ManageEngine
Log360

CISO HANDBOOK

CYBERSECURITY METRICS, BUDGETING, AND LEADERSHIP

By Varun K and Hiranmayi Krishnan

LEARN HOW TO

- Track key metrics to gauge security effectiveness
- Build an effective cybersecurity budgeting strategy
- Transition from security leaders to business leaders

Table of Contents

Introduction	1
CISOs transition to business leaders	2
Key performance metrics that CISOs should track	4
Building an effective budgeting strategy	11
• What to watch for while planning the budget	12
What determines the success of a CISO?	13
Does having a CISO make sense for a startup?	14
About the authors	16
References	17

Introduction

Gone are the days of organizations focusing only on compliance. In today's world, organizations—even governments—have understood the need for, and shifted their focus to cybersecurity risk and posture management. A prime example of this is the Singapore government's adoption of the Zero Trust model.

The new normal of the hybrid work model brought with it a host of security challenges. IT security teams had to quickly devise complex strategies to overcome them. Spearheading their efforts to ensure business continuity and their organization's cybersecurity were the chief information security officers (CISOs).

CISOs are the backbone behind the security infrastructure of organizations. They're pivotal for balancing an organization's security budget and security needs, including the need for skilled cybersecurity personnel. They are now needed more than ever because studies suggests that:

- Businesses are estimated to lose approximately $10.5 trillion in 2025 due to cybercrime.[1] This drives the need for leadership that focuses on business risk-based security KPIs at a macro level.

- Cybersecurity spending is projected to exceed $188 billion in 2023.[2] Such large investments in cybersecurity necessitates an acceptable return on investment, and CISOs are typically directly responsible for this.

- 70% of organizations have reported a shortage of personnel in their security team, and 94% of security teams report being impacted by these talent shortages.[3] Tackling this requires strategic recruitment, and the nurture of internal talent.

To stay ahead of these challenges, CISOs should acquire and apportion their cybersecurity budget optimally. They should identify and deploy the right cybersecurity solutions, implement industry best practices, and track the right metrics to effectively elevate their cybersecurity posture.

This e-book covers:

- How CISOs have transitioned from security leaders to business leaders
- Which key performance metrics CISOs should track
- How to build an effective security budgeting strategy
- How to determine the success of a CISO
- How startups can benefit from having a CISO

CISOs transition to business leaders

CISOs are no longer confined to the role of security leaders. The participation of CISOs in board meetings has become a growing trend, as data security is increasingly considered a business critical risk. Though CISOs work on protecting organizations from new, unknown threats daily, their expertise extends beyond overseeing how security teams manage and mitigate security incidents. They are increasingly consulted for decision-making in areas such as technology investments, handling of customer data, data privacy, workforce expansion, and recruitment. CISOs are undoubtedly seen as business leaders rather than just technologists.

Below are some top operational areas that CISOs oversee (see Figure 1). Their involvement levels may vary depending on their organization's size, industry, and security maturity.[4]

Figure 1: Top operational areas that CISOs oversee

Security operations center

CISOs manage a tireless group of analysts constantly working on anomaly detection, threat mitigation, and incident management.

Third-party security risk management

CISOs oversee the digital risks, personally identifiable information, and privacy concerns associated with vendors and third-party organizations.

Product security

CISOs ensure security through design. Besides the company's security architecture, CISOs also help create impenetrable products by significantly influencing the development of secure software.

Pen testing and red teaming

CISOs often have direct responsibility for penetration testing and red teaming exercises that continuously test and bolster the organization's security posture.

Compliance regulations

CISOs oversee the legal ramifications of breaches, including the impact of privacy concerns, and maintain compliance with government and other cybersecurity regulations.

Disaster recovery planning

A successful data breach can halt business operations, damage the organization's reputation, and incur regulatory penalties. A crucial responsibility of CISOs is disaster recovery planning, which involves the strategy to reduce the impact of the data breach or cyberattack, and enable business continuity.

To deliver these functions and to ensure the organization's holistic security, CISOs should track certain key performance indicators.

Key performance metrics that CISOs should track

CISOs should track certain metrics to gauge the efficiency of their SOC, and to see how effectively they've achieved their goals. Doing so can help them see how the security function has progressed in each of the metrics over time. Metrics will also help CISOs benchmark against industry standards and understand critical areas of improvement.[5]

Let's now look at the 13 metrics that a CISO should track.

1

Incident rate

The incident rate indicates the number of security incidents that have occurred over a specific time period. CISOs should track incidents that were successfully mitigated and those that weren't. From this, they'll gain insights into how effective their security solution is and how frequently bad actors target their organization.

CISOs should track:

- The number of incidents in which attackers had successfully breached the network.
- The number of incidents in which attackers attempted to breach the network but failed.

By tracking these on a regular basis, they'll get a fair idea of the number of possible breaches they can expect quarter-to-quarter.

This will undoubtedly help CISOs during budget meetings with the board. When incident rate trends are presented along with the findings of breach likelihood, cost, and risk, the board will understand the extent of threats aimed at their organization. They'll be more inclined to renew or increase their cybersecurity investment following the review of this crucial data.

2

Breach likelihood

Breach likelihood tells CISOs how likely they are to suffer a breach if the current attack trend continues. While incident rates are metrics measured after the fact, breach likelihood is a metric that denotes the possible number of security incidents that organizations are likely to face, taking into account their risks and the security controls in place.

To that effect, CISOs should consider the total number of incidents (both successful and failed breach attempts), and third-party risk assessment scores. They should also use the insights inferred from their UEBA solution (possessing peer group analysis and seasonality capabilities) to determine the organizational risk and department-wise risk. CISOs can then use predictive modeling and analytics to determine the likelihood of breaches and project how much it would cost the company if the predictions were to come true.

3

Cost per incident

Data breaches cost organizations their reputation and money. The average cost of a data breach is $4.35 million, according to IBM's Cost of a Data Breach Report 2022.[6] By measuring the cost per incident (sometimes referred to as breach impact), CISOs can determine the true impact of breaches on business, and can compare and identify how much higher or lower their costs are when compared to industry standards.

4

Risk exposure

Risk exposure is the product of breach likelihood and breach impact.

Risk exposure = Breach likelihood * Breach impact

Tracking this helps CISOs strengthen their organizations' defenses against risks. CISOs can only secure their organization when they know what threats they're exposed to. Measuring risk exposure is a good way to calibrate the source and degree of threats. It also helps CISOs obtain budget approvals from the board to prevent these risks from becoming security incidents.

5

Severity level of breach

The severity of a breach indicates its magnitude and the level of its devastation. For every security breach, the CISO should track its severity. One way to do this is to use a scale of 1-5 (with "5" being the highest). The measure of breach severity can be qualitative or quantitative, depending upon constraints faced by the CISO. Tracking breach severity shows CISOs the true reflection of their security posture, because an organization with an effective security team and solution will have a minimal number of severe breaches.

6

Mean time to detect (MTTD)

The MTTD tells CISOs how long it has taken their security team to detect a breach. Organizations should aim to minimize the MTTD because the faster the detection, the less time an attacker remains unchallenged in the network, and the quicker the threat mitigation.

7

Mean time to respond, recover, and resolve (MTTR)

MTTR could mean any of the following depending on how an organization chooses to define the term. The CISO should be tracking all of them.

- *Mean time to respond:* This refers to the average time taken by the organization to return to its operational condition following a breach notification.
- *Mean time to recover:* This refers to the average time taken by an organization to fully recover from a security incident.
- *Mean time to resolve:* This refers to the average time taken to resolve an incident completely. This includes the time spent detecting the threat, eradicating it, and preventing it from recurring.

8

Mean time to patch (MTTP)

The MTTP is also referred to as the vulnerability patch response time. This indicates how quickly the security team implements patches to software and applications in devices once they discover vulnerabilities. CISOs should ensure that there's minimal delay between a patch release and its implementation. To accomplish this, they should start by tracking the number of unpatched devices using vulnerability scanners.

