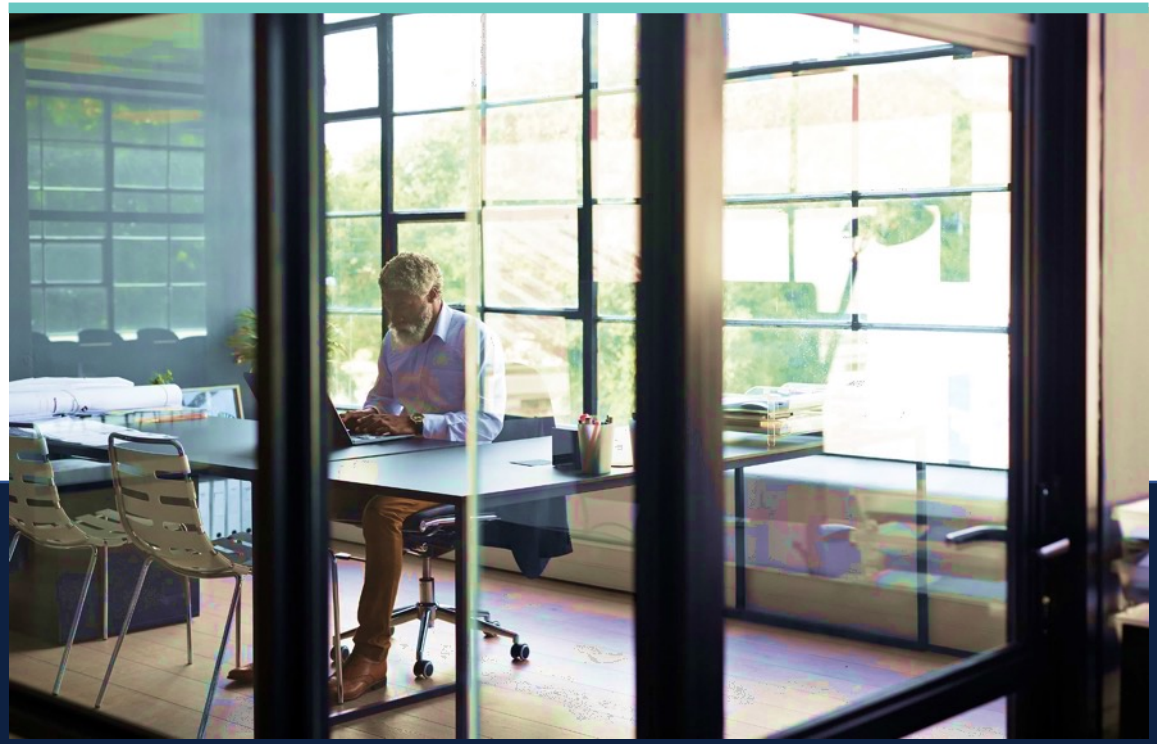
servicenow

PULSE REPORT GATEPOINT RESEARCH

OPERATIONAL TECHNOLOGY SECURITY STRATEGIES

SUMMARY RESULTS



NOVEMBER 2022

WHO DID WE SURVEY?

Between August and October 2022, Gatepoint Research invited selected executives to participate in a survey themed *Operational Technology Security Strategies*.

Candidates from several industries were invited via email and 139 executives have participated to date.

Management levels represented are all senior decision-makers: 22% hold the title CxO, 17% are VPs, and 61% are directors.

100% of responders participated voluntarily; none were engaged using telemarketing.

