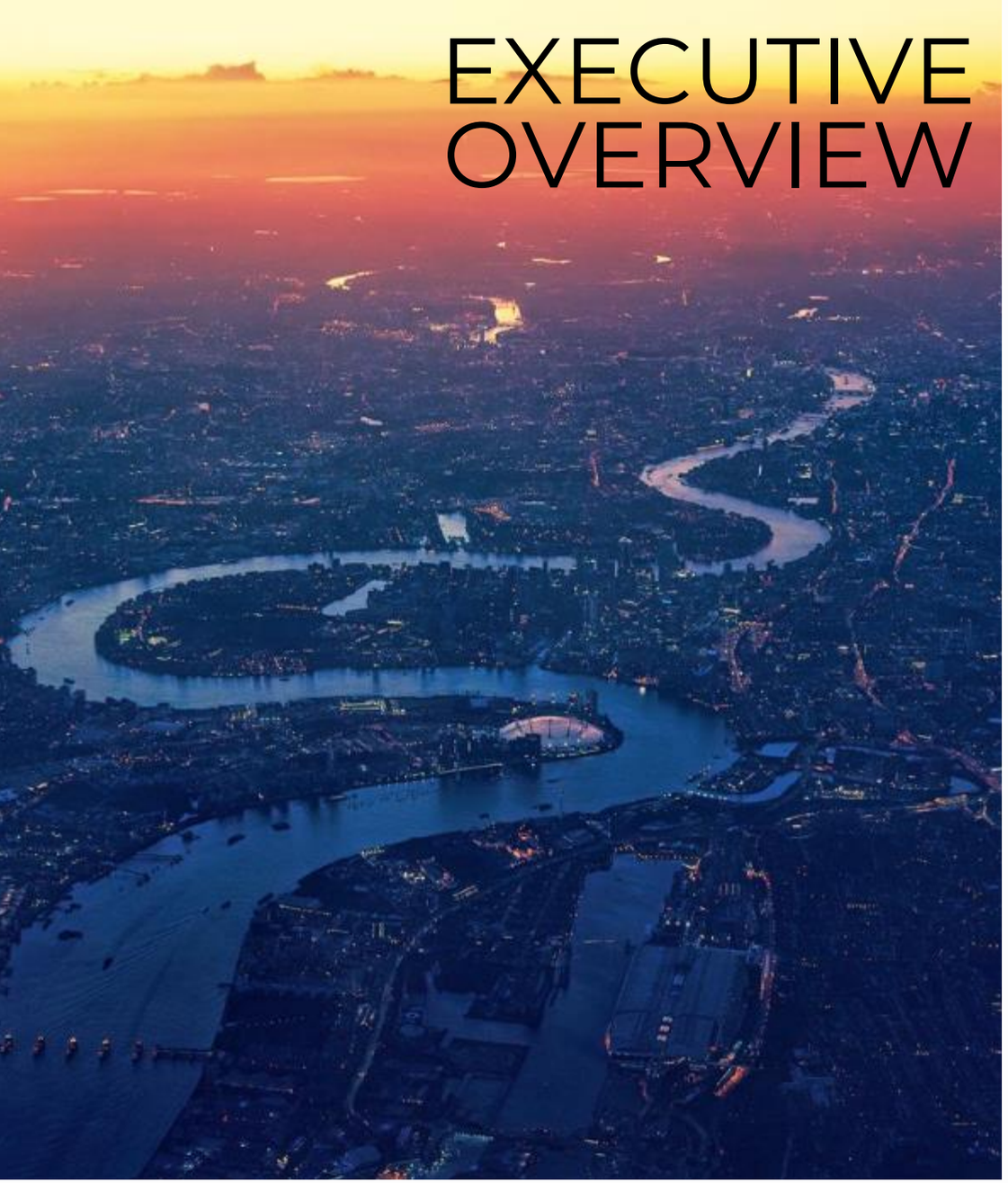
Operational Technology Cybersecurity Trends

Summary Results | August 2021



EXECUTIVE OVERVIEW

Between June and July 2021, Gatepoint Research invited selected IT/OT, Security and Operations executives to participate in a survey themed *Operational Technology Cybersecurity Trends.* 102 executives have participated to date.

- Management levels represented are all senior decision makers and influencers: 10% hold the title CxO, 6% are VPs, 22% are directors, 52% are managers, and 10% are security engineers or architects.

- Survey participants represent firms from a wide variety of industries, including Power, Chemicals, Oil & Gas, Life Sciences, Food & Beverage, Pulp & Paper, DCS & Engineering Services, Mining & Metals, and Manufacturing.

The cyber risks that may affect Operational Technology (OT) and Industrial Control Systems (ICS) extend well beyond headline-grabbing malicious outside actors. The unintentional security breaches posed by employees or contractors can be just as disastrous. Or, simply not having an up-to-date inventory of control system configurations might take an entire production facility offline. How are organizations doing at staying on top of OT/ICS cybersecurity threats?

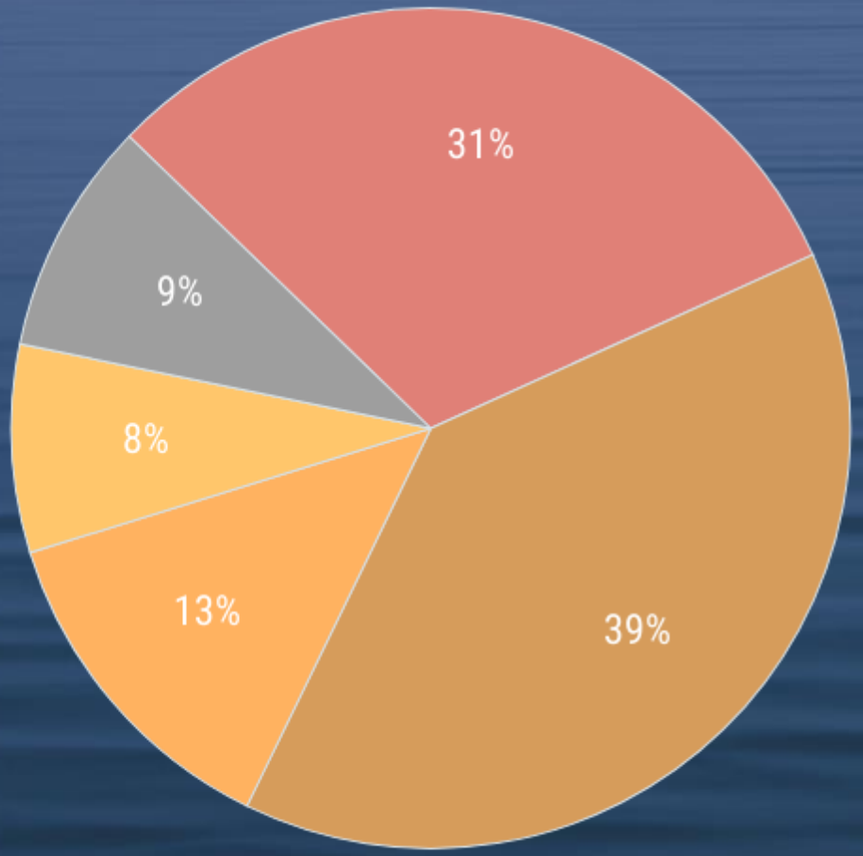
This survey asked respondents to report:

