Insight paper

Securing an Open AI-Driven Mobile Network

ERICSSON

AT&T

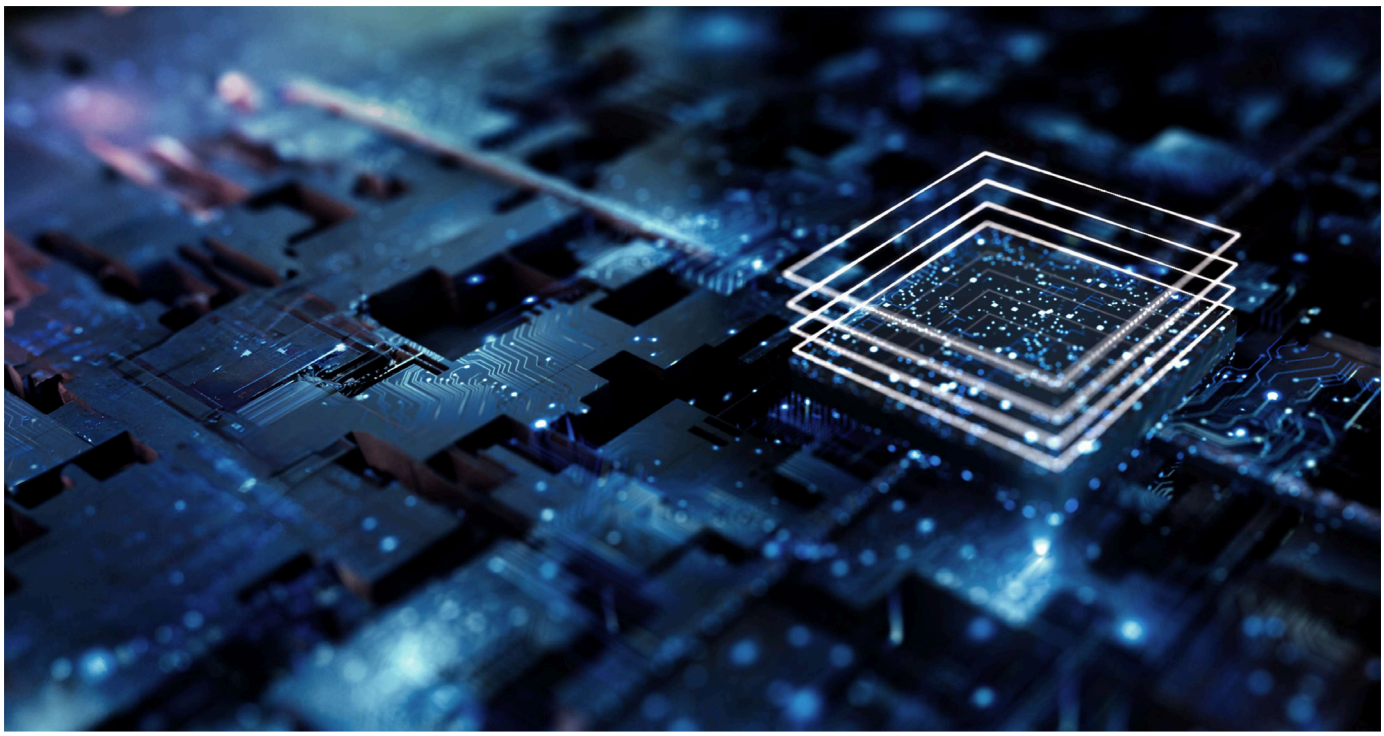
Introduction

Mobile networks are undergoing a generational change, becoming AI-driven and open. While these changes will be invisible to customers, they are profoundly changing the design and operation of mobile networks. Service providers are partnering with their network vendors to unlock the potential for creating ever-more reliable, efficient, intelligent and secure networks so that subscribers can count on connectivity and privacy. As threats to networks are becoming more sophisticated, members of the mobile industry are partnering to share threat intel information to develop mitigations to protect against new and old threats.

Today's 5G Core networks support service-based architectures (SBA) with each network function (NF) exposing standardized, open interfaces to the other components. The backhaul between the Radio Access Network (RAN) and Core is also open, as are the 3GPP-defined roaming interfaces between mobile providers. O-RAN opens the functional blocks for the fronthaul, the management interfaces, and the underlying compute infrastructure based upon O-RAN ALLIANCE specifications. Providers and vendors will need to continue to partner to address new and existing threats on open interfaces.

The use of Artificial Intelligence (AI) and Machine learning (AI/ML) in mobile networks has begun. AI/ML is a transformative technology that will drive innovative use cases, service enhancements, and operational efficiencies in mobile telecommunication networks. Use cases include advanced RAN management, traffic steering, beamforming and anomaly detection. O-RAN includes standardized frameworks for including AI/ML. Unlike open interfaces, which have mature security protections, security for AI/ML is in its early, formative phase. Threats to AI/ML have been documented by OWASP-NIST and other leading organizations, and mitigations are being applied to provide confidentiality, integrity, availability, authentication, and authorization protections. AI/ML-specific security controls will be needed in addition to the security controls and best practices supported in products and used in networks today. Rapid orchestration and automated deployment of newly developed security measures will be imperative o securing AI/ML services.

Moving forward, the key to securing mobile networks against sophisticated threat actors will be cooperation and partnership among service providers, vendors and government agencies. Vendors and providers will need to secure the AI used in their networks, secure the open network architectures, and prepare for quantum computing. Providers will share information about the threats to their interconnect networks. Vendors and providers will continue to improve network security by using secure development practices and adopting evolving security controls. Security tests will also continue to improve through test driven development, unit and end-to-end testing by vendors and providers, and security certification. The challenges to secure AI and open networks and prepare for quantum era threats are described in the rest of this paper.



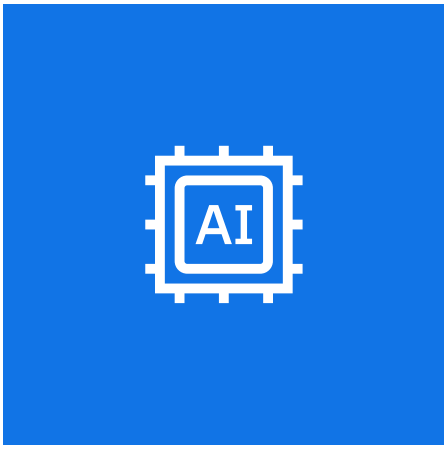
Challenge 1: Secure AI

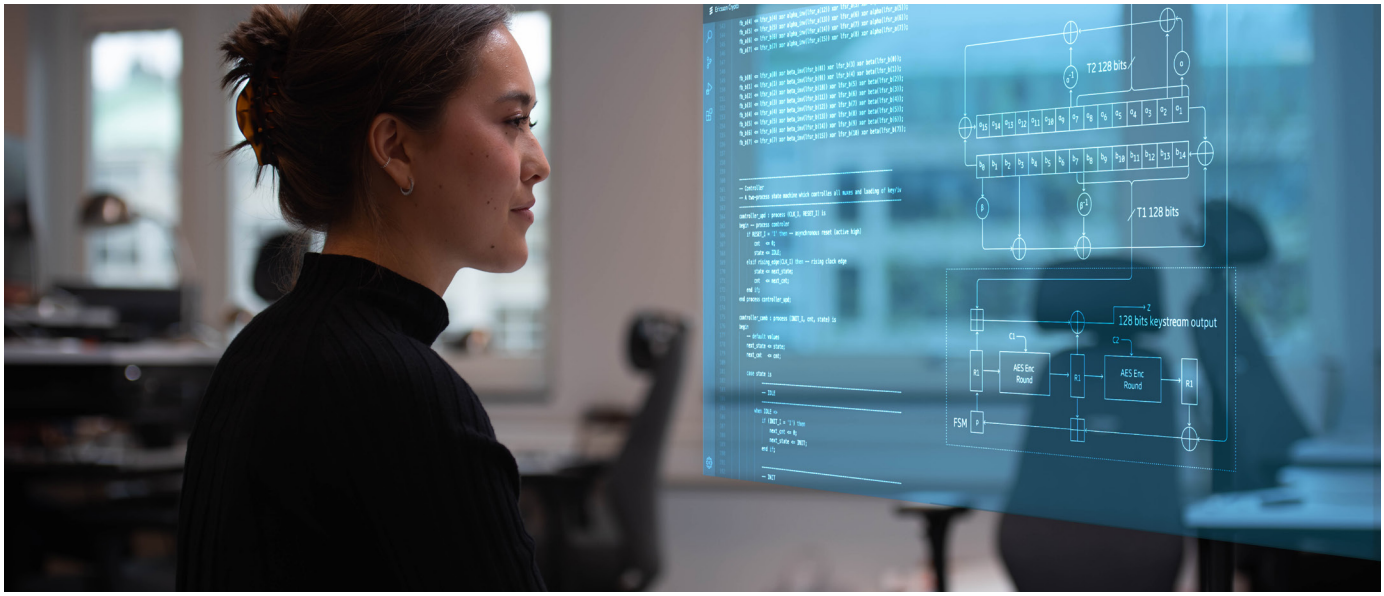
AI/ML will change the operation of mobile networks. Machine learning models are being developed to help providers with energy savings, beamforming and fault detection. AI/ML will accelerate the move to zero touch operations and AI/ML will be used to automatically detect and respond to potential anomalies and security incidents.

To realize the power of AI, the confidentiality, integrity, and availability protections of AI/ML will be paramount. Many organizations including NIST [1,2], OWASP [3], ENISA [4,5], ETSI [6], BSI [7], ISO [8], and ITU-T [9] have documented both threats against AI/ML and recommendations for mitigating security risks to AI systems. Threats include model and data poisoning, model skewing and inversion, input manipulation attacks, transfer learning, membership inference, feature manipulation, model theft and AI supply chain attacks among others. Although the attacks are well documented, detecting these types of attacks is difficult because models evolve with training and new data inputs. *The NIST AI Risk Model Framework* [2] and the *NIST Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations* [1] provide guidance for AI-specific protections against attacks targeting AI/ML systems. Additionally, the controls described in the *NIST Cybersecurity Framework* [10] provide a first line of defense.

