NOKIA

5G Managed Security Survey 2022

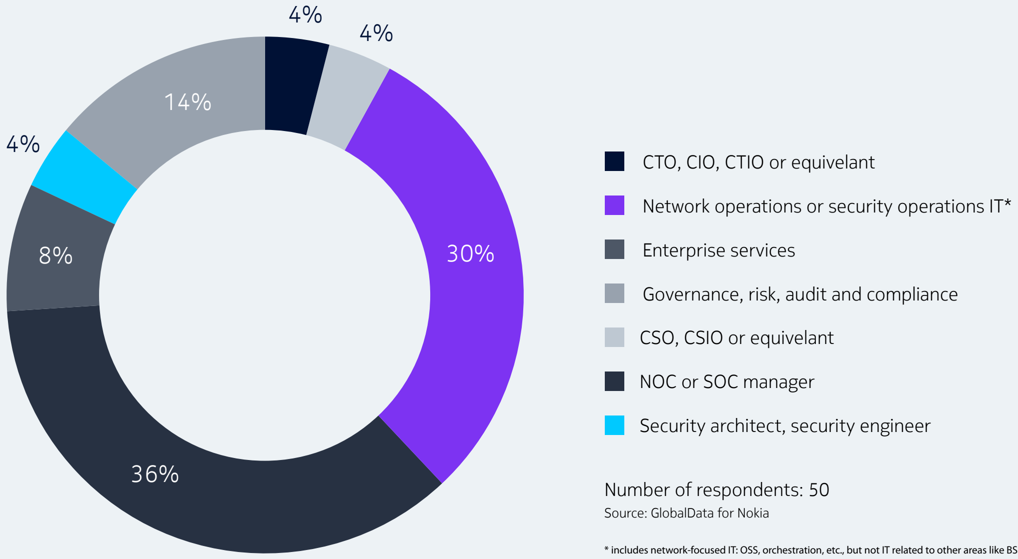
The current landscape and a forward-looking analysis

Survey description

Nokia commissioned GlobalData to conduct research into the current and future 5G security landscape and the managed security services market. Online surveys and 4 in-depth interviews were conducted in Spring 2022 and consists of 50 CSP respondents spread equally among APAC, LATAM, North America, Europe, and MEA. Included are 39 respondents from mobile network operators and 11 from group offices.

The research results includes a compilation and analysis of their responses.

Respondents by functional area



Number of respondents: 50

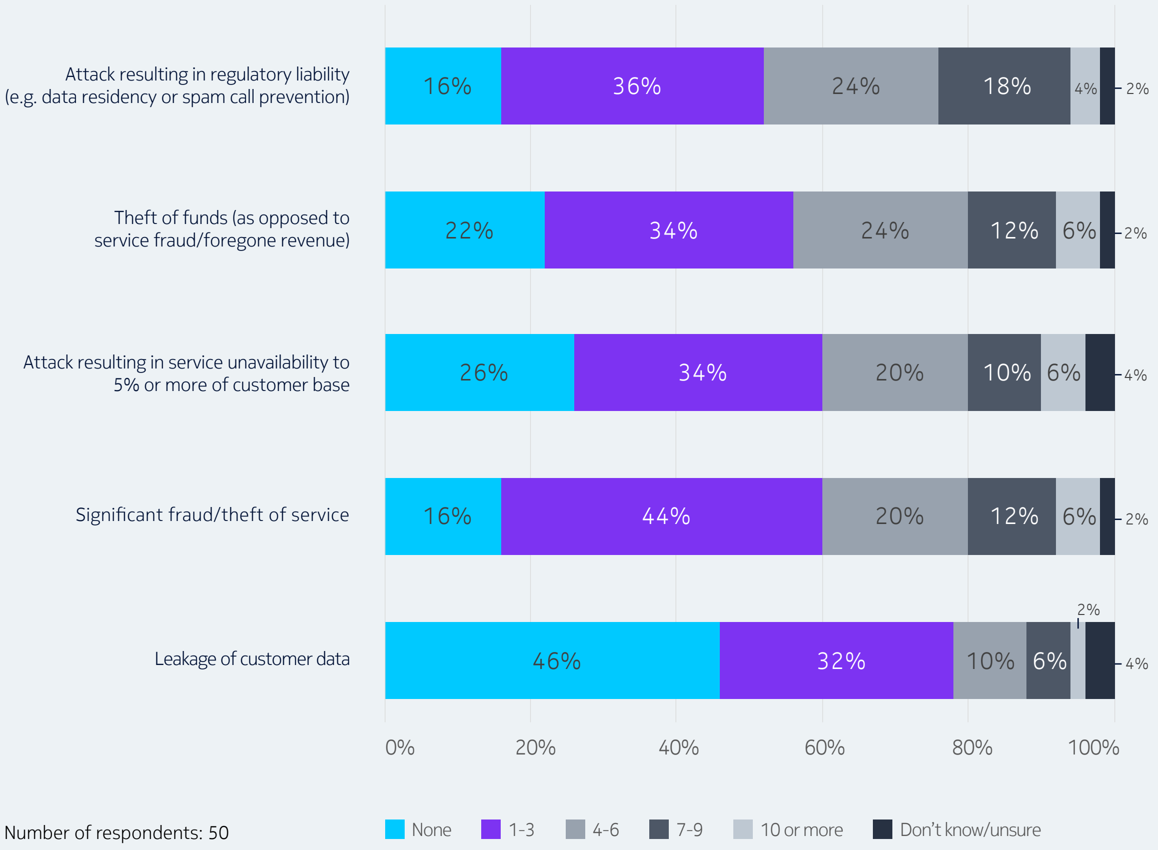
Source: GlobalData for Nokia

* includes network-focused IT: OSS, orchestration, etc., but not IT related to other areas like BSS or corporate functions

Breaches are the rule, not the exception

- In almost every category, the overwhelming majority has experienced at least one breach in the last twelve months
- At least 1/3 of respondents report 8 or more breaches in a single category
- Based on the responses, CSPs are in a constant struggle as cyber threats evolve

Number of breaches of the following types your company has experienced in the last 12 months