- What is their organization's perception of OT/ICS cyber risk? How have security incidents changed in the past year?

- What approaches does their organization take to prevent OT/ICS security threats? And how long does it typically take to detect a threat?

- What are their top OT/ICS security initiatives currently?

What is your organization's perception of operational technology (OT) and industrial control systems (ICS) cyber risk?



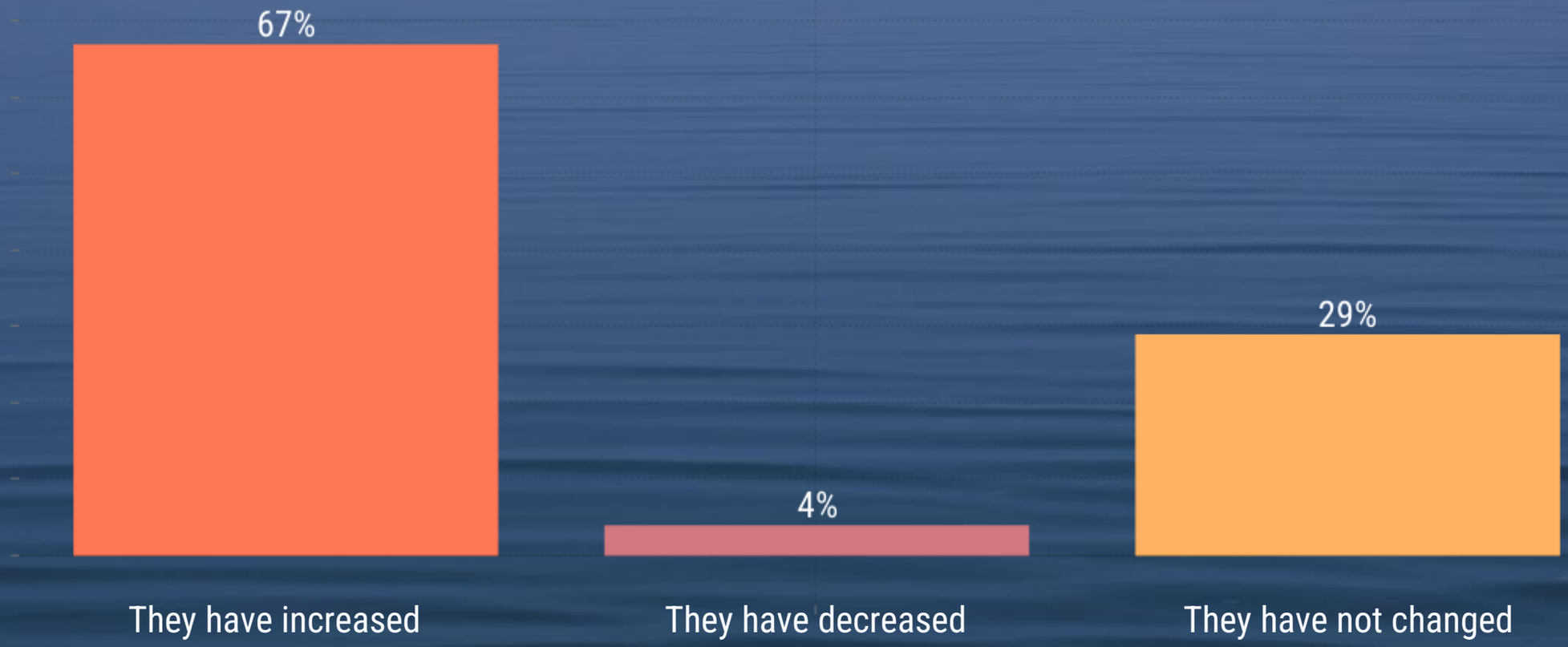
Severe/Critical	31%
High	39%
Moderate	13%
Low	8%
Not sure	9%

70% of Survey respondents rate the potential OT/ICS cyber risk as either severe or critical.

Summary Results | August 2021

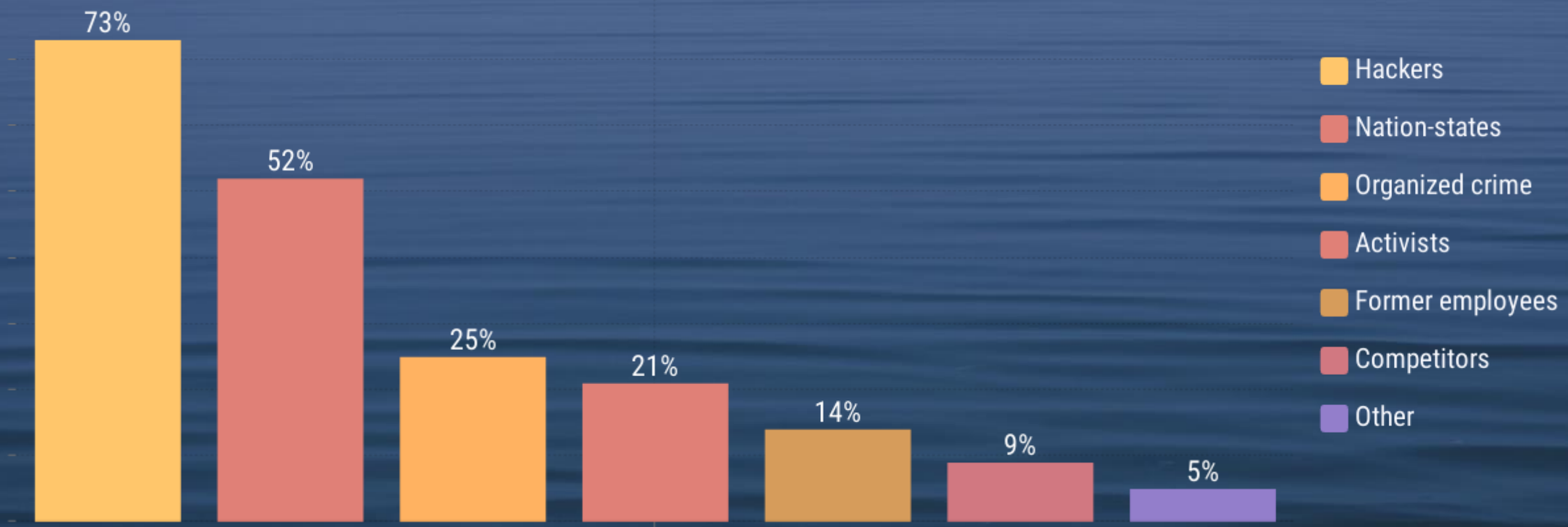
GATEPOINT RESEARCH PulseReport

How have OT/ICS security incidents changed in the past year?



A staggering 67% of survey participants report an increase in OT/ICS security incidents in the past year.

Which two malicious OT/ICS security threats concern you the most?

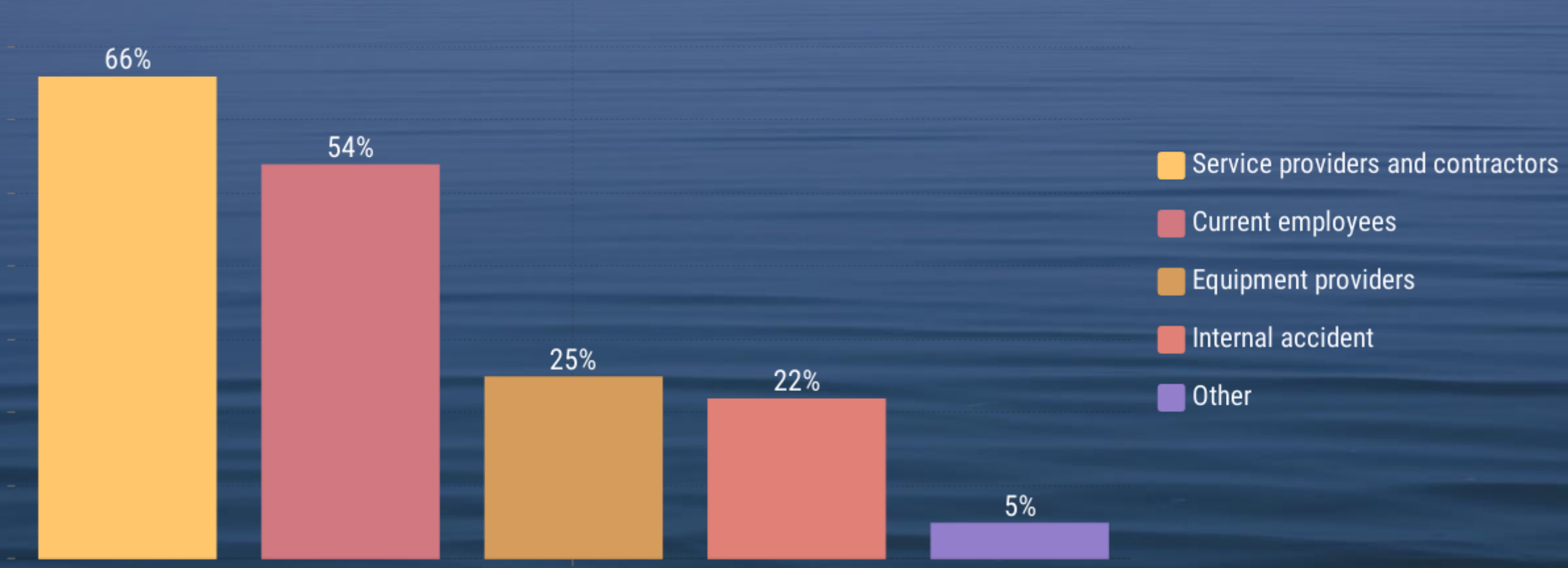


Of all malicious security threats, nearly three quarters of respondents rate hackers as their highest concern, with more than half also being worried about nation-states.

Summary Results | August 2021

GATEPOINT RESEARCH PulseReport

Which two user groups pose the greatest *unintentional* OT/ICS security risk?

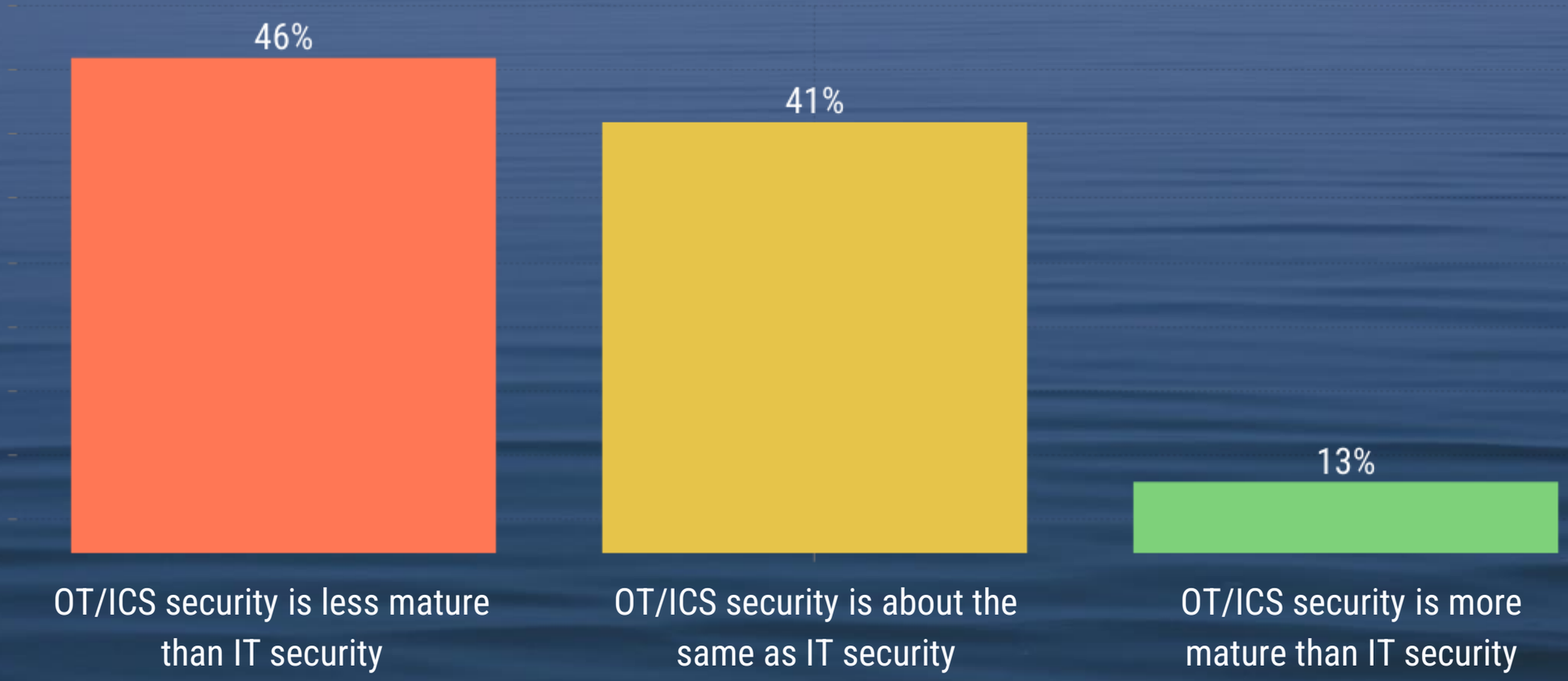


Two thirds of those surveyed are primarily concerned about unintended security breaches caused by service providers and contractors. More than half cite the OT/ICS security risk posed by current employees to be a top worry for them.

Summary Results | August 2021

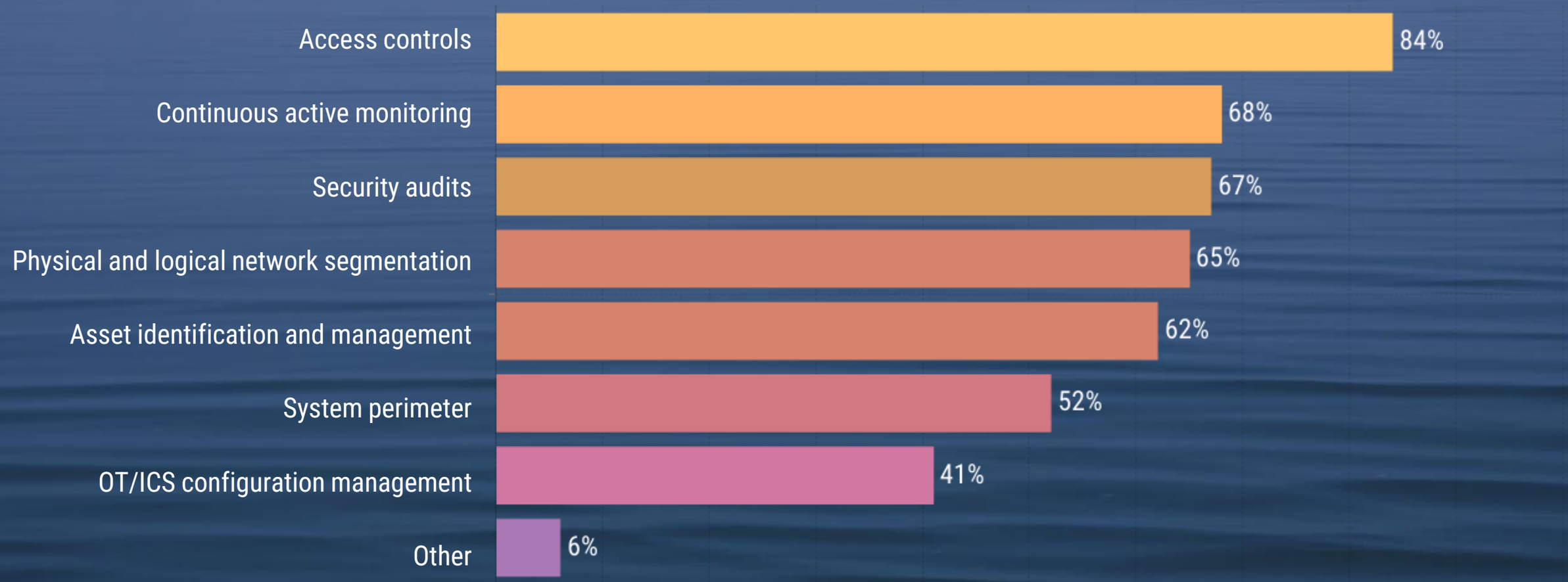
GATEPOINT RESEARCH PulseReport

How do you rate OT/ICS cybersecurity vs. IT cybersecurity maturity in your organization?



Nearly half of respondents rate OT/ICS security as less mature than IT security; just 13% say it exceeds IT security.

What approaches does your organization take to prevent OT/ICS security threats?

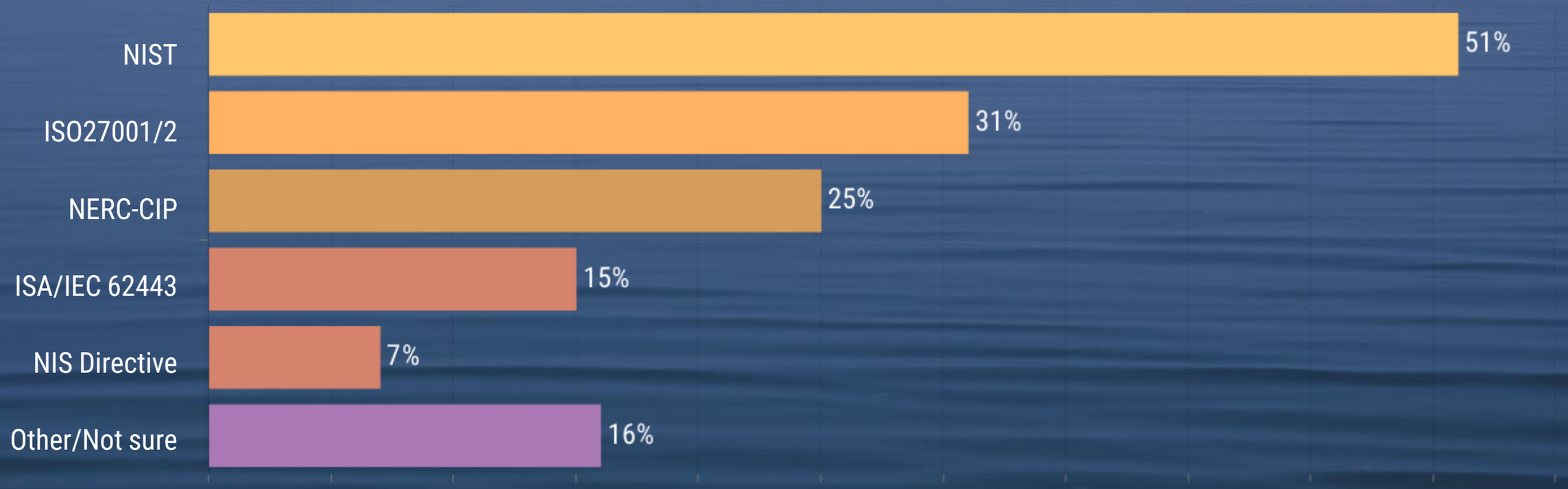


Most organizations surveyed are fairly proactive in their prevention of OT/ICS security threats, with more than half implementing 6 of the 7 methods listed.

Summary Results | August 2021

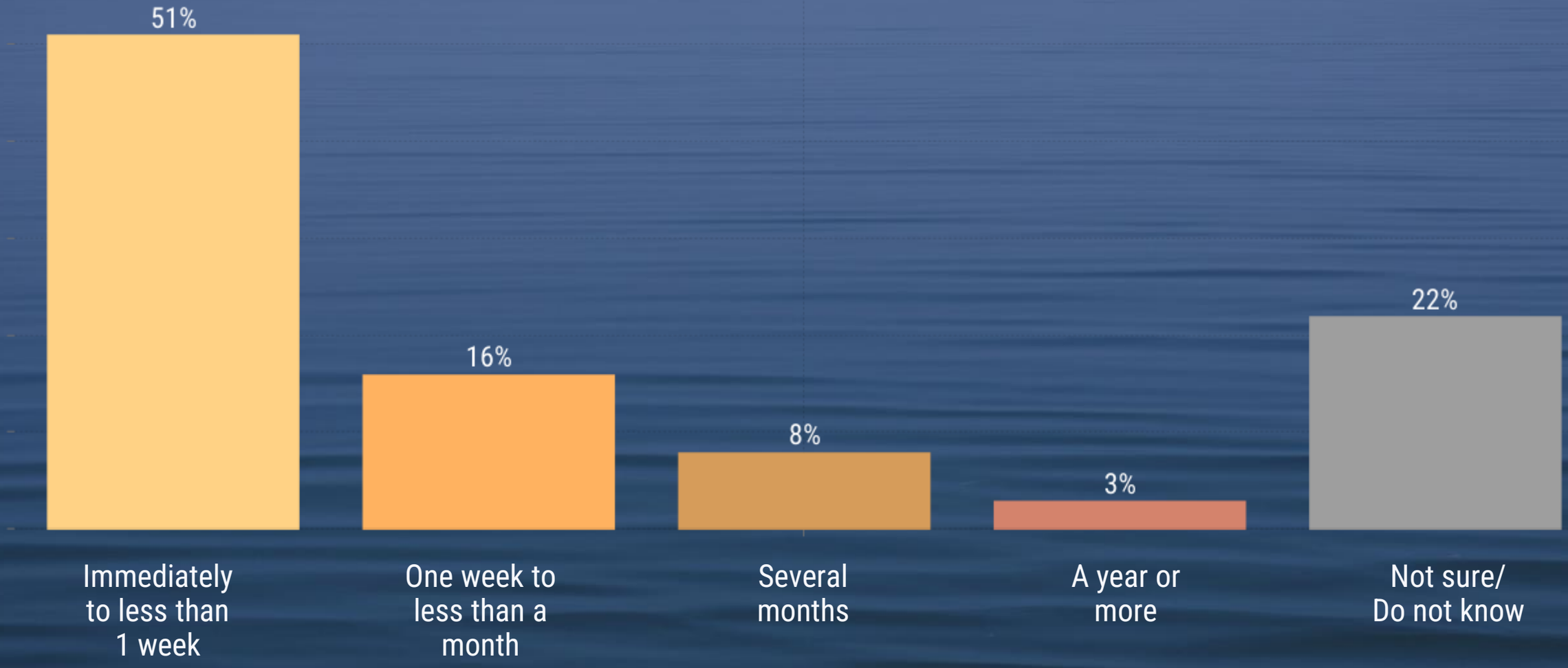
GATEPOINT RESEARCH PulseReport

What security frameworks are you using?



