

# 10 CRITICAL

## CYBERSECURITY METRICS FOR CSOs





# 10 critical cybersecurity metrics for CSOs

## Introduction

**D**espite the best-laid defenses, security incidents and data breaches continue to occur. All that chief security officers (CSOs) can do is keep a close eye on their organization's security perimeter. However, monitoring thousands of users and endpoints is no easy feat. A simpler option is to answer just one question: How secure is my organization now? In this e-book, we've compiled a list of 10 metrics that can give you a clear picture of your organization's security status.

### **Mean time to acknowledge (MTTA)**

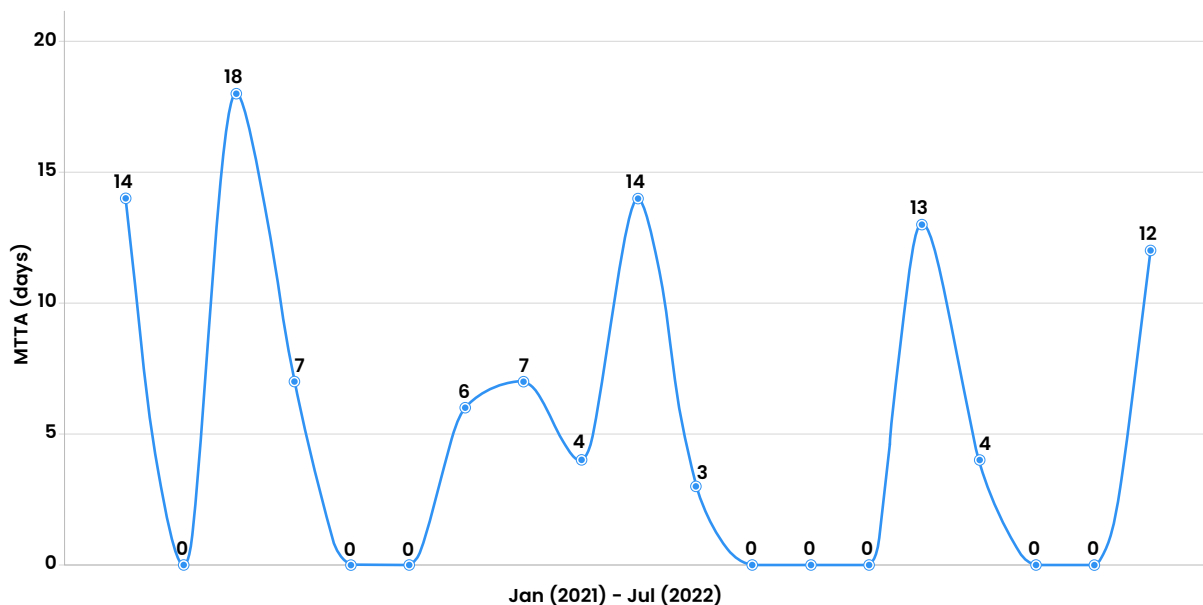
**S**ecurity incidents are expensive and embarrassing, and they pinpoint flaws within an organization's secure framework. While security incidents can be prevented by implementing security best practices and measures, in the rare case that an event occurs, it's critical for security teams to detect the breach before it spirals into a large-scale security incident.

The MTTA tells you how long it takes for your organization to acknowledge a security incident or breach and start working on resolving it. MTTA can also be described as a measure of your organization's ability to race against time and identify an intruder present in your network.

The report below displays the trend of MTTA events for the last two years.



### Trend of MTTA



The report above shows that the average time to acknowledge events for Zylker Corp. (a fictional company) is much less than **the industry average of 80 days**<sup>[1]</sup>.

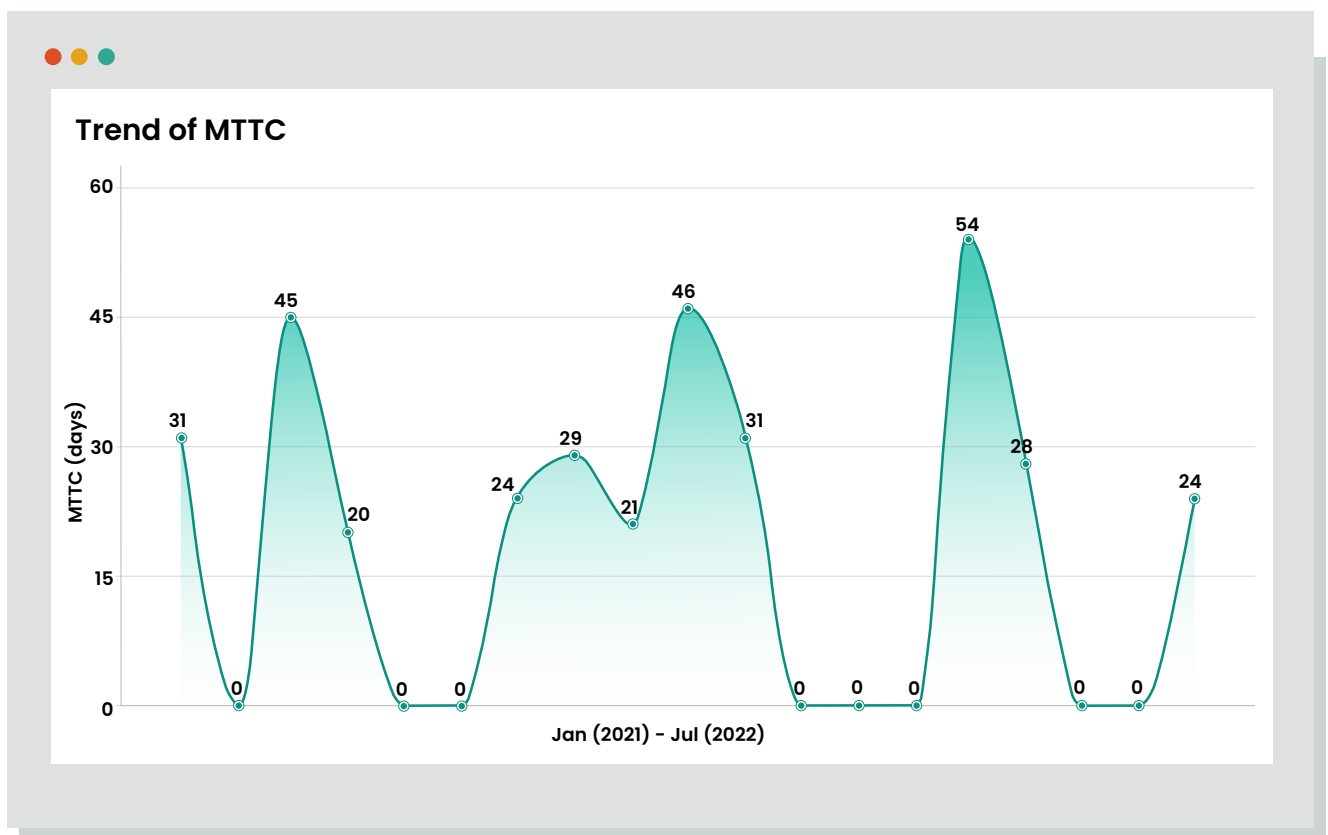
Needless to say, it's important to keep this metric as low as possible; the longer an intruder remains in your system, the greater the risk for your data.

## 2 Mean time to contain (MTTC)

**T**hreat containment is incredibly challenging for security teams due to slow threat detection and acknowledgment of security incidents. The impact of a security threat increases with the time it takes for the technicians to identify, acknowledge, and resolve it, so time is always critical for security teams.

The MTTC gives you a holistic view of your security team's operations. The MTTC is the average time taken to detect, acknowledge, and resolve a security threat, and prevent any further impact. In other words, it is the time taken to close an identified attack vector across all your organization's endpoints.

Here's a sample report that shows the trend of MTTC incidents for the last two years.



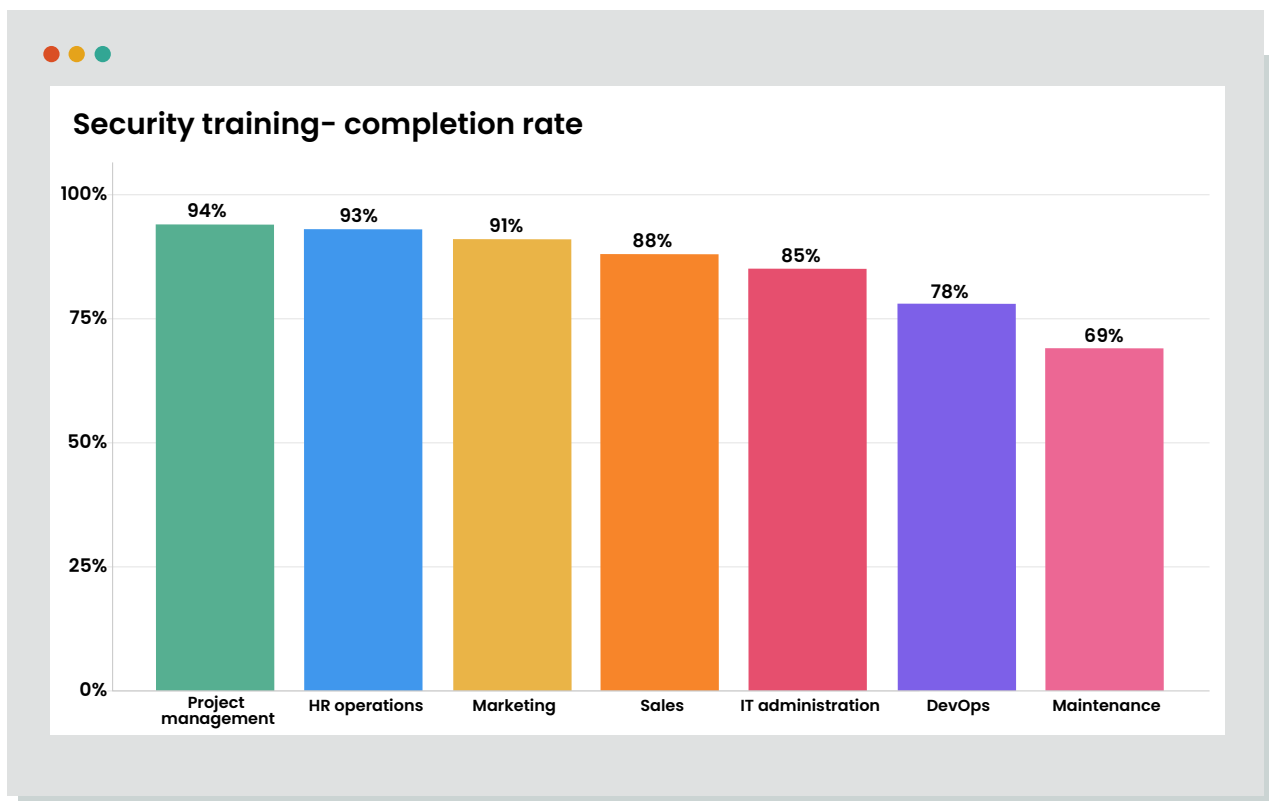
MTTC is an important metric that measures the incident management performance of your organization—it's critical to always keep it as low as possible.

## 3

## Cyberdefense preparedness level

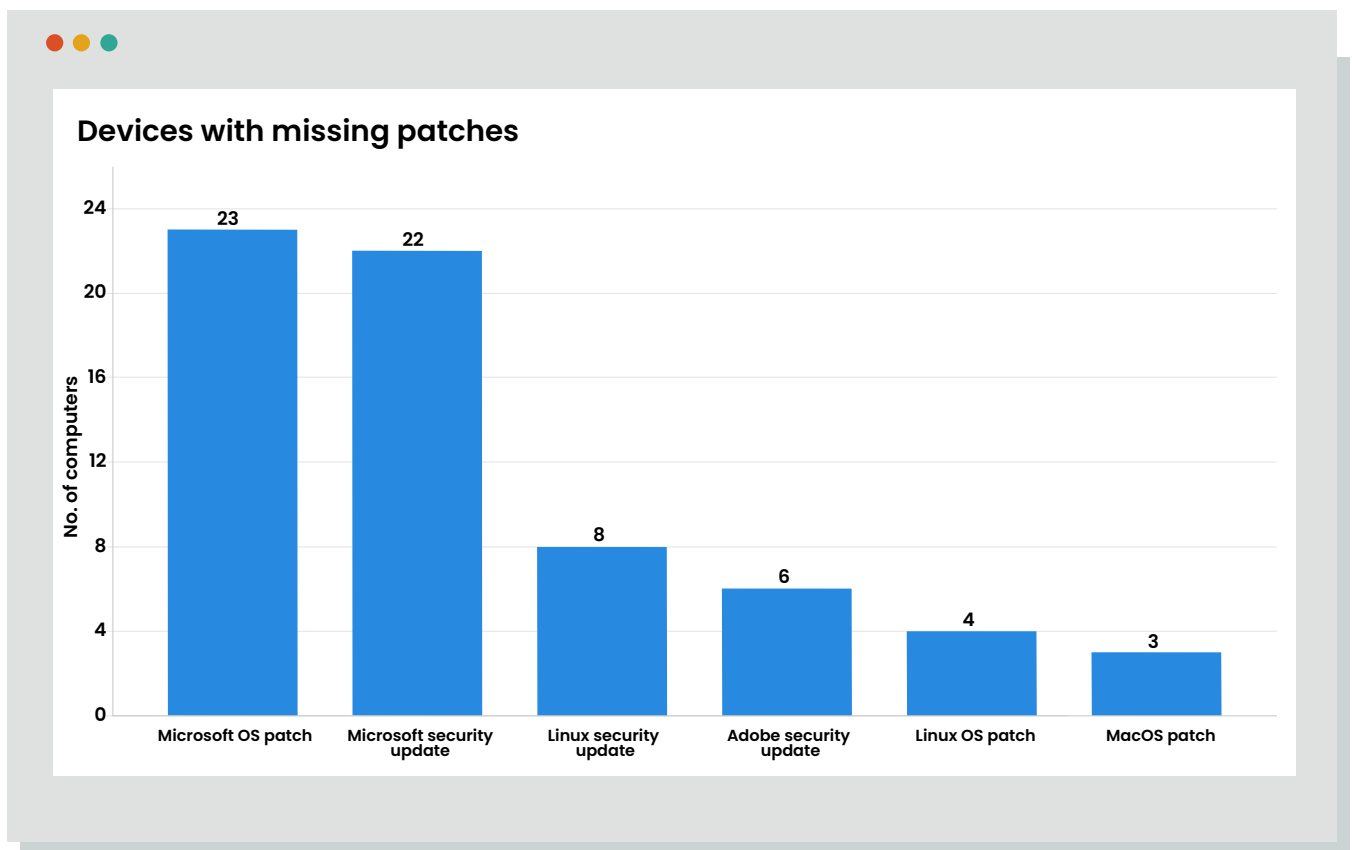
In 2016, a Snapchat employee was tricked by an email from<sup>[2]</sup> a scammer who impersonated the company's CEO. This phishing attack allowed the attacker to access the payroll information of a group of current and former employees.

Negligence isn't always the reason for security breaches. Sometimes, employees can cause unintentional damage due to a lack of knowledge, especially in a hybrid work environment. Monitor your organization's cyberdefense preparedness level by maintaining tabs on the percentage of employees that completed their security training, and ensure that this number stays as high as possible.



The report above shows the total percentage of employees who have completed their training over a few years.

Security patches are also critical to securing your data from attackers. Patches should be deployed on time to eliminate any critical vulnerabilities in your system. Enforce regular patching of servers and gateway appliances, and keep tabs on the number of critical and missing patches. Look for missing patches and monitor if your endpoints are patched and up to date.



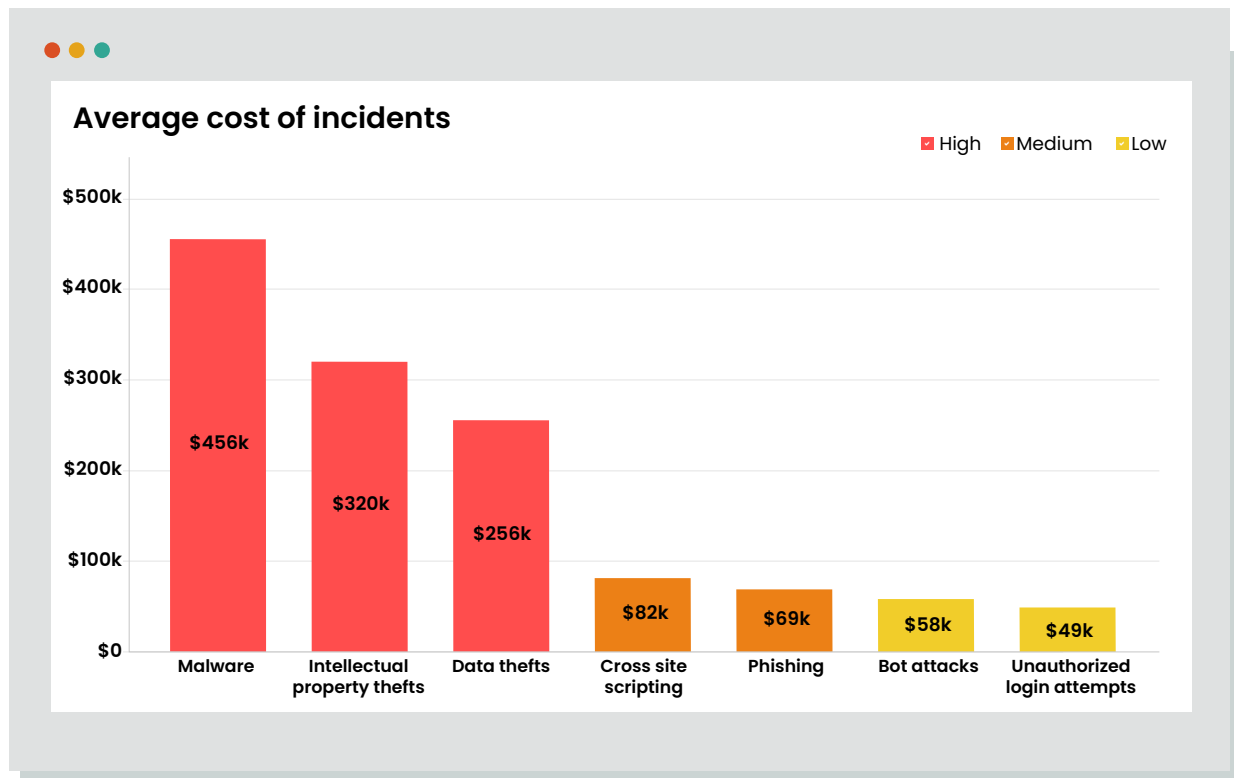
The report above shows a list of systems that are missing patches and are vulnerable to external threats. It's critical to take actions to prevent mishaps in the organization. You can also identify the systems with missing patches to isolate them during an attack. By isolating a vulnerable system, you can terminate the attacker's access to other systems and network sources.

## 4

## Cost per incident

**B**esides reputational damage, security incidents also take a chunk of the IT budget for repair and restoration. While security teams tend to focus on resolving the incidents, not much attention is paid to tracking the overall costs of each security incident. Instead, they rely on estimates. While estimates are effective to a certain extent, they aren't accurate. Measuring cost per incident enables you to compare your costs against industry standards, and allows you to measure security holistically. Indirectly, the cost per incident can also act as a driving force behind enforcing stricter rules and regulations so that employees adhere to security standards.

Cost per incident is a key metric that indicates the average cost of responding to and resolving a cyberattack, and is usually measured per incident. Cost per incident is calculated by adding up the expenses incurred by various teams, such as the security team, the IT support team, and network operators. These expenses are calculated by measuring the total time a security incident was open and by calculating the hourly costs of resources that were deployed to fix the issue. Cost per incident is also inclusive of new technology or external consultants that were engaged to combat the security incident. Here's a sample report that shows the average cost per incident for a few incidents based on business impact for the past year.



The report above shows the cost per incident for high-impact incidents is nearly twice or thrice as high as those with lower business impact.

## 5 Cyber risk assessment score

While technology simplifies your organization's operations, it also comes with numerous vulnerabilities that can be exploited by attackers. Practically every organization is at risk of a cyberattack. For this reason, it is critical to map vulnerabilities and the impact associated with them.

Organizations can better identify, resolve, and mitigate risks by frequently performing cyber risk assessments. The cyber risk assessment process enables you to prioritize vulnerabilities that, if compromised, have a greater impact on the business. Here's a risk heat map of an organization plotted using the cyber risk assessment score.



### Risk heat map

	Rare	Unlikely	Moderate	Likely	Almost certain
Severe	35	48	39	5	1
Major	144	208	101	69	61
Moderate	58	39	49	31	3
Minor	59	110	129	139	92
Insignificant	204	300	105	101	22

The risk heat map states that six security issues are severe and most likely to occur. By eliminating these severe security incidents, the organization will have fewer or no data breaches or compliance problems.

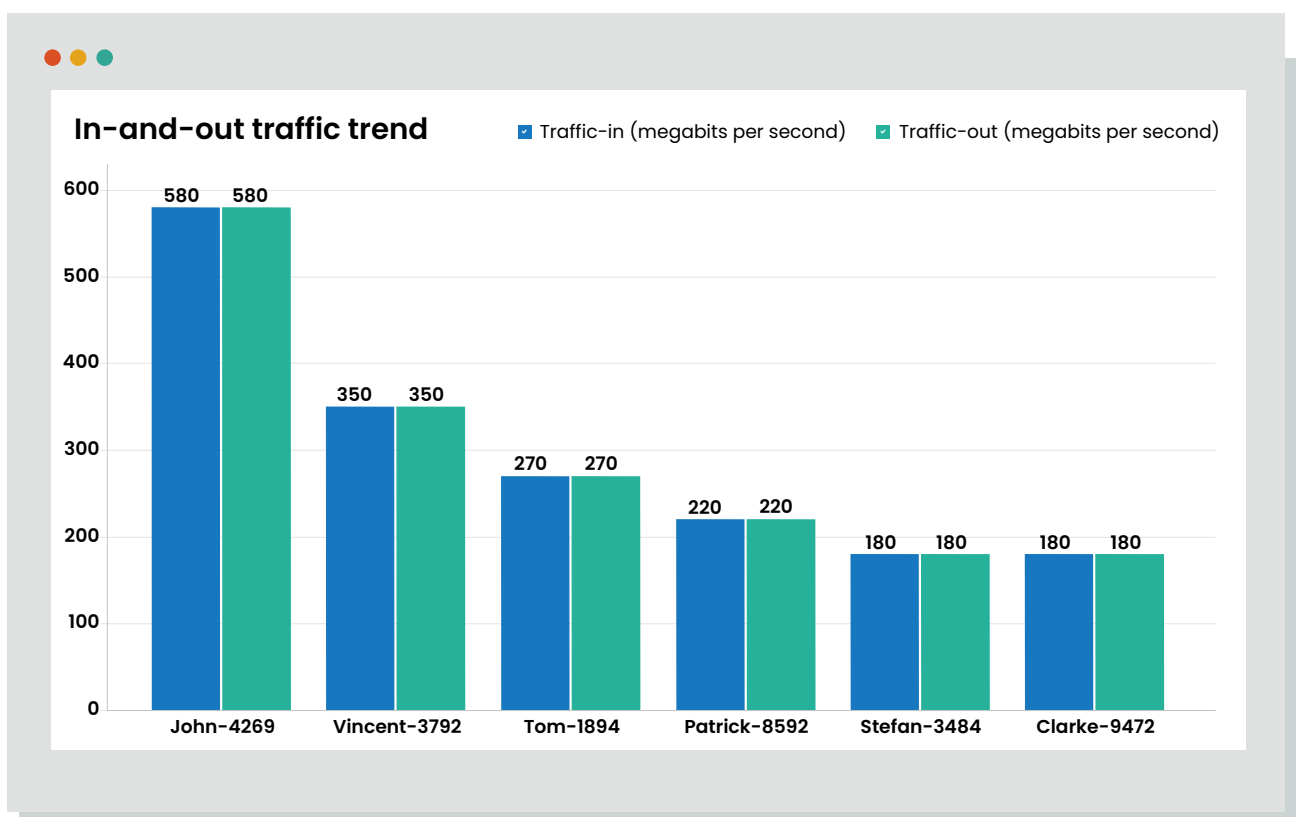
## 6

## Data movement via the corporate network

**N**etworks are the most critical and vulnerable part of an organization, and they are often the entry points for an attack. In 2020, attackers gained access to **130 private and corporate Twitter<sup>[3]</sup>** accounts in which 45 accounts were used to promote a Bitcoin scam. Dozens of popular accounts were also hacked.

Attackers who intend to steal data usually do so frequently and in small amounts, but never in one go. Measuring the volume of in-and-out traffic per minute can reveal how much data you lose, and further investigation will enable you to flag the reason behind this issue. Analyzing the volume of data and in-and-out traffic from a security perspective is a tedious task due to the varying work natures of different teams like marketing, sales, and DevOps. However, analyzing the in-and-out traffic of data for each department enables you to identify suspicious activities.

The report below shows the weekly trend of in-and-out traffic per minute in the admin department. The user (John) has slightly higher in-and-out traffic when compared to the rest of the team.



## **7** Intrusion attempts

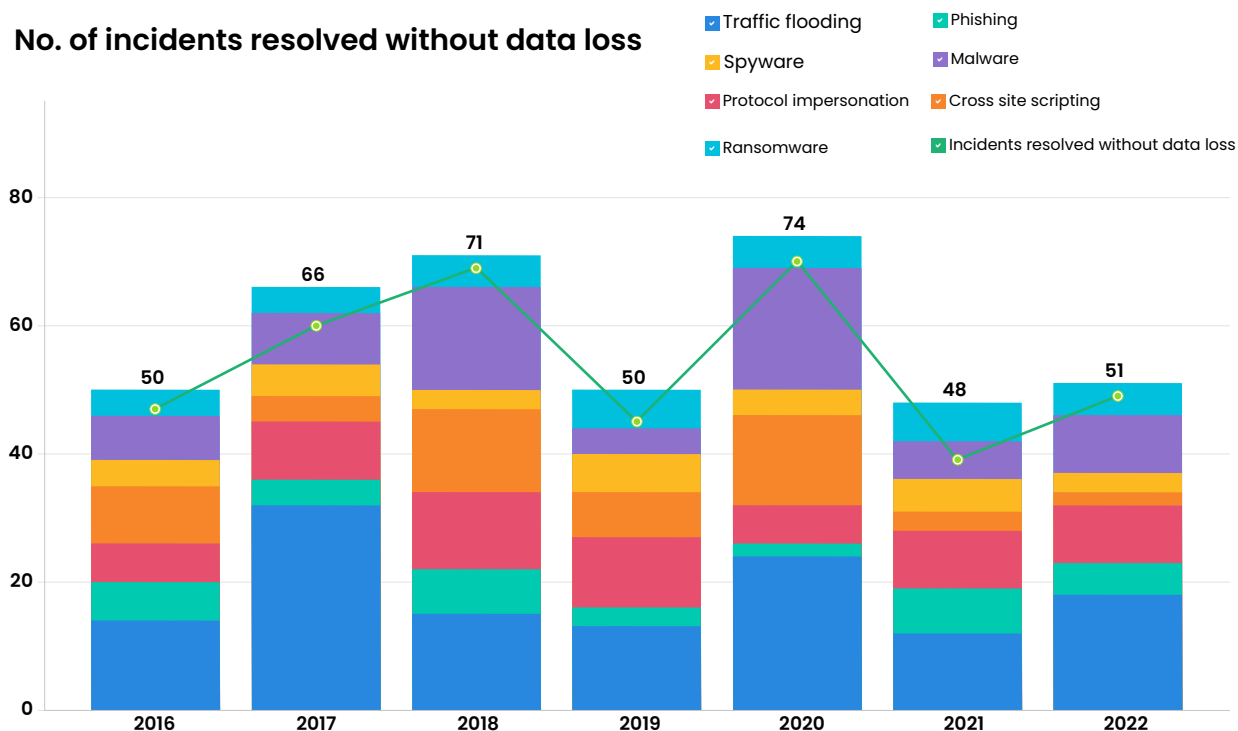
**N**o organization is immune to threats. Malicious insiders and cyberattackers seek vulnerabilities to infiltrate networks. Organizations should ensure that their networks are as resilient as possible against cyberattacks.

