knowledge17

WORK at LIGHTSPEED™

Making Sense of Events Through the Noise

BRIAN BOYD
Solution Architect
Sabre

© 2017 ServiceNow All Rights Reserved

servicenow

Speaker Introduction



NAME: Brian Boyd

TITLE: Solution Architect

FUNCTION: Automation Development

COMPANY: Sabre

EXPERIENCE: 12 years with Travelocity & Sabre, (10 years operations + 2 years development)

TEAM FOCUS: Automation & Tooling

MY ROLE: Event Management Lead

© 2017 ServiceNow All Rights Reserved

My Company



NAME: Sabre

INDUSTRY: Technology

MARKET FOCUS: Sabre provides technology solutions for the travel & tourism industries

COMPANY'S PRIMARY PRODUCTS/SOLUTIONS: GDS for Inventory, Pricing of Air & Hotel, Software For Airlines & Hoteliers, Tripcase Mobile App

QUICK FACTS: 100K Messages Per Second

12 Billion Shopping Requests Per Year

$120 Billion Of Travel Spend Per Year

© 2017 ServiceNow All Rights Reserved

Objectives



- Learn about Sabre's journey in implementing Event Management
  - How Sabre implemented ServiceNow Event Management
  - What Sabre's Event Management solution looks like
  - The value of Event Management
  - The challenges experienced

© 2017 ServiceNow All Rights Reserved

The Problem

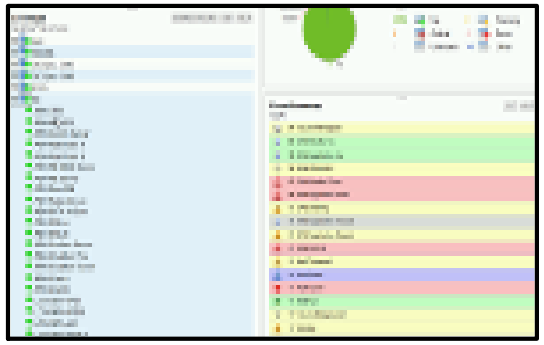
- We are missing notifications of service impact
  - Customers are often reporting them to us
- Why?
  - Multiple dashboard
  - Too much noise
  - Manual, repetitive work

© 2017 ServiceNow All Rights Reserved

Multiple Dashboards

Where do we look?

- Over 60 different tools generating alerts
- Siloed teams, limited visibility

Command Center	Network	Storage	Application Teams
			

© 2017 ServiceNow All Rights Reserved

Too Much Noise

We got an alert, but …

- Dashboard always full of alerts
- No automated prioritization
- Minimal de-duplication
- No correlation

… the alerts are meaningless!



© 2017 ServiceNow All Rights Reserved

Manual, Repetitive Work

- Search for Knowledge Article
  - 2-3 minutes per alert
- Create Incident
  - Inconsistently performed
  - Inaccurate reporting

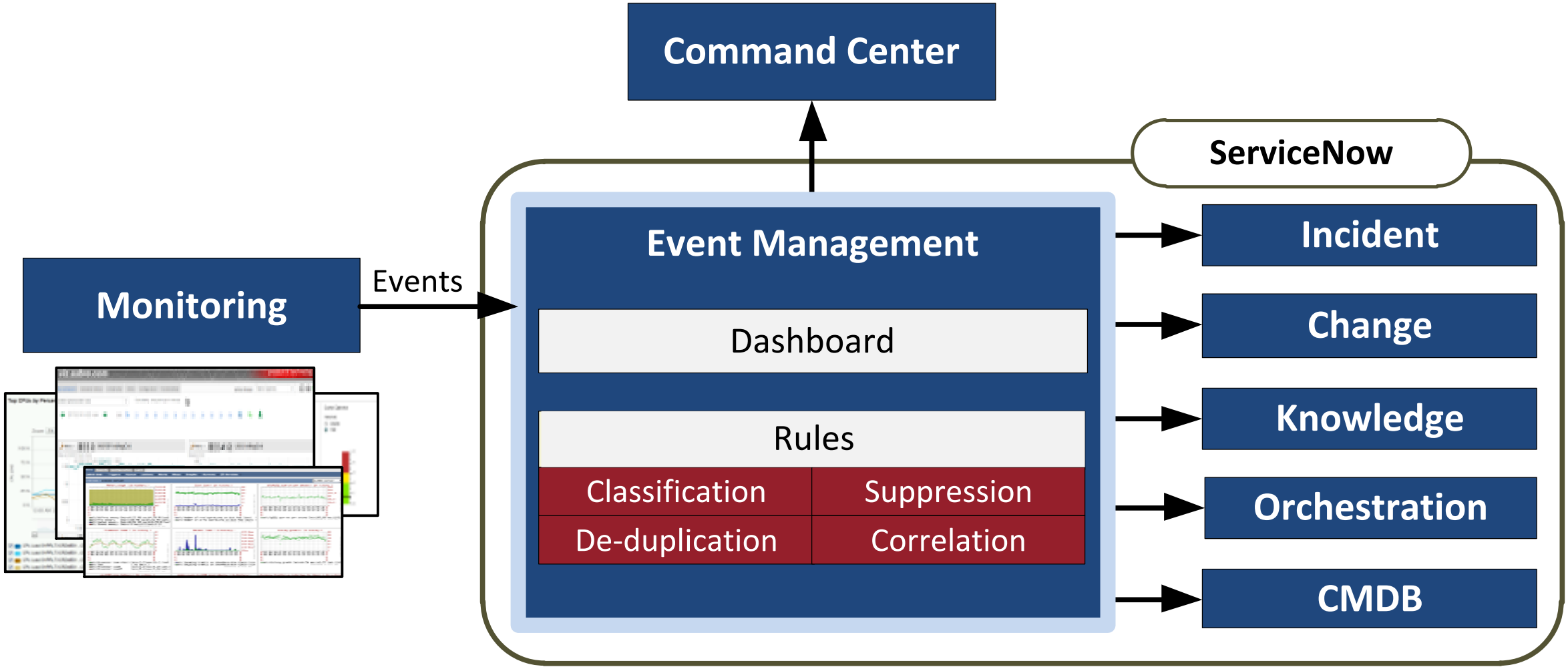
© 2017 ServiceNow All Rights Reserved

The Goals

- Short-term
  - To not miss any alerts of service impact
- Long-term
  - To reduce MTTR through advanced correlation and automated remediation