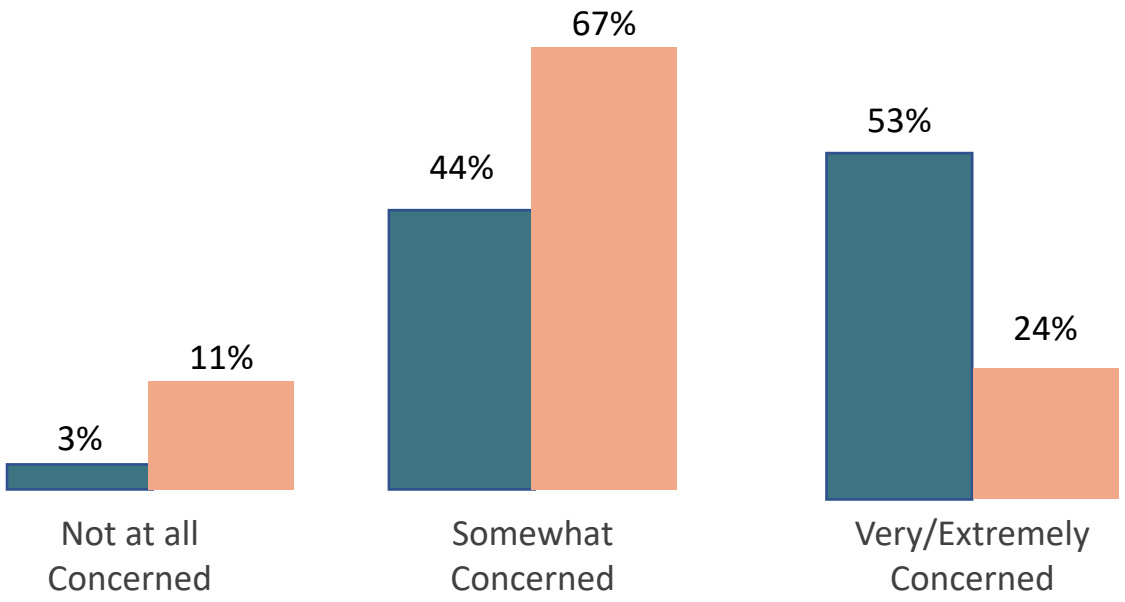
EXECUTIVE SUMMARY

A single malware or ransomware attack can compromise a manufacturer's reputation, or worse. While ransomware remains at the top of the list of manufacturers concerns, OT device attacks are a growing threat. These threats can create havoc and result in big losses by shutting down production.

Vulnerabilities in the OT landscape can only be addressed if the security team has visibility to the whole environment and can compartmentalize risks with proper context. Working with their security counterparts, manufacturing operators, can increase visibility, remediate common vulnerabilities and when an attack happens, they can execute their plans to respond and minimize production downtime.

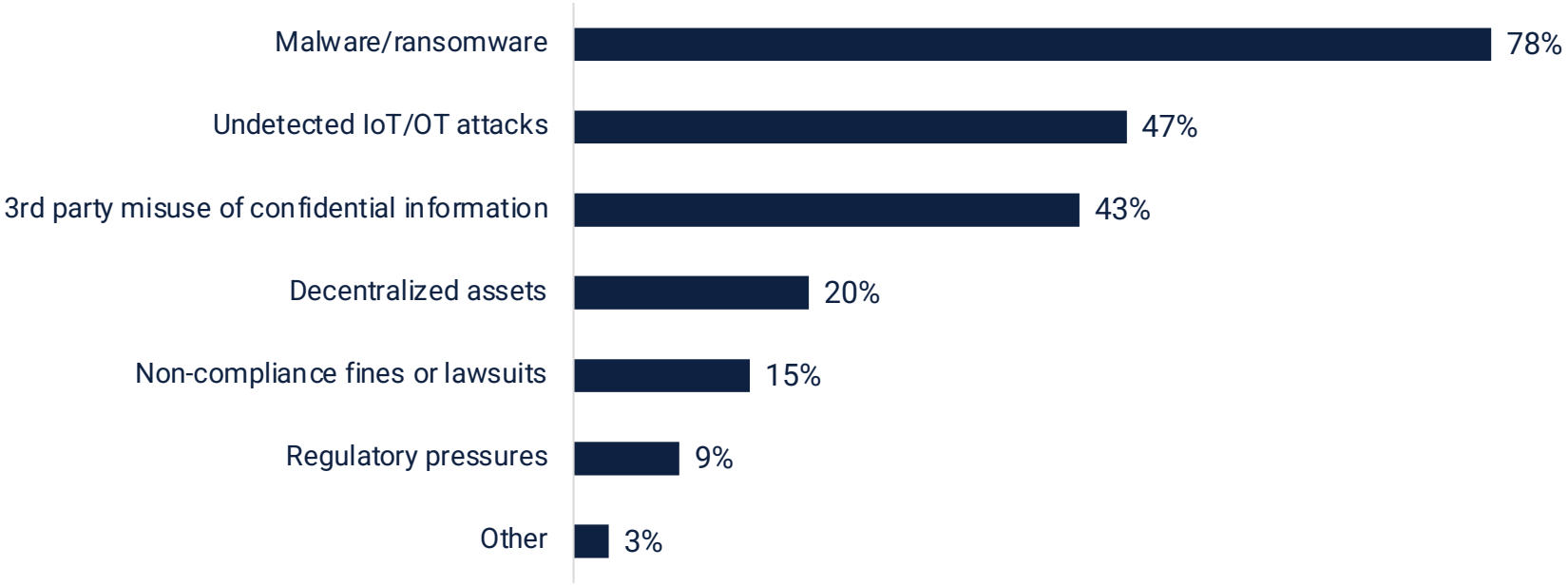
This survey hi-lights manufacturers concerns, preparedness and cross functional alignment and sheds light on areas for improvement.

How concerned are you about a cyber-attack on your operational technology (OT)?



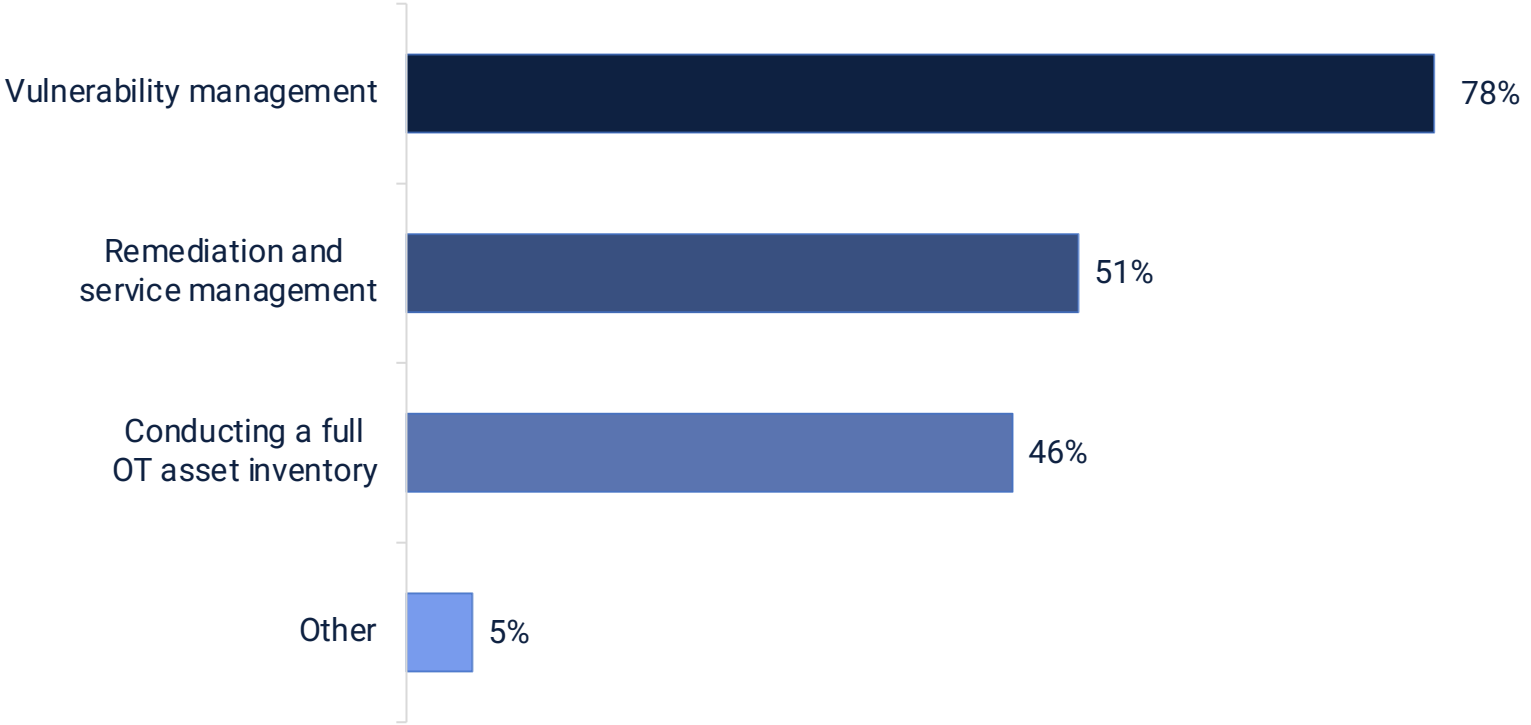
Overall, respondents have varying levels of concern about cyber attacks on their OT. However, the IT/Security executives see things in a darker light. Segregating their answers hi-lights the difference. Only 3% of security execs are "not at all concerned" vs. 11% of respondents in other titles. While 53% of security execs are "very/extremely" concerned vs 24% of those not in IT/security roles)

What are your top concerns related to securing OT assets?



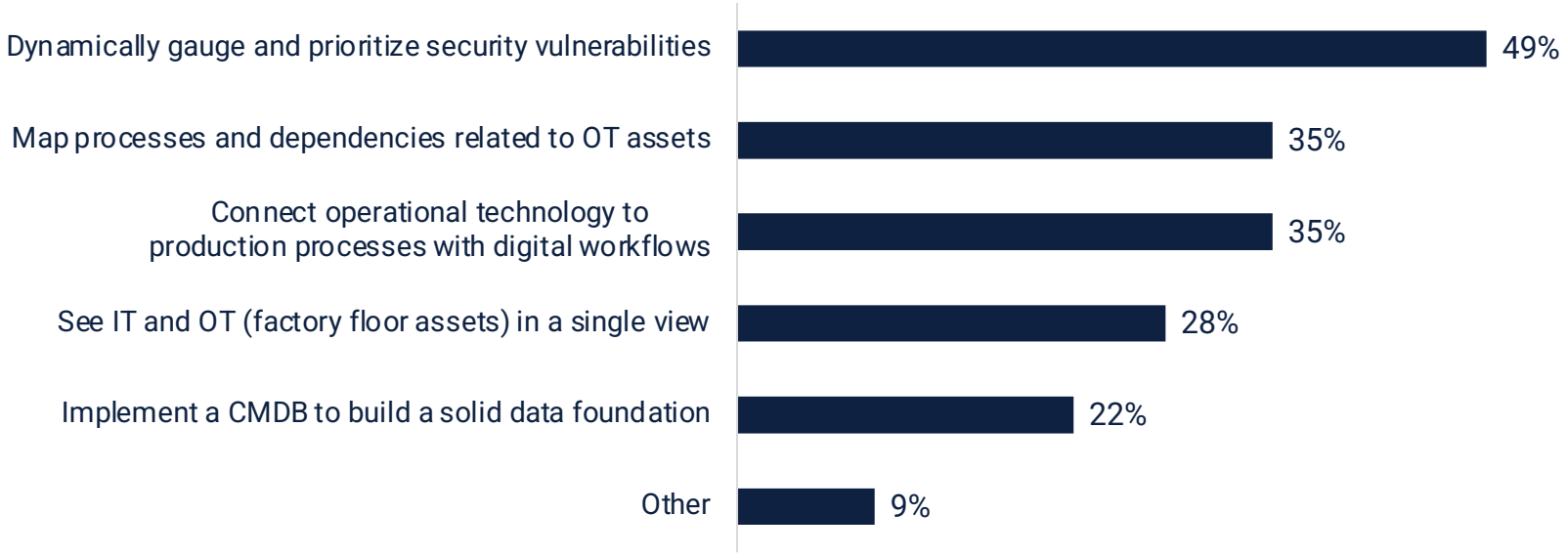
Malware and ransomware top the list of worries shared by more than three-fourths of respondents. Undetected IoT or OT attacks rank second (cited by 47%), with de-centralized assets fourth (cited by 20%)

In what OT initiatives is your organization investing?



