# Cyber Threat Intelligence Webinar

January 2026

TLP:CLEAR

# Coming up today….

- **How exciting was 2025?**
- **Accelerating Threats in the New Year**
- **Geopolitical overview and outlook**


As a reminder:

- The session is recorded and will be available here > https://vimeo.com/showcase/11639190
- A copy of the slides will be shared via email after the webinar
- Please share your questions and comments using the Q&A Function



TLP:CLEAR

# But first…

# Let’s reflect with a poll or two

Risk emerges when capability and intent meet opportunity.

2025 was a year of expanding opportunity.

# How Exciting was 2025?

## Most Impactful incidents were not all driven by new threats

Many of the major incidents we saw last year relied on techniques that have been around for years: credential theft, social engineering, abuse of trusted access.

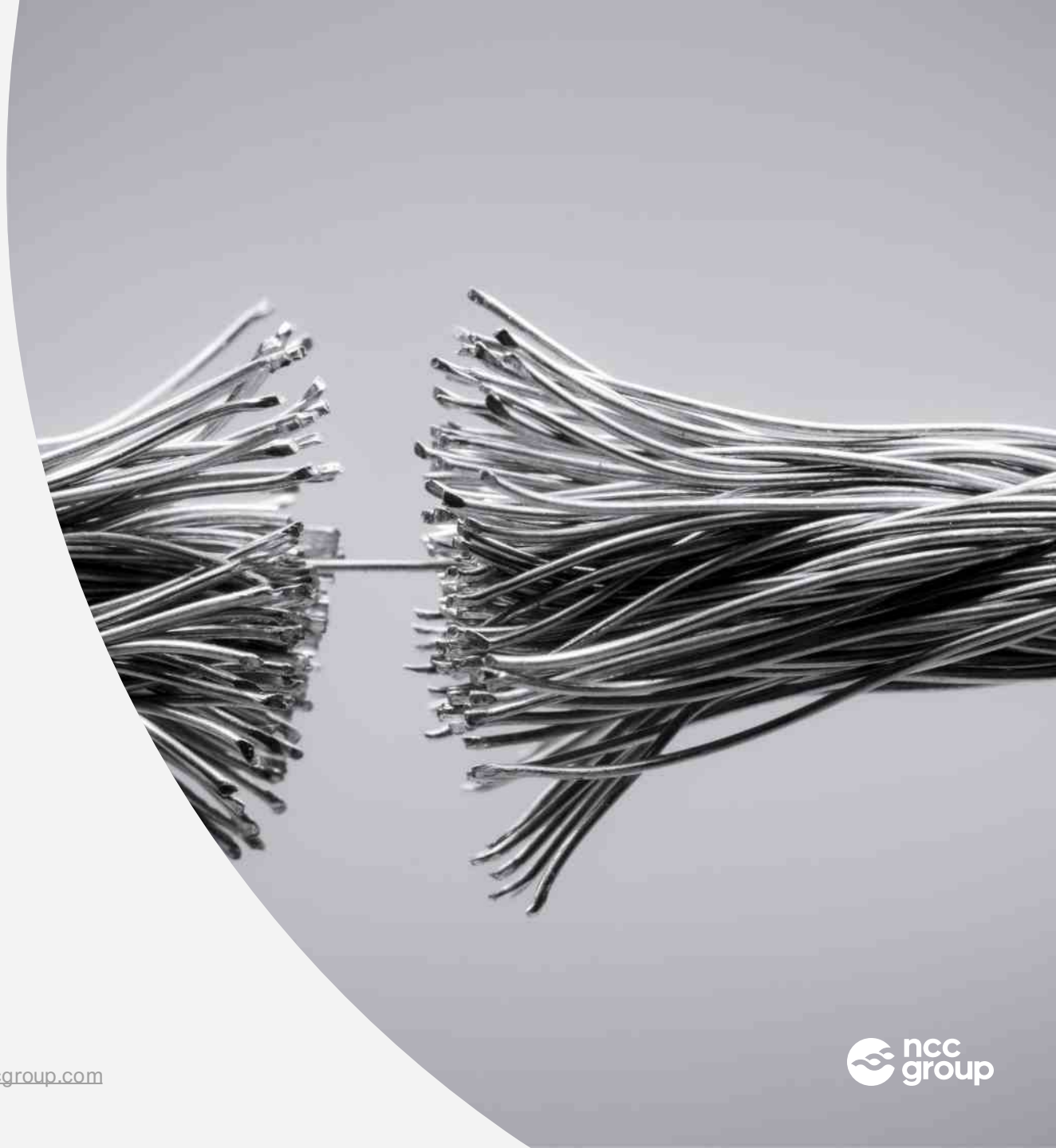
The difference wasn’t innovation; it was how much damage those techniques could now cause in complex, interconnected organisations.

