knowledge17

WORK at LIGHTSPEED™

Security Automation That Won't Get You Fired

MYKE LYONS
DIRECTOR, SECURITY BUSINESS UNIT
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Speaker Introduction



NAME: Myke Lyons

TITLE: Director, Security Business Unit

FUNCTION: Head of Security Strategy

COMPANY: ServiceNow

EXPERIENCE: 16+ years in IT / Security

EXPERTISE: Security, Ops, Cooking

ACHIEVEMENTS: Intra-preneur …

CURRENT PROJECTS: Driving process efficiencies. Automating all security and compliance work streams

© 2017 ServiceNow All Rights Reserved

Session Overview – Getting Started with Automation



Objectives

- Automation, how and where to begin

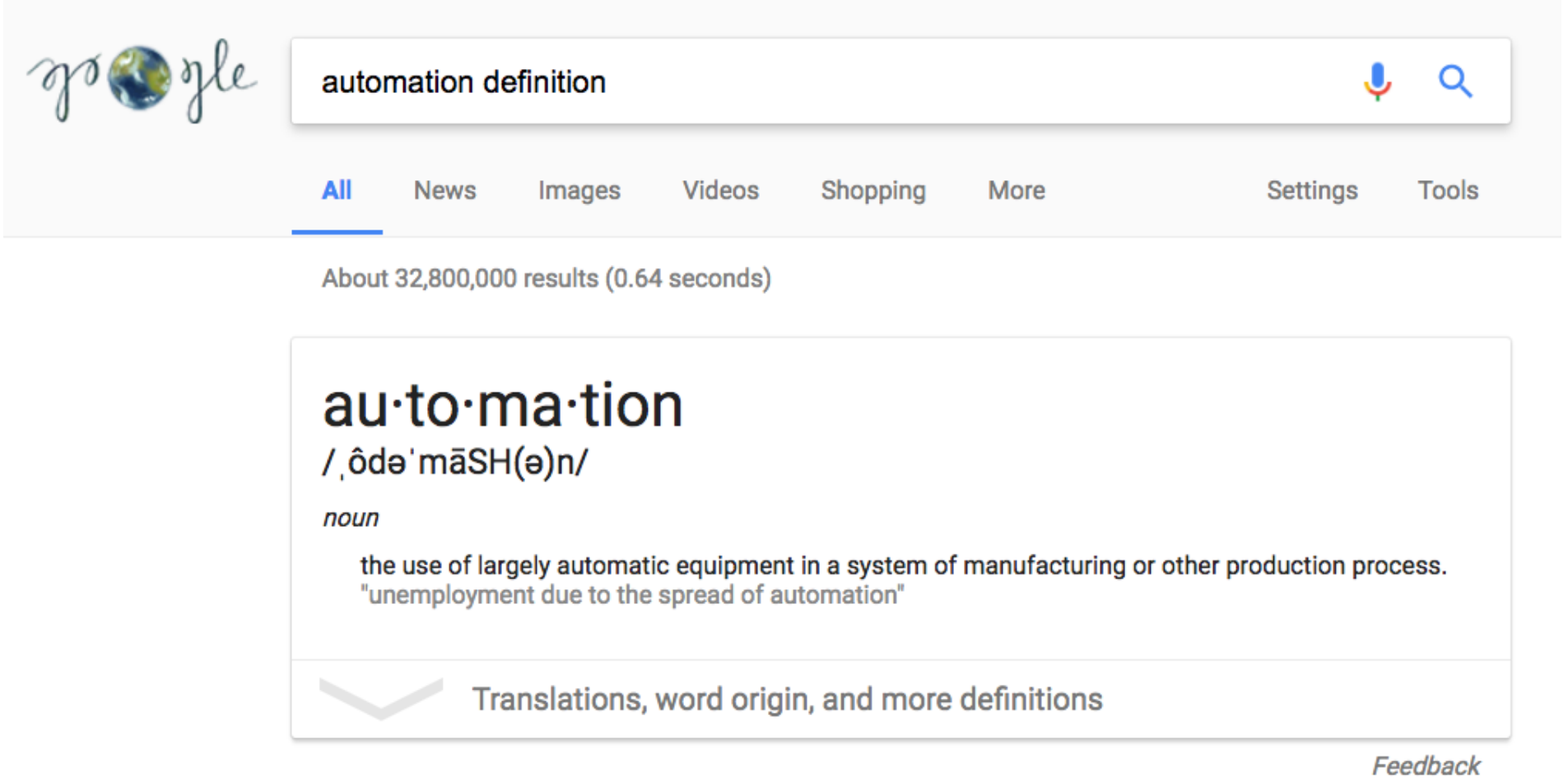


What You Will Learn

- Some of the definition(s) of Automation
- Learn about automating Enterprise Security Response
- Crawl, walk, run

© 2017 ServiceNow All Rights Reserved

One in ~32 million definitions

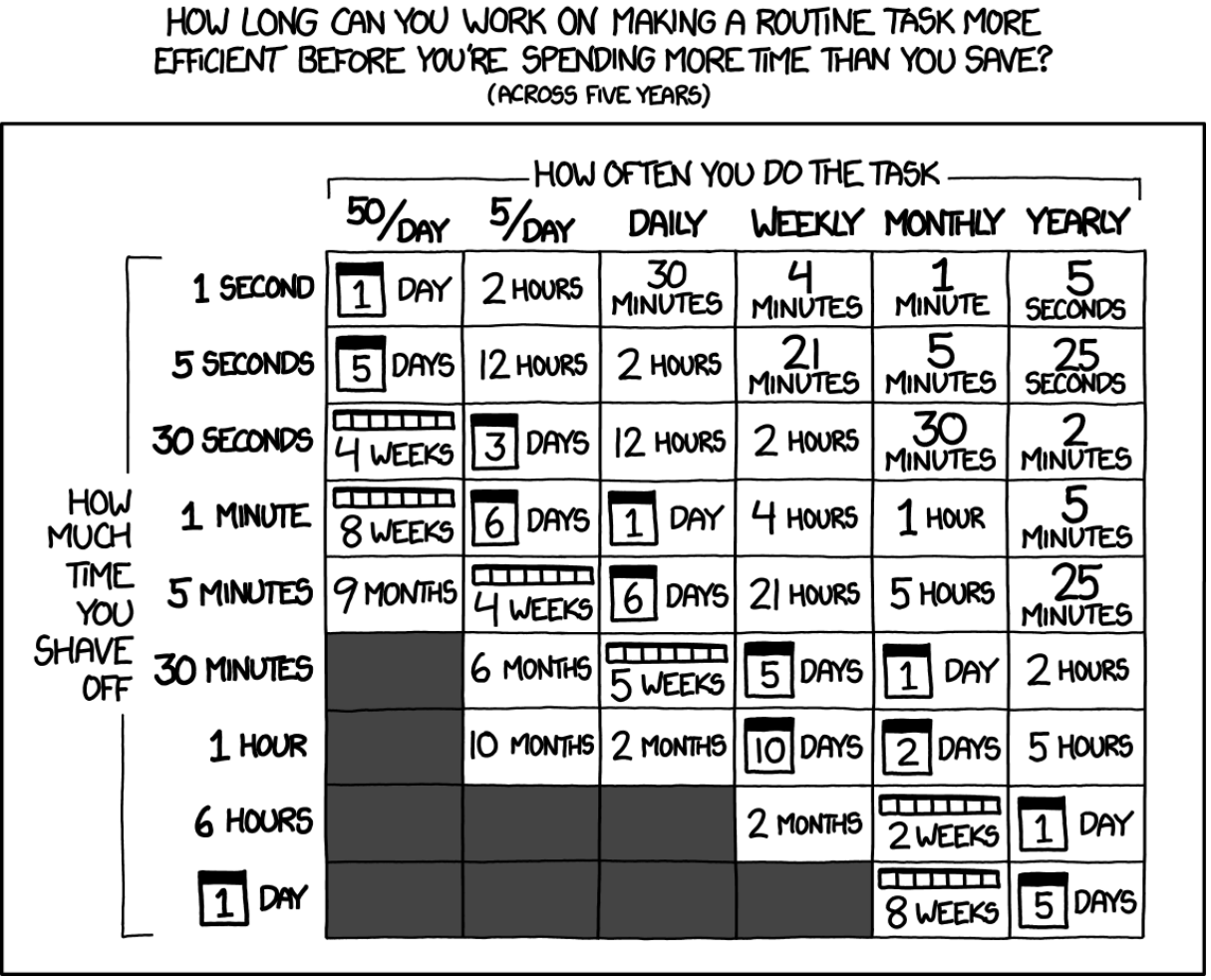


Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

Is it Risky?

"Automate and/or die" – Anton Chuvakin



Yes! But you are probably doing it today

© 2017 ServiceNow All Rights Reserved

Most Widely KNOWN Automation

- The most common automation story is auto-blocking an infected system
- The auto-blocking tools vendors warn that if you don't automate you will make the cover of the NY Times
- Most folks remember the heydays when IPS was taking down production business applications every Friday at beer o'clock
  - That of course is when the IPS appliance CPU wasn't at 100%
- Many of these were poorly designed automation tools built with the of best intentions

© 2017 ServiceNow All Rights Reserved

Crawl, Walk, Run, Robot





© 2017 ServiceNow All Rights Reserved

Soo….What Can You automate? (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

© 2017 ServiceNow All Rights Reserved

Start Passively

- Automate process lookups
  - What is running?
    - Is this normal?
  - What is open?
- Explode malware in sandbox
- Pull asset records
  - Who owns it?
  - Where is it?
- Threat lookups
  - Have I seen this before?
  - Has someone else seen it?

© 2017 ServiceNow All Rights Reserved

Grow to Human Stopgaps

- 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

© 2017 ServiceNow All Rights Reserved

Go Active

- Move to active after significant testing
- Blocking
  - Can be disruptive but can also be undone quickly
- Disabling accounts
  - Can keep you out of the headlines
- Audit everything!
  - Create Change records for every automated task
- Do more with the same!
  - Automation allows your analysts to operate at lightspeed

© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Start passively

2

Grow to gated automation

3

Move to active (albeit carefully)

© 2017 ServiceNow All Rights Reserved

Add Information on Upcoming Security Track sessions

© 2017 ServiceNow All Rights Reserved

Take the Survey

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

Thank You

Myke Lyons

Director, Security BU

ServiceNow

© 2017 ServiceNow All Rights Reserved

Q & A

MYKE LYONS
DIRECTOR, SECURITY BU
ServiceNow

© 2017 ServiceNow All Rights Reserved