The O-RAN ALLIANCE has studied the threats to AI/ML [11] and proposed requirements [12] that help provide confidentiality, integrity and availability of AI/ML in an O-RAN network and can also be extended to protect AI/ML resources in other parts of a mobile network. In addition to traditional confidentiality, integrity and availability controls, the O-RAN ALLIANCE recommends the use of controls such as differential privacy in training and inference, checks for model poisoning, model splitting, feature scaling, distillation of teacher models, and cryptographic watermarking of models to further protect AI/ML.

AI/ML is a unique trichotomy for security as it can be used as a security tool to strengthen defense against cyberattacks on telecommunication networks and services, an attack target to influence outcomes or steal information, and an attack tool used by adversaries to thwart network security control and exploit network weaknesses. The dark side of AI/ML is its use to enhance the effectiveness of cyberattacks. Industry stakeholders should expect AI-driven attacks on mobile networks and the need to enhance visibility to detect and respond to such attacks.



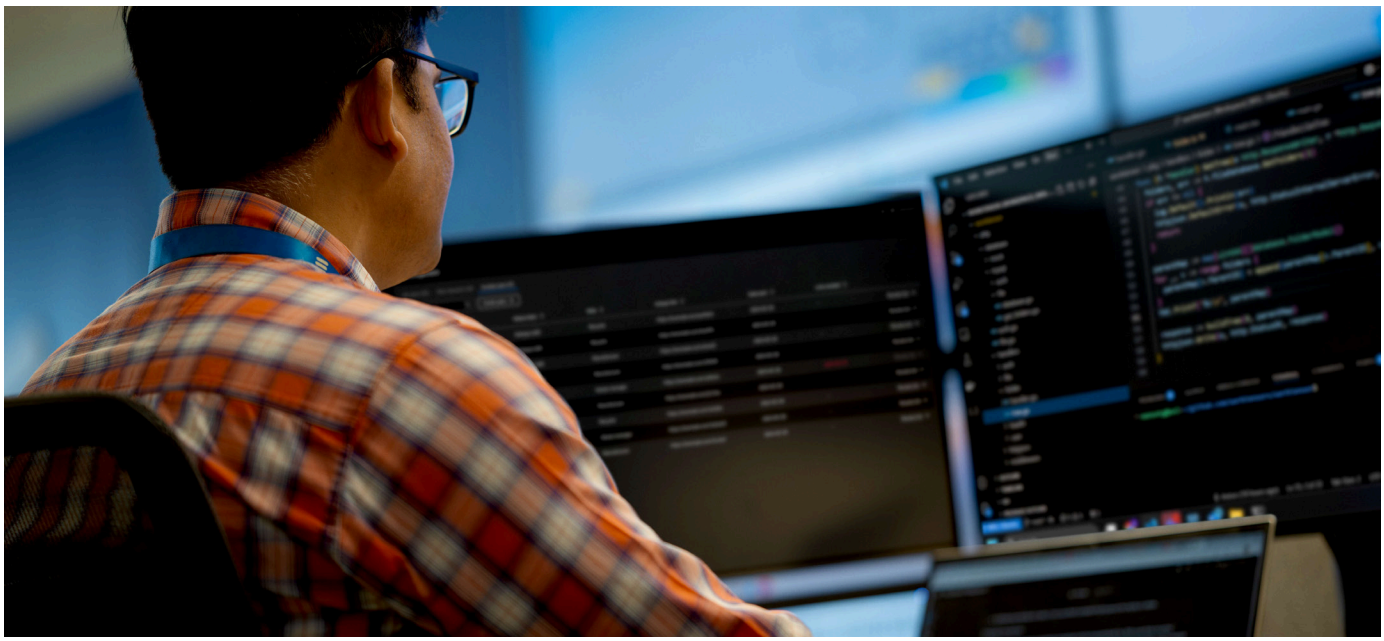


Challenge 2: Secure open networks

The 5G network is the most open mobile network to date. The 5G Core (5GC) is defined by its SBA and service-based interfaces (SBI). The O-RAN architecture [13] opens the RAN by defining open interfaces for the fronthaul, management planes and Cloud-native Network Functions (CNFs) running on the O-Cloud. The architecture also defines interfaces for integrating AI/ML into the network and defines APIs for interacting with RAN NFs. Open, standardized interfaces and APIs provide interoperability and a consistent security baseline. This can more quickly uncover security flaws, leading to more rapid patching. The approach of open, standardized interfaces also allows providers to mix and match best-in-class network functions. These interfaces are secured using 3GPP and O-RAN standardized interfaces that use IETF or IEEE standardized security protocols, such as TLS, SSH, IPsec, MACsec and 802.1X.

