servicenow

# Security Automation & Orchestration That Won’t Get You Fired

Syra Arif

Advisory Security Solutions Architect
ServiceNow
@syraarif

November 2017

# Speaker Introduction

**NAME:** Syra Arif

**TITLE:** Advisory Security Solutions Architect

**FUNCTION:** Security

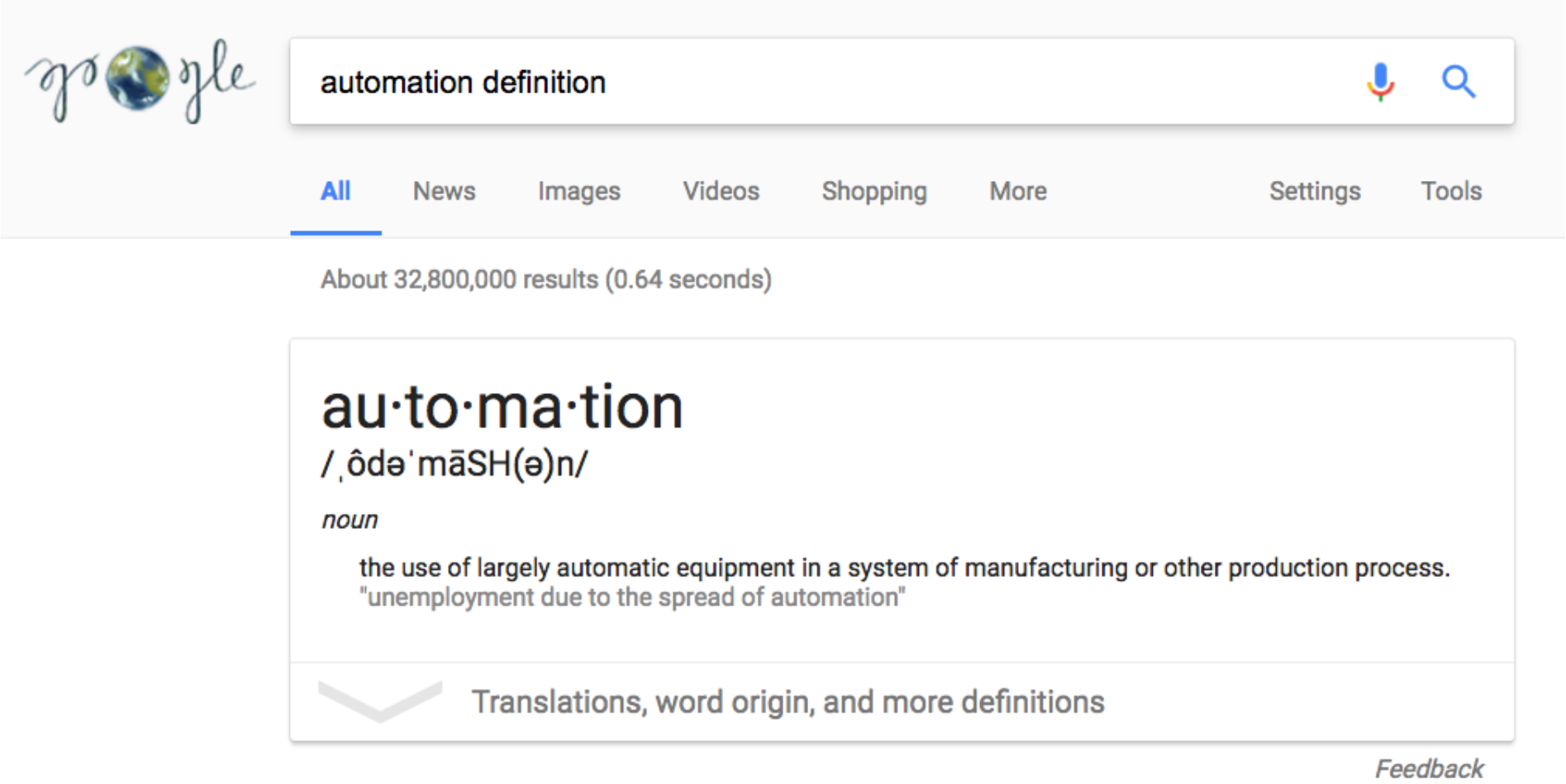
**COMPANY:** ServiceNow

**EXPERIENCE:** Diverse technical background including Governance, Risk & Compliance, Identity & Access Management, Security Operations

