Ponemon INSTITUTE

State of Enterprise Linux Security Management

Sponsored by TuxCare

Independently conducted by Ponemon Institute LLC

Publication Date: March 2022

Ponemon INSTITUTE

State of Enterprise Linux Security Management

Ponemon Institute, March 2022

Part 1. Executive Summary

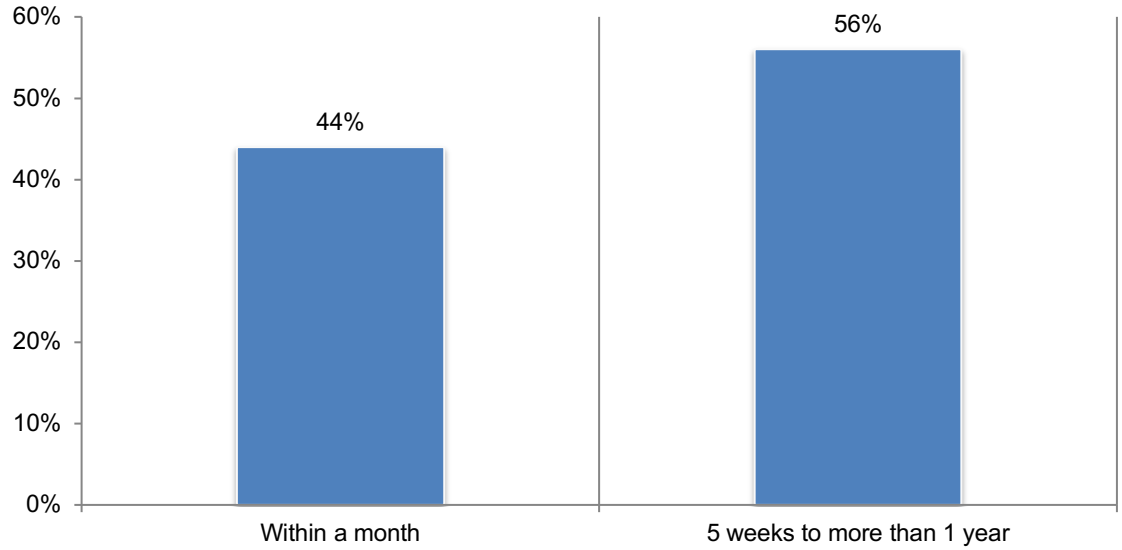
The purpose of this study is to understand how organizations are managing security and stability in the Linux suite of products. According to the research, organizations are spending an average of $3.5 million annually monitoring systems for threats and vulnerabilities, patching, documenting and/or reporting on the patch management process. It also includes the downtime hours due to patching of vulnerabilities. Despite the cost and time, most participants in this research are not confident in their ability to detect vulnerabilities, prevent threats and patch vulnerabilities in a timely manner.

Linux is an open-source operating system that sits underneath the software on a computer, receiving requests from programs and relaying these requests to the computer's hardware. The code used to create Linux is free and available to the public to view, edit and for users with the appropriate skills to contribute to.

Sponsored by TuxCare, Ponemon Institute surveyed 564 IT and IT security practitioners in 16 different industries in the United States (the complete list of industries is shown in the Appendix of this report. Organizations represented in this research have an average of 31 personnel in the security function. The study was fielded in September 2021

Patching is not done on a timely basis. Once a critical or high priority vulnerability is detected, on average only 29 percent of respondents say their organizations can patch it within 2 weeks. As shown in Figure 1, 44 percent of respondents say it takes a month and 56 percent of respondents say it can take an average of 5 weeks to more than 1 year.

Figure 1. Once you detect a critical or high priority vulnerability, how long on average does it take to patch?



The following findings illustrate the current state of enterprise Linux security management.

- **Organizations are at risk because vulnerabilities take more than a month to more than a year to patch, according to 56 percent of respondents.** According to 54 percent of respondents, this time to patch has significantly increased (19 percent) or increased (39 percent) in the past two years. As a result, most respondents are not confident in their organizations' ability to detect vulnerabilities or prevent threats and patch vulnerabilities in a timely manner.

- **On average, organizations are spending 1,075 hours each week to monitor and patch vulnerabilities.** The most time spent each week is patching applications and systems (340 hours) and the time caused by downtime due to patching vulnerabilities (340 hours). Monitoring systems for threats and vulnerabilities take 280 hours each week and documenting and/or reporting on the patch management process takes 115 hours each week. For context, these figures relate to, approximately, an IT team size with 30 people and a workforce of 12,000, on average, across respondents.

- **Ransomware attacks are becoming more lucrative for hackers.** More than half of respondents (51 percent) say in the past 12 months their organizations had at least one ransomware attack.

- **Steps taken to prioritize vulnerabilities are not effective.** Fifty-three percent of respondents say it is difficult to prioritize which vulnerabilities need to be patched first. Currently, vulnerabilities are prioritized based on vulnerability factors such as exploit availability (53 percent of respondents), type of system impacted (51 percent of respondents), business risk of systems affected by the vulnerability (47 percent of respondents) and CVSS (46 percent of respondents).

- **Organizations believe virtualization and database live patching are very important to improving the patching process.** Seventy-two percent of respondents say virtualization stack live patching and database live patching are very important. Sixty-nine percent of respondents say integrating live patching services with existing management and monitoring systems already used are important. Sixty percent of respondents say their organizations are very effective at live patching services in supporting productivity, security and compliance.

Part 2. Detailed learnings

In this section, we provide an analysis of the research findings. The complete findings are presented in the Appendix of this report. We have organized the report according to the following themes:

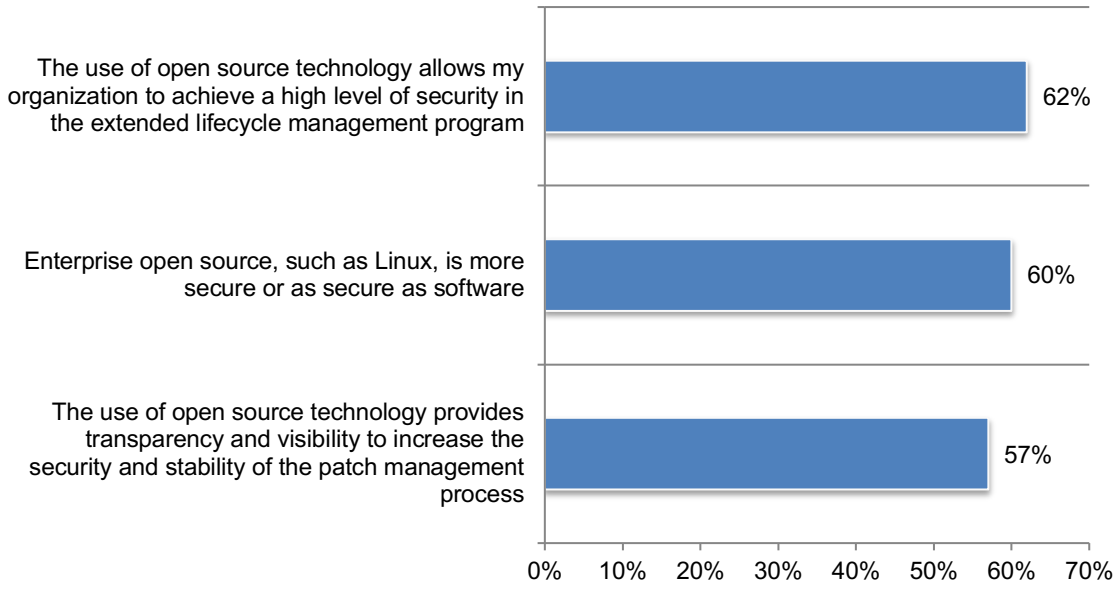
- State of Linux at the enterprise level
- Cyberattacks and vulnerability management
- Solutions to improving the patching of vulnerabilities: live patching and automation
- The cost and time spent monitoring and patching vulnerabilities
- Organizational leadership is needed to improve patching
- Enterprise roadblocks to vulnerability management

State of Linux at the enterprise level

It is well established that Linux offers security, transparency and visibility to organizations. As shown in Figure 2, an important benefit of Linux is that the use of open-source technology allows organizations to achieve a high level of security in the extended lifecycle management program (62 percent of respondents).

Enterprise open-source is also considered more or as secure as proprietary software (60 percent of respondents). Further, the use of open-source technology provides transparency and visibility to increase the security and stability of the patch management process (57 percent of respondents) and as a result improves the ability to patch vulnerabilities in a timely manner.