© 2017 ServiceNow All Rights Reserved

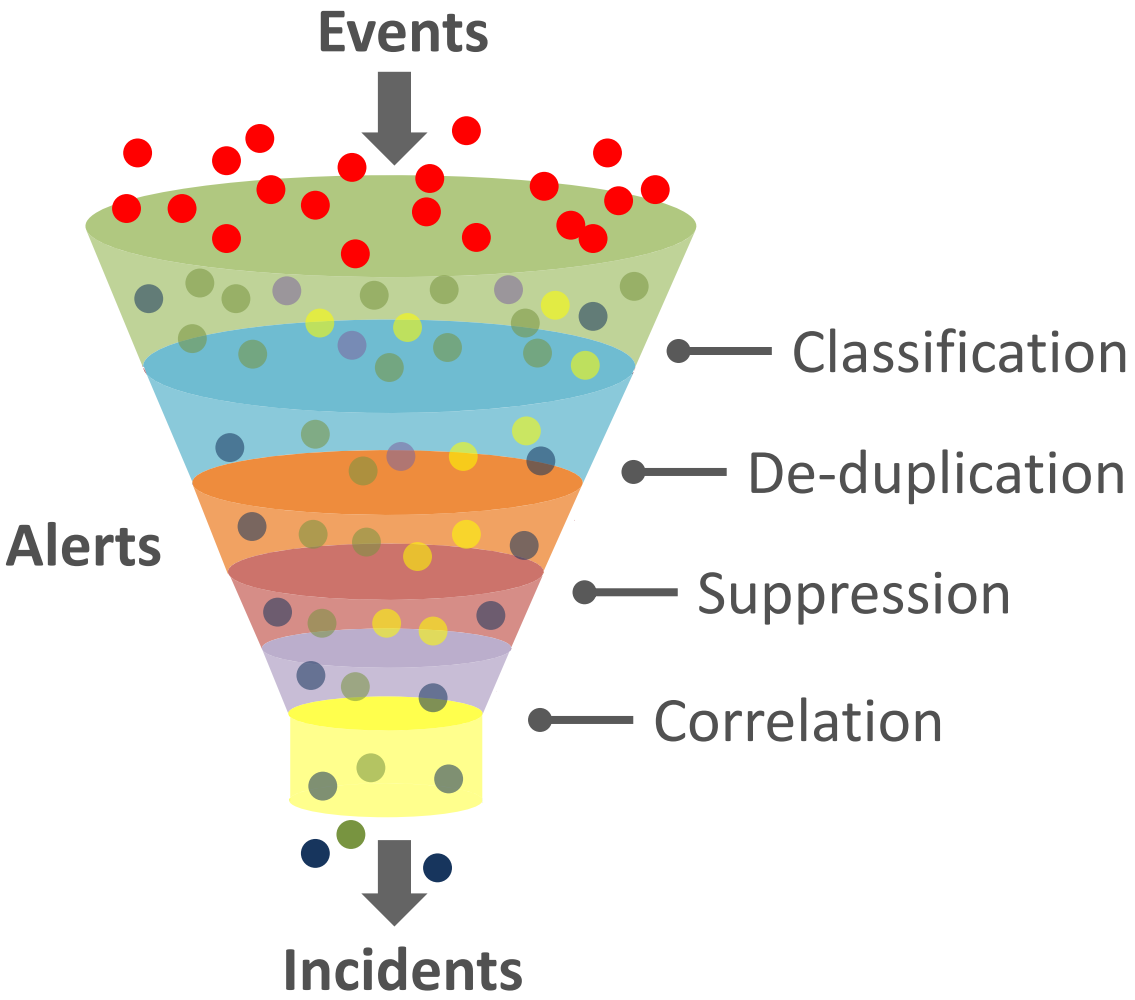
Solution: Event Management



© 2017 ServiceNow All Rights Reserved

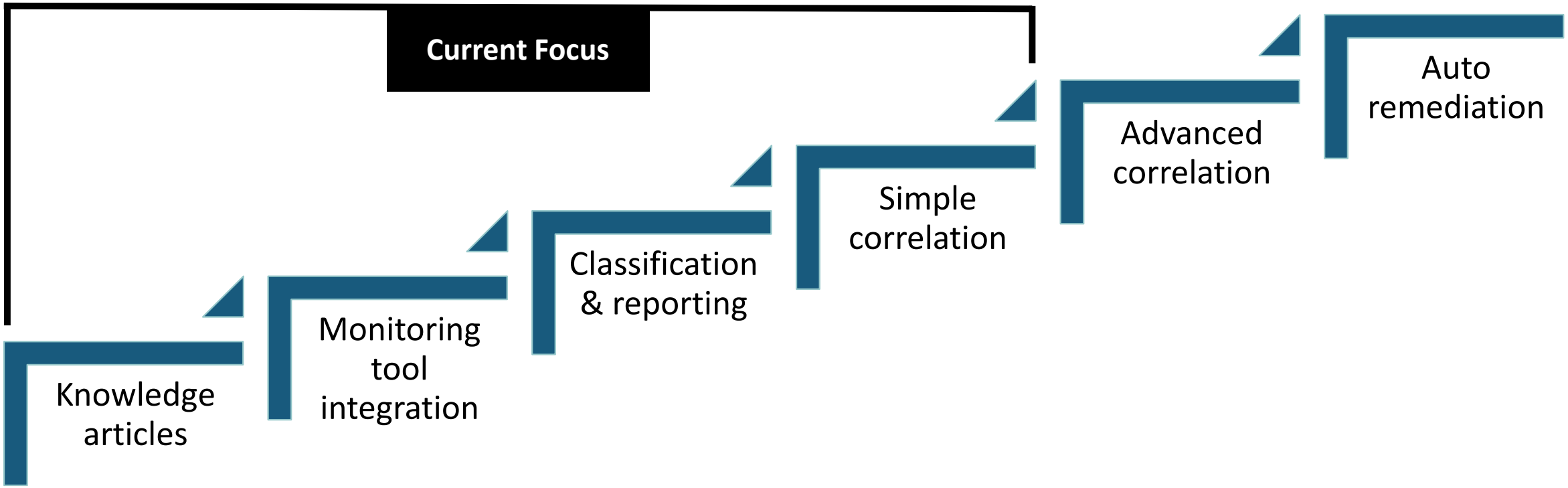
Terminology

- Event
  - Raw notification from monitoring tools
  - Classification, de-duplication and suppression
- Alert
  - “Smart” events
  - Correlation



© 2017 ServiceNow All Rights Reserved

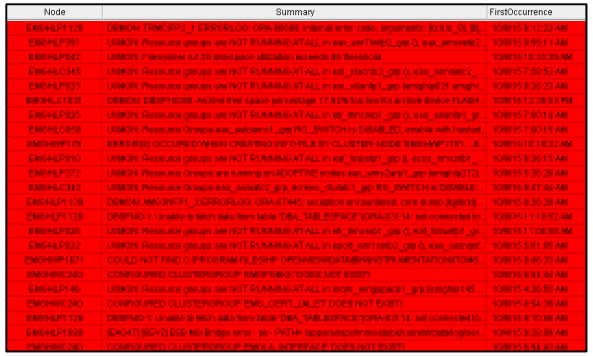
Implementation Strategy



© 2017 ServiceNow All Rights Reserved

Where Did We Start?

- People
  - 2 Sabre developers
  - ServiceNow Professional Services
- Monitoring integrations
