Streamlining SecOps:

Enhancing security and operations with n8n

Table of Contents

Introduction

Today's digital security landscape is dynamic, requiring forward-thinking security. As cybersecurity threats grow increasingly complex, security operation (SecOps) has become unquestionably important. The inter-connectedness of applications, mass adoption of the cloud, and even the shift toward remote working have led to an influx of cybersecurity threats. To prevent these attacks from hitting your organization and plaguing your users, you need an effective SecOps strategy.

But to have successful SecOps, you need to manage workflows efficiently. Workflow management is crucial to SecOps because it ensures the communication and collaboration between security and operations teams are seamless, fast, and consistent. It involves establishing SecOps processes, defining the roles and responsibilities of security and operations team members, and outlining what communication channels they'll use. Additionally, workflow management is essential for prioritizing and allocating resources to maintain a top-tier security posture.

Leveraging a security orchestration, automation, and response (SOAR) platform is one of the best ways to enhance your SecOps workflow management. SOAR platforms enable your teams to automate security operations, expedite responses to security incidents, and manage threats by identifying, assessing, and helping remediate incidents. And thanks to automation, response times are drastically reduced.

SecOps workflow management offers many benefits. But it's not just that having an effective workflow is advantageous: Lacking one can be a tremendous hindrance.

First, without transparent processes and predetermined communication channels, the chance of incidents going undetected — or at least experiencing delayed resolutions — skyrockets. These oversights can compound vulnerabilities and, at worst, cause full-on breaches.

Also, a lack of workflow automation and standardization translate to costly inefficiencies in time and resources.

Finally, priorities can become misaligned when security and operations teams fail to coordinate and collaborate. Their approaches to problem-solving can conflict, ultimately interfering with the effectiveness of their incident responses.

Establishing a streamlined SecOps workflow is essential and doesn't have to be complicated. Read on to learn how n8n can help you effortlessly enhance your security and operations.

Unveiling n8n: Enabling SecOps through workflow management

Top-notch SecOps requires top-notch tools. Enter n8n: a powerful automation tool that enables teams to create and manage workflows easily — SecOps workflows included.

n8n offers dynamic integration capabilities that simplify creating automated workflows. It integrates with numerous services, APIs, and applications, including some of the biggest names in the tech business. n8n's integrations include customer relationship management (CRM) systems, email and SMS services, project management tools, and much more. Don't see an application that's part of your current workflow? No problem — your teams can send **HTTP requests** or **write JavaScript code** to accomplish almost anything. And if your technicians are stuck on where to get started, n8n offers **over 600 workflow templates**.

Workflows built in n8n support conditional logic, data transformation, and error handling — and your organization can use them all to enhance your SecOps strategy. With the ability to trigger actions based on specific events, security and operations teams can create comprehensive, tailored workflows to ensure they manage and mitigate all incidents — and *potential* incidents — without a hitch.

In addition to enabling customized workflows, n8n offers flexible deployment methods. Teams can deploy n8n in the cloud, so your organization can leverage all the benefits of cloud-based integrations and services. But **unlike other workflow management tools**, n8n doesn't lock you into cloud deployment. You can also run it on-premises, making it an ideal choice when you need to comply with strict data privacy requirements — or even if you're just ultra-cautious with data management. By running n8n on-premises, you maintain total control over your data and workflows, reducing some of the typical risks of using cloud-based software.

n8n is also no-code — a factor that's key to its utility. Teams can create powerful workflows just by dragging and dropping prebuilt nodes (applications, services, and APIs) and defining their parameters, inputs, and outputs. With this intuitive visual interface, there's no need for extensive coding knowledge. This approach makes n8n accessible to both technically inclined and less technically inclined users, reducing the time to get your SecOps workflows up and running.

Because of its workflow automation capabilities, n8n can act as a SOAR tool to help with the following functions:

- Automating the incident response process
- Integrating security tools into SecOps workflows
- Creating event-based triggers to escalate incidents effectively
- Increasing collaboration and communication between teams to encourage a quick incident response time and boost overall productivity

Thanks to its unified platform, n8n helps organizations like yours overcome SecOps challenges, including missed incident reports, ineffective incident escalation measures, poor communication with users, inconsistent issue tracking, and siloing. Because n8n enables security and operations teams to integrate disparate security tools, data sources, and incident notification systems, SecOps teams can clarify and refine their processes — ultimately strengthening your organization's security posture.

