

The Case For Time To Automation

A CISO's Guide To Scalable Defense

Rethinking Metrics, Workforce Strategy,
And AI In The Modern SOC



Introduction

Cybersecurity leaders are grappling with unprecedented challenges: a severe talent shortage, an accelerating threat landscape, and the limitations of legacy tools. To thrive in 2025, security programs must rethink how they measure success.

Time to Automation (TTA), the speed at which a security team can convert a needed detection or response into an automated workflow – is emerging as the most vital metric for modern security operations. In BlinkOps' State of Security Automation report that surveyed 1,000+ security practitioners, 81% identified AI-driven automation as a top strategic priority, and Time to Automation has overtaken traditional KPIs as the top metric to improve.

This ebook explores why TTA is so critical, contrasting it with legacy metrics like MTTR and MTTD, and provides evidence-backed analysis on how faster automation can mitigate breaches and alleviate operational burdens. We also examine how new technologies – particularly agentic AI and large language models (LLMs) – enable rapid automation, and offer practical guidance on measuring and improving your organization's TTA.

The goal is to equip CISOs and security practitioners with data and insights to make Time to Automation the centerpiece of security strategy in 2025.





Table Of Contents

- | | | | |
|---|--|---|---|
| 1 | Cybersecurity Workforce Shortage: An Urgent Risk | 4 | Faster Automation = Fewer Breaches And Less Burnout |
| 2 | Limitations Of Legacy SOAR Tools | 5 | Agentic AI And LLMs: Accelerating Automation |
| 3 | TTA Vs. Traditional Metrics | 6 | Measuring And Improving TTA: A Practical Guide |

Cybersecurity Workforce Shortage: An Urgent Risk

The cybersecurity workforce gap has reached an alarming scale, creating an urgent imperative to automate. Globally, the industry faces a shortfall of around 4 million skilled cybersecurity professionals, leaving many organizations understaffed.

This skills crisis is only growing – by 2030 the overall talent shortage across industries is projected to hit 85 million workers, and cyber teams will remain under-resourced. The operational consequences are dire. With too few analysts, security teams struggle to keep up with alerts and incidents, increasing the likelihood that threats slip through unnoticed.

In fact, two-thirds of organizations report that cyber skills shortages are adding extra risk to their environment. Evidence bears this out: more than half of organizations that suffered a breach in 2024 had significant security staff shortages at the time.

This shortage translates into slower incident response, mounting backlogs of uninvestigated alerts, and overworked personnel at high risk of burnout.

A recent (ISC)² study found the global cyber workforce gap has surged to 4.8 million unfilled positions (a 19% increase in one year) and 58% of professionals say the skills shortfall puts their organization at significant risk.

In short, demand for security expertise far outstrips supply, and manual operations simply cannot scale to fill the gap. This makes smart automation an operational necessity. By automating repetitive tasks and first-line responses, organizations can multiply the impact of their limited staff, allowing analysts to focus on high-value work. In the face of an enduring talent drought, accelerating Time to Automation is becoming critical for maintaining an effective defense.

Limitations Of Legacy SOAR Tools

Security Orchestration, Automation, and Response (SOAR) platforms were supposed to be the answer to workflow automation. However, they're starting to show their age. A core problem is the heavy maintenance and development they require.

Traditional SOAR implementations often demand teams of engineers to write Python scripts and maintain complex playbooks for every integration and response. This leads to brittle systems that lag behind attacker techniques. In fact, many SOAR playbooks are outdated before they're even deployed, due to the rapid evolution of threats. When an attack technique changes or a new threat emerges, legacy playbooks can't adapt on the fly – they must be re-coded and retested, a process too slow for the speed of the modern enterprise.

Legacy SOAR's rigidity also causes scalability issues. Under high alert volumes, traditional SOAR schedulers often become overwhelmed, resulting in processing bottlenecks and delayed responses. This is especially problematic in large enterprises or MSSP environments

where surges of events are common – the SOAR platform itself can choke under pressure, leaving security teams unable to react in time. Another shortcoming is the lack of flexibility and integration. Older SOAR solutions typically support only a fixed set of integrations and may restrict using certain libraries or APIs due to security concerns, limiting customization. For example, some legacy platforms won't allow importing modern Python SDKs for cloud or endpoint tools, hampering the development of tailored automation workflows.

The result is that security teams end up spending inordinate effort building and maintaining adapters, or paying for professional services to bridge gaps. All of this adds up to high cost and complexity: dozens of playbooks needing constant updates, fragile workflows that break with minor changes, and a reliance on a few automation experts to keep things running. Early-generation SOAR delivered on orchestration in theory, but in practice many implementations became slow, rigid, and costly to operate. As one analysis succinctly put it, "legacy playbooks and high-maintenance frameworks can't keep up with today's threat landscape." Modern security operations require a more agile approach.

TTA Vs. Traditional Metrics

(MTTR, MTDD, Etc.)

For years, security teams have tracked metrics like Mean Time to Detect (MTDD) – the average time to identify a threat – and Mean Time to Respond (MTTR) – the average time to contain or remediate a threat.

These metrics gauge how well a SOC reacts to incidents after they occur. Time to Automation (TTA), by contrast, is a proactive metric. It measures how fast the team can implement a new automated defense or process once a need is identified. In essence, TTA captures the agility of your security operations: the shorter the TTA, the quicker you can deploy countermeasures to new attack techniques or emerging risks.

Traditionally, reducing MTTR and MTDD has been a priority – for example, minimizing the dwell time of attackers in your network. But focusing solely on these reactive metrics misses a growing part of the picture. If your team can detect and remediate an incident in hours (good MTTR), that's laudable – but what if you could have automated

that response in advance, preventing hours of manual effort in the first place? This is where TTA comes in.

In 2025, experts argue that TTA is the single most important metric for security to focus on, even more than MTTR. The reasoning is straightforward: speed is survival in cybersecurity, and if it takes weeks or months to automate a response workflow, your organization is perpetually in reactive mode. Every day of delay gives adversaries an opening to exploit.

By contrast, a low (fast) TTA means your defenses can evolve almost as quickly as the threats. It's not that MTTR and MTDD cease to matter – rather, a fast Time to Automation directly improves those traditional metrics. Organizations that aggressively automate security processes have demonstrated orders-of-magnitude improvements in response times. Case in point: companies with extensive automation have reduced their incident response times by up to 99% in some scenarios. While that figure is striking, it underscores how automated workflows (for detection, containment, ticketing, etc.) can shrink response intervals from hours to seconds.

In other words, TTA is a leading indicator for how well you will be able to minimize detection and response times in the future. Security teams already recognize this shift. In BlinkOps' State of Security Automation report, 45% of organizations admitted it took them as long as two to three months to fully deploy their most recent security automation, while only 15% achieved automation within a month. This lag is becoming untenable "in an environment where attackers move in seconds".

Traditional metrics only measure how fast you react after an incident is detected; Time to Automation measures how fast you can prepare for and even preempt incidents, by getting new automated controls in place. In the face of rapidly evolving threats, TTA has become a strategic metric that can determine whether a security program remains one step ahead of attackers – or falls irreparably behind.



Faster Automation = Fewer Breaches And Less Burnout

Does accelerating Time to Automation actually pay off? Evidence from both data and real-world scenarios says yes. Fast automation can dramatically reduce the likelihood and impact of breaches, while also relieving the operational burden on security teams.

From a breach mitigation standpoint, the correlation is clear. Organizations with high automation maturity experience far quicker incident containment and lower breach costs. According to IBM's global analysis, companies that extensively deployed security AI and automation identified and contained breaches 108 days faster on average than those with no automation – 247 days vs. 355 days – and saved approximately \$2.2 million in breach costs as a result. This huge time savings (roughly a 30% shorter breach lifecycle) means attackers have far less dwell time to do damage. Other studies echo the benefit: breaches are consistently more costly and longer-lasting at organizations that haven't automated their security, whereas those who have invested in automation cut down both response time and financial impact significantly. In practical terms, a breach that might

take an unautomated company until November to fully contain could be cleaned up by September if automation is in place. Faster containment not only limits damage – it also reduces the extensive labor of investigation and recovery, which is where much breach cost accrues.

