etis TNO

European Telecommunications ISAC

Telco Security Landscape 2023

Publisher	ETIS | The community for telecom professionals www.etis.org
Coordinator	Andrija Višić (ETIS Central Office) av@etis.org
Editors	Philippe Vuilleumier (Swisscom) Richard Kerkdijk (TNO)
Release date	March 20th 2023
Copyright	© 2023 ETIS, all rights reserved

Contents

Preface

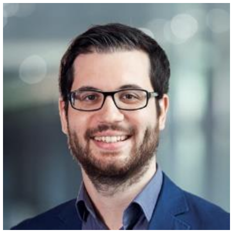
The modern digital society that all citizens, industries and governments exist within is massively - and increasingly - dependent on hyper-interconnected communications infrastructure. This is not a new phenomenon, but this surging dependency has made the protection of this infrastructure more critical than ever. To do this effectively requires a sound understanding of technical and non-technical threats, both now and in the future. Interestingly though, the essential role that communications infrastructure plays is often only recognised when it no longer functions due to operational failures, natural disasters or even military conflict.

As technology advances and the telecommunications industry evolves, security teams are faced with a variety of new challenges, but also offered new opportunities to protect the interests of their companies better. In view of this, the European Telecommunications ISAC (ET-ISAC) is proud to share this first public edition of its annual Telco Security Landscape. The aim is to share insights from our security practitioners on current and emerging issues and stimulate ideas and inspiration for our peers in other sectors.

We would like to thank our colleagues in the ET-ISAC and at the ETIS Central Office in Brussels for their support in preparing this publication and hope that it will be a useful reference for you.

Enjoy the read!

Rolv. R. Hauge
Head of security
advisory at Telenor
and chair of ETIS
Information Security
Working Group



Stefan Kuch
Head of Swisscom
CSIRT and chair of
ETIS CERT-SOC
Telco Network

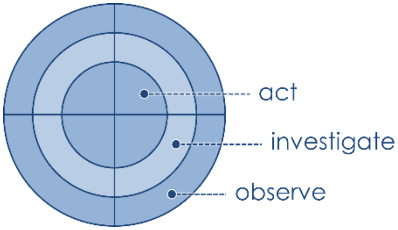
Introduction

The **Telco Security Landscape** depicts key developments that will affect the (cyber) security priorities for European telecommunications providers over the coming years. It is compiled on an annual basis and serves as a strategic guide for the ET-ISAC's activities and meeting agendas. Over the years, it also proved valuable to drive and validate security strategies of individual companies in the ISAC's constituency. Through this public report, the ET-ISAC would like to share insight into its current focus areas and inspire security leaders in other industries to reflect on their relevance as well.

The landscape is visualised in a radar diagram where topics are classified as threats, opportunities or both, as colour coded below:

🔴 = threat
🟢 = opportunity
🟠 = combination of both

In essence, the closer a topic is placed to the center of the radar diagram, the higher ET-ISAC perceives its priority. Here the radar distinguishes three specific action perspectives. The center ring comprises topics that the industry needs to **act** upon in the short term, whereas the middle and outer rings encompass topics that ET-ISAC wishes to **investigate** further or merely **observe** for now.



All topics depicted in the Telco Security Landscape stem from insights provided by security leaders in the European telco industry. In the final quarter of each year, these topics are collected, evaluated and weighted through a series of workshops with ET-ISAC delegates (typically Chief Information Security Officers (CISOs) and representatives thereof). These workshops are indepently facilitated by Dutch knowledge institute TNO who also compile the output report and visualisation.

Telco Security Landscape 2023

This year's Telco Security Landscape is comprised of eight threats, one distinct opportunity and two developments that (to some extent) exhibit both characteristics. Combined, they offer a viable perspective on strategic security issues that will affect the telco industry in its entirety and thus warrant a degree of collaboration under the ET-ISAC umbrella. Each landscape topic is briefly described below and the overall radar visualisation is subsequently depicted on page 8-9.

01 **scarcity of cyber security talent.** There is a structural shortage of a skilled cyber security workforce. Much the same as for companies in other industries, telcos will need to invest in recruitment and optimise conditions to retain staff for a career in cyber security. Regarding the latter, the salaries and career paths offered by big tech companies increasingly set the standard that telcos will need to compete with.

02 **migration to public cloud.** Primarily driven by cost and efficiency, there is a tendency to move telco systems and infrastructure to public cloud environments. In particular situations, this can be beneficial from a security perspective as well. The implication, however, is a reliance on fairly generic certifications and attestations (e.g. an ISO/IEC 27001 or ISO/IEC 27017 certificate). There is a need to assess more closely under which circumstances such generic assurance will suffice. Furthermore, the allocation of security relevant responsibilities between cloud providers and cloud consumers needs to be understood in relative detail and appropriately acted upon.

03 **cloud native infrastructures.** Telco internal infrastructures increasingly employ cloud technologies such as Docker and Kubernetes. This requires a fundamental rethinking of traditional security models and architectures, and an appropriate focus on emerging issues such as the security of Application Programming Interfaces (APIs). Many CISO teams will likely need to re-skill to govern and facilitate this appropriately.

