ncc group

FOX IT
part of ncc group

Cyber Threat Intelligence Report

Review of December 2025

Contents

Section 1
Executive Summary

Ransomware attacks increased to 783 recorded listings in December 2025. This uptick aligns with the observed recurring rise in activity during the holiday period, when staffing levels are reduced. The increase is also driven in part by resurgent LockBit 5.0 activity, which has repositioned the group among the top three most prolific threat actors this month. Qilin remains the most active ransomware group, accounting for 22% of recorded listings.

Beyond the numbers, this month's Ransomware Spotlight examines the use of insiders by ransomware groups, citing reports of operators approaching employees to assist in malicious activities in exchange for a share of the payment. This trend is likely to raise heightened concern amid growing financial pressures.

For our Geopolitical Developments, this monthly pulse highlights Ukraine's expanding strikes on Russian assets, the US-Venezuela tanker seizure and subsequent retaliatory cyber activity, and the EU's major Ukraine funding decision. These developments elevate geopolitical tensions, heighten the risk of cyber-espionage, and influence operations.

The December Emerging Cyber Security Trend section examines the growing risk of authorisation sprawl, defined as the unmanaged and excessive permissions, roles, and access rights across multiple environments. Threat actors are increasingly exploiting these legitimate access paths to evade security controls and conduct malicious activities.

Section 2

Ransomware Statistics: December 2025

13%

Global ransomware attacks increased by 13% in December 2025

29%

Industrials accounted for 29% of ransomware attacks in December 2025

22%

Qilin was responsible for 22% of attacks in December 2025

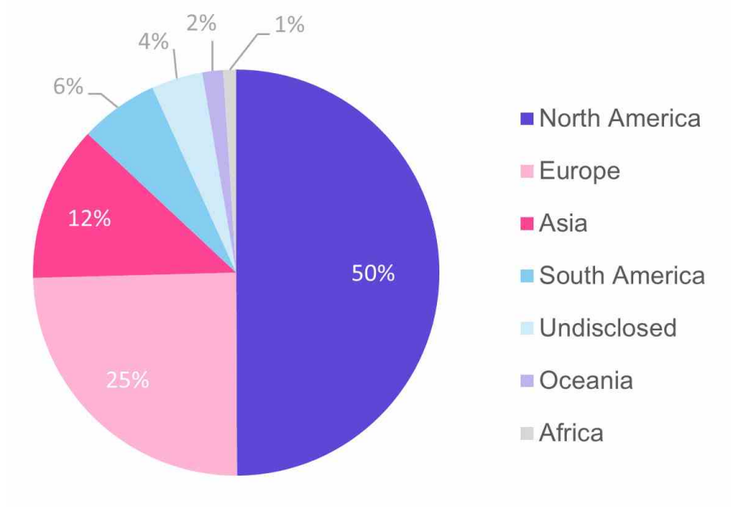


Figure 1 Ransomware Attacks by Region – December 2025

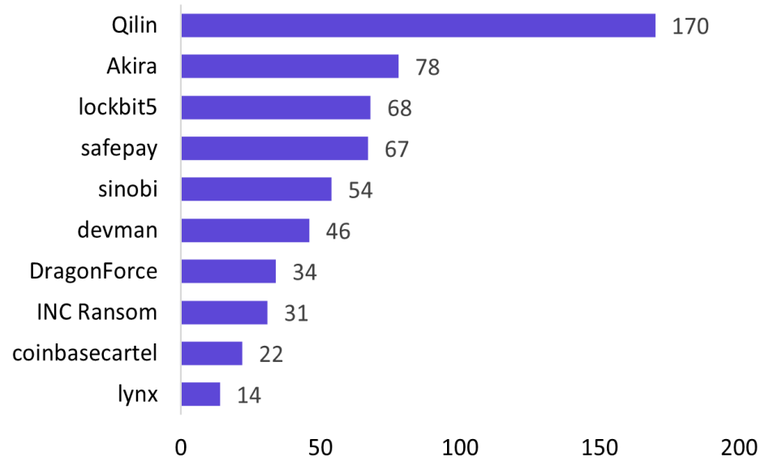


Figure 2 Top Threat Actors – December 2025

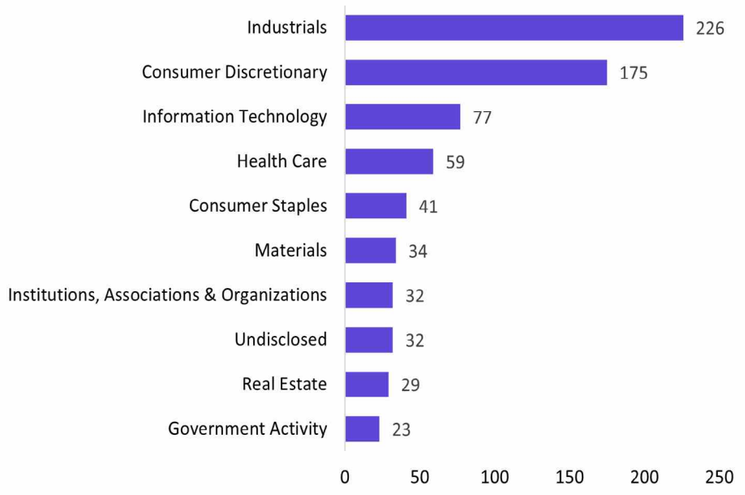


Figure 3 Top Targeted Sectors – December 2025

Key Events

13/12/25

Pierce County Library System

A cyberattack by INC Ransom group on the Pierce County Library System exposed personal data and sensitive employee details of over 340,000 people.

15/12/25

Askul

A ransomware attack by RansomHouse on Japanese e-commerce firm Askul resulted in the theft of about 740,000 customer, partner, and employee records, and disrupted order and shipping operations.

22/12/25

Romanian National Water Agency

A ransomware attack shut down about 1,000 IT systems at Romania's national water agency, forcing staff to use phones and radios, though water service was unaffected.

NCC Service

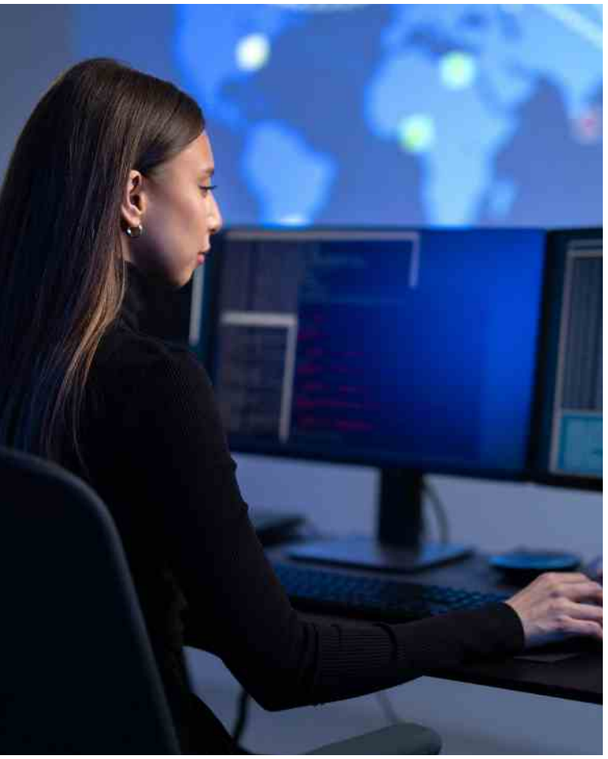
NCC Group can support you to mitigate against the ransomware threat. Please see our contact details at the end of this report should you require assistance.

Section 3
Ransomware Spotlight

Introduction and Overview

On 29 December 2025, two cyber security professionals, an incident response manager and a ransomware negotiator pleaded guilty to collaborating with the ALPHV/BlackCat Ransomware-as-a-Service (RaaS) operation in multiple attacks targeting US-based companies.[1]

In separate statements, the former employers of the accused emphasised that their activities occurred outside company infrastructure, with no impact on customers. Both were terminated following the discovery of their activities. Such incidents highlight how ransomware gangs may leverage employed cyber professionals as skilled affiliates with the promise of large commissions upon successful payment.



Two Cyber Security Professionals Plead Guilty to Working with RaaS Gangs

A court in Florida accepted the guilty pleas of Ryan Goldberg, a ransomware negotiator at Sygnia, and Kevin Martin, an incident response manager at DigitalMint. Both collaborated with BlackCat/ALPHV in a series of ransomware attacks targeting five US companies between April and December 2023.[2] The targets included organisations in healthcare, manufacturing, pharmaceuticals, and engineering. Indictments were filed in October with guilty pleas to obstruct commerce through extortion entered in December 2025.In November, Sygnia released a public statement indicating that Goldberg was terminated upon discovery of the allegations and their activities were unrelated to internal clients and infrastructure. DigitalMint also clarified that Martin's attacks occurred outside the company's infrastructure and no client data was accessed or compromised.

This may be one of the first documented cases of cyber professionals using their technical knowledge to support RaaS operations. Financial incentives such as a 20% commission from the operator is the likely motivation behind their activities.[3] External factors such as the rising cost of living and dissatisfaction with their current pay could also be viewed as drivers of collusion.

RaaS Gangs Using Insider Threats in 2025

In September 2025, the BBC reported that the Medusa ransomware gang offered one of their employees 15% of a future ransomware payment for access to their infrastructure. Medusa requested login details and security codes that would be used to extort their organisation. The threat actor then attempted to entice the employee by providing an increased commission of 25%.[4] Reach out managers used by RaaS gangs have been observed to approach privileged employees working within organisations and trusted third parties who provide critical business services.

In a broader context, insider threat risks have been increasing in recent years. Research by Ponemon found that insider security incidents had a potential impact of $17.4 million in 2024, an increase from $16.2 million in 2023.

In response, organisations have begun doubling their budget allocations for insider risk management programmes.[5] As organisations build their defences against ransomware, insider recruitment can provide several benefits from an attacker's perspective. Credentials from insiders can allow MFA, endpoint, and intrusion detection to be bypassed under the guise of legitimate user behaviour. Attackers can exploit employee grievances by attempting to be problem solvers through lucrative commissions.

Implications of Insider Threats on the Ransomware Landscape

Insider incidents related to ransomware gangs have been prevalent for years. LockBit 2.0 pioneered the approach by promising 'millions of dollars' to corporate insiders. In 2025, DBIR report found that 18% of their recorded incidents originated from an internal threat.[6]

Some sectors like Education Services (38%) and Real Estate (36%) organisations have higher than average numbers for insider threat incidents.[7] These developments potentially indicate a higher incidence of insider threat factors such as unmanaged access, employee disgruntlement, and lack of monitoring.

Organisations may need to begin evaluating their own internal insider threat management programme. The presence of increasing general insider, risk in combination with strong financial incentives, is a potential indicator that many organisations may be at risk.

Mitigations and Recommendations

Insider threats require mitigations that can change depending on an organisation's context. Organisations may choose to implement access controls and the implementation of the principle of least privilege as well as user behaviour monitoring and data loss prevention. Lastly, organisations should focus on building a strong security culture of reporting and prevention. Many guidelines highlight these key components are essential to mitigating insider risk. Publicly available guidelines such as the CISA Insider Threat Mitigation Guide or the NCSC Insider Threat Guidance can also be used to great effect.[8]

Final Thoughts

Humans as attack vectors have always been a prominent cyber risk. However, insider risk is likely to become a more prominent concern due to the number of factors that can make human targets vulnerable. Employment conditions, financial, and personal struggles can easily drive individuals within organisations to engage in malicious activity. These drivers are difficult to detect and mitigate, forcing many organisations to absorb the risk. Upon internal assessment, organisations that are at particular risk from insiders may have to consider planning and implementing mitigations for a dynamic threat. Insiders also allow threat actors to take the path of least resistance by bypassing core technical challenges.

Section 4
Geopolitical Developments

NCC Group's Threat Intelligence Team highlights geopolitical developments from the month which have the capacity to influence the cyber threat landscape.

10/12/25

On 10/12/25, the US seized the Venezuelan oil supertanker, the VLCC Skipper.[9] The vessel has been under US Treasury sanctions since 2022 for its alleged role in an oil-smuggling network financing Iran's Revolutionary Guard and Hezbollah.[10] On 16/12/25 US President Trump ordered a complete blockade of all sanctioned oil tankers entering or leaving Venezuela and suggested Venezuela give up land, oil, and assets to the USA. Efforts to seize further sanctioned vessels were subsequently reported.[11]

Within days of the seizure, PDVSA - the Venezuelan state-owned oil and gas company which owns the Skipper - announced they had experienced a cyber-attack and publicly blamed the USA. Despite claiming operations were unaffected, media sources reported administrative systems were disrupted, forcing staff to disconnect from internal networks and halting oil cargo deliveries.[12]

Figure 4 - Map showing countries and key cities of the Black Sea area

15/12/25

On 15/12/25, Ukraine reported it had, for the first time, damaged a Russian submarine using underwater drones.[13] The vessel was docked at a Russian naval base in Novorossiysk at the time. For Ukraine, the attacks form part of a wider campaign disrupting Russia's military capabilities and oil economy through attacks on Russian vessels and infrastructure inside Russia, throughout the Black Sea and even beyond.[14,15,16,17,18,19] Russia's response included a campaign of attacks between 26-30/12/25 against multiple Ukrainian Black Sea ports.[20]

Russia and Ukraine continue to be criticised over collateral damage: vessels registered in Turkey, Panama, Slovakia, Palau and Liberia were struck in Ukrainian ports.[21] Multiple Ukrainian attacks on Russia's Black Sea oil terminal in Novorossiysk damaged export infrastructure shared by Kazakhstan and USA oil companies.[22] On 03/12/25 and 16/12/25 respectively, the Romanian and Turkish military destroyed drones approaching their airspace and national waters from the Black Sea.[23,24]

19/12/25

On 19/12/25, European Union leaders agreed to provide a €90 billion loan to Ukraine to fund their continued defence against the Russian invasion for the next 2 years.[25]

Despite earlier opposition, Russia-friendly member states Hungary, Slovakia, and the Czech Republic did not block the decision – which required unanimity to pass. Without new funding, Ukraine was projected to run out of money in the second quarter of 2026.

To date, despite continued efforts, EU leaders have been unable to identify an acceptable mechanism to use €210 billion of frozen Russian assets held by EU member state financial institutions as a source of funding for Ukraine. In the interim period, the EU has agreed to an indefinite freeze, replacing the current six-month extension by a review system.[26]

What NCC are watching

On 05/12/25 the US government published their 'National Security Strategy'.[27] Taking a less traditional format, the document articulates how US foreign policy will support stated US priority interests, underpinned by President Trump's 'America First' policy. Notable areas potentially relevant to drivers of the cyber threat landscape are highlighted below:

- Described as the 'Trump Corollary' to the Monroe Doctrine, the US seeks to be the unchallenged dominant power in the "Western Hemisphere", using military and lethal force as necessary, and protecting and developing "strategic points and resources" with regional "partners".
- Prioritisation of nation-state threats based on their ability to "become so dominant" that they "could threaten [US] interests". China is expressly referenced but also implied within the Asia section; for example, through the inclusion of the need to "end . . . grand-scale intellectual property theft and espionage", and the requirement to "work to align the actions of our allies and partners" to prevent "domination by any single competitor nation".
- Absence, or minimal reference to nation-states historically included as threats; specifically North Korea and Iran. Reference to Russia as a threat is limited to European relations, requiring "significant US diplomatic engagement". Ending the Ukraine war is described as "a core interest" in which the "Trump Administration finds itself at odds with European officials who hold unrealistic expectations".
- Clear articulation of the importance of Taiwan, and broader freedom of movement in the Indo-Pacific. A preference to deter "a conflict over Taiwan" through "preserving military overmatch" is described as "a priority".
- The Middle East is framed as an economic opportunity, particularly in the area of technology. However, core interests include ensuring freedom of movement through the Strait of Hormuz and Red Sea, and "that Israel remain secure".
- Explicit reference to the need to use private sector relationships to "help maintain surveillance of persistent threats to US networks, including critical infrastructure" and to "network defense" and "offensive cyber operations".
- In Europe, the risk of migration and political trends are stressed. Framed as a threat to European nations' abilities to contribute to US interests as stable and like-minded allies, the strategy defines the need to restore "Europe's civilizational self-confidence and Western identity". Describing the current US administration as a necessary remedy to the previous US political and foreign policy "elites", President Trump's government commits to "oppose elite-driven, anti-democratic restrictions on core liberties in Europe, the Anglosphere, and the rest of the democratic world, especially among our allies".
- Commitment "to ensure that US technology and US standards—particularly in AI, biotech, and quantum computing—drive the world forward."

