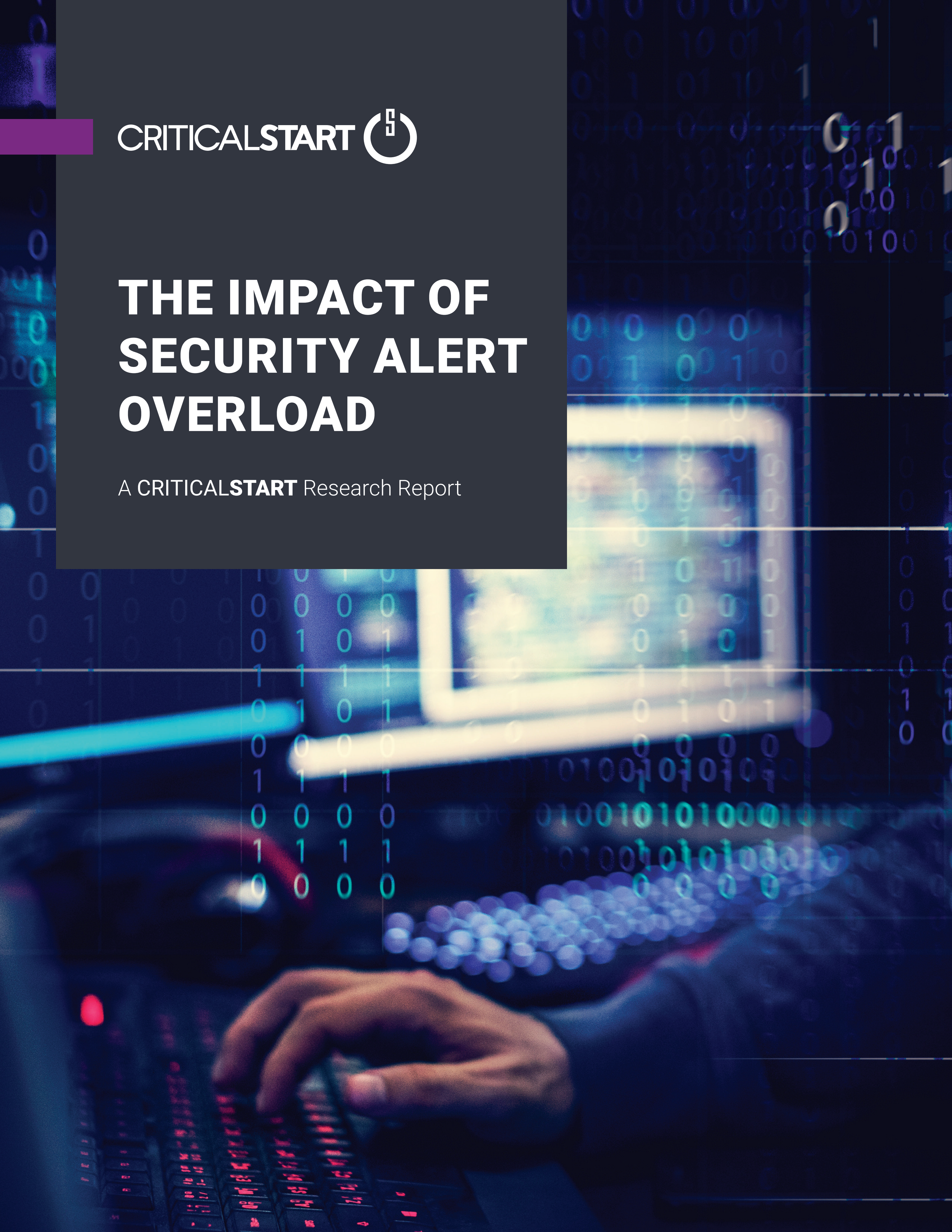


THE IMPACT OF SECURITY ALERT OVERLOAD

A CRITICALSTART Research Report

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 SURVEY GOAL AND METHODOLOGY

CRITICAL**START** conducted a survey of more than 50 Security Operations Center (SOC) professionals across enterprises, Managed Security Services Providers (MSSP) and Managed Detection & Response (MDR) providers to evaluate the state of incident response within SOCs. The survey was fielded Q2 2019.

The report and analysis are based on the responses received from this sample with comparisons drawn to the same questions asked in the company's 2018 report.

This year's report revealed that SOC analysts continue to face an overwhelming number of alerts each day that are taking longer to investigate, resulting in many SOC analysts believing their primary job responsibility is to "reduce the time it takes to investigate alerts."

