knowledge17

WORK at LIGHTSPEED™

BRE4023: Turning Infrastructure Events into Actions

TONY BRANTON
SENIOR ADVISORY SOLUTION ARCHITECT
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Service availability challenges
- How ServiceNow is helping eliminate service outages
- Overview and tips for integrating events
- Q & A

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



NAME: Tony Branton

TITLE: Senior Advisory Solution Architect

FUNCTION: ITOM Practice

COMPANY: ServiceNow

EXPERIENCE: 3 years at ServiceNow, 15 years in ITOM industry, 25 years in IT industry

EXPERTISE: Event Management, Discovery, Service Mapping, Orchestration Cloud Management

© 2017 ServiceNow All Rights Reserved

Session Overview



Objectives

- Get best practices and real-world advice on how to ingest events from across your infrastructure and turn them into actions. Learn how automation can provide immediate action to resolve problems before they turn into full-blown outages



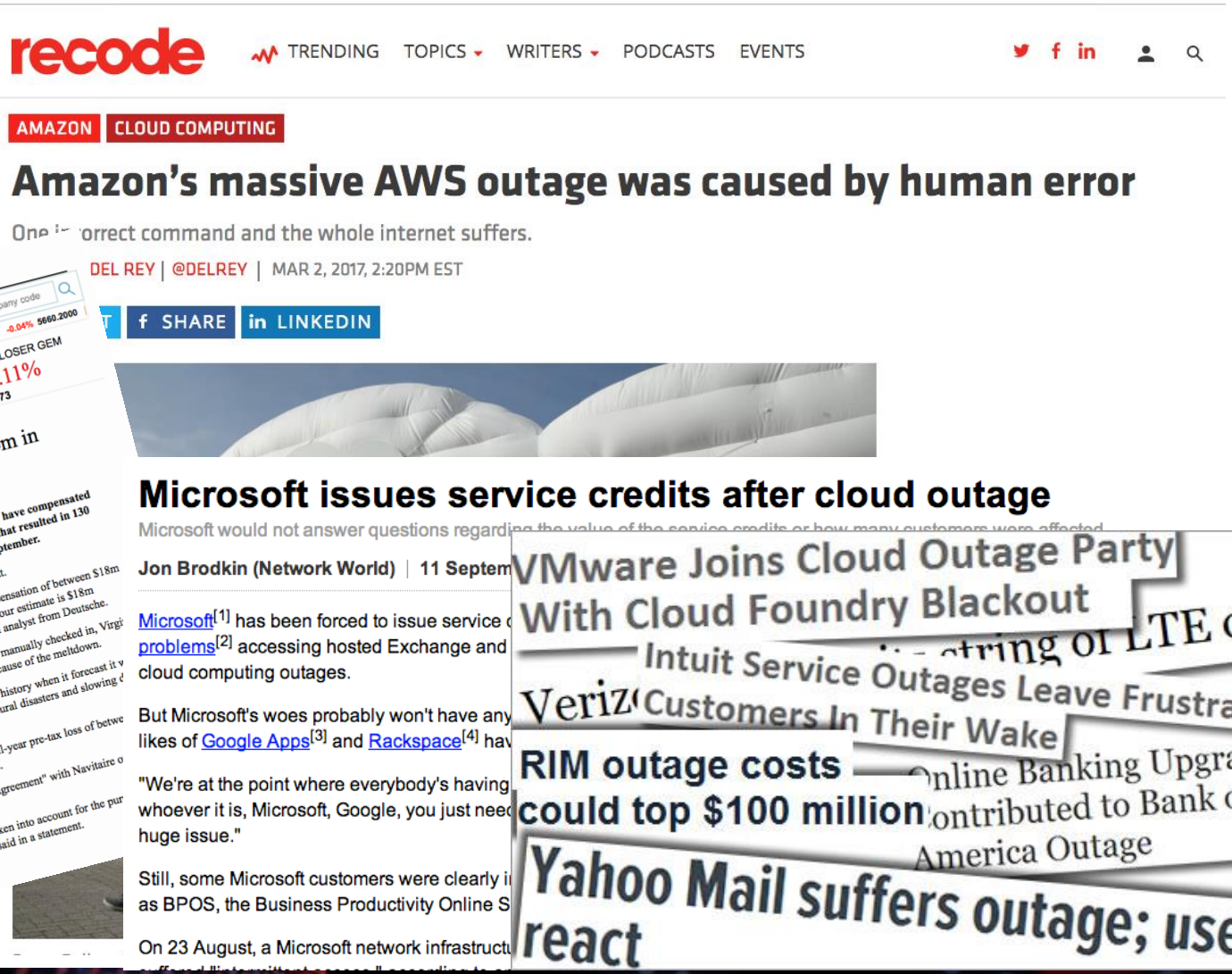
What You Will Learn

- Service availability challenges
- How ServiceNow is helping eliminate service outages
- How machine learning applies
- Overview and tips for integrating events