Another aspect of openness is the move from purpose-built network functions to software realizations of network functions, often as containers, running on cloud platforms such as Kubernetes. This reduces coupling between application software and the underlying compute layer, providing greater flexibility in how updates and security improvements are introduced over time. The disaggregation of software from hardware can also be used to protect the cloud platform from vulnerabilities in the application, and the application from vulnerabilities in the cloud platform. The United States Government provided guidance on protecting the cloud in 5G deployments as part of its *Enduring Security Framework* publications [14].

The third aspect of open networks is the use of open source software within the network functions and the compute layer. For many years, open source received little scrutiny, but events such as Heartbleed (2014) and Log4j (2021) raised awareness of the potential of security flaws in open source to impact mission-critical system [15]. Open source can be used securely if it is produced by trustworthy communities, actively maintained, securely consumed, and updated with available security patches. There are many robust security tools available that help prevent malicious open source use in code, and assist in updating packages, and identify vulnerabilities in open source packages. A software bill of materials (SBOM) [16] is another valuable tool for monitoring open source use in the network.



Challenge 3: Quantum computing

The ATIS 2025 report, *Preparing 5G for the Quantum Era: An Analysis of 3GPP Architecture and the Transition to Quantum-Resistant Cryptography* [17], describes the profound effects that Cryptographic Relevant Quantum Computers (CRQCs) will have on existing cryptography practices, particularly within the telecommunications infrastructure. Some cryptographic mechanisms that ensure confidentiality, integrity and authenticity will become vulnerable to breaches as CRQCs are used to efficiently solve the computationally difficult mathematical problems that form the foundation of modern cryptography. This potential breakthrough in quantum computing threatens to compromise encrypted communications, expose sensitive data, and undermine the security foundations of current telecom networks. The adoption of post-quantum cryptography (PQC), designed to resist both classical and quantum attacks, is essential to safeguarding the long-term security of telecommunications.

The transition to PQC introduces its own set of challenges: increased computational overhead, larger key sizes, and potential compatibility issues with existing infrastructure. In mobile networks, the implementation of PQC may need to be carefully managed to balance security with performance. For example, the resource-constrained environments of the RAN and mobile devices may struggle with the higher computational demands of some PQC algorithms, potentially impacting latency and throughput. New complexity will be introduced due to the need to ensure backward compatibility and interoperability as existing systems migrate to quantum-resistant cryptography. Key management systems will require upgrades to handle the complexities of PQC while maintaining robust automation and crypto agility. This proactive approach ensures that mobile networks remain secure and reliable in the face of quantum-era challenges, preserving trust and compliance with evolving security standards.

Securing the Mobile Network

While vendors and service providers address the security challenges of AI, openness, and quantum computing, they must also continue to execute in four additional areas to enable service providers to build secure end-to-end networks that protect against evolving external and internal threats. First, critical to protecting the network is understanding the threat landscape. Service providers are leading this through collective cybersecurity efforts. Second, NF vendors are following secure development practices such as security by design and remediation of vulnerabilities. Third is provider deployment of strong and scalable security controls aligned with the domains described in the NIST Cybersecurity Framework (CSF) [10]. Fourth is security testing, which runs the gamut of test-driven development, unit and end-to-end testing by vendors and providers, and security certification. These four areas of security are discussed in the following sections.

Understanding the Threats: Collective Cybersecurity

Modern telecommunications networks depend on interoperability between operators' networks to provide customers with seamless connectivity.

Recognizing that all mobile networks face the same threats and threat actors, AT&T has helped assemble a group of Chief Information Security Officers (CISOs) from the telecommunications sector across North America, Europe, and the Indo-Pacific region to collaborate on addressing the evolving and sophisticated threats facing our industry. By identifying opportunities for cooperation, engagement with the vendor community and encouraging threat defenders to regularly connect and participate in joint exercises, this group is strengthening our collective defense.

Building trust within our community of threat defenders provides a critical foundation for sharing insights, lessons learned, and best practices. In late 2025, threat defenders from more than a dozen telecommunications companies competed in a cyber competition hosted by AT&T that allowed for them to train together and build trusting cybersecurity relationships. The coalition of CISOs and their threat defenders are building on this momentum and regularly engaging and sharing threat related information to help build strong collective cybersecurity defense for the sector.

Secure Development Practices

Advanced Persistent Threats (APTs) perform lateral movement by exploiting vulnerabilities and misconfigurations once inside a network. APTs can be mitigated by reducing software vulnerabilities, validating secure configurations, and secure storage of credentials.

