knowledge17

WORK at LIGHTSPEED™

Integrated Security Operations – The Difference between Knowing and Guessing

MATTHEW O'BRIEN
SENIOR GLOBAL PRODUCT MANAGER, CYBERSECURITY
DXC.technology

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- About DXC.technology
- The Problem
- The Approach
- The Solution
- ISecOps Demo
- The Lessons

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



NAME: Matthew O'Brien

Title: Senior Global Product Manager, Cybersecurity

Function: Security Product Development and Integration

Company: DXC.technology

EXPERIENCE: 20+ years IT Experience with emphasis on IT/Enterprise Architecture, Technology Strategy, Policy and Process, and directing the development of DXC's managed security services portfolio

EXPERTISE: IT governance and strategy, risk management, enterprise architecture, solution design, technology planning, and policy design

CURRENT PROJECTS: Intelligent SOC, ISecOps evolution and integration

© 2017 ServiceNow All Rights Reserved

My Company



NAME: DXC.technology

Industry: Global IT Services Company

Market Focus: DXC Technology is the world's leading independent, end-to-end IT services company. We guide clients on their digital transformation journeys, multiply their capabilities, and help them harness the power of innovation to thrive on change.

DXC Security - ISecOps Solution Highlights

- Security Incident and Vulnerability Management and Response
- Integrated Security Controls for enhanced and automated Security Operations
- Dashboards for Analyst and Customer visibility into the Enterprises Security Posture and workflow management

The DXC Difference

- Technology independence
  - Working with our global partner network, we deliver best-of-breed solutions to meet each client's unique needs and technology preferences
- Clear and confident vision
  - We have met the challenges of innovation many times before, and have a clear and confident vision for navigating the future
- World-class talent
  - We are investing to attract and upskill the talent that will lead global business tomorrow

© 2017 ServiceNow All Rights Reserved

Session Overview



Objectives

- To demonstrate how DXC transformed its security incident response and vulnerability management processes to better manage and respond to threats across the enterprise



What You Will Learn

- Understand the environment and security challenges facing DXC and the market in general
- Learn about DXC's Integrated Security Operations managed service
- Gather key lessons related to ISecOps implementation and management
- Discuss how the lessons may apply to you for your initiatives/projects

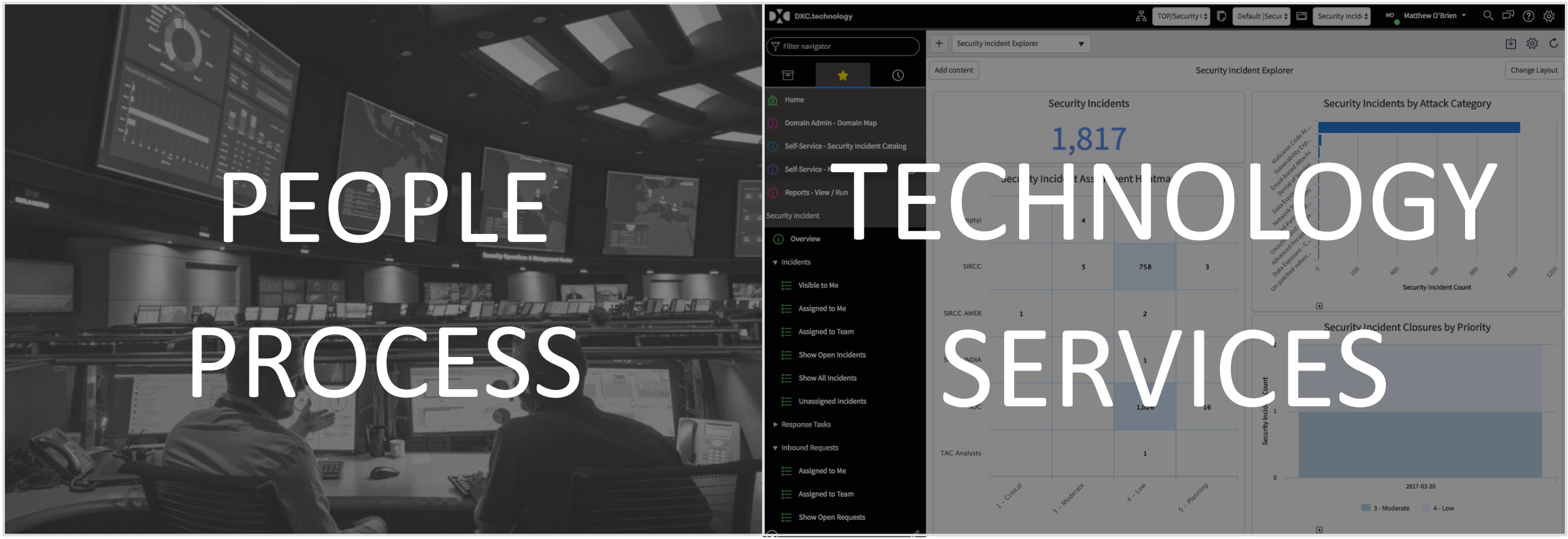
© 2017 ServiceNow All Rights Reserved

What is Integrated Security Operations (ISecOps)?