  - Oracle Enterprise Manager
    - Database team required automatic creation of incidents to replace manual creation process
    - Quick win!
  - Service Provider monitoring
    - Represents 70% of all events
    - 3.9 million events per month



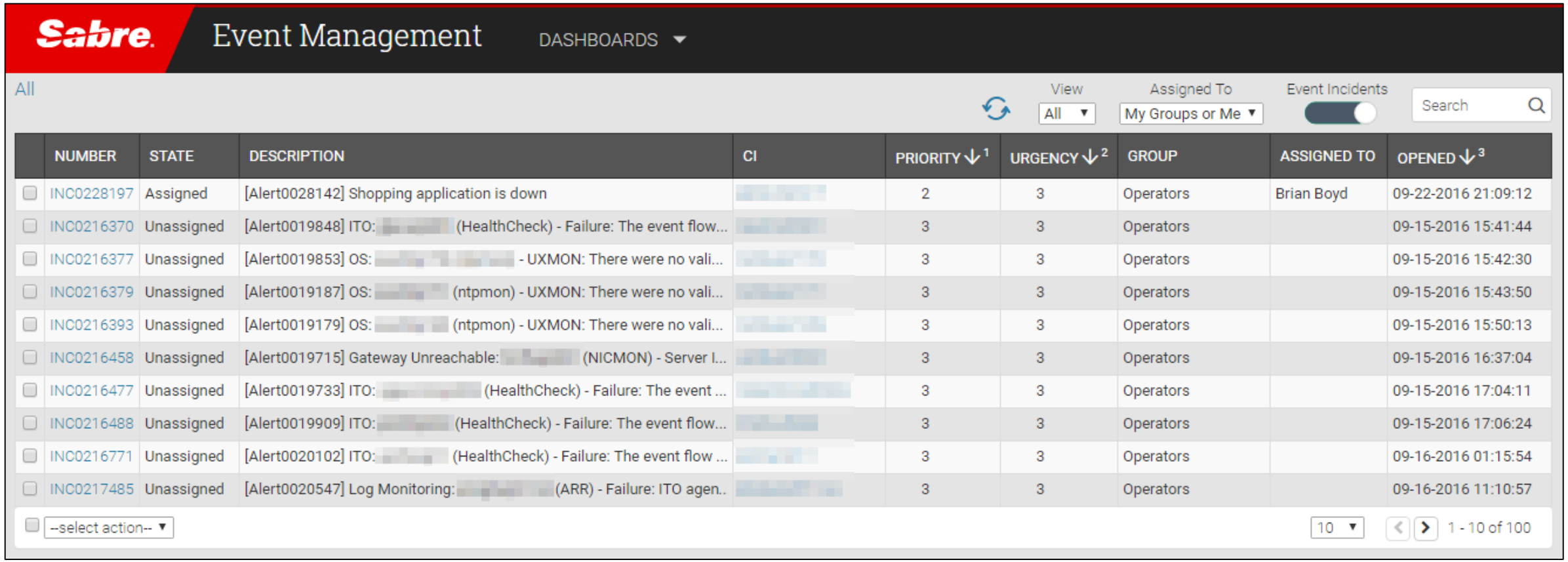
© 2017 ServiceNow All Rights Reserved

Implementation Decisions

- Should the Command Center watch alerts or incidents?
  - Decided on Incidents
    - Minimize the different records to interact with
    - Any alert requiring action must create an incident, so automate it
    - Ownership, SLA/OLA tracking

