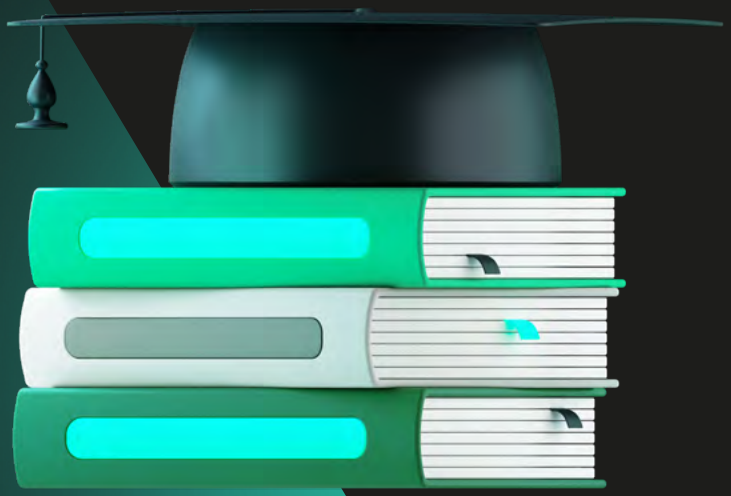
kaspersky



Effective onboarding and mentorship in SOC teams

This essay was written by Renat Gimadiev, SOC Solutions Expert in Kaspersky's Expert Security Solutions department. It highlights the critical role of structured onboarding and mentorship in modern SOCs, showing how intentional programs can accelerate analyst readiness, improve retention and reduce burnout.

It draws from real-world challenges to outline actionable strategies that help new hires become productive, including:

- Structured onboarding plans (e.g., 30/60/90-day models with balanced theory and practice)
- Defined mentorship roles and responsibilities (mentor, buddy, supervisor, mentee)
- Practical knowledge transfer techniques, including shadowing, guided practice and feedback loops
- Key performance indicators (e.g., time to independence, QA error rate and mentor satisfaction)

By using these approaches, organizations can steadily build up new hires into confident analysts who can strengthen a SOC's detection, response and resilience.

Why onboarding and mentorship matters

In a security operations center (SOC), people are the most critical asset. Advanced tools and well-defined processes are vital, but it is the human factor that ultimately determines how effectively threats are detected, investigated and neutralized.

A new analyst's first weeks in the SOC are the most crucial. Without a clear onboarding path, colleagues' empathy and support, they risk becoming overwhelmed, underperforming, or leaving prematurely. Similarly, the absence of structured mentorship leaves knowledge transfer to chance, which can lead to wavering investigation quality, slower response times and missed critical incidents.

The data confirms this risk: in the 2023 (ISC) Cybersecurity Workforce Study survey, more than 20% of SOC analysts reported high stress and burnout, with many leaving their role within two years.[1] Studies also show that it typically takes between six and nine months for an analyst to reach independent productivity if onboarding is unstructured. In contrast, organizations that invest in structured mentorship programs can increase their retention rates by 20–30% on average. In practice, this might mean pairing every new hire with a mentor for their first investigations.

Effective onboarding and mentorship programs address these challenges by providing clarity, structure and ongoing guidance. They help new hires become productive faster, make the team more resilient during high-pressure incidents and keep people from leaving too soon. Equally important, they encourage ongoing learning rather than a one-time training push.

Clear roles and expectations

The success of onboarding and mentorship depends on clearly defined roles. While each SOC may have its own staffing structure, the following roles are highly recommended:

1

Supervisor (SOC Manager/CISO) – Oversees the onboarding and mentorship program, aligns it with business objectives and compliance requirements, and reviews progress over time.

2

Mentor (Senior Analyst) – Guides the new hire through processes, tools and team culture; provides regular feedback; and shares real-world experience.

3

Buddy (Shift Analyst) – Serves as an informal go-to person for day-to-day questions, helping navigate workflows and tools.

4

Mentee (New Hire) – Actively participates in learning, seeks feedback, documents lessons learned and progressively takes on more responsibility.

[1] ISC. How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. (ISC 2023).

Designing the onboarding journey

A well-structured onboarding process ensures that the new SOC analyst gains knowledge and confidence without being overloaded with routine tasks and difficult cases. One of the most popular and proven models is the 30/60/90-day plan, which balances theoretical learning with practical exposure during the probation period. Here is a brief outline:

First 30 days — Orientation and observation:

Introduction to SOC mission, team structure and escalation paths; basic tool navigation; shadowing mentors; meeting with different teams like IT, Legal and other departments. At this stage, new hires can also participate in tabletop exercises or gamified mini-scenarios, which help them practice without the pressure of real-time incidents.

Days 31–60 — Guided practice:

Handling low-severity alerts with supervision, running predefined queries, drafting tickets and contributing to knowledge-base articles. This phase should also include virtual shadowing sessions and exposure to other security functions (e.g., brief rotations with threat hunters or forensics teams) to provide broader context.

Days 61–90 — Independent operations:

Taking ownership of tier-one triage, leading investigations with mentor review and beginning to mentor the next group of mentees. By this point, analysts should demonstrate adaptability, but progression speed may vary – some may be ready in 60 days, while for others it might take up to 120 days. The key is maintaining weekly feedback loops between the mentee, mentor and SOC manager to ensure alignment and prevent important details from being missed.

In conclusion, every SOC analyst learns differently – some rush through the basics in weeks, while others need more time to absorb new concepts fully.

Building an effective mentorship program

Mentorship is evidently a structured process with defined stages and measurable outcomes. Don't forget to follow these steps in your mentoring journey:

Observe → co-pilot → lead: mentee first shadows the mentor, then co-pilots during tasks, and finally leads incidents with minimal intervention.

Cadence: weekly 1:1 meetings, daily shift briefs, formal skill check, obstacles overview, etc.

Best practices: limit mentees per mentor, e.g, maximum two mentees per one mentor; document feedback; celebrate milestones; and ask for feedback regularly.

KPIs

Metric	Definition	Target	Why it matters
Time to independence	Days until a new hire can handle basic incidents solo	60–90 days	Reduces team workload
QA error rate	Percentage of incident tickets with deviations from standards	<5% after 90 days	Ensures quality and compliance
Retention rate	Percentage of hires still in role after 6–12 months	>85%	Reduces recruitment and training costs
Mentor/mentee satisfaction	Feedback from structured surveys	≥4/5	Indicates engagement and program value
Runbook adherence	Percentage of steps followed correctly	>95%	Maintains consistency and audit readiness

Best practices: pair tool training with process context, maintain and regularly update a living knowledge base, recognize and reward best mentors, and use blended learning formats.

Common pitfalls: overloading mentors, focusing only on hard skills, inconsistent feedback from mentees, and treating onboarding as one-time instead of an ongoing process.

Conclusion

Onboarding and mentorship go far beyond simple HR checklists – they are strategic investments that directly impact SOC performance and quality of service. With a structured program, analysts get up to speed sooner and are less likely to burn out. That stability means fewer hiring cycles and lower costs for the organization.

Beyond productivity, these initiatives enhance the quality of detection and response. Analysts who are onboarded effectively are more confident in handling incidents, follow playbooks and runbooks with greater precision, and contribute to the continuous improvement of the SOC knowledge base. Without mentorship, critical know-how can leave with the person – like that one analyst who remembers all the SIEM quirks and tricks.

From a business perspective, this translates into measurable outcomes: faster mean time to detect (MTTD), shorter mean time to respond (MTTR), improved audit readiness and stronger compliance posture. For leadership, investing in people creates a resilient SOC culture where analysts feel supported, valued and motivated to grow.

In the end, the best tools won't help if people aren't ready enough. Strong onboarding and mentorship build the kind of team that can react fast when the next threat hits. No one knows when exactly that might happen – so the team must be ready and improve their skills continuously.