Network intrusions are caused by a few techniques, like traffic flooding that targets web servers, protocol impersonation, and cross-site scripting in which the attacker injects malicious content into the targeted organization's website. Intrusions always imperil the security of the network and its data, so it's critical to detect them to thwart potential attackers before they even attempt to access a network. Recently, IT organizations and online brands have been the common subjects of these attacks. Now, putting a positive spin on intrusions, past network intrusions should be considered as an opportunity to deal with a possible future attack effectively.

Keeping track of intrusion attempts in your organization will provide information about the different types of attacks witnessed in the past and the incidents that were resolved without data loss. Here's a sample report that shows the trend of attacks in the past.



### No. of incidents resolved without data loss



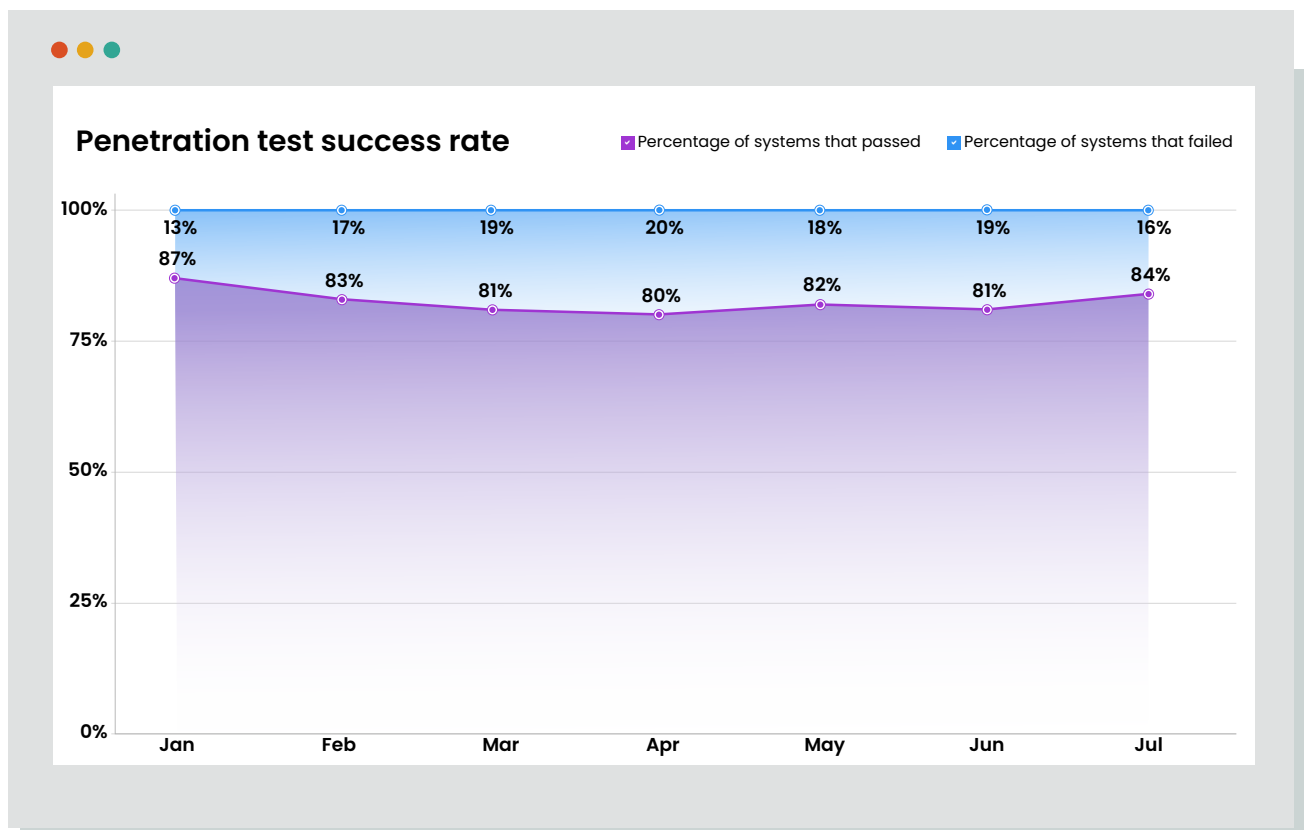
According to the report above, Zylker Corp. (a fictional organizational) resolved a high number of intrusions successfully. Interestingly, some common attacks such as traffic flooding, malware, and protocol impersonation seem like the most common attempts. This stresses the need for more thorough employee training, which can easily help reduce the number of such intrusions.

## 8

## Penetration success rate

Vulnerabilities and threats are increasing in tandem with the advancement of technology. Preparation, timely detection, and mitigation are the weapons organizations have to combat the menace of security threats. There are a few techniques, like penetration testing, that can mitigate the damage of a security incident by instantly detecting and resolving them.

Penetration testing, or pen testing, is a simulated attack the organization can perform frequently to check for any exploitable vulnerabilities. Manual penetration tests, run by a group of white-hat hackers, or automated tests, performed by software, are a few popular options for pen tests. The insights gathered from pen testing can be leveraged to fine-tune security policies and patch detected vulnerabilities. The sample report below illustrates the penetration test success rate.