© 2017 ServiceNow All Rights Reserved

Service Delivery Issues Make Headlines

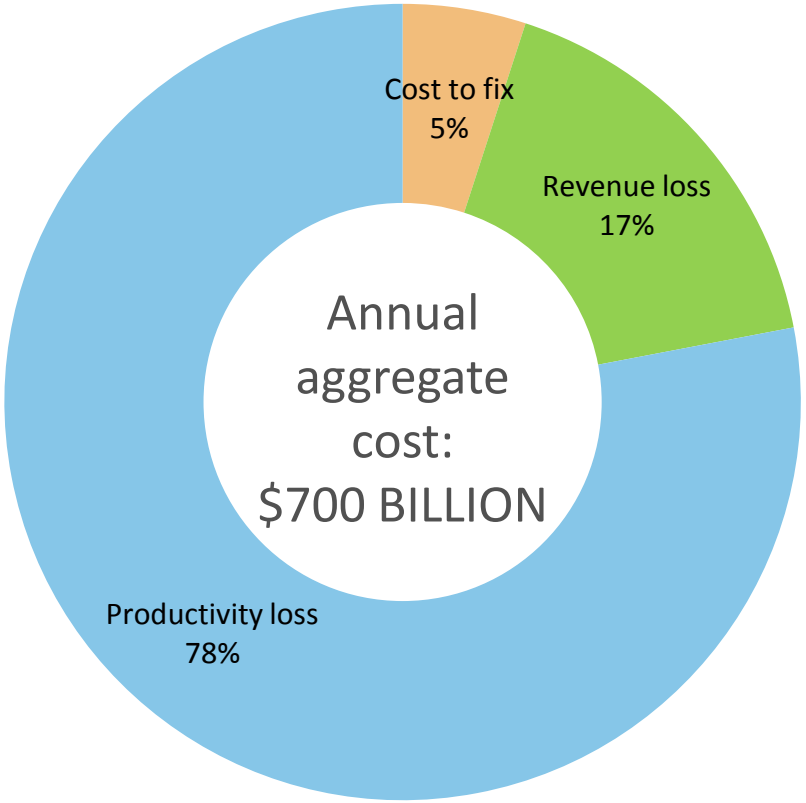




© 2017 ServiceNow All Rights Reserved

Main Cost of Outages

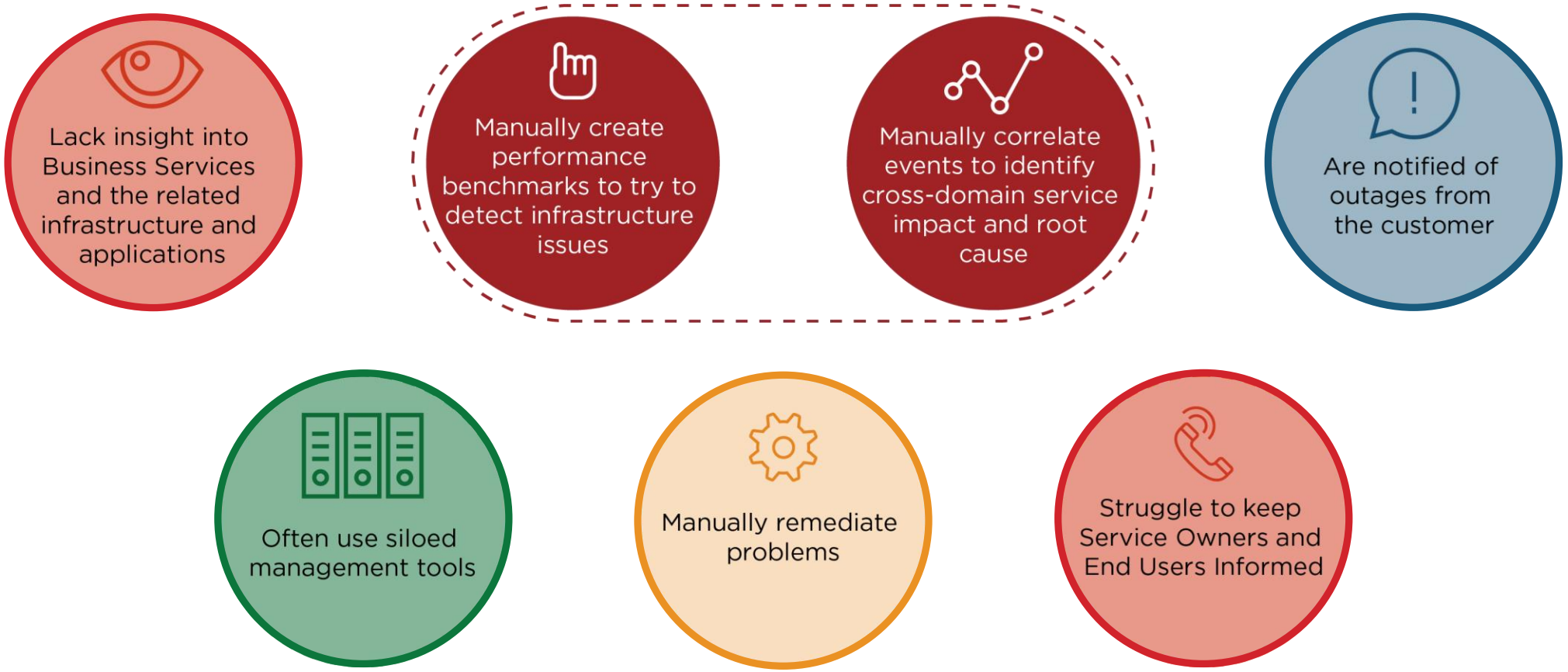
"A small investment in increasing the reliability of ICT systems provides an outsized return by reducing productivity and revenue losses"



IHS, IHS Infonetics The Cost of Server, Application, and Network Downtime: Annual North American Enterprise Survey and Calculator; 2016

