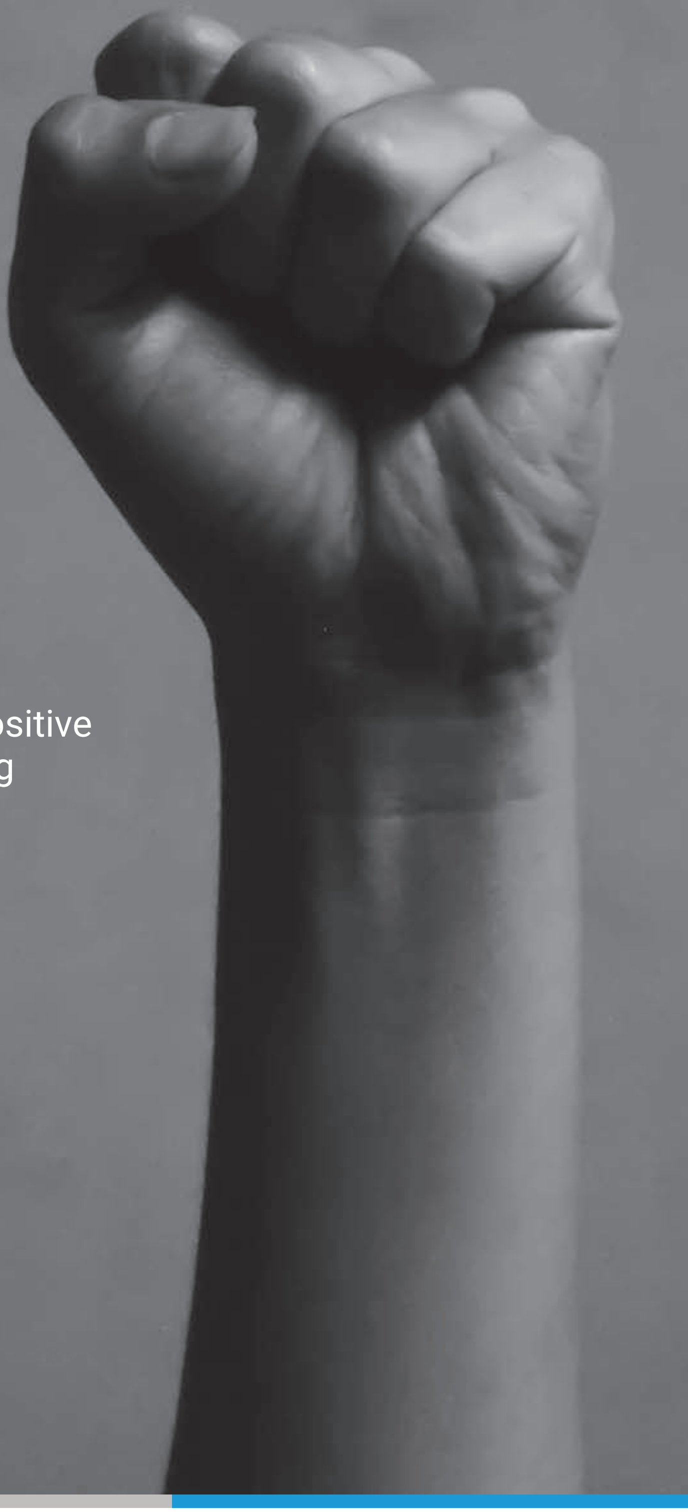
CRITICALSTART

YOU DESERVE BETTER

Incident responders overwhelmed by false-positive security alerts; waste hours daily investigating false-positives, survey report reveals



COMPANIES ARE FACING A GREATER VOLUME OF SECURITY ALERTS THAN EVER BEFORE – AND EACH ONE CAN TAKE FROM MINUTES TO HOURS TO INVESTIGATE

TABLE OF CONTENTS

1 | EXECUTIVE SUMMARY

MSSP INCIDENT RESPONDERS ARE WASTING AN ENORMOUS NUMBER OF HOURS AND RESOURCES PROCESSING USELESS SECURITY ALERTS

1.1 SURVEY GOAL AND METHODOLOGY

Advanced Threat Analytics (ATA) conducted a survey of nearly 50 managed security services providers (MSSPs) to evaluate the state of incident response within their security operations centers (SOCs). Demographic data of survey respondents was not collected.