Real-world examples illustrate how low TTA can thwart incidents that would otherwise escalate. Consider the Log4j zero-day vulnerability (December 2021) as a representative scenario. In organizations where creating a new detection and patching workflow required significant custom scripting (a “high” TTA environment), it might have taken days or weeks to roll out an automated response. During that window, attackers had free rein to exploit the flaw at scale. By contrast, organizations with a very short TTA were able to pivot within hours – quickly deploying automated scans for vulnerable systems, applying virtual patches or isolation rules, and alerting staff to indicators of compromise. This rapid reaction significantly shrank the attack surface and contained the threat before it caused major damage. Numerous incident post-mortems show that speed of response is critical; automation gives that speed. A study of 2023 breaches even found that companies suffering incidents often cite slow manual

processes as a contributing factor – over 50% of breached organizations reported high staffing and skills shortages, indicating they couldn't respond fast enough with the resources they had.

Faster automation helps mitigate breach risk and relieves the chronic operational burden placed on security analysts. In most SOC environments, teams handle a constant deluge of alerts. Without automation, analysts must devote hours each day to repetitive tasks such as triage, enrichment, and initial investigation. These efforts consume time and attention that could be applied to more strategic or high-risk issues.

Organizations that automate frontline processes report significant efficiency gains. Automating enrichment and correlation workflows across tools can reduce manual triage by multiple hours per analyst per week. Scaled across a team, this frees up hundreds of hours annually, allowing teams to reallocate that time to proactive threat hunting or in-depth investigations.

Additional studies show that automating threat research tasks—such as extracting indicators, matching attack patterns, or linking vulnerabilities to assets—can reduce false positives by up to 40% and save hundreds of engineering hours each year. As noise decreases, analysts regain bandwidth to focus on meaningful alerts.

Burnout among security professionals is a measurable and growing issue. According to the 2024 Stress & Burnout in Cybersecurity report from MultiTeam Solutions, over 50% of respondents expected to experience burnout within one year if workplace conditions remained unchanged. The top contributors were alert fatigue, repetitive workflows, and lack of support. These are precisely the areas where automation has the most immediate impact.

By making Time to Automation a core metric, organizations increase their ability to deploy new workflows quickly, reduce reliance on manual labor, and preserve the well-being of their teams. TTA measures not only technical agility but also operational sustainability. When automation timelines are short, breach response is faster, fatigue is lower, and teams are more capable of maintaining long-term performance under pressure.



Agentic AI And LLMs: Accelerating Automation

A major reason TTA is becoming the focal metric in 2025 is the rise of new technologies – particularly agentic AI and large language models (LLMs) – that enable dramatically faster automation timelines.

Agentic AI refers to AI systems (often powered by LLMs) that can act as autonomous “agents,” making decisions and performing tasks without step-by-step human direction. In the security realm, agentic AI can observe input (like an alert or incident report), analyze context, and execute an appropriate sequence of actions – essentially functioning like a tireless Tier-1 analyst or automation engineer that works at machine speed. This has game-changing implications for TTA.

LLMs (Large Language Models) such as GPT-4 or similar have the ability to understand natural language and even generate code or scripts. This allows a new paradigm: instead of a human writing a complex playbook in a SOAR platform, an analyst can simply describe

the desired workflow in plain English and let an AI-driven system generate the automation. In effect, LLMs “write the playbooks” for you. This vastly reduces the time and skill needed to implement a new automated process – what once took weeks of coding might now be built in hours or minutes by an AI assistant. For example, an LLM-based automation tool can integrate with your ticketing, firewall, and SIEM APIs and, when given a high-level instruction (“isolate any host showing X malware signature and open an incident ticket”), it can produce the necessary workflow on the fly. Early adopters are reporting an order-of-magnitude acceleration in automation development.