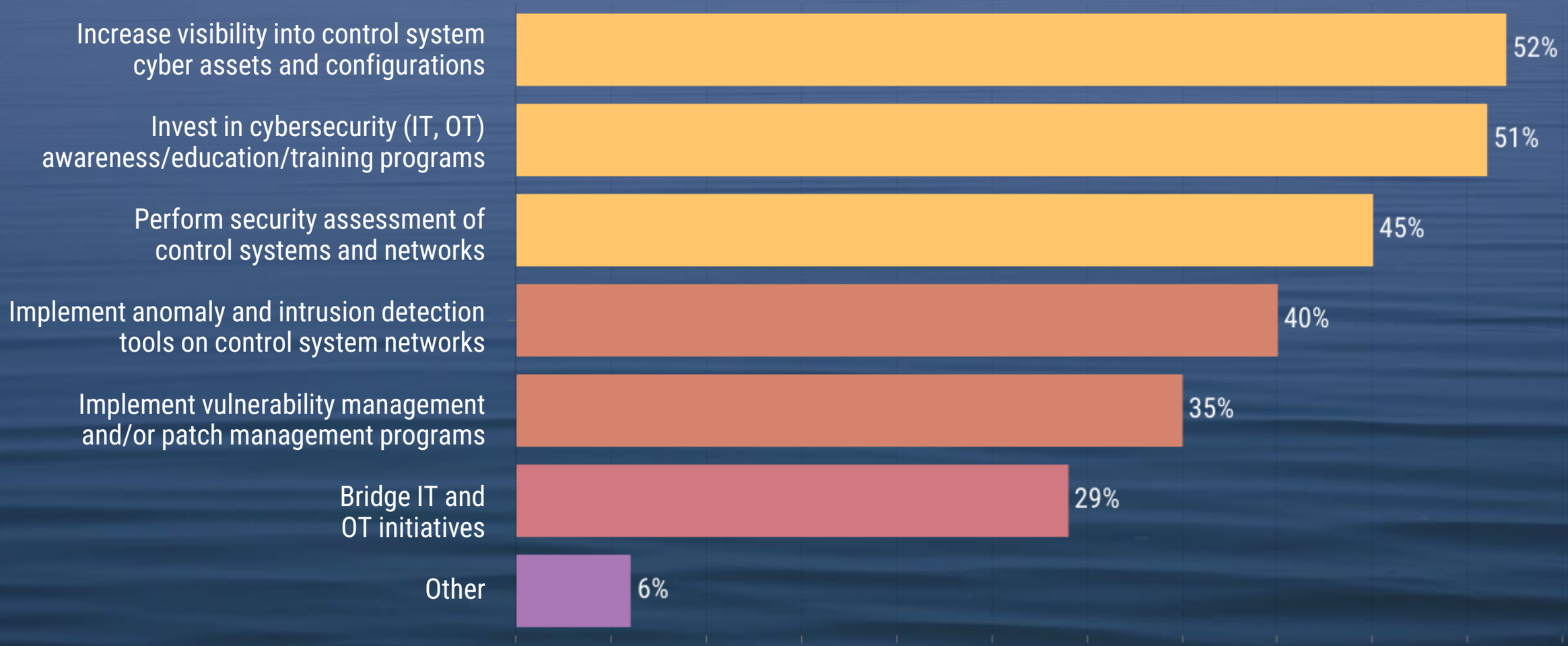
Just over half of survey participants use NIST. Least popular is NIS Directive, with only 7% indicating usage.

How long does it typically take to detect an OT/ICS security threat?



Although half of respondents can detect a security threat in less than a week, 27% say it could take anywhere from a week to a year or more - and 22% don't even know how long it might take.

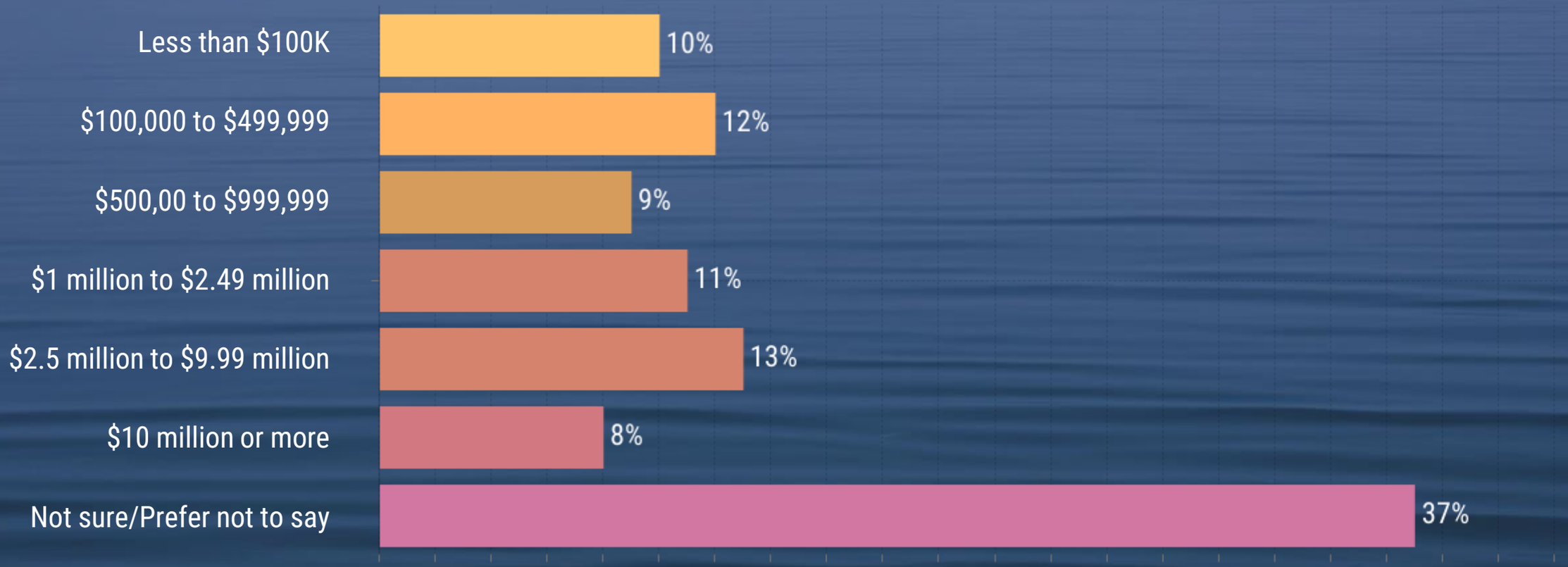
What are your top 3 OT/ICS security initiatives currently?



Respondents are primarily focused on three top initiatives: increasing visibility into control system cyber assets and configurations, expanding cybersecurity awareness/education, and assessing security of control systems and networks.

GATEPOINT RESEARCH PulseReport

What is your organization's total OT/ICS cybersecurity budget for 2021?