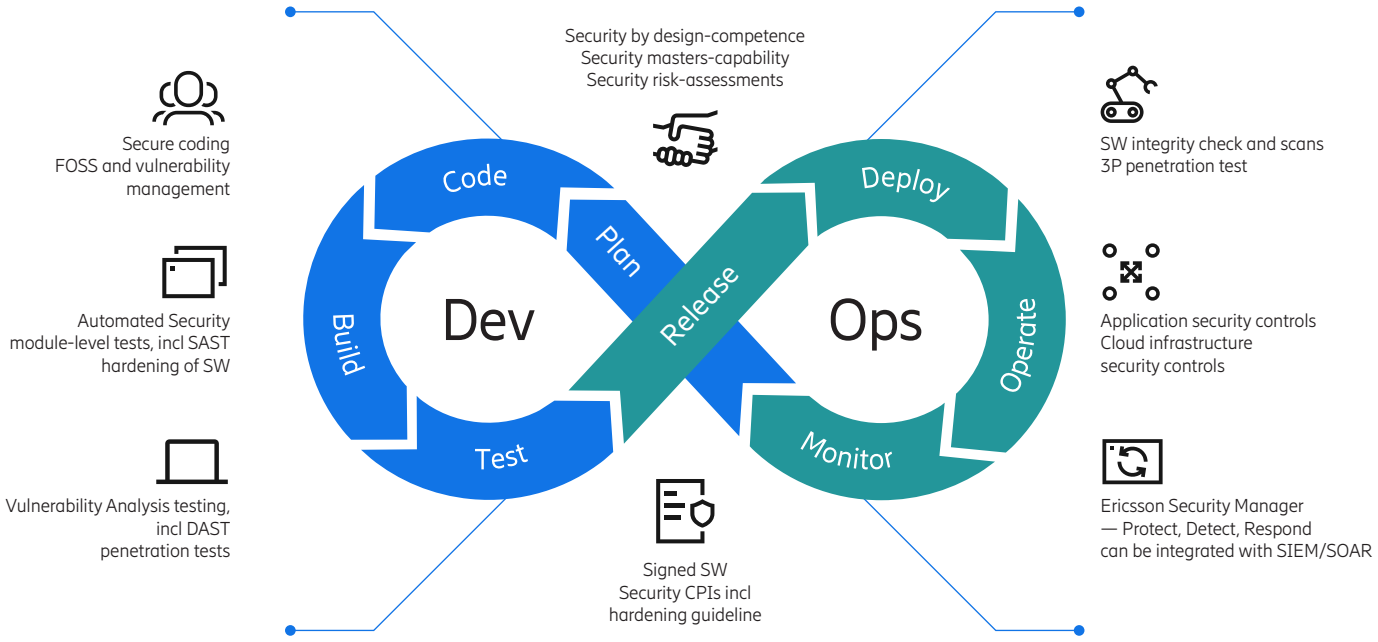
Securing software development is the evolution of the software development lifecycle to embed security practices and principles into every phase of the lifecycle. Software development practices include staying current with the latest versions of third-party packages in each release and developing emergency patches for critical vulnerabilities. A fundamental practice for secure software development is to have secure consumption of third-party software, particularly FOSS, which can have varying degrees of support for security maintenance [15]. Secure software development best practices have been made publicly available by BSA, OWASP, SAFECode, and OpenSSF and Ericsson is an active contributor of secure open source. Software vendors for communications critical infrastructure must follow development processes to ensure known vulnerabilities are remediated.

NIST used these best practices to establish the *Secure Software Development Framework (SSDF)* in NIST SP 800-218 [18] to help software producers reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. Other organizations such as CISA [19] provide timeframes for addressing vulnerabilities, so that the most critical vulnerabilities are fixed in no more than 30 days.

AT&T and Ericsson systematically incorporate security into all relevant aspects and phases of our end-to-end products' value flow. As a supplier, Ericsson's efforts in this area follow a well-established internal control framework known as the *Ericsson Security Reliability Model (SRM)* [20]. SRM enables a managed, risk-based approach to security and privacy implementation where requirements are tailored to the target environment and demands. Ericsson has a framework for the DevSecOps approach, as shown in Figure 1, that integrates security into a Continuous Integration/Continuous Deployment (CI/CD) pipeline where feasible. Security tests are performed throughout the pipeline with minimal human interaction.

Ericsson automates where possible and introduces security early in the process to catch and mitigate vulnerabilities efficiently. Automation includes different types of security tests, including static code analysis, software composition analysis, and dynamic application security testing. AT&T, as a consumer of products for deployment in a commercial setting, implements obsessive vetting of software (trust but verify) from suppliers to be free of vulnerabilities, as well as strict policies of Least Privilege and Zero-trust across all platforms that operate in the network. Operating a secure network demands continuous scanning and monitoring of production systems to recognize nefarious activity and to identify any APTs which could be present in the network by exploiting a previously unknown zero-day vulnerability. AT&T actively works with its supply chain partners, including Ericsson, to advance our platform and product capabilities to alert the presence of APTs and track their actions.

Figure 1. Ericsson SRM for DevSecOps

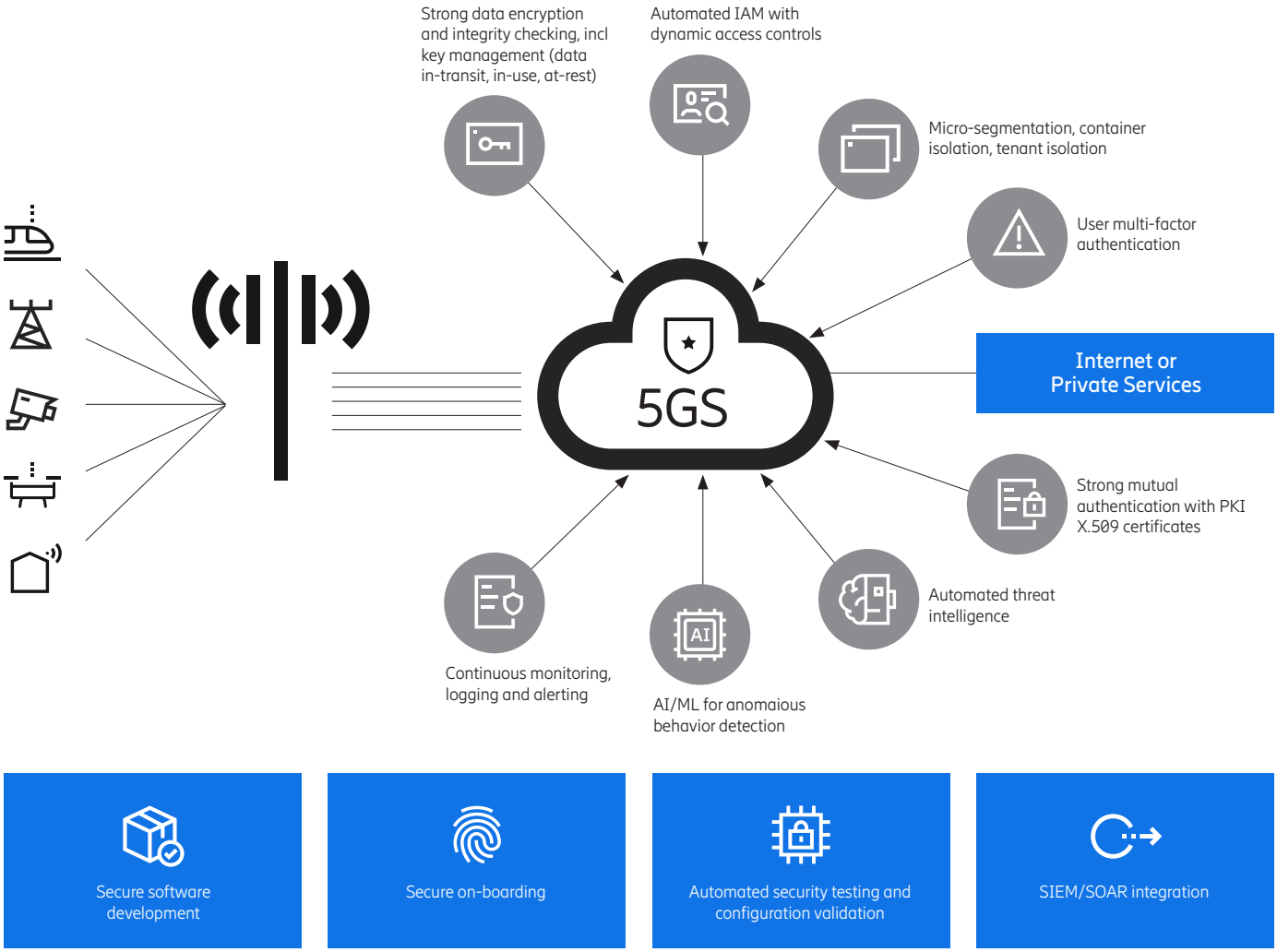


Secure Deployment and Operation

Service provider networks are protected with layers of security corresponding to the NIST Cybersecurity Framework [10] and following CISA recommendations [21,22]. Increasingly, providers are driving towards zero trust architectures (ZTA) as described by NIST [23] and CISA [24]. ZTA recognized that perimeter security alone is insufficient: a mature cyber defense assumes the adversary is already inside the network. ZTA is an evolution of traditional perimeter security that establishes micro-perimeters to secure networks from evolving external and internal threats. ZTA is a characteristic of the network enabled by security standards and products that implement those standards, as shown in Figure 2. ZTA dovetails with the NIST CSF and needs to be implemented end-to-end across the network because any part of the network with a lower security posture could be exploited to establish a beachhead for lateral movement. ZTA is an important goal for securing critical infrastructure, including 5G Core networks and RAN, to protect against threat actors seeking to find an access point for reconnaissance, data exfiltration, unauthorized control and/or network disruption.