© 2017 ServiceNow All Rights Reserved

When Problems Occur IT Operations Teams…



© 2017 ServiceNow All Rights Reserved

ServiceNow Helps…

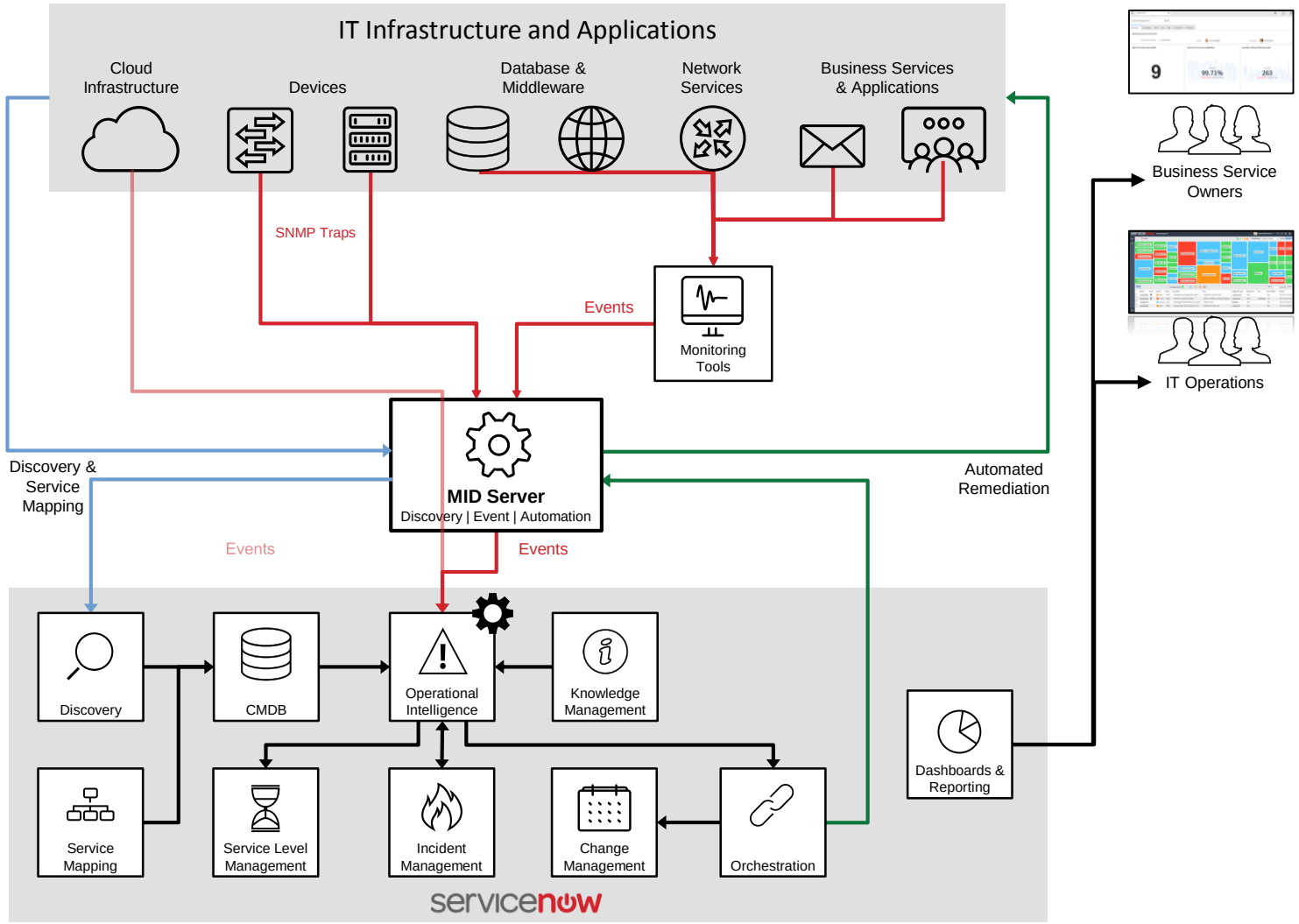
Eliminate service outages by proactively identifying service issues, pinpointing disruptions, and automating remediation



© 2017 ServiceNow All Rights Reserved

Eliminate Service Outages

- Discovery and Service Mapping
  - Discover CIs & map business services
- Operational Intelligence
  - Consolidate events
  - Normalize, filter, de-dupe, regulate, correlate
  - Map alerts to CIs and services to understand service impact
  - Group related alerts and identify probable root causes
  - Link alerts to Knowledge articles
- Service Management
  - Create incidents and other tasks automatically using Alert Rules
  - Trigger SLAs
- Orchestration
  - Manual or automated remediation using Alert Rules and orchestration workflows
  - Automatically create change request and run corrective actions to restore business service
- Visibility for IT Operations and Service Owners through dashboards and reports



© 2017 ServiceNow All Rights Reserved

Connect to Multiple Monitoring Tools

Machine learning analyzes events collected, filtered, and normalized from multiple monitoring tools to rapidly understand impact to business services.

