The State of Security by Design and Threat Modeling in 2025

Primary research findings

Introduction

In 2025, threat modeling and security by design have become foundational elements of application security programs in medium- to large-scale software organizations. Our survey of security practitioners reveals that over three quarters view threat modeling as a top priority and that eight out of ten anticipate its adoption to increase further this year. While under half perform formal threat modeling on every release, the majority (68%) undertake it during requirements gathering.

Product quality, risk reduction, and regulatory compliance are the primary drivers of threat modeling investment. Organizations report using multiple threat-modeling solutions, ranging from commercial platforms to open-source tools, integrated into their CI/CD pipelines. Despite these investments, keeping pace with an evolving threat landscape remains the foremost challenge, followed by increasing scope, and a lack of expertise in AppSec best practices and processes. Given the latter, not surprisingly almost all organizations report offering security best practices and training to their developers. Against this backdrop, it is disappointing to learn that most companies still manage security manually; automation though not widely used, works. Automations allows for dramatic reductions in critical vulnerabilities and their associated costs.

As threat modeling scales across the software development lifecycle, success hinges on automation, investing in specialized training, improving toolchain interoperability, and defining clear metrics to demonstrate return on investment. Ensuring best practices are deeply woven into every stage of development is necessary to sustain risk reduction and uphold compliance.

Commissioned Surveys By Security Compass

Survey Participants

- 130 respondents from the US (77%) and Canada (13%) with a minimum of 500 developers.
- Targeted half individual contributors (50%) and half (50%) managers and above who had self-reported competency in secure coding standards and regulations.

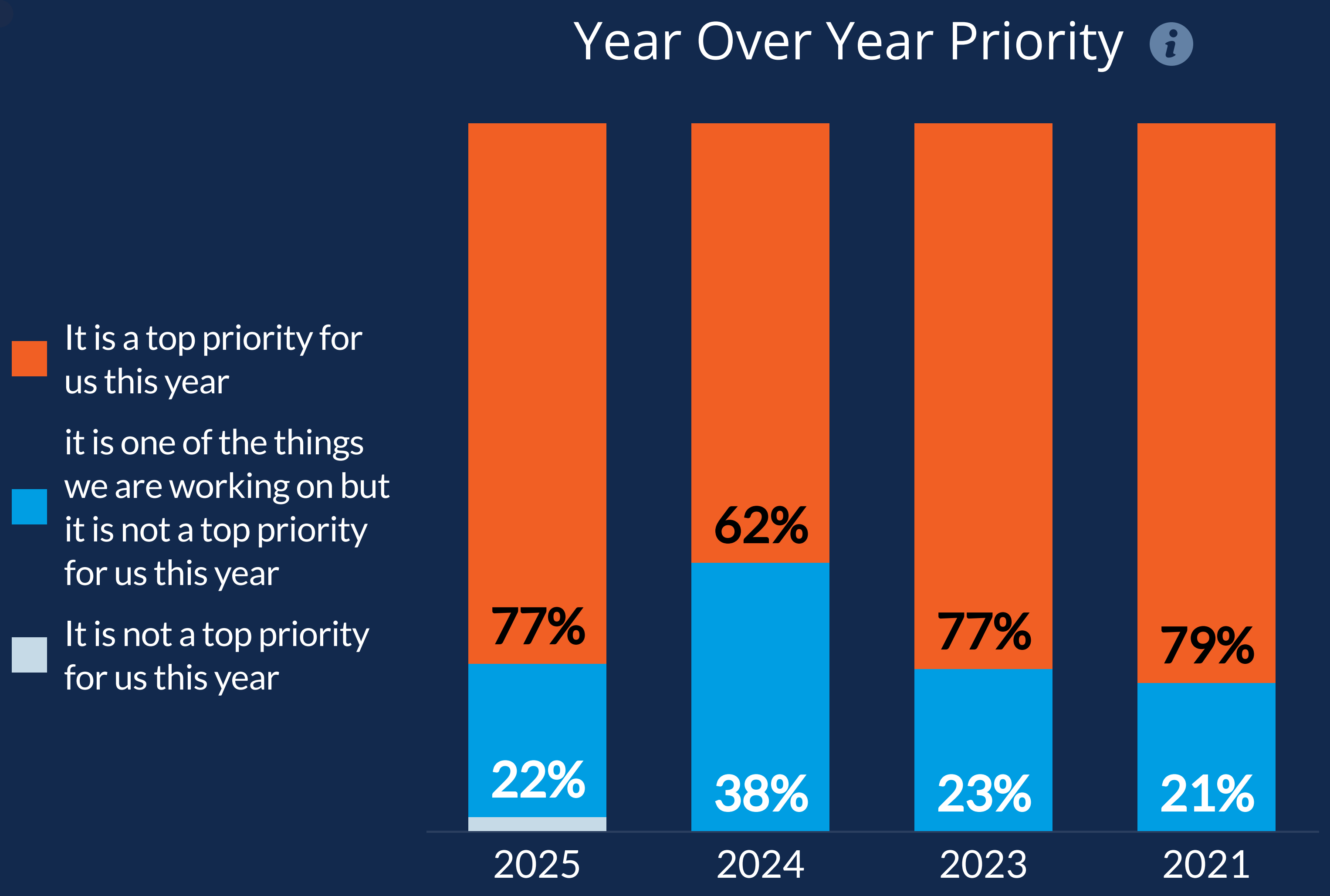
The survey was conducted by Golfdale Consulting.

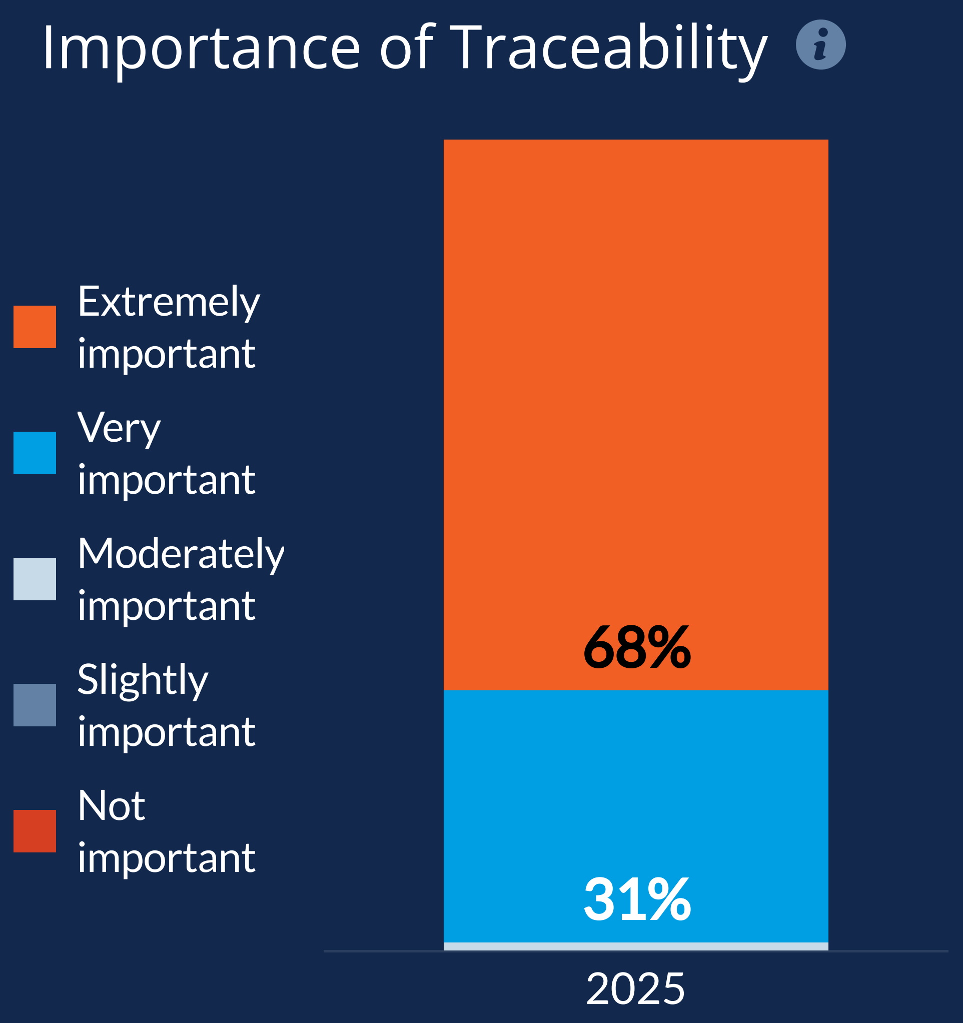
> Threat modeling is the cornerstone of security by design. When automated and woven into requirements building, design reviews, and CI/CD pipelines, it empowers teams to uncover and neutralize risks early, streamline development, and deliver resilient, compliant software on time and on budget.

