THREAT MODELING CONNECT
POWERED BY IRIUSRISK

2024-2025

# State of Threat Modeling Report

# Introduction

Welcome to the first-ever State of Threat Modeling Report, covering January through December 2024. This was, as far as we know, the first ever survey report of threat modeling practices within companies. The survey results are based on 73 complete responses, 60 of which are the basis for the data presented as they represent the threat modeling practices of each responder's respective company.

The report aims to capture and share key trends, benchmarks, challenges, and best practices in threat modeling. It's important to note that because threat modeling is typically an activity that companies perform, the questions in the survey were focused on the actual activities performed at a company, rather than trying to capture an individual's personal views on how threat modeling should be done.

This survey and report were created as a community-based effort, and the intent isn't to tell you how to threat model, nor for you to confirm that you threat model the 'right way'. The survey and report were created because as a community we deserve to see the breadth and depth of approaches to threat modeling to inspire us to keep on improving our approaches and better serve our partners, businesses, and to manage the risks we all face.

The data presented in this report is as interesting for what it normalizes, as it is interesting for the diversity it captures. Threat modeling is an extremely flexible approach to the security analysis of virtually any system, it should be no surprise then to expect contrasts in the data represented in this report, and yet amongst the diversity within the report, also find the trends and common practices that the community shares, representing our ability to learn from each other.

The report is split into the following sections:

- **Key Findings**. These are some curated report areas of particular interest to the community, making for some interesting reading and immediately demonstrating the value of seeking data for understanding how companies threat model.
- **Who Responded**. This covers the demographics of who responded to the survey and the companies they represent.
- **Threat Modeling Program**. This covers questions relating to setup and design of threat modeling as a business activity.
- The sections **How**, **Output**, and **Reporting** are meant to roughly align with the lifecycle of a typical threat model.
- **Challenges**. This covers the potential challenges companies face throughout their threat modeling activity.

Lastly, a huge thanks to everyone who responded. Hopefully this survey will be a regular occurrence on the threat modeling community calendar, and with increased community support will continue to offer valuable, data driven insights.

## Assumptions

To make processing the numbers simpler, it was assumed that each survey respondent works for a separate company (or operates a separate threat modeling activity if within the same company).

## Data

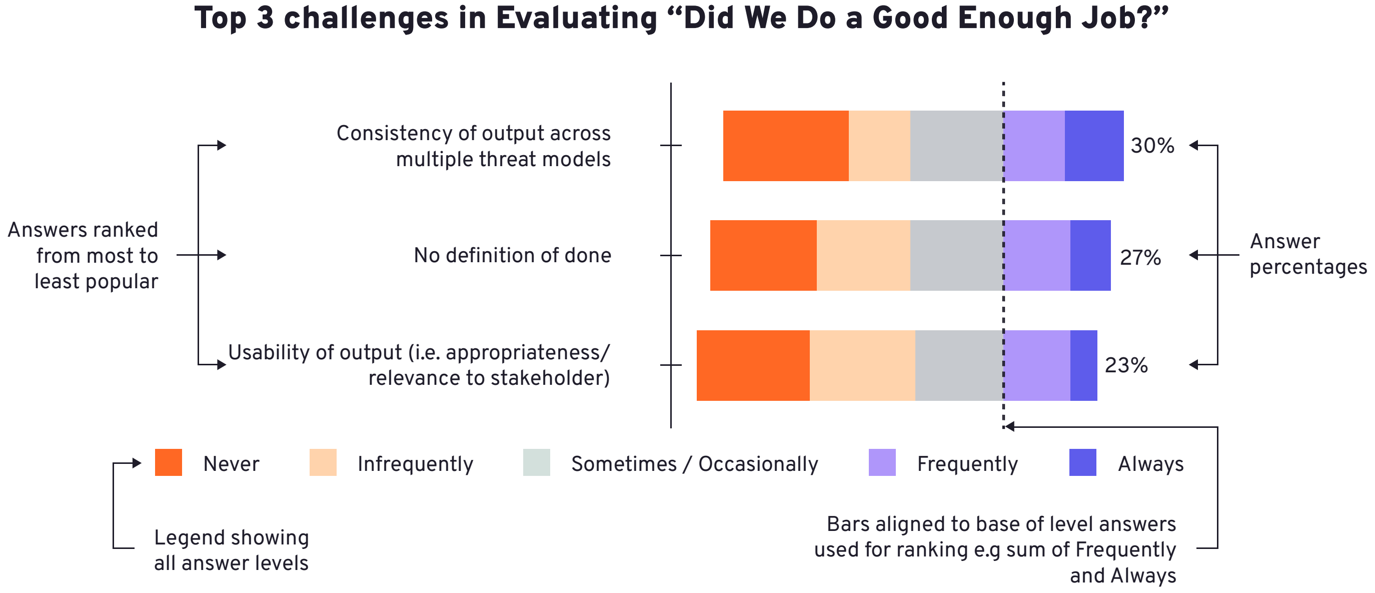
- Survey Responses - Contains the processed results from the survey. This data was used as the basis for the information presented in this report. Where this report mentions a question e.g. "Q19", the table of responses can be found in this document.
- State of Threat Modeling Survey Answers Data (Shareable) - Contains the raw answer data for the Google Form used to ask the survey questions.

## Guide

The survey asked many questions using a Likert scale which lets respondents choose the level at which they align/use/agree about something. Many of the graphs in this report use a Likert scale chart to represent the responses. The charts used are simplified though and aim to provide 2 main pieces of information:

- The ranked order of preference. This is presented by the ordering of the answers.
- The relative preference of the answers. This is presented by showing the percentage of answers at a particular level (usually the sum of the top 2 levels).

The stacked bar chart for each answer is also aligned to the levels being used in the ranking. Whilst all the levels are shown in the bar chart, this is secondary information that the reader can follow-up on by using the Survey Responses.



# Contents

# Key Findings

# Popular Approaches

### *STRIDE dominates, but most companies are influenced by 4 approaches on average.*

We all want to know "what approach to threat modeling is the most popular?" However, the hypothesis behind this question was that a company's approach to threat modeling is often not exactly aligned with a particular published approach, but rather has been customized to suit their needs, and likely has been influenced by one or more of the numerous approaches to threat modeling that exist. This is why we asked (Q15) 'how aligned' your threat modeling approach was with various well known approaches, as this will reveal not only which approaches are most instructive, but which approaches guide or influence how a company threat models.

The top 5 most popular approaches, by percentage of respondents, that had any kind of alignment to how their company threat models, were:

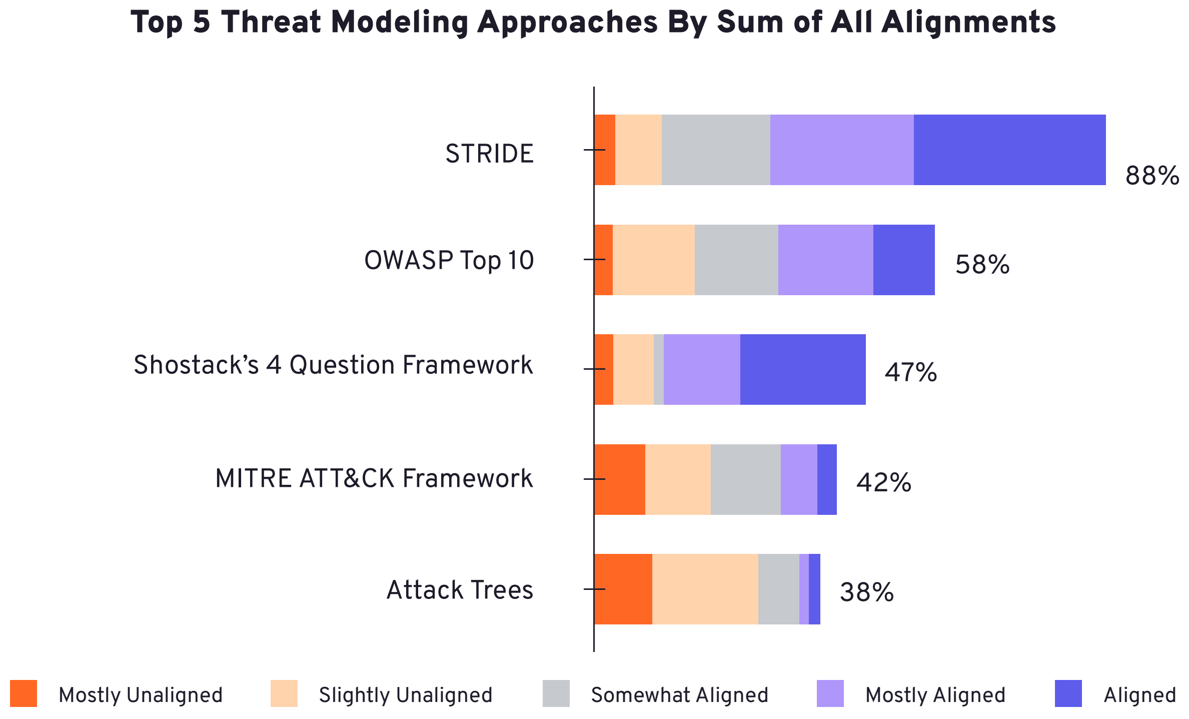


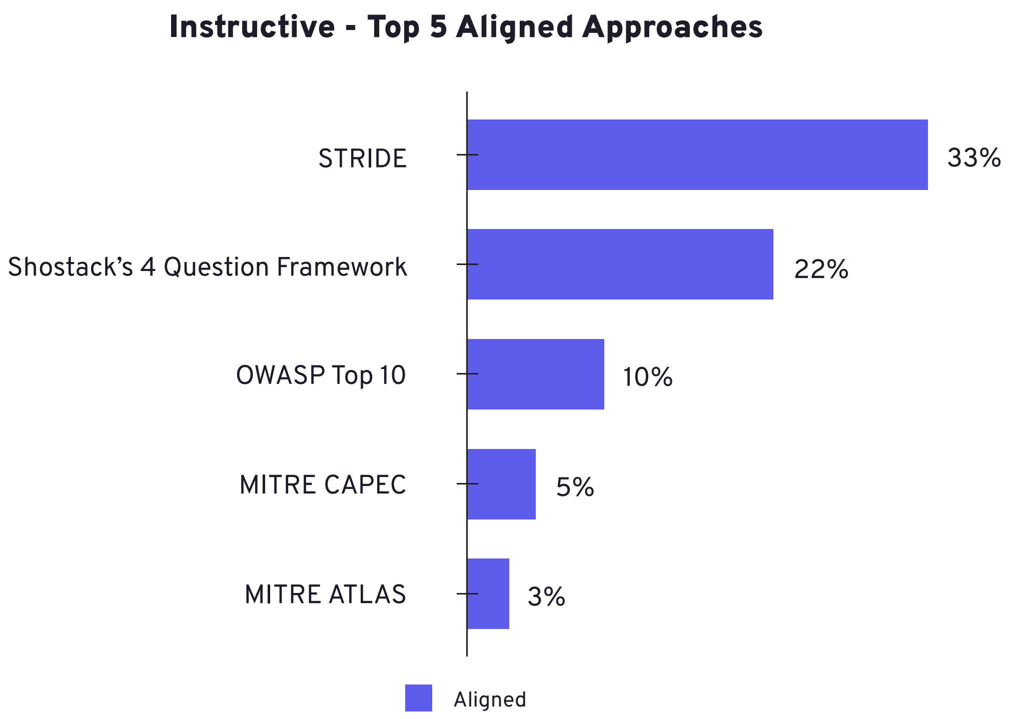
**Figure 1. STRIDE, OWASP Top 10, and Shostack's 4 Question Framework show the highest alignment with current threat modeling practices.**

*Likert scale chart of top 5 alignments of different approaches, ordered by the sum of all alignment categories. Respondents could have responded for multiple approaches, or responded "N/A" for approaches they don't use ("N/A" numbers not shown).*

However, just because an approach is not the most used, doesn't mean it isn't influential, so we can break down the numbers by how aligned different approaches are. We created 3 categories;

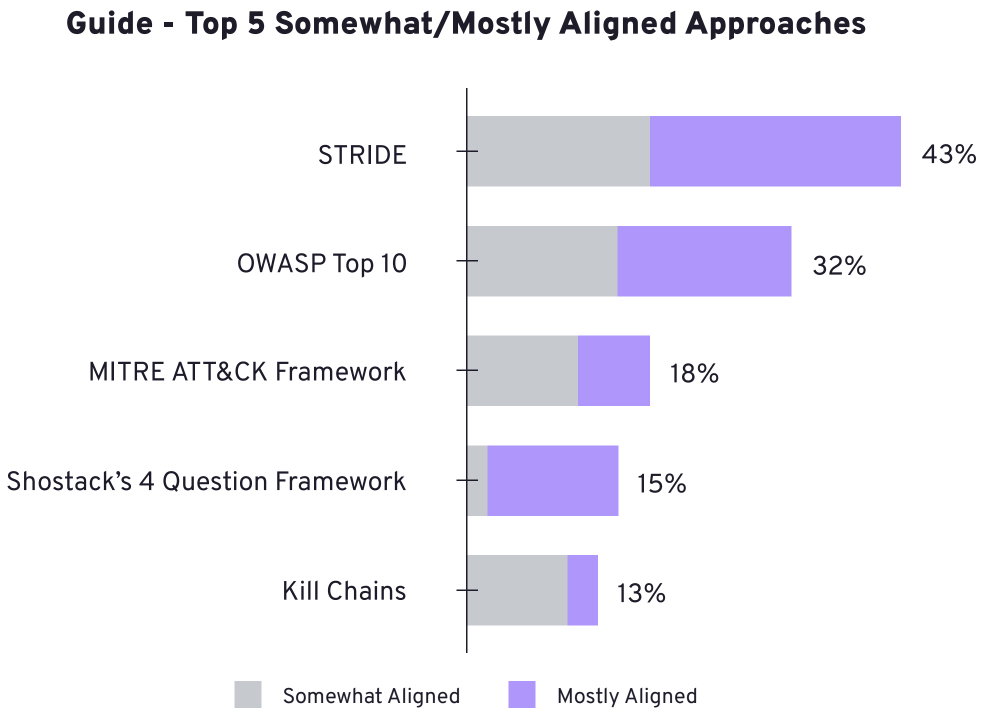
- **Instructive** - approach selected as Aligned
- **Guide** - approaches selected as Somewhat Aligned or Mostly Aligned
- **Influencer** - approaches selected as Mostly Unaligned or Slightly Aligned

Here are the top 5 for each.