**EXPERTISE:** Bridging the gap between security & agility and focusing on the customer experience

**CURRENT PROJECTS:** ServiceNow Security Operations & Governance, Risk, and Compliance

# One in ~32 million definitions



# Only ~521K for Orchestration

Google

orchestration definition

All News Images Videos Maps More Settings Tools

About 521,000 results (0.54 seconds)

**or·ches·tra·tion**

/ˌôrkəˈstrāSHən/

*noun*

1. the arrangement or scoring of music for orchestral performance.
   "Prokofiev's mastery of orchestration"
2. the planning or coordination of the elements of a situation to produce a desired effect, especially surreptitiously.
   "the orchestration of the campaign needed tightening"

Translations, word origin, and more definitions

*Feedback*





servicenow

# Truth or Fiction

## Security and Risk Automation

All “runbooks” must be defined in advance

Our team, tools and processes are *“good enough”*

Automation is too hard

Automation will make my security team into robots

Workflow and Automation will solve everything

This is just a passing fad…





servicenow

# Is it Risky?

## “Automate and/or die” – Anton Chuvakin

HOW LONG CAN YOU WORK ON MAKING A ROUTINE TASK MORE EFFICIENT BEFORE YOU'RE SPENDING MORE TIME THAN YOU SAVE?
(ACROSS FIVE YEARS)

| HOW MUCH TIME YOU SHAVE OFF | HOW OFTEN YOU DO THE TASK: 50/DAY | 5/DAY | DAILY | WEEKLY | MONTHLY | YEARLY |
|---|---|---|---|---|---|---|
| 1 SECOND | 1 DAY | 2 HOURS | 30 MINUTES | 4 MINUTES | 1 MINUTE | 5 SECONDS |
| 5 SECONDS | 5 DAYS | 12 HOURS | 2 HOURS | 21 MINUTES | 5 MINUTES | 25 SECONDS |
| 30 SECONDS | 4 WEEKS | 3 DAYS | 12 HOURS | 2 HOURS | 30 MINUTES | 2 MINUTES |
| 1 MINUTE | 8 WEEKS | 6 DAYS | 1 DAY | 4 HOURS | 1 HOUR | 5 MINUTES |
| 5 MINUTES | 9 MONTHS | 4 WEEKS | 6 DAYS | 21 HOURS | 5 HOURS | 25 MINUTES |
| 30 MINUTES | | 6 MONTHS | 5 WEEKS | 5 DAYS | 1 DAY | 2 HOURS |
| 1 HOUR | | 10 MONTHS | 2 MONTHS | 10 DAYS | 2 DAYS | 5 HOURS |
| 6 HOURS | | | | 2 MONTHS | 2 WEEKS | 1 DAY |
| 1 DAY | | | | | 8 WEEKS | 5 DAYS |

Yes! But you are probably doing it today





servicenow

# Most Widely *KNOWN* Automation

- Intrusion Prevention Systems
- Anti-virus and signature updating
- The auto-blocking tools vendors warn that if you don’t automate you will make the cover of the NY Times
- These were poorly designed automation tools built with the best of intentions

# Crawl, Walk, Run, **Robot!**





servicenow

# Soo….What Can You Automate in the SOC? (Without Getting Fired*)

- Start with something simple, repetitive, important - and something that is going to save your analysts' time
- A typical phishing investigation can take about 20-30 minutes and requires a lot of manual steps
  - When not followed up on it can lead to large and costs infection
  - When following up you may miss other pressing issues
  - Initial (triage) research does not require a particular set of skills

* if you are fired for doing everything I outline here you have my sympathy but I surely am not to blame

# Start Passively

## Automate Process Lookups

- What is running?
- Is this normal?
- What is normal?

## Explode Malware in Sandbox

- Is there any reason for a human to be involved?
- Just report the results so an analyst can take action

## Pull Asset Records

- Who owns it?
- Where is it?

## Threat Lookups

- Have I seen this before?
- Has someone else seen it?

