tines

The essential guide to workflow automation

for security teams

including AI-powered automation

Contents

A word from Eoin Hinchy
CEO and co-founder, Tines

In my 15 years as a security practitioner, both working on incident response and overseeing security teams, I saw a major problem: too much work and not enough staff. More specifically, I saw overworked staff doing repetitive, mundane tasks leading not only to burnout, but to human error that could cost a company millions.

What we needed was a way to get away from monotonous tasks, and focus on projects that could add value to the organization, and put security analyst and engineer skills to better use.

The solution? Workflow automation, which gives teams the tools to automate processes like phishing attack responses, suspicious logins, vulnerability management, and even employee onboarding and offboarding with a few drag-and-drop actions.

Workflow automation has the potential to save teams thousands of hours of work, freeing them up for high-impact projects, and improving total productivity.
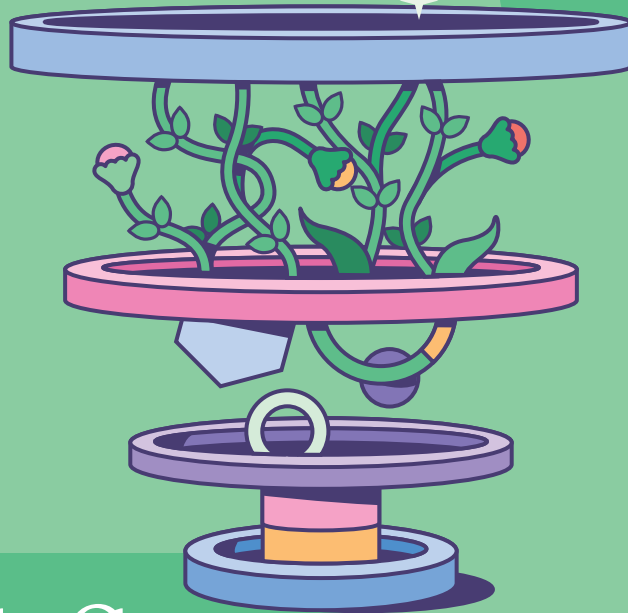
And with recent technology advancements, this potential has never been greater. AI is uniquely well-suited to workflow automation. Of course, there are very real concerns around privacy, security, and usability. But it's exciting to see that, when done correctly, implementing AI in workflow automation can make workflows easier and faster to build and run, while keeping your data private and secure.

We wrote this guide to serve as the ultimate resource on workflow automation. We'll run through its evolution, explain why this technology is critical for security teams, outline how you can bring the power of workflow automation to your team, and share best practices. I hope it inspires you to embrace workflow automation as a solution to your team's biggest security challenges.

→ Learn more about how we're empowering security teams to build AI-powered workflows: tines.com/ai

> "Workflow automation has the potential to save teams thousands of hours of work, freeing them up for high-impact projects, and improving total productivity."

Why do we *need* workflow automation?

Workflow automation makes it possible for everyone on the team, regardless of their technical skill, to build, run, and monitor their most important workflows. Traditionally, this meant the introduction of coding and scripting. But this is rapidly being replaced by no-code and natural language solutions like Tines. These solutions offer a visual interface for building workflows.

Dragging and dropping actions into a workflow, team members can turn processes built on repetitive, manual tasks into hands-off workflows that only loop them in when their judgment is required. By embracing workflow automation, teams can operate more effectively, mitigate risk, reduce tech debt, and focus on the work that matters most.

"A workflow approach that enables automated tasks (e.g., the automation of steps in a marketing campaign or a sales process) to be performed."

GARTNER'S DEFINITION OF AUTOMATED WORKFLOW MANAGEMENT

Phase 1 **Automation as a feature**

Security automation started as a feature of larger software solutions like RSA Archer that could automate tasks like data collection and reporting in a single dashboard. It allowed for little customization for organization-specific needs, meaning that automation wasn't available across all workflows, but only for what the tool's features allowed.

Phase 2 **Emergence of SOAR tools**

As demands on security teams became more complex, so did the number of technologies and solutions needed. Increased tools came with increased alerts, placing further strain on the team's time. First-generation SOAR tools addressed these needs, but building workflows capable of handling a variety of tools and use cases proved challenging and costly. While these platforms created a single place to manage and monitor workflows, they still relied heavily on a deep understanding of code to power them.