9

Level of security maturity

CISOs need to know how prepared their security team is to defend against cyberattacks. They can test and assess their organization's security maturity with the help of proactive approaches such as pen testing (or ethical hacking), red teaming, and cyberwar gaming. Ethical hackers perform pen testing to identify security vulnerabilities in a system or an application, whereas in red teaming, a dedicated group of individuals, either in-house or outsourced, operate with the explicit permission of C-suite executives to infiltrate the organization.

On the other hand, facilitators (either CISOs or external war game experts), conduct cyberwar games to test and improve the incident response and security preparedness of an organization.

CISOs should determine which approach will best meet their organization's current needs and accommodate their future security requirements.[7] They can then rate themselves as low, medium, or high based on the findings to identify their level of security maturity.

Alternatively, CISOs can use a cybersecurity framework such as the Essential Eight to identify where their organization's security maturity level lies. According to the Essential Eight Maturity Model, organizations can classify themselves into various maturity levels based on the risks posed by cyberattackers likely to attack them, and the techniques or trade craft used by them to carry out an attack.[8] Figure 2 will give CISOs an idea as to how this model helps organizations identify their security maturity level.

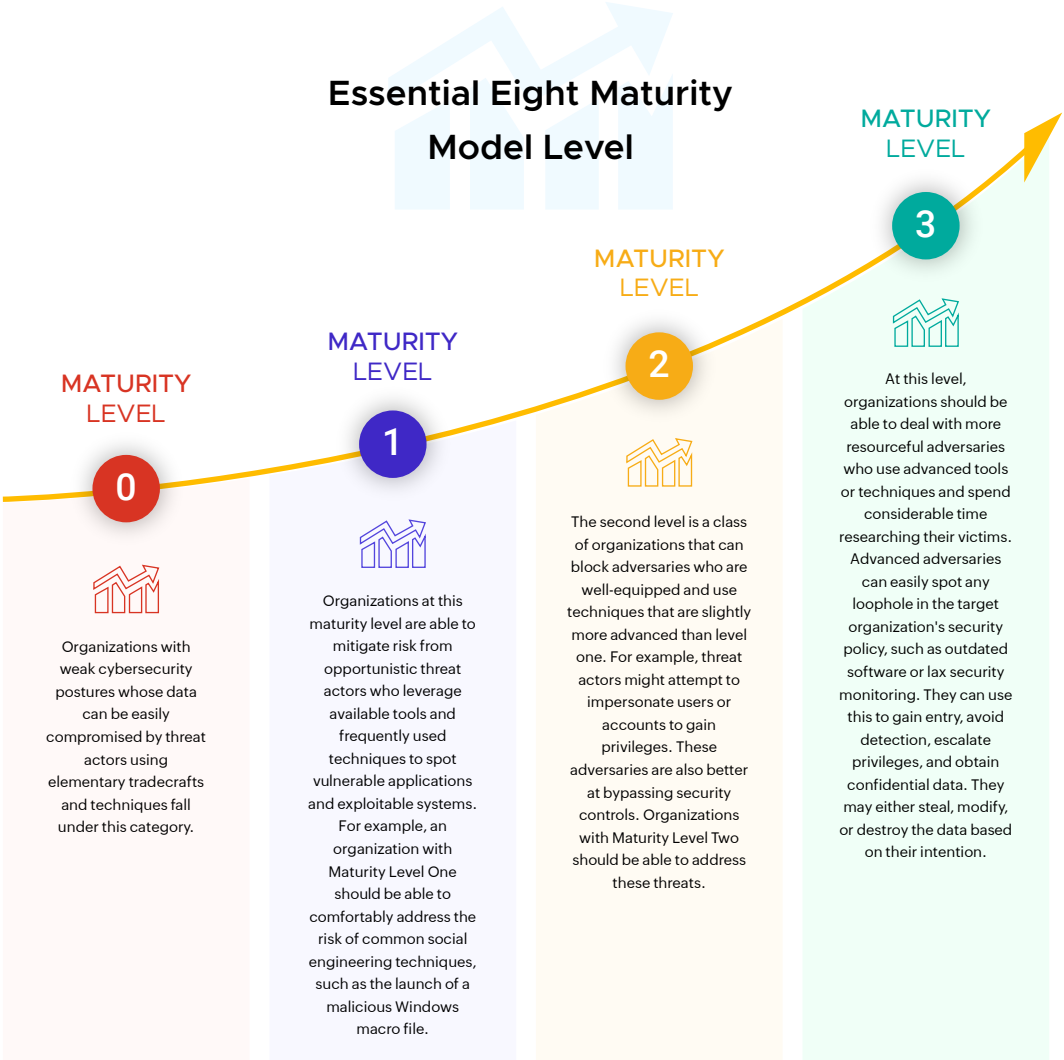


Figure 2: Essential Eight Maturity Model

10

Percentage of users not using multi-factor authentication

Threat actors often use compromised credentials to gain entry into a network. Organizations which encourage the use of MFA are less likely to face an attack due to compromised credentials since attackers can no longer gain access with only the password.

CISOs should track users who aren't using MFA, and should ensure that they start adopting MFA as a part of their normal logon routine. This should be reflected when tracking this metric month-to-month. CISOs can look into their Active Directory to identify the MFA status of users.

Percentage of users not using MFA = (Number of users with MFA status as disabled/Total number of users in the organization) * 100

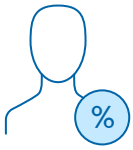
CISOs should work towards bringing down this percentage significantly.

11

Frequency of backup

In 2022, the average cost of a ransomware attack—not including the cost of the ransom itself—was $4.54 million.[9] Ransomware attacks are terrifying because organizations might still not gain access to their original data as attackers could manipulate the data, or fail to give the decryption key even if organizations pay the ransom. It's imperative for organizations to have backups to verify the authenticity of their data. If a CISO ensures that the security team backs up the data frequently, then they might even get away without having to pay the ransom.

