# Key Actions to Enable Automation for Mobile Network Security Operations

**Jarno Kämppi and Karo Saharinen**
Jamk University of Applied Sciences, Jyväskylä, Finland

AB7833@student.jamk.fi
karo.saharinen@jamk.fi

**Abstract**. Over time, the landscape of Cyberspace surrounding Internet Service Providers (ISPs) has undergone enduring transformations. Notably, mobile networks, integral to contemporary societal infrastructure, consistently encounter evolving cybersecurity threats and risks. ISP processes have adapted with a persistent focus on optimizing network performance and availability, yet the challenges emerge from a laborious and protracted network change management process, hindering the practical automation of network security. Addressing the rightful demand for the highest level of security from mobile network users, our research question probes: "How can we intensify the emphasis on network security and facilitate the automation of network security operations?" To delve into this, we conducted extensive interviews with ISPs globally, affirming the inherent difficulty in automating security operations. The findings categorize challenges into three domains: Security Culture, Operational Processes, and Tools. Cultivating a security culture demands a pivotal commitment to change from top management, coupled with dedicated time and resources. Essential to this is the enhancement of security competence, extending beyond specialists to encompass network engineering staff. Robust network security not only safeguards against threats but significantly influences various business processes. Initiating a secure network requires ISPs to articulate explicit security requirements during the network procurement process, exerting pressure on vendors to fortify systems with a security-by-design approach at the factory. Critical to this is the secure deployment of networks, integrating comprehensive network hardening during the build phase. However, findings indicate a prevalent oversight where network security configuration changes are often neglected or deprioritized in favor of network performance. Achieving a harmonious balance between security and performance necessitates a predefined agreement on a network security configuration baseline. This collaborative effort involves network security specialists and competent network engineers. To effectively monitor and enforce network security configuration, ISPs require automation-enabled tools with the predefined baseline, offering capabilities for monitoring and enforcing network assets. In conclusion, our research emphasizes the imperative need for a paradigm shift in organizational culture, operational processes, and tool utilization to enhance the focus on network security and enable the critical automation of network security operations within the ever-evolving landscape of Cyberspace.

Keywords: Cyber Security, Mobile Network Operations, Security Operations, Network Change Management.

## 1. Introduction

In contemporary times, businesses and societies heavily depend on mobile networks managed by Internet Service Providers (ISPs). The advent of 5G technology introduces novel cybersecurity requirements due to its seamless connectivity for devices and businesses. The vast interconnection of millions of devices through mobile networks renders these networks increasingly susceptible to cyber threats (Pejanović-Djurišić et al., 2022). While considerable attention is focused on securing end-user devices, it is crucial to underscore the significance of fortifying the network infrastructure for both connection and usage.

Presently, mobile network operators face the challenge of managing diverse technological generations (Teng et al., 2020). Simultaneously, new investments become imperative to align networks with the evolving demands of customers and societies. The obsolescence of aging technologies poses hurdles in acquiring updated software featuring essential security patches while securing skilled resources for maintenance activities becomes challenging as the emphasis shifts toward emerging technologies.

Despite these challenges, the fundamental objective of any corporation or business remains the generation of profit for its stakeholders (Suhaily Maizan et al., 2021). Revenue streams are derived from customer contracts wherein communication service providers commit to delivering contracted services. Consequently, a significant emphasis is placed on network performance, encompassing dimensions such as network availability and data throughput. Presently, security considerations do not hold a prominent position in discussions surrounding network performance, and the augmentation of network security incurs high costs. As a non-profit-generating expense, security competes with other investments that directly impact profitability.

In the context of modern mobile networks, comprising a multitude of assets, manual monitoring and configuration prove to be laborious and costly endeavors (Anirban et al., 2023). In some instances, the sheer volume of network assets makes manual monitoring and enforcement impractical (Lee et al., 2014). To heighten

network security for businesses and societies, there is a need to integrate automation into security operations. Justifying long-term investments in security is essential, as a significant security incident can have far-reaching consequences on trust and reputation. The erosion of trust and reputation, in turn, can exert deleterious effects on the overall well-being of a business. Furthermore, there are identified gaps in network and security management platforms (Steinke et al, 2018).