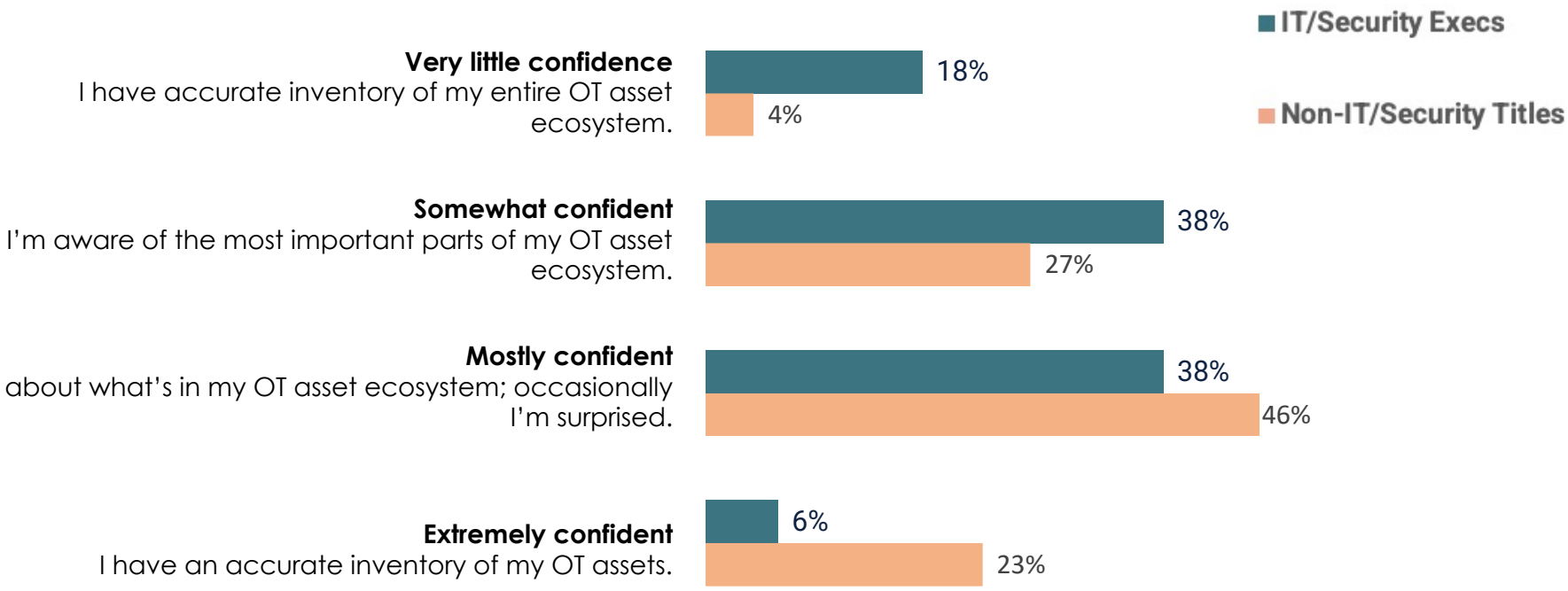
Investing in vulnerability management is heavily favored by most (78%) of respondents. 51% will put money into remediation and service management, and 46% say conducting an OT asset inventory is on the spend list.

What do you need to do to solve current or potential OT security challenges?