© 2017 ServiceNow All Rights Reserved

Command Center Dashboard

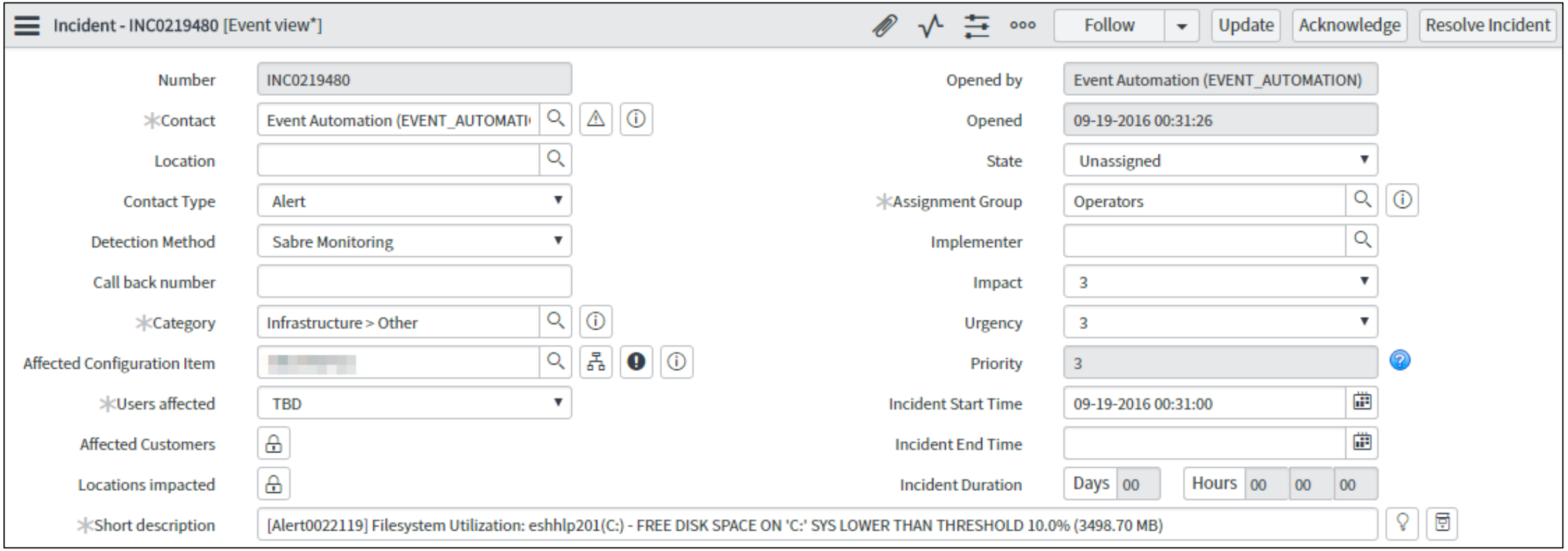


	NUMBER	STATE	DESCRIPTION	CI	PRIORITY ↓1	URGENCY ↓2	GROUP	ASSIGNED TO	OPENED ↓3
☐	INC0228197	Assigned	[Alert0028142] Shopping application is down		2	3	Operators	Brian Boyd	09-22-2016 21:09:12
☐	INC0216370	Unassigned	[Alert0019848] ITO: (HealthCheck) - Failure: The event flow...		3	3	Operators		09-15-2016 15:41:44
☐	INC0216377	Unassigned	[Alert0019853] OS: - UXMON: There were no vali...		3	3	Operators		09-15-2016 15:42:30
☐	INC0216379	Unassigned	[Alert0019187] OS: (ntpmon) - UXMON: There were no vali...		3	3	Operators		09-15-2016 15:43:50
☐	INC0216393	Unassigned	[Alert0019179] OS: (ntpmon) - UXMON: There were no vali...		3	3	Operators		09-15-2016 15:50:13
☐	INC0216458	Unassigned	[Alert0019715] Gateway Unreachable: (NICMON) - Server I...		3	3	Operators		09-15-2016 16:37:04
☐	INC0216477	Unassigned	[Alert0019733] ITO: (HealthCheck) - Failure: The event ...		3	3	Operators		09-15-2016 17:04:11
☐	INC0216488	Unassigned	[Alert0019909] ITO: (HealthCheck) - Failure: The event flow...		3	3	Operators		09-15-2016 17:06:24
☐	INC0216771	Unassigned	[Alert0020102] ITO: (HealthCheck) - Failure: The event flow ...		3	3	Operators		09-16-2016 01:15:54
☐	INC0217485	Unassigned	[Alert0020547] Log Monitoring: (ARR) - Failure: ITO agen..		3	3	Operators		09-16-2016 11:10:57