## 2. Challenge

Given the historical emphasis on the performance and availability of networks, existing business processes align with this central objective (Aykurt et al, 2023). For instance, the network change management process is commonly characterized by its cumbersome and slow nature. Even minor and straightforward alterations to network configurations necessitate navigating through an extended network change management process. Consequently, the immediate automation of network security becomes unattainable.

Automation means we allow technology to monitor and control operations or production (Shetty, 2021). In practical terms, we must place a significant degree of trust in technology, entrusting our business operations to its capabilities. The current solutions for mobile networks are excessively intricate, making the maintenance and operation of networks demanding (Aykurt et al, 2023). Simultaneously, meeting all business targets poses a considerable challenge. Communication Service Providers bear the responsibility of serving as critical infrastructure in our society (Homeland Security, 2015).

In the realm of cybersecurity, Internet Service Providers (ISPs) are obligated to deliver top-tier services under any given scenario. To fulfill these obligations comprehensively, ISPs must establish geo-redundancy for all network assets responsible for carrying traffic. Additionally, every alteration or operation within the network undergoes thorough scrutiny by the change control process to guarantee adherence to all obligations. (Drvodelić Cvitak, 2010). This entails subjecting every modification in network configuration, encompassing alterations in security-related settings, to a meticulous network change management process. The existing operational methodology appears hierarchical, time-intensive, and notably distant from the realm of automation. Frequently key personnel within organizations lack the necessary cybersecurity skills, and there is a need to enhance cybersecurity competencies. (Aaltola et al, 2022).

## 3. Research Methodology & Analysis

We opted for the qualitative research methodology to address the query "Why is automation for Security Operations not enabled?" In qualitative research, our exploration centers on comprehending the perspectives of individuals or groups regarding the problem (Creswell, 2014).

Over the course of multiple mobile network deployments, we have consistently observed a recurring pattern during the implementation of cybersecurity measures in these networks. During the network launch phase, there is a pronounced emphasis on optimizing network performance, as the marketing and contracts to customers revolve around significantly enhanced speeds and reduced latency. The competition among Internet Service Providers (ISPs) intensifies as each endeavours to offer the most high-performing network, thereby attracting the highest number of subscribers. Moreover, there is a collective aspiration among ISPs to be the first to introduce 5G services. These pursuits bind a considerable amount of resources, garner undivided attention, and elevate network performance as the paramount priority.

Throughout these network deployments, we have identified analogous challenges associated with the implementation of cybersecurity measures. Some of these challenges persist even after the network has been launched and transitioned into production. Our research inquiry seeks to address the question "How can we enhance the emphasis on network security and facilitate the automation of network security operations?". In pursuit of this answer, we conducted interviews with senior professionals in the telecommunications and security domains from ISPs worldwide.

### 3.1 Questionnaire & Interviews

The development of the Semi-Structured Interview template emanated from insights derived from experiences and challenges encountered during the implementation of cybersecurity measures in mobile network deployments. Employed for the collection of open-ended qualitative data, the semi-structured interview approach adheres to predetermined discussion topics (Creswell, 2013). This approach facilitates focused conversations while allowing for the exploration of new areas.

The interview template, was segmented into three overarching Themes, namely:

1. Organization & Security Establishment
2. Operational Processes
3. Tools and Methods Utilized in Operations

Each Theme is accompanied by a defined discussion objective. In pursuit of these objectives, we formulated key questions designed for elucidation through open discussion.

Within Theme 1, we gathered data about the organization under investigation and how security is instituted within the corresponding organization. This entailed a concentrated examination of organizational structure and the establishment of security governance across the organizational framework. In Theme 2, a detailed discussion unfolded regarding the operation of both mobile network operation and its security operation. The principal objective was to conclude the authority of executing the network security configuration changes, with a secondary objective focused on determining ownership of network asset security. Theme 3 delved into an exploration of the tools employed for security operations and areas where additional support is deemed necessary. The interviews, conducted via video conference, were recorded to facilitate comprehensive analysis. Interviews were anonymous and material was only shared with participants, and the identity of the Internet Service Provider (ISP) and its physical location have been safeguarded as confidential information.

