Ponemon INSTITUTE

The State of Software Supply Chain Security Risks

Sponsored by Black Duck

Independently conducted by Ponemon Institute LLC

Publication Date: May 2024

The State of Software Supply Chain Security Risks
Prepared by Ponemon Institute
May 2024

Part 1. Introduction

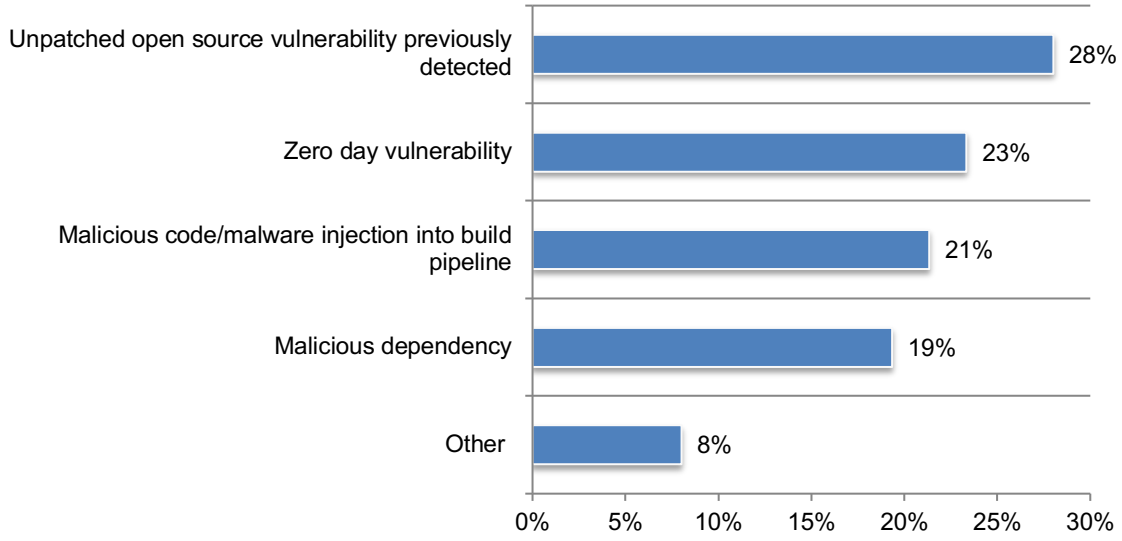
The purpose of this research is to understand how prepared organizations are in reducing software security risks in the supply chain. Sponsored by Black Duck, Ponemon Institute surveyed 1,278 IT and IT security practitioners who are in organizations that are committed to achieving a secure software supply chain and have some level of responsibility for their organizations' software supply chain security strategy. The regions and country in this research are North America (613 respondents), EMEA (362 respondents) and Japan (303 respondents).

According to the National Institute of Standards and Technology (NIST), **a software supply chain attack can be as sophisticated as malware injection or as simple as an opportunistic exploitation of an unpatched vulnerability**. The malicious code then ends up in an organization's system and may allow the hacker to gain access to sensitive data or compromise its code to gain access to customers. This may result in a ransomware attack or other malicious incidents. Typically, attackers find a weak link in the supply chain and use it to move up or across the supply chain to their real targets.

Vulnerabilities are the root cause of attacks against many of the software supply chains in this research. Fifty-nine percent of organizations in this research have been impacted by a software supply chain attack or exploit and 54 percent of these respondents say the attacks happened in the past year.

As shown in Figure 1, 28 percent of respondents say the root cause of the attack or exploit was an unpatched open source vulnerability previously detected and 23 percent of respondents say it was the result of a zero day vulnerability. Fifty percent of these organizations took more than a month to respond to the attack.

Figure 1. What was the root cause of the attack or exploit?



Recommendations to reduce software supply chain risks based on the research findings

Maintain visibility into everything your applications are composed of, especially when it comes from a third party. Other actions include continuously monitoring running applications for threats, compare supplied SBOMs to known malicious packages and malware, conduct a dynamic analysis of a running application and conduct a binary analysis of application dependencies.

Detect, track, and manage open source dependencies in source code, files, containers, and artifacts. Most organizations do not know the extent of their open source dependencies and unmanaged dependencies can be a security vulnerability. Managing dependencies involves understanding and adhering to the licenses associated with each component. Open source libraries can have vulnerabilities that, if not addressed promptly, may expose the entire project to potential threats. Regularly updating and monitoring dependencies can mitigate such risks.

To secure the software supply chain, it is important to continuously monitor to detect new vulnerabilities' risk status and the severity of the risk. Security risks are constantly changing and evolving. Therefore, it is important to continuously monitor to detect new vulnerabilities and the severity of risk.

While AI-generated code has significant benefits, there are security risks that require evaluation and assessment. Such benefits include increased developer productivity and automated decision-making. To ensure the successful adoption of AI, organizations need to have processes to evaluate IP, security risk and code quality. Evaluations should be automated because manual evaluations are insufficient and too labor intensive.

Maintaining a SBOM is a best practice and key to a successful supply chain security program. Import third-party SBOMs and evaluate for component risk. Generate SPDX and CycloneDX SBOMs containing open source, proprietary and commercial dependencies. Customize SBOM fields to align with industry, regulatory or customer requirements. Build SBOMs automatically with CI/CD tool integrations and APIs.

Part 2. Key findings

In this section, we provide a deeper dive into the research findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- How prepared are organizations to secure the software supply chain?
- Securing open source software in the supply chain
- The security of commercial software in the supply chain
- The role of the secure software development life cycle (SSDLC) in securing the software supply chain
- The use of AI in the SDLC and its impact on security in the software supply chain
- The role of Software Bill of Materials (SBOMS) in securing the software supply chain

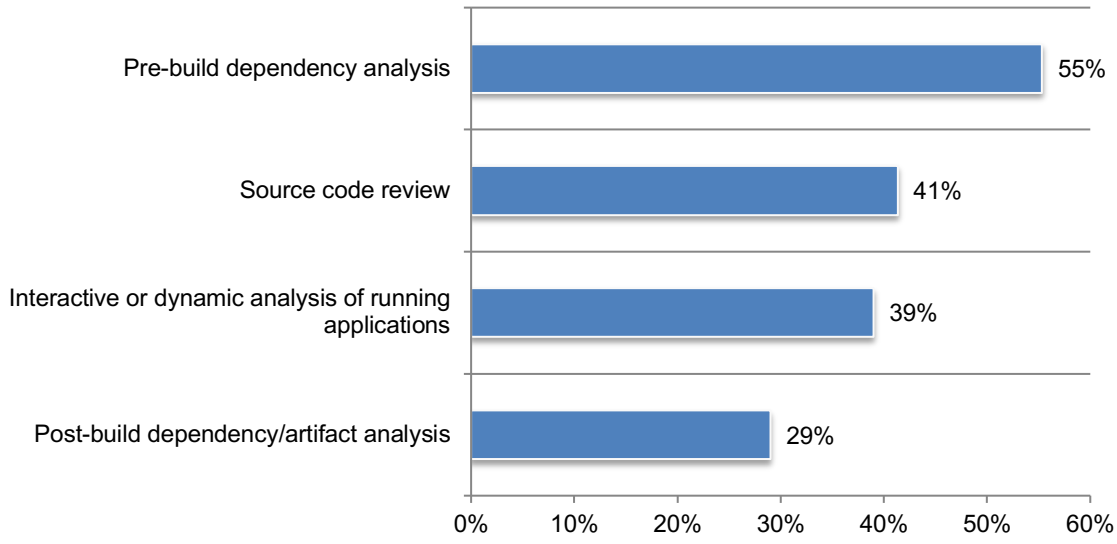
How prepared are organizations to secure the software supply chain?

A lack of commitment by respondents' organizations to reduce the risk of malicious code/malware threatens the security of software supply chains. Only 39 percent of respondents say their senior leadership are very or highly committed to reducing the risk of malicious code/malware in software supply chains. Fifty-three percent of respondents say their organizations evaluate software for malicious packages.

Fifty-five percent of respondents say to prevent malicious packages from impacting the software it builds their organizations analyze pre-build dependency. Other steps taken are reviews of source code (41 percent of respondents) and an interactive or dynamic analysis of running applications analysis (39 percent of respondents), as shown in Figure 2.

Only 45 percent of respondents say their organizations have a process for protecting against malicious open source packages (e.g. those injected via typo-squatting, dependence confusion or brand jacking).

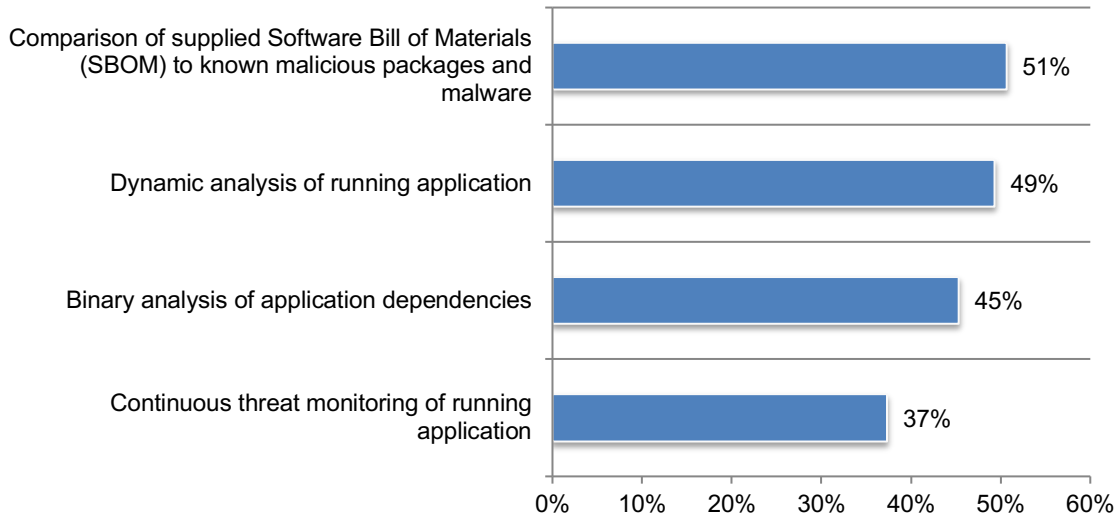
Figure 2. How does your organization evaluate software to prevent malicious packages from impacting the software it builds?
More than one response permitted



Malware planted in a software update was the method used to attack SolarWinds and is evidence that it is critical to evaluate third-party software. Sixty-three percent of respondents say their organizations evaluate third-party software for malware.