ROHIT SETHI
CEO, Security Compass

Priority of Threat Modeling and Traceability

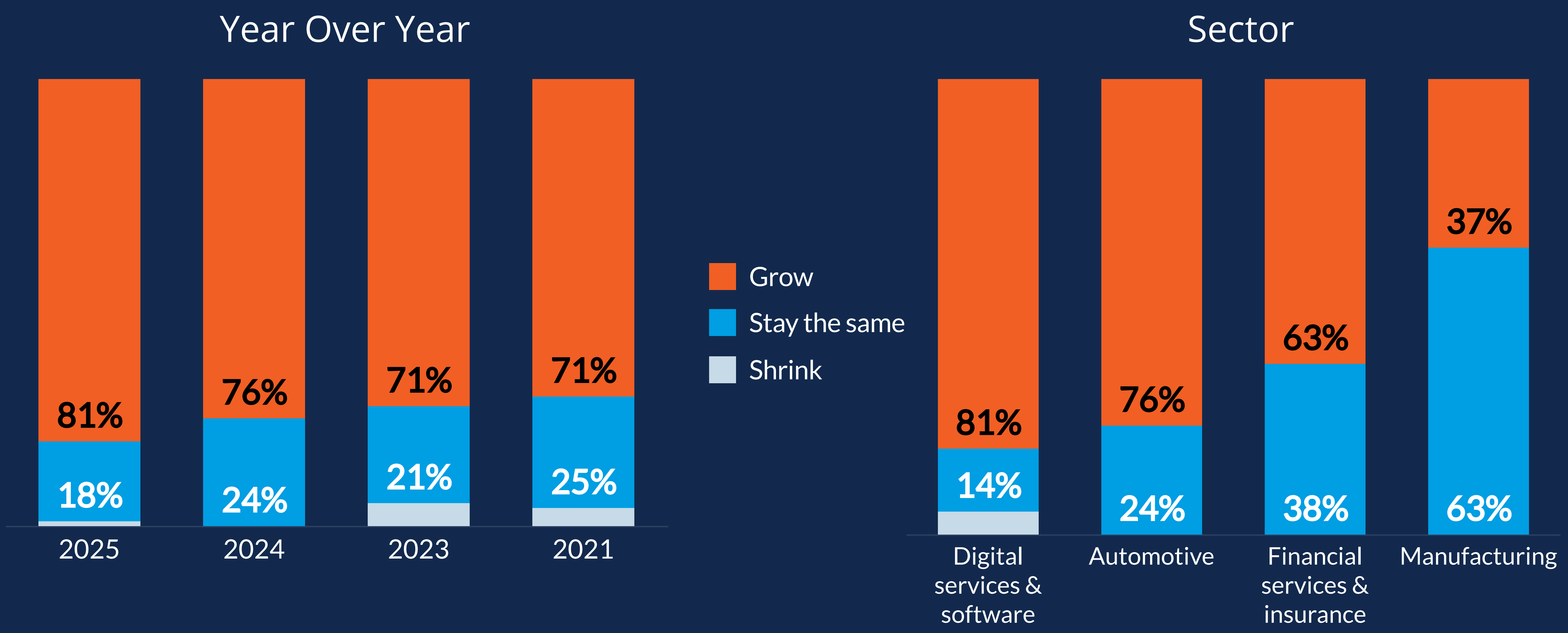
In 2025, almost eight out of ten companies view Threat Modeling as a top priority. Traceability is “extremely” or “very important” to almost all (99%) enterprises that do Threat Modeling.





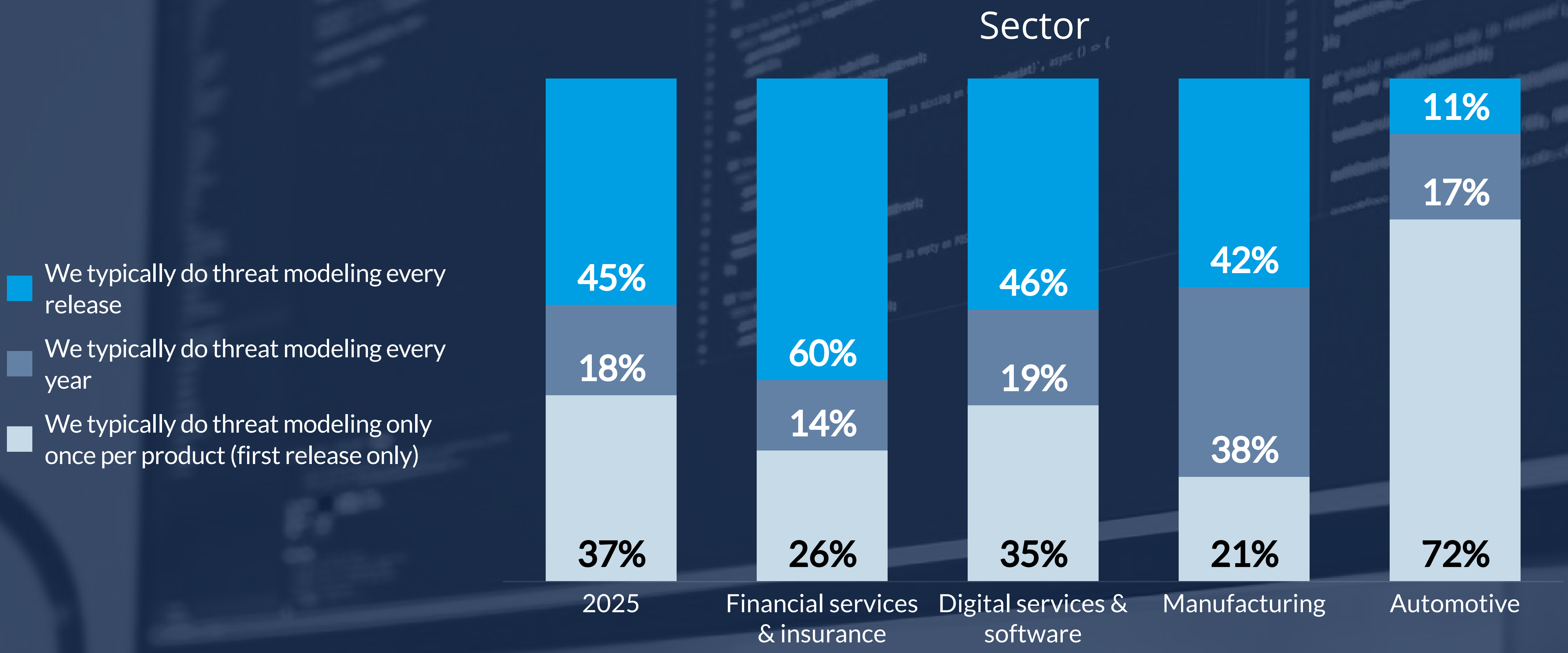
Growth of Threat Modeling

In 2025, more than eight out of ten companies expect the amount of Threat Modeling to grow, a five point increase over 2024 and a steady, incremental increase in expectations of growth YoY since 2021. It is most prevalent in Digital Services & Software, and least prevalent in the Manufacturing sector.



