IDC | ANALYZE THE FUTURE

The Voice of the Analysts

Improving Security Operations Center Processes Through Advanced Technologies

RESEARCH BY:

Christina Richmond
Program Vice President,
Security Services, IDC

Craig Robinson
Program Director,
Security Services, IDC

Martha Vazquez
Senior Research Analyst,
Security Services, IDC

January 2021 | IDC Doc. #US47227621

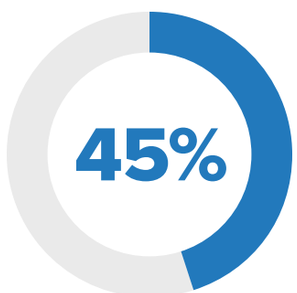
Navigating this InfoBrief

Click on titles or page numbers to navigate to each section.

The Stakes Are High

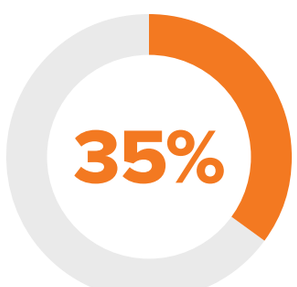
Security risk leaders, security analysts, and their service provider partners are under enormous pressure to keep their organizations secure from expanding security attacks. This is a challenge — and as more and more data is collected, the number of alerts increases exponentially.*

Analysts look at thousands of alerts every day.



of alerts end up being false positives, making the analyst's job less efficient and slowing workflow processes.

What's worse,



of respondents ignore alerts when the queue gets too full!

Managed security service provider analysts who miss just one alert could end up with a breach that impacts multiple clients.

- Analysts need to work smarter and faster than ever before.
- Human-only alert intervention is inefficient.
- Automation is needed to make sure that alerts get the proper analysis and response they deserve.
- New approaches are needed to keep up with the changing security landscape.

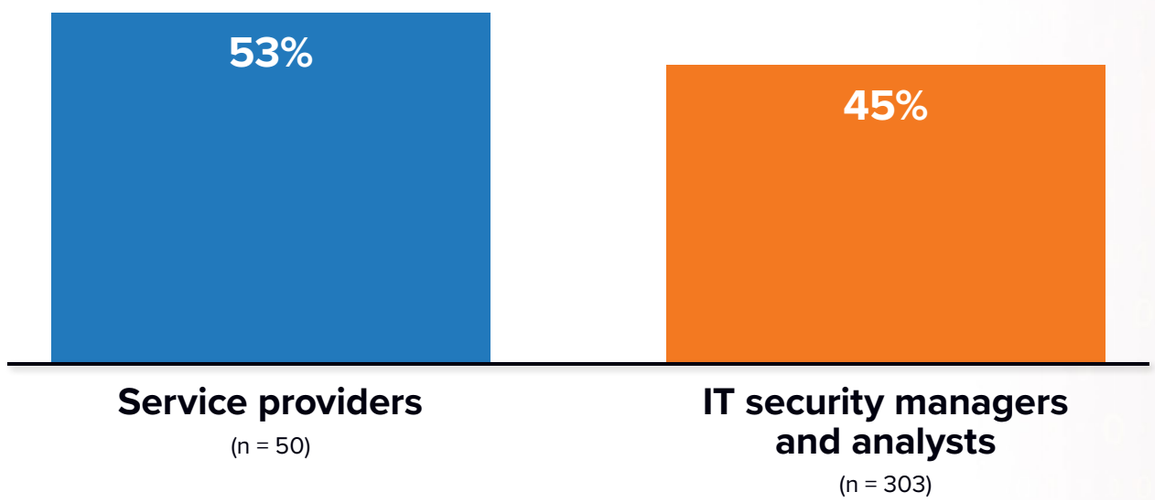
*IDC surveyed 300 experienced IT security managers and security analysts in the U.S. working in security operations centers (SOCs) in multiple verticals, such as financial, healthcare, and government. We also surveyed 50 managed security service providers to understand their current daily challenges in the SOC.

Source: Security Analyst Alert Fatigue Survey, IDC, October 2020. Base = All Respondents, Mean, Service Provider, and Non-Service Provider respondents.

Alert Overload in the Security Operations Center

Security Analysts in the Enterprise

Q. What percentage of alerts that you personally receive turn out to be **false positives**? An alert is a notification that a particular event (or series of events) has occurred, which is alerts are sent to responsible parties for the purpose of spawning action.



At least 45% of alerts are false positive. Valuable time is spent inefficiently sifting through them, creating dreaded "alert fatigue." Or worse, analysts ignore alerts!

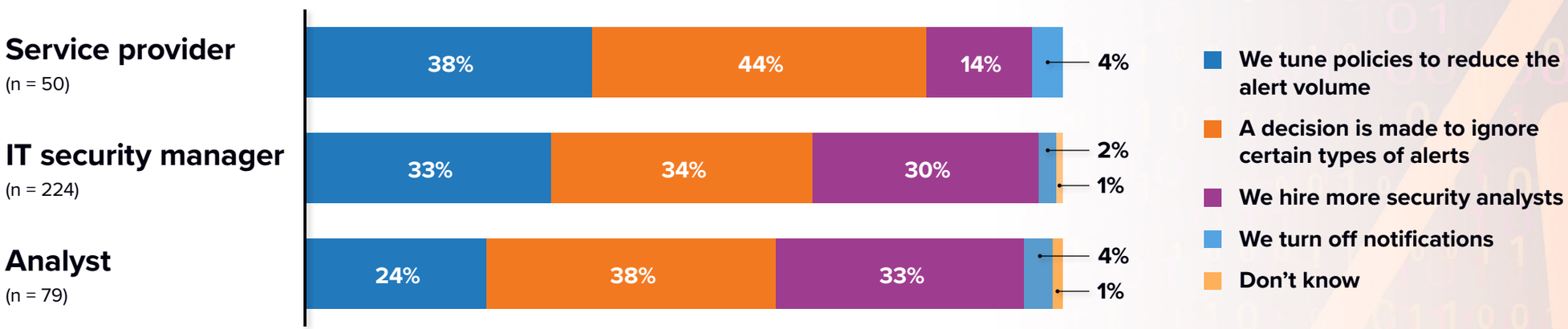
Impact of False Positives

Analysts Within Service Providers

Organizations look to service providers for:

- tier 2 monitoring
- threat hunting
- threat intelligence services
- deployment and cyber hygiene

Q. What typically happens when your SOC team has too many alerts to process?



A wider scope of visibility by analysts in service provider environments sees 53% false positives, a higher number than for those working in specific industries. When their queue is too full, 44% will ignore alerts!

Fear of Missing Incidents (FOMI) Is Real

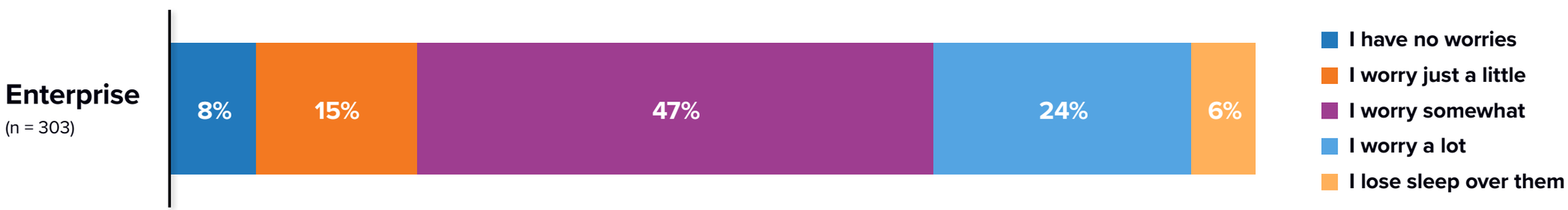
Just how big is FOMI among analysts and managers?

3 in 4 analysts are **worried** about missing incidents

1 in 2 analysts **worry "somewhat"** about missing incidents

an additional **1 in 4** analysts **worry "a lot."**

Q. Which of the following best reflects your level of worry regarding missing incidents? An incident is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business.

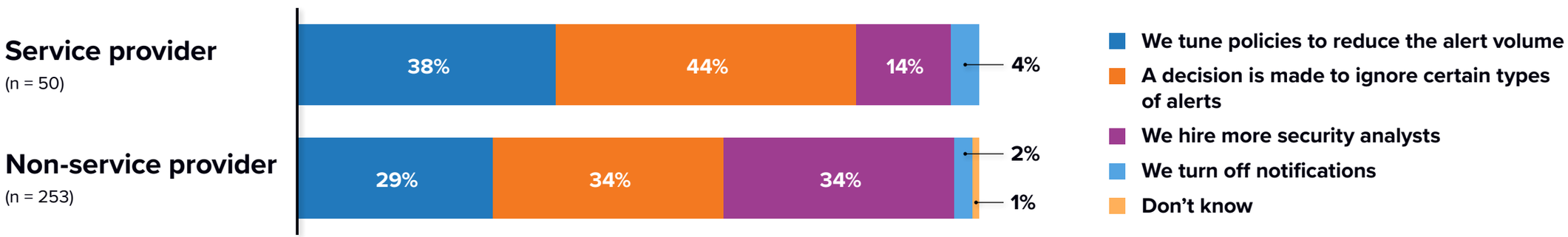


6% of security managers are losing sleep.

Managed Security Service Providers Also Suffer from Fear of Missing Incidents (FOMI)

However, they handle alert overload differently from enterprise organizations.

Q. What typically happens when your analyst team has too many alerts to process?



Managed security service providers are put at greater risk by choosing to ignore certain type of alerts.

As service providers, they handle more alerts and attempt to reduce the volume by ignoring certain types of alerts and rewriting policies...

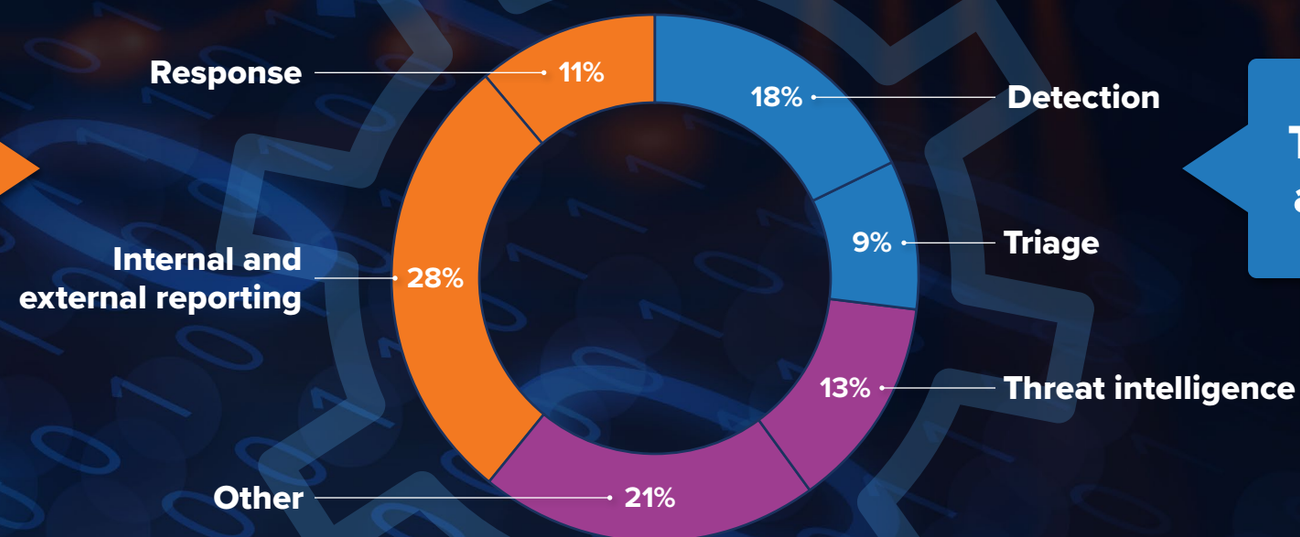
but

they do not hire more analysts to handle the volume.

Specific Areas to Automate to Fight Fear of Missing Incidents (FOMI)

Q. In your opinion, please rank the top five activities you feel would be best to automate.
(Percentage of respondents ranking these first)

Chief areas of automation for service providers



Top of mind for analysts

How to Combat Fear of Missing Incidents (FOMI)

Automation of security processes can help alleviate the challenges faced by security operations teams.

Investments in advanced technologies

—specifically automation capabilities—are believed to reduce time-consuming tasks such as reporting, threat detection, and response.

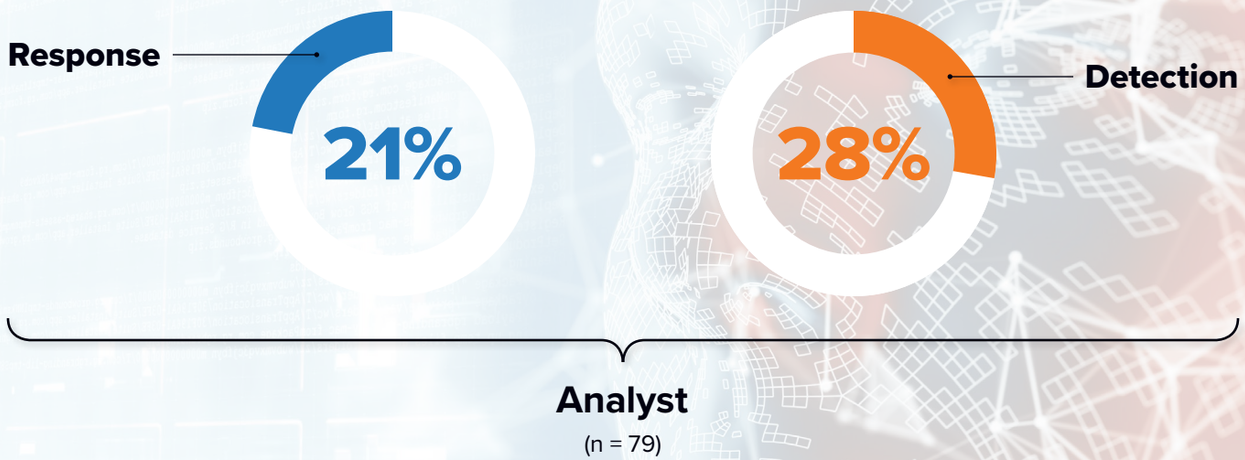
To keep up with the ever-expanding attack surface and increase in alerts, organizations see benefit from automation and the creation of

consistent and repeatable processes to

- Improve security analyst efficiency by allowing them to focus on higher-level tasks such as threat hunting and cyber investigations
- Reduce alert fatigue by removing the need for constant console monitoring
- Strengthen security posture

Machine Learning and Artificial Intelligence Improve Service Workflow Beyond Automation

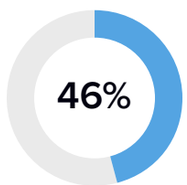
Q. In your opinion, please rank the top five activities you feel would be best to automate.
(Percentage of respondents ranking these first)



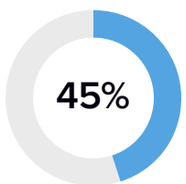
Adding advanced technologies like extended detection and response (XDR), machine learning (ML), and artificial intelligence (AI) provides needed context to power investigations while simultaneously reducing FOMI.

Top Choices Among Analysts to Investigate Alerts

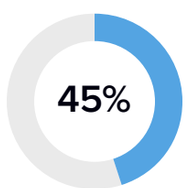
Q. What tools does your analyst team use to investigate alerts?
(Percentage of respondents selecting)



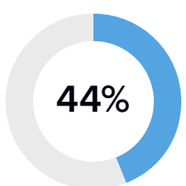
Security orchestration automation and response (SOAR) tools



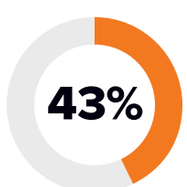
Threat hunting



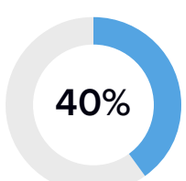
Security information and event management (SIEM) software



Threat intelligence platforms



Machine learning and artificial intelligence



Scripting (Python, Powershell, etc.)

2 in 5 analysts

are using ML and AI technologies alongside Security Orchestration Automation and Response (SOAR) tools, Security Information and Event Management (SIEM) software, threat hunting, and other security functions.

Top Services Outsourced to Managed Security Service Providers

Q. What services does your managed service provider (either MSP or MSSP) offer?
(Percentage of respondents selecting, top three mentions in bold)

	Analyst (n = 58)	IT Security Manager (n = 161)	Total (n = 219)
Tier 2 monitoring	**48%**	**42%**	**44%**
Threat hunting	33%	**46%**	**42%**
Security technology deployment and hygiene	**34%**	**45%**	**42%**
Threat intelligence	33%	**45%**	**42%**
Tier 1 monitoring	**36%***	40%	39%
High-level analysis	33%	34%	34%
Incident Response	24%	31%	29%
Managed Detection and Response (MDR)	12%	22%	20%

*Only large organizations and analysts (versus IT security managers) add tier 1 monitoring to their list of desired services from an MSSP.

Note: Managed by IDC's Quantitative Research Group. Data not weighted. Use caution when interpreting small sample sizes.

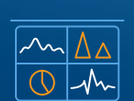
IDC Recommendations

Leverage advanced technology capabilities such as automation to create happier and more successful analysts.

Reduce and automate functions that are not aligned to analysts' core mission.

Enable analysts to do what they do best—hunt, detect, and eliminate the bad guys.

Create more productivity, reduce stress, and help analysts feel more energized about their jobs.



Use automation in the right place to handle the high volume of data to help analysts devote more effort to higher-value activities.

About the Analysts

Christina Richmond
Program Vice President,
Security Services, IDC

Christina Richmond is the Program Vice President for IDC's Security Services research practice. She is responsible for the day-to-day management of the program. Core research coverage for the team includes, but is not limited to, security consulting, integration, and managed services. In addition, the team looks at services that help organizations adopt emerging technologies like Cloud, Edge, and IoT as well as key focus areas such as Risk, Data Privacy, and Compliance. Christina brings a wealth of security services expertise and knowledge to the position and is frequently sought after by IT security executives to share her research and insights on dynamics and trends in the security industry.

More about Christina Richmond

Craig Robinson
Program Director,
Security Services, IDC

Craig Robinson is a Program Director within IDC's Security Services research practice, focusing on managed services, consulting, and integration. Coverage areas include IoT Security, Blockchain Services, Threat Detection, and Response services. Craig delivers unparalleled insight and analysis, leveraging his unique experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research, and guidance to vendors, service providers, and clients worldwide.

More about Craig Robinson

Martha Vazquez
Senior Research Analyst,
Security Services, IDC

Martha Gomez Vazquez is a Senior Research Analyst for IDC's Security Services research practice. In this role, she is responsible for IDC's worldwide research and analysis on enterprise and service provider security consulting, integration, and managed services as well as hardware and software support and deployment needs. She provides insightful market analysis and research to vendors, service providers, and end-user clients worldwide. Martha brings a breadth of knowledge and expert advice to assist vendors in developing marketing strategies, research, strategic alliances, and partners in this market.

More about Martha Vazquez

Message from the Sponsor

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation state grade threat intelligence, and world-renowned Mandiant consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

IDC | ANALYZE THE FUTURE idc.com @idc

IDC. Doc. #US47227621