Evolution

Phase 3 **Low-code and no-code automation**

Low-code and no-code automation reduced the need for coding skills, allowing non-developers to build automated workflows using simple drag-and-drop interfaces. Suddenly, automation was accessible to everyone on the team.

There was just one problem. No-code automation platforms varied wildly in capability, from lightweight no-code platforms like Zapier, which are great for basic tasks, and by extension non-technical teams, to platforms like Tines which can handle the massive

complexity that security teams encounter. This led to what's known as automation sprawl, when various teams implement their own automation solutions without proper coordination, resulting in siloed processes, integration challenges, and a lack of visibility.

Phase 4 Natural language workflows

The evolution of AI and LLMs marks a natural progression in workflow automation accessibility. Moving from low code to no code to natural language allows everyone on the security team to start building quickly. The learning curve has flattened, and the user's ability to build accelerated. The best workflow automation platforms allow users to employ a private and secure language model to help them build their workflows. They can also author data transformation with all the power of code, without the need to read or write it.

With workflow automation, the person closest to the problem has everything they need to build the solution. Barriers to entry have never been lower and the potential impact across our security teams has never been greater. And it's not just good news for the less-technical team members. Natural language is the ideal way to work together as a team because it allows everyone to literally speak the same language.

What's next? Hyperautomation

With more and more automation programs reaching an advanced stage, new security challenges emerge. When automation is siloed across different departments, it not only makes it harder to manage the organization's security program, it can create new vulnerabilities as less-technical employees embrace the technology. This is where hyperautomation comes in.

Described by Gartner as, "the orchestrated use of multiple technologies, tools or platforms, including artificial intelligence (AI) and machine learning…", hyperautomation allows organizations to automate at the highest level of effectiveness. It provides security teams with critical visibility over automated processes across teams and departments, and the opportunity to build workflows that connect multiple departments. The result? Robust, integrated processes that optimize resources and make it easier to improve security across the organization.

> "With workflow automation, the person closest to the problem has everything they need to build the solution."

tines

81% of security practitioners say their workload has never been higher

VOICE OF THE SOC REPORT

Benefits

Incident readiness

When a security incident occurs, the demands on security teams are huge. A calm and well-functioning team beats an overworked one every time.

But creating this kind of working environment is easier said than done. According to the Voice of the SOC report, 81% of security practitioners say their workload has never been higher.

In damage-control moments, minutes and even seconds count enormously, and already having automated workflows in place frees your team to turn their full attention to responding to and resolving the incident. They can also collect information and context about an incident in seconds, and know when to alert a human for more critical decision-making.

Faster time to value

With workflow automation, processes that typically took days or weeks to complete can be reduced to minutes or even seconds, thus significantly increasing time to value. Workflow automation also reduces project management needs, communication burdens,

unnecessary feedback loops, and other extra steps that can be condensed with automated workflows. With over 500 cyber attacks being logged every second globally, increasing speed across the security team is crucial.

Significantly improved retention

The Voice of the SOC report found that 63% of practitioners experience some level of burnout, and that spending time on manual tasks is the most frustrating aspect of their job.

No one wants to do boring and menial work, and team members who burn out through mind-numbing toil simply leave their jobs. When low-level tasks are automated, security teams can focus on the high-impact work that drew them to the profession in the first place, whether that's threat hunting, risk management, or incident response.

63% of security practitioners experience some level of burnout

VOICE OF THE SOC REPORT

Fewer mistakes

Mundane work isn't just bad for humans – humans are bad at it, too. Hours of menial, repetitive work increases the likelihood of error, which increases the chances of a security incident. Gartner predicted that lack of talent or human failure will cause more than 50% of significant cyber incidents by 2025.

Automated workflows function predictably and consistently, reducing false positives and false

negatives. Workflow automation also reduces error because the practitioners who are most familiar with the processes are the ones actually building, running, and monitoring the workflows. The data backs this one up – in a study by IDC, 79% of respondents said that automation helped them reduce errors or mistakes.

A culture of secure automation

When we remove the need to rely on other teams when building workflows, the potential for automation across the organization grows exponentially. For example, a security analyst builds a Slack-based chatbot for a threat intelligence workflow, which can then be used by their colleague in IT for their employee offboarding workflow.

I've witnessed many teams with access to workflow automation have that light bulb moment and realize, 'We could automate this!', then immediately start building the new workflow, allowing for more innovation and quicker application.