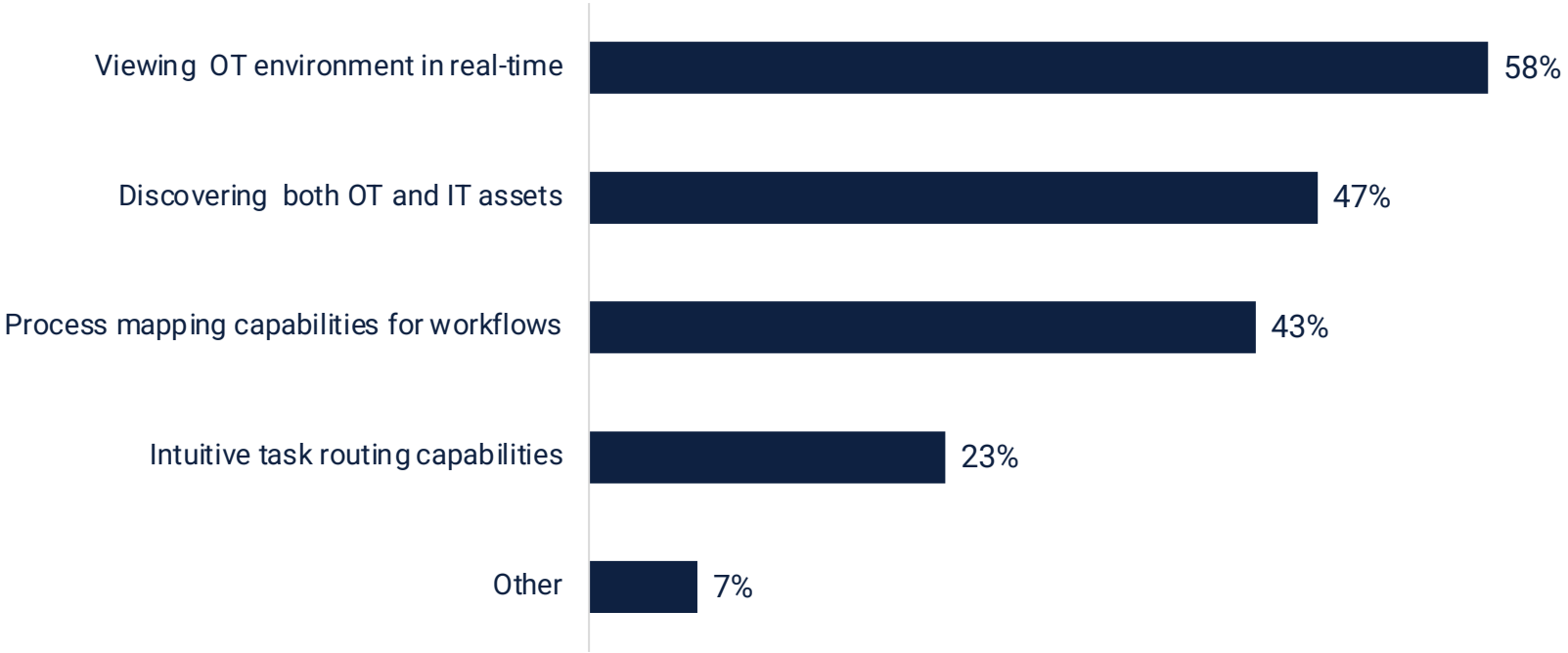
Security challenges—current or future—might be addressed with a tool that can gauge and rank them, say 49% of those surveyed. Other solutions favored by respondents include mapping OT asset processes and dependencies (35%), connecting OT tech and production process using digital workflows (also 35%), a single view of assets (28%), and a CMDB (22%).

What describes your confidence in your organizations inventory of the OT asset ecosystem?