- AWS CloudWatch
- HP OM
- IBM Netcool OMNIbus
- Hyperic
- Microsoft SCOM
- SolarWinds
- VMware vRA
- Zabbix

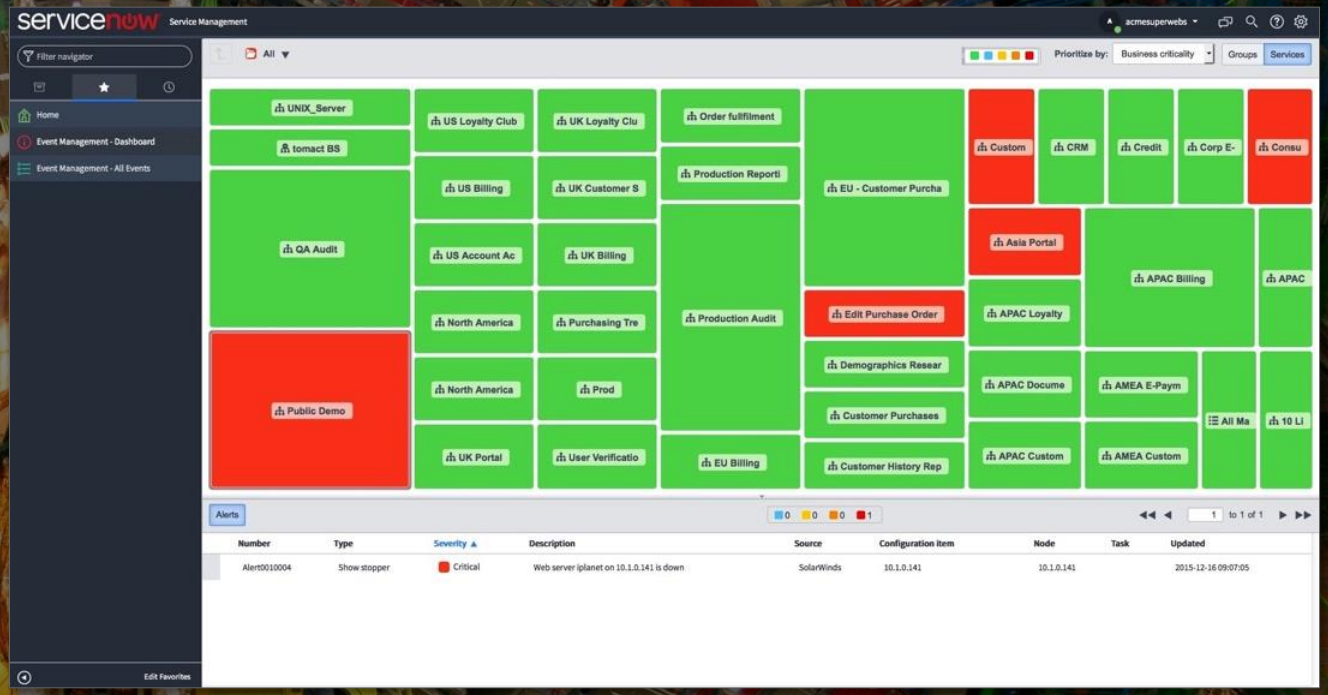
OOTB

- AppDynamics
- DynaTrace
- New Relic
- Entuity
- PRTG
- Splunk
- SumoLogic
- ThousandEyes

REST

- CA UIM
- Nagios XI
- Oracle Enterprise Manager
- Zenoss

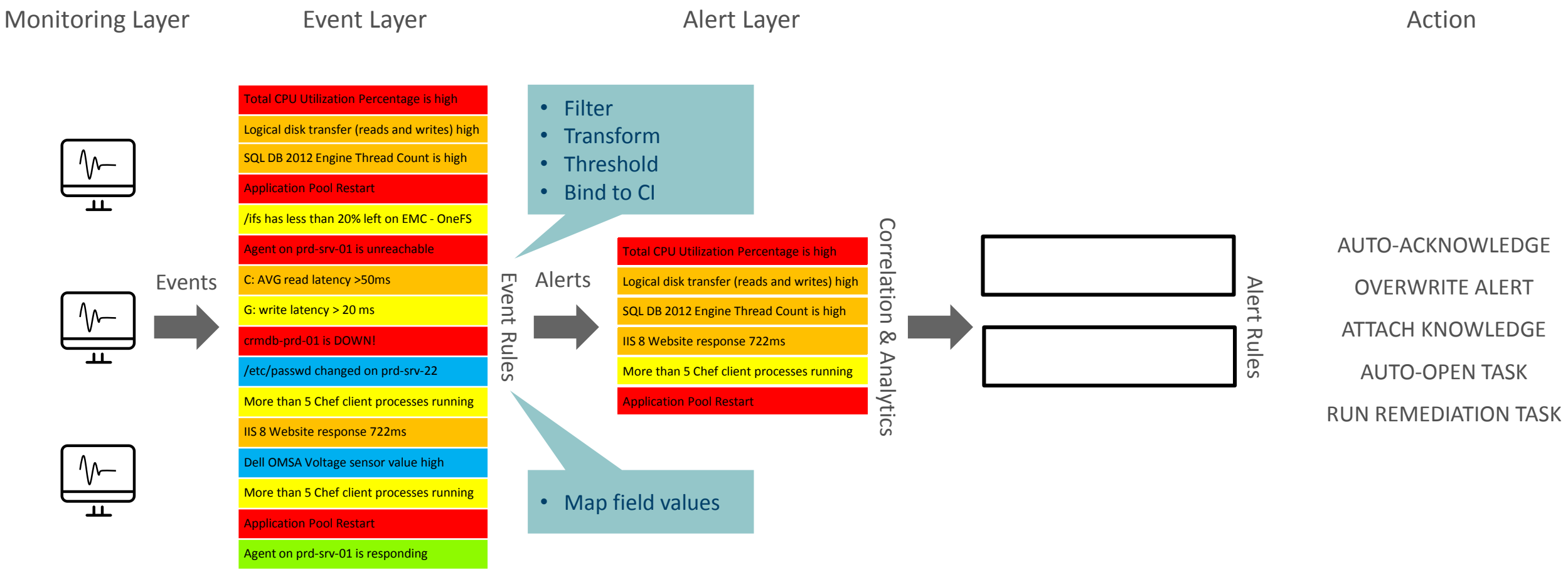
SNMP



Product names referenced are trademarks or registered trademarks of their respective holders and not ServiceNow.