To cope with the onslaught of alerts, managed security providers simply try to hire more analysts or direct existing ones to ignore certain types of alerts and turn off key features that generate too many alerts – negatively impacting business models and leaving enterprises more susceptible to attacks. The most striking finding is the direct toll the alert overload problem is having on SOC analyst retention.

1.2 KEY FINDINGS

- **NUMBER OF ALERTS:** 70% of respondents investigate 10+ security alerts each day, **up dramatically from last year** when only 45% reported investigating more than 10 each day.
- **TIME TO INVESTIGATE:** 78% of respondents state that, on average, it takes 10+ minutes to investigate each alert, **up from 64% last year**.
- **FALSE-POSITIVE RATE: Respondents still struggle with false-positives**, with nearly half of them reporting a false-positive rate of 50% or higher, nearly identical to last year.
- **RESPONSE TO ALERT OVERLOAD:** When their SOC has too many alerts for analysts to process, 38% either turn off high-volume alerting features or hire more analysts, **both up significantly from last year**.
- **MAIN JOB RESPONSIBILITY:** The number of respondents that feel their main job responsibility is to analyze and remediate security threats has **dropped dramatically from 70% down to 41%** as analysts increasingly believe their role is to reduce alert investigation time or the volume of alerts.
- **CUSTOMER TRANSPARENCY: 57% of respondents** report that MSSPs and MDRs offer customers **limited to no transparency** into investigations or underlying data.
- **CUSTOMER COMMUNICATIONS:** In the age of the mobile enterprise, **email is still king for customer communications** with 73% of respondents reporting it is their primary means of interacting with customers.
- **ANNUAL TRAINING:** Nearly half of respondents say they **get 20 or fewer hours of training per year**.

SOC ANALYST TURNOVER

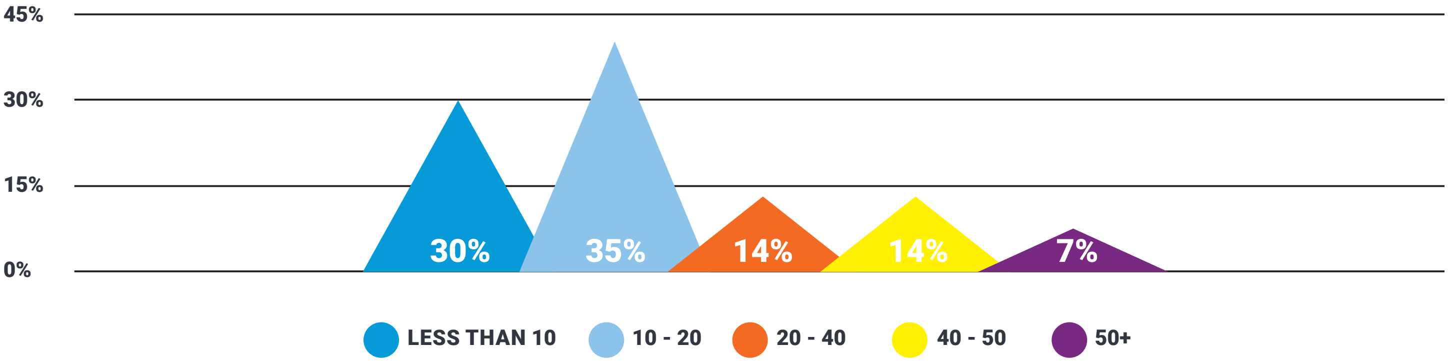
More than three-quarters of respondents report a turnover rate of over 10% of all analysts in their SOC, with nearly half reporting a significant rate of 10-25% turnover.

CRITICALSTART

2 SOCs STILL OVERWHELMED BY “ALERT OVERLOAD”

As IT infrastructures have become increasingly complex to secure against accelerating threats – combined with a tight labor market for cybersecurity experts – enterprises are turning to managed security providers to complement and extend their security and risk management. As the research continues to show, this simply shifts the burden of analyzing an oppressive number of alerts from the enterprise to the managed security provider – a number that then dictates how they hire, staff and run their business.

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



MORE THAN

70%

investigate 10 or more alerts a day

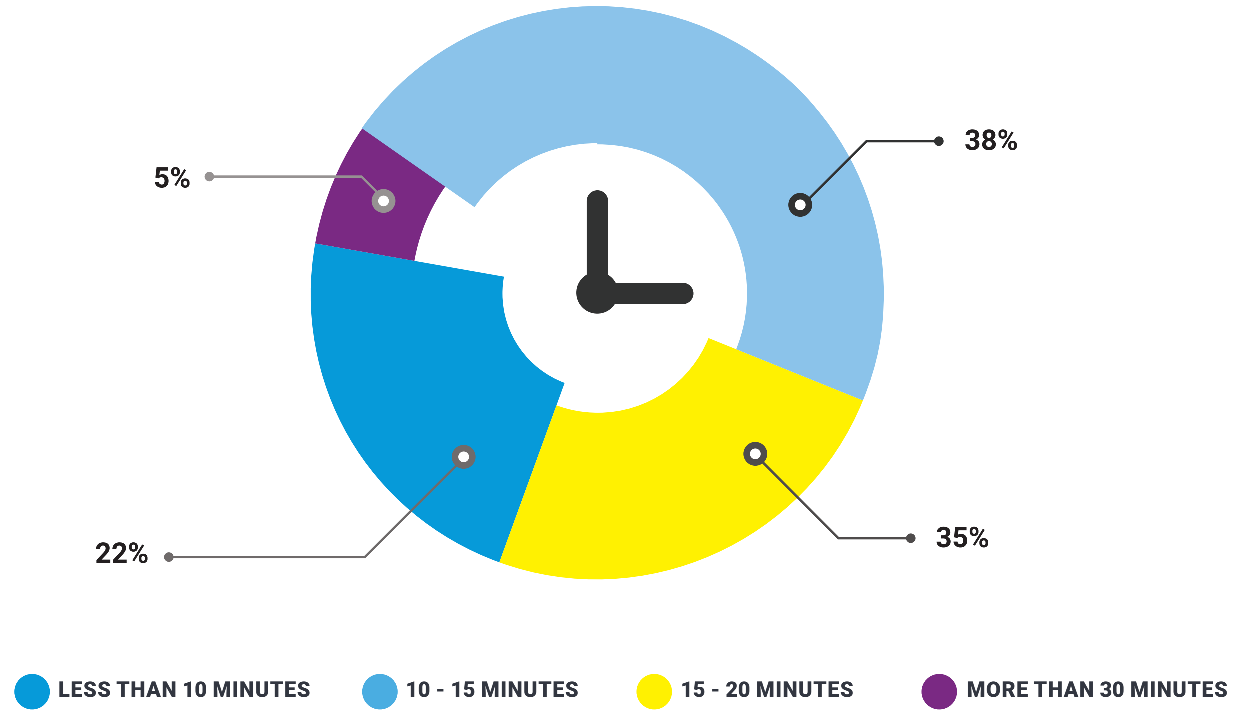
CRITICAL**START**’s research once again validates the industry’s “alert-overload” problem that incident responders are facing with more than 70% reporting they investigate 10 or more alerts each day, up from 45% last year.

CRITICALSTART

3 ALERT OVERLOAD: THE IMPACT ON ANALYST TIME

A subjective process, security analysis takes time for analysts to properly synthesize and investigate incident data from multiple sources, but the time required only serves to compound the alert-overload issue. If there are too many alerts, analysts are forced into a compromise somewhere in the process, either the time to investigate alerts or the number of alerts they can review.

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



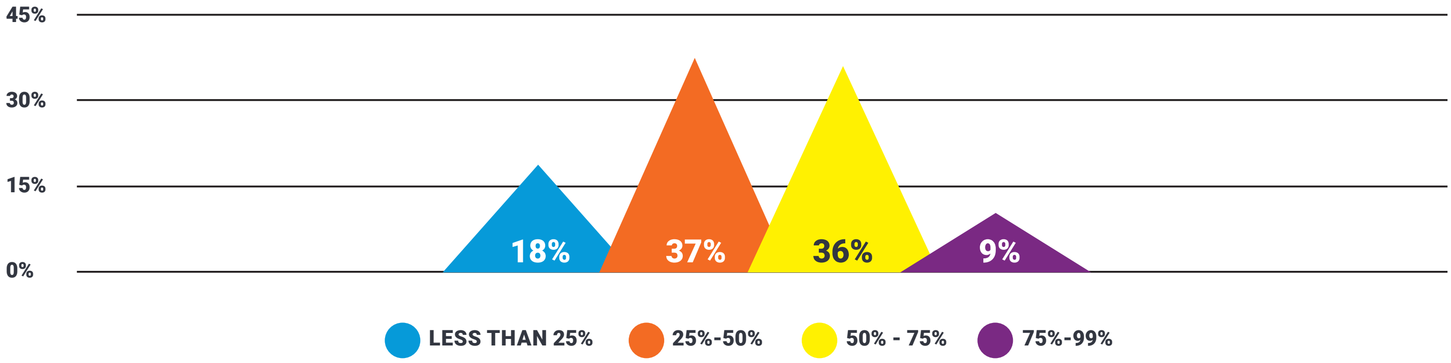
78% of survey respondents state that, on average, it takes 10+ minutes to investigate each alert, which is up from 64% in last year's report. And the number of respondents saying it takes less than 10 minutes is down from last year's 36% to 22%. These numbers underscore that alert investigations are taking longer than just one year ago.

