FireEye
SECURITY REIMAGINED

SPECIAL REPORT

THE NUMBERS GAME:

How Many Alerts is too Many to Handle?

CONTENTS

Introduction

The numbers are staggering. Security alerts come in by the thousands every month, and you and your IT team are tasked with handling each one. Even when alerts are caught and categorized correctly, the sheer volume is overwhelming. And when they're not responded to quickly, the consequences can be disastrous.

The high volume of alerts requires a level of management that exceeds what most companies are realistically able to maintain. A worldwide survey of C-level security executives at large enterprise companies reveals that varying types organizations face very similar scenarios in the monumental task of managing security alerts. From too few resources to too many false-positives, respondents weighed in on how tools and technology help them handle today's ever-increasing number of alerts.

We hope that these findings will help you assess the current state of your alert process and how to improve your organization's management of it.

37% of respondents face more than 10,000 alerts each month

Executive Summary

In a recent survey of security management conducted by IDC on behalf of FireEye, we learned that large enterprises rely on security personnel to fulfill multiple roles and responsibilities — an expectation that can prove disastrous when it comes to finding and escalating a critical alert.

Security personnel at all levels face wading through data, false alarms and duplicate alerts. While security teams comb through mounds of noisy data and cull alerts, too many still need to be addressed at the upper levels, making an already cumbersome process virtually impossible to manage.

The statistics that follow only tell part of the story. We review everything from the origin, quality and quantity of alerts to how they're managed. The percentages may present a familiar scenario in your company, or perhaps they will surprise you. Regardless, they'll help you assess your security standings in comparison to companies around the world.

But with all of the data we provide in this report, one metric will prove most important to your own network security needs: How long does it take for you to act on your security alerts? The answer to that is key to assessing the security of your companies' network.

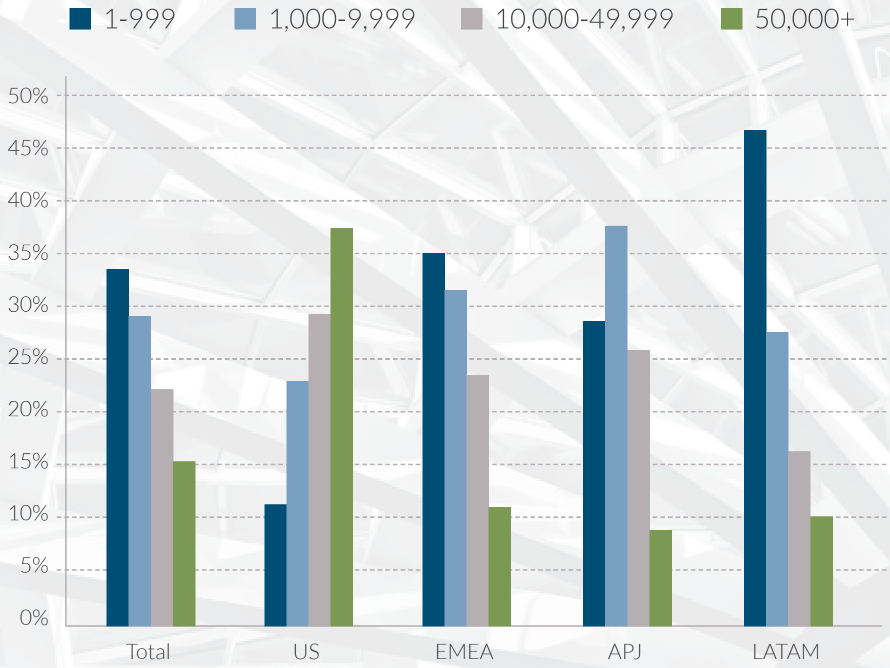
More than 40% of respondents manually review each alert

Alerts – Origins and Volume

How many security alerts does your organization receive per month?

Volume of Alerts

- 37% of respondents indicated they face over 10k alerts/month. The low end of that range, (10k) translates to 300+/day, and ~14/hr, so a nearly constant occurrence.
- Within the US, 37% of organizations face more than 50k alerts per month. Latin American organizations are most likely to see less than 1000 alerts/month.



Source: IDC Survey, sponsored by FireEye, Advanced Threat Readiness Assessment, September 2014; n=505

Maximum Volume – Minimum Staff

More than 35% of companies say they spend 500 hours per month responding to alerts. The IT security specialists who respond are typically tasked with multiple security responsibilities, though, which makes missed alerts more likely. Add to that alerts that are evaluated incorrectly — either due to error or to manipulative attackers — and the effects of alert overload are multiplied.

When analysts either don't have ample time to thoroughly review alerts due to overtasking, or are not specialists in alert investigation, costly mistakes result.