→ Learn more about the challenges and opportunities for security teams, in the Voice of the SOC, our survey of 900 security professionals: tines.com/soc

Common misconceptions

Misconception:

"I could just write a script for this."

You *could* just write a script – if you know how to. But security practitioners often don't have that skill, meaning they have to outsource their automation to others. Additionally, the easy part with code is writing it the first time. The hard part is the deployment, security upgrades, maintenance, versioning, and downtime that comes afterward. This is especially challenging when your best team members move on to other organizations (and at least some of them will, very soon – 55% of security practitioners say they're likely to switch jobs in the next year.)

The right workflow automation platform encourages collaboration and ensures that any number of team members can step in when required. Technical users who do know code can instead focus on the output of the overall workflow, rather than the process of coding it.

"The best workflow automation platforms make it easy to put a human in the loop for important decisions."

Misconception:
"This isn't powerful enough for our workflow."

Workflow automation platforms provide security teams with the building blocks they need to power their most important workflows, from simple unrecognized login alerts to complex, all-encompassing vulnerability management.

There's no limit to how complex the workflow can be or how many steps can be automated – if you can imagine it, you can do it.

Ideally, your platform allows your workflows to scale automatically to meet your specific requirements. And it has a robust set of trust and security capabilities – role-based access control, audit logs, version history, error handling, credential management, and approval-based change control – to keep your workflows secure.

Misconception:
"Managing integrations is painful."

We've reached a point where teams are turning away from multi-product platforms towards laser-focused tools that provide best-in-class solutions, like JIRA, Slack, and others.

This means that connecting the tools in your stack has never been more important. When your organization's tools – custom and off-the-shelf – talk to each other, you can maximize your data and resources.

Best-in-class workflow automation platforms make it easy to integrate across your tech stack.

Misconception:
"Automation will implement rash decisions during remediation."

Automation isn't necessarily all or nothing, as many may assume. The best workflow automation platforms make it easy to put a human in the loop for important decisions. The same is true for any AI-powered capabilities within these platforms.

Instead of automating black and white remediation actions like blocking an account after a suspicious login, these workflows ask the affected user or an analyst for their input first. This can easily be facilitated through automated Slack messages or chatbots – "Did you recently log in from a certain location?" – and implementing actions based on their response.

Misconception:
"Automation means replacing team members."

From what I've seen, this very rarely happens in practice. Firstly, there's always more work to do and bigger problems to solve. The security landscape is ever-changing and these teams need to constantly adjust and improve in order to keep pace.

It's far more common to see benefits for team members once they start building their own workflows. They gain a valuable new skill, the ability to create efficiencies across the security team and enhance key processes.

As they begin to automate their repetitive, manual tasks, it frees them up to focus their skills and attention on high-impact work like improving the organization's security posture.

Additionally, because of the ease of using workflow automation, builders can maintain and evolve their own workflows, which is especially beneficial as processes, tools, and threats continue to evolve.

Automation simply unlocks the potential of team members – and team members who are engaged in and excited by their work stick around.

Case study
Elastic

elastic

Elastic is the leading platform for search-powered solutions. The InfoSec team at Elastic deals with a high influx of alerts, noise, and false positives, but, until recently, they carried out little to no automation. Let's look at what happened when they started using workflow automation platform Tines.

BEFORE TINES

- Little to no automation on InfoSec team, automation was done through time-consuming Python scripts

- Unscalable systems for alert management

AFTER TINES

- 49 automated workflows and counting, for threat detection, alert investigation, and more

- Scalable processes

- Reduced alert fatigue

- 750 days of analyst time recovered annually for more impactful work

Key workflow: alert investigation and triage

The Elastic team use this workflow to create, enrich, and distribute Elastic SIEM alerts to their analysts via Slack. One week after kicking off this workflow, the team found that they had processed the same amount of work that would have taken them 93 days previously.

→ Read the full case study: tines.com/elastic

"Tines is doing the work of at least three FTEs and, most importantly, is allowing us to be more thorough in the work that we do."

DANIEL GALLAGHER, SECURITY AUTOMATION ENGINEER

ELASTIC

Embracing
workflow
automation

tines

In thinking about a more sustainable, scalable future for your team, auto-mation is going to be the most important strategy you could implement.

When your team members have the tools they need to automate repetitive tasks, they're not only creating more efficient workflows for everyday processes, they're freeing up their time to do what they love, whether that's security analysis or compliance management.