# How Exciting was 2025?

## Familiar weaknesses caused outsized harm at scale

Small control gaps didn’t stay small.

A single compromised identity could move laterally across cloud services, SaaS platforms, and third-party integrations in ways that weren’t fully understood internally.



# How Exciting was 2025?

## Attackers succeeded by understanding organisations

Attackers spent time learning how approvals worked, how access was granted, and which processes were trusted by default.

They exploited routine behaviour rather than technical blind spots.

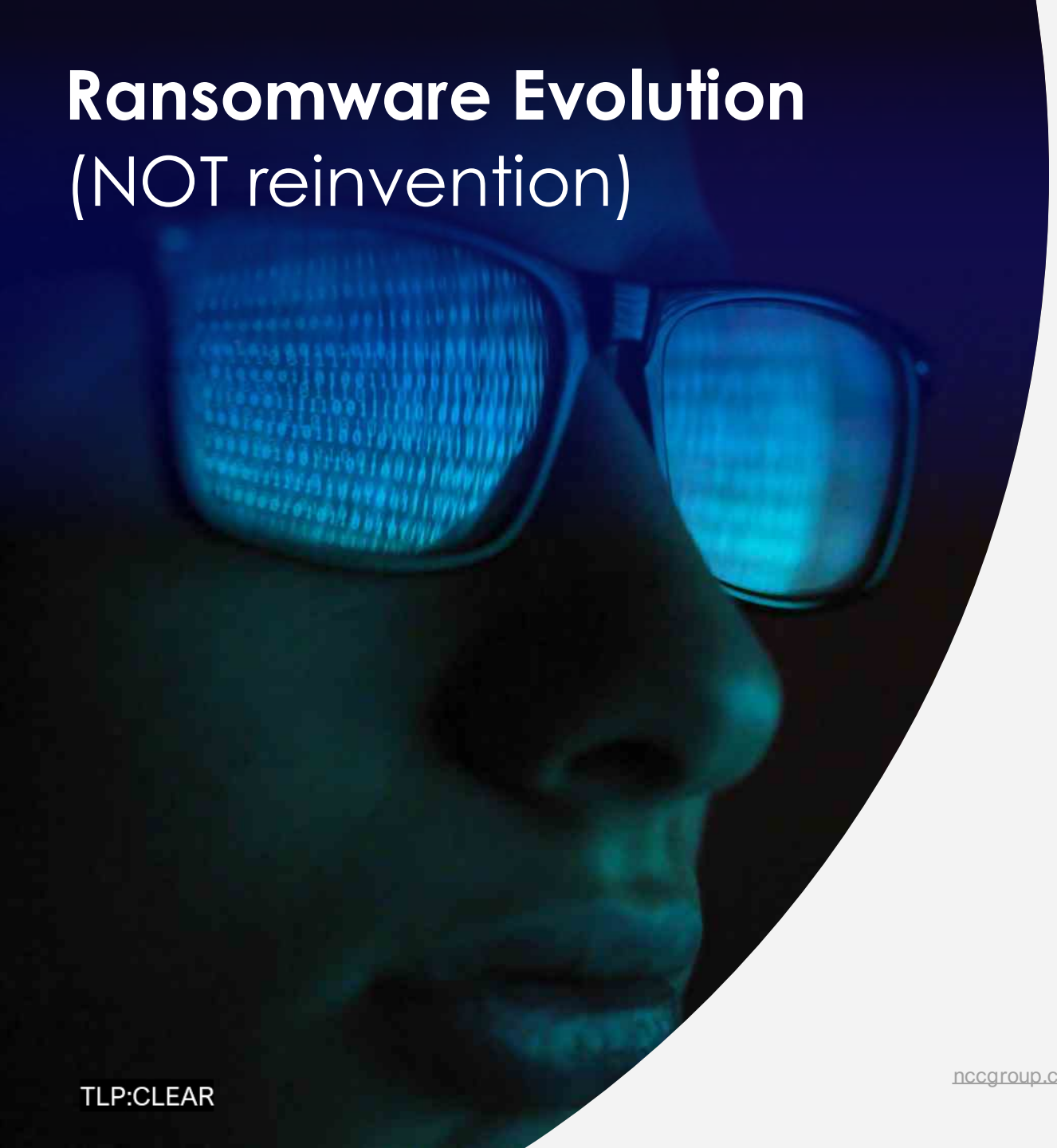
# How Exciting was 2025?

