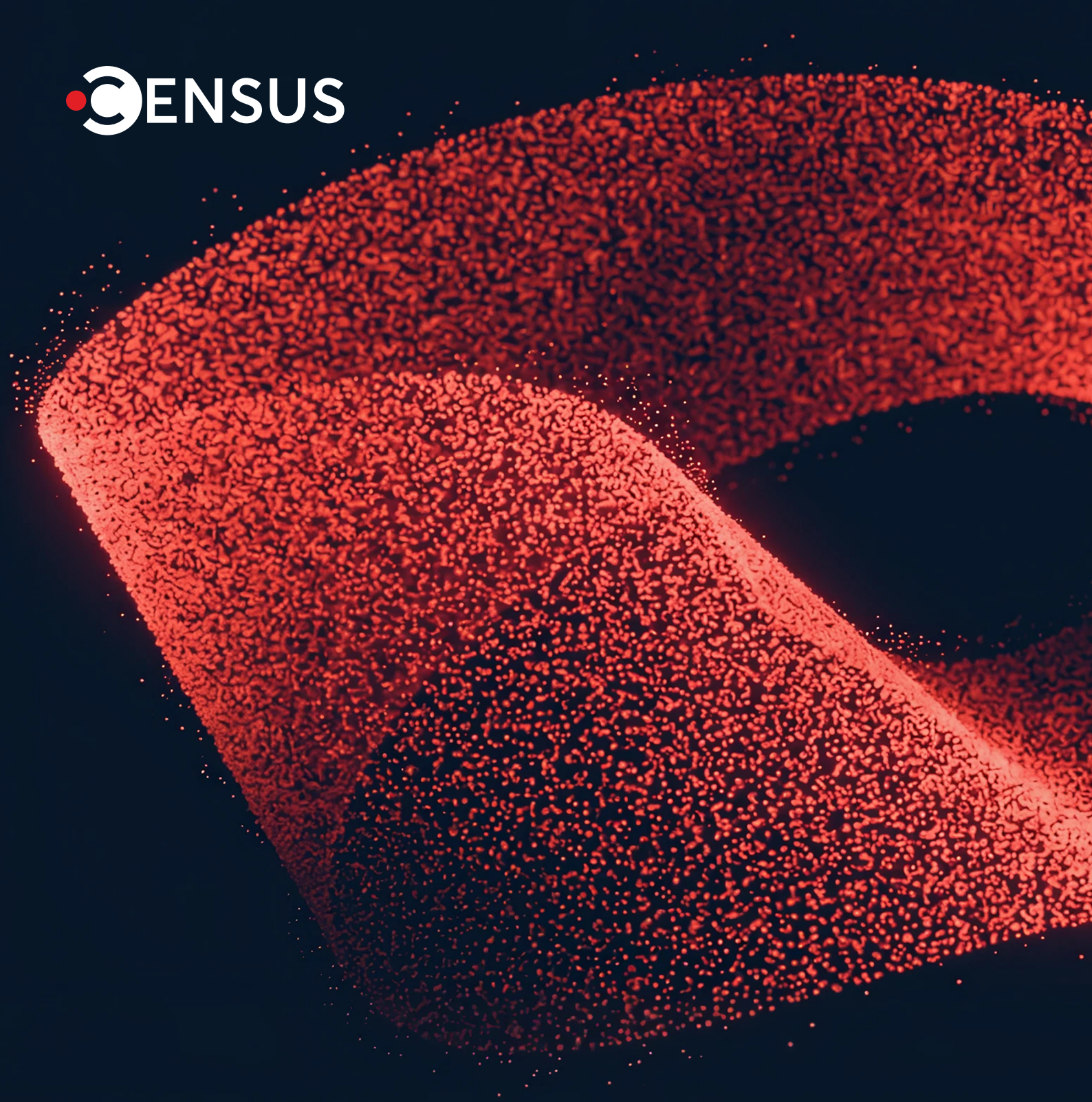
CENSUS



LATERAL MOVEMENT AND OT ESTATE HARDENING

LATERAL MOVEMENT AND OT ESTATE HARDENING

END-TO-END OT SECURITY ENGINEERING, FROM ADVERSARIAL ANALYSIS TO IMPLEMENTED CONTROLS

Many successful OT intrusions begin outside the control environment. Attackers enter through corporate IT, remote-access infrastructure, vendor connections, or exposed services, then move laterally toward the control layer using the trust relationships and network paths engineers depend on every day. Patching and replacement are often constrained by availability, safety, vendor support, and limited maintenance windows. The challenge does not end with identifying the exposure. It ends with engineering the fix around equipment that cannot be taken offline.

CENSUS SOLUTIONS

OT SECURITY PROGRAM DELIVERY

End-to-end engagement from attack-path mapping and architecture redesign through control implementation. The flagship program for operators hardening a complete industrial estate.

IT-TO-OT SECURITY ASSESSMENT

Comprehensive review of the OT risk originating in the IT domain. Produces IT-to-OT lateral movement mapping, zone-boundary analysis, remote-access audit, and a prioritised remediation plan.

SECURE ARCHITECTURE AND SEGMENTATION

Segmentation design, hardened remote and vendor access paths, secure management zones, and compensating controls for systems that cannot be patched or replaced.

INDUSTRIAL PRODUCT SECURITY

For OEMs, integrators, and asset owners. Protocol analysis, firmware assessment, and secure communication design for embedded controllers, IoT sensors, and special-purpose devices.

OT ENGAGEMENT FRAMEWORK

ASSESS → DESIGN → BUILD

ASSESS

- Attack paths mapped from IT to the control layer
- Architecture, zone boundary, and remote access
- Findings prioritised by operational feasibility

DESIGN

- Secure OT architecture and segmentation
- Hardened remote and vendor access paths
- Risk-reduction controls for legacy systems

BUILD

- Network hardening and zone isolation
- Deployment of hardened remote and privileged access
- Implementation of compensating controls

OT-facing discovery is passive by design. No active scanning or interaction with control equipment is required, and no planned production interruption is needed.

Census combines offensive expertise with production-grade engineering at the network, system, and device layers. Our experts have conducted authorised OT penetration testing across operational industrial environments, including oil refinery infrastructure and industrial manufacturing facilities. Our researchers hold doctorate-level expertise in ICS and embedded systems security, with hands-on experience across industrial protocols, firmware-level analysis of controllers, and passive OT network instrumentation.

Knowing how these systems are compromised is what makes the difference in designing defences that hold.

15+
YEARS OF INNOVATION

100+
SECURITY ENGINEERS

4
GLOBAL OFFICES

ISO 27001 CREST
CERTIFIED AND ACCREDITED

CYBERSECURITY ENGINEERING | TIGER TEAM® OFFENSIVE TESTING | IT AND OT SECURITY | PRODUCT SECURITY | CLOUD SECURITY | AI SECURITY | PQC RESILIENCE

WWW.CENSUS-LABS.COM
SALES@CENSUS-LABS.COM

IDENTIFY THE GAPS BEFORE ATTACKERS DO

An ASSESS engagement maps viable routes from corporate IT to the control layer, scoped to your architecture and designed around operational safety.