Threat Intelligence Research

Sponsored by Nisos - The Managed Intelligence Company™

Research Results August 2022

Threat intelligence is critical for organizations, but many are **struggling to harness** the full power of their **threat intelligence** sources, **leaving them overwhelmed**

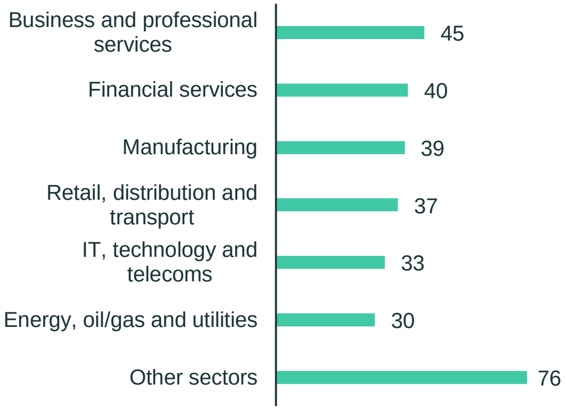
By **entrusting** threat intelligence to a **third-party provider**, organizations can move their threat intelligence **from reactive to proactive**

VansonBourne

Sponsored by
NISOS

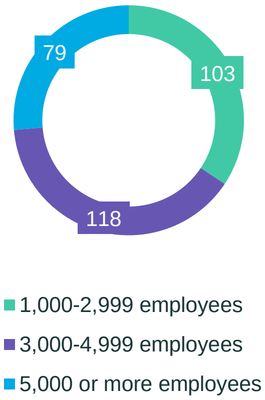
300 senior security decision makers were interviewed in July 2022, split in the following ways…

…by organization sector



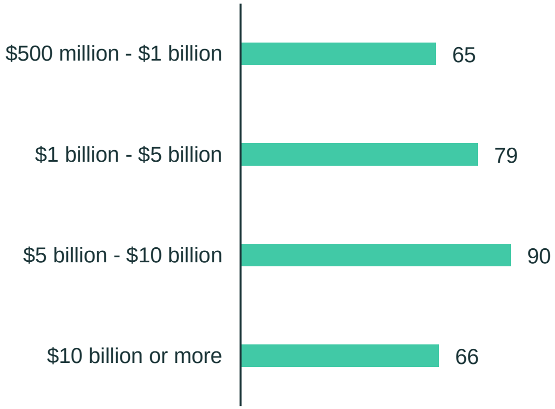
Within which sector is your organization? [300]

…by organization size



How many employees does your organization have globally? [300]

…by organization revenue



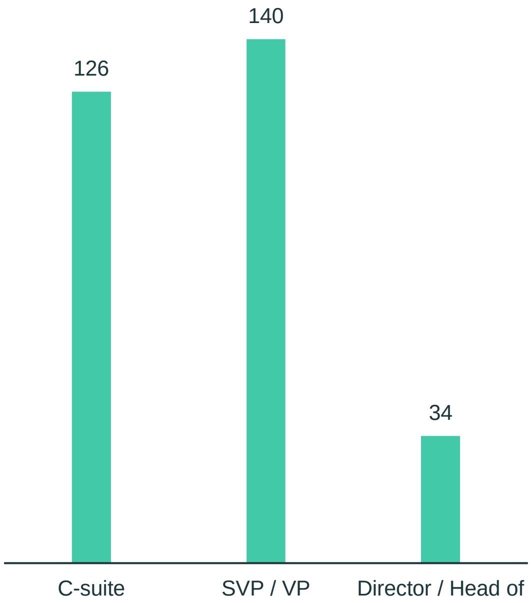
What is your organization’s global annual revenue? [300]

VansonBourne

Sponsored by NISOS

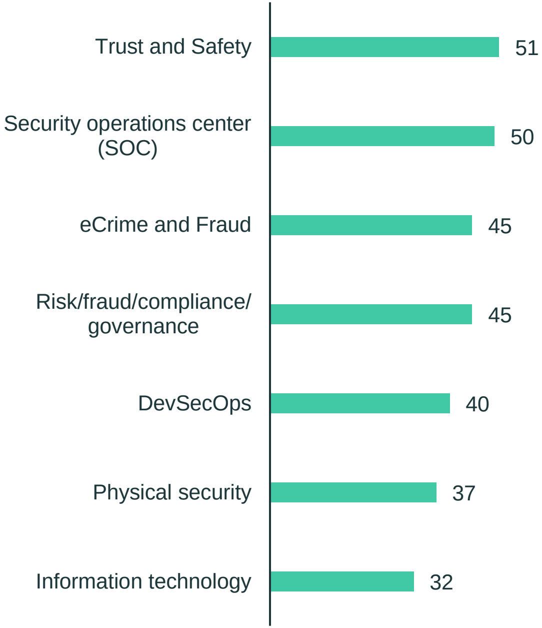
300 senior security decision makers were interviewed in July 2022, split in the following ways…

…by respondent seniority



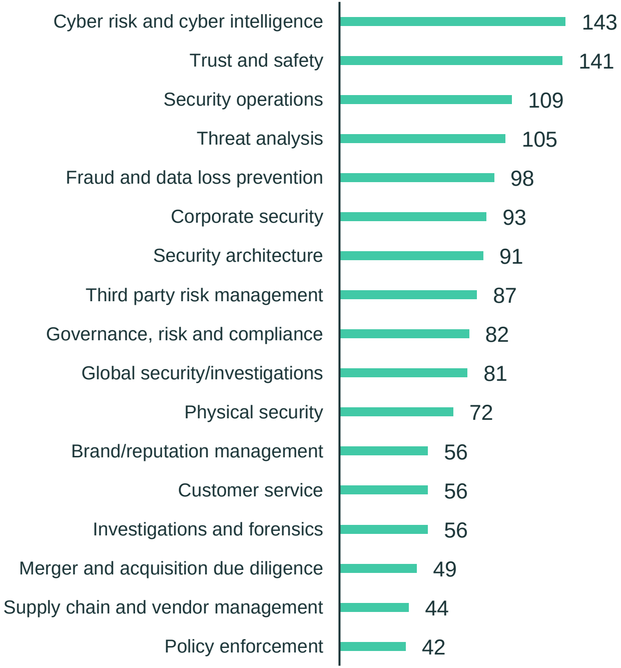
Which of the following most closely aligns with your job title? [300]

…by respondent department



In which one of these functional areas are you primarily employed within your organization? [300]

…by respondent responsibility



Which of the following responsibilities fall under your remit? [300]

3 areas of interest:

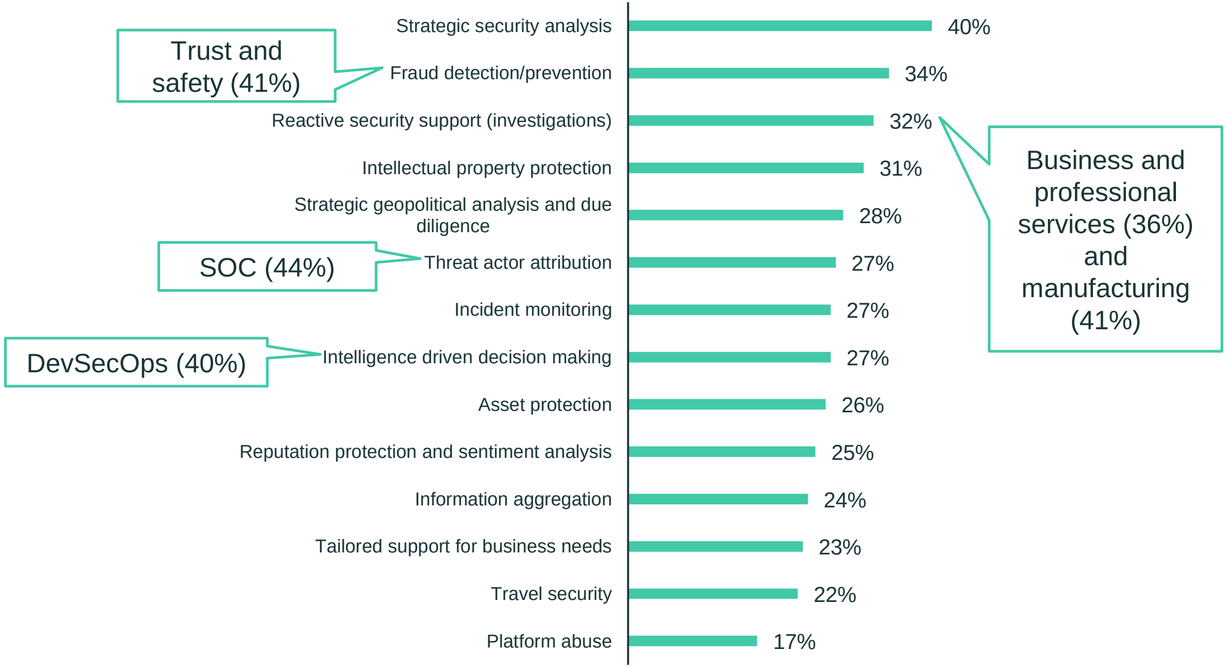
1. Threat intelligence overwhelm
2. Third-party threat intelligence services: a shining light
3. Transitioning threat intelligence from reactive to proactive

1. Threat intelligence overwhelm

Threat intelligence is an important component for organizations’ security protocols, and it’s something that all surveyed organizations are currently using

100%

Of respondents report that their organization is currently utilizing threat intelligence



Trust and safety (41%)

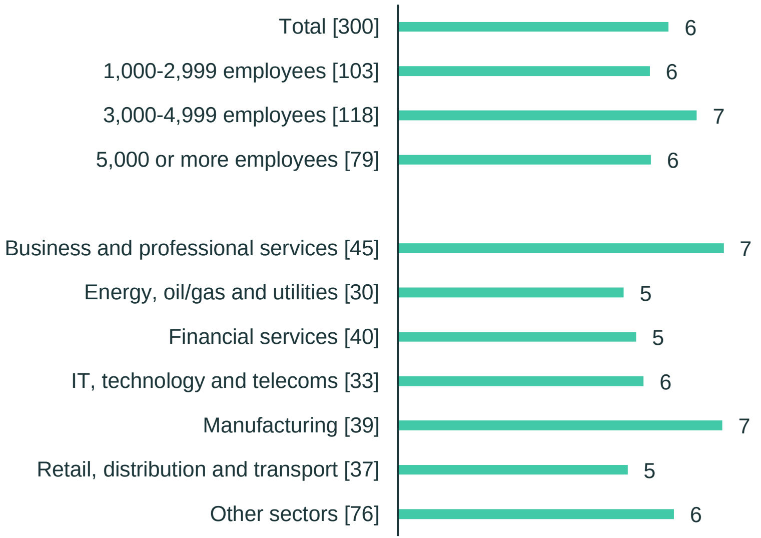
SOC (44%)

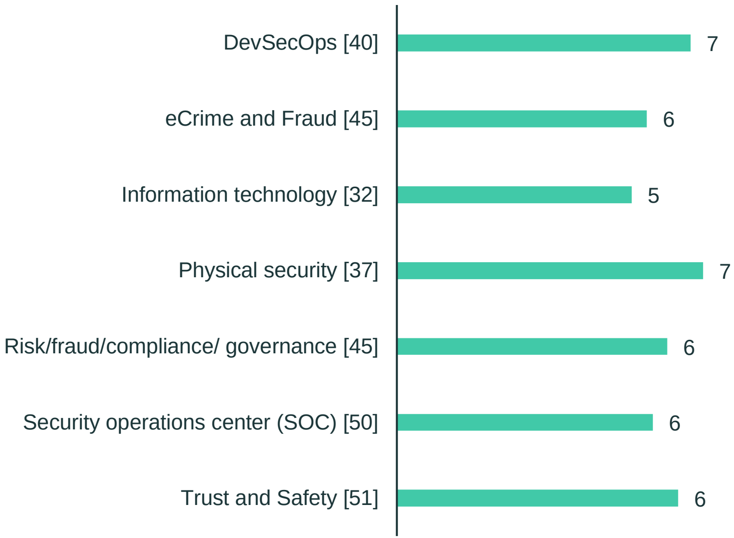
DevSecOps (40%)

Business and professional services (36%) and manufacturing (41%)

What is your organization currently using threat intelligence for? [300] omitting some answer options, call outs highlighting most likely answer for each department and sector if it wasn’t “strategic security analysis” or had the same respondent count as “strategic security analysis”

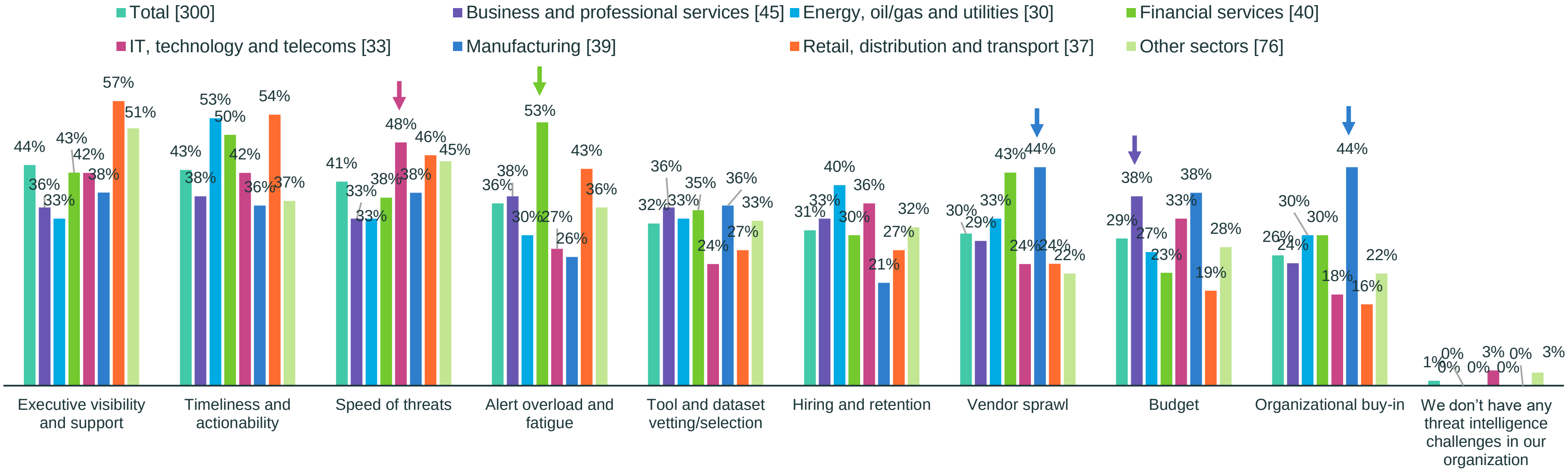
On average, organizations are using between 5 and 7 different threat intelligence sources





Average number of threat intelligence sources respondents' organizations currently use. [Base sizes in chart] split by organization size, sector and respondent department

Many organizations are facing challenges in this area, with these varying between different sectors

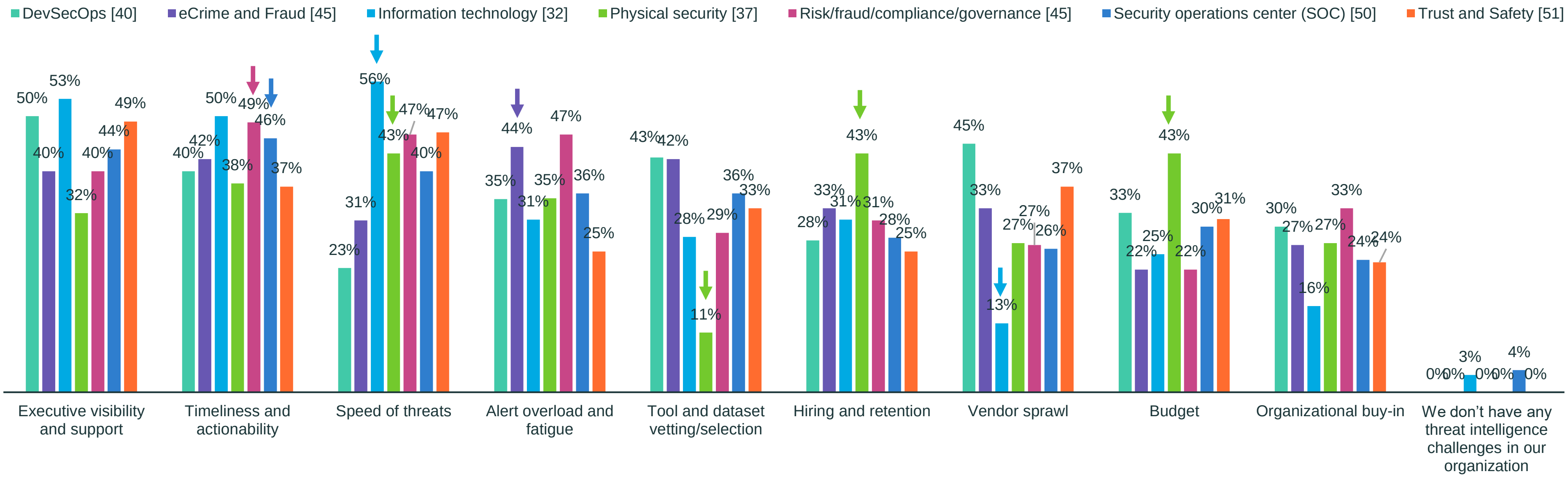


Does your organization face any of the following threat intelligence challenges? [Base sizes in chart] split by organization sector, omitting some answer options

VansonBourne

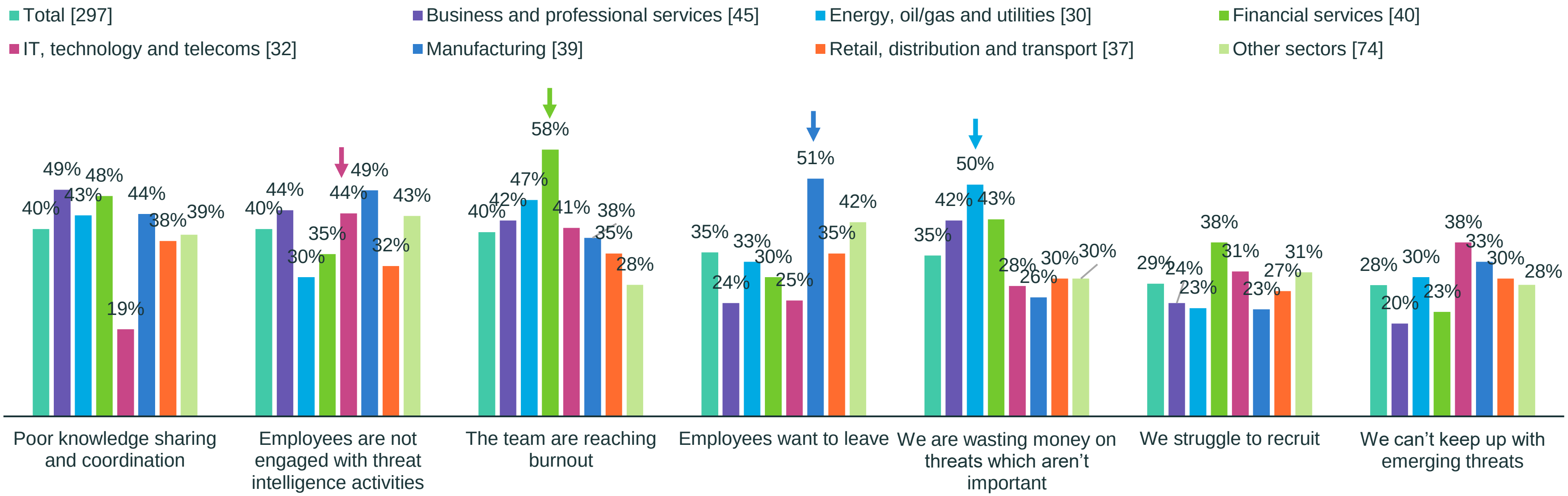
Sponsored by NISOS

Challenges also remain widespread across the different respondent departments



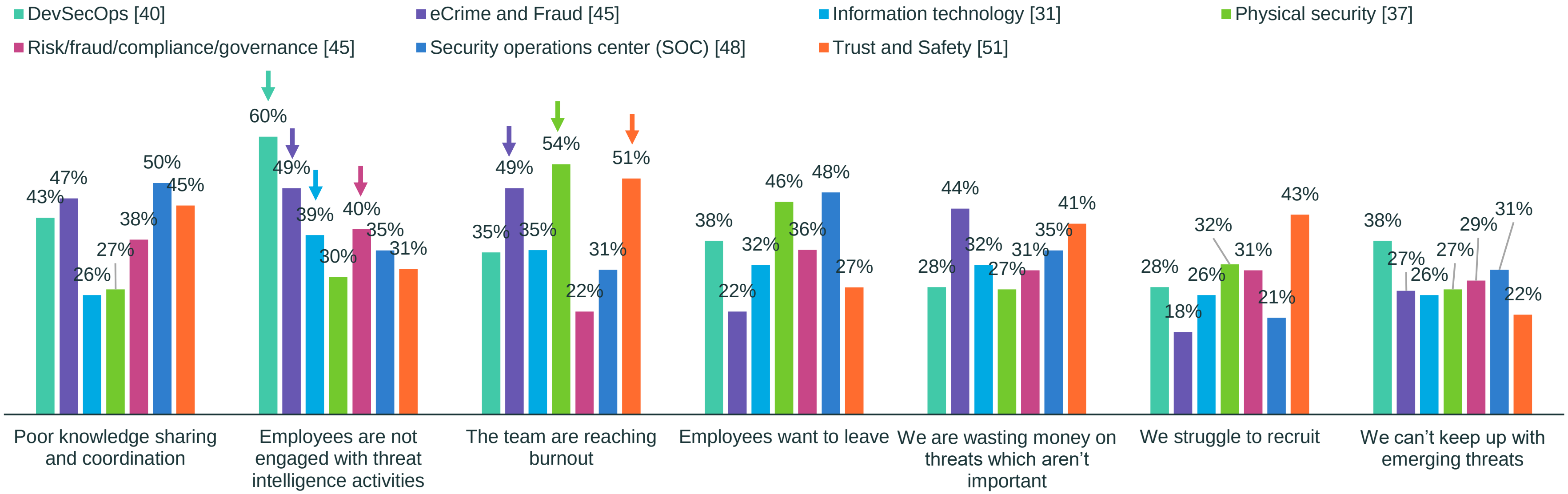
Does your organization face any of the following threat intelligence challenges? [Base sizes in chart] split by respondent department, omitting some answer options

Threat intelligence challenges cause untold problems for organizations



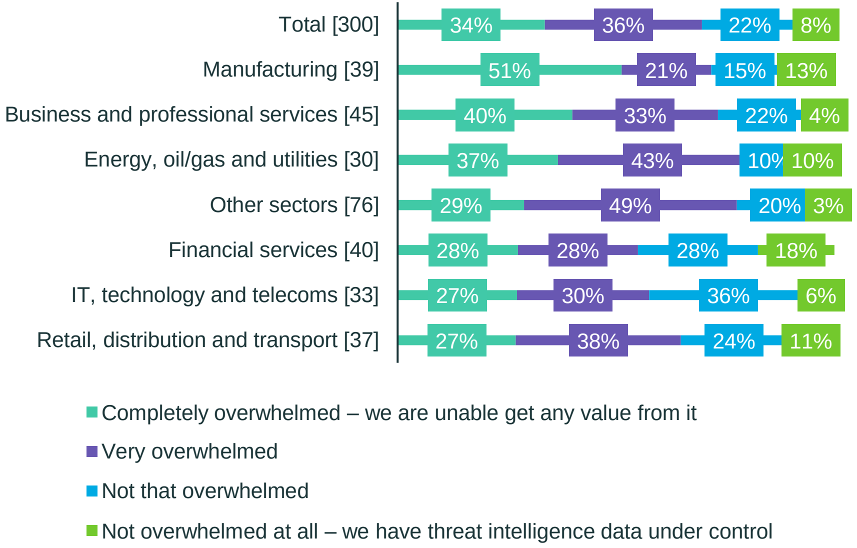
What problems do these threat intelligence challenges cause for your organization? Respondents who experience threat intelligence challenges [base sizes in chart] split by organization sector, omitting some answer options

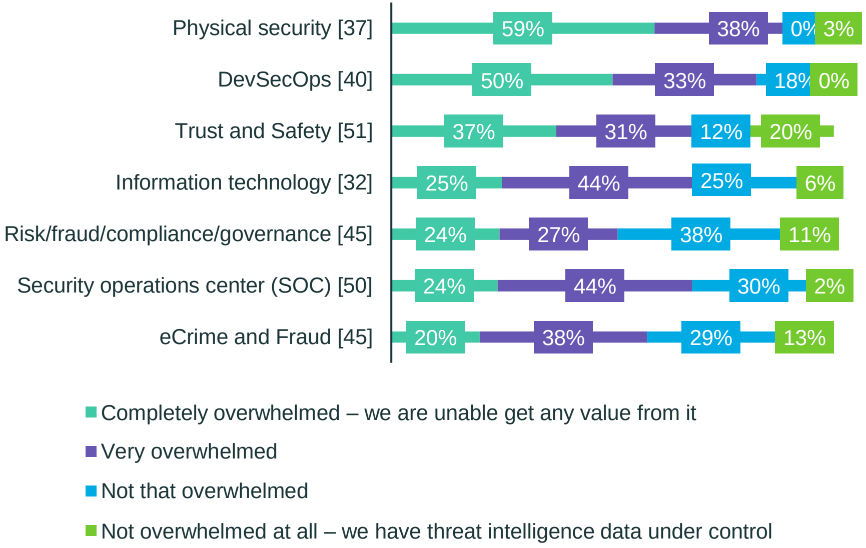
For three out of the seven departments interviewed, burnout is a real problem



What problems do these threat intelligence challenges cause for your organization? Respondents who experience threat intelligence challenges [base sizes in chart] split by respondents' department, omitting some answer options

Given the number of challenges and problems facing organizations, it’s no wonder they are feeling overwhelmed…

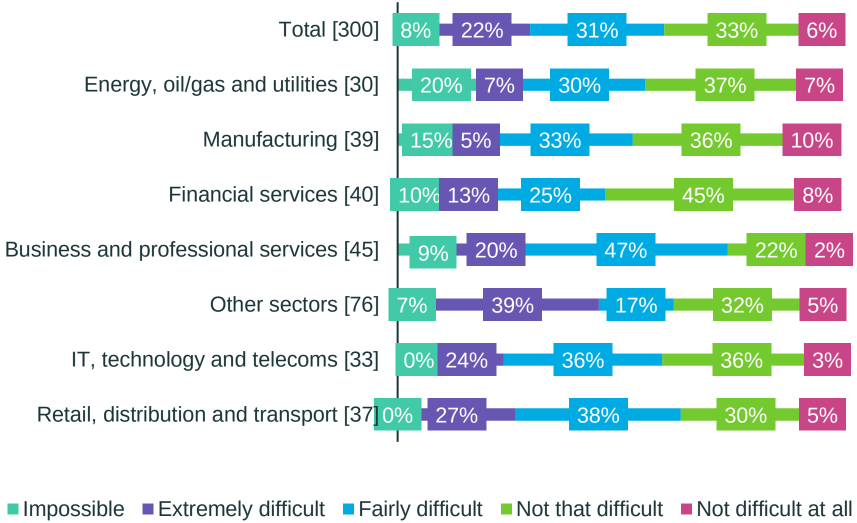


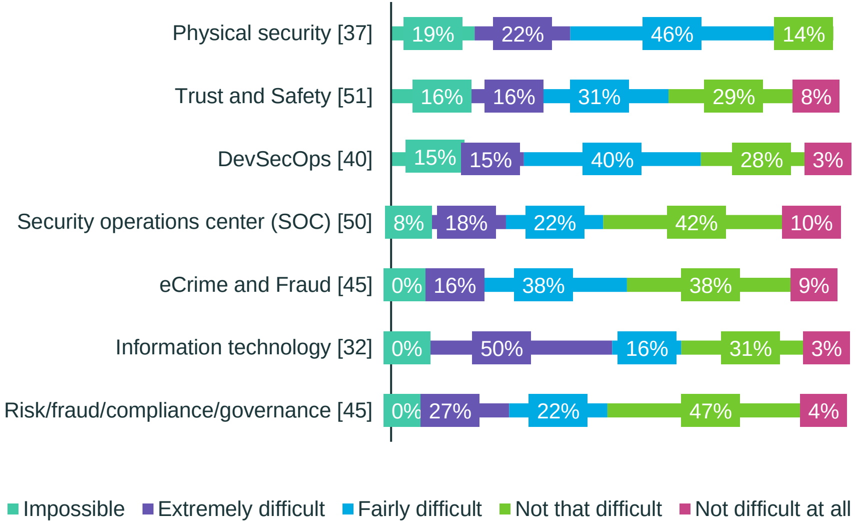


To what extent do you feel overwhelmed by the amount of the threat intelligence data available to you in your organization?]Base sizes in chart] split by organization sector and respondent department, omitting some answer options

Sponsored by NISOS

…with many finding it difficult to conclude actionable insight from their threat intelligence sources





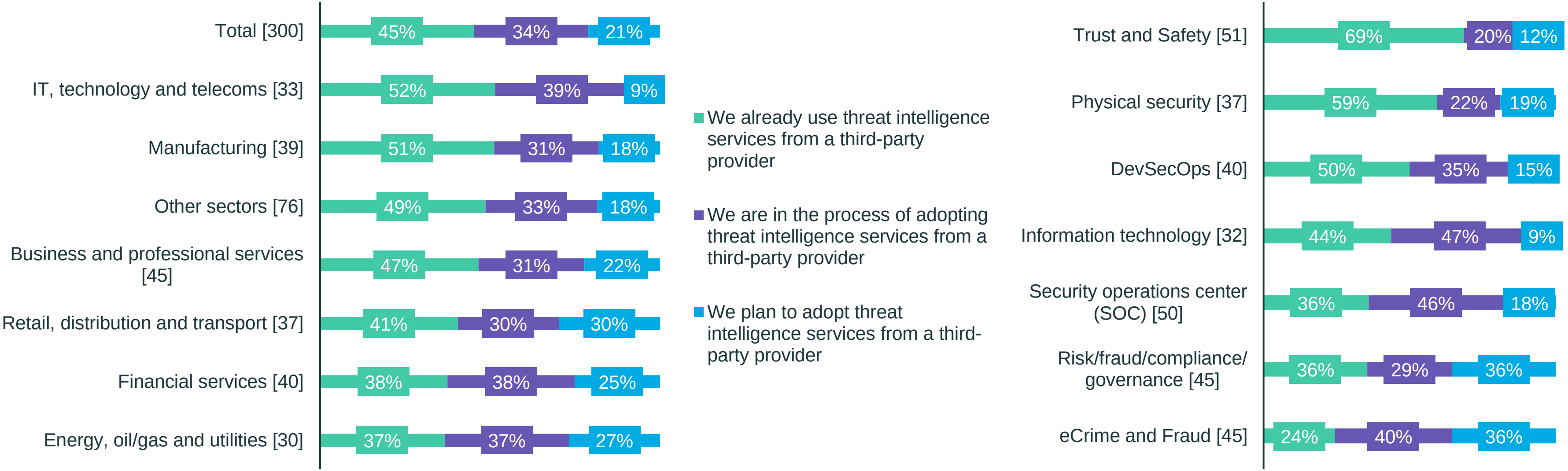
How difficult does your organization find concluding actionable insight from your threat intelligence sources?]Base sizes in chart] split by organization sector and respondent department, omitting some answer options