Since nearly eight out of 10 survey respondents note that they investigate at least 10 alerts daily, and the majority spend between 10 and 30+ minutes analyzing each one, we can safely assume that many incident responders are spending between 2.5 and 5 hours each day investigating alerts.

4 ARE YOU (FALSE) POSITIVE?

The alert overload problem is further exacerbated by the number of false-positives that SOC analysts waste valuable time and resources pursuing. Similar to last year, nearly half of survey respondents report a 50% or higher false-positive rate.

TYPICALLY, WHAT PERCENTAGE OF THE ALERTS THAT YOU INVESTIGATE ARE FALSE POSITIVES?



ALMOST HALF REPORT A

50%

or higher false-positive rate

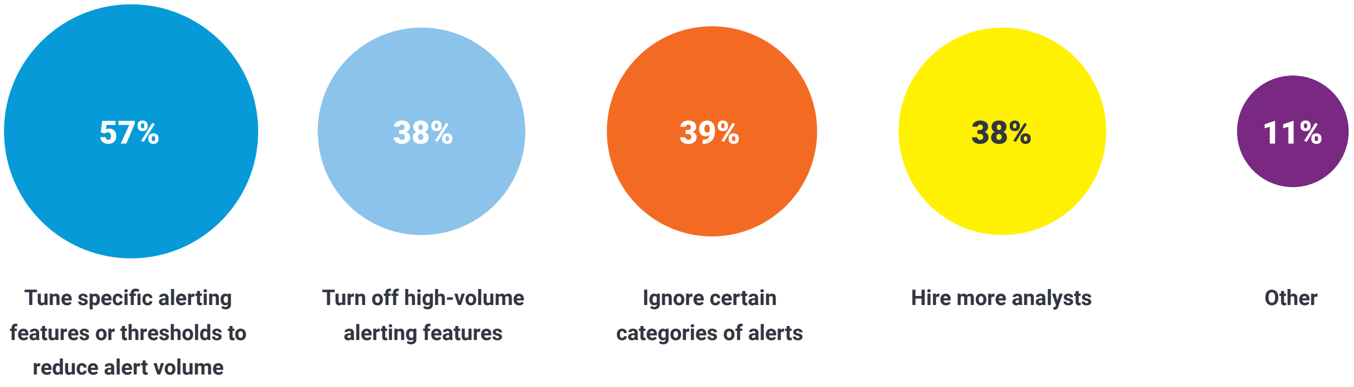
False-positive rates continue to be so high because SIEM and incident response tools are tuned to identify suspicious events, but end up generating alerts on well-known and safe activity resulting in far too many investigations that end up with false-positives. While these tools can help in aggregating and coordinating data to analyze and process alerts, they do not address the challenges of increasing alert volume and the high rate of false-positives.

5 ALERT OVERLOAD DICTATES BUSINESS MODELS

As originally identified in the 2018 report, the alert overload problem extends beyond enterprise security levels and analyst investigation time, it fundamentally drives the business models, impacting staffing and operational processes.

When asked what they do if their SOC has too many alerts for analysts to process, 57% of respondents said that their primary approach is to tune specific alerting features or thresholds to reduce alert volume. This was the primary approach last year as well, although with 67% using it. While that would seem like good progress, respondents this year also reported they ignore certain categories of alerts (39%); turn off high-volume alerting features (38%); and hire more SOC analysts (38%) – with the latter two categories showing increases over the previous year of 11% and 14% respectively.

IF YOUR SOC HAS TOO MANY ALERTS FOR THE ANALYSTS TO PROCESS, WHAT DO YOU DO?



