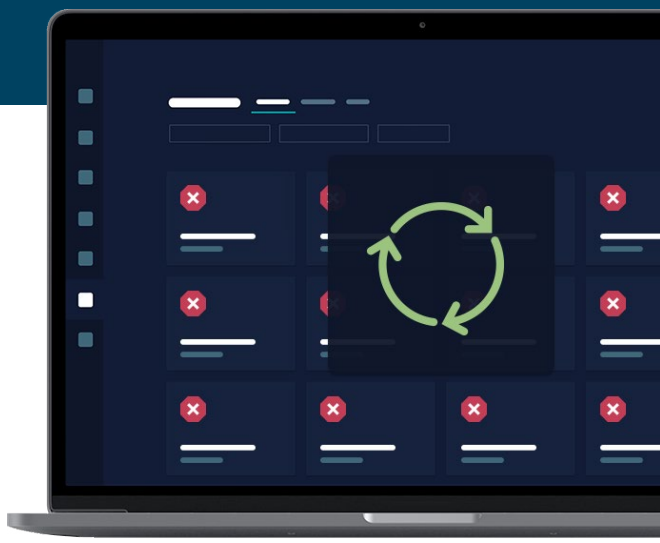
RELIAQUEST

Rethinking Security Automation:

Six Best Practices to Improve Visibility and Accelerate Response

Can automation solve security's "tool fatigue" challenge?

How to use automation strategically across existing investments to gain context and insights for faster detection and response



Introduction

There are tools for analyzing just about every type of security threat, and for collecting data that adds context to potential threat activity. The problem today is that there are too many tools, too little integration among them, and more noise than a team can analyze and understand – all of which add up to less visibility, less efficient security teams, and increased risk.

In a survey of senior security leaders conducted by 451 Research,[1] the inability to integrate security products was named the top challenge in security management. "A failure to integrate drastically reduces visibility across the environment and wastes time and manpower maintaining disparate tools, rather than consolidating insights from multiple sources into a single pane of glass," 451 Research reported.

Automation is supposed to solve the "too many tools" problem, surfacing the most critical issues by running playbooks and processes against common threats like phishing, and freeing up valuable resources for other tasks. But the reality is that expectations for automation have outpaced its capabilities to drastically reduce human intervention in security monitoring.

> **Enterprises are overwhelmed with security tools and the complexity they create. Can automation knit them together to improve threat visibility and accelerate response?**

[1] 451 Research, Tackling the Visibility Gap in Information Security, July 2019: https://www.reliaquest.com/resources/study-tacking-the-visibility-gap-in-information-security/.

In this paper, you'll learn:

- WHY organizations have high expectations for automation – and why they need to dial back or revise these expectations
- HOW the problems of "too many tools" and "too much data" negatively impact visibility into your environment
- HOW automation, applied correctly, simplifies threat detection and response and adds context to threats and workflows

Is automation making promises it can't keep?

Automation is still on the upward hype cycle, according to Gartner's 2019 Hype Cycle for Threat-Facing Technologies[2] – which means security teams too often expect stellar results from automation solutions with little expert oversight. The technologies most frequently associated with automation today are Security Orchestration, Automation, and Response (SOAR) systems.

The high expectations of automation as a security problem-solver fall into three categories:

1. USING AUTOMATION AS A REPLACEMENT FOR EXPERIENCE.

According to Gartner's recent market guide to SOAR solutions[3], buyers are seeking out automation features because they're short on staff. As the report notes, businesses see the need to automate repeatable tasks and streamline workflows, which can help them orchestrate security tasks at scale.

But there's a key qualifier, as the Gartner guide says, noting that while SOAR can give teams greater reach, it can't actually replace your security team. In other words, an organization needs mature processes and people in place if it is to get true value from automation.

Organizations may place too much confidence in the playbooks provided by automation vendors. But because every security organization is different, canned playbooks are rarely transferable from one team to the next. Playbooks need constant care and

> **Using automation intelligently requires a team's familiarity with runbook steps to identify opportunities for automation, as well as intimate knowledge of internal systems to enable and maintain integrations.**

[2] Gartner Research, Hype Cycle for Threat-Facing Technologies 2019, July 2019: https://www.gartner.com/en/documents/3947404/hype-cycle-for-threat-facing-technologies-2019.
[3] Gartner Research, Market Guide for Security Orchestration, Automation and Response Solutions, June 2019: https://www.gartner.com/en/documents/3942064/market-guide-for-security-orchestration-automation-and-r.

feeding to ensure they are working properly – it's not a case of "set it and forget it." To the contrary: Technologies and threats are constantly changing, and therefore, so must the playbooks.

This is why teams need the knowledge to personalize runbooks and translate the steps into orchestration engines.

2. FOCUSING ONLY ON THREAT CONTAINMENT OR MITIGATION.

Automation certainly helps security organizations diagnose and stop threats. The mistake is in assuming mitigation is all that automation can do, and not applying automation's features to other types of high-value tasks. **Automation used only for mitigation presents a missed opportunity to gain context and intelligence around threats – knowledge that can be used to prevent future threats from gaining traction.** In addition, collecting contextual data is often a repetitive task in investigative response that aligns well with automation.

Automatic mitigation is challenging to use, because security teams worry that by automatically blocking IP addresses or disabling users, they'll interfere with legitimate business processes. If you have concerns about using automation for mitigation, why not apply it to more benign tasks to help expedite threat qualification and root cause determination?

3. TRYING TO USE AUTOMATION AS THE "CONNECTOR" FOR DATA SOURCES.

Automation has also been talked up as the answer to the orchestration problem – that is, aggregating data from systems and process alerts, and adding visibility that was lacking across disparate security solutions.

But while SOAR solutions can aggregate alarms and then orchestrate response processes, they are rarely collecting large sets of data across multiple technologies like SIEM, EDR, cloud services and third-party apps to enable single-source investigations.

Nor are they making the data easy to consume, or normalizing it. This is a key missed opportunity to become the "connector" for data sources, forcing security teams to spend additional time and resources to try and make sense of all the data returned.

The corollary to the "too many tools" problem is the "too much data" problem – data contained in a so-called "data lake." It's a problem that organizations hope automation can solve. In 451 Research's survey of senior security leaders, 49 percent said that their investments in SIEM (security information and event management) and endpoint detection and response systems overwhelm their security operations capacity.

The goal of the enterprise "data lake" – that is, understanding the data available and what it's telling the organization– isn't easy to achieve. There are many challenges, such as collection methods, processing, storage requirements, and licensing inhibitors. There are also logical reasons organizations choose not to collect security data in a single repository, such as incompatible data formats and admin overhead. Even if a team selected just two security solutions – a next-generation firewall and an endpoint detection and response system – most organizations will choose not to send every network detail and every endpoint detail to their SIEM solution.

The result is that even with just two security products, workflows are already impaired. Teams are required to bounce back and forth between the different repositories and tool-specific workflows.

Organizations that try to funnel all data into a single, searchable repository find that the solutions are usually expensive and require yet more time and staff to maintain them. That defeats the purpose of seeking out tools that automate security and generate data, since security teams are trying to get by with less staff and more streamlined budgets.

> **Organizations that try to funnel all data into a single, searchable repository find that the solutions are usually expensive and require yet more time and staff to maintain them.**

The result is a growing amount of detail within disparate security tools that never make it to the single, searchable data lake, generating "data ponds". These "data ponds" hide relevant information to an investigation. Automation engines demand detailed requests, which means teams receive responses with highly specific and limited data from the data lake– as opposed to a broader set of data around a threat event that sheds light on attackers' methods and mitigation tactics.

Even if teams can extrapolate data from several disparate sources focused around the activities of a specific threat, they must rely on manual methods to consolidate it or make it usable, such as exporting the data into common formats like CSV or into a NoSQL database. But data incompatibilities and administrative complexities still crop up. And the monumental task of normalizing the data remains.

Best practices for addressing security challenges through automation

Used correctly, automation removes the repetitive and mundane tasks that hinder focus on threat investigations. Automation can also uplevel security when it's used for more than simple task management. It can cut through the alert noise so that security teams can focus on learning about threats and applying that knowledge to develop new threat mitigation strategies and protect the business.

1. APPLY AUTOMATION TO WHAT YOU KNOW – NOT WHAT YOU DON'T KNOW.

Use automation for specific processes that you know and trust, instead of applying it to every source in the environment. Automation not only requires intimate knowledge of incident response processes, it also requires insight and access into the integrated systems. For example, if the desired automated process is to trigger a vulnerability scan on a target host:

- Is there a supported API available that can programmatically trigger a scan?
- Is there knowledge of the correct API call to trigger a scan?
- What inputs does the API require?
- Does the security team have API credentials?
- What activity warrants a scan to be triggered?
- How will scan results be collected or returned, and in what format? How will this format align with the other data you have?
- Does triggering a scan require oversight outside security?
- Are any hosts considered off limits to a scan? If so, how will you account for them?

As you can see, even apparently innocuous steps to gather contextual information about hosts become challenging without a deep understanding of the process you want to automate, your organization's policies, and the system you are integrating.

2. PUT DATA INTO CONTEXT.

Instead of relying on manual sifting and parsing of data, deploy automation to correlate data from across multiple sources, and separate relevant alerts from irrelevant data and false positives. Automation normalizes data into a view that helps security teams make better decisions and removes the blind spots that are barriers to decision-making.

With this normalized view, teams gain context around workflows. This provides the background for choosing which plays to run against which attacks.

3. TAKE LOW-HANGING-FRUIT TASKS OFF THE TABLE.

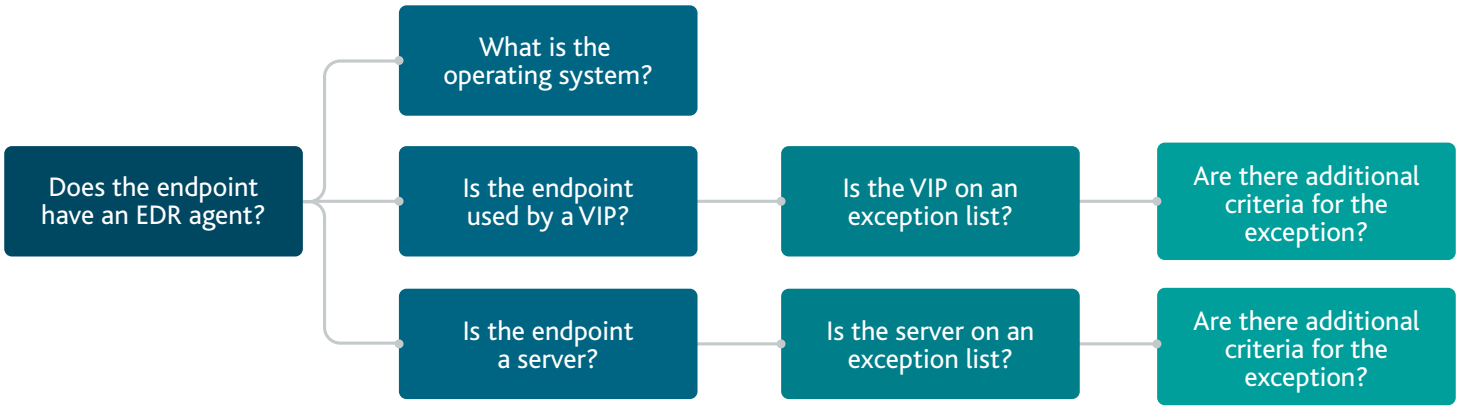
To free up security experts for strategic projects, apply automation to remedial tasks such as enriching data to help provide additional context around threats as well as entities (including users, devices, and apps). Automation shouldn't be used to replace security professionals: It should be used to allow these professionals to flex their decision-making muscles.

4. ACCESS THE BEST DATA FOR SPECIFIC INVESTIGATIONS.

Using a normalized view, automation can fetch data for the chosen investigation, creating a unified presentation layer and applying consistent filtering to enable faster analysis and response times.

5. CREATE A DECISION MATRIX.

Let's say a team's task is to quarantine a host via an endpoint detection and response (EDR) solution. Here is a sample of questions automation needs to account for:



A good automation solution incorporates these decisions into its playbook actions to remove manual effort by the analyst.

6. DEPLOY MORE PLAYBOOKS WITH LESS MANAGEMENT OVERHEAD.

As Gartner notes, organizations want to use automation to fill in skills gaps. However, current automation tools still require code development to create plays and playbooks. For example, while the SOAR solution "invokes" automation, the development and maintenance of SOAR code falls to the customer. But security professionals are not programmers. An automation toolkit should not require security professionals to develop and maintain their own code, but instead should focus on what play to run and when.

> **An automation toolkit should not require security professionals to develop and maintain their own code, but instead should focus on what play to run and when.**

The next steps for enterprises

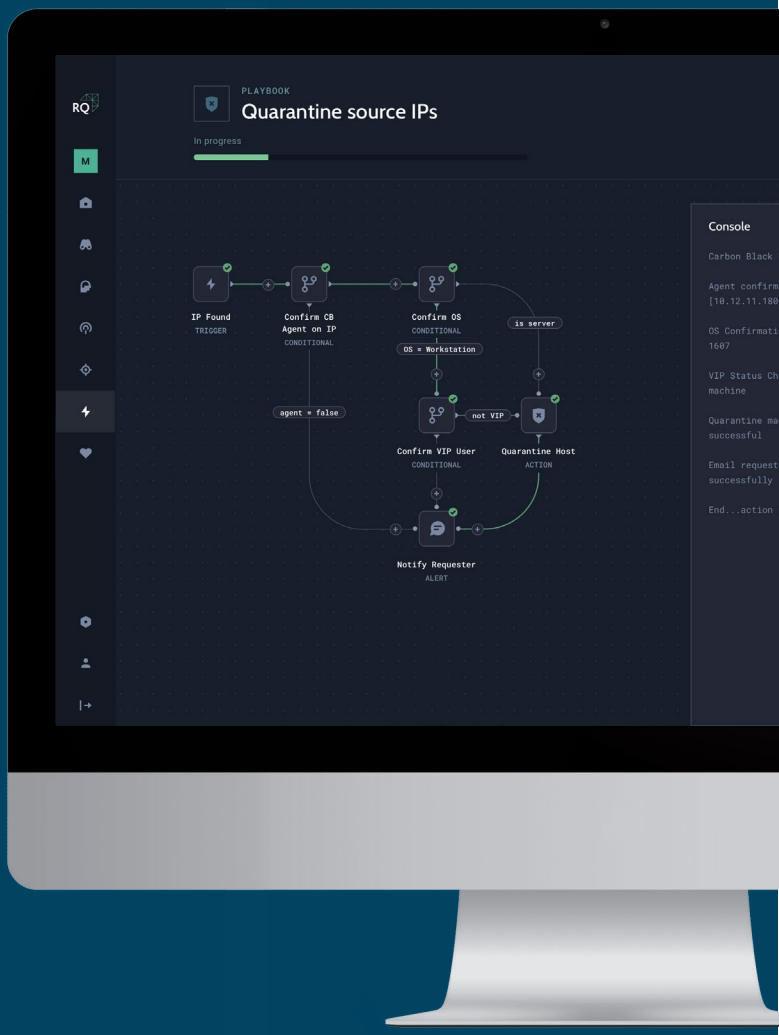
For organizations looking to adopt automation to improve security instead of complicating it, these steps can accelerate adoption.

1. If you haven't already, create runbooks for commonly seen threat types. Start with threats for which you have high confidence in alerting.
2. Review your runbooks to inventory each system accessed or touched.
3. Find common systems across your runbooks, and discover which systems are used the most often.
4. For those systems not owned directly by security, start conversations with owners sooner than later.
5. Assess the level of difficulty in developing and maintaining an integration. For example, what could change? Who is the contact if the integration is broken?
6. Develop automation for low-effort integrations that occur the most often.
7. Use automation to mitigate threats based on alerts in which you have high confidence. Keep in mind that you may not need to automate everything from start to finish; some automations may still require human interaction.

How ReliaQuest Improves Visibility & Accelerates Response

ReliaQuest fortifies the world's most trusted brands against cyber threats with GreyMatter, its platform for proactive security model management. GreyMatter increases enterprise visibility while automating threat detection and response. It does this by unifying and integrating existing SIEM, EDR, multi-cloud, and third-party apps to deliver a centralized, transparent view across the environment. The platform's analytics provide actionable reporting and metrics that measure ongoing improvement of the security model, so teams can recognize and communicate success across the environment.

With ReliaQuest GreyMatter, playbook implementation is streamlined through our orchestration engine to deliver tailored actions with certified integrations into your security controls like EDR, multiple cloud tools, and third-party apps. Understanding your environment is complex and programming is not your forte – receive personalized playbooks tuned to your environment, with continued validation, so you can concentrate on higher-level decision-making and responding to critical threats. ReliaQuest GreyMatter increases transparency and provides a detailed record for every executed playbook.



ReliaQuest applies automation to enable enterprises to expedite incident response with playbooks designed and tested to work with each organization's unique infrastructure.

LEARN MORE ABOUT RELIAQUEST GREYMATTER

RELIAQUEST

Make Security Possible™

(800) 925-2159 www.reliaquest.com info@reliaquest.com

Copyright © 2018 ReliaQuest, LLC. All Rights Reserved. ReliaQuest, RQ, and the ReliaQuest logo are trademarks or registered trademarks of ReliaQuest, LLC of its affiliates. All other products names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. All other information presented here is subject to change and intended for general information. Printed in the USA.