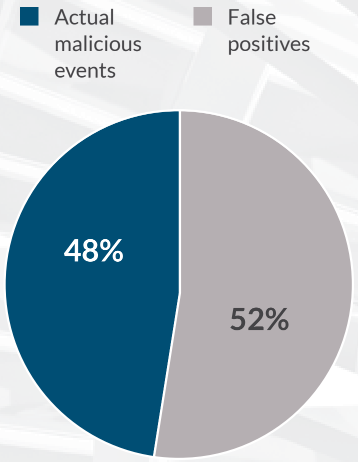
37% face 10,000+ alerts monthly

Most get at least 300/day or 14/hour

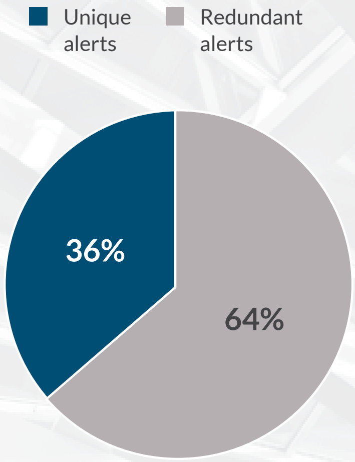
3 full-time positions

Effectiveness

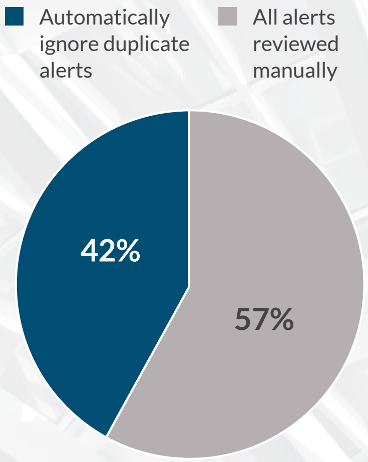
Percentage of False Positives



Percentage of Redundant Alerts



Organizations Automating Alert De-duplication



Alert Duplication

- Respondents indicated nearly half of alerts were false positive, and over one-third of all alerts were redundant across multiple threat detection platforms.
- Less than 60% respondents implemented a process to automatically ignore duplicate alerts. This was driven in part by Latin America, which had the highest amount of manual reviews.
- A large number of organizations are manually responding to redundant alerts that are only 50% likely to be an actual malicious event.

Source: IDC Survey, sponsored by FireEye, Advanced Threat Readiness Assessment, September 2014; n=505

Noisy Environments

Noise is a significant issue, with more than half of alerts being false positives. This number is likely even higher if the alerts have not been correlated and deduplicated, since more than one-third of them are redundant. All this adds up to a scenario where platforms are generating too much data that is simply ineffective. Worse, it's wasting precious hours to review it all.

That review process is costly. Less than 60% of companies have a process to automatically ignore redundant alerts, which means they are manually responding to alerts that contain an actual malicious event less than half the time.

More than 1/3 of alerts are duplicates

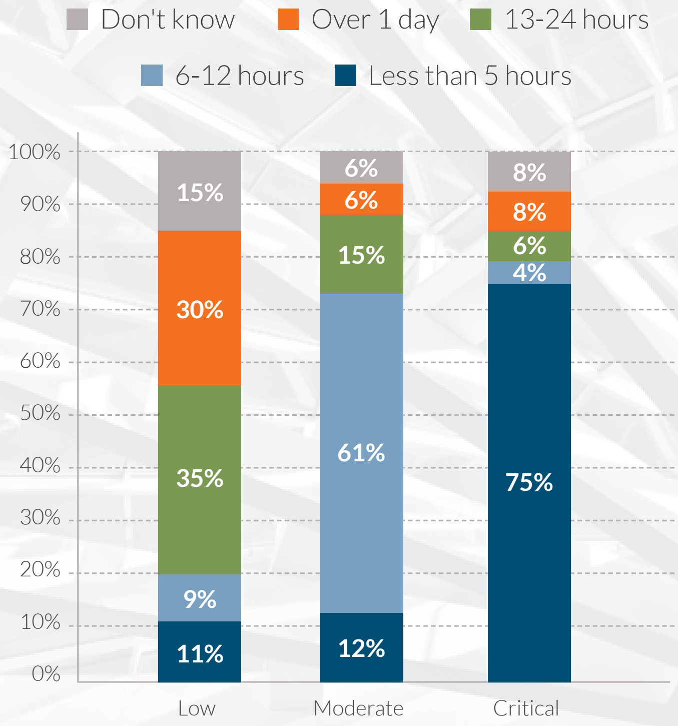
At least 50% of alerts are false positives

Addressing Alerts

What is the lag time between an alert and it being reviewed?

Speed of Alert Review

- Most organizations have a good handle on critical alert response: 75% say response takes less than 5 hours.
- There is a definite lag with moderate and especially low priority alerts. 30% of organizations indicated response to low priority alerts takes over 1 day, putting more pressure on products to accurately categorize alerts.



Source: IDC Survey, sponsored by FireEye, Advanced Threat Readiness Assessment, September 2014; n=505

Response Times

Response times were relatively standard across our survey, with critical alerts being reviewed in less than five hours. But reviews are, of course, only the first step. Analysts then need to identify whether an alert is an actual attack, remediate any compromised systems and complete forensic investigations to mitigate damages. Any delay in the initial review time slows the entire process.

Alerts must be accurately categorized for ultimate success. If a critical alert is labeled as low-priority and doesn't receive a quick response, it could prove disastrous.

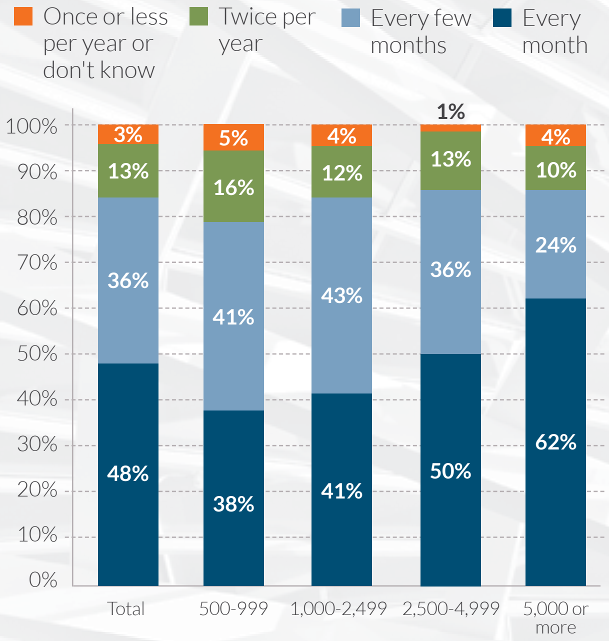
Critical alert response takes less than 5 hours 75% of the time

Low-priority alerts take more than one day

60% say moderate alert responses take between 6-12 hours

Alert Management

How often does your organization review and refine security product configurations to reduce the number of alerts?



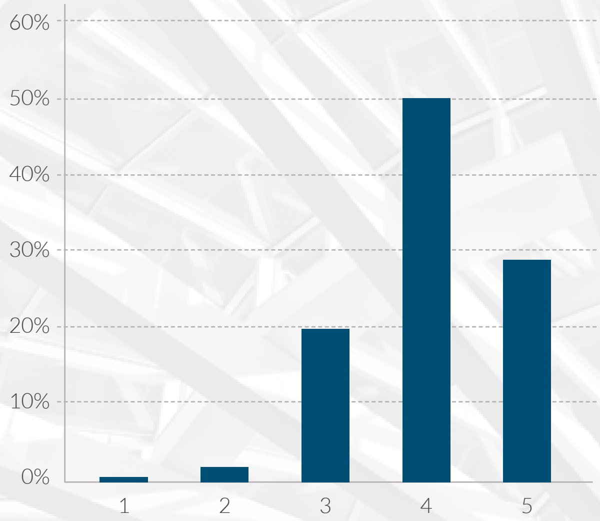
Frequency of Configuration Review

- A high number of organizations are reviewing configurations monthly specifically to try to reduce alerts. Over 60% of the largest organizations review monthly, and nearly 40% of SMBs .

Source: IDC Survey, sponsored by FireEye, Advanced Threat Readiness Assessment, September 2014; n=505

How well do your organization's current products segment alerts into critical, moderate, low priority?

Please use a 5 point scale where 5 is an excellent job and 1 is a poor job. [Percentage ranking 4 or 5]



Effectiveness of Alert Segmentation

- Despite the preceding data, alert segmentation is rated very favorably by respondents.
- Organizations are wasting time responding to alerts and continually configuring products to try to reduce alerts, but may be so entrenched in that cycle that they don't realize they have a problem.

The Argument for Outsourcing

Organizations recognize that consolidation is an effective way to deal with the complex task of managing network security. In the U.S., 94% of companies either have consolidated their security management or have at least considered it — suggesting an understanding of the benefits it brings.

However, most organizations still manage their IT security in-house, despite wanting strong security in place and recognizing that outsourcing is a way to achieve that.

