CRITEC GROUP



TRUST

Assumes users are safe.

Assumes access is legitimate.

Traditional security models were built around trusted users, trusted devices, and trusted access. As organisations become more connected, distributed, and automated, identity is becoming one of the most critical areas of operational risk.



Most breaches now begin with **identity compromise.**

Not sophisticated malware.
Not advanced exploits.

Credentials.
Access.
Trust.

IDENTITY

is becoming the new security perimeter.

Human identities, machine identities, service accounts, and AI agents are rapidly expanding visibility and access challenges.



CRITEC GROUP

CONVERGENCE

Identity governance. Privileged access. Zero trust.



These are no longer **isolated security functions.**

As digital environments become more autonomous, identity becomes operational risk.