And n8n doesn't just talk the talk — it also walks the walk. n8n can handle up to 220 workflow executions per second on a single instance, and it's easy to scale up and add more resources as needed. A multi-instance n8n configuration can receive around 2500 workflow executions per second, so your n8n SecOps workflows can still efficiently run when working at scale. Additionally, teams can benchmark their specific use case to better understand n8n's performance capabilities.

Leveraging n8n for efficient alert handling in SecOps

Of course, knowing if and when incidents occur is one of the most critical steps in an effective SecOps workflow. Unfortunately, SecOps is plagued with a condition that, when unchecked, can have tremendous consequences: alert fatigue.

Alert fatigue is an imposing problem in SecOps. It happens when security teams receive such a high volume of alerts — primarily for low-priority events — that it becomes overwhelming. This constant stream of notifications can leave workers feeling drained and less attentive to (or concerned about) alerts. As a result, messages about high-stakes incidents tend to get lost in the noise. When security teams miss these notifications, they take longer to resolve the incidents, leaving your organization vulnerable to prolonged attacks.

Alert handling software is essential to your efforts to mitigate alert fatigue. But many software approaches to alert handling contain deficiencies that contribute to it. Some of the most high-impact shortcomings include the following:

- **A lack of contextualization and prioritization** — Many alert handling solutions create alerts without contextualizing them within your organization's environment or its overall security posture. This lack of context can overwhelm security teams with (irrelevant) alerts. As a result, it's tricky for teams to determine which incidents are critical — and which aren't. Ultimately, the incident response process lags, and the lack of an intelligent, holistic workflow can result in missed or mismanaged alerts.
- **A lack of automation** — Some alert handling tools lack advanced automation capabilities, so SecOps teams become burdened with manually investigating and triaging security incidents. Apart from being wildly inefficient, a manual approach to incident management substantially increases the chances of teams making mistakes and missing alerts, leaving room for vulnerabilities to proliferate. With such a rapidly evolving security landscape, no organization should take this risk.
- **A lack of integration between tools** — Siloed tools are a massive time-sucker. Siliong makes it extremely difficult for SecOps teams to gather, consolidate, and analyze information, leading to missteps, miscommunications, and superficial fixes.

To conquer these deficiencies, your organization can invest in a more advanced, connected, intelligent tool like n8n.

With n8n's powerful workflow automation capabilities, your teams can create top-tier alert handling workflows to ensure they don't miss critical incidents. n8n's approachable interface makes it easy to design workflows that automatically receive, process, escalate, and triage alerts based on preset conditions. This way, your notification handling processes reflect your organization's security objectives and requirements.

Additionally, n8n's sizable collection of integrations prevents siloing. These integrations include security information and event management (SIEM) tools, communication tools, incident ticketing software, logging systems, and much more. Thanks to these integrations, SecOps teams in your organization can aggregate data from multiple sources, quickly identify root causes, and work proactively to mediate future incidents — all necessary for swift, thorough, and ultimately successful SecOps.

The following section highlights how n8n ensures the right people receive the right alerts at the right time, illustrating its impact on your SecOps workflows.

Alert handling case study: Monitoring load balancer traffic for attacks

n8n's alert handling capabilities enable SecOps teams to create seamless, detailed workflows that actively combat alert fatigue. With n8n's easy-to-use interface, your organization can implement various alerting workflows that reflect an incident's severity and send those alerts to the correct people when it's most appropriate.

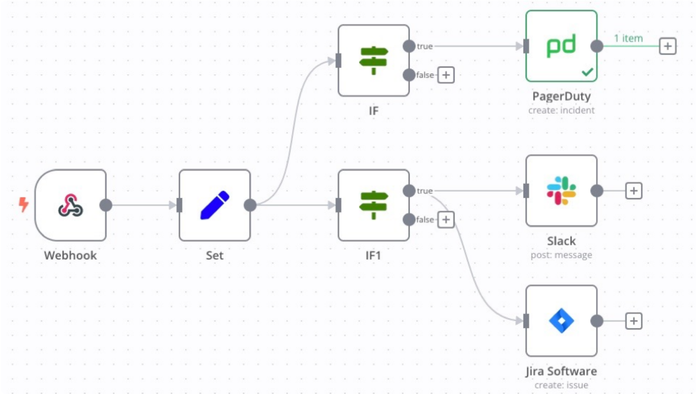
Using n8n, SecOps teams can create alerting workflows supporting reactive and proactive remediation. Let's explore these different workflows in detail.

When a concerning issue or urgent security incident arises, teams must know as soon as possible. These critical notifications *cannot* get lost in a stream of low-stakes alerts. n8n shines in this regard.

Your organization can, for example, use n8n to help identify any hackers attacking a load balancer at the front of a network stack. SecOps teams can integrate **Splunk** into their n8n workflow to get alerts when current requests per second exceed the expected amount — say, 1,000 requests per second. Using 1,000 requests as the marker, SecOps teams can configure their n8n workflow to notify relevant team members when the requests meet predetermined thresholds.

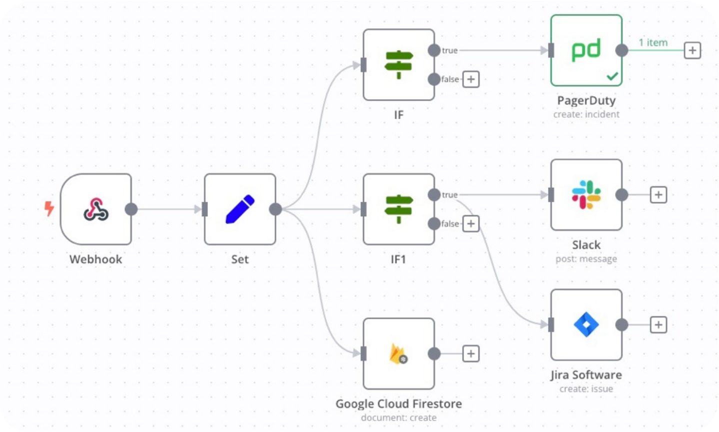
For this example, teams can configure n8n to send alerts if Splunk reports that the requests per second are significantly over the expected amount. If the system receives 2,000 requests or more when you only expect 1,000, it could indicate an attack.To communicate the matter's urgency and reach relevant people immediately, SecOps teams can configure the workflow in PagerDuty to notify SecOps team members — and even the account manager — of the issue. Once n8n triggers the workflow, **PagerDuty** sends an SMS notification to relevant parties with a list of alerts, asking for a reply to acknowledge or resolve said warnings. It also delivers the same message via an automated phone call.

If the number of requests per second is still high but not quite as severe (say, between 1,500 and 2,000), n8n may not need to notify teams on PagerDuty directly. For this case, configuring it to create a ticket in Jira Software would be a better fit so that SecOps teams can look into the issue asynchronously. Additionally, your teams can configure it to send Slack direct messages to relevant team members or SecOps and infrastructure management channels for extra coverage.

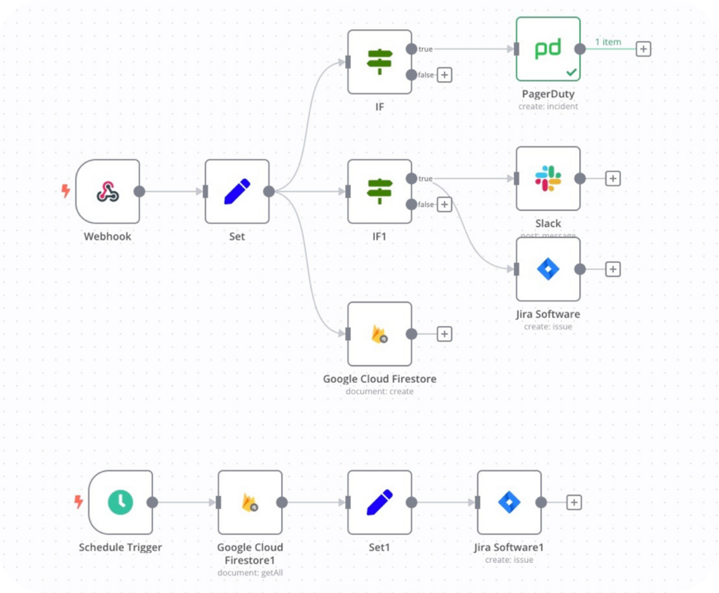


Setting strict parameters for when to notify teams is vital for preventing alert fatigue. But just because there's no immediate crisis doesn't mean that incidents or performance anomalies aren't significant. It requires a balance: Teams can't overlook minor security hiccups in favor of only addressing high-priority items. Your SecOps strategy should focus on reactivity *and* proactivity to maintain a strong security posture.

n8n supports proactive incident-prevention workflows too. To demonstrate, let's return to the previous requests per second example. Suppose SyncroMSP tracks that requests per second exceed the anticipated 1,000 but are fewer than the 1,500 required to create a Jira Software ticket. In this case, your organization can configure n8n using Splunk to track requests per second across a period — such as a month — and collect it in a NoSQL cloud data-base like [Google Cloud Firestore](). This way, teams can later access and analyze historical data about anomalies or unexpected spikes in traffic.



Worried everyone will forget these spikes? No problem! It's easy to schedule a trigger in n8n to create a Jira Software ticket, telling SecOps teams to revisit those low-urgency incidents.



By reminding your teams to investigate trends that might link these spikes, n8n helps your organization improve its security standing and mitigate potential future security problems.

Issue tracking and enrichment: n8n's approach to incident response and prevention

Once teams know about an issue and your automated tools create a ticket, someone must track it until its resolution. Organizations need a robust tracking system to ensure every ticket gets noticed and resolved promptly. Ticket tracking tooling enables SecOps teams to log, categorize, and triage security incidents, assigning the work to the best-suited team.

In addition to tracking issues and their resolutions, a strong SecOps strategy needs issue enrichment — the process of gathering detailed, relevant information about incidents and their context. SecOps teams should explore and integrate threat intelligence, user behavior information, and historical incident data to gain deeper insights into an incident's cause, impact, and future implications.

Effectively tracking and enriching issues enables your organization to refine its SecOps workflows, improve incident resolution efficiency, and reduce the time necessary to respond to incidents. These aspects also support proactive incident mitigation by encouraging SecOps teams to document and analyze issues and identify patterns in security incidents.

n8n can simplify this process by helping automatically create and track tickets. Besides working with Jira Software, n8n integrates with GitHub and GitLab. These integrations help improve collaboration, make real-time updates during the incident resolution process, and handle any issues that arise sooner.

When integrated with security monitoring and log analysis tools, n8n also makes it easier to identify false positives. Its use of machine learning algorithms helps your organization improve the accuracy of its threat detection practices.

Additionally, consolidating and correlating data from multiple sources helps SecOps teams enrich their understanding of incidents and respond effec-tively to future threats. This threat intelligence — the practice of collecting knowledge and experience-driven information about a security event — is instrumental in proactively mitigating security attacks.

Using n8n's extensive integration library, SecOps teams can aggregate data from threat intelligence feeds, like MISP, and security analytics tools, including Elastic Security, to collect and analyze threat intelligence data automatically. Your teams can predict and prevent threats more easily by tying these data sources into n8n. These integrations also help you manage vulnerabilities by automating and streamlining the following threat management processes:

- **Automate scans** — With n8n, SecOps teams can place a trigger within their workflows to execute a vulnerability scan. For example, they can configure n8n to start a Rundeck job that scans code for vulnerabilities.
- **Prioritize vulnerabilities** — n8n can help SecOps teams prioritize vulnerabilities. Using the data from Rundeck's vulnerability scans (for example) — including the number of vulnerabilities identified, the number of occurrences, and Rundeck's prioritization of those vulnerabilities — n8n can trigger a preset workflow to help SecOps teams resolve high-priority issues immediately.

- **Communicate results** — n8n can use this preset workflow to send the scan results via a method suiting the vulnerability's severity, like Slack, email, SMS, or a Jira Software ticket.

Let's review a real-world example of how n8n supports issue tracking and remediation.

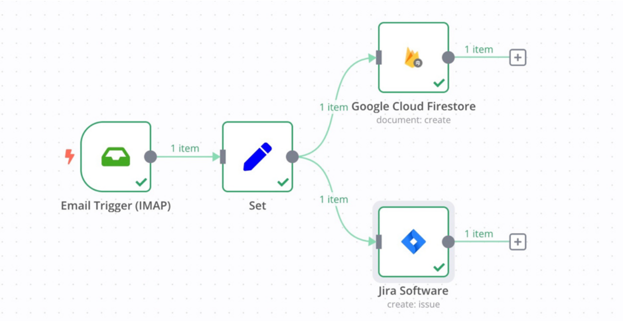
Issue tracking case study: Investigating phishing emails

Phishing remains a recurring security incident that many organizations repeatedly face. Phishing emails can pose a significant security threat to your organization, so it's crucial to log and analyze them — not just delete and forget them.

Say an employee within your organization receives an email they suspect is a phishing attempt. If they've opened the email, whether intentionally or accidentally, they can send it to your SecOps team's internal diagnostics email.

The SecOps team can develop an n8n workflow triggered by receiving that email. They can configure the workflow first to create a Google Cloud Firestore document that includes the email's data (sender, contents, date, and the like) for future analysis. Documenting this information makes it easier for SecOps teams to identify patterns in these attempts and proactively bolster security measures with these patterns in mind.

