Alert Overload Still Plagues Cybersecurity Industry

A CRITICALSTART Research Report on Trends in the Cybersecurity Industry

CRITICALSTART
They're good. We're better.

Table of Contents

Executive Summary

01

Survey Goal & Methodology

Our annual survey compares the state of cybersecurity in 2020 to the landscape in 2019 to identify trends.

Click here to view the 2019 Report

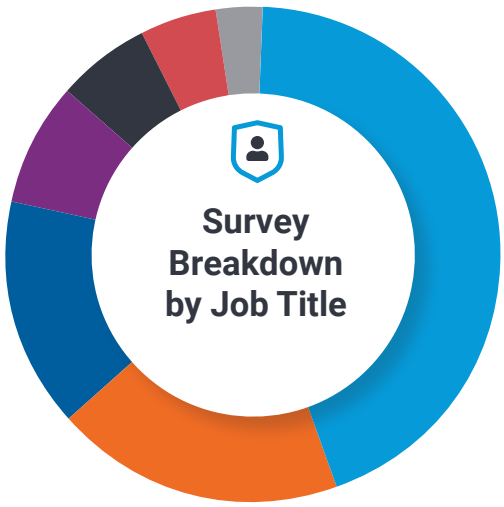
Top Level Insights

While we did see a broad-spectrum increase in generated alerts in 2020, it wasn't the rise in the overall volume that caught our attention. It was the shift in the types and priority level of alerts that marked a change in the security landscape.

Much of the shift can be attributed to the fact that the complexity of today's work environment has changed significantly compared to a year ago. The rapid migration to remote work shifted the level of exposure while much of the corporate world struggled to respond with the appropriate level of protection. This gap was exploited by targeted ransomware attacks and large nation-state level campaigns.

The change in the complexity of the environment and the lack of an established, hardened perimeter to protect that environment is what likely led to higher criticality of alerts and more successful attacks overall.

For this report, we surveyed 100 cybersecurity professionals to learn what they experienced last year and discover how the industry has—or hasn't—evolved.



- 44% Security Engineers
- 19% Director of Security Infrastructure
- 15% Executive/C Suite
- 8% VP of Security/ Infrastructure
- 6% NOC Engineer
- 5% CSO/CISO
- 3% Other

Lack of Investigation

47% are investigating only **10-20** alerts per day.

Job Security

46% state that they have experienced **10-25%** turnover at their organization during 2020.

Longer Hours

A **10%** drop in investigations that took 10 minutes or less while investigations of 11-15 minutes increased by **5%**.

Focus on Training

38% get 10-20 hours of cybersecurity or technology training annually.

False Positives Plague Industry

68% reported that **25-75%** of the alerts they investigate are false positives.

Mobility on the Rise

43% interact through a mobile app to investigate, escalate, and remediate incidents from anywhere.

Turning a Blind Eye

49% turn off high-volume alerting features when there are too many alerts to process.

Quantity or Quality?

33% state that analyzing and remediating security threats is their main job, **35%** state that investigating as many alerts as they can is their primary focus.

Alert Overload Isn't Going Away

02

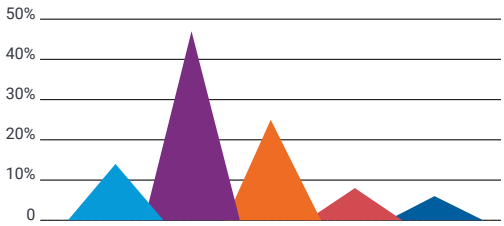
With such a prominent shift in the criticality of alerts, we explored if organizations are investigating and resolving these alerts properly to prevent breaches and limit the dwell time of potential attackers.

Question

Number of Alerts:

How many incidents do you personally investigate each day on average?

Answers



14% less than 10 (30% in 2019)

47% 10-20 (35% in 2019)

25% 21-40 (14% in 2019)

8% 41-50

6% 50+

Key Takeaway

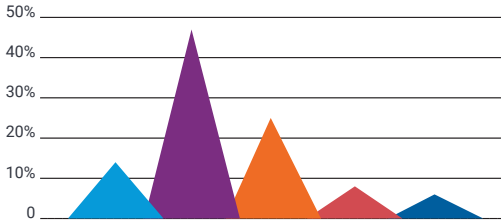
This data begs a startling question: With almost 50% of respondents only investigating up to 20 alerts per day (and with this figure climbing 12% compared to the previous year), how many alerts are not investigated or even worse, ignored, when an organization generates an average of 5,000 alerts daily?

Question

Average Time to Investigate:

How much time does the average incident/ alert take you to investigate?

Answers



12% less than 10 minutes (22% in 2019)

43% 11-15 minutes (38% in 2019)

29% 16-20 minutes

16% more than 20 minutes

Key Takeaway

There was a 10% drop in investigations that took 10 minutes or less while investigations lasting 11-15 minutes increased by 5%. Organizations must get a handle on what is leading to fewer alerts being investigated, but for longer amounts of time. This feeds directly into what we asked our respondents next.

Positively False: Alert Overload Compounded by Non-Threats

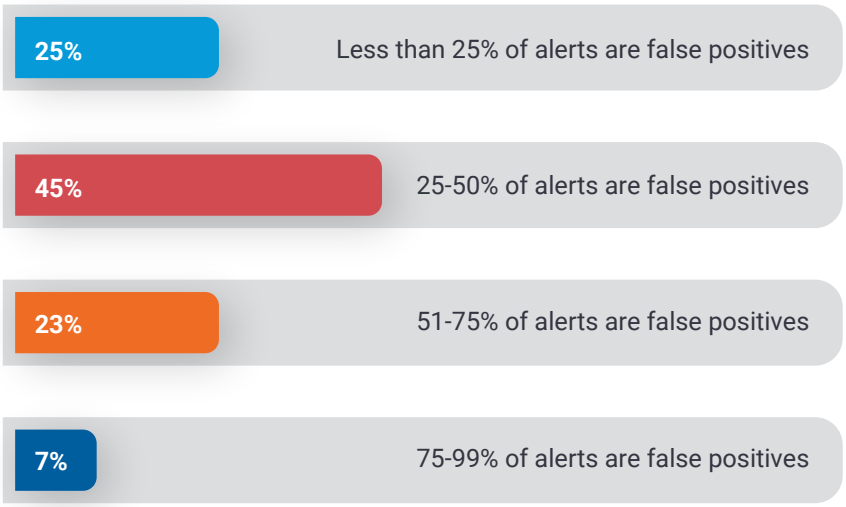
03

One of the most troubling findings for the cybersecurity industry is that 68% of respondents reported that more than 25% of the alerts they investigate are false positives. This volume inevitably leads to countless hours wasted, opening the security door to real threats that are either missed or flat out ignored.

Question

Typically, what percentage of the alerts you investigate are false positives?

Answers



Key Takeaway

A deep analysis of these figures hints at a more disturbing trend: If a significant portion of respondents are only investigating 20 alerts per day, and a large group spends 11-15 minutes investigating alerts, that's over two hours per day of wasted work. And if ¼-¾ of the time spent on those alerts is wasted on false positives, that means an analyst can lose 1-3 hours per day on average.

Calculating the Waste Equation

If you're worried that your team is wasting time chasing false positives, ask yourself the following:

- How many alerts are being generated per day?
- How many are actually investigated?
- How many are false positives?
- How much risk is actually mitigated considering the time wasted on false positive alerts?

The Cost of Ignorance

04

So, what is driving this trend of so few alerts being evaluated and so much time wasted on the ones that are actually investigated? Our next question provides insight.

Question

If your SOC has too many alerts for the analysts to process, what do you do?

Answers

68% reduce the alert volume of specific alerting features or thresholds, up from 57% in 2019

28% ignore certain categories of alerts, decreasing from 39% in 2019

49% turn off high-volume alerting features compared to 38% in 2019

42% hire more analysts

Key Takeaway

The responses to this question confirms that a limited number of alerts are being investigated. This number is shrinking not because threats are going away—it is because security professionals are spending undue time triaging false positives and silencing or ignoring a majority of alerts that do surface. And while it's true that **increased adoption for detection tools** within the security ecosystem could play a role in driving down human intervention on alerts, the response above reveals a much more serious issue for the industry.

Faced with alert overload and fatigue, almost half of respondents are turning off high-volume alerts, while almost one-third are ignoring certain alert categories. This can open a significant vulnerability for an attacker to exploit.

49% of respondents turn off high-volume alerting features compared to 38% in 2019.

Eye on Alerts

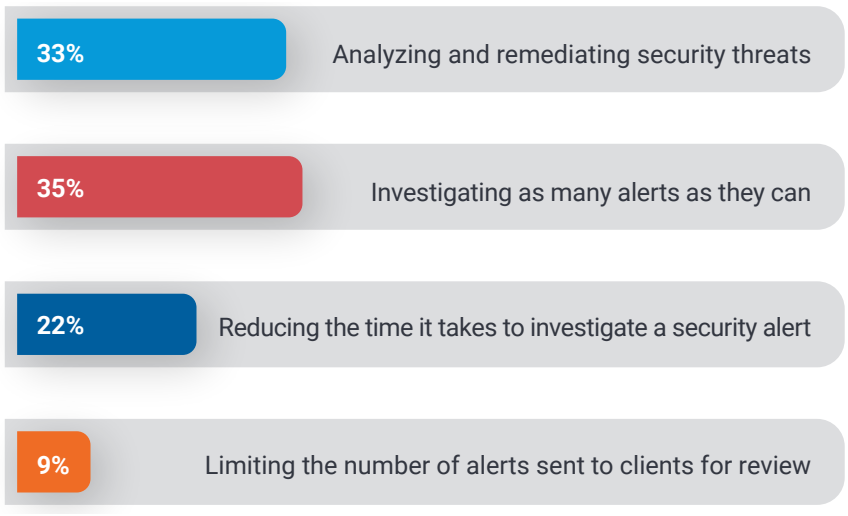
05

With alert fatigue seemingly dominating a security professional's day, we asked what they believed to be the primary part of their job.

Question

What do you feel is the main part of your job?

Answers



Key Takeaway

These responses point to alerts that are not analyzed and remediated, as much as they were instead processed on a quantity basis. This can mean that important alerts are not receiving the proper escalation.

35% of respondents state that investigating as many alerts as they can is the main part of their job.

Email is King, but Mobile is Gaining

06

Along with where they spend their time, how security professionals coordinate with their teams is of real importance, as communication and coordination can make a real difference in limiting the dwell time of an attacker.

Question

How do you interact with your team?

Answers

72% through email alerts

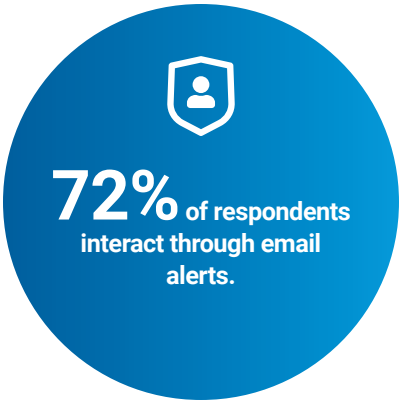
60% through a mobile app for alert notification and ticketing, compared to 40% in 2019

60% through a desktop portal (in SOC or VPN), compared to 47% in 2019

43% through a mobile app to investigate, escalate, and remediate incidents from anywhere, compared to 25% in 2019

Key Takeaway

While email still leads the pack, there is increasing adoption of mobile applications to investigate, escalate and remediate alerts, as well as responding to alert notifications and ticketing. This trend highlights the importance of capabilities within a mobile app, as ticketing and alert notification are only part of what users really need to do their job effectively.



Back to School

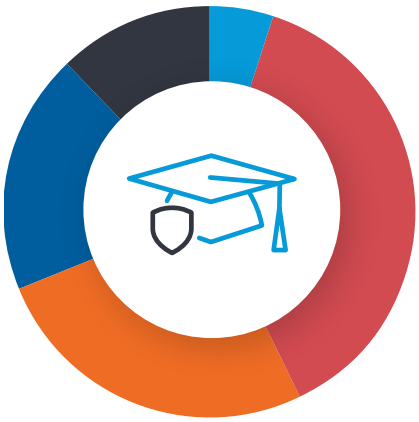
07

Respondents indicated a renewed focus on training in 2020. This could be due to COVID-19, as security team members likely had more time to focus on online training.

Question

How much cybersecurity or technology training do you get annually?

Answers



5%
get less than 10 hours of training annually

38%
get 10-20 hours annually

26%
get 21-40 hours of training annually

19%
get 41-80 hours of training annually

12%
get more than 80 hours of training annually

Key Takeaway

Within cybersecurity, we are also seeing more MSS providers and professional services companies offering training to customers. They are also requiring more training within MSSP organizations. This could be due to more organizations realizing the need to amp up their offensive and defensive security strategies.

Cybersecurity professionals with cloud experience will be in high demand in 2021. A report from Atlas VPN found the need for cloud security experts will

increase 115%

over the next five years.

Help Wanted

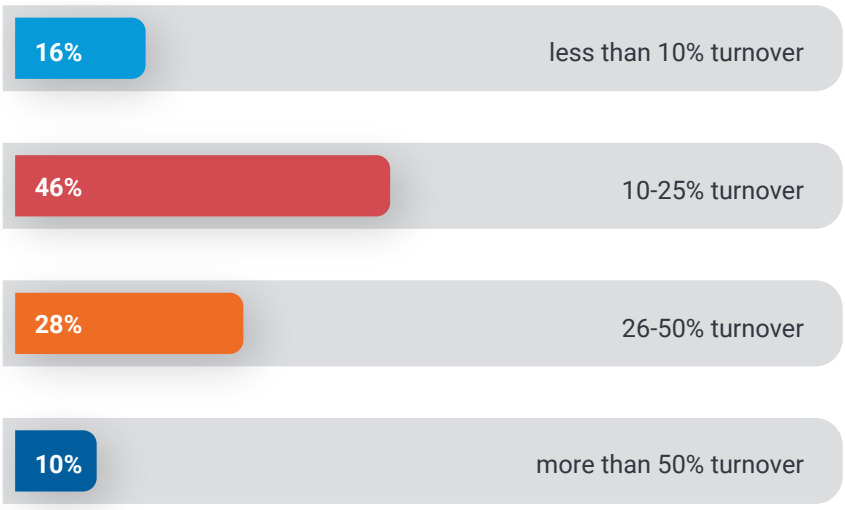
08

Finally, we wanted to gauge the impact of 2020 on the labor market for cybersecurity. This proved to be a bright spot for the year, as respondents indicated turnover was remarkably similar to 2019 in spite of the economic and business challenges posed by the ongoing pandemic.

Question

How much turnover has your SOC experienced in 2020?

Answers



Key Takeaway

While it would be reasonable to expect an increase in turnover due to COVID-19, security professionals may be seeking stability and not considering a job change in the current economic climate. These figures could also be due to the critical importance of cybersecurity during the dramatic increase in the global remote workforce.

46% of respondents state that they have experienced 10-25% turnover.

COVID-19 Impact in 2020

66% of respondents reported seeing an increase in alerts since the known spread of COVID-19 began in mid-March.

89% said they have been forced to work remotely as a result of COVID-19.

80% responded they have taken steps to change the security posture of their organization because of COVID-19 induced remote work.

The remote work trend, while significant, likely only accelerated and exacerbated security trends that were in motion prior to the rise and spread of the pandemic. Although these shifts were already well under way, there is no doubt that the staying power of COVID-19 has altered the security landscape, resulting in changes and impacts that will continue to be felt long into the future.

About CRITICALSTART

09

CRITICALSTART believes in MDR that doesn't suck. We believe that to achieve that means detecting every threat and resolving every alert. That's why we don't prioritize—we itemize. We've built a registry of all trusted behaviors that is continuously updated so our clients can benefit from the experiences of everyone in the community. This means we can reduce false positives and focus on un-trusted behavior to tackle it with a relentless resolve.

CRITICALSTART offers an award-winning portfolio of end-to-end security services, including MDR and professional services built around three core values:

1. Do what's right for the customer.
2. Do what's right for our employees.
3. Don't do things that suck!

Visit www.criticalstart.com for more information.