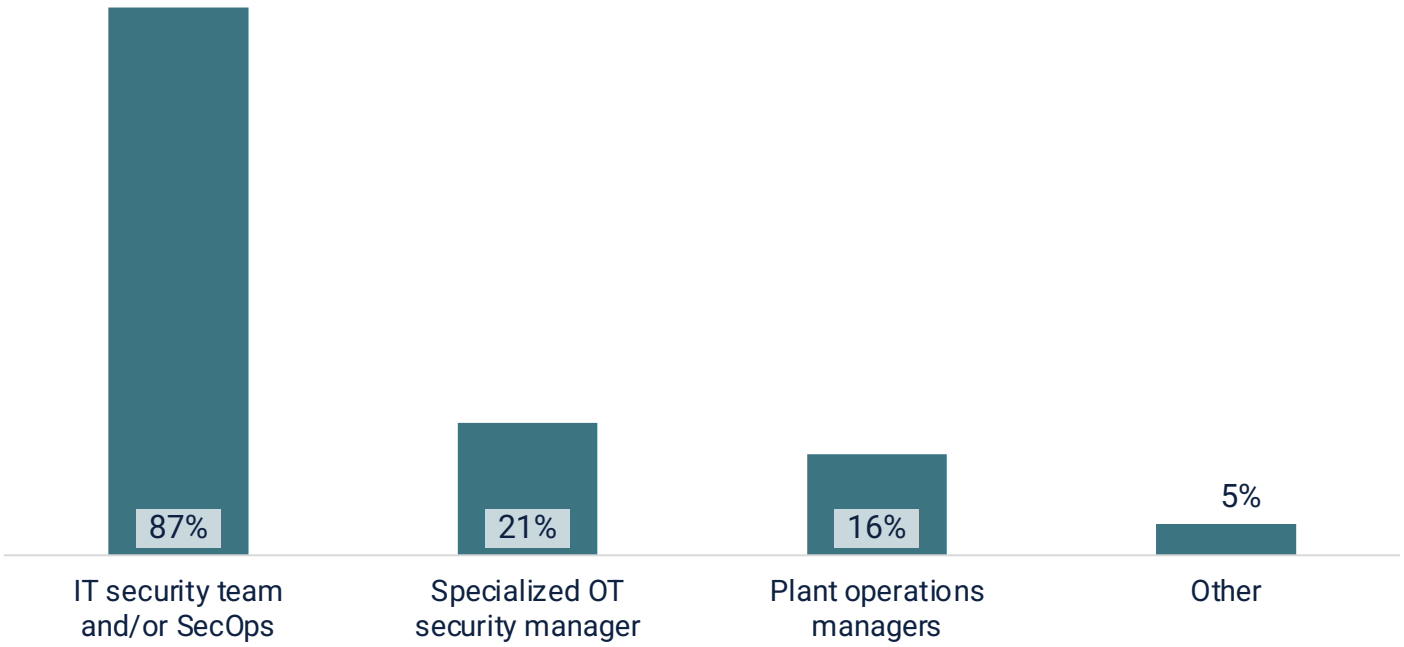
It is not surprising that many respondents' confidence in being able to inventory all their OT assets is a shaky. The respondents that are directly responsible for cyber-security are less confident, overall, than those that are not.

What is most important to you in an OT security solution?



An OT security solution must allow visibility into my whole environment, in real time, say 58%. Being able to discover OT and IT assets is essential to 47%, and nearly as many want their solution to enable process mapping capabilities for workflows. Intuitive task routing is important to 23%.

Who has day-to-day responsibility for securing all your OT?



Most organizations have IT security/SecOps teams handle OT security.