As shown in Figure 3, steps taken to evaluate third-party software for malware include comparing supplied SBOMs to known malicious packages and malware (51 percent of respondents) conducting a dynamic analysis of a running application (49 percent of respondents) and conducting a binary analysis of application dependencies (45 percent of respondents). Only 37 percent of respondents are continuously monitoring running applications for threats.

Figure 3. How does your organization evaluate third-party software and artifacts for malware?
More than one response permitted



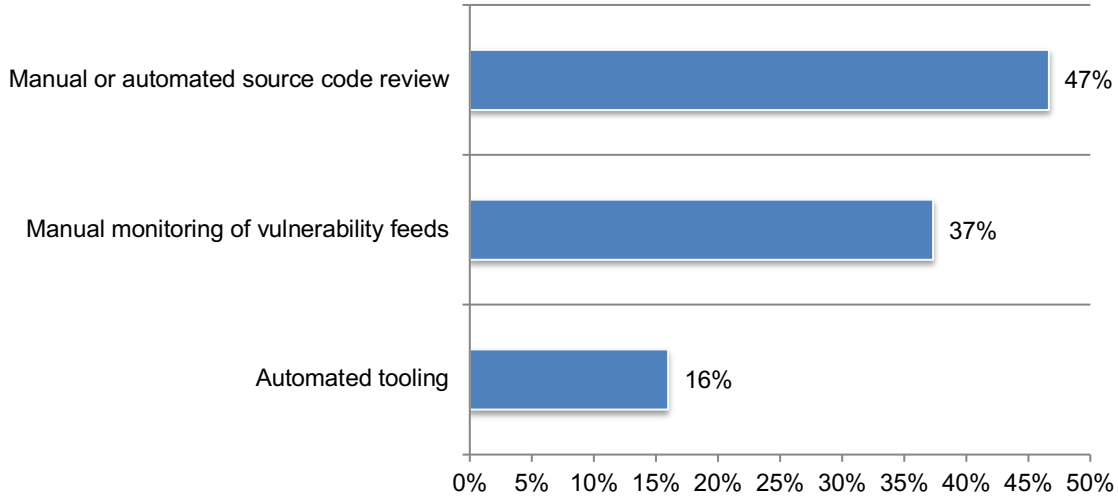
Budgets and other resources are not considered adequate to secure the software supply chain. While 45 percent of respondents say supply chain compromises such as SolarWinds and Kaseya have increased investment in software supply chain security, only 38 percent of respondents say budget and staffing dedicated to securing the supply chain is sufficient or very sufficient.

Organizations represented in this research have an average IT budget for 2024 of $282 million. An average of 25 percent or $70.5 million is allocated to IT security and 19 percent or $13.4 million is allocated to investments in technologies, security personnel and services to secure the supply chain.

Vulnerabilities put software supply chains at risk. Only 38 percent of respondents say their organizations are very or highly effective in detecting and responding to an attack on a software vulnerability. Almost half of respondents (47 percent) say it takes at least a month to more than 6 months to respond to a critical software vulnerability.

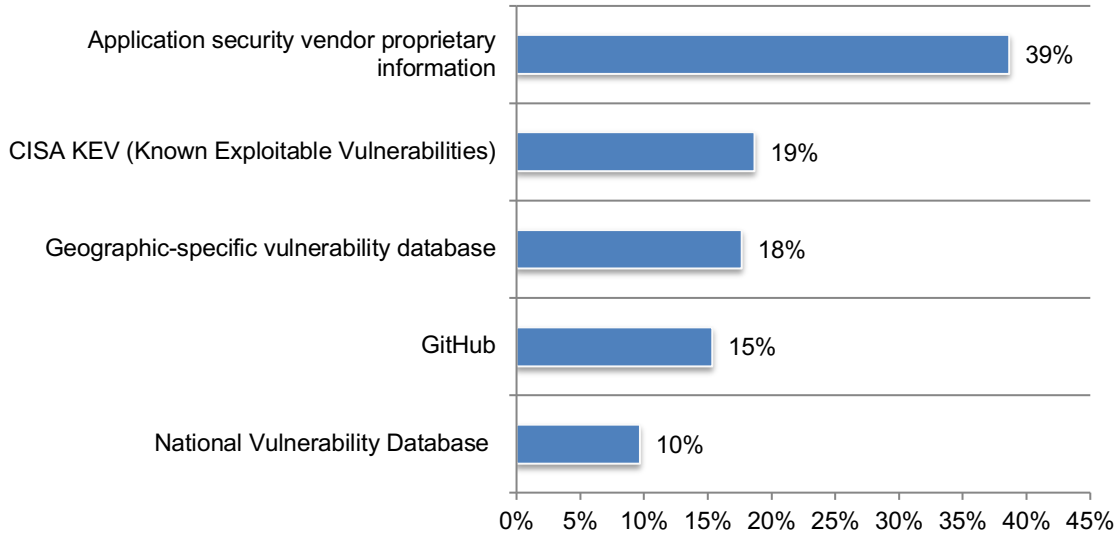
As shown in Figure 4, to monitor for new software vulnerabilities, 47 percent of respondents say their organizations use manual or automated source code review to monitor for new software vulnerabilities. Thirty-seven percent of respondents say they use manual monitoring of vulnerability feeds. Manual tracking is insufficient and labor intensive. Because of staffing shortages, it is important to consider automated tooling.

Figure 4. How does your organization monitor for new software vulnerabilities?



Many organizations are dependent on the application security vendor's proprietary information to identify software vulnerabilities. This may indicate that organizations are not being as proactive or involved as they should be in identifying software vulnerabilities to reduce risk. As shown in Figure 5, 39 percent of respondents say their organizations' source for software vulnerability information is the application security vendor's proprietary information.

Figure 5. What is your organization's source of software vulnerability information?
Only one choice permitted



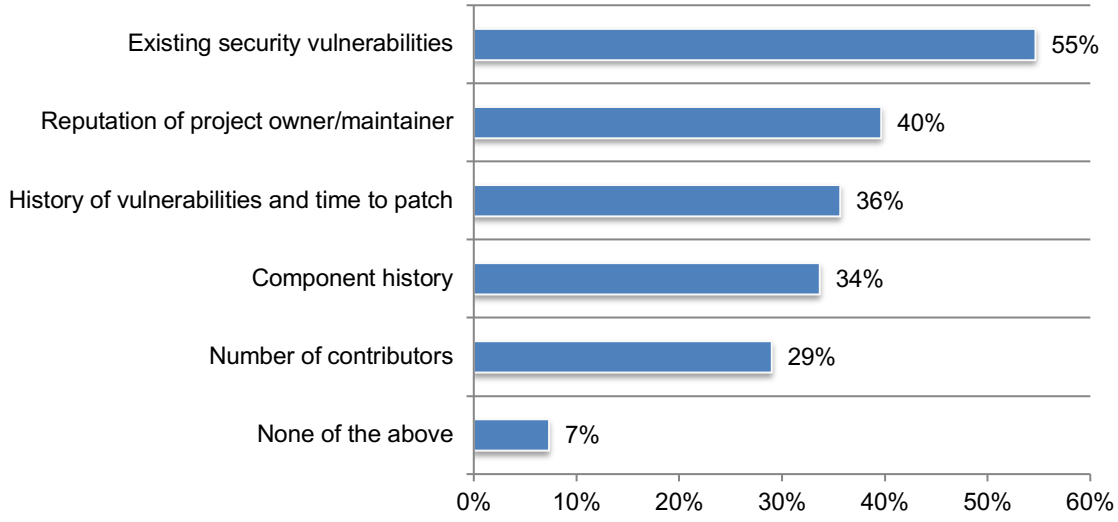
Securing open source software in the supply chain.

Vulnerabilities in open source software are another serious threat to the security of the software supply chain. Sixty-five percent of respondents say their organizations use open source software. However, less than half of these respondents (47 percent) say their organizations are very or highly effective in securing open source software in the supply chain.

The annual "Open Source Security and Risk Analysis" (OSSRA) report, now in its ninth edition, examines vulnerabilities and license conflicts found in over 1,000 codebases across 17 industries. According to the 2024 OSSRA report, 84 percent of codebases examined contained at least one open source vulnerability.

As shown in Figure 6, the three primary factors used to evaluate the security of open source components are existing security vulnerabilities (55 percent of respondents), reputation of project owner/maintainer (40 percent of respondents) and the history of vulnerabilities and time to patch (36 percent of respondents).

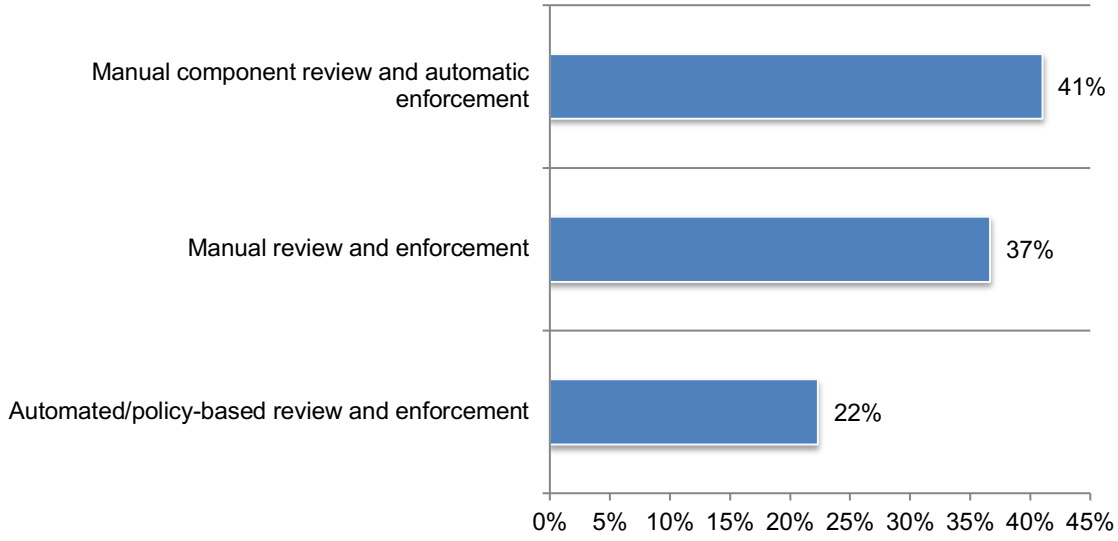
Figure 6. What factors are used to evaluate the security of open source components?
Two responses permitted



Few organizations are using automation to approve or forbid open source dependencies. Open source dependencies are external libraries, frameworks or modules that a software project relies on to function. These components are developed independently by other individuals or groups and are made available for anyone to use, modify and distribute. A benefit of using open source dependencies is that software development can be speeded up. However, their use can also present security risks, especially if the dependencies aren't tracked or known. The use of automation can make tracking and identifying dependencies more efficient and effective.

