RAPID7

WHITEPAPER

Security Automation Best Practices

A guide to making your security team successful with automation

TABLE OF CONTENTS

Introduction

The best security postures are those that are built on efficiency and time-to-response. While processes make it possible to get a job done faster, creating ones that solve practical problems and result in measurable efficiency gains can be a time-consuming task, and without the expertise required to create and build them, they simply don't get done. This is where security automation comes in.

What Is Security Automation?

Security automation streamlines a series of repetitive, manual tasks into cohesive and automated workflows.

By plugging a set of tasks into an automated system (such as those involved in phishing investigations), security processes become:

- **More efficient**
- **Less prone to human error**

With increased efficiency, better and faster decisions can be made, which in turn can improve your organization's entire security posture. Even better, with repetitive and manual tasks taken care of by automation, security personnel can instead focus on more strategic work, which boosts their job satisfaction and ensures you're retaining good talent.

Security Automation: A Tough Nut to Crack

Historically, security automation has been difficult to implement, which is why many companies have yet to take advantage of it. Many security tools aren't built to play well with others. So without deep programming knowledge (a skill most security teams lack), building automation between tools has until recently been an impossibility.

And even if programming skills **do exist** within your company, it's not easy to pull in resources from across departments – at least not in a timely way.

If you do have access to programming resources, do you know what a well-defined process looks like? Knowing how to define a process is one challenge, and the others are finding the time to do so, testing its effectiveness, and then implementing it. Security teams often have far more urgent tasks to tend to, such as responding to malware infections, phishing attempts, or trying to patch the latest system vulnerability.

This whitepaper will serve as a practical guide for security teams on automation best practices. You will learn when automation is right for your organization, what tasks are best to automate, practical ways to begin implementing automation, and how to incorporate human decision points along the way.

Automation is on the fast track to maturation, and security teams may find themselves surprised at how easy it actually can be to set up and scale automated processes with the right tools. Read on for our four best practices to help ensure your team is set up for success.

BEST PRACTICE 1

Prepare Your Security Organization for Success

The two most important ingredients of security automation are: your security tools and the processes that tie them together to get a job done. So first, you need the right tools in place in order to leverage automation.

Security Tools

For security teams just starting out, the bare minimum tools to have include:

- **IntrusionDetection**
- **Firewall**
- **Ticketing**
- **Team Communication**

If you have the basics in place, the next layer of tools, which can tell you a much more complete story about your company's security posture, include:

- **Threat Intel**
- **Malware Analysis**
- **Forensics**

Security Processes

Once you have the right tools in place, you can start to define what security processes you need to get tasks done. The processes you should be focused on are the ones that solve practical problems — the ones your company most often faces — such as app vulnerability scanning, phishing investigations, and threat hunting. Every company is different as far as the threats they see most frequently and the data and systems that require the most protection.

In short your processes should:

1. **Have clear goals.**
   This should include the assets you're looking to protect and the threats you're protecting against.

2. **Address scale.**
   A process is best introduced when it can address issues of scale, such as triaging 1,000+ alerts a day.

3. **Be achievable.**
   Do you have the people, tools, and budget required to make the process possible? As an example, you might need one security analyst, one security engineer, a $200/month security monitoring tool, and a $100/month malware protection tool.

Next, lay out step-by-step the tasks involved in each of your most important processes. What needs to happen first? What tasks must occur in parallel? Where is human insight required?

Once you've mapped out the process, test it to make sure it achieves the intended goals. When you feel the process works (e.g. it's clear to everyone what to do and when), then move onto the next step — planning for implementation.

Don't know where to start when creating security processes? We got you.

Download our guide

Make a Choice: Build or Buy?

Do you have the resources internally to build custom automation, or will you need to look for a pre-built security automation tool? If you're one of the lucky few companies with a programming-savvy security employee or easy access to development resources, you may be able to do this in-house or with the help of consultants (this option can be a costly one, however).

If you decide to build automation in-house, make a plan and determine:

- **Scope**
  Are you orchestrating and automating a simple process, or an entire system? How long will it take? What does implementation look like?
- **Resources**
  How many programmers will you need? Will you need to hire consultants?
- **Environment**
  How many tools do you have? Do these tools have flexible APIs? What languages are they built in? What automation languages play nice with your current tools?
- **Budget**
  Based on scope, resources, and environment, what will the total project cost?

You'll also have to think about maintenance, especially when adding new tools or processes to your security operations. While not a part of the initial project, automation maintenance should be a consideration for building, especially as scale comes into the equation.

Of course, most companies have a hard time finding security folks, let alone those who also know how to code. And pulling a developer from engineering is either impossible or involves a long time table.

The reality is that most companies don't have the resources or bandwidth to build in-house and are better off investing in an automation solution.

If that's the case, you can look to security automation tools such as InsightConnect that are able to orchestrate security tools into a centralized location and automate processes using easy-to-build workflows. A security automation solution enables security teams to quickly build and maintain automated workflows without the development team's regular intervention.

It's also oftentimes more time-effective and cost-effective to use a security automation tool, as creation of automation is streamlined and maintenance is usually handled within the product and takes scale into account.

Things to consider when buying a solution:

Scope
How easy is it to connect my tools? How quick is it to add automation to my workflows? Does the tool suit the needs for my current processes? Is there ability for human intervention? Can it scale?

Resources
How many people need to be involved in setting up the platform? How many people will you need to build automation? How many people will you need for maintenance?

Environment
Will it fit into my current environment? Does it connect with my current suite of tools? How easy is it to update?

Budget
Considering the scope, resources, and environment, and compared with building, is it more cost-effective to use a solution?

As you decide which option is right for you — build or buy — consider running a test instead of proof-of concept (POC), which we explain in detail on page 11.

Add Automation When the Time Is Right

There is a right time to bring in automation and a wrong time to bring it in. The wrong time is, of course, when you don't havethe key tools in place and don't yet have a set of well-defined processes.

The time is right for automation when:

- **You have the right tools in place**
- **There is a set of tasks that are well-defined**
- **These tasks are easily repeatable and doesn't require human intervention**

These are also good signs that it's high time to automate:

- **The tasks take up too much time for someone to do manually**
- **You need to solve for the talent gap or can't afford more security hires**
- **Breaches begin to fall through the cracks**
- **The team is experiencing alert fatigue**
- **Problematically slow time-to-resolution**

In short, if your team is spending a lot of time on low-value tasks that are repetitive and there is a need to focus on higher value tasks, you're a prime candidate for automation.

Let's use the above formula to determine when to automate a common security task: malware analysis. Check out the table on the following page:

CRITERIA	EXAMPLE ANSWERS
Are the right tools in place?	**Yes**, we have malware analysis and ticketing in place.
Is there a set of tasks that are well defined?	**Yes**, once we receive an alert: gather intel, detonate file, and determine (a) is malware (then block hash and create ticket), or (b) is not malware (and take no action).
Are the tasks repeatable?	**Yes**, the tasks are similar for every malware investigation.
Do these tasks require human intervention?	**Yes** and **No** — the investigation doesn't, but if a threat requires deeper forensics, an analyst needs to get involved.
Do these tasks take up too much time?	**Yes**, they take up time we should be spending responding to these types of threats!
Do you have budget for more security hires to solve for this?	**No***, we don't have budget for another full-time security hire to do this with 3 analysts already on our team. Note: Security automation can help
Is your team experiencing fatigue from these alerts?	**Yes**, malware is a big problem for us; our team is spending 30% of their time investigating these alerts alone.
Is the time-to-response for malware threats getting worse?	**Yes**, alerts are starting to slip through the cracks and we're finding malware too late, risking our company's entire security posture.
CONCLUSION	Automate the complete malware analysis process

In this example, it's a clear win to automate malware analysis and response. By connecting your security tools with an automation system, which can gather this information and correlate it for you, your team can:

- **Eliminate handling low-level, repetitive tasks**
- **Solve for the talent gap**
- **Respond faster to threats**

In the Appendix, there is a blank worksheet of the chart above to use when analyzing the candidacy of security processes for automation. We recommend you conduct this exercise for all of your top security processes.

