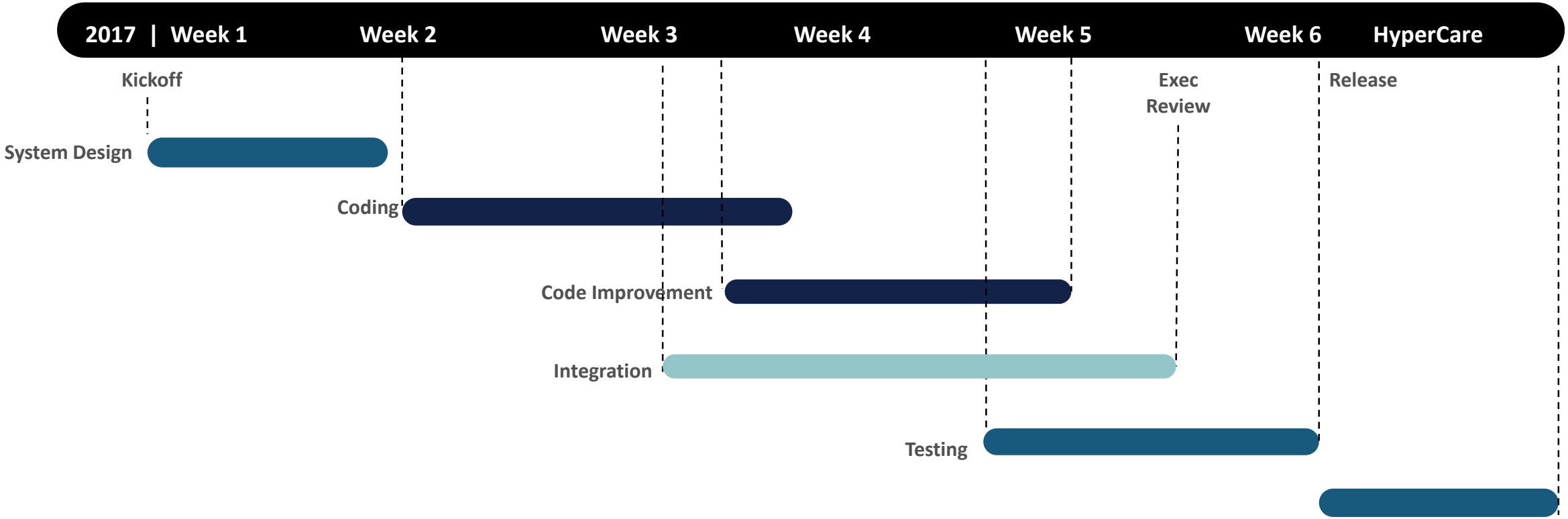
Solution – Strategy and Approach

With modern solutions, detecting Vulnerabilities and Threats is no longer the key issue. KPMG sees that organisations struggle more to implement efficient and effective collaboration between security and IT.

Process & Workflow Gap	Responsibility Gap & Overlap	Tooling & Automation Gap	Service Level Gap	Role of ServiceNow
Reviewed and analysed existing processes	Designed and implemented ServiceNow Security Operations suite	Linked ITSM incident process to security incident response	Enabled threat intelligence capability to obtain immediate information around indicators of compromise	ServiceNow played an important role in bridging the gaps between IT & Security