Number of respondents: 50

Source: GlobalData for Nokia

64%

of CSP respondents say that their teams spend over **30% of their time on automatable tasks.**

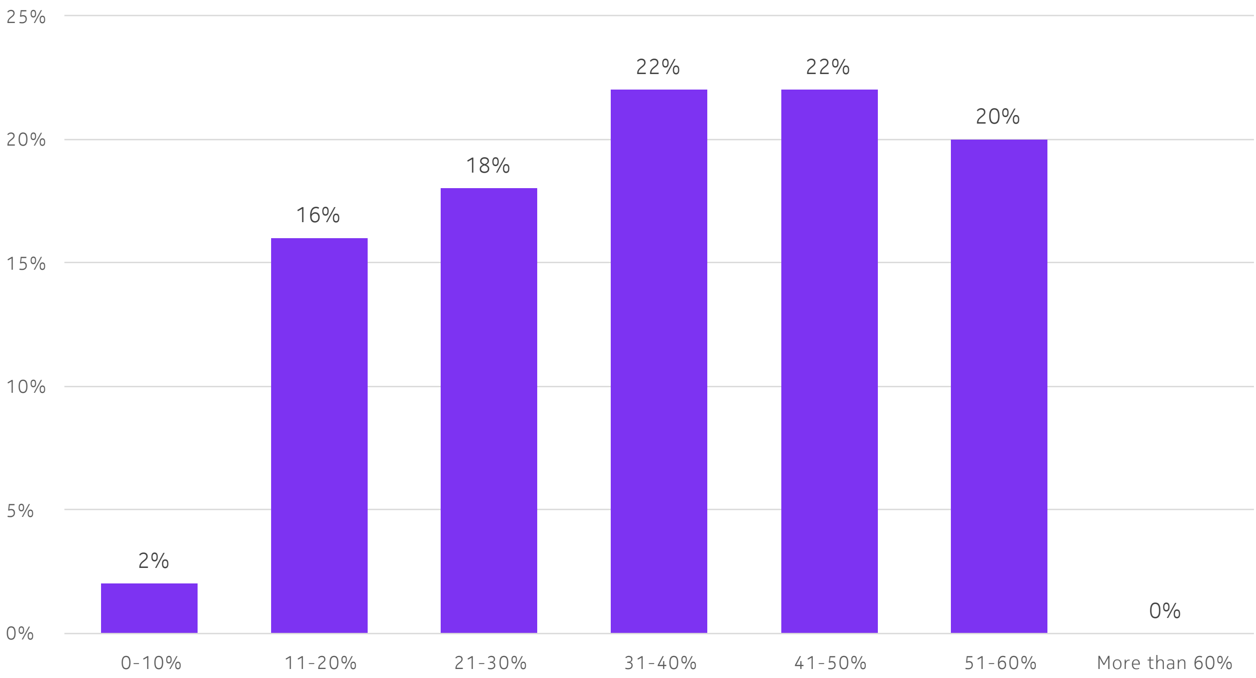
42%

of respondents spend over **40% of their time on these tasks.**

Given the shortage of security specialists, automation should be a key priority for every CSP.

Security teams spend huge amounts of time on manual tasks

Percentage of time that your company's security teams spend on vulnerability and threat management tasks that could be automated



Number of respondents: 50

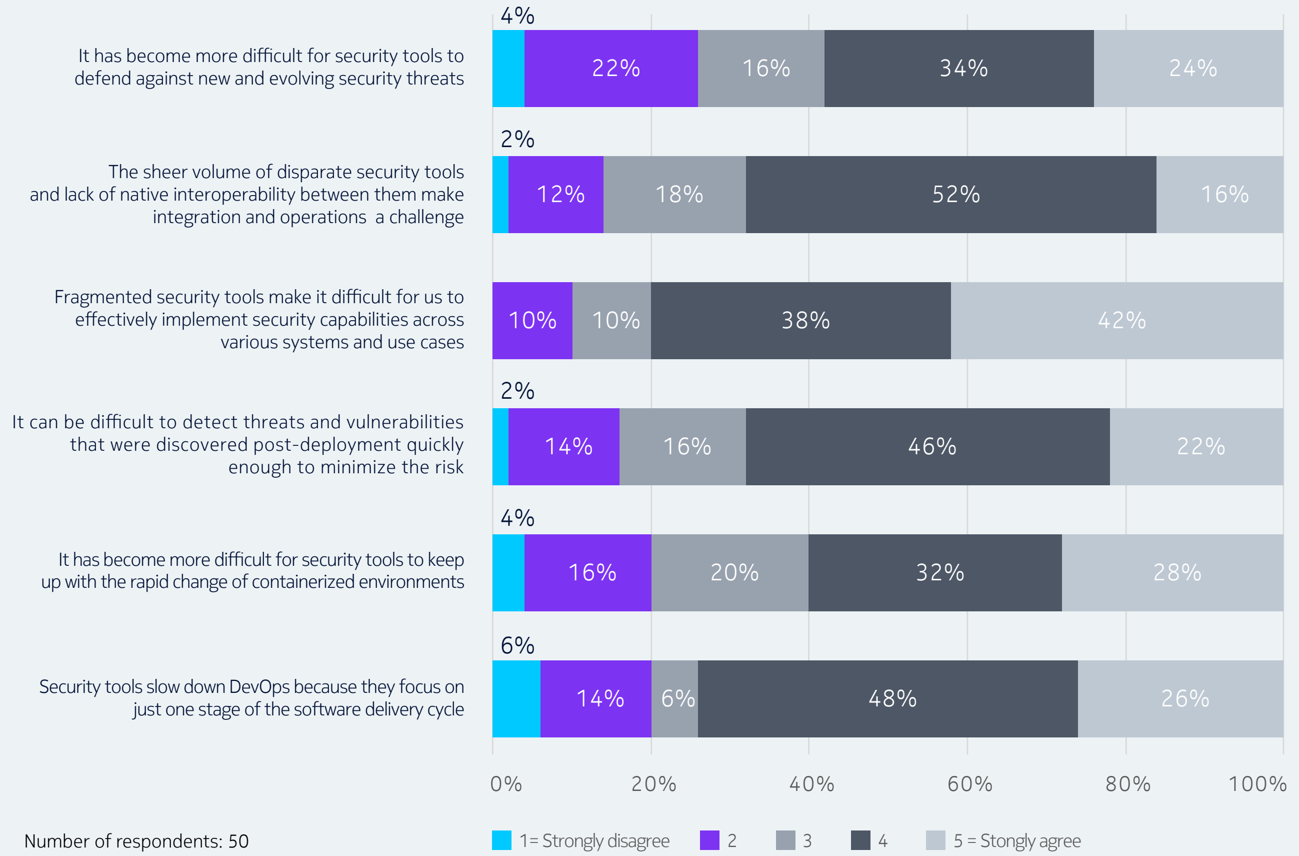
Source: GlobalData for Nokia

Why? Fragmentation is a huge issue

“No matter where the hole is, the boat is going to sink.”

North American Tier One

What are the main challenges with existing security tools and approaches in security operations? To what extent do you agree with each of the following statements?



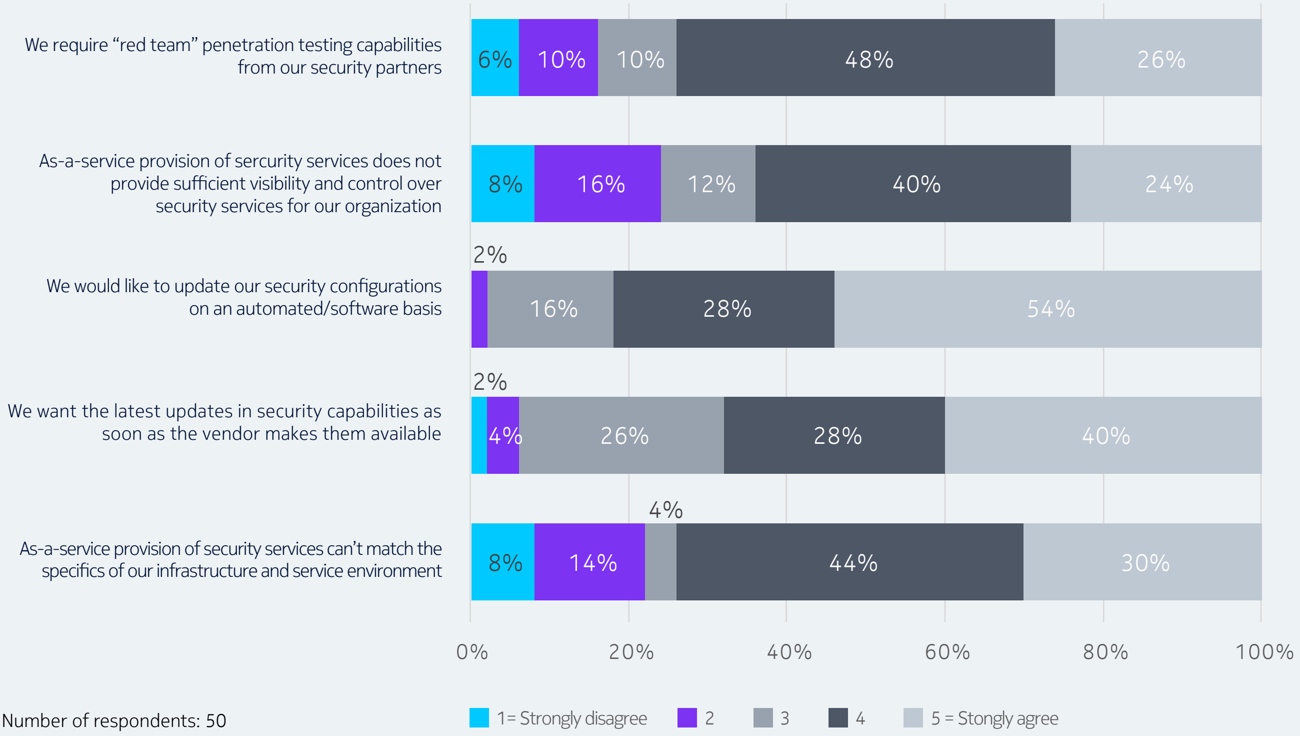
Number of respondents: 50

Source: GlobalData for Nokia

CSPs want benefits of aaS, but doubt that it meets their needs

- Strong desire for automation and frequent updates
- But: CSPs think their environments are too complicated and believe aaS doesn’t give enough control and visibility
- CSP respondents believe red team requirements will grow but finding skilled people is the challenge