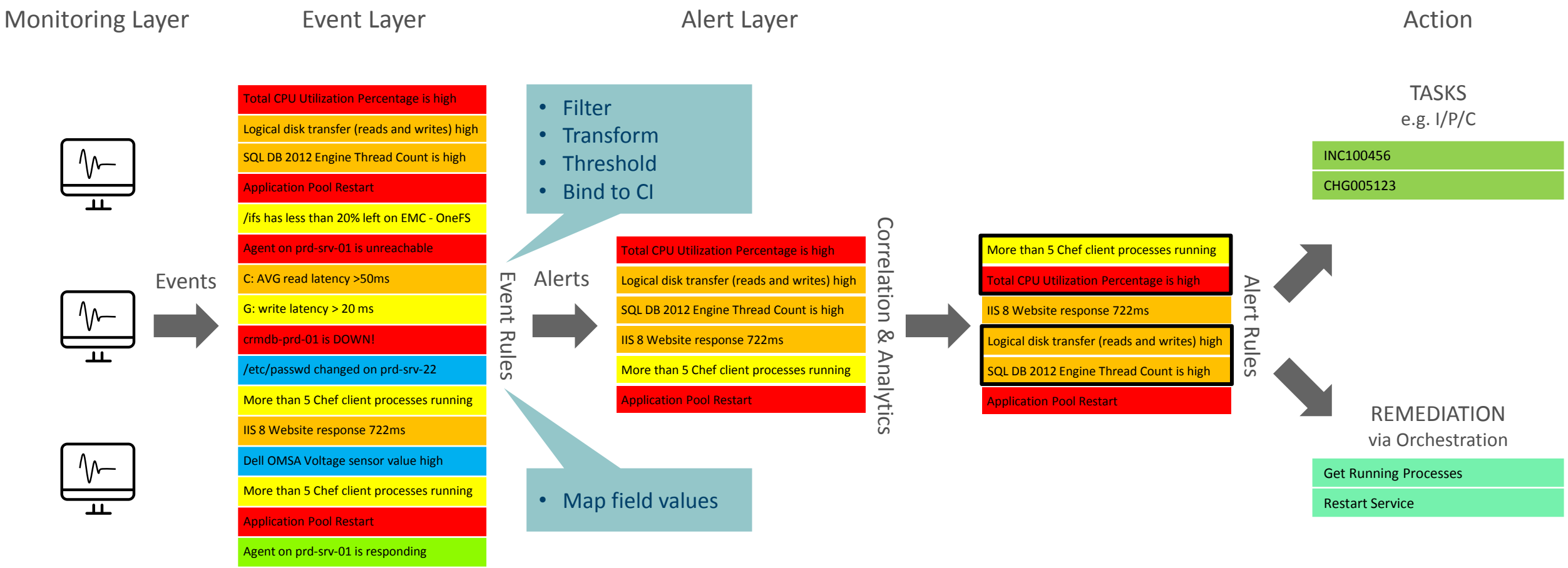
© 2017 ServiceNow All Rights Reserved

Event and Alert Processing



© 2017 ServiceNow All Rights Reserved

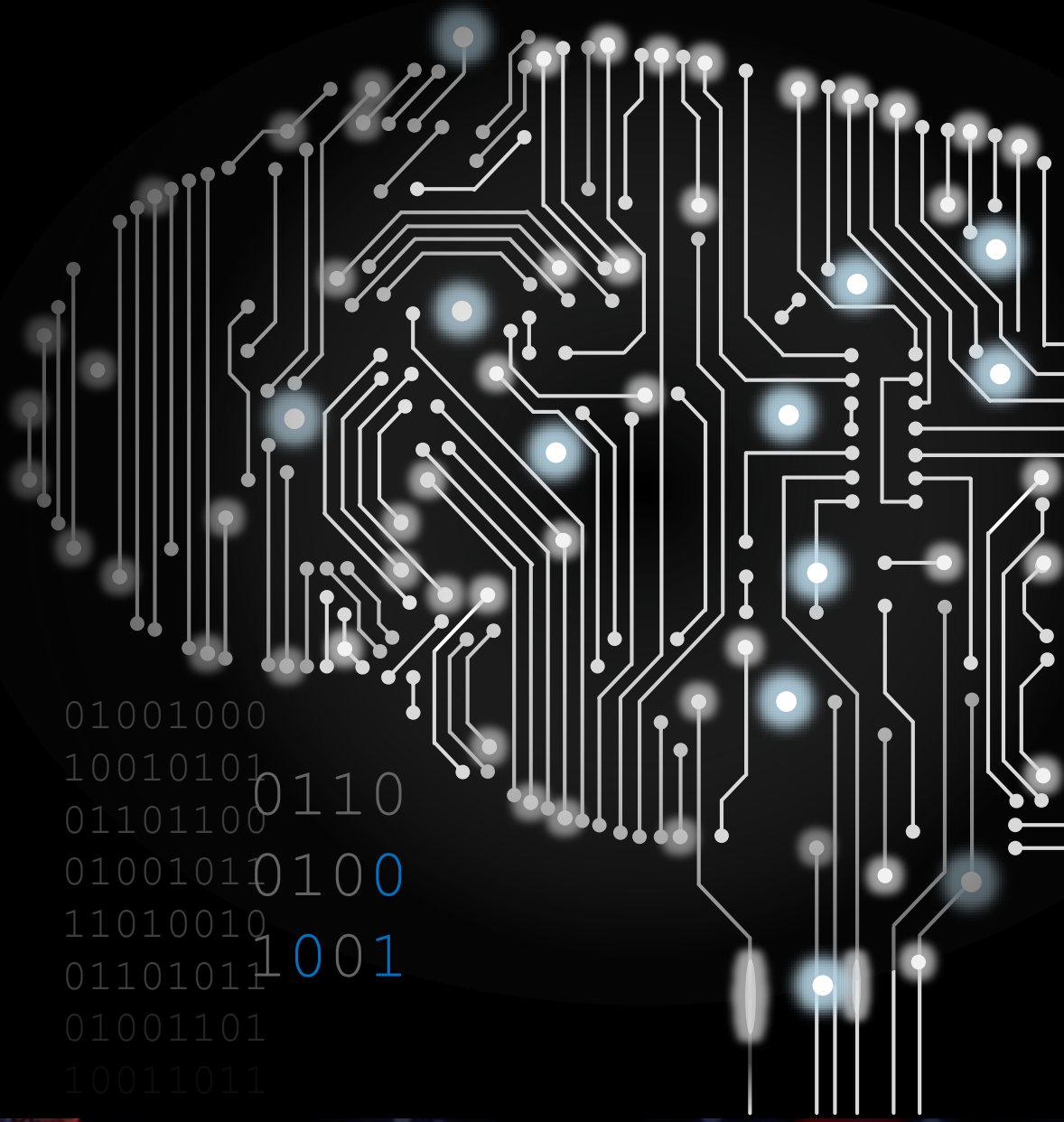
Event and Alert Processing



© 2017 ServiceNow All Rights Reserved

“what we want is a machine that can learn from experience.”

- Alan Turing, 1947



© 2017 ServiceNow All Rights Reserved

Machine Learning

Alert Aggregation

- Alerts can be combined and treated as a single phenomenon.