### 3.2 Data Analysis

The data analysis process employed Microsoft Office tools and encompassed the following sequential steps:

1. Integration of Data
2. Data Cleansing
3. Data Categorization
4. Data Anonymization
5. Preliminary Analysis
6. In-Depth Data Analysis
7. Concluding Remarks

In the first step, all interview data was consolidated into a unified Excel table. Subsequently, in the second step, any extraneous or unnecessary data entries were removed. The third step involved categorizing the data based on the geographical presence of the Internet Service Provider (ISP). Following this, in step four, the data underwent anonymization, involving the removal of respondent-specific information. The fifth step comprised an initial analysis, while the sixth step involved a comprehensive examination of the data. Finally, in the seventh step, conclusive insights and findings were drawn.

## 4. Results

Following the analysis phase, the outcomes were categorized into three subdomains: Security Culture, Operational Processes, and Tools. The conclusions are evident; however, as anticipated, variances in Internet Service Provider (ISP) responses were detected. These can be observed from the results in Table 1. It can be deduced that the operational processes of ISPs are comparable. Our thorough investigation provides evidence supporting the limitation imposed on the implementation of automation in security operations.

**Table 1.** ISP responses to key questions.

| | ISP 1(Global) | ISP 2 | ISP 3 | ISP 4(Global) | ISP 5 |
|---|---|---|---|---|---|
| ***Security culture*** | | | | | |
| Is cybersecurity policy implemented? | Yes | Yes | Yes | Yes | Yes |
| Is cybersecurity measured?(KPI) | Yes | Yes | No | Yes | Yes |
| Is cybersecurity part of business governance? | Yes | Yes | No | Yes | No |
| Is dedicated cybersecurity department established? | Yes | Yes | Yes | Yes | Yes |
| Format of Security Operations Center (SoC) | Outsourced | Outsourced | Outsourced | Inhouse Central, several ISP's | Inhouse |
| ***Operational processes*** | | | | | |
| Format of Network Operations Center (NoC) | Inhouse | Inhouse | Inhouse | Inhouse | Inhouse |
| Change Management process implemented | Yes | Yes | Yes | Yes | Yes |
| SoC authorized to execute network configuration | No | No | No | No | No |
| Who monitors network security? | SoC | SoC | SoC | SoC | SoC |
| Who owns network asset security? | NW Operations | NW Operations | NW Operations | NW Operations | NW Operations |
| NoC authorized to execute network configuration | Yes, change control | Yes, change control | Yes, change control | Yes, change control | Yes, change control |
| ***Tools*** | | | | | |
| SIEM (Security Incident and Event Management) | Yes | Yes | Yes | Yes | Yes |
| IAM (Identity and Access Management) | Yes | Yes | Yes | Yes | Yes |
| Manual Annual Security Audits | Yes | Yes | Yes | Yes | Yes |
| Manual Annual security hardening monitoring | Yes | No | Yes | Yes | No |

### 4.1 Results, Security Culture

The outcomes of the interviews reveal that Internet Service Providers (ISPs) commonly maintain distinct Chief Information Officer (CIO) organizations and Chief Network Officer/Chief Technology Officer (CNO/CTO) organizations, each operating autonomously with unique business objectives. In all surveyed ISPs, a Security organization is overseen by the Chief Information Security Officer (CISO), reporting directly to the CIO.

In the rapidly evolving contemporary landscape, safeguarding assets becomes indispensable for organizational resilience. The swift evolution of technology and cyberspace, encompassing cybercrime and hacking techniques, presents a formidable challenge for ISPs striving to keep pace. All ISPs interviewed have instituted a dedicated Security organization to protect their assets and operations. This contemporary security apparatus aligns with defined business strategies and adapts to business requirements set by owners. ISP security organizations play a pivotal role in defining security policies and ensuring their comprehensive implementation, continuous security monitoring, and ongoing improvement across the organization. Meanwhile, the network operations department remains steadfast in its commitment to achieving optimal network performance.