State whether you agree or disagree with the following statements

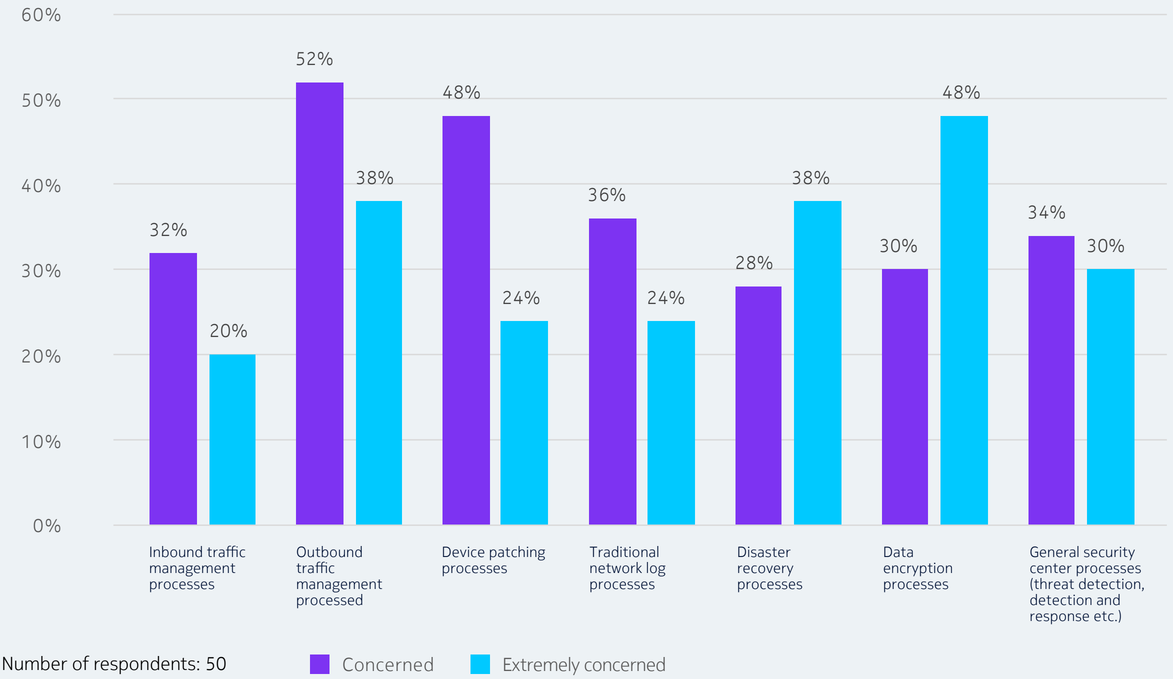


Number of respondents: 50

Source: GlobalData for Nokia

CSPs are looking for security assurance in their 5G operations especially for ransomeware

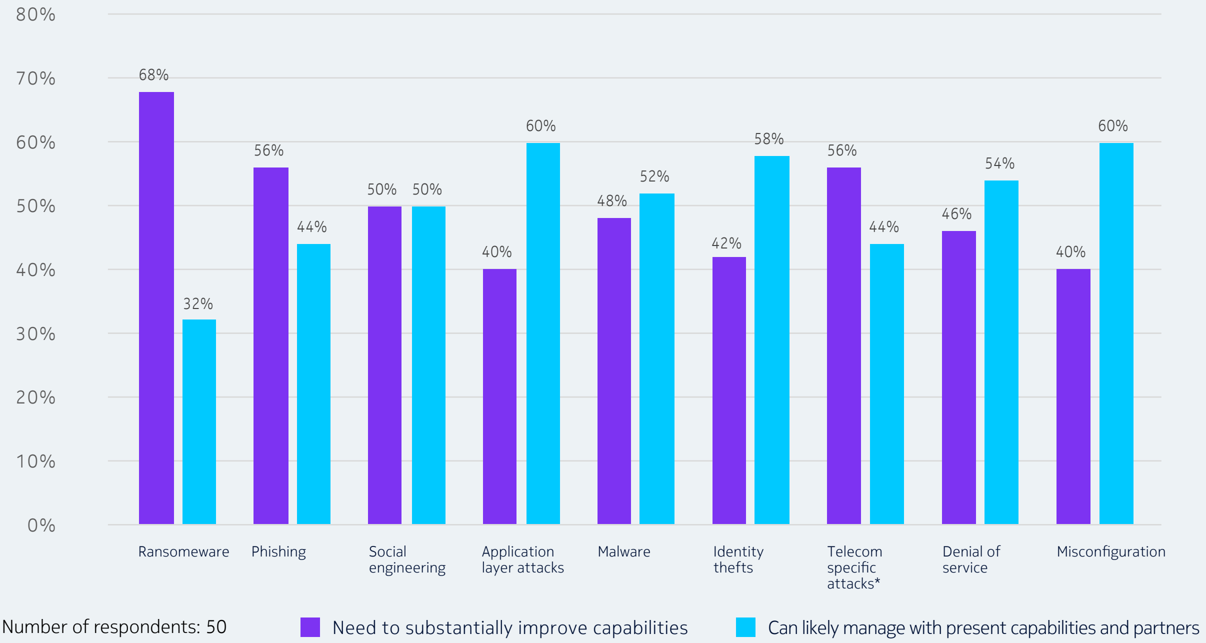
Are you concerned about weaknesses in the following processes negatively impacting the overall performance of your security assurance?



Number of respondents: 50

Source: GlobalData for Nokia

Does your company need to substantially improve its capabilities for 5G operations, or are your present capabilities and partner relationships likely sufficient to manage the threat?



Number of respondents: 50

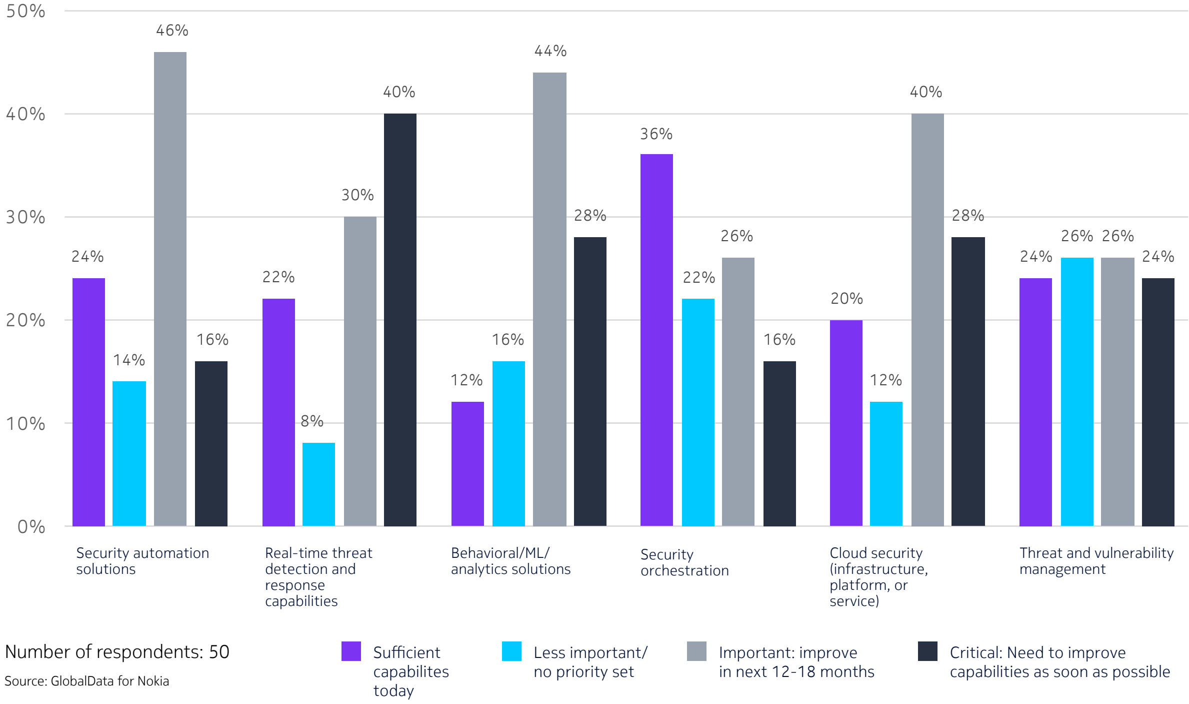
Source: GlobalData for Nokia

*Like illegal call redirection, interception, messaging attacks, etc.

Threat detection and response is an immediate need for CSPs

40% of CSP respondents need help with detection and response right now.

70% need help now or in the near future.

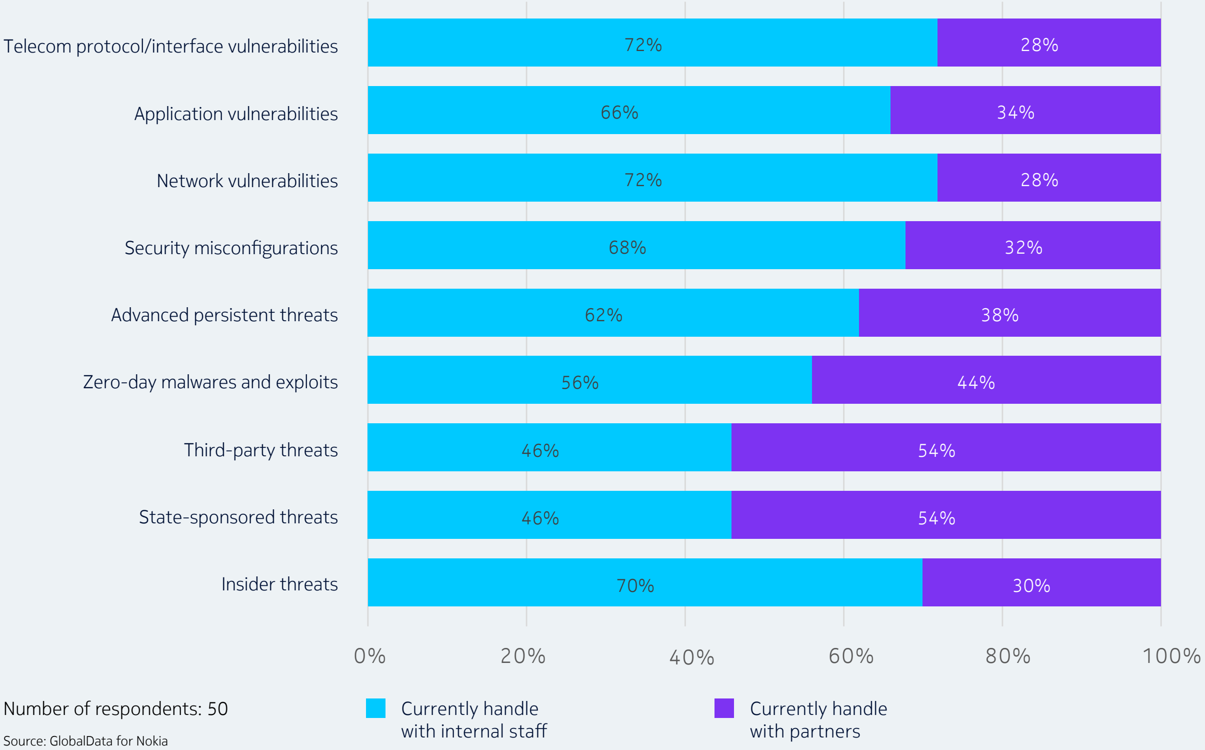


Number of respondents: 50

Source: GlobalData for Nokia

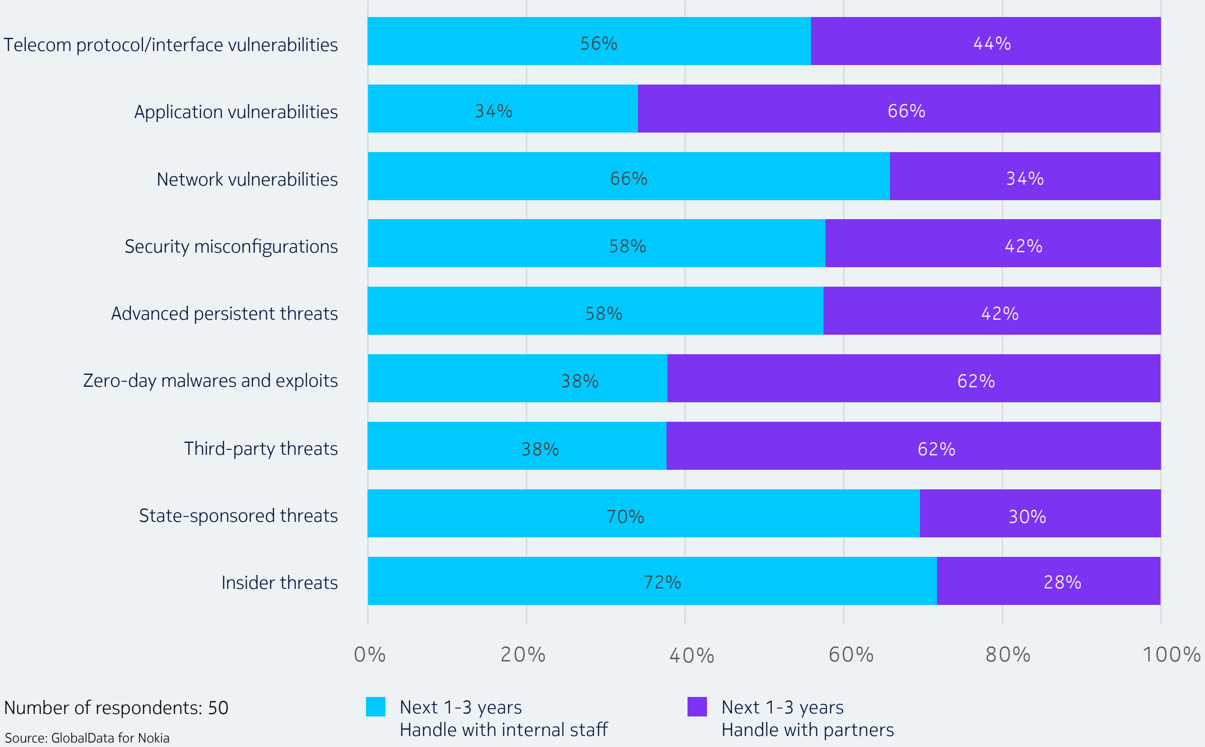
CSPs will grow security partner relationships in the next three years