--select action-- 10 1 - 10 of 100

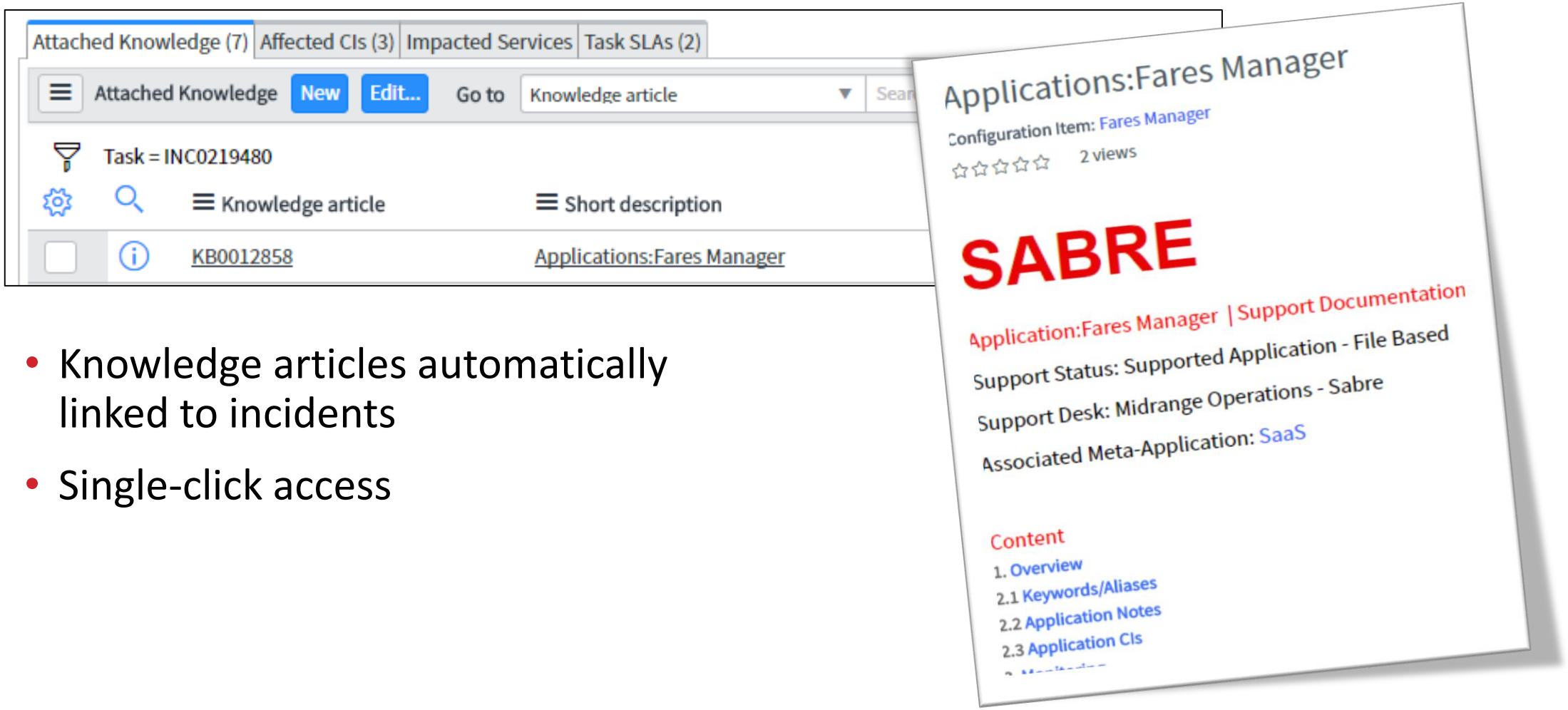
© 2017 ServiceNow All Rights Reserved

Event-Generated Incident



© 2017 ServiceNow All Rights Reserved

Knowledge Articles



- Knowledge articles automatically linked to incidents
- Single-click access

© 2017 ServiceNow All Rights Reserved

Monitoring Event Feeds

- Monitoring tools send “heartbeat” events
- Quickly detect when a specific monitoring tool is unable to send events to ServiceNow

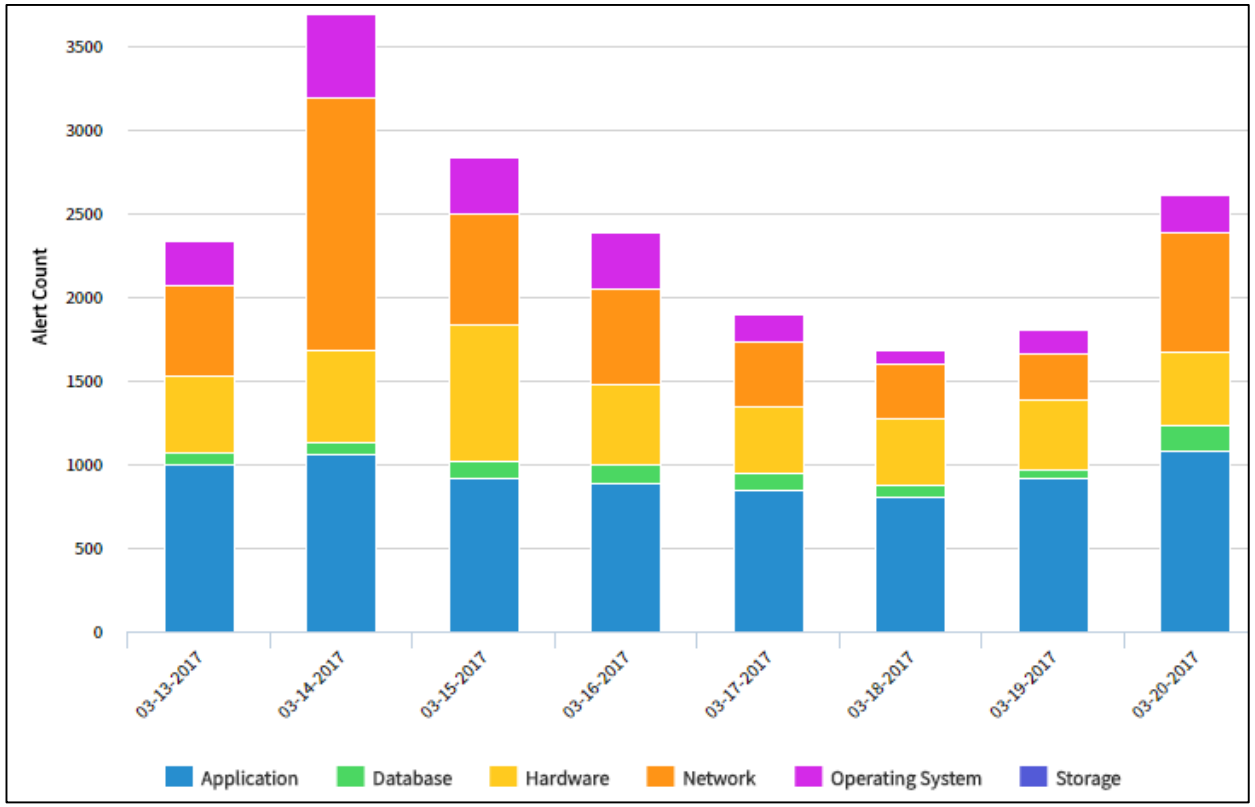
Name ▲	Events being received
AppDynamics	true
ATSE Zabbix Prod	true
Solarwinds Application (Austin)	true
Solarwinds Application (Lewisville)	true
Splunk SHS	true

Incident created

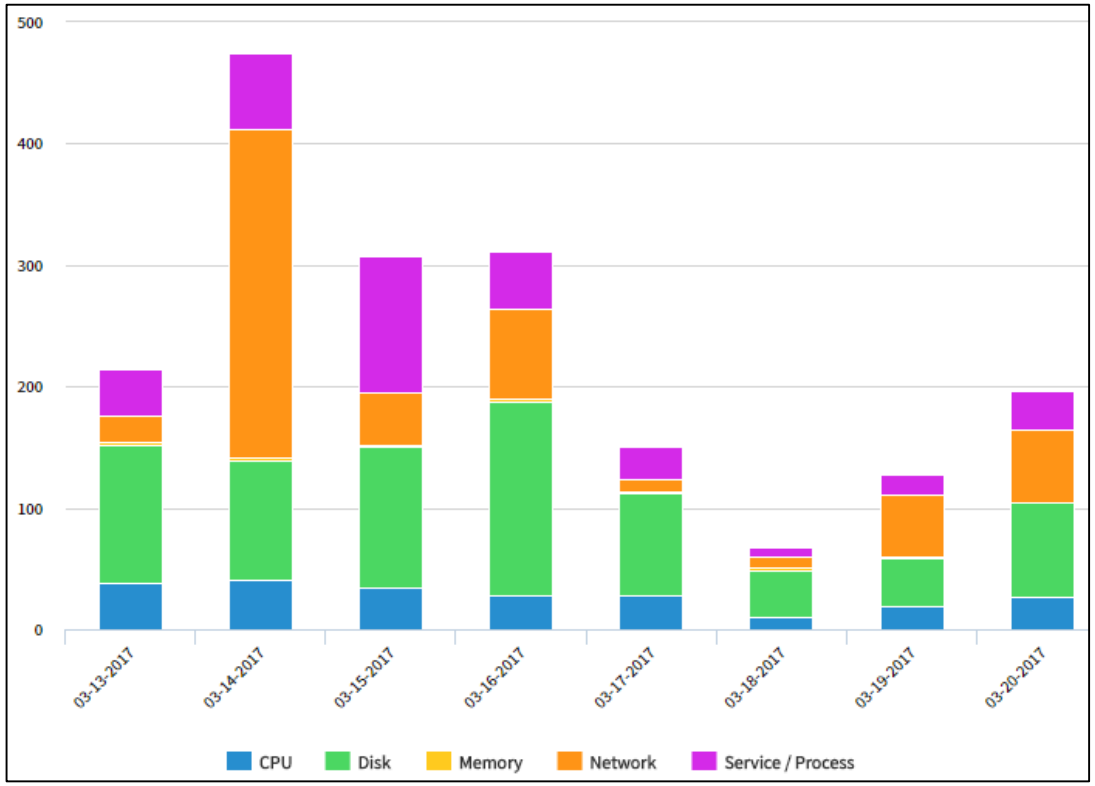
Event Management has received No Events in the last 15 minutes from Solarwinds Application (Lewisville). ServiceNow instance is sabre.

© 2017 ServiceNow All Rights Reserved

Classification



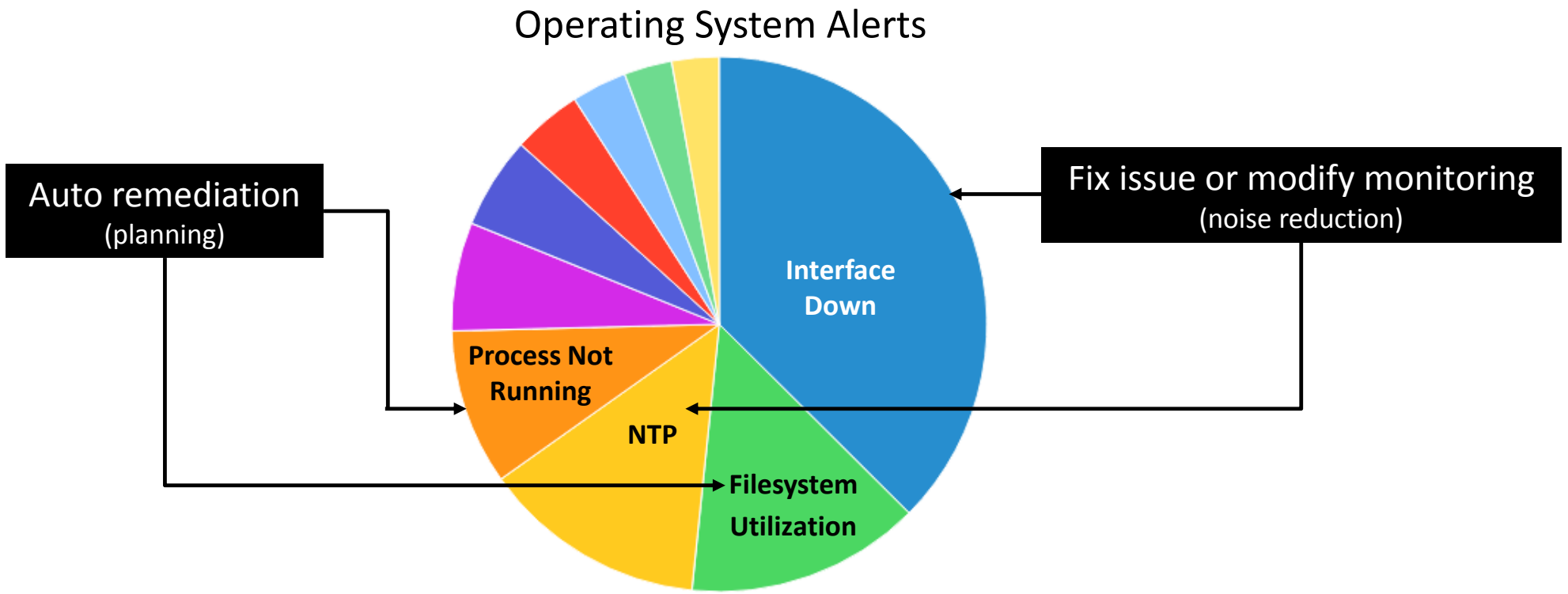
Operating System Alerts



© 2017 ServiceNow All Rights Reserved

Classification

- Classification helps with noise reduction and planning



© 2017 ServiceNow All Rights Reserved

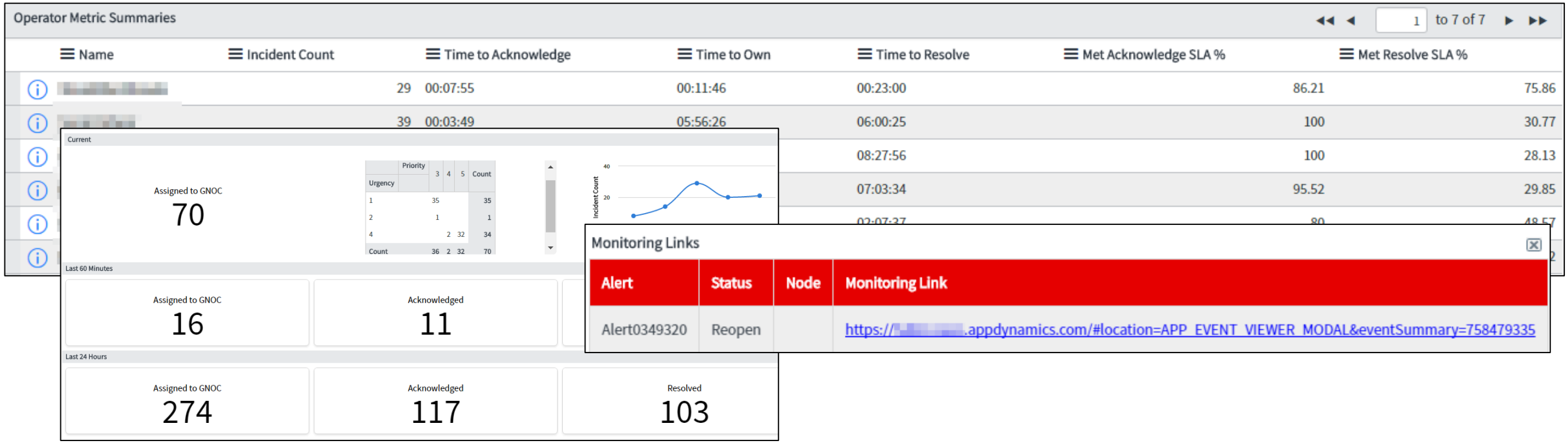
Reporting

- Don’t underestimate its power in reducing noise
  - A specific server has alerted every day for the past 3 months that its E drive is filling up
    - Adjust the monitoring threshold or increase the filesystem size
  - 32% of the event-generated incidents are open for more than 2 months
    - These incidents are tied to events continuously being generated – NOISE!!
    - Fix the issue or adjust the monitoring alert

© 2017 ServiceNow All Rights Reserved

Additional Customizations

- Command Center Operator performance reporting
- Deep link to monitoring tools from Incident
- Turnover Logs

