Survey: IT Leaders Have Misplaced Confidence in Their Security Tools

ThreatModeler®

A ThreatModeler White Paper

December 2022

Survey: IT Leaders Have Misplaced Confidence in Their Security Tools

EXECUTIVE SUMMARY

ThreatModeler commissioned a survey of IT security leaders to identify key trends and pain points facing businesses as they seek to build and maintain secure and resilient information architectures. The results highlight an apparent conflict between the leaders' confidence in their security tools and their ability to manage vulnerabilities.

Enterprises today are dealing with ballooning security threats, increasingly complex architectures and a lack of skilled workers to meet every day needs. This survey investigated whether enterprises are turning to automation and/or proactive technology solutions to reduce the burden on development and security teams when building and maintaining those architectures. The survey also sought to understand what IT leaders are focused on as we move into 2023.

While almost 80% of leaders are confident they've selected the right security tools, almost two thirds are worried that their architecture isn't resilient. This can be explained, in part, by an acknowledged difficulty in prioritizing security issues and a cybersecurity skills gap/labor shortage.

The most notable result was the impact of threat modeling. Leaders in enterprises that have incorporated threat modeling not only perceived an increase in efficiency and effectiveness of their tools (+15%), but also felt their architectures are more secure (+10%) as a result of discovering defects sooner in the SDLC.

Threat modeling continues to make great inroads as a tool to bridge DevOps and security. Going forward, IT leaders will likely continue viewing threat modeling as an important tool to improve their security and confidence in their system architectures.

SURVEY METHODOLOGY

From October 28, 2022, through November 3, 2022, ThreatModeler, in conjunction with SurveyMonkey, conducted a survey of 261 IT leaders (Owner, Executive, C-Level, Senior Management) in the U.S.

To preserve confidentiality, the survey did not capture any personally identifiable information of the participants. Data collection, to some degree, relied on participants estimating quantities like efficiency and effectiveness. The survey was comprised of a series of 10, multiple choice and true/false questions. The participants were instructed to choose the answer that best matched their current situation.

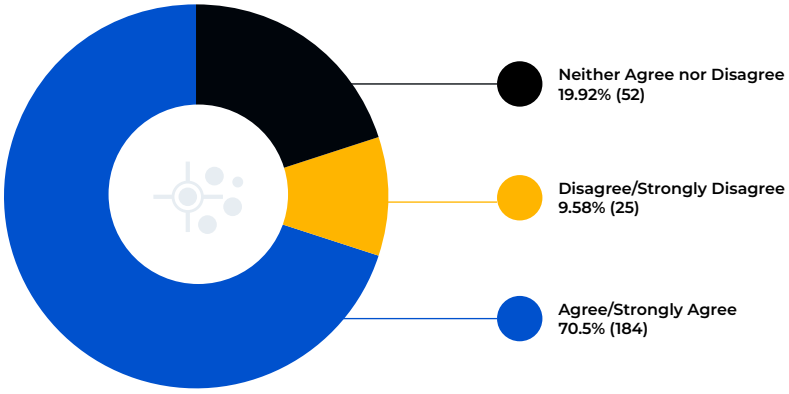
KEY FINDINGS

Most IT leaders have confidence in their security tool selection

All IT leaders understand the importance of having a resilient system architecture. To that end, they vary on their execution based largely on their perceived priorities and available resources. They use these factors to drive their investment in different tools and methodologies.

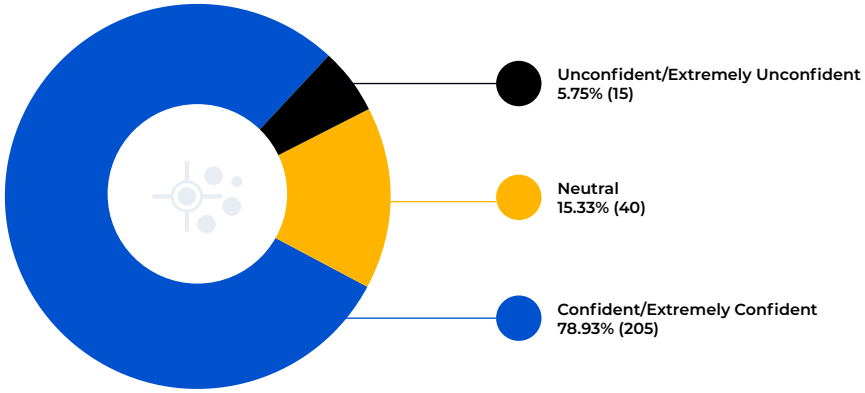
With all the variations, the one common theme running through the survey results is that a majority of IT leaders are confident in the tools they've selected to keep their architecture secure.