For each of the security challenges, are you more likely to handle it with internal staff or through partners, both currently and over the next 1-3 years?



Number of respondents: 50

Source: GlobalData for Nokia

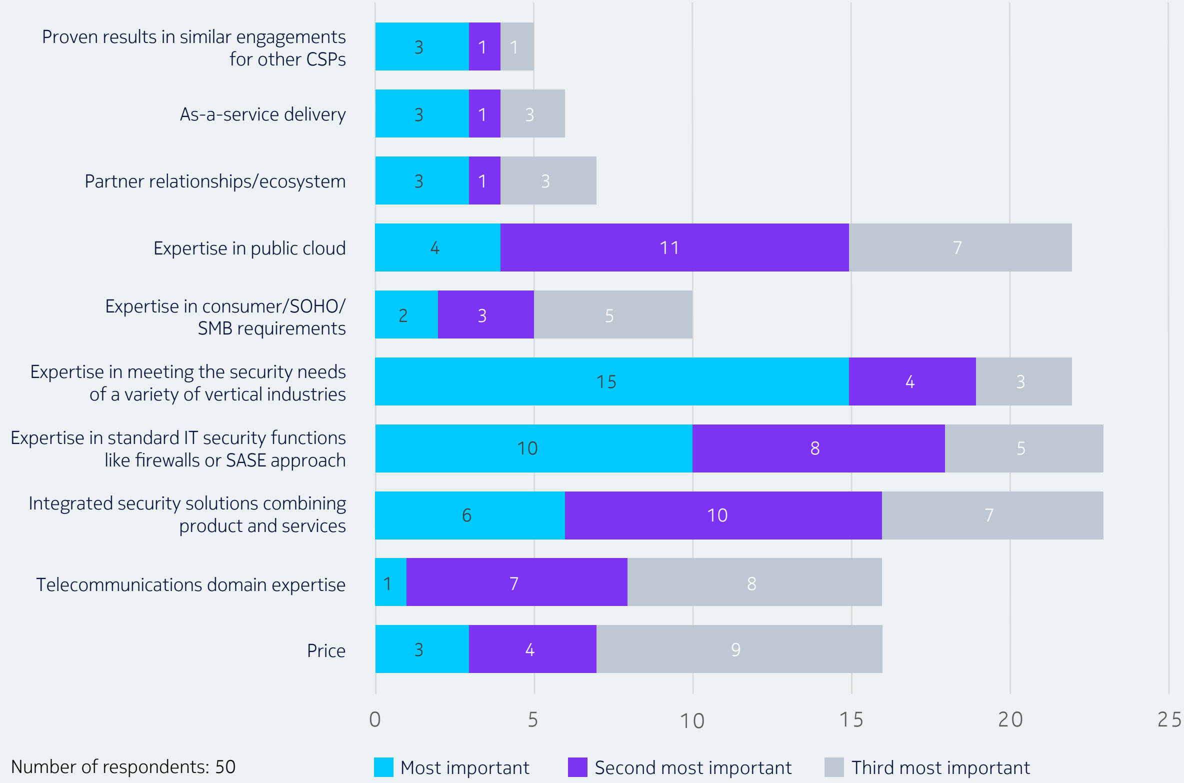


Number of respondents: 50

Source: GlobalData for Nokia

CSPs are looking for a managed security services partner with deep expertise in public and hybrid cloud

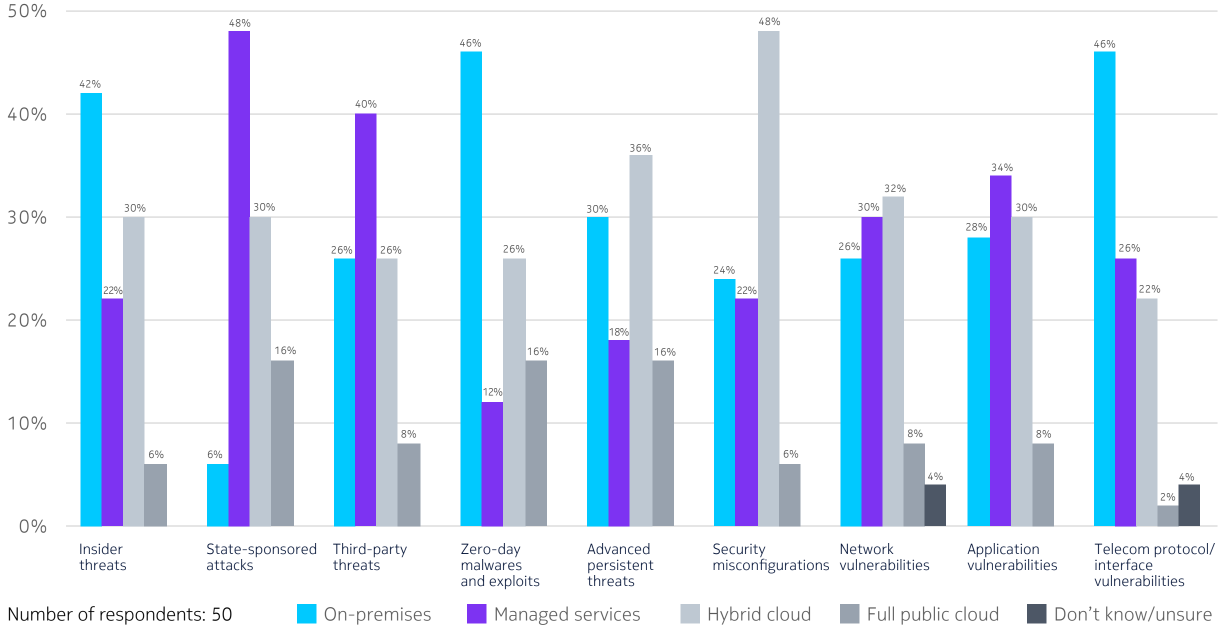
Rank the three most important characteristics for you when selecting a managed security services partner.