Only 48 percent of respondents say their organizations have a method for approving or forbidding open source dependencies. To approve or forbid open source dependencies, 41 percent of these respondents say they use manual component review and automatic enforcement followed by manual review and enforcement (37 percent of organizations). Only 22 percent of respondents say the method used is automated/policy-based review and enforcement, as shown in Figure 7.

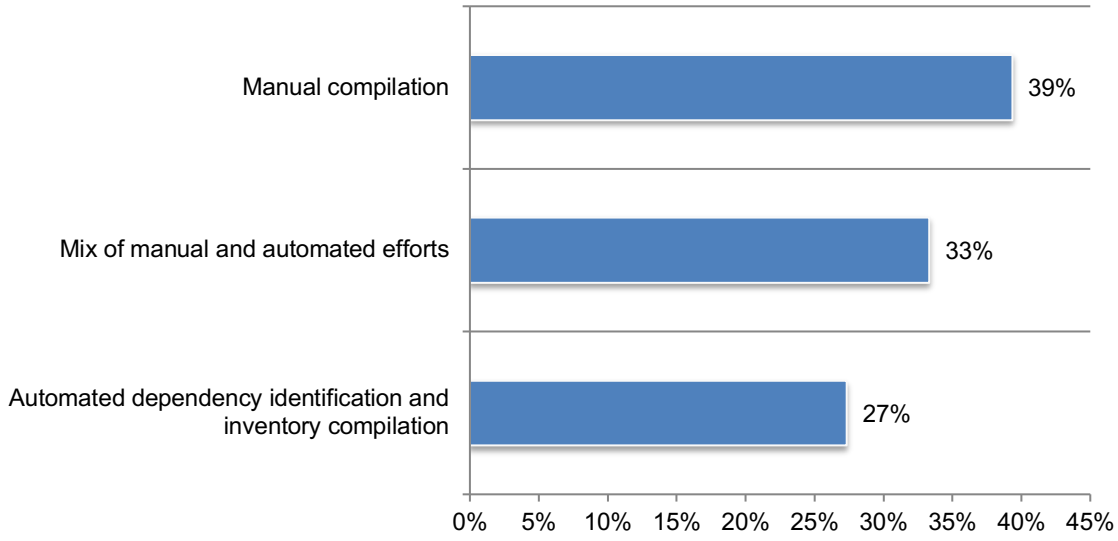
Figure 7. What best describes the method for approving or forbidding open source dependencies?
Only one choice is permitted



Most organizations do not know the extent of their open source dependencies. Unmanaged dependencies can introduce security risk. Open source libraries can have vulnerabilities that, if not addressed promptly, may expose the entire project to potential threats. Regularly updating and monitoring dependencies can mitigate such risks.

As shown in Figure 8, only 39 percent of respondents say their organizations keep an inventory of open source dependencies. To maintain the inventory, 39 percent say their organizations use manual compilation followed by 33 percent of respondents who say they use a mix of manual and automated efforts.

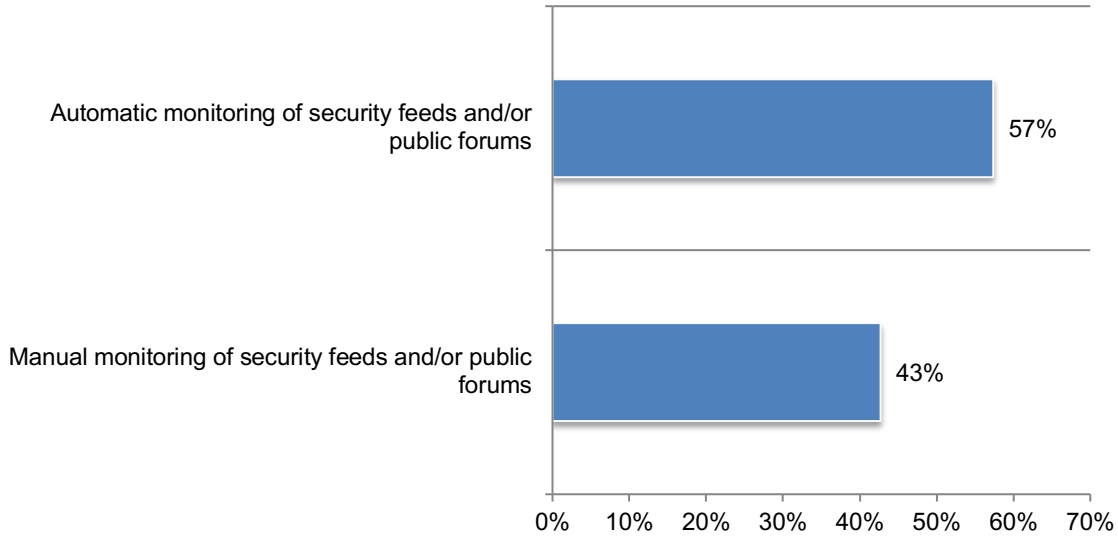
Figure 8. What best describes the process used to maintain this inventory?



To secure the software supply chain, it is important to continuously monitor to detect new vulnerabilities' risk status and the severity of the risk. Security risks are constantly changing and evolving. Therefore, it is important to continuously monitor to detect new vulnerabilities and the severity of risk.

Few organizations (41 percent of respondents) continuously monitor open source dependencies for new vulnerabilities. Of these respondents, 57 percent of respondents say their organizations conduct automatic monitoring of security feeds and/or public forums followed by 43 percent of respondents who say their organizations conduct manual monitoring of security feeds and/or public forums, as shown in Figure 9.

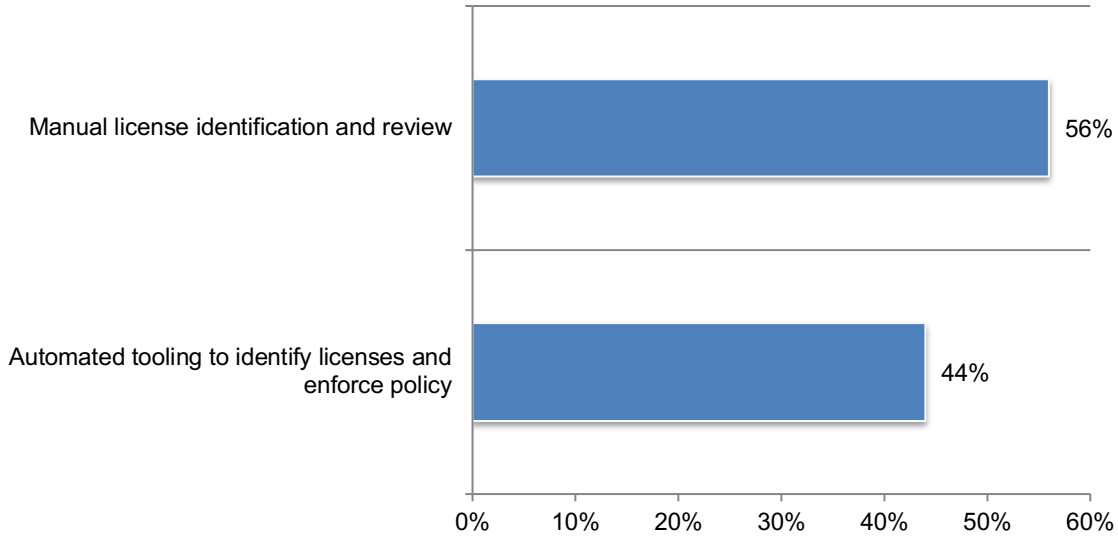
Figure 9. How does your organization continuously monitor open source dependencies for new vulnerabilities?
Only one choice permitted



Managing dependencies involves understanding and adhering to the licenses associated with each component. Only 40 percent of respondents say their organizations track IP/license obligations associated with the dependencies being used. According to the 2024 OSSRA report, 53 percent of open source codebases contained license conflicts.

Figure 10 presents the processes used to track IP/license obligations by the 40 percent of respondents. The primary method used for tracking is manual license identification and review (56 percent of respondents) and automated tooling to identify licenses and enforce policy (44 percent of respondents).

Figure 10. What best describes the processes used to track IP/license obligations?
Only one choice permitted



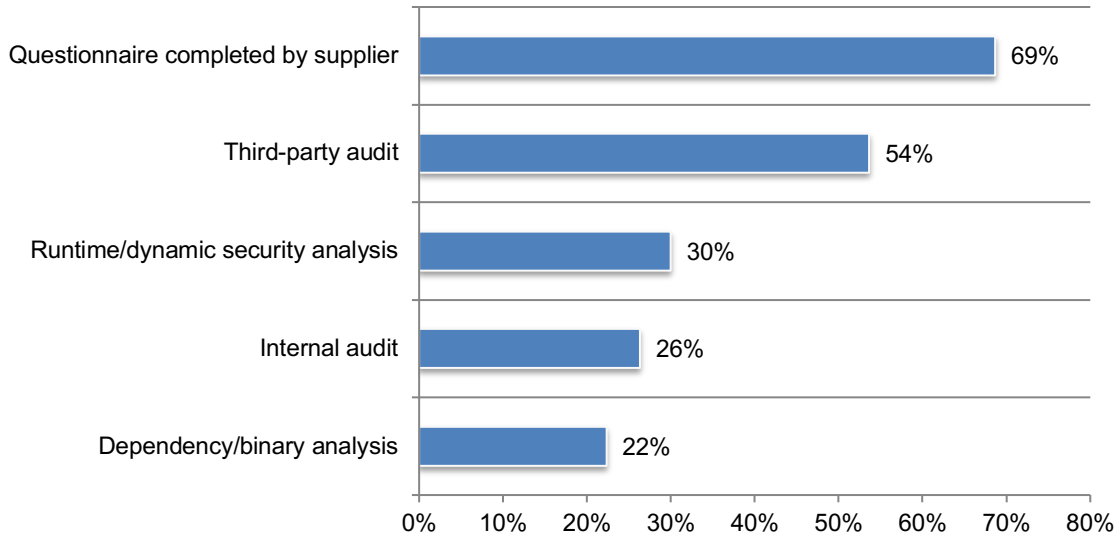
The security of commercial software in the software supply chain

Failure to assess risk in commercial software poses a security threat to the software supply chain. Forty-six percent of respondents say their organizations leverage commercial software. Of these, only 41 percent of respondents say their organizations are very or highly committed to evaluating the security of commercial software.

As shown in Figure 11, only 44 percent of respondents say their organizations conduct a risk assessment for commercial software used or procured. If they do assess risk, 69 percent of respondents rely upon questionnaires supplied by the supplier and 54 percent of respondents say an audit is conducted by a third party.

These reviews of commercial software suppliers occur once during initial contract discussions (29 percent of respondents), during contract renewal (22 percent of respondents) or never (21 percent of respondents).

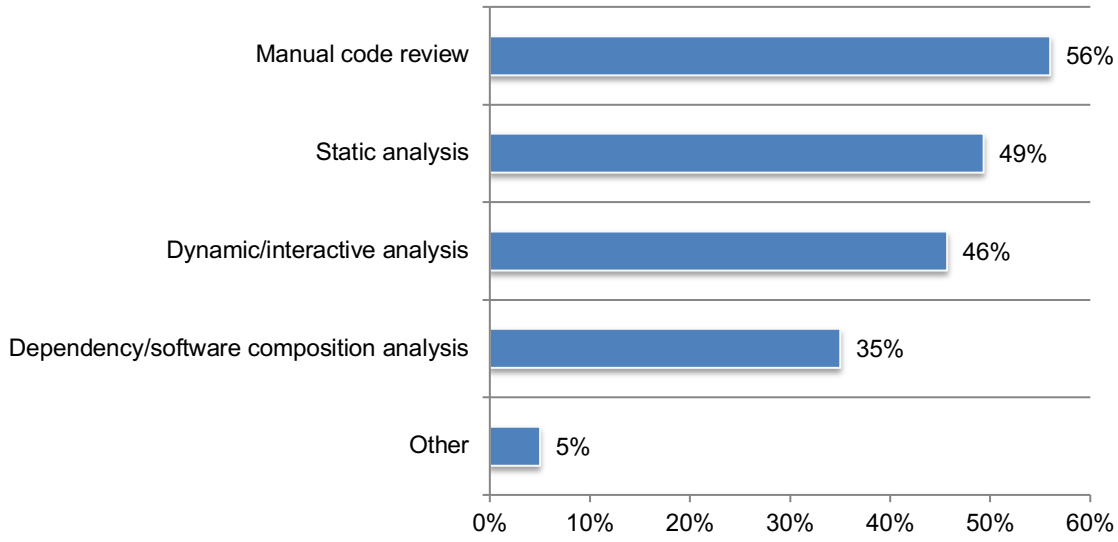
Figure 11. What type of risk assessment of commercial software used or procured?
More than one response permitted



The role of the SSDLC in securing the software supply chain

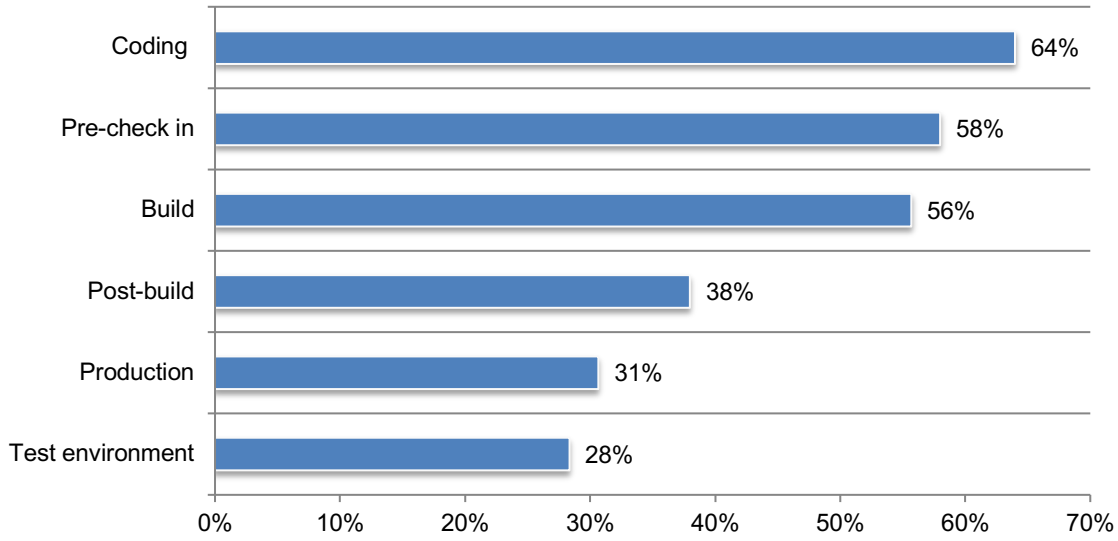
Fifty-four percent of respondents say their organizations review code for security and quality. The Secure Software Development Lifecycle (SSDLC) is the process followed to develop a software product safely and securely. It is a structured way of building software applications with security as a top-of-mind consideration. Figure 12 describes how the 54 percent of respondents review code for security and quality issues. Manual code review (56 percent of respondents) and static analysis (49 percent of respondents) are the methods most often used to review code.

Figure 12. How do your development teams review code for security and quality issues?
More than one response permitted



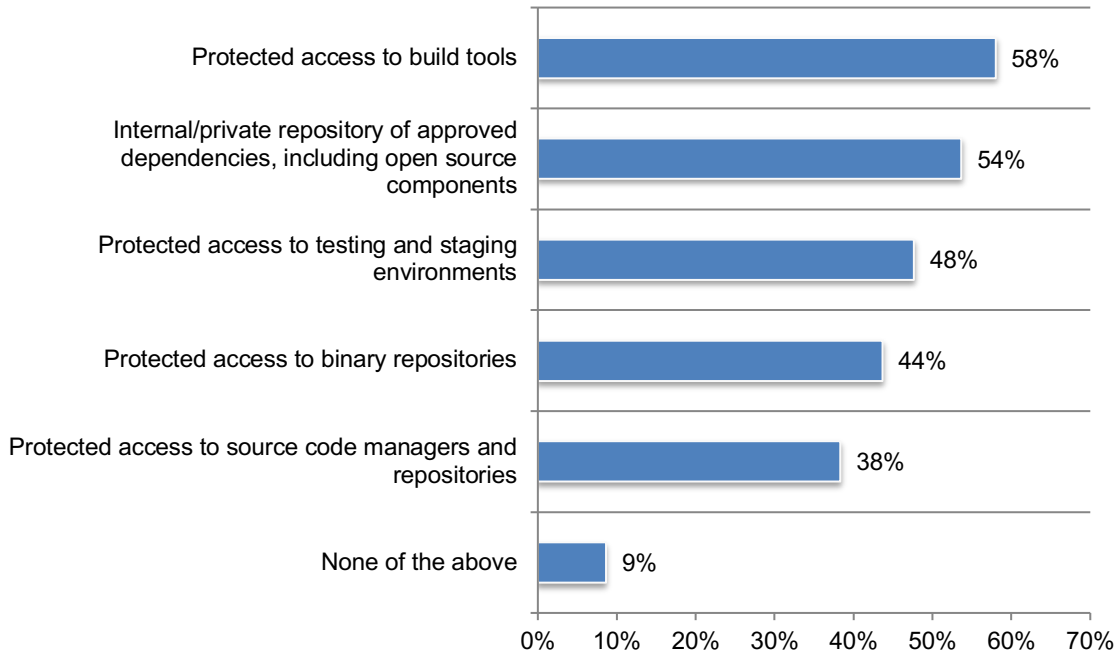
As shown in Figure 13, security analyses by the development teams in the SDLC most often occur in coding (64 percent of respondents), pre-check in (58 percent of respondents) or build (56 percent of respondents).

Figure 13. Where in the SSDLC do development teams perform security analyses?
More than one response permitted



As shown in Figure 14, to protect the integrity of the SSDLC, 58 percent of respondents say they use protected access to build tools, 54 percent of respondents say they have an internal/private repository of approved dependencies, including open source components and 48 percent of respondents say their organizations use protected access to testing and staging environments.

Figure 14. How does your organization protect the integrity of the SSDLC?
More than one response permitted



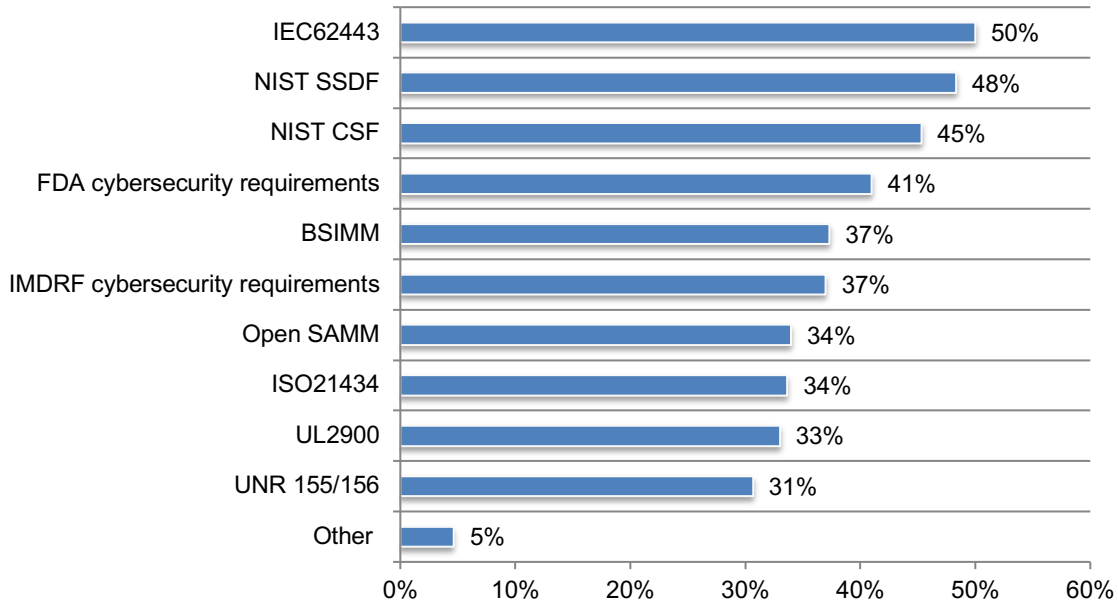
Fifty-seven percent of respondents say their organizations follow a standard model for secure software development, as listed in Figure 15. As an international standard, the International Electrotechnical Commission IEC 62443 family of standards is the result of the standards creation process where 89 national committees involved agree upon a common standard. Fifty percent of respondents say their organizations are following IEC 62443 model.