Instructive - Top 5 Aligned Approaches

**Figure 2: Top 5 threat modeling approaches with the highest alignment. One-third of respondents use STRIDE, while around one-fifth align with Shostack's 4-question framework.**



Guide - Top 5 Somewhat/Mostly Aligned Approaches

**Figure 3: The top five threat modeling approaches most commonly reported as Mostly Aligned or Somewhat Aligned by respondents.**

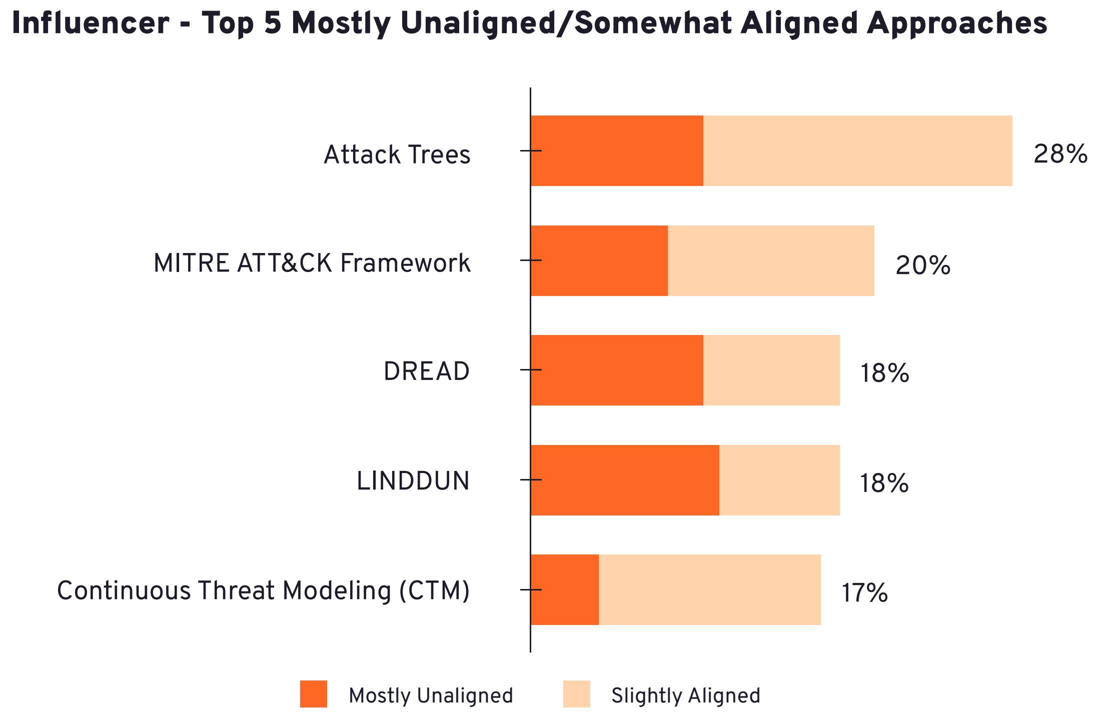


**Figure 4: The top five threat modeling approaches most frequently reported as Slightly Aligned or Mostly Unaligned by respondents.**

The approaches that are the most strictly followed are STRIDE and Shostack's 4 Question Framework. STRIDE is also a guide to how many companies threat model, along with the OWASP Top 10. Interestingly, the complete data set indicates there are many, quite evenly split, approaches that companies have a small alignment with, implying they have been influenced by them in how they have designed their own approach to threat modeling.

Also, there were on average 4 approaches that survey participants listed as having some kind of alignment to how their company threat models, with on average 1 approach for Slightly Aligned, 1 for Somewhat Aligned, 1 for Mostly Aligned and 1 for Aligned. There was no restriction in the survey on how many approaches responders could align with, and some participants responded with up to 10 (some responded alignment to all 26, but these responses were disregarded as misunderstanding the question).

**One-third of respondents use STRIDE, while around one-fifth align with Shostack's 4-question framework.**

# Tools

## *Dedicated tools are used by the minority; generic tools are the core to most practices.*

Tools are an important part of threat modeling and many companies use them to help scale their threat modeling process. A survey goal was to establish which tools were being used as a regular part of how a company threat models, but also how satisfied those companies were with the tool (Q19).

In terms of this report, we just list the tools that are most commonly used and the satisfaction levels across all tools (as the goal is to highlight the tools doing things right, and not to pass judgement on less popular tools).

Only 35% of responders said they regularly use a threat modeling tool (Q18), which in itself is a revealing insight into the community. Whether companies that don't use tools do so because they can't find a tool that works for them, feel they don't need one, or some other reason, this wasn't captured in this year's survey. Companies can be using more than 1 tool (or may have used more than 1 regularly within the time period covered by the survey).
Of the 28 tools listed only 13 were indicated as being used by survey respondents, with the average number of tools in use being 2.3 tools per company.

**Top 5 Most Used Dedicated Threat Modeling Tools**

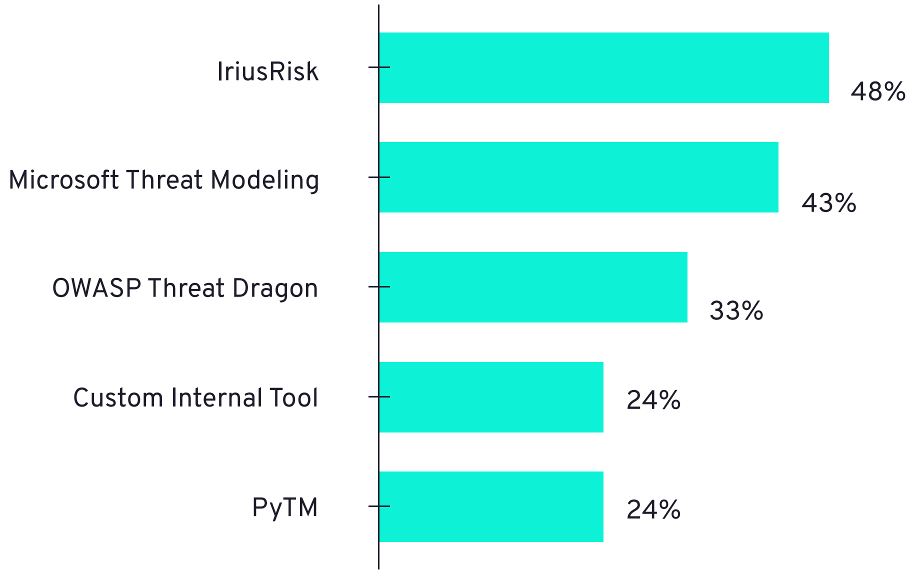


**Figure 5: IriusRisk and Microsoft Threat Modeling Tool are the most commonly used tools among respondents, with several also using OWASP Threat Dragon or internal/custom solutions.**

*Respondents rated their satisfaction with each tool separately, or could have responded "N/A" for tools they don't use The percentages shown are the sum across all satisfaction categories.*

As a minority of respondents are actually using dedicated threat modeling tools, it's hard to draw data driven conclusions about the satisfaction level of specific tools. We can look at satisfaction levels across all tools though.

**Distribution of Satisfaction Levels Across All Tools**

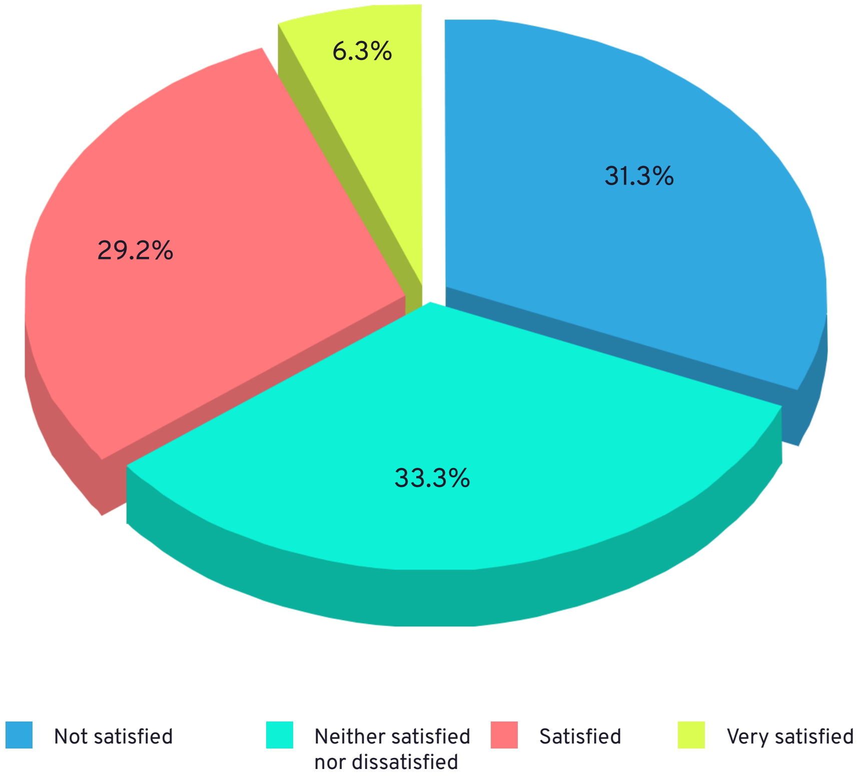


**Fig 6: Satisfaction levels for tools fall into roughly; a third are satisfied, a third are neutral and a third are not satisfied.**

*Percentage values are across all respondents who answered for any tool.*

As the numbers are so evenly split between the different satisfaction levels (if we combine Satisfied and Very Satisfied), interpreting this data likely depends on whether you take a 'glass half full' or a 'glass half empty' perspective, which in-turn probably depends on your own experience with dedicated threat modeling tools. Perhaps the next survey can tease out what functionality of dedicated tooling tools are meeting the community's needs, and what functionality isn't.

Additionally, generic tools are in use as well, highlighted in the following graphic. Some of these numbers are more interesting when viewed as what some companies aren't using, as they imply 27% aren't using a drawing tool and 37% aren't using ticketing software.

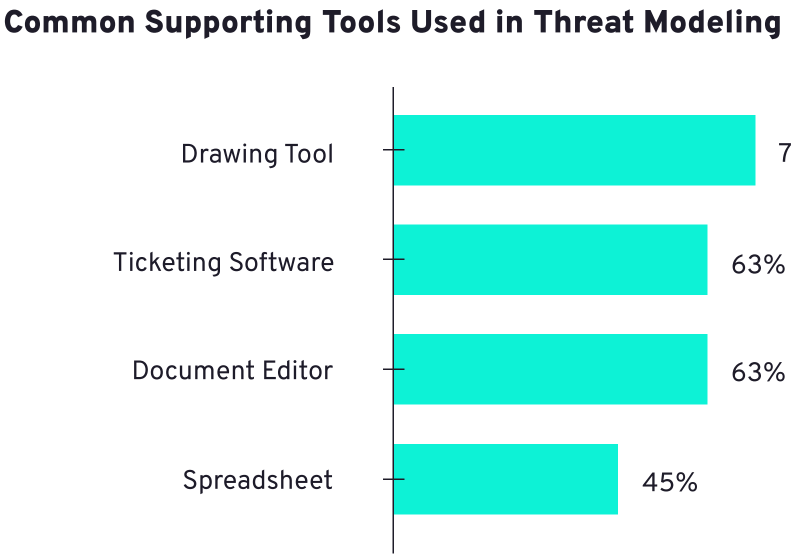


**Figure 7: Drawing tools are the most commonly used supporting tool (73%), followed closely by ticketing software and document editors (63%), while spreadsheets are less frequently used.**

# Diagrams

## *Diagrams are nearly always required, but vary in accuracy and function.*

Diagrams are one of the most commonly used tools to help with how a company threat models. The goal of asking about diagrams (Q27) was to figure out how essential a diagram is in terms of deriving threats as part of a threat model. This is relevant because diagrams are also a high cost/friction part of threat modeling, especially if they need to be created from scratch.

**Requirement for a System Diagram in Threat Modeling**

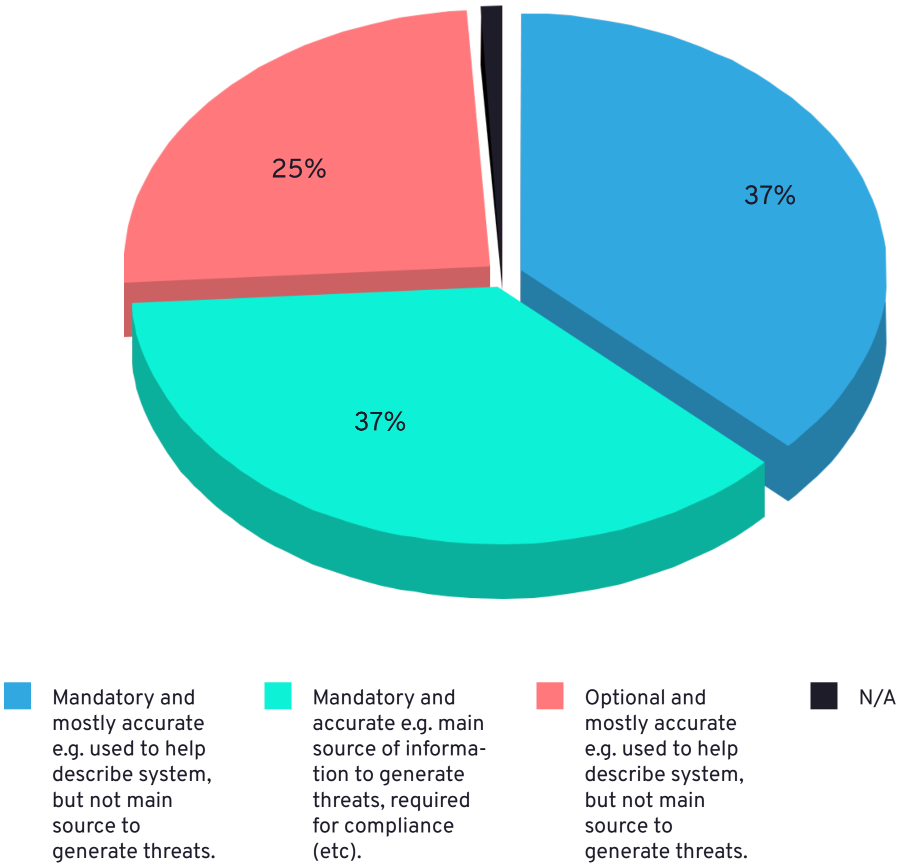


**Figure 8: While there's no clear consensus on requiring accurate diagrams for threat generation, most companies treat diagrams as essential to their threat modeling process.**

# Trust Boundaries

## *Widely adopted by companies, with most defining it as 'shared trust levels'.*

72% of survey participants use trust boundaries as part of how their company threat models (Q28). However, what each company means by trust boundary might not be the same, so the goal of this question was to establish some data about what definitions are the most common (Q29).

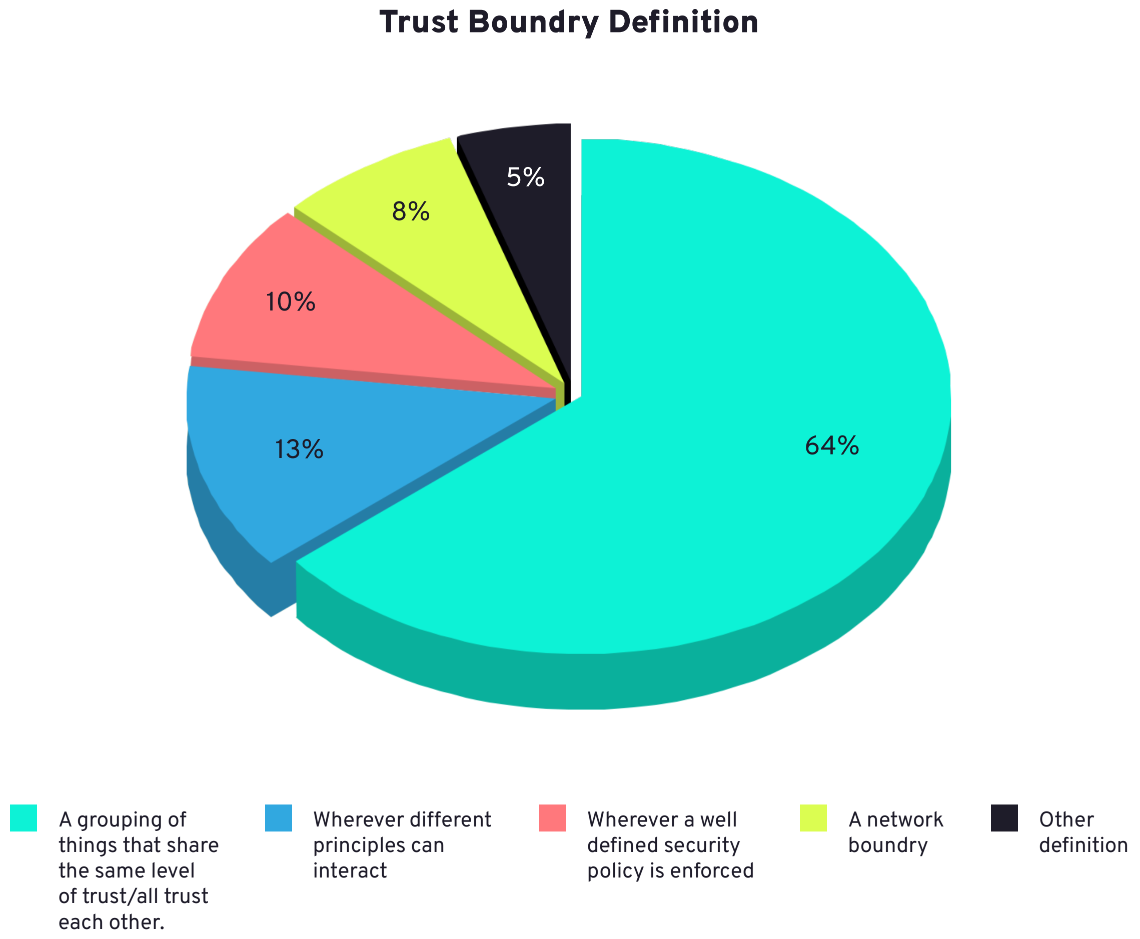


**Figure 9: Most respondents (64%) define trust boundaries by shared trust levels, with fewer citing interaction points, policies, or network boundaries.**

So it seems there is a fairly clear preference for how a trust boundary is defined, but we'll leave it to the community to debate the relative merits of the different definitions (or even if the survey missed some).

# Threat Model Count

## *Most companies create 10-100 models per year, regardless of size.*

What number of threat models are companies getting done each year? (Q42). Productivity in threat modeling is an indicator for how effective your threat modeling practice is. This question aims to give a broad understanding of the number of threat models companies are producing, so you can compare your own practice.

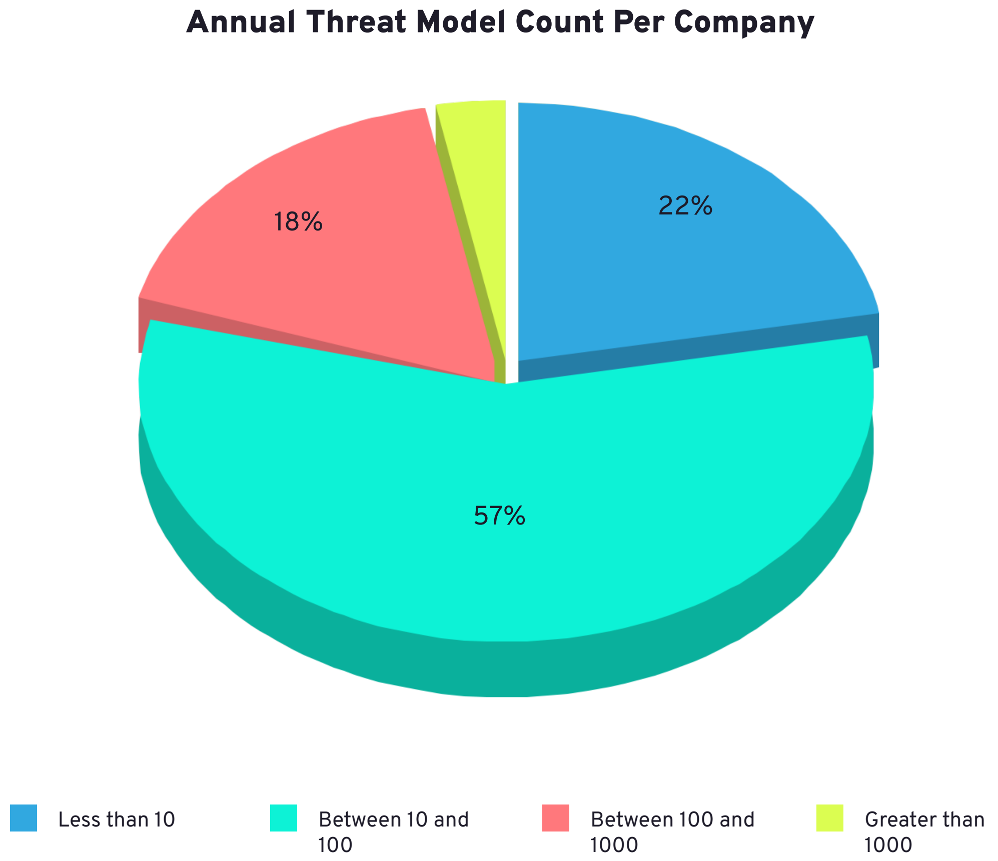


**Figure 10: The majority of companies (57%) create between 10 and 100 threat models per year, with smaller groups producing fewer than 10, or more than 1000, annually.**

Most companies are producing about 10 to 100 threat models a year.  But surely it would depend on company demographics right? The data indicates not as much as you'd think.

- The size of a company wasn't a clear factor, as amongst the respondents representing companies of sizes 100-999, 1000-9999 and 10000-99999, the number of responses in the 10-100 count of threat models was much higher than other count ranges, and roughly equal regardless of company size.
- The size of the Security Team wasn't a clear factor, as Security Teams of ~5 in number were the major contributors to getting a count of 10-100 threat models, and bigger teams were as likely to produce a 10-100 count of threat models as they were to produce a higher count.

- The number of Security Champions wasn't a clear factor, as companies with any number less than 50 (including no Security Champions) were still more likely to produce a count of 10-100 threat models than any other count range.

For companies doing 1000+ threat models, there were only a couple of respondents, but those were large companies (100,000+), large Security Teams (10+), and a large number of Security Champions (20+).

## Reporting

### *Reporting remains a big gap – impacting leadership engagement and support.*

Are threat modeling practitioners reporting the threat modeling work they do to management, giving management visibility of the effort and results? (Q44). Support from management is usually essential for the success of any security program activity, and giving management visibility into the activity is usually required for continued support.

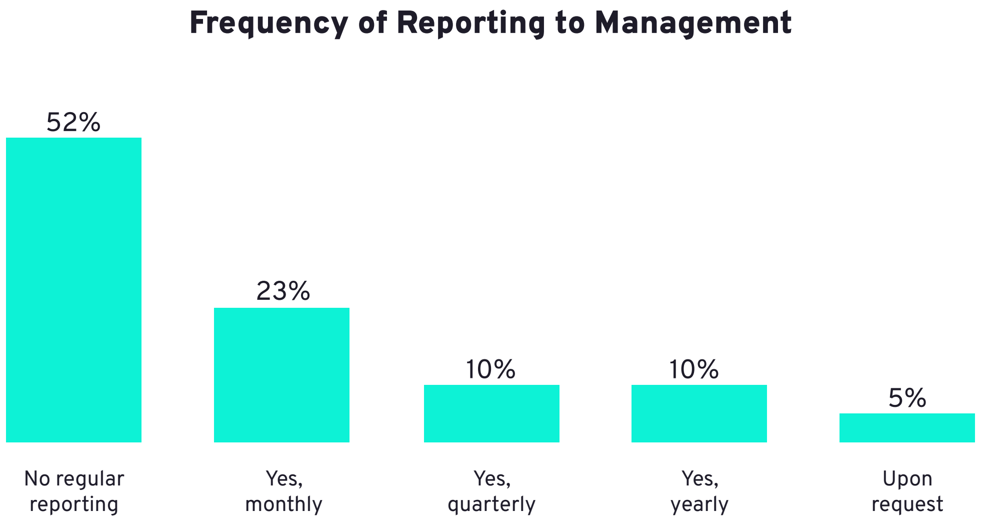


**Figure 11: Over half of respondents (52%) don't report threat modeling results to management regularly; 23% do so monthly, with fewer reporting quarterly or yearly.**

Add to this that only 25% of companies have a threat model dashboard (of any kind) (Q43). Cross-referencing reporting data with Challenges, there were 4 times as many responses indicating "Lack of executive support" being "Always" or "Frequently" a challenge when no reporting was being done, compared to when reporting was being done.

# Challenges

## *On average, organizations face 10 persistent challenges in their threat modeling activities.*

Threat modeling is certainly not without its challenges. The survey had a list of 37 different challenges we queried respondents about (Q46-Q50), and the challengers certainly resonated with people. On average companies have 10 challenges that they “Always” or “Frequently” have to deal with.

Here are the top 10 challenges that participants responded that they “Always” or “Frequently” have to deal with:

**Top 10 Challenges in Threat Modeling By Frequency**

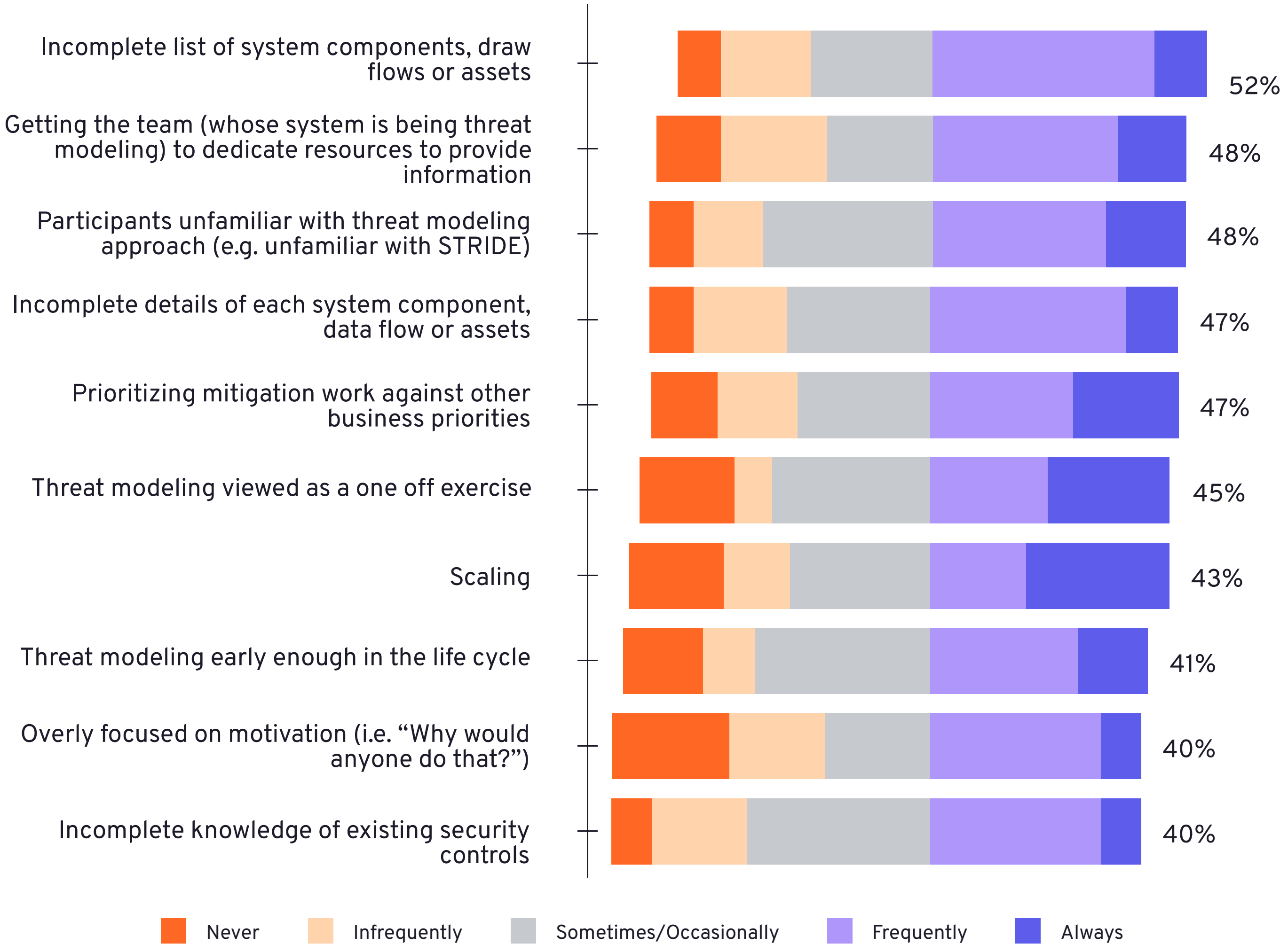


**Figure 12: Key challenges include incomplete system details and limited resources, with over 40% also citing scaling, timing, and approach-related issues.**

*Respondents evaluated each challenge by how frequently it was a challenge. Top 10 challenges ranked by (and aligned on) sum of Frequently or Always a challenge (number shown is percentage sum).*

The percentages might not seem that high, but that is because they don’t include the numbers for “Sometimes/ Occasionally”, if we do include those numbers we get 9/10 of the same threats (slightly different order) and the percentages are all between 68-80%.

That said, some of the Challenges turned out not to be significant challenges at all, here are the bottom 5 Challenges (respondents giving the Challenge a ranking of "Never" or "Infrequently")

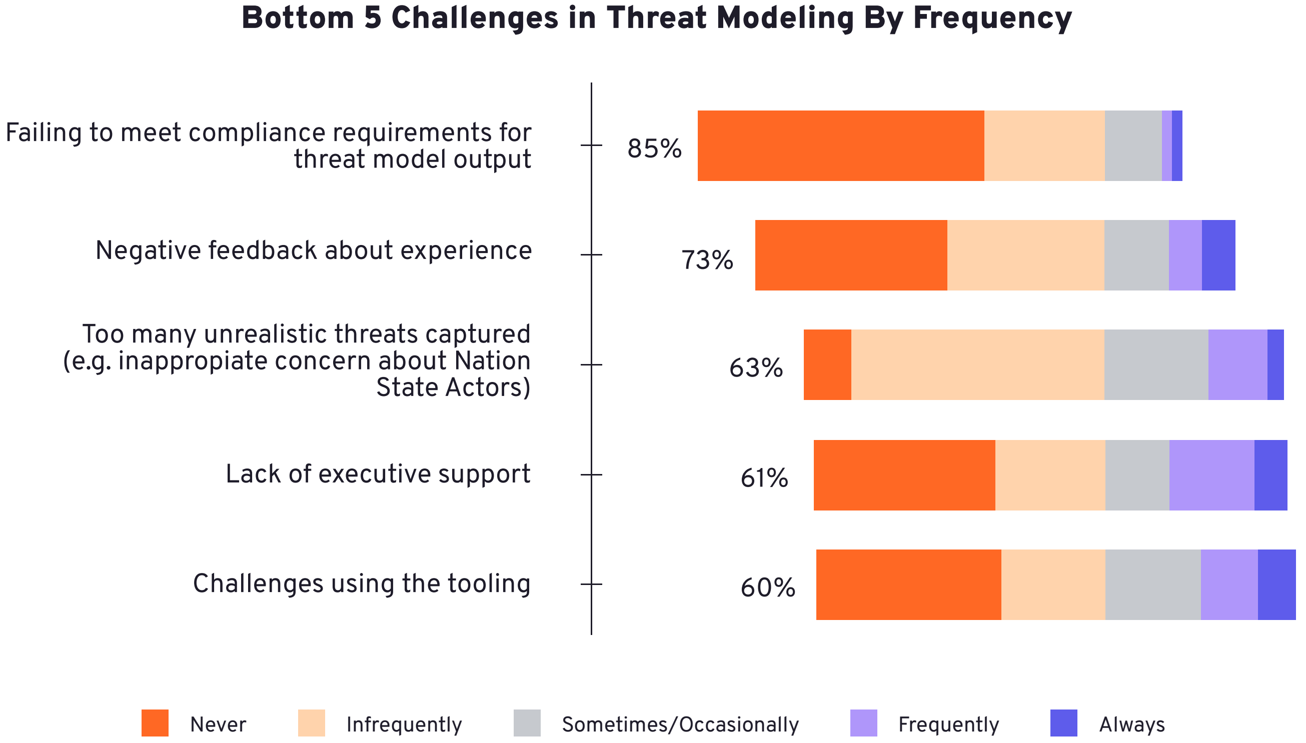


**Figure 13: Most respondents rarely encounter issues like compliance failures, negative feedback, lack of executive support, or tool-related challenges.**

*Bottom 5 challenges ranked by (and aligned on) sum of Never or Infrequently a challenge (number shown is percentage sum).*

Some of these non-challenges may be a bit misleading though as companies without compliance requirements or companies that aren't using tools, will clearly not have those respective challenges, which then skews the numbers for understanding these challenges for those companies they apply to.

**The top challenge was identified as 'Incomplete list of system components, draw flows or assets.' The least challenging area was found to be 'Failing to meet compliance requirements for threat model output.'**

# Respondents: People & Companies

The threat modeling survey was always more about how companies threat model than how people do, but it was pragmatic to capture who the actual people answering the survey were (Q1), in case it was going to be relevant to other survey answers. The vast majority (68%) were Security Team members, with a variety of other job titles making up the remainder. This is good as Security Team members really were the target population for the survey. In terms of threat modeling experience (Q2) there was a great variety, with 8+ years being the largest group (30%), but generally survey respondents were experienced with 78% having more than 2 years experience.

However, since a threat modeling activity is a company activity, it is company demographics that are required to give context to the answer of survey questions. The high level breakdown is:

- **Geographic area (Q4)** - Europe (50%), North America (42%), Asia-Pacific (7%) and Latin America (2%)
- **Threat Modeling Program Maturity (Q5)** - 0-2 years (43%), 3-4 years (38%), with other year ranges 10% or less
- **Industry (Q6)** - Dominated by Software (25%), Technology (22%), and Finance (12%), with 12 other industries at 5% or less.
- **Number of employees (Q7)** - There was a skew to larger companies with; 1-100 (5%), 100-1k (22%), 1k-10k (32%), 10k-100k (33%), 100k+ (8%)

Looking at the cross-sectional data of program maturity and number of employees, as you might expect there is a trend for larger companies to have more mature programs, with the single biggest demographic (20%) being 3-4 years maturity and 10k-100k employees.

# Threat Modeling Program

For threat modeling to be an effective security activity, it has to be more than just good at finding threats, it must be a program of work that demonstrates business value, and be operated in a manner consistent with other business activities.

In this section, we'll explore the key components of threat modeling programs, reflecting how companies are approaching sponsorship (leadership support), alignment with compliance frameworks (to secure sponsorship), areas of application (beyond compliance), program coverage (how extensively systems are threat modeled), team sizes, and the training and resources provided to support these efforts.

# Sponsorship: Executive Support & Gaps

Executive sponsorship (Q8) for any business activity is usually essential, and 60% of survey participants reported having executive sponsorship (CISO or other executive), whilst 28% only had Security Team or Project sponsorship, and 12% had no sponsorship.

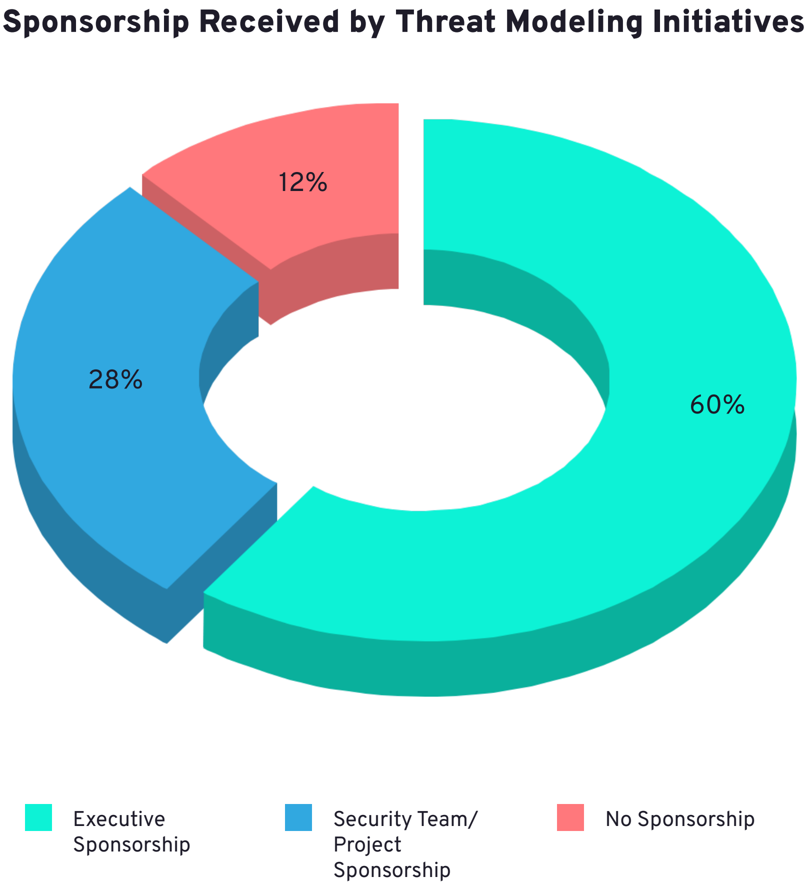


**Figure 14: Most respondents (60%) have executive sponsorship, while others rely on Security Team support or have no sponsorship at all.**

# Aligning Threat Modeling with Compliance

One of the best ways to get sponsorship is to align threat modeling with another activity (Q10) such as compliance with a regulation/framework/standard, and 85% of survey participants reported threat modeling supports such compliance, with the top 5 being (with 16 others reported by 5% or less):

### Top 5 Compliance Frameworks Most Commonly Supported by Threat Modeling Programs

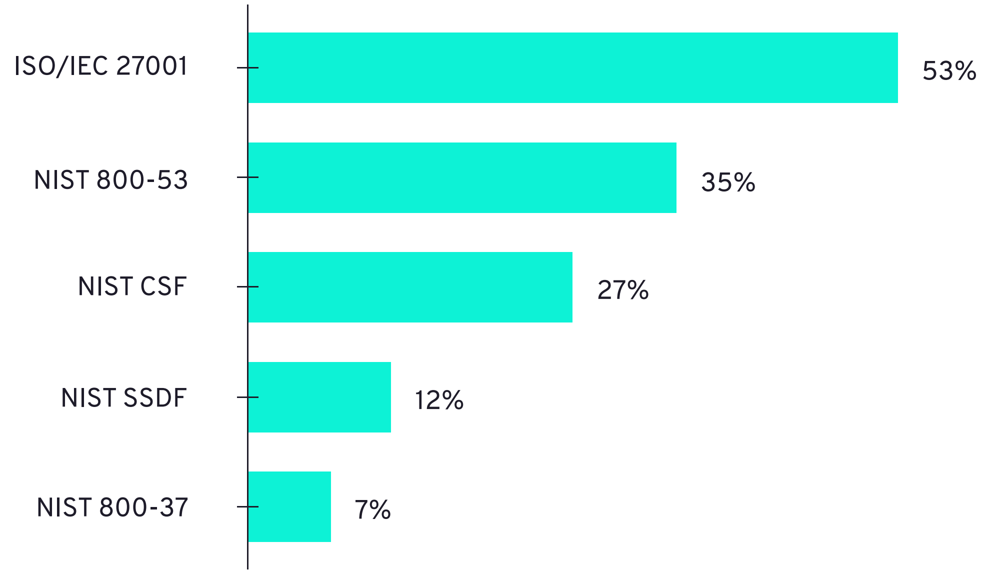


**Figure 15: ISO/IEC 27001 is the most referenced standard (53.3%), followed by NIST 800-53 (35%) and NIST CSF (26.7%).**

## Broad Application: Beyond Software

Threat modeling supports risk analysis for more than just compliance purposes, so the survey asked generically what sort of areas were threat modeled within survey respondents companies (Q9):

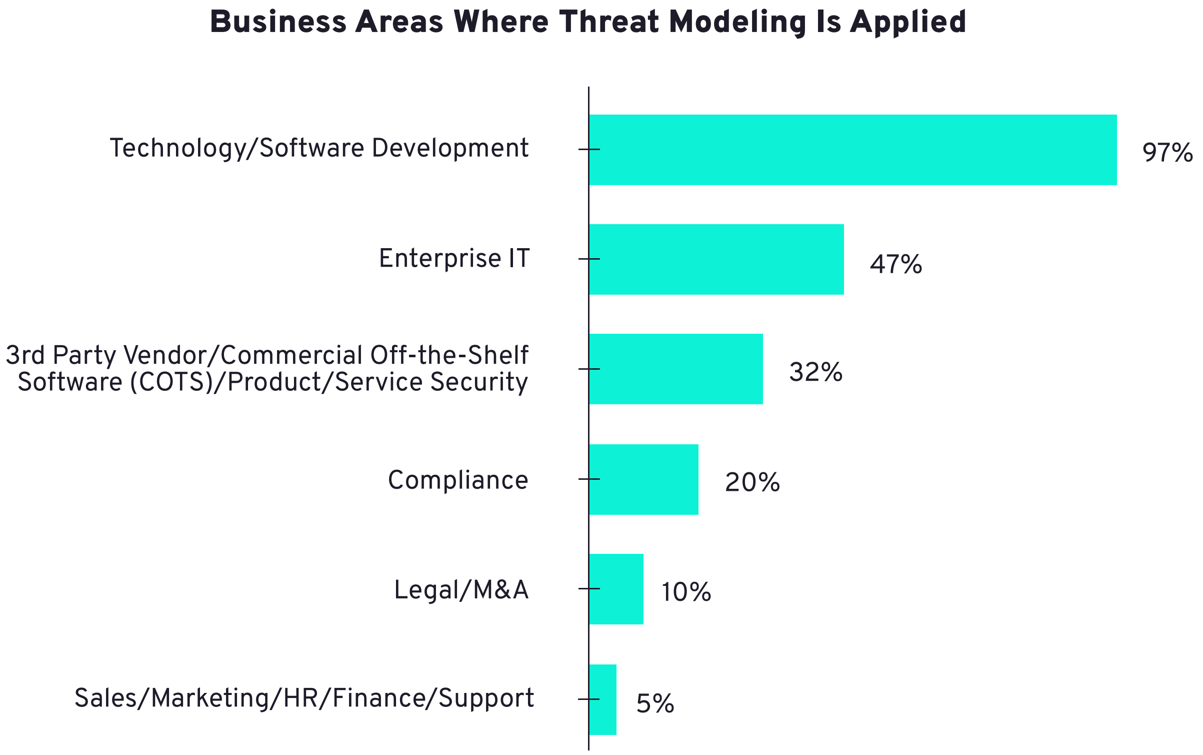


**Figure 16: Threat modeling is most common in technology and software development (97%), with fewer organizations applying it to compliance, vendor assessment, or business functions like Legal and HR.**

Unsurprisingly, software is a target for threat modeling almost universally, but Enterprise IT and COTS systems also show significant numbers, indicating threat modeling's broad applicability to help analyze risk. Interestingly, only 20% of survey participants answered Compliance, but significantly higher numbers stated they were using threat modeling as part of meeting a regulation/framework/standard, but that may just be a matter of interpretation of an overloaded word like 'compliance'.

# Selective Threat Modeling Due to Resources

93% of companies aren't threat modeling all their relevant systems (and the 7% that are, really need to share their secret!) (Q23), which means companies are being selective about what to threat model as resource limitations are a reality most companies have to cope with. 27% are able to threat model all their systems that meet a risk threshold, but 55% are constrained by their threat modeling capacity with the most common in-take approach for threat modeling work being ad-hocly identified systems (20%) and risk ranking (15%).

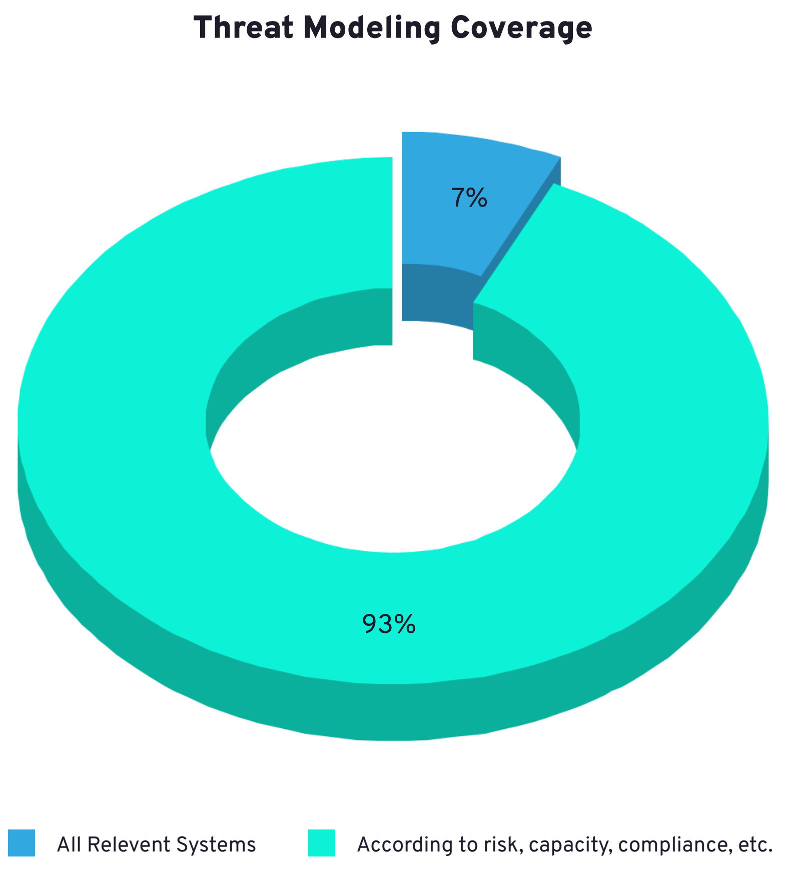


**Figure 17: Only 7% of companies threat model all relevant systems; most limit efforts based on risk, capacity, compliance, or demand.**

## Security Team Size & Champion Programs

A company's threat modeling capacity (Q13) will be constrained by resources and 47% of companies have 2-5 members of the Security team who support the threat modeling process. 18% of companies only have a single person helping, while 32% are lucky enough to have 6 or more people.

Using Security Champions (Q14) is another way to provide support for threat modeling, but 35% of companies report not having a Security Champions program, and 28% of those that do, report threat modeling is not a focus of that program. 18% of companies have 1-10 Security Champions supporting threat modeling, and 18% are fortunate enough to have more than 10 supporting it.

## Training & Resources

Training (Q11) can often be key to helping people and teams help themselves to contribute to threat models, thus freeing up capacity for Security. Companies report providing the following resources to help with threat modeling:

### Training and Educational Resources Provided for Threat Modeling

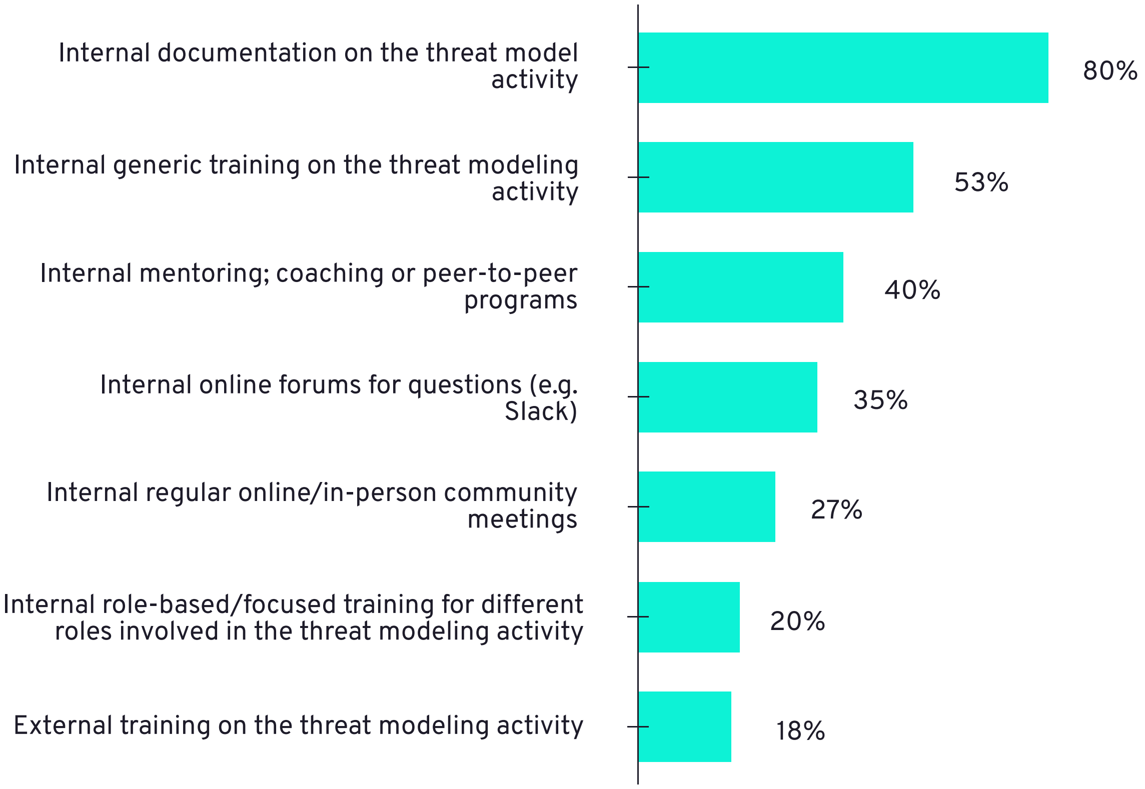


**Figure 18: Most companies support threat modeling with internal documentation (80%) and training (53%), while mentoring, forums, and community meetings are less common.**

# How

The threat modeling program needs to be supported by an effective approach to finding threats. The "how" of threat modeling is something the community is constantly evolving, and the survey was hoping to capture a snapshot of some of the most relevant aspects.

# Scoping: Managing Complexity

How to scope a threat model (Q24) is essential for making sure the activity doesn't become a huge drain on resources, and the most popular approaches to divide a system into manageable threat modeling chunks were:

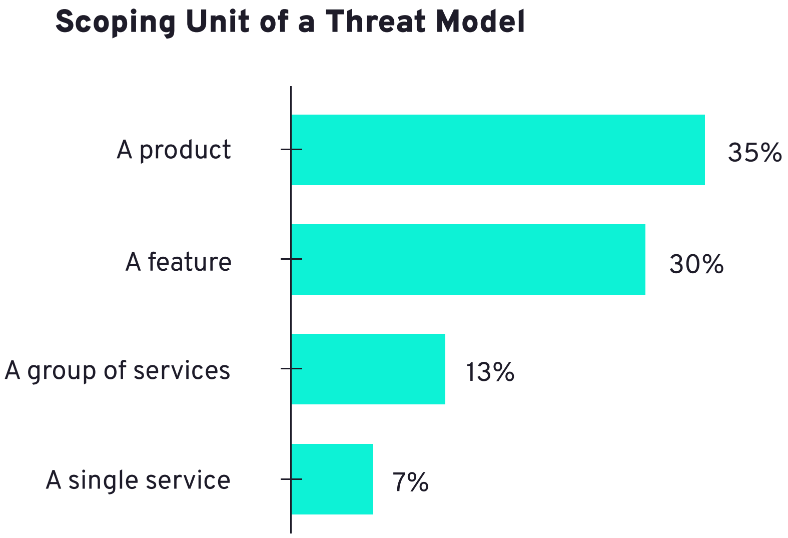


**Figure 19: Most companies scope threat models at the product (35%) or feature (30%) level, with fewer scoping around services.**

Another way to manage resource for a given scope is to decide how many threat models to generate (Q25), with the popular approaches being:

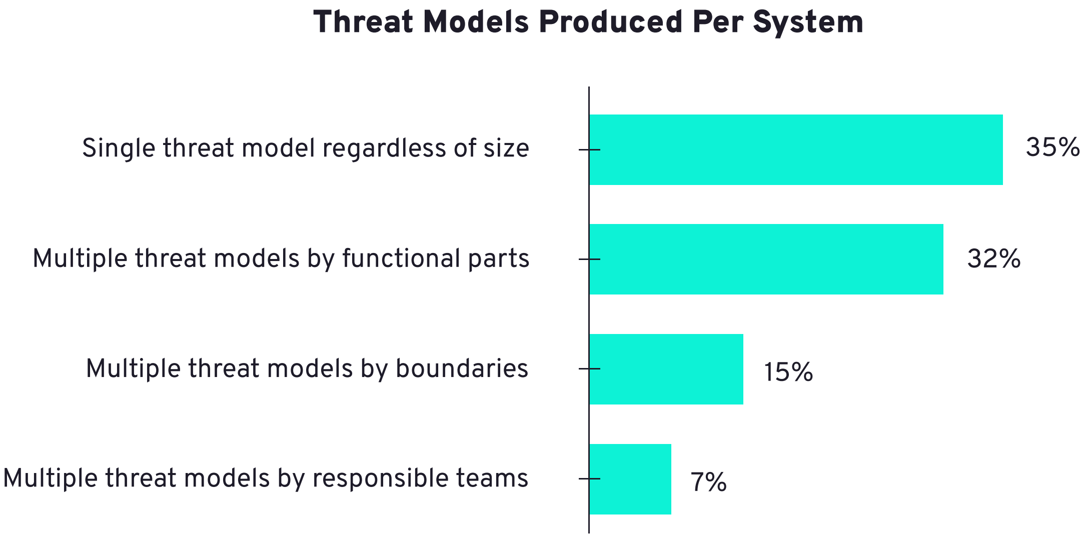


**Figure 20: 35% of respondents create one threat model per system, while others divide models by functionality, boundaries, or team ownership.**

# Threat Types: Architecture & Design Focus

What threats we look for (Q26) also impacts the threat modeling effort, but more importantly will really define what sort of contribution to overall security threat modeling makes as one of several security activities. The most popular types of security issues that companies threat modeling activities are designed to find are:

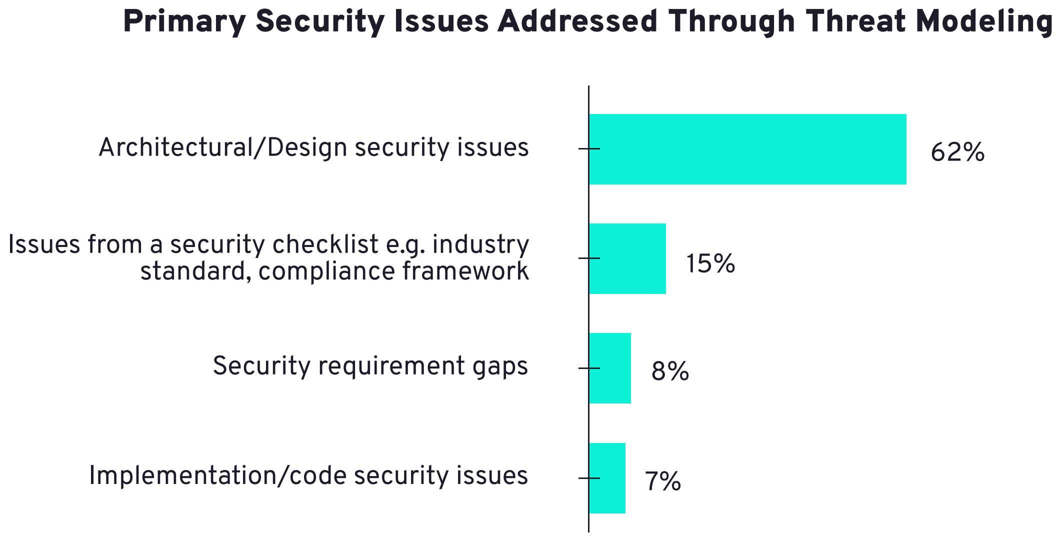


**Figure 21: Threat modeling mainly focuses on architectural and design issues (62%), with fewer targeting checklists, requirement gaps, or code-level vulnerabilities.**

Threat modeling is traditionally an activity to find architecture and design security issues, and so it's no surprise this is the most common type of security issues the activity is designed to find. Still, that 7% of companies primarily using threat modeling to find implementation or code security issues, likely challenges some expectations of what threat modeling should be used for.

# Information Sources: System Foundations

Gathering the right information is crucial to finding relevant threats. The survey looked to understand what sources of information are used to understand the system being threat modeled (Q31), and what internal (Q32) and external (Q33) resources are used to derive threats from this information. These questions were asked on a scale because this better reflected the flexibility in most threat modeling approaches, but still gave room for more definitive responses (such as "Not Used" and "Never").

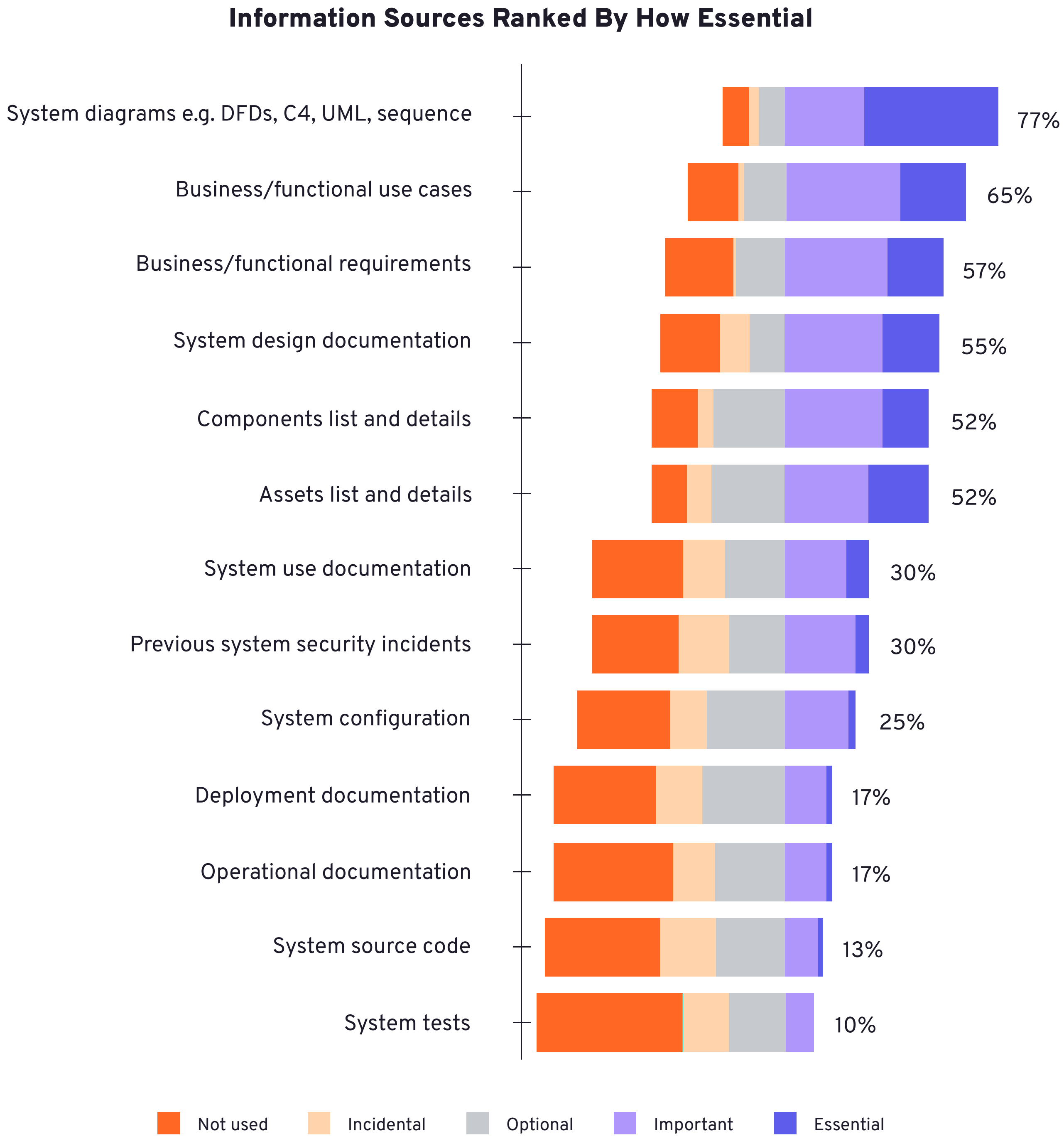


**Figure 22: System diagrams (77%) and business use cases (65%) are the most valued sources for threat modeling, while system tests, source code, and operational docs are less commonly used or considered essential.**

*The Information Sources listed are ranked by (and aligned on) sum of Important or Essential.*

It's clear that the vast majority of approaches will use any information source they have access to, but the sources of preference are those describing the system design (which nicely aligns with the majority of approaches seeking to find architecture/design security issues). It's interesting to note the sources that are confidently stated as not being used, although the survey didn't capture the difference between these sources being available and not used, versus *not* being available and hence not used.

## Resources for Threat Generation: Internal & External Tools

With the available information to hand, threat modeling needs to generate relevant threats. Experience certainly helps when it comes to generating threats, but the survey wanted to understand what resources companies make available or use to generate threats.

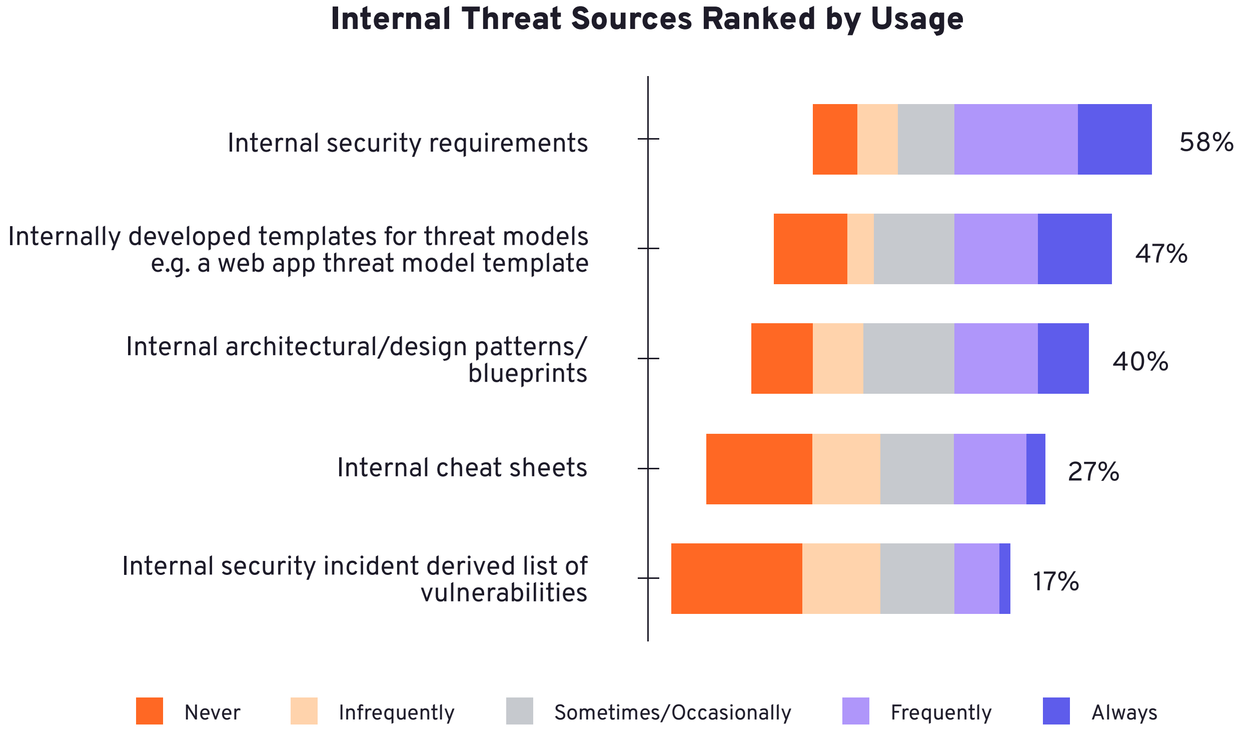


**Figure 23: Internal security requirements (58%) and templates (47%) are the primary resources for threat derivation, with less reliance on incident-based vulnerability lists.**

*The Threat Sources listed are ranked by (and aligned on) sum of Frequently or Always.*

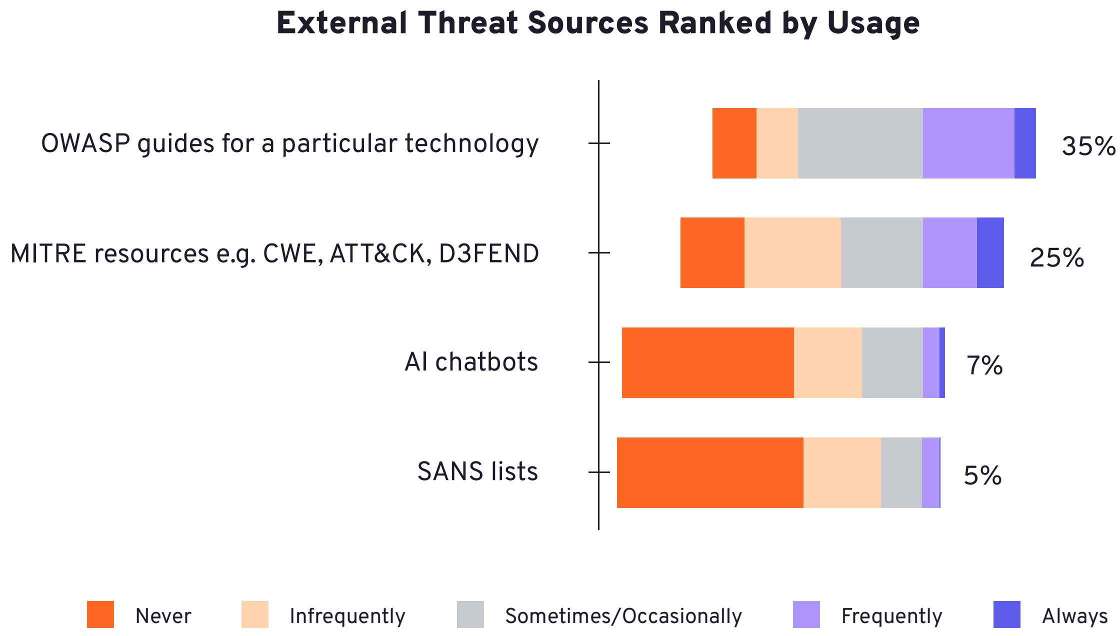


**Figure 24: OWASP and MITRE resources are the most frequently used external sources for deriving threats, while tools like AI chatbots and SANS lists are rarely used.**

*The Threat Sources listed are ranked by (and aligned on) sum of Frequently or Always.*

Some resource types for generating threats are clearly popular, but the numbers don't imply any particular source is invaluable. Perhaps more interesting are the numbers for resources that are never used, as many of these are quite small, which could imply that people will use resources that make sense for them in any given situation and see no reason to restrict themselves. OWASP guides particularly stand out as an external resource people will always look to leverage if relevant.

**OWASP resources are the most frequently used external threat sources (35%). Tools like AI chatbots are currently rarely used (7%).**

# Contributors: Roles in Threat Management

Documented threats are obviously useful, but it's humans that tend to be able to find the threats (and controls) that are unique to a system. The survey looked to establish who in a company contributes most to threats (Q34) and controls (Q35). It comes as little surprise then that Security Team members are considered as Frequently or Always contributing relevant threats 80% of the time, and about 50% of the time threats also come from developers and Security Champions. The numbers are fairly similar for Frequent or Always contributors of mitigations with Security Team members at 70%, Security Champions at about 50%, but developers slightly higher (than threats) at 63%, which makes sense since they know their systems the best. Not a single respondent in the survey said that Security Team members Never contribute threats, although 1 respondent said the Security Team never contributes mitigations. According to the data then, Security Team members seem to be doing their job (granted, mostly in their own opinion).

**Contribution to Threat Identification and Mitigation By Roles**

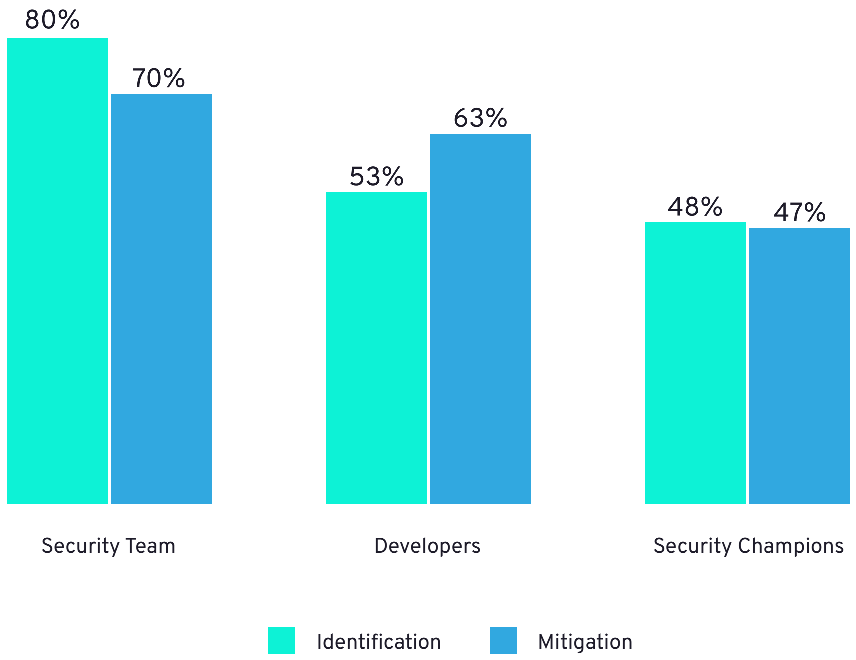


**Figure 25: Security Teams lead threat identification and mitigation, with Developers and Security Champions also contributing significantly. Testers, Ops, and managers contribute less than 15%.**

*Only the top 3 contributors are listed and are ranked by sum of Frequently or Always.*

# Concluding Threat Models: When to Stop

All good things must come to an end, and it's no different for threat models, but how is such a decision made? (Q36)

## Decision Criteria for Ending a Threat Modeling Activity

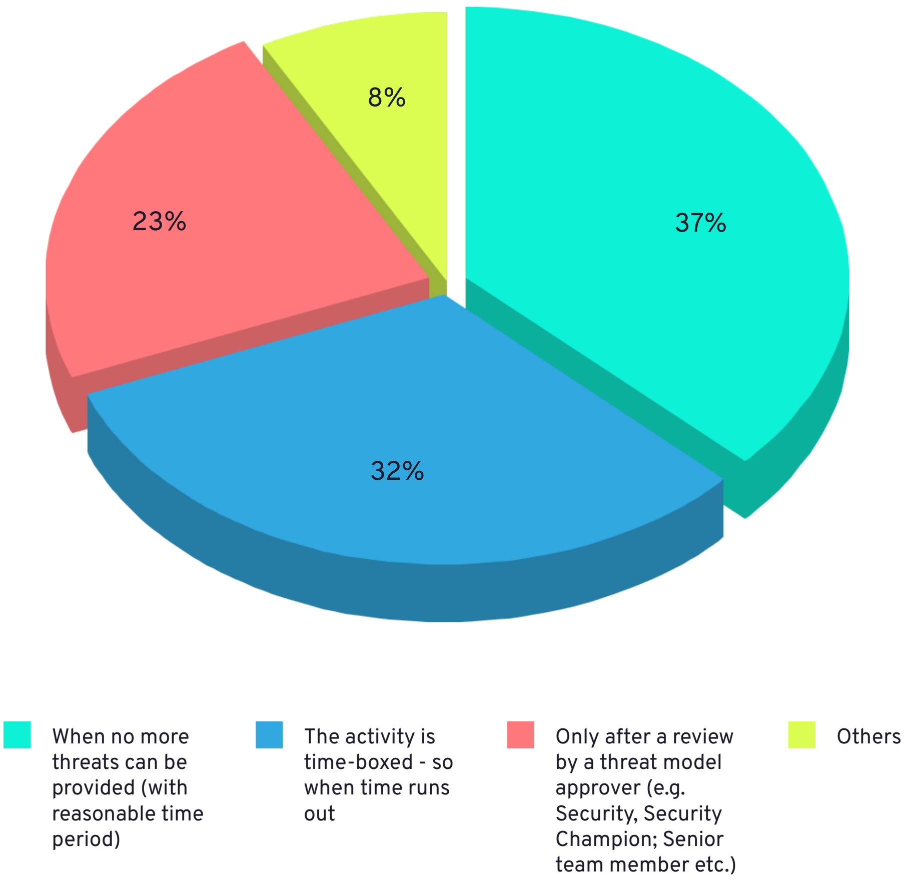


**Figure 26: Most organizations end threat modeling when no new threats are found (37%) or when it reaches its time-boxed limit (32%), with fewer requiring formal review or approval.**

No clear preference here amongst the community, perhaps again showing that people are adapting their threat modeling activity to suit the needs of the business.

# Managing Threat Model Updates

Just because a threat model has to end doesn't mean it shouldn't be updated to stay relevant, and the survey wanted to know how companies treat updates to a threat model (Q37).