Number of respondents: 50

Source: GlobalData for Nokia

Would you rather have your security requirements managed on premises, via managed services, via a hybrid private/public cloud solution, or fully from the public cloud?

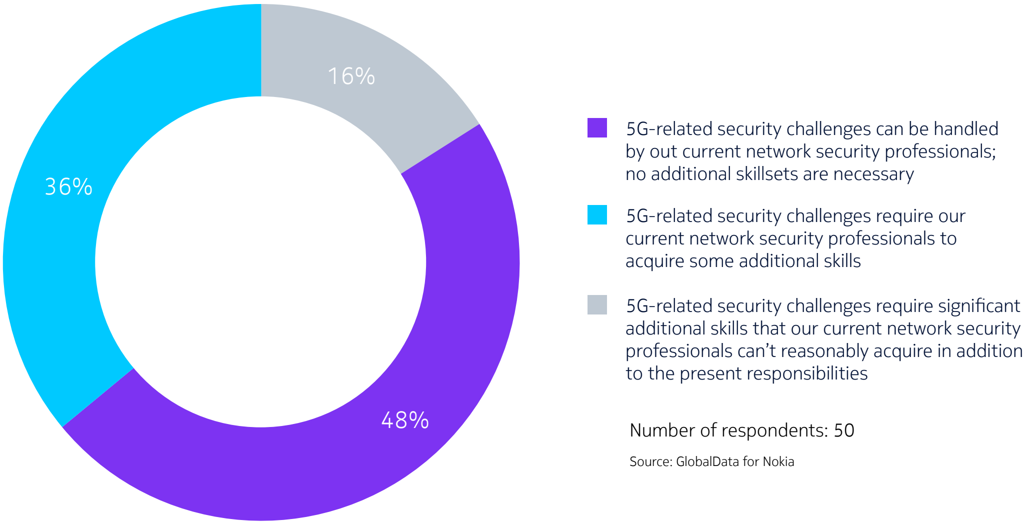


Number of respondents: 50

Source: GlobalData for Nokia

CSPs believe current network security professionals will need to acquire additional skills for 5G

Do you believe that 5G will significantly challenge your current network security staff?



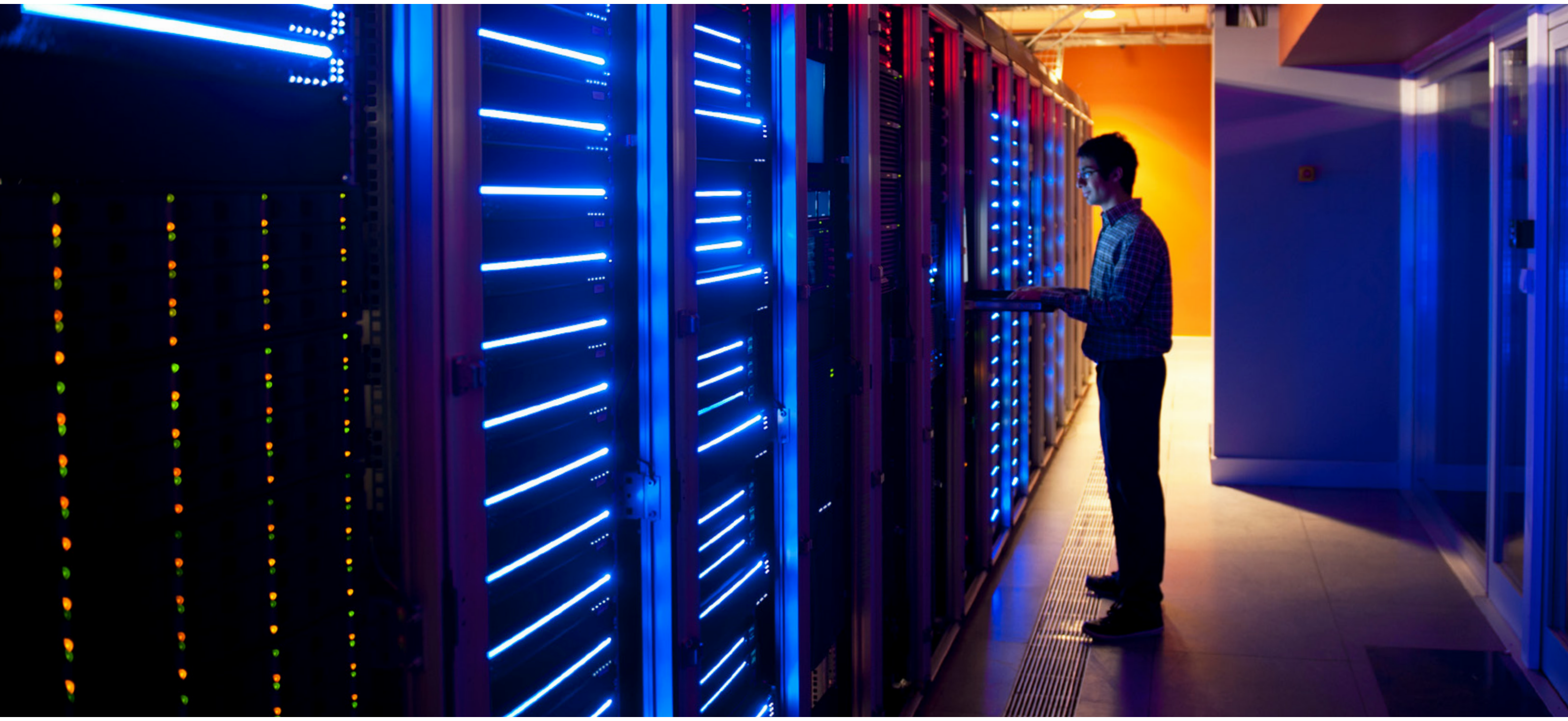
🟪 5G-related security challenges can be handled by out current network security professionals; no additional skillsets are necessary