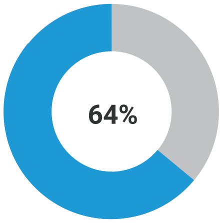
This report and the analysis within are primarily based on the responses received from this sample, though we believe these research findings are representative of the larger MSSP community.

At a high level, this research found that MSSP incident responders are wasting an enormous number of hours and resources processing useless security alerts – a problem that impacts staffing, operational business models and security effectiveness. Additionally, the survey found that incident responders often cope with this problem by reducing the sensitivity of security equipment or ignoring alerts altogether – thus leaving their organizations more vulnerable and susceptible to attacks.

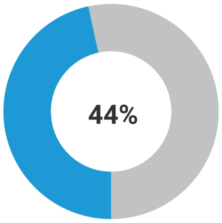
1.2

KEY FINDINGS

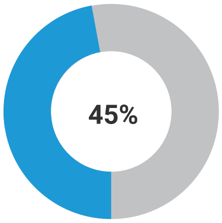
Let's start with the raw numbers:



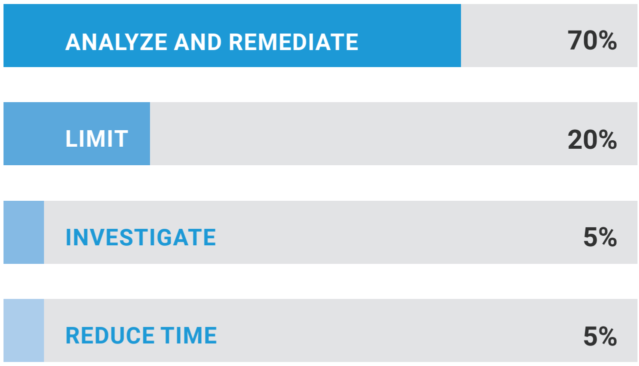
64% of survey takers stated that, on average, it takes 10 minutes or more to investigate each alert, with 11% reporting they spend 30 minutes or more on each.



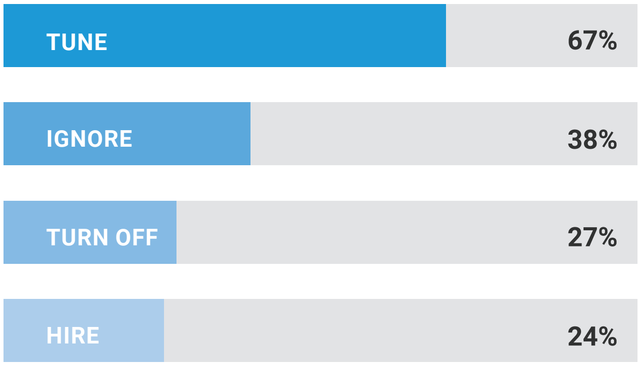
44% of respondents experience a 50% or higher false-positive rate, with 22% reporting a false-positive rate between 75% and 99%.



Nearly 45% of respondents investigate 10 or more security alerts each day. 11% said they investigate more than 50 alerts daily.



Respondents feel their main job responsibility is to: analyze and remediate security threats (70%); limit the number of alerts sent to clients for review (20%); investigate as many alerts as possible (5%); and reduce the time it takes to investigate a security alert (5%).



Respondents say that when their SOC has too many alerts for analysts to process they: tune specific alerting features or thresholds to reduce alert volume (67%); ignore certain categories of alerts (38%); turn off high-volume alerting features (27%); and hire more analysts (24%).

Each of these statistics represents a "chapter" in the alert-overload story. The following sections go into further detail on how, combined, they can actually impact MSSP operating models.

2 | MSSPS *OVERWHELMED* BY ALERT OVERLOAD

Enterprises often look to outsource security services that they don't have the time or resources to manage effectively in-house, and incident response is one of the most prominent examples. As cybercriminals get more sophisticated and malware continues to evolve, companies are deploying more point solutions to protect themselves. But all those applications have their own set of alerts and notifications, which means companies are facing a greater volume of security alerts than ever before – and each one can take from minutes to hours to investigate. As a result, they're turning to MSSPs to take the problem off their hands.

For MSSPs, this situation is both good and bad. On the plus side, it's bringing in new business. On the flip side, MSSPs are inheriting the burden of analyzing an oppressive number of alerts on behalf of their clients – and they aren't immune to the time, resources and budget drain that prompted enterprises to outsource this task in the first place. MSSPs need the right infrastructure and staff support to effectively manage incident response, so they can deliver on service-level agreements and meet their clients' needs without driving operating costs to unacceptable levels.

ATA's research findings validate the alert-overload problem that MSSP incident responders are facing, with nearly 45% of survey takers reporting that they investigate 10 or more alerts each day; 22% investigate between 10 and 20 alerts each day; 11% investigate 20-40 daily; and 11% investigate 50 or more.

Volume is only half of the story. The other half is the time required to investigate each security alert. 64% of survey respondents state that, on average, it takes 10 minutes or more to investigate each alert; 33% say it takes between 10 and 20 minutes to investigate each alert; 20% say it takes between 20 and 30 minutes; and 11% state it takes 30 minutes or more. Only 36% say that each alert takes fewer than 10 minutes to analyze.

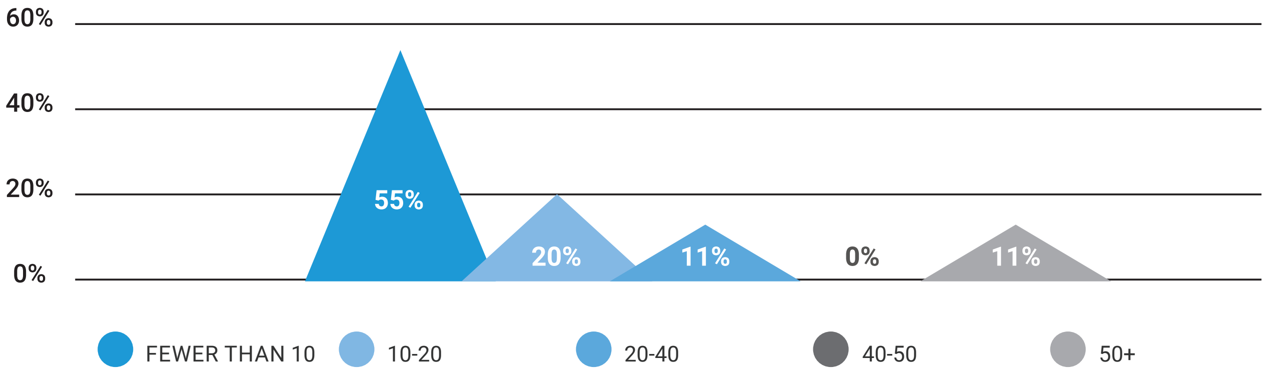
Why does this matter? Let's consider a very conservative example based on the survey data. In an environment where each analyst has to investigate 10 alerts per day, taking just 12 minutes per incident for the investigation, with a 50+% false-positive rate, that's one hour of wasted time per day. At this rate, the SOC is paying for an extra headcount for every eight analysts (paying for the eight analysts, plus the equivalent of another headcount in wasted time). And that's a best-case scenario. The picture looks significantly worse if:

The false-positive rate is higher (which is likely is give 46% report a false-positive rate between 50-99%) **or**

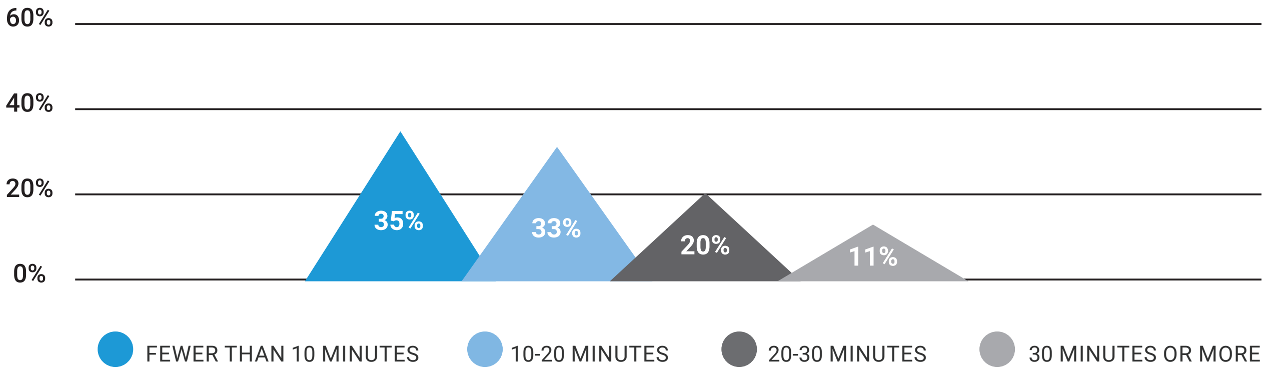
The number of alerts is higher (like in the case of the 22% who are each investigating 20 alerts or more).

In less conservative scenarios, wasted headcount can account for 40% or more of total analyst spend. And, when analysts are wasting time, they are not delivering meaningful service to clients – so this problem not only bloats operating costs, it also compromises service levels.

HOW MANY INCIDENTS/ALERTS DO YOU PERSONALLY INVESTIGATE PER DAY ON AVERAGE?



HOW MUCH TIME DOES THE AVERAGE INCIDENT/ALERT TAKE YOU TO INVESTIGATE?



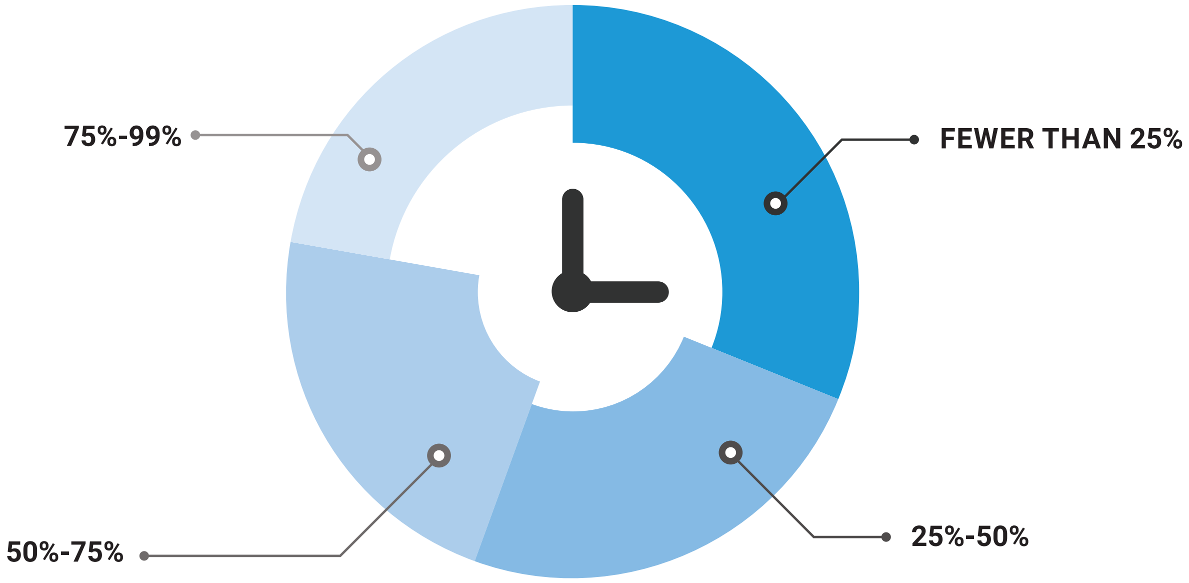
The best-case scenario still has incident responders spending close to two hours each day investigating alerts. In the worst-case scenario, they can spend the entire workday investigating alerts and still not get to them all. When one considers that many of these alerts are benign (see next section), this means MSSPs are paying armies of analysts to spend large portions of each day on fruitless activity.

This is where an event orchestration platform can help. For example, Josh Maberry, director of security operations at MSSP Critical Start, said about their use of Advanced Threat Analytics, *"The event orchestration platform really helps our team operate at peak efficiency. Without it, the work that takes our team of 12 would easily require a team of 50. It changes the game for MSSPs that traditionally have no other option than to double or triple their teams to keep up with the alert volume."*

3 | ARE YOU (FALSE) POSITIVE?

