Ericsson

Global leader in telecom security

Wireless networks are critical infrastructure, providing communication for public safety, healthcare, manufacturing, transportation, commerce, and other use cases. These networks face increasing threats from sophisticated threat actors including Nationstate actors attacking networks with Advanced Persistent Threats (APTs) that exploit vulnerabilities, unsecure credentials, and misconfigurations to move laterally and persist undetected in networks.

Ericsson is the world's leading trusted telecom supplier - protecting critical infrastructure today, prepared for the evolving threat landscape and providing the United States with secure national critical infrastructure.

Ericsson security at work in the USA

60% of wireless traffic in the US

is carried on Ericsson-powered networks across all 50 states

1st and largest US manufacturer of 5G infrastructure

Secure, long-term manufacturing and supply chain resiliency for essential network infrastructure

Research and development center

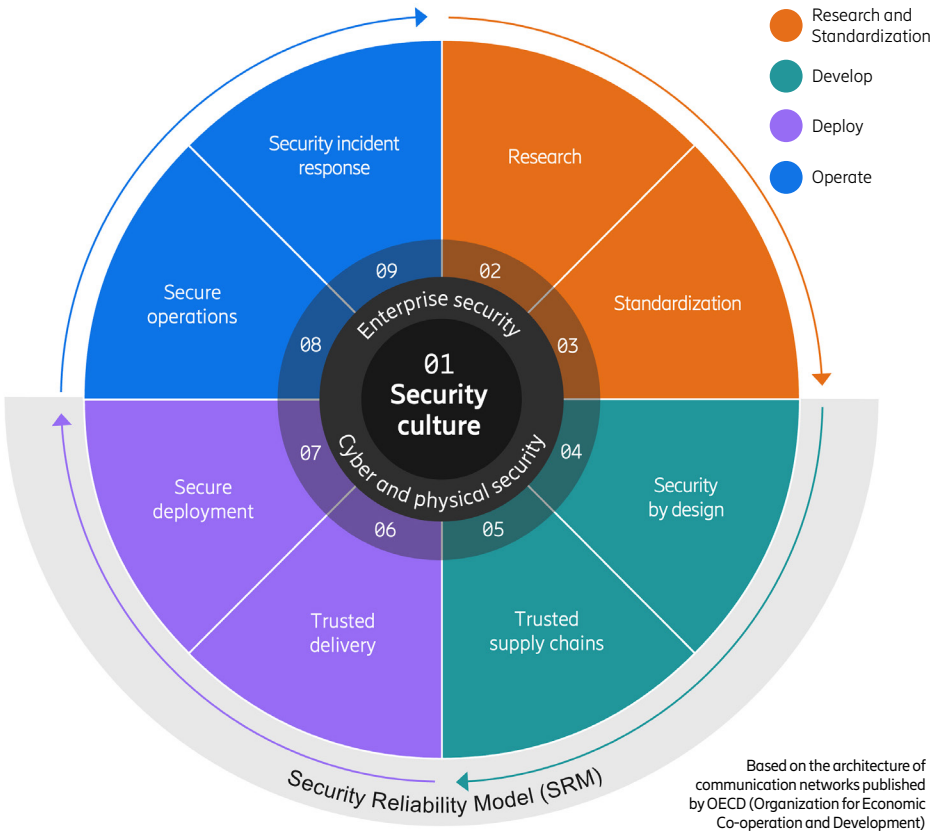
in Austin TX, Ericsson design center focused on trusted Silicon development, ASIC platforms ensuring secure boot and PQC support

Founding member of CTIA 5G security testbed

at the University of Maryland, together with MITRE, AT&T, and T-Mobile.

Ericsson holistic security posture is protecting critical telecom infrastructure

Ericsson has the leading security posture in the telecom industry, enabling our customers to build and operate the most secure networks that are compliant with US Government standards and requirements while remaining adaptable and resilient to emerging and future threats.



Based on the architecture of communication networks published by OECD (Organization for Economic Co-operation and Development)

Ericsson: 9-point security posture

01 Security culture supported by cyber and physical security

Our security and privacy posture starts with our security culture and frameworks with deep integration into our organization's operations, values, and strategic objectives. This includes mandatory security training globally and a specialized program with ~ 5000 Security champions and masters ensuring the protection of both our customers and Ericsson's assets. Our security and privacy posture are cemented through our security frameworks. We follow industry BCP and requirements such as NESAS, SCASes and ISO27001 with ISMS securing our Enterprise, and SRM (Security Reliability Model) securing our product and service posture.

Research and Standardization

02 Research

Ericsson Research focuses on defining 6G security by driving a thorough threat analysis and a security architecture aligned with new requirements, by driving open standards, applying zero-trust principles, and taking a holistic view on security, including implementation, deployment, and operational security aspects. Relevant technologies are AI and automation, network exposure and API security, assurance and situational awareness, and quantum-safe cryptography for resilience against future threats. Together, these domains aim to create adaptive, trusted digital infrastructures resilient to evolving threats in line with regulatory demands.