12



Percentage of watchlisted users

Watchlisted users refers to the riskiest users. For example, employees usually work within a specific timeframe, say, 9am to 6pm. But it is wise to add them as watchlisted users if they demonstrate work-related activity round the clock, or if they indicate increased activity outside their usual work hours. Similarly, it is wise to closely monitor users who are connected to many or key assets. CISOs also should be vigilant in tracking the number of watchlisted users as an unexplained increase indicates a potential insider attack.

Percentage of watchlisted users = (Total number of watchlisted users/Total number of users in the organization) * 100

Tracking this can help CISOs identify if there's a sizable difference in their riskiest users quarter-to-quarter.

13

Return on investment

CISOs need to guide the board to make security investments based on their organization's security goals and risk appetite. Only then will they observe a positive ROI. For example, an organization that invests in a suitable backup solution could save the company millions of dollars just by avoiding the payment of ransom. A CISO's ability to convince the board about its security ROI will determine the organization's immediate and future security investments. So, it's important for CISOs to track their security spending and ROI metrics.

The table below summarizes the key metrics that CISOs should track and what insights they'll gain from them.

Metrics	Key takeaways
Incident rate	• Are the number of incidents reducing month-to-month? If so, how much? • Tracking this will help CISOs measure the effectiveness of their detection technologies such as SIEM.
Breach likelihood	• What's the probability of a breach taking into account their current security controls in place? • What would be the breach impact if the estimated number of likely breaches were to occur?
Cost per incident	• What is the total cost associated with a security incident in their organization? • Is it greater or lesser than the industry standards? This will tell CISOs if they're on the right track or if they need a course correction to reduce the costs.
Risk exposure	• What's the status of their risk exposure taking into account breach likelihood and impact? • Tracking these can help CISOs achieve budget approvals, and prevent undesirable attacks.
Severity level of a breach	• On a scale of 1-5, how severe are the breaches? • How many breaches exceed level 3? • Tracking these will give CISOs a true reflection of their organization's security posture.