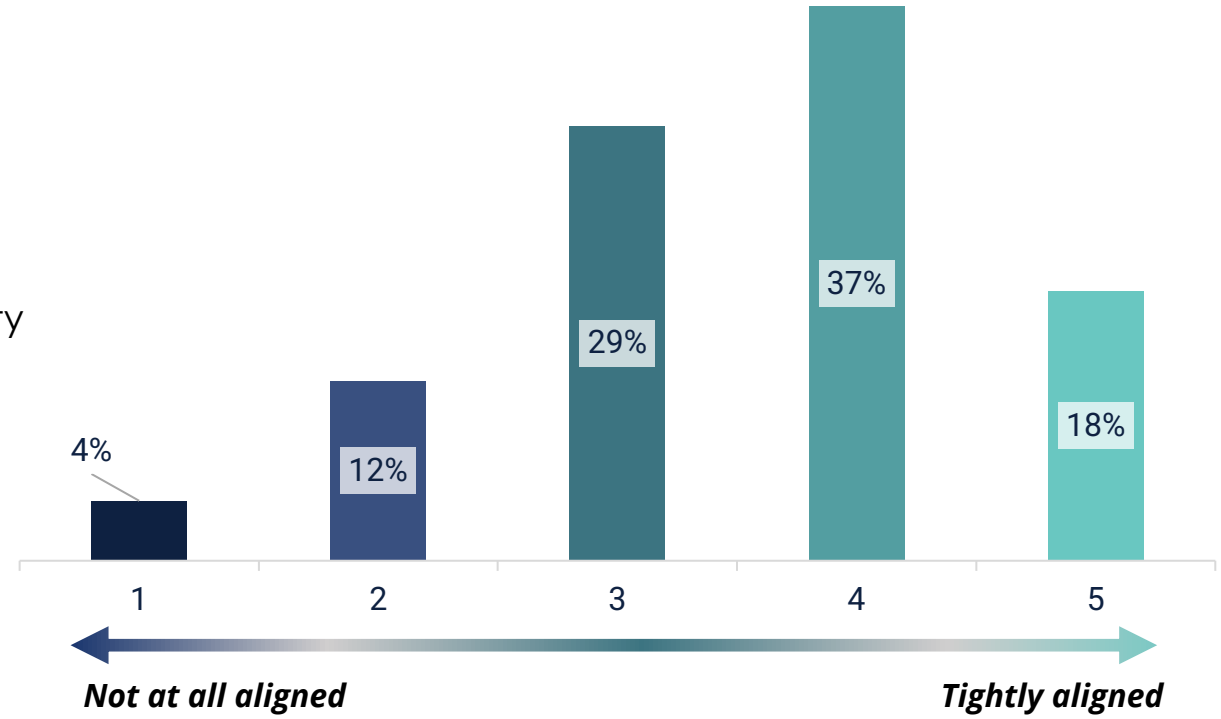
Plant operations managers are becoming more active in security response and recovery planning.

How closely aligned are your operations team and IT teams in securing your OT?

(Rate 1 to 5: 1 = 1 = Not at all aligned, 5 = Tightly aligned)

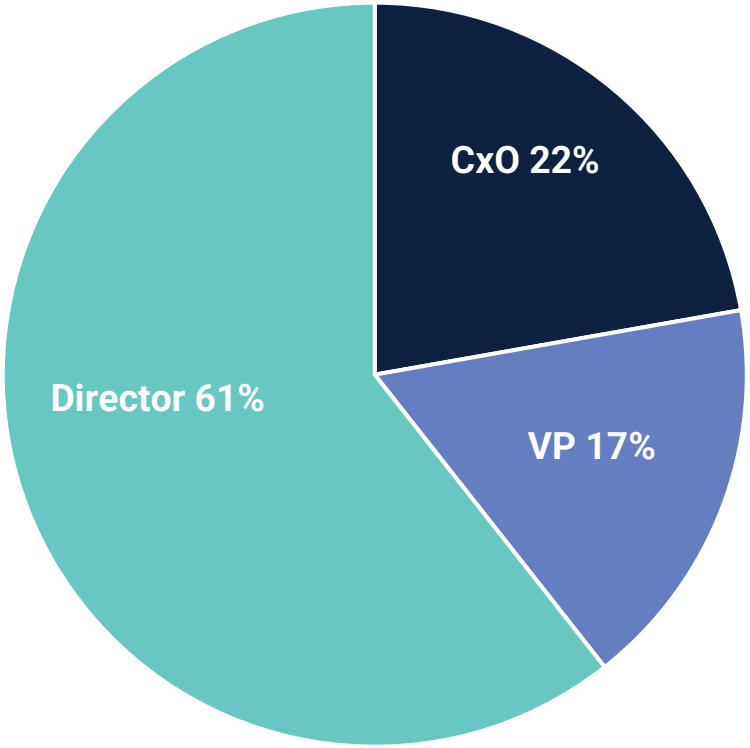
Fortunately, 55% of respondents have good alignment between the ops and IT teams for OT security.

On the flip side, 45% of teams have an opportunity to improve synching their teams.



JOB LEVEL

All respondents to this survey hold executive or director-level positions in their organization.



About the Company

ServiceNow offers an operational technology management solution that provides a complete and contextual view of OT systems, connecting them to digital workflows so you can assess, prioritize, and respond to events and threats.

Learn more at servicenow.com