Perhaps the worst part of the alert-overload problem is that incident responders are spending hours each day on security alerts that turn out to be redundant or false-positives. 44% of survey respondents report a 50% or higher false-positive rate; 22% experience a 50-75% false-positive rate while the other half reports a rate between 75 and 99%. 24% of survey takers say their organization's false-positive rate is between 25 and 50%, and only one-third say it's less than 25%.

HOW MUCH TIME DOES THE AVERAGE INCIDENT/ALERT TAKE YOU TO INVESTIGATE?



Why is the false-positive rate so high? Because SIEM and incident response tools search through alerts to find "the potential bad" and "suspicious events," which generate far too many false-positives for most incident response teams to investigate. While these tools can help decrease the amount of time it takes responders to analyze and process alerts, they don't tackle the challenges of alert volume and false-positives.

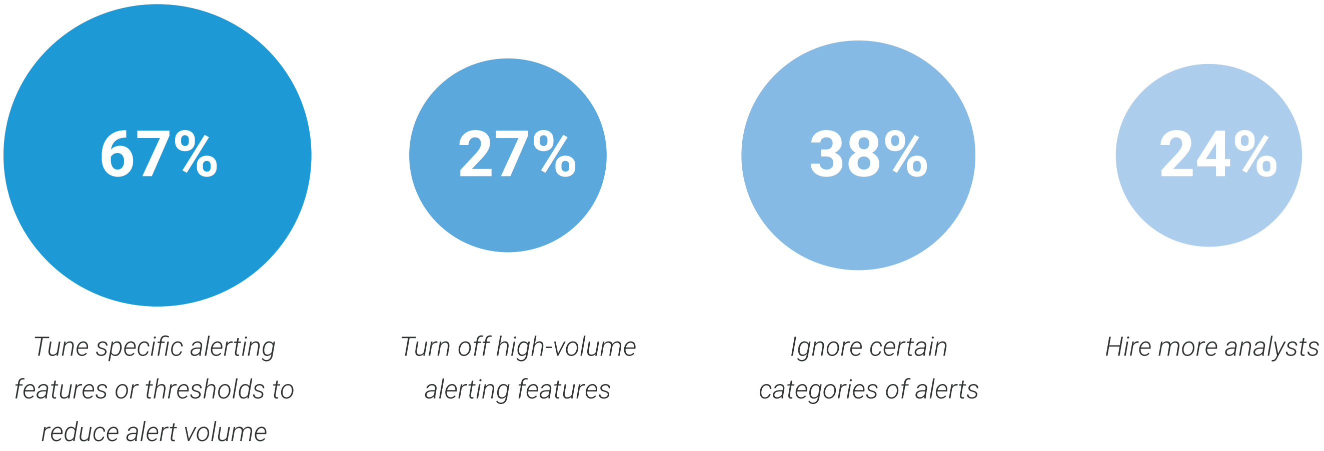
Devoting so much time and effort to investigating benign alerts can severely compromise security effectiveness, as analysts are waylaid from acting on actual threats and incidents. As mentioned earlier in this report, when analysts waste hours each day processing volumes of useless security alerts, it impacts MSSP operating models because they must devote headcount to wasteful activities, which also impairs service deliver to clients.

4 | ALERT OVERLOAD DICTATES MSSP BUSINESS MODELS

Security vulnerabilities and inflated operational expenses aren't the only outcomes associated with the alert-overload problem. For many MSSPs, the volume of security alerts has grown so out of control that it dictates their staffing, business models and operational processes. In MSSP circles, this is referred to as "Alert Tyranny."

When asked what they do if their SOC has too many alerts to process, respondents said they: tune specific alerting features or thresholds to reduce alert volume (67%); ignore certain categories of alerts (38%); turn off high-volume alerting features (27%); and hire more analysts (24%).

IF YOUR SOC HAS TOO MANY ALERTS FOR THE ANALYSTS TO PROCESS, WHAT DO YOU DO? SELECT ALL THAT APPLY.



Hiring the necessary number of qualified, experienced personnel to review, investigate, analyze and keep pace with the onslaught of alerts is expensive, resource-intensive, and prevents organizations from providing superior levels of service and security. Changing operational processes and reducing the sensitivity of security equipment, like turning off specific features and narrowing evaluation criteria, greatly increases the risk that legitimate security events will go undetected. And ignoring alerts from deployed solutions altogether is both highly dangerous and a waste of technology investment.