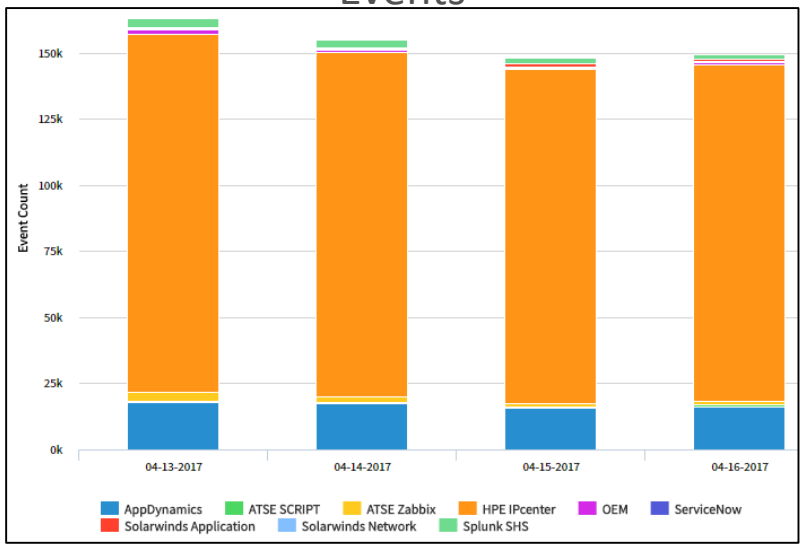


© 2017 ServiceNow All Rights Reserved

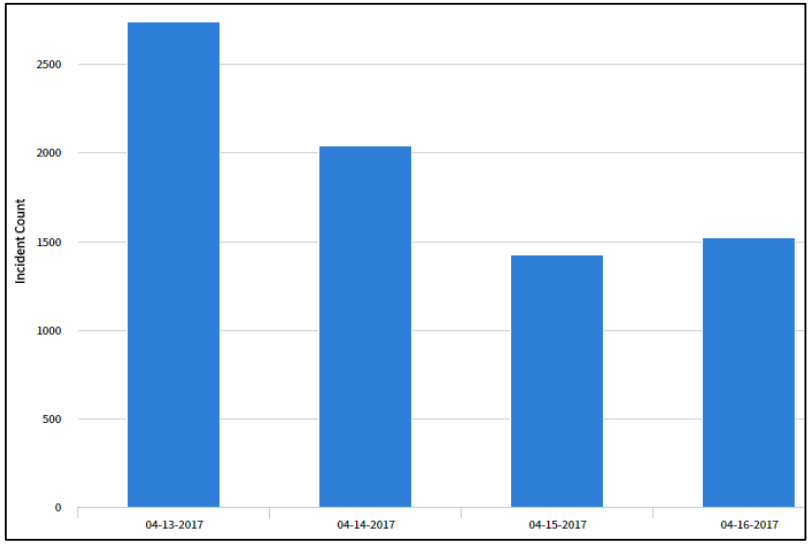
Current State

- 8 monitoring integrations completed
- 150k events per day
- 1,800 incidents per day
- Migration of Command Center to ServiceNow completed 3 months ahead of schedule

Events



Incidents



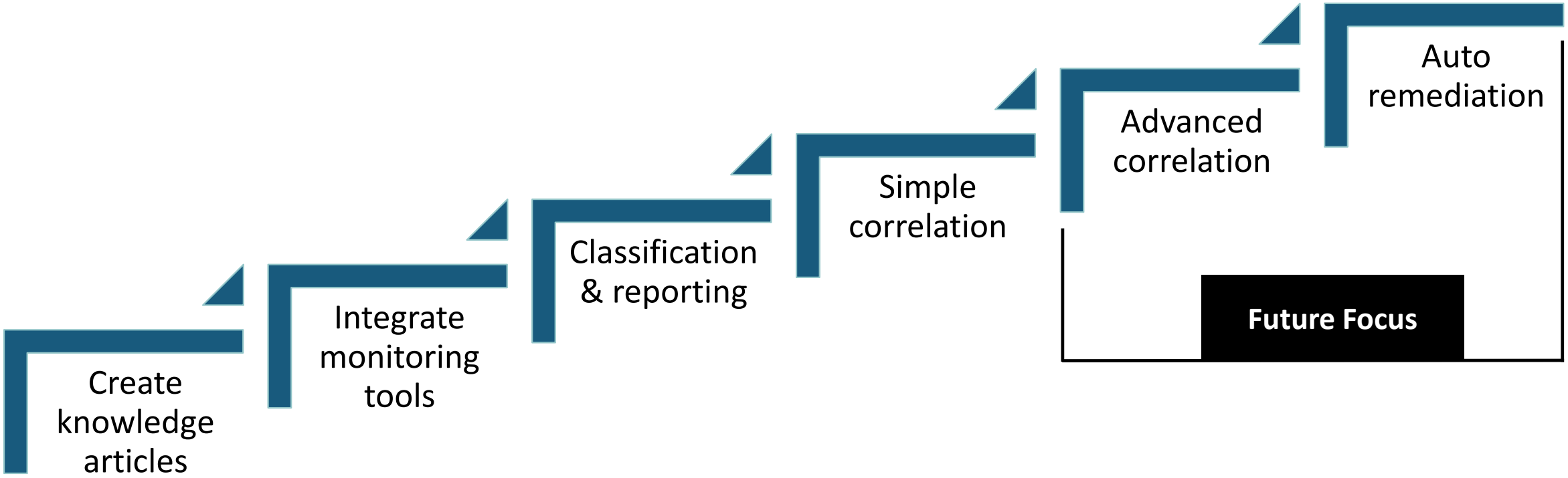
© 2017 ServiceNow All Rights Reserved

Current State

		Before		After
Multiple Dashboards	# of dashboards	> 60	→	1
Too Much Noise	# Command Center tickets in queue	> 100	→	< 5
	Event to incident ratio	Unknown	→	83 : 1
Manual Work	Time to create incident	2-3 minutes	→	0
	Time to locate knowledge article	2-3 minutes	→	< 30 seconds

© 2017 ServiceNow All Rights Reserved

Next Steps



© 2017 ServiceNow All Rights Reserved

Challenges

- Dashboards
  - Out of the box focuses on Alerts, not Incidents
- Rules for Incidents
  - Setting fields such as Urgency, Impact and Assignment Group
  - Linking to records such as Knowledge Articles
- Job scheduler
  - Stopped processing

© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Leverage the integration with Incident, Change, Knowledge and CMDB.

2

Don’t overlook categorization and reporting for reducing noise.

3

If a feature doesn’t exist, write it yourself.

© 2017 ServiceNow All Rights Reserved

Q & A

BRIAN BOYD
Solution Architect
Sabre

© 2017 ServiceNow All Rights Reserved

Take the Survey

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

Thank You

Brian Boyd

Solution Architect

Sabre

© 2017 ServiceNow All Rights Reserved