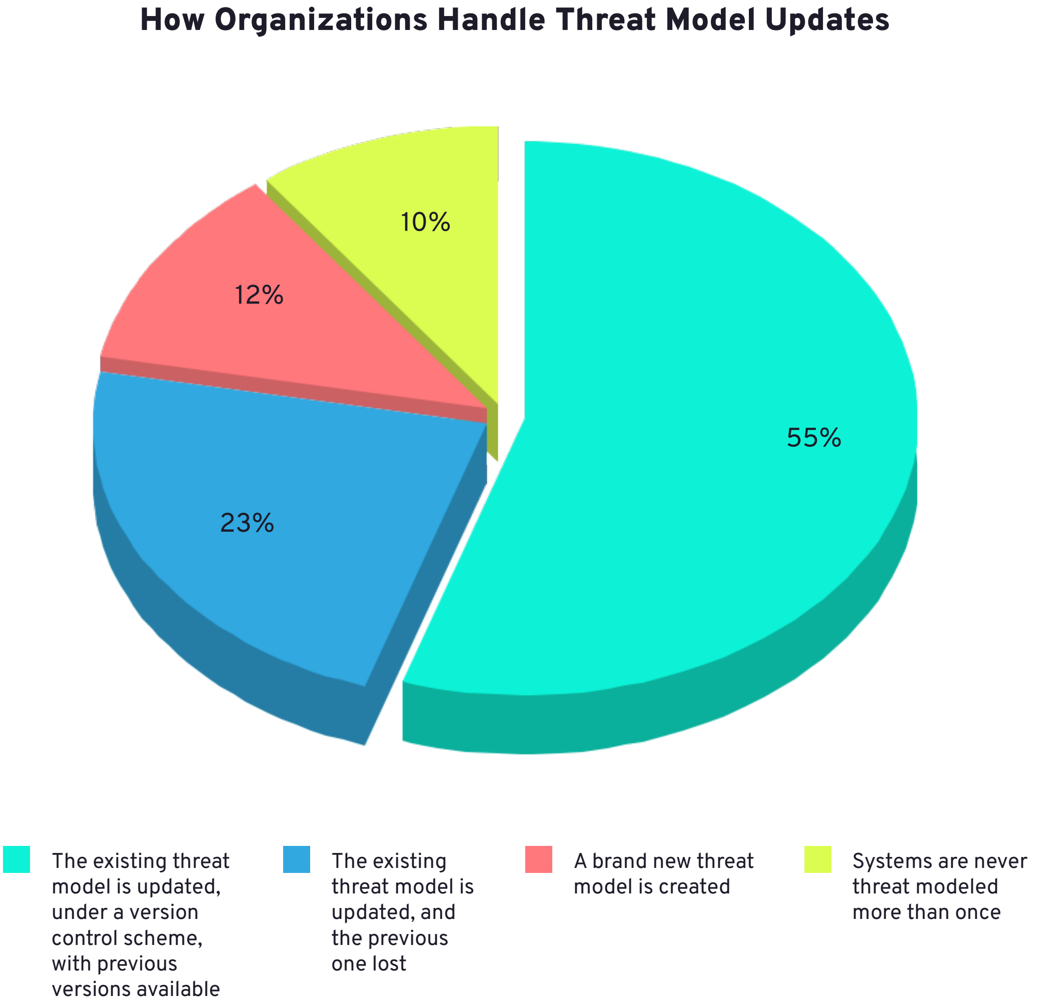


**Figure 27: Over half (55%) update threat models under version control, while others overwrite, restart, or don't update models.**

Perhaps threat modelers have been hanging out with developers for so long now that we are starting to pick up some of their habits, and certainly there are worse habits to adopt than version control. Either way, there is a clear message with 90% of companies deciding to threat model their systems more than once - a threat model is for system life, not just system sign-off (to paraphrase the expression "a dog is for life, not just for Christmas").

# Output

A threat modeling program will be designed to meet the needs of the business, but the survey wanted to capture more than just what the program is designed to do, by also capturing the reality of which stakeholders actually consume the outputs of the threat model.

In the survey, these consumers of threat models were split into internal consumers (Q40) and external (to the company) (Q41) consumers.

## Consumption by Stakeholders

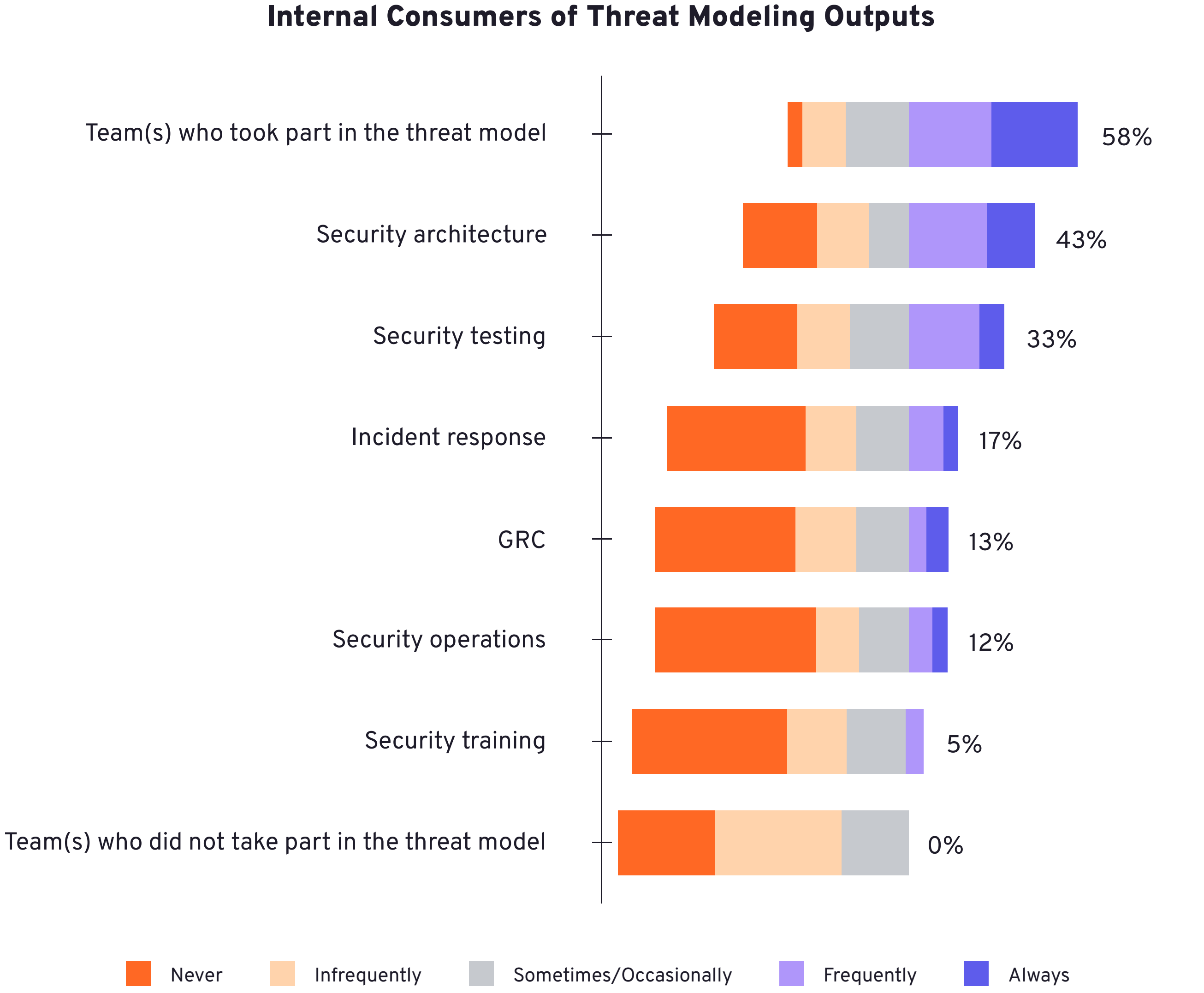


**Figure 28: Threat modeling outputs are most used by teams involved in the threat modeling process (58%) and security architecture (43%), with less use by security training and operations.**

*The Internal Consumers listed are ranked by (and aligned on) sum of Frequently or Always.*

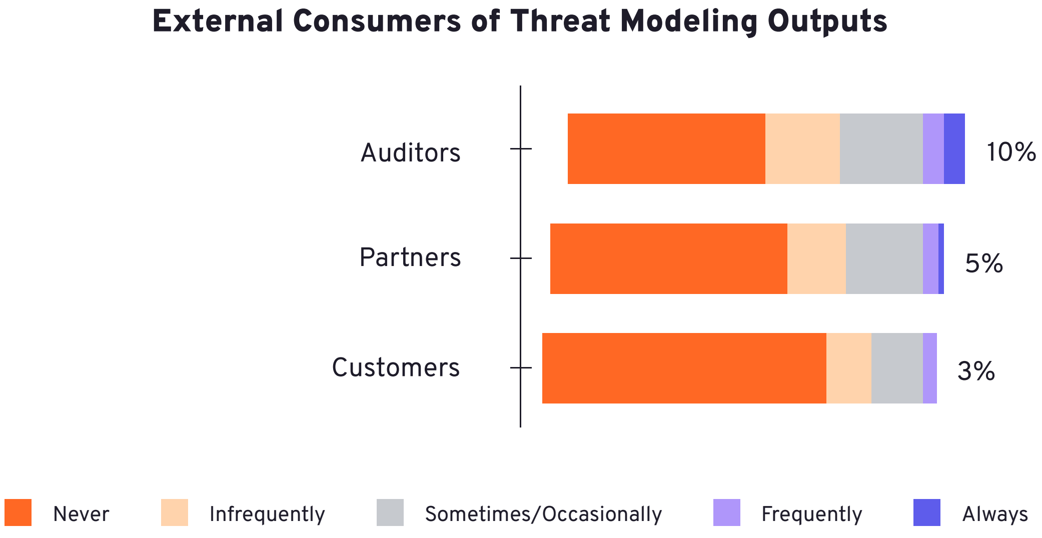


**Figure 29: Few respondents share threat models externally; when they do, auditors are the primary recipients, with partners and customers receiving them less often.**

*The External Consumers listed are ranked by (and aligned on) sum of Frequently or Always.*

Sharing threat models externally seems to be something most companies do not regularly do, presumably this is because threat models can contain sensitive information. It does beg the question of how the community is supposed to share threat models when we struggle to share them with those who arguably have a vested interest.

## Limited Access to Threat Models

The data for sharing internally (Q39) indicates some companies are sharing threat models (53%), but the numbers imply that sharing regularly (28%) is not particularly widespread outside of those groups usually involved in the threat modeling activity. It's difficult to look at these numbers and not wonder whether threat modeling would be more broadly adopted if it was made more available and more applicable to indirect consumers (i.e. not those whose system was being threat modeled).

One explanation for limited consumption of threat models is that they are simply not available (Q38), and the survey wanted to capture whether this was the case. 34% say they are not sharing threat models internally, which includes 22% actively restricting access to threat models internally. 53% responded that they are sharing threat models internally, which included 28% actively promoting the threat models of others. Cross referencing these responses by industry didn't suggest sharing restrictions are industry driven as the most restrictive sharing industry was "Technology" and the most active sharing industry was "Software".

# Reporting

*While some companies track systems modeled or threats identified, 43% report no metrics at all.*

The survey questions related to reporting have already been partially covered in the Reporting section under Key Findings, but beyond whether it is happening the survey also wanted to capture what metrics are being reported (if any) (Q45).

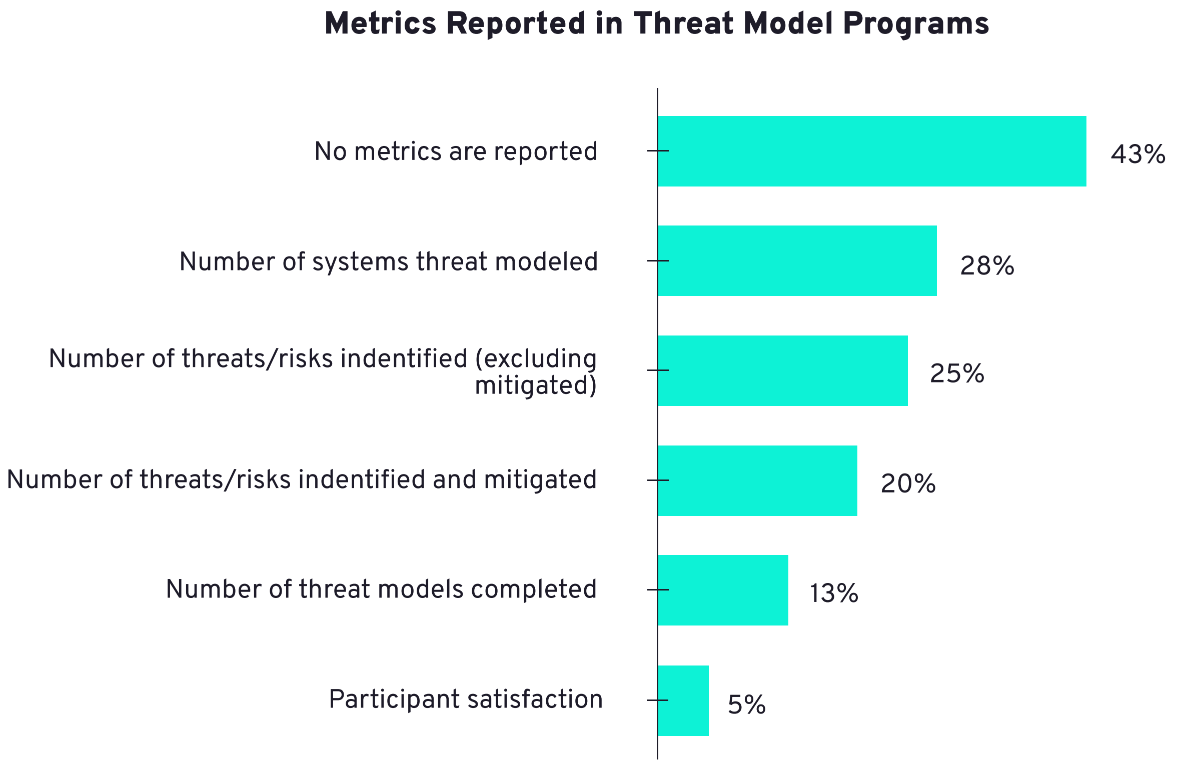


**Figure 30: While 43% of organizations don't report metrics, others track system counts, threats identified and mitigated, models completed, and participant satisfaction.**

Focusing on what metrics are reported, the data doesn't indicate any clear consensus on the type of metrics that should be reported. Certainly reporting risks identified (whether mitigated or not) makes up the largest response, but it's unclear if this is primarily trying to report on the effectiveness of the threat modeling program, or if it is trying to report on risk to the business.

# Challenges

*Early phases of threat modeling pose the greatest difficulties.*

The other Challenges section looked at the questions about challenges in aggregate, but it is also worthwhile to look at them as they appeared in the survey, split out according to the 4 question framework (Q46-Q49).

## Incomplete System Information & Resource Limits

The top 3 “What are we working on?” challenges feature in the top 5 overall challenges, so clearly the first phase of threat modeling is where companies are struggling the most. Also noteworthy are the small “Never“ numbers, implying these challenges are broadly relevant, as almost everyone is facing these challenges to some extent. The implications of the first aspect of threat modeling representing the greatest challenges has implications, because if the first aspect is a big challenge then arguably that will impact the effectiveness of every other aspect of threat modeling.