2. Third-party intelligence services: a shining light

VansonBourne

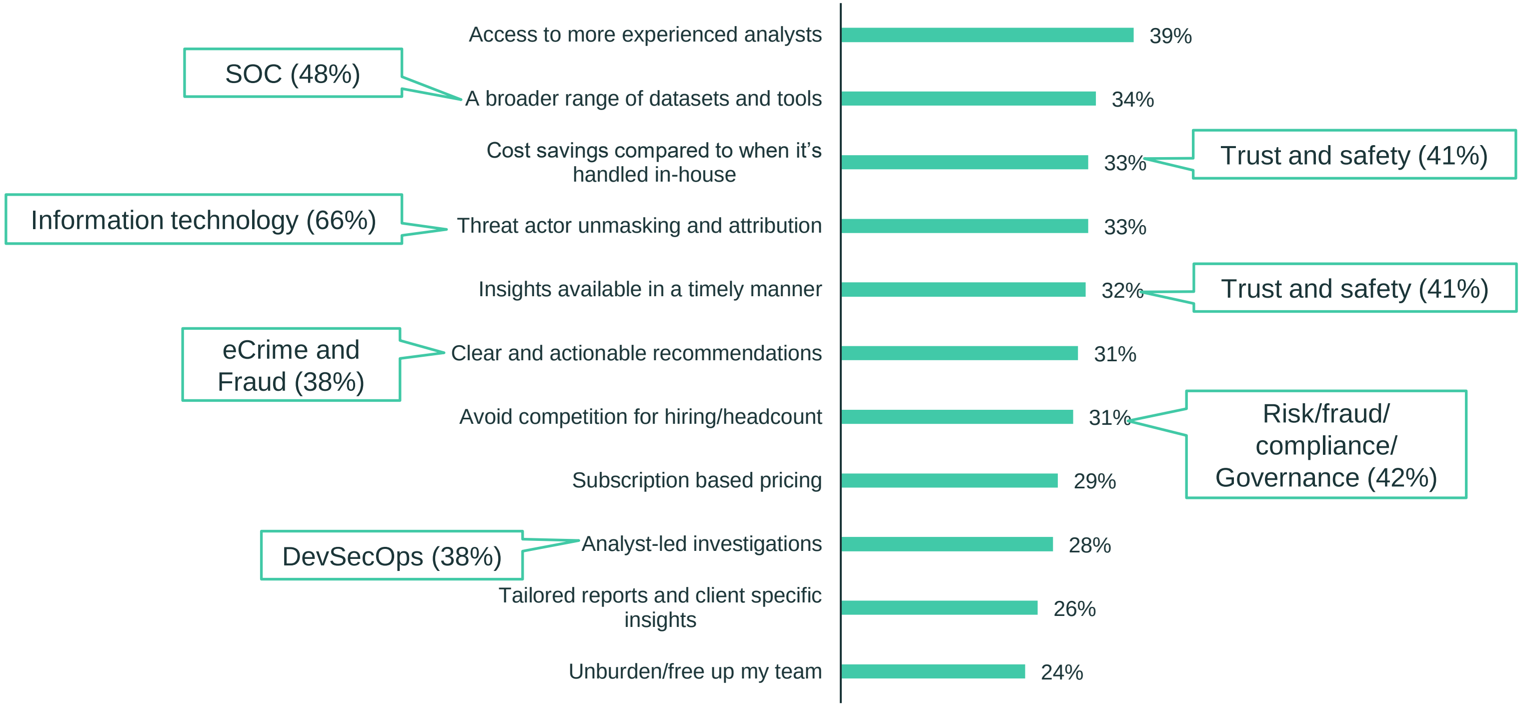
Sponsored by NISOS

All surveyed organizations are either using, adopting or have plans to adopt threat intelligence services from a managed services provider



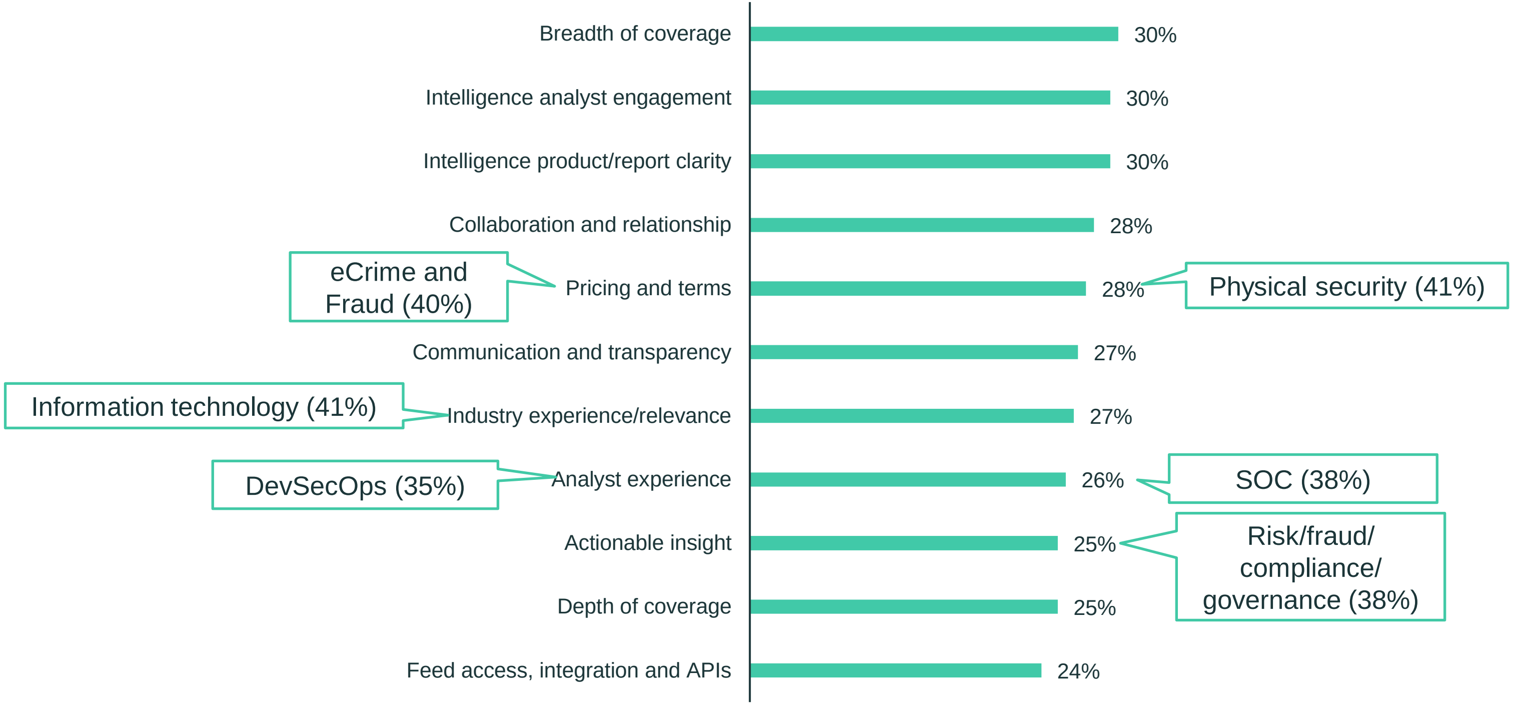
Does your organization currently use or plan to use threat intelligence services from a managed services provider? [Base sizes in chart] split by organization sector and respondent department, omitting some answer options

The expected benefits from a managed threat intelligence provider are vast…



What benefits would your organization expect to gain with a managed threat intelligence provider? [300] omitting some answer options, call outs highlighting each departments' most likely answer if it wasn't "access to more experienced analysts" or if another option had the same respondent count as "access to more experienced analysts"

…and align with what's important to organizations



eCrime and Fraud (40%)

Physical security (41%)

Information technology (41%)

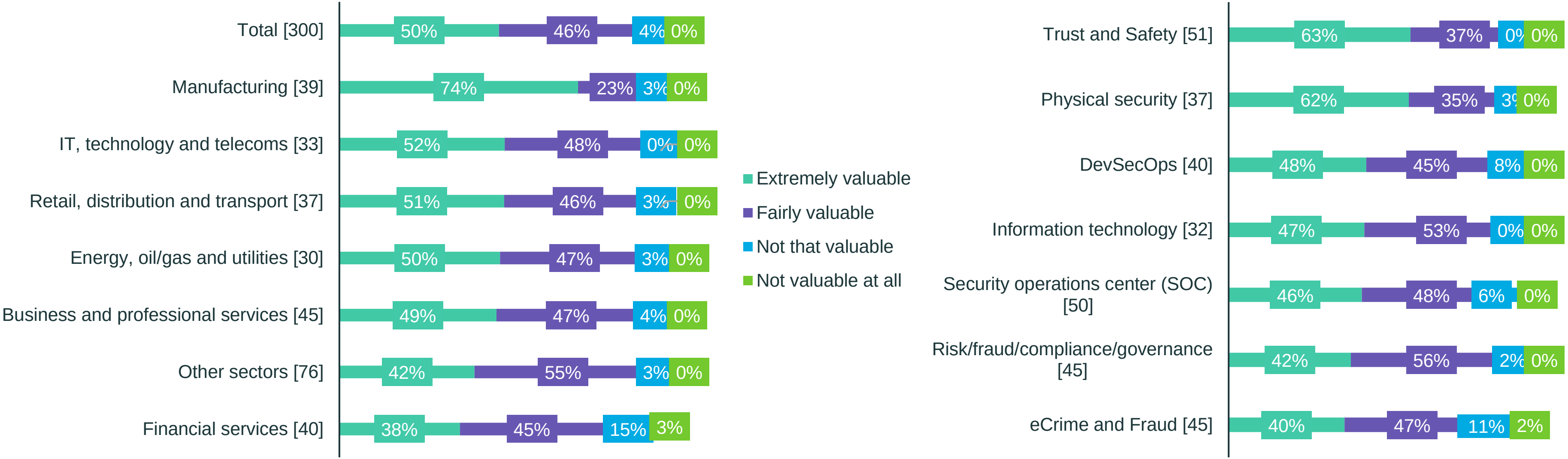
DevSecOps (35%)

SOC (38%)

Risk/fraud/ compliance/ governance (38%)

What's most important to your organization when considering a managed threat intelligence provider? Combination of responses ranked first, second and third [300] omitting some answer options, call outs highlighting each departments' most likely answer if it wasn't "breadth of coverage" or if another answer option had the same respondent count as "breadth of coverage"

Given that access to more experienced analysts was the most likely benefit reported, it's no surprise that direct consultation with an analyst is considered valuable by most



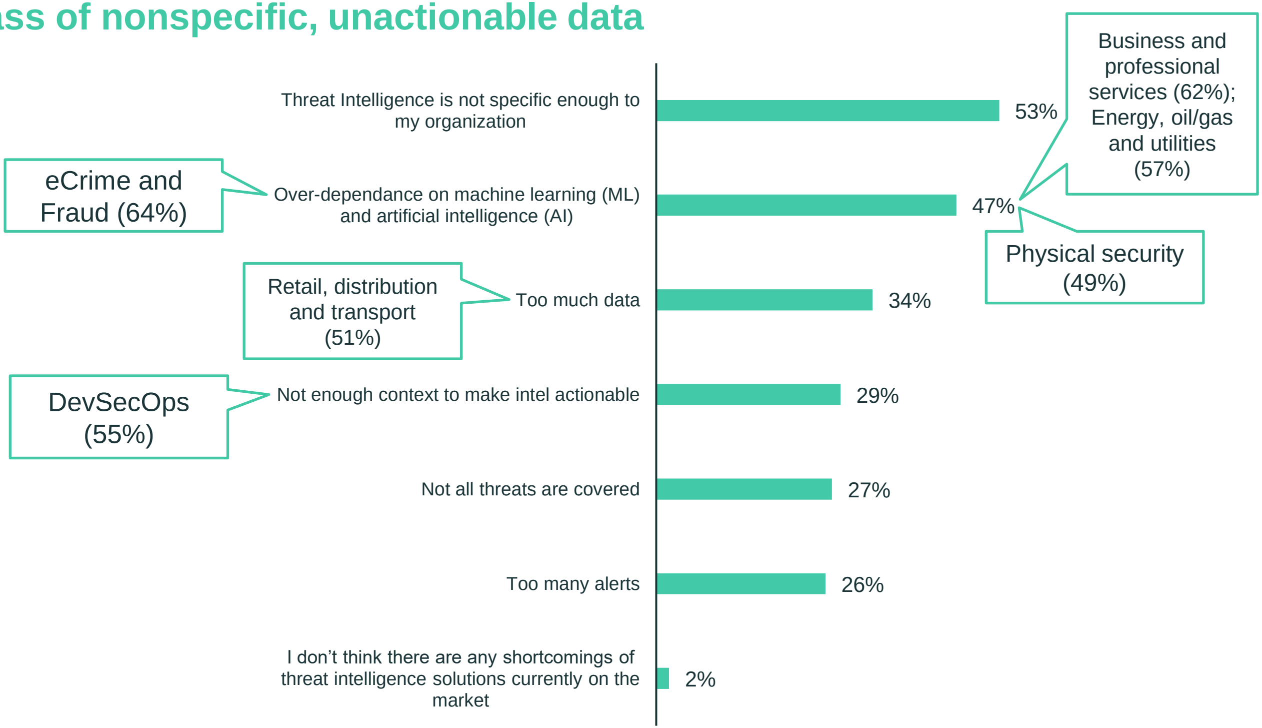
To what extent would direct consultation with a threat intelligence analyst be valuable to your organization?]Base sizes in chart] split by organization sector and respondent department, omitting some answer options

However, some respondents believe that current threat intelligence solutions have some shortcomings, all which point mass of nonspecific, unactionable data

87%

Agree they would benefit from a consultative approach to threat intelligence

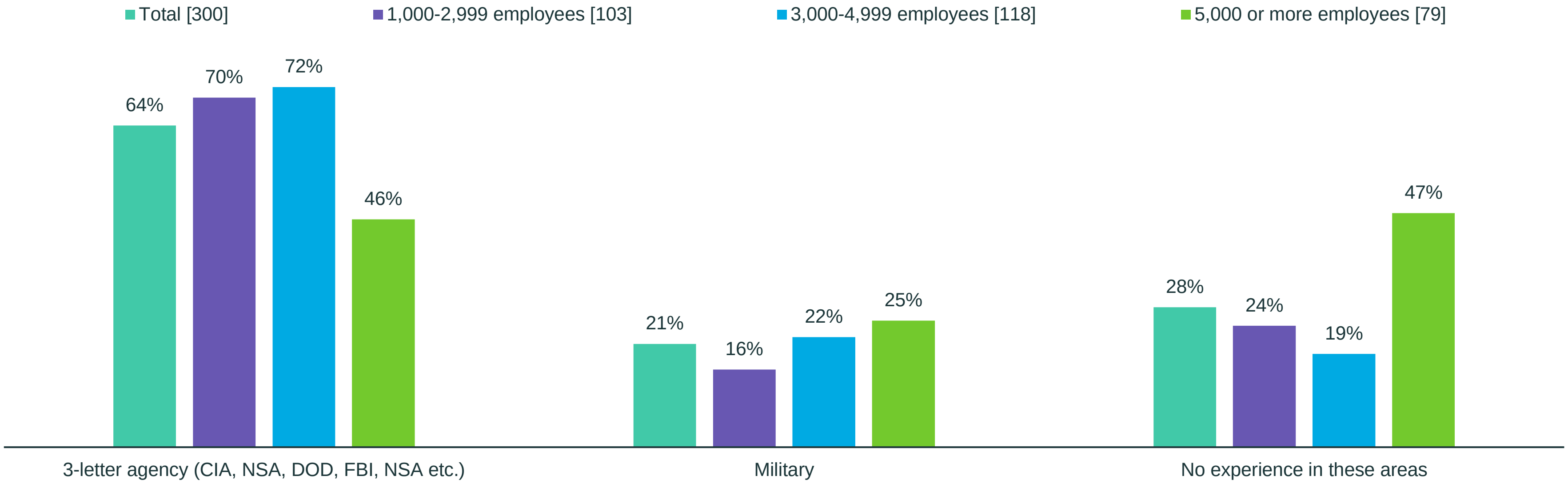
[300]



In your opinion, what do you believe are the shortcomings of threat intelligence solutions currently on the market? [300] omitting some answer options, call outs highlighting each department and sectors most likely answer if it wasn't "threat Intelligence is not specific enough to my organization"

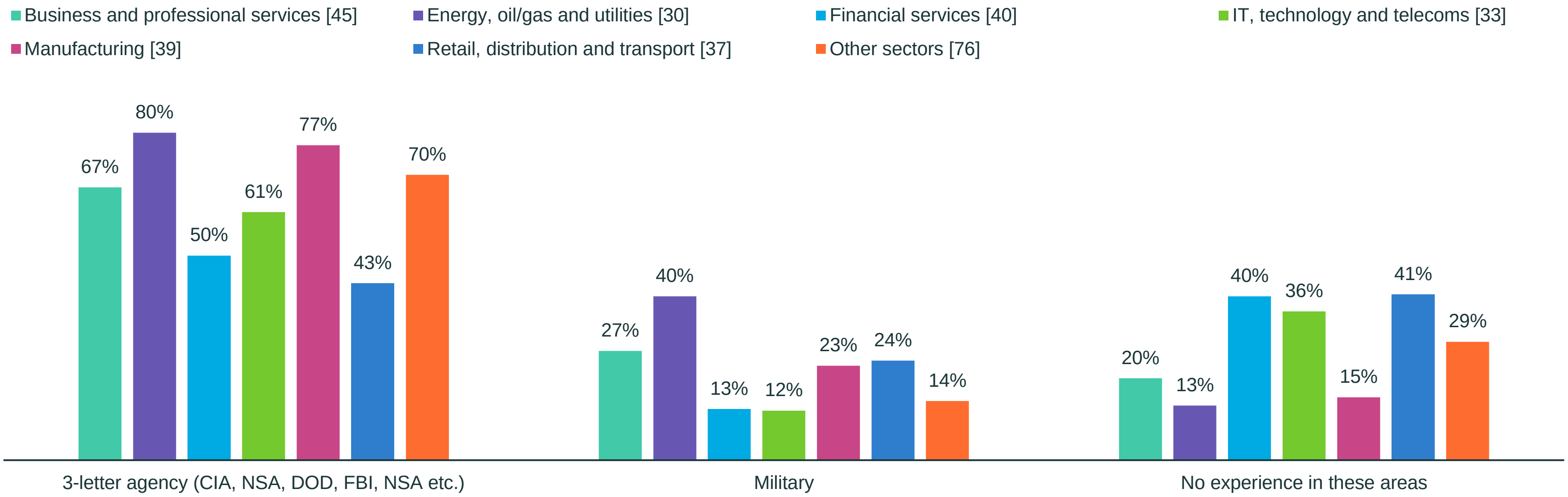
3. Transitioning from reactive to proactive