Section 5

Emerging Cyber Security Trend: Authorisation Sprawl: An Emerging Identity-Driven Attack

Introduction and Overview

Authorisation sprawl is an emerging attack vector that exploits the uncontrolled growth in identities, roles, permissions, API tokens, and delegated access privileges in modern enterprise environments such as cloud and SaaS platforms.[28] Many business functions now adopt SaaS platforms such as Salesforce, GitHub, Jira, and Confluence, while IT deploys single sign-on (SSO) solutions like Okta or Microsoft Entra to manage usability and scale. As a result, a single authenticated user may gain access to dozens of cloud and SaaS systems through persistent session tokens, OAuth grants, API keys, and delegated trust relationships. These access mechanisms are often long-lived, widely scoped, and reused across environments, forming a dense web of authorisation that extends far beyond the original intent of each access decision.

Mismanaged identities remain a significant driver of cloud breaches. A report shows that 31% of cloud breaches result from excessive permissions, and identity and access issues rank among the top causes of cloud security incidents.[29] According to an industry survey, 50% of employees were found to possess excessive access privileges relative to their job functions, which fuels privilege creep and widens the attack surface over time.[30]

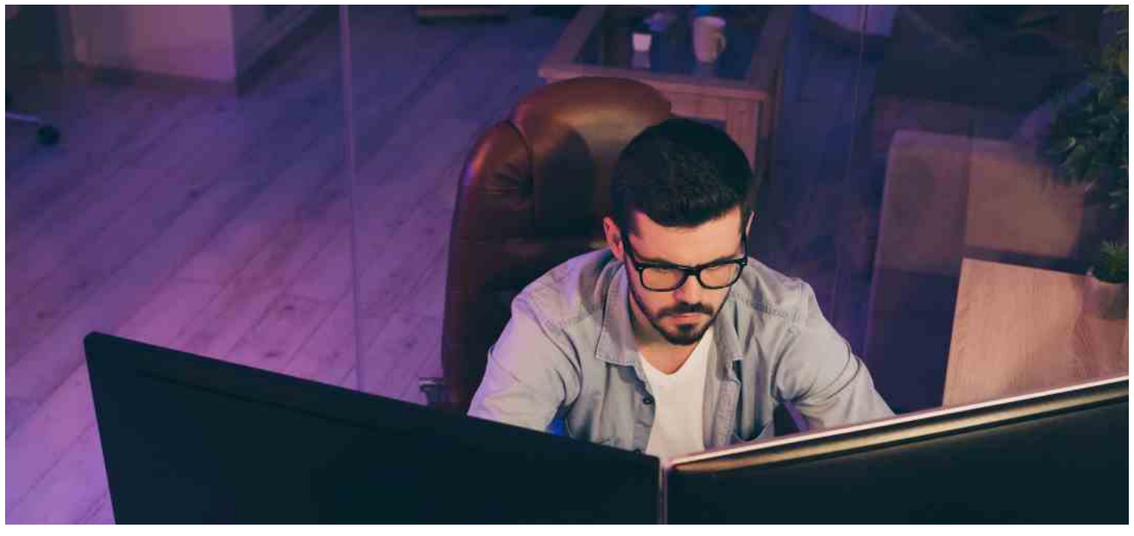
Many cybercriminal groups have actively exploited this authorisation sprawl attack patth within targeted organisations. It allows them to reuse legitimate access mechanisms to infiltrate environments and move laterally without malware deployment or alert triggers. In mid-2025, ShinyHunters launched a campaign which relied on social engineering tactics to get employees to install a malicious version of Salesforce's Data Loader tool.[31]

This granted the threat actor significant capabilities to access, query, and exfiltrate sensitive information directly from compromised Salesforce customer environments. This activity underscores the rise in trend in which threat actors are increasingly targeting IT support personnel for gaining initial access, exploiting their roles to compromise valuable enterprise data.

These figures demonstrate both the scale and speed of identity sprawl across the enterprise IT ecosystem. This is far from a niche configuration issue; it is a measurable and accelerating security risk that aligns with the broader trend where attackers increasingly exploit valid access paths rather than traditional vulnerabilities. Authorisation sprawl is an emerging attack enabler, specially in modern environments, where human and non-human identities and permissions are being mishandled. As access permissions and interconnected systems continue to expand across cloud and SaaS systems, threat actors will increasingly leverage legitimate access paths that evade traditional detections.

Mitigating authorisation sprawl requires organisations to shift their focus from authentication-centric defences to a broader governance of authorisation and entitlement usage. As attackers increasingly exploit legitimate permissions rather than bypassing controls, organisations must reduce excessive access, limit privilege duration, and improve visibility across identity-driven environments.

