CYBER SECURITY TRENDS INSIGHT REPORT

2022

trillium Information Security Systems

INSTITUTUM DE EXCELLENTIA

TABLE OF CONTENTS

INTRODUCTION

Each year Trillium Information Security Systems (TISS) publishes industry insight reports which focus on uncovering, discovering and understanding trends, insights and challenges faced by organizations and cybersecurity leaders in Pakistan. Since Pakistan specific data is unavailable in security surveys conducted across the globe, our aim for the Trend Insights Report is to fill this gap. We hope that through this effort, the Pakistani cybersecurity industry, community, and cybersecurity leaders will benefit from meaningful local data and insights. TISS remains committed to serving the cybersecurity community thus, through this effort which is now in its 4th year, we bring Pakistan specific data to the cybersecurity community to help provide cybersecurity teams and leaders with situational awareness to plan and strategize better.

In this report, we have surveyed more than 100 Senior Cybersecurity Leaders in Pakistan, at 100 different small-large scale organizations, that have between 200 to 10,000 employees. Our focus was to gain insights into what challenges and threats they faced in year 2021 and using the Predict, Prevent, Detect, Respond Framework what technologies these organizations require in order to build their cybersecurity programs and strategies.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

STARTING NOTES FROM CYBER SECURITY LEADERS

JAWAD KHALID MIRZA

CHIEF INFORMATION SECURITY OFFICER
ASKARI BANK LTD.

TISS take excellent initiative in 2021 to launch Trend Insight Report reviewing cyber challenges faced by Cyber Security industry in Pakistan.

Pakistan has the highest tele density 75% in the region and the cheapest rates for radio internet to have ever been offered, and due to this factor Pakistan has a large internet users' base, an increasing digitized security apparatus as well as banking system, which depend on internet connectivity. Pakistan has also incorporated laws to tackle threat emanating from cyber- attacks, which do not seem to cover the threats in depth and wholeness. As threats evolve and come from varied foes and adversaries, we must continuously assess them and make necessary modification and rectifications in our strategy.

Obviously, security surveys are important especially in Pakistan where such kind of centralized intelligence or industrial practices data is not available; it will help organizations and security leaders for analysis of current cyber attack patterns in emerging technologies, top cyber threats and controls which are using in cyber industry. These kinds of surveys enable us to keep up to date with industrial best practices.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