Intelligence Driven, automated security incident response and vulnerability management

Integrated Security Operations and Incident Response

Incident and Vulnerability Management Platform



© 2017 ServiceNow All Rights Reserved

Industry Trends - Digital Needs a New Style of Protection

PERVASIVE MOBILITY

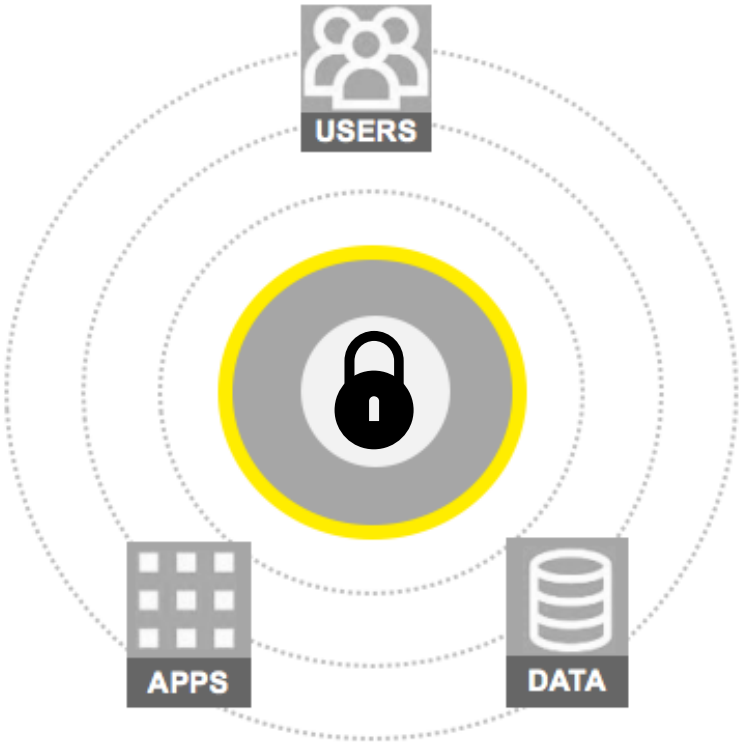
Less enforcement and control over enterprise data access from a myriad of uncontrolled devices sharing applications and systems. Increased complexity, risk and non-compliance.

PRIVACY | PROTECTION | MANAGEMENT

DIGITAL WORKFLOW

Inability to detect advanced threats and incidents, minimizing detection time and remediation across a growing number of attack surfaces.

DETECT | RESPOND | REMEDIATE



HYBRID INFRASTRUCTURE

Loss of visibility control and data through insecure Shadow IT, API and interfaces. Inadequate governance, risk, compliance and control of ongoing use of cloud applications and infrastructure.

VISIBILITY | POLICY | CONTROLS

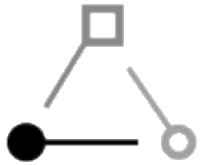
BIG DATA ANALYTICS

Rapid growth and exchange of data with lack of classification and protection at scale leading to loss. Insufficient governance and enforcement leading to non compliance and fines.

ACCESS | AUDIT | AUTHORIZE

© 2017 ServiceNow All Rights Reserved

Security Teams are Under Pressure



IT departments feel the squeeze but…

budgets are under pressure and security is now a board-level issue



The innovative adversary

is increasingly sophisticated and, on average, goes undetected for 99 days[1]



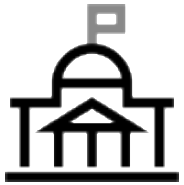
Security operations

need maturity, speed & scale to move beyond real-time threat monitoring



Next generation threats

such as ransomware or file-less, memory-based malware makes it difficult to stay secure



Regulatory pressures

grow for industry and geography compliance requirements such as GDPR



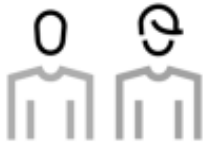
Widening skills gap

makes it hard to attract, train, and retain security professionals, yet the demand for security talent is expected to increase by 53% in 2017[2]



Device, cloud explosion

is causing significant increases in the enterprise threat surface



People are weakest link

and require awareness and training to protect against the 80% of attacks that target user access[3]

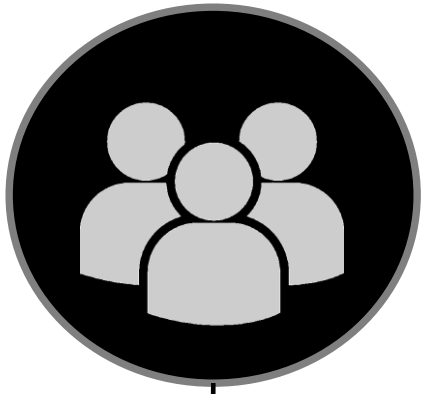
Sources:1: Mandiant M-Trends 2017 Report; 2: US Bureau of Labor Statistics, 3: CyberArk Security Report 2015

© 2017 ServiceNow All Rights Reserved

Sources:1: Mandiant M-Trends 2017 Report; 2: US Bureau of Labor Statistics, 3: CyberArk Security Report 2015

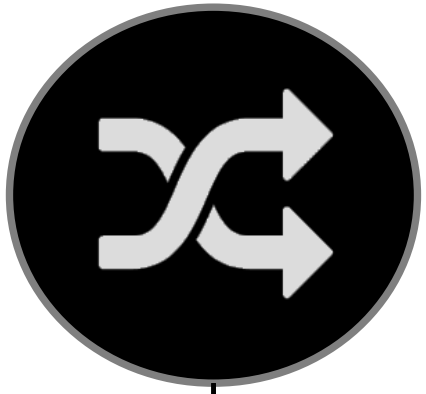
We have Invested Heavily in Trying to Protect Our Enterprise

People



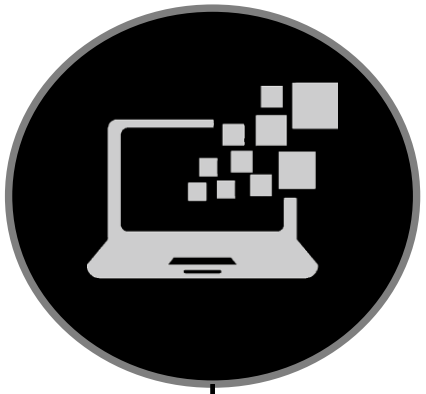
- Security Operations
- Engineering
- Security Incident Response

Process



- Managing Events
- Managing Vulnerabilities
- Managing Security Incidents
- Managing Assets

Technology



- Protection Technologies
- Detection Technologies
- Visibility Technologies

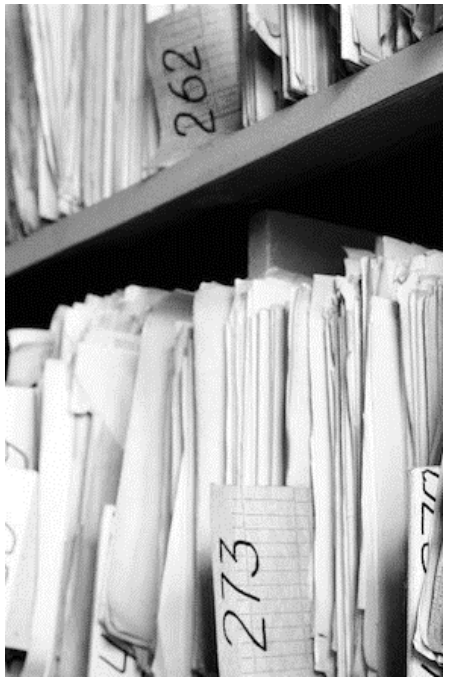
© 2017 ServiceNow All Rights Reserved

Our Problems

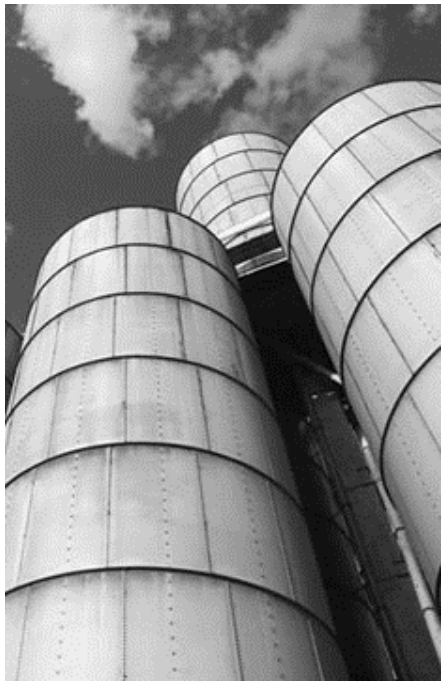
Too Many Alerts & No Context



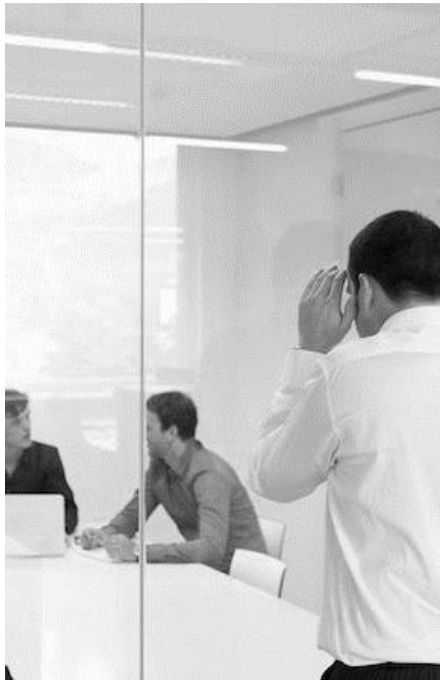
Manual Processes and Tools



Information Silos: Security vs. IT



Limited Enterprise Visibility



Increasing Compliance Requirements



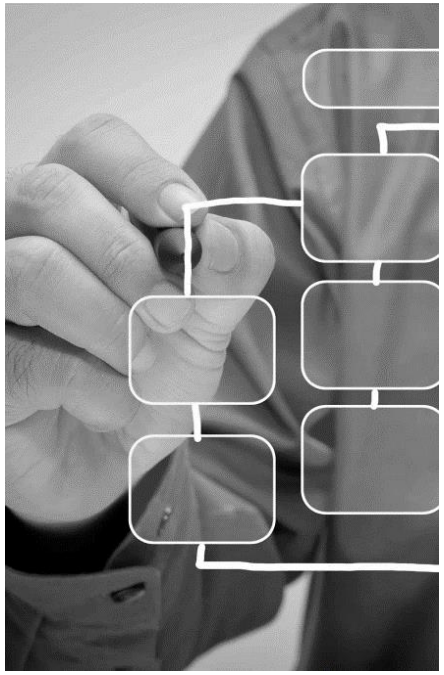
© 2017 ServiceNow All Rights Reserved

Our Business Goals

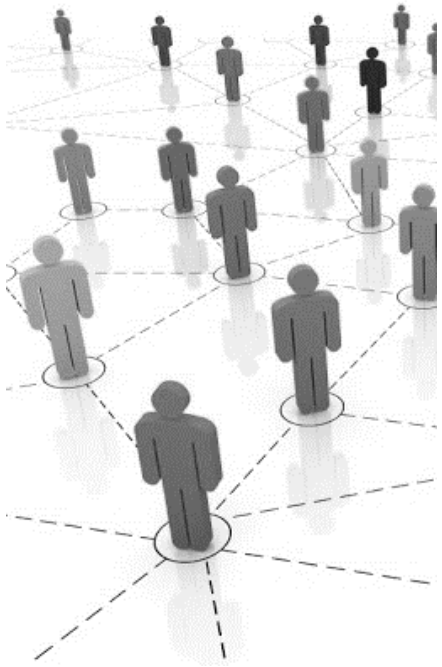
- Integrate teams across the organization ✓



- Reduce manual workloads and processes ✓



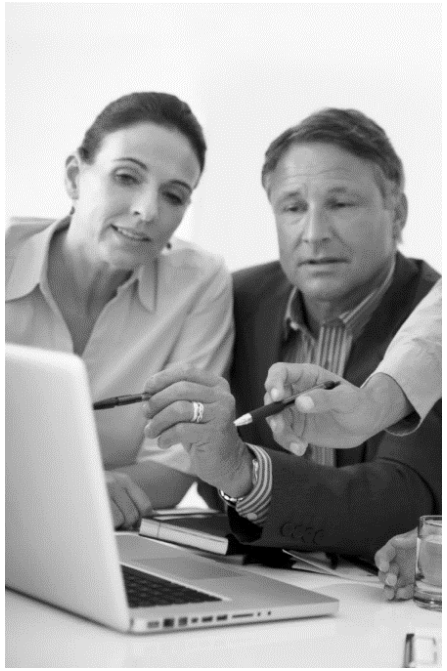
- Enterprise visibility of security posture ✓



- Reduce time to manage incidents & vulnerabilities ✓



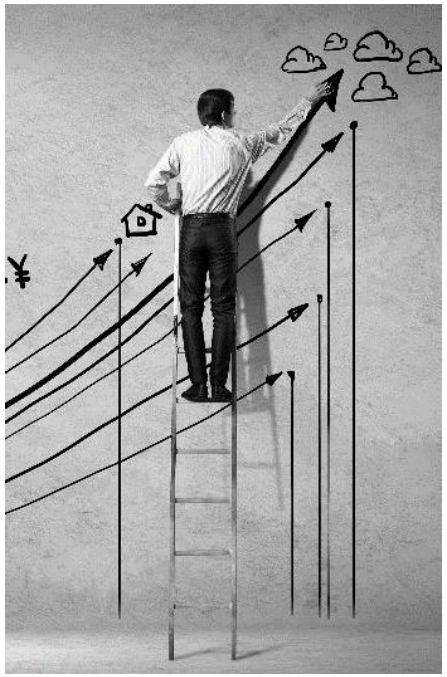
- The ability to easily audit security processes ✓

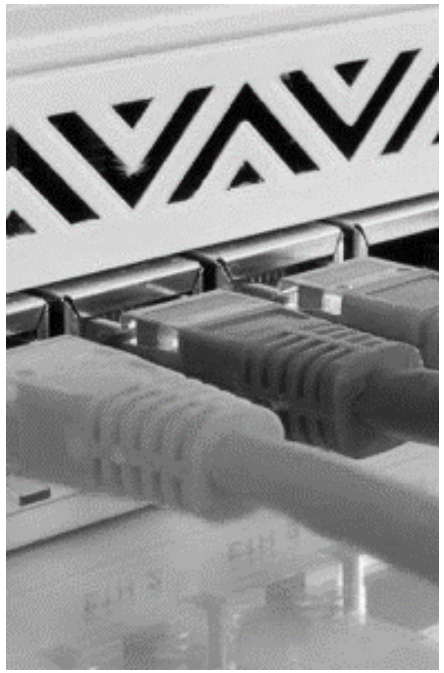


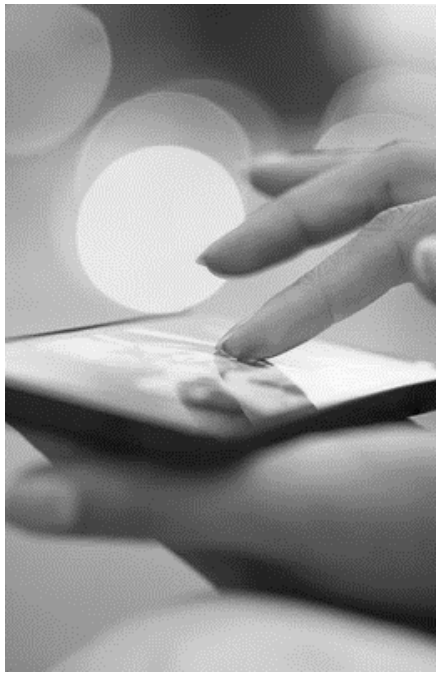
© 2017 ServiceNow All Rights Reserved

Our Technology Goals

- A solution that scales with the enterprise ✓
- The ability to leverage existing technology investments ✓
- Consolidate legacy technology into single platform ✓
- Enable granular control over data and access ✓
- Reduce technology spend ✓











© 2017 ServiceNow All Rights Reserved

Our Solution

Benefits

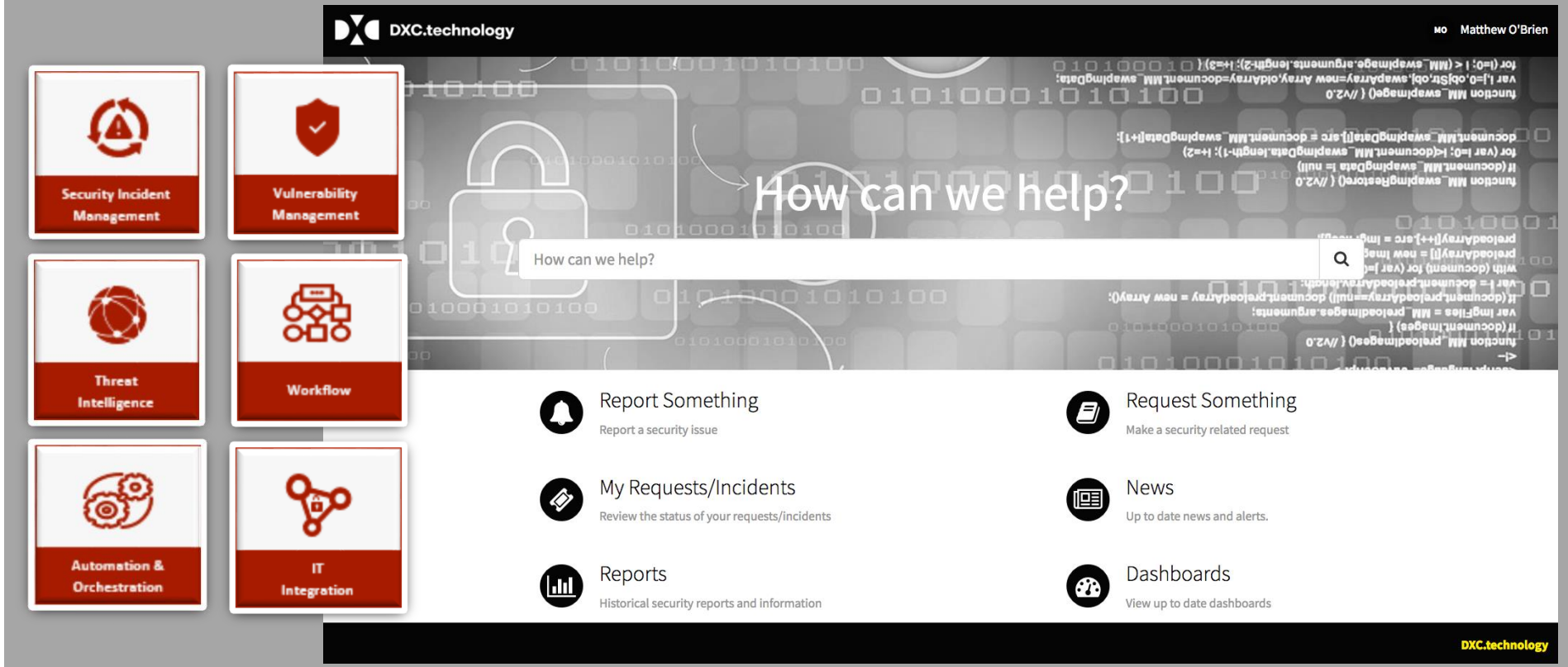
Enhanced Incident and Vulnerability Management

Operational Interlock

Improved Visibility

Reduced Time to Manage & Respond to Security Threats

iSecOps as a Service



© 2017 ServiceNow All Rights Reserved

Our Solution

Vulnerability Scanning

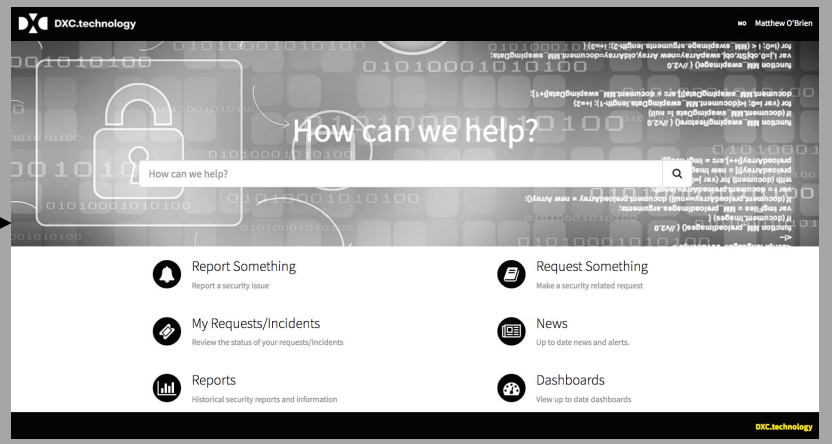
Qualys

Event Monitoring

SIEM
CrowdStrike Falcon
Firewalls
IDS/IPS
Endpoint Protection

Threat Libraries

Virus Total
CrowdStrike*



Service Catalogue
Executive Dashboard
Incident Notification
Reporting

ServiceNow Modules

Vulnerability Management

Security Incident Response

Threat Intelligence

iSecOps Analysts

Business Assets
CMDB
Service Models

Runbooks
Security Processes
Workflow

© 2017 ServiceNow All Rights Reserved

Our Solution – Framework & Methodology

ISecOps Delivery as a Service

Presentation & Reporting



Visualized Security Posture



Efficient Security Response

ISecOps
Portal/Ticketing/Reporting/Client Engagement



Security Management



Streamline Remediation

Management & Response

Security Incident Response

Security Operations Center		Account Security Management	Incident and Forensics Capabilities
Cyber Operations Cyber Service Management Integration, Controls Management	**Threat Analysis Center** Monitoring, Correlation , Incident Management and Triage, Threat Analysis	**Cyber Assurance & Compliance** Service Level Management, Cyber Compliance Reporting	**Cyber Consulting** Strategic Consulting, Incident Response, Forensic Investigation

Security Controls & Process Integration

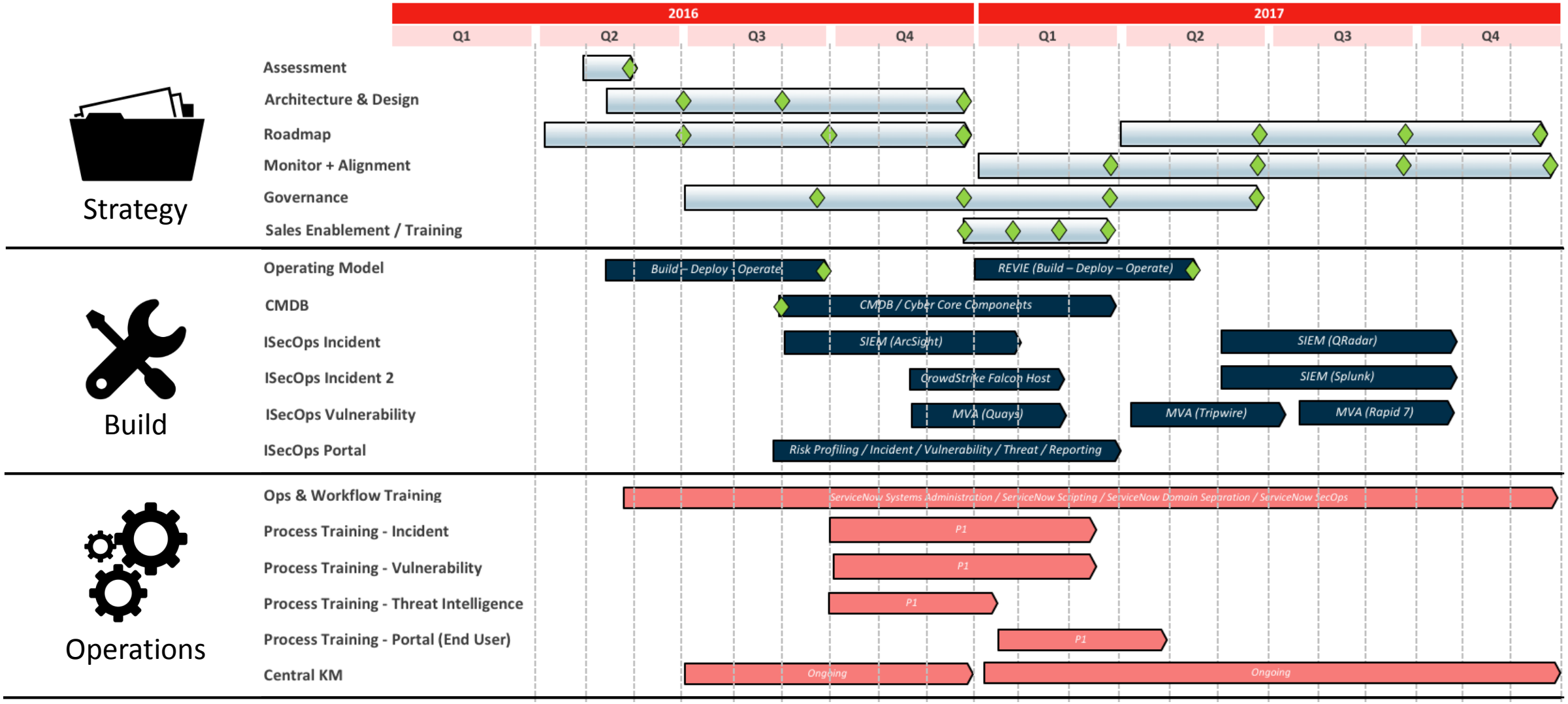
Cyber Security Controls Integration				Process and Services Integration			
SIEM Service Integration	MVA Service Integration	CTI Service Integration	CrowdStrike Integration	Vulnerability Management	Incident Management	Enterprise Security Roadmap	Digital Attack Simulation

ServiceNow SecOps Platform

Security Incident Management	Vulnerability Management	Threat Intelligence	Workflow	Automation & Orchestration	IT Integration

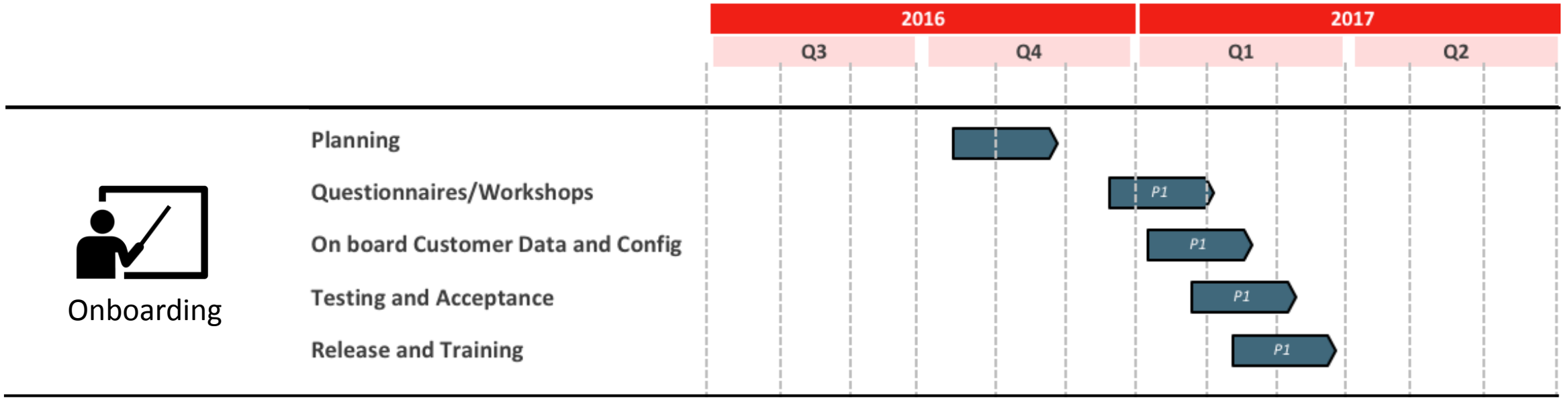
© 2017 ServiceNow All Rights Reserved

Our Development and Deployment Timeframe



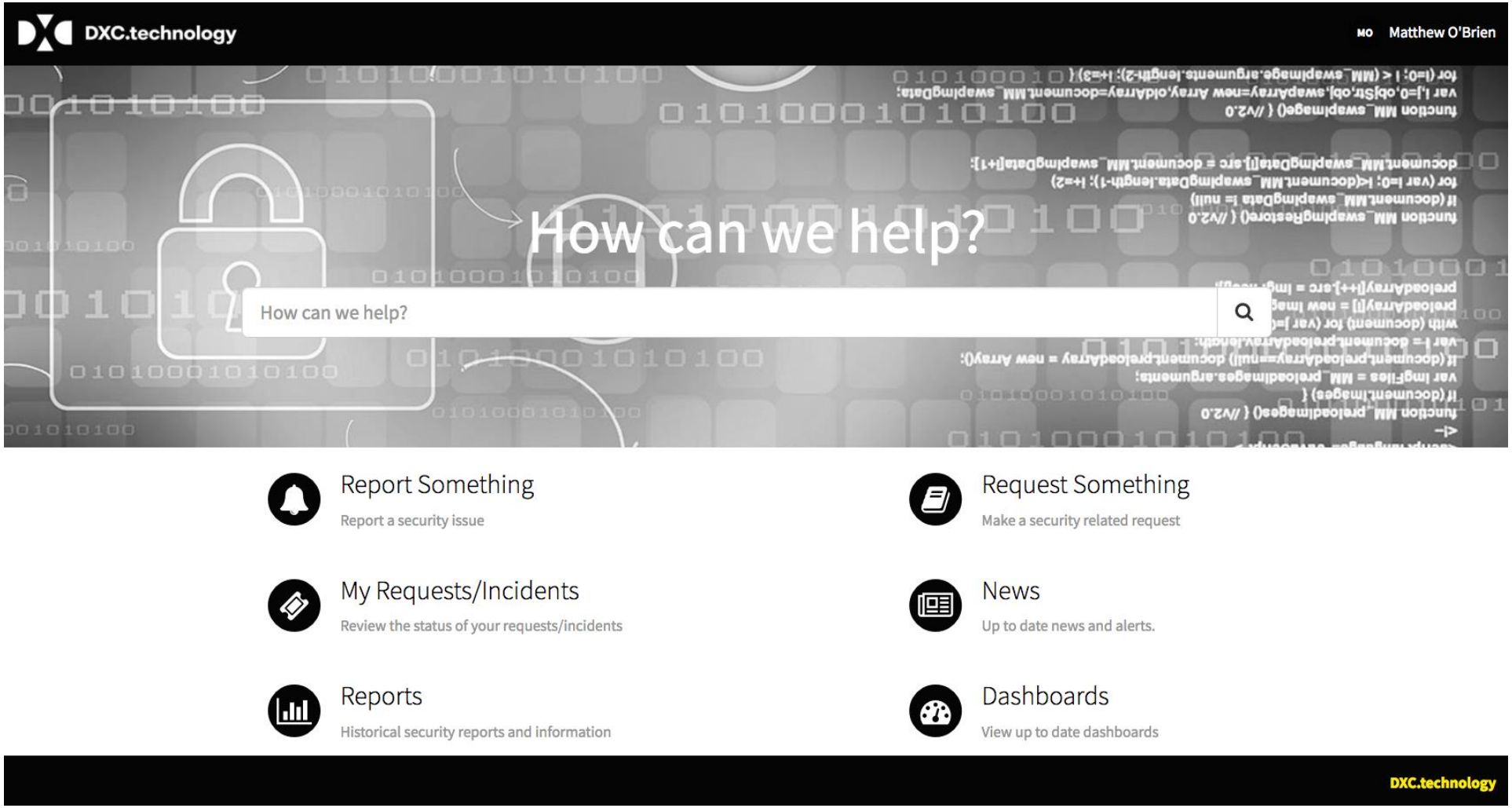
© 2017 ServiceNow All Rights Reserved

Our Enablement – 8 Week Implementation, Testing, and Training



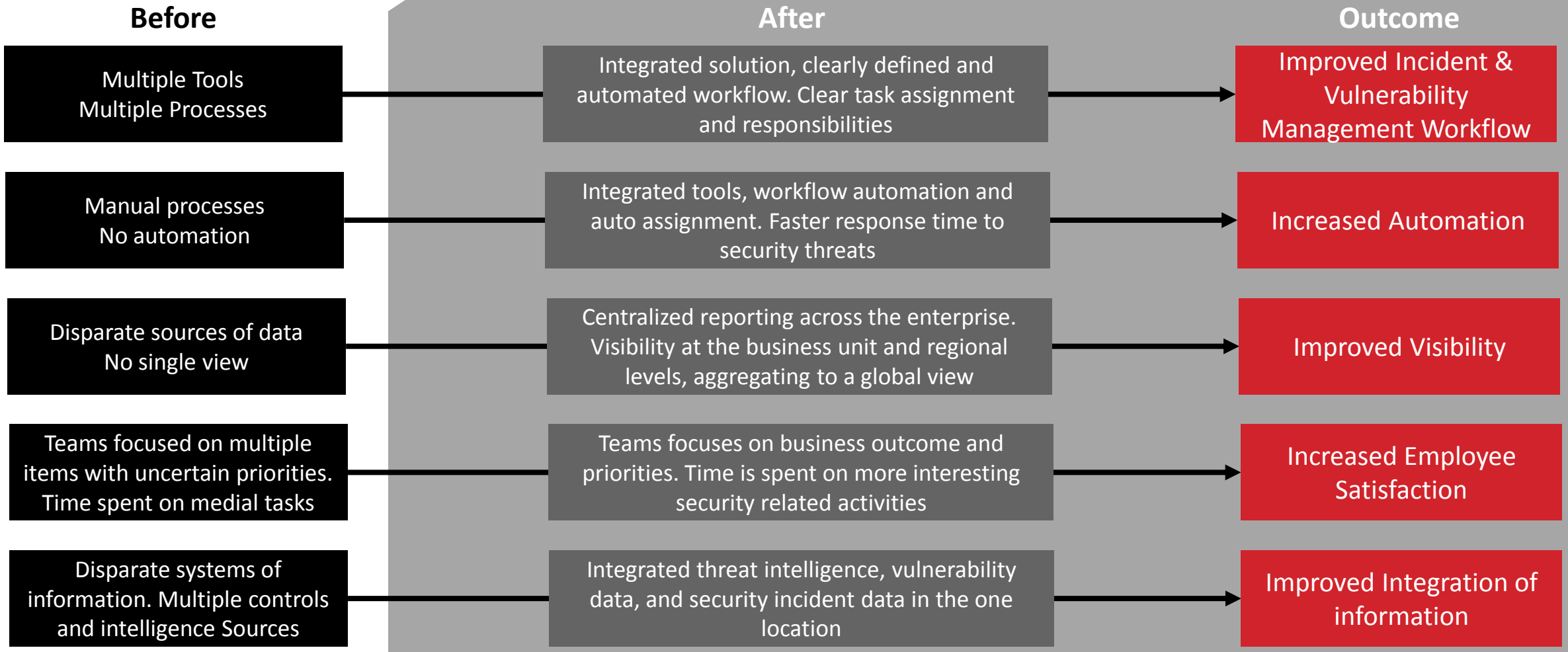
© 2017 ServiceNow All Rights Reserved

Solution – Demo



© 2017 ServiceNow All Rights Reserved

Value Outcomes



© 2017 ServiceNow All Rights Reserved

Value Outcomes

An increase of up to

50%

Process driven response

Shift from Manual to process driven response



Security Event Triage Time

5X

FASTER

In attributing indicators of compromise to security incidents

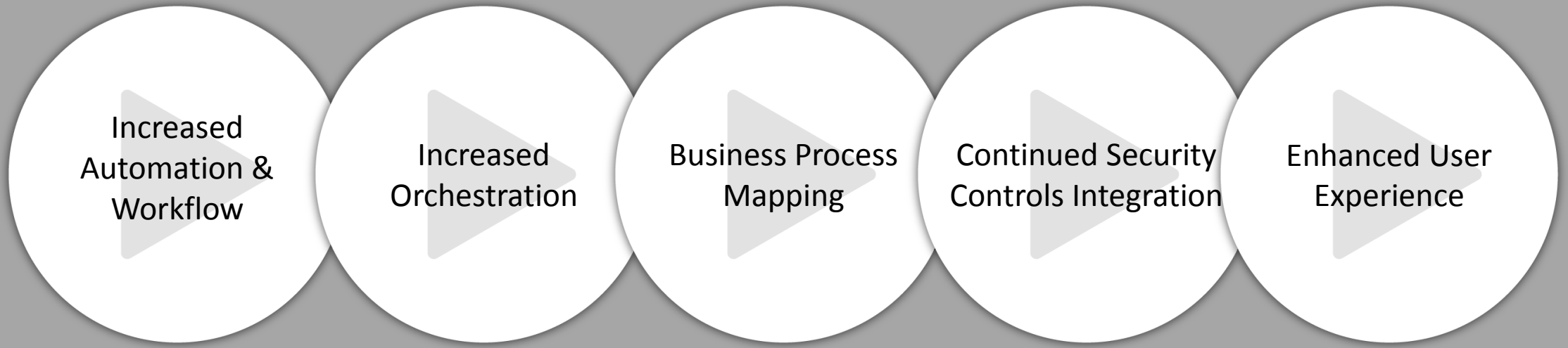
© 2017 ServiceNow All Rights Reserved

Lessons Learned

1. Don’t underestimate the support required by your security teams for controls integration and process mapping
2. Spend time on the user interface, the portal and the reporting and analytics. This is the face of your solution and where you’ll be judged
3. Review your existing processes before trying to map them into the platform. Mapping a bad, ineffective process just makes the bad process execute more quickly
4. Engage early and often with the operations teams, such as your SOC, Threat Intelligence and Forensics teams. Ensure everyone has the required time committed
5. Talk often to your key stakeholders throughout the development and integration processes. Show them what’s happing and leave no surprised for your go live date

© 2017 ServiceNow All Rights Reserved

Our Next Steps



© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Understand your environment

Be clear about what you want

2

Make it intuitive and make it easy

Usability is essential

3

Get security support for your integration

Capability can breed complexity

Plan, plan, plan, and then execute.

© 2017 ServiceNow All Rights Reserved

Thank You

MATTHEW O'BRIEN
SENIOR GLOBAL PRODUCT MANAGER, CYBERSECURITY
DXC.technology

@MatthewOBrienAU | #Know17

© 2017 ServiceNow All Rights Reserved

Q & A

MATTHEW O'BRIEN
SENIOR GLOBAL PRODUCT MANAGER, CYBERSECURITY
DXC.technology

© 2017 ServiceNow All Rights Reserved

Take the Survey

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

Thank You

Matthew O'Brien

Senior Global Product Manager, Cybersecurity

DXC.technology

© 2017 ServiceNow All Rights Reserved