In fact, one security automation platform observed
10× to 100× faster Time to Automation
when leveraging AI agents and LLM-driven no-code
builders, compared to traditional methods

While that is a vendor-specific figure, it illustrates the potential scale of improvement – what used to require a dedicated team can now sometimes be achieved by a single analyst teaming with an AI.

Agentic AI goes further by dynamically adapting and acting in real-time. An AI agent in a SOC could, for instance, receive an unusual alert, perform complex triage steps (consult threat intel, gather system data, correlate events across logs), and decide on a containment action – all autonomously. The SANS Institute describes agentic AI as a “cutting-edge use of generative AI that surpasses SOAR’s limitations by automating complex triage and investigation processes that have long hindered automation.” These AI agents can handle multi-stage decision-making and edge cases that static playbooks struggled with, finally addressing bottlenecks that kept some incident response tasks manual. In doing so, agentic AI fulfills the long-promised vision of a self-driving SOC, where mundane incidents are resolved end-to-end without human intervention. This directly shrinks TTA because the moment a new pattern or need is identified, an AI agent can be authorized to take on that task immediately, without waiting for a human to formalize a playbook.

The industry is moving quickly to embrace this capability. Over half of organizations plan to deploy autonomous AI agents for real-time threat detection and enforcement in the next few years.

In a BlinkOps survey, **53% of security teams said they intend to use AI-driven agents to bolster threat detection, and 46% plan to use them for automated policy enforcement** (e.g. blocking malicious activity as it happens)

Only a negligible 3% of respondents said they have ruled out autonomous AI entirely. This indicates that a large majority see agentic AI as the future of security operations.

Crucially, these technologies don’t replace human experts but rather augment and accelerate them. An AI assistant can generate a draft automation in seconds, which a human can then review and fine-tune – dramatically shortening the iteration cycle. Or the AI can handle 80% of low-level incidents, freeing human analysts to focus on the 20% of truly complex cases. By leveraging LLMs and agentic AI, organizations can drive their Time to Automation down to unprecedented levels, enabling them to respond to new threats almost as fast as those threats emerge. The net effect is a far more agile and scalable security posture, which is exactly why TTA is becoming the metric that top-performing security teams obsess over in 2025.

Measuring And Improving TTA: A Practical Guide

Adopting Time to Automation as a core metric requires clearly defining how to measure it and taking intentional steps to improve it. Unlike traditional metrics that have well-established formulas, TTA can initially seem abstract – but it can be broken down into concrete components. To effectively quantify TTA in your environment, consider tracking the key stages of your automation process:

1

Ideation

How long does it take to identify or design a new workflow that addresses a security need? (For example, from the moment a new threat is discovered or a manual pain-point is recognized, until a plan for automation is formulated.)

2

Implementation

The time from deciding to create an automation to having it developed and deployed in your toolset. This often includes coding or configuring the workflow, integrating systems, etc.

3

Testing

The time spent validating the new automation (simulating the scenario, QA, and adjusting for false positives/negatives) before it goes live.

4

MTTR for the new threat

Once the automation is live, how quickly does it detect and respond to the targeted scenario? This ties back to traditional MTTR, but specific to the new capability – demonstrating the benefit of having automated it.

5

ROI (Hours Saved)

The number of analyst hours saved by the automation over a defined period (e.g. per month). This can be measured by tracking how often the automated workflow runs and estimating the manual effort each run would have required.

By measuring these components, you create a baseline for your current Time to Automation. For instance, you might find it currently takes 4 weeks to go from idea to deployed automation (ideation + implementation + testing), and that each automation saves 10 hours of work per week once active. With a baseline, you can set targets to shorten each stage. Many teams adopt an agile approach: break down big automation projects into smaller, incremental builds that can be implemented faster, thereby reducing TTA.

Track the metrics continuously and report on them alongside traditional SOC KPIs. If your ideation phase is slow (perhaps due to bureaucratic approval processes), that's an area to streamline. If implementation is the bottleneck (perhaps due to lack of developer resources), that's where new tools or training can help.

Improving TTA is as much about people and process as it is about technology. Some practical guidance includes:



Empower and Upskill Your Team

Because skilled automation engineers are in short supply, invest in training existing analysts on automation and scripting. Close to 44% of organizations say it's difficult to hire for automation/AI roles, and 35% admit they lack in-house skills to build or maintain automated workflows. Upskilling internal staff can address this gap. Notably, 68% of organizations plan to increase focus on security automation skills development per recent research – reflecting the industry consensus that talent development is key. By having more team members capable of creating automations, you avoid bottlenecks where only one or two specialists hold up progress. Consider creating a dedicated “Automation Tiger Team” or center of excellence that mentors others and propagates automation best practices across the SOC.



Leverage No-Code Platforms

One major way to cut implementation time is to use security automation platforms that offer visual workflows, templates, and AI-assisted development, rather than hand-coding everything. Modern SOAR successors and hyperautomation tools allow analysts (even those without deep coding skills) to assemble playbooks via drag-and-drop or natural language prompts. This drastically lowers the technical barrier to automation. Low-code, AI-powered tools make automation more intuitive, adaptive, and far less dependent on specialized coding skills. By adopting such platforms, organizations enable a broader set of team members to contribute to automation efforts, increasing parallelism and speed. The result is not only faster TTA but also improved morale – analysts can translate their ideas into working automations quickly, which reinforces a culture of innovation.



Modularize and Reuse

Design your automation workflows in a modular fashion with reusable components (sub-playbooks, scripts, API calls). This way, creating a new workflow doesn't start from scratch each time – you can snap together proven modules. If you've already automated IP blocking in one context, re-use that module for the next relevant playbook. Reuse accelerates implementation and testing significantly. Some leading teams maintain internal libraries of automation "building blocks" that anyone can pull from, cutting TTA for new workflows by avoiding reinventing the wheel.



Foster Cross-Team Collaboration

Often, a slow ideation or testing phase is because the security team works in a silo. Engage IT operations, development, and risk teams early when devising new automations. Their input can help identify requirements or catch issues sooner, speeding up deployment. Also, collaborate with peer organizations through information-sharing groups to exchange automation scripts and ideas – this can jumpstart your efforts for certain use cases (with appropriate security vetting). The broader your support network, the faster you can go from a known need to an implemented solution.



Set TTA Goals and Track Progress

Just as you might have a goal for MTTR ("e.g. contain critical incidents within 1 hour on average"), set specific goals for Time to Automation. For example, a CISO might set a directive: "Within the next year, we aim to automate any repeatable Tier-1 SOC task within 2 weeks of identifying it." Having a formal goal helps drive the necessary investment and urgency. Monitor TTA metrics over time and report them to stakeholders. Seeing TTA improve (e.g. from months to days) is a powerful demonstration of increased operational agility, which boards and executives will appreciate in terms of risk reduction.



Adopt Agentic AI Proactively

As discussed, technologies like AI agents can supercharge automation velocity. Pilot these capabilities in low-risk environments to evaluate their effectiveness. For example, you might deploy an AI "SOC assistant" to auto-triage phishing emails and see how well it reduces analyst workload and speeds response. More than half of organizations are already on track to use AI agents, so falling behind in experimentation could hurt your competitiveness. That said, introduce AI with proper oversight – ensure there are feedback loops where humans review AI-driven actions initially, to build trust and prevent errors. When wisely implemented, agentic AI can take your TTA from days to minutes, but it should complement a strong foundation of process and talent.

In summary, improving Time to Automation is a multifaceted effort: measure it rigorously, remove friction at each stage, equip your people with the right skills and tools, and embrace new technologies that can expedite automation safely. By doing so, you transform TTA from an abstract idea into a manageable, quantifiable metric that drives day-to-day decision making. The payoff for sharpening this metric is huge – a security organization that can rapidly adapt at machine speed, despite human resource limits. In a threat landscape where attackers continuously innovate, a low TTA could very well be the difference between business resilience and breach headlines.






The Bottom Line

As we head into 2025, Time to Automation (TTA) is coming to the forefront as the metric that encapsulates security operational excellence. The reasons are clear. A cybersecurity workforce shortage of historic proportions means we can no longer depend on throwing people at problems – we must automate to scale our defenses. Yet legacy SOAR tools and traditional approaches have left many teams automating too slowly, with rigid playbooks that can't keep up with agile attackers. The focus on mean-time-to-detect and respond, while still important, addresses only the symptoms of incidents after they occur. TTA addresses the root: it measures how quickly we can empower ourselves with automated defenses before or immediately as incidents unfold. By minimizing TTA, organizations inherently improve all other outcomes – breaches are contained faster (or prevented outright), analysts are less overburdened, and the business faces less risk exposure.

New advancements in AI and automation technology are turning what used to be month-long projects into near-instant capabilities. Leveraging agentic AI and LLMs, security teams can iterate and deploy automations at a speed that was pure fantasy a few years ago. The tools are finally catching up to the needs. Those security leaders who prioritize TTA will position their organizations to be proactive, resilient, and scalable despite adversity. They will create a security operation that is adaptive – one that can roll with whatever new threat or mandate tomorrow brings, without missing a beat. On the other hand, organizations that stick to slow, manual methods will find themselves increasingly unable to withstand the pressure of both threat volume and talent scarcity.

CISOs should champion Time to Automation as a board-level metric, communicating that it directly correlates to risk reduction and operational efficiency. By presenting data on how improving TTA lowers incident impacts and saves resources, security leaders can gain buy-in for investments in automation platforms, AI capabilities, and training programs. In the end, focusing on TTA is about building a security muscle that reflexively responds at machine speed.

In the high-stakes cyber battlefield of 2025, the agility to automate swiftly may very well determine which organizations stay secure and which fall victim to the next breach. Time to Automation is more than a metric – it's a mindset of continuous improvement and agility that will define the next era of cybersecurity defense.



References

1. **World Economic Forum – Cybersecurity Talent Shortage.** WEF report on the global cyber workforce gap and its risks. Apr 28, 2024.
2. **BlinkOps (BusinessWire Press Release) – State of Security Automation 2025.** Survey of 1,000+ security professionals on AI-driven automation, TTA, and agentic AI adoption. Apr 23, 2025.
3. **IBM Security – Cost of a Data Breach Report 2024.** Industry study by IBM/Ponemon; organizations with extensive AI-driven automation contained breaches 108 days faster with \$2.2M lower costs. 2024.
4. **BlinkOps Blog – “Time To Automation (TTA): The single most important security metric for 2025.”** Blog by Gil Barak discussing skills shortages, legacy SOAR limits, and the urgency of TTA. Mar 3, 2025.
5. **BlinkOps Blog – “From Legacy SOAR to AI-Driven Security: How TTA Became the New Standard.”** Discussion of legacy SOAR challenges and benefits of low TTA with AI-driven automation. 2025
6. **MSSP Alert – “Why the World’s Top MSSPs are Ditching Legacy SOAR for Hyperautomation.”** Article outlining legacy SOAR limitations (scalability, multitenancy, maintenance) and newer alternatives. 2024
7. **MultiTeam Solutions. (2024). Stress & Burnout in Cybersecurity: The Risk of a Thousand Papercuts.** [PDF]
8. **SANS Institute Webcast – “Agentic AI-Powered SOC’s: Overcoming SOAR’s Unfulfilled Promises.”** Conference session description explaining how generative AI agents automate complex SOC processes beyond legacy SOAR. Oct 2024.
9. **Secureframe – “110+ Latest Data Breach Statistics for 2025.”** Compilation of breach data; includes stats on staffing shortages in breached orgs and the impact of AI/automation on breach costs and times. 2025.



blinkops.com