Frequency of Threat Modeling

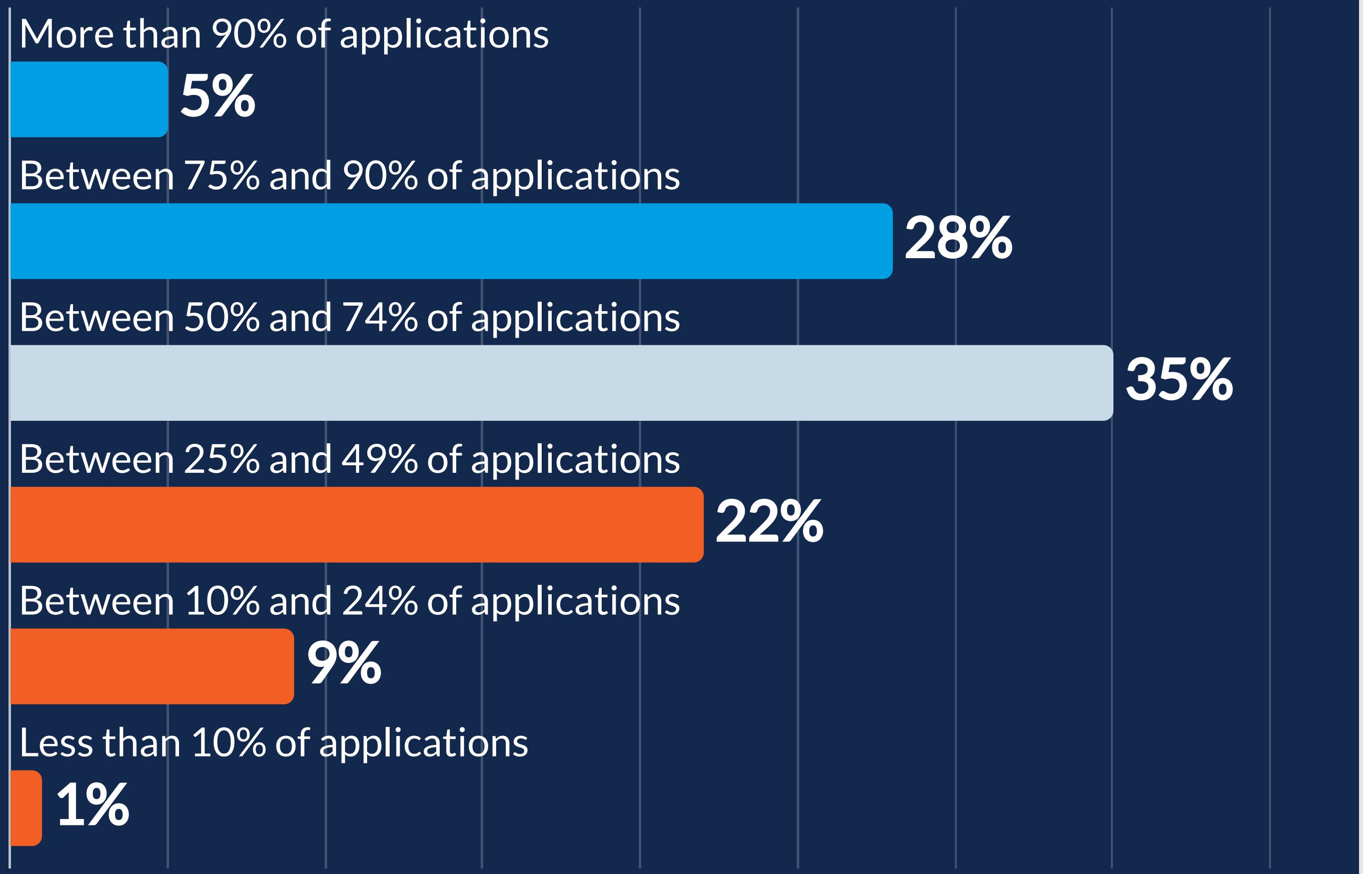
Less than half the companies that do Threat Modeling actually do so for every application release.
This happens most often in the Financial Services & Insurance sector, least often in Automotive.



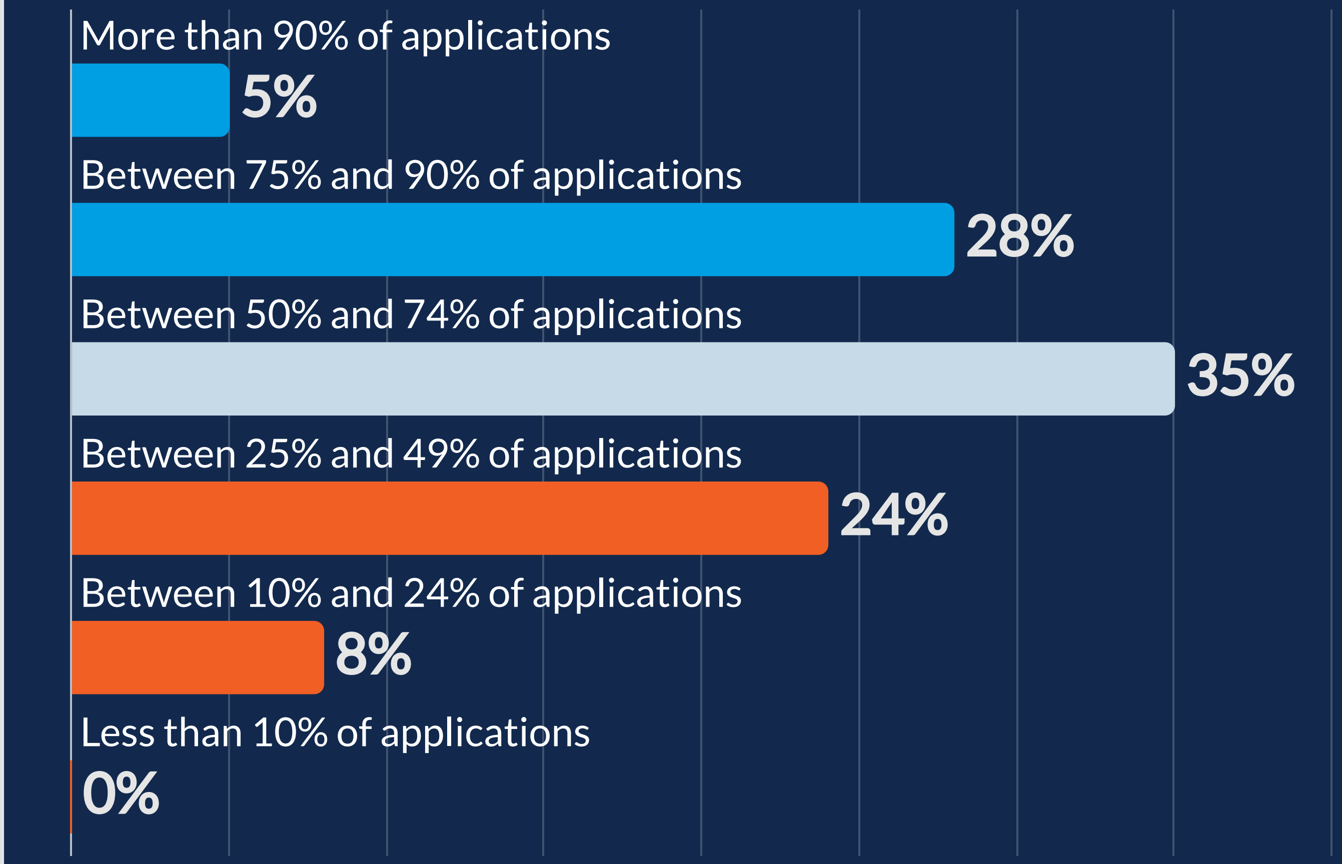
% of Apps With Defined Security Requirements and TM

There is very close alignment between the percent of applications with defined security requirements and the percent that threat models are performed on. For both, one third (33%) define security requirements and conduct Threat Modeling on over three quarters of their applications.

Percent with Specific AppSec Requirements

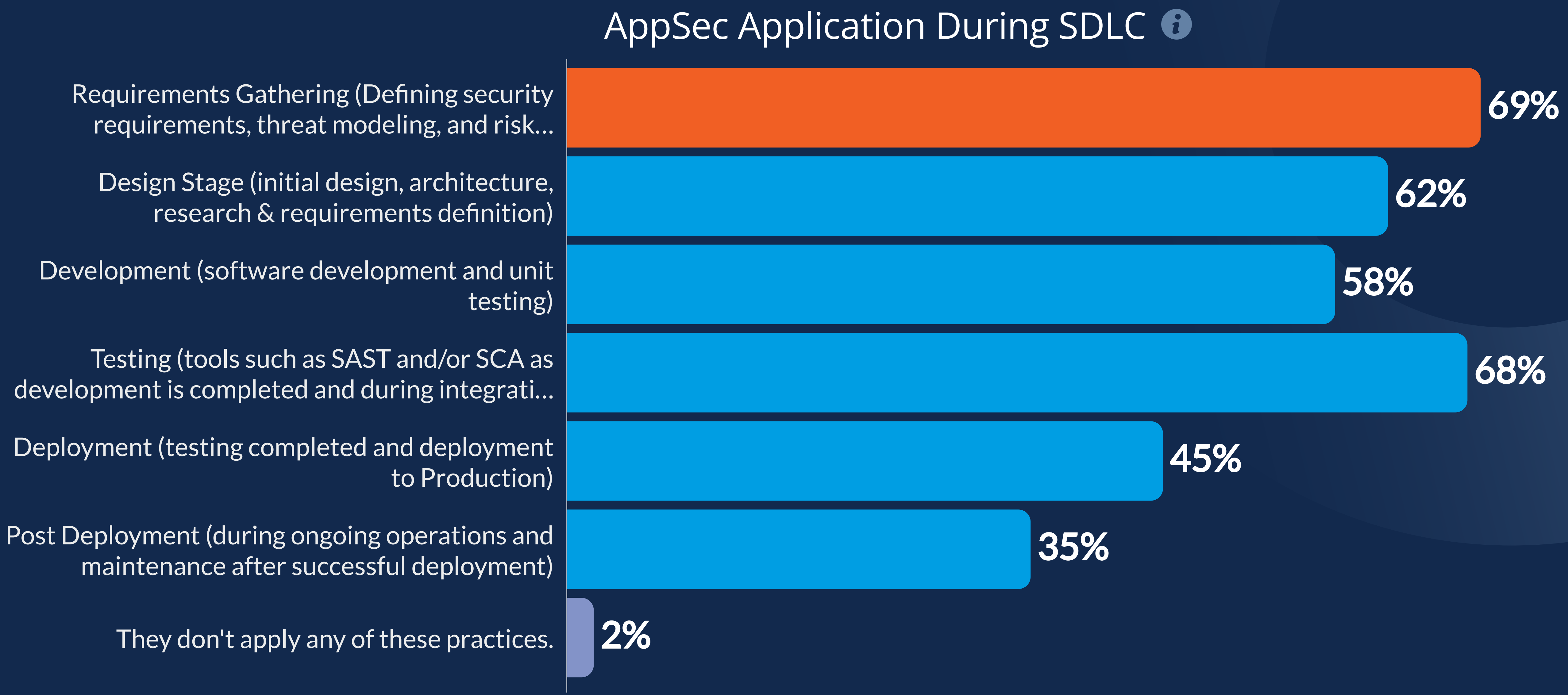


Percent of Apps TM Is Performed On



AppSec Application During the Software Dev Life Cycle

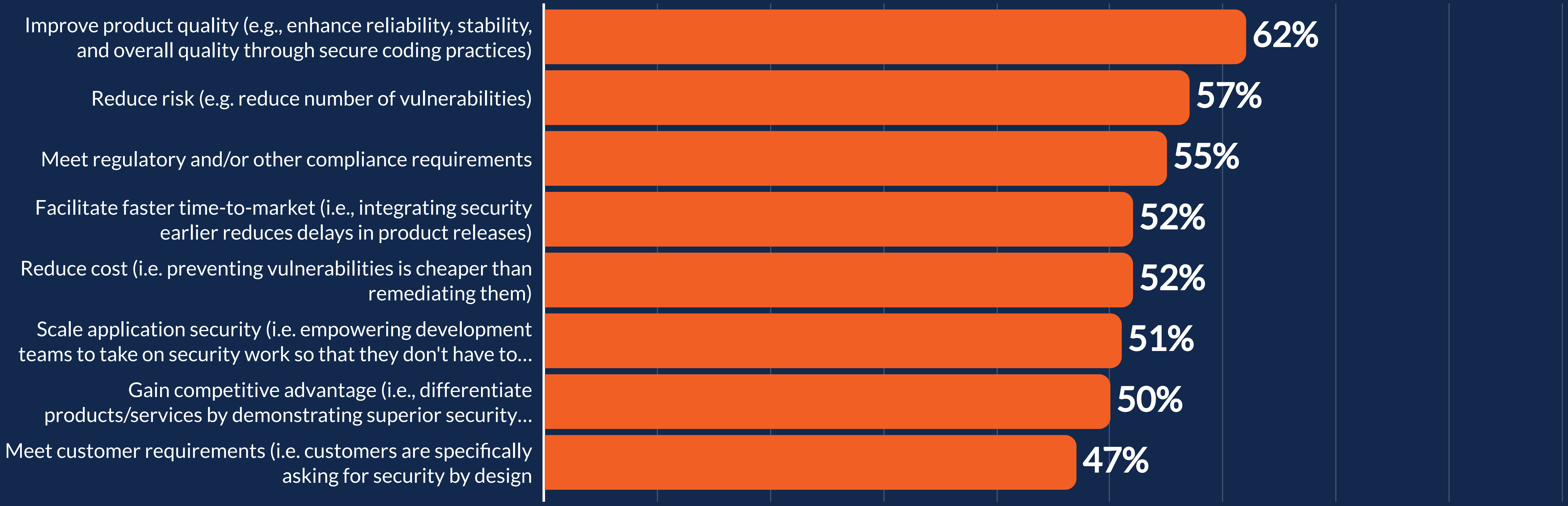
Over two thirds of large software developing companies include Threat Modeling at the Requirements Gathering Stage.



Reasons for Practicing Security by Design

Product quality trumps all other reasons for practicing Security by Design in 2025. In the Automotive Sector, security by design is required to meet regulatory requirements versus a demand by customers, resulting in faster time to market because vehicles cannot be sold without meeting these standards.

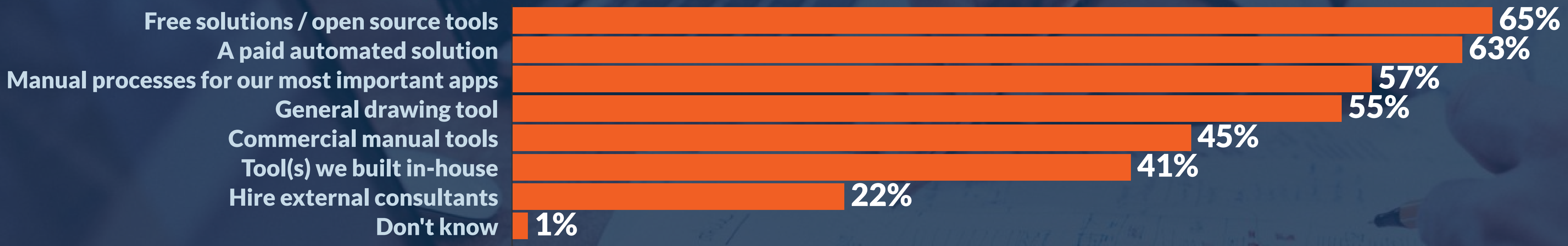
2025	Manufacturing	Financial services & insurance	Digital services & software	Automotive

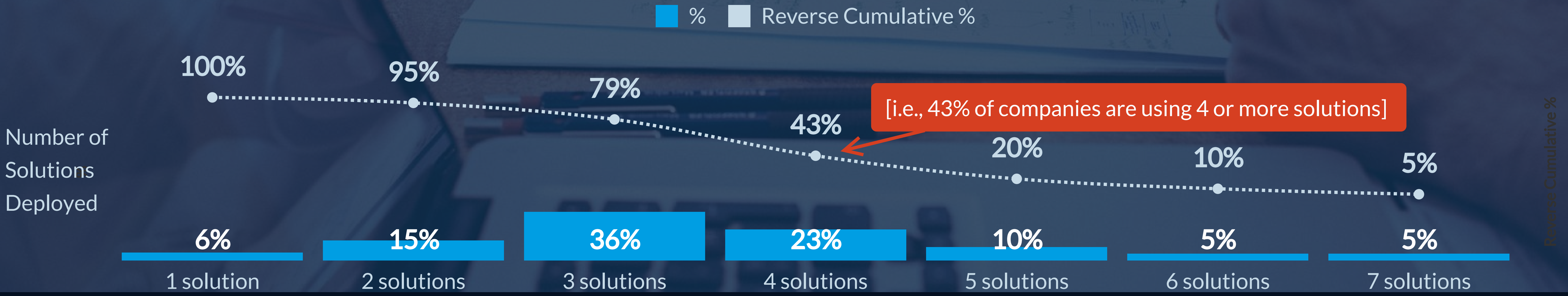


Solutions Used for Threat Modeling

Medium sized companies are more likely to use a wider array of solutions for Threat Modeling vs. larger enterprises. Almost 8 out of 10 are using 3 or more solutions.

2025 | $500M to less than $1B (n=26) | $1B+ (n=104)



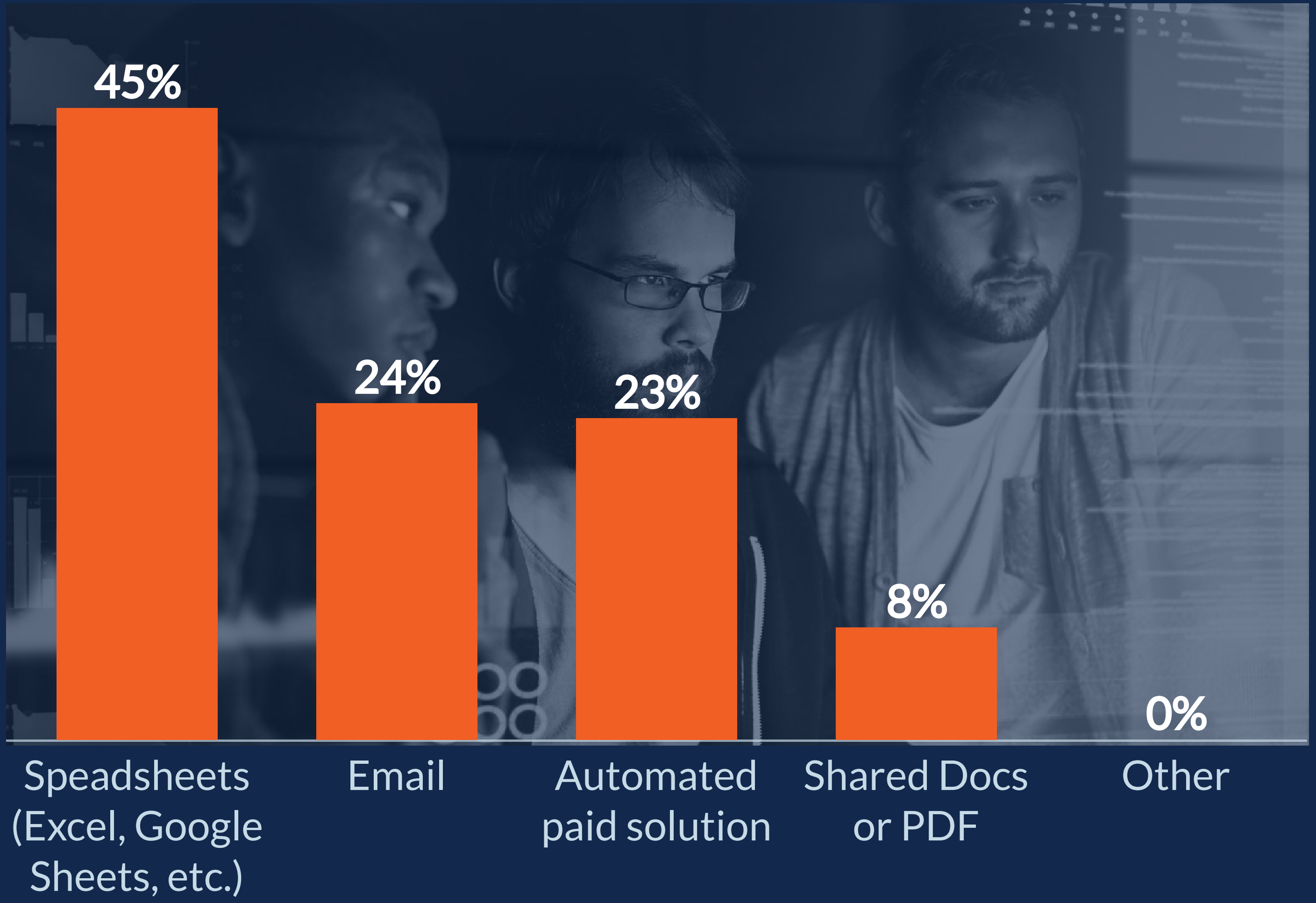


[i.e., 43% of companies are using 4 or more solutions]

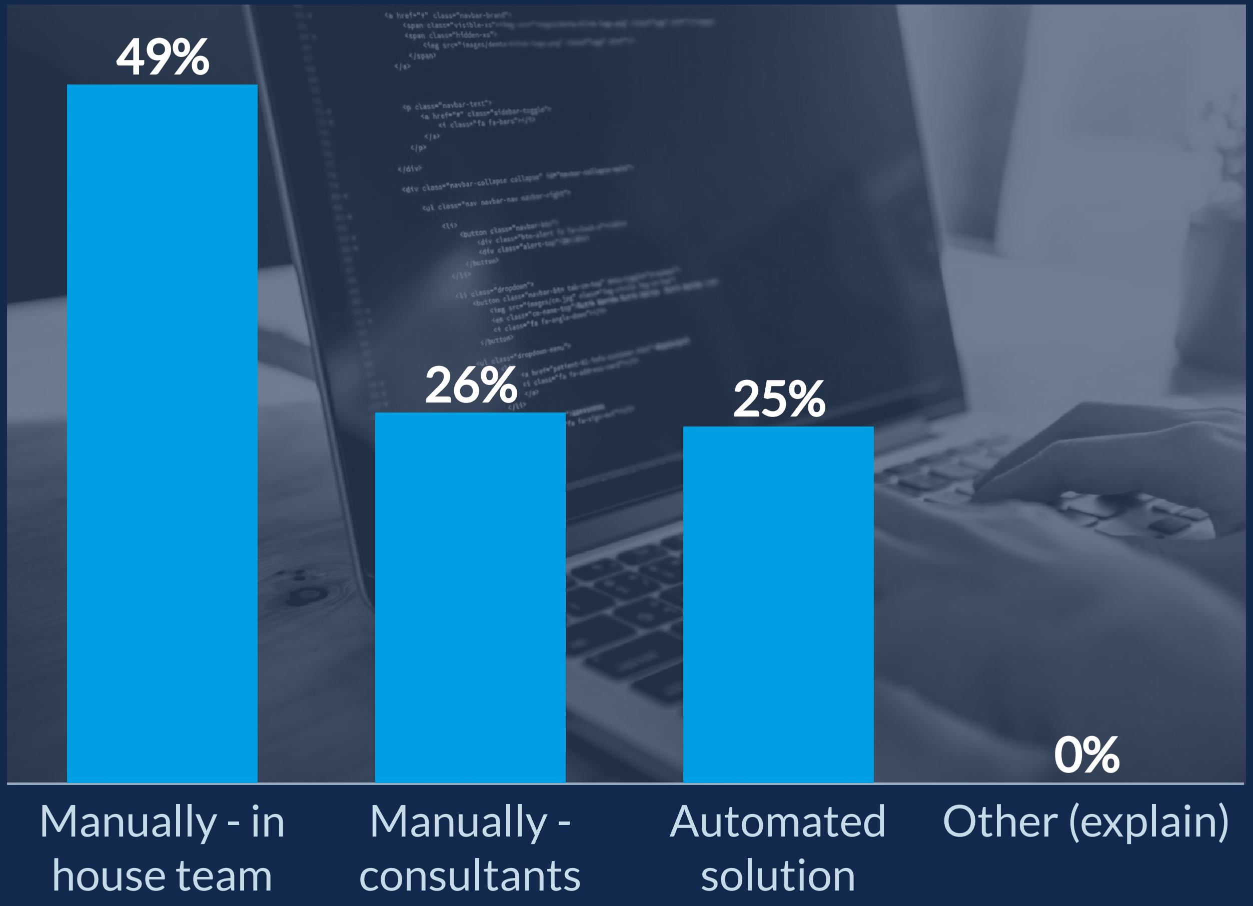
Managing Security Requirements

Most companies still manage security manually; automated solutions are underutilized. Cross analyzing the two findings, automation is clearly more efficient: 70% of automated users also update their requirements automatically, versus just 13% of manual in-house teams. Automation though not widely used, works.