Given that mobile networks constitute integral components of societal critical infrastructures, heightened attention is imperative for effective Cyber Security Management. The Cyber Security process is executed and governed across the organization through an Information Security Management System (ISMS), representing a systematic approach to managing Information Security processes and activities. According to insights gathered from interviews, there is a crucial need to elevate the perceived value of security and enhance the comprehension of security risks among network operations staff. The personnel within Network Operations often lack the necessary expertise to execute network security operations, or it is not explicitly designated as part of their responsibilities. Dawson and Thomson (2018) share a common conclusion and emphasize that individuals working in the cyber domain should possess a blend of technical expertise and specialized knowledge within the respective domain. Despite the existence of Key Performance Indicators (KPIs) aimed at monitoring security quality, our research reveals a consistent prioritization of business targets over security objectives.

Further research indicates that Global ISPs typically adopt a structured approach to establishing security frameworks, often driven by a dedicated central Security organization throughout the corporation. However, this central entity lacks the authority to alter operational processes, which remain under the purview of business owners, particularly in network operations. Conversely, smaller local ISPs operating within a single country tend to exhibit more flexible approaches to cybersecurity governance.

In a broader context, there exists a general inclination and top management support for automation. In some instances, automation is explicitly established as a collective goal, predominantly motivated by considerations of financial savings.

### 4.2 Results, Security Operations, and Network Operations Processes

In accordance with our research findings, it is evident that the Security Operations Center (SOC) and Network Operations function as distinct entities, each possessing autonomous Processes, Tools, People, and Budget allocations. This separation is presented in Figure 1.

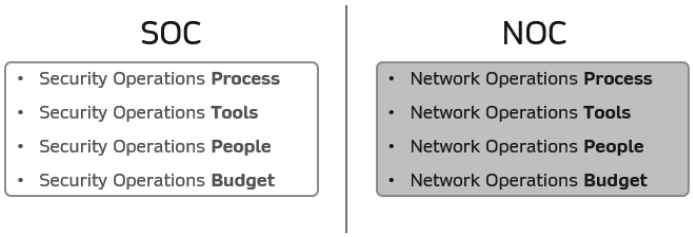


**Figure 1. The Security Operations Center and Network Operations Center are independent organizational units.**

The Security Operations Center (SOC) is tasked with executing security operations, encompassing activities such as security monitoring, threat detection, security maintenance, and managing security incidents. Network security configuration changes requested by the SOC follow the same aforementioned change management process.

In contrast, Network Operations oversees the management and upkeep of the mobile network infrastructure, with a broad mandate covering network planning, deployment, optimization, monitoring, troubleshooting, and maintenance. Every alteration in the network undergoes an extensive network change management process, involving detailed documentation of change requests. During the execution of the change management process, the change advisory board analyzes the potential network impact, subsequently accepting or rejecting the requested change.

Our research findings indicate that SOC staff lacks the authority to implement changes in the network directly, while Network Operations is permitted to execute changes through the network change management process. This dichotomy results in prolonged lead times for network security changes. Moreover, the change advisory board and network operations staff often struggle to comprehend the impact of network security configuration changes.

The reasons prohibiting the automation of security operations can be summarized as follows:

1. The application of the Network Change Management process for every network change.
2. Restrictions on the SOC to enact security configuration changes in the network.
3. The change advisory board or network operations staff may not fully grasp the impact of security configuration changes.

Addressing security noncompliance and seeking resolution necessitates collaborative efforts between at least two distinct organizations, namely the SOC and Network Operations. Our research underscores the existence of significant barriers hindering the achievement of automated network security operations.

### 4.3 Results, Tools for Security Operations

Based on the interviews conducted, Internet Service Providers (ISPs) employ a diverse range of tools for the implementation and monitoring of their security posture. Many of these tools necessitate specialized expertise and manual labour. In instances where this specialized expertise is lacking internally, ISPs may procure it from third-party suppliers (3PP), posing a challenge to the continuous monitoring of security posture. Some security-related activities are performed on an annual basis, potentially leaving security vulnerabilities unaddressed for extended periods.

