TLP: CLEAR

RETAIL & HOSPITALITY ISAC

# BENCH MARK

Practitioner

JANUARY 2023

# TABLE OF CONTENTS

# INTRODUCTION

Information security practitioners are fundamental to securing their organizations' critical assets and information. In the inaugural RH-ISAC Practitioner Benchmark, we surveyed more than 100 practitioners to better understand the challenges and priorities staff have in executing daily job functions.

We learned that 83% serve more than one job function, which means that employees have a valuable and diverse skill set across security operations (76%), threat intelligence (66%), and risk management (66%). And, regardless of what job functions they serve, the majority of practitioners (63%) assessed their skills between the intermediate and advanced levels.

According to practitioners, vulnerability management is both the top risk their organizations face and the top initiative their teams need to prioritize in 2023, which aligns with the top initiative CISOs reported in our CISO Benchmark Report. Focus areas for practitioners include: patching, configuration management database (CMDB), asset management, and penetration testing.

When it comes to improving their teams' collective information security operations, nearly half (48%) said they need to focus on developing security architecture capabilities within the next 12 months; specifically, secure coding, DevSecOps, infrastructure-as-code, orchestration and automation, and tool integrations.

Practitioners generally have a positive outlook for 2023, with 93% who believe they have the necessary skill sets to perform their job effectively. The biggest challenge? Time management: the average practitioner spends up to 68% of a typical 40-hour work week on non-primary job functions like team meetings and pivoting between multiple tools.

We hope you find the data in this report to be insightful and offer a glimpse into the practitioner perspective. Thank you to everyone who completed the survey to give peers a better understanding your experiences. We are grateful for the work you do every day for your teams and for our community.

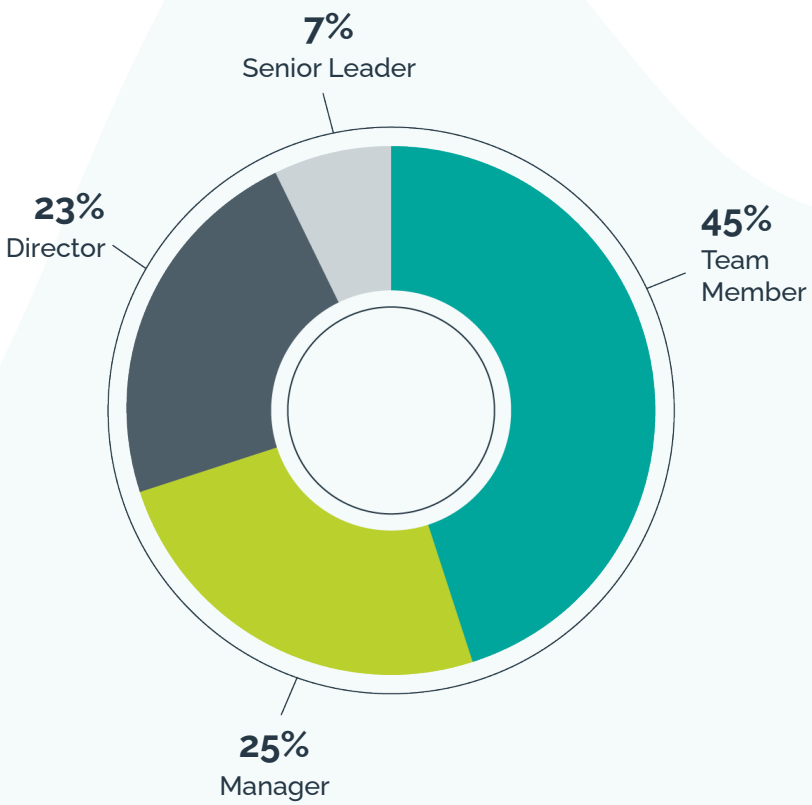
*— Kristen Dalton | RH-ISAC | Director of Strategic Engagement, Research & Analytics*

## SURVEY DEMOGRAPHICS

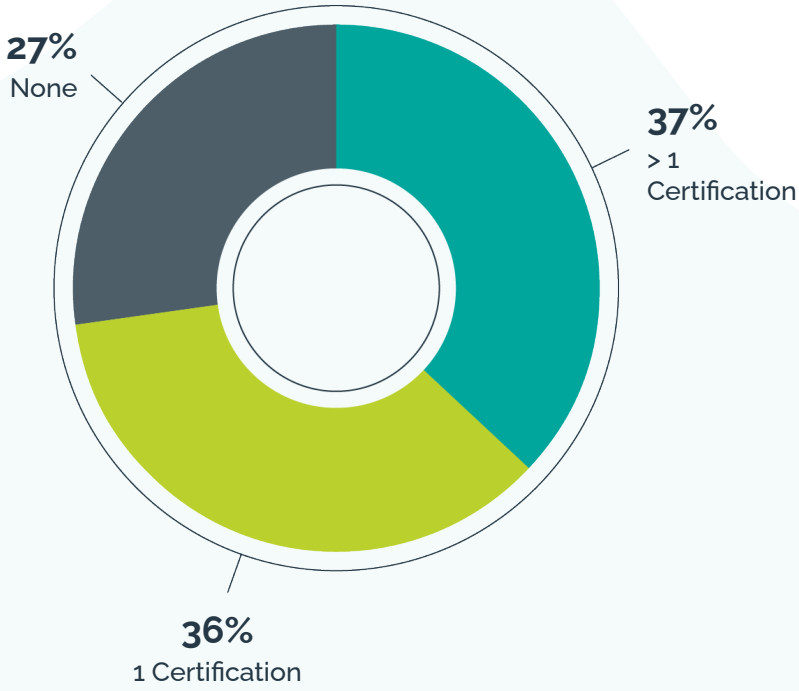
The RH-ISAC fielded its inaugural Practitioner Benchmark online in September and October 2022. It generated 105 unique responses, and all submissions were anonymous.

Nearly half (49%) of security practitioners who completed the survey manage a team, and 63% have at least one certification. CISSP (30%) and CompTIA (18%) are the most popular certifications among practitioners, regardless of role.