More than 70% agree or strongly agree their current SDLC tools and processes efficiently and effectively detect vulnerabilities.



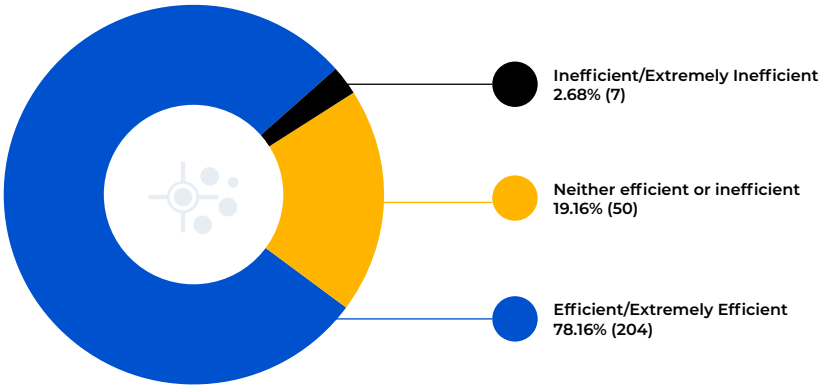
Q5 Your current software development lifecycle (SDLC) tools and processes efficiently and effectively detect vulnerabilities.

Nearly 79% are confident or extremely confident that their security tools are sufficient to prevent breaches and downtime.



Q7 How confident are you that your current security tools are sufficient to prevent breaches/downtime?

More than 78% say their current security tools are efficient or extremely efficient in terms of budget, labor and time resources used.



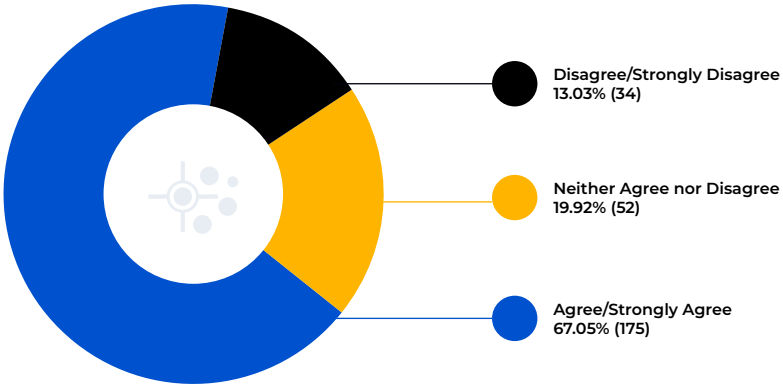
Q8 How efficient are your current security tools in terms of team resources (budget, labor, time)?

Most IT leaders struggle to identify and prioritize threats

Despite confidence in their tool selection, many IT leaders are not as confident in the security of their architecture or their ability to prioritize threats. This begs the question, do IT leaders have misplaced confidence in their choice of security tools?

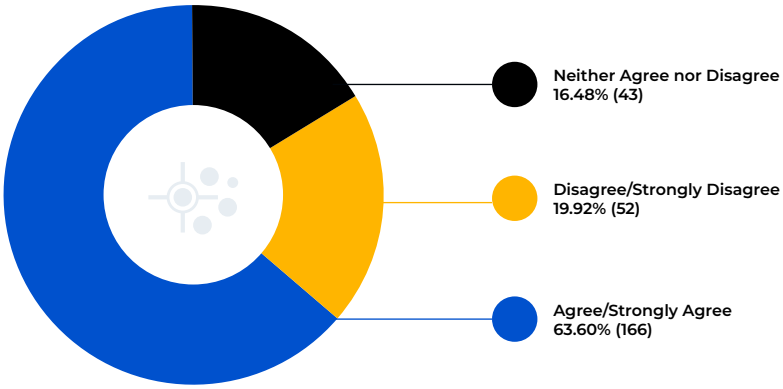
A majority also acknowledge a labor/skills gap contributing to these issues, and many have turned to technology as a result. That technology includes tools help identify vulnerabilities earlier in the SDLC and an increased reliance on automated solutions.

More than 67% of IT leaders agree or strongly agree that their team has found it difficult to keep their architectures resilient in face of increased IT/OT architecture complexity and rising threats.