Once the phishing complaint is on record, n8n can trigger a Jira Software ticket to tell SecOps team members to investigate the email in a secure setting.



Using this workflow, SecOps teams can review the email described in the ticket to confirm whether it was a phishing attempt and ask the employee if they've experienced any effects from opening the email. Then, the SecOps teams can determine whether to take action, like changing passwords or running anti-malware software.

Enhancing user interaction and remediation with n8n

User interaction is a crucial part of SecOps processes for several reasons:

- **Users are at the forefront of your organization's defense strategy** — Users are often the targets of malicious actions like phishing attacks. Ensuring all your users know how to report incidents or suspicious activities is instrumental to your organization's security posture.
- **User feedback helps with incident detection and mitigation** — Collecting user feedback helps SecOps teams detect and mitigate vulnerabilities. As highlighted in the previous phishing

example, communicating with users can also help SecOps teams track a security incident's impact.

- **Users should be actively involved in your organization's cybersecurity strategy** — Involving all users in your SecOps process encourages a culture of collaboration and accountability. It empowers everyone to help maintain account, data, and system security.

n8n facilitates user interaction through its support for tools that automatically gather user reports and compile their data. In addition to Jira Software, n8n integrates with ticketing systems like **ServiceNow**, SIEM incident management platforms like Splunk, and collaboration tools like **Google Sheets** and **Form.io**. These integrations help users notify stakeholders of issues as soon as possible.

SecOps teams can create n8n workflows to collect data from user feedback channels, like forms or incident ticketing/management systems, as the first step toward resolution. Then, n8n's built-in operations ensure the data is structured and relevant before notifying SecOps teams via your organization's alert handling workflow.

If a user submits a report or form stating they're experiencing an issue, a workflow in n8n notifies SecOps teams. From there, someone can apply a patch for that specific user. The workflow can trigger patch management tools to deploy the necessary updates across the network using native **GitHub** and **GitLab** integrations.

Along with integrated tools, n8n has built-in error-handling mechanisms, including error-catching nodes and conditional branches. It also supports custom error handling using JavaScript code execution nodes. These features enable SecOps teams to implement advanced, autonomous error patching logic — all from within n8n.

Ensuring SecOps continuity and procedural efficiency with n8n

Continuity and procedural efficiency are imperative to the success of your SecOps strategy. After all, organizations need to ensure their services can weather whatever unforeseen, perhaps disastrous, circumstances they encounter.

Disaster planning is essential to mitigating risks and ensuring continuity. This planning can involve implementing failover mechanisms that maintain critical functions even during system failures or malicious attacks.

To ensure continuity, your organization should establish procedural tasks — standardized processes and response protocols — to ensure you don't lose continuity. Procedural tasks outline what steps SecOps teams should follow to respond to incidents, detect threats, and implement mitigation strategies. When used effectively, they help you maintain continuity and security in the face of incidents.

n8n supports maintaining procedural tasks through its advanced automation capabilities. Because SecOps teams can design and implement workflows that trigger based on predetermined conditions, it's easier for them to implement standardized procedures and swift fixes when security incidents occur.

Additionally, with n8n's conditional flow options, SecOps teams can use these customized, regulated workflows to respond to events immediately, regardless of what occurs. This approach saves time, ensures consistency across incident responses, and enables SecOps teams to focus on critical decision-making tasks rather than performing repetitive, time-consuming work.

When teams work reactively, proactively, and procedurally, you can rest assured that you have a robust, reliable, and secure system.

More for less with n8n

Workflow tooling must be just right, but choosing a workflow automation tool can be complex. Many tools are available, and their advantages are not inherently obvious.

Because particular features and facets of a workflow tool can make or break your experience, it's vital to compare your options and find the tool that perfectly fits your needs. Let's take a quick look at what makes n8n a better choice for your organization than other leading tools.

The workflow automation landscape

Swimlane is a popular SOAR tool to help SecOps teams fight alert fatigue and streamline workflows. While it has an intuitive interface and helps teams connect siloed tools, it has limitations that n8n doesn't experience.

Most notably, Swimlane is a proprietary solution, so your organization will likely experience vendor lock-in. With this situation comes limited integrations and, consequently, a lack of flexibility. In contrast, n8n's open-source availability, support for HTTP requests, and hefty integration library ensure your SecOps team won't experience these constraints.

n8n also outperforms Workato, a fully cloud-native automation platform comprising prebuilt connectors. Users have cited Workato as difficult to use, somewhat code-heavy, and lacking connectors. In contrast, n8n's interface is instinctual and requires much less coding, thanks to its extensive integration library.