As part of following NIST and CISA cybersecurity recommendations, including ZTA, the providers will implement and continue to evolve protective and detective security controls throughout their networks. The evolution will include X.509 certificate-based authentication for all system-to-system access, multifactor authentication for human access, least privilege authorization, data encryption at rest and in transit, endpoint detection and response, runtime configuration monitoring, software vulnerability monitoring, security logging and monitoring to a SIEM/SOAR, and network segmentation. Providers will also continue to evolve their continuous integration and continuous deployment (CI/CD) pipelines to increase the frequency of software deployment, thus removing vulnerabilities from production more rapidly.

Figure 2. ZTA critical control groups



Testing and Certification

Trust but verify. All network functions are tested before being deployed in the production network. The testing begins with the vendor where unit and end-to-end tests as well as vulnerability scans, such as static and dynamic application security tests, and configuration scans are run prior to release. Any problems that cannot be fixed, such as open source vulnerabilities without fixes, are documented with release notes, remediation roadmaps, and compensating controls the operator can implement while waiting for fixes.

Providers test the security of the vendor network functions by running container scans and various types of binary scans. The expectation is that these scans will find nothing that is not already documented in the release notes. Where problems are found, the provider brings them back to the vendor for patching, ideally, in the current release.

Certification by external testers is a third, and critical, area of testing. AT&T and Ericsson align our organizations, processes and systems to industry and regulatory standards. We use conformance statements for selected products to demonstrate our security compliance to external stakeholders such as regulators and customers. The combined approach is aligned with the GSMA's Network Equipment Security Assurance Scheme (NESAS). Ericsson assesses its purpose-built basebands and Cloud RAN basebands in this manner. NESAS Conformance results are posted at GSMA | NESAS Conformance Results—Industry Services.

Delivering a Secure AI-Driven Open Network

Telecommunications critical infrastructure plays a crucial role in national security for every nation. Building solid, robust and reliable solutions is essential to meet the demands of society that expect secure, resilient mobile connectivity services. Securing the AI-driven open networks requires both vendors and service providers to keep getting better at the standard security practices of secure development, secure operations and security testing. Key focus areas include:

- Prioritizing remediation of known vulnerabilities and applying the current software releases.
- Enhancing runtime monitoring of network functions.
- Developing CI/CD pipelines to implement frequent updates and patches across tens of thousands of network elements.
- Protecting the confidentiality and integrity of data at rest and in transit.
- Upgrading cryptography rapidly to ready the networks for quantum computing.
- Implementing security controls to enable an end-to-end ZTA.
- Automating security testing.

Service providers need to collaborate by sharing information about the threats to their networks and solutions to those threats with each other and their vendors. As we have learned through Salt Typhoon, nation state actors are able to inject APTs simultaneously into multiple operator networks. While controls and mitigations to secure AI are evolving, AI will also need to be used as a security tool to help secure the network.

Providers will simultaneously use AI in their networks as they discover how to protect AI from new classes of attacks such as model poisoning, model skewing and model inversion. Protecting AI models and data with strong access and monitoring controls will be the best first lines of defense as new techniques are developed to both protect against and detect attacks on AI. Providers also will need mitigations in place to minimize the damage from AI-based attacks.

Telecom network security is never complete because threats are constantly evolving. Recent attacks targeting communications networks have heightened awareness of evolving APTs. The telco industry is continuing its pursuit of a ZTA to defend against external and internal attacks. Assume the adversary is in the network, because often they are. Network products with ZTA-enabling security features, security built-in using secure software development processes, product hardening following best practices from industry and government, and continuous monitoring for visibility and AI-based detection will enhance the network security posture to better defend against sophisticated APTs.

Securing open platforms will require providers and vendors to develop expertise in virtualization technologies that have already been embraced at scale by IT staffs. Emerging technologies like AI and quantum computing coupled with open architectures will change how we secure networks. AT&T and Ericsson are committed to continue leading the communications industry to secure 5G and evolving 6G networks.

Authors

Jeff Collins
Head of Customer Security Solutions, Ericsson Americas

With a career spanning over 15 years, Jeff is a distinguished professional known for his expertise in product management, customer partnerships, and strategic leadership. He currently spearheads security initiatives at Ericsson, leveraging his extensive experience across numerous domains such as telecommunications, virtualization, orchestration, and networking.

Jeff is a passionate advocate for innovation and collaboration actively contributing to numerous open-source projects and standardization organizations to drive progress within global communities. He is a Certified Information Systems Security Professional (CISSP). Jeff holds a Master of Software Engineering and a Bachelor of Computer Science. He is further advancing his academic journey by pursing a Ph.D. at Southern Methodist University.

Scott Poretsky
Director of Security, Ericsson Americas

Scott Poretsky is Ericsson America's Director for Security Policy and Standards in the Strategy and Technology team. He has over 30 years of industry experience in a variety of networking and security technologies. Scott is focused on securing telecom critical infrastructure through 6G security, Open RAN security, AI security, cloud security and zero trust architecture. Scott is Co-Chair of O-RAN Alliance's Security Work Group (WG11) and Co-Chair of ATIS TOPS Study Group on Zero Trust and 5G. He has served as Ericsson's FCC CSRIC Member and in multiple CSRIC working groups. Scott has one patent and numerous published papers and is a frequently invited speaker. Scott is a Certified Information Systems Security Professional (CISSP) and Certified Cloud Security Professional (CCSP). He earned an MSEE from the Worcester Polytechnic Institute (WPI) and BSEE from the University of Vermont.

Nicholas Thompson
Director, RAN Transformation, AT&T

Nicholas Thompson is a Director of Radio Access Network (RAN) technology at AT&T, currently leading the Advanced RAN Transformation team. His career spans 30 years, beginning with market-based design, optimization, and automation of analog cellular networks and evolving into leadership roles focused on the design, planning and deployment of Open RAN architectures. For the past five years, Nick has focused on the "art of the possible" within emerging technologies—including Open Network Management, Automation, and Cloud RAN—by defining long-term roadmaps and driving successful, scaled introductions. Nick holds both a bachelor's and a master's degree in Electrical Engineering from the University of Wisconsin–Madison.

Amy Zwarico
Cybersecurity Director, AT&T's Chief Security office

Amy Zwarico is a Cybersecurity Director in AT&T's Chief Security office, specializing in 5G, software and open source security. She is an active security contributor to the O-RAN ALLIANCE and to Linux Foundation Networking. Amy has worked in the telco industry for 30 years, where she began her career implementing web-based integrations to BSS/OSS systems. For the past 25 years she has focused on mobility security, application security, cloud security and applied cryptography. She holds a Ph.D. in Computer and Information Science from the University of Pennsylvania.

References

[1] NIST AI 100-2e2023 Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, draft white paper, US DoC NIST January 2024.

[2] NIST AI 100-1: Artificial Intelligence Risk Management Framework (AI RMF)", January 2023. https://doi.org/10.6028/NIST.AI.100-1.

[3] OWASP Top 10 Machine Learning Security risks, 2023 https://owasp.org/www-project-machine-learning-security-top-10/.

[4] ENISA: "Securing Machine Learning Algorithms"; https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms.

[5] ENISA: "Artificial Intelligence Cybersecurity Challenges"; https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

[6] ETSI GR SAI 004 v1.1.1: "Securing Artificial Intelligence (SAI); Problem Statement", December 2020.

[7] BSI: "AI SECURITY CONCERNS IN A NUTSHELL"; https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Practical_AI-Security_Guide_2023.pdf

[8] ISO/IEC WD 27091, Cybersecurity and Privacy, Artificial Intelligence, Privacy protection: https://www.iso.org/standard/56582.html.

[9] ITU-T TR XSTR-SEC-AI: "Guidelines for security management of using artificial intelligence technology"; https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-PDF-E.pdf.

[10] NIST Cyber Security Framework; https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[11] O-RAN.WG11.TR.AIML-Security-Analysis: "Study on Security for AI/ML".

[12] O-RAN.WG11.TS.SRCS: "O-RAN Security Requirements and Controls Specifications".

[13] O-RAN.WG1.TS. OAD: "O-RAN Architecture Description".

[14] "Security Guidance for 5G Cloud Infrastructures", US NSA ESF, October 2021.

[15] Open source software security in an ICT context - Ericsson, Ericsson, January 2021.

[16] "The Minimum Elements for a Software Bill of Materials (SBOM), Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity", U.S. DoC and NTIA, July 2021".

[17] "Preparing 5G for the Quantum Era: An Analysis of 3GPP Architecture and the Transition to Quantum-Resistant Cryptography," ATIS, 2025.

[18] Secure Software Development Framework (SSDF), version 1.1, NIST SP 800-218, US DoC NIST, February 2022.

[19] BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems | Cybersecurity & Infrastructure Security Agency April 29, 2019.

[20] The Ericsson Security Reliability Model – security by design.

[21] "Enhanced Visibility and Hardening Guidance for Communications Infrastructure", US DHS CISA, December 2024.

[22] "Product Security Bad Practices", US DHS CISA, January 2025.

[23] Zero Trust Architecture, Special Publication (SP) 800-207, US DoC NIST, Aug 2020.

[24] Zero Trust Maturity Model, version 2.0, US DHS CISA, April 2023.

About AT&T

We help more than 100 million U.S. families, friends and neighbors, plus nearly 2.5 million businesses, connect to greater possibility. From the first phone call 140+ years ago to our 5G wireless and multi-gig internet offerings today, we @ATT innovate to improve lives. For more information about AT&T Inc. (NYSE:T), please visit us at about.att.com. Investors can learn more at investors.att.com.

About Ericsson

Ericsson enables communications service providers and enterprises to capture the full value of connectivity. The company's portfolio spans the following business areas: Networks, Cloud Software and Services, Enterprise Wireless Solutions, Global Communications Platform, and Technologies and New Businesses. It is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's innovation investments have delivered the benefits of mobility and mobile broadband to billions of people globally. Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.
www.ericsson.com

www.ericsson.com

SE-126 25 Stockholm, Sweden
Telephone +46 10 719 00 00

March 2026, Rev. 1