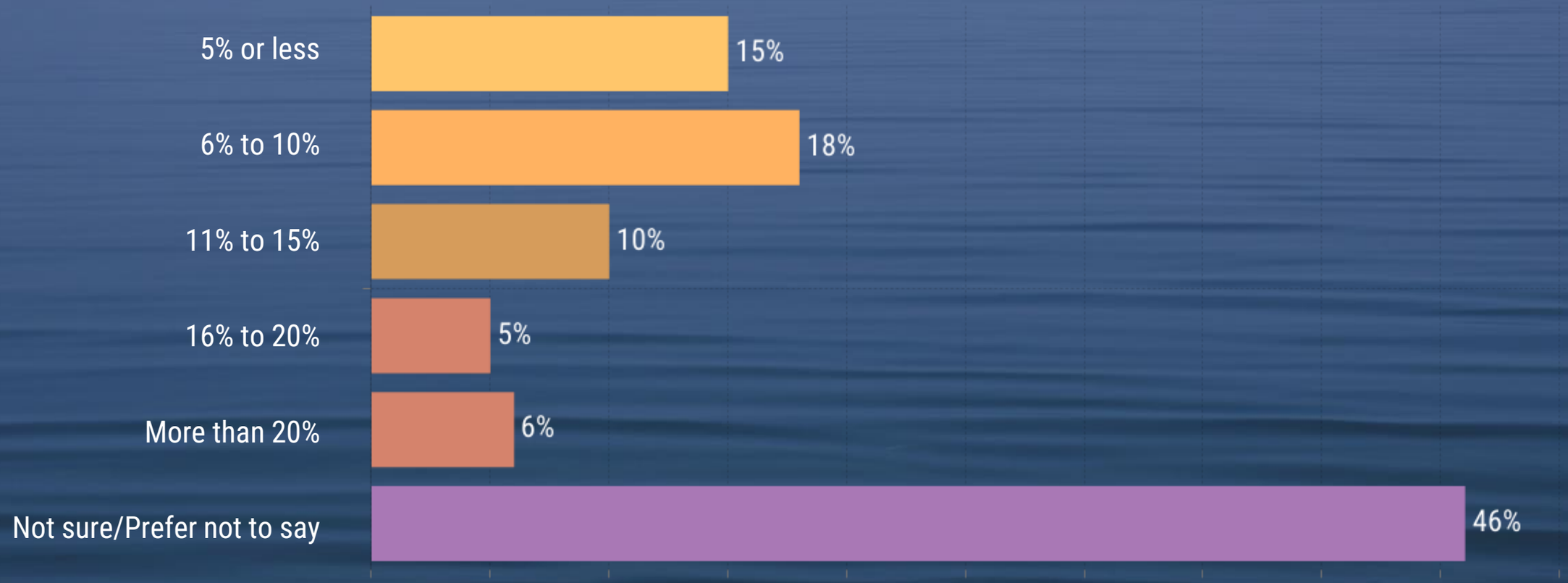


OT/ICS security budgets run a fairly wide gamut, from less than $100k to $10 million or more.
37% of survey participants are either not sure or prefer not to divulge.

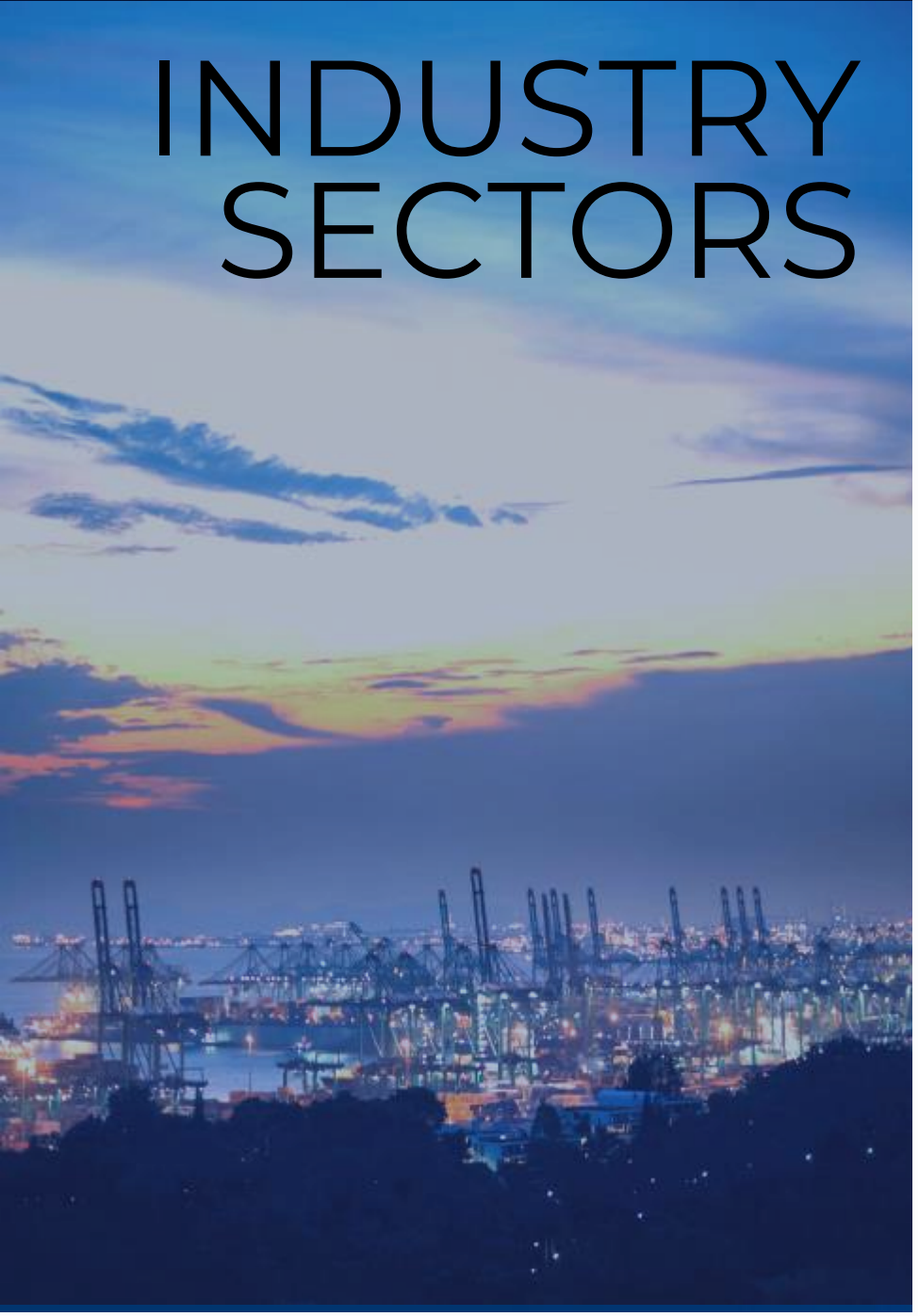
Summary Results | August 2021

GATEPOINT RESEARCH PulseReport

What percent of the total IT budget is allocated to OT/ICS cybersecurity?



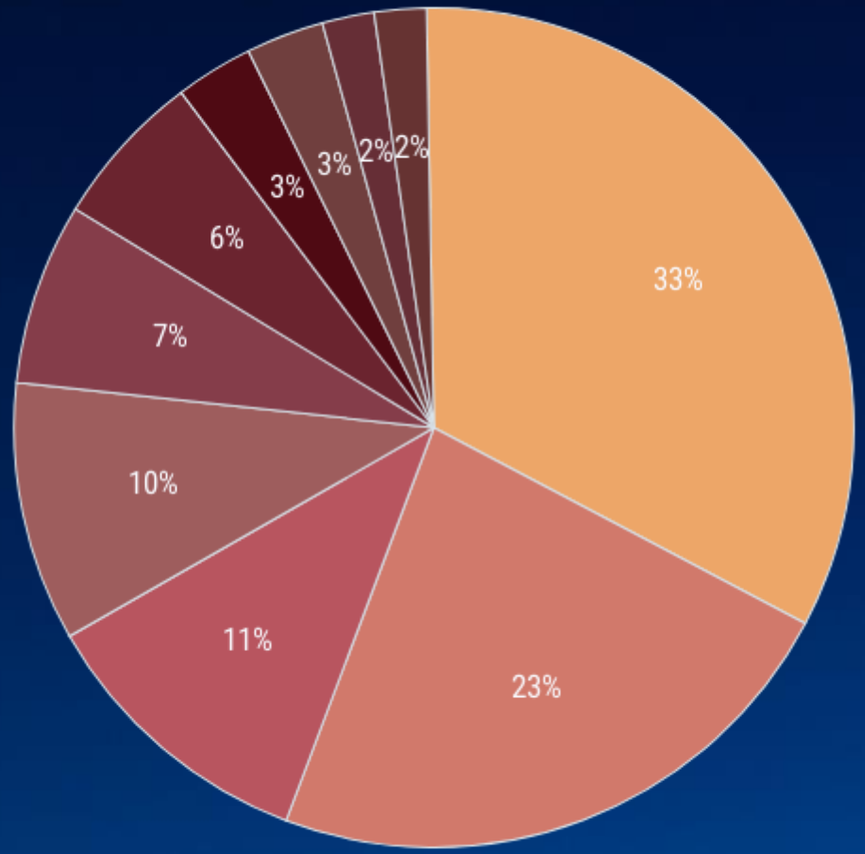
Considering the total IT budget for organizations, OT/ICS allocation is as low as 5% (or less), up to as much as 20% or more among those surveyed, though almost half would rather not disclose (or just do not know).



INDUSTRY SECTORS

Survey participants represent primarily power, chemicals and refining industries.

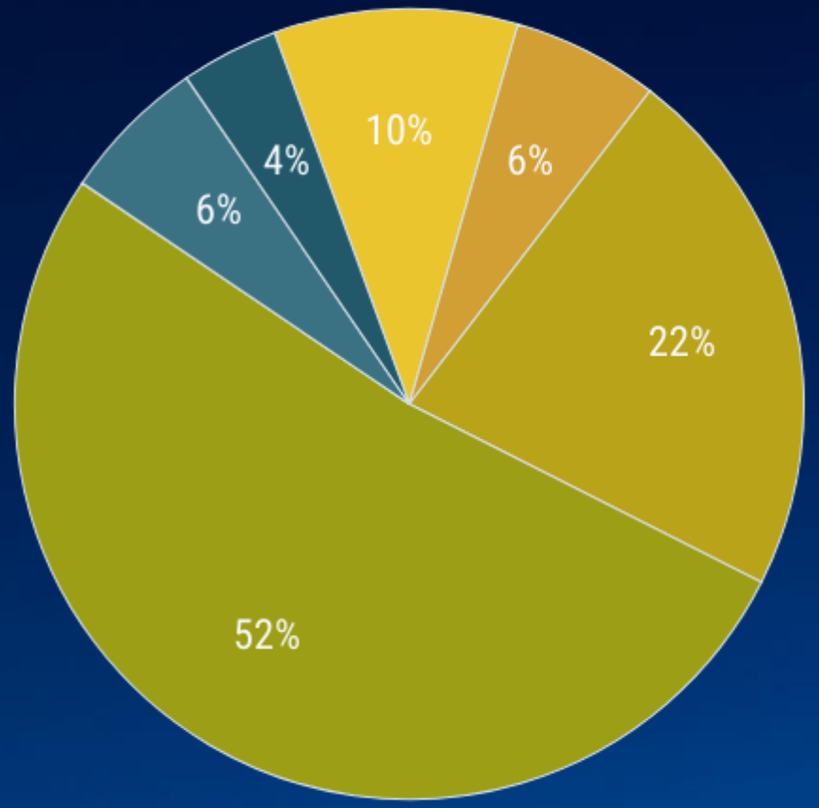
Power	33%
Chemicals	23%
Oil and Gas	11%
Life Sciences	10%
Food and Beverage	7%
Pulp and Paper	6%
DCS and Engineering Service	3%
Mining and Metals	3%
Manufacturing	2%
OTHER	2%



JOB LEVEL

38% of survey respondents hold director or executive level positions in their organization.

CxO	10%
VP	6%
Director	22%
Manager	52%
Security Engineer	6%
Security Architiect	4%



PAS, part of Hexagon, delivers software solutions that prevent, detect, and remediate cyber threats; reduce process safety risks and optimize profitability; and enable trusted data for decision-making.

PAS helps industrial organizations ensure OT Integrity, including 13 of the top 15 refining and 13 of the top 15 chemical companies.

Learn more at cyber.pas.com