BEST PRACTICE 4

Know Which Tasks Are Ideal for Automation

Automation is not a cure-all and doesn't work for every single security task out there. There are times when human insight is critical throughout the process, or at a particular point in the process.

Here are examples when human insight must be a part of the process:

- **If you have to piece together insight from different data points and make a rational judgment call (e.g. "are these password failure alerts from a brute force attack or did someone forget their password?")**
- **If you are handling highly sensitive tasks (e.g. assigning Windows drivers)**

In short, if a task requires reason beyond what a machine can correlate, human insight should be a part of the process.

There are many effective ways to marry automation with human insight to ensure your team is focused on the most valuable tasks while automation picks up everything else. Let's take handling password failures as an example.

TASK	AUTOMATE OR HUMAN INSIGHT?
Collect password failure data and alerts from security systems	Automation
Decide if it's a brute force attack (response: block the IP) or if someone forgot their password (response: notify and help the user)	Human Insight

When a task requires human insight, a person is involved at a point in the process, and able to leverage intel that automation has already gathered so that they can jump right into analysis and response mode.

Testing Automation's Capabilities

If security automation is new to your organization, or you want to test it out on a single use case before fully rolling it out, it's smart to run a trial or test of an automation solution.

At this point, you will have either decided that automation can be built-in house or that you will be bringing in a security orchestration and automation product. Either way, a test ensures you can rapidly prototype security automation and demonstrate the value of it to your company before you invest more resources into it.

How to conduct a test:

1. Choose an automation system to test
2. Choose a use case that impacts your org regularly
3. Connect your tools and add your defined processes
4. Set a timeframe to test (e.g. 30 days)
5. Determine success criteria for the test, such as:
   a. 95% of tasks to be automated
   b. 30 minutes of investigation time saved per alert
   c. 80% increase in productivity across the security team

Assuming the test is a success, you can move forward with your security automation system of choice by building out all of your security use cases into automated processes. Remember to use the checklist in the Appendix and insert human analysis where appropriate. Automate what machines do best so humans can focus on what they do best.

Implementing Security Automation

When the time is right for automation, and if automation is executed successfully, it will be welcomed with open arms by security teams and the organization at large. Eliminating repetitive tasks gives team members time to not only respond to more events, but it also allows them to focus on important tactical and strategic work.

If you've ruled out building automation in-house, turn to a platform that does security automation and orchestration for you. Adding an orchestration layer will connect your systems, tools, and processes together, allowing you to quickly leverage automation without the setup and configuration hassle.

InsightConnect's orchestration and automation platform handles all of this for you so that you don't have to write even a single line of code. With a large library of built-in plugins and connect-and-go workflows, teams can create powerful machine-to-machine security automation, no code necessary.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on Twitter.

About InsightConnect

InsightConnect is a security orchestration and automation solution that enables your team to accelerate and streamline time-intensive processes without writing a single line of code. With 200+ plugins to connect your tools and easily customizable connect-and-go workflows, you'll free up your team to tackle other challenges, while still leveraging human decision points when it's most critical. With significant time savings and productivity gains across overall security operations, you'll go from overwhelmed to operating at maximum efficiency in no time.

Appendix

Security Automation Checklist

Security Process: _____

Criteria	Answer
Are the right tools in place?	
Is there a set of tasks that are well defined?	
Are those tasks easily repeatable?	
Do these tasks require human intervention?	
Do these tasks take up too much time from security personnel?	
Do you have budget for more security hires?	
Is your team experiencing alert fatigue?	
Is time-to-response getting worse?	
CONCLUSION	