Getting started

Start small and experiment with core use cases

Leaders often fear they don't have the bandwidth or tooling in place to fully leverage automation. Or, if they adopt automation, they want to automate all their processes immediately. Cloud-based workflow automation platforms offer you the freedom to start small with free community editions or trials and grow as your business needs evolve. You can start with a set of core use cases and demonstrate their value before expanding.

Setting your teams up for success

Think about whether the time is right to build an internal SOC

The days of having a SOC as a standalone team responsible for security are coming to a close. Not only have their costs risen in recent years, but their complexity has too.

As organizations recognize that security touches everyone, security professionals will be embedded into each team and department. Security leaders should consider whether the investment required in building a SOC would be better spent elsewhere, like implementing automation, embracing AI in workflow automation, or developing more iterative approaches to security. While SOCs are phased out, an outsourced SOC or MSSP could provide an interim solution.

Invest in best-in-breed solutions

According to the latest research, organizations experience an average of 1,258 attacks per week. Threats are frequent and pervasive, and are becoming too sophisticated to be handled by one-size-fits-all solutions. Organizations wanting to stay ahead in their security approach need to un-bundle their stacks and all-in-one "big box shops" and invest in best-of-breed security tools designed for specific purposes.

Thanks to workflow automation, the overhead costs associated with managing best-in-breed solutions are no longer a hindrance to investment. Since the best workflow builders connect to both known and custom tools, automation reduces the risk of fragmentation.

Finding success

Embrace cross-team collaboration

The most successful organizations are the ones in which teams collaborate and communicate effectively across security, IT and beyond.

I witnessed this first-hand as the leader of security teams. They're tasked with performing remediations for their organization, yet much of that work is often found on software that the security team has no direct control over. Security teams then find themselves dependent on other teams for their own success – teams whose priorities may not align with the priorities of SecOps. This misalignment and limited access can allow vulnerabilities to remain unaddressed.

Security teams need to find ways to work with other departments to gain access, which will not only require relationship-building and trust, but the ability to adequately communicate why SecOps needs access to those systems. Other departments may be reluctant to grant open-ended, manual access, but may be more willing to allow access, provided it is only used in automated scenarios with known inputs and outputs.

Build a culture of automation

To see continued success, security leaders need to promote a culture of automation across their teams. This means that, any time team members are faced with an inefficient, time-consuming, or monotonous process, their first thought is, "Can we automate some or all of this?"

A culture of automation will get teams used to recognizing where they can make their tools work harder for them and allow them to shift their focus to more pressing matters.

Leaders can start by doing the following:

· Annotate as you build your automated workflows so that colleagues can understand how the workflow executes.

· Extract the shared sequences that begin to pop up repeatedly into modules that can be reused across your workflows.

· Set up monitoring to ensure that when something does break, a human gets notified.

· Continuously improve upon your workflows, and think creatively about what can make the workflow run faster.

· Demonstrate the value you find in automation to leadership.

Case study
Oak Ridge National Laboratory

A federally-funded organization and pioneer in technological advancement, Oak Ridge National Laboratory used workflow automation platform Tines to accelerate their zero trust goals and strengthen their security posture.

BEFORE TINES

- Managing automation through manual scripts

- Only engineers could build, run or monitor workflows
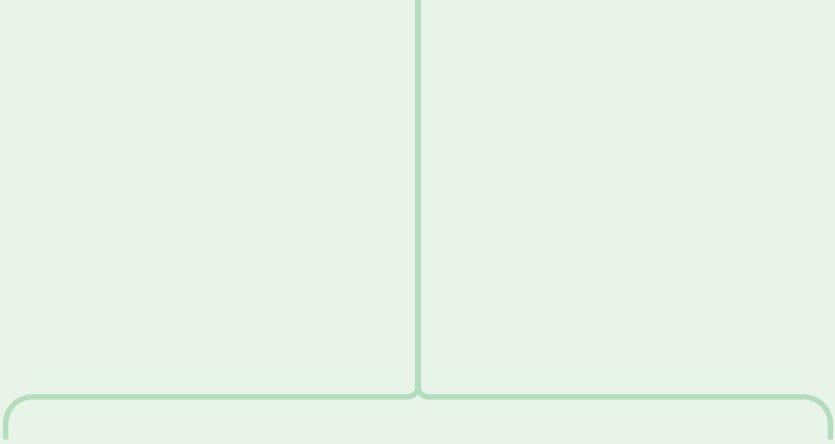
- Long waiting periods

- No automated reports

AFTER TINES

- Managing automation through a flexible, scalable workflow platform

- Anyone on the team can build, run and monitor workflows

- No waiting period

- Automated reporting leading to improved visibility and time savings

Key workflow: IP analysis

Analysts at Oak Ridge National Laboratory gather network information from databases via their APIs and update Tenable with over two million IP addresses in a matter of seconds. This helps the team evaluate and break down those IP addresses for vulnerability, evaluate the data, and then push it to Tenable. To comb through this volume of IP addresses manually, before Tines, was not even a possibility.

→ Read the full case study: tines.com/ornl

"It was a game changer during onboarding when we could connect all our systems... Our ability to integrate new tools has taken out so much of our everyday tasks from before."

MIKE CRIDER, CYBER VULNERABILITY ANALYST

OAK RIDGE NATIONAL LABORATORY

Step 1 **Outline your goals**

Define the specific objectives you want to achieve through workflow automation. This could include increasing efficiency, mitigating risk, or effectively scaling your processes.

Step-by-step guide

Step 2 **Find internal champions**

This is critical to the success of your automation program as you pursue buy-in from key stakeholders.

You can achieve this by:

- Identifying teammates who can advocate for the use of a workflow builder
- Hosting knowledge-sharing sessions
- Finding joint automation opportunities through cross-functional collaboration
- Recognizing and rewarding builders for their achievements

Step 3 **Evaluate your options**

As you begin searching for the right platform, look for vendors who are experienced in supporting your specific use cases. For example,

if you spend most of your time following up on suspicious logins, and they don't have examples to share, take a look elsewhere.

Additionally, ask how the platform integrates with your in-house APIs. Legacy SOAR platforms typically feature pre-baked integrations, but only for a limited number of popular tools. Seek out a platform that can integrate with all of your organization's tools, no matter how niche or custom they may be.

Five things to look for in a security workflow platform:

1. The ability to collect information from anyone – not just your teammates – at any point in the workflow run

2. A low barrier to entry – the more team members building, the better for everyone

3. Intuitive UX – a user-friendly interface that accelerates build time

4. Deployable AI-powered capabilities – they should be secure, private, intuitive, and deliver return on investment

5. Flexibility – a platform that can connect to all of your tools, internal and external

Step 4 **Run a POC process**

When it comes time to demo, don't pick a simplified workflow, but ask the vendor to run a more complex one that closely mimics the types of tasks you want to automate – a good vendor will be excited by the challenge!

Platforms should be robust enough to automate complex, lengthy workflows, yet many of the platforms that sell themselves as "powerful" have surprisingly low operational limits. Leverage free community editions and trials to put platforms to the test.

Evaluate AI-powered capabilities with extra scrutiny – in their haste to ride the AI wave, some vendors have shipped demoware. Be sure the

vendor's capabilities are deployable, and look closely at how costs will be incurred. AI in workflow automation should be secure, private, and intuitive.

Step 5 **Purchase the best tool for the best price**

As you explore options, consider the pricing model (e.g. data ingestion or storage rates) and not just the price tag to get started. And be sure to ask how pricing will change as usage increases, as many vendors obscure their pricing structure.

Committing to workflow automation means scaling the number, size, and throughput of workflows, and you need to know what you can expect to pay. Look for a model that will encourage as many team members as possible to build automated workflows, without worrying about hitting a data cap or a user license limit.

Step 6 **Build workflows iteratively**

Once you have your workflow automation platform up and running, the best approach is to start small with prototypes and MVPs, and then keep evolving the complexity.

Deploy the simplest usable version to production first, and then expand workflows little by little to cover edge and corner cases. This allows builders to become more creative with their automation, building more sophisticated processes as they go.

Because of the accessibility of workflow automation, security teams can maintain and evolve their workflows in production, and iterating those workflows as their company's processes and threats continuously change. One thing to remember is not to price the maintenance of automation at zero. Even if it's built flawlessly the first time around – which is rare – external context will always change, necessitating future iteration.

MARS

Case study
Mars

Mars is a global company and family-owned business with the footprint of a small country. Their security team looked for a new workflow platform to replace an underperforming SOAR tool, which, frustratingly, only one team member could use.

BEFORE TINES

- Only one team member could use their SOAR

- Relying on that one team member put them at greater risk

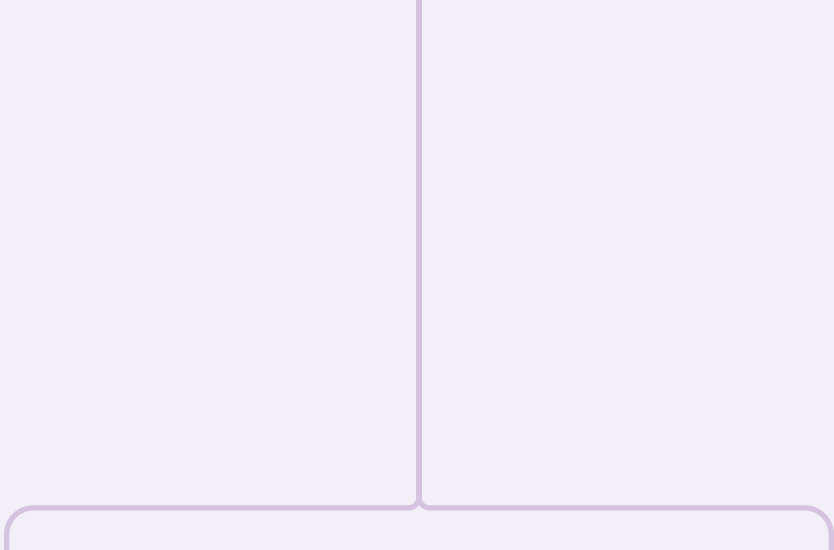- A large library of workflows needed streamlining

AFTER TINES

- Everyone on the team can build, run, and monitor workflows

- Fully migrated all workflows in a couple of months

- Consolidated, efficient workflows

- Faster workflow build times

- Coverage of 80-90% of sources for true positives

Key workflow: alert triage and escalation

One of the security team's key workflows receives alerts from the cloud security platform Wiz, triages them and assigns it to the right team in ServiceNow. This workflow includes a structured escalation path, ensuring that high-priority issues are promptly addressed and managed effectively.

→ Read the full case study: tines.com/mars

"Because of the flexibility of the Tines platform, we were able to consolidate use cases."

GREGORY PONIATOWSKI

DIRECTOR OF CYBER THREAT AND VULNERABILITY, MARS

Workflow
best
practices

Modularize

As you build more workflows, you'll inevitably repeat certain steps, for example, "post a message to the team Slack in this format." It's a good idea to extract shared sequences so that they can be reused across other workflows.

Engage

You're going to need a way for people on your team and outside of your team to easily interact with your workflows. Sometimes you'll want them to kick off a workflow, for example by providing information on a suspicious email. Other times, you'll need them to answer a question mid-workflow, for example, to approve or deny a user's tool access. Features like Tines Pages help you seamlessly collect information from anyone at multiple stages of a workflow run.

Monitor

Some of your workflows will be mission-critical, and so, it's important to be aware when something unexpected happens. Set up monitoring to make sure somebody gets notified when any of your tools within a workflow has an issue – for example, the API for an upstream system is down, a credential expires, or no alerts have been received recently.
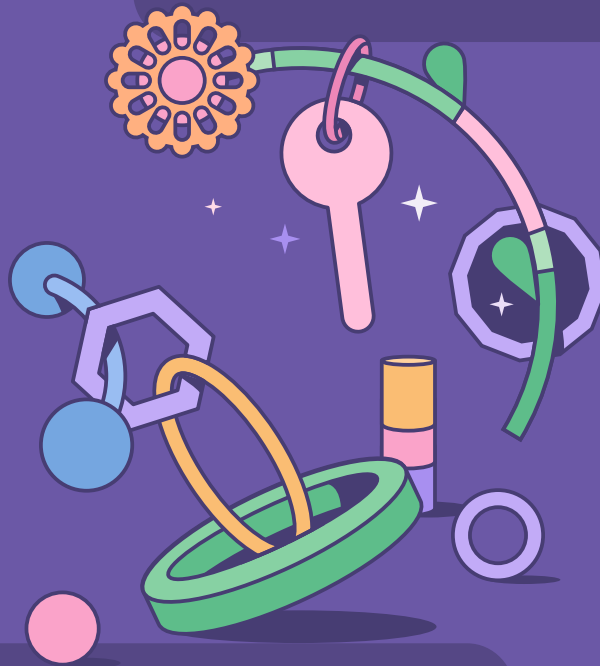
Evolve

The best workflows are continuously improved. From time to time, analyze a random workflow run and creatively think about what could make the task faster or the outputs more useful. If your platform allows you to run an LLM within the context of your workflow, ask whether AI can be used to work faster or more efficiently?