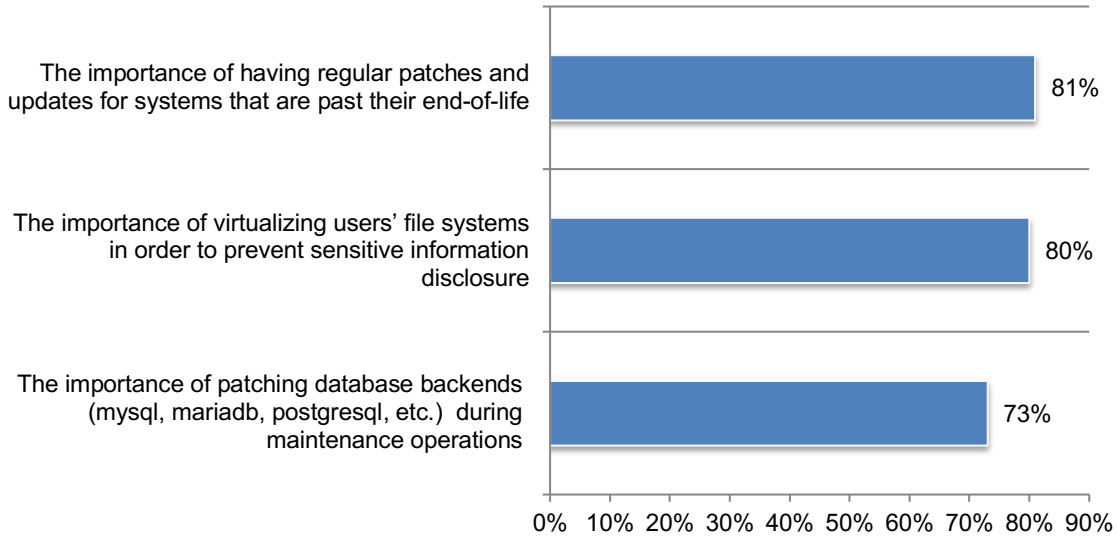
Figure 2. Perceptions about the security and business benefits of Linux
Strongly Agree and Agree responses combined



The use of open-source technology enables a high level of security in the extended lifecycle management program. Respondents were asked to rate the importance of patching and virtualization on a scale of 1 = low importance to 10 = high importance.

Figure 3 represents only the high importance responses (7+ responses), 81 percent of respondents say it is important to have regular patches and updates for systems that are past their end-of-life. Also important is virtualizing users' file systems to prevent sensitive information disclosure (80 percent of respondents) and patching database backends during maintenance operations (73 percent of respondents).

Figure 3. The importance of regular patching, virtualizing users' file systems and patching database backends during maintenance operations
On a scale from 1 = low importance to 10 = high importance, 7+ responses presented

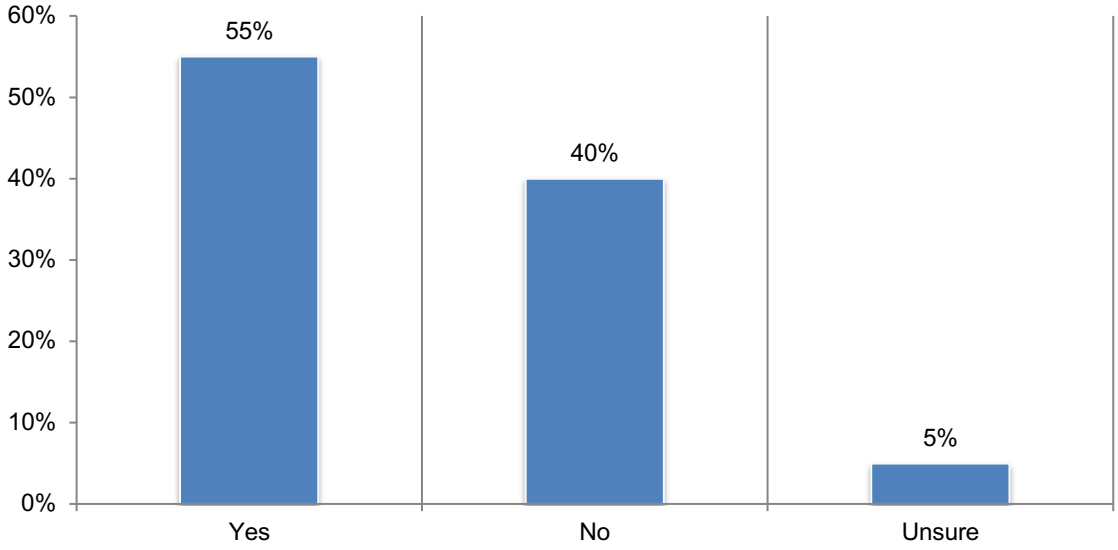


Cyberattacks and vulnerability management

Cybersecurity incidents are occurring because a patch was available for a known vulnerability but not applied. In the past two years, 65 percent of respondents say their organizations had a cybersecurity incident primarily caused by human error (50 percent of respondents) or a criminal external attack to disrupt and affect system availability (47 percent of respondents).

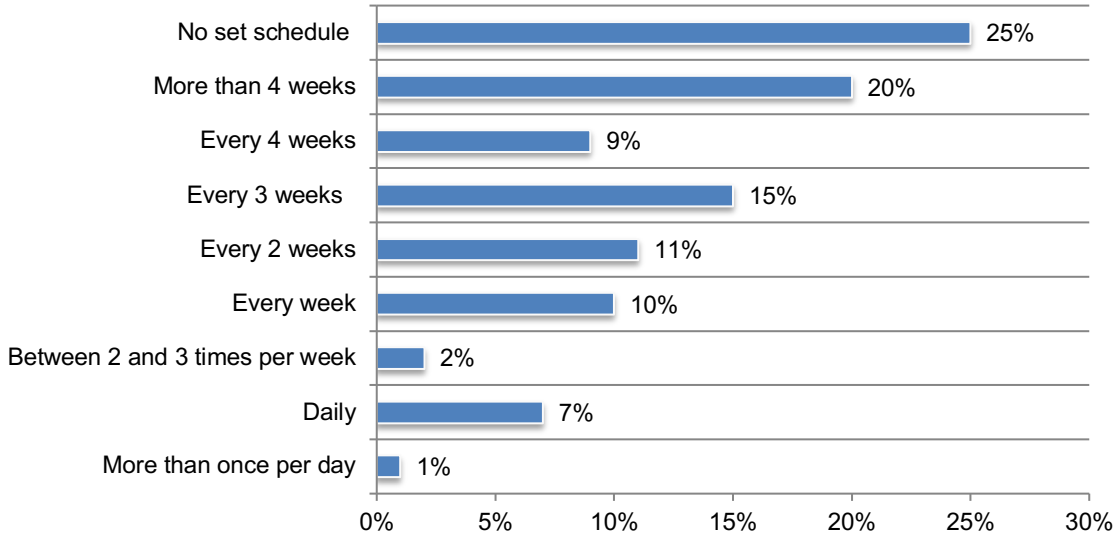
According to Figure 4, 55 percent of these respondents say these incidents occurred while a patch was available for a known vulnerability but was not applied. Forty-three percent of these respondents say their organizations were aware of this vulnerability prior to the cybersecurity incident.

Figure 4. Did any of these cybersecurity incidents occur while a patch was available for a known vulnerability but was not applied?



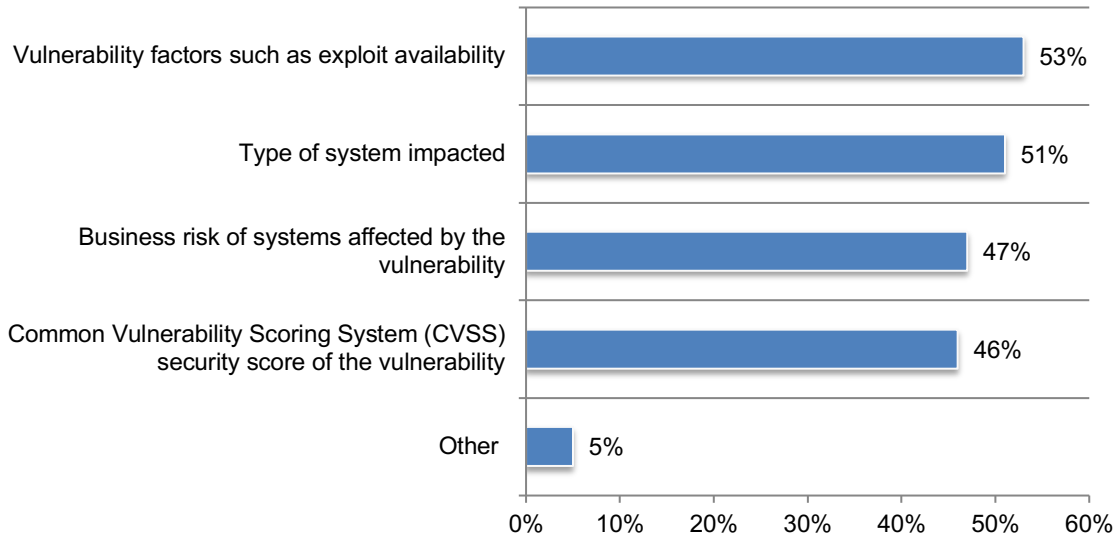
Scanning for vulnerabilities is infrequent and possibly due to the time involved in scanning. Specifically, security experts need to review the results, complete remediation and follow-up to ensure risks are addressed. As shown in Figure 5, 25 percent of respondents say there is no set schedule for scanning and another 20 percent of respondents say it takes more than 4 weeks.

Figure 5. How often does your organization scan for vulnerabilities?



Steps taken to prioritize vulnerabilities are not effective. The findings reveal that 53 percent of respondents say it is difficult to prioritize what needs to be patched first. According to Figure 6, vulnerabilities are prioritized based on vulnerability factors such as exploit availability (53 percent of respondents), type of system impacted (51 percent of respondents), business risk systems affected by the vulnerability (47 percent of respondents) and CVSS (46 percent of respondents).