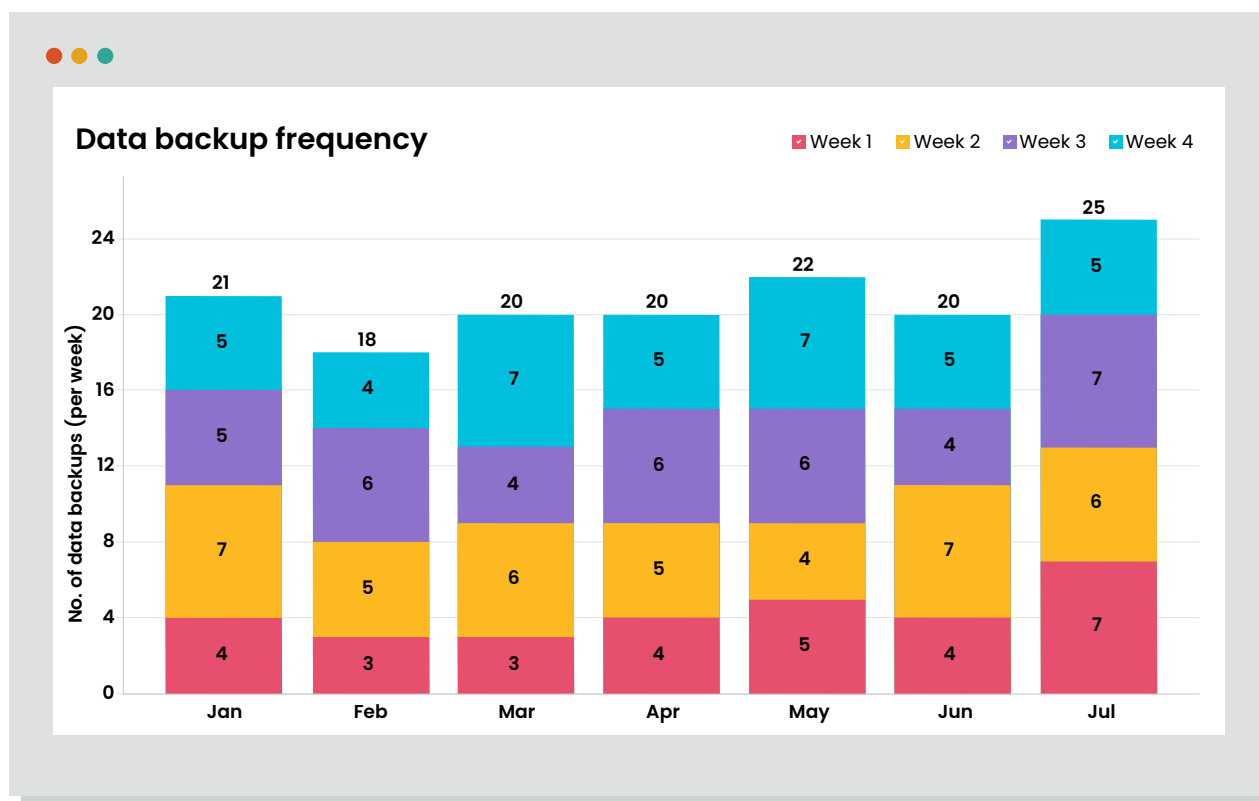


According to the report, 80% of systems have passed the penetration test. This calls for further tightening security protocols to ensure 100% pen testing clearance.

## 9 Data backup frequency per week

**H**ave you ever lost crucial data due to an incident? Or, have you ever felt a moment of panic where you thought you did? To lose critical data due to an incident or any other reason is unacceptable. That's where data backup comes in. Performed periodically, data backups can save you from costly data loss.

Backups are the reprieve you need to restore your data, regardless of the type of attack. Imagine data backup as a member of your incident recovery team. With data backup, you're one step ahead of attacks that result in data loss. Here's a sample report that illustrates the frequency of data backups.