STARTING NOTES FROM CYBER SECURITY LEADERS

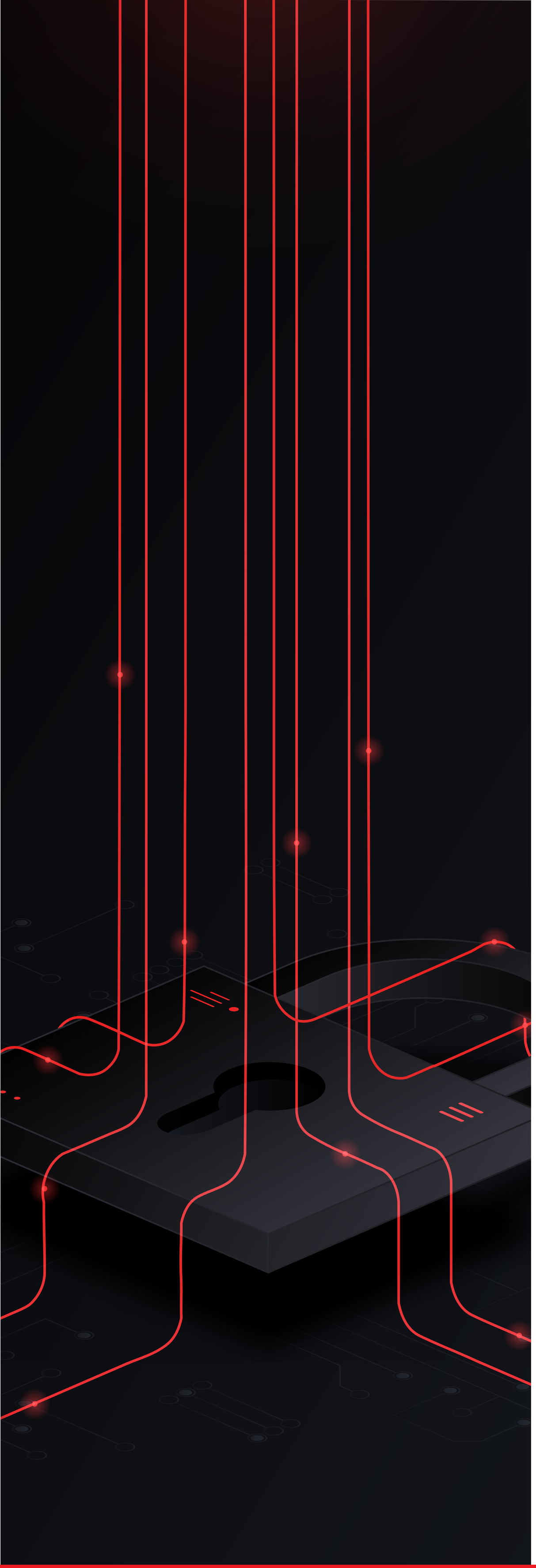
SHUMAILA HAMEED

GM SECURITY OPERATIONS CENTER

PTCL

PTCL Group is working with TISS since a decade now on various fronts i.e. Endpoint Protection Platforms, SIEM services and Penetration testing. Working with TISS on different projects has given us good insight and knowledge to their capabilities and skills. Trends Insight Report is an excellent opportunity provided by TISS to share the experience and challenges relevant to cybersecurity within Pakistan. No organization, big or small, is immune from a devastating effects of cyber attack as they have become more sophisticated, illusive, and targeted than ever before. Today's hyper-connected world creates more opportunities for cybercriminals, and every IT environment is a potential target: on-premise networks, cloud, mobile, and IoT devices. But forewarned is forearmed hence organizations need to adopt proactive measures to stay ahead of cyber activities, not merely detect and remediate them. Relying on remediation can have devastating consequences to any organization, as once the malware was able to penetrate an IT surrounding – in many occasions this means infection that will spread in seconds and will be merely impossible to get rid of. Organizations today should assume that they will eventually be compromised at some point. Even if an organization is equipped with the most comprehensive, state-of-the-art security products, the risk of being breached cannot be eliminated. Detecting and automatically blocking the attack at an early stage can prevent damage. To win the cyber security battle, companies need strong threat intelligence, threat prevention technology, and a consolidated security architecture that protects all attack vectors.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.



REPORT HIGHLIGHTS

This year's survey results reveal 5 key points that we believe may be particularly important for organizations to know:

1. It's worth noting that for most of the organizations cyber security budget increased on average between 5% to 10%.

2. The survey identified that 39% of organizations have in-house cyber-security operations services. The percentage for out-sourced cybersecurity services was limited to 5% only.

3. In 2021, phishing was responsible for more than 50% of reported security incidents.

4. 49% of the survey participants are dealing with social engineering and phishing attack tactics due to lack of security awareness trainings.

5. The most in-demand technologies in 2021 were:

- Cyber Threat Intelligence
- Security Information and Event Management (SIEM)
- Vulnerability Management Tools
- Database Activity Monitoring (DAM)
- Endpoint Detection and Response (EDR)

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

SURVEY

INSIGHTS

Disclaimer:

For questions that use multiple select options, the total number of answer choices selected for a question is greater than the number of respondents that answered the question. This has caused the total response percentages to exceed 100%.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

01

CAN YOU DESCRIBE YEAR-TO-YEAR SPENDING IN TERMS OF YOUR INFORMATION SECURITY BUDGET?

DECREASED FROM

5% to 10%

INCREASED FROM

5% to 10%

INCREASED MORE THAN

10%

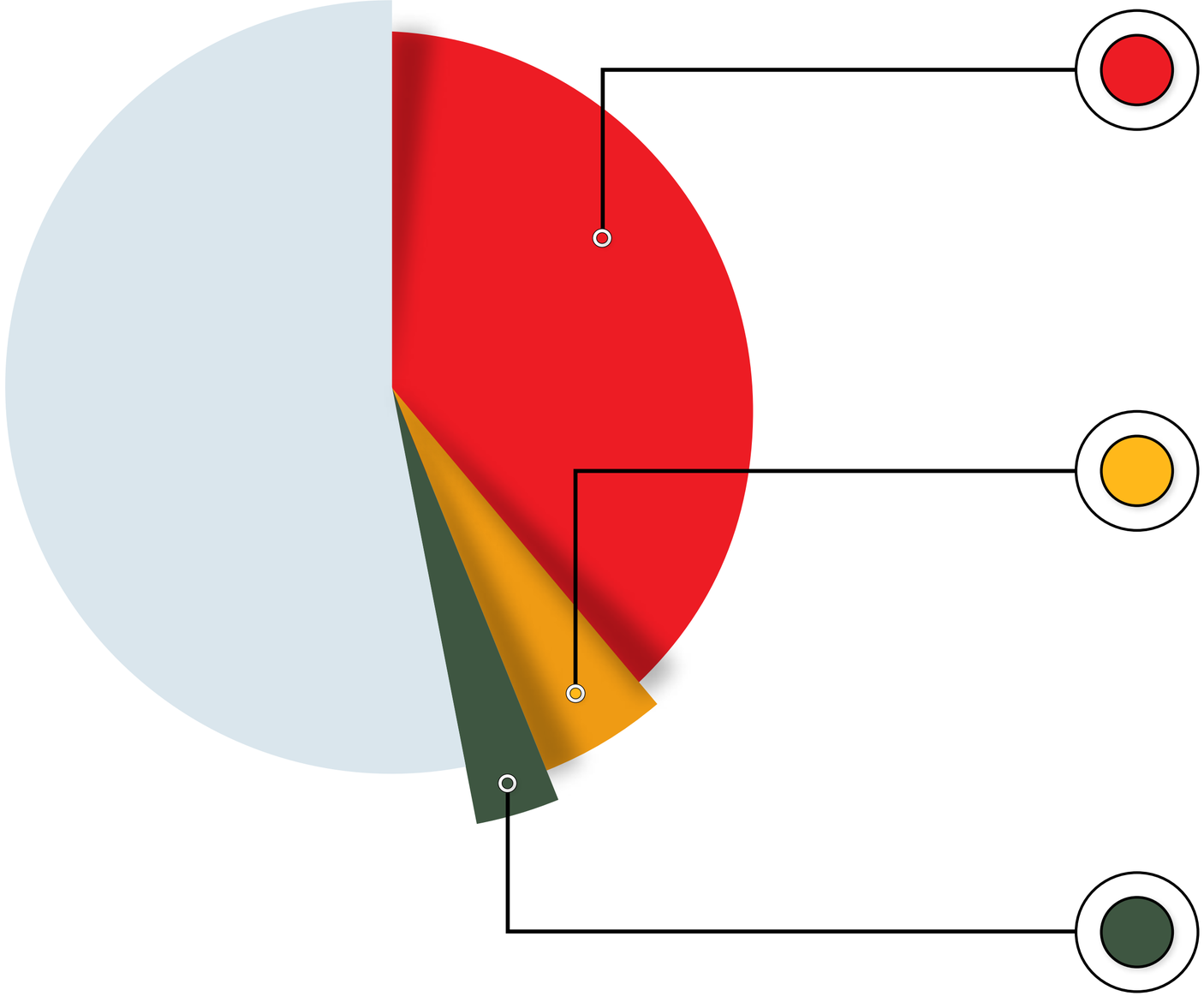
KEY TAKEAWAYS

While there are several determining factors for this, we found the most common responses for the rise in security budget that includes:

- Stronger alignment between security leaders and the business
- Rising threats including an uptick in ransomware
- Protecting innovation and growth initiatives
- Increased awareness of cybersecurity across an organization
- Compliance and regulatory mandates

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

HOW ARE YOUR SECURITY RESOURCES SOURCED?



KEY TAKEAWAYS

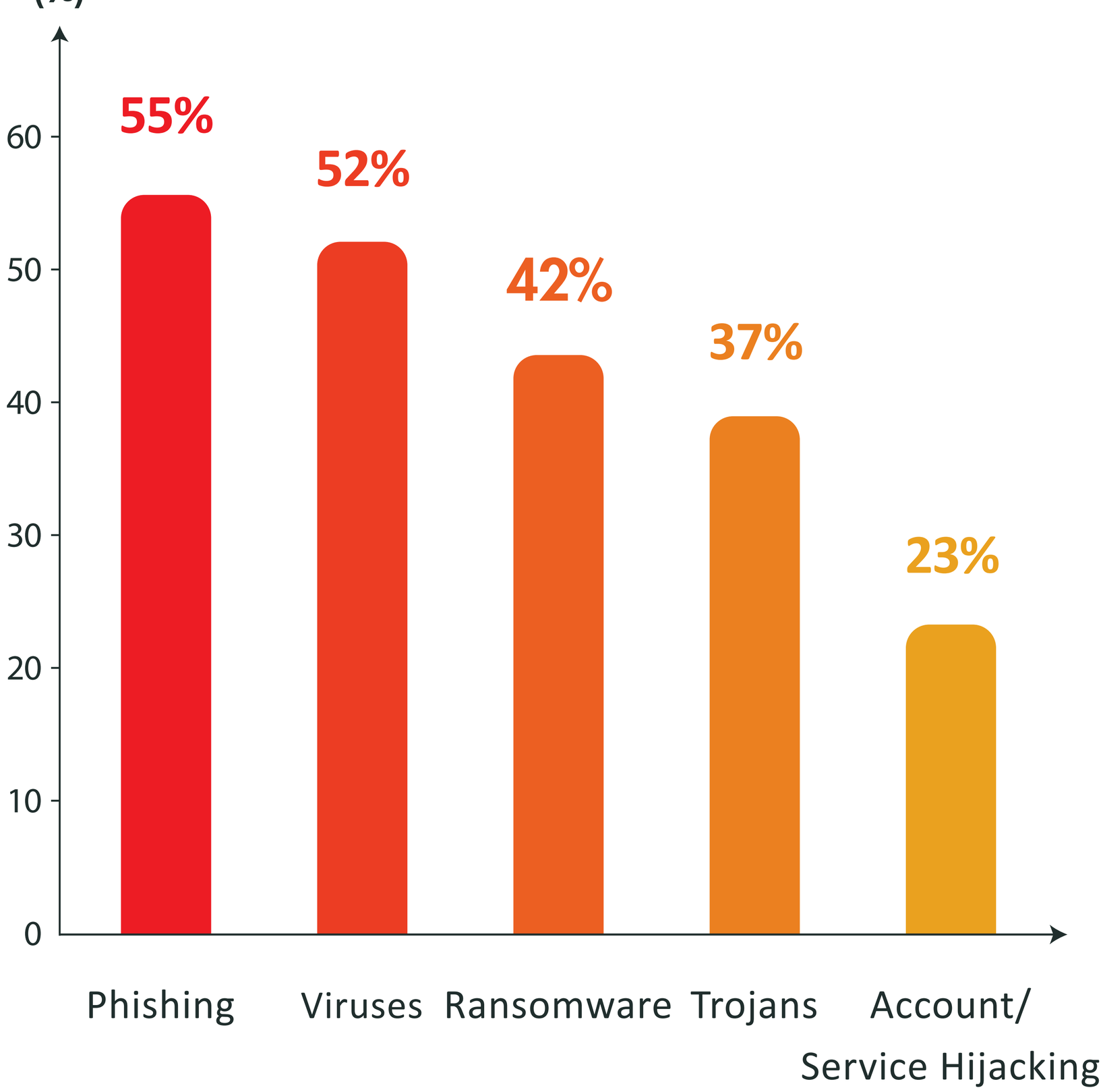
Based on some of top security trends across the globe, these are some of the top services you should consider to out-source:

1. **Security operations**
2. **Vulnerability Management**
3. **Employee education & training**

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

03

WHAT WERE THE TOP 5 CYBER THREATS TARGETING YOUR ORGANIZATION IN 2021?