Figure 6. How do you prioritize vulnerabilities?
More than one response permitted

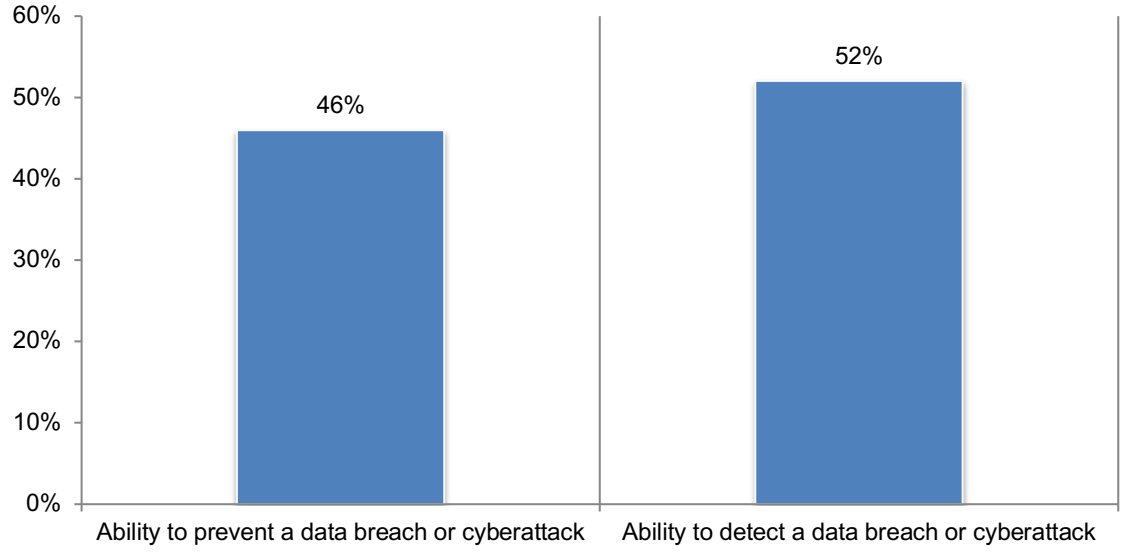


Effective vulnerability management is critical because of the difficulty in preventing future cyberattacks. Only 49 percent of respondents say their organizations have the expertise to prevent, detect and respond to cybersecurity incidents targeting it.

Respondents were asked to rate their organizations' ability to prevent and detect a data breach or cyberattack on a scale of 1 = low ability to 10 = high ability. Figure 6 presents the high ability responses (7+ on the 10-point scale).

As shown, less than half (46 percent) of respondents have a high-level of ability to prevent such attacks and slightly more than half (52 percent) of respondents say their organizations have a high ability to detect these attacks.

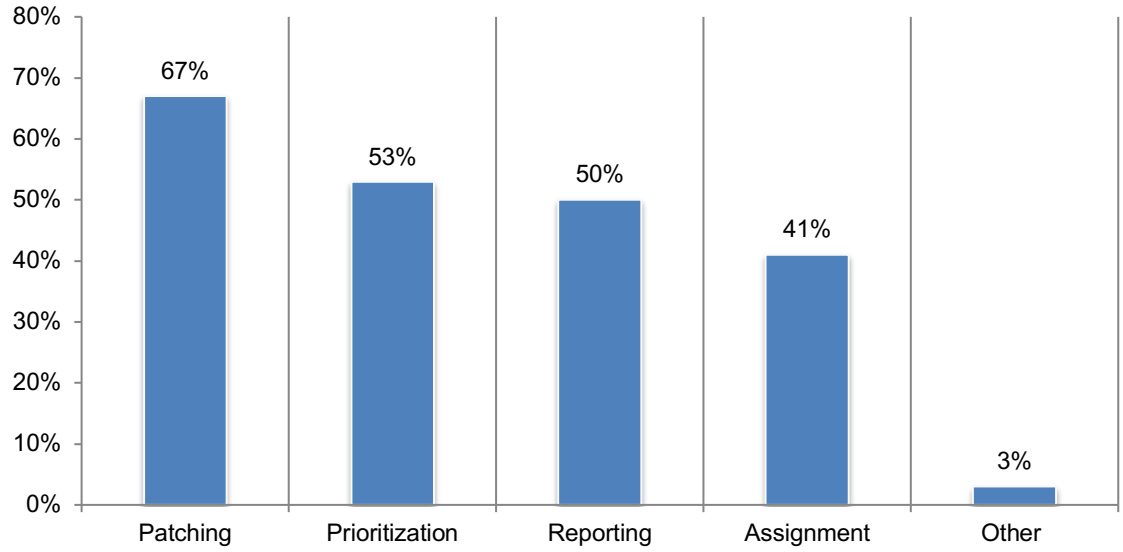
Figure 7. The ability to prevent and detect a data breach or cyberattack
On a scale from 1 = low ability to 10 = high ability, 7+ responses presented



Solutions to improving the patching of vulnerabilities: live patching and automation

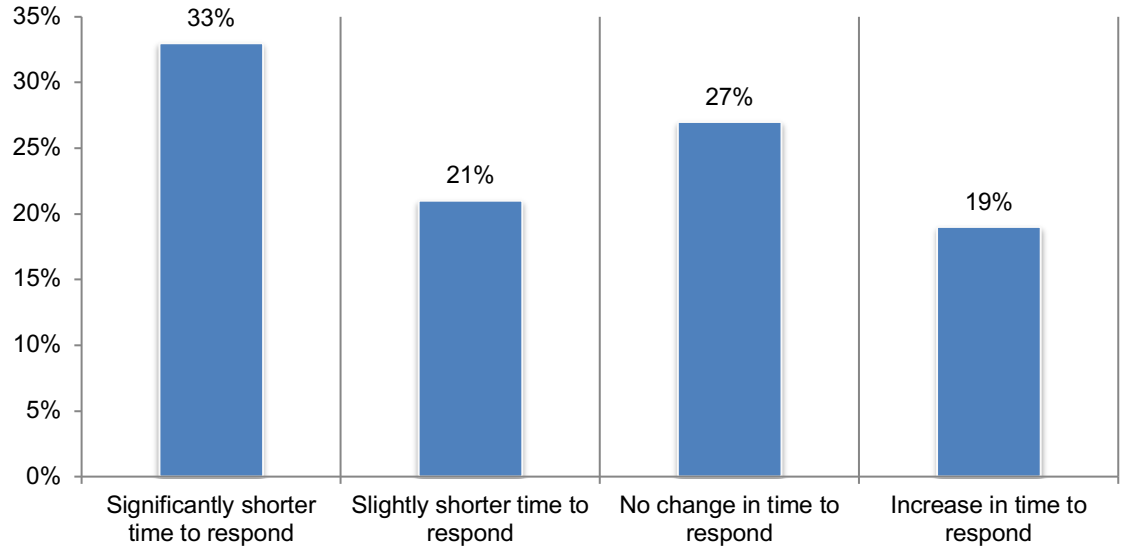
More automation is needed to improve the patching process. Only 44 percent of respondents say their organizations automate patching. As shown in Figure 8, automation is mostly used to automate patching (67 percent of respondents) followed by prioritization (53 percent of respondents).

Figure 8. If your organization uses automation, what steps do you automate?
More than one response permitted



Automation successfully reduces the time to respond to vulnerabilities. According to Figure 9, of the 44 percent of respondents who say their organization uses automation, 54 percent of respondents say automation significantly reduces the time to respond (33 percent) or shortens the time to respond to vulnerabilities (21 percent).

Figure 9. If yes, how has automation impacted the time it takes to respond to vulnerabilities?



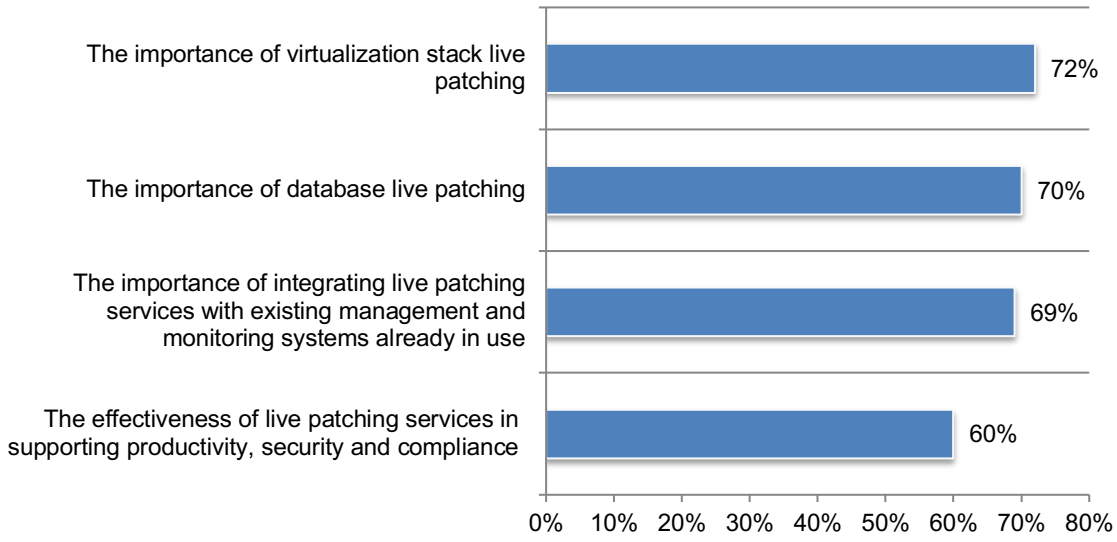
Looking at live patching

In the context of this research**, live patching** is the process of deploying carefully prepared and extensively tested patches to a Linux kernel while the server is still running, updating it automatically. Live patching is rebootless and reduces patching tasks by as much as 60 percent

Organizations believe virtualization and database live patching are very important to improving the patching process. Respondents were asked to rate the importance of virtualization stack and database live patching on a scale of 1 = low importance to 10 = high importance.

Figure 10 shows the high importance/effectiveness responses (7+ responses on the 10-point scale). Seventy-two percent of respondents say virtualization stack and 70 percent of respondents say database live patching are very or highly important. Sixty-nine percent of respondents say integrating live patching services with existing management and monitoring systems already in use are highly or very important. Sixty percent of respondents say their organizations are effective or very effective at live patching services in supporting productivity, security and compliance.

Figure 10. How important is live patching?
On a scale from 1 = low importance/effectiveness to 10 = high importance/effectiveness, 7+ responses presented



The cost and time spent monitoring and patching vulnerabilities

Table 1 provides the average amount of time organizations spend on monitoring systems for threats and vulnerabilities and patching. As shown, organizations are spending the most time patching applications and systems (340 hours) and downtime hours due to patching of vulnerabilities (340 hours). While the least amount of time is spent documenting and/or reporting on the patch management process, such documentation can be key to improving the patching process going forward.

The average total number of hours is 1,075. The average hourly rate for an IT and IT security practitioner is $63.50*. As shown in the Table, we multiply the hours by the average total weekly cost. Based on a 40-hour week for the IT security team, the cost can be as high as $68,263 or $3,549,676 annually.

For context, these numbers relate to an extrapolated average IT team size of approximately 30 members and an overall organization size of around 12,000 people [Appendix Table S3 and S5, respectively].

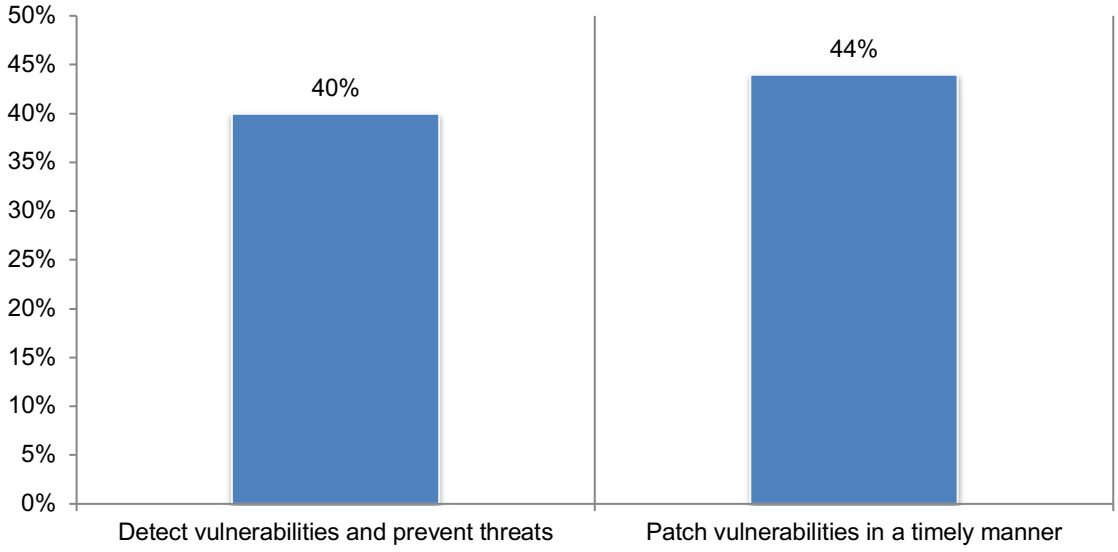
Table 1. The average weekly cost and time spent monitoring and patching vulnerabilities	Hours per week
Hours spent each week monitoring systems for threats and vulnerabilities	280
Hours spent each week patching applications and systems	340
Hours spent each week documenting and/or reporting on the patch management process	115
Downtime hours occurs due to patching of vulnerabilities	340
Average total hours per week	1,075
Average total weekly cost (1,075 x $63.50)	$68,263
Average total annual cost ($68,263 x 52 weeks)	$3,549,676

*Based on Ponemon Institute benchmark research (2021)

Organizations are at risk because of the inability to detect and patch vulnerabilities in a timely manner. According to the research, only 43 percent of respondents say the IT security function has adequate staffing to patch vulnerabilities in a timely manner.

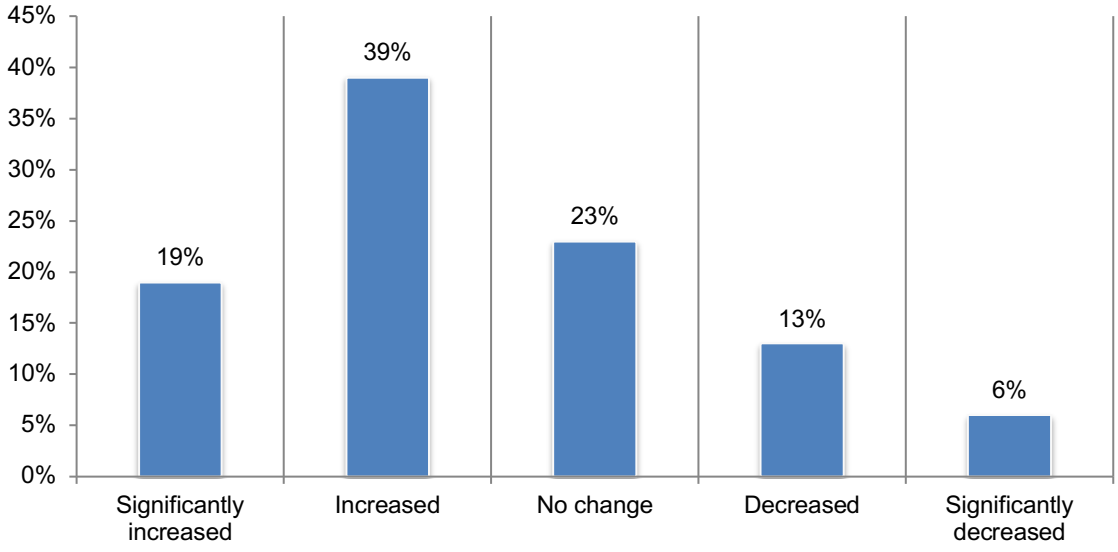
Respondents were asked to rate their organizations' ability to detect and patch vulnerabilities in a timely manner on a scale from 1 = low ability to 10 = high ability. Figure 11 presents the high ability responses (7+ on the 10-point scale). Only 40 percent of respondents rate their organizations' ability to detect vulnerabilities and prevent threats as high and only 44 percent of respondents say their organizations patch vulnerabilities in a timely manner.

Figure 11. Organization's ability to detect and patch vulnerabilities in a timely manner
On a scale from 1 = low ability to 10 = high ability, 7+ responses presented



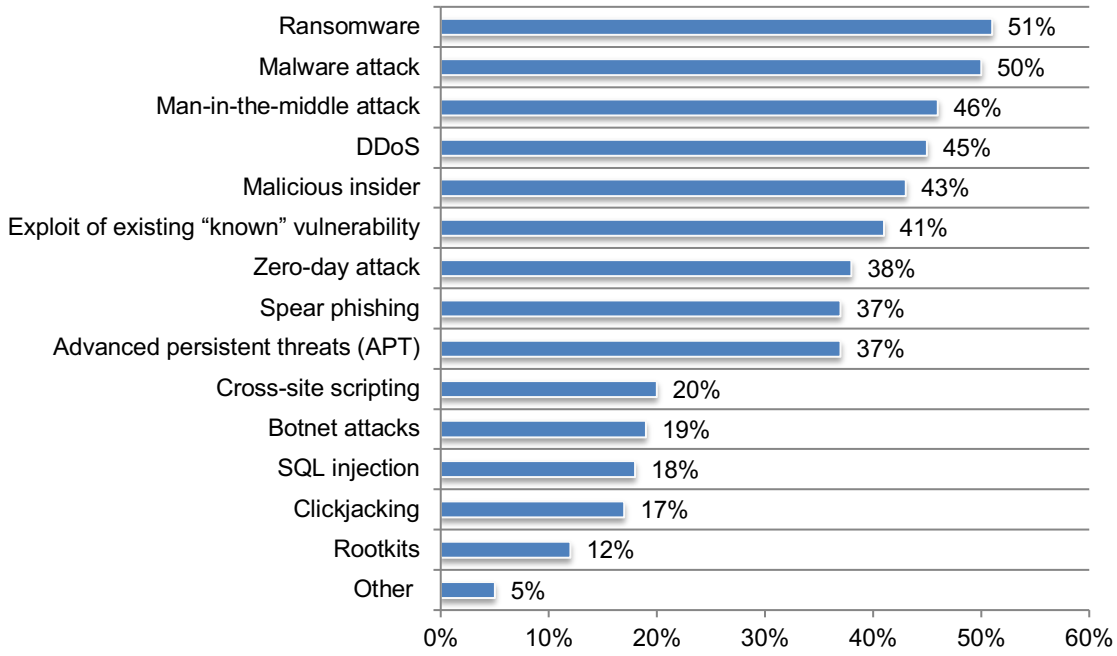
Fifty-eight percent of respondents say the time to patch critical vulnerabilities has significantly increased (19 percent) or increased (39 percent).