All ISPs surveyed utilize a Security Incident and Event Management (SIEM) tool for threat detection and an Identity and Access Management (IAM) tool to govern and oversee network access. The SIEM tool, employed by the Security Operations Center (SoC), automates threat detection monitoring. However, the SoC is not authorized to enact changes in the network, necessitating network operations to enforce security posture through a change management process. Network operations staff controls access to network assets using IAM. SIEM and IAM serve as foundational elements for maintaining security posture.

Our research also indicates that ISPs routinely conduct manual security audits, encompassing activities such as vulnerability assessments (both internal and external), manual hardening monitoring, and, in some cases, penetration testing. Regulatory requirements often guide ISPs to perform these manual audits annually.

ISPs recognize the need for improved tools to visualize the state of network security, monitor network security hardening, and manage software patching for network assets.

## 5. Proposals

Internet Service Providers (ISPs) have allocated substantial resources and financial investments to establish cybersecurity practices and implement cybersecurity frameworks within their networks. However, despite these investments, the realization of security automation requires concurrent development in three critical domains: Security culture, Business processes, and Tools.

### 5.1 Proposals for Security Culture

Establishing a robust security culture requires proactive leadership from top management, demanding a significant investment of both time and resources. The gradual cultivation of such a culture necessitates a systematic, incremental approach, acknowledging that its establishment is a process that unfolds over time. At present, the Security Operations Center (SoC) is responsible for overseeing security monitoring and proposing security configuration enhancements for network assets, subject to approval or rejection by network operations.

To empower network engineering staff to take responsibility for security monitoring and configuration of the assets they oversee, there is a critical need to enhance their security competence. Network asset owners must gain a comprehensive understanding of the impact of security risks, acknowledging accountability for security configuration as an integral part of operational processes. The overarching goal is to instigate change and development among individuals executing business processes, fostering a security culture. The ultimate objective is to equip Network Security Operations personnel with the competencies needed to conduct fundamental security monitoring and configuration for the assets they manage, enabling them to be accountable for the security operations of these assets.

The Information Security Management System (ISMS) acts as the framework for establishing the security posture objective and is crafted and overseen by a specialized security organization. The heightened awareness of security risks within the network operations department facilitates their substantial engagement in the formulation and execution of ISMS. This strategy guarantees a thorough evolution in the security culture, contributing to the advancement of the company's ISMS to the next level.

In addition to basic security training, fostering awareness of cybersecurity risks could be achieved through participation in or organization of Cyber Exercises and the execution of penetration testing by ethical hackers within the similar ISP environment.

The ongoing transition of networks from virtualized environments to cloud-native environments represents a fundamental shift in network operations, necessitating competence development. This transformation presents an opportune moment to align actions for security and network operations competence development.

Research findings emphasize the independence of the Security Operations Center and Network Operations, each executing their respective processes, utilizing distinct tools, personnel, and budgets. To enhance the security culture, some responsibilities of the Security Operations Center should transition to Network Operations. The development of network security competence among network operations staff should encompass security monitoring and configuration of network assets as integral components of their responsibilities. Meanwhile, the Security Operations Center should hone its focus on and specialize in IT infrastructure security monitoring and security incident management. The evolved organizational diagram with responsibilities is presented in Figure 2.

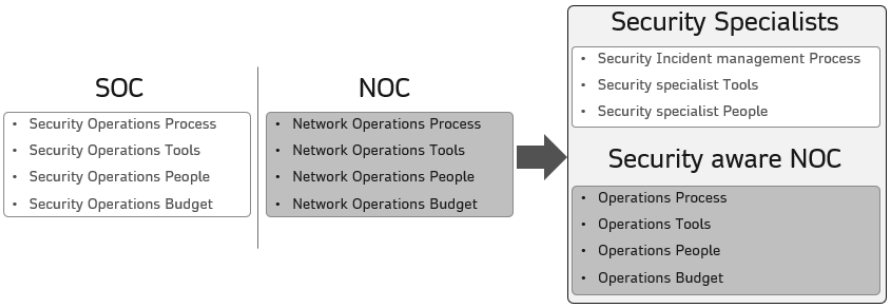


**Figure 2. Evolving security culture from separated SOC and NOC to security aware NOC.**

To foