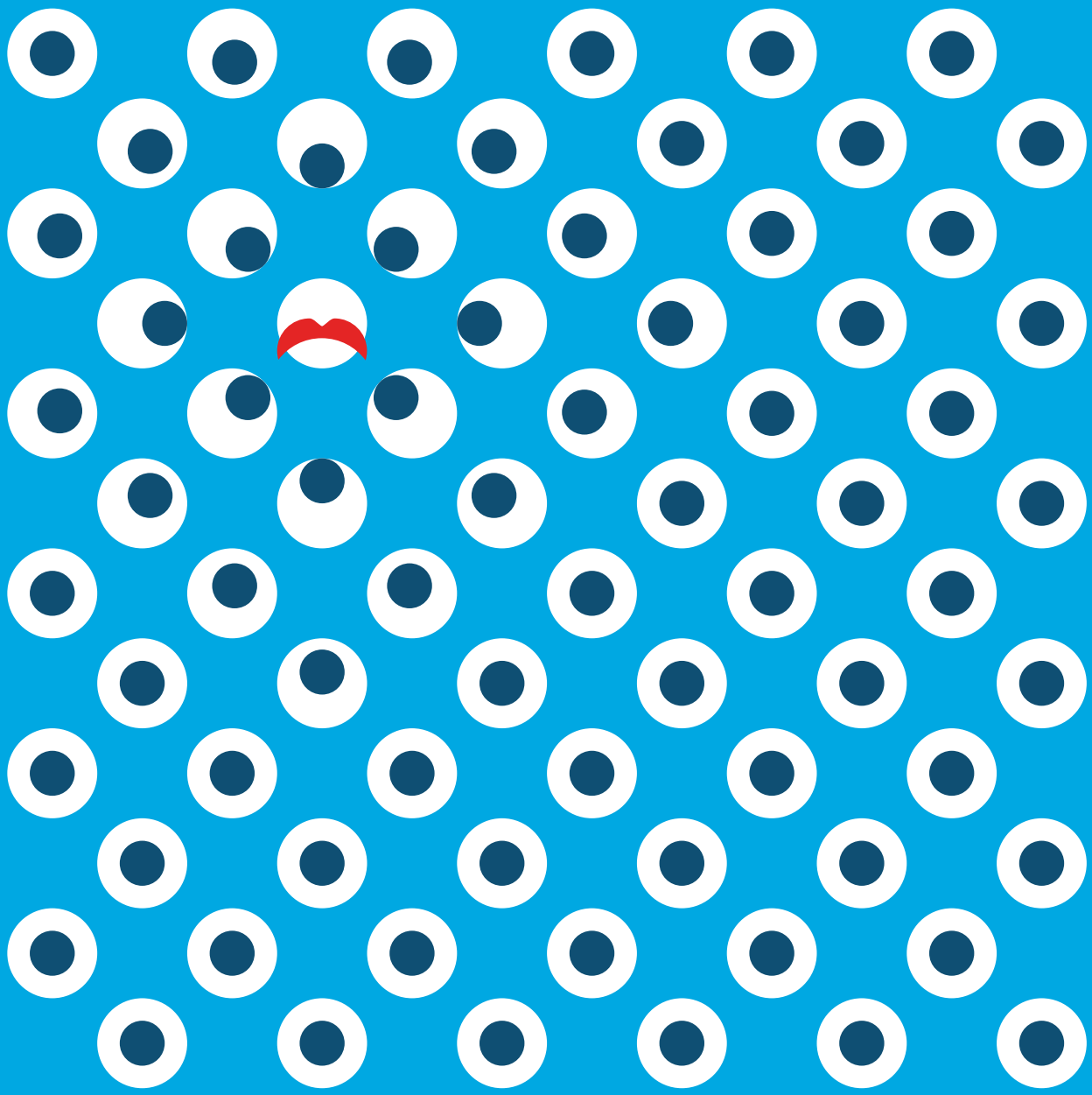


Cisco 2018 Asia Pacific Security Capabilities Benchmark Study

Regional Breach Readiness

cisco

Table of Contents

Executive Summary

Asia Pacific is an exciting region where great strides are being made in digital transformation. It is home to significantly diverse economies and is remarkably leading the charge in developing connected cities of the future—smart cities. Many economies are seeing the benefits of these rapid developments, and as the Internet of Things (IoT) becomes commonplace in organizations and workers continue to work remotely and flexibly, more devices are becoming connected to the Internet.

While this has opened up greater avenues for growth and development, it provides more opportunities for threats to get through and risks for businesses and individuals. Along with this, attackers are getting increasingly sophisticated and are employing cutting-edge techniques to breach organizations.

2017 saw an unprecedented wave of cyber attacks, yet cybersecurity measures are too often reactive responses instead of cornerstones of a sound digital infrastructure. To put this into perspective, in the Asia Pacific region, companies receive 6 threats every minute but only **50% of alerts are being investigated**.

The Cisco 2018 Asia Pacific Security Capabilities Benchmark Study—conducted by independent third-party researchers—offers insights on security practice from more than 2,000 respondents across 11 countries. This includes China, Korea and Japan in North Asia, the Southeast Asian nations of Singapore, Thailand, Malaysia, Vietnam, Philippines and Indonesia, Australia in the south, and India.*

In this report, we highlight the potential economic loss across Asia Pacific due to cybersecurity incidents and the fact that defenders have a lot of work to do and challenges to overcome. Our research and insights are intended to help organizations respond effectively to today's rapidly evolving and sophisticated threats.

The key findings from this report are:

1. **Breaches**

   In Asia Pacific, many companies receive up to 10,000 threats a day according to our study. That means 6 threats are received every minute. **69% of companies surveyed receive more than 5,000 threats a day.** However, only 50% of the total numbers of alerts are investigated.

2. **Lack of security readiness**

   Our study asked 2,000 respondents, **about the digital security infrastructure they have in place**. As many as 9% of respondents said that they do not have any dedicated cybersecurity professionals at their organizations, while 13% do not have executives who have direct responsibility and accountability for the cybersecurity of their organizations.

   Amongst the respondents only 42% said that executive leadership considers cybersecurity a high priority, and just 44% strongly agree that security roles and responsibilities within organizations should have a clear chain of command.

3. **Economic and reputational fall out**

   Cyber attacks are having far-reaching ramifications that include financial and reputational losses to companies. **In Southeast Asia, 51% of all cyber attacks resulted in a loss of more than USD$1 million.** Nearly 10% of respondents said that cyber attacks cost them more than USD$5 million. 33% of respondents in the study said a security breach can cost them anywhere between USD$1 - 5 million.

4. **Multi-pronged attacks**

   The form of cyber attacks is also changing. Attackers are now not just targeting IT infrastructure, but are now also targeting operational technologies (OT) that impact the day-to-day functioning and running of a business.

   30% of organizations have already seen cyber attacks along those lines, while 50% said they expect this to be the case moving forward. In addition, **41% of Asia Pacific respondents said their businesses would be affected if their operational infrastructure is compromised.**

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.

5. Increased scrutiny from stakeholders

In addition to financial losses, cybersecurity incidents are also undermining Asia Pacific organizations' ability to gain confidence with their consumers and other stakeholders, with **72% remarking that greater privacy concerns from their customers** is adding more time to their sales cycle. Nearly half say their sales cycle is delayed by more than a month.

In the coming year, executives also believe that scrutiny from stakeholders such as investors, insurance companies, regulators, business partners, executive leadership, watchdog/interest groups, the media, and employees will start to rise.

Recommendations for defenders

When adversaries inevitably strike their organizations, will defenders be prepared, and how quickly can they recover?

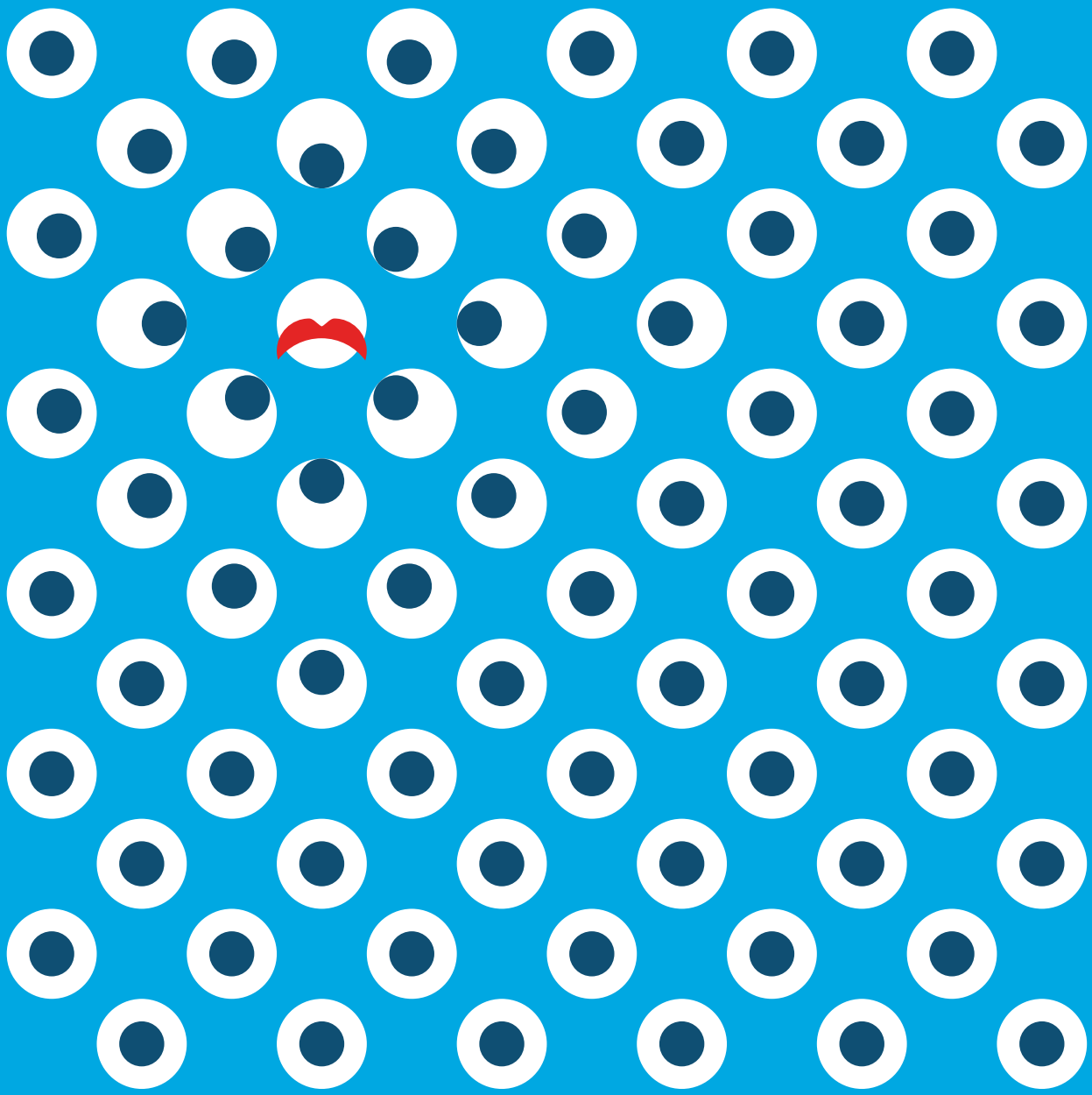
Even so, defenders will find that making strategic security improvements and adhering to common best practices can reduce exposure to emerging risks, slow attackers' progress, and provide more visibility into the threat landscape. They should consider:

- Implementing first-line-of-defense tools that can scale, like cloud security platforms.
- Confirming that they adhere to corporate policies and practices for application, system and appliance patching.
- Employing network segmentation to help reduce outbreak exposures.
- Adopting next-generation endpoint process monitoring tools.
- Accessing timely, accurate threat intelligence data and processes that allow for that data to be incorporated into security monitoring and eventing.
- Performing deeper and more advanced analytics.
- Reviewing and practicing security response procedures.
- Backing up data often and testing restoration procedures processes that are critical in a world of fast-moving, network-based ransomware worms and destructive cyberweapons.
- Reviewing third-party efficacy testing of security technologies to help reduce the risk of supply chain attacks.
- Conducting security scanning of microservice, cloud service, and application administration systems.
- Reviewing security systems and exploring the use of SSL analytics and, if possible, SSL decryption.

Defenders should also consider adopting advanced security technologies that include machine learning and artificial intelligence capabilities. With malware hiding its communication inside of encrypted web traffic, and rogue insiders sending sensitive data through corporate cloud systems, security teams need effective tools to prevent or detect the use of encryption for concealing malicious activity.

About the report

The ***Cisco 2018 Asia Pacific Security Capabilities Benchmark Study*** presents our latest security industry advances designed to help organizations and users defend against attacks. We also look at the techniques and strategies that adversaries use to break through those defenses and evade detection. The report also highlights major findings from the **Cisco 2018 Security Capabilities Benchmark Study**, which examines the security posture of enterprises and their perceptions of their readiness to defend against attacks.



The Evolution of Breaches

Regional Overview

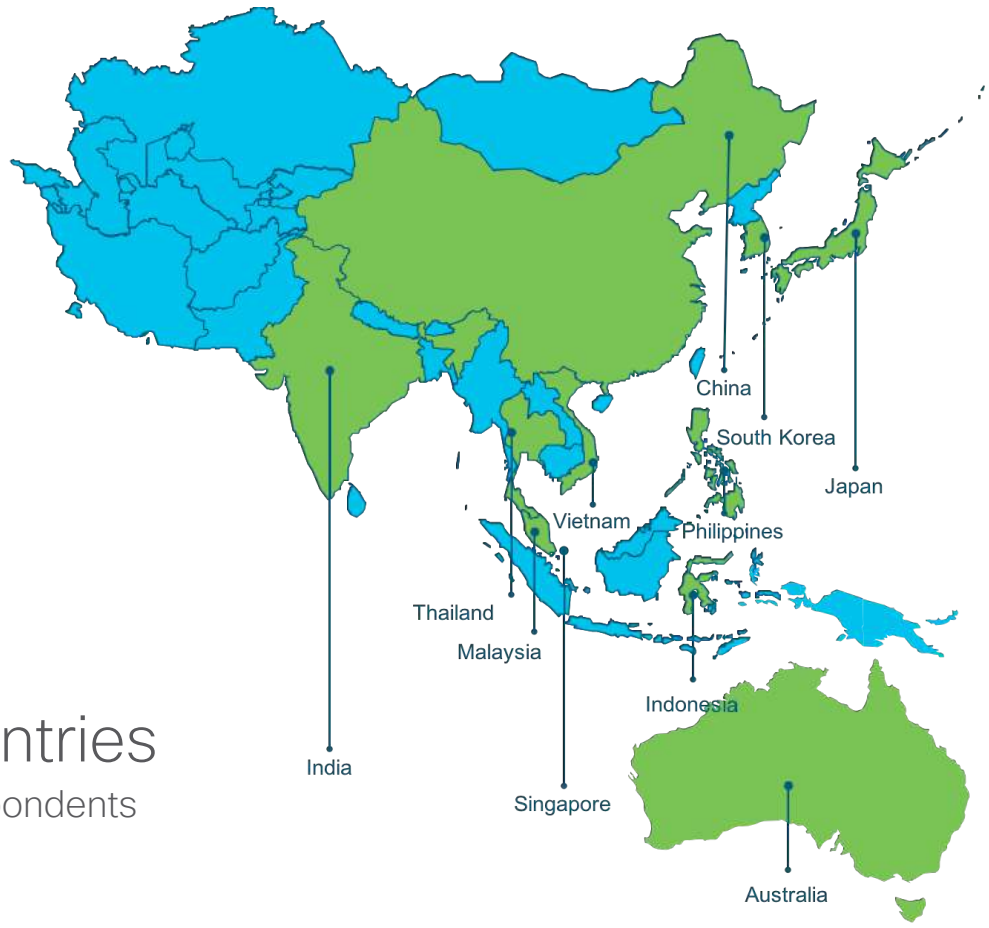
Regional Overview

Security is a numbers game, pure and simple. Relentless, well-funded, resourceful attackers have unlimited chances to get into networks, and they only need to be right once. Tireless defenders have to be right every single time to stop attackers getting in. Much is written about the threat landscape and the latest attacks; in this report we will focus on the defenders' story. When threats inevitably strike, will defenders in the Asia Pacific region be prepared, what is the impact of an attack and how quickly can they recover critical business services?

The evolution of breaches

Findings from the Cisco 2018 Asia Pacific Security Capabilities Benchmark Study—which offers insights on security practice from more than 2,000 respondents across 11 countries—show that defenders have a lot of challenges to overcome. The study covers China, Korea and Japan in North Asia, the Southeast Asian nations of Singapore, Thailand, Philippines, Malaysia, Vietnam and Indonesia, Australia in the south, and India. We also compared this data with the findings from our global benchmark study, which covered 3,600 respondents across 26 countries.

What follows is a summary of the key findings covering readiness for breach, causes and challenges faced, the effect of breach, and next step recommendations.



11 Countries

2,000 Respondents

To gauge the perceptions of defenders on the state of security in their organizations, we asked Chief Information Security Officers (CISOs) and Security Operations (SecOps) Managers in several countries and at organizations of various sizes about their security resources and procedures.

What we've learned through our research for the Cisco Asia Pacific 2018 Security Capabilities Benchmark Study is that defenders have a lot of work to do and challenges to overcome. We found that, taken as a region, the findings within Asia Pacific were generally comparable within a small margin to the global findings; given the diversity of markets, this is perhaps not surprising. When you dig beneath the regional surface and look at the country-level data, large gaps start to emerge between global practices and regional behavior.

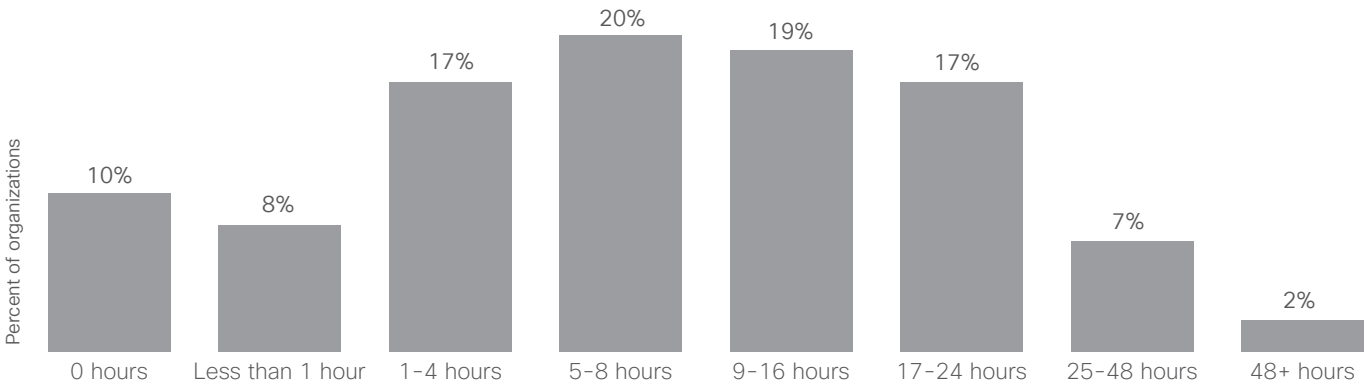
Not if but when: the impact of a breach

There's no real disparity between regional and global data in the fact that almost a third of all breaches are disclosed by a third party data source, which is something that all companies need to be conscious of and work to improve. Australia reported the lowest figure in this category with only 24% of breaches being reported by a third party data source.

When breaches occur, 41% of Asia Pacific respondents reported that the number one affected business process is operations, which is comparable with worldwide findings, but in this region, brand reputation is a firm number two on the list of concerns for 36% of respondents, whereas it is only fourth on the list of concerns at a global level, suggesting that businesses in Asia Pacific overall are more concerned about the damage to their reputation than their counterparts elsewhere.

In terms of the impact of the breach on operations, a large majority of regional defenders reported that systems were down for under 24 hours, which is comparable to the global figure of 91%. But only half the respondents reported that systems were backed up within 8 hours whereas the worldwide study showed 55% restoring services within the 8 hours window.

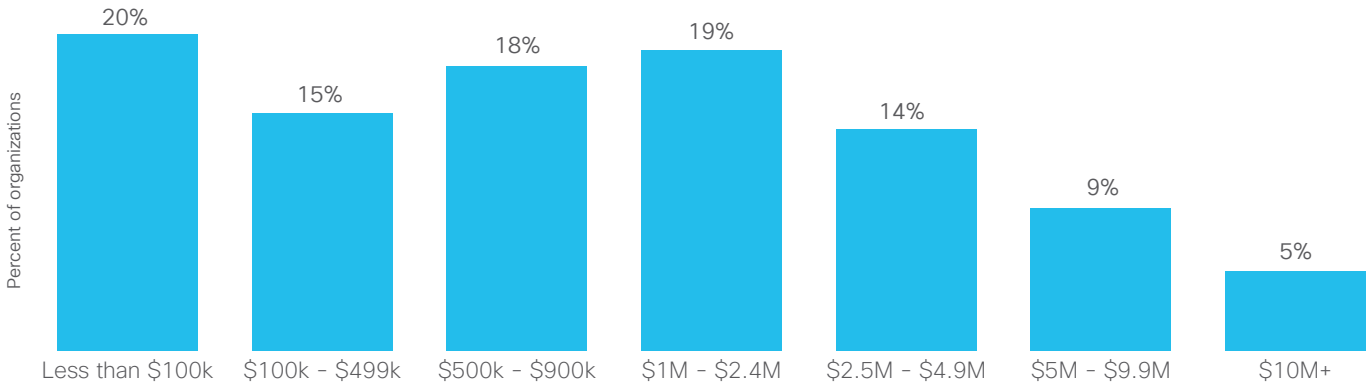
Figure 1 Estimated outage due to breach in APJC



Q: Thinking back to the most severe security breach your organization managed in the past year, how long were systems down due to the breach?

The fear of breaches is founded in the financial cost of attacks, which is no longer a hypothetical number. Breaches cause real economic damage to organizations, damage that can take months or years to resolve. The cost of a breach in the region is similar to, if slightly higher in some cases than our global findings; 33% of respondents reported that a breach could cost between USD$1-5 million, compared to 30% globally. In Australia, 9% of respondents reported that breaches cost more than USD$10 million, whereas in Korea that number is 0%.

Figure 2 Cost of breaches in APJC

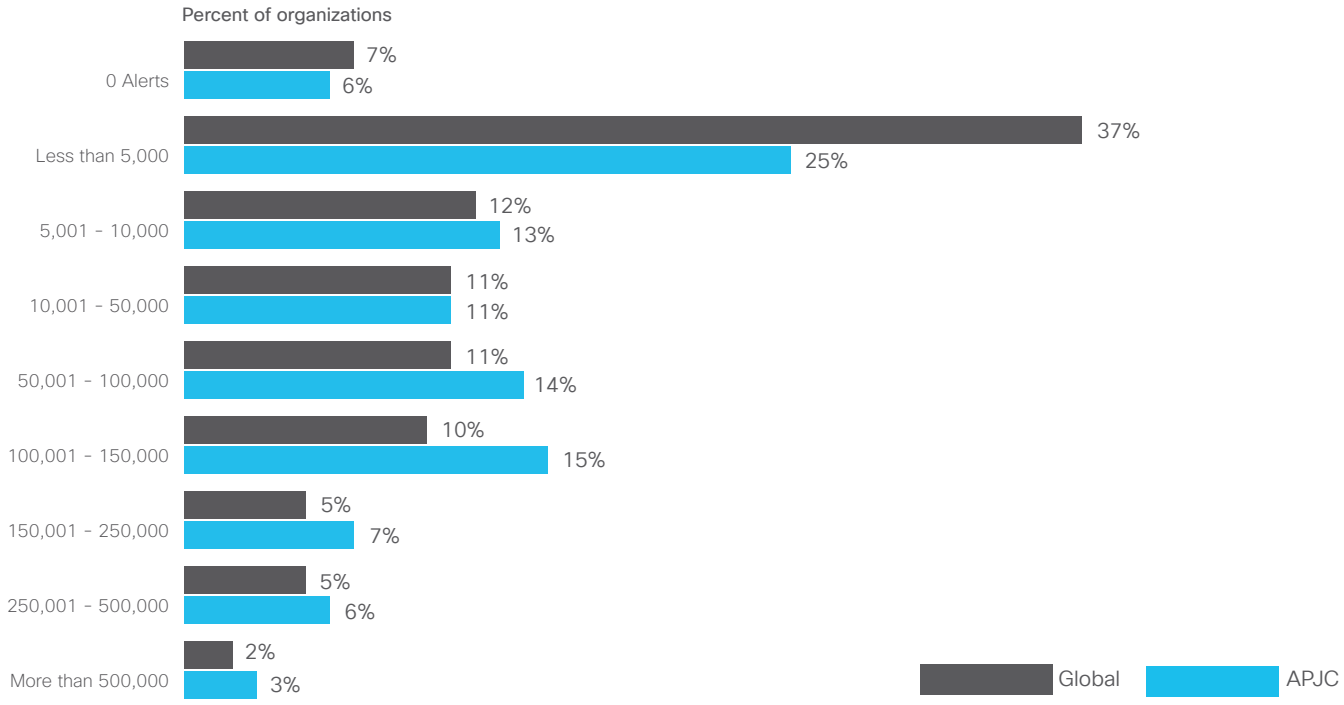


Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the itmpact of the attack?

Alerts and breach response

Security practitioners in Asia Pacific are being kept busier than their global counterparts; at a worldwide level, 37% of respondents reported receiving fewer than 5,000 alerts per day whereas in the region, that figure is only 25%. The real challenge, as ever, lies in what comes after the alert is received: how many are actually investigated. The regional figure is 56% which is in line with worldwide expectations, although still far too low, meaning that almost half of alerts are being investigated in some way. Korea fares worst in this category with only 30% of alerts being investigated, and Australia comes out best with 72%. The results are similar when you drill further to see how many of the investigated alerts are in fact legitimate. In Australia, 65% of investigated alerts are legitimate compared with the Asia Pacific figure of 44%, suggesting that Australian security systems have a higher level of accuracy; Korea reports only 16% of alerts as legitimate which suggests that more work is needed to help security professionals get more accurate information about their environment and attacks against it.

Figure 3 Number of daily security alerts in APJC



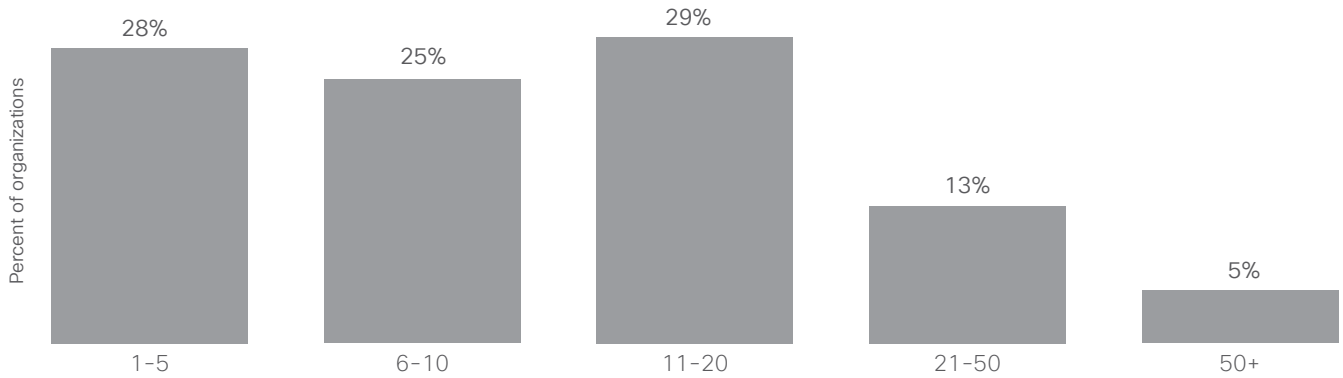
Q: On average, how many security alerts does your organization see on a daily basis?

Complexity created by vendors in orchestration

Defenders are implementing a complex mix of products from a cross-section of vendors: an arsenal of tools that may complicate rather than clarify their security capabilities. This complexity has many downstream effects on an organization's ability to defend against attacks, such as increased risk of losses.

Across Asia Pacific, 47% of respondents report having more than 10 vendors in their security environment and 5% have more than 50; the two countries reporting more complex than average environments are Australia with 12% reporting more than 50 vendors and India with that figure at 8%.

Figure 4 Number of different security vendors in enviroment in APJC



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

Complexity is not the only thing that is holding back defenders. Regional security professionals cite budget (32%), interoperability with legacy systems (30%), and lack of trained personnel (27%) as their key constraints when managing security. Almost two-thirds of respondents, or 59%, report experiencing cyber fatigue and have given up trying to stay ahead of malicious attackers. This is compared to a global figure of 46% and suggests that more needs to be done in the region to equip defenders with adequate tools. Japan tops the list of individual countries in this area with 76% reporting cyber fatigue, compared with just 29% in China.

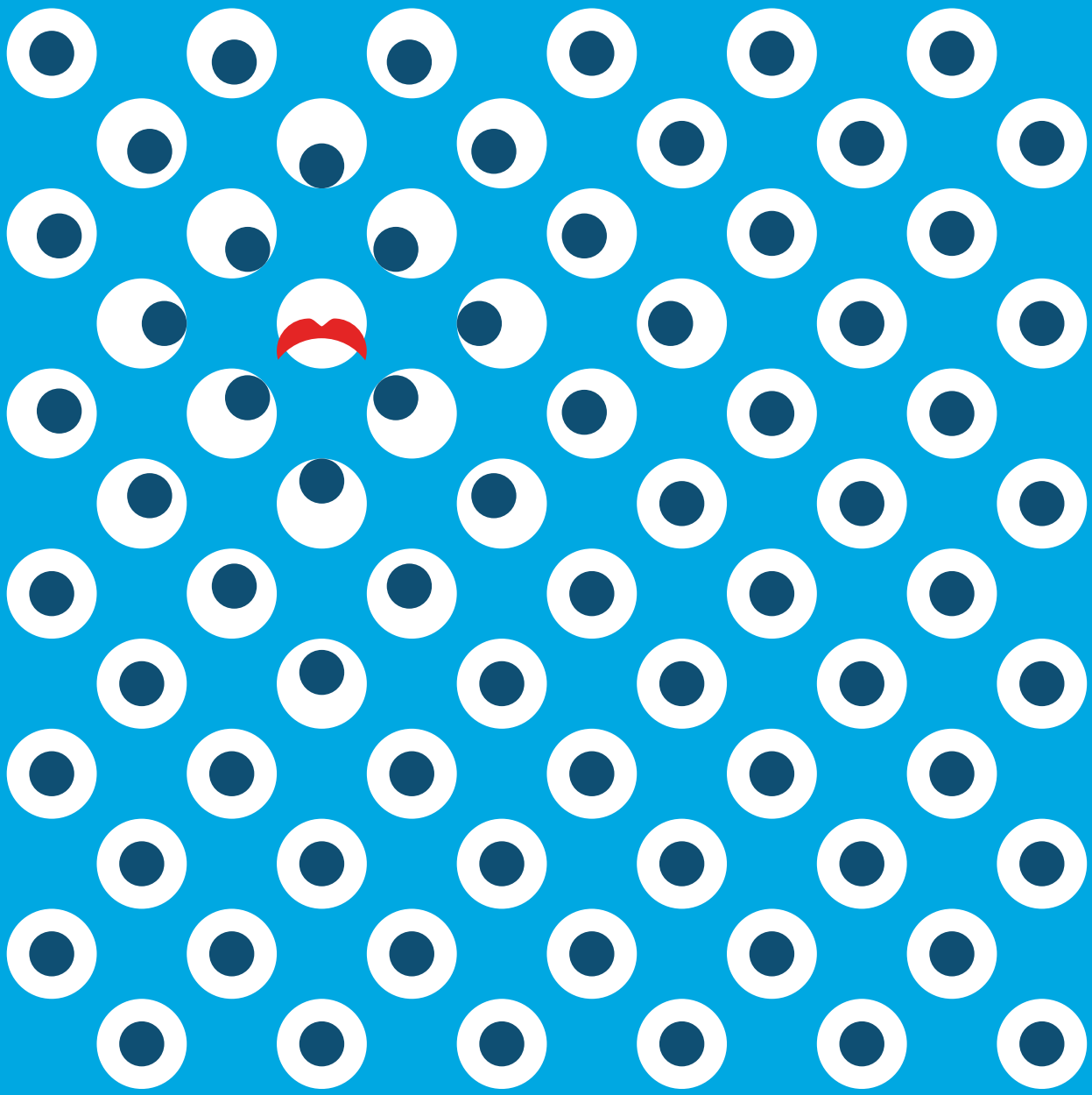
What's next?

Defenders will find that making strategic security improvements and adhering to common best practices can reduce exposure to emerging risks, slow attackers' progress, and provide more visibility into the threat landscape.

Five principles to consider:

1. Implementing first-line-of-defense tools that can scale, like cloud security platforms.
2. Employing network segmentation to help reduce outbreak exposures.
3. Adopting next-generation endpoint process monitoring tools.
4. Accessing timely, accurate threat intelligence data and processes that allow for that data to be incorporated into security monitoring and eventing.
5. Reviewing and practicing security response procedures.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Australia Viewpoint

Country Overview

Australia Viewpoint:

A nation under attack has an efficient response

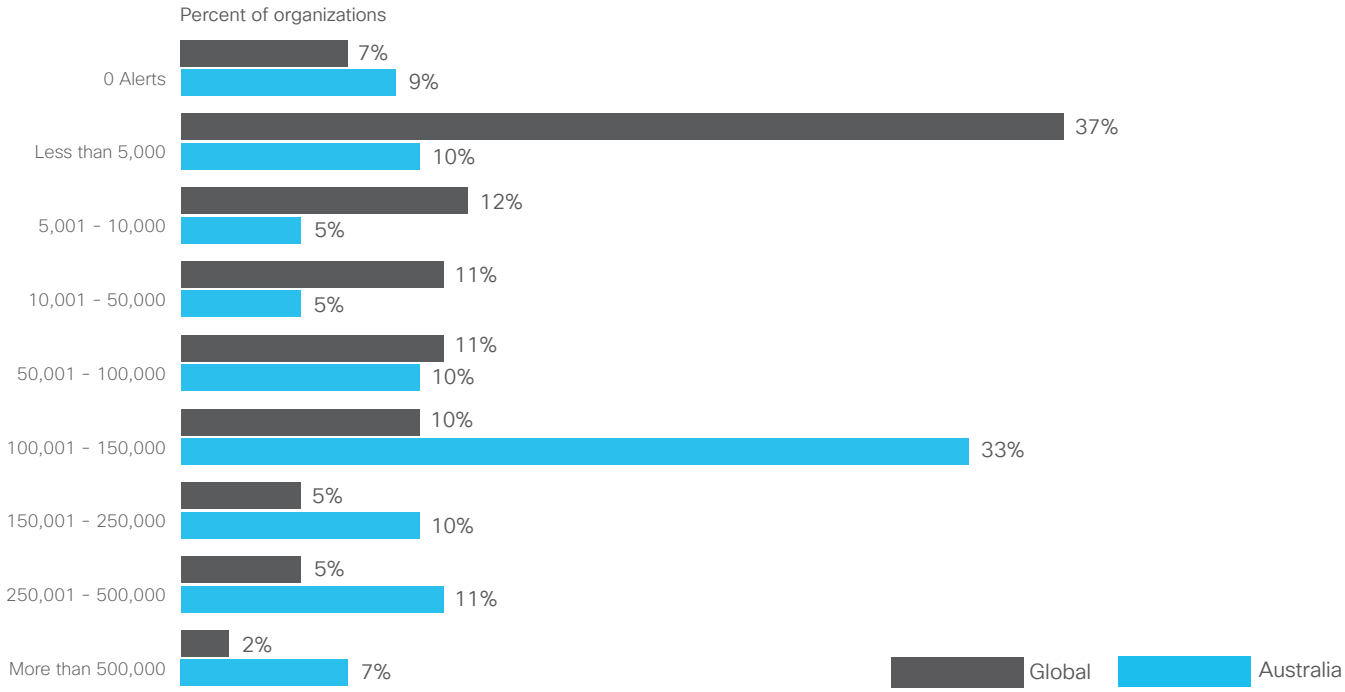
What we've learned through our research for the Australia viewpoint is that the nation appears to be dealing with more attacks than most other countries. At least this is the conclusion if you examine the amount of alerts that security professionals are dealing with and the amount of them that turn out to be legitimate (65%) and Japan (45%).

More organizations in Australia are reporting dealing with more alerts than their global and regional peers: 81% of companies are facing more than 5,000 alerts per day, by far the highest number in the region. Moving higher up the ladder, 33% of organizations deal with 100,000 – 150,000 alerts, which is the highest in the region and higher than the global figure of 10%. At the top end of the scale, 7% of Australian organizations are seeing more than 500,000 alerts compared to 2% across the globe .

Investigating these alerts is the next step and Australia performs well by this measurement: 72% of alerts are investigated, well ahead of the regional and global benchmarks (both 56%). The next step for defenders is to ensure that they are working on the right items; especially given the vast number of alerts they have to address. It turns out that 65% of investigated alerts are legitimate, which still leaves a third of alerts as false alarms, but this is by far the highest in the region and better than both the global benchmark (34%) and the regional standard (44%). This does still mean that a full 35% of investigated alerts are false alarms, so not only is malware getting through the pile of logs that are not attended to, but a vast amount of valuable work is being done on files that don't need it.

The percentage of legitimate alerts that are eventually remediated is 69% which is again ahead of the global (50%) and Asia Pacific (53%) benchmarks. This leaves 31% of legitimate alerts not remediated and in need of improvement.

Figure 5 Number of daily security alerts in Australia

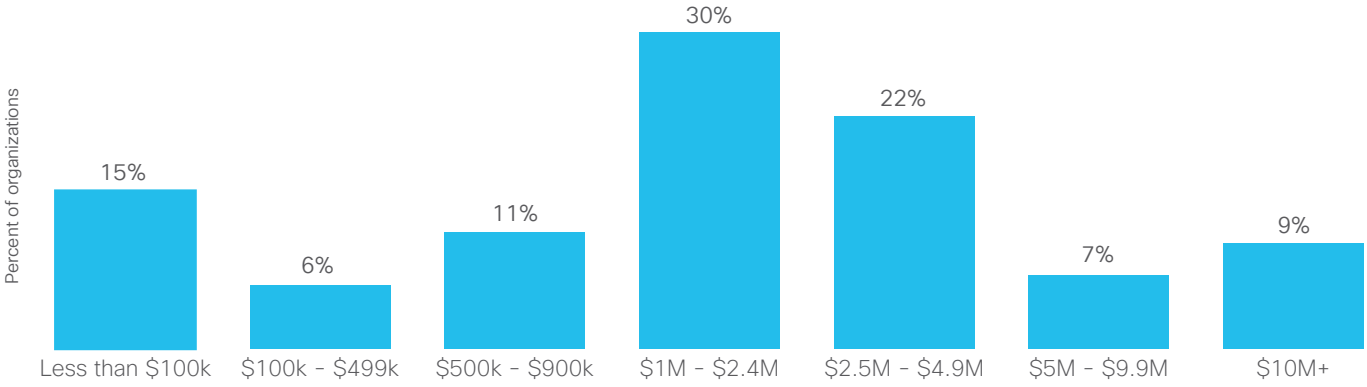


Q: On average, how many security alerts does your organization see on a daily basis?

That's the bad news, but as you might expect, Australian defenders are not taking this lightly; not only do they lead the region and beat global statistics in responding to alerts, with 72% of alerts investigated, they are finding more malicious activity with 65% of alerts being legitimate and, most tellingly that 69% of alerts are remediated. This means that security professionals are scaling up to meet the need, potentially through automation, and that they are able to find the alerts that matter in the mass of information that they have to digest. This compares very favorably to other markets such as Korea, where out of 30% of alerts investigated only 16% are legitimate, suggesting that defenders there are not able to keep pace with the volume of attacks or drill down to find the alerts that matter.

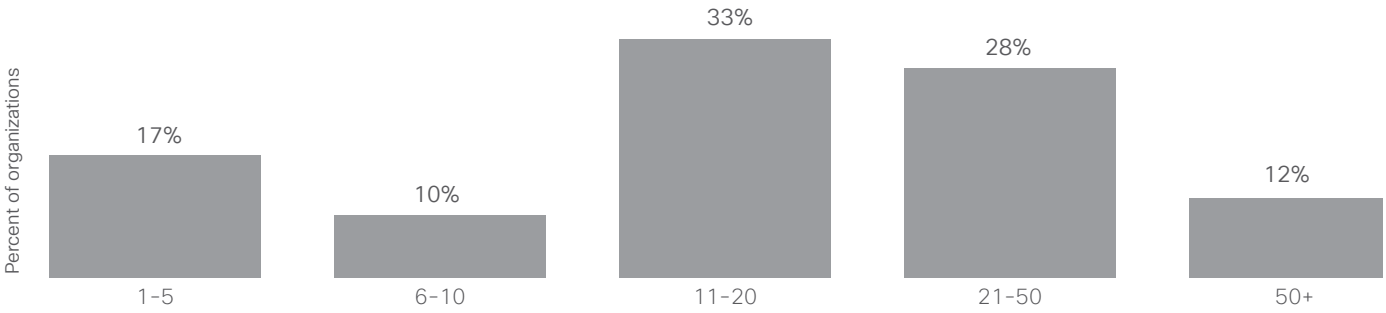
The cost of a breach is highest in Australia with 52% reporting that an attack costs between USD$1-5 million, compared to Japan (23%) and India (25%) and that a full 9% reported costs of more than USD$10 million, which in Korea is 0%. And given the demonstrably large costs of a breach, it's reassuring to learn that 81% of Australian respondents report that they reacted to a breach, with improvements in security threat defense policies, procedures or security technologies.

Figure 6 Cost of breaches in Australia



Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

Figure 7 Number of different security vendors in environment in Australia

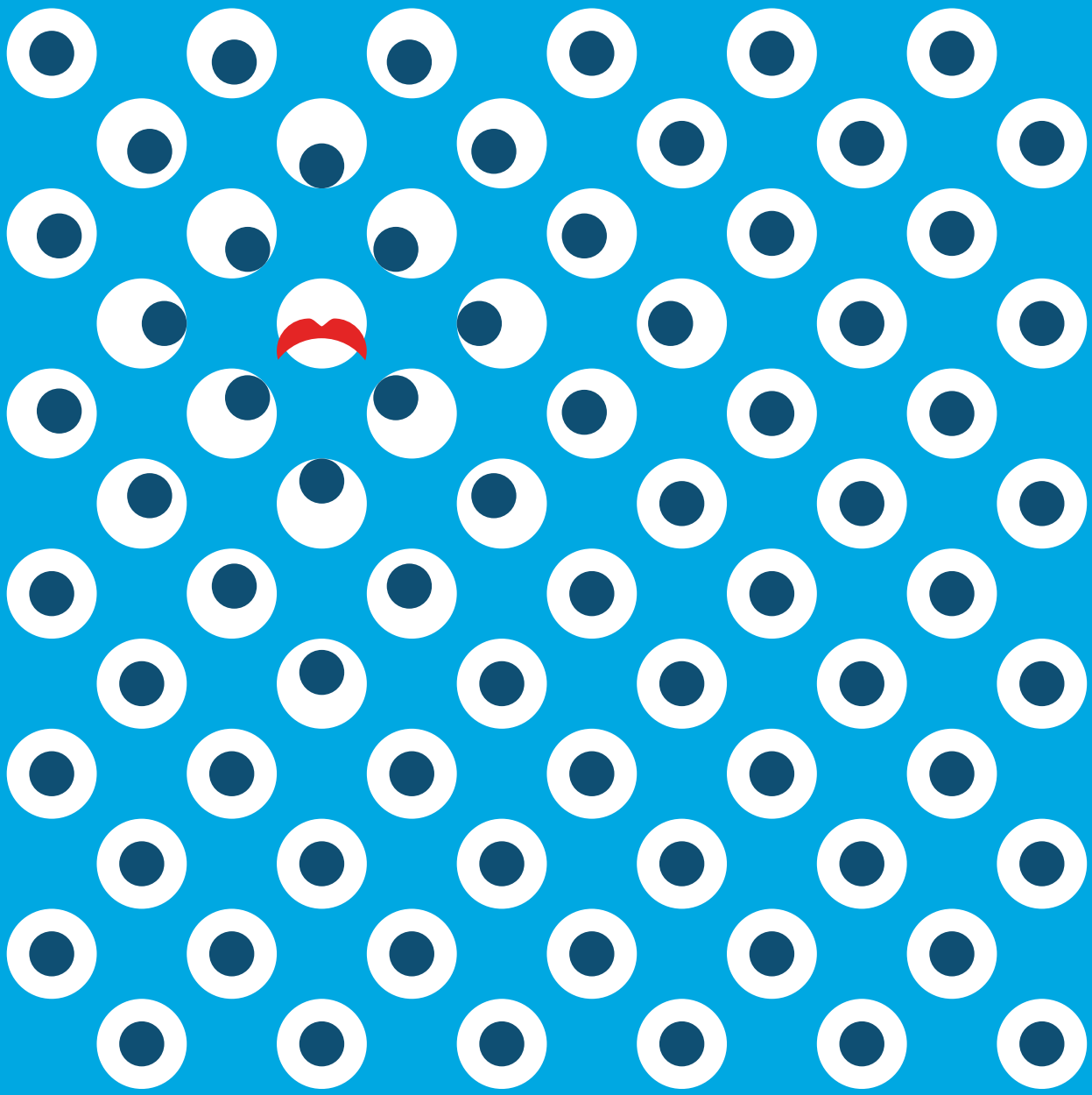


Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

Australia also leads the way with the highest number of vendors being used with 12% reporting more than 50 vendors which compares unfavorably with the global figure of 5% and regional neighbors such as China (3%) and Japan (1%).Maybe it's not surprising then that Australian defenders (69%) are third in the region after Japan (76%) and Thailand (37%) when it comes to reporting cyber fatigue, where defenders have basically given up trying to stay ahead of malicious threats and actors, both of which are way above the worldwide figure (46%).

The cyber fatigue suggests that despite the number of tools and vendors that defenders in Australia are deploying, there is room for more automation, perhaps through an architectural approach. The country still reports a high number (74%) of respondents citing a lack of trust in architectures as a reason to buy best of breed: it's possible that cyber fatigue could be reduced with a re-examination of an integrated security architecture as an enabler of an automated response.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



China Viewpoint

Country Overview

China Viewpoint:

These security policies need tuning

What we've learned through our research for the China viewpoint is that the nation appears to be dealing with fewer alerts than their counterparts around the globe and in Asia Pacific, with only 48% of companies facing more than 5,000 alerts each day. The 52% of respondents reporting that they face fewer than 5,000 daily is not only higher than the regional average (31%) but also much higher than northern neighbor, Japan (21%).

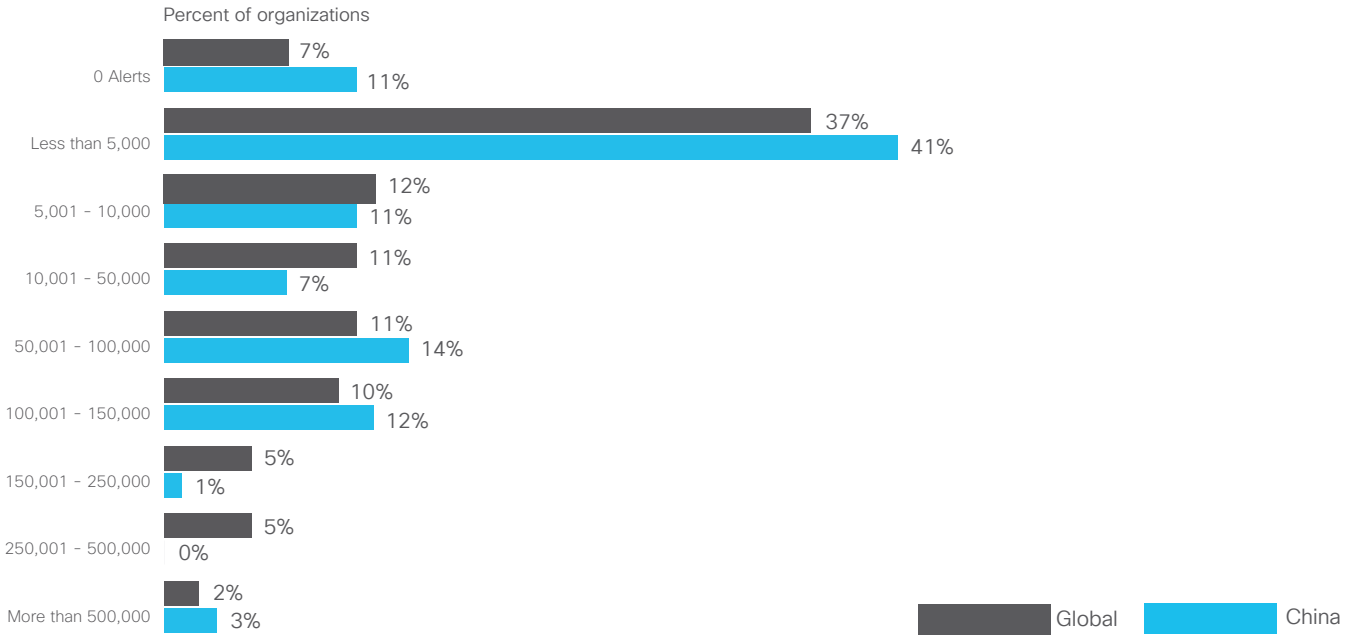
It's possible, of course, that China in general is seeing fewer attacks and that the great firewall comes with some advanced malware protection, but given the global nature of cybercrime and the relatively contentious position of China in the threat landscape, it's unlikely that such a statistical anomaly has occurred. More likely, especially when you consider that only 55% of respondents consider their security infrastructure "very up-to-date" (compared with 68% in the region and 78% in India) that the security tools deployed are simply not catching enough of the bad stuff and therefore not generating the necessary alerts.

This is interesting given that only 36% of alerts are investigated, well below the regional threshold (56%) and a nation of advanced defenders such as Australia (72%); of those only 23% are legitimate compared with the region (44%) and Australia (65%). This tells us that when less than a quarter of investigated alerts turn out to be legitimate, pretty soon the SIEM-that-cried-wolf gets deprioritized.

Investigating alerts is only the first step; defenders also need to ensure that they are working on the right items; especially given the vast number of alerts they have to address. It turns out that only 23% of investigated alerts are legitimate, which is second lowest in the region, well behind the leader Australia (65%) and less effective than both the global benchmark (34%) and the regional standard (44%). It's ahead only of Korea (16%) and that's not a benchmark to aim for. This means a full 77% of investigated alerts are false alarms, so not only is malware getting through in the pile of logs that are not attended to, but a vast amount of valuable work is being done on files that don't need it.

The percentage of legitimate alerts that are eventually remediated is 43% which is behind the global (50%) and Asia Pacific (53%) benchmarks, and indicates that there is work to do at all stages of an alert.

Figure 8 Number of daily security alerts in China



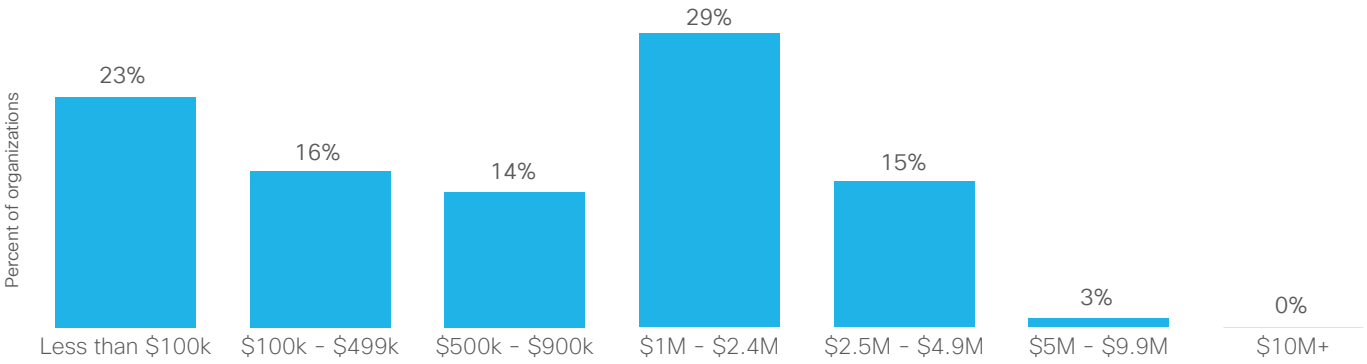
Q: On average, how many security alerts does your organization see on a daily basis?

Whatever the root cause, China defenders need to look long and hard at the accuracy of their security stack and breach response, because, as with anywhere in the world, breaches don't come cheap. 44% of respondents report the cost of a breach as being between USD$1-5 million, compared with only 33% regionally and 25% in India.

China certainly has fewer breaches (less than 1%) costing more than USD$10 million which is better than Australia (9%) and the region (5%) but what's really interesting is the reaction to a breach in China. Only 33% reported that in the wake of an attack, they created the role or hired a Chief Information Security Office (CISO) and it was second last on the list of priorities, which does not compare favorably with the region as a whole where it is a top priority and 44% of respondents said they had filled the top security post in reaction to an incident. Where China is leaps and bounds ahead of the region and indeed the world, is in cybersecurity awareness training. Whether using web or email, mobile devices or laptops on or off network, users are the first target for attackers.

A full 50% of China respondents organized awareness education in the wake of a breach – and it was a number one priority – compared with only 43% in the region where it came third as a priority and 41% in Australia where it trailed in fifth place on the priority list.

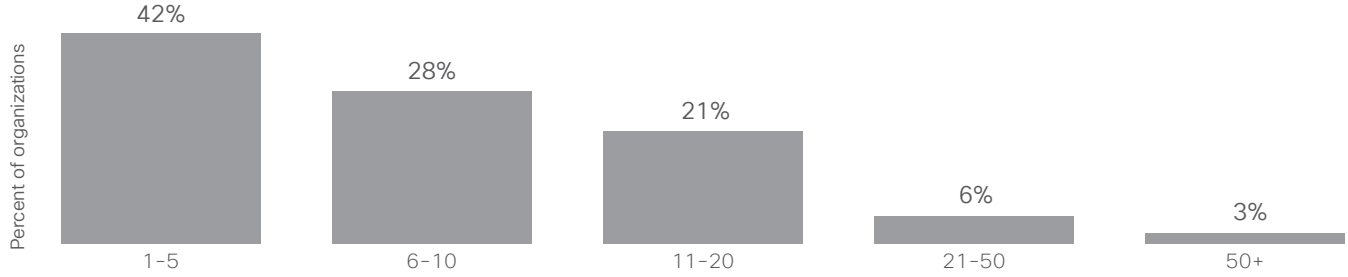
Figure 9 Cost of breaches in China



Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

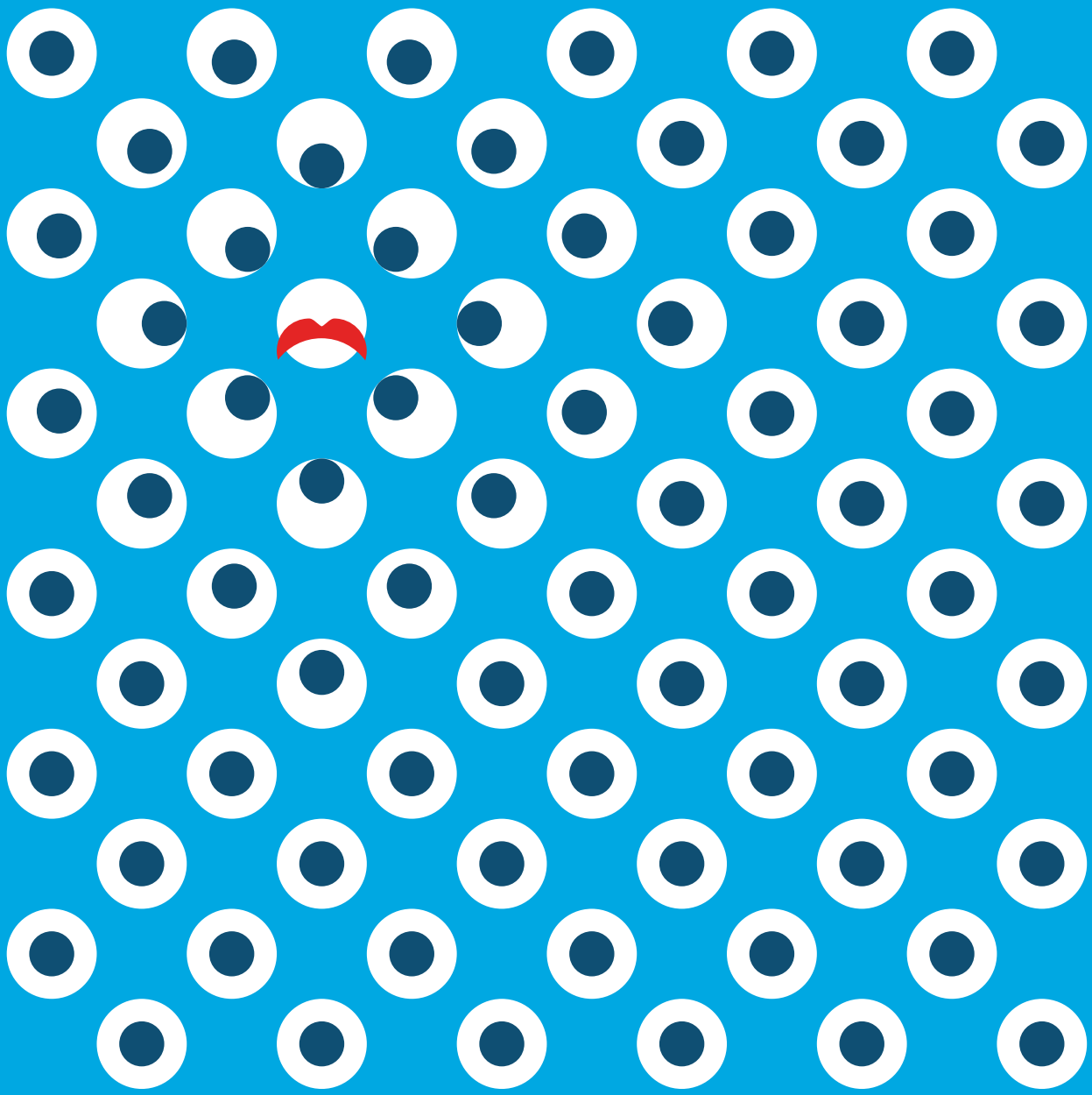
Another aspect of cybersecurity that causes defenders headaches around the world but that seems more under control in China is the issue of vendor sprawl and consolidation. Only 30% report having more than 10 vendors in their security stack, compared with 47% in the region and 73% in Australia, and only 3% have more than 50 vendors compared with 6% in the region and 12% in Australia. If this is the result of creating architectures with fewer vendors to deliver more accurate detection and faster remediation, that would be truly enlightened, although looking back at the accuracy of the alert investigations, you would have to conclude that China defenders have not yet achieved total success in architectural security. Pair this with the knowledge that China exhibits the lowest levels of cyber fatigue (29%) compared with the regional average of 59% and that they were the only country in the region that called out "lack of knowledge about advanced security". China needs to look harder at what's trying to get in and build more effective security postures to keep more of that bad stuff out.

Figure 10 Number of different security vendors in environment in China



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



India Viewpoint

Country Overview

India Viewpoint:

Defending in an extreme market

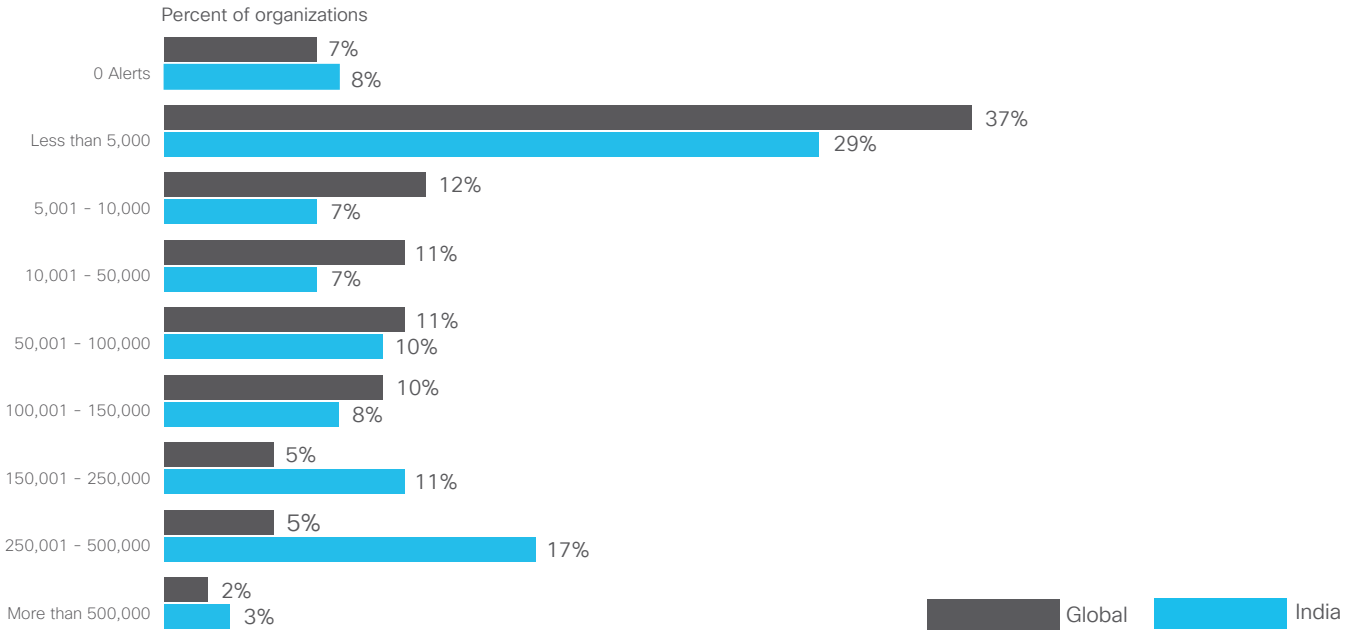
What we've learned through our research for the India viewpoint is that while at first glance the number of alerts that defenders face each day does not seem to be too wide of the norm, there is one bracket in which India posts a significant discrepancy. A full 17% of defenders tell us that they are dealing with 250-500,000 alerts per day which is way above the regional benchmark of 6% and even higher than the second place Australia at 11%. Does India face a larger number of attacks or are some defenders in the nation detecting more attempted breaches?

Like their Australian counterparts, India's defenders are, relatively speaking, on fire when it comes to responding with a full 61% of alerts investigated, compared with the global and regional benchmark of 56%. Admittedly that still leaves 39% of alerts unattended and could still mean almost 200,000 alerts are being ignored each day. Which of those alerts points to malware or as potential breach? India's defenders are doing their best to analyze the alerts that they do investigate.

Investigating alerts is only the first step; defenders also need to ensure that they are working on the right items; especially given the vast number of alerts they have to address.

It turns out that only 44% of investigated alerts are legitimate, which is second highest in the region, well behind the leader Australia (65%) but is better than both the global benchmark (34%) and on par with the regional standard (44%). This means a full 56% of investigated alerts are false alarms, and a vast amount of valuable work is being done on files that don't need it.

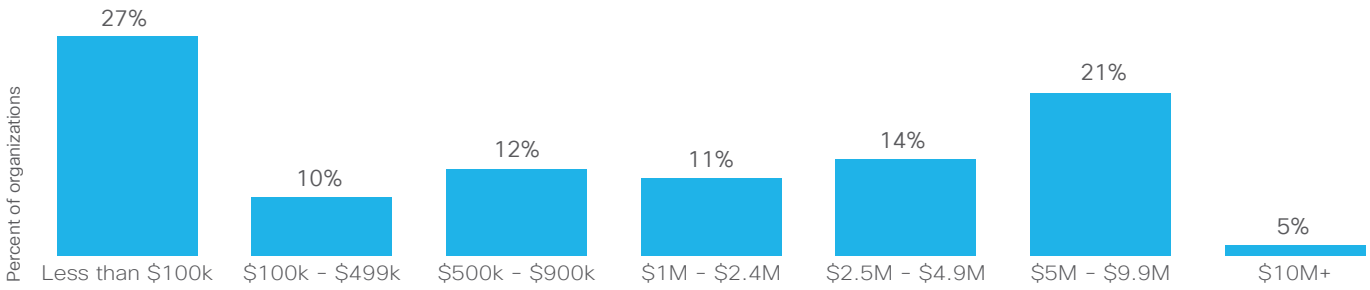
Figure 11 Number of daily security alerts in India



Q: On average, how many security alerts does your organization see on a daily basis?

The distribution of data about the cost of a breach is interesting in two areas; while India displays no statistical anomaly in the below USD$500,000 category, when you go deeper still and look at the sub-USD$100,000 category, it is a leader with 27% of respondents citing that as the cost of a breach. This compares with 23% in the nearest comparative country, China, and is way above Indonesia which has the smallest number of respondents in this category at 13%. This suggests that a larger number of Indian breaches cost less than regional neighbors. Until, that is, you look at the second standout figure from the report, which is the number of respondents who told us that a breach cost USD$5-10 million, which in India was a staggering 21% compared to the regional benchmark (9%) and the Australia figure (7%). Breaches create something like a lopsided well curve (see figure below), and are either very low cost in India or very high cost, with less in the middle of the cost distribution than in other markets. Australia, by comparison, is more of a bell curve with a fat middle and lean edges, suggesting that India is, at least from a defender's perspective in Asia, a market of extremes.

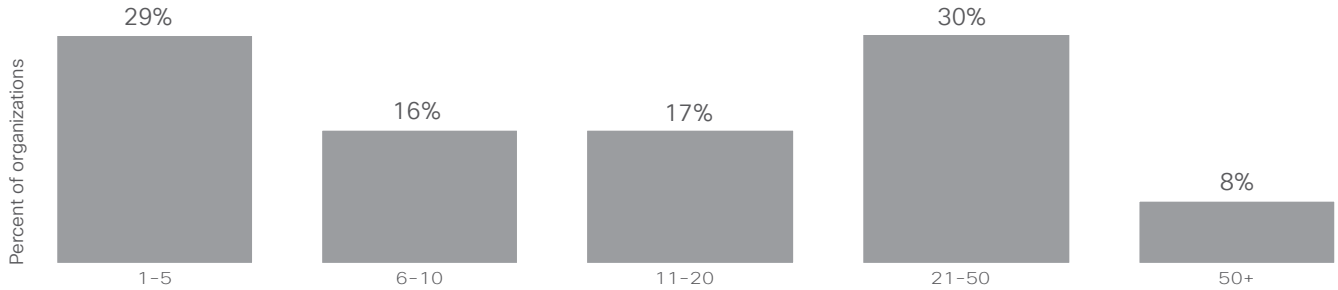
Figure 12 Cost of breaches in India



Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

And a number that India can stand proudly behind reveals that defenders are up to the fight offered by the threat landscape; 70% of respondents tell us that a breach drove improvements in security to a great extent, compared with the regional benchmark of 50% and Japan (15%). Along with China (50%), India leads in offering cybersecurity awareness training to staff following a breach (50% and the number one response), which demonstrates that, among other influencing factors, India is responding to concerns it has about the readiness of the people to fight cybercrime, as defenders in India cite lack of trained staff as the second highest reason for not adopting advanced security practices and technology.

Figure 13 Number of different security vendors in environment in India

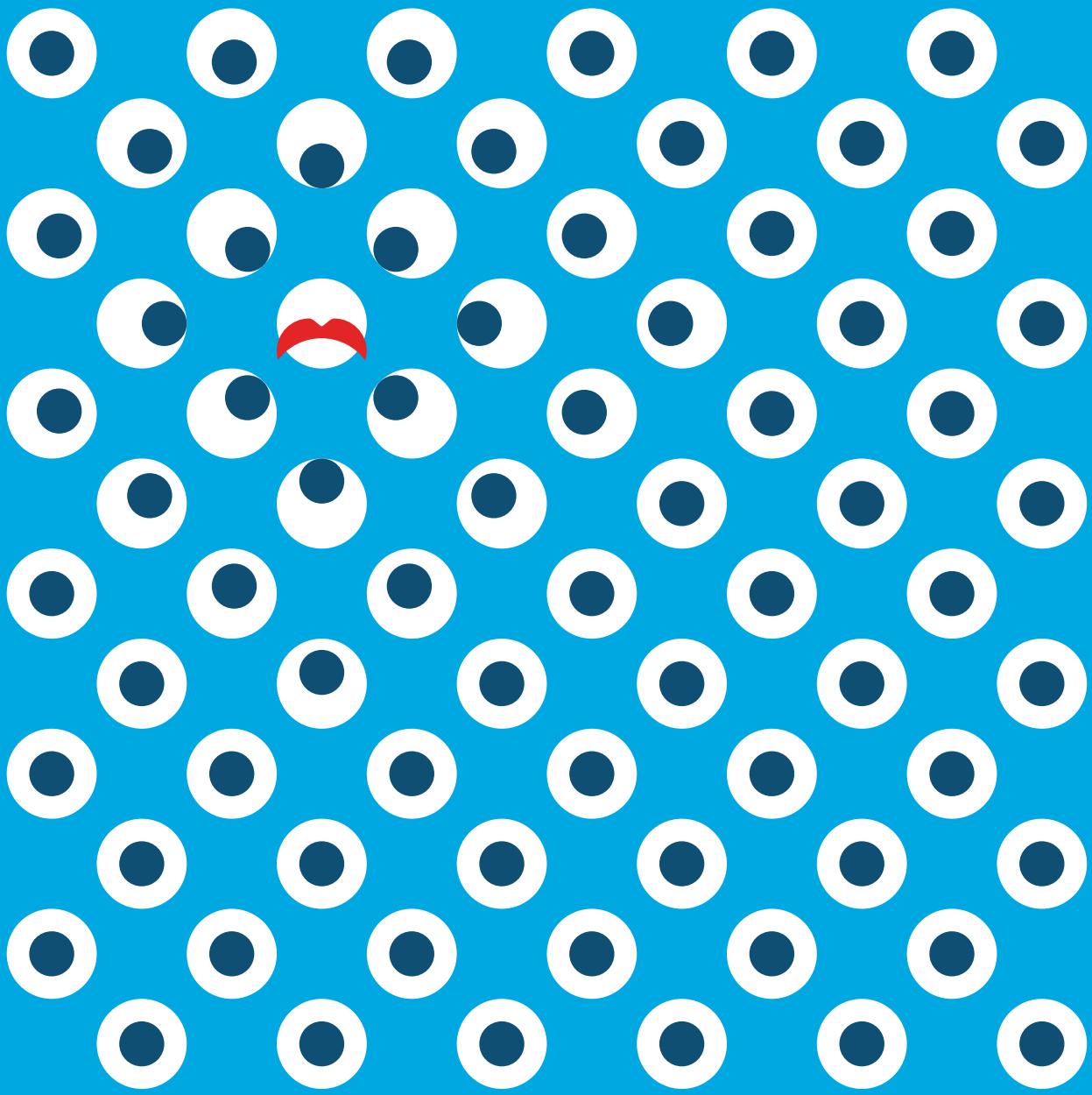


Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

India comes in second place with regards to the vendor environment they have built to respond to threats, with 57% reporting more than 10 vendors, which is higher than the regional benchmark of 47% and behind the regional leader Australia (73%). The same is true for the amount of respondents reporting more than 50 vendors (8%) which is ahead of the region (5%) and behind Australia (12%).

Perhaps not surprising then, when you consider the threat to business posed by considerable cost of some Indian breaches and the challenge offered by multi-vendor environments, that India leads the region in turning to automation to help solve the problem; 96% of respondents report that they use automation to reduce the level of effort compared with 83% regionally and 92% in Australia.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Indonesia Viewpoint

Country Overview

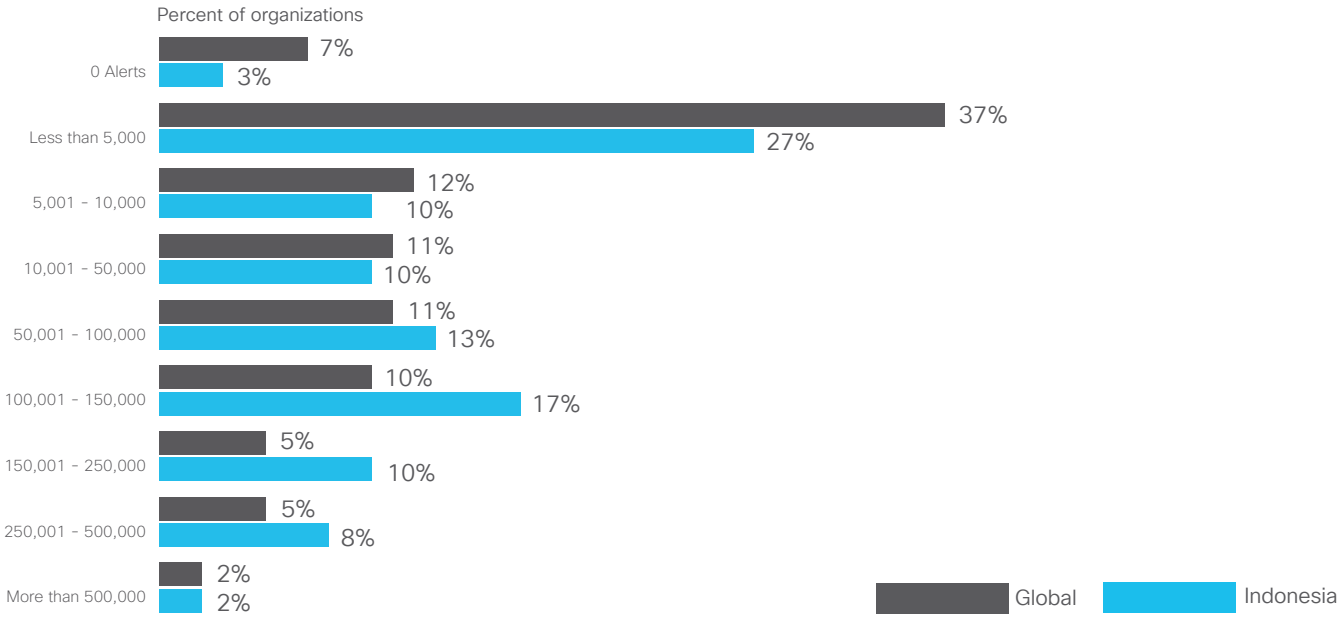
Indonesia Viewpoint:

Giant cyber problems need big answers

Like a resting giant, the vast archipelago of Indonesia lies peacefully wrapped around a huge swath of Southeast Asia, dominant both in land mass and population within the region. What we've learned through our research for the Indonesia viewpoint is that while the cybersecurity environment in this sprawling country is anything but peaceful, defenders here are facing fewer alerts than some of their regional neighbors. While 70% of companies see more than 5,000 alerts per day, 30% of respondents report seeing fewer than 5,000 alerts daily—lower than the regional benchmark of 31% and higher than Australia (19%) and Japan (21%).

Put simply a greater number of security teams are facing a smaller number of alerts. Less exciting is news from the other end of the spectrum where 17% of defenders are facing 100 – 150,000 alerts per day, which is third highest in the region behind Australia (33%) and Thailand (19%); it seems some are dealt an easier hand in Indonesia while a large number are playing with some very bad cards.

Figure 14 Number of daily security alerts in Indonesia

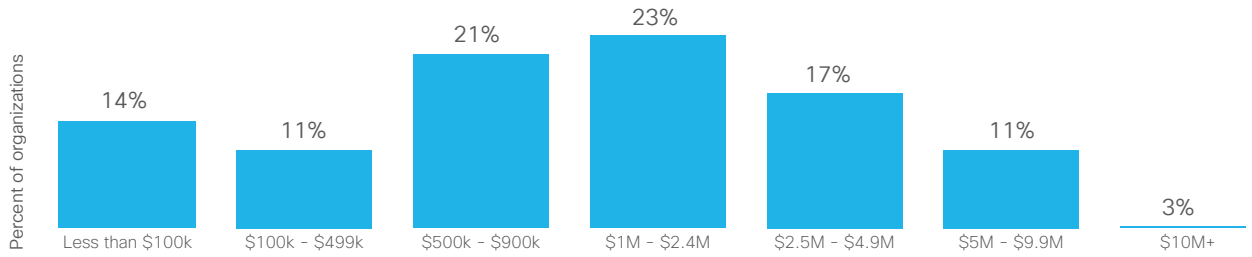


Q: On average, how many security alerts does your organization see on a daily basis?

If cybersecurity were a game of cards, the winning hand is held by the player who can respond fastest to the greatest number of alerts, identify which are genuine and remediate those that pose the greatest threat to the organization. In this scenario, Indonesia does not hold any aces. Despite reporting that they face as many alerts if not more than their neighbors, Indonesian defenders are only able to respond to 47% of alerts, which is behind both regional (56%) and global benchmarks (56%) but ahead of individual countries such as China (36%) and Thailand (37%). It seems that defense teams are better able to identify which alerts are more important as Indonesia reports that 38% of alerts are legitimate, which is above the global benchmark (34%) but behind the regional number (44%). This suggests that they are doing better than some in keeping up with the demands of the modern threat landscape.

Discovering the right alerts is only one part of delivering an efficient, coordinated response; you also have to do something about the problem once you find it. Indonesia lags in the number of legitimate alerts that are remediated at only 42%, second last only to Thailand (37%) and behind the regional benchmark (53%).

Figure 15 Cost of breaches in Indonesia



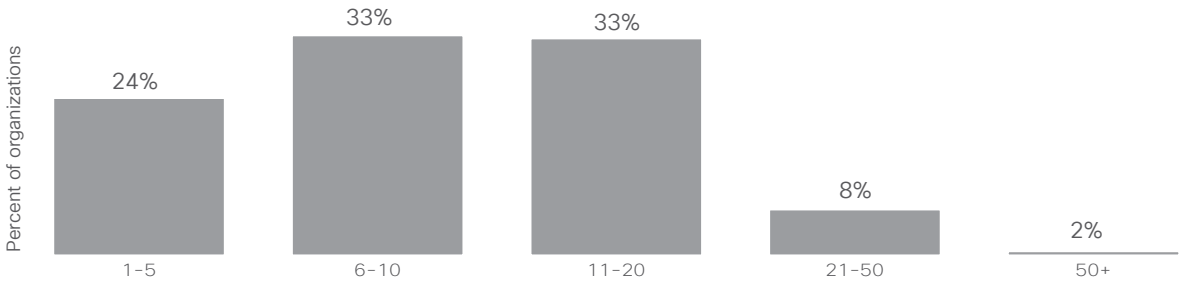
Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

The cost of a breach is as prohibitive in Indonesia as elsewhere, with the price tag fairly consistent across the board; fewer people report that breaches cost less than USD$100,000 (14%) compared with 20% for the region and 30% for worldwide comparison; a fairly high 40% report that breaches cost between USD$1-5 million compared with a worldwide figure of 30% and a regional benchmark of 33%. What's most noticeable for this country with one of the lower per capita GDPs in the region is that 3% still put the cost of a breach above USD$10 million and this is in the range as the regional benchmark (5%) and equal to the worldwide standard.

What really matters in the face of the evidence of large numbers of un-investigated alerts and the increasing cost of breaches, is the response by defenders; in Indonesia there is still much work to do in this area. Training of staff is fourth on the list of priorities, and in a market where there is an acute shortage of skilled cybersecurity professionals, continuing to train new staff and hone the skills of existing defenders would seem to be crucial. This is particularly true when you consider that 31% report that breaches were discovered and disclosed by a third party, which is higher than the global (28%) and regional benchmark (29%). Defenders don't seem as jaded in Indonesia, with 58% claiming to suffer from cyber fatigue which is in line with the regional benchmark, ahead of the worldwide figure (46%), and well behind Japan (76%) and Australia (69%); training talent that still has plenty of energy could make a real difference.

And solving people challenges is something that cybersecurity managers should focus on to more accurately deal with that high volume of alerts before defenders in Indonesia face insurmountable odds and fatigue increases.

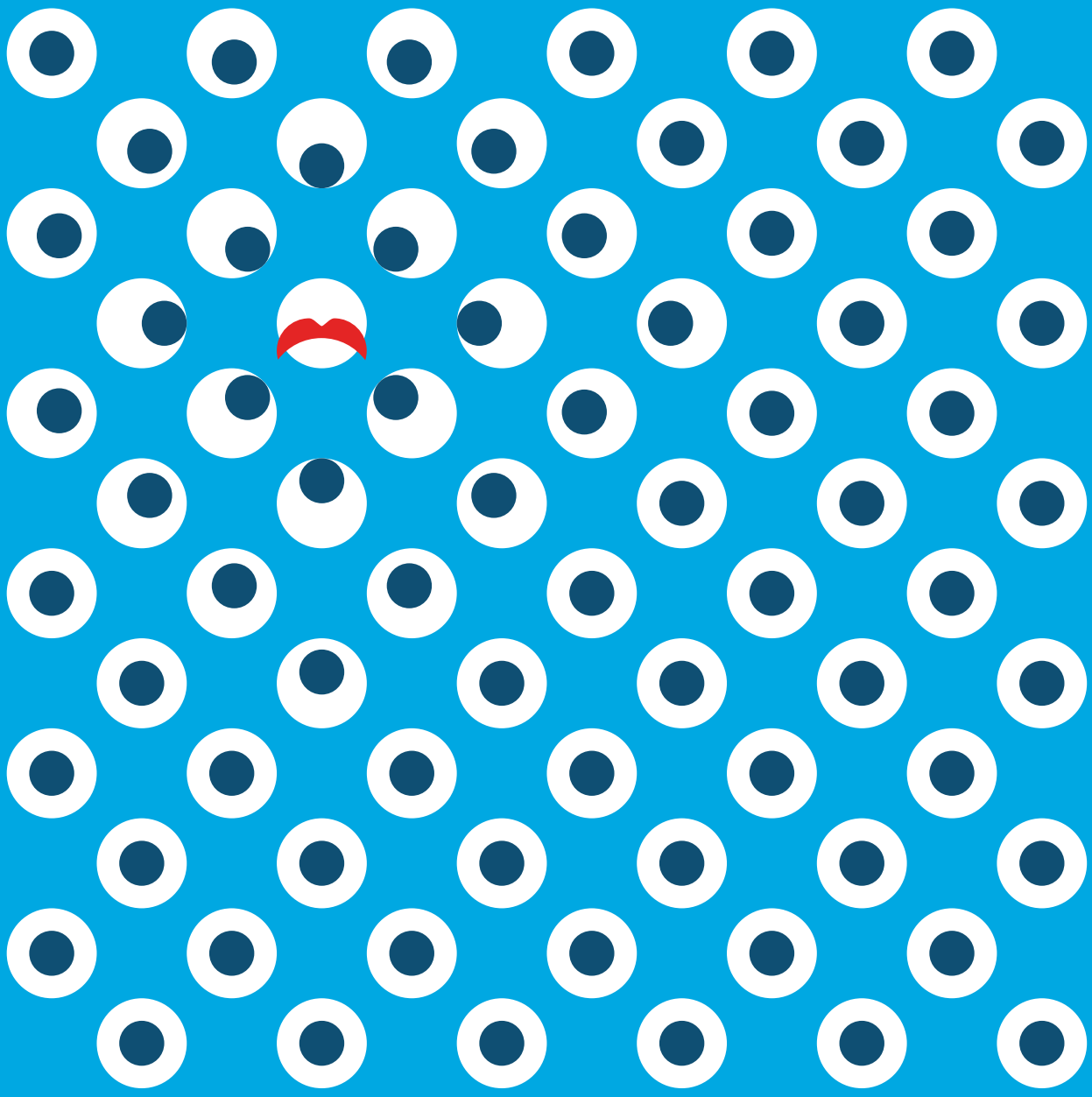
Figure 16 Number of different security vendors in environment in Indonesia



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

More people are needed to deal with more products and devices, and Indonesia has been investing in building well-stocked environments with which to deal with the ever-changing threat landscape. Following the maxim that less is more and that fewer products means fewer gaps through which attackers can move. 43% report having more than 10 vendors in their security environment and 52% have more than 10 products. This means Indonesia is keeping better control than Australia with 73% there reporting more than 10 vendors and 76% more than 10 products. Indonesia does even better towards the top end of the scale, with only 9% reporting having more than 50 products which is better than the global (13%) and regional (16%) benchmarks, none of which is clear in terms of next steps, especially when you consider that 87% of Indonesia defenders responded that it was somewhat or very difficult to orchestrate alerts from multiple vendors, which is higher than the region (82%) and the global benchmark (74%) but lower than some regional colleagues. With a lower record on alert identification and remediation, better scores on cyber fatigue and training, Indonesia has to find a way to direct its cybersecurity professionals' energy towards better training to figure out how to solve the sprawling cyber challenges of giant Indonesia.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Japan Viewpoint

Country Overview

Japan Viewpoint:

Strong security results in cyber fatigues

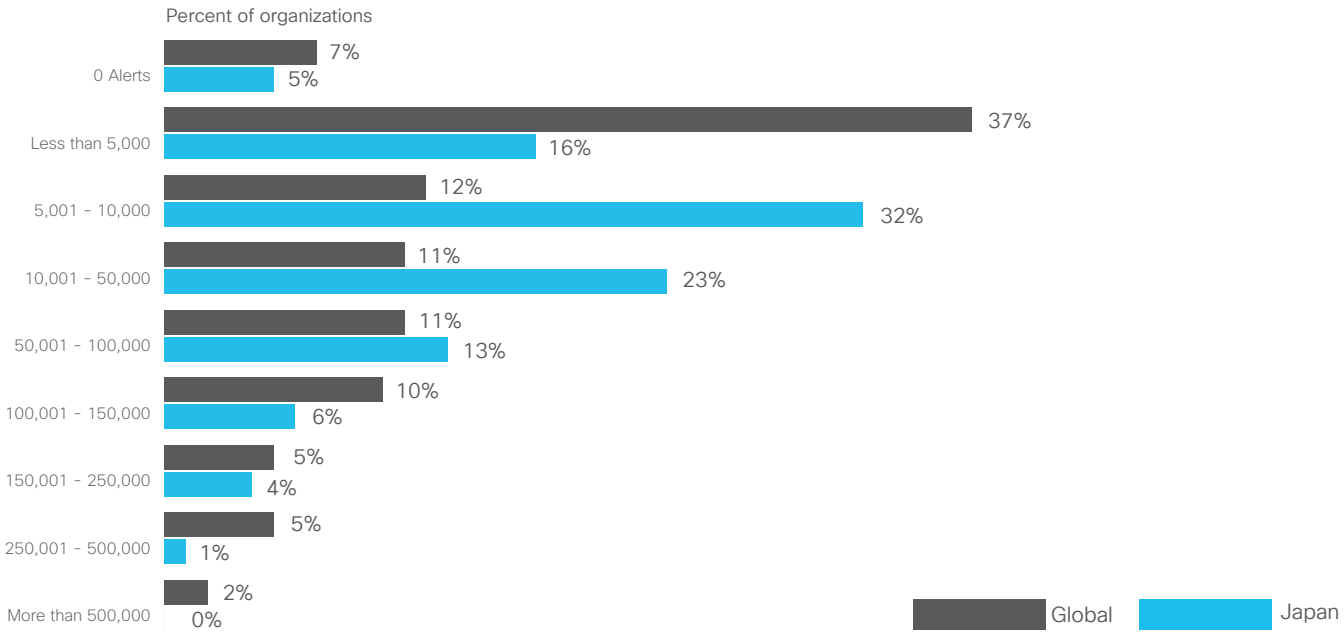
What we've learned through our research for the Japan viewpoint is that this second largest of Asia's economies lands squarely in the middle for many of the key indicators: not too hot and not too cold runs the defender landscape across topics such as volume of alerts and cost of a breach, and Japan is fully in line with the rest of the world in terms of multi-vendor environment management.

Certainly there are some discrepancies when you drill into the details, like how 79% of companies see more than 5,000 alerts per day, for example. The 21% of Japanese defenders who report seeing fewer than 5,000 alerts per day is low compared to the global benchmark of 44% but when you move the needle to look at 10,000 alerts per day or fewer, the difference is wiped out, with the number at 53% for Japan and 56% global. And when you get to the upper end of the scale, Japan has the lowest number of defenders reporting 100-150,000 alerts per day across the whole region, with 6% in this category compared with the regional benchmark of 15%. The number of alerts investigated that turn out to be legitimate and then get remediated are also reasonably in line with global and regional benchmarks; in this space, Japan is roughly on par with India, ahead of China and behind Australia.

Investigating alerts is only the first step; defenders also need to ensure that they are working on the right items, especially given the vast number of alerts they have to address. It turns out that only 45% of investigated alerts are legitimate, which is second highest in the region, well behind the leader Australia (65%) but is better than both the global benchmark (34%) and the regional standard (44%). This means a full 55% of investigated alerts are false alarms, so not only is malware getting through the pile of logs that are not attended to, but a vast amount of valuable work is being done on files that don't need it.

The percentage of legitimate alerts that are eventually remediated is 51% which is on par with the global (50%), and Asia Pacific (53%) benchmarks, and is second again only to Australia (69%).

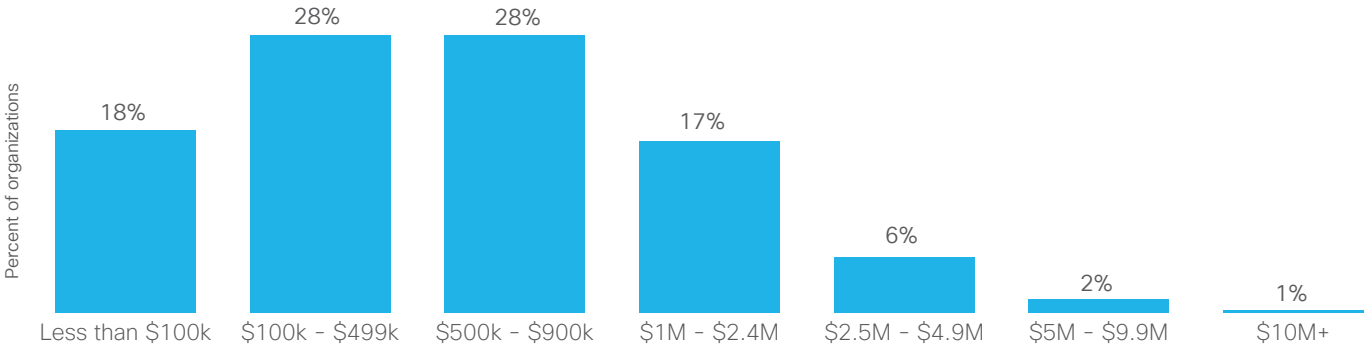
Figure 17 Number of daily security alerts in Japan



Q: On average, how many security alerts does your organization see on a daily basis?

All of which is interesting because it's possible that there is some good news, at least if the reported cost of breach is anything to go by. The dollar figure assigned to the cost of the breach appears to be lower in Japan than anywhere else, with 74% of respondents reporting that breaches cost under USD$1 million, compared with only 32% in the same bracket in Australia. Only 23% are in the USD$1-5 million bracket, compared with 52% in this band in Australia, where we see the highest cost of breaches and a 33% benchmark within the region. Even India, where you might expect costs to be lower, reports more breaches costing USD $1-5 million (25%) and also reports more breaches costing over USD$10 million (5%) compared with Japan (1%).

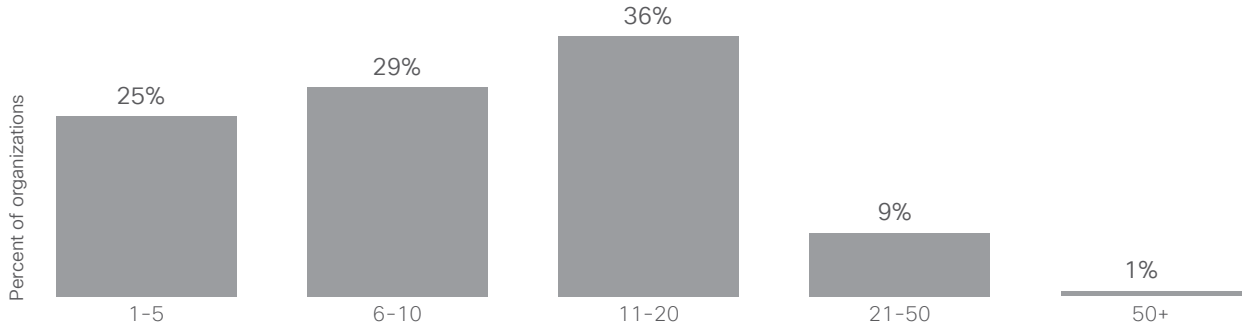
Figure 18 Cost of breaches in Japan



Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

Cracks start to emerge in the Japanese security story when you examine the response to a breach. First of all, only 15% report that a breach drove improvements to a great extent, lower than global benchmarks (47%) and the leading regional countries, Australia (81%) and India (70%). Add to that the fact that Japan is the least likely to train staff in the wake of an incident (33% and 10th on the list of priorities), and they are least likely to automate their defenses (27%, last on the list of 12 priorities). This is doubly worrying when you consider that Japanese defenders (28%) cite "lack of trained staff" as the third biggest obstacle to adopting advanced security technology. When you consider that Japan is the only country to admit "reluctance to purchase until technology is proven" (as the second biggest obstacle at 28% of respondents) you could be forgiven for wondering if Japan has yet joined the dots and completed the narrative on security; it would certainly be interesting to see what changes could be identified in the readiness for a breach if staff were better trained and the latest technology deployed.

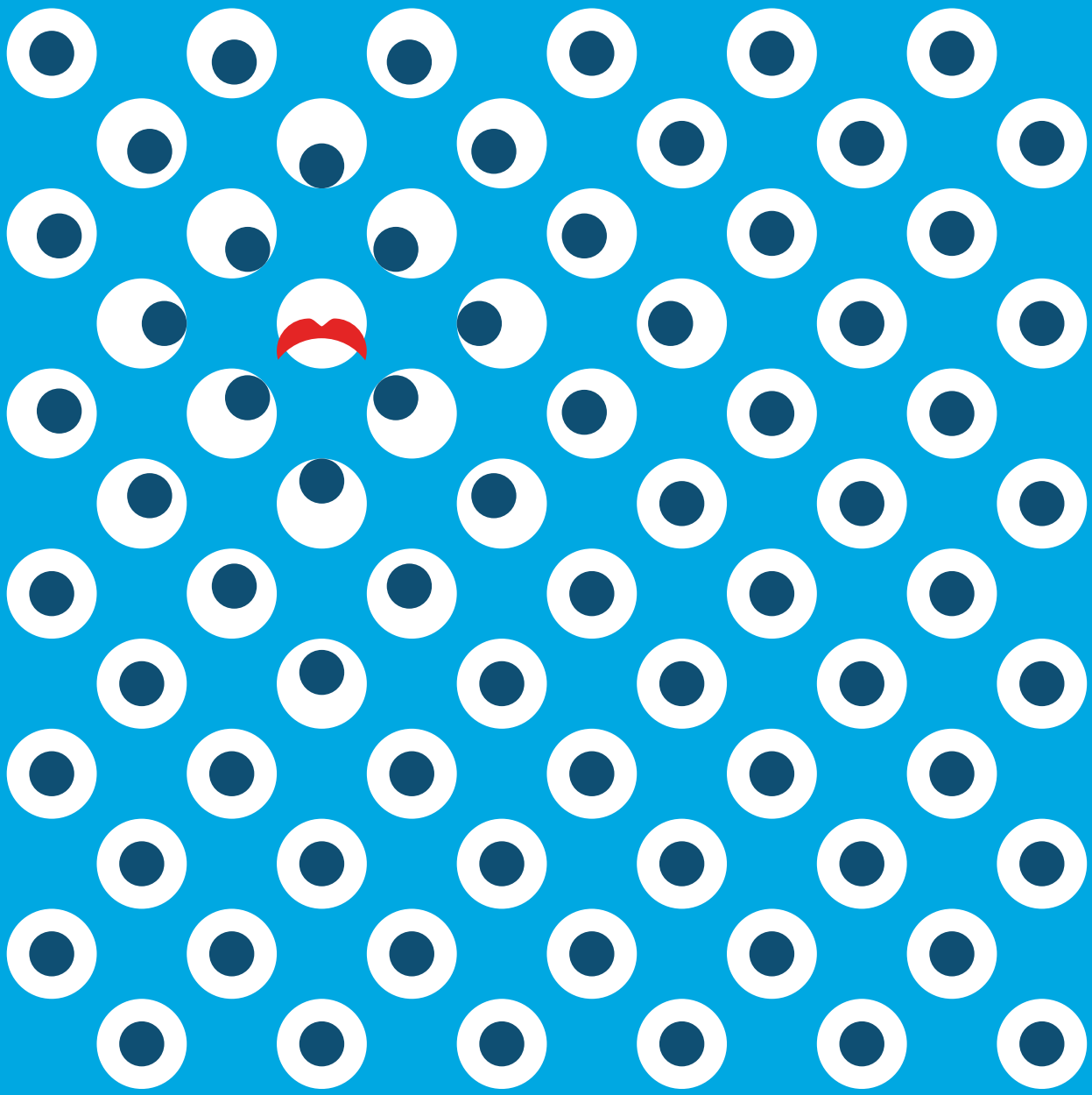
Figure 19 Number of different security vendors in environment in Japan



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

All of which sets up the biggest discrepancy of all; Japan reports a standard to low number of vendors and products in their security stack, reports the least difficulty in orchestrating alerts, which is not surprising if the environment is simpler, and yet they report the highest levels of cyber fatigue in the region. Only China is lower (30%) when reporting more than 10 vendors in their environment as compared to Japan (46%), and yet only 60% find it somewhat or very challenging to orchestrate alerts, compared with 82% in Australia and a whopping 95% in China. All this and still 76% of respondents claim cyber fatigue, compared with Australia (69%) and the region (59%).

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Korea Viewpoint

Country Overview

Korea Viewpoint:

Training needed in the fight against bad actors

What we've learned through our research for the Korea viewpoint is that the country faces large cybersecurity challenges: 61% of companies see more than 5,000 alerts per day. Only 39% of Korea defenders report seeing fewer than 5,000 alerts, which is lower than the global standard of 44% but comfortably higher than the regional benchmark of 31%.

This means that Korea is out in front within Asia Pacific in pushing the number of daily alerts seen lower. This reduces the amount of work needed and allows already overworked security teams to focus on what is important. There is good news at the top end of the spectrum as a lower proportion of Korea defenders (14%) are seeing 100–150,000 alerts per day, higher than global (10%) and below the region (15%).

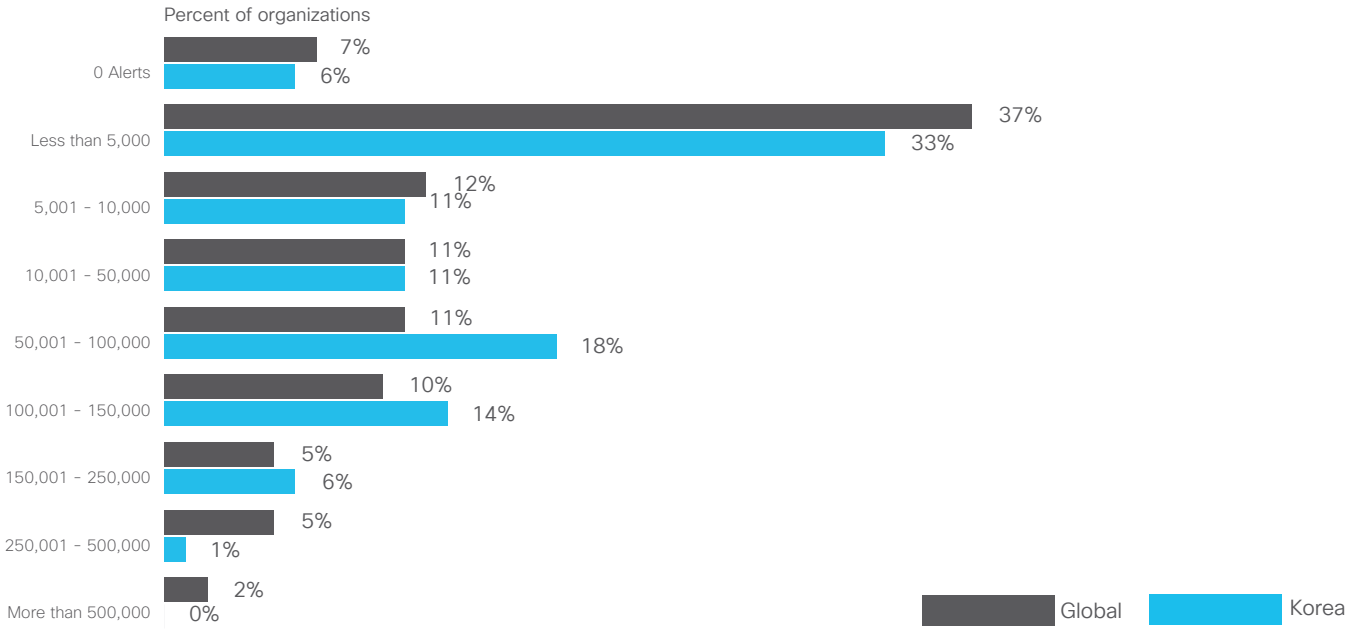
The good news is not sustained and 70% of alerts are not investigated. Delivering an efficient, coordinated response to alerts is also clearly a challenge, and only 30% of alerts are investigated each day. This does not compare well with the global and regional benchmarks, which at 56% is already unacceptably low, this means that 70% of alerts are not acted on, which in turn shows either lack of capability or capacity. For the small number of companies with up to 150,000 alerts, this means tens of thousands of incidents not triggering a response. Which alerts contain malware? That's anyone's guess. Korea defenders need to find new ways to scale their operations and get to more alerts.

Investigating alerts is only the first step. Defenders also need to ensure that they are working on the right items, especially given the vast number of alerts they have to address.

It turns out that only 16% of investigated alerts are legitimate, which is by far the lowest in the region, below second lowest China (23%) and is even a little behind the global benchmark (34%). It trails behind the regional standard (44%) and compares unfavorably with the stronger countries in region, such as Australia (69%). This means a full 84% of investigated alerts are false alarms, so not only is malware getting through the pile of logs that are not attended to, but a vast amount of valuable work is being done on files that don't need it.

The percentage of legitimate alerts that are eventually remediated is 40%, which is behind the global (50%), and Asia Pacific (53%) benchmarks, and is, in fact, amongst the lowest in the region with only Thailand (37%) and Vietnam (39%) lower.

Figure 20 Number of daily security alerts in Korea



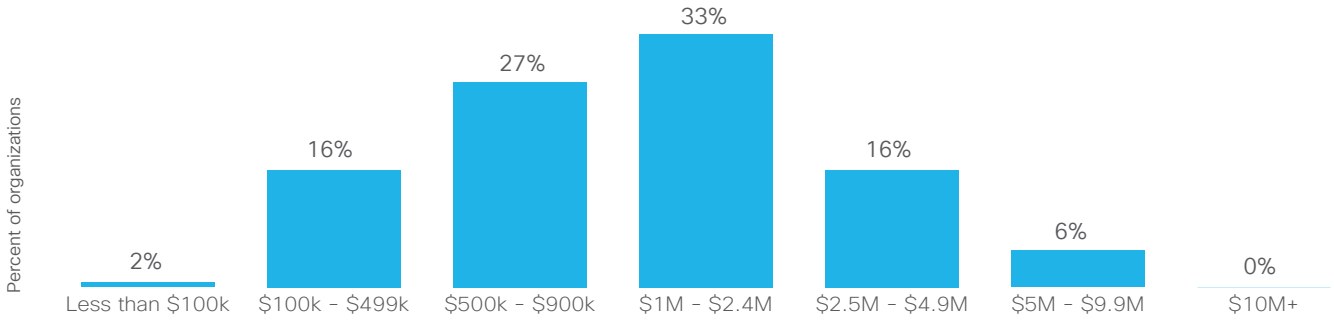
Q: On average, how many security alerts does your organization see on a daily basis?

This tells us that Korea defenders have work to do all the way through the funnel, from managing vast numbers of alerts, and then sifting through that mass to find what needs to be investigated, and then remediating more of the alerts.

This is particularly worrying because breaches are just as costly in Korea. Compared to the region, more alerts in Korea cost between USD$1-5 million (49%) than Asia Pacific (33%) and the global standard (30%).

The scales tip towards the lower end of the breach dollar impact in the Korea, where only 2% of breaches cost under USD$100,000 compared with the region (20%) and the globe (30%). The second standout figure from the report is that none of the incidents cost more than USD$10 million which is low compared with the region (5%) and the worldwide number (3%), and comfortably under the Australian figure (9%), the regional high watermark, suggesting that breach costs are not yet out of control.

Figure 21 Cost of breaches in Korea

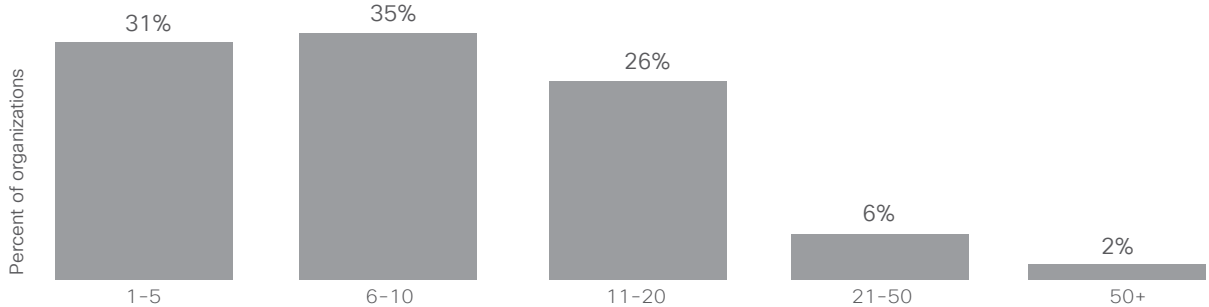


Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

What really matters in these analyses is examining the response to breaches, and Korea is less in line with regional best practices. 54% of respondents engaged staff in training and it was top of the list of responses. This is an obvious win, when "lack of knowledge" was cited as a top three reason for the lack of adoption of advanced security processes. Also in the top three were "compatibility with legacy systems," and, at number one like many other countries, lack of budget.

Stakeholder and board-level management are required to make real progress. And solving people challenges is something that cybersecurity managers cannot ignore; a mere 39% of respondents claimed that they were suffering from cyber fatigue, low compared to the region (59%) but that is still over a third of the defenders needing to learn better ways to more accurately deal with that high volume of alerts before they drown in a sea of un-investigated alerts.

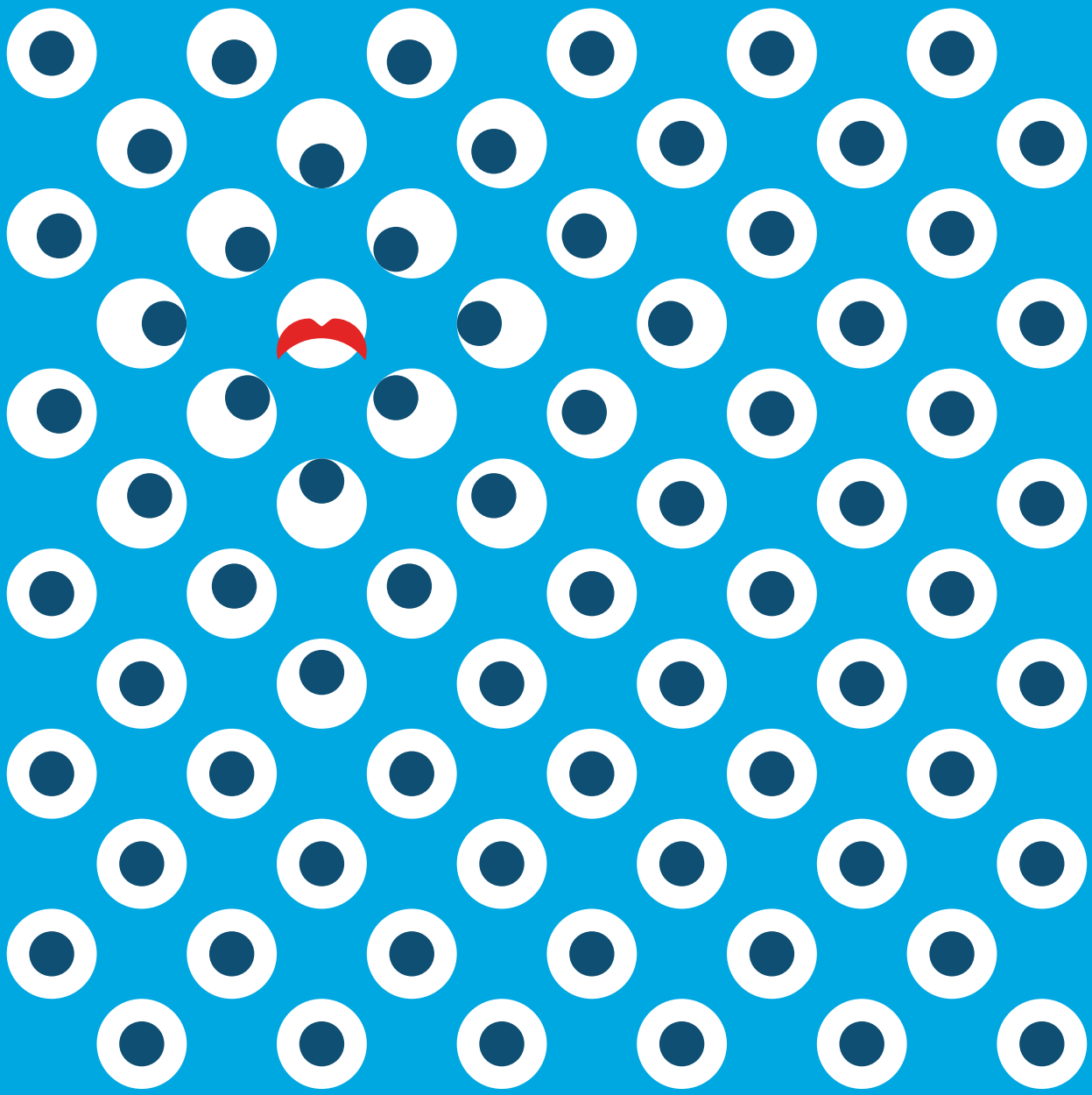
Figure 22 Number of different security vendors in environment in Korea



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

It's not as if Korea has not been investing in building well-stocked environments to deal with the ever-changing threat landscape: 34% have more than 10 vendors and 50% have more than 10 products. Following the maxim that fewer products means fewer gaps through which attackers can move, this means Korea is keeping better control than Australia with 73% there reporting more than 10 vendors and 76% more than 10 products. The cause of cyber fatigue lies in the numbers: 92% of Korea defenders responded that it was somewhat or very difficult to orchestrate alerts from multiple vendors, which is higher than the region (82%) and the global benchmark (74%). They may not all admit fatigue but they are as overwhelmed as any other country in the fight against the growing threat. Training, orchestration and automation will go a long way to solving Korea's cybersecurity challenges.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Malaysia Viewpoint

Country Overview

Malaysia Viewpoint:

Getting to simple security ain't easy

What we've learned through our research for the Malaysia viewpoint is that the country is under attack and is fighting back. A full 63% of companies report seeing more than 5,000 alerts per day, meaning only 37% of Malaysia defenders report seeing fewer than 5,000 alerts; lower than the global standard of 44% and slightly higher than the regional benchmark of 31%.

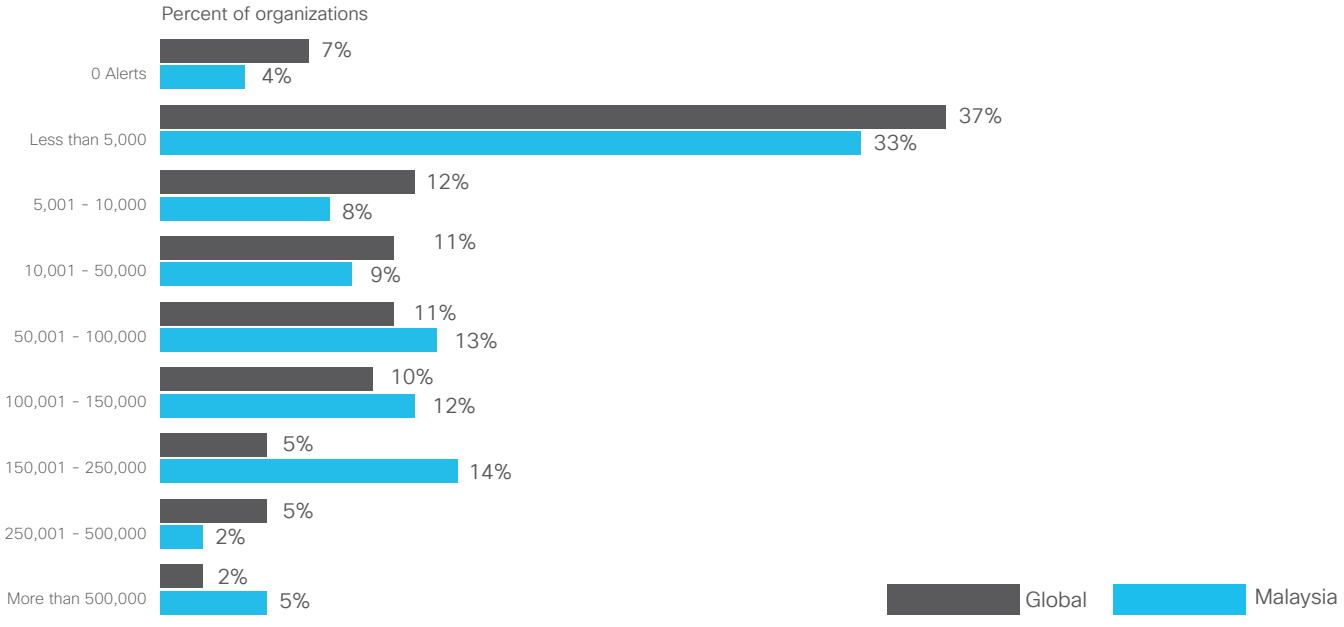
This means that Malaysia—and the region—has more work to do in pushing the number of daily alerts seen lower through techniques such as automation. There is good news at the top end of the spectrum as a lower proportion of Malaysian defenders (12%) are seeing 100-150,000 alerts per day, than both global (10%) and the region (15%), and on par with India (8%) in Asia Pacific.

The challenging news does not stop there, because delivering an efficient, coordinated response to alerts is also an area that Malaysia's security practice are still grappling with. 60% of alerts are not investigated, meaning only 40% of alerts are investigated each day. Compared with the global and regional benchmarks, which at 56% is already low, this shows either lack of capability or capacity. Given the global shortage of cybersecurity talent, it would seem that Malaysia defenders are probably stretched with their current workload and so need to find new ways to scale their operations.

Investigating alerts is only the first step; defenders also need to ensure that they are working on the right items; especially given the vast number of alerts they have to address. It turns out that only 36% of investigated alerts are legitimate, which is not the lowest in the region (Singapore, 25%) and is a little ahead of the global benchmark (34%) but is behind the regional standard (44%) and trails behind India (52%) and Australia (69%).

The percentage of legitimate alerts that are eventually remediated is 42%. This is not only behind the global (50%), and Asia Pacific (53%) benchmarks, it is also the lowest in the region with only Thailand (37%) and Vietnam (39%) lower. This tells us that Malaysia defenders have work to do all through the funnel, from managing vast numbers of alerts, sifting through that mass to find what needs to be investigated and then remediating more of the alerts.

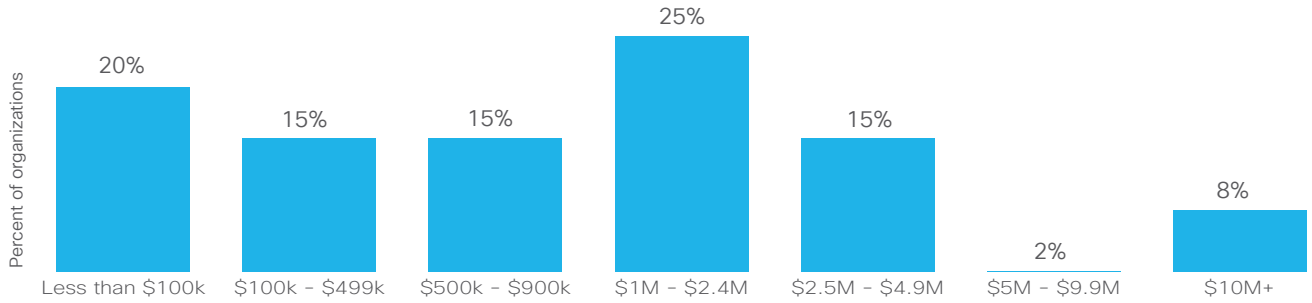
Figure 23 Number of daily security alerts in Malaysia



Q: On average, how many security alerts does your organization see on a daily basis?

This is particularly worrying because breaches are just as costly in Malaysia. Compared to the region, fewer alerts in Malaysia cost between $1-5 million (40%) than Asia Pacific (33%) and the global standard (30%). A highlight for Malaysia is that a whopping 20% of breaches cost under USD$100,000 compared with the region (20%) and the globe (30%). The second standout figure from the report is that a huge 8% of incidents cost more than USD$10 million which is high compared with the region (5%) and the worldwide number (3%), and comparable as the Australian figure (10%). This suggests that breach costs are higher than should be expected and are potentially spiralling out of control.

Figure 24 Cost of breaches in Malaysia

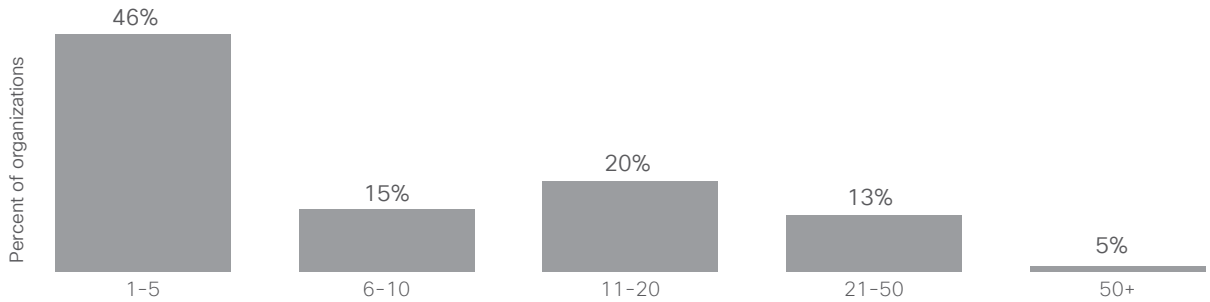


Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

What really matters in these analyses is examining the response to breaches and Malaysia here has some good news. 59% of respondents tell that primary response to a breach was to engage staff in training. It was top of the list of responses compared with countries like Australia where staff training only ranked as fifth priority, and Japan where training was only 10th on the list. This is particular enlightened of defenders in Malaysia when you consider that "lack of knowledge" was cited as the third most popular reason for the lack of adoption of advanced security processes. Solving the people problem goes a long way to addressing the security challenge. Like global and regional responses indicated, Malaysia also cited budget as the number one challenge in this area which suggests that stakeholder and board-level management are required to make real progress.

Solving people challenges is something cybersecurity managers cannot ignore. A mere 49% of respondents claimed that they were suffering from cyber fatigue– low compared to the region (59%) but that still means half of the defenders need to learn better ways to more accurately deal with a high volume of alerts before they drown in a sea of uninvestigated alerts.

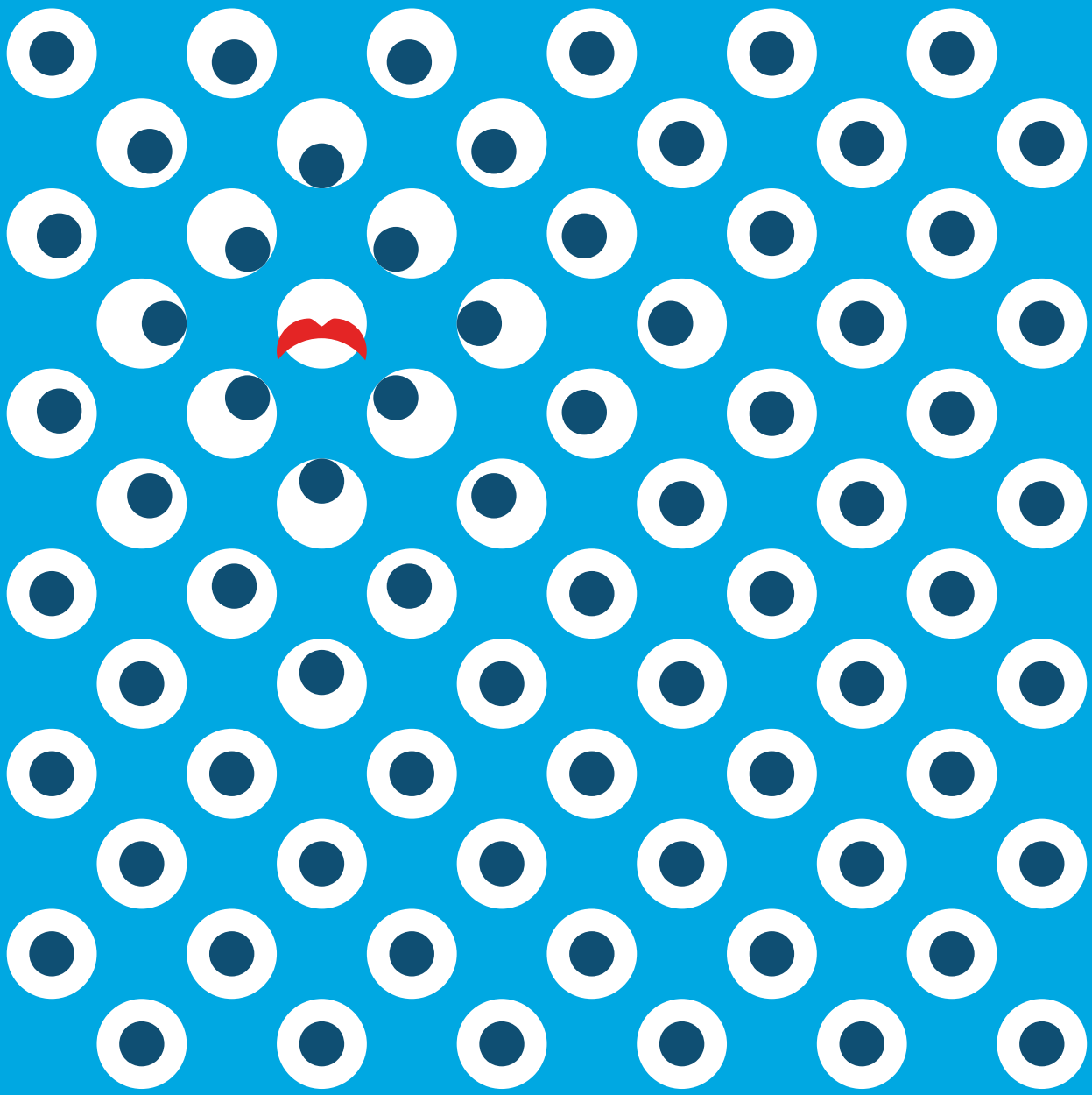
Figure 25 Number of different security vendors in environment in Malaysia



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

It's not as if Malaysia has not been investing in building well-stocked environments to deal with the ever-changing threat landscape: 39% have more than 10 vendors and 37% have more than 10 products. Following the maxim that fewer products means fewer gaps through which attackers can move, this means Malaysia is keeping better control than Australia with 73% there reporting more than 10 vendors and 76% more than 10 products. The cause of cyber fatigue lies in the numbers: 98% of Malaysia defenders responded that it was somewhat or very difficult to orchestrate alerts from multiple vendors, which is higher than the region (82%) and the global benchmark (74%). Training, orchestration and automation will go a long way to solving Malaysia's cybersecurity challenges.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Philippines Viewpoint

Country Overview

Philippines Viewpoint:

Rapid remediation reduces breach impact

In the Philippines, a massive 53.% of companies report seeing more than 5,000 alerts per day which means everyone is busy. The 48% of Philippines' defenders who report seeing fewer than 5,000 alerts is much lower than the global standard of 44% but comfortably higher than the regional benchmark of 31%.

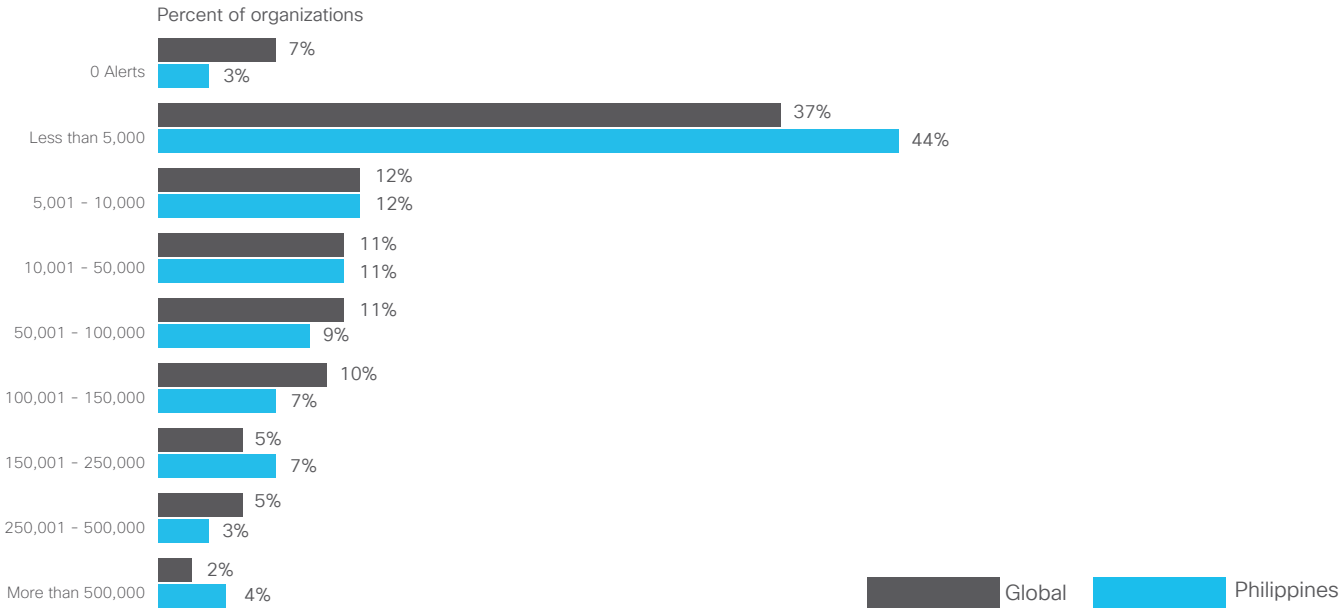
This means that the Philippines is ahead of the region in pushing the number of daily alerts seen lower. This reduces the amount of work needed and allows already overworked security teams to focus on what is important. There is good news at the top end of the spectrum as a lower proportion of Philippines defenders (7%) are seeing 100-150,000 alerts per day, than both global (10%) and the region (15%). This makes them similar to Japan (6%), the country in Asia Pacific with the lowest score in this range.

However, 51% of alerts are not investigated.Delivering an efficient, coordinated response to alerts is also clearly an area that the Philippines' security practice is still grappling with. The 49% of alerts that are investigated each day compares well with the global and regional benchmarks, which at 56% is already low. This means that 51% of alerts are not acted on, which shows either lack of capability or capacity. Which alerts refer to a real threat? That's anyone's guess. Philippines defenders need to find new ways to scale their operations and attend to more alerts.

Investigating alerts is only the first step; defenders also need to ensure that they are working on the right items, especially given the vast number of alerts they have to address. It turns out that only 32% of investigated alerts are legitimate, which means a full two-thirds of alerts are false alarms. This is not the lowest in the region (Korea, 16%) and is even a little behind the global benchmark (34%). It trails behind the regional standard (44%) and compares unfavorably with the stronger countries in region, India (44%) and Australia (65%).
Not only is malware getting through the pile of logs that are not attended to, but a vast amount of valuable work is being done on files that don't need it.

The percentage of legitimate alerts that are eventually remediated is 49%—only a fraction behind the global (50%) and Asia Pacific (53%) benchmarks, and is, in fact, amongst the highest in the region with only India (52%), Japan (51%) and Australia (69%) higher. This tells us that the Philippines' defenders have work to do at the midpoint of the funnel, from managing vast numbers of alerts, then sifting through that mass to find what needs to be investigated. They are doing better than many at remediating more of the alerts.

Figure 26 Number of daily security alerts in the Philippines

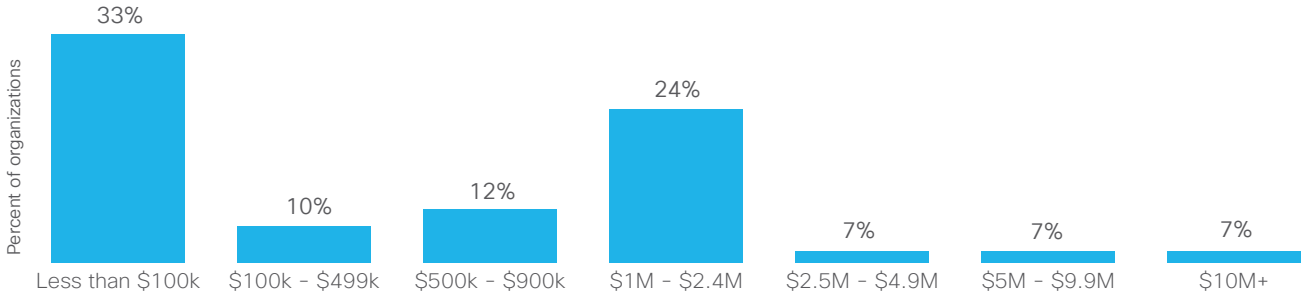


Q: On average, how many security alerts does your organization see on a daily basis?

This is particularly worrying because breaches are just as costly in the Philippines, where 67% of breaches cost more than USD$100,000. Compared to the region, way fewer alerts in the Philippines cost between USD$1-5 million (31%) than Asia Pacific (33%) and the global standard (30%).

The scales tip towards the lower end of the breach dollar impact in the Philippines, where a solid 33% of breaches cost under USD$100,000 compared with the region (20%) and the globe (30%).

Figure 27 Cost of breaches in the Philippines

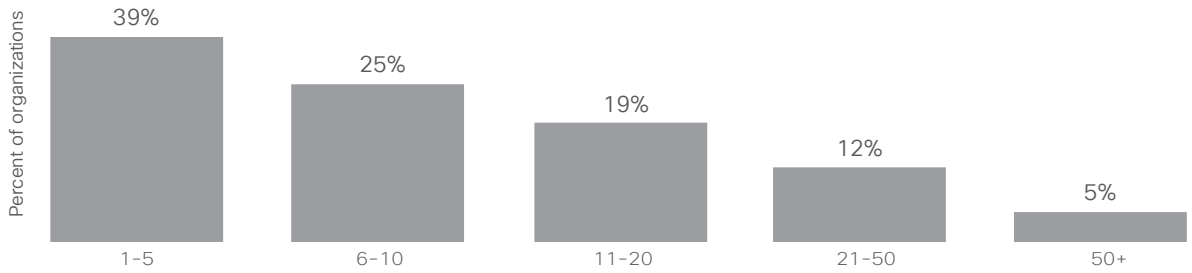


Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

What really matters in these analyses is examining the response to breaches and the Philippines is less in line with regional best practices. 44% of respondents tell that top of the list of responses to a breach was to engage staff in training. It was 9th of the list of responses compared with countries like Thailand, India and Malaysia where it only ranked top; it's more in line with Japan where training was only 10th on the list. Critics of this approach might be silenced by the country's impressive alert remediation performance; in the Philippines, "lack of knowledge" was not cited as a top three reason for the lack of adoption of advanced security processes. Much more important were compatibility with legacy systems, unwillingness to try new solutions until they are proven and, at number one like many other countries, lack of budget. Stakeholder and board-level management are required to make real progress.

Solving people challenges is something that cybersecurity managers cannot ignore. A mere 27% of respondents claimed that they were suffering from cyber fatigue, low compared to the region (59%). But that is still over a quarter of the defenders needing to learn better ways to more accurately deal with that high volume of alerts are needed before they drown in a sea of un-investigated alerts.

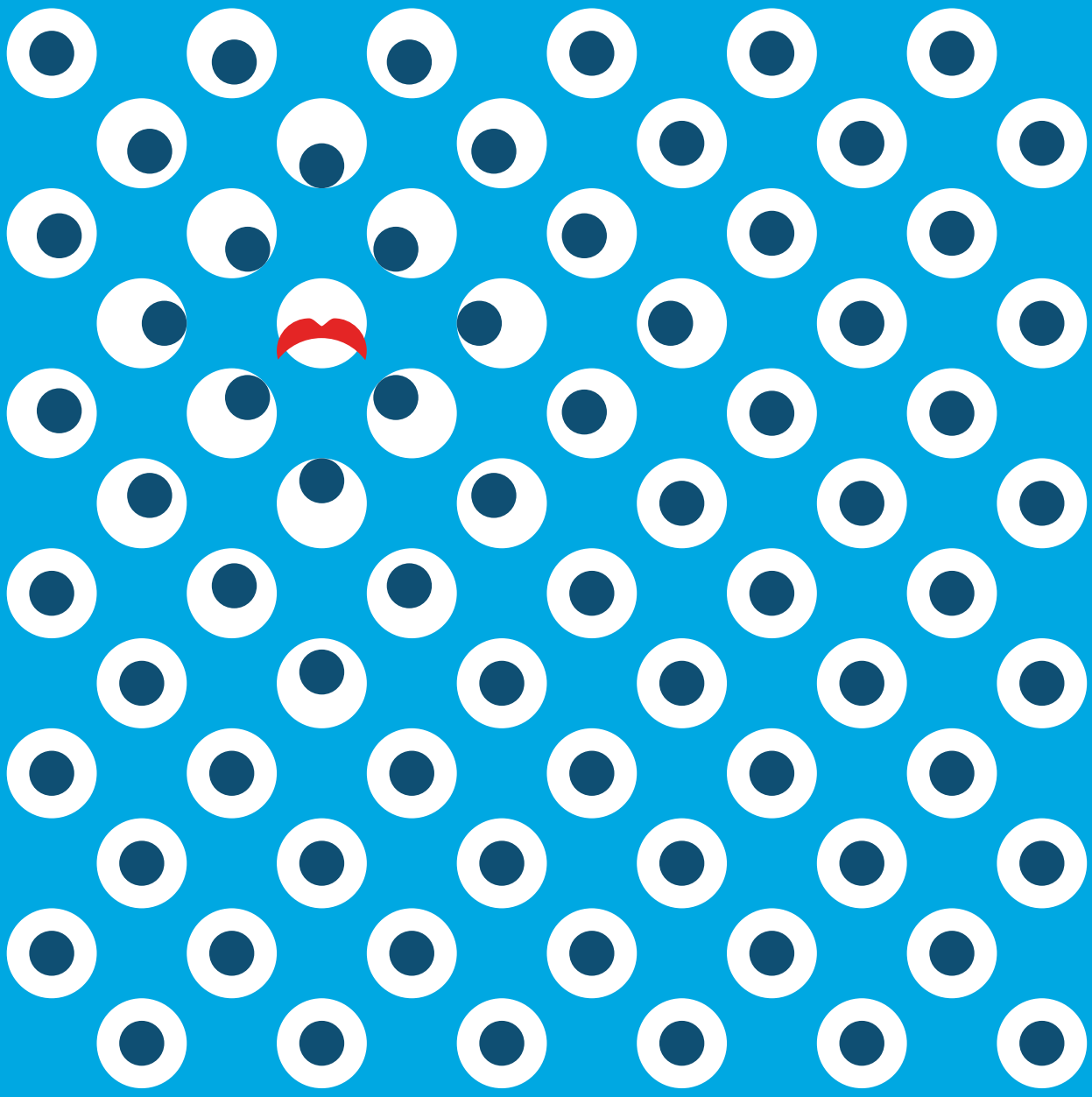
Figure 28 Number of different security vendors in environment in the Philippines



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

It's not as if the Philippines has not been investing in building well-stocked environments with which to deal with the ever-changing threat landscape: 36% have more than 10 vendors and 33% have more than 10 products. Following the maxim that fewer products means fewer gaps through which attackers can move, this means the Philippines is keeping better control than Australia with 73% there reporting more than 10 vendors and 76% more than 10 products. The cause of cyber fatigue lies in the numbers: 96% of the Philippines defenders responded that it was somewhat or very difficult to orchestrate alerts from multiple vendors, which is higher than the region (82%) and the global benchmark (74%). They may not admit fatigue but they are as overwhelmed as any other country in the fight against the growing threat. Training, orchestration and automation will go a long way to solving Philippines' cybersecurity challenges.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Singapore Viewpoint

Country Overview

Singapore Viewpoint:

Rapid responses and effective remediation curb cyber fatigue

What we've learned through our research for the Singapore viewpoint is that the country is under attack and is fighting hard.

What does the attack landscape look like? Try 68% of companies facing more than 5,000 attacks daily. The converse of which is that a reasonably conservative 32% of Singapore defenders report seeing fewer than 5,000 daily alerts, which is not as high as the global standard of 37% but ahead of the regional benchmark of 31%. This means that Singapore is ahead of the region in driving the number of daily alerts seen low enough to do something about. Reducing the amount of work needed allows already overworked security teams to focus on what is important.

There is work still to be done at the top end of the spectrum as 13% of Singapore defenders are seeing 100–150,000 alerts per day, slightly higher than the global (10%) but behind the regional (15%) benchmarks.

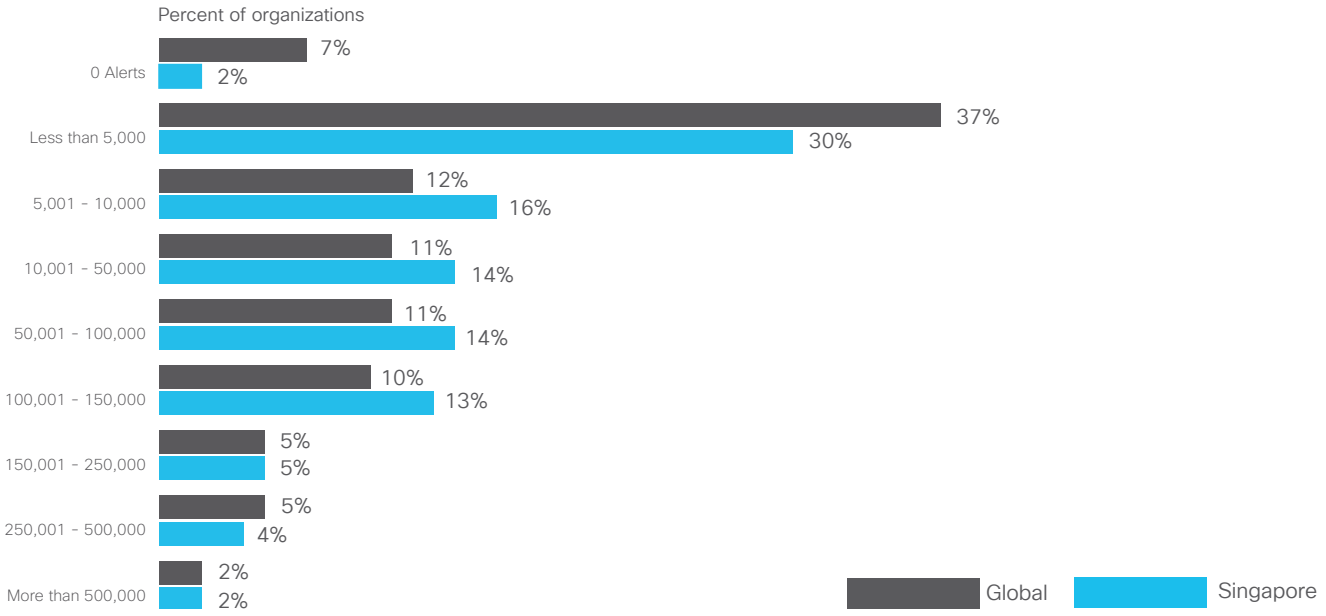
Delivering an efficient, coordinated response to alerts is also clearly an area that Singapore security practices are still grappling with. Only 41% of alerts are investigated each day. While this compares unfavorably with the global and regional benchmarks, which at 56% is already unacceptably low, it also means in real terms that 59% of alerts are not acted on. This shows either lack of capability or capacity.

If you are only investigating half your alerts, how do you know it's the correct half? Never mind how to achieve a 50% investigation rate in the first place.

Investigating alerts is only the first step. It turns out that only 25% of investigated alerts are legitimate, which is not the lowest in the region (Korea, 16%) but is behind all other benchmarks, including the global figure (34%), the regional standard (44%). This compares unfavorably with the stronger countries in region, India (44%) and Australia (65%). This means a full 75% of alerts are false alarms, and a vast amount of valuable work is being done on events that don't need it. This lack of precision is a weakness in defense, and hackers love an Achilles' heel.

The percentage of legitimate alerts that get remediated is 50%, putting it on par with the global (50%) and Asia Pacific (53%) benchmarks, and is, in fact, amongst the highest in the region with only India (52%), Japan (51%) and Australia (69%). Singapore defenders have work to do at the top of the funnel; they are certainly reducing the number of alerts that need to be seen, and then are remediating a lot of the critical incidents, but between those two areas, they need to find new ways to sift through the mass of data to better identify which alerts require attention.

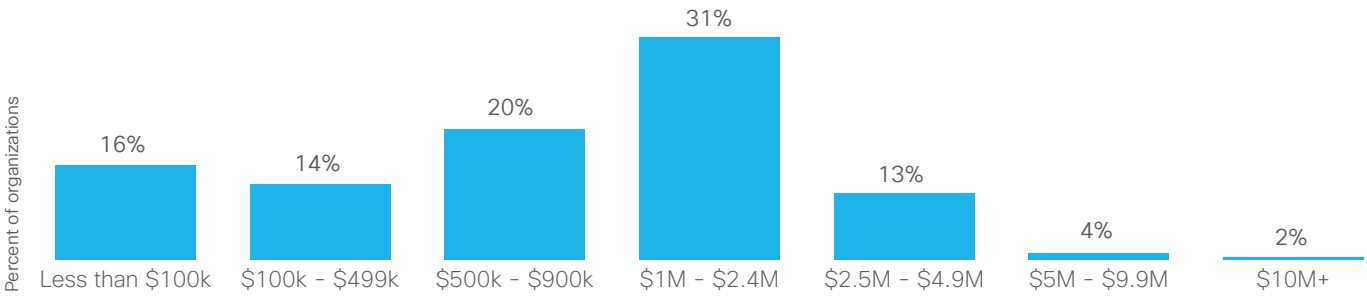
Figure 29 Number of daily security alerts in Singapore



Q: On average, how many security alerts does your organization see on a daily basis?

This is particularly worrying because breaches are just as costly in Singapore, and 84% of breaches cost over USD$100,000. Compared to the region, Singapore reported higher percentage of breaches costing between USD$1-5 million (44%) as Asia Pacific (33%), and the global standard (30%), meaning that almost half are in the middle of the cost impact spectrum. In Singapore, where 16% of breaches cost under USD$100,000 compared with the region (20%) and the globe (30%), defenders are seeing more breaches that register on the mid to high end of the cost spectrum. The second standout figure from the report is that a tiny 2% of incidents cost more than USD$10 million compared with the region (5%) and the worldwide number (3%), suggesting that at least some elements of breach costs at the top end are under control.

Figure 30 Cost of breaches in Singapore

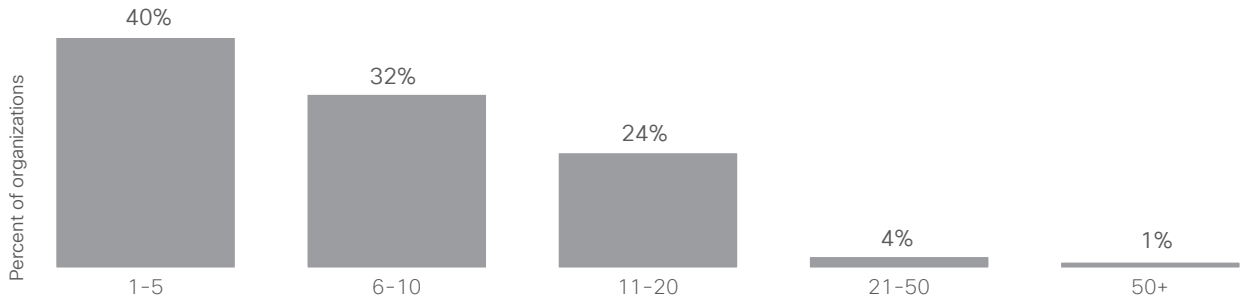


Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

What really matters in these analyses is examining the response to breaches and 46% of respondents report that they would engage staff in training, which also seems smart, especially when you consider that in Singapore, "lack of trained staff" was cited as the number two reason for the lack of adoption of advanced security processes. The number one reason, like many other countries, is lack of budget, meaning that an effective "people plan" plus stakeholder and board-level persuasion are required to make real progress.

Solving people challenges is something that cybersecurity managers cannot ignore; a full 36% of respondents, claimed that they were suffering from cyber fatigue, which is much lower than the region (59%). This suggests that defenders feel more ready to address the threat landscape and is good in comparison with the region. However, in real terms it shows that a third of defenders feel overwhelmed and need to learn better ways to more accurately deal with the high volume of activity before they drown in a sea of uninvestigated and possibly irrelevant alerts.

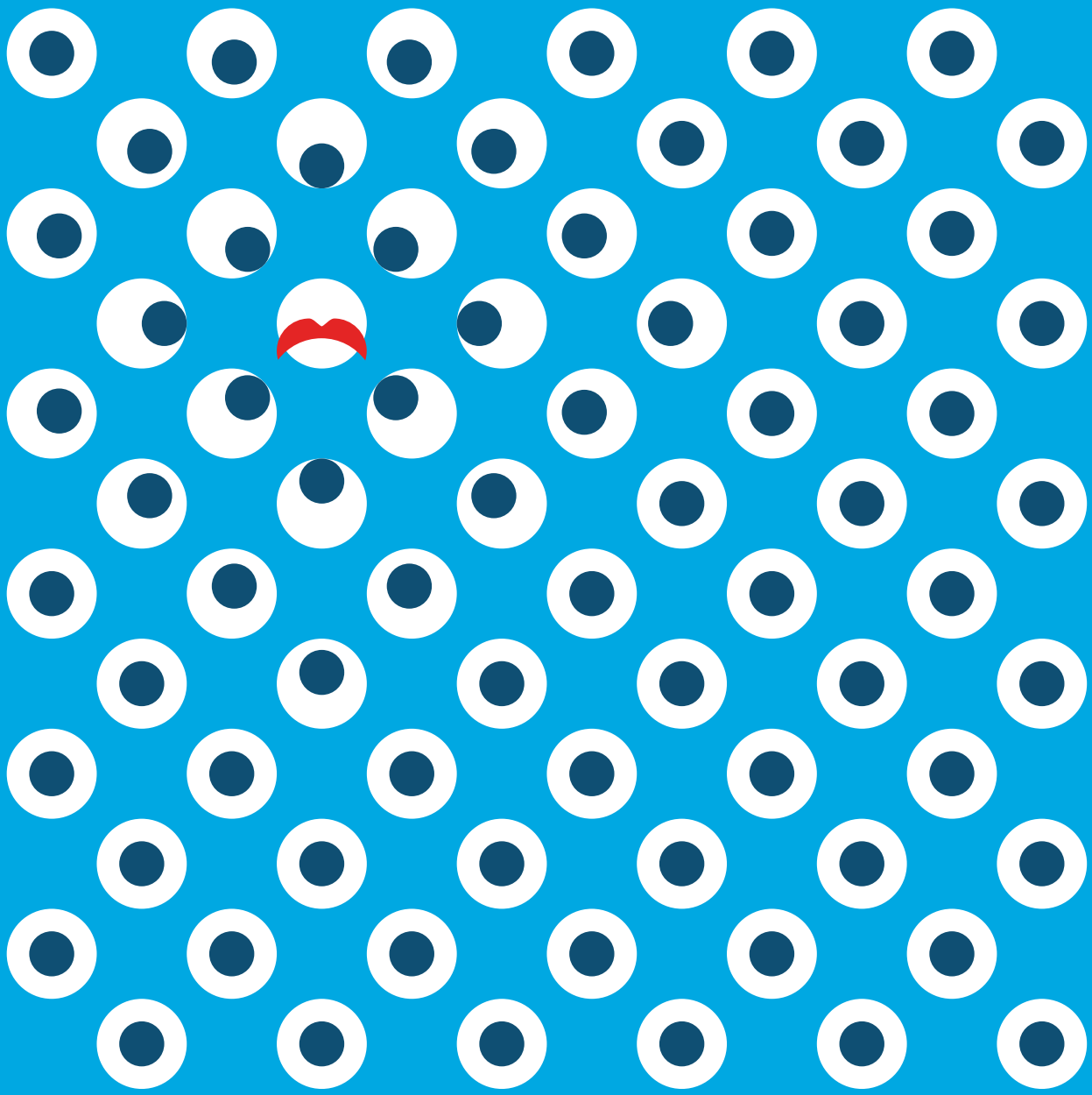
Figure 31 Number of different security vendors in environment in Singapore



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

It's not as if Singapore has not been investing in building well-stocked security environments: 28% have more than 10 vendors and 48% have more than 10 products. Following the maxim that fewer products means fewer gaps through which attackers can move, this means Singapore is keeping better control than Australia with 73% there reporting more than 10 vendors and 76% more than 10 products. The cause of cyber fatigue lies in the numbers: 99% of Singapore defenders responded that it was somewhat or very difficult to orchestrate alerts from multiple vendors, which is higher than the region (82%) and the global benchmark (74%). They are fatigued and as overwhelmed as any other country in the fight against the growing threat. Training, orchestration and automation will go a long way to solving Singapore's cybersecurity challenges.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Thailand Viewpoint

Country Overview

Thailand Viewpoint:

Cyber fatigue demands a different approach

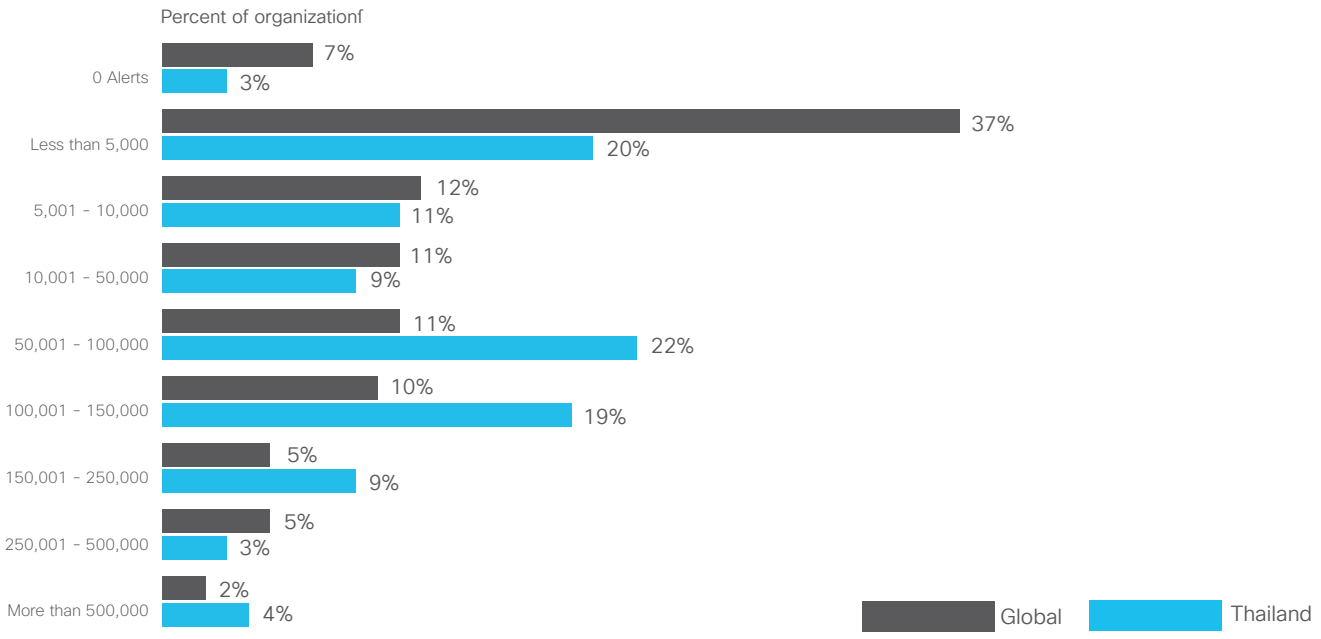
What we've learned through our research for the Thailand viewpoint is that defenders in the kingdom have their work cut out for them, at least in terms of managing alerts, and that they are not always able to keep up with the demands of the modern threat landscape. While, at first glance the number of alerts that defenders face each day seems inline with the global and regional benchmarks, it soon becomes apparent that Thailand skews towards the higher volumes of alerts.

Only 23% of Thailand defenders report seeing fewer than 5,000 alerts, which is much lower than the global standard of 44% but more or less in line with the regional benchmark of 31%. The disparity occurs when you look to make up the delta in the reporting, and realise that a greater proportion of Thai defenders (19%) are seeing 100-150,000 alerts per day, which is higher than both global (10%) and the region (15%) and second only to Australia in the region.

The challenging news does not stop there, because delivering an efficient, coordinated response to alerts is also clearly an area that Thai security practice are still grappling with. Only 37% of alerts are investigated each day compared with the global and regional benchmarks, which at 56% is already unacceptably low. Investigating alerts is only the first step; defenders also need to ensure that they are working on the right items; especially given the vast number of alerts they have to address. It turns out that only 32% of investigated alerts are legitimate, which is not the lowest in the region (Korea, 16%) but is a little behind the global benchmark of 34% and way behind the regional standard (44%). This means that 32% of the work done is to confirm that no work needed to be done and that means bad stuff stands a greater chance of getting through.

The percentage of legitimate alerts that are eventually remediated is 37% which is not only behind the global benchmark (50%) and Asia Pacific (53%), but is in fact, lowest in the region. This tells that Thai defenders have work to do all through the funnel, from managing vast numbers of alerts, sifting through that mass to find what needs to be investigated and then remediating more of the alerts.

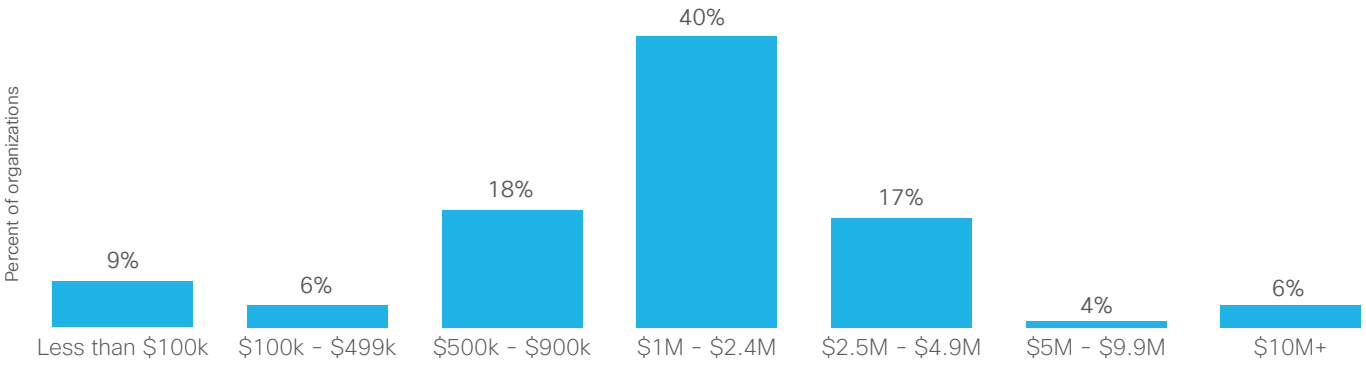
Figure 32 Number of daily security alerts in Thailand



Q: On average, how many security alerts does your organization see on a daily basis?

This is particularly worrying because it's not like breaches come cheap in Thailand. Compared to the region, more alerts in Thailand cost between USD$1-5 million (57%) which is higher than Asia Pacific (33%) and the global standard (30%). The second standout figure from the report is that a full 6% of incidents cost more than USD$10 million which is high compared with the region (5%) and the worldwide number (3%) but nowhere near as high as the Australian figure of 9%, suggesting that breach costs are as high as can be expected without spiralling out of control.

Figure 33 Cost of breaches in Thailand

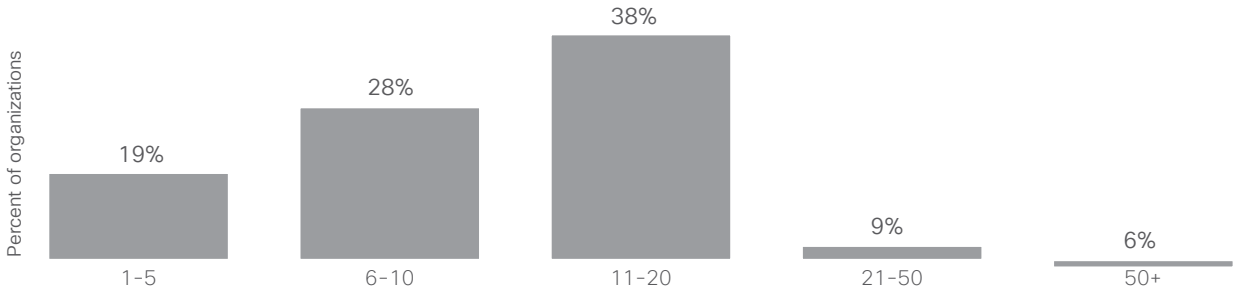


Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

What really matters in these analyses is examining the response to breaches and Thailand here has some good news. 37% of respondents tell that the primary response to a breach was to engage staff in training. It was top of the list of responses compared with countries like Australia where it only ranked as fifth priority and Japan where training was only 10th on the list. This is particular enlightened of defenders in Thailand when you consider that "lack of knowledge" was cited as the second most popular reason for the lack of adoption of advanced security processes. Solving the people problem goes a long way to addressing the security challenge. Like global and regional responses indicated, Thailand also cited budget as the number one challenge in this area which suggests that stakeholder and board-level management are required to make real progress.

Solving people challenges is something that cybersecurity managers cannot ignore; a vast 73% of respondents claimed that they were suffering from cyber fatigue, suggesting that more training, additional automation and better ways to more accurately deal with a high volume of alerts are needed before Thai defenders drown in a sea of un-investigated alerts.

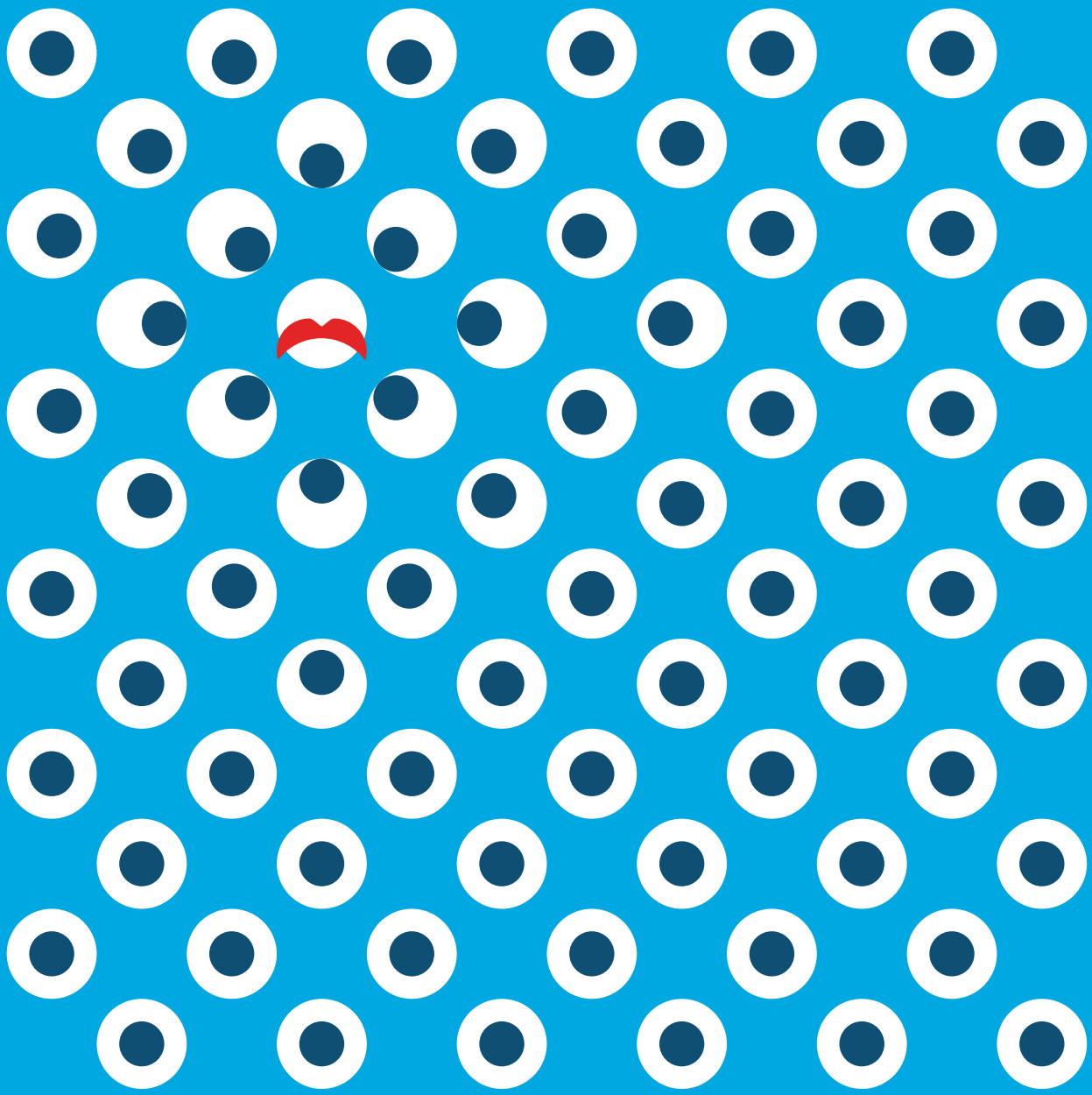
Figure 34 Number of different security vendors in environment in Thailand



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

It's not as if Thailand has not been investing in building well-stocked environments with which to deal with the ever-changing threat landscape with 53% having more than 10 vendors and 61% having more than 10 products. Following the maxim that fewer products means fewer gaps through which attackers can move, this means Thailand is keeping better control than Australia with 73% there reporting more than 10 vendors and 76% more than 10 products. And suddenly the cause of cyber fatigue is clear; 98% of Thai defenders responded that it was somewhat or very difficult to orchestrate alerts from multiple vendors, which is higher than the region (82%) and the global benchmark (74%). Training, orchestration and automation will go a long way to solving Thai challenges.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



Vietnam Viewpoint

Country Overview

Vietnam Viewpoint:

Add precision to tenacity to set new standards

What we've learned through our research for the Vietnam viewpoint is that the country is fighting back hard; looking to land the first blow in the fight against bad actors.

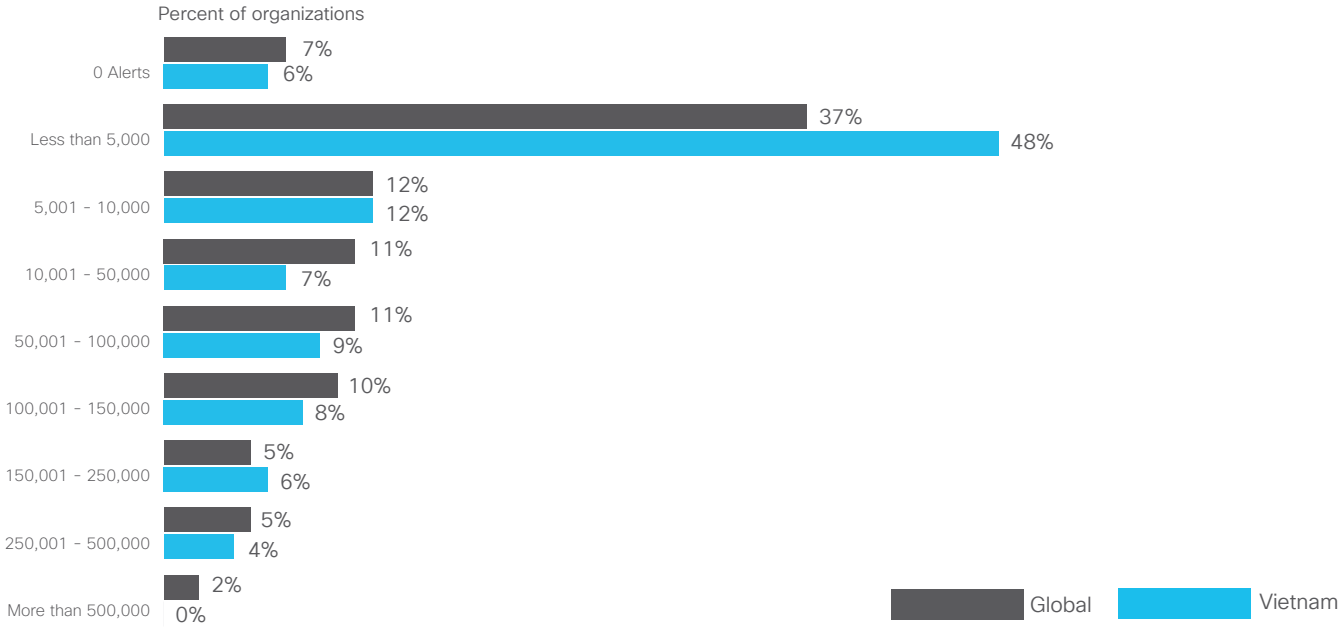
In Vietnam, 46% of companies see more than 5,000 alerts per day; on the flip side, this means a whopping 54% of Vietnam defenders report seeing fewer than 5,000 alerts, which is much higher than the global standard of 44% and more than double the regional benchmark of 31%. There is work still to be done at the top end of the spectrum as a lower proportion of Vietnam defenders (8%) are seeing 100–150,000 alerts per day, than both the global (10%) and the regional (15%) benchmarks. This is good, but they are ahead of Japan (6%), the country in Asia Pacific with the lowest score in this range. This indicates that the Vietnam is forcing the number of alerts faced daily into the lower, more manageable, ranges and is a promising start to analysis.

Delivering an efficient, coordinated response to alerts is also clearly an area that Vietnam security practice are still grappling with. Only 50% of alerts are investigated each day. While this compares somewhat favorably with the global and regional benchmarks, which at 56% is already unacceptably low, this means that a full half of all alerts are not acted on, which in turn shows either lack of capability or capacity. For the small number of companies with up to 150,000 alerts, this means tens of thousands of incidents not triggering a response. To paraphrase an old advertising maxim: if you are only investigating half your alerts, how do you know it's the correct half? Vietnam defenders need to find new ways to scale their operations and attend to more alerts.

Investigating alerts is only the first step; defenders also need to ensure that, when they start attending to their queue, that they are working on the right alerts. It turns out that only 28% of investigated alerts are legitimate, which means a full 72% of alerts are false alarms, so not only is malware getting through in the pile of logs that are not attended to but a vast amount of valuable work is being done on files that don't need it. This lack of precision is a weakness in defense, and hackers love an Achilles' heel.

39% of legitimate alerts are eventually remediated, which is well behind the global (50%), and Asia Pacific (53%) benchmarks, and is, in fact, amongst the lowest in the region with only Thailand (37%) lower. This tells us that Vietnam defenders have work to do at the midpoint of the funnel on down. They are certainly reducing the number of alerts that need to be seen, but following that they need to better manage and then sift through that mass to find what needs to be investigated; they should pay particular attention to remediating more of the alerts.

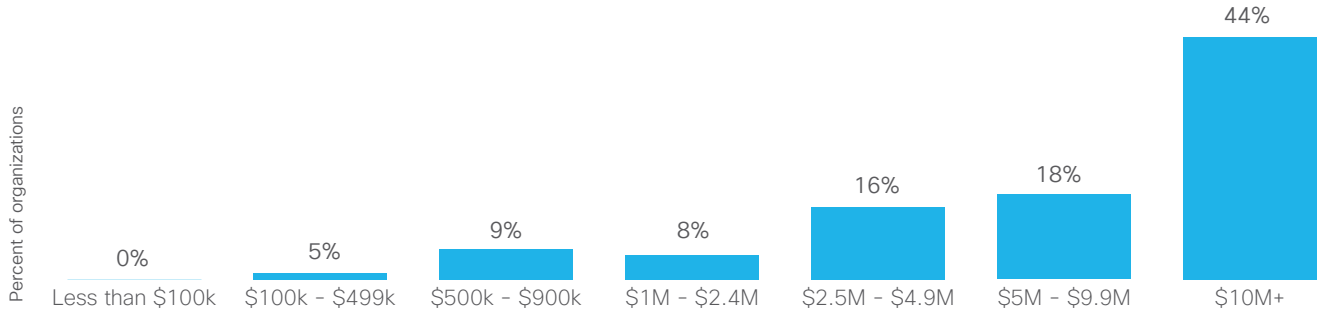
Figure 35 Number of daily security alerts in Vietnam



Q: On average, how many security alerts does your organization see on a daily basis?

This is particularly worrying because breaches are just as costly in Vietnam, with all of the breaches costing more than USD$100,000. Compared to the region, slightly fewer alerts in Vietnam cost between USD$1-5 million (24%) than Asia Pacific (33%) and on par with the global standard (30%). The scales do not tip towards the lower end of the breach dollar impact in the Vietnam, where none of the breaches cost under USD$100,000 compared with the region (20%) and the globe (30%). The second standout figure from the report is that a vast 44% of incidents cost more than $10 million which is off the charts compared with the region (5%), the worldwide number (3%), and even the second highest in the region Australia (10%), suggesting that some breach costs at the top end are out of control.

Figure 36 Cost of breaches in Vietnam

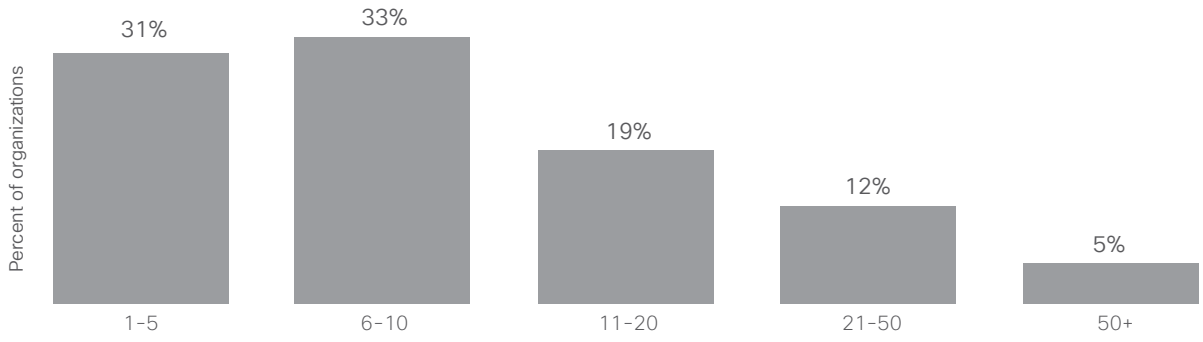


Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

What really matters in these analyses is examining the response to breaches and Vietnam is less in line with regional best practices. 61% of respondents tell that top of the list of responses to a breach was to engage staff in training compared with countries like Philippines and Japan where it ranked ninth and tenth respectively; it's more in line with Thailand and India which also ranked training top of the list. The approach seems smart, especially when you consider that in Vietnam, "lack of knowledge" was cited as the number one reason for the lack of adoption of advanced security processes and the third reason was lack of trained personnel. At number two, like many other countries, was lack of budget, meaning that an effective "people plan" plus stakeholder and board-level persuasion are required to make real progress.

And solving people challenges is something that cybersecurity managers cannot ignore. A full 62% of respondents claimed that they were suffering from cyber fatigue, slightly above the region (59%), and almost two thirds of defenders needing to learn better ways to more accurately deal with that high volume of alerts are needed before they drown in a sea of un-investigated and possibly irrelevant alerts.

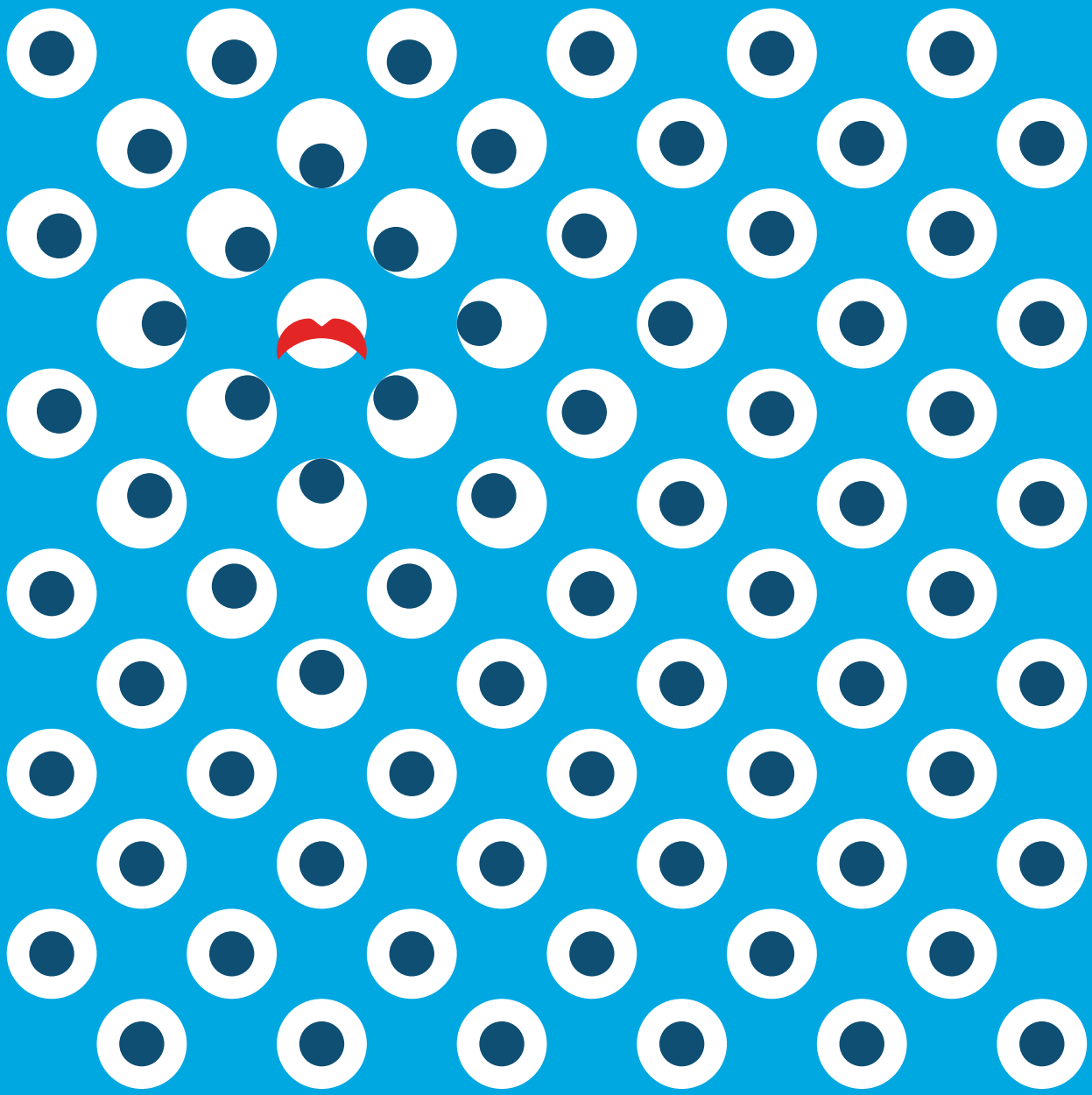
Figure 37 Number of different security vendors in environment in Vietnam



Q: How many different security vendors (i.e. brands, manufacturers) are in your security environment?

In Vietnam, 34% of companies have more than 10 vendors and 43% have more than 10 products. Following the maxim that fewer products means fewer gaps through which attackers can move, this means Vietnam is keeping better control than Australia with 73% there reporting more than 10 vendors and 76% more than 10 products. The cause of cyber fatigue lies in the numbers: 86% of Vietnam defenders responded that it was somewhat or very difficult to orchestrate alerts from multiple vendors, which is higher than the region (82%) and the global benchmark (74%). They are as fatigued and overwhelmed as any other country in the fight against the growing threat. Training, orchestration and automation will go a long way to solving Vietnam's cybersecurity challenges.

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.



About Cisco

About Cisco

Cisco delivers one of the industry's most comprehensive advanced-threat protection portfolios of solutions across the broadest set of attack vectors. Our threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection for customers of all sizes, around the world, in all industries.

The connective tissue for this portfolio is threat intelligence that enables Cisco security products and solutions to see more threats, block more attacks and respond faster when the inevitable happens. Cisco Talos is the industry's leading threat intelligence and research team, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open-source community. This amounts to a daily ingest of billions of web requests and millions of emails, malware samples, and network intrusions.

Cisco's sophisticated infrastructure and systems consume this telemetry, helping machine-learning systems and researchers track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, and email, and from the cloud, to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our products and services offerings that are immediately delivered globally to Cisco customers.

To learn more about our threat-centric approach to security, visit cisco.com/go/security.
Validation, and Advanced Security Research and Government. For more information, visit trust.cisco.com.

Updates and corrections

To see updates and corrections to the information in this project, visit cisco.com/go/errata.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published February 2018