knowledge17

WORK at LIGHTSPEED™

Tales from the Trenches: Converting Your Security Runbook into Security Operations Workflows

BRYCE G. SCHROEDER
SR. DIRECTOR, SECURITY & RISK PRACTICE
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Session Overview

Overview | Value | Truth & Fiction | The Journey | Always Improve



Objectives

- How to move your runbook into Security Operations



What You Will Learn

- ServiceNow Security Operations Overview
- Value of security workflow automation
- Truth or Fiction? Myths versus Reality
- How to start, beginning the journey
- Always Improving

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



NAME: Bryce Schroeder

TITLE: Sr. Director, Security and Risk Practice

FUNCTION: Security

COMPANY: ServiceNow

EXPERIENCE: 17 years Solutions & Systems Engineering, 10 years R&D/product management, 7 years IT

EXPERTISE: Systems & Security Architectures, solving problems

CURRENT PROJECTS: ServiceNow Security Operations & GRC

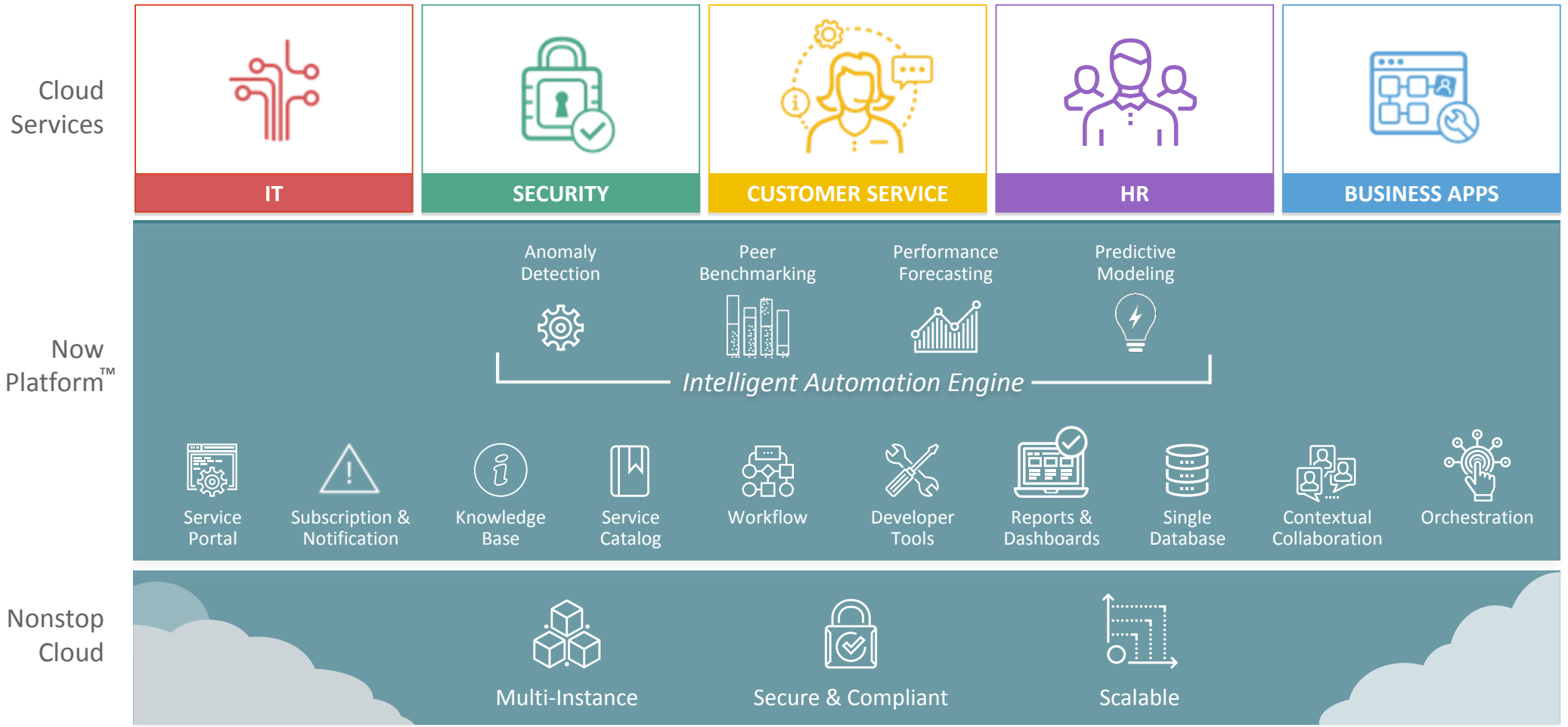
Tektronix® Sun microsystems Symantec. NetApp™ tripwire™ servicenow

Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

ServiceNow

ServiceNow System of Action™



© 2017 ServiceNow All Rights Reserved

Introducing Enterprise Security Response



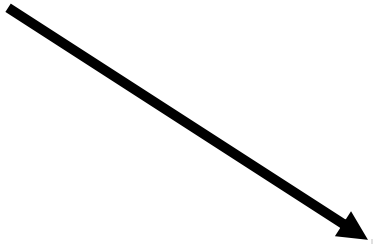
Security Incident Response

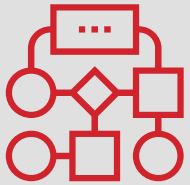


Vulnerability Response



Threat Intelligence





Workflow



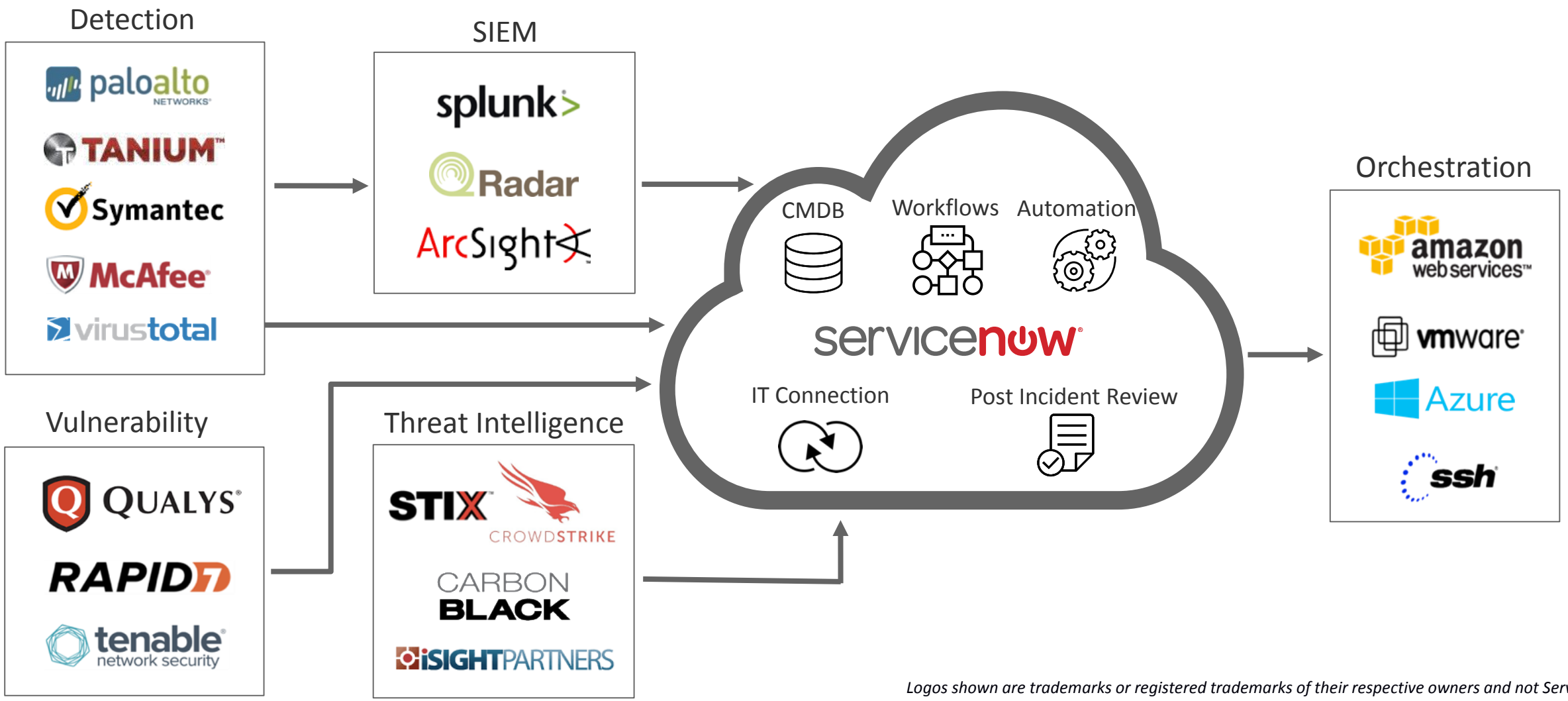
Automation & Orchestration



Deep IT Integration

© 2017 ServiceNow All Rights Reserved

Where Does Security Operations Fit?

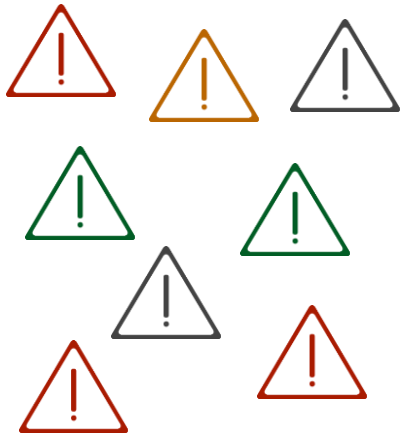


Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

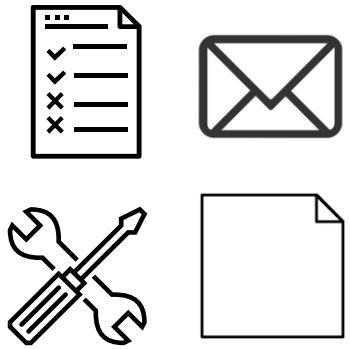
© 2017 ServiceNow All Rights Reserved

Security Teams are Overwhelmed

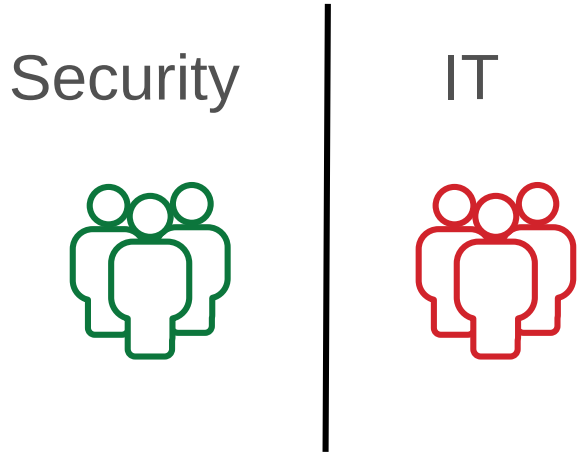
Too Many Alerts & No Context



Manual Tools



Siloed from IT



© 2017 ServiceNow All Rights Reserved

ServiceNow Security Operations Automation Value

servicenow securityoperations



FIND AND PRIORITIZE CRITICAL THREATS

Business context and threat intelligence enrichment

REDUCE MANUAL TASKS

Automate investigations; orchestrate tools

DEFINITIVE VIEW OF SECURITY POSTURE

Metrics, service levels, and dashboards

dashboards

© 2017 ServiceNow All Rights Reserved

TRADITIONAL SECURITY INCIDENT RESPONSE

- ✗ Multiple disparate security data sources
- ✗ Hard to trace communication via email
- ✗ Data in spreadsheets and multiple databases
- ✗ Long ramp times for new team members
- ✗ Inconsistent security incident response
- ✗ Lack of visibility across security team to KPIs, trends & Incidents in process

SERVICENOW SECURITY OPERATIONS

- ✓ Unified platform with structured, task based, security incident process flow
- ✓ Consistent Business Criticality between IT & Security to IT
- ✓ Single “source of truth” for Incidents, Assets, Problems and Changes.
- ✓ Analyst time spend on Security Incident diagnosis, rather than mundane data gathering
- ✓ Rapidly evolve & improve Security Incident response process with workflow
- ✓ Full visibility of KPIs, Trends & Incidents

© 2017 ServiceNow All Rights Reserved

With Security Operations, You Can Automatically…

- Prioritize based on the business criticality of the asset
- Correlate threat intelligence data
- Request enrichment/enhancement from additional security tools
- Assign tasks to the right people
- Apply emergency patches
- Remediate incidents
- Create post-incident reviews
- Set SLAs & escalations
- More…



© 2017 ServiceNow All Rights Reserved

ServiceNow Security Operations Automation Value

servicenow securityoperations



FIND AND PRIORITIZE CRITICAL THREATS

Business context and threat intelligence enrichment

REDUCE MANUAL TASKS

Automate investigations; orchestrate tools

DEFINITIVE VIEW OF SECURITY POSTURE

Metrics, service levels, and dashboards

dashboards

© 2017 ServiceNow All Rights Reserved

Truth or Fiction

Security and Risk Automation

All “runbooks” must be defined before automating response

Automate response?

Our team, tools and processes are “GOOD ENOUGH”

Automation is too hard, we are a security team not workflow automation experts

Automation will make my security team into droids & robots

Workflow and Automation will solve everything

This is just a passing fad…

© 2017 ServiceNow All Rights Reserved

Resolve Real Security Threats Fast

	MODERNIZE	TRANSFORM	INNOVATE
MINDSET			
CONSUMERS	Security Analysts	CISO, IT, Security Organization	Security Operations
PHASE	UNIFY RESPONSE	BUSINESS INTEGRATION	INTELLIGENT AUTOMATION
CAPABILITIES	Security Incidents; Vulnerability Management; Reporting & Dashboards	Business Prioritization; Risk & Impact Awareness; Threat Intelligence; Int. with Incident, Problem & Change	Trusted Security Circles; Automated Remediation; Security Biz Apps
BUSINESS VALUE	Faster Security Response *(quick & prioritized response)*	Improved Situational Awareness *(full organization)*	Intelligent Enterprise Protection *(customized intelligent automation)*
BUSINESS OUTCOMES	Reduced time to resolve incidents Less time spent on manual tasks Efficient resolution of security incidents Automation of basic manual tasks (e.g. assignment, post-incident review) Reduced backlog of security incidents & vulnerabilities Consistent process with baseline performance metrics	Reduced risk through improved visibility Data-driven business decisions Business-critical prioritization Reduction of business risk through visibility into critical services Efficient collaboration with IT Reduced time spent on enrichment tasks through automation & threat intelligence Comprehensive view of security posture	"Community-Aware Security" End-to-end automation Reduced risk via industry-specific threat intelligence Freed up resources for value-add decisions Reduced decision-making time Fully automated remediation based on security decisions Compressed E2E time to remediate Proactive and Predictive visibility of Threats

© 2017 ServiceNow All Rights Reserved

Security Operations Maturity Levels



A large percentage of organizations are working at Level 1

1 – Basic Operations

Basic Incident Ticketing,

Incident Response Definition

Integration with core security systems

Process and Accountability Defined

2 – Visibility and Performance

Value-based Prioritization,

Visibility and Reporting

Prioritization by Impact

KPIs, Reporting and SLAs

Noise Reduction

3 - Context and Enrichment

Enhanced data enrichment tied to incidents

Context-driven detection

Automate data gathering tasks

Threat intelligence integrated with IR

Time to Detect per event reduced

4 - Automated Remediation

Automated Response Actions for Proactive

Measures and Countermeasures

Integrated Change Request and History

Compress the time to contain and remediate incidents

Enable visibility for changes and task fulfillment across teams

Easily handle common attacks to improve response closure

5 – Real-Time Risk Visualization

Circles of Trust for Peer Intel Sharing

Dynamic Workflow to Educate and Enable SOC Teams

Security Information Network for intel and attack method updates

Automated querying of internal and supplier environments

Educational expert systems and best practice sharing

ENHANCED TIME TO DETECT AND RESPOND

SECURITY OPERATIONS MATURITY

© 2017 ServiceNow All Rights Reserved

Customer Journey with Security Operations

Built on the ServiceNow Platform



© 2017 ServiceNow All Rights Reserved

UNIFY RESPONSE

Step 1

INVENTORY



- ✓ Authorized devices and software
- ✓ Services needing protection
- ✓ Security sensors
- ✓ Enforcement technologies
- ✓ Response playbooks

Step 2

CONNECT



- ✓ Security alert sources
- ✓ Vulnerability scanners
- ✓ Email distributions & notifications
- ✓ Asset discovery

BUSINESS INTEGRATION

Step 3

CONFIGURE



- ✓ Security Incident & Vulnerability workflows
- ✓ SLAs, dashboards & reports
- ✓ Threat intelligence sources
- ✓ Business criticality & risk calculators
- ✓ Role based access

Step 4

LAUNCH



- ✓ Automated security incident response
- ✓ Automated vulnerability response
- ✓ Threat intelligence collection
- ✓ Security request catalog

INTELLIGENT AUTOMATION

Step 5

MEASURE



- ✓ MTT: Identify, contain, eradicate, review & respond
- ✓ Vulnerability aging
- ✓ Attack trends
- ✓ Response trends
- ✓ Vendor effectiveness
- ✓ Automation ROI

Step 6

REFINE



- ✓ Further automate response tasks
- ✓ Enrichment sources & methods
- ✓ Personalized apps for Security & Risk Management
- ✓ Data-driven strategic planning

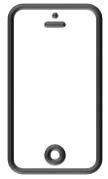
© 2017 ServiceNow All Rights Reserved

Step 1

Inventory



Customer Journey to Security Operations:
Step 1 : Inventory



Authorized devices and software



Services Needing Protection



Security Sensors



Enforcement Technologies



Response Playbooks

© 2017 ServiceNow All Rights Reserved

Step 2

Customer Journey to Security Operations:
Step 2 : Connect

Connect





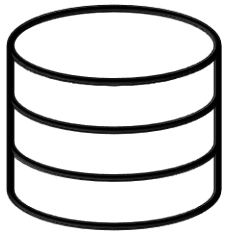
Security Alert Sources



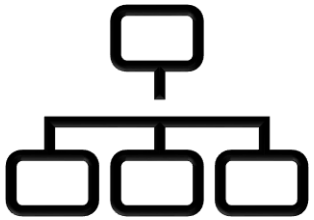
Vulnerability scanners



Email Distribution
&
Notification



Asset Discovery/CMDB



Service Map

© 2017 ServiceNow All Rights Reserved

Step 3

Customer Journey to Security Operations:
Step 3 : Configure

Configure





Vulnerability Response workflows



Security Incident Response workflows



SLAs



MTTI
MTTR
MTTE



Time Based Escalation



Backlog & trend
Incidents
Vulnerabilities

Existing Incident Flows

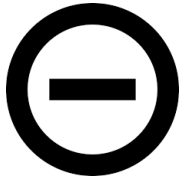




















© 2017 ServiceNow All Rights Reserved

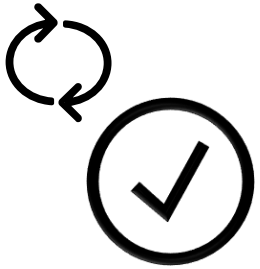
Step 4

Launch

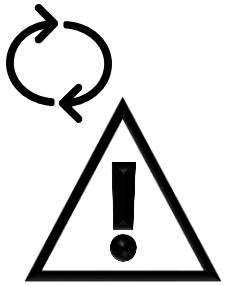
Customer Journey to Security Operations:
Step 4 : Launch



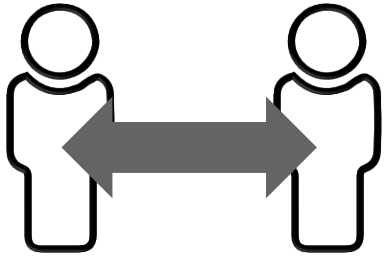
Runbook Automation



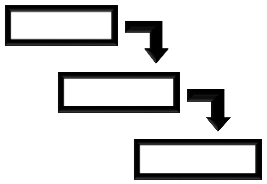
Approval workflows



Incident Creation



Security / IT Communication Remediation



Remediation workflow



Prioritization & Exceptions



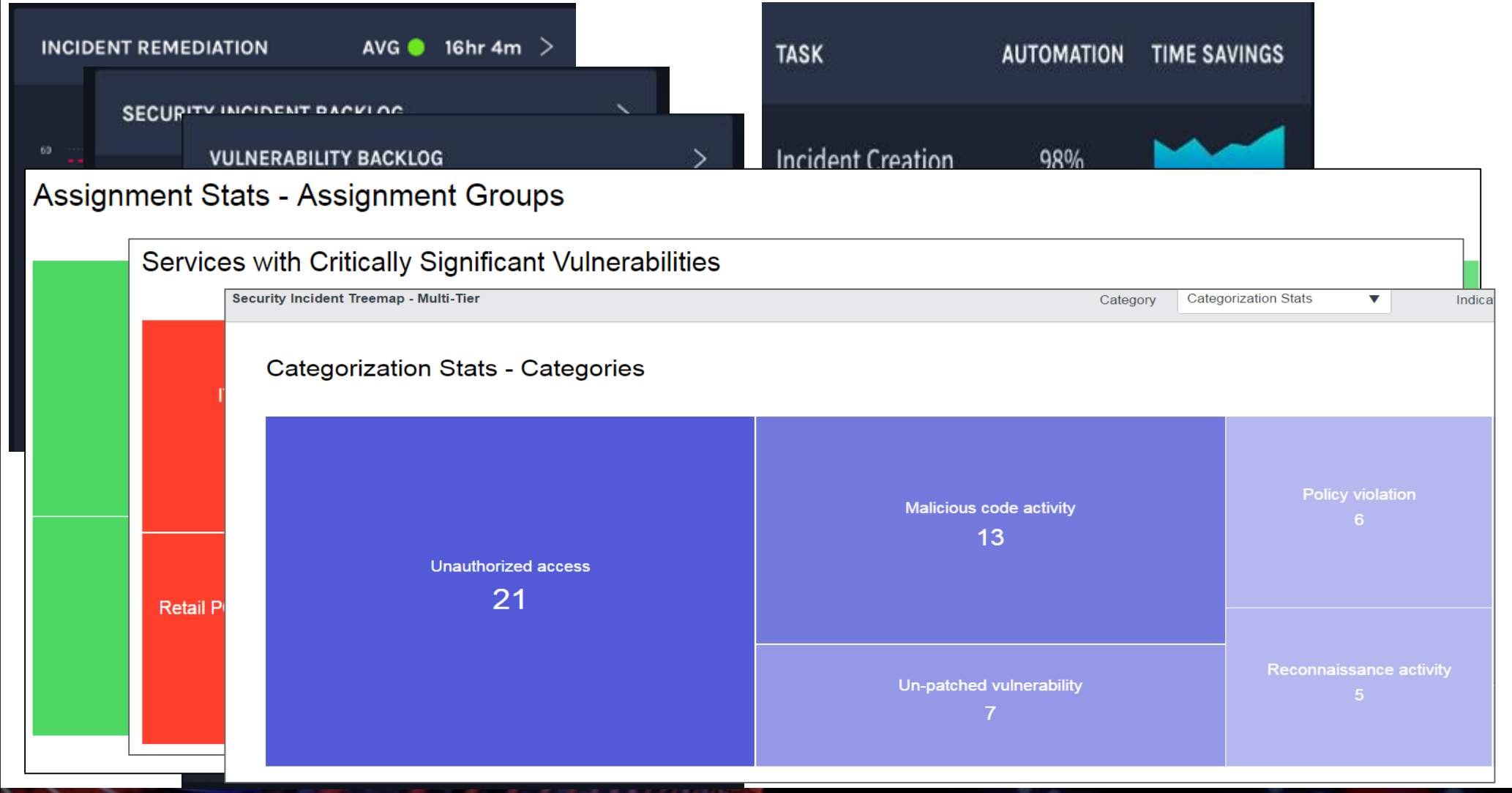
Threat Intelligence Feeds

© 2017 ServiceNow All Rights Reserved

Step 5

Customer Journey to Security Operations:
Step 5 : Measure

Measure



© 2017 ServiceNow All Rights Reserved

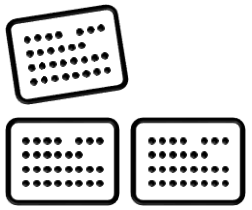
Step 6

Refine

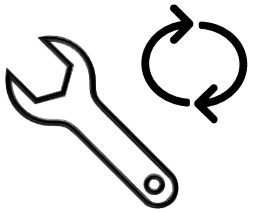
Customer Journey to Security Operations:
Step 6 : Refine



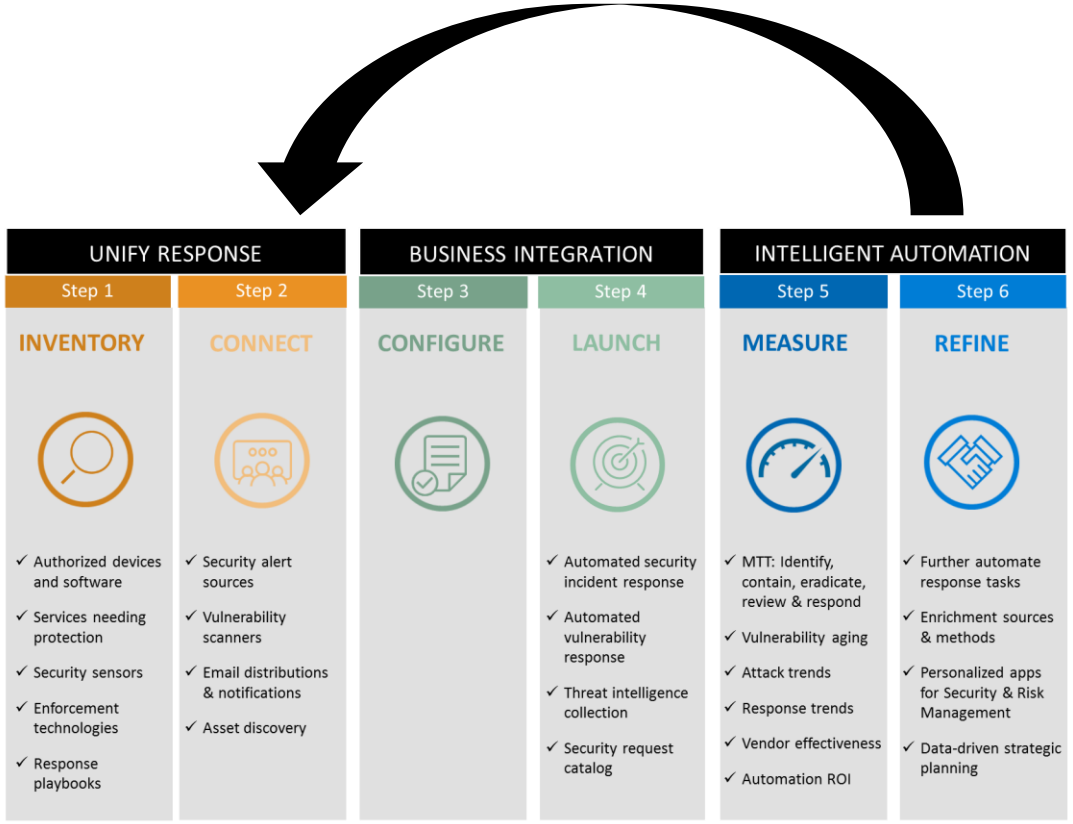
Threat Hunting



Custom Security Apps

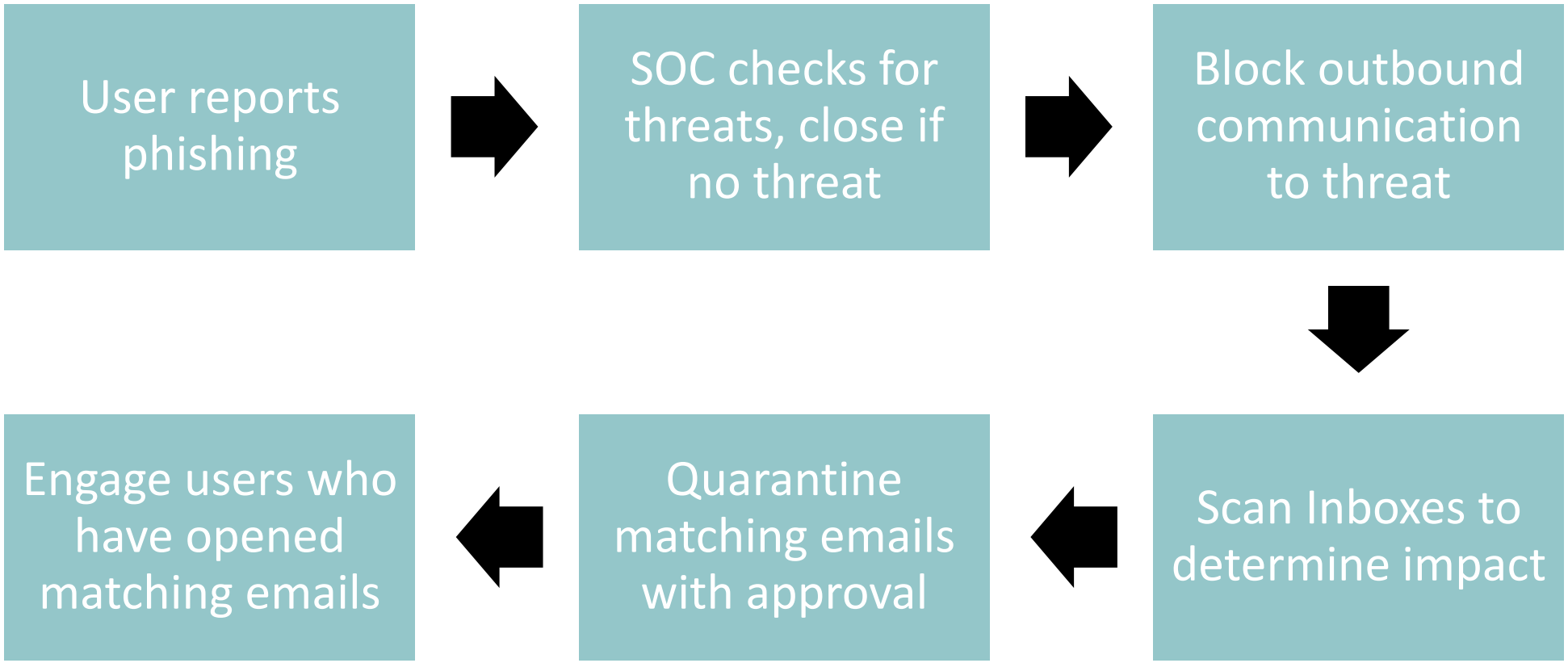


Refine & Further Automation



© 2017 ServiceNow All Rights Reserved

Security Ops Use Case: Phishing with Large Financial Institution



© 2017 ServiceNow All Rights Reserved

Security Technology Partners





























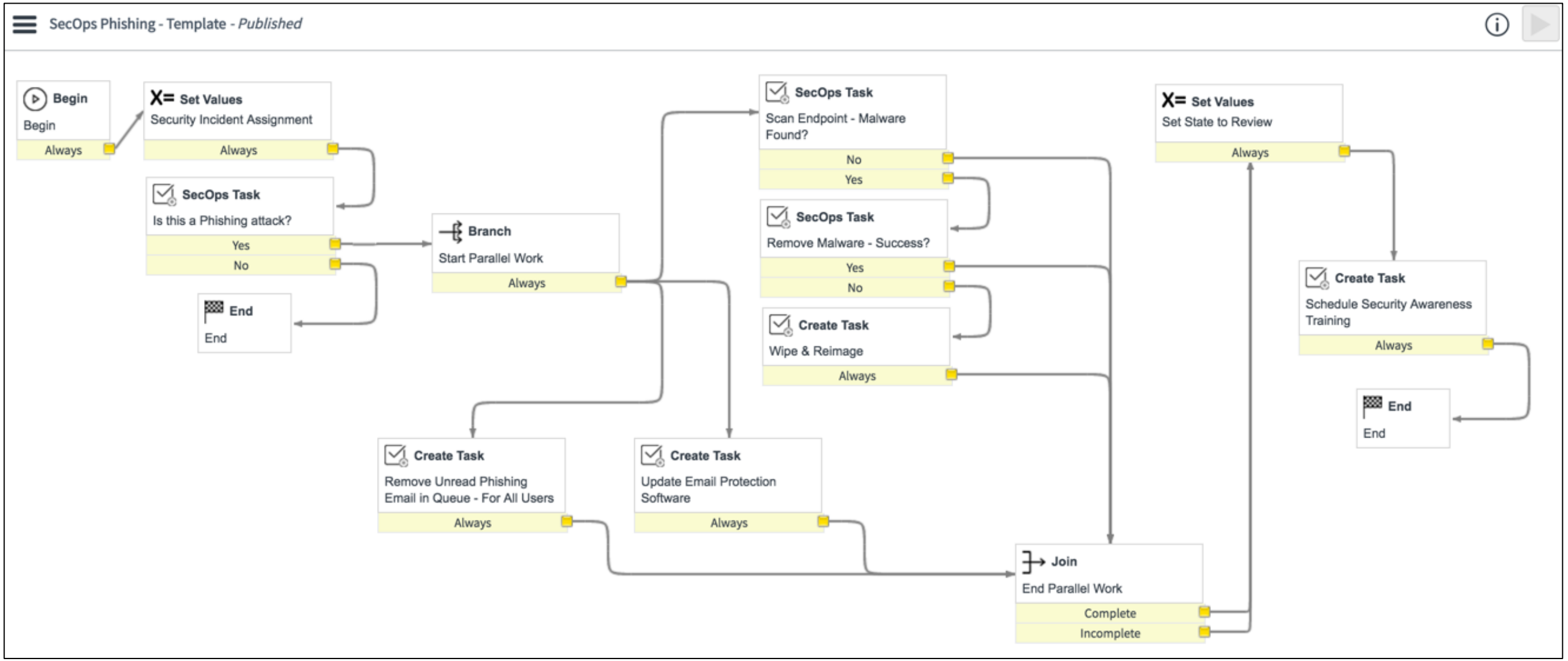


Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

Demo Segment

Phishing



© 2017 ServiceNow All Rights Reserved

Other ways to get there

- ServiceNow Professional Services
- Certified Security Services partner
- Security Integration Training
- More

© 2017 ServiceNow All Rights Reserved

Learn More About Security at ServiceNow

- Security Automation That Won't Get You Fired
- Tales from the Trenches: Converting Your Security Runbook into Security Operations Workflows
- Security Keynote
- Threat Intelligence Sharing: How Participation Will Dramatically Improve Your Security Posture
- What's New in Security Operations in Jakarta and What's Coming Next

© 2017 ServiceNow All Rights Reserved

ServiceNow Security Operations Automation Value

servicenow securityoperations



FIND AND PRIORITIZE CRITICAL THREATS

Business context and threat intelligence enrichment

REDUCE MANUAL TASKS

Automate investigations; orchestrate tools

DEFINITIVE VIEW OF SECURITY POSTURE

Metrics, service levels, and dashboards

dashboards

© 2017 ServiceNow All Rights Reserved

Thank You

BRYCE G. SCHROEDER
SR. DIRECTOR, SECURITY & RISK PRACTICE
ServiceNow
Bryce.Schroeder@ServiceNow.com

© 2017 ServiceNow All Rights Reserved

Take the Survey

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

Thank You

Bryce G. Schroeder

Sr. Director, Security & Risk Practice

ServiceNow

Bryce.Schroeder@ServiceNow.com

© 2017 ServiceNow All Rights Reserved

The Journey – How To Begin

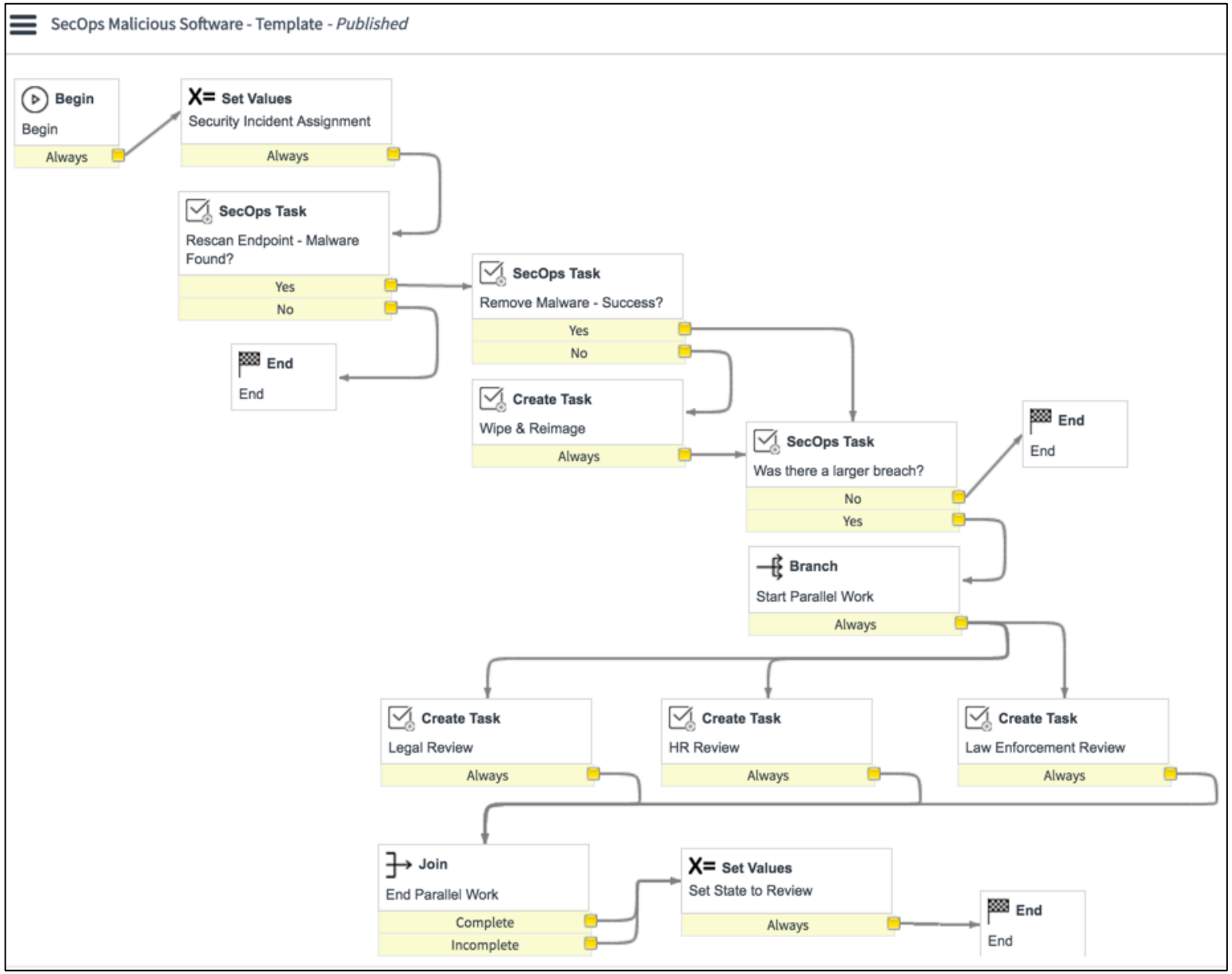
"Perfection Is The Enemy Of Progress"

- Pragmatic "KISS"
- Break into phases
- Focus on Business Outcomes
- Follow a methodology:
  - Choose security data source
  - Create (or modify existing) workflow to automate outcome
  - Measure and Visualize
  - Repeat



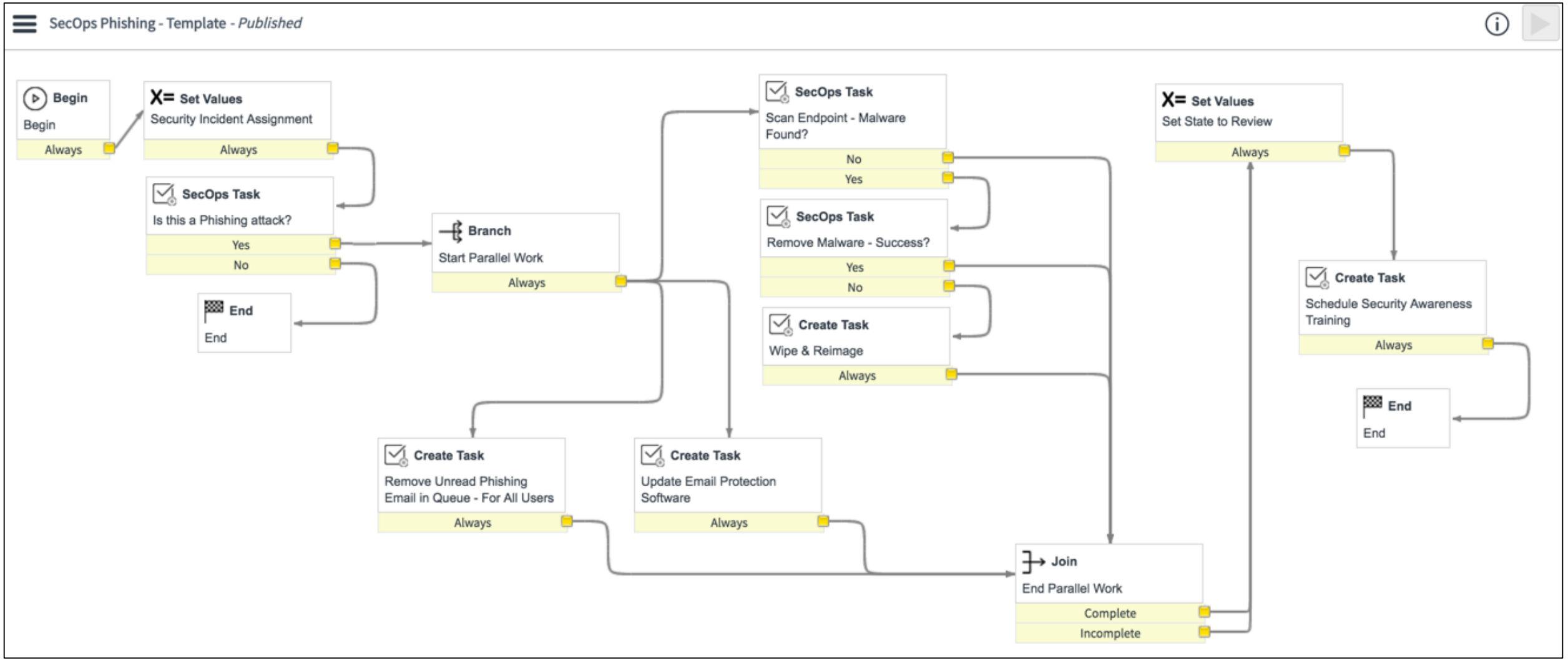
© 2017 ServiceNow All Rights Reserved

Malicious Software



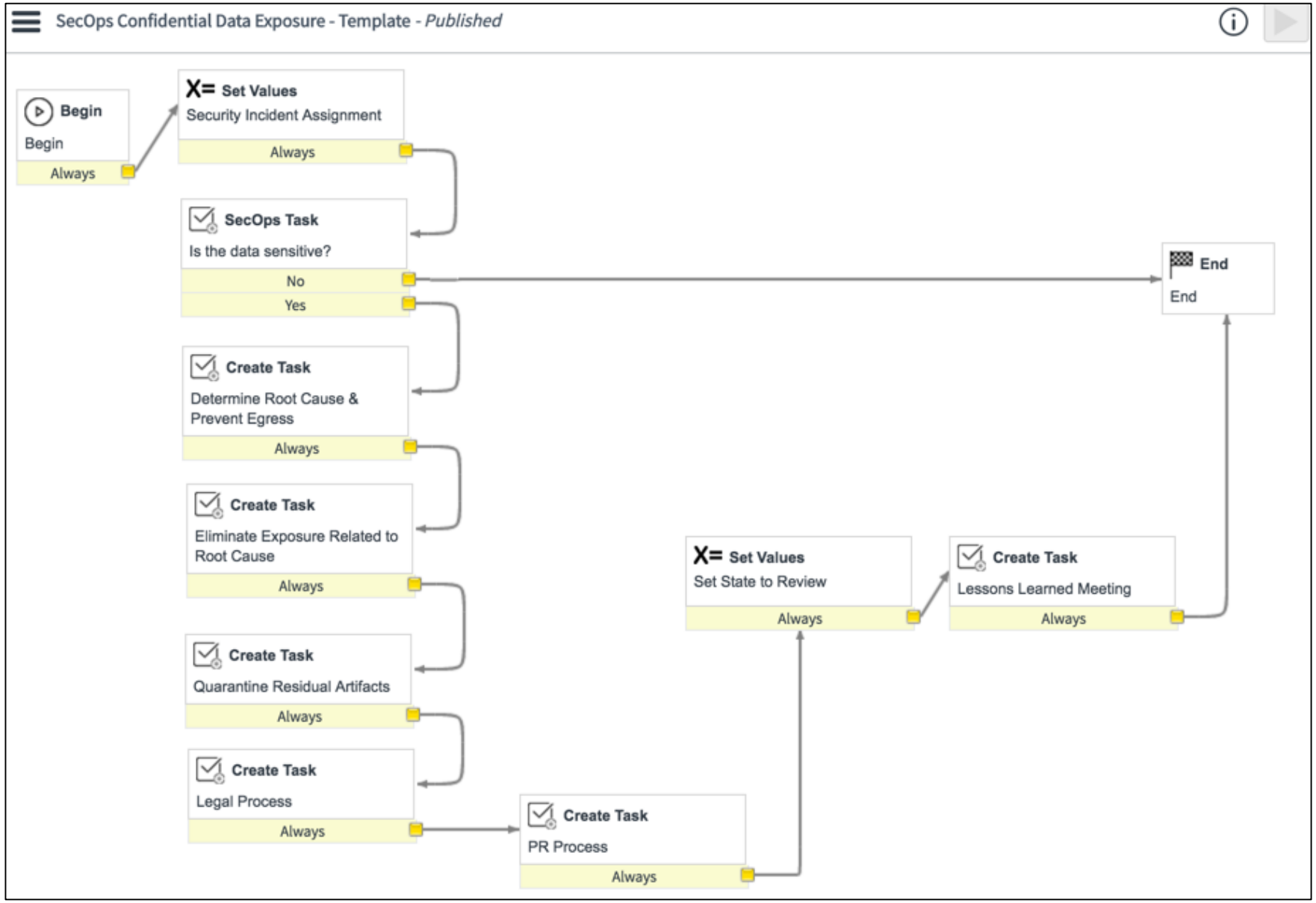
© 2017 ServiceNow All Rights Reserved

Phishing



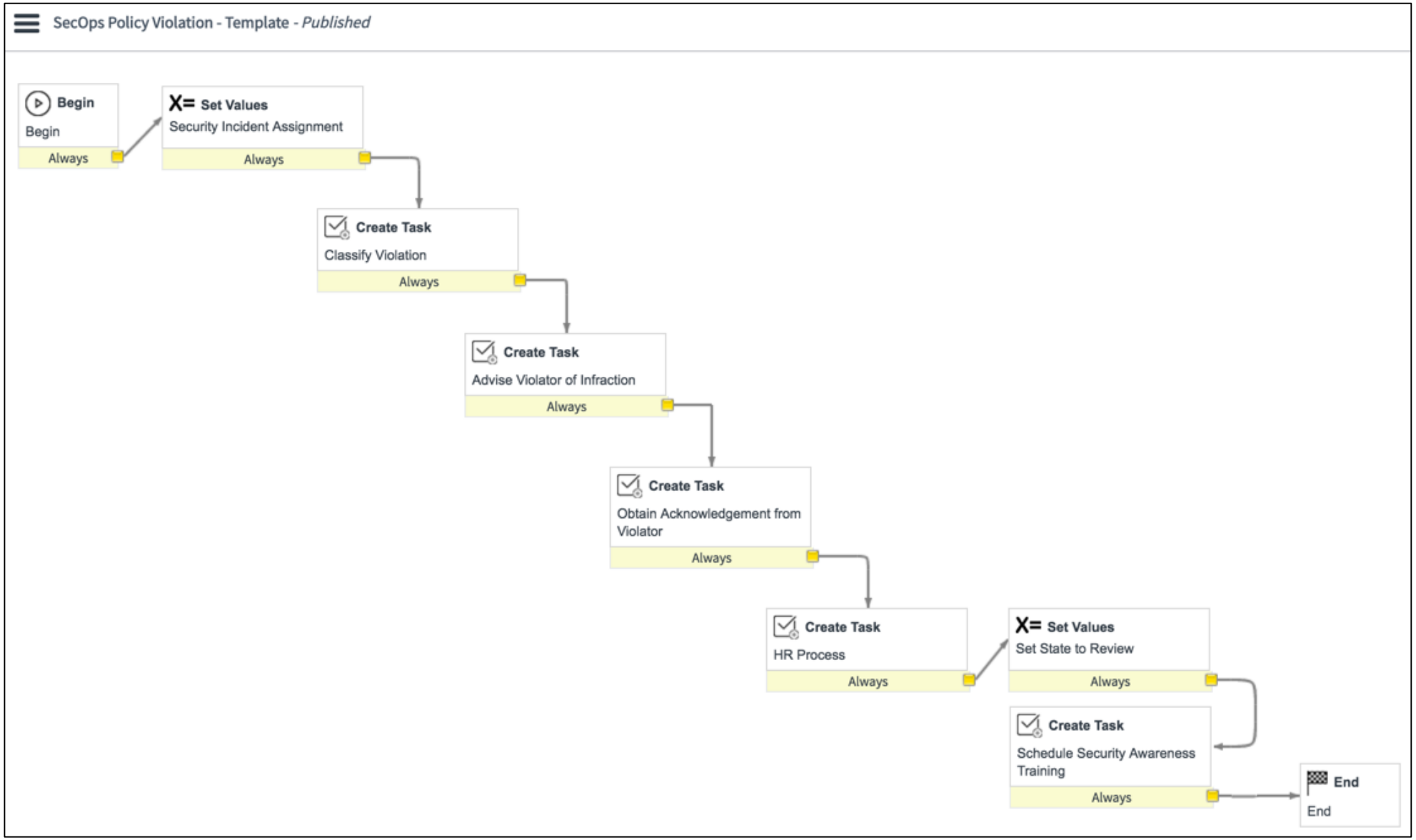
© 2017 ServiceNow All Rights Reserved

Confidential Data Exposure



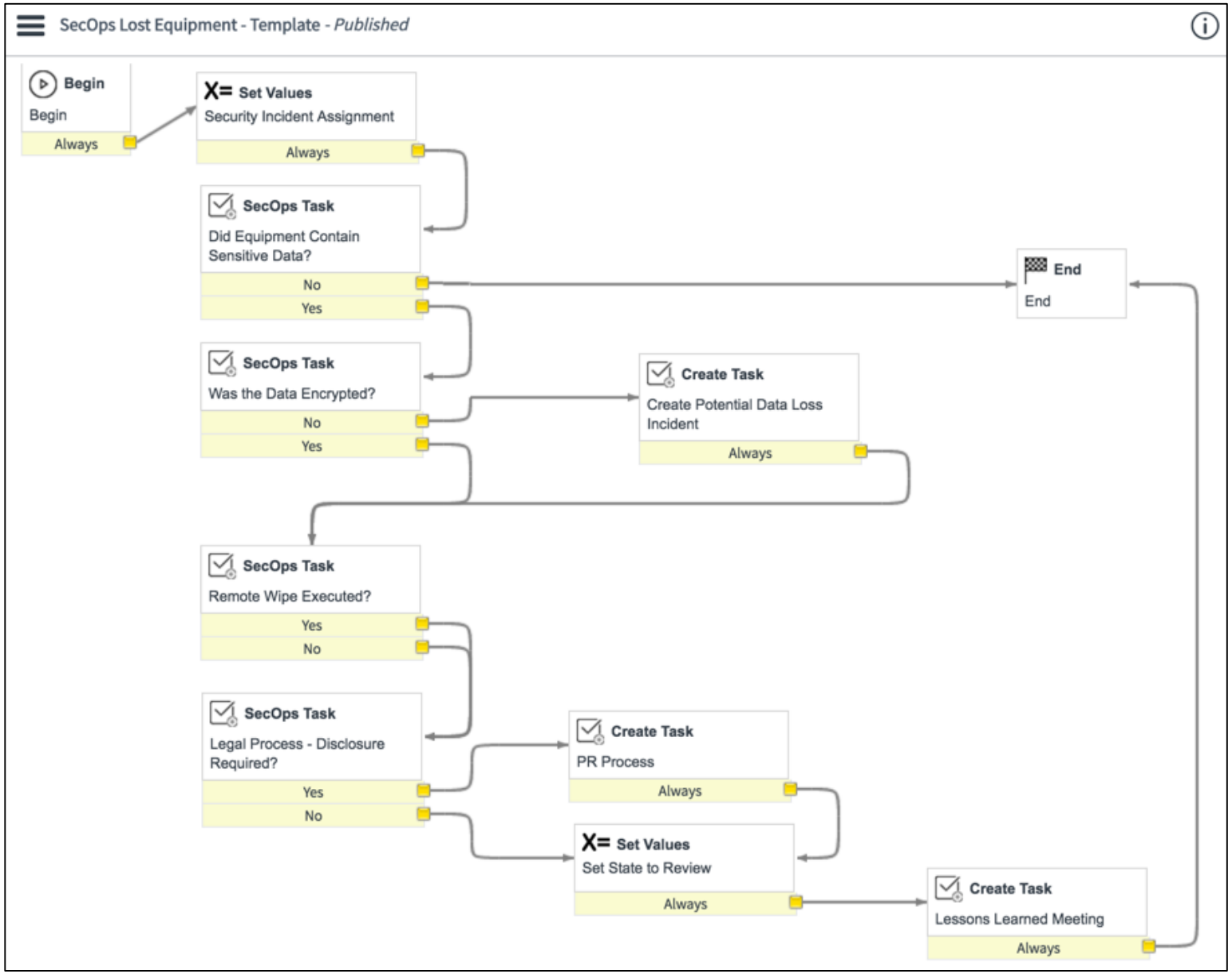
© 2017 ServiceNow All Rights Reserved

Policy Violation



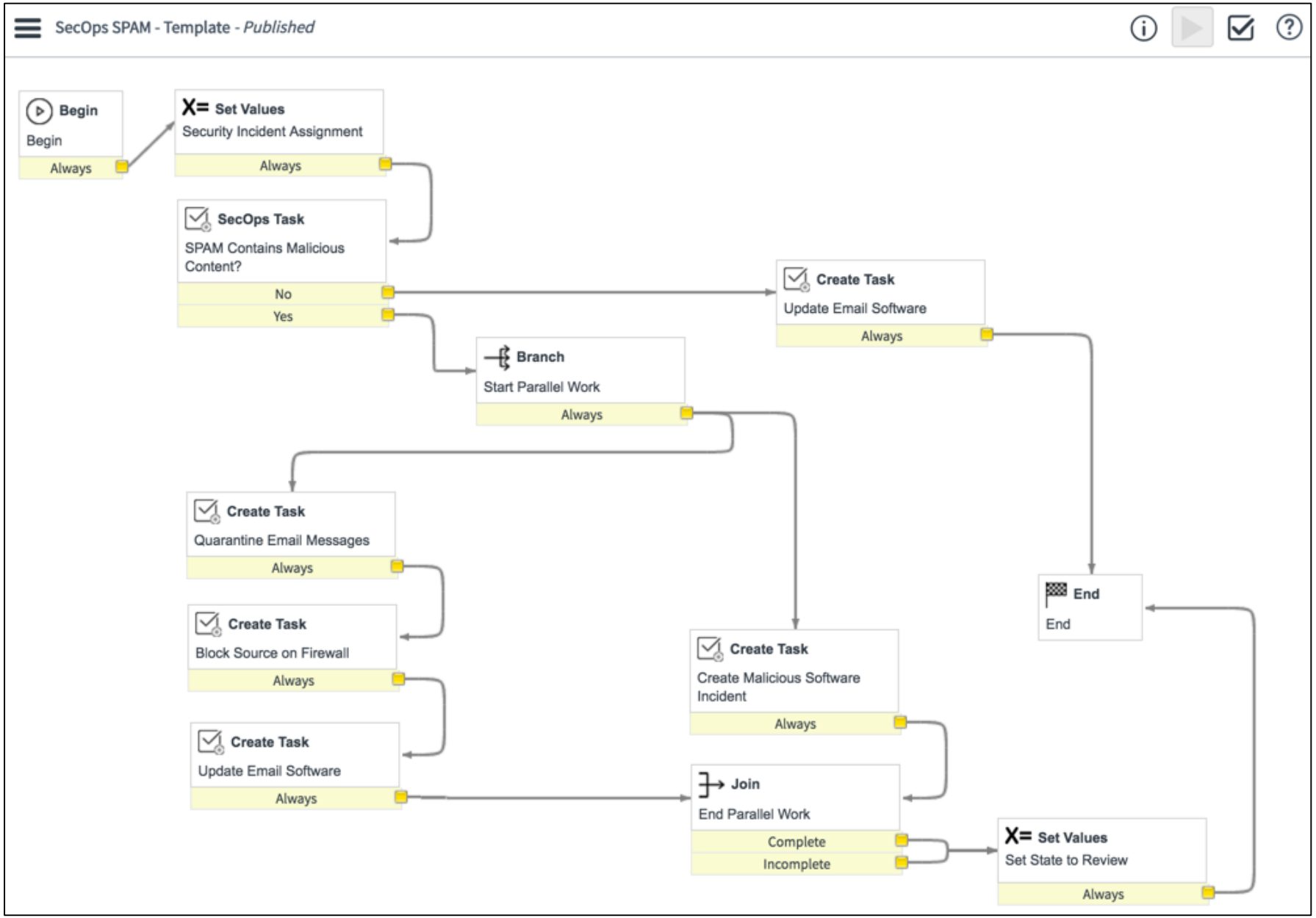
© 2017 ServiceNow All Rights Reserved

Lost Equipment



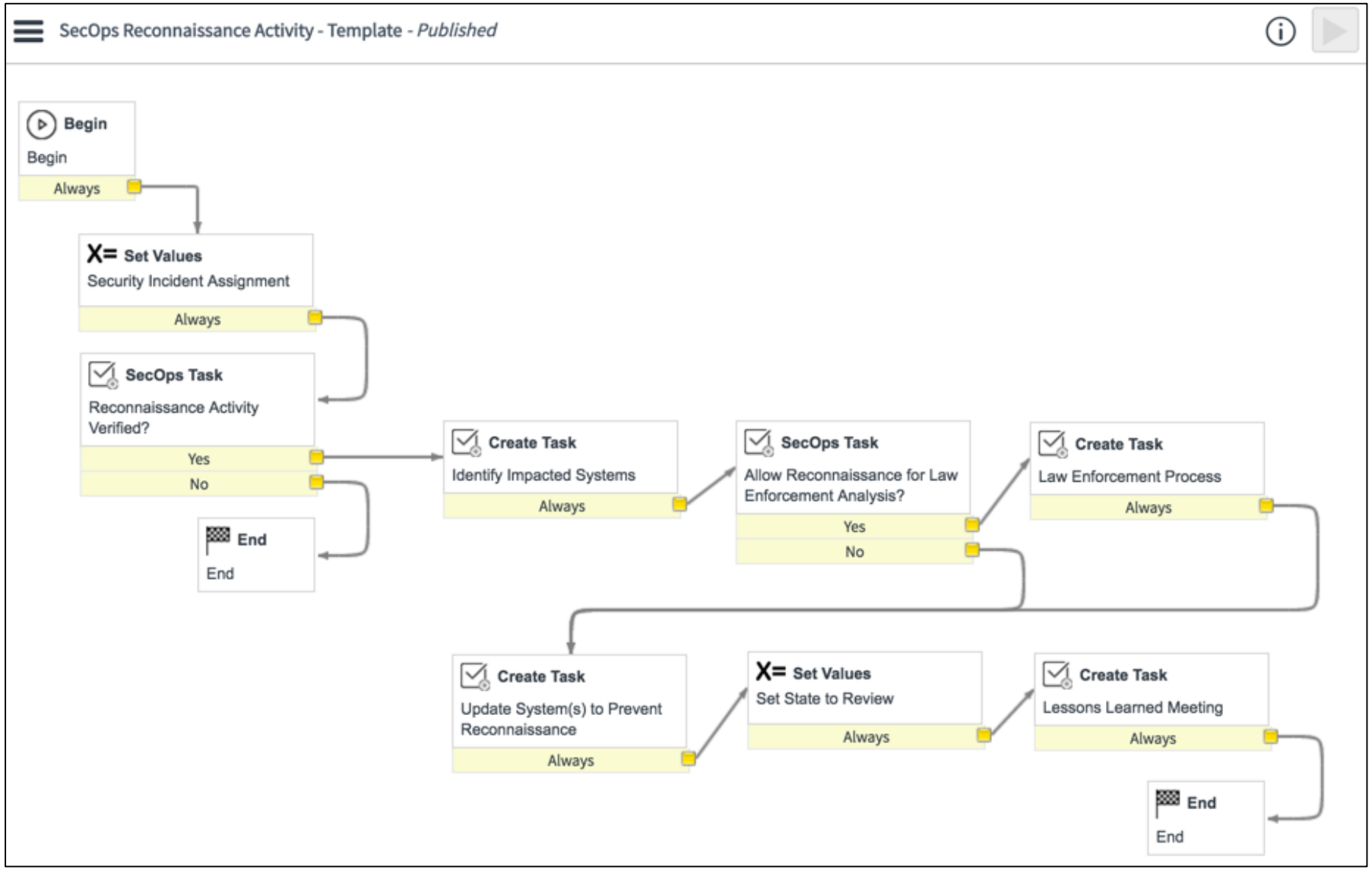
© 2017 ServiceNow All Rights Reserved

SPAM



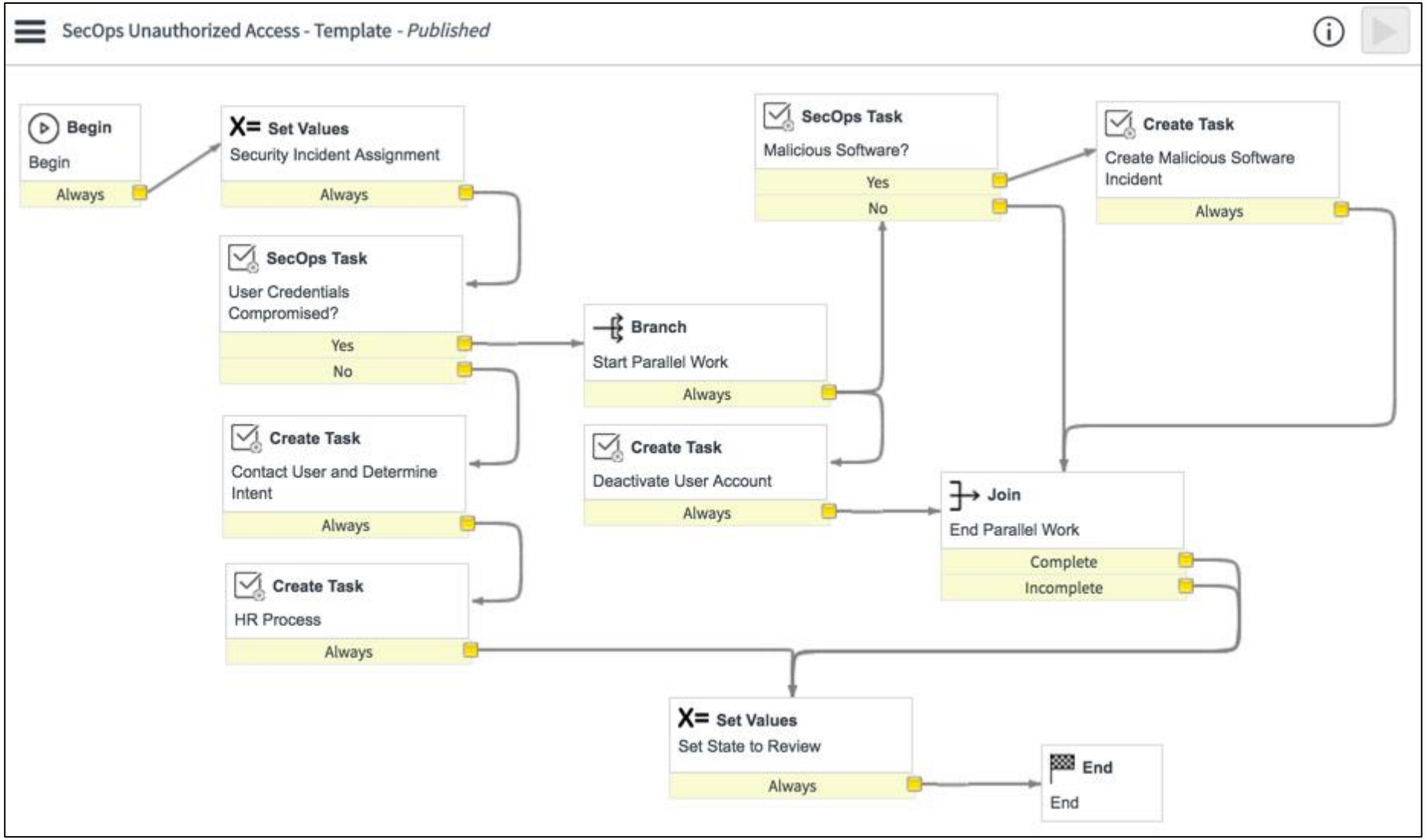
© 2017 ServiceNow All Rights Reserved

Reconnaissance Activity



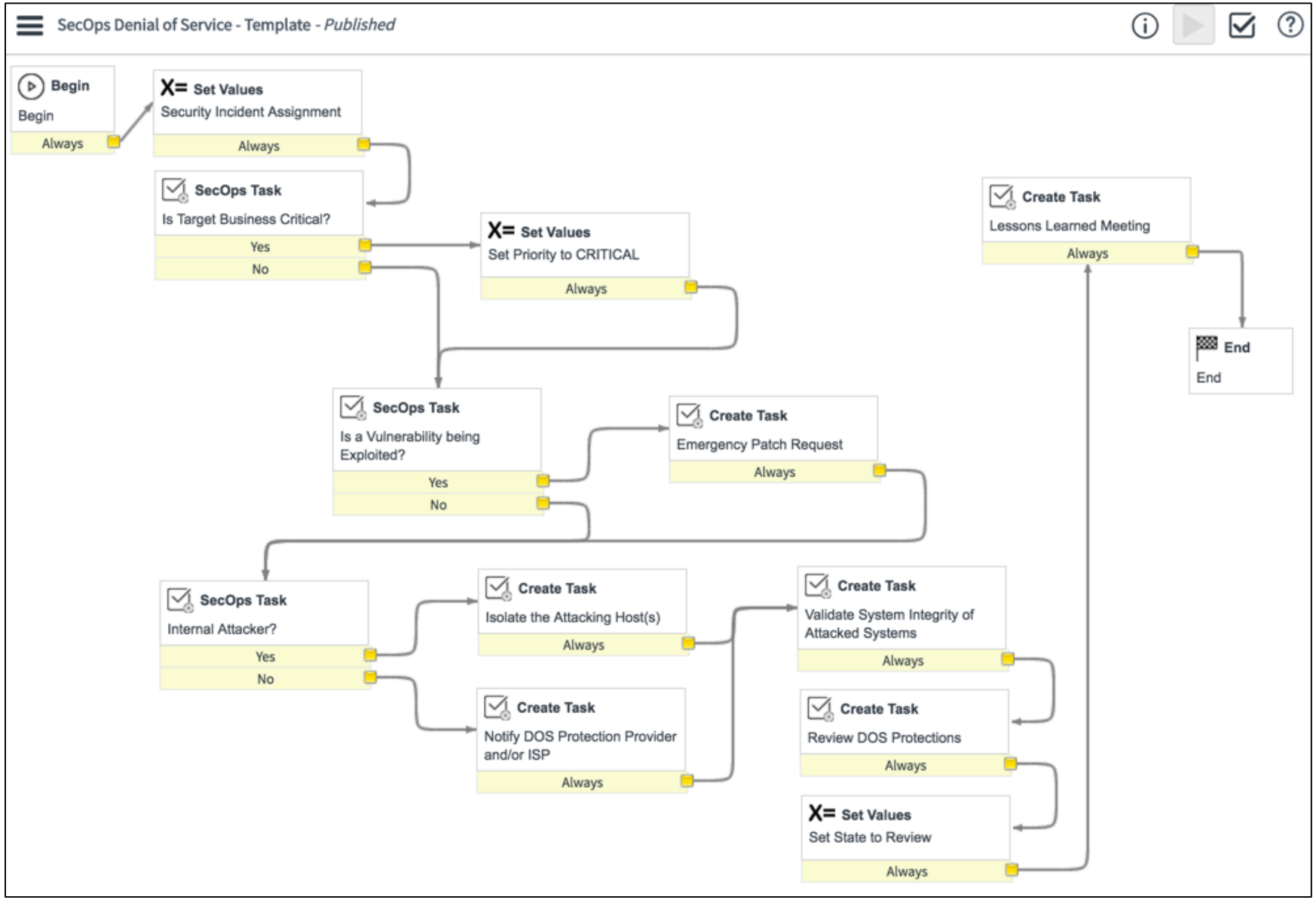
© 2017 ServiceNow All Rights Reserved

Unauthorized Access



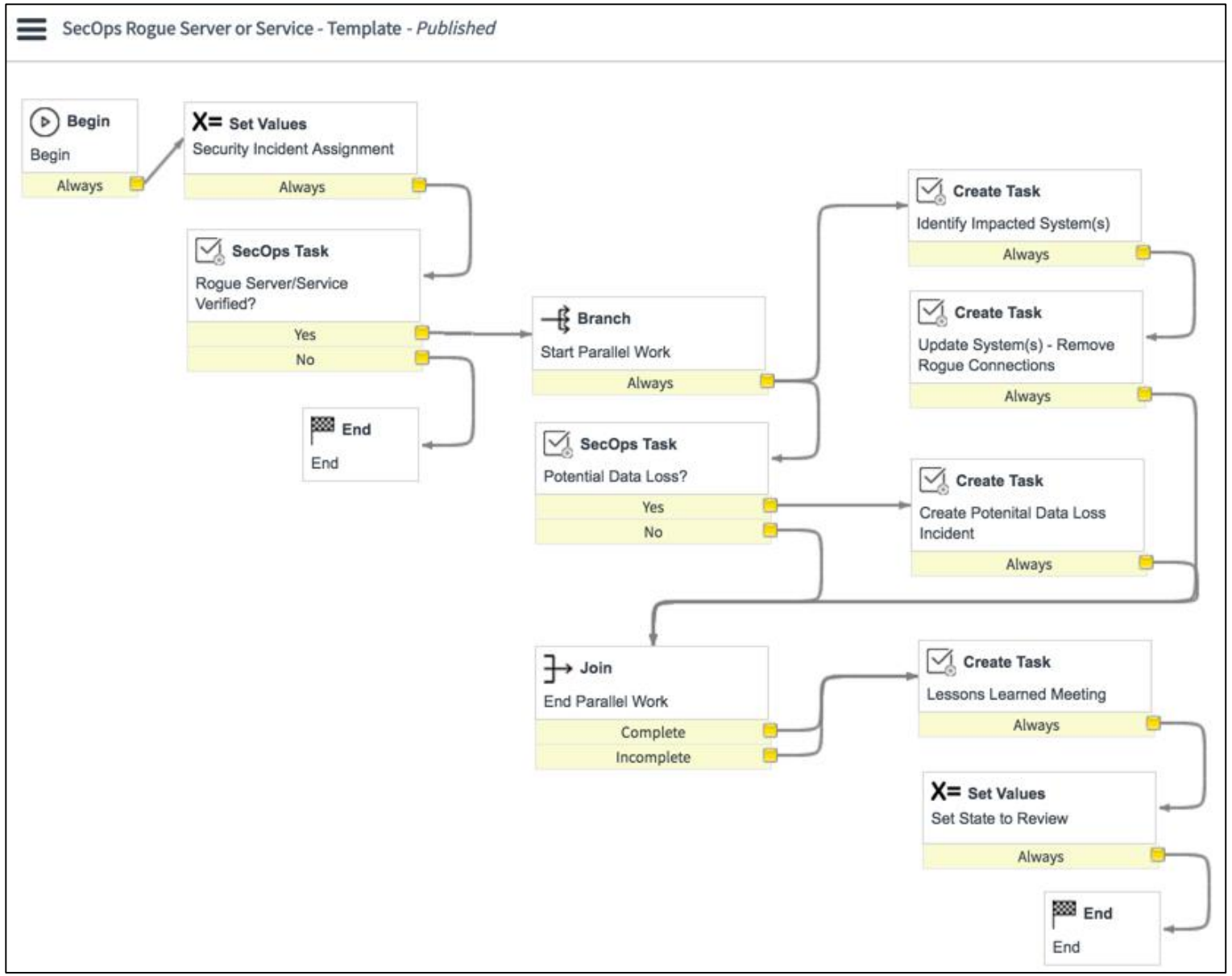
© 2017 ServiceNow All Rights Reserved

Denial of Service



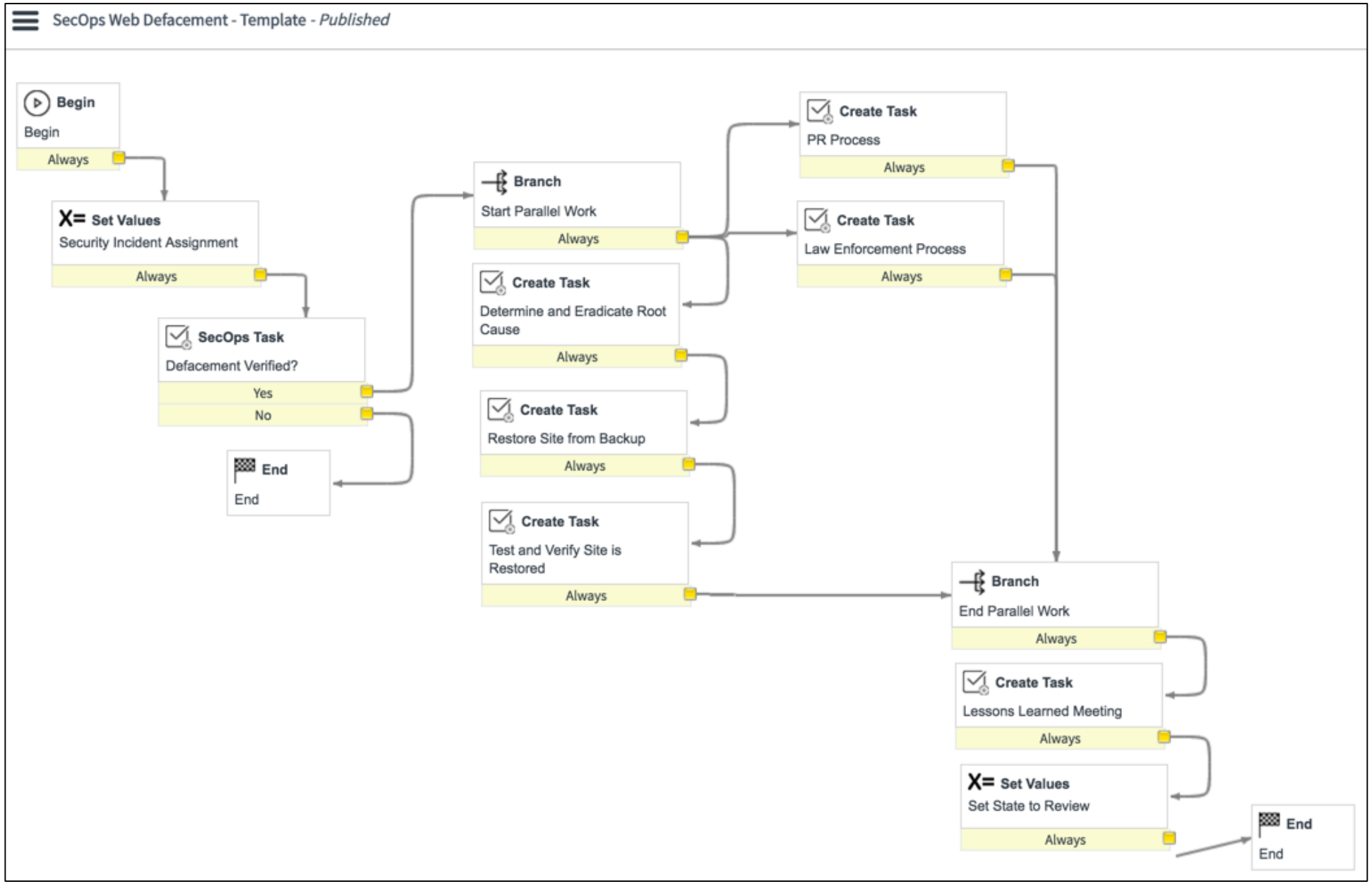
© 2017 ServiceNow All Rights Reserved

Rogue Server or Service



© 2017 ServiceNow All Rights Reserved

Web Defacement



© 2017 ServiceNow All Rights Reserved

Foundation Services for Resolve Real Security Threats Fast

Minimize time to identify and resolve threats by providing visibility to security alerts, standardizing processes, and integrating with IT

CONSULT	IMPLEMENT	OPTIMIZE	TRAIN
			
• Leads workshops to assess security incident response and/or vulnerability management program • Develop services strategy and roadmap	• Configure Security Operations • Develop reporting and analytics to view key performance indicators	• Review implemented solution to understand the newly defined baseline • Ensure outcome was achieved	• Key customer personnel to take Security Operations System Administrator training to manage the solution

Outcome delivered in 3 to 6 months for most customers

© 2017 ServiceNow All Rights Reserved