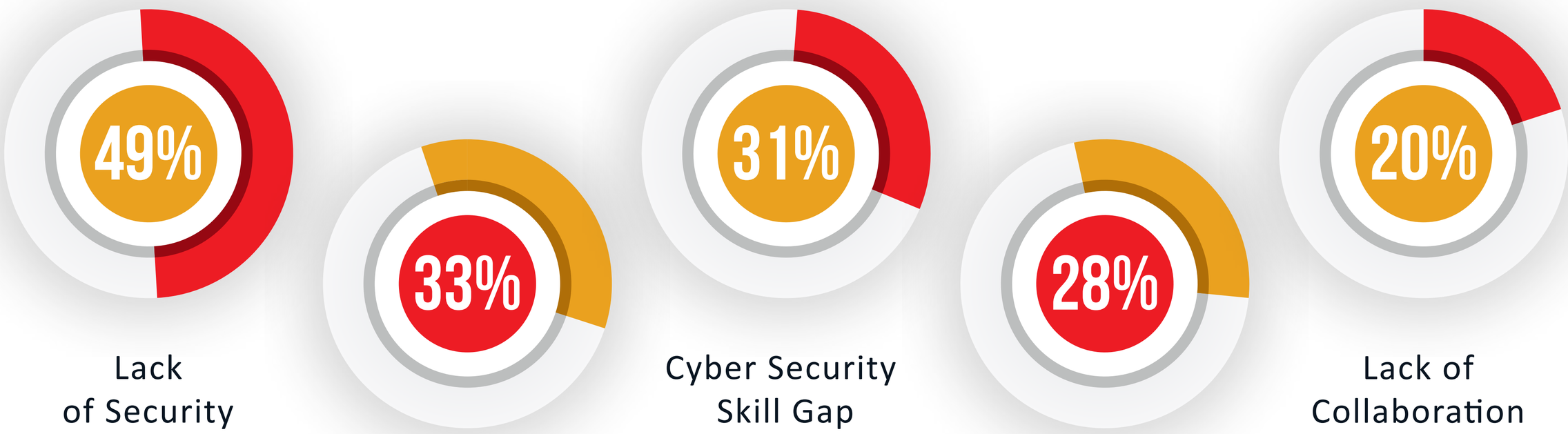
KEY TAKEAWAYS

- Phishing is a huge threat and growing more widespread every year.
- The most well-known computer security threat, a computer virus grabs second place in breaches.
- Ransomware attacks remains constant threat for all sectors in year 2021.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

04

WHICH OF THE FOLLOWING BARRIERS INHIBIT YOUR ORGANIZATION FROM ADEQUATELY DEFENDING AGAINST CYBER THREATS?



KEY TAKEAWAYS

- Lack of security awareness poses a major threat to businesses, organizations are putting their reputation and competitive advantage at risk by not addressing the 'human factor' in cyber security.

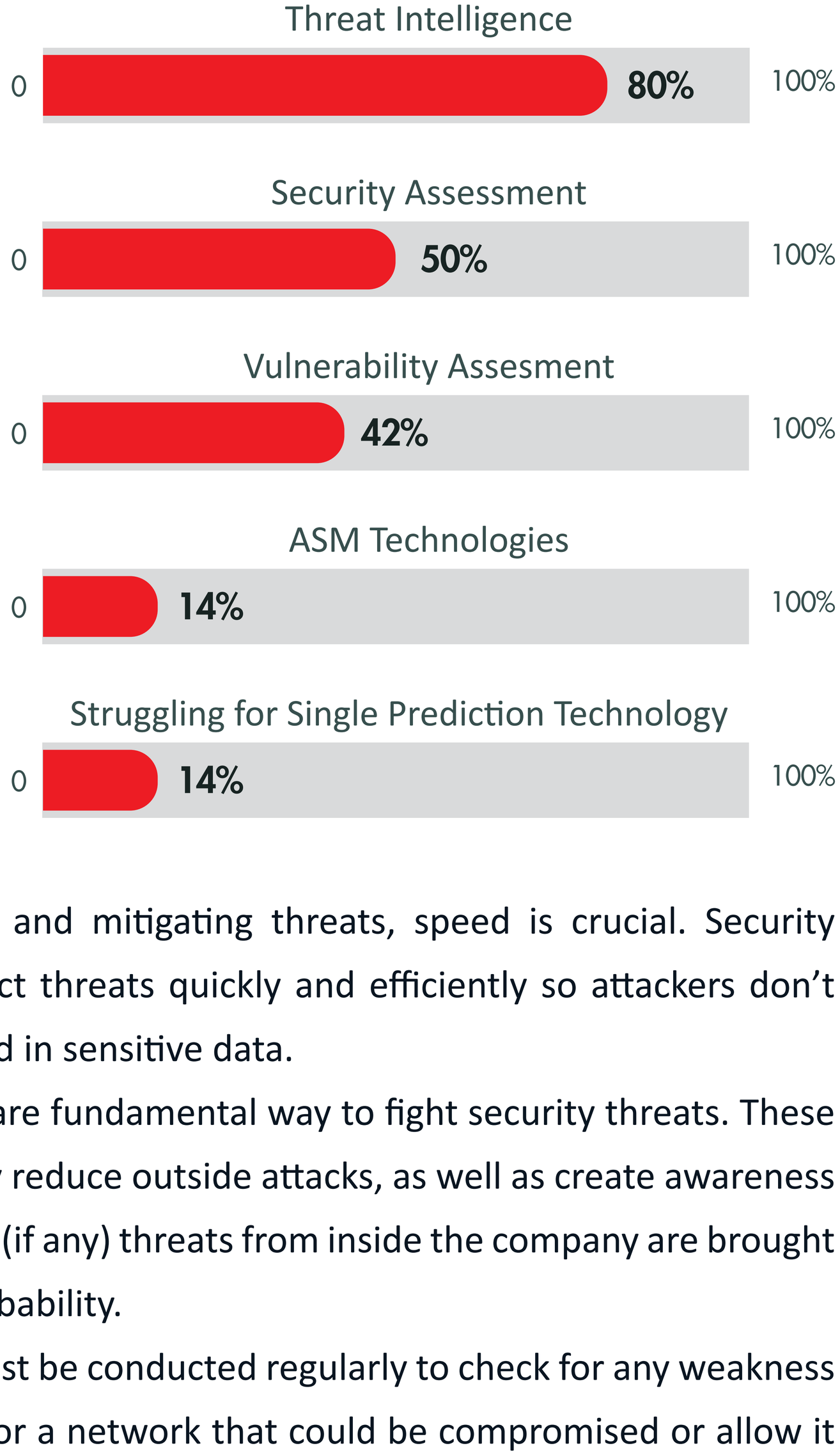
- Cybersecurity budgets have largely remained insufficient, even as instances of cyber-attacks continue to increase globally.