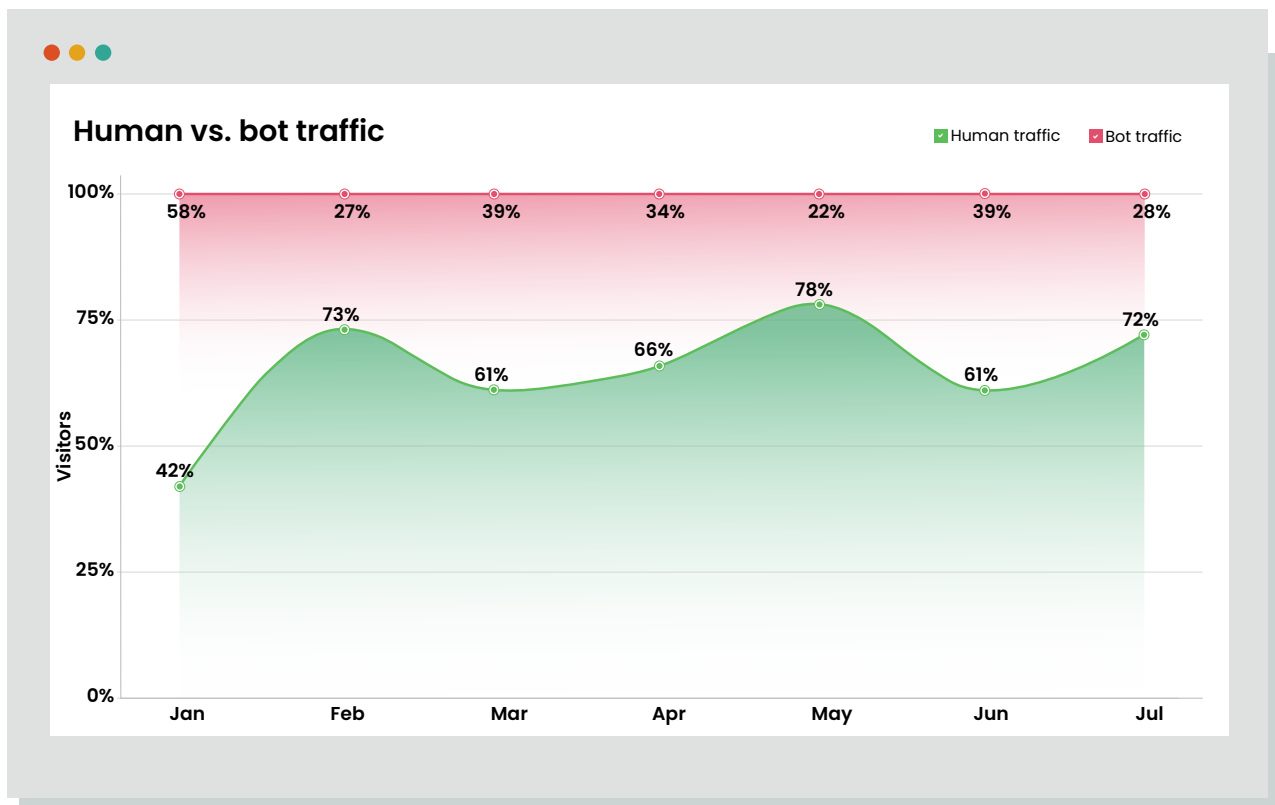


Setting up a routine for data backup requires a substantial amount of effort. However, it's a solid assurance for the security of your data.

## **10 Traffic analysis: The percentage of human and bot traffic to your websites**

**B**ot traffic has outpaced human traffic on the internet. Though you may see a steady flow of visitors to your website, a sizable chunk of that web traffic is compromised by bots, both safe and spam bots. Copyright bots, SEO tool crawlers, and other safe, automated bots are a few examples of safe bot traffic. However, there are also a rising number of harmful bots that use your website for nefarious purposes, such as spam bots and scrapers.

The current challenges in identifying malicious bots stem from the fact that the bots have become more sophisticated. However, keeping track of both human and bot traffic to your websites while taking into account these factors will be helpful; unusual rises in traffic, low time spent on the website, frequent visits from a specific IP address, high page views, and high bounce rates are all indicators of malicious bot traffic to your website. Here's a sample report that shows the split of traffic to a website.



The report concludes that overall traffic is higher when bot traffic is higher. This might be an indication of a pending attack. This calls for stringent security efforts and alerts for security teams when bot traffic surges beyond a fixed threshold.

## Conclusion

Cyberattackers are constantly looking for a flaw in the defenses of IT systems. To avoid falling prey to these attacks, you should not stop with just implementing the right tools and technology. You should also monitor the efficacy of cybersecurity in your organization. We hope that this e-book has highlighted some of the critical cybersecurity metrics that can help you measure the success of cybersecurity in your organization at a glance.

To learn more about the role of analytics in cybersecurity, check out some of our other resources.





# About

**ManageEngine Analytics Plus** is a self-service, AI-driven IT analytics solution that helps organizations implement complex initiatives that address requirements of expanding businesses. Analytics Plus visualizes IT data from several applications, and integrates out-of-the-box with several popular IT applications such as ServiceDesk Plus, Jira, Service Now, Zendesk, and Endpoint Central. Analytics Plus features an AI-powered analytics assistant that responds to voice and text prompts to provide meaningful visualizations. This eliminates the need for a data analyst to aid help desk managers, and reduces report building time while enabling organizations to make faster, data-driven decisions.

[Try Analytics Plus for free](#) to kickstart your IT analytics journey. Want to know more about the product before giving it a try?

[Sign up for a free virtual tour with one of our experts.](#)

**280K**  
customers  
across the world

**20+**  
years of IT  
management experience

**90+**  
products  
and free tools

**190+**  
countries  
served

## Reference

1. [https://www.varonis.com/blog/data-breach-statistics#:~:text=The%20average%20time%20to%20contain,of%20315%20days%20\(IBM\)](https://www.varonis.com/blog/data-breach-statistics#:~:text=The%20average%20time%20to%20contain,of%20315%20days%20(IBM))
2. [https://techcrunch.com/2016/02/29/snapchat-employee-data-leaks-out-following-phishing-attack/?guccounter=1&guce\\_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnNvbS8&guce\\_referrer\\_sig=AQAAAHw1VVAsFUksxLj8YWBNjD0DAiKoigBVWuxJprgN5ZJKuCShIsIKWRx-nbeXw6RtQ61Lsn4-U\\_h6Lpy\\_TVyGItoSaszZgGC-9fKMZkiF5Zuyalf53EQ6SJ1bNozbe-f2XF89sSm8kpRhWENjhoFgWJnUy5wf9Rcanx7zFirmHbd7](https://techcrunch.com/2016/02/29/snapchat-employee-data-leaks-out-following-phishing-attack/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnNvbS8&guce_referrer_sig=AQAAAHw1VVAsFUksxLj8YWBNjD0DAiKoigBVWuxJprgN5ZJKuCShIsIKWRx-nbeXw6RtQ61Lsn4-U_h6Lpy_TVyGItoSaszZgGC-9fKMZkiF5Zuyalf53EQ6SJ1bNozbe-f2XF89sSm8kpRhWENjhoFgWJnUy5wf9Rcanx7zFirmHbd7)
3. [https://en.wikipedia.org/wiki/2020\\_Twitter\\_account\\_hijacking](https://en.wikipedia.org/wiki/2020_Twitter_account_hijacking)