# Gate your automation as you mature

Disable Account: Only when confirmed to be compromised

Block on Firewall: Only block known infected systems

Reset passwords

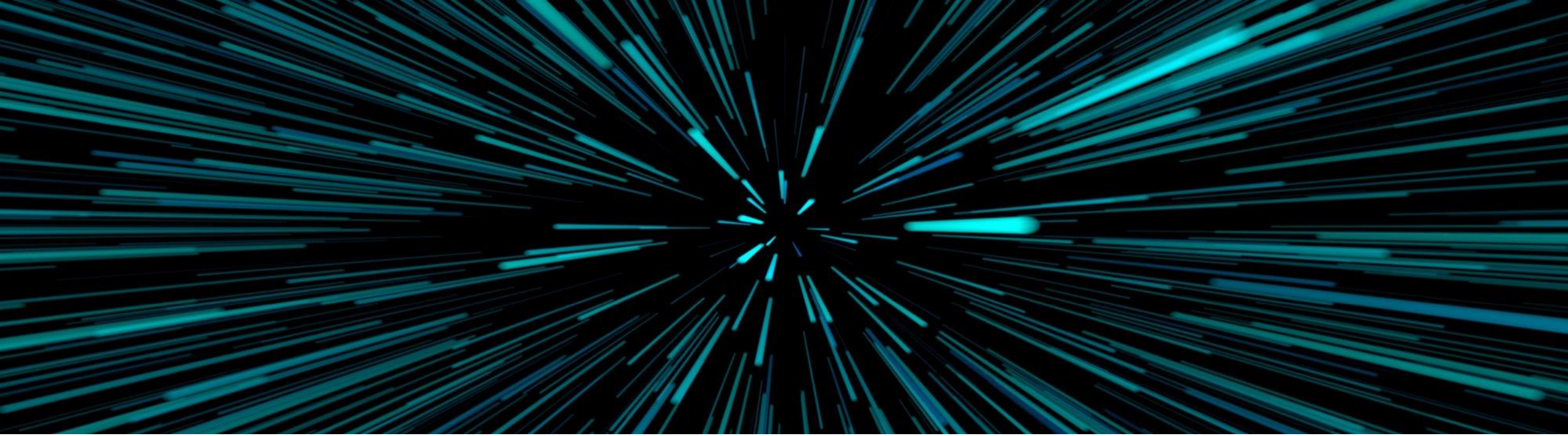
Delete phishing email(s)

Push button automation

# Go Active (after significant testing)

| Blocking | Disabling Accounts | Auditing Everything | Do More With the Same |
| --- | --- | --- | --- |
| • Can be disruptive but can also be undone quickly | • Can keep you out of the headlines | • Create change records for every automated task | • Automation allows your analysts to operate faster |

# Measure & Refine



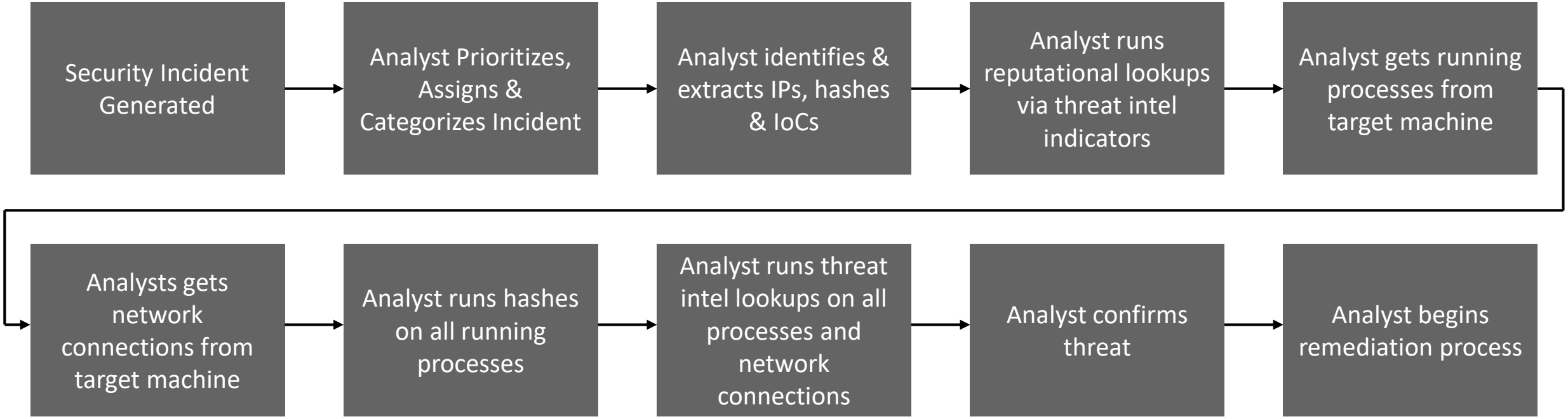
# Security Incident Response



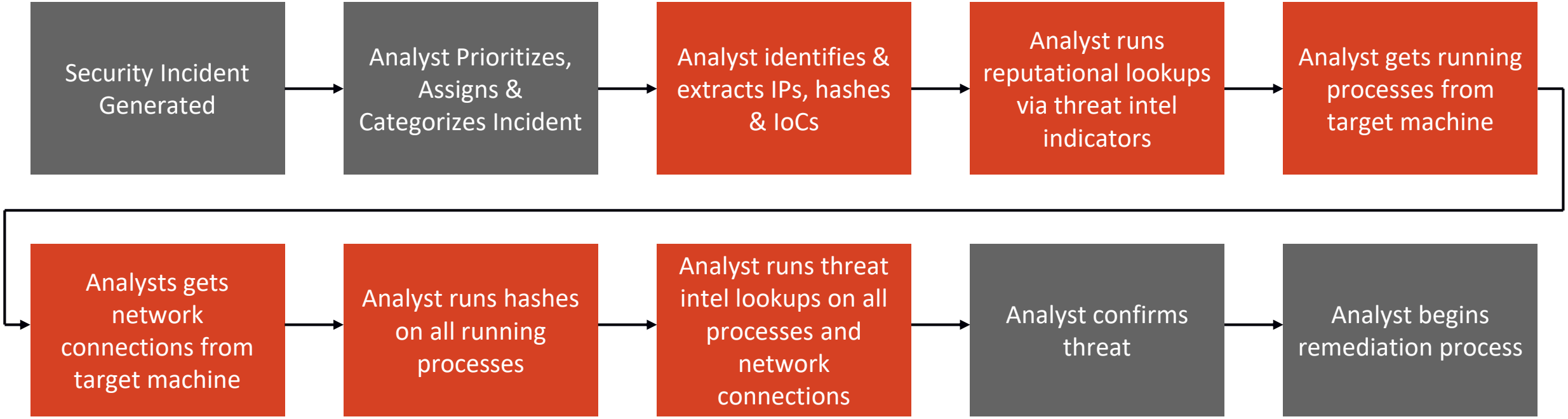


servicenow

# An Example: The Typical Incident Investigation Process



# An Example: The Incident Investigation Process with Automation

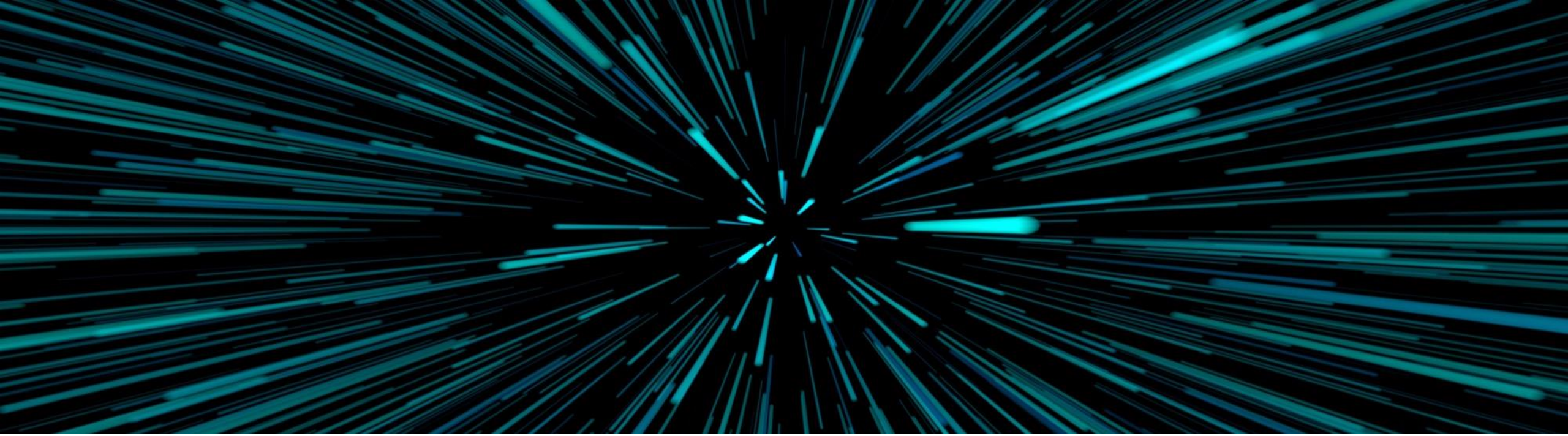



Red Boxes = Data Enrichment Activities





servicenow

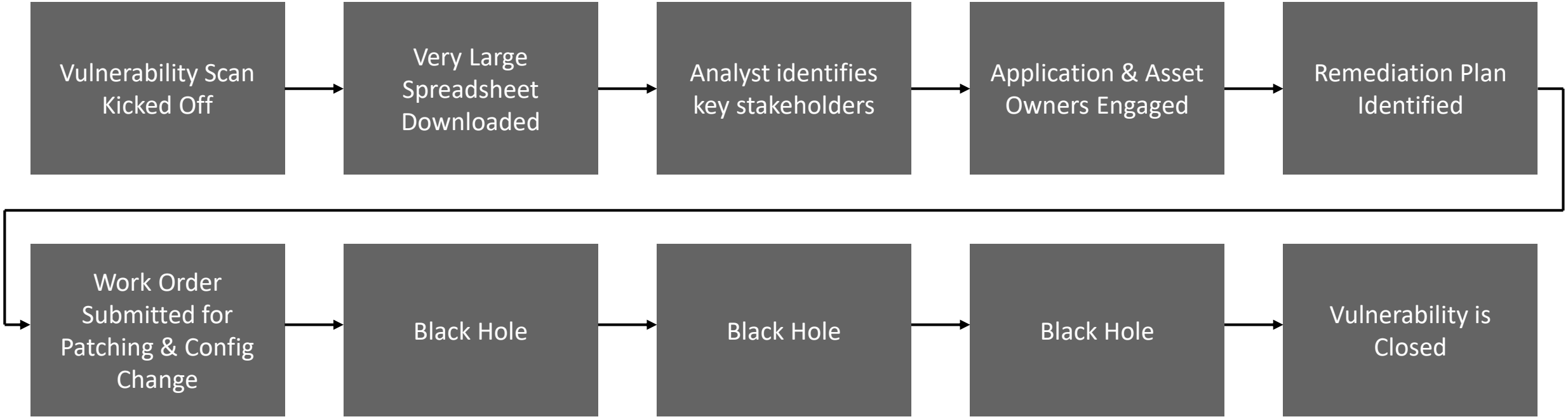


# Vulnerability Response

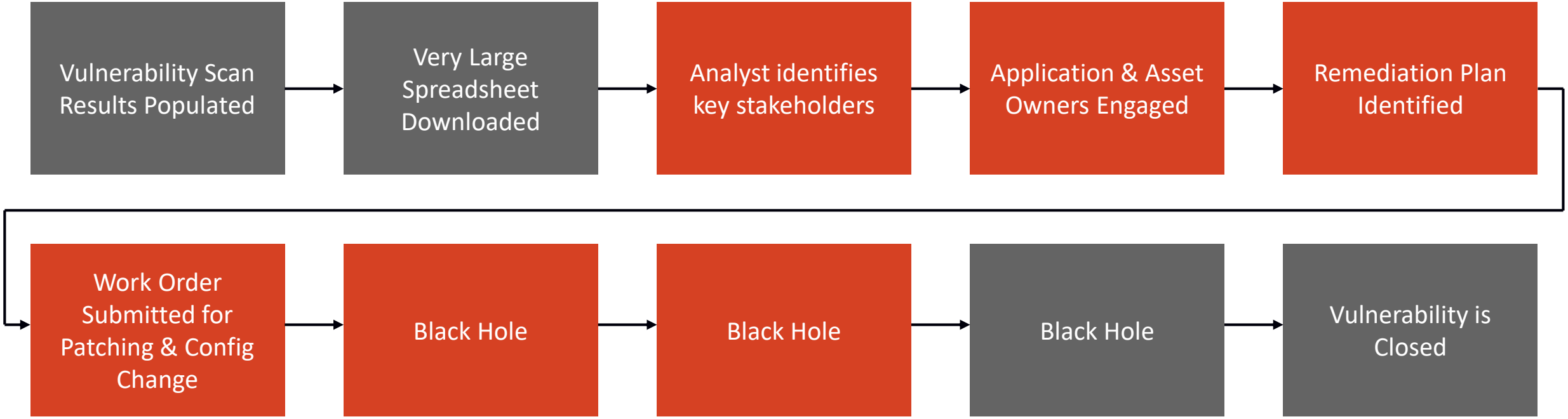
# How do I Automate Vulnerability Response?

- A key part of vulnerability response is Change Management
- Identifying & tracking the vulnerability lifecycle is tedious
  - When not followed up on it can lead to large issues later
  - Too many players across multiple teams
  - Knowing who is doing what is difficult when IT is responsible
- Automated Patch Management sounds awesome, but difficult when IT owns Change Management

# An Example: The Typical Vulnerability Response Process



# An Example: The Incident Investigation Process with Automation




Red Boxes = Spreadsheet Lookups & Black Holes with Limited Visibility into Change Management





servicenow

# Takeaways

1

Start passively

2

Grow to gated automation

3

Move to active (albeit carefully)





servicenow

servicenow

# Visit ServiceNow at Booth #608

https://www.servicenow.com/sec-ops

@syraarif