- Too many organizations are stuck in a constant cycle of trying to fill cybersecurity job vacancies. A better strategy is to start building and investing in talent pipelines.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

05

WHAT DATA PREDICTION TECHNOLOGIES ALREADY IN USE IN YOUR ORGANIZATION?

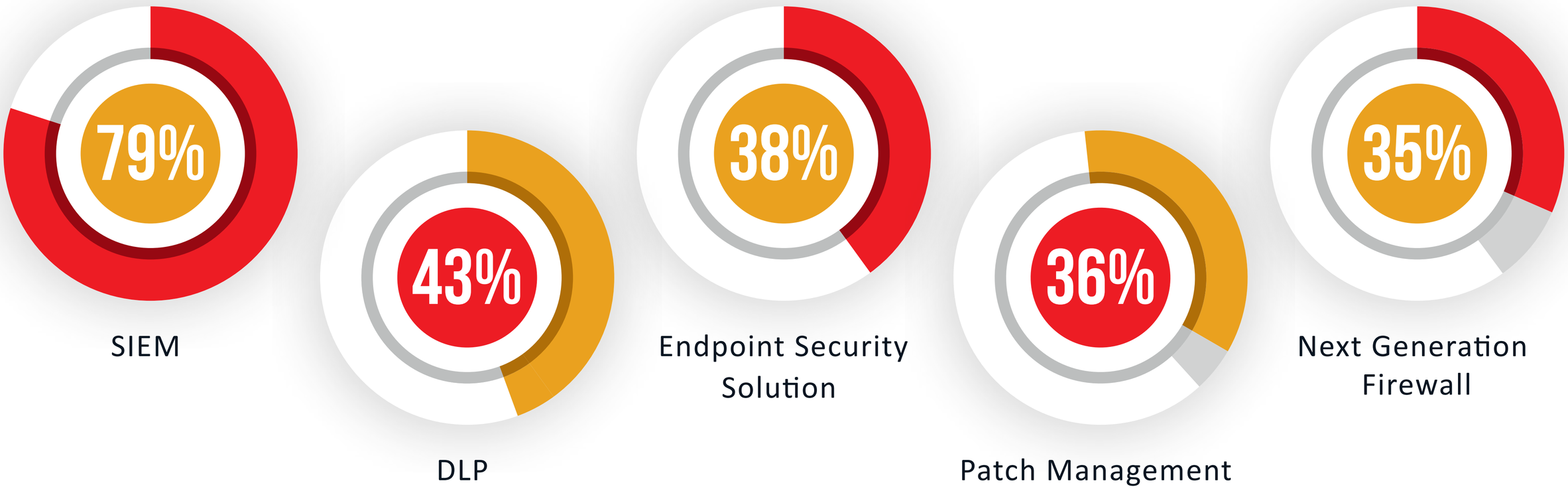


KEY TAKEAWAYS

- When it comes to detecting and mitigating threats, speed is crucial. Security programs must be able to detect threats quickly and efficiently so attackers don't have enough time to root around in sensitive data.
- Security assessment services are fundamental way to fight security threats. These assessments help to significantly reduce outside attacks, as well as create awareness within the company so potential (if any) threats from inside the company are brought down to a minimum level of probability.
- A vulnerability assessment must be conducted regularly to check for any weakness within an application, a system or a network that could be compromised or allow it to be accessible to an unauthorized third party. These assessments are never ending tasks, as every software or system upgrade changes or adds certain code or features which weren't a part of the equation during the scan performed previously.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

WHAT ARE THE TOP 5 CYBER THREAT PREVENTION TECHNOLOGIES THAT YOU CURRENTLY NEED TO ADAPT IN YOUR ORGANIZATION?



KEY TAKEAWAYS

- With a Security Information and Event Management (SIEM) solution, organizations get to integrate risk assessment services. SIEM tools make it possible for you to analyze network behavior in different circumstances and factors based on security sources for any condition.