Figure 12. How has the time to patch a critical vulnerability in the past two years?



As ransomware attacks become more lucrative for hackers, more than half (51 percent) of respondents say in the past 12 months their organizations had at least one ransomware attack. Figure 13 presents a list of exploits or compromises organizations experienced in the past year. Ransomware is the most frequent but almost equally frequent are malware attacks (50 percent of respondents).

Figure 13. Did your organization have any of the following exploits or compromises in the past 12 months?
More than one response permitted

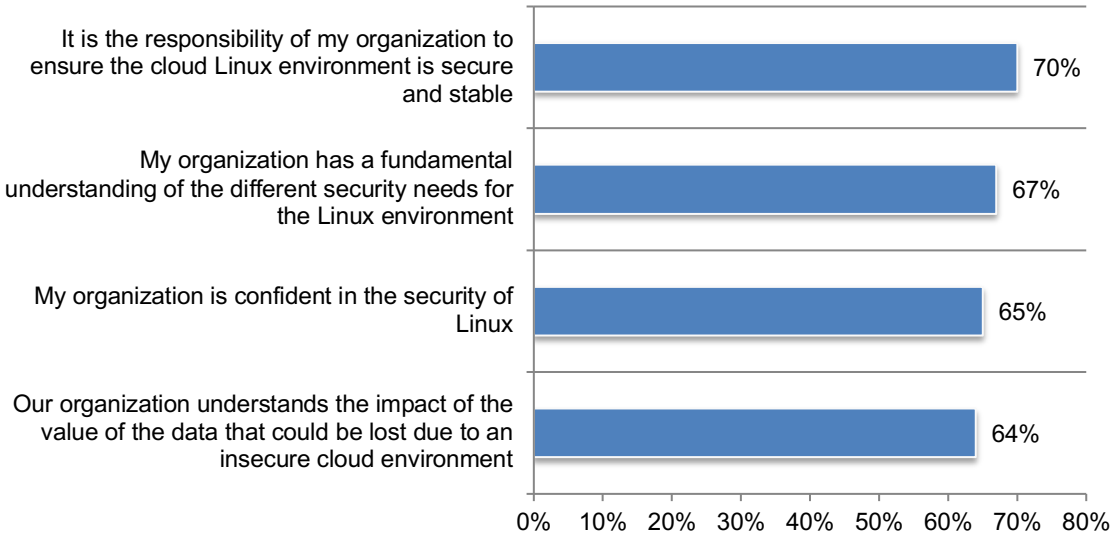


Organizational leadership is needed to improve patching

Organizations consider it their responsibility to ensure the cloud Linux environment is secure. As shown in Figure 14, 70 percent of respondents say their organizations are responsible for ensuring the cloud Linux environment is secure and 64 percent of respondents say their organizations understand the impact of the value of the data that could be lost due to an insecure cloud environment.

Sixty-seven percent of respondents say their organization has a fundamental understanding of the different security needs for the Linux environment.

Figure 14. Organizations' perceptions about cloud security and Linux
Strongly agree and Agree responses combined

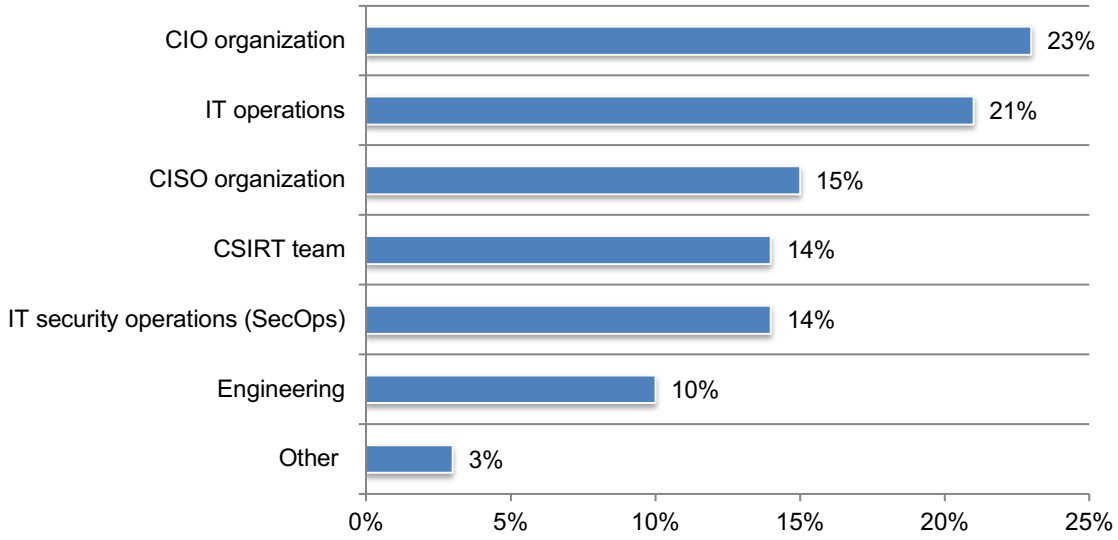


IT, but not IT security, is most responsible for applying most of the patches. According to Figure 15, 44 percent of respondents say CIOs (23 percent) or IT operations (21 percent) are responsible for patching. Only 15 percent of respondents say the CISO organization is most responsible.

A potential obstacle to reducing cyberattacks is that the IT and IT security functions may have different priorities when allocating resources to vulnerability and patch management. Senior leadership should consider assigning responsibility for applying patches to the CISO and not the CIO and IT functions because of the different priorities they may have in allocating much needed resources. A lack of accountability is a factor that delays the vulnerability patching process.

The lack of resources is another significant problem for timely patching. Currently, if CISOs are responsible most respondents say they do not have the staff to patch in a timely manner.

Figure 15. Which team is responsible for applying the majority of patches?

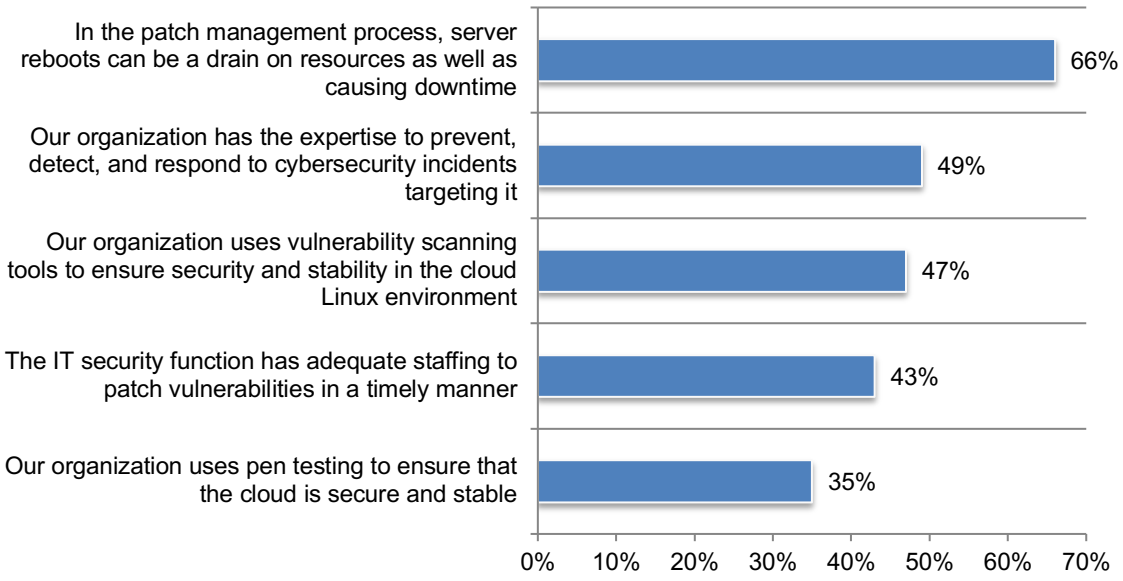


Enterprise roadblocks to vulnerability management

A lack of resources and in-house expertise prevent timely patching. Figure 16 presents respondents' opinions about their organizations' patch management process. According to the research, delays in patching leave organizations vulnerable to successful cyberattacks. Sixty-six percent of respondents say server reboots can be a drain on resources as well as cause downtime. Further, only 43 percent of respondents say the IT security function has adequate staffing to patch vulnerabilities in a timely manner.

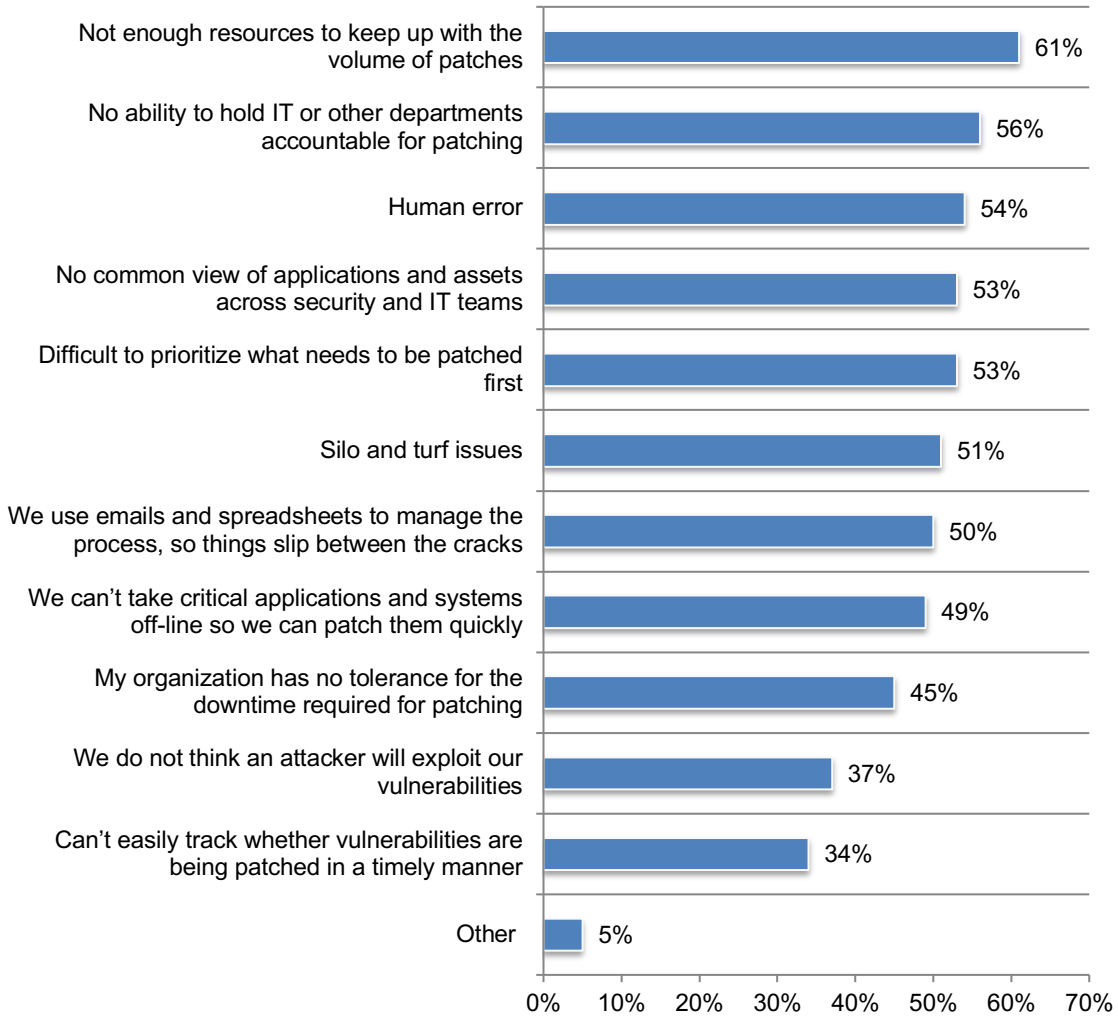
As discussed previously, 70 percent of respondents say it is the responsibility of their organizations to ensure the cloud Linux environment is secure and stable. However, only 35 percent of respondents say their organization uses pen testing to ensure that the cloud is secure and stable.

Figure 16. Perceptions about the patch management process
Strongly Agree and Agree responses combined



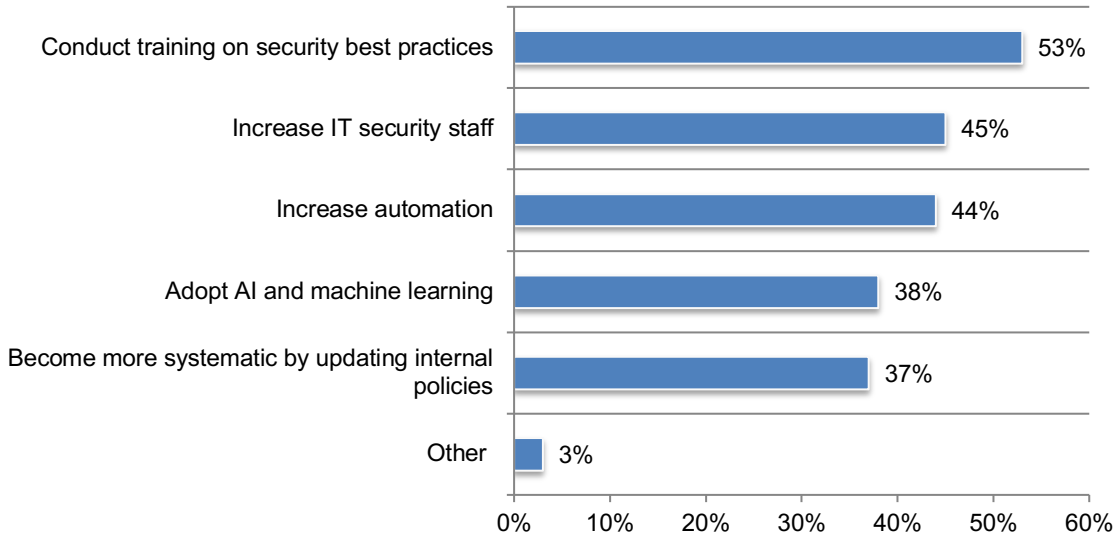
The lack of accountability is affecting organizations' ability to keep up with the volume of patches. Figure 17 presents a list of factors that can cause major delays in the patching process. The human factor is number one reason for such delays. These include the lack of resources to keep up with the volume of patches (61 percent of respondents), no ability to hold IT or other departments accountable for patching (56 percent of respondents) and human error (54 percent of respondents).

Figure 17. Which factors cause major delays in your vulnerability patching process?
More than one response permitted



Replace manual patching with automation. Timely patching and vulnerability management continues to be mostly manual. According to Figure 18, the focus on improving patching and vulnerability management is on training (53 percent of respondents). Only 44 percent of respondents say organizations are increasing automation and adopting AI and machine learning (38 percent of respondents).

Figure 18. What steps did your organization take to improve its patch and vulnerability management processes?
More than one response permitted



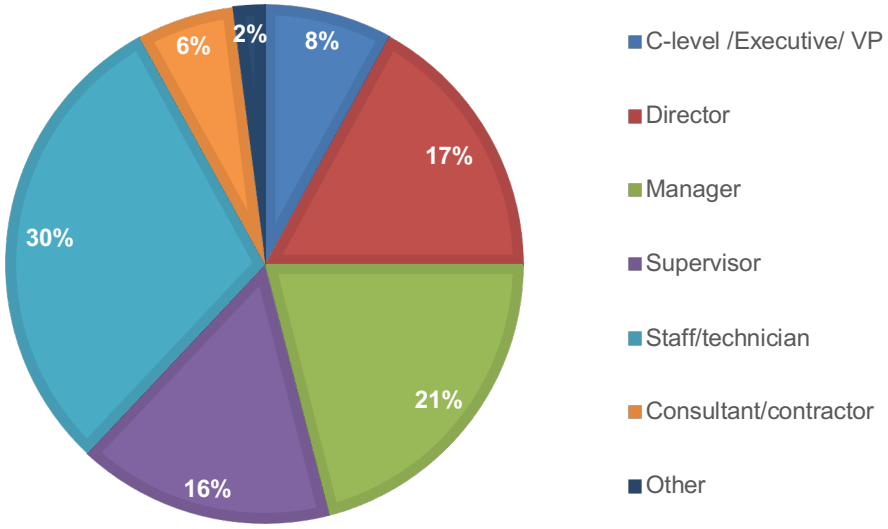
Part 3. Methodology

A sampling frame of 14,505 IT, IT security practitioners were selected as participants to this survey. All respondents use Linux within their organizations. Table 2 shows 609 total returns. Screening and reliability checks required the removal of 45 surveys. Our final sample consisted of 564 surveys or a 3.9 percent response.

Table 2. Sample response	Freq	Pct%
Sampling frame	14,505	100.0%
Total returns	609	4.2%
Rejected or screened surveys	45	0.3%
Final sample	564	3.9%

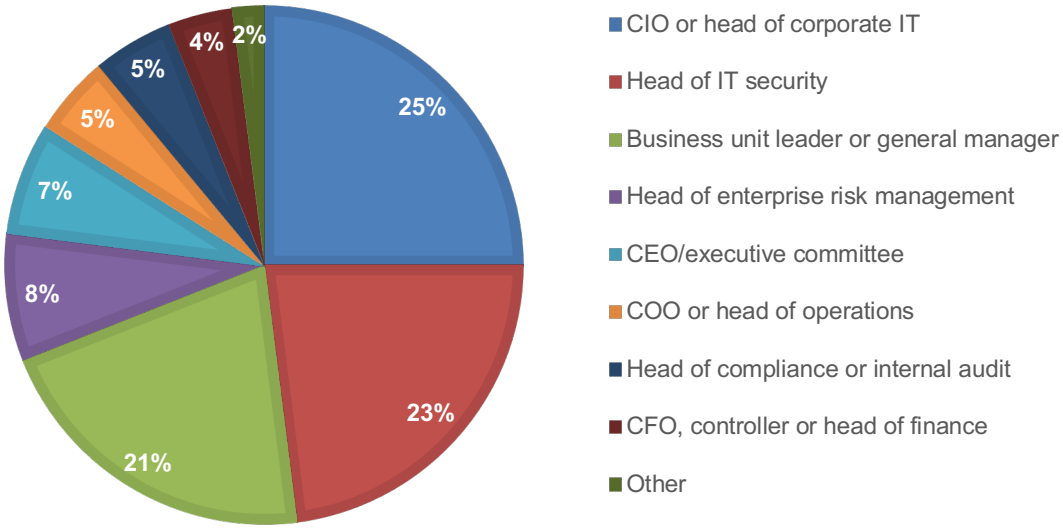
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (62 percent) of respondents are at or above the supervisory levels. The largest category at 30 percent of respondents is staff/technician.

Pie Chart 1. Current position within the organization



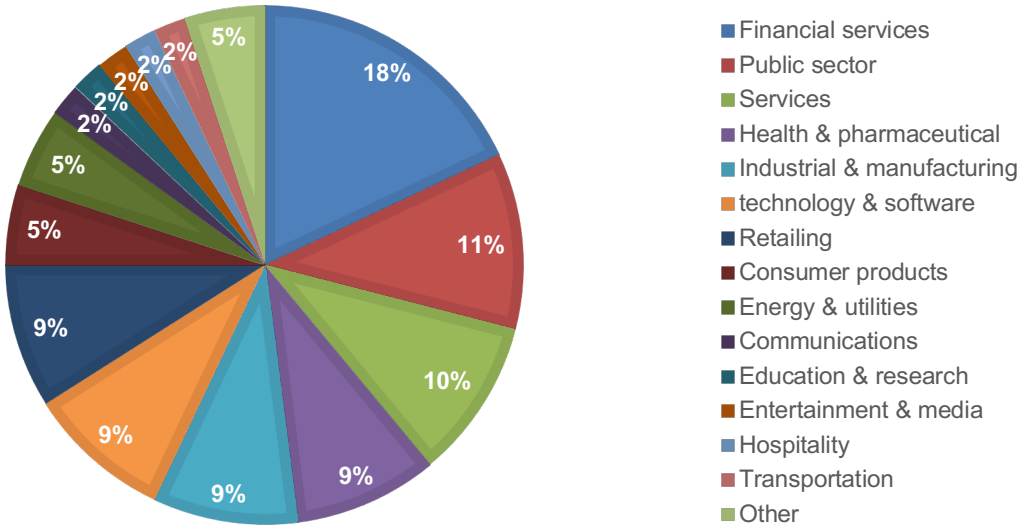
Pie Chart 2 reports the primary person the respondent reports to within the organization. Twenty-five percent of respondents report to the CIO or head of corporate IT, 23 percent of respondents report to the head of IT security, and 21 percent of respondents report to the business unit leader or general manager.

Pie Chart 2. Primary person respondent reports to within the organization



Pie Chart 3 reports the industry focus of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by public sector (11 percent of respondents), services (10 percent of respondents), health and pharmaceuticals, industrial and manufacturing, technology and software, and retailing (each at 9 percent of respondents).

Pie Chart 3. Industry focus of respondents' organizations



Part 4. Caveats

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 or 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 al survey questions. All survey responses were captured in September 2021.

Survey Response	Freq	Pct%
Total sampling frame	14,505	100.0%
Total returns	609	4.2%
Rejected surveys	45	0.3%
Final Sample	564	3.9%

Part 1. Screening

S1. What best describes your organizational role or area of focus?	Pct%
IT security operations (DevSecOps)	11%
IT operations	30%
CSIRT team	13%
CIO organization	14%
CISO organization	21%
Research & development	3%
Risk & governance	5%
Security analyst	3%
None of the above (stop)	0%
Total	100%

S2. Does your organization use Linux?	Pct%
Yes	100%
No (stop)	0%
Total	100%

S3. How many IT and IT security personnel does your organization have?	Pct%
Less than 5 (stop)	0%
5 to 20	38%
20 to 50	45%
50+	17%
Total	100%
Extrapolated value	30.7

S4. What best describes the infrastructure or technology stack in your organization?	Pct%
Open source (e.g. Linux)	43%
Proprietary (e.g. Microsoft)	39%
Combination of open source and proprietary	18%
None of the above (stop)	0%
Total	100%

S5. What range best describes the full-time headcount of your global organization?	Pct%
Less than 500 (stop)	0%
500 to 1,000	19%
1,001 to 5,000	33%
5,001 to 10,000	23%
10,001 to 25,000	14%
25,001 to 75,000	7%
More than 75,000	4%
Total	100%
Extrapolated value	12,008

Part 2. Cyberattack experience

Q1. Did your organization have a cybersecurity incident in the **past 2 years**?	Pct%
Yes	65%
No (skip to Q4)	28%
Unsure (skip to Q4)	7%
Total	100%

Q2. What were the root causes of these cybersecurity incidents? Please check all that apply.	Pct%
Criminal external attack to disrupt/affect system availability	47%
System glitch	34%
Human error	50%
Malicious insider	43%
Other (please specify)	7%
Total	181%

Q3a. Did any of these cybersecurity incidents occur while a patch was available for a known vulnerability but was not applied?	Pct%
Yes	55%
No	40%
Unsure	5%
Total	100%

Q3b. If yes, was your organization actually aware that it was vulnerable prior to the cybersecurity incident?	Pct%
Yes	43%
No	50%
Unsure	7%
Total	100%

Q4. Did your organization have any of the following exploits or compromises **in the past 12 months**? Please check all that apply.	Pct%
Advanced persistent threats (APT)	37%
Botnet attacks	19%
Clickjacking	17%
Cross-site scripting	20%
DDoS	45%
Exploit of existing “known” vulnerability	41%
Malicious insider	43%
Ransomware	51%
Rootkits	12%
Spear phishing	37%
SQL injection	18%
Malware attack	50%
Zero-day attack	38%
Man-in-the-middle attack	46%
Other (please specify)	5%
Total	479%

Part 3. Patching and vulnerability management

Q5a. Does your organization use on-premises virtualization?	Pct%
Yes	61%
No (please skip to Q6a)	29%
Don’t know (please skip to Q6a)	10%
Total	100%

Q5b. If yes, which one does your organization use?	Pct%
QEMU/KVM	21%
XEN	19%
VMware	41%
Hyper-V	13%
Other (please specify)	6%
Total	100%

Q5c. If yes, does your organization have spare hardware capacity (i.e. extra servers) to accommodate virtualized workloads during maintenance operations?	Pct%
Yes	51%
No	49%
Total	100%

Q6a. Did your organization take steps to improve its patch and vulnerability management processes? Please select all that apply.	Pct%
Yes	52%
No (please skip to Q7a)	48%
Total	100%

Q6b. If yes, what steps did your organization take? Please select all that apply.	Pct%
Increase automation	44%
Adopt AI and machine learning	38%
Increase IT security staff	45%
Conduct training on security best practices	53%
Become more systematic by updating internal policies	37%
Other (please specify)	3%
Total	220%

Q7a. Does your organization use live patching services as defined above?	Pct%
Yes	76%
No (please skip to Q8)	24%
Total	100%

Q7b. Using the following 10-point scale, please rate the effectiveness of live patching services in supporting productivity, security and compliance from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 or 2	3%
3 or 4	11%
5 or 6	26%
7 or 8	31%
9 or 10	29%
Total	100%
Extrapolated value	6.94

Q7c. Using the following 10-point scale, please rate the importance of integrating live patching services with existing management and monitoring systems already in use from 1 = low importance to 10 = high importance.	Pct%
1 or 2	5%
3 or 4	6%
5 or 6	20%
7 or 8	30%
9 or 10	39%
Total	100%
Extrapolated value	7.34

Q7d. Using the following 10-point scale, please rate the importance of database live patching from 1 = low importance to 10 = high importance.	Pct%
1 or 2	0%
3 or 4	7%
5 or 6	23%
7 or 8	31%
9 or 10	39%
Total	100%
Extrapolated value	7.54

Q7e. Using the following 10-point scale, please rate the importance of virtualization stack live patching from 1 = low importance to 10 = high importance.	Pct%
1 or 2	2%
3 or 4	10%
5 or 6	16%
7 or 8	40%
9 or 10	32%
Total	100%
Extrapolated value	7.30

Part 4. Attackers' ability to exploit vulnerabilities

Q8. Using the following 10-point scale, please rate your organization's ability to **prevent** a data breach or cyberattack from 1 = low ability to 10 = high ability.	Pct%
1 or 2	13%
3 or 4	21%
5 or 6	20%
7 or 8	28%
9 or 10	18%
Total	100%
Extrapolated value	5.84

Q9. Using the following 10-point scale, please rate your organization's ability to **detect** a data breach **or** cyberattack from 1 = low ability to 10 = high ability.	Pct%
1 or 2	12%
3 or 4	15%
5 or 6	21%
7 or 8	21%
9 or 10	31%
Total	100%
Extrapolated value	6.38

Q10. Using the following 10-point scale, please rate your organization's ability to quickly detect vulnerabilities and prevent threats from 1 = low ability to 10 = high ability.	Pct%
1 or 2	12%
3 or 4	19%
5 or 6	29%
7 or 8	21%
9 or 10	19%
Total	100%
Extrapolated value	5.82