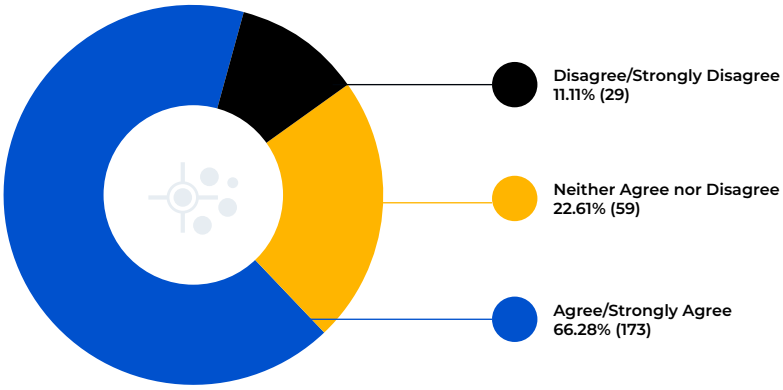
Q1 Your team has found it difficult to keep your architectures resilient in the face of increased IT/OT architecture complexity and rising threats

Even when aware of vulnerabilities, nearly 64% of IT leaders agree or strongly agree their teams found it difficult to prioritize which ones the security team should address first.



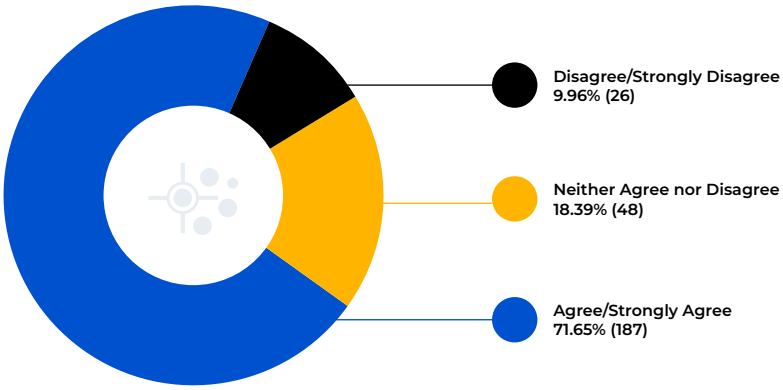
Q2 Even Aware of vulnerabilities, your team finds it difficult to prioritize which ones the security team should address first

More than 66% of IT leaders agree or strongly agree the labor/skills challenges have led their team to seek solutions that identify architecture vulnerabilities earlier in the SDLC.



Q4 Labor and/or skills challenges have led your team to seek solutions that identify architecture vulnerabilities earlier (shifting left) in the software development lifecycle (SDLC).

More than 71% of IT leaders agree or strongly agree the labor/skills shortages have led their team to seek more automated solutions within the SDLC.



Q3 Labor and/or skills challenges have led your team to seek more automated solutions within the software development lifecycle (SDLC).

Threat modelers feel better about their security posture

Regardless of what other security tools they choose, IT leaders who incorporate a threat modeling tool in their security toolbox feel better about the resiliency of their architecture. Threat modelers have an increased confidence in their ability to detect threats earlier and thereby keep them from getting into production.

Threat modelers also are more confident in their ability to prevent breaches and downtime, and feel better overall in terms of resource usage.

Overall, 70.5% of IT leaders agree or strongly agree their current SDLC tools and

processes efficiently and effectively detect vulnerabilities, but that number rises to over 86% for those who leverage a threat modeling tool

Overall, nearly 79% of IT leaders are confident or extremely confident that their security tools are sufficient to prevent breaches/downtime, but that number rises to more than 87% for those who leverage threat modeling

Overall, 78% of IT leaders say their current security tools are efficient or extremely efficient in terms of team resources (i.e., budget, labor, time), but that number rises to more than 86% for those who leverage threat modeling.

IT leaders who leverage threat modeling tools are 10% more likely to have a focus on finding tools that prevent vulnerabilities from making it to production when planning security budgets than IT leaders in general (45.8% versus 35.6%).

IT leaders who leverage threat modeling tools are nearly 8% less likely to have a focus on finding tools that quickly identify and mitigate zero-day threats as they emerge when planning security budgets than IT leaders in general (38.9% versus 46.7%).

WHAT THE RESEARCH TELLS US ABOUT THREAT MODELING

It is clear that IT leaders across the United States are struggling to keep up with increasing architecture complexity and the rapid proliferation of threats. While leaders are looking for more opportunities to automate and be proactive in their approaches, they still express broad confidence in their current tools. We all know the old adage, "The definition of insanity is doing something over and over again and expecting a different result." So, are enterprise leaders insane? Well, no. The truth is that these tools do work – until they don't.