### Participants by Job Role




### Participants with Certifications

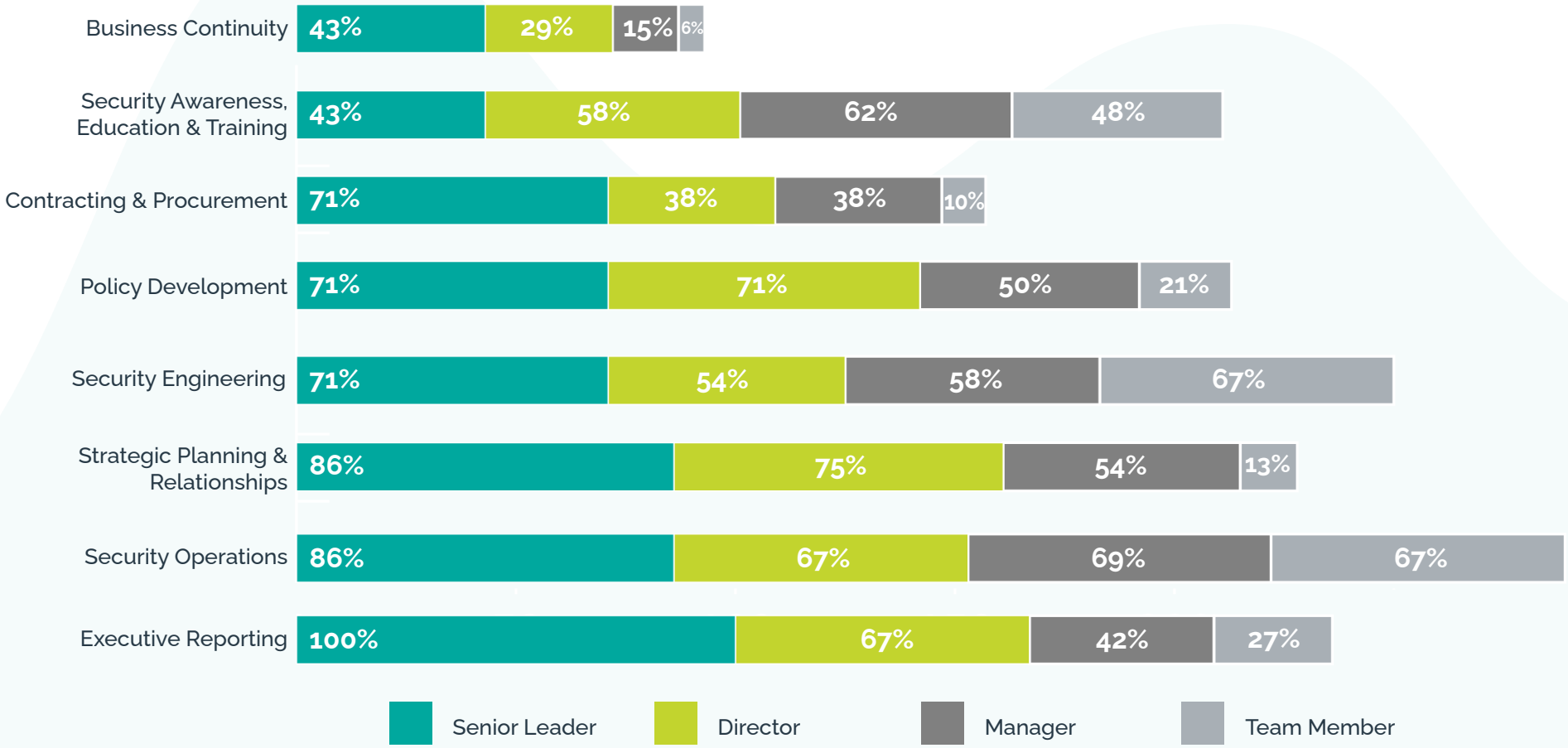


## ORGANIZATIONAL DUTIES

At least two-thirds (67%) of senior leaders and directors have executive reporting, strategic planning and relationships, contracting and procurement, policy development, security operations, and security engineering as part of their duties.

The primary duties for nearly 50% of all managers and team members are security operations, security engineering, security awareness, education, and training.

### Organizational Duties by Role

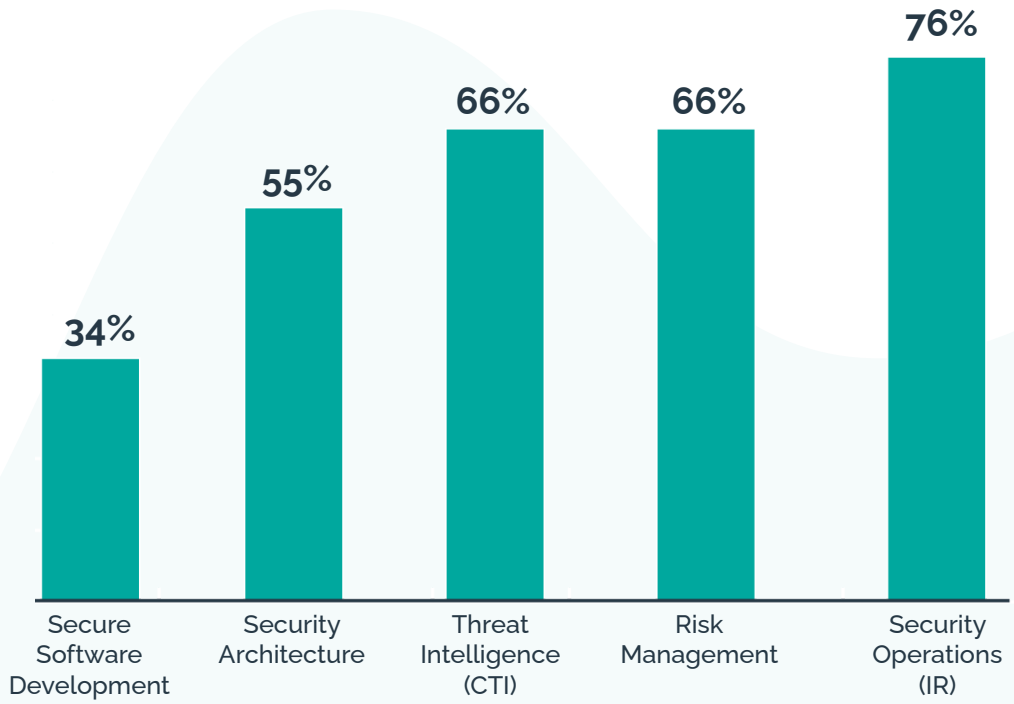


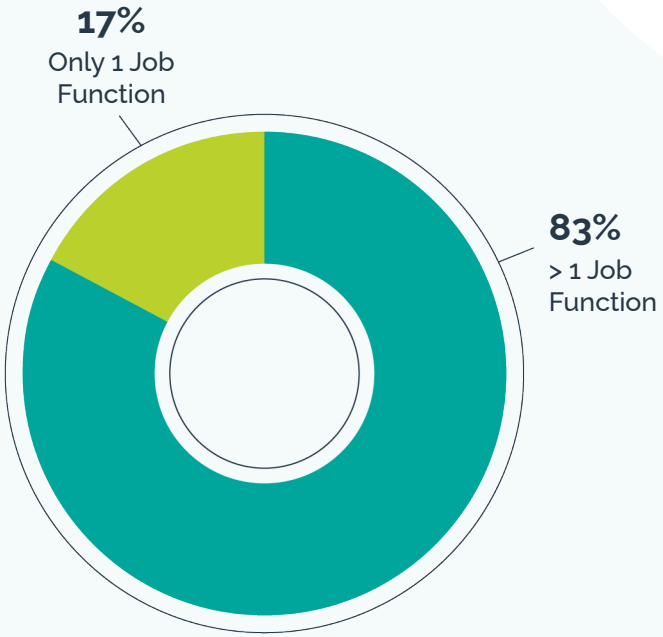
# SUMMARY OF FINDINGS

## JOB FUNCTIONS

Most practitioners wear multiple hats in their current roles, with **83% serving more than one job function**. Security operations (IR) is the top primary job function, served by 76% of practitioners, while two-thirds support threat intelligence and risk management.

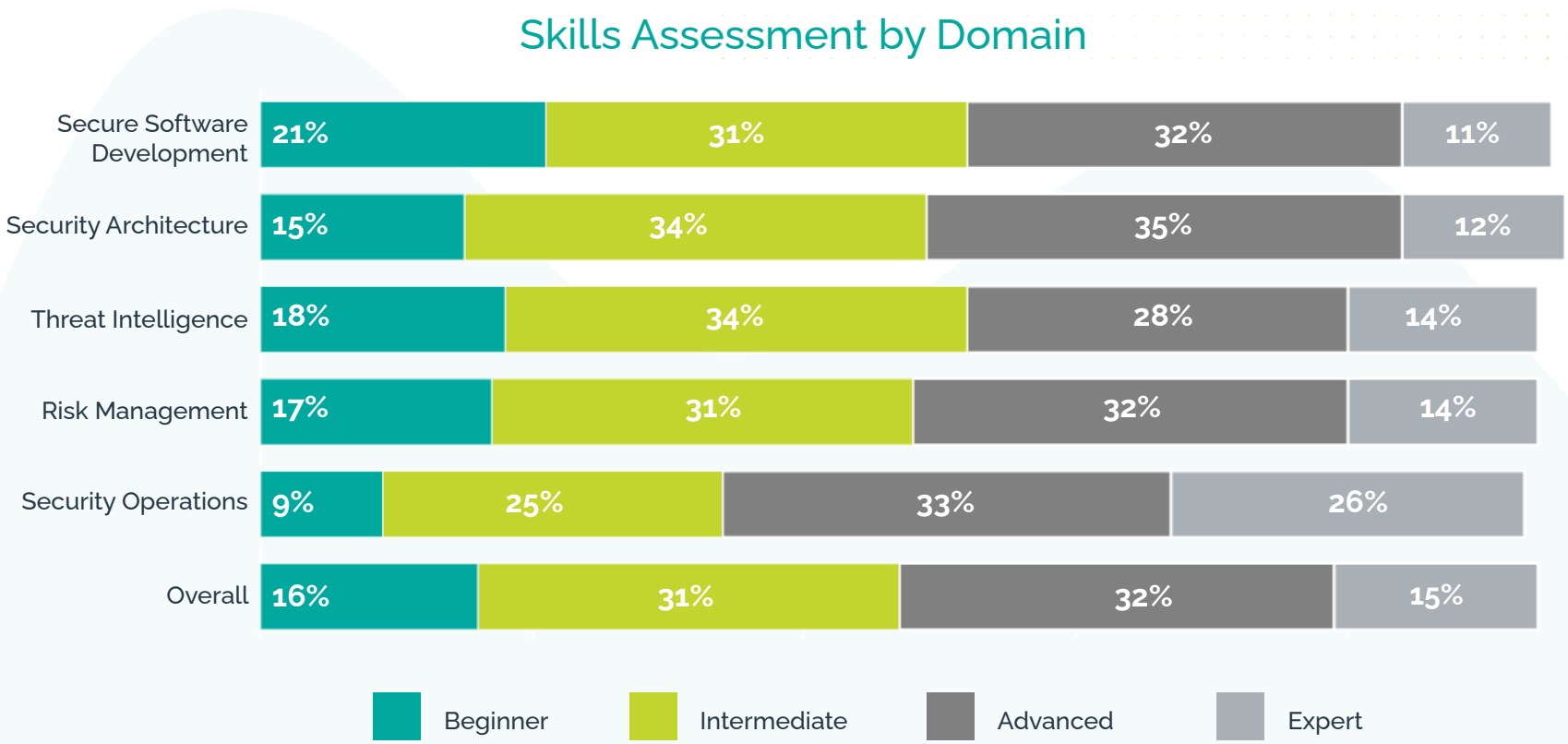
### Primary Job Functions



## SKILLS ASSESSMENT

The majority of practitioners **(63%) believe their skill sets are between intermediary and advanced**, regardless of what job functions they serve. The chart below shows how practitioners assessed themselves across each domain.



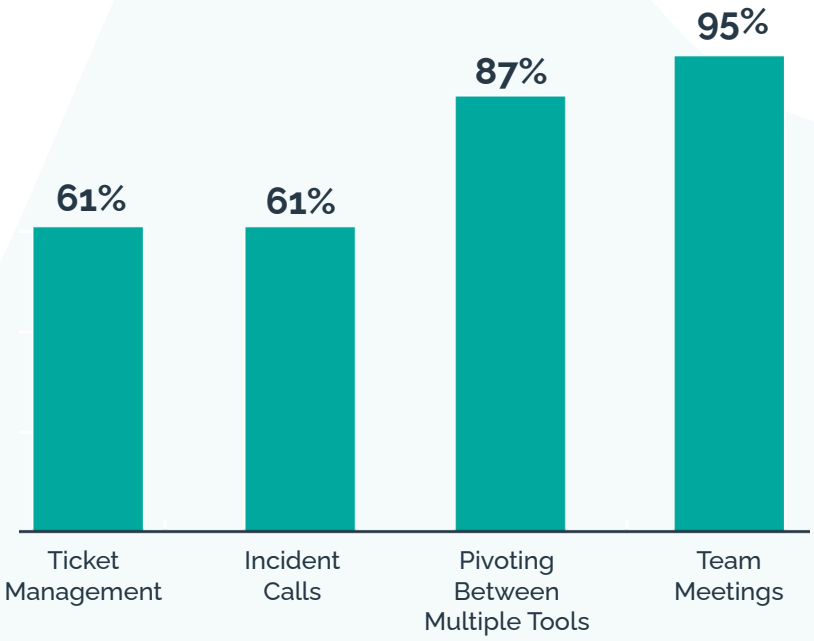

Security operations has the highest level of proficiency, with 56% ranking their skills at the advanced and expert levels, while both threat intelligence and secure software development have the lowest level of proficiency, with 52% ranking their skills at the beginner or intermediate levels, respectively.

# TIME MANAGEMENT

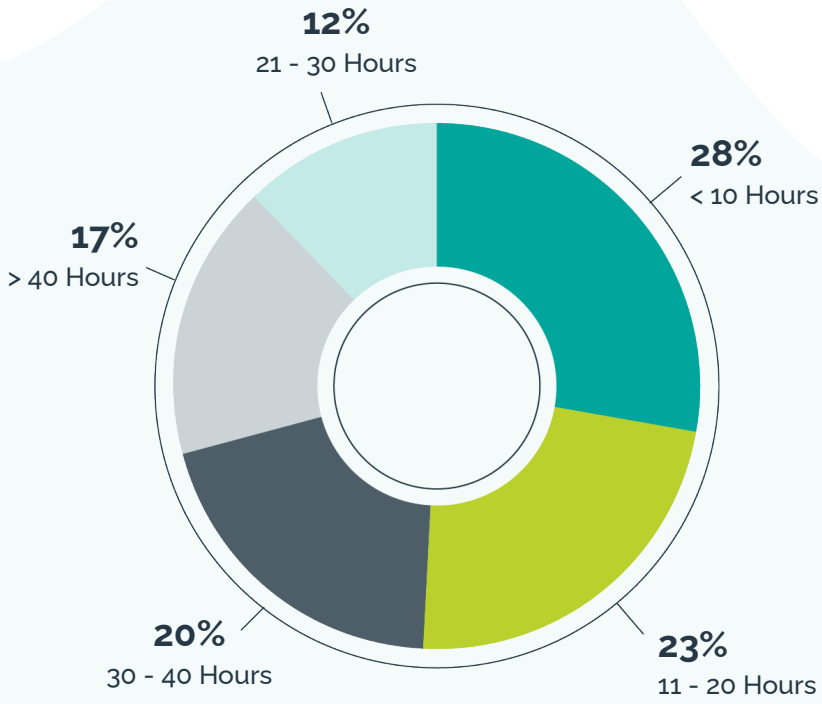
While 73% of practitioners spend up to 40% of their given workweek on their primary job functions, there are several daily activities they are also responsible for. Senior leaders spend less time on ticket management, while most directors, managers, and team members pivot between multiple tools every day.

Surprisingly, the average practitioner spends 27 hours of their week – **68% of a typical 40-hour work week – on non-primary job functions** (i.e., daily activities) listed below. There's an opportunity to evaluate how effective tools and team meetings are; perhaps consolidating both would give practitioners more time to focus on their primary job functions.

## Daily Activities

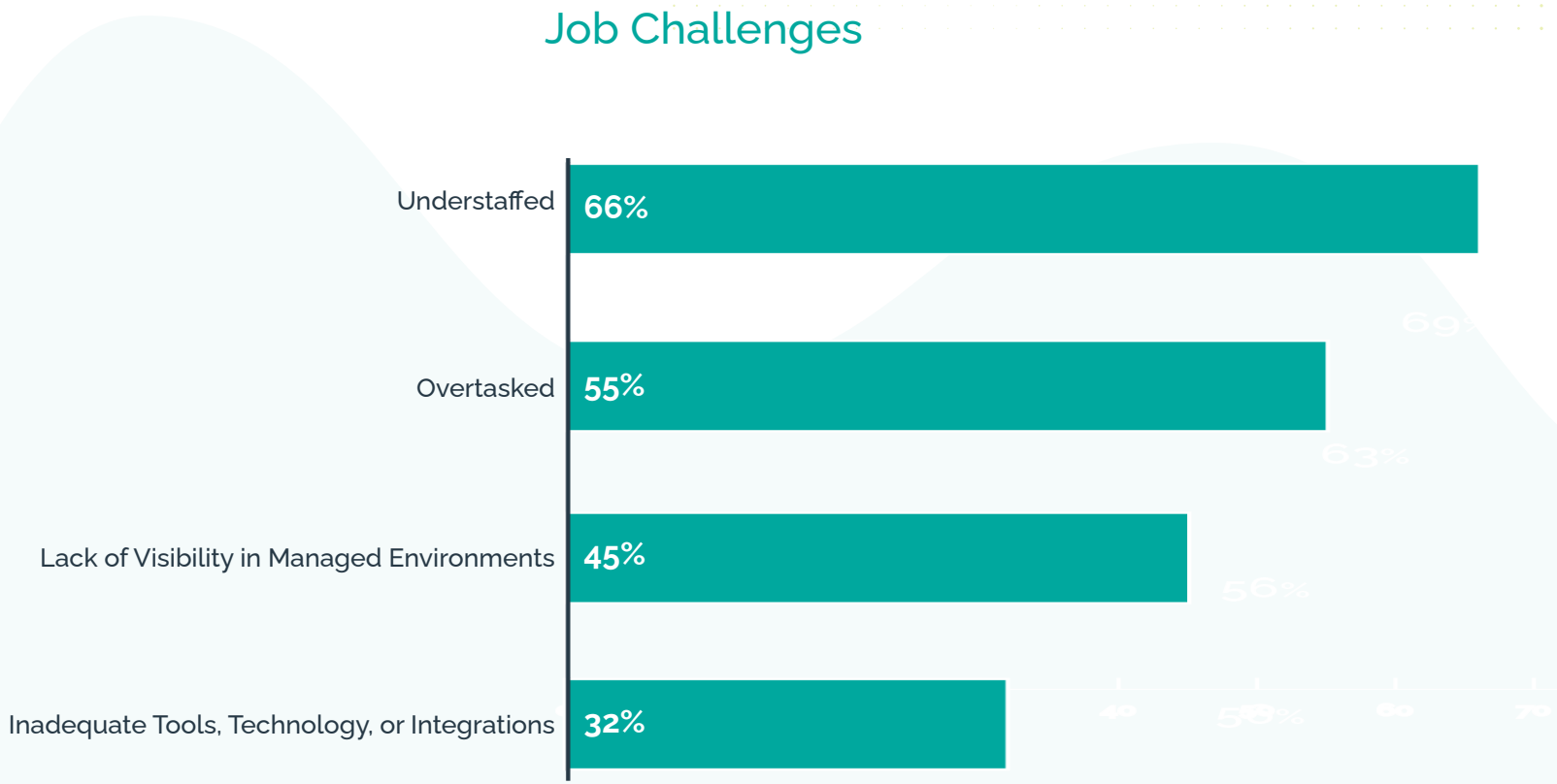



## Time Spent on Activities in a Given Week



## CHALLENGES

In addition to time management, the majority of practitioners cited being understaffed and overtasked as the top challenges to being effective in their jobs.



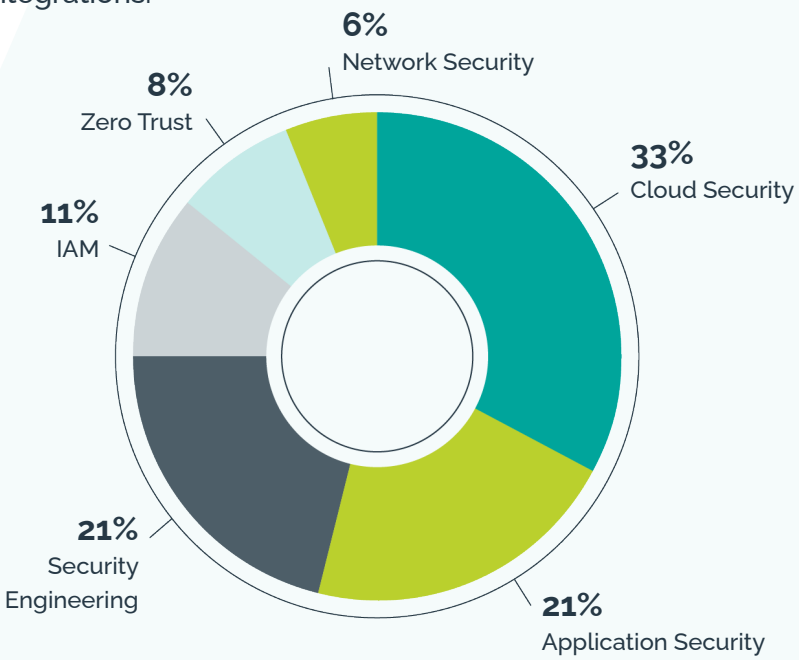
# IMPROVEMENT AREAS

To improve their teams' collective information security operations, nearly half **(48%) of practitioners said they need to develop security architecture capabilities** within the next 12 months. Nearly a quarter (21%) of practitioners will be focused on improving security operations.

## Security Architecture Skills to Develop in 2023

Categorized within the security architecture domain, **cloud security (33%) was the top capability practitioners will be focused** on in 2023, followed by application security (21%) and security engineering.

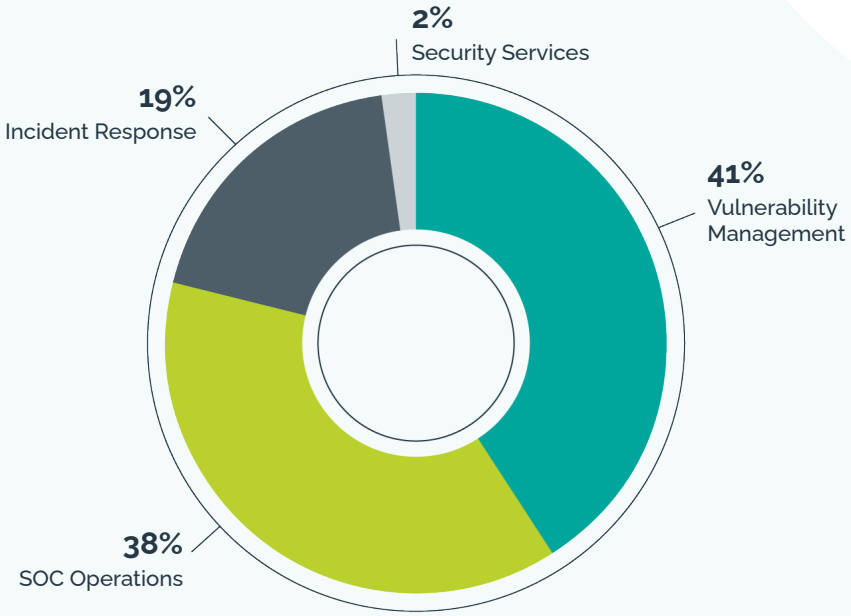
Application security includes DevSecOps, secure coding, software development, and infrastructure-as-code. Security engineering includes orchestration and automation, and tool integrations.




## Security Operations Skills to Develop in 2023

Within security operations, **vulnerability management (41%) was the primary improvement area** for practitioners. This includes configuration management database (CMDB), asset management, patching, and pen testing.