MTTD	• How quickly is the security team detecting threats? • Can the organization reduce its MTTD by investing in a SIEM solution to foil cyberattacks swiftly? • If the organization already has a SIEM solution, has its MTTD improved?
MTTR	• What's the average time to respond, recover, and fully resolve a security incident? • Tracking this can help CISOs identify if their MTTR is getting better with time. This will reflect the performance of their team *and* their SIEM solution.
MTTP	• How quickly is the security team implementing patches to vulnerable software and applications? • The quicker they are, the fewer the incidents CISOs will have to worry about.
Level of security maturity	• CISOs should use cybersecurity frameworks to determine their organization's security maturity level. • Identifying this can help them develop a plan to elevate their security maturity to a higher level.
Percentage of users not using MFA	• How many users are not using MFA? • Is this number decreasing month-to-month? • Tracking this can help organizations prevent cyberattacks.
Frequency of backup	• How frequently do the organizations backup their data? • If an attack were to occur tomorrow, what would be the extent of its impact on their business? • How soon will they be able to resume operations?
Percentage of watchlisted users	• CISOs should know how many risky users are there in their organization and who they are. • Is there a decrease in this percentage month-to-month? If an employee were to attempt an insider attack, would their SIEM solution be able to identify and thwart it in real time?
ROI	• Is the CISO observing a positive ROI from their security spending? • Tracking this will positively impact their board's future security budget approvals.

Needless to say, tracking these metrics can help CISOs communicate clearly with the board. Providing insights on key metrics can help CISOs obtain the necessary budget funding and help them decide how to utilize the budget efficiently. Security budgeting involves both capital expenditure and operational expenses, and it has to be carefully planned with the future in mind.

Building an effective budgeting strategy

Not all security budgets are the same. The obligation falls on CISOs to meet the security needs of their organization within the budget allocated by the board. Irrespective of how modest or large the organization's security budget is, here are some essentials to consider before allocating monetary resources.[10]

Dedicate a percentage of their budget to network security

Organizations gain and lose employees on a daily basis. So, gaining complete visibility into their network and users in real time should be a CISO's top priority. If an organization doesn't scale up its security posture with changing times and growing employees, it could spell disaster. CISOs can thwart security threats by upgrading their organization's network security, and assigning a portion of the budget to that process.

Invest in endpoint protection

Endpoint devices, a key component of an organization's network, are increasingly exploited. This is why CISOs should focus on upgrading their endpoint protection. Investments in endpoint security should include firewall and antivirus upgrades. CISOs should also invest in a unified SIEM solution that can read telemetry from across the organization's endpoint devices for real-time monitoring.

Allocate a budget for data storage

Every organization's data is a risk magnet, and is the main reason for CISOs to invest in security. CISOs should figure out how much data they're going to store on-premises, and in the cloud by conducting research, and price comparisons. The costs differ depending on the type of storage.

Set aside funds for disaster recovery

Having real-world business experience, CISOs know that no matter how hard they try, their security plan isn't going to be foolproof. It's imperative they have a backup fund that is only used for security incidents.

Invest in employee training for security awareness

A CISO's security strategy is only successful if the users on their network are aware of security procedures, and know what actions can compromise the network. While security training might not involve excessive expenditures, it's good to earmark a percentage of the budget for training. Some organizations have started investing in microtraining options to enhance employee security awareness. These dynamic training methods provide feedback to users who perform any activity considered suspicious. A short video or a screen pop-up provides feedback. Microtraining provides employees with learning based on risky situations so they become more aware of their specific behaviors that could compromise security in the organization.

What to watch for while planning the budget

Risks that arise out of geopolitical tensions

State-sponsored cyberattacks have been on the rise and the Russia-Ukraine war is proof. Nation-states often hire attackers to infect critical infrastructure with malware. If their organization deals with government-related critical utilities, a CISO needs to ensure they have security controls in place to prevent a geopolitical attack.

Increasing cyber insurance costs

Since many organizations are aware that they will eventually suffer from a breach, they've begun to invest in cyber insurance. Cyber insurance premiums are increasing as policies become more complex and comprehensive. Rates are often determined based on the effectiveness of an organization's security measures, so one way to reduce premium costs is to ensure their CISO have put better controls in place.

The costs of compliance

The costs to adhere to compliance mandates often increase as they change. However, if organizations focus on implementing and maintaining effective security strategies with fine-tuned security controls, compliance to most mandates is automatic. In the long run, even if CISOs invest more to adhere to regulatory measures, this offsets the costs they might incur from penalties and reputational damage.