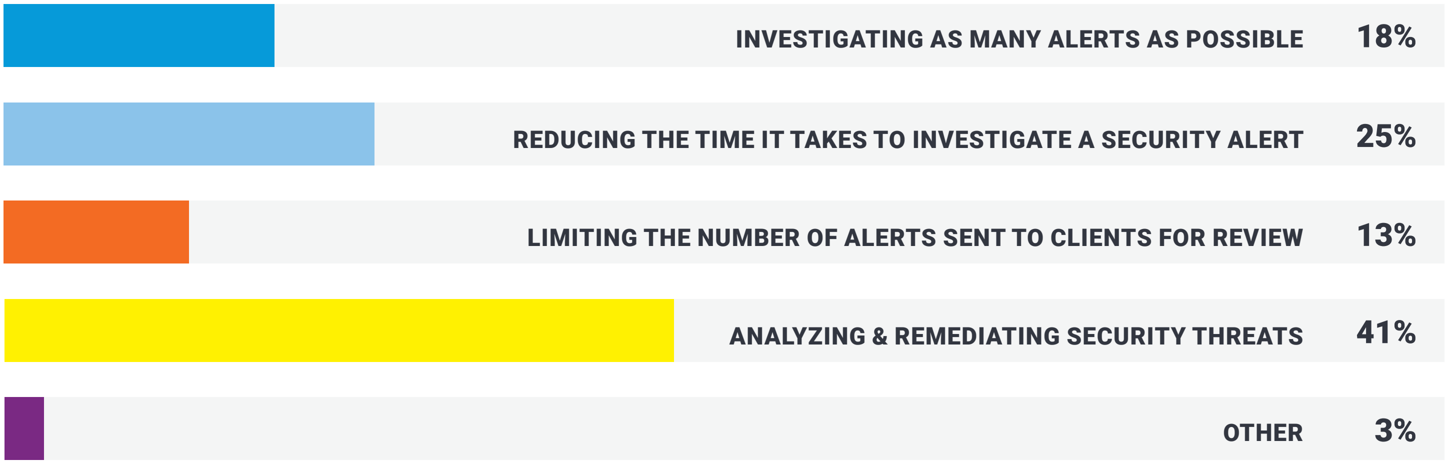
As this year's responses show, MSSPs, MDRs and enterprises continue to struggle with how best to manage the alert overload problem, with significant increases in the number of respondents hiring more analysts or turning off security features, underscoring the market challenge in trying to keep up with the volume of alerts.

6 THE TYRANNY OF ALERTS

By definition, the SOC analyst role is to investigate and prevent malicious activity and intruders, but eventually the sheer number of alerts and limited time to process them has an impact on how they view the requirements of their role.

When survey respondents were asked what they feel is the main responsibility of their job, 41% said it was analyzing and remediating security threats, however that number was down dramatically from 70% last year.

WHAT DO YOU FEEL IS THE MAIN FOCUS OF YOUR JOB AS A SOC ANALYST?



5x

more respondents than last year report reducing investigation time as the main part of their job

As could be expected, the number who responded that investigating as many alerts as possible was the primary responsibility jumped from 5% last year to 18% this year. In addition, the number that said reducing the time it takes to investigate a security alert increased five times, from 5% last year to 25% this year.

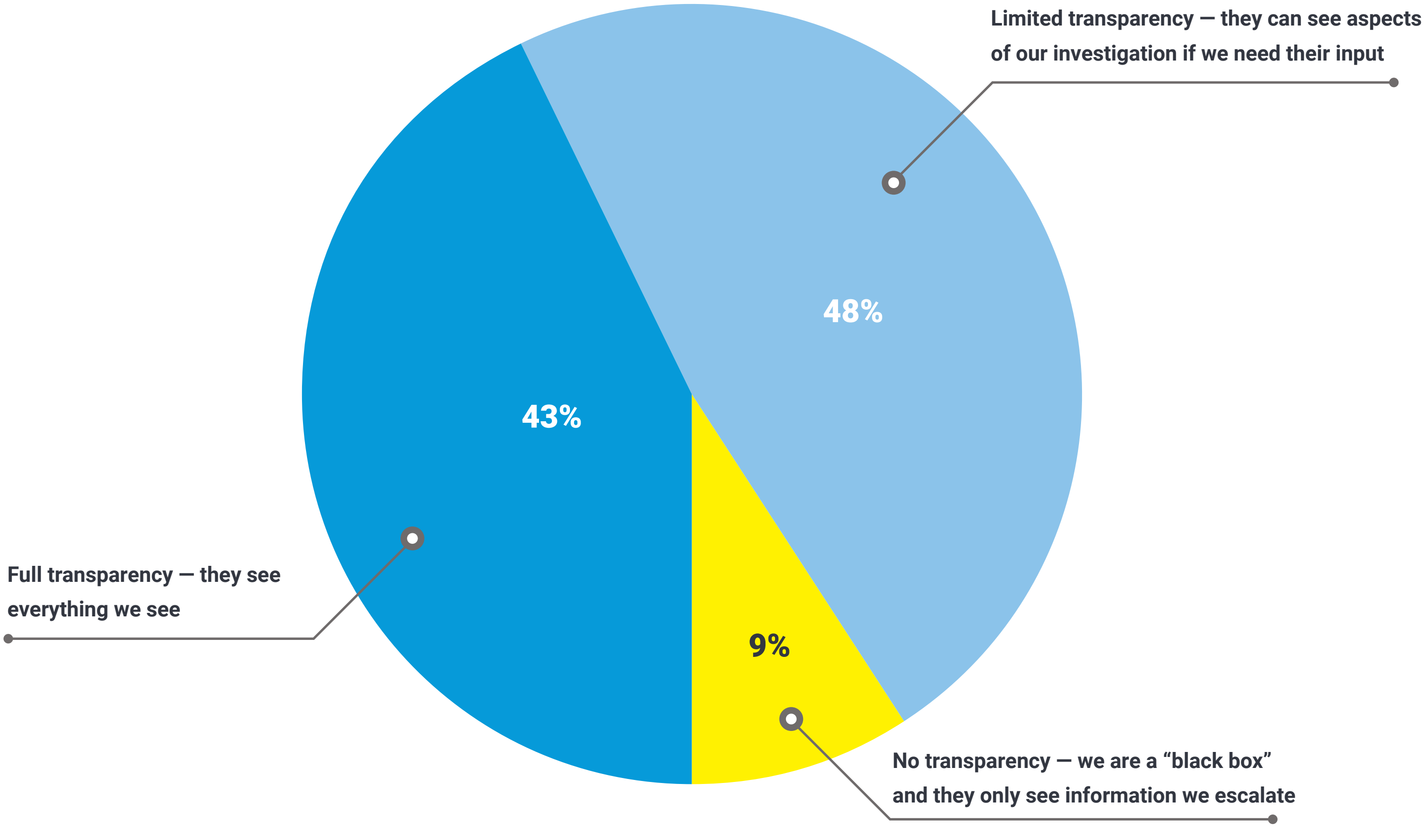
7 “BLACK BOX” VS. FULL TRANSPARENCY

As more enterprises outsource some or all of their security to address the alert overload problem, they are realizing there are dramatically different operational models between managed security providers.

Many managed security providers take a “black box” approach where the only access a client has to an issue or investigation is when the MSSP or MDR forwards them details that need further review or context. If organizations want to pursue their own analysis, they are not able to do so. Other MSSPs and MDRs provide more access all the way up to full transparency where a client can see and access everything that the SOC analysts see whenever they want.

Based on survey respondents, a clear majority (57%) report they offer limited to absolutely no transparency to their clients. In these situations, clients who are paying for managed security services only see information relevant to their enterprise security if the MSSP or MDR escalates an incident to them needing further information.

HOW TRANSPARENT ARE SOC ANALYSTS WITH CUSTOMERS/USERS REGARDING INVESTIGATIONS?

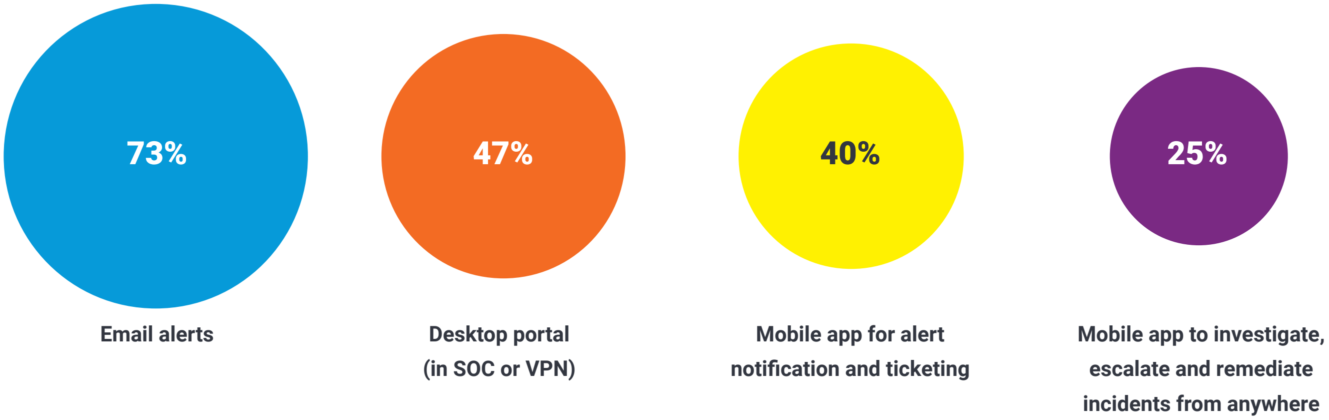


8 CUSTOMER COMMUNICATIONS

This year's survey also investigated the primary means of communications between SOC analysts – either in-house or at an MSSP/MDR – and their enterprise clients and customers.

Email dominated as the go-to communications channel at an overwhelming 73% of respondents followed by a desktop portal accessed in the SOC (or through a VPN) at 47%. Survey respondents did say that 40% leverage a mobile app for alert notification and ticketing while only 25% said they used a mobile app to investigate, escalate and remediate incidents from anywhere.

HOW DO YOU INTERACT WITH CUSTOMERS/USERS?



SOC COMMUNICATIONS COMPARISON

EMAIL ALERTS LEAD AT

73%

vs.

