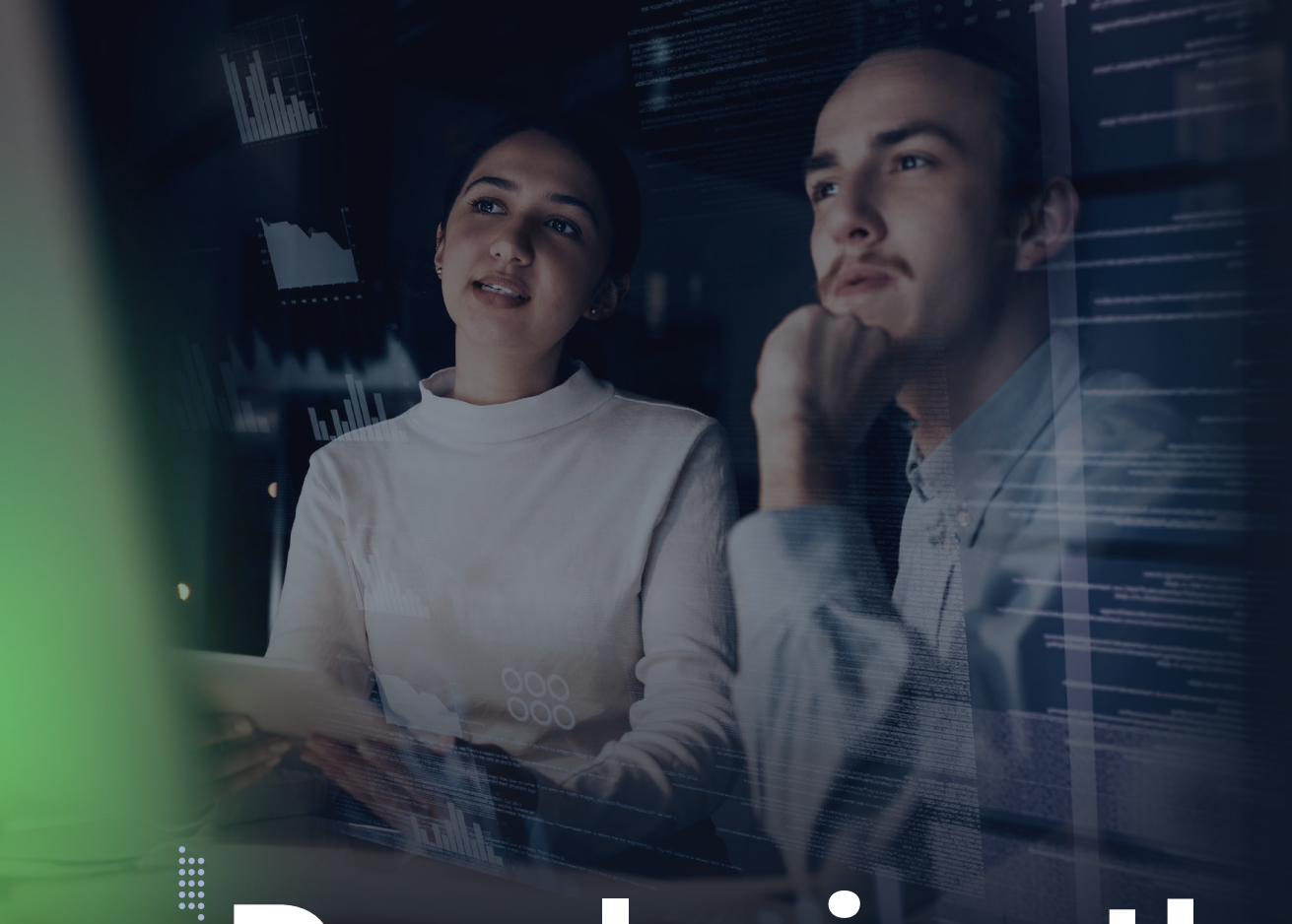


Developing the modern SOC analyst:

A report on 360° upskilling

BY HACKTHEBOX

Based on survey insights from 400 active cybersecurity professionals

2023

SUMMARY

SUMMARY

The rampant talent and skills shortage in cybersecurity is arguably most notable in SOC teams. Demand[1] for security analysts alone is expected to be 150% higher than the average growth projected for all occupations, and it's easy to see why:

Migration to cloud technology and adoption of remote work continues to rapidly widen the scope and responsibilities of the SOC. Traditional attack surfaces and network perimeters are expanding to become more public and porous, exposing a host of new challenges and risks that teams must be able to proactively detect and defend.