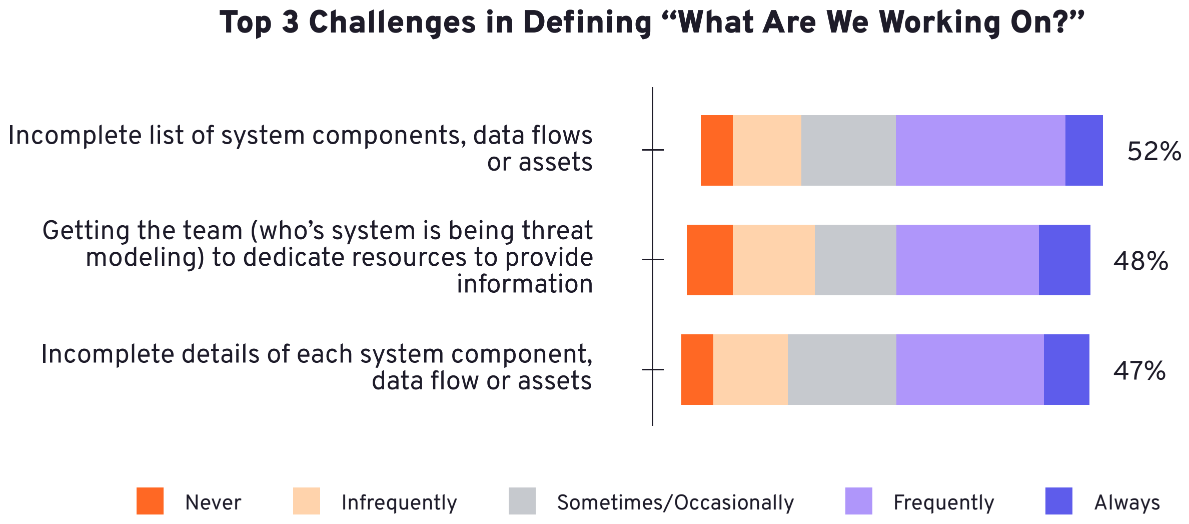


**Figure 31: The main challenges include incomplete system component lists and difficulties in securing team resources to provide necessary information.**

*The Top 3 Challenges listed are ranked by (and aligned on) sum of Frequently or Always.*

# Familiarity & Focus Issues

Unfamiliarity with threat modeling is the 2nd (equal) most overall challenge, so despite the efforts to provide resources to support threat modeling, the struggle is real to get teams to adopt the process. Backing up that unfamiliarity is the focus on motivation, another common mistake in threat modeling. Lastly, knowledge of security controls as a challenge is arguably a chicken and egg problem, because a threat model is a great way to capture security controls teams sometimes don't even know they have.

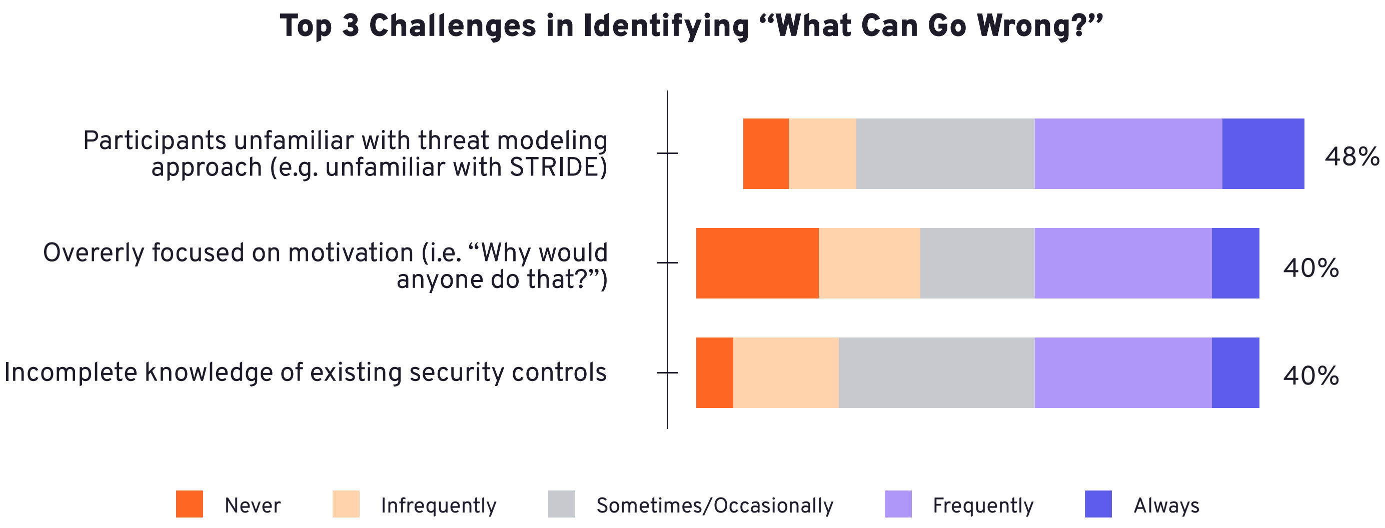


**Figure 32: Key challenges include unfamiliarity with threat modeling approaches, excessive focus on attacker motivation, and gaps in knowledge of existing security controls.**

*The Top 3 Challenges listed are ranked by (and aligned on) sum of Frequently or Always.*

# Prioritizing Mitigations vs. Business Priorities

Companies experience the challenge of prioritizing mitigations against other work, well, that is a challenge across the board for more than just threat modeling, more than just security activities in general; prioritizing work is just a constant challenge for all business activities, so this one comes as little surprise.

**Top Challenges in Deciding "What Are We Going to Do About It?"**

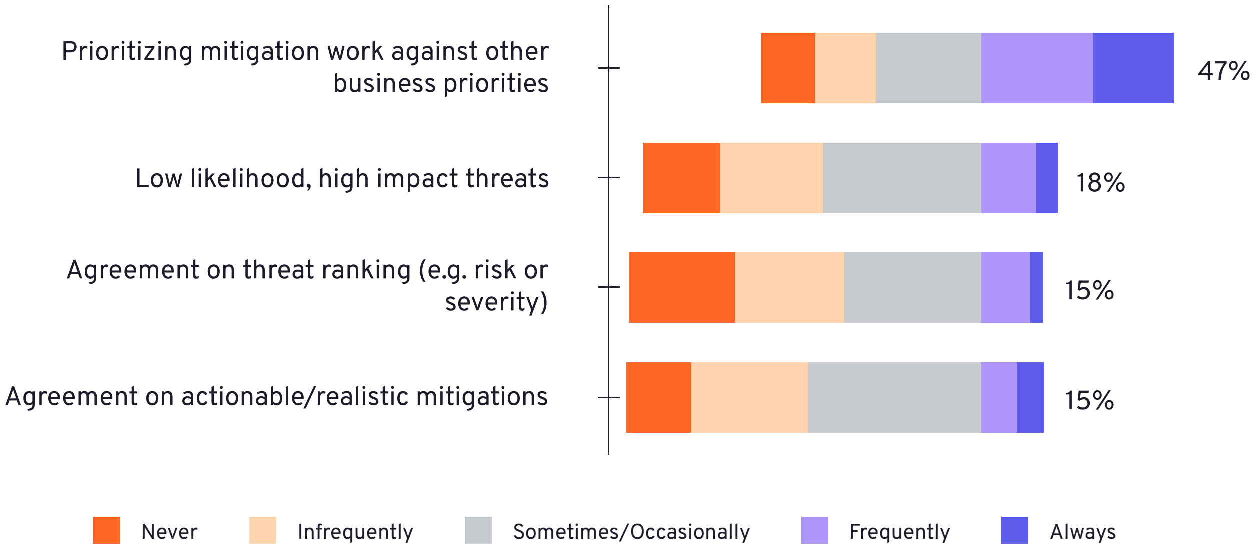


**Figure 33: The main challenge is balancing mitigations with business priorities, along with agreeing on threat rankings and feasible mitigations.**

*The Challenges listed are ranked by (and aligned on) sum of Frequently or Always.*

## Consistency & Completion Criteria

The last aspect of threat modeling, “Did we do a good enough job?”, has the lowest numbers of companies finding challenges in this area, and that arguably says something about the perception of importance of this aspect compared to the others.

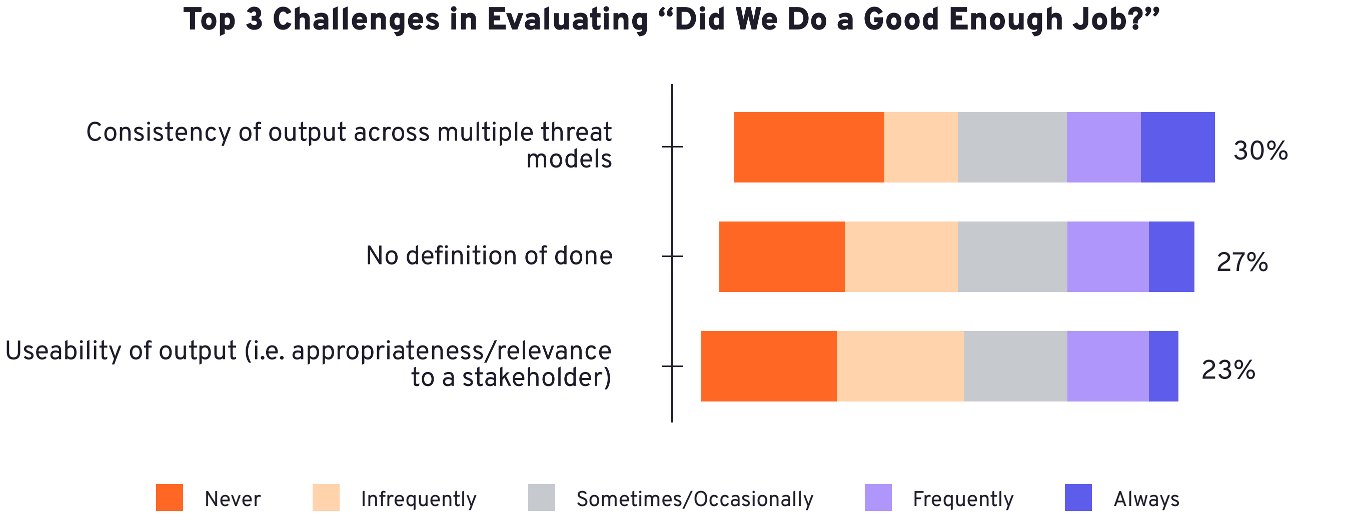


**Figure 34: Top 3 Challenges in Evaluating “Did we Do a Good Enough Job?” include maintaining consistency, defining completion criteria, and meeting stakeholder needs.**

*The Top 3 Challenges listed are ranked by (and aligned on) sum of Frequently or Always.*

**The lowest number of challenges were found in the final question of the the Four Question Framework; ‘Did We Do a Good Enough Job?’**

# Overcoming One-Off Perceptions & Scaling

These challenges for a threat modeling program (Q50) read as a who's who of well known program challenges. Most companies want to threat model; early, often and broadly, and solving for that is difficult.

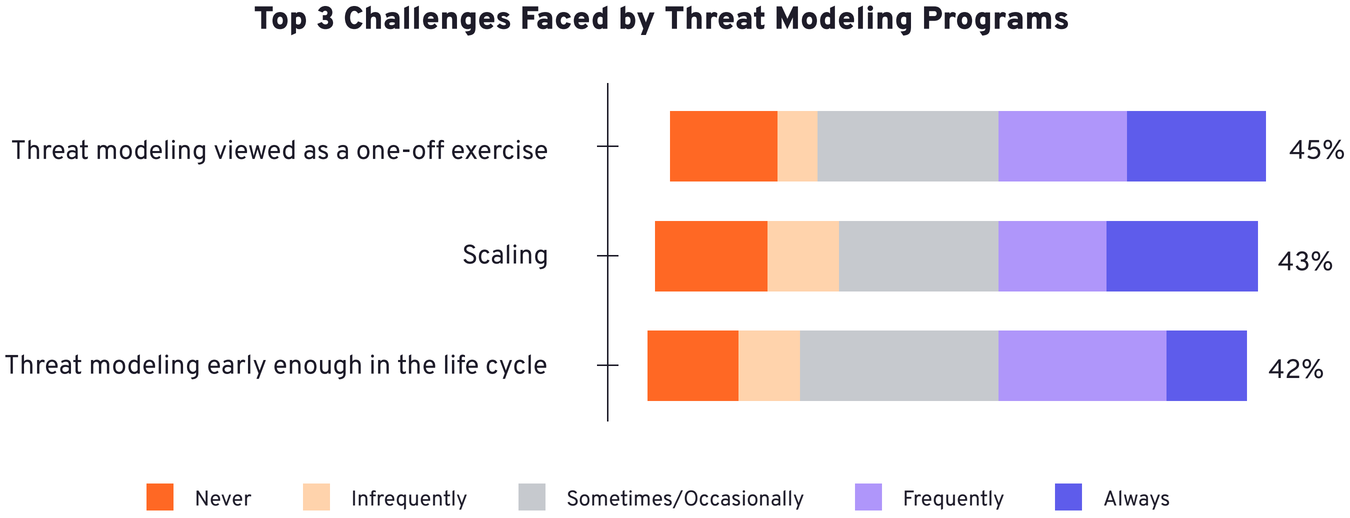


**Figure 35: Top challenges include overcoming the view of threat modeling as a one-off task, scaling it, and integrating it early in development.**

*Top 3 challenges ranked by (and aligned on) sum of Frequently or Always a challenge. Numbers shown are percentages.*

# Conclusion

Normally making sweeping statements about threat modeling is, to say the least, often controversial. That's because there has never been much data to back up such a statement, but that changes with this survey report. Does that make any particular statement correct, certainly not, but to form an opinion based on an interpretation of data is the basis of all science, so it's certainly the best way to do it.

A little controversy though can be good to stimulate a debate in the community. Let's draw some conclusions about what this survey is telling us about threat modeling.

- **We love STRIDE**
- **We leverage generic (non-dedicated) tools to threat model**
- **We use trust boundaries, and they refer to components that trust each other**
- **Diagrams and threat modeling go hand in hand**
- **We don't produce more than about 100 threat models a year**
- **We don't report to management about threat modeling, and when we do we don't align on what metrics to report**
- **We use threat modeling as evidence of compliance (even if we don't admit it)**
- **We threat model for architecture/design issues**
- **We'll take any information we can to help create a threat model. Threat modeling practitioners live off the land**
- **We'll generate threats from any source, but it's mostly coming from Security and the team involved**
- **We don't share threat models very often or very broadly**
- **We struggle to get the information we need to threat model**
- **The teams we work with struggle to learn threat modeling**
- **We don't focus on whether we did a good job threat modeling**
- **Many threat modeling challenges aren't special, and are the same as any other business activity**

Don't agree? Well, what does the data tell you? Share your thoughts with us.

## About the SOTM Project

The SOTM project is a community-driven initiative – by practitioners, for practitioners. It regularly publishes the State of Threat Modeling (SOTM) report to capture how threat modeling evolves across the industry, using real-world data and practitioner insights. Each edition provides a valuable benchmark for teams to reflect on, compare, and improve their own practices.

Sign up for updates on the next survey and report, or visit our website to learn more.

THREAT MODELING CONNECT
POWERED BY IRIUSRISK