The fundamental reason breaches continue to rise is that cybersecurity is a strategic problem we are trying to solve via tactical means. Enterprise cybersecurity is like a nation-state fighting off marauders – the nation will always have the fancier tools, but the marauders have time, surprise, and a much larger attack surface on their side. If the nation just sits and waits for an attack before reacting, it will always be chasing ghosts. Of course, this isn't how war works. Nations always gain an understanding of the whole battlefield and prioritize the protection of their most important assets. They also ensure their supply lines of information and resources (i.e. the network) are as short and protected as possible. The key in all of this is **strategic proactivity.**

DevSecOps enables us to bring the concept of strategic proactivity to enterprise cybersecurity. DevSecOps is a software development approach that integrates

security into the software development process. It is a combination of the principles of DevOps, which emphasizes collaboration and communication among software developers, and the practice of incorporating security measures into the development process.

The goal of DevSecOps is to make security an integral part of the software development process, rather than an afterthought. This involves incorporating security tools and practices into the development workflow, so that security is considered and addressed at every stage of the development process. The best tool through which enterprises can implement DevSecOps is threat modeling.

Threat modeling is an important security practice for enterprises because it helps organizations identify potential security threats and vulnerabilities in their systems and networks. This enables them to take proactive measures to protect against these threats, rather than reacting to security breaches after they have occurred. By identifying potential threats and vulnerabilities early on, organizations can implement appropriate controls and safeguards to prevent attacks and reduce the potential impact of a security breach. Additionally, threat modeling can help organizations prioritize their security efforts and allocate resources more effectively.

An effective threat modeling program should be an ongoing process that is integrated into the organization's overall security strategy. It should involve all relevant stakeholders, including executives, security professionals, and business leaders, and should be based on a thorough understanding of the organization's assets, operations, and potential threats. The threat modeling process should involve the following steps:

1. Identify and document the organization's assets, including sensitive data, systems, and networks.
2. Identify potential threats and vulnerabilities, taking into account the organization's specific operations and industry.
3. Evaluate the potential risks associated with each identified threat and vulnerability.
4. Develop and implement controls and safeguards to mitigate these risks.
5. Monitor and assess the effectiveness of the implemented controls and safeguards, and make any necessary adjustments.

Traditionally, threat modeling was a resource-intensive, manual and non-collaborative process. However, ThreatModeler has developed a collaborative platform where security experts and non-security professionals alike can visualize design flaws within a few hours or minutes instead of weeks.

ThreatModeler's solutions enable organizations to implement true DevSecOps by providing actionable insights through continuous monitoring and empowering teams to discover unknown flaws in real-time. Through its integration with CI/CD and ALM toolchain, ThreatModeler empowers security architects, developers and operations to keep track of mitigation progress until the threat modeled architecture is production ready.

A key feature of the ThreatModeler platform is IaC-Assist, a plug-in that enables organizations to reduce their threat drift from code to cloud by reducing the manual labor required to scan and remediate security threats. IaC-Assist allows DevOps teams to continuously evaluate their infrastructure-as-code (IaC) on the fly by developing a visual representation of potential flaws. The patented technology integrates into the CI/CD pipeline and encourages a more proactive, preventative approach to cloud security that saves organizations time, money and resources. IaC-Assist's automated capabilities improve developer productivity by identifying the design flaw or vulnerability, explaining the issue represented, and providing just-in-time contextual guidance for revision.

If IT and security leaders implement strategic proactivity via DevSecOps and threat modeling, they will be providing much different answers to similar surveys next year. They will be less likely to be overwhelmed by complex architectures and rising threats and far better positioned to prioritize vulnerabilities as they are identified. Ultimately, through these approaches, IT and security leaders will be correct to have confidence in their tools, because they will have done the work on the front end to ensure resilience, stability, and compliance.

Click here to learn more about ThreatModeler, or watch a demo.

ABOUT THREATMODELER

ThreatModeler® is an automated threat modeling solution that fortifies an enterprise's SDLC by identifying, predicting and defining threats, empowering security and DevOps teams to make proactive security decisions. ThreatModeler provides a holistic view of the entire attack surface, enabling enterprises to minimize their overall risk.

ThreatModeler Software, Inc.
101 Hudson Street
Suite 2100
Jersey City, NJ 07302

+1 (201) 266-0510

info@threatmodeler.com