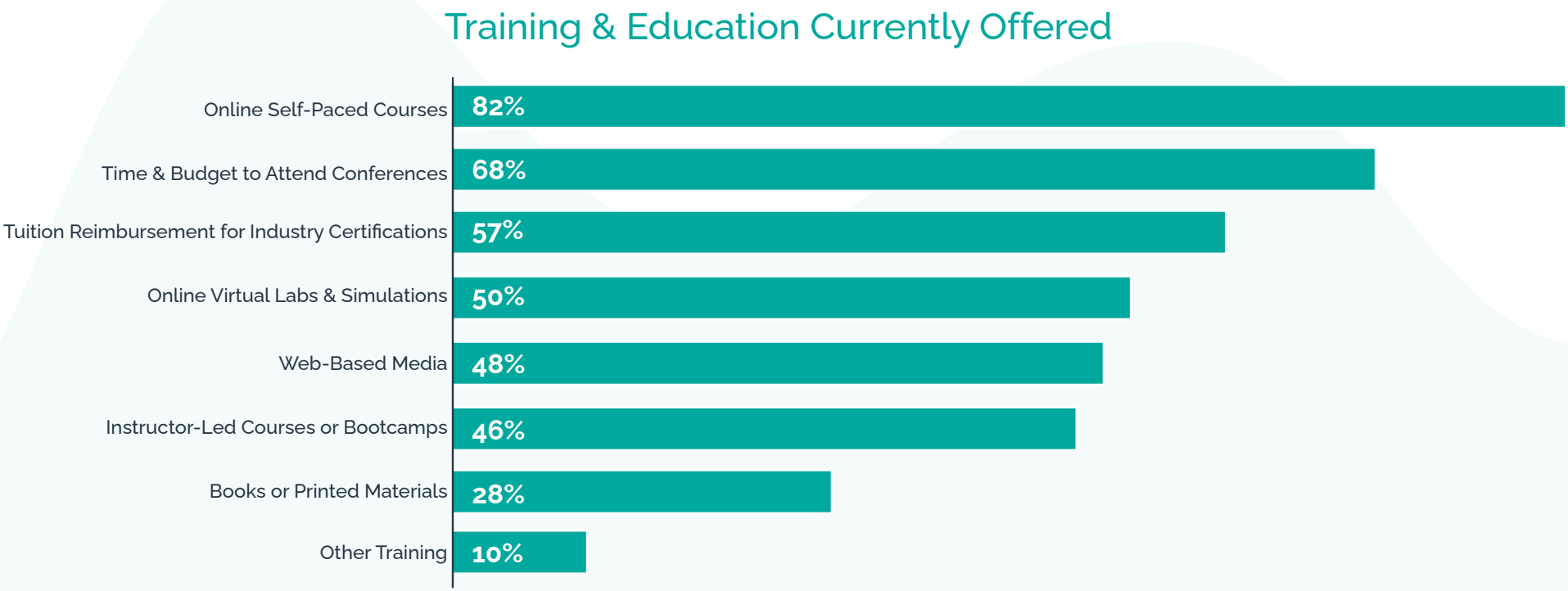
SOC Operations (38%) was the secondary focus area, including developing policies, procedures, and playbooks, and improving overall SOC management.



## TRAINING & DEVELOPMENT

According to the Agree Statements (see Figure 2 in the Appendix), 93% of practitioners feel they have the necessary skill sets they need to perform their jobs effectively, and more than 80% believe their teams have the necessary skill sets to effectively protect critical assets and information.

Additionally, 87% said their organization enables them to develop the skillsets they need to be effective in their current roles. The chart below highlights the types of training and education organizations currently offer:



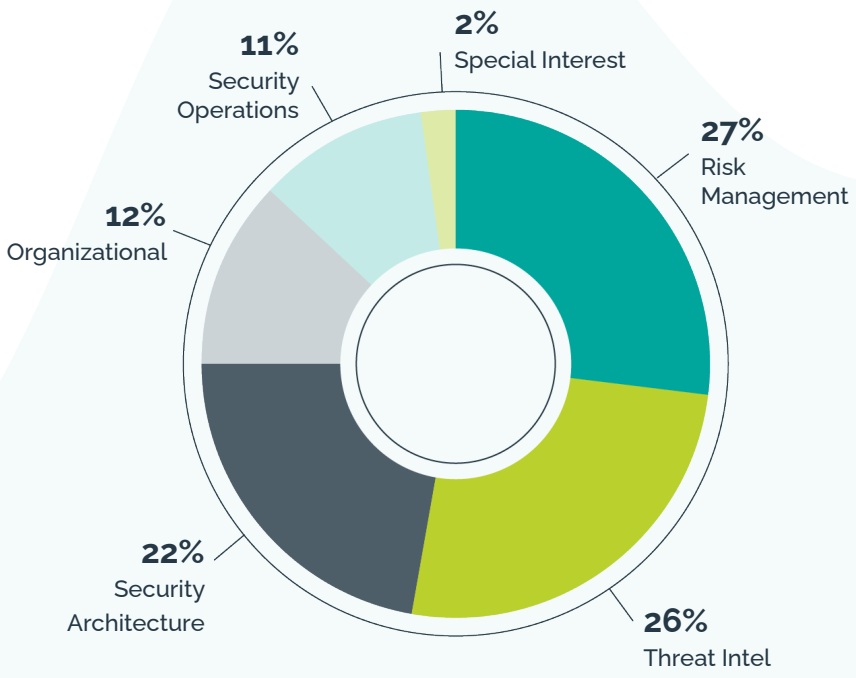

Interestingly, the while 84% of practitioners believe their organization enables them to develop the skills needed to advance in their careers, nearly half (48%) do not feel their organizations effectively communicate what skills are needed for career advancement.

# ORGANIZATIONAL RISKS & SECURITY INITIATIVES

According to practitioners, vulnerability management is both the top information security risk their organization currently faces and the top initiative their teams need to prioritize in 2023.

The charts below show that while organizations are currently facing risks related to risk management (27%), threat intelligence (26%), and security operations (22%), practitioners believe that initiatives related to security architecture should be prioritized in 2023, specifically identity and access management and security engineering.

## Top InfoSec Risks by Domain




## Top Initiatives in 2023