- Key relationships between alerts are discovered and stored for analysis
- Noise can be eliminated by only displaying alerts that are related

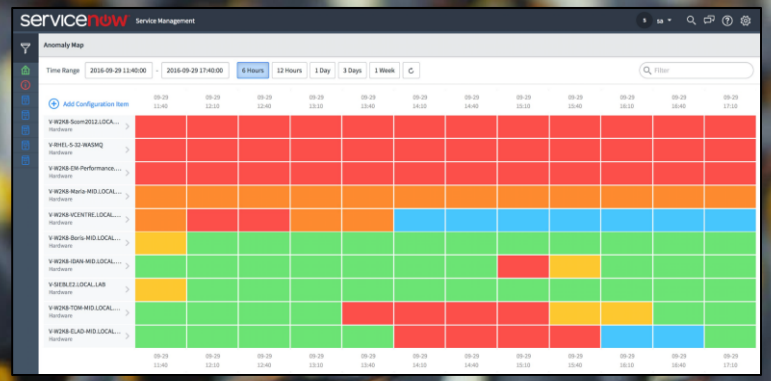
Root Cause Analysis (RCA)

- Assign probabilities to root causes when a significant event (alarm, failure, etc.) could have been the result of more than one upstream event
- Most likely root causes can be investigated before less likely root causes
- Discover causal relationships between events unknown to the designer of the service model