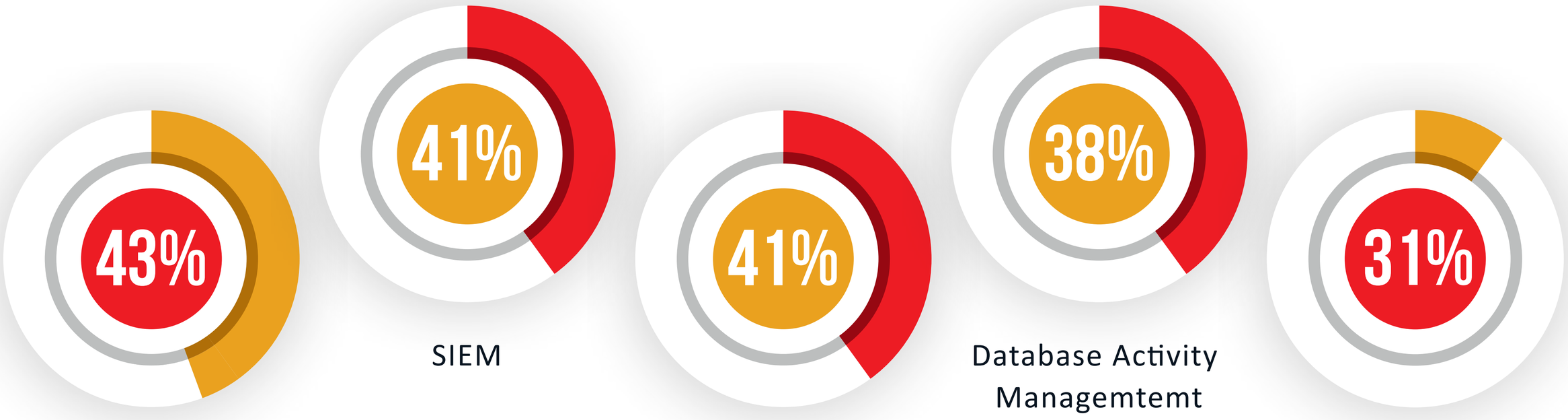
- DLP facility helps you to identify, monitor and protect data in storage as well as in motion over the network. Enforcement of DLP technology enables monitoring of the location and usage of data as well.

- The Endpoint Security Solution you depend on should align with the priorities that matter most to you. The solution must ensure system uptime for users, find more opportunities for automation, and simplify complex workflows.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

07

WHAT ARE THE TOP 5 CYBER THREAT DETECTION TECHNOLOGIES THAT YOU CURRENTLY NEED TO ADAPT IN YOUR ORGANIZATION?

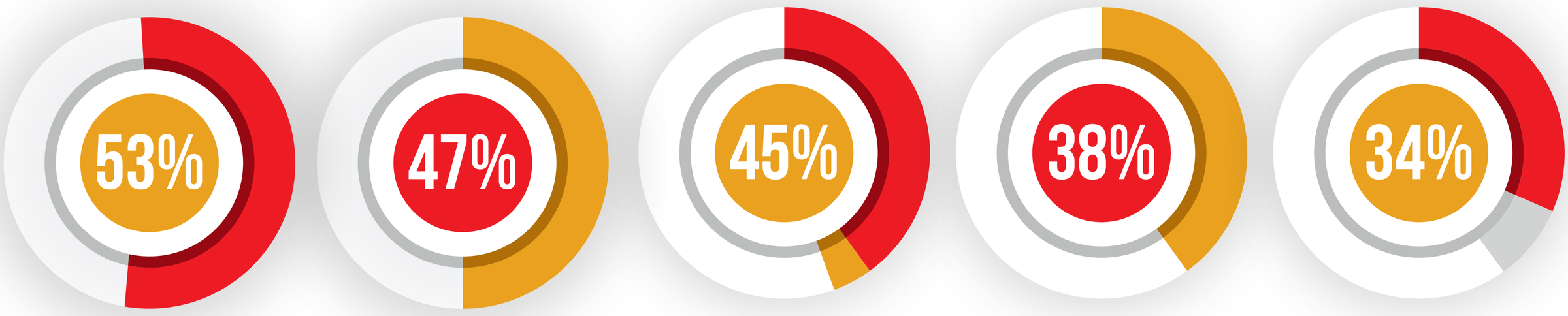


KEY TAKEAWAYS

- Organizations can use CTI technology to improve their cybersecurity and weaken the probability and damage of future cyberattacks. The top three benefits of Cyber Threat Intelligence are:
    - Cost effective
    - Improves the efficiency of security team
    - In-Depth Cyber Threat Analysis
- A VAPT is a proactive approach to strengthening an organization's cyber defenses. Organizations conduct VAPT periodically to actively strengthen their security posture.
- Organizations consider Database Activity Monitoring technology an important set of their enterprise compliance and security management requirements.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

WHAT ARE THE TOP 5 CYBER THREAT RESPONSE TECHNOLOGIES THAT YOU CURRENTLY NEED TO ADAPT IN YOUR ORGANIZATION?



KEY TAKEAWAYS

- To supplement endpoint security with increased detection, investigation, and response capabilities, organizations require EDR solutions as their first line of defense enabling comprehensive endpoint security management strategies.