Tines is another workflow automation tool that n8n outshines. n8n offers over 200 integrations, more than Tines offers out of the box. So, n8n is a great deal more flexible. Additionally, Tine's less-intuitive interface makes it harder to integrate with third-party services than n8n.

If your organization is just stepping into workflow automation, know you're not alone. Many companies — particularly startups — don't use a workflow automation tool. It's typical for organizations to rely on a custom set of Python scripts instead of investing in an automation tool like those above.

Although this approach might work in the short term, as companies grow and workflow complexity increases, the cracks in a manual approach start to appear. For SecOps, these cracks quickly become high-risk.

Switching from a collection of Python scripts to an automation tool might seem like a lot of work for your SecOps teams. But with n8n, it doesn't have to be. n8n offers your team the same functionality without the organization and management-related challenges that these scripts breed when working at scale.

For performance and ease of use, n8n comes out on top.

You can't beat n8n's pricing

The heading says it all: n8n's pricing simply can't be beat. Its **affordable, transparent pricing model** makes it highly competitive — and appealing — to organizations working at scale.

For example, Swimlane's cloud pricing ranges from €54,145 ($59,000 USD) to €385,444 ($420,000 USD) per year, according to its **Amazon Web Services (AWS) Marketplace listing**. There's no clear pricing listed on Swimlane's website, so you'd need to **contact them** to get an accurate model. Workato doesn't have any publicly available pricing, so you'd have to go out of your way to contact them just to get a quote and estimate your costs. Tines also requires you to book a demo just to learn about **enterprise pricing**.

In contrast, **n8n's cloud packages** start at €20 per month for 5,000 work-flow executions, with packages designed for enterprise use. And these prices are fully transparent: Unlike other automation tools, n8n doesn't charge your organization to run more advanced or complex workflows. Whether your teams use many connectors or a few simple workflows, pricing is the same.

Also, our execution advantage ensures you only pay for full workflow executions — not per operation, step, or task. This model guarantees your costs are predictable, transparent, and scalable, regardless of the workflows' complexity. Moreover, n8n doesn't have premium applications. Your package includes all 200+ integrations.

In addition to these cost-effective pricing models, an open-source community version of n8n is available on GitHub, where SecOps teams can build and test workflows on a smaller scale. This community version has a **fair-code** distribution model, so n8n's source code is always available and offers the option to self-host.

Speaking of self-hosting, enterprises can also self-host n8n if they prefer this approach or must meet regulatory requirements. It's not just the community version! With n8n, your organization can enjoy a fully on-premises workflow solution — which most competitors don't offer. And if they do provide on-premises hosting, their pricing is higher than n8n. Plus, you still have to expose some of your data to the hosting company. Meanwhile, with n8n, you can keep your private information private. n8n ensures that self-hosting isn't just possible — it's reasonably priced and easy to implement.

n8n's hands-off approach

n8n offers a hands-off approach once your workflows are in place. Less-technical staff can maintain the workflows using n8n's drag-

and-drop visual interface, freeing your more senior technical and SecOps team members to work on more critical and time-sensitive tasks.

Conclusion

SecOps unites security and operations teams to detect security threats and vulnerabilities proactively, respond to security incidents swiftly, and implement incident mitigation strategies. When you build security practices into your operations, you protect your users, data, and reputation — even in an ever-evolving cybersecurity landscape.

But you need efficient workflows for your organization to succeed at SecOps. When it comes to security, time is of the essence. There's no room for missed notifications, tedious work, or struggling to determine the next steps. Using n8n's customizable, conditionalized workflows, your SecOps teams never get bogged down or lost in the incident resolution process. They'll see alerts, quickly implement mitigation steps, and benefit from crystal-clear team communication.

Additionally, n8n's workflows support proactively handling vulnerabilities, not just reacting. With integrations and tooling to support data collection and analysis, vulnerability prioritization, and incident ticketing, your SecOps teams can gain a holistic view of your organization's security posture — and bolster it as needed.

n8n's efficiency, reliability, and user-friendly interface help free more of your SecOps team's time to do their most important work. And with a cost-effective pricing model, plus the option to host on-premises, n8n can meet your organization's financial, regulatory, and security needs without breaking the bank.

To streamline your organization's workflows and take your SecOps to the next level, **learn more** about n8n.

For more information, learn more at:

n8n.io

n8n