Ultimately, adapting to today's turbulent threat landscape requires SOC staff—especially analysts on the frontline of threat detection, triage, and response—to constantly upskill and stay ahead of increasingly sophisticated attacks and emerging risks.

But which fundamental skills does the modern SOC analyst need to succeed in their role?

We surveyed 400 active cybersecurity professionals in the Hack The Box (HTB) database to find out. This report focuses on discovering what those on the frontlines of cybersecurity consider essential skills for SOC analysts. We also explored the career ambitions of offensive and defensive security professionals (and how leaders can adapt their upskilling strategy in response to retain and engage top talent).

KEY FINDINGS

KEY FINDINGS

Defensive security professionals express a strong interest in offensive security

This presents leaders with an opportunity to simultaneously engage, retain, and “reskill” existing employees. 360-degree upskilling programs—that balance offensive and defensive security training—will pave the way for stronger security postures and engaged staff.

46%

Incident Handling Processes & Methodologies

Fundamental skills set the foundation for the analyst. **46%** of incident responders rated **knowledge of Incident Handling Processes and Methodologies** as the most important knowledge domain.

40%

Cloud security skills

Over **40%** of professionals believe that **cloud security skills** will be a key priority for analysts over the next five years.

58%

Prefer Machines

When it comes to improving Digital Forensics & Incident Response (DFIR) skills, **58%** of professionals said they **prefer Machines** (instances of vulnerable virtual machines) as their favorite way to learn.

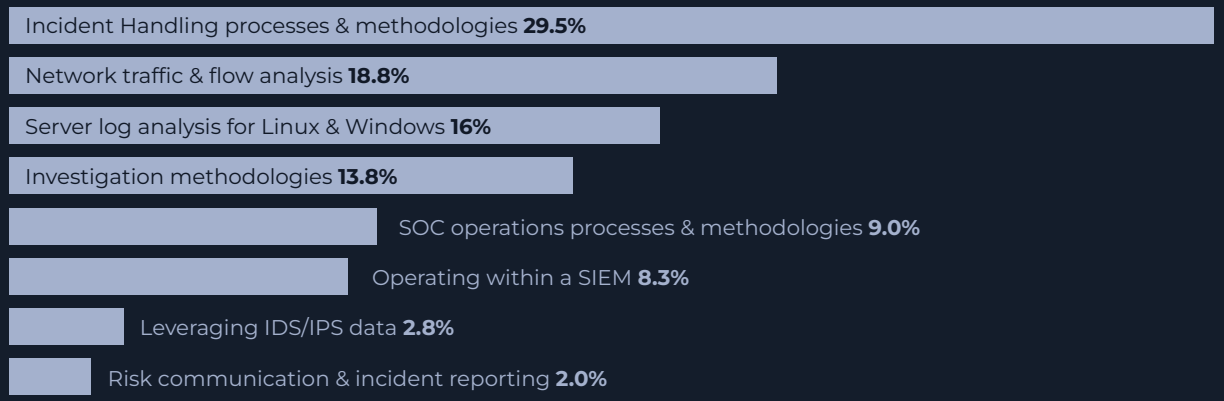
31%

Pursuing a career strictly in red teaming

Hybrid blue/red teamers are on the rise: while **31%** of professionals expressed an interest in **pursuing a career strictly in red teaming,** most want to explore both offensive and defensive cybersecurity careers.

Mastering the fundamentals of incident handling and traffic analysis is key

Most important knowledge domains for SOC analysts



Despite defending an expanding network perimeter proliferated by complex systems, fundamental skills are still a priority for analysts.

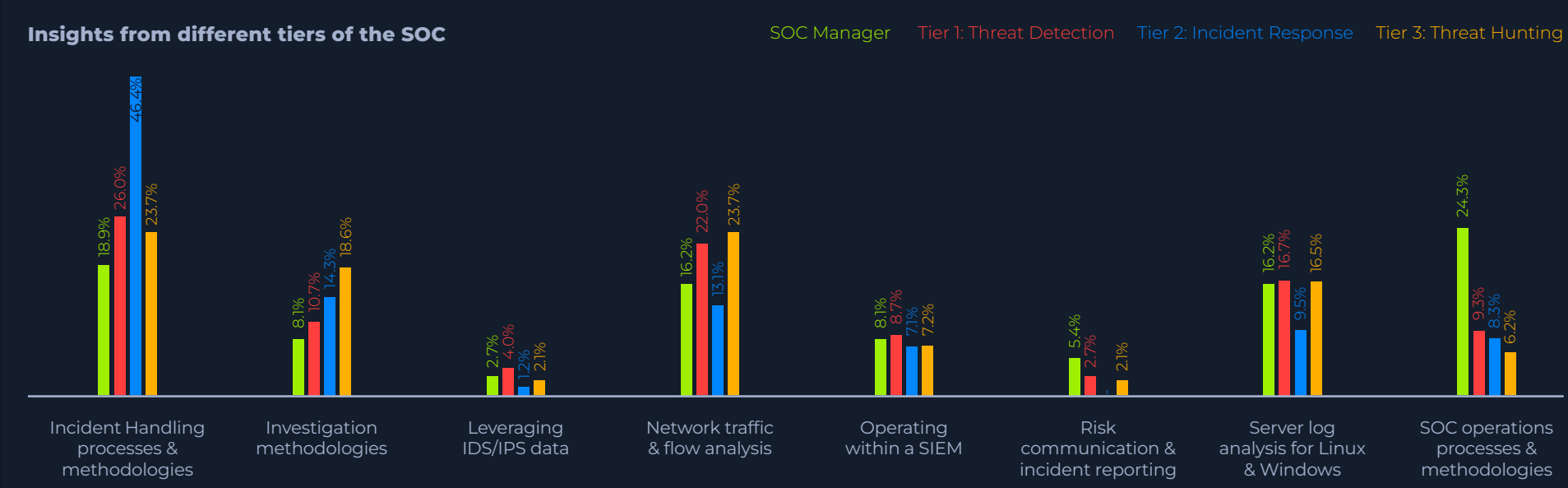
Nearly a third (29.5%) of professionals rated Incident Handling Processes and Methodologies to be the most important knowledge domain for SOC analysts to master. Alongside Incident Handling Processes and Methodologies, Network Traffic and Flow Analysis, and Server Log Analysis skills ranked second and third respectively on the list of essential skills.

This highlights the need for analysts to develop well-balanced expertise across the core domains of cybersecurity to identify and monitor events, accurately analyze alerts, and help SOC teams implement security measures that mitigate risks before they materialize.

> “The two most challenging publicly known incidents I’ve worked on were likely the HO-Mobile data breach (which impacted 2.5 million users) and the HSE ransomware attack by Conti (which degraded Ireland’s public health services).
>
> My key takeaway from both incidents is the criticality of having efficient IR (incident response) processes and ensuring the real basics are done right.
>
> So it makes sense for any security leadership team (and up-and-coming analyst) to prioritize these essential skills, as the vast majority of incidents I’ve handled across eight years in the field weren’t triggered by APTs chaining multiple zero-day exploits to compromise an environment—human error, misconfigurations, and poor incident response processes played a key role.”

Sebastian Hague,
Defensive Content Lead
@ **Hack The Box**

SOC managers expect a broader understanding of process and methodology



Hinting at the brewing expectation of future SOC analysts to have broader skill sets and deep knowledge of processes, a larger percentage of SOC managers (24.3%) rated overall knowledge of SOC Processes and Methodologies as being more important than Incident Handling Processes and Methodologies.

In comparison, respondents who identified as working in Threat Detection and Incident Response regarded Incident Handling Processes and Methodologies as the most important skill for an analyst to be effective in their role.

While the vote for the most important skill amongst SOC tiers was distributed between Incident Handling Processes and Methodologies and Network Traffic and Flow Analysis, a significant number (46.4%) of incident responders showed confidence in incident handling as being the most important skill for analysts.

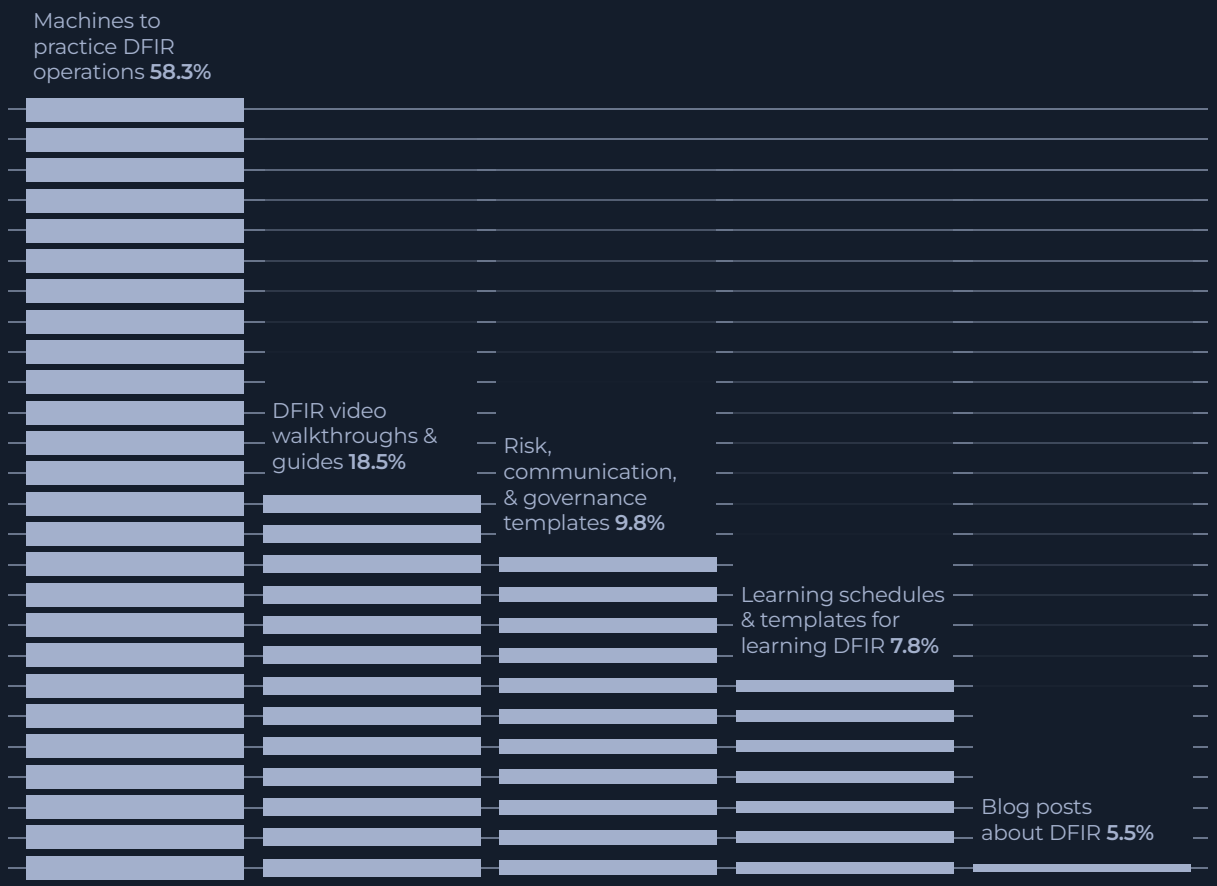
Most professionals prefer practical learning content to improve DFIR skills

With an industry-wide talent shortage and the number of threats on the rise, maintaining and acquiring new DFIR skills is critical for both existing and upcoming SOC professionals.

When asked which they were most interested in to improve their DFIR skills, over half (58.4%) of security professionals ranked practical Machines (instances of vulnerable virtual machines) as the resources they're most interested in.

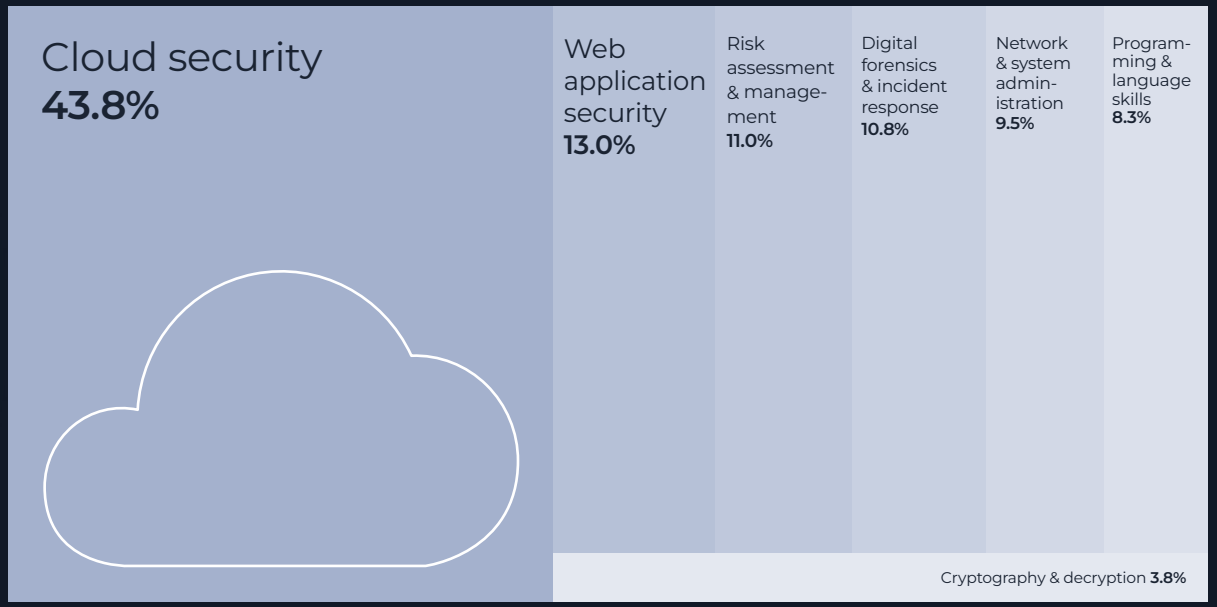
Considering that HTB is a platform dedicated to hands-on focused skills, this doesn't come as a surprise. It does, however, reinforce the growing need for hands-on and practical cybersecurity platforms to proactively upskill employees.

Preferred tools for learning DFIR skills



Cloud expertise will be essential for future analysts

Most important skill for analysts over the next 5 years



43.8% of all surveyed security professionals believe that cloud security skills will be amongst the most important for analysts in the next five years.

Increasing reliance on cloud systems introduces more complex and distributed architectures, and of course, more components and services to secure.

Analysts (and all tiers of the SOC) will need to adapt by upskilling on specific security configurations and monitoring, all while navigating a new era of shared responsibility with cloud providers.

The en masse shift to cloud environments also shows how knowledge expectations for SOC professionals are dictated by the live threat and tech landscape. Keeping up with real-world risks means skills that were once considered "bleeding-edge" can easily be rendered as "expected," even for junior or entry-level SOCs.

One example is basic-intermediate knowledge of defending against Active Directory (AD) attacks. Years ago, it was considered part of a seasoned SOC professional's arsenal, but that's no longer the case.

Since AD attacks are common practice among attackers nowadays, today's junior SOC professionals should be aware of common AD attack vectors and how to detect them. The same holds true for knowledge of defending cloud environments.

The rise of the hybrid blue (and red) teamer

Pursuing a career in red vs. blue teams

When asked which career they are looking to pursue, most professionals expressed an interest in both the offensive and defensive cybersecurity career paths. 31% expressed an interest in strictly red teaming. In contrast, a smaller number (10.5%) said they wanted to only pursue a career in blue teaming.

Furthermore, 3 in 10 users (30.8%) expressed an interest in pursuing a blue team career before moving into an offensively-oriented role.

Nearly the same amount (27.8%) of professionals, however, planned their careers the opposite way around, showing an interest in offensive security roles before switching to a career path in defensive security. As the line between attack and defense blurs, this career curiosity towards offensive and defensive security unveils an emerging type of security professional, the hybrid: a practitioner invested, and potentially versed in, both defensive and offensive security skills and methodologies.

360° upskilling programs: a modern leader's strategy to develop and retain in-house talent

Your SOC team may want to learn the skills to "anticipate" or emulate real adversaries, but do they have the chance to do so?

Traditional cybersecurity analyst roles are typically focused on identifying and mitigating security threats, often in a reactive manner. Modern analyst roles, however, focus more on preempting adversaries and designing security controls that proactively detect and prevent threats.

For SOC leaders grappling with the rampant burnout and talent shortages amongst security teams, this highlights a critical lesson in using skills development to engage, retain, and reward alert-fatigued and under-staffed teams.

Support your people in learning complimentary cyber skills like engineering, automation, and, of course, attacking—they're likely already interested in these domains.

Amidst tightening budgets and talent shortages, building in-house talent this way serves as a strategic, people-focused approach to avoiding costly vacancies and skills gaps, which only increase the risk of breaches and place additional strain on under-staffed teams.

As our survey insights show, this hybrid approach to training also offers potential higher levels of employee engagement and retention, offering staff the opportunity to "reskill" in a domain they're interested in without leaving their organization.

ABOUT HTB

ABOUT HACK THE BOX

Hack The Box specializes in distinguished practical and guided defensive and offensive cybersecurity upskilling programs aligned with the NIST NICE and MITRE ATT&CK frameworks, as well as unrivaled hands-on labs designed to help organizations close skills gaps, hire top talent, and protect infrastructure.

Loved by a global cybersecurity community of more than 2 million members, HTB is helping security leaders across the world equip their teams with the skills and expertise needed to proactively secure and protect their organizations.

Whether you're sharpening specific techniques, training up junior staff, or looking to recruit skilled cybersecurity talent, Hack The Box has a solution to fit your needs.

Measure, assess, and proactively close your organization's cybersecurity skills gap with a single platform focused on developing your cyber workforce.

Methodology

This report is based on a survey of 400 active cybersecurity professionals on the HTB upskilling platform conducted in April 2023. Professionals who identified themselves as being part of or leading a cybersecurity team were surveyed with custom questions related to the future of SOC analyst skills and their learning preferences.

Sources:
[1]: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

1.5k+
Businesses upskill with HTB

788+
CTFs, meetups & trainings organized globally

900+
Universities enrolled

2M+
Community members worldwide

2023

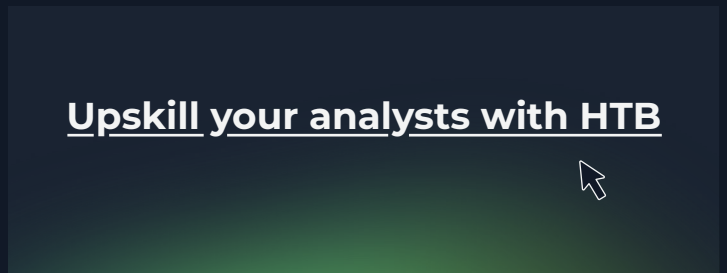
Developing the

MODERN SOC ANALYST

A REPORT BY HACKTHEBOX

HTB BUSINESS

Upskill your analysts with HTB



sales@hackthebox.com