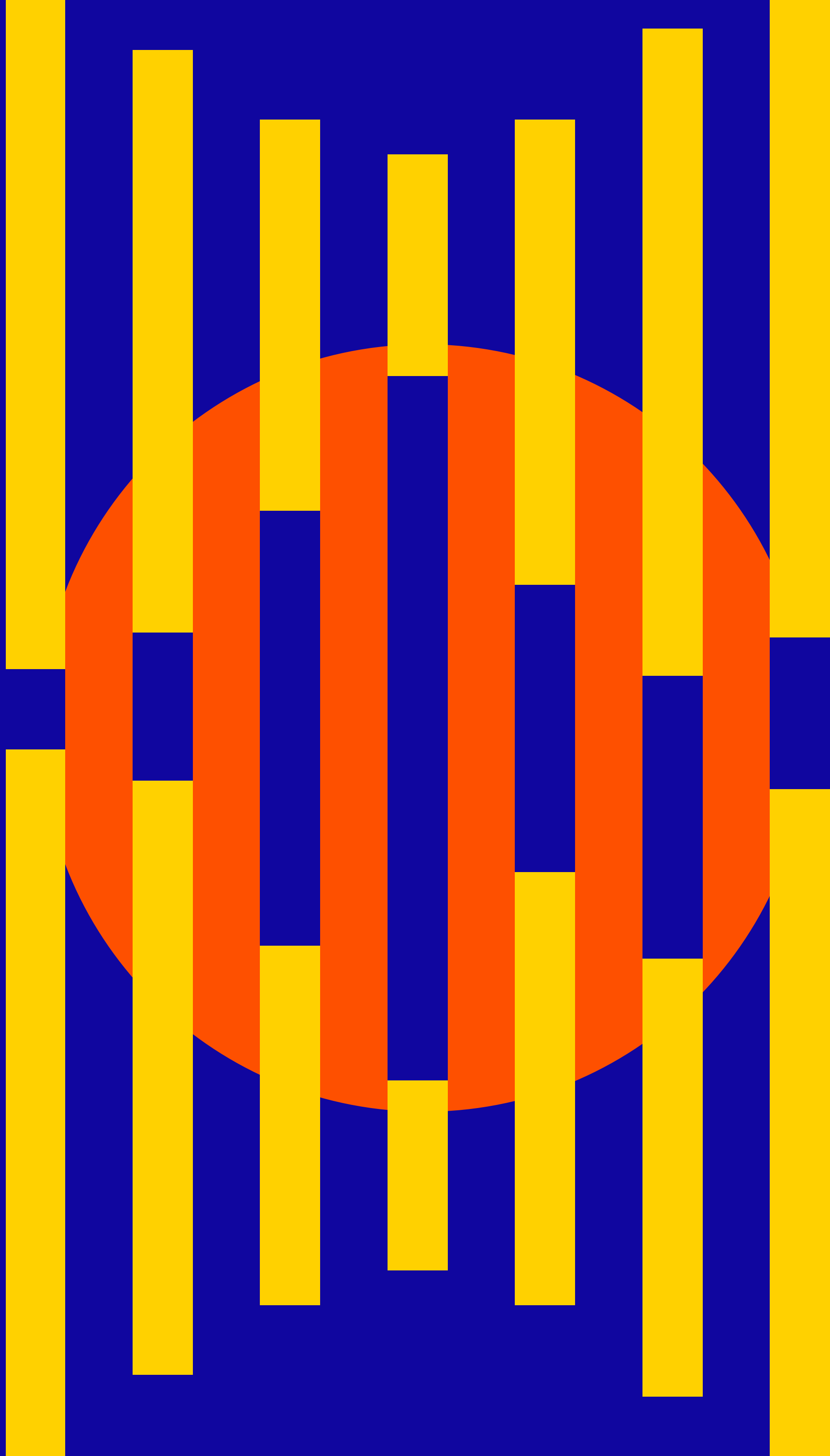
The 4 Perils of Cybersecurity False Positives

Why It’s Time to Cut the Noise in Your Data (& How to Do It)

censys



Are You Paying Attention to the False Positives in Your Threat Intelligence Data?

It happened again.

You know this cybersecurity song-and-dance all too well.

You spent the last three hours investigating a threat that your automated monitoring tool alerted you to, only to discover … there's no threat at all. The tool spotted some strange but harmless activity on your network, and incorrectly flagged it as malicious. As a result, you were sent on a wild goose chase that upended your morning.

You sigh, and take a deep swig of coffee. You wish you could say this kind of mistake was unusual, but it happens almost every day, multiple times a day.

It's the peril of false positives, and you've come to accept it as a part of your job. False positives are the pesky, persistent inconveniences that you and your team just can't seem to escape.

In fact, because you encounter them so often, they hardly faze you anymore. They're just part of the laundry list of cybersecurity stressors that your team has started to feel powerless against.

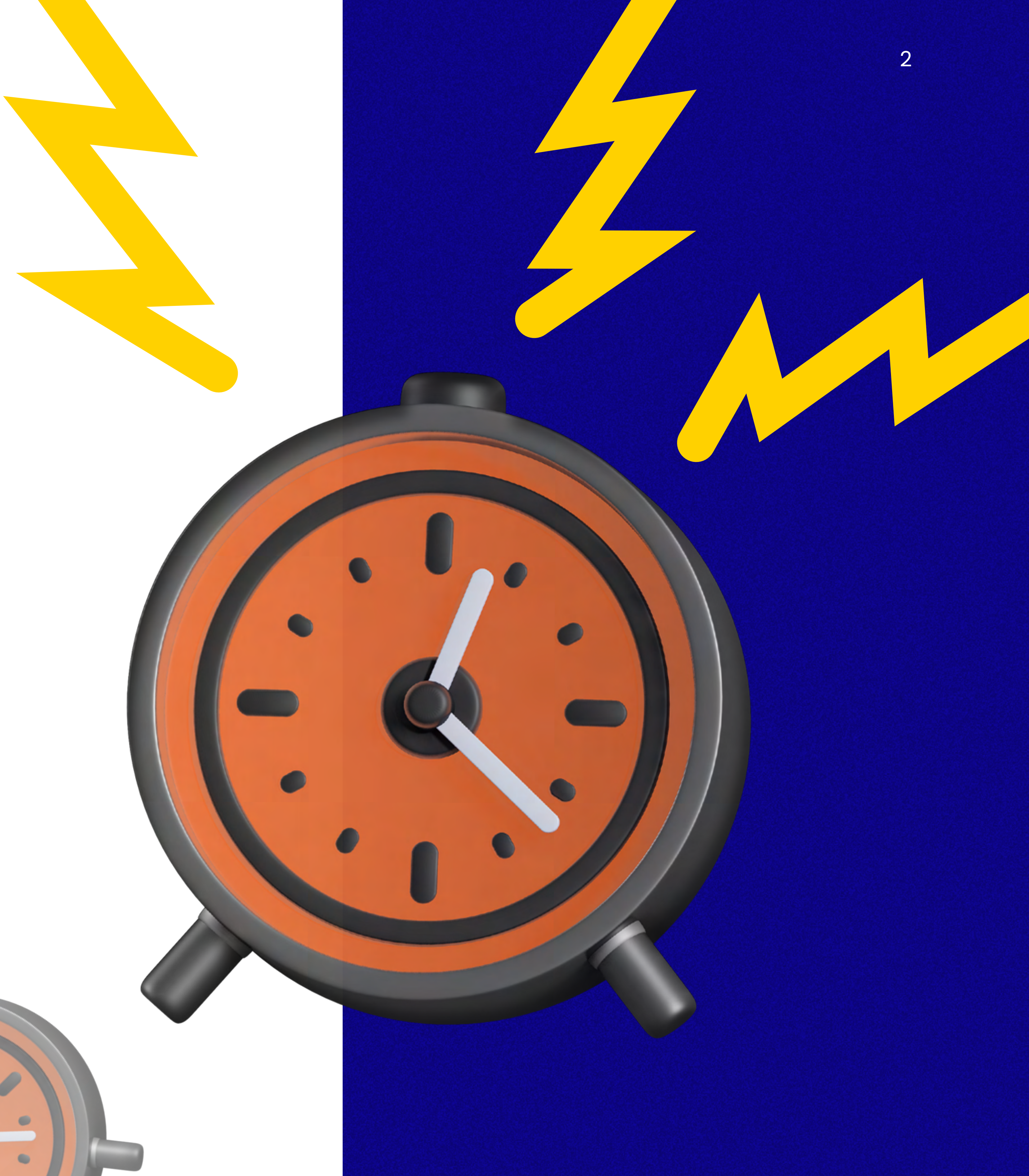
Plus, you tell yourself, it's better to deal with tools that flag harmless activity than tools that miss threats altogether, right?

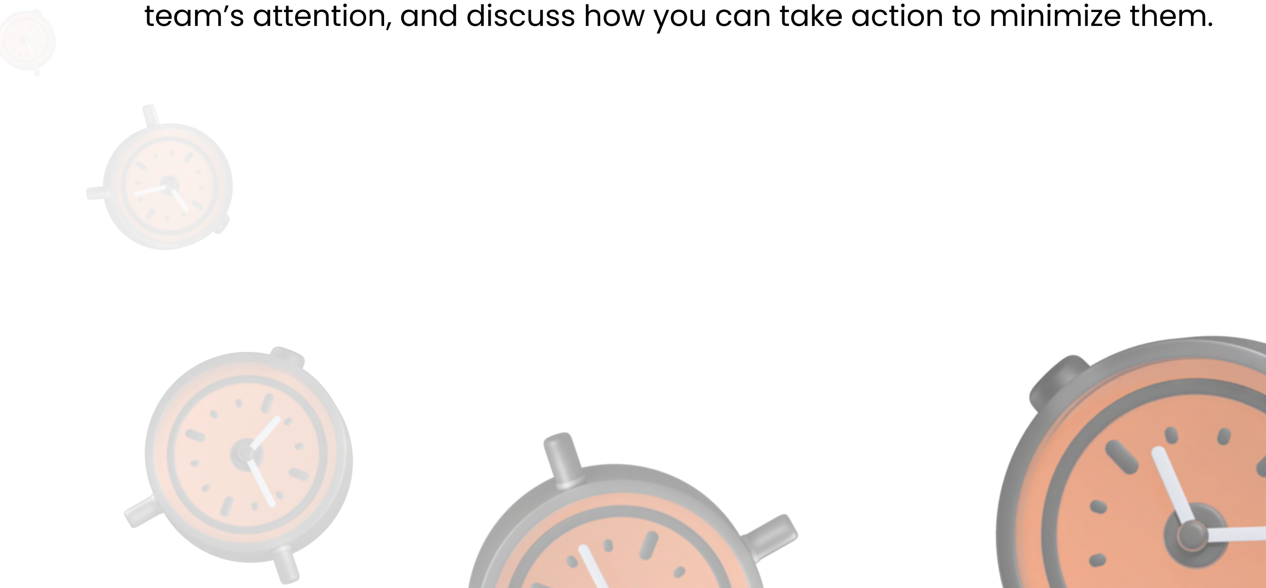
If this sounds familiar, this guide is for YOU.

False Positives Aren't Inevitable

False positives don't have to come with the territory. And if your team has stopped paying attention to the significant consequences they incur, or believe they should be tolerated because they're better than the alternative, consider this your wake up call.

In this guide, we highlight four key reasons false positives demand your team's attention, and discuss how you can take action to minimize them.





Houston, We Have a False Positives Problem

Let’s first level set with an understanding of just how pervasive false positives can be.

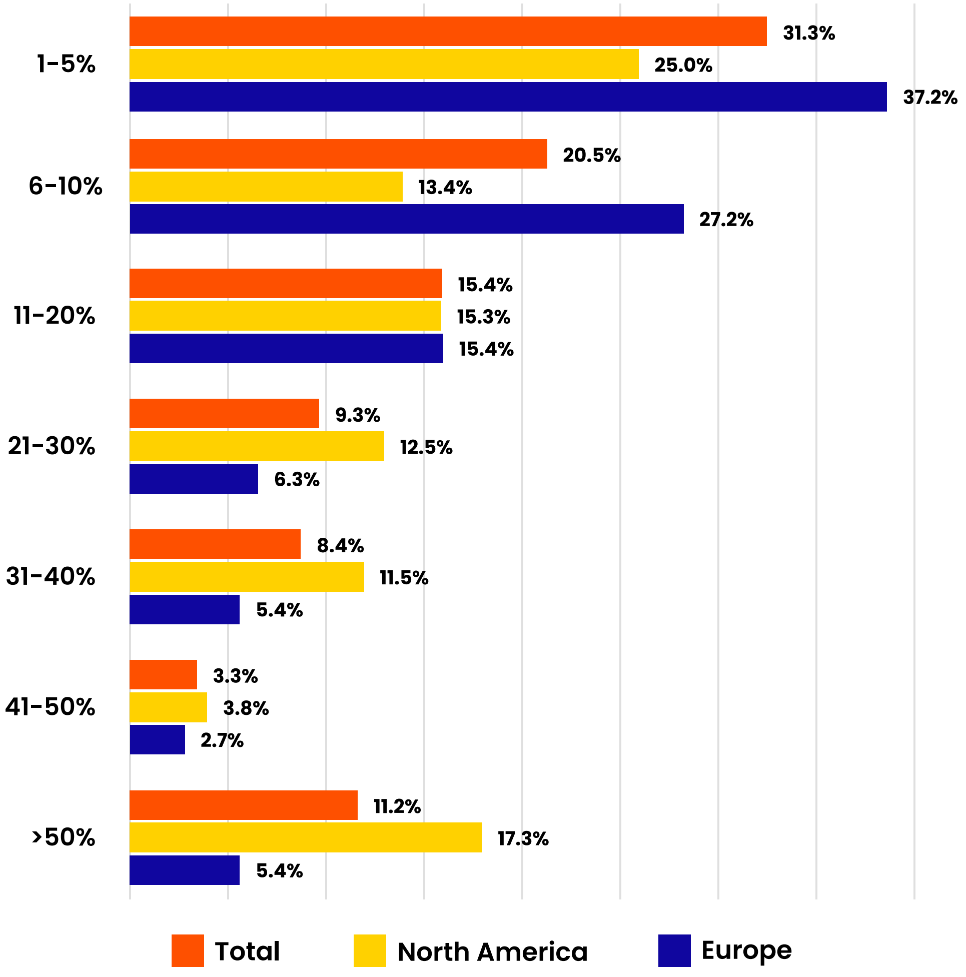
In our 2024 State of Threat Hunting Report, we found that almost all threat hunters encounter false positives in their work – and not just occasionally. Nearly one-third of respondents said that within the last year, at least 20% of the threats they identified were false positives. That’s one false positive threat for every five threats.

When looking at responses by region, our reporting found that 17% of threat hunters in North America encountered more than 50% of false positives in their findings. That’s a staggering rate of inaccuracy for almost 20% of threat hunters to be up against.

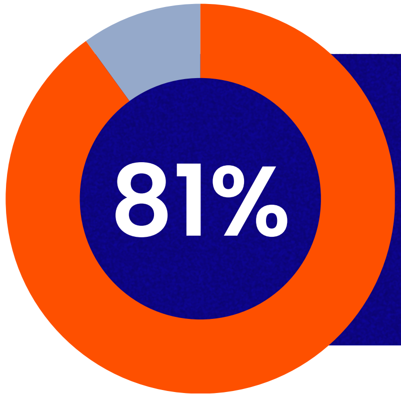
Given these findings, it makes sense that achieving fewer false positives was also identified by our respondents as one of the **top three things** that would improve their jobs.

> “False positives are the main stressor for me. When it happens [the threat report provided to management turns out to be inaccurate, due to false positives], I feel real shame.”
>
> - Threat Hunter, Mid-Sized Organization

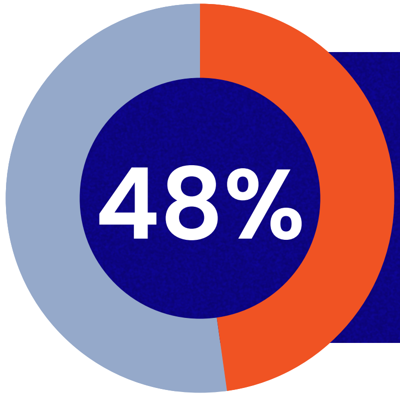
Approximately what percentage of the threats you have identified in the last 6-12 months have turned out to be false positives?



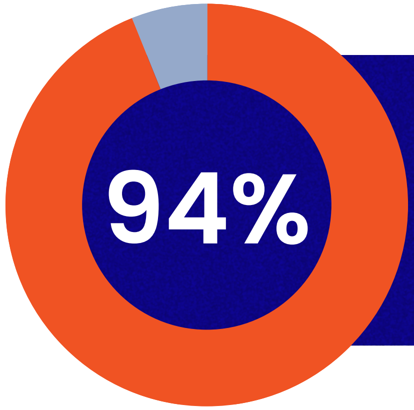
Other studies report that false positives are even more prevalent:



of IT professionals surveyed in the Orca Security 2022 Cloud Security Alert Fatigue Report said that 20% of their security alerts are false positives.



of the enterprise organizations receive more than 10,000 security alerts each day. 52% of those alerts are false positives, according to a Cybersecurity Insider report. That's an incredible volume of false alarms that teams are asked to make sense of.



of 500 DevSocOps professionals surveyed by InfoSecurity Magazine, report false positives in vulnerability reports, while 67% find them often or all the time.

False positives rates may vary from study, but collectively, they paint a bleak picture:

False positives are rampant.

Teams like yours may acknowledge they're up against an onslaught of false positives, but the majority have yet to make any meaningful headway against them.

It's time to change that. Here's why.

1

False Positive Peril #1

Your Valuable Time Is Wasted

False positives deserve attention and action because they steal your time. This is time better spent fighting real threats, or tackling other security tasks.

Responding to one false positive might not seem like a big deal, but time adds up quickly. For every alert that triggers a ticket, there's an analyst on the other end (maybe it's you!) that has to validate it. This involves learning about the nature of the threat, where it's coming from, what it might impact, and so on. It's investigative work that requires a fair amount of time and consideration.

When these alerts are false positives, not only are ticket queues jammed with extra noise, but time is wasted on completely unnecessary investigation.

False positives can eat up even more time because these alerts often lack needed context.

The underlying data gaps at the root of false positives can make it difficult to validate the threat, and send analysts searching down rabbit holes of disparate data sources.

> “More than 60% of security professionals estimate their security function spends over 3 hours per day validating false positives. Nearly 30% are spending over 6 hours on this task. Most agree that it is too much, and the time could be better utilized. For most, it is the part of their job they like least.”
>
> - InfoSec Europe Study

The Clock Is Ticking

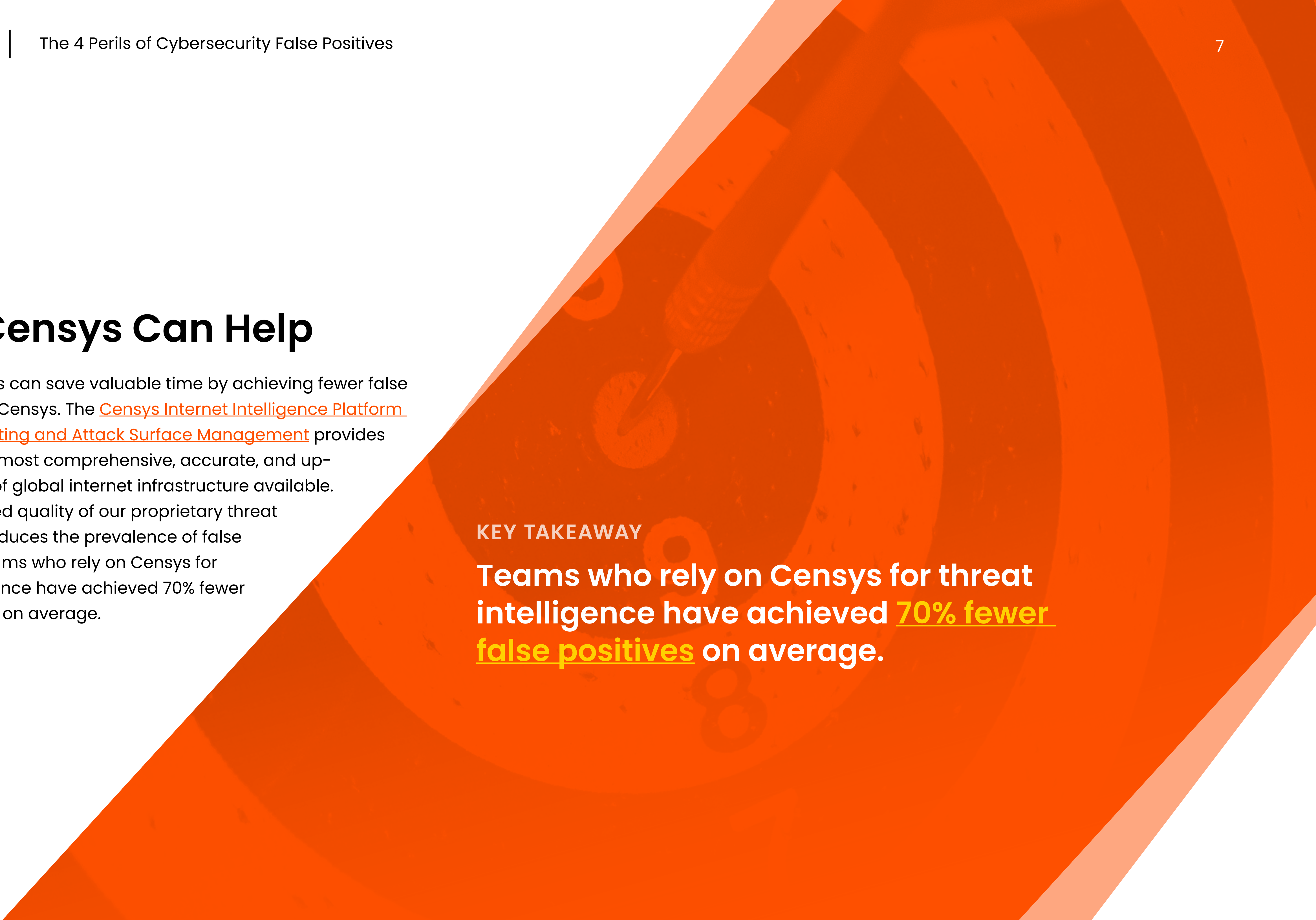
Wasted minutes become wasted hours, and even days, as the weeks go on. The Morning Consult reports that SOC analysts waste up to a third of their day on threats that pose no threat to the organization.

This lost time is even more concerning when considered in light of the total volume of threats that teams are up against. False positives not only inflate alert numbers, but make it even harder for analysts to get to the many real threats to the organization. Consider that fifty-nine percent of IT professionals say they receive more than 500 security alerts per day.

With this kind of threat volume, there’s no question that time is of the essence. Is your team spending it wisely?

How Censys Can Help

Security teams can save valuable time by achieving fewer false positives with Censys. The Censys Internet Intelligence Platform for Threat Hunting and Attack Surface Management provides access to the most comprehensive, accurate, and up-to-date view of global internet infrastructure available. The unmatched quality of our proprietary threat intelligence reduces the prevalence of false positives – teams who rely on Censys for threat intelligence have achieved 70% fewer false positives on average.



KEY TAKEAWAY

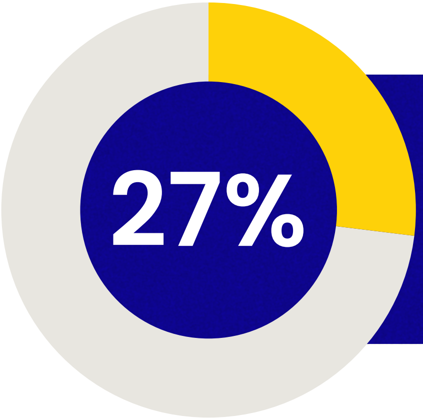
Teams who rely on Censys for threat intelligence have achieved 70% fewer false positives on average.

2

False Positive Peril #2

Alert Fatigue Leads to Burnout

False positives can also cause alert fatigue: a common side effect of noisy systems. After wasting so much time on false positives day in and day out, it's easy to see why some analysts may start to tune out the noise. Why spend time investigating every alert when so many aren't even real?



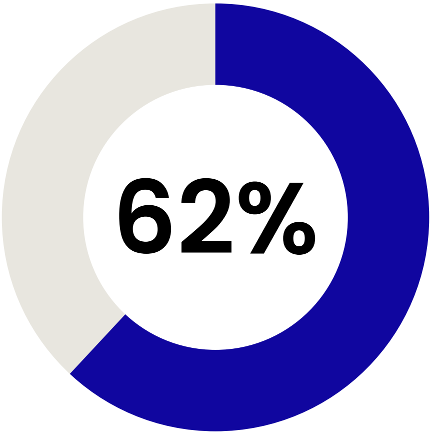
of all notifications are ignored or never investigated reported by IDC.

Security analysts with alert fatigue may start to:

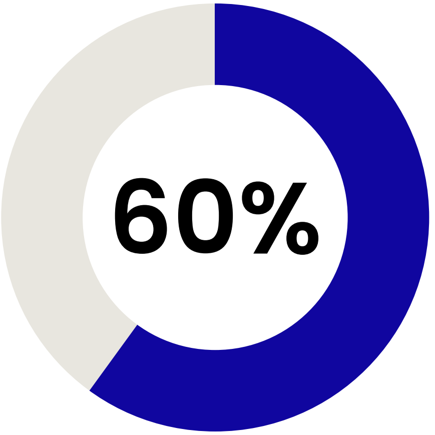
- Only pay attention to select, high-risk alerts
- Increase alert response time
- Scale back their investigative efforts
- Ignore alerts altogether

Teams Start to Feel the Burn(out)

Chronic alert fatigue can manifest into more systemic issues and affect the entire health of the team. A study from Orca Cloud Security found that:



of respondents say that alert fatigue has contributed to turnover



of respondents said that alert fatigue has created internal friction

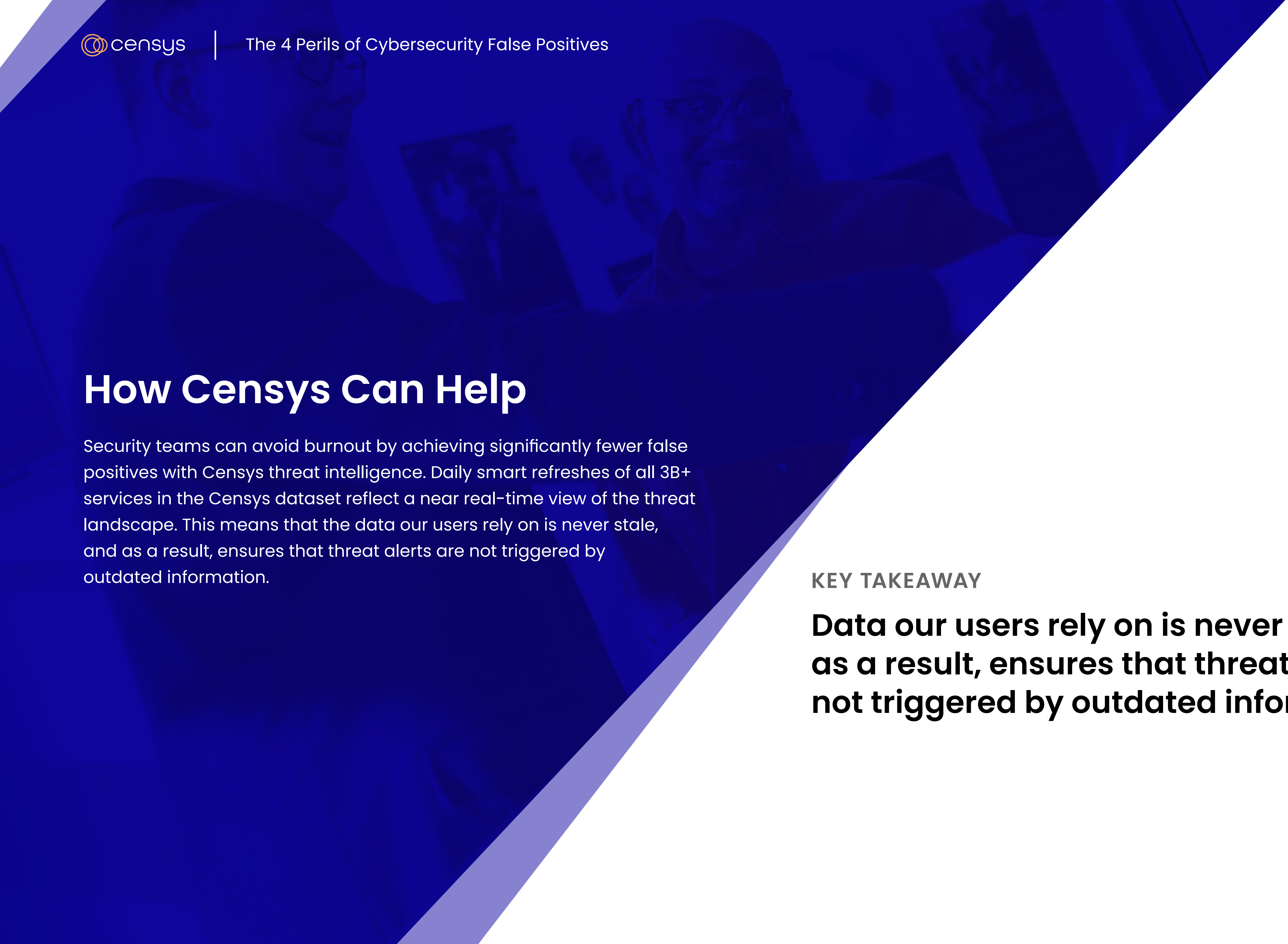
Another study from TrendMicro finds that the majority of respondents feel their team is overwhelmed by the volume of alerts they receive, and 55% say they're not confident in their ability to prioritize and respond to them.

This may be due in part to the fact that the task of monitoring and triaging alerts is often assigned to junior analysts who are still trying to learn the ropes and "not mess up." Navigating a barrage of alerts, without the experience or accurate tools to make sense of them, can become a hefty mental load.

Teams Are Already Stressed

False positives only add to what is an inherently stressful industry. Our 2023 State of Security Leadership Report found that 39% of security leaders were concerned about their own burnout, and 32% were concerned about the mental and physical well-being of their teams. Twenty-five percent of respondents in our 2024 State of Threat Hunting Report said that they were close to burnout.

In a function as critical as cybersecurity, organizations can't afford a revolving door of talent due to burnout. Are false positives worth your team's burn?



How Censys Can Help

Security teams can avoid burnout by achieving significantly fewer false positives with Censys threat intelligence. Daily smart refreshes of all 3B+ services in the Censys dataset reflect a near real-time view of the threat landscape. This means that the data our users rely on is never stale, and as a result, ensures that threat alerts are not triggered by outdated information.

KEY TAKEAWAY

Data our users rely on is never stale, and as a result, ensures that threat alerts are not triggered by outdated information.

3

False Positive Peril #3

You Risk Losing Credibility with Stakeholders

Sometimes you don't know you're dealing with a false positive until *after* you've sounded the alarm to stakeholders. This significantly increases a false positive's potential fallout and doesn't always cast your team in a flattering light.

The Communication Chain Reaction

Communicating about a threat at minimum will involve your incident response team, but as you know, it doesn't always stop there. When a threat poses a big enough risk, communications will also need to involve directors, VPs, and CISOs -and, depending on the nature of the threat, stakeholders outside of the security function. Think: public relations, legal, finance, operations, or the C-suite.

If a threat poses a potential risk to customers, or if it could have wide-reaching implications for the business as a whole, these other stakeholders will need to know.

Try as you might to catch false positives before sharing out with stakeholders, it isn't always easy, and false positives can still slip through. If the threat intelligence your alerting system is using is inaccurate or has gaps, you may not have the ability to determine that a threat is actually benign, and will go forward with sounding the alarm.

Cascading action from stakeholders will ensue: meetings, internal memos, external communications, operations changes, and more. Yet, when you inevitably discover the "threat" wasn't so threatening after all, you and your security team may be left sheepishly holding the bag, with perhaps a little bit less credibility to your name as a result.

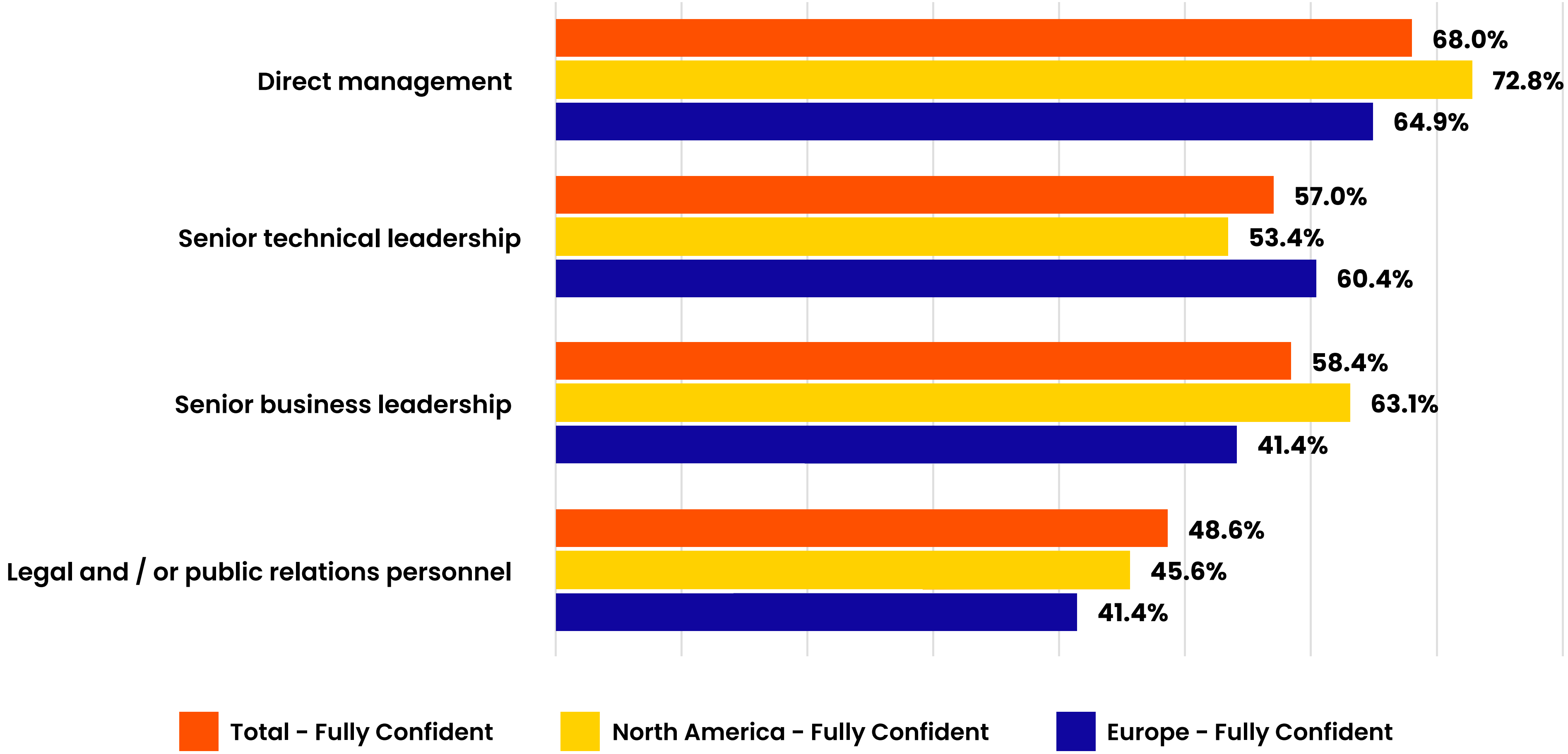
Less than half reported that they were confident communicating about threats with a potential negative impact to PR and legal, and only 68% were confident communicating with their direct management.

Communicating About Threats Is Already a Challenge

Admitting your team got it wrong isn't a great look, and it may explain why the threat hunters we surveyed in our 2024 State of Threat Hunting Report don't feel confident communicating with stakeholders.

How confident are you in your ability to communicate threat hunting results that may negatively impact your organization to these stakeholders?

False positives only add to these communications challenges, working against your confidence and undermining stakeholder trust in your team's abilities.



How Censys Can Help

Censys threat intelligence provides security teams with rich, detailed context about potential threats, including detailed visibility into open ports and running protocols, regardless of standard port assignment, to understand host intent. This context empowers teams to understand threats more deeply and communicate about them with more confidence.

KEY TAKEAWAY

Censys empowers teams to understand threats more deeply and communicate about them with more confidence.

4

False Positive Peril #4

You Miss a Critical Threat, and Pay the Price

We've arrived at the most damaging risk of all: missing a critical threat, and letting the organization fall victim to an attack.

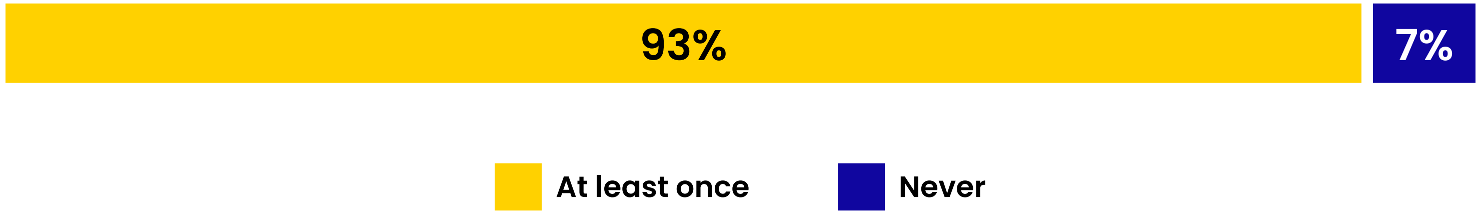
False positives make it more difficult for you to respond to threats that actually pose a critical risk to the organization. As you chase proverbial shadows and divert attention from genuine risks, adversaries have the time they need to strike.

Missing a critical threat isn't just a worst-case scenario. Critical threats *are* being missed. Fifty-five percent of respondents to Orca Security's report said that critical alerts are often missed on a daily or weekly basis.

This is particularly concerning given that we know the overall volume of cyber threats is growing thanks to increasingly sophisticated adversaries who are turning to AI to launch attacks at scale.

In our 2023 State of Security Leadership Report, 93% of surveyed security leaders said that their organization had experienced a successful cyber attack with a material impact within the last year. Fifty-two percent had experienced between two and five successful attacks within the last year.

In the past 12 months, how many times was your organization affected by a cyberattack that caused material damage?



The cost of a successful breach is rising, too. The average cost of a cyberattack in the U.S. is a whopping $9.8 million dollars, and has been steadily on the rise since 2023 according to reporting from Statista.

As security teams like yours face a higher volume of increasingly expensive threats that actually pose a risk to the organization, they simply can't afford to be burdened by those that don't.

How Censys Can Help

Censys discovers new services on the internet six times faster than the closest competitor. Our rapid time-to-discovery empowers security teams to stay a step ahead of adversaries and better defend their organizations from costly cyberattacks.

KEY TAKEAWAY

Our rapid time-to-discovery empowers security teams to stay a step ahead of adversaries and better defend their organizations from costly cyberattacks.

How to Cut the Noise

We've made it through the four key reasons false positives demand your attention! Hopefully now, more than ever before, you're convinced that false positives are worth taking action against. But what should that action look like?

There are a couple of supporting measures you and your team can pursue to achieve fewer false positives. However, as we'll get to shortly, there's one essential measure that addresses the root cause of false positives.

First steps to minimizing your risk of false positives can include:

ADJUSTING ALERT CONFIGURATIONS

An important first step is fine-tuning the alert configurations on your security monitoring tools. Alert triggers should be set to your organization's specific environment and should be adjusted as your analysts learn more about what kind activity tends to trigger false positives. A "set-it-and-forget-it" mindset will not do you any favors when it comes to alert configurations.

REFINING MATCHING ALGORITHMS

As part of your alert configurations, you may also want to revisit your organization's threshold for risk. It could be the case that the matching requirements you've set on your alerts (such as, "flag activity that is 50% similar to known threats") is too low, and in turn, counting too much benign activity as risks. Increasing your matching threshold can weed out more of these.

CHOOSING TOOLS THAT OPTIMIZE ALERTS

Your team could also consider switching detection and monitoring tools for those with alerting systems that are designed to reduce false positives and strategically manage alerts.

For example, you may want to upgrade to a tool that includes more context about threats in tickets, or uses AI to learn about the most common types of false positives your organization encounters.

However, even with proper alert configurations on more discerning systems, these tools still ultimately have to rely on the threat intelligence at hand.

Which is why to truly cut the noise, it ultimately comes down to the data.

Teams Need Superior Threat Intelligence

The only way that security teams can meaningfully achieve fewer false positives in the long run is to improve the accuracy of their threat intelligence.

Threat monitoring tools can only act on the information that's provided to them, and if information about the threat landscape is inherently inaccurate, false positives will prevail – and teams will lack the essential context needed to spot them.

Not All Data Is Created Equal

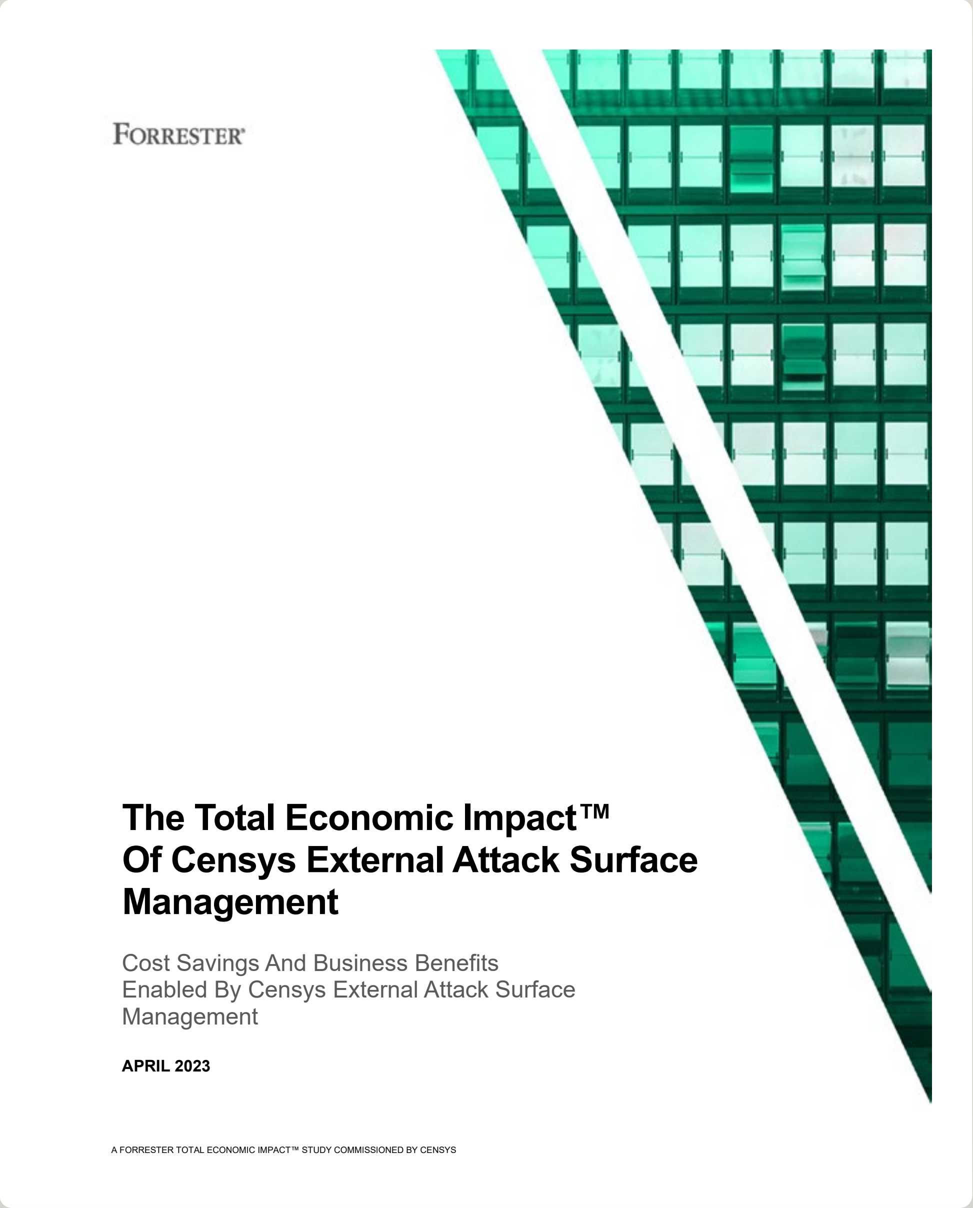
Though there are many different sources of threat intelligence, both open source and vendor-backed, the reality is that most offer an insufficient view of the global threat landscape. Many threat intelligence sources simply aren't scanning global internet infrastructure often enough to pick up on changes, or don't have the depth and breadth of coverage to provide threat monitoring tools with the context needed to determine whether suspicious activity is malicious or benign.

Achieve Fewer False Positives with Censys

Teams plagued with false positives can rely on Censys for the superior threat intelligence they need to cut the noise.

Unlike other threat intelligence sources, Censys' proprietary internet scanning engine provides the most comprehensive, accurate, and up-to-date view of global internet infrastructure available. No other provider offers the depth and breadth of threat intelligence that Censys does. As a result, teams can benefit from dramatically fewer false positives.

> "Censys's data accuracy reduces the number of false positives that the composite organization receives by 70%."
>
> TEI of Censys EASM, 2023



FORRESTER

The Total Economic Impact™ Of Censys External Attack Surface Management

Cost Savings And Business Benefits Enabled By Censys External Attack Surface Management

APRIL 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY CENSYS

What to Look for In Threat Intelligence

Cybersecurity teams need threat intelligence that is:

01 Up-to-Date

What was a potential threat yesterday could be long gone today. Data that's only refreshed on a weekly, monthly, or intermittent interval can leave teams searching in the dark and acting on incorrect information. Teams need threat intelligence that is updated on a daily basis to ensure that alerts are only triggered by real-time threats.

How Censys Solves

Censys provides the most comprehensive and up-to-date visibility of hosts and services on the global internet. This ensures that teams are only alerted to credible, real-time threats.

CENSYS PROVIDES

Daily comprehensive scans of the top 100+ ports and proprietary ML-based discovery of services across all 65k ports (**Censys is the only vendor to do this**)

Daily smart refreshes of all 3B+ services in the Censys dataset give our users confidence that information about potential threats is accurate and up-to-date.

Discovery of new services on the internet six times faster than the closest competitor.

02 Comprehensive

Threat intelligence is accurate when it reflects a complete view of the global threat landscape. Comprehensive scanning coverage across all hosts and services on the public-facing internet ensures that no threats are missed, and that teams can gain a complete understanding of their attack surface to determine what activity is, or is not, typical.

Research found that on average, Censys discovered over 80% of common services within the first 24 hours of new services going online, while our closest competitor found only 12%.

How Censys Solves

Censys offers unparalleled depth and breadth of internet scanning coverage. Censys scans the entire public-facing internet to provide the most comprehensive view of global internet infrastructure. This extensive coverage ensures that security teams have a more complete understanding of their threat landscape.

CENSYS PROVIDES

Multi-perspective scanning from 7 Tier-1 ISPs across 3 continents

~100 Deep Protocol Scanners and Automatic Protocol Detection to identify services running on unassigned ports

Cloud scanning to capture ephemeral cloud services

The **world's largest x.509 certificate database** to identify related infrastructure and suspicious hosts

03 Contextualized

As they say, context is key. The more threat monitoring tools understand about a potential threat - origin, time online, related certificates, historical – the more accurate their alerts can be. Threat context also gives analysts the ability to more swiftly validate that a threat is in fact a risk to the organization, and allows for more accurate incident response and stakeholder reporting.

How Censys Solves

Censys threat intelligence is enriched with detailed context to identify host types and understand how assets are connected and configured. This allows teams to quickly investigate and validate threats.

CENSYS PROVIDES

Detailed visibility into open ports and running protocols, regardless of standard port assignment, to understand host intent (**Censys is the only vendor to do this**)

Geolocation data to understand where a host resides

Configuration and registration data to understand and determine ownership

Software detection to identify potential, threats, risks, and vulnerabilities

Device type labels to clearly identify host type (i.e. IoT, Database, VPN, etc.)

Getting Started with Censys

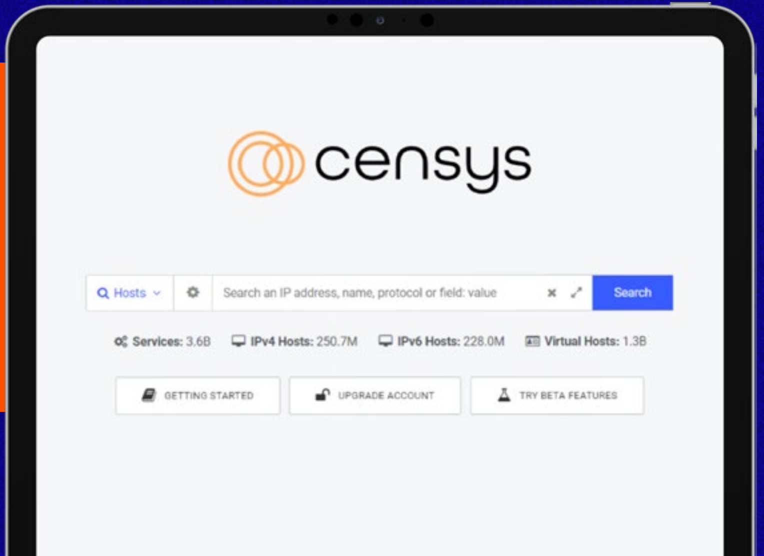
Ready to upgrade your threat intelligence? Tap into the power of our industry-leading threat intelligence and achieve fewer false positives with the Censys Internet Intelligence Platform for Threat Hunting and Attack Surface Management!

Visit us at censys.com

Learn more about how you can put Censys to work for your team!

Interested in an up-close look at our data?

Head on over to search.censys.io to explore our expansive dataset.



Services: 3.6B IPv4 Hosts: 250.7M IPv6 Hosts: 228.0M Virtual Hosts: 1.3B

Who We Are

Censys is the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management, known for discovering assets six times faster than its closest competitor. Censys offers the most comprehensive, accurate, and up-to-date map of the internet available with daily refreshes of billions of services and the world's largest certificate database empowering our customers to proactively discover, prioritize and remediate threats. Established by the creators of ZMap and trusted by the U.S. Government, along with over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the internet.