## Intelligence existed before many incidents

In multiple cases, the risks exploited had already been described in intelligence, audits, or risk registers.

The issue was not ignorance, it was delay and deprioritisation.

# **Ransomware Evolution**
# (NOT reinvention)



- Extortion pressure comes more from data theft than encryption
- Downtime and recovery time now drive business impact
- Shared services and suppliers increase blast radius
- Faster compromise = less time to detect or contain

TLP:CLEAR

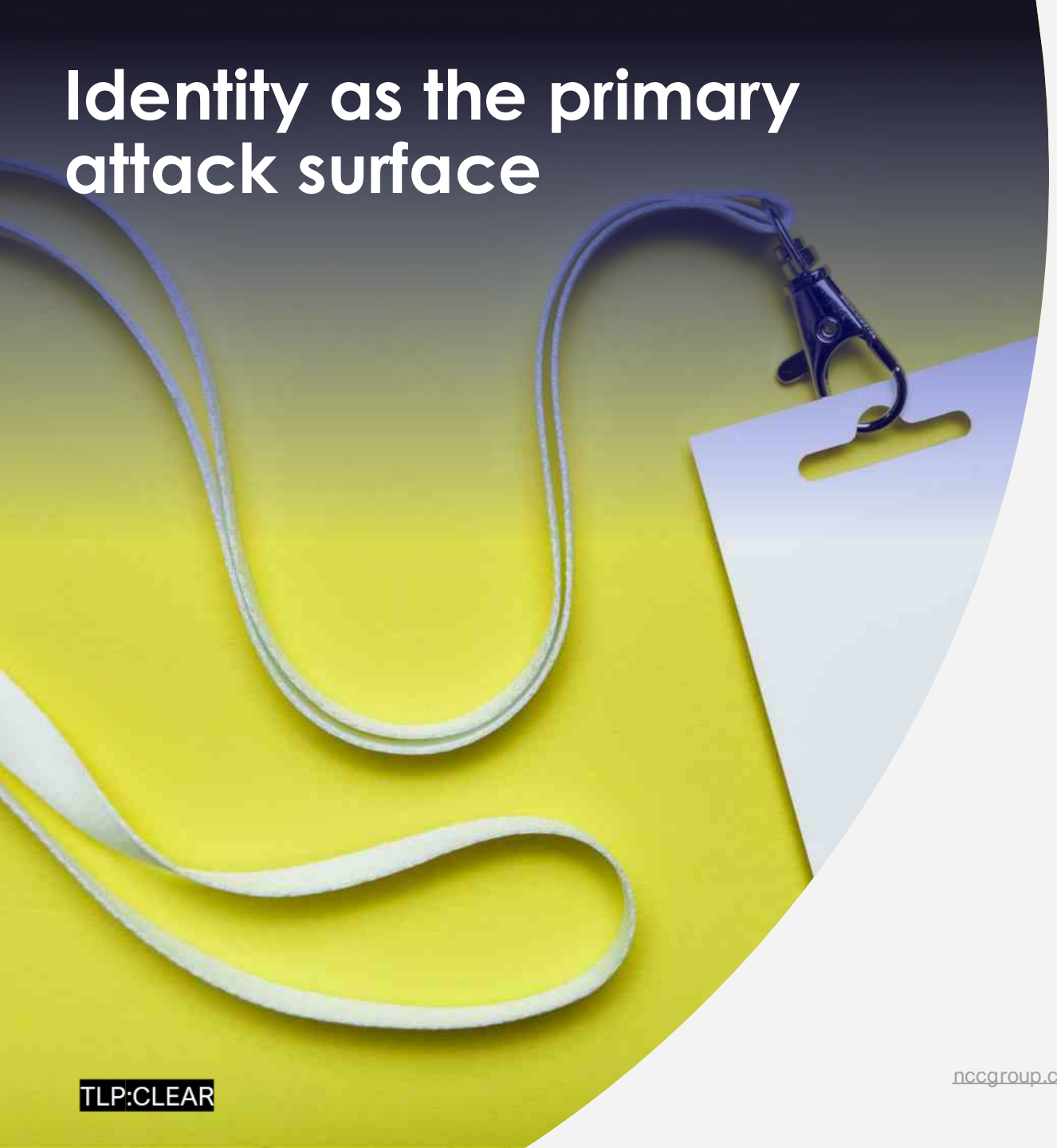
# Supply chain compromise as a force multiplier

- Organisations inherit risk through dependencies they do not control
- Software, SaaS, MSPs, and identity providers expand attack paths
- Trust relationships define impact more than perimeter controls
- Governance gaps matter as much as technical weaknesses

TLP:CLEAR

# Accelerating Threats in the New Year

# Identity as the primary attack surface



- Credentials, tokens, and identities targeted over exploits
- MFA fatigue, OAuth abuse, stale service accounts
- Cloud and SaaS expand exposure invisibly
- Identity failures often bypass traditional security monitoring

TLP:CLEAR

# AI-enabled social engineering at scale

- Higher volume, higher quality phishing and pretexting
- Better language, timing, and contextual awareness
- Voice and identity impersonation lowering fraud barriers
- Awareness models based on spotting “bad emails” are failing

# Geopolitical Overview

# 2026 Outlook: What's Coming Next

- Nation-state cyber activity surged as geopolitical flashpoints intensified; cyber operations used as instruments of hybrid warfare and strategic influence.

- Russia focused on political, military, and Ukraine-related intelligence collection; expansion of groups targeting European defence and political entities.

- China demonstrated unmatched persistence, long-term access, and major telecom sector compromises across multiple continents, supported by a deep private-sector ecosystem.

- Iran & North Korea continued regionally motivated espionage, global targeting tied to sanctions, nuclear issues, and foreign policy influence.

- North Korea remained dominant in financially-motivated APT activity, stealing $2B+ in cryptocurrency

# 2025: The impact of geopolitics

- Cyber operations fully integrated into statecraft—expect continued synchronisation with diplomatic, military, and economic objectives.

- Faster TTP evolution as public attribution accelerates APT adaptation cycles; groups like Coldriver showed the ability to operationalise new malware within days.

- Greater specialisation and collaboration inside APT ecosystems

- More aggressive exploitation of zero-days and cloud/SaaS vectors, demonstrated repeatedly in 2025 campaigns.

- Rising cross-nation collaboration among hostile states (Russia–Iran–NK) and rapid proliferation of commercial intrusion capabilities, extending APT-level operations to new actors.

# Threat = Capability + Motivation + OPPORTUNITY

# Annual Threat Monitor Report – Coming soon!!

# Next Webinar:

## Tuesday 24th February

TLP:CLEAR

# Thank you.

Together we're creating a more secure digital future