04 **geopolitical tension.** Geopolitics can affect the availability of specific equipment and (spare) parts or make the supply of energy less stable, potentially impacting telco service continuity. In addition, some governments may impose restrictions on working with specific vendors or service providers in view of national security concerns.

05 **third party dependency.** Security in core telco operations often relies heavily on the capability of vendors to which particular (maintenance) duties have been outsourced. Governing this appropriately can be challenging and will likely become even more complex now that telcos are increasingly integrating native software development pipelines with those of their suppliers.

06 **supply chain integrity concerns.** Hardware and software supply chains come with systemic risks that need structural attention. Initiatives such as GSMA's Network Equipment Security Assurance Scheme (NESAS) address the issue to some extent, but do not cover all associated risks (nor all relevant equipment).

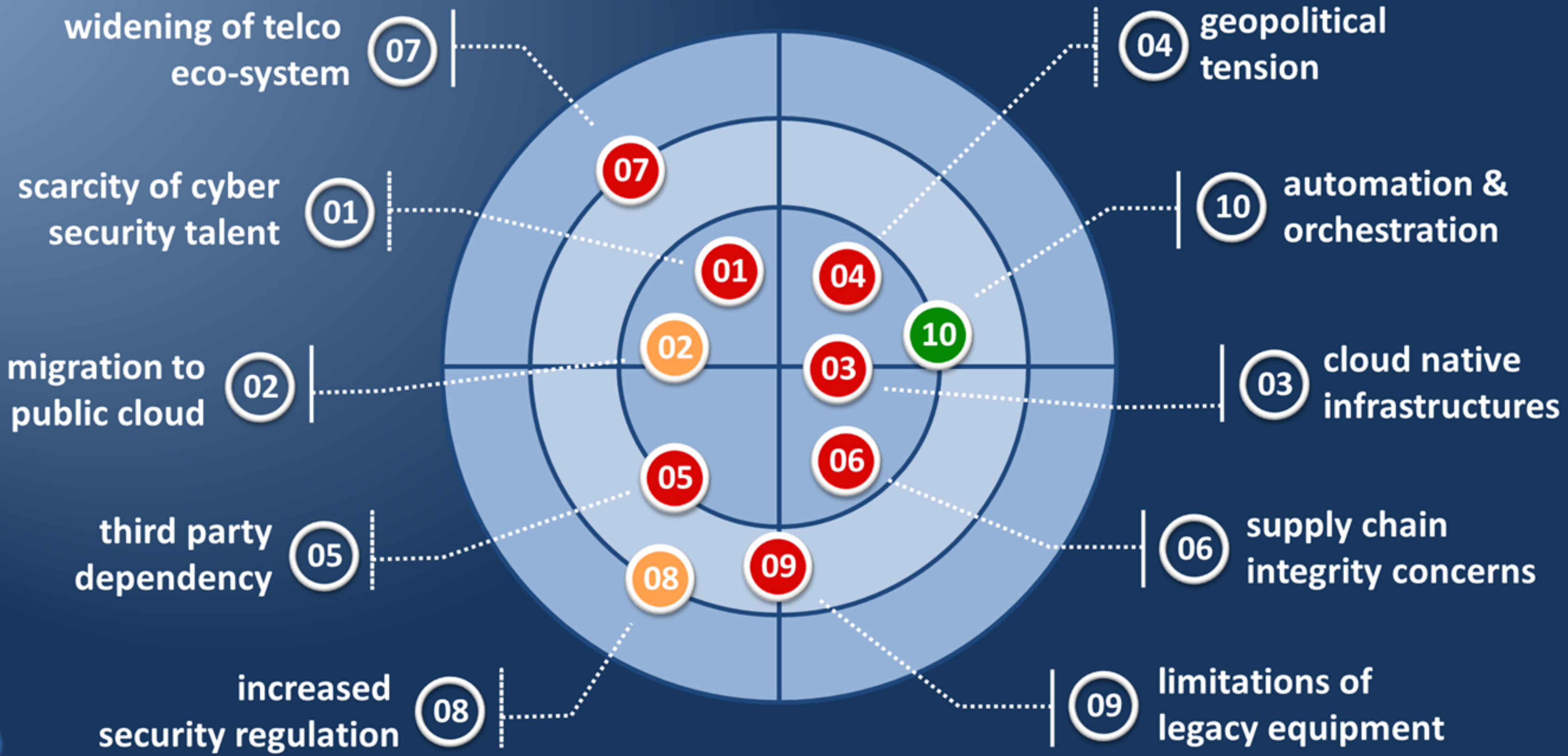
07 **widening of telco eco-system.** The telco ecosystem is gradually expanding, not only through the advent of new technologies (e.g. cloud, Open Radio Access Network (O-RAN), edge computing) but also due to new players entering the market. This calls for specific security practices that deal with the increased complexity and the multitude of interfaces towards new (not necessarily trusted) entities and technologies.