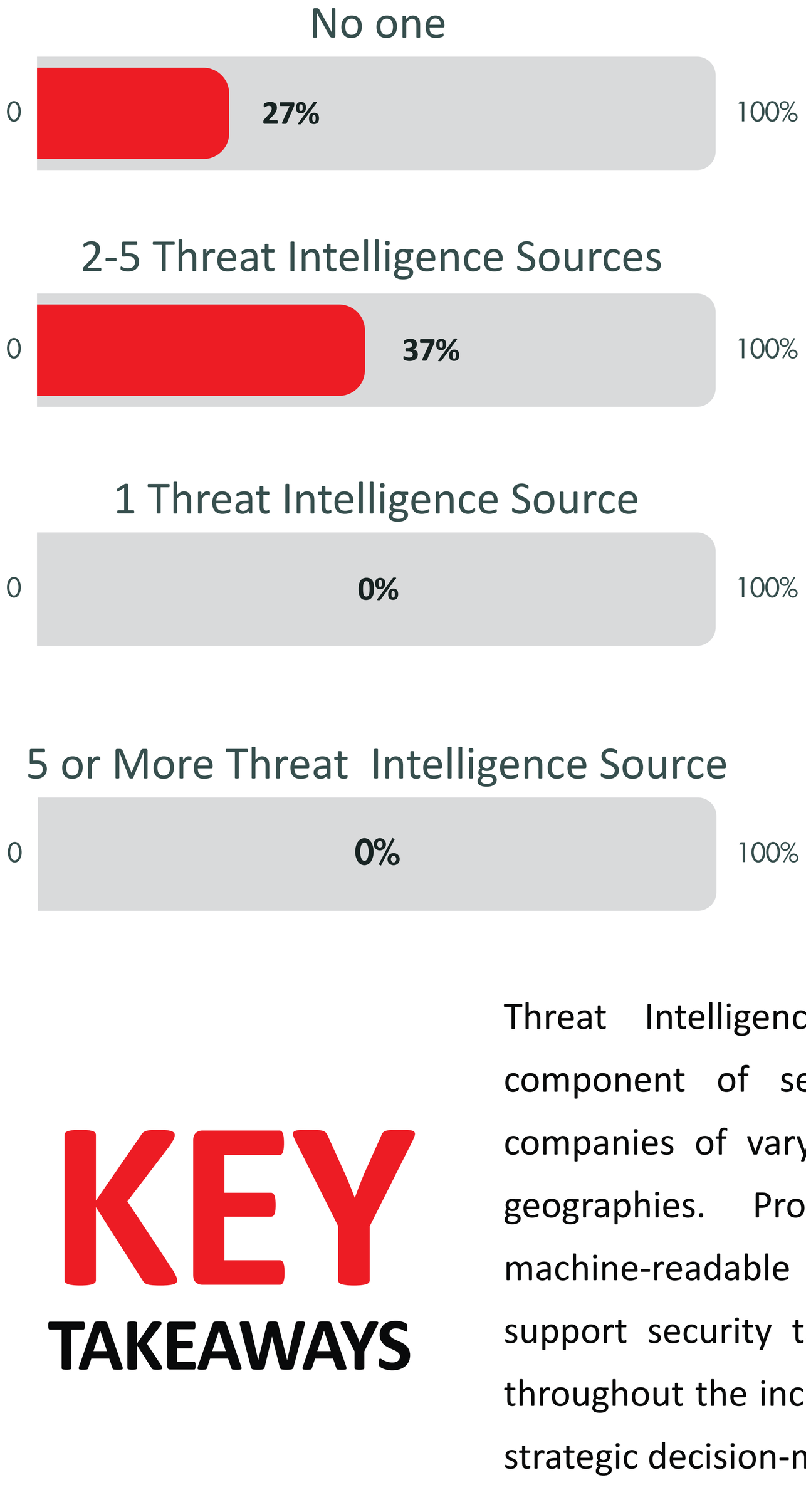
- With new, sophisticated threats being launched, traditional firewalls are becoming less and less capable of adequately protecting corporate networks.
  Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.

- SOAR addresses several vital aspects that cybersecurity teams often cope with. The skill shortage, poor response time, and inability to properly assess every alert as it arrives in real-time underlines the necessity of SOAR. But while the overall ROI of SOAR still is debatable for some, the future is bound to revolve around SOAR.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

09

HOW MANY THREAT INTELLIGENCE SOURCES DO YOU UTILIZE AS PART OF YOUR THREAT DETECTION AND RESPONSE PROGRAMS?



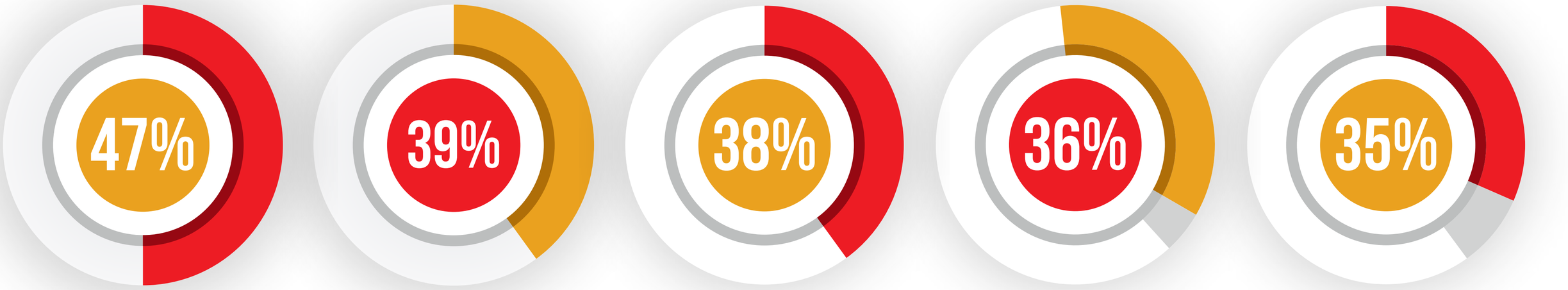
KEY TAKEAWAYS

Threat Intelligence has already become a key component of security operations established by companies of varying sizes across all industries and geographies. Provided in human-readable and machine-readable formats, threat intelligence can support security teams with meaningful information throughout the incident management cycle and inform strategic decision-making.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

10

WHICH TOP 5 SECURITY CONTROLS ARE/WERE THE MOST EFFECTIVE FOR YOUR ORGANIZATION IN YEAR 2021?