MOBILE APPS ONLY AT

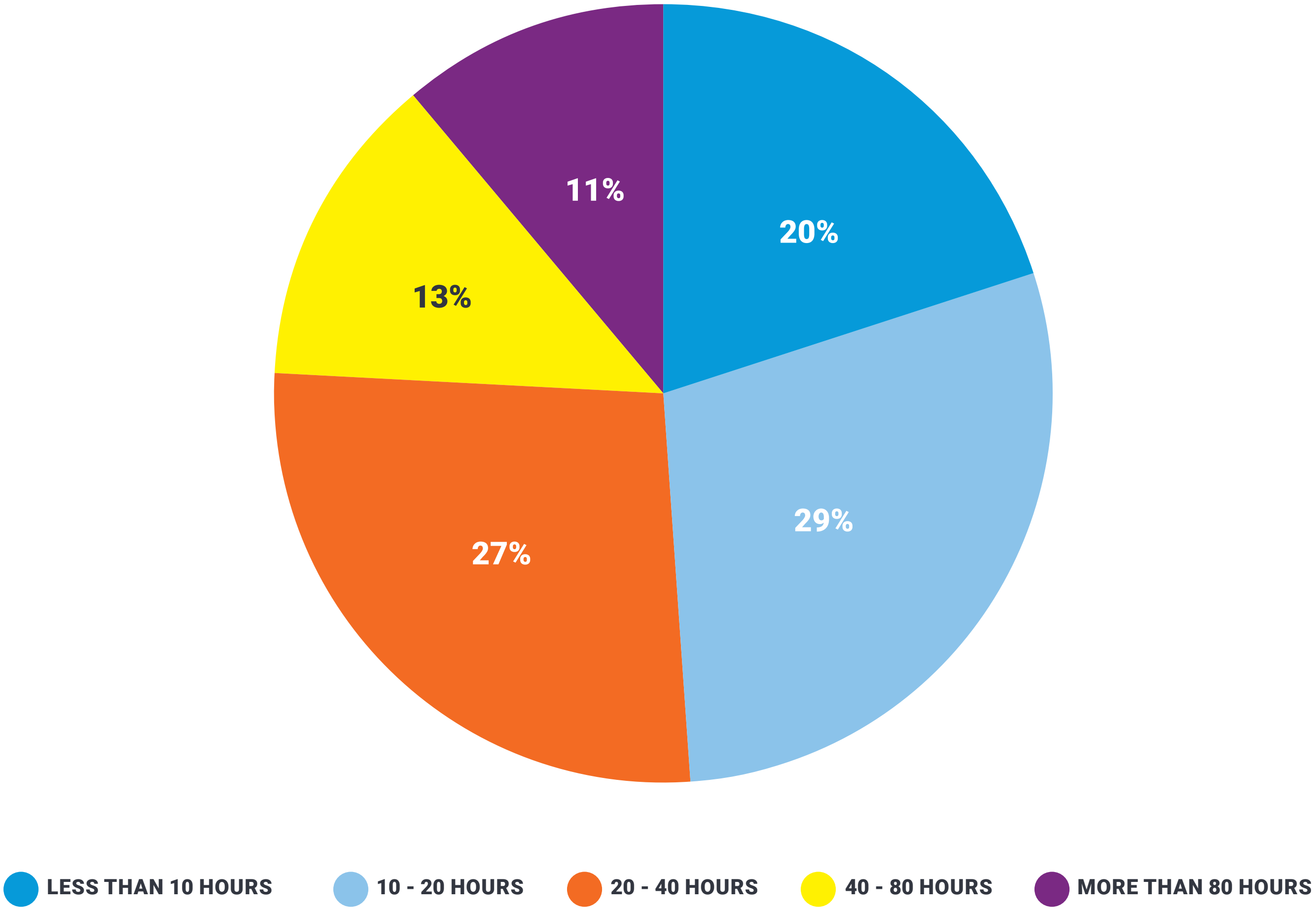
25%

9 CYBERSECURITY TECHNOLOGY TRAINING

Given the dynamic, fast-paced nature of cybersecurity and the need for analysts to stay ahead of the constantly-evolving methods and attack vectors of hackers, this year's survey explored how much training SOC analysts average on an annual basis.

Surprisingly, 50% of respondents report they receive 20 or fewer hours of training annually, which works out to be a little over an hour and half per month. However, this is clearly an area where MSSPs and MDRs are beginning to differentiate themselves as 13% of respondents reported receiving 40-80 hours of training annually and 11% said they received more than 80 hours.

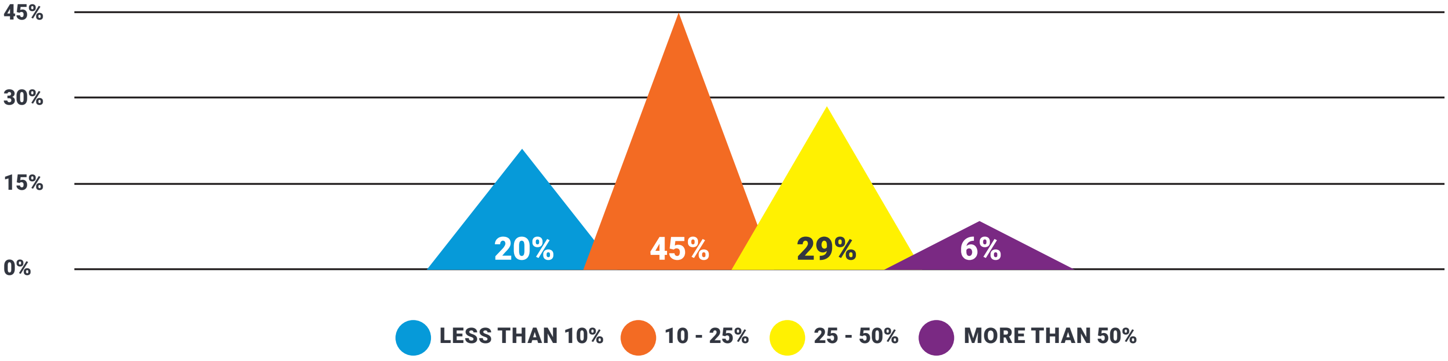
HOW MUCH CYBERSECURITY OR TECHNOLOGY TRAINING DO YOU GET ANNUALLY?



10 SOC ANALYST TURNOVER

In a new question, the survey sought to understand the level of SOC analyst turnover in a given year as an indicator of the alert overload problem. Being buried in alerts, many of them false-positives, and being forced to try and reduce the time to investigate them with little to no training sounds like a high-stress work environment that is ripe for analyst churn. And the numbers illustrate that.

HOW MUCH TURNOVER HAS YOUR SOC EXPERIENCED IN THE PAST 12 MONTHS?



80%

experienced 10% or more analyst turnover

The vast majority (80%) of survey respondents said their SOC had experienced at least 10% analyst turnover. The largest pool of respondents (45%) noted they had experienced 10-25% turnover while more than a third (35%) had lost a quarter or more SOC analysts in less than 12 months.

CRITICALSTART

11 ABOUT CRITICAL**START**

CRITICAL**START**, the MDR experts that leave nothing to chance. The company developed the industry's only cloud-based, SOAR platform that resolves 99% of security events on its own to eliminate compromises and stop breaches. Our mission is simple: protect our customers' brand while reducing their risk. We do this for enterprises through our award-winning portfolio of end-to-end security services, including MDR and Professional Services.

Visit **www.criticalstart.com** for more information.

CRITICAL**START**