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
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...
Is it Risky?

“Automate and/or die” – Anton Chuvakin

Yes! But you are probably doing it today
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!**
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**
- Can be disruptive but can also be undone quickly

**Disabling Accounts**
- Can keep you out of the headlines

**Auditing Everything**
- Create change records for every automated task

**Do More With the Same**
- Automation allows your analysts to operate faster

Measure & Refine
Security Incident Response
An Example: The Typical Incident Investigation Process

1. Security Incident Generated
2. Analyst Prioritizes, Assigns & Categorizes Incident
3. Analyst identifies & extracts IPs, hashes & IoCs
4. Analyst runs reputational lookups via threat intel indicators
5. Analyst gets running processes from target machine
6. Analyst begins remediation process
7. Analyst confirms threat
8. Analyst runs threat intel lookups on all processes and network connections
9. Analyst runs hashes on all running processes
10. Analyst gets network connections from target machine
An Example: The Incident Investigation Process with Automation

- **Security Incident Generated**
- **Analyst Prioritizes, Assigns & Categorizes Incident**
- **Analyst identifies & extracts IPs, hashes & IoCs**
- **Analyst runs reputational lookups via threat intel indicators**
- **Analyst gets running processes from target machine**
- **Analysts gets network connections from target machine**
- **Analyst runs hashes on all running processes**
- **Analyst runs threat intel lookups on all processes and network connections**
- **Analyst confirms threat**
- **Analyst begins remediation process**

Red Boxes = Data Enrichment Activities
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

1. Vulnerability Scan Kicked Off
2. Very Large Spreadsheet Downloaded
3. Analyst identifies key stakeholders
4. Application & Asset Owners Engaged
5. Remediation Plan Identified
6. Work Order Submitted for Patching & Config Change
7. Black Hole
8. Black Hole
9. Black Hole
10. Black Hole
11. Vulnerability is Closed
An Example: The Incident Investigation Process with Automation

Vulnerability Scan Results Populated → Very Large Spreadsheet Downloaded → Analyst identifies key stakeholders → Application & Asset Owners Engaged → Remediation Plan Identified

Work Order Submitted for Patching & Config Change → Black Hole → Black Hole → Black Hole → Black Hole → Vulnerability is Closed

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

1. Start passively
2. Grow to gated automation
3. Move to active (albeit carefully)
Visit ServiceNow at Booth #608

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

@syraarif