The NIST Secure Software Development Framework (SSDF) is a set of fundamental, sound, and secure software development practices based on established secure software development practice documents from organizations such as BSA, OWASP and SAFECode.

Following the SSDF practices should help software producers reduce the number of vulnerabilities in released software, reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent recurrences. Also, because the SSDF provides a common language for describing secure software development practices, software producers and acquirers can use it to foster their communications for procurement processes and other management activities. Forty-eight percent of respondents say their organizations follow NIST SSDF.

The NIST Cybersecurity Framework (CSF) provides guidance on how to reduce cybersecurity risks. NIST has expanded the CSF's core guidance and developed related resources to help users get the most out of the framework. These resources are designed to provide different audiences with tailored pathways into the CSF and make the framework easier to put into action. Forty-five percent of respondents say their organizations follow NIST CSF.

Figure 15. Which standard model(s) for secure software development does your organization follow?
More than one response permitted

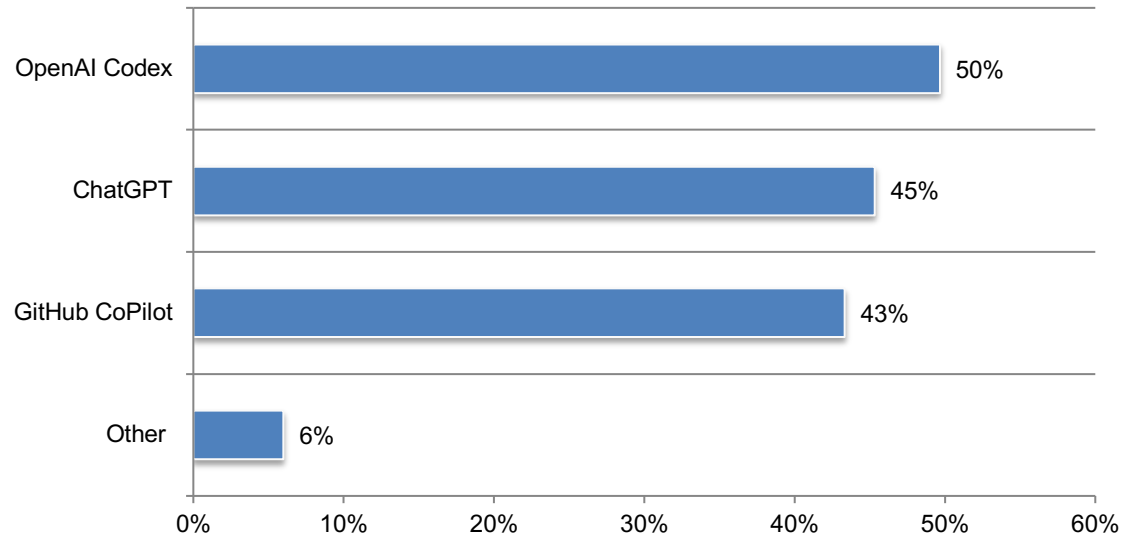


The use of AI in the SDLC and its impact on security in the software supply chain

The use of AI in the SDLC is gaining traction. Fifty-two percent of respondents say their development teams leverage AI tools to generate code. According to Charlotte Freeman, Software Security Advocate for Black Duck, organizations should embrace the transformative potential of AI while safeguarding their intellectual property, ensuring code quality, and navigating ethical considerations. By strategically incorporating AI, organizations can enhance efficiency, automate decision-making, and stay ahead in the ever-evolving field of software development.[1]

Figure 16 lists the AI tools used by development teams to generate code. Of the 52 percent of respondents, 50 percent say their organizations use OpenAI Codex, 45 percent of respondents say they use ChatGPT.

Figure 16. Which AI tools do your development teams use?
More than one response permitted

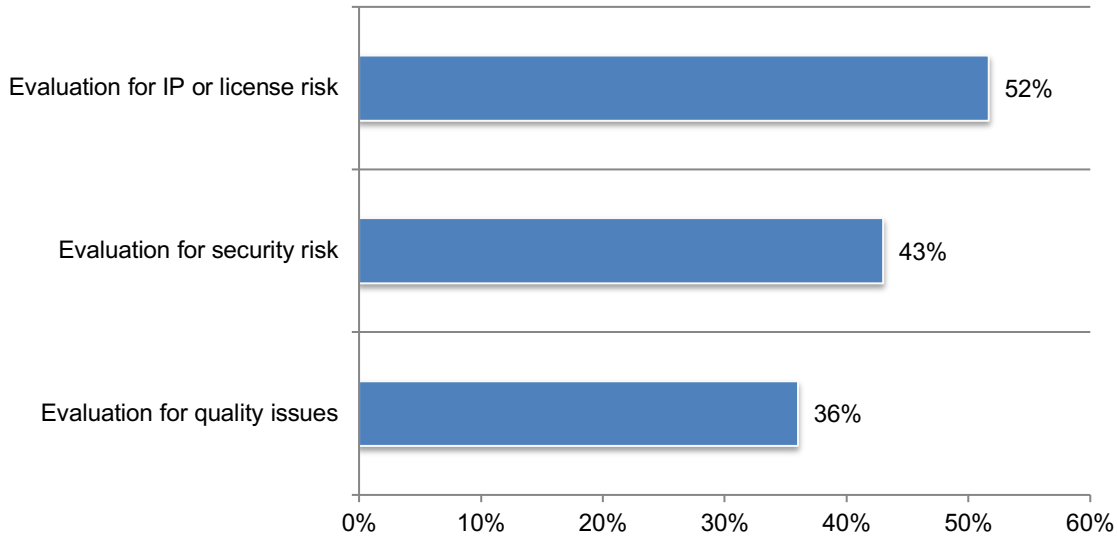


[1] "How AI Is Changing Software's Role in the SDLC", by Charlotte Freeman, Black Duck blog, February 19,2024.

While AI has significant benefits, there are security risks that require evaluation and assessment. To ensure the successful adoption of AI, organizations need to evaluate IP, security risk and code quality. However, only 32 percent of organizations have processes in place to evaluate AI-generated code.

Of these respondents, as shown in Figure 17, the processes most often used are evaluation for IP or license risk (52 percent) and evaluation for security risk (43 percent). Fifty-one percent of respondents say their organizations perform these evaluations with automation and 49 percent of respondents say it is done manually.

Figure 17. What processes are in place to evaluate AI-generated code?
More than one response permitted

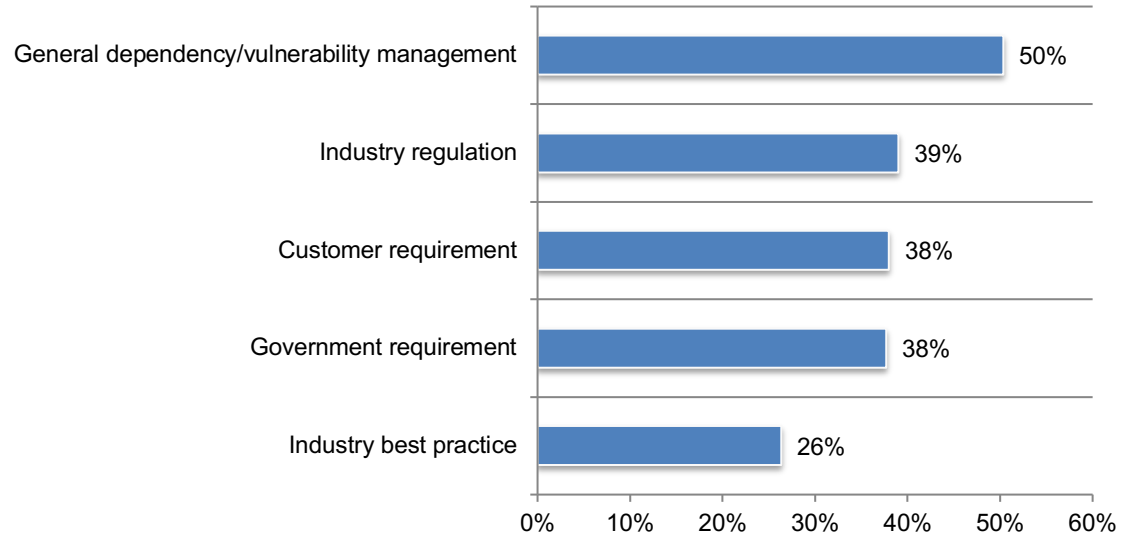


The role of Software Bill of Materials (SBOM) in securing the software supply chain

SBOMs are a best practice and critical to having a secure software supply chain, but only 35 percent of respondents say their organizations produce or generate SBOMs. A SBOM is a nested inventory of list of ingredients that make up software components. As shown in Figure 18, the main reasons for generating SBOMs are general dependency/vulnerability management (50 percent of respondents), industry regulations (39 percent of respondents) and government requirements (38 percent of respondents).

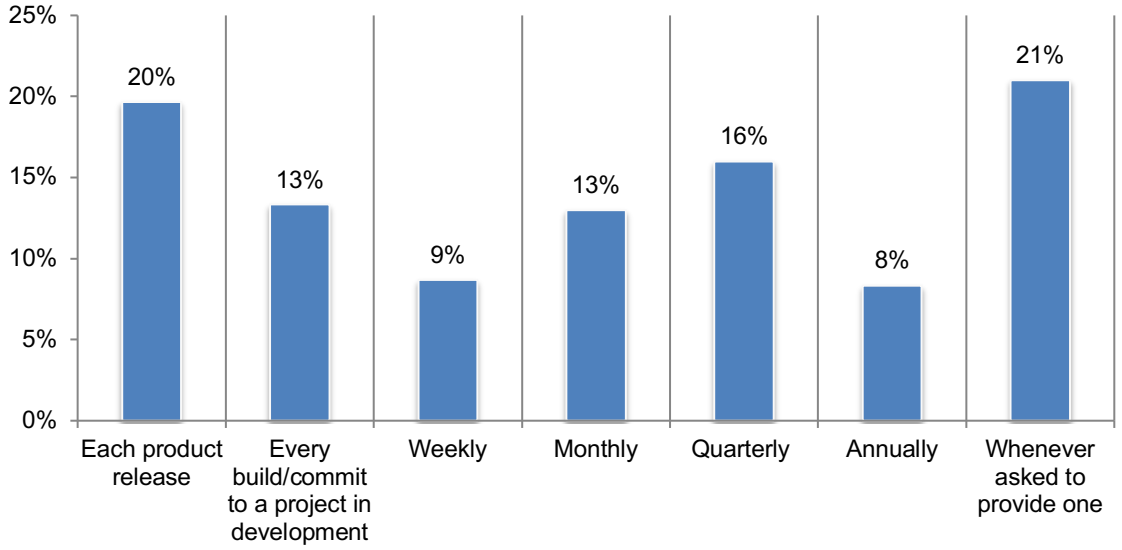
It is critical to track and avoid IP/license conflicts. However, only 26 percent of respondents say their organizations' legal/governance team has a role in verifying the accuracy of SBOMs and their role is primarily to allow distribution (39 percent of respondents) and to define distribution rules (37 percent of respondents).