Communicate value

After investing in workflow automation, it's important to demonstrate value to leadership. For previously manual processes, a good system is to estimate the number of minutes each step used to cost, and track the accumulated data of actual human hours saved. Ideally, the platform would allow you to report on this automatically.
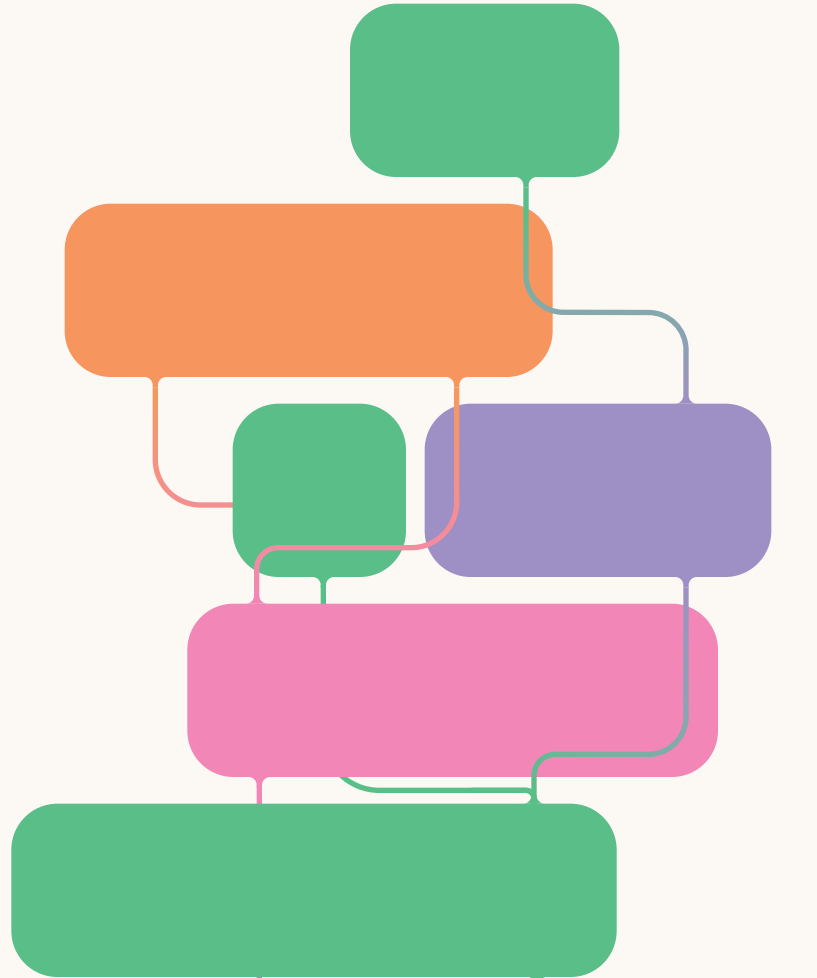
The future is workflow automation + AI

Workflow automation isn't simply taking the mono-
tonous tasks off your team's plate, but giving your
security practitioners the tools to get creative with
what they automate and evolve the efficiency of their
workflows. And AI can make these workflows easier
to build and run. Not only will your teams become
more efficient and processes more streamlined,
but your people will be empowered to focus more
time and energy on the work that matters most.

Workflow automation for security teams

The world's smartest security teams
– from startups to the Fortune 10 –
trust Tines to power their most
important security workflows.

→ Book a demo to learn more about
how your team can embrace workflow
automation: tines.com/book-a-demo

→ Sign up free at: tines.com

RESOURCES CITED:

Voice of the SOC: https://www.tines.com/reports/voice-of-the-soc-2023/

Check Point report: https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

Gartner Predicts 2023: Cybersecurity Industry: https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025

IDC, A robot for every worker: https://proedge.pwc.com/resources/download-a-robot-for-every-worker-an-idc-white-paper

BT cybercrime report 2023: https://newsroom.bt.com/cybercrime-more-than-500-potential-attacks-clocked-every-second/

tines