© 2017 ServiceNow All Rights Reserved

Solution – Timeline



© 2017 ServiceNow All Rights Reserved

Value Outcomes

A decrease of

60%

Response Time

Vulnerability Response Time



Months to Minutes Response

3X

FASTER

Security Incident Response Time

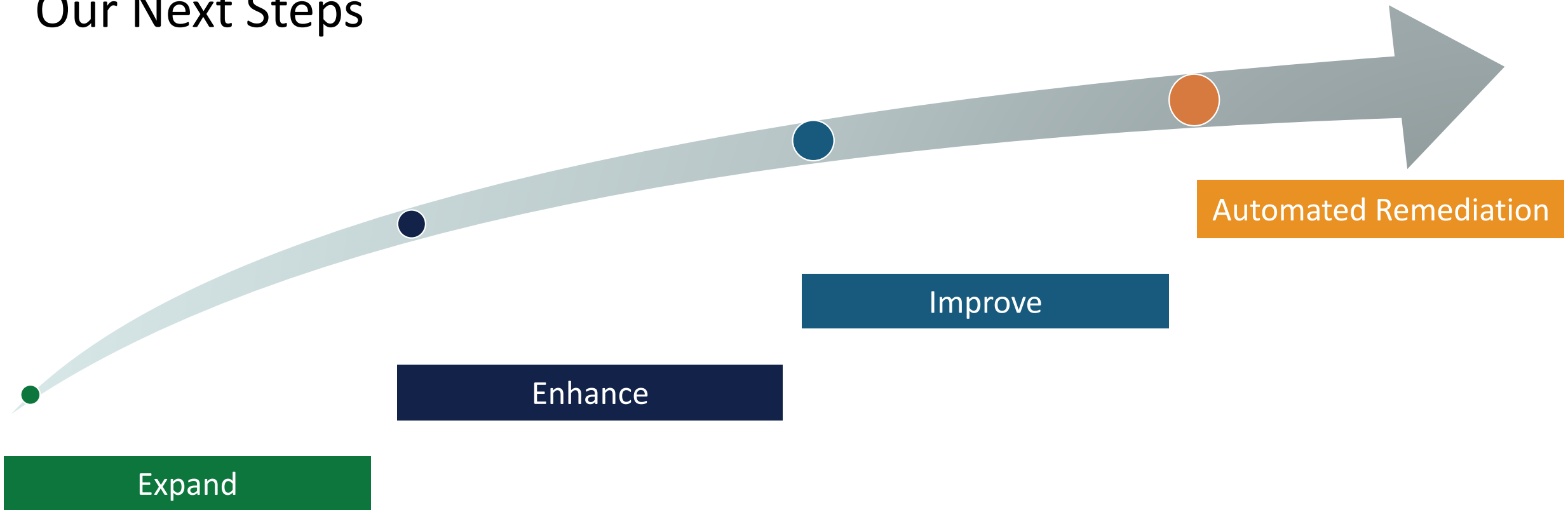
© 2017 ServiceNow All Rights Reserved

Lessons Learned

- Leadership from the top is essential
- Documenting each process prior to development is critical
- Identifying key metrics and expected outcomes early
- Organisational Change Management & training is an absolute must

© 2017 ServiceNow All Rights Reserved

Our Next Steps



© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Document processes to streamline operations and build a fit for purpose Security Operations capability



2

Your CMDB is a critical component to a robust Security Operations capability



3

Start with the basics and grow your Security Operations capability



© 2017 ServiceNow All Rights Reserved

Solution at a Glance

- Vulnerability Response
- Security Incident
- Threat Intelligence

Deployed in

6 weeks

1 Single repository for all Security incidents enabling holistic reporting and responding to security incidents in a standardized way

24

Including incoming Events from **FireEye**

60% Reduction in Vulnerability response time*

Significantly reducing vulnerability window and improving AMPs security posture

1 Single 'Front Door' to engage with AMP's Cyber Team

With an initial number of **8** Security catalogue items

AMP

AMP is a Global 2000 financial services company in Australia and New Zealand with superannuation, investment products, insurance, financial advice and banking products including home loans and savings accounts

50% of CIs updated with correct IP information as part of a vulnerability scan

resulting in a significant improvement in **CMDB data quality**

30% reduction* in SIR Resolution time

50,000 Vulnerable items processed, prioritized and actioned

within 24 hours from Go-Live

* Projected metric

© 2017 ServiceNow All Rights Reserved

Q & A

DR. MARILYN K NELSON
PARTNER
KPMG Australia

RAHN WAKELEY
HEAD OF TECHNOLOGY – CYBER SECURITY
AMP

© 2017 ServiceNow All Rights Reserved

Thank You

DR. MARILYN K NELSON
PARTNER
KPMG Australia

RAHN WAKELEY
HEAD OF TECHNOLOGY – CYBER SECURITY
AMP

© 2017 ServiceNow All Rights Reserved

Take the Survey

Please take a moment to complete a session survey in the Knowledge17 app.

Thank You

Dr. Marilyn K Nelson

Partner

KPMG Australia

Rahn Wakeley

Head of Technology – Cyber Security

AMP

© 2017 ServiceNow All Rights Reserved