Figure 18. Why does your organization generate SBOMs
More than one response permitted



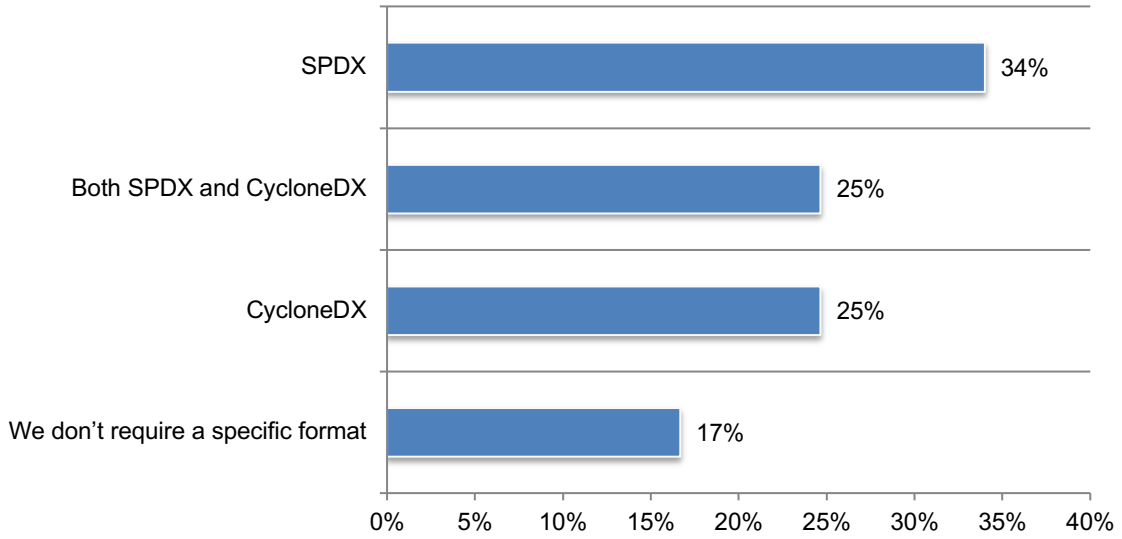
No regular schedule for generating SBOMS can impact the security of the software supply chain. Of the 35 percent of respondents, only 20 percent of respondents say SBOMs are generated at the time of a product release. Only 21 percent of respondents say whenever asked to provide one, as shown in Figure 19.

Figure 19. How often does your organization generate SBOMs?



As shown in Figure 20, the formats most often used to generate SBOMs are SPDX (34 percent of respondents), CycloneDX (25 percent of respondents), both SPDX and Cyclone DX (25 percent of respondents). Seventeen percent of respondents say a specific format is required.

Figure 20. Which format does your organization require for the requested SBOM?

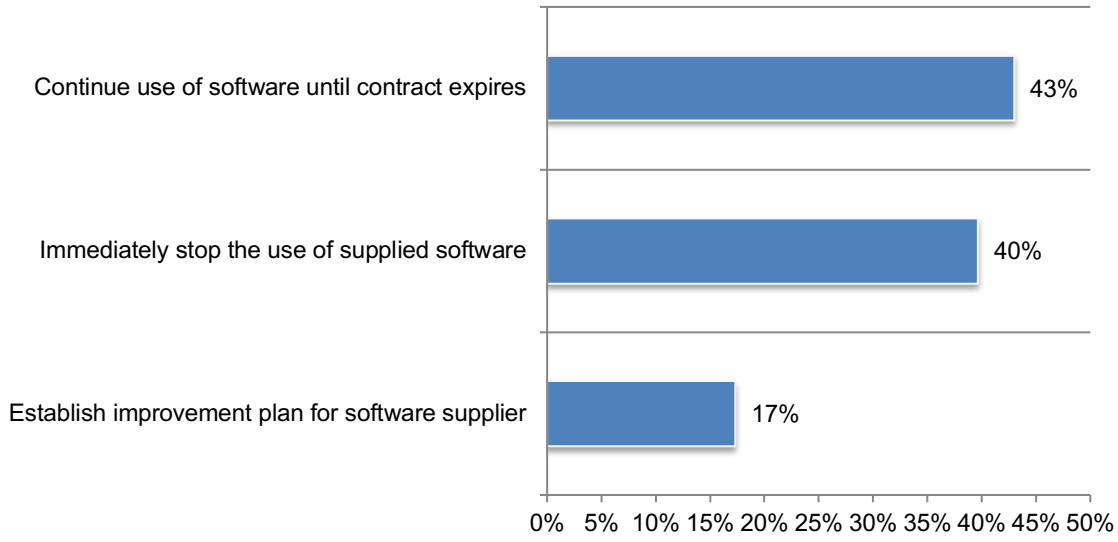


,

Only 40 percent of respondents immediately stop the use of supplied software if the supplier does not provide a requested SBOM. Twenty-nine percent of respondents request SBOMs from suppliers and the format most often required is SPDX (34 percent of respondents), CycloneDX (25 percent of respondents) and both SPDX and CycloneDX (25 percent of respondents). Only 34 percent of respondents say their suppliers include vulnerability disclosures with the SBOMs they provide. Only 40 percent of respondents say their organizations validate SBOMs provided by suppliers.

As shown in Figure 21, if suppliers do not provide a requested SBOM, 43 percent of respondents say their organizations continue the use of software until the contract expires and 40 percent of respondents say they immediately stop the use of supplied software. Only 17 percent of respondents say their organizations establish an improvement plan for software suppliers.

Figure 21. How does your organization handle suppliers who do not provide requested SBOM?



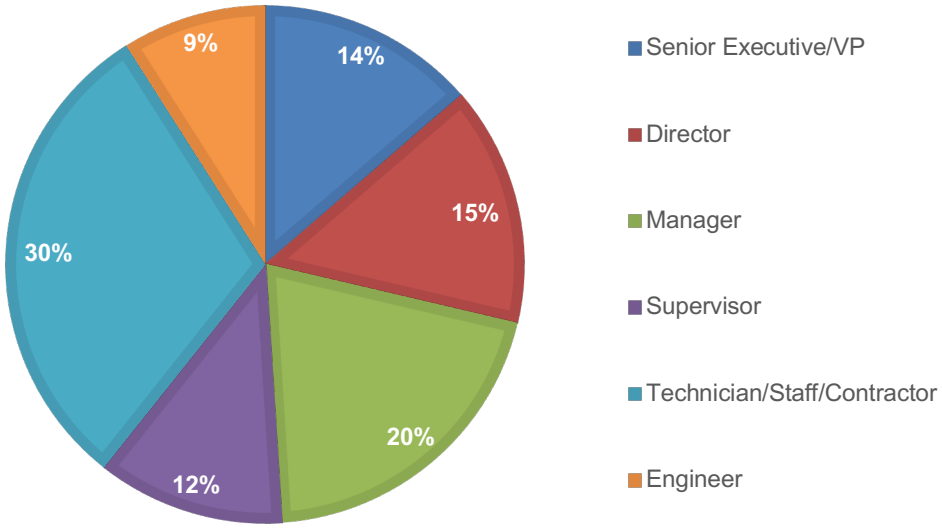
Part 3. Methodology

A sampling frame of 45,710 IT and IT security practitioners who are in organizations that are committed to achieving a secure software supply chain and have some level of responsibility for their organizations' software supply chain security strategy were selected as participants to this survey. Table 1 shows 1,456 total returns. Screening and reliability checks required the removal of 178 surveys. Our final sample consisted of 1,278 surveys or a 3.4 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	37,399	100.0%
Total returns	1,456	3.8%
Rejected or screened surveys	178	0.5%
Final sample	1,278	3.4%

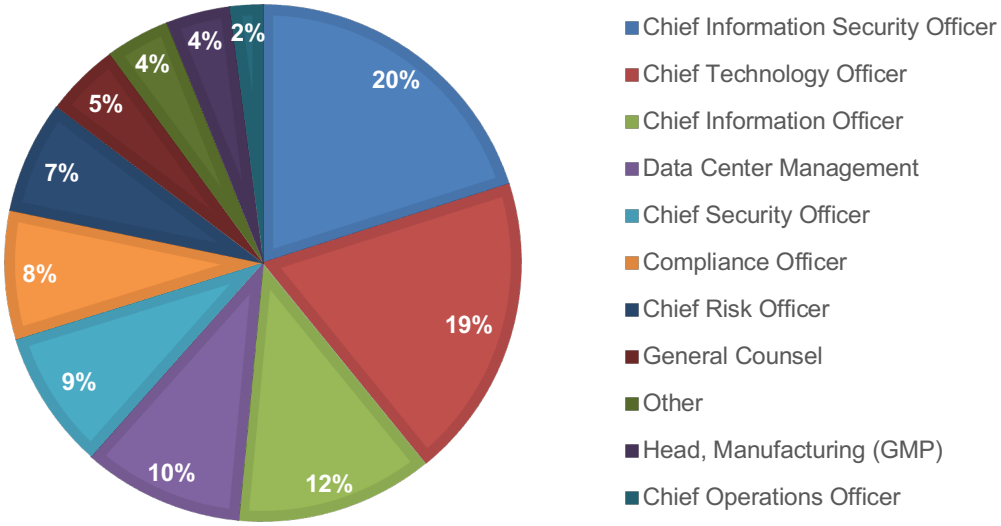
Pie chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (61 percent) of respondents are at or above the supervisory levels. The largest category at 30 percent of respondents is technician/staff/contractor.

Pie chart 1. Current position within the organization



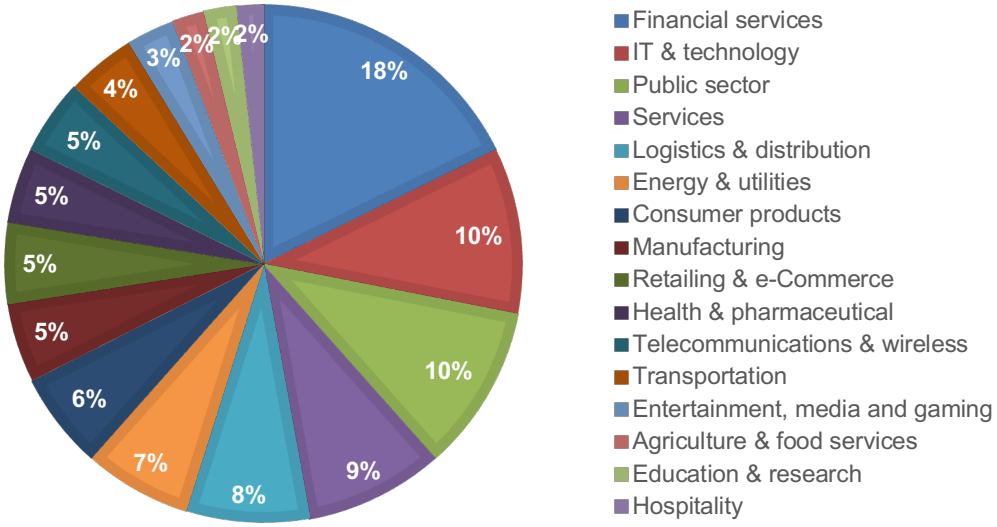
As shown in Pie chart 2, 20 percent of respondents report to the chief information security officer, 19 percent of respondents report to the chief technology officer, 12 percent of respondents report to the chief information officer, and 10 percent of respondents report to data the center management.

Pie chart 2. Direct reporting channel



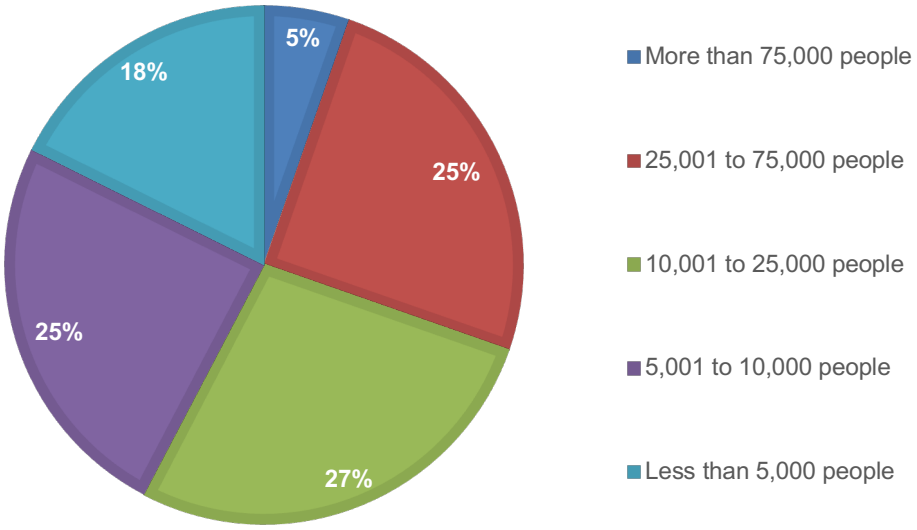
Pie chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by IT and Technology (10 percent of respondents), public sector (10 percent of respondents), services (9 percent of respondents), logistics (8 percent of respondents), and energy and utilities (7 percent of respondents).

Pie chart 3. Primary industry classification



As shown in Pie chart 4, more than half (57 percent) of respondents are from organizations with a headcount of more than 10,000 employees

Pie chart 4. Worldwide headcount



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT and IT Security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to survey questions. All survey responses were captured in February 2024.

Survey response	Consolidated
Total sampling frame	37,399
Total returns	1,456
Rejected surveys	178
Final sample	1,278
Response rate	3.4%

Part 1. Screening

S1. How much responsibility do you have for setting and/or implementing your organization's software supply chain security strategy?	Consolidated
I have complete responsibility for the strategy	40%
I share responsibility with others	60%
I have no responsibility (stop)	0%
Total	100%

S2. How committed is your organization to achieving a secure software supply chain?	Consolidated
Very committed	49%
Committed	33%
Somewhat committed	18%
Not committed (stop)	0%
Total	100%

S3. What best describes your role in your organization? Please select **one choice** only.	Consolidated
Chief Information Security Officer (CISO)	16%
Chief Technology Officer (CTO)	12%
Chief Data Officer (CDO)	8%
Product security analyst	12%
DevSecOps team	11%
Head of the Security Operations Center (SOC)	12%
Security Products Testing	8%
Security Engineering	12%
Reverse engineers/vulnerability researchers	8%
None of the above (stop)	0%
Total	100%

Part 2. Background on security posture

Q1. How sufficient are available resources dedicated to securing the supply chain on a scale from 1 = not sufficient to 10 = very sufficient	Consolidated
1 or 2	12%
3 or 4	20%
5 or 6	30%
7 or 8	21%
9 or 10	17%
Total	100%

Q2. Who is **most responsible** for software supply chain security in your organization? Please select **one choice** only.	Consolidated
Chief Information Security Officer (CISO)	15%
Chief Technology Officer (CTO)	16%
Chief Data Officer (CDO)	9%
Product security analyst	8%
DevSecOps team	8%
Head of the Security Operations Center (SOC)	7%
Security Products Testing	8%
Security Engineering	9%
Reverse engineers/vulnerability researchers	9%
No one person is most responsible	11%
Other (please specify)	1%
Total	100%

Q3. What type of software does your organization build? Please select the **one** most applicable.	Consolidated
Enterprise applications	34%
Web applications	30%
Commercial of-the-shelf software (COTS)	28%
Embedded/firmware	8%
Total	100%

Q4. Approximately, what range best defines your organization's 2024 IT budget?	Consolidated
< $1 million	4%
$1 to 5 million	6%
$6 to $10 million	10%
$11 to $50 million	13%
$51 to $100 million	15%
$101 to $250 million	14%
$251 to $500 million	15%
$501 to $750 million	13%
$751 million to $1 billion	7%
More than $1 billion	3%
Total	100%
Extrapolated value	$ 282

Q5. Approximately, what percentage of the 2024 IT budget will be allocated to IT security?	Consolidated
< 1%	1%
1% to 2%	4%
3% to 5%	7%
6% to 10%	11%
11% to 15%	14%
16% to 20%	17%
21% to 30%	12%
31% to 40%	13%
41% to 50%	12%
More than 50%	10%
Total	100%
Extrapolated value	25%

Q6. Approximately, what percentage of the 2024 IT security budget will be allocated to securing the software supply chain such as investment in technologies, security personnel and services?	Consolidated
< 1%	5%
1% to 2%	7%
3% to 5%	9%
6% to 10%	12%
11% to 15%	15%
16% to 20%	18%
21% to 30%	11%
31% to 40%	11%
41% to 50%	8%
More than 50%	4%
Total	100%
Extrapolated value	19%

Q7. Did supply chain compromises such as the SolarWinds and Kaseya increase your organization's investment in software supply chain security? Please use the 10-point scale below from 1 = no increase to 10 = significant increase.	Consolidated
1 or 2	8%
3 or 4	16%
5 or 6	31%
7 or 8	26%
9 or 10	19%
Total	100%

Q8. Has your organization been impacted by a software supply chain attack or exploit?	Consolidated
Yes	59%
No (please skip to Q12)	24%
Unsure (please skip to Q12)	17%
Total	100%

Q9. When did the attack or exploit occur?	Consolidated
Less than 6 months ago	25%
6 months to 1 year	29%
1 year to 2 years	30%
More than 2 years	16%
Total	100%

Q10. What was the root cause of the attack or exploit? Please select **one** choice only.	Consolidated
Unpatched open source vulnerability previously detected	28%
Zero day vulnerability	23%
Malicious dependency	19%
Malicious code/malware injection into build pipeline	21%
Other (please specify)	8%
Total	100%

Q11. How long did it take to respond to the attack?	Consolidated
Less than 1 day	13%
1 day to 1 week	14%
1 week to 1 month	19%
1 month to 3 months	25%
3 months to 6 months	15%
More than 6 months	10%
Not sure	5%
Total	100%

Part 3. Securing open source software

Q12. Do your development teams use open source software?	Consolidated
Yes	65%
No (please skip to Q20)	31%
Unsure (please skip to Q20)	4%
Total	100%

Q13. How effective is your organization in securing open source software? Please use the 10-point scale below from 1 = not effective to 10 = highly effective.	Consolidated
1 or 2	9%
3 or 4	21%
5 or 6	23%
7 or 8	20%
9 or 10	27%
Total	100%

Q14. What factors are used to evaluate the security of open source components? Please select the top two choices.	Consolidated
Existing security vulnerabilities	55%
History of vulnerabilities and time to patch	36%
Reputation of project owner/maintainer	40%
Number of contributors	29%
Component history	34%
None of the above	7%
Total	200%

Q15a. Does your organization have a method for approving or forbidding open source dependencies?	Consolidated
Yes	48%
No (please skip to Q16a)	38%
Unsure (please skip to Q16a)	13%
Total	100%

Q15b. What best describes the method for approving or forbidding open source dependencies? Please select **one** choice only.	Consolidated
Manual review and enforcement	37%
Manual component review and automatic enforcement	41%
Automated/policy-based review and enforcement	22%
Total	100%

Q16a. Does your organization keep an inventory of open source dependencies?	Consolidated
Yes	39%
No (please skip to Q17a)	42%
Unsure (please skip to Q17a)	19%
Total	100%

Q16b. What best describes the process used to maintain this inventory? Please select **one** choice only.	Consolidated
Manual compilation	39%
Automated dependency identification and inventory compilation	27%
Mix of manual and automated efforts	33%
Total	100%

Q17a. Does your organization continuously monitor open source dependencies for new vulnerabilities?	Consolidated
Yes	41%
No (please skip to Q18a)	49%
Unsure (please skip to Q18a)	9%
Total	100%

Q17b. How does your organization continuously monitor open source dependencies for new vulnerabilities? Please select **one** choice only.	Consolidated
Manual monitoring of security feeds and/or public forums	43%
Automatic monitoring of security feeds and/or public forums	57%
Total	100%

Q18a. Does your organization track IP/license obligations associated with the dependencies being used?	Consolidated
Yes	40%
No (please skip to Q20)	49%
Unsure (please skip to Q20)	11%
Total	100%

Q18b. What best describes the processes used to track IP/license obligations? Please select only **one** choice.	Consolidated
Manual license identification and review	56%
Automated tooling to identify licenses and enforce policy	44%
Total	100%