CISOs should keep these points in mind as they strategize their security expenditures, regardless of the size of their budget. Our next section talks about the criteria used to weigh and assess the long term success of a CISO.

What determines the success of a CISO?

In addition to short-term KPIs, including the MTTD, the various forms of MTTR, the number of incidents mitigated, and breach costs, the success of a CISO also depends on certain accomplishments, such as:

Cybersecurity framework development

Have the CISOs developed and established a successful cybersecurity management program that aligns with their organization's strategic vision? Have they revamped organizational policies and built appropriate teams and processes?

Cybersecurity culture cultivation

Have the CISOs cultivated a strong cybersecurity environment where managers and end users are well-trained and aware of digital risks? Did they conduct innovative employee training, workshops, benchmarking, and periodic assessments to develop a more mature cybersecurity culture?

Stakeholder management

How effectively have the CISOs liaised with security vendors and business partners? How favorable were the outcomes? How effective were they in balancing their organization's business vision and security goals?

Security budgeting

How much budget have they managed so far in their tenure as a CISO? Have they delivered a positive return on investment; if so how much? How skillful are they in evaluating vendors and negotiating contracts with them?

Global exposure

How effectively are they managing large, distributed teams across geographies? A successful CISO is not confined by their organization's security needs. They stay up to date with global trends and practices in cybersecurity, and implement them effectively.[11]

According to Marlin Hawk's Global Snapshot: The CISO in 2021 report, 53% of CISOs have been in their roles for two years or less, and 64% were hired from another organization.[12] In most cases, a breach at an organization can be the result of the previous CISO. It is vital to give a new CISO time and to measure the organization's security success over the long term.

When it comes to SMBs and startups, many security specialists are accomplishing the duties of a CISO without having the title. Hiring a CISO for the first time can be a challenge. New organizations often wonder if they need a CISO during their growth stage. Many believe they only need one when their organization is large enough.

Does having a CISO make sense for a startup?

Startups tend to obsess with growth and nothing else. However, placing cybersecurity on the back burner in the hopes of putting out fires as they happen can be harmful. Startups can't limit themselves to responding to and mitigating security incidents; they must have a strong security culture, an impenetrable product architecture, and proper business recovery plans.

Remarkably, some startups, like those in the payment platform space, handle more sensitive data than big businesses. What's more, large corporations often depend on startup products for their crucial business activities, and vice versa. Woven into the fabric of the overall business ecosystem are SMBs and startups. And everybody is vulnerable to cyberattacks, which can have downstream effects that can reach their business partners and customers.

Here are some startup characteristics that highlight why they need a CISO:

A CISO can help increase the security maturity

Attackers often believe that startups lack a CISO and take security for granted, assuming no security strategy and risk or recovery planning is in place. The expertise of a CISO can help a startup develop better security maturity and mitigate these attacks. This includes building from scratch and managing a tailored, scalable security program by putting in place the necessary security policy and controls, and deploying the right security solutions for network visibility, detection, and response.

A CISO can help design secure software development practices

A startup's core competency is its products, and a crucial growth indicator is client retention. An attacker may exploit a susceptible program or insecure code, and compromise devices and steal data. CISOs play a crucial part in providing knowledgeable guidance on creating solutions that are secure by design.

Imagine a breach due to a vulnerable code in the product, which could be detrimental to customer retention and also future funding prospects. Startups can benefit significantly from a secure product design, especially in their nascent stage. Product security is a question of reputation, which is difficult to regain once lost.

CISOs help manage risks with multiple third-party vendors

Startups tend to employ third-party solutions for their business needs, such as cloud service providers, email and chat applications. While this offers flexibility and agility, monitoring these third-party solutions for security risks and their handling of sensitive data is crucial. Think of supply-chain attacks where an attacker infiltrates an organization's network through a partner or vendor having access to their systems and data. Finding the best fit that aligns with their organization's security needs among hundreds of providers is a vital KPI for a CISO.