Email & Web Browser

Inventory & Control of Hardware Assets

Maintainence Monitoring & Analysis of Audit logs

Malware Defence

Vulnerabilty Management

KEY TAKEAWAYS

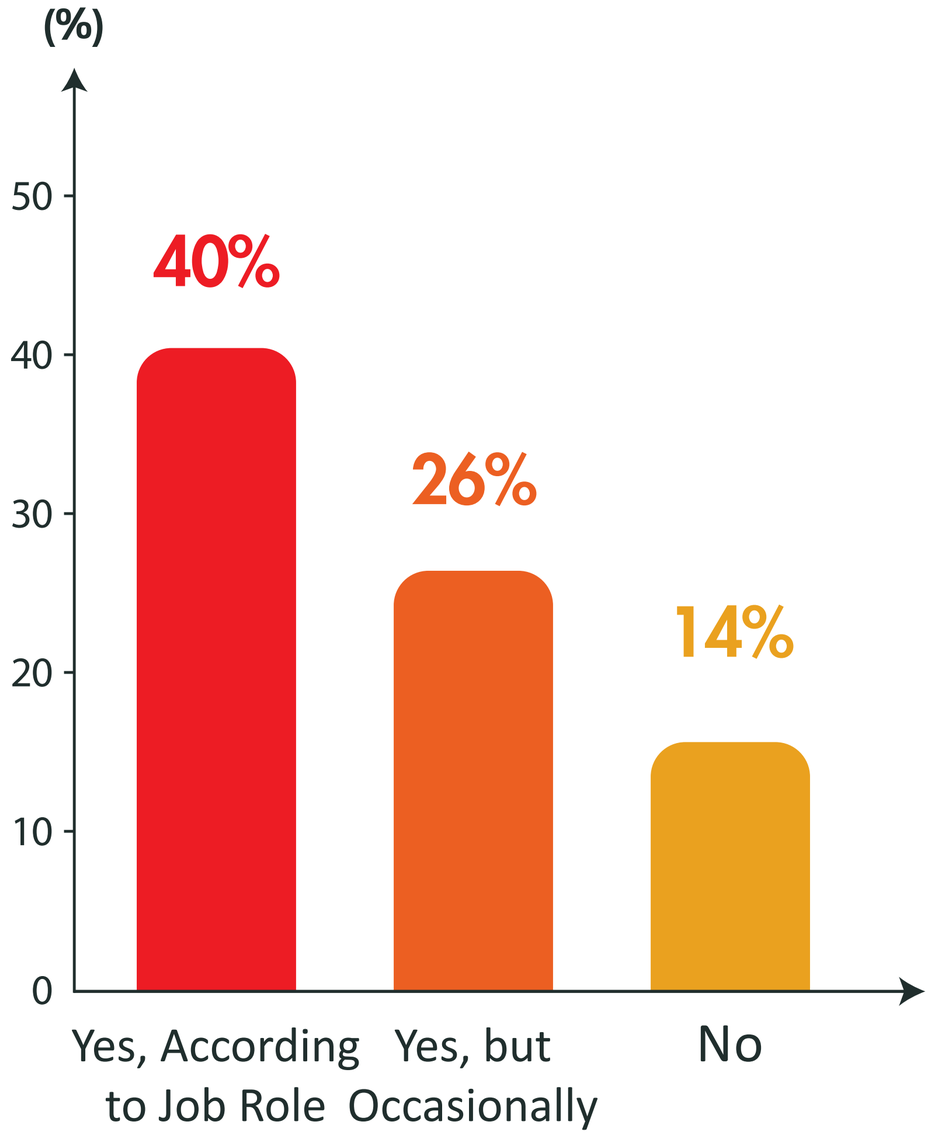
- Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Key points to remember while applying controls for email and web browser are:
  - Ensure Use of Only Fully Supported Browsers and Email Clients
  - Use DNS Filtering Services
  - Maintain and Enforce Network-Based URL Filters
  - Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
  - Implement DMARC
  - Block Unnecessary File Types
  - Deploy and Maintain Email Server Anti-Malware Protections

- Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

- Because IT environments generate so many events, you need log management to ensure you capture valuable information and can analyze it quickly. All software and hardware assets, including firewalls, proxies, VPNs and remote access systems, should be configured to retain valuable data.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

DOES YOUR ORGANIZATION PROVIDE EMPLOYEE TRAINING TO RAISE IS AWARENESS?



KEY TAKEAWAYS

- Most of the enterprise level organizations consider regular security awareness trainings and cybercrime protection programs in order to learn how to protect themselves from emerging cybercrime threats. For them, regular security awareness trainings helps to keep security always in the mind of the users.
- 26% of respondents consider occasional sessions are enough for them however, training for new hires is essential.
- A small number of respondents believe that trainings are needed when employees are not performing up to a certain standard or at an expected level of performance.

Copyright © 2022 Trillium Information Security Systems (Pvt) Ltd. All rights reserved.

CONCLUSION

Trillium Information Security Systems would like to thank all the **organizations** and **individuals** who **participated in the survey for the year 2021**. Thank you, readers, for spending time here with us yet again. We hope that the information contained in these pages has been of assistance to you and that you found it both informative and easy to understand. As we mentioned at different points in this year's report, it is not always easy to see what is coming at us around the next bend. We encourage you, our readers, to reach out to us with your questions, comments and thoughts. Stay safe, and be security smart!

Report Compiled & Prepared By

Anam Zahra _Marketing Intelligence & Training Lead

Copyright © 2022 Trillium Information Security Systems (Pvvt) Ltd. All rights reserved.