Q19. Who is primarily responsible for open source license IP/license obligations? Please select only one choice.	Consolidated
Legal	17%
Application security	36%
Development	25%
Product/project management	22%
Total	100%

Part 4. The use and security of commercial software in the supply chain

Q20. Does your organization leverage commercial software?	Consolidated
Yes	46%
No (please skip to Q25)	54%
Total	100%

Q21. How committed is your organization to evaluating the security of commercial software? Please use the 10-point scale below from 1 = not committed to 10 = highly committed.	Consolidated
1 or 2	19%
3 or 4	22%
5 or 6	18%
7 or 8	21%
9 or 10	20%
Total	100%

Q22. Does your organization conduct a risk assessment for commercial software used or procured?	Consolidated
Yes	44%
No (please skip to Q25)	56%
Total	100%

Q23. What type of risk assessment is performed? Please select all that apply.	Consolidated
Questionnaire completed by supplier	69%
Third-party audit	54%
Internal audit	26%
Dependency/binary analysis	22%
Runtime/dynamic security analysis	30%
Total	201%

Q24. How often do you review the security of your organization's commercial software suppliers?	Consolidated
Never	21%
Once, during initial contract discussions	29%
Quarterly	16%
Yearly	12%
During contract renewal	22%
Total	100%

Part 5. Reducing the risk of malicious code/malware

Q25. How committed is your organization in reducing the risk of malicious code/malware? Please use the 10-point scale below from 1 = not committed to 10 = highly committed	Consolidated
1 or 2	21%
3 or 4	22%
5 or 6	17%
7 or 8	21%
9 or 10	18%
Total	100%

Q26a. Does your organization evaluate software for malicious packages?	Consolidated
Yes	53%
No (please skip to Q29a)	47%
Total	100%

Q26b. How does your organization evaluate software to prevent malicious packages from impacting the software it builds? Please select all that apply.	Consolidated
Pre-build dependency analysis	55%
Post-build dependency/artifact analysis	29%
Source code review	41%
Interactive or dynamic analysis of running applications	39%
Total	165%

Q27a. Does your organization evaluate third-party software for malware?	Consolidated
Yes	63%
No (please skip to Q28)	37%
Total	100%

Q27b. How does your organization evaluate third-party software and artifacts for malware? Please select all that apply.	Consolidated
Binary analysis of application dependencies	45%
Dynamic analysis of running application	49%
Comparison of supplied Software Bill of Materials (SBOM) to known malicious packages and malware	51%
Continuous threat monitoring of running application	37%
Total	183%

Q28. Does your organization have a process for protecting against malicious open source packages (e.g. those injected via typo-squatting, dependence confusion brand jacking, etc.)?	Consolidated
Yes	45%
No	45%
Unsure	10%
Total	100%

Part 6. The SDLC and use of AI in securing the software supply chain

Q29a. Does your organization review code for security and quality issues?	Consolidated
Yes	54%
No (please skip to Q30a)	46%
Total	100%

Q29b. How do your development teams review code for security and quality issues? Please select all that apply.	Consolidated
Manual code review	56%
Static analysis	49%
Dependency/software composition analysis	35%
Dynamic/interactive analysis	46%
Other (please specify)	5%
Total	191%

Q30a. Do your development teams perform security analysis in the SDLC?	Consolidated
Yes	44%
No (please skip ro 31)	56%
Total	100%

Q30b. Where in the SDLC do development teams perform security analyses? Please select all that apply.	Consolidated
Coding	64%
Pre-check in	58%
Build	56%
Post-build	38%
Test environment	28%
Production	31%
Total	275%

Q31. How does your organization protect the integrity of the SDLC? Please select all that apply.	Consolidated
Internal/private repository of approved dependencies, including open source components	54%
Protected access to build tools	58%
Protected access to source code managers and repositories	38%
Protected access to binary repositories	44%
Protected access to testing and staging environments	48%
None of the above	9%
Total	250%

Q32a. Does your organization follow a standard model for secure software development?	Consolidated
Yes	57%
No (please skip to Q33a)	43%
Total	100%

Q32b. Which standard model(s) for secure software development does your organization follow? Please select all that apply.	Consolidated
NIST SSDF	48%
IEC62443	50%
BSIMM	37%
Open SAMM	34%
NIST CSF	45%
UL2900	33%
FDA cybersecurity requirements	41%
IMDRF cybersecurity requirements	37%
ISO21434	34%
UNR 155/156	31%
Other (please specify)	5%
Total	395%

Q33a. Do your development teams leverage AI tools to generate code?	Consolidated
Yes	52%
No (please skip to Q37)	48%
Total	100%

Q33b. Which AI tools do your development teams use? Please select all that apply.	Consolidated
GitHub CoPilot	43%
ChatGPT	45%
OpenAI Codex	50%
Other (please specify)	6%
Total	144%

Q34. Does your organization have processes in place to evaluate AI-generated code?	Consolidated
Yes	32%
No (please skip to Q37)	68%
Total	100%

Q35. What processes are in place to evaluate AI-generated code? Please select all that apply.	Consolidated
Evaluation for IP or license risk	52%
Evaluation for security risk	43%
Evaluation for quality issues	36%
Total	131%

Q36. How does your organization perform these evaluations? Please select **one** choice only.	Consolidated
Manually	49%
Automated/with tools	51%
Total	100%

Part 7. Reducing the risk of software vulnerabilities

Q37. How does your organization monitor for new software vulnerabilities? Please select only **one** choice.	Consolidated
Manual monitoring of vulnerability feeds	37%
Manual or automated source code review	47%
Automated tooling	16%
Total	100%

Q38. What is your primary source of software vulnerability information? Please select only **one** choice.	Consolidated
National Vulnerability Database (NVD)	10%
Geographic-specific vulnerability database	18%
GitHub	15%
CISA KEV (Known Exploitable Vulnerabilities)	19%
Application security vendor proprietary information	39%
Other (please specify)	0%
Total	100%

Q39. How effective is your organization in detecting and responding to an attack on a software vulnerability? Please use the 10-point scale below from 1 = not effective to 10 = highly effective.	Consolidated
1 or 2	20%
3 or 4	22%
5 or 6	19%
7 or 8	21%
9 or 10	17%
Total	100%

Q40. How long does it take your organization to respond to a critical software vulnerability?	Consolidated
Less than 1 day	14%
1 day to 1 week	13%
1 week to 1 month	21%
1 month to 3 months	22%
3 months to 6 months	15%
More than 6 months	10%
Not sure	5%
Total	100%

Part 8. The production and generation of Software Bill of Materials (SBOM)

Q41. Does your organization produce or generate SBOMs?	Consolidated
Yes	35%
No (please skip to Part 9)	56%
Unsure (please skip to Part 9)	9%
Total	100%

Q42a. Does your organization's legal/governance team have a role in verifying the accuracy of SBOMs?	Consolidated
Yes	26%
No (please skip to Q43)	74%
Total	100%

Q42b. What role does the legal/governance team have in verifying the accuracy of SBOMs? Please select all that apply.	Consolidated
Allow distribution	39%
Define distribution rules	37%
Establish publication guidelines	32%
Define information inclusion guidelines	28%
Other (please specify)	7%
Total	143%

Q43a. Does your organization request SBOMs from suppliers?	Consolidated
Yes	29%
No (please skip to Q48)	43%
We don't have software suppliers (please skip to Q48)	28%
Total	100%

Q43b. Which format does your organization require for the requested SBOM? Please select one choice only.	Consolidated
SPDX	34%
CycloneDX	25%
Both SPDX and CycloneDX	25%
We don't require a specific format	17%
Total	100%

Q44. How does your organization handle suppliers who do not provide requested SBOM? Please select **one** choice only.	Consolidated
Immediately stop the use of supplied software	40%
Continue use of software until contract expires	43%
Establish improvement plan for software supplier	17%
Total	100%

Q45. Does your organization validate SBOMs provided by suppliers?	Consolidated
Yes	40%
No	60%
Total	100%

Q46. What does your organization import SBOMs into? Please select all that apply.	Consolidated
ITSM	49%
SEIM	45%
SOAR	48%
Package manager	26%
Application security tools	27%
Total	195%

Q47. Does your supplier include vulnerability disclosures with the SBOMs they provide?	Consolidated
Yes	34%
No	66%
Total	100%

Q48. Which format does your organization use to generate a SBOM? Please select **one** choice only.	Consolidated
SPDX	31%
CycloneDX	42%
Both SPDX and CycloneDX	27%
Total	100%

Q49. Why does your organization generate SBOMs? Please select all that apply.	Consolidated
General dependency/vulnerability management	50%
Government requirement	38%
Industry regulation	39%
Industry best practice	26%
Customer requirement	38%
Total	191%

Q50. How does your organization generate SBOMs? Please select all that apply.	Consolidated
Manual process	47%
Free/open source tooling	44%
SCA tool	37%
Third party	31%
Other (please specify)	7%
Total	166%

Q51. How often does your organization generate SBOMs Please select one choice only.	Consolidated
Each product release	20%
Every build/commit to a project in development	13%
Weekly	9%
Monthly	13%
Quarterly	16%
Annually	8%
Whenever asked to provide one	21%
Total	100%

Part 9. Organization and respondents' demographics

D1. What organizational level best describes your current position?	Consolidated
Senior Executive/VP	14%
Director	15%
Manager	20%
Supervisor	12%
Technician/Staff/Contractor	30%
Engineer	9%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	Consolidated
Chief Financial Officer	1%
Chief Operations Officer	2%
General Counsel	5%
Head, Manufacturing (GMP)	4%
Head, Product Engineering	1%
Head, Quality Assurances	1%
Chief Information Officer	12%
Chief Technology Officer	19%
Chief Information Security Officer	20%
Chief Security Officer	9%
Compliance Officer	8%
Data Center Management	10%
Chief Risk Officer	7%
Other	1%
Total	100%

D3. What best describes your organization's primary industry classification?	Consolidated
Aerospace & defense	0%
Agriculture & food services	2%
Consumer products	6%
Education & research	2%
Energy & utilities	7%
Entertainment, media and gaming	3%
Financial services	18%
Health & pharmaceutical	5%
Hospitality	2%
IT & technology	10%
Logistics & distribution	8%
Manufacturing	5%
Public sector	10%
Retailing & e-Commerce	5%
Services	9%
Telecommunications & wireless	5%
Transportation	4%
Other (please specify)	0%
Total	100%

D4. What is the worldwide headcount of your organization?	Consolidated
Less than 5,000 people	18%
5,001 to 10,000 people	25%
10,001 to 25,000 people	27%
25,001 to 75,000 people	25%
More than 75,000 people	5%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.