Enforcing the principles of least privilege across all identities, including users, service accounts, and applications, requires organisations to continuously monitor and audit access privileges, remove any unused or excessive permissions and ensure that authorisation scopes remain aligned to their operational needs.[32]



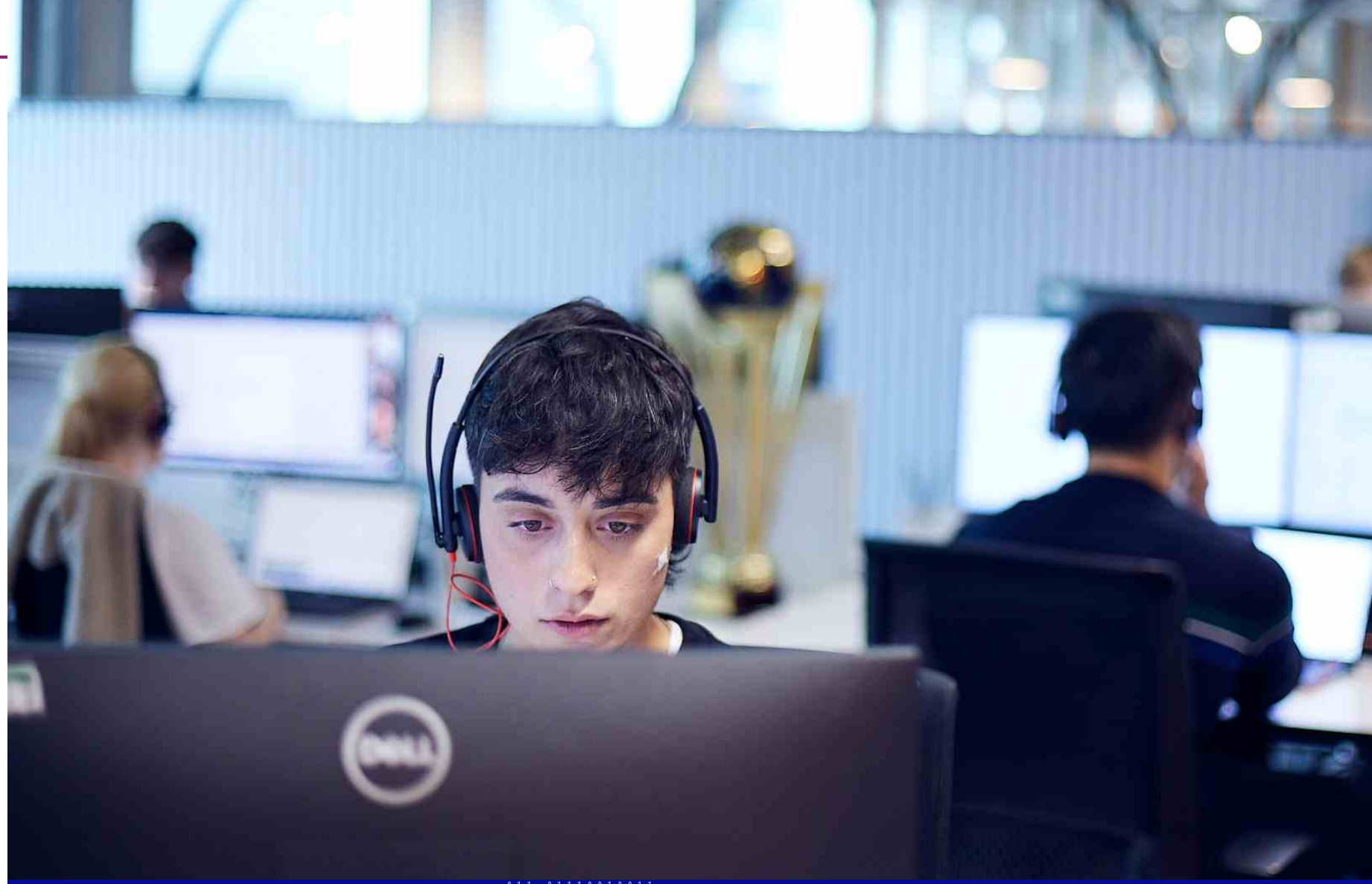
About NCC Group

“People powered, tech-enabled cyber security”