5 | BATTLING ALERT *TYRANNY*

This research shows that MSSP incident responders continue to be overwhelmed by false-positive security alerts, and until recently, they only had a few options to address this challenge (as noted in question four) – none of which resulted in a sustainable business model or security effectiveness.

A growing number of MSSPs are using event orchestration to combat alert tyranny. This approach typically uses some combination of network data, customer-specific patterns, white-list data and crowdsourced event-reduction playbooks to sift through, identify and remove the “known good” or “normal” events, leaving only genuine threats behind for responders to analyze. When executed properly, this approach automates the investigation and removal of false-positive alerts and can dramatically reduce alert volume (some MSSPs report a near elimination of false positives).

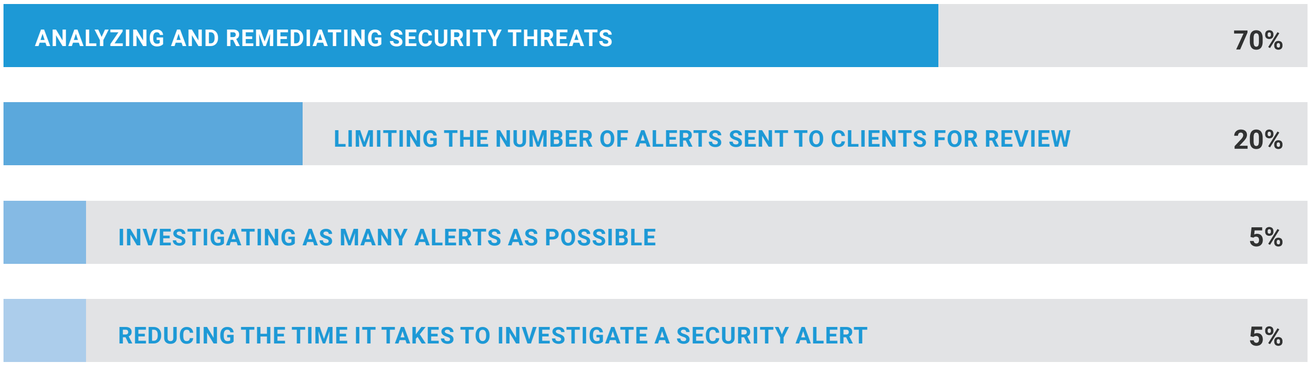
The net result is that MSSPs and MDRs can reduce the alert-overload problem and take a more efficient and strategic approach to security operations. They can not only be more efficient than clients at processing alerts, they can also be far more accurate in identifying threats. This results in better service to clients and greater profit margins for MSSPs.

The best way for MSSPs and Managed Detection and Response (MDR) service providers to break free from alert tyranny is to invest in technology that:

- Decreases the number of incidents generated by screening out “the good” to laser-focus on “the bad” **and;**
- Automates alert analysis in a way that makes it unnecessary for a human to ever touch a false-positive.

When survey respondents were asked what they feel is the main responsibility of their job, 70% said analyzing and remediating security threats; 20% said limiting the number of alerts sent to clients for review; 5% said investigating as many alerts as possible; and the remaining 5% said reducing the time it takes to investigate a security alert.

WHAT DO YOU FEEL IS THE MAIN RESPONSIBILITY OF YOUR JOB?



Event orchestration technology makes it possible for that 70% to do their intended job successfully, while forcing the remaining 30% to rethink their strategy, rewrite the rules and implement a more logical, effective and efficient solution to the alert-overload problem.

MSSP INCIDENT RESPONDERS CONTINUE TO BE OVERWHELMED BY FALSE-POSITIVE SECURITY ALERTS

6 | ABOUT CRITICAL START

Critical Start is the fastest-growing cybersecurity integrator in North America. Our mission is simple: protect our customers' brands and reduce their business risk. We do this for organizations of all sizes through our award-winning portfolio of end-to-end security services – from security-readiness assessments using our proven framework, the Defendable Network, to the delivery of managed security services, incident response, professional services, and product fulfillment. Critical Start has been named to the CRN 2018 Tech Elite 250 and top 100 Security MSPs lists. Critical Start acquired Advanced Threat Analytics (ATA) in 2018.
Visit **www.criticalstart.com** for more information.