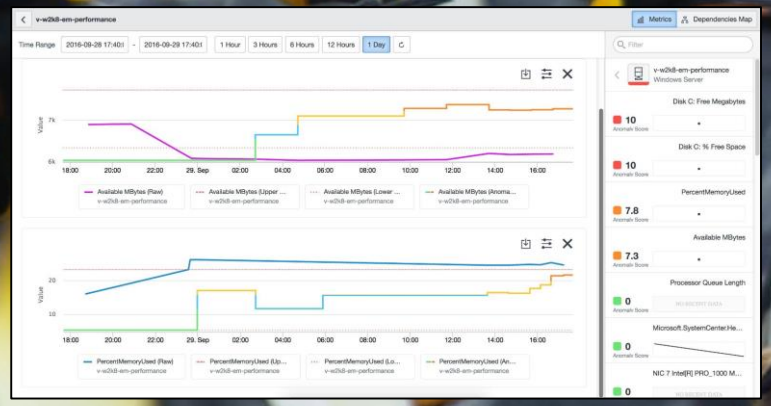
© 2017 ServiceNow All Rights Reserved

Anomaly Detection

Machine learning applied to operational metrics provides insight to CI anomalies



Anomaly Map



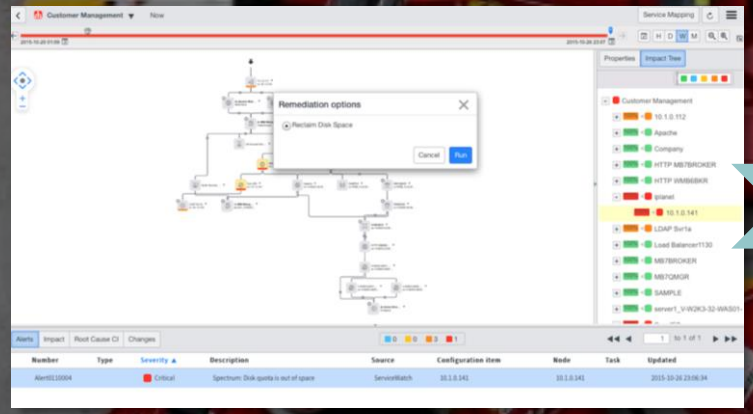
Metric Explorer

© 2017 ServiceNow All Rights Reserved

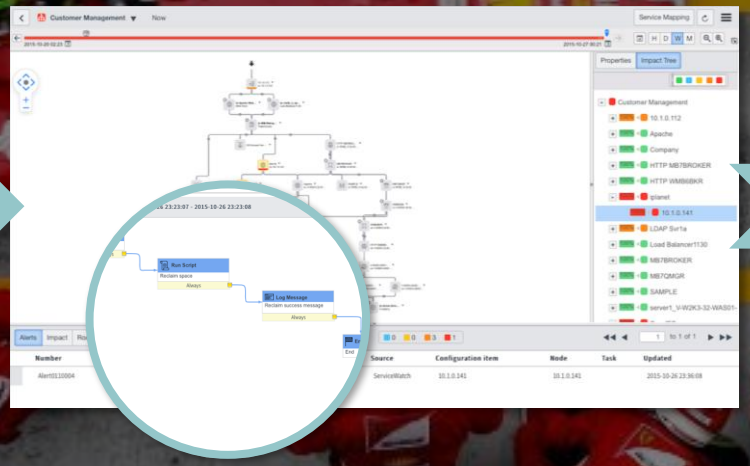
Remediation

Accelerate MTTR by automating corrective actions with ServiceNow Orchestration

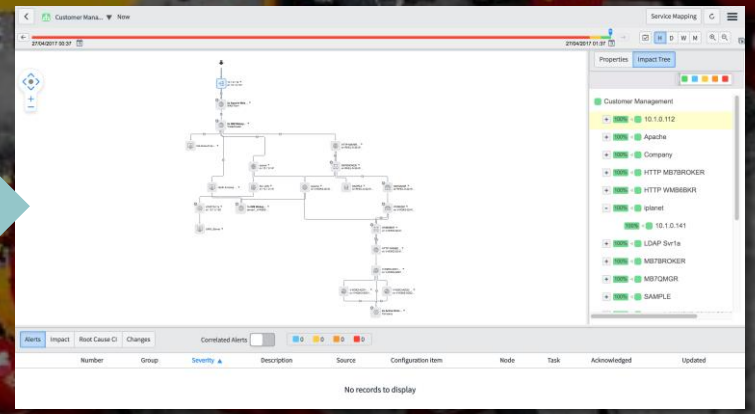
Trigger Remediation



Run Remediation



Service Health Restored

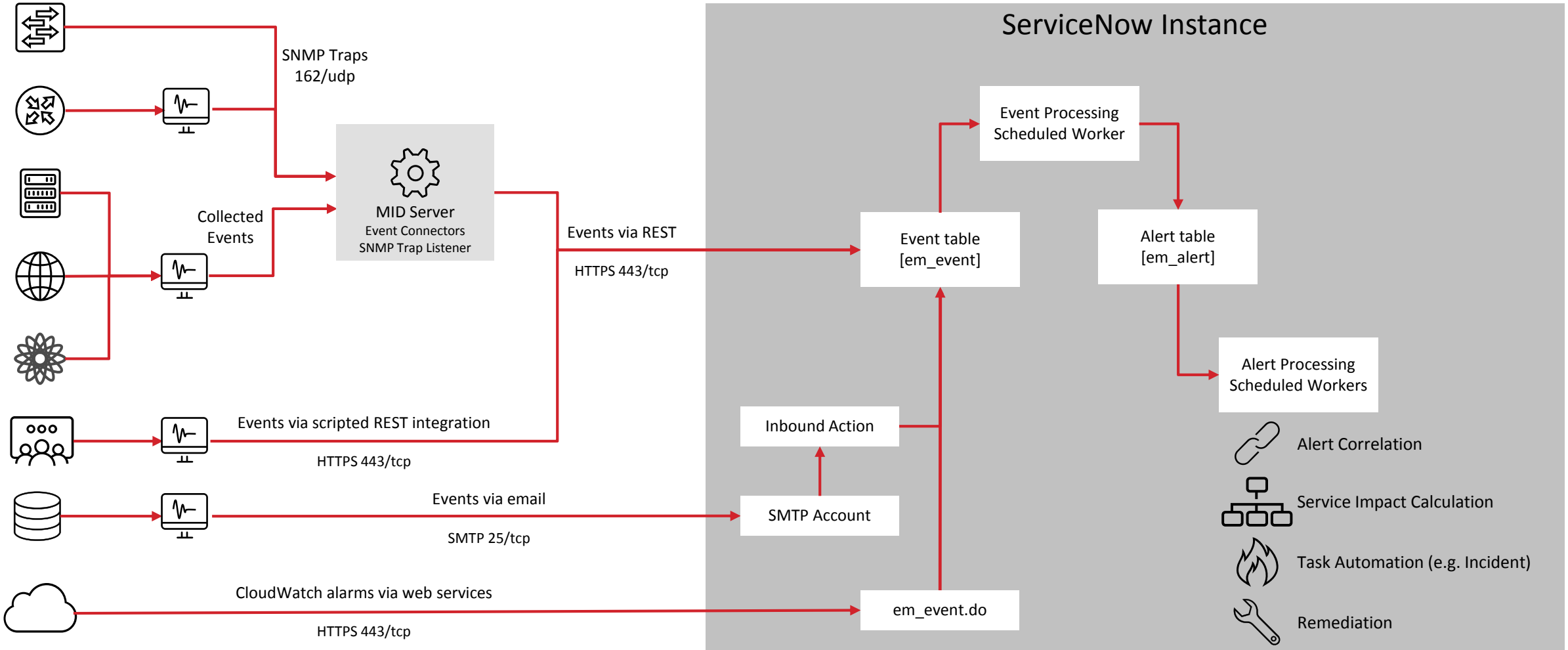


© 2017 ServiceNow All Rights Reserved

Overview and Tips on Integrating Events

© 2017 ServiceNow All Rights Reserved

Event Integration Overview



Infrastructure | Monitoring | Event Collection | Event Management

© 2017 ServiceNow All Rights Reserved

Deciding on an Integration Method

Criteria	Connector	REST	Web Services	SNMP	Email
OOTB supported monitoring tool	X				
Bi-directional support required	X				
Monitoring tool can trigger script/command		X			
Cloud-based monitoring (AWS CloudWatch, Azure, etc)			X		
Event source can forward SNMP traps				X	
Event source can send email notifications					X
MID server required	X			X	

© 2017 ServiceNow All Rights Reserved

Event Integration Tips

- Test production events in a non-production environment.
  - Integrate with non-production element managers and ServiceNow® instances.
  - If non-production element managers are not available, send events from element managers to both production and non-production environments.
- SNMP traps
  - Use a monitoring tool to send SNMP traps rather than sending them directly from devices.
  - Review the MIB(s) to determine their dependencies – MIB files must be uploaded in the correct dependency order.
  - Upload MIBs prior to defining event rules to avoid having to rewrite the Event Rules.
- Web service API
  - Using a web service API for integration can reduce the number of Event Rules needed.
  - Use dedicated credentials for Event Management integration. Optionally, designate credentials specific to each event source.
  - Use cURL instead of Python, Perl, and so on.
  - Use ServiceNow REST API Explorer to produce code snippets for JavaScript, Perl, Python and PowerShell
  - Use Postman to test sending events.
- CloudWatch
  - Use dedicated credentials for integrating CloudWatch with ServiceNow.
- Email
  - Use email only if the source has a low volume and other options are not available.
  - Inbound actions will be easiest to manage if mail messages are in a consistent format

© 2017 ServiceNow All Rights Reserved

Tips on Alert Actions and Remediation

- Alert Action Rules
  - A scheduled job applies Alert Rules to new Alerts every 11 seconds. If an Alert Rule does not immediately start, allow 10–15 seconds before troubleshooting.
  - Use the Order field to control which Alert Rule runs if two Alert Rules have similar conditions set.
- Task Templates
  - Create a user called Event Management (or a similar name) so that the Created by field in a task template (for example, Incident) can be set to indicate that Event Management was the source of the task.
  - To perform any dynamic value assignment or to override OOB dynamic value assignment, use the EvtMgmtCustomIncidentPopulator script include.
- Remediation
  - Always set orchestration workflow properties to the Remediation Task [em_remediation_task] table.
  - You can test workflows by setting the table to [Global] and running them in the editor. Remember to set it back to [em_remediation_task].
  - Use ECC Queue and Workflow > Live Workflow > All Contexts to find more detailed information on remediation activities.

© 2017 ServiceNow All Rights Reserved

Wrap Up

© 2017 ServiceNow All Rights Reserved

Value Outcomes

Time Warner

99.2%

Reduction in Incidents to Events

"With ServiceNow, we're much more proactive. Because of this, we've actually reduced the number of high-impact incidents, and we're resolving them more quickly."

- Olga Krasovski, Director of Service Management

Zillow

< 100

Incidents per day

"By consolidating our monitoring and managing our events consistently, ServiceNow Event Management gives us the ability and confidence to take on new challenges."

- Seth Thomas, Director, Site Operations

TransAlta

80%

Reduction in Outages

"By the time our users notice a service issue, we've already told them about it and we're working on a fix"

– Jamie Duncalf, IT Operations Manager

© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Integrating event sources is not difficult, and typically a one-time activity

2

Alert automation can begin with creating Incidents, and progress to remediation

3

The unique ServiceNow® single platform enables you to achieve true closed-loop alert and incident management

© 2017 ServiceNow All Rights Reserved

Q & A

TONY BRANTON
SENIOR ADVISORY SOLUTION ARCHITECT
ServiceNow

© 2017 ServiceNow All Rights Reserved

Take the Survey

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

Thank You

Tony Branton

Senior Advisory Solution Architect

ServiceNow

© 2017 ServiceNow All Rights Reserved