Over 60% of large organizations review alert configurations monthly

Most companies are pleased with their alert risk categorization

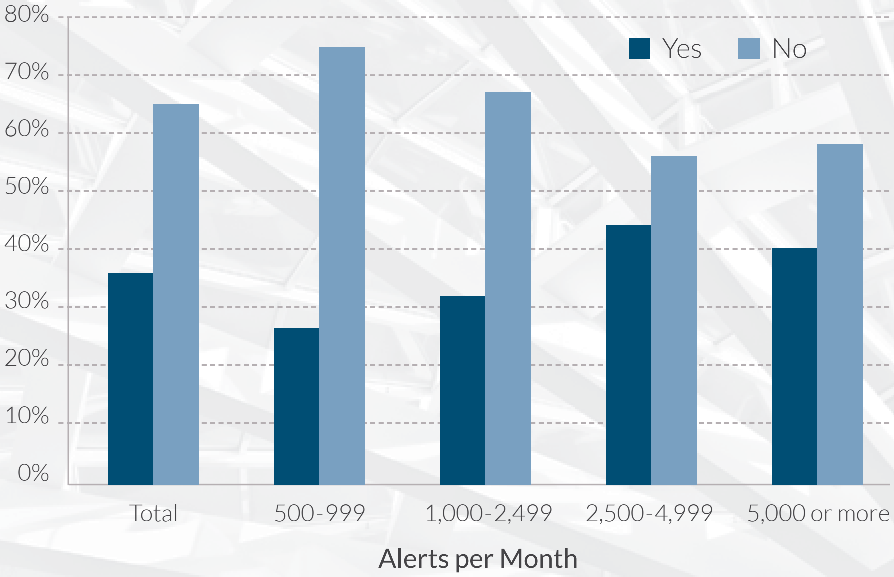
35% outsource alert monitoring

Key Takeaways

Is alert monitoring outsourced?

Outsourcing Alert Monitoring

- Organizations facing between 50-100k alerts per month are most likely to outsource alert monitoring.
  - These companies were typically between 1000-4999 employees.
  - Typically, these organizations don't have the same resources as very large firms to handle in house, but are targeted more often than smaller counterparts.



Source: IDC Survey, sponsored by FireEye, Advanced Threat Readiness Assessment, September 2014; n=505

Security monitoring requires a thorough assessment for optimal effectiveness. Many organizations have a staff of specialized security personnel who manage a large number of consoles, but they are tasked with multiple functions that stretch resources thin. Despite already-high numbers of alerts that are increasing, a smaller percentage of organizations plan to increase personnel to manage their alert systems.

Nearly 75% of respondents do not have dedicated staff to monitor and respond to alerts, and instead look to their product administrators for alert management.

Only 35% of organizations outsource. When companies do decide to hire a third party for alert management, it is for improved security — not as a money-saving measure.

KEY TAKEAWAYS

- Alert response requires 500+ hours per month for 35% of large organizations
  - That's equal to 3 full-time positions just monitoring alerts
  - Most security staff have collateral duties beyond alert response
- Despite a false positive half of the time, 40% of organizations manually review every alert
- 36% of alerts are redundant, but still are manually reviewed
- More than 60% review alert configurations monthly to reduce the number of alerts
- Organizations count on their products to accurately categorize alerts
  - 30% say it takes 1+ days to respond to low-priority alerts
  - If categorized incorrectly, hackers have more time inside a network

Conclusion and Recommendations

The statistics demonstrate that efficient alert management is lacking in organizations, large and small, across the globe. The number of alerts is overwhelming and can't be managed by a staff that is already stretched too thin. And already-overtasked C-level executives have a tall order to identify and respond to the real risks in a ocean of data. Too often, companies are simply trying to keep up rather than determining how to improve the process.

If resources were reallocated, alert management could become nimble and efficient. Organizations need to consider alternatives including proactive testing, policy review, and new initiatives to better manage the alert process.

Specifically, companies who outsource alert monitoring stand a greatly improved chance of seeing and responding to critical alerts in a timely fashion. In addition, by reducing the responsibility load on their IT staffs, they also better allocate their resources.

50%: the amount budgeted for alert monitoring

The importance of accurate technology can't be overlooked. Organizations need platforms capable of reviewing and alerting across multiple consoles to identify and mitigate threats, and that provide efficient workflows to streamline the analysis process when time is critical.

Alert monitoring accounts for roughly half of most companies' IT security budgets. This survey demonstrates the overwhelming need for organizations to review their alert management process to better respond to alerts before they become full-fledged attacks.

To learn more about
how FireEye can help you focus
on the alerts that matter, visit:
http://www.fireeye.com/products-and-solutions/threat-analytics-platform.html

About FireEye

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,700 customers across 67 countries, including over 157 of the Fortune 500.

FireEye®

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**