Respondents are more likely to have prior experience from 3-letter agencies than the military, with larger organizations the most likely to have no experience in these areas



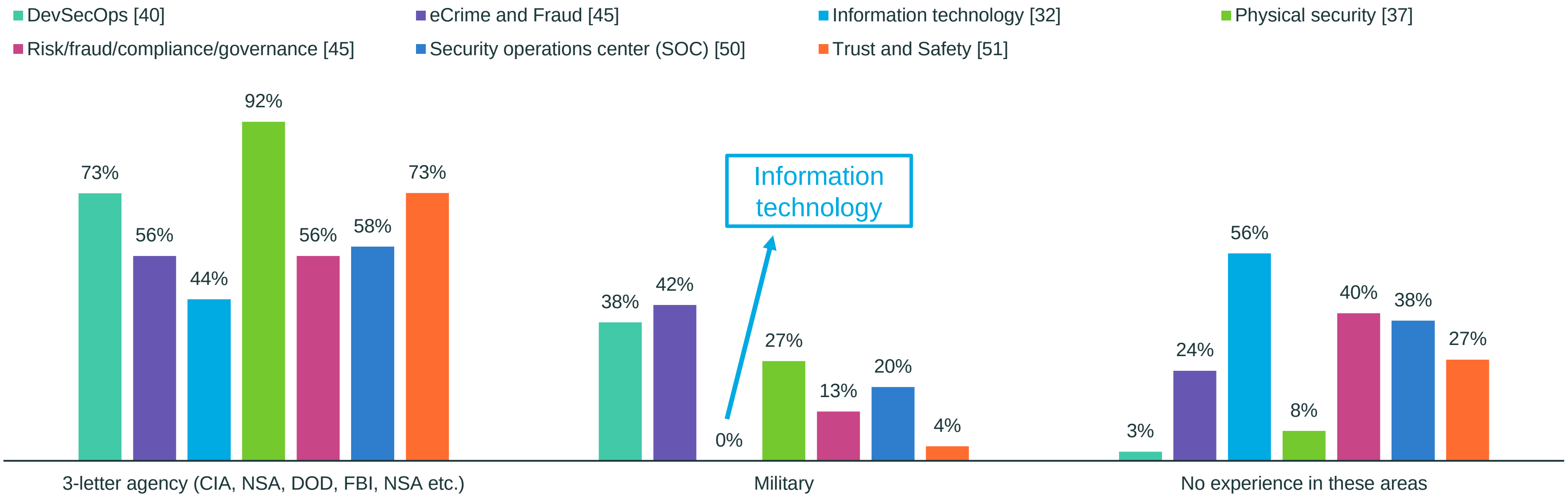
Do you have prior experience as a threat intelligence analyst at a 3-letter agency or in the Military? [Base numbers in chart] split by organization size, omitting some answer options

Energy, oil, gas and utilities are the most likely sectors to have this prior experience



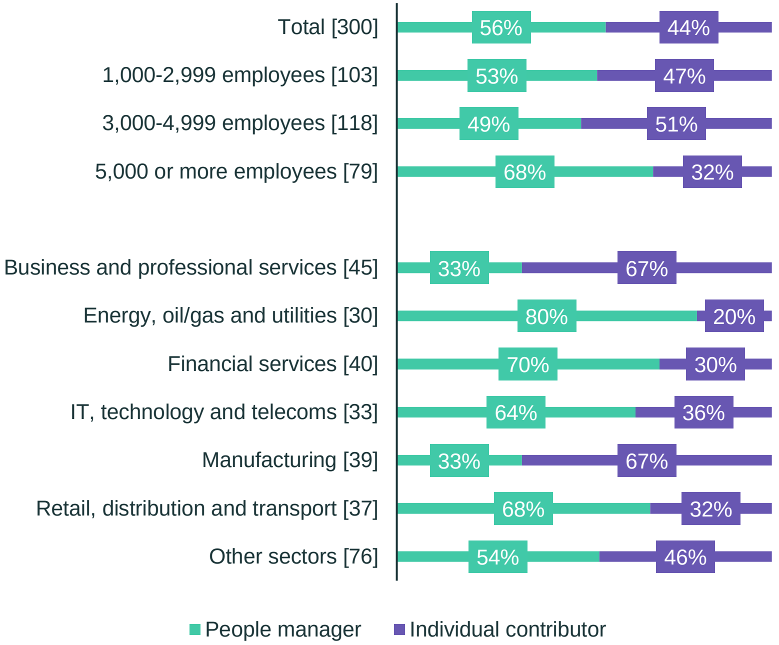
Do you have prior experience as a threat intelligence analyst at a 3-letter agency or in the Military? [Base numbers in chart] split by organization sector, omitting some answer options

Respondents from the information technology department are the least likely to have prior experience in these areas



Do you have prior experience as a threat intelligence analyst at a 3-letter agency or in the Military? [Base numbers in chart] split by respondent department, omitting some answer options

Overall, there is an almost equal mix between people managers and individual contributors however this does vary, especially in larger organizations and within the energy, oil, gas and utilities sector

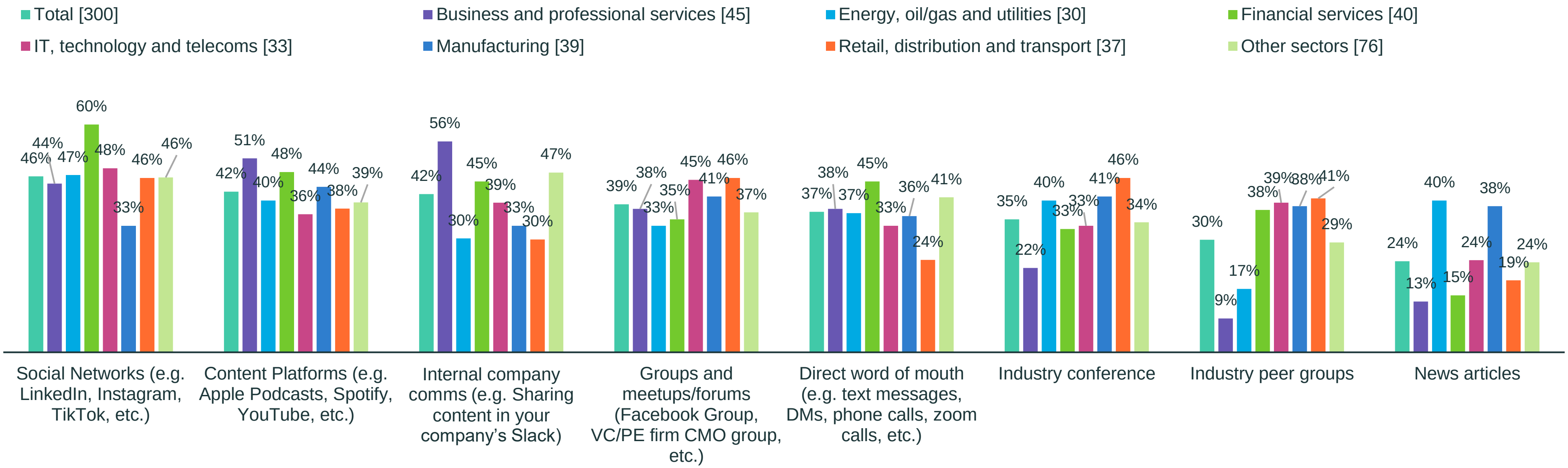


Within your current role, would you consider yourself as an individual contributor or a people manager? [Base sizes in chart], split by organization size and sector, omitting some answer options

VansonBourne

Sponsored by NISOS

Social networking is among one of the most popular ways senior security decision makers access threat intelligence related information relevant to their role



Where do you access threat intelligence related information relevant to your role? [Base sizes in chart] split by organization sector, omitting some answer options

The use of these sources varies greatly between the different departments

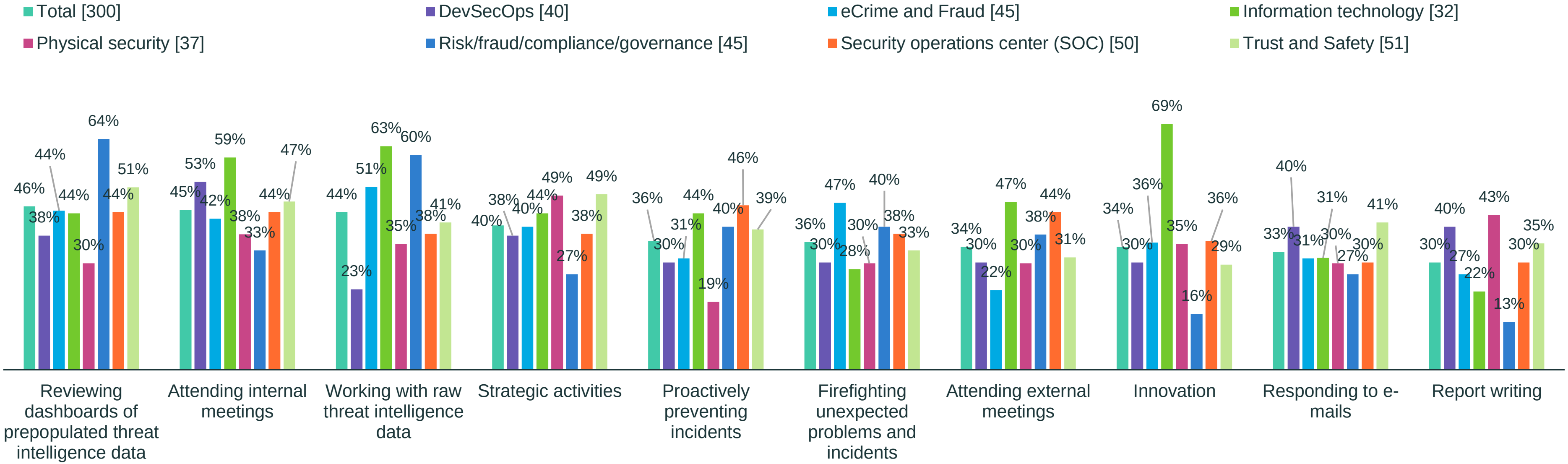
Respondent department	Most likely source	Second likely source	Third likely source
DevSecOps [40]	Industry peer groups (43%) / Email lists (43%)	Internal company comms (40%)	Direct word of mouth (38%)
eCrime and Fraud [45]	Direct word of mouth (49%)	Social Networks (47%)	Content Platforms (44%)
Information technology [32]	Groups and meetups/forums (59%)	Social Networks (56%)	Internal company comms (53%)
Physical security [37]	Content Platforms (49%)	Periodicals and journals (41%)	Industry conference (38%)
Risk/fraud/compliance/governance [45]	Groups and meetups/forums (58%)	Content Platforms (47%)	Social Networks (44%) / Internal company comms (44%)
Security operations center (SOC) [50]	Social Networks (50%)	Content Platforms (44%)	Internal company comms (40%)
Trust and Safety [51]	Social Networks (55%)	Internal company comms (49%)	Content Platforms (41%)

Where do you access threat intelligence related information relevant to your role? [Base sizes in chart] split by respondent department, omitting some answer options

VansonBourne

Sponsored by NISOS

Activities in a typical workday vary greatly between the different departments…

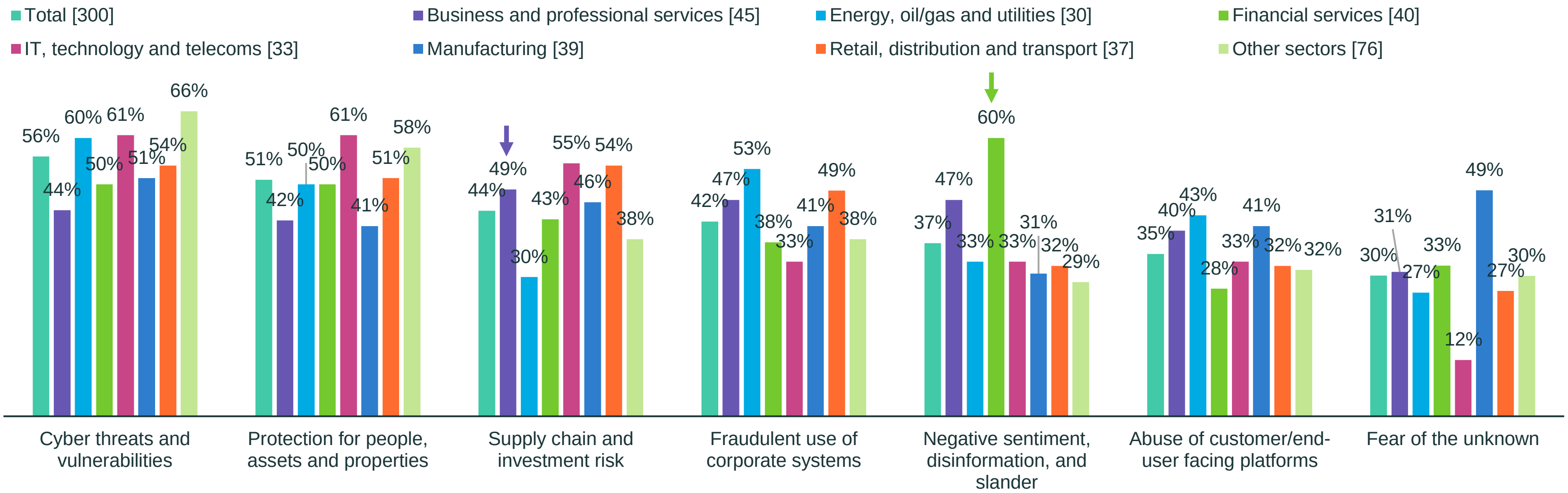


Which of the following do you do throughout a typical day at work? [Base sizes in chart] split by respondents' department, omitting some answer options

VansonBourne

Sponsored by NISOS

Cyber threats and vulnerabilities is the most urgent problem for all but the business and professional services sector, who report supply chain and investment risk as theirs



What are the most urgent problems you experience in your role? Combination of responses ranked first, second and third [Base sizes in chart], split by organization sector, omitting some answer options

VansonBourne

Sponsored by NISOS

Organizations agree that threat intelligence can be very reactive and requires more human input to truly realize it's full potential

95%

93%

88%

Agree that threat intelligence in their organization needs more human input to truly realize its full potential

[300]

82%

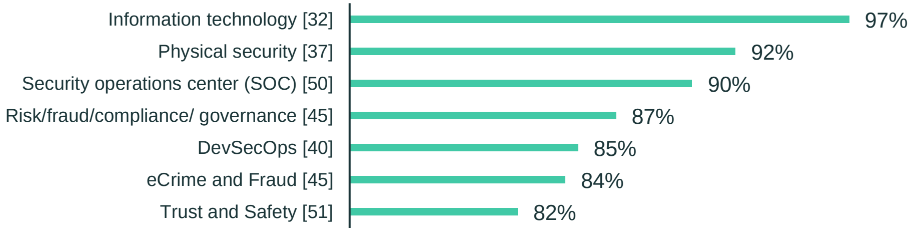
Agree their organization's approach to threat intelligence is very reactive

[300]

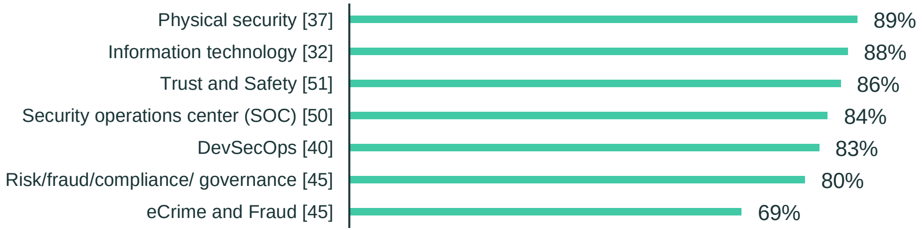
92%

90%

Threat intelligence in my organization needs more human input to truly realize its full potential



My organization's approach to threat intelligence is very reactive



Percentage of respondents who agree with the above two statements [base sizes in chart] split by respondent department

Thank you

To find out more, please visit:
vansonbourne.com

Research methodology

Nisos commissioned independent market research agency Vanson Bourne to conduct research into the threat intelligence landscape.

The study surveyed 300 senior security decision makers in July 2022 from organizations with 1,000 or more employees across all public and private sectors.

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit vansonbourne.com

VansonBourne

Sponsored by

NISOS