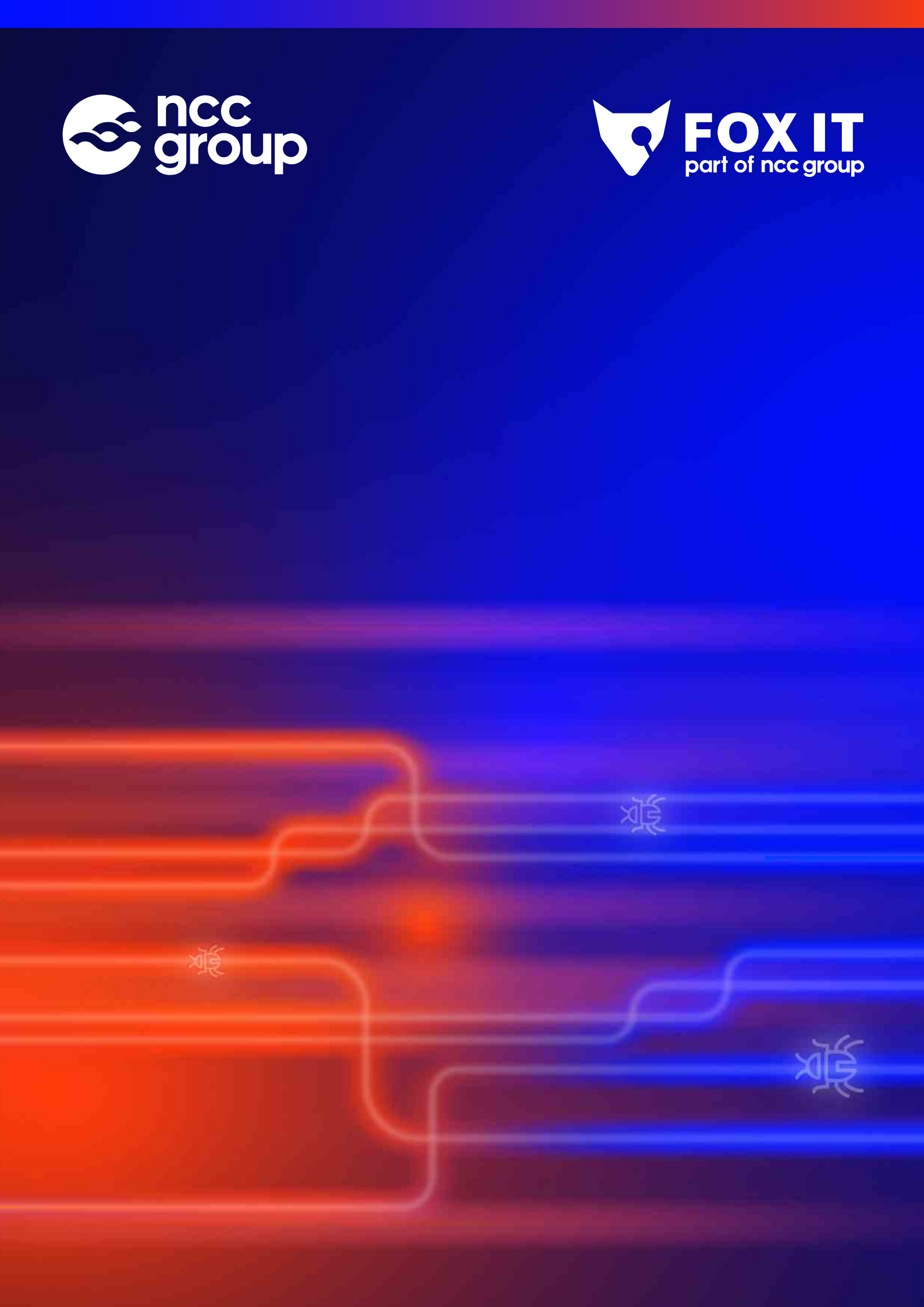
We’re a people powered, tech-enabled global cyber security and resilience company with over 2,200 colleagues around the world.

For over 25 years, we’ve been trusted by the world’s leading companies and governments to manage and deliver cyber resilience, working together to create a more secure digital future. We are proud to deliver important and groundbreaking projects for our clients.

We operate as one global business, with in-country delivery tailored to local needs and cultures, as well as a global delivery team to respond quickly to our clients’ challenges. Headquartered in the UK, we also have a significant market presence in Europe, North America and APAC.



+44 (0)161 209 5200
response@nccgroup.com
www.nccgroup.com


ncc group
FOX IT
part of ncc group