kaspersky

Optimizing SOC operations with tailored playbooks: features of effective playbook development

Introduction: what a SOC playbook is (and isn't)

Many scenarios that teams encounter in a security operations center (SOC) eventually resurface, like waves returning to shore. They may look unique, but the underlying patterns are the same. SOC playbooks, which are step-by-step instructions tied to incident categories, are labor-saving tools that help you address these scenarios.

A playbook gives analysts a clear path forward under time and pressure constraints. It shouldn't be confused, however, with an incident response (IR) plan, which is the blueprint that defines an organization's high-level structure, roles and policies. While the IR plan guides strategy, such as which regulators must be notified after a breach, it lacks the granular, practical direction an analyst requires during an event.

Playbooks help by breaking down complex categories of threats into specific, repeatable actions that analysts can trust. This ultimately speeds up response and reduces risk. Without them, analysts must translate broad policies into action, often in the midst of a crisis. And if they can't grasp the next step, they may find themselves in stasis when every second counts.

SOCs that maintain playbooks alongside an IR plan cover both strategy and execution. The plan defines who does what and why, while the playbook describes how to do it. Together, these tools help to build resilience in the face of recurring threats.

Sequence counts – IR plan → detection capabilities → playbooks

The sequence of preparation matters when developing playbooks – it must be logical. First you should develop the IR plan in coordination with IT, risk management and other key stakeholders. Each group has responsibilities when an incident affects systems, people or reputation, so it's important that they're aligned.

The SOC can then focus on building its detection capabilities, because it makes little sense designing playbooks for threats you cannot identify. This does not, however, mean a SOC should stop at a narrow set of detections and consider it "job done." A limited view of threats leaves analysts unprepared, and poor response to any possible incident is a failure.

> Before developing playbooks you need to fully understand your detection capabilities. You don't initially need playbooks for something you can't detect.

Andrey Tamoykin, Kaspersky Cybersecurity Expert

The priority should be playbooks for incidents the team can detect with confidence before expanding coverage to more scenarios as visibility improves. This logical approach balances readiness with realism:

- The IR plan ensures broad alignment.
- Detection defines what can be acted on immediately.
- Playbooks translate those capabilities into consistent action.

The playbook library grows alongside detection capability over time, covering not just the known and expected but also the less common and more complex.

Who do playbooks benefit and how?

Playbooks bring value across the SOC, but their key impact is on day-to-day execution, as they provide both structure and efficiency. Teams can thus respond in a coordinated way with time saved debating next steps. This is important in the current landscape, with so many SOCs being overworked.

In terms of individuals, analysts benefit the most because playbooks give them clear, repeatable instructions tied to specific scenarios. This means that instead of guessing or reinventing the process with each alert, they can follow a tested path. Uncertainty is reduced and newer or more junior analysts can get up to speed more quickly. (For some perspective, 46% of InfoSec pros said it took more than a year before they were comfortable or confident in their first cybersecurity role.[1])

> By optimizing the response area, you increase the overall performance of the whole SOC – but analysts benefit more than all others.

Andrey Tamoykin, Kaspersky Cybersecurity Expert

Playbooks also limit decision fatigue. During a long shift or fast-moving incident, having a predefined sequence of actions reduces mental strain. The result is faster, more consistent responses across the team. Over time, this consistency strengthens the SOC's reliability and allows leaders to focus on improving overall strategy and resilience.

[1] Kaspersky, Portrait of Modern Information Security Professional, (Kaspersky Daily, 2024).

Continuous improvement and triggers for review

A playbook that is never updated quickly loses its value. Threats evolve, tools change and lessons emerge from real-world incidents. Playbooks must be reviewed on a regular schedule, ideally at least once a year. This ensures they reflect current processes, technology and business priorities.

> Almost every activity in a SOC is about continuous improvement — and playbooks are no exception.

Andrey Tamoykin, Kaspersky Cybersecurity Expert

Event-based reviews are just as important. Any time there is a change in detection logic, a shift in infrastructure or a significant incident, the related playbook should be revisited. These are moments when gaps are exposed and improvements become clear. Updating in response to such events ensures the SOC is always building back stronger.

By combining regular reviews with event-driven updates, organizations can maintain playbooks that grow with the SOC. The result is a resource that remains trusted and effective over time.

What "good" looks like – the metrics that matter

A strong playbook is not only clear and practical but also delivers measurable results. The right metrics show whether a playbook is working as intended. One key measure is mean time to triage: how quickly analysts can confirm whether an alert is a true positive or a false positive, so resources can be focused where they matter. Quality of triage is also reflected in false positive and false negative rates. Too many false positives waste time, while false negatives mean real threats are being missed.

> Time to triage is one of the most important metrics – we need to validate security incidents as fast as possible.

Andrey Tamoykin, Kaspersky Cybersecurity Expert

Mean time to respond is another vital metric, because it tracks how quickly the SOC can contain an incident and provide recommendations for mitigation. Delays increase risk, while speed proves the team's effectiveness.

Getting playbook automation right

Automation coverage matters too. Tracking the percentage of tasks automated in each playbook shows where efficiency is improving and where manual effort dominates.

But while automation can transform playbooks, it shouldn't be the starting point. A well-tested manual playbook is the foundation, ensuring processes are sound before tasks are automated. From there, automation can be layered in stages. Basic enrichment speeds up access to context, while task orchestration links actions across tools. Human-in-the-loop keeps analysts engaged where judgment is required.

> It's better to start developing playbooks without automation than not having them at all.

Andrey Tamoykin, Kaspersky Cybersecurity Expert

Full automation is possible, but only for low-risk and well-understood scenarios. Human confirmation is crucial for high-impact actions, such as isolating business-critical hosts or deleting accounts. In these cases, blind automation can cause more harm than the threat itself. The goal is balance: automation should remove repetitive work while analysts retain oversight of sensitive decisions. This approach – when executed correctly – creates a SOC where technology amplifies human judgment rather than replacing it.

Playbook scoping and structure

Playbook scoping starts with incident categories, typically 20 to 30 that the SOC can reliably detect. Each category should have its own playbook, with possible branches to cover common variants. A solid playbook balances shared core steps, such as triage and containment, with tailored actions for specific threats like viruses or backdoors. This ensures consistency without losing precision.

> We don't need a playbook for a backdoor. We need a playbook for malware infection – with special statements for a backdoor if it is really required in your particular case.

Andrey Tamoykin, Kaspersky Cybersecurity Expert

In smaller SOCs, the SOC manager often leads development and approval. In larger ones, a research lead or subject matter expert validates each playbook for relevance, necessity and alignment with detection capabilities, ensuring the library's effectiveness.

Practical rollout: start simple and grow with your capability

Rolling out playbooks should start simple. Begin with a handful of checklist-style tasks that address the most common, repeatable incidents. As your detection capabilities and technology mature, expand the library to cover more categories and introduce automation where it adds obvious value. The key is to grow playbooks at the same pace as the SOC's capability.

> You don't need to spend more time on the playbook than it will save you.

Andrey Tamoykin, Kaspersky Cybersecurity Expert

You should avoid investing time in complex or theoretical playbooks that bring little efficiency in practice. A focused, evolving approach ensures playbooks remain useful, manageable and aligned with the team's real-world needs.

Key takeaways

Effective incident response starts with preparing in the right order: build the IR plan, assess detection capabilities and then create playbooks. Success should be measured with clear metrics, including time to triage, time to respond, false positive and negative rates, and automation coverage.

Remember that playbooks are not static; they must be reviewed regularly and after any major change to your tools or infrastructure. While automation can add speed and efficiency, it must be balanced with human expertise for critical decisions.

The best results come from starting simple, proving value early and scaling your playbooks in line with the SOC's maturity and capability.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With over a billion devices protected to date from emerging cyberthreats and targeted attacks, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection, specialized security products and services, as well as Cyber Immune solutions to fight sophisticated and evolving digital threats. We help over 200,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

www.kaspersky.com