CISOs are advisors to drive a security roadmap

Startups and SMBs seek advice on the current security landscape and develop a robust risk management program for the future. The recent pandemic, for example, left many startups scrambling to adapt to remote work and newer cyberthreats. With a CISO in place, focused leadership can oversee the course of action and build a roadmap for future resilience.[13]

After all, startups and SMBs often grow to become enterprises eventually. While they might not initially be a popular target to attackers, like huge enterprises, they shouldn't make themselves easier targets.

Regardless of the organization's size, consulting a CISO only after a severe incident or breach can be detrimental. A solid security plan that is methodically built from the ground up is vital.

About the authors

Varun K

Varun currently works as a product marketing specialist for IT security solutions at ManageEngine, the IT management division of Zoho Corporation. He has authored various blogs on the latest trends in cybersecurity. His favorite themes include SIEM, cloud security, and security orchestration, automation, and response (SOAR).

Hiranmayi Krishnan

Hiranmayi is a cybersecurity enthusiast who works at ManageEngine. She is an avid blogger of the latest trends in cybersecurity, and her main areas of interest are UEBA, and incident management through SOAR.

About ManageEngine Log360

ManageEngine Log360, a unified SIEM solution with integrated DLP and CASB capabilities, helps organizations thwart attacks, monitor security events, and comply with regulatory mandates. The solution comes bundled with a log management component that provides better visibility into network activity, an incident management module that helps quickly detect, analyze, prioritize, and resolve security incidents, an ML-driven UEBA add-on that baselines normal user behaviors, and spots anomalous user activities, and a threat intelligence platform that leverages dynamic threat feeds for security monitoring and helps enterprises stay on top of attacks.

For more information about Log360, visit manageengine.com/log-management

To explore the security benefits of Log360

Personalized demo Download

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus
Exchange Reporter Plus | M365 Manager Plus

References

1. Fox, Jacob. "Cybersecurity Statistics for 2023." *Cobalt* (blog). Dec 27, 2022. Accessed Jan, 2023. https://www.cobalt.io/blog/cybersecurity-statistics-2023

2. Ibid.

3. Ibid.

4. K, Varun. "Criteria to measure CISO success." *ManageEngine Expert Talks* (blog). Dec 7, 2022. Accessed Jan, 2023. https://www.manageengine.com/log-management/cyber-security/criteria-to-ciso-job-success.html

5. Krishnan, Hiranmayi. "13 key performance metrics that CISOs should track." *ManageEngine Expert Talks* (blog). Jan 4, 2023. Accessed Jan, 2023. https://www.manageengine.com/log-management/cyber-security/key-metrics-cisos-should-track.html

6. IBM. "Cost of a Data Breach Report 2022", 5-6. Accessed Jan, 2023. https://www.ibm.com/downloads/cas/3R8N1DZJ

7. Krishnan, Hiranmayi. "How to proactively secure your organization against cyberattacks." *ManageEngine Expert Talks* (blog). Dec 7, 2022. Accessed Jan, 2023. https://www.manageengine.com/log-management/cyber-security/how-to-proactively-secure-your-organization-against-cyberattacks.html

8. A, Anupama. *Essential Eight Explained*. 2022. Accessed Jan, 2023. https://download.manageengine.com/log-management/manageengine-log360-essential-eight-explained.pdf

9. IBM. "Cost of a Data Breach Report 2022", 6.

10. Austin, Tanya. "How to define an effective cybersecurity budget for 2023." *ManageEngine Expert Talks* (blog). Dec 12, 2022. Accessed Jan, 2023. https://www.manageengine.com/log-management/cyber-security/how-to-define-an-effective-cybersecurity-budget-for-2023.html

11. K, Varun. "Criteria to measure CISO success," blog.

12. Hawk, Marlin. "Global Snapshot: The CISO in 2021." Accessed Jan 2023. https://www.marlinhawk.com/docs/Marlin-Hawk-Report-Global-CISO-2021.pdf

13. K, Varun. "Do startups need a CISO?" *ManageEngine Expert Talks* (blog). Dec 26, 2022. Accessed Jan, 2023. https://www.manageengine.com/log-management/cyber-security/ciso-job-startup.html