Q11. Using the following 10-point scale, please rate your organization's ability to patch vulnerabilities in a timely manner from 1 = low ability to 10 = high ability.	Pct%
1 or 2	11%
3 or 4	13%
5 or 6	32%
7 or 8	25%
9 or 10	19%
Total	100%
Extrapolated value	6.06

Q12. Using the following 10-point scale, please rate the importance of having regular patches and updates for systems that are past their end-of-life from 1 = low importance to 10 = high importance.	Pct%
1 or 2	2%
3 or 4	4%
5 or 6	13%
7 or 8	43%
9 or 10	38%
Total	100%
Extrapolated value	7.72

Q13. Using the following 10-point scale, please rate the importance of virtualizing users' file systems in order to prevent sensitive information disclosure from 1 = low importance to 10 = high importance.	Pct%
1 or 2	0%
3 or 4	5%
5 or 6	15%
7 or 8	39%
9 or 10	41%
Total	100%
Extrapolated value	7.82

Q14. Using the following 10-point scale, please rate the importance of patching database backends (mysql, mariadb, postgresql, etc.) during maintenance operations from 1 = low importance to 10 = high importance.	Pct%
1 or 2	2%
3 or 4	5%
5 or 6	20%
7 or 8	33%
9 or 10	40%
Total	100%
Extrapolated value	7.58

Q15. How often does your organization scan for vulnerabilities?	Pct%
More than once per day	1%
Daily	7%
Between 2 and 3 times per week	2%
Every week	10%
Every 2 weeks	11%
Every 3 weeks	15%
Every 4 weeks	9%
More than 4 weeks	20%
No set schedule	25%
Total	100%

Q16a. Once you detect a **critical or high priority** vulnerability, how long on average does it take to patch?	Pct%
Up to 1 day	5%
1 day	7%
3 days	0%
1 week	8%
2 weeks	9%
3 weeks	6%
4 weeks	9%
5 weeks	11%
6 weeks	12%
7 weeks	6%
8 weeks	9%
9 weeks to 6 months	5%
7 months to 1 year	8%
More than 1 year	5%
Unsure	0%
Total	100%

Q16b. How has this time changed in the last 2 years?	Pct%
Significantly increased	19%
Increased	39%
No change	23%
Decreased	13%
Significantly decreased	6%
Total	100%

Q17. How do you prioritize vulnerabilities? Please select all that apply.	Pct%
Common Vulnerability Scoring System (CVSS) security score of the vulnerability	46%
Type of system impacted	51%
Vulnerability factors such as exploit availability	53%
Business risk of systems affected by the vulnerability	47%
Other (please specify)	5%
Total	202%

Q18. Do you have a single view of the full vulnerability management lifecycle, including exception handling?	Pct%
Yes	31%
No	69%
Total	100%

Q19. Which factors below cause major delays in your vulnerability patching process? Please select all that apply.	Pct%
Human error	54%
We can't take critical applications and systems off-line so we can patch them quickly	49%
We can't easily track whether vulnerabilities are being patched in a timely manner	34%
We use emails and spreadsheets to manage the process, so things slip between the cracks	50%
We find it difficult to prioritize what needs to be patched first	53%
We don't have enough resources to keep up with the volume of patches	61%
We don't have a common view of applications and assets across security and IT teams	53%
We do not think an attacker will exploit our vulnerabilities	37%
Technologies such as automation reduce the risk of not patching quickly	34%
Silo and turf issues	51%
We don't have the ability to hold IT or other departments accountable for patching	56%
My organization has no tolerance for the downtime required for patching	45%
Other (please specify)	5%
Total	582%

Part 5. Attributions: Please express your opinion about each one of the following statements using the scale below each item. **Strongly Agree and Agree response combined**.	Pct%
Q20a. The IT security function in our organization has adequate staffing to patch vulnerabilities in a timely manner.	43%
Q20b. Enterprise open source, such as Linux, is more secure or as secure as software.	60%
Q20c. The use of open source technology allows my organization to achieve a high level of security in the extended lifecycle management program.	62%
Q20d. The use of open source technology provides transparency and visibility to increase the security and stability of the patch management process.	57%
Q20e. My organization has a fundamental understanding of the different security needs for the Linux environment.	67%
Q20f. My organization is confident in the security of Linux.	65%
Q20g. It is the responsibility of my organization to ensure the cloud Linux environment is secure and stable.	70%
Q20h. Our organization understands the impact of the value of the data that could be lost due to an insecure cloud environment.	64%
Q20i. Our organization has the expertise to prevent, detect, and respond to cybersecurity incidents targeting it.	49%
Q20j. Our organization uses vulnerability scanning tools to ensure security and stability in the cloud Linux environment.	47%
Q20k. Our organization uses pen testing to ensure that the cloud is secure and stable.	35%
Q20l. In the patch management process, server reboots can be a drain on resources as well as causing downtime	66%
Q20m. Compliance requirements are important when defining patch management operations.	62%

Part 6. Estimating time to detect and contain vulnerabilities

Q21. Approximately how many hours each week are spent **monitoring** systems for threats and vulnerabilities? Please estimate the aggregate hours of the IT and IT security (DevSecOps) team.	Pct%
Less than 5 hours	3%
5 to 10 hours	2%
11 to 25 hours	5%
26 to 50 hours	7%
51 to 100 hours	12%
101 to 250 hours	21%
251 to 500 hours	31%
More than 500 hours	19%
Total	100%
Extrapolated value (hours)	280

Q22. Approximately how many hours each week are spent **patching** applications and systems? Please estimate the aggregate hours of the IT and IT security (DevSecOps) team.	Pct%
Less than 5 hours	0%
5 to 10 hours	3%
11 to 25 hours	0%
26 to 50 hours	9%
51 to 100 hours	11%
101 to 250 hours	13%
251 to 500 hours	35%
More than 500 hours	29%
Total	100%
Extrapolated value (hours)	340

Q23. Approximately how many hours each week are spent **documenting and/or reporting** on the patch management process (in conformance with policies or compliance mandates)? Please estimate the aggregate hours of the IT and IT security (SecOps) team.	Pct%
Less than 5 hours	5%
5 to 10 hours	8%
11 to 25 hours	11%
26 to 50 hours	30%
51 to 100 hours	21%
101 to 250 hours	11%
251 to 500 hours	8%
More than 500 hours	6%
Total	100%
Extrapolated value (hours)	115

Q24. Based on the size and complexity of your organization's tech stack, approximately how much downtime do you estimate occurs due to patching of vulnerabilities?	Pct%
Less than 5 hours	0%
5 to 10 hours	3%
11 to 25 hours	0%
26 to 50 hours	9%
51 to 100 hours	11%
101 to 250 hours	13%
251 to 500 hours	35%
More than 500 hours	29%
Total	100%
Extrapolated value (hours)	340

Q25. Using the following 10-point scale, how much of a problem is downtime due to patching vulnerabilities from 1 = not a problem to 10 = huge problem.	Pct%
1 or 2	1%
3 or 4	5%
5 or 6	8%
7 or 8	40%
9 or 10	46%
Total	100%
Extrapolated value	8.00

Q26. Which team in your organization is responsible for applying the majority of patches?	Pct%
IT security operations (SecOps)	14%
IT operations	21%
CSIRT team	14%
CIO organization	23%
CISO organization	15%
Engineering	10%
Other (lease specify)	3%
Total	100%

Q27. On average how much time is lost coordinating with the responsible team before a patch is applied (i.e. other business units, other IT teams and users)?	Pct%
Less than 1 day	19%
Less than 1 week	21%
1 week to 2 weeks	25%
2 weeks to 3 weeks	10%
3 weeks to 1 month	8%
More than 1 month	7%
None – My team is fully responsible for patching vulnerabilities so we do not coordinate with other teams	10%
Total	100%
Extrapolated value	11.67

Q28a. Does your organization use automation to assist with vulnerability management?	Pct%
Yes	44%
No	56%
Total	100%

Q28b. If yes, what steps do you automate? Please select all that apply.	Pct%
Prioritization	53%
Assignment	41%
Patching	67%
Reporting	50%
Other (please specify)	3%
Total	214%

Q28c. If yes, how has automation impacted the time it takes to respond to vulnerabilities?	Pct%
Significantly shorter time to respond	33%
Slightly shorter time to respond	21%
No change in time to respond	27%
Increase in time to respond	19%
Total	100%

Q29. Do you report how quickly specific types of vulnerabilities are remediated?	Pct%
Yes	41%
No	59%
Total	100%

Part 7. Organizational demographics

D1. What best describes your position level within the organization?	Pct%
C-level /Executive/ VP	8%
Director	17%
Manager	21%
Supervisor	16%
Staff/technician	30%
Consultant/contractor	6%
Other (please specify)	2%
Total	100%

D2. What best describes your reporting channel or chain of command?	Pct%
CEO/executive committee	7%
COO or head of operations	5%
CFO, controller or head of finance	4%
CIO or head of corporate IT	25%
Business unit leader or general manager	21%
Head of compliance or internal audit	5%
Head of enterprise risk management	8%
Head of IT security	23%
Other (please specify)	2%
Total	100%

D3. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	9%
Hospitality	2%
Industrial & manufacturing	9%
technology & software	9%
Public sector	11%
Retailing	9%
Services	10%
Transportation	2%
Other (please specify)	3%
Total	100%

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.