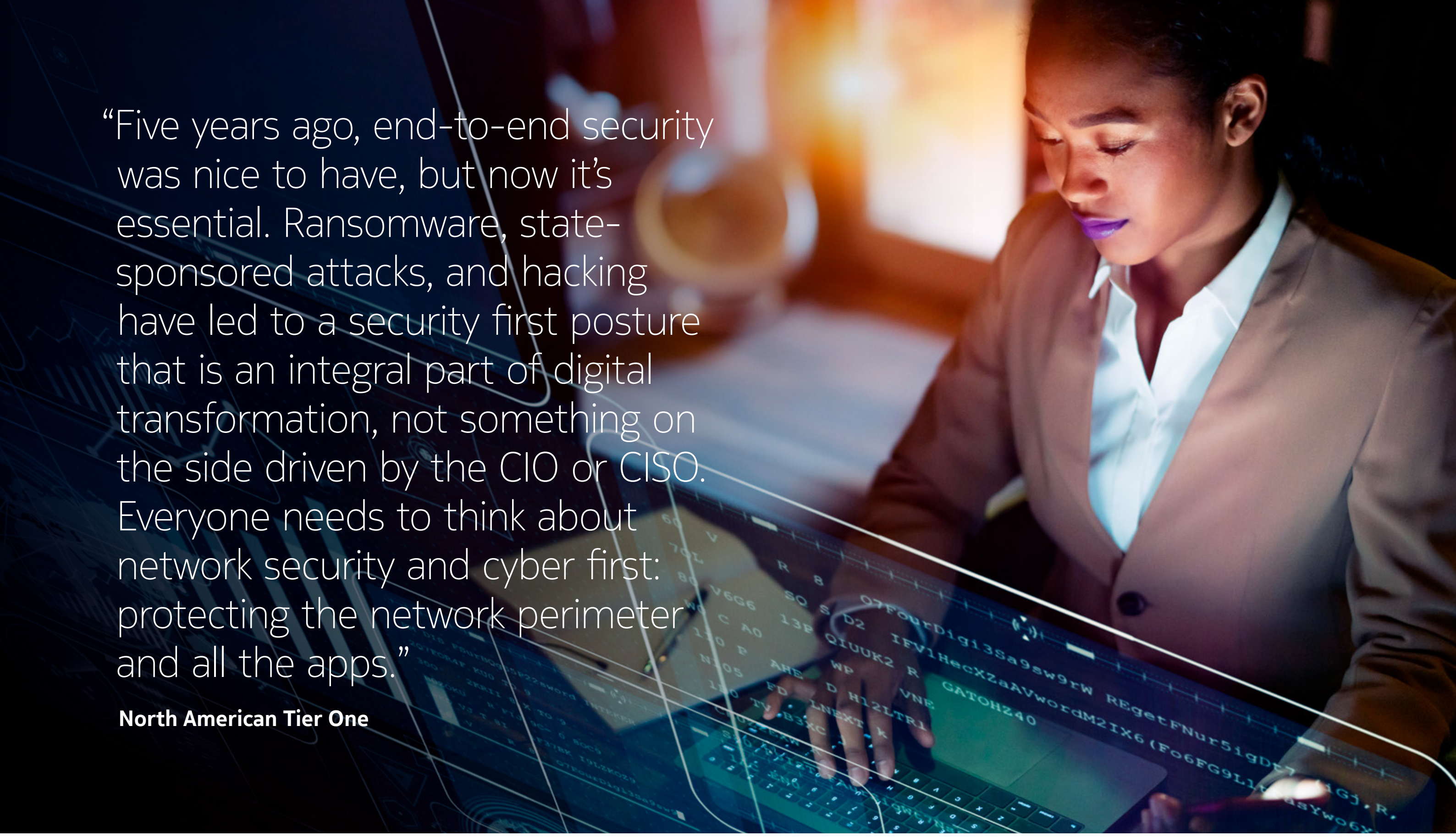
🟦 5G-related security challenges require our current network security professionals to acquire some additional skills

⬜ 5G-related security challenges require significant additional skills that our current network security professionals can’t reasonably acquire in addition to the present responsibilities

Number of respondents: 50

Source: GlobalData for Nokia





> “Five years ago, end-to-end security was nice to have, but now it’s essential. Ransomware, state-sponsored attacks, and hacking have led to a security first posture that is an integral part of digital transformation, not something on the side driven by the CIO or CISO. Everyone needs to think about network security and cyber first: protecting the network perimeter and all the apps.”
>
> **North American Tier One**

Summary

The 5G threat landscape is constantly evolving and cyber threats are becoming more sophisticated causing CSPs to struggle to keep up with the abundance of changes and attacks. It’s a matter of when a breach will occur so automation is key for CSPs who are spending too much time on manual tasks which will increase the efficiency of their security teams. Fragmented security tools and lack of automation has made it challenging for CSPs to quickly defend and respond to threats. As CSPs migrate to 5G SA to offer more value-added services for customers, they will require help from partners for 5G security including for Managed Security Services (MSS).

About Nokia

We create technology that helps the world act together.

As a trusted partner for critical networks, we are committed to innovation and technology leadership across mobile, fixed and cloud networks. We create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Adhering to the highest standards of integrity and security, we help build the capabilities needed for a more productive, sustainable and inclusive world.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2022 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID212741 (October)