08 **increased security regulation.** Upcoming regulation, both at national and European level, will come with new security obligations and put pressure on CISO teams. Prominent examples include the European Cyber Resilience Act (CRA), the revised Network and Information Security (NIS2) Directive, the Critical Entities Resilience (CER) directive and the new 5G security guidelines under the European Electronic Communications Code (EECC). A potential positive effect is that this offers an incentive to elevate internal security discipline (compliance) and improve the reliability of IT products and services.

09 **limitations of legacy equipment.** Legacy infrastructure that coexists alongside newer technologies increasingly results in complex environments that are inherently hard to protect. This challenge is not necessarily new, but rapidly becoming more urgent because migration to public cloud (topic #02) will increase the external exposure of legacy systems.

10 **automation and orchestration.** In the monitoring, response and intelligence space, automation may become the game changer that closes (or at least reduces) the present gap between attackers and defenders (not least in terms of speed). The potential of automation also extends to areas such as DevSecOps and third party assurance and might even contribute to talent retention (topic #01) since it will allow security specialists to focus on more fulfilling duties.

etis TNO innovation for life



07 widening of telco eco-system

01 scarcity of cyber security talent

02 migration to public cloud

05 third party dependency

08 increased security regulation

04 geopolitical tension

10 automation & orchestration

03 cloud native infrastructures

06 supply chain integrity concerns

09 limitations of legacy equipment

TELCO SECURITY LANDSCAPE 23

Featured: Swisscom’s automation journey

Swisscom is strongly embracing the **automation and orchestration** opportunities that are described in this year's telco security landscape (topic #10). In our modern and ever-changing threat landscape a Security Operations Center (SOC) must be able to cope with many different threats and whether the team consists of two or twenty devoted security professionals, we believe that automation is the key to a successful threat detection and response programme.

To master the automation challenge, Swisscom deployed a Security Orchestration Automation and Response (SOAR) solution in 2020. In the three years that have passed, our analysts have clearly come to work more efficiently, not least because many repetitive tasks have been taken off their hands. This was made possible by integrating case management systems with security appliances, asset databases and ticketing tools across our ecosystem to allow the security analyst to focus on the analysis itself. If analysts need to perform the same action more than twice, we automate it. We focus on repetitive tasks but only automate what makes sense to help the human analyst. In doing so we have freed our analysts from fairly monotonous and unfulfilling duties, reducing the risk of alert fatigue and potentially missing a relevant event or attack.

Moving forward, we want to make even greater use of the possibilities of automation and orchestration because scalability is crucial for our security operations. Also taking the **scarcity of security talent** (landscape topic #01) into consideration, it will allow us to continuously cover more threats without having to hire a great many analysts. And in the not-too-distant future, automation coupled with integrated machine learning might even support analysts directly in their decision making, e.g. on the most appropriate course of action in response to a particular event.

Lorenz Inglin
Head of Cyber
Defense at Swisscom

Closing words

The telco industry is undergoing massive changes, both from a business and a technology perspective. Meanwhile the political and societal environment in which telecoms providers need to operate is far from stable and the adversaries that target telco infrastructures are evolving at an exponential rate. Amidst all this, the ET-ISAC hopes to contribute to the continued evolution of telco security postures by actively collaborating on the topics outlined in this report.

Obviously, this concise overview of strategic developments does not capture every nuance or detail and for each topic that was included in the landscape the most appropriate way forward will often depend on an organisation's particular context and circumstances. Nonetheless we hope this security landscape will aid both telecoms providers and organisations in other (vital) industries to refine their security priorities for the upcoming year(s). The ET-ISAC would also welcome further dialogue with fellow security professionals on the presented topics. If you are interested in such engagement or would like to hear more about the specific activities that the ET-ISAC is undertaking this year, please reach out to us via isac@etis.org.

The telco security landscape will be reviewed and updated in the fourth quarter of this year and the ET-ISAC will release a new edition early 2024. It will be complemented with a more technical reflection on current threats around the summer.

About

ETIS - the Community for Telecom Professionals in Europe, is a partnership-based foundation that drives collaboration and information sharing among European telecommunications providers. Its mission is to enable parties across the telco ecosystem to reach their strategic objectives and improve their business performance. To this end, the ETIS Central Office in Brussels coordinates a great variety of working groups and task forces, all populated with experts and stakeholders from across the European telco industry. These groups include the ETIS Information Security WG (oriented at CISOs and representatives thereof) and the ETIS CERT-SOC Telco Network (focused on intelligence sharing and operational collaboration), that jointly also comprise the European Telecommunications ISAC (ET-ISAC). ETIS is entirely governed by telcos and actively collaborates with bodies such as ENISA, ETNO, ITU and the GSMA where appropriate. The ET-ISAC is part of a larger network of vital industry ISACs that spreads all across Europe. For more information please visit the working group pages on www.etis.org.

TNO - The Netherlands Organisation for Applied Scientific Research, is one of Europe's leading R&D and innovation bodies. Its mission is to strengthen the competitiveness of companies and the welfare of society in a sustainable way. TNO is a non-profit organisation that operates independently and objectively and its many working areas include telecommunications and cyber security. TNO is a longstanding partner of ETIS and a core member of the ETIS Information Security WG. Its role includes coordination of the group's annual security landscaping activity, of which this publication is the result. For more information, please visit www.tno.nl/en/.

etis TNO