03 Standardization

Ericsson invests heavily in security standardization and community influence and is a leading contributor across regional and global standards and policy organizations including 3GPP, O-RAN ALLIANCE, IETF, ETSI, GSMA, ATIS and NIST. Our investments advance security standards globally. Ericsson is also a leader in government-industry collaboration to secure critical infrastructure including FCC CSRIC and DHS SCRM. Leadership positions include Co-Chair of the Security Working Group in O-RAN ALLIANCE, Co-Chair of ATIS Steering Group on Enhanced Zero Trust in 5G and Chair of ETSI SAGE (Security Algorithms Expert Group). Ericsson provides leadership for standardization of Post-Quantum Cryptographic (PQC) algorithms at industry SDOs.

Develop

04 Security by design

Ericsson develops security features for operators to achieve a ZTA in their network based upon NIST SP 800-207. Ericsson adheres to secure software development using GSMA NESAS (Network Equipment Security Assurance Scheme), 3GPP SCAS (Security Assurance specifications) and Ericsson Security Reliability Model (SRM), which is guided by the NIST Secure Software Development Framework (SSDF). Ericsson follows best practices such as least privilege access, data encryption, and continuous monitoring during design and development phases and we apply DevSecOps with Continuous Integration/Continuous Deployment (CI/CD).

Ericsson is a leader in foundational technologies including 5G SA, Open RAN, Continuous Security Monitoring and AI/ML-based security automation. We implement a unified and robust foundation for secure operations across Ericsson Silicon with hardware-based security across the radio portfolio.

05 Ericsson trusted, diversified and transparent supply chain

Ericsson maintains a secure and resilient supply chain. Our manufacturing and development processes are built on end-to-end traceability, rigorous quality controls, integrity checks, regular site audits and thorough testing. Our Business Continuity Management (BCM) framework aligns with ISO 22301 standards, ensuring the resilience of our operations and supply chain. Through the company's USA 5G Smart Factory, Ericsson addresses a critical challenge ensuring secure, long-term manufacturing and supply chain reliability. The company actively manages security risks globally while complying with regional and customer-specific regulations. Our hardware and software supply chains:

- Are GSMA NESAS compliant
- Comply with industry security standards from 3GPP and O-RAN Alliance
- Are certified under ISO/IEC 27001:2022
- Use weighted measurements from multiple data sources when vetting security in open-source software
- Ensure software supply chain security, including Software Bill of Materials (SBOM) and alignment to TIA SCS 9001
- Adopt strong product security requirements for suppliers
- Are resilient with local hardware manufacturing, product development and new product introduction

Deploy

06 Trusted delivery

Trusted delivery is ensured by alignment to the TIA Supply Chain Security SCS 9001, secure transport by our suppliers (C-TPAT requirements) and providing our SW via a secure download from the Ericsson Software Gateway. Software downloads include a signature providing a trust anchor guaranteeing origin and secure transit. Systems hardening is aligned with US DHS CISA guidance.

07 Secure deployment

Deployment is secured through dedicated security competence. Dedicated configuration and hardening guidelines include rigorous system hardening aligned with US DHS CISA guidance to reduce attack surfaces and strengthen resilience. Our deployment practices leverage ZTA-enabling security features, public key infrastructure and centralized identity management. Ericsson deployment teams use secure network design principles and protect traffic and data through confidentiality and integrity protection with NIST-approved ciphers.

Operate

08 Secure operations

Ericsson flagship security solution, Ericsson Security Manager (ESM) acts as an enabler for Zero-Trust implementation during operations, helping our customers comply with CISA hardening guidelines. ESM enables continuous mobile security monitoring based upon NIST Cybersecurity Framework (CSF) including:

- Leading capability for false base station detection and anti-jamming
- Leading capability for threat and vulnerability intelligence
- CISA configuration auditing
- Comprehensive Attack Surface Management
- Extended Detection and Response
- Certificate and Trust Management

Ericsson uses our Ericsson Vulnerability Management System (EVMS) to monitor and track all published vulnerabilities and security updates that impact our products. Our PSIRT, product development, 3PP technology and customer support organizations then work as trusted intermediaries to all stakeholders to ensure proper notification and action.

09 Security Incident Response

Incident response is a key part of managing vulnerabilities. Ericsson Product Security Incident Response Team (PSIRT) provides immediate global response and support for any incident, partnering with customers and law enforcement to recover from and resolve cyber threats. Ericsson partners in the Common Vulnerabilities and Exposures (CVE) Program and designated CVE Number Authority (CNA). Ericsson Threat Intelligence reports, recurring security bulletins and CVE information are resources for our customers. Ericsson is also part of GSMA CVD program supporting researchers and the wider ecosystem resolve vulnerabilities and protect customer security.