Managing Security Requirements



Keeping Requirements Up to Date

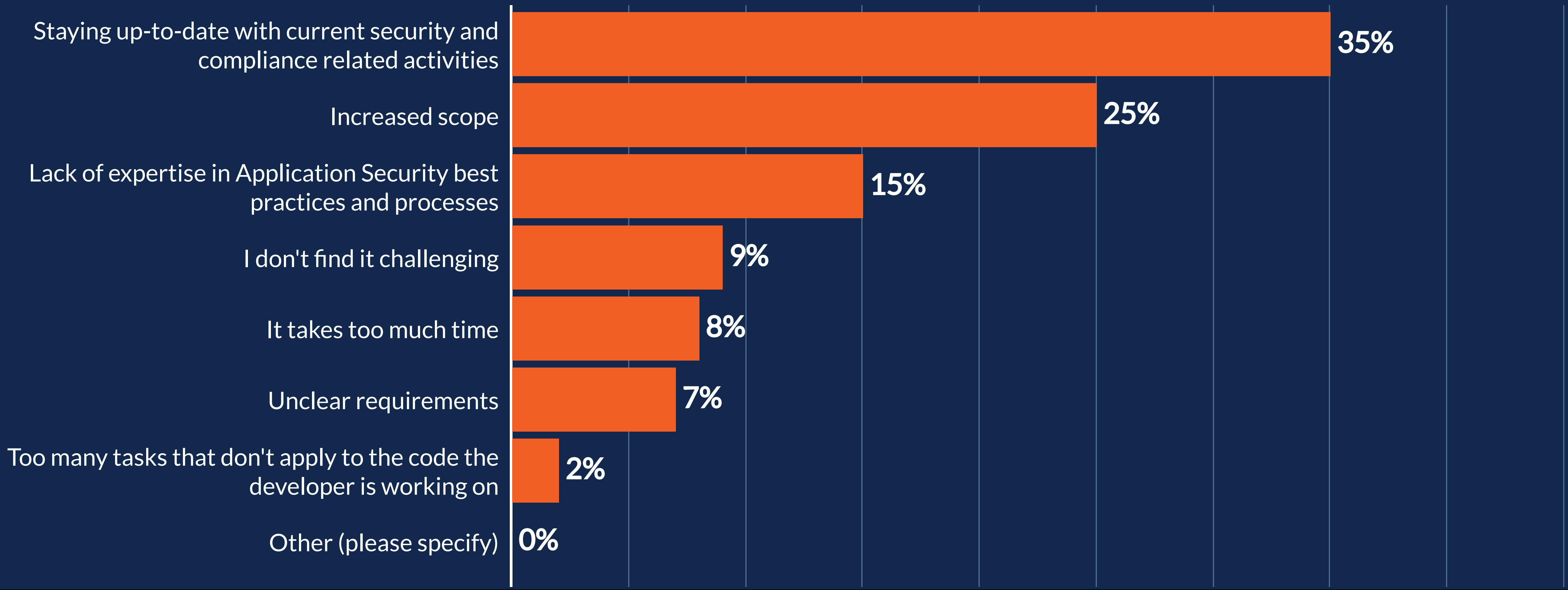


Key Challenges

Staying current continues to be the most challenging aspect of security and compliance requirements. Scalability remains the #1 challenge, as it was in 2024.

External ⓘ and Internal ⓘ Challenges

Overall Challenges | 2025 Internal Challenges | 2024 Internal Challenges

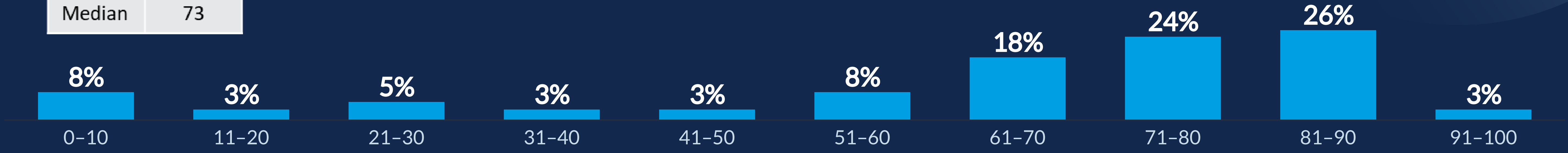


Critical or High-Risk Vulnerabilities

There has been a steep rise in vulnerabilities in 2025, with over half claiming there are over 70 per app. That said, almost 2/3s of these vulnerabilities are offset by using Security Requirements or Threat Modeling.

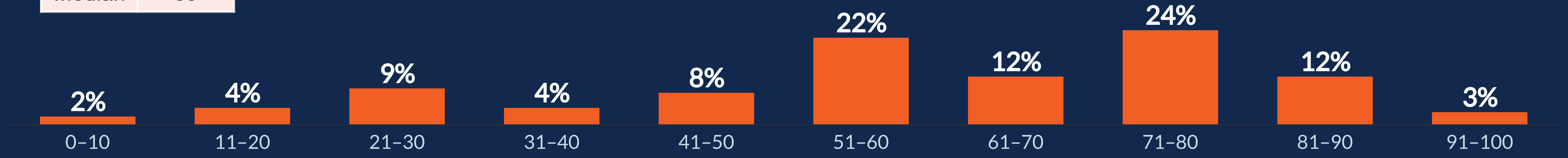
	2025
Mean	89
Median	73

Average Number of High/critical Risk Vulnerabilities per App per Year



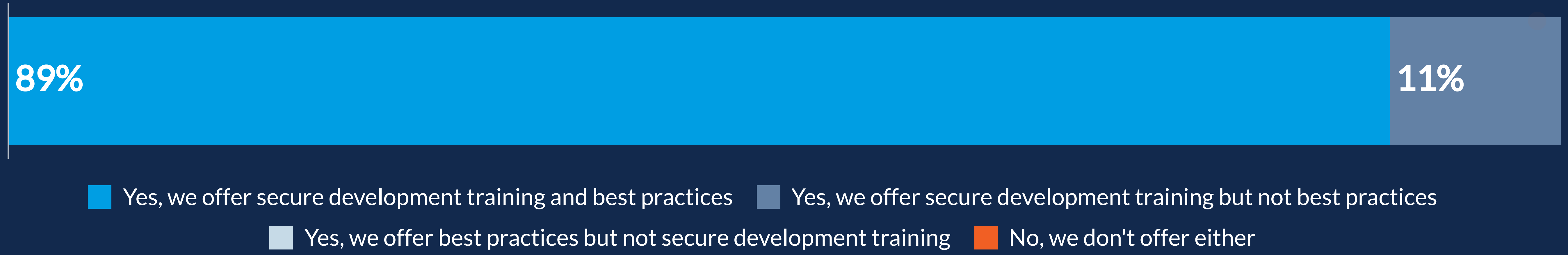
	2025
Mean	61
Median	65

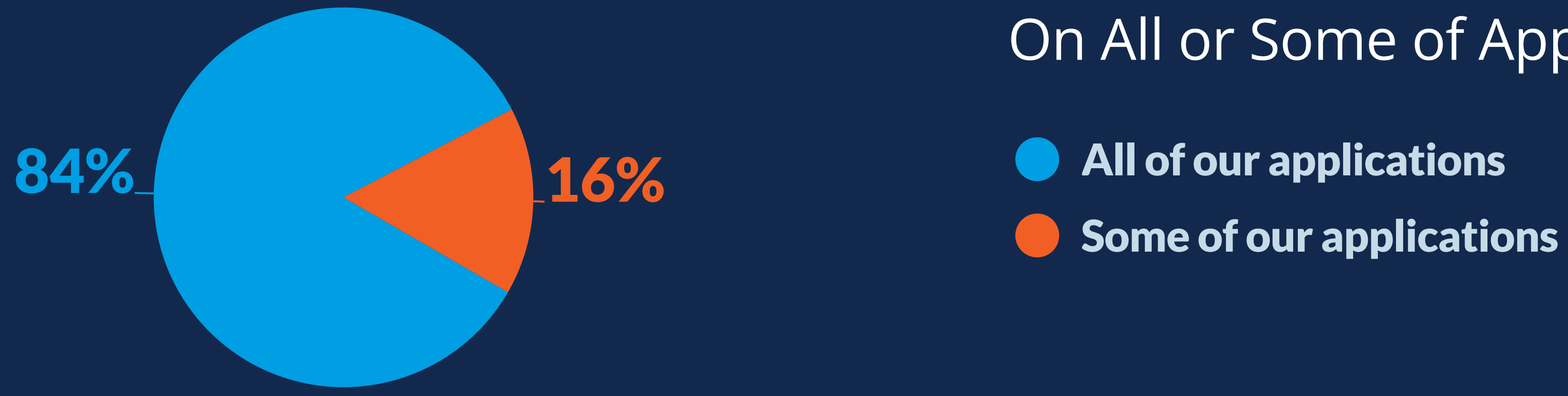
Average Reduction in Number of High/critical Risk Vulnerabilities Per App per Year from Use of Threat Modeling



Secure Development Training

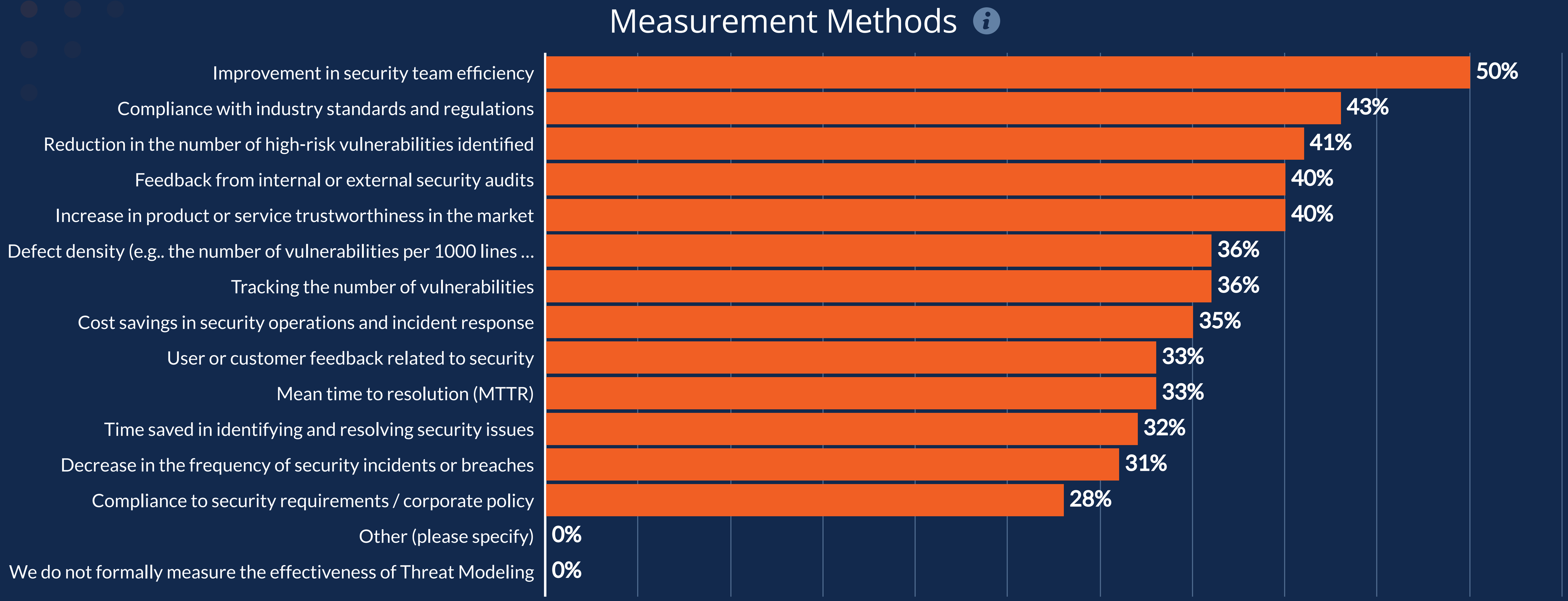
Most companies provide secure development training and best practices and do so for all of their applications. Those who offer both are most likely to do so for all oftheir applications.





Threat Modeling Measurement Methods

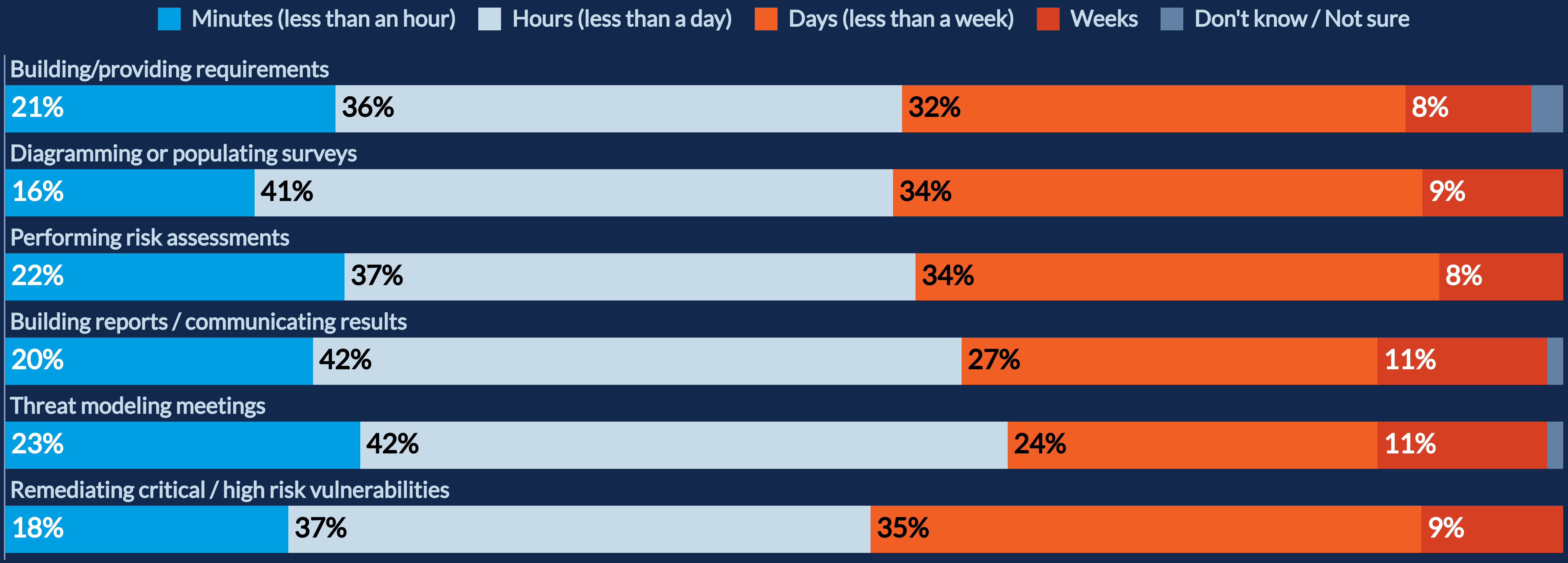
Improvement in security team effectiveness (a new item added in 2025) is the #1 cited measure of Threat Modeling effectiveness.



Task Performance Cumulative Time Effect

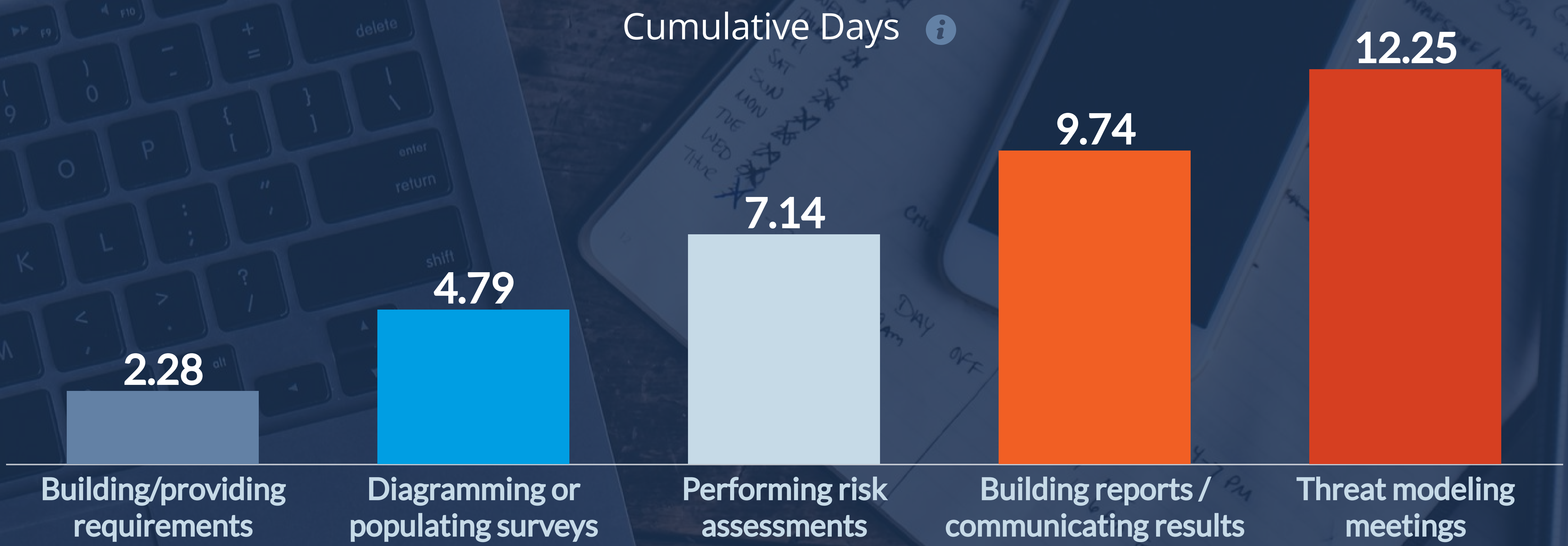
Looking to the "doing tasks" (aside from meetings and reporting of results), for most companies the time spent remedying critical/high risk vulnerabilities is approximately the same time spent as diagramming or populating surveys.

How Long Does It Take?



Task Performance Cumulative Time Effect

Across all steps involved, the average amount of time spent on Threat Modeling is over 12 days in total.



*Analysis method: “minutes” = 0.03 days; “hours” = 0.3 days; “days” = 3 days; “weeks” = 15 days for each activity.

Average Cost to Fix A Critical or High Risk Vulnerability

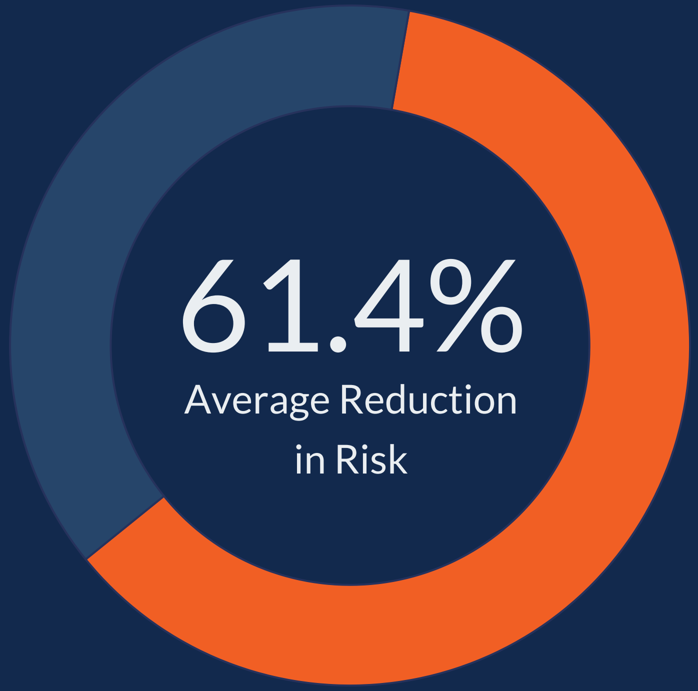
The budgets for Threat Modeling have rise substantially YoY, up on average almost $20,000 from 2024.

Find and Fix

10k - 69K

Cost to Fix a High-Risk Vulnerability

Threat Modeling & Security Results



Source: 2025 Security by Design and Threat Modeling Survey, Golfdale & Security Compass

Conclusion

In 2025, threat modeling has emerged as a cornerstone of effective security by design, with mature organizations embedding it consistently from requirements gathering through deployment. Our study demonstrates that those who integrate structured risk identification, formal “security by design” policies, and automated checks directly into CI/CD pipelines achieve markedly stronger security outcomes and smoother development workflows.

Yet success depends on more than tooling. Teams must invest in role-based training that aligns with real-world scenarios and prioritize interoperability across their security toolchain. Clear metrics tied to vulnerability reduction, remediation speed, and compliance posture are essential to measure return on investment and to sustain executive support.

Looking ahead, the most resilient organizations will be those that weave threat modeling into their culture: empowering developers with hands-on guidance, enforcing and achieving requirements through automation, and continuously refining practices in response to an evolving threat landscape. By doing so, they not only meet today’s regulatory and contractual demands but gain a lasting competitive advantage through higher product quality, faster time-to-market, and strengthened customer trust.

```
    "./styles/BadgesList.css";
port Gravatar from "./Gravatar";

nction useSearchBadges(badges) {
 const [query, setQuery] = React.useState("");
 const [filteredBadges, setFilteredBadges] = React.useState

 React.useMemo(() => {
    const result = badges.filter(badge => {
      const nameComplete = `${badge.firstName} ${badge.lastName}
      const normalizeQuery = query.toLowerCase();

      return nameComplete.includes(normalizeQuery);
    });

   setFilteredBadges(result);

 }, [badges, query]);

 return { query, setQuery, filteredBadges };

unction BadgesList(props) {
 const badges = props.badges;
 const {query, setQuery, filteredBadges} = useSearchBadges

 if(filteredBadges.length === 0) {
   return (
     <div>
       <div className="form-group">
         <label>Filter Badges</label>
         <input
           type="text"
```

Secure Development Resources

For more cybersecurity resources please visit: https://resources.securitycompass.com/
Phone: 1-888-777-2211 | . Email: contact@securitycompass.com

About Security Compass
Security Compass helps organizations build secure and compliant software by design. SD Elements, our core platform, enables teams to identify potential threats and generate security requirements before coding begins. Seamless integrations with existing DevSecOps tools and workflows enable developers to produce secure code efficiently. Our Application Security Training combines a rigorous curriculum with hands-on labs, equipping developers with the skills to build secure software with confidence. To discover how Security Compass enables secure software development at scale, visit www.securitycompass.com.

About Golfdale Consulting, Inc.
Golfdale Consulting Inc., trusted advisors to growth focused business leaders. Golfdale expertise and hands-on approach with senior executives spans three critical areas: 1) global market research and insights; 2) analytics and the application of decision sciences; and 3) advocacy for evidence based regulatory reform and market impact. Follow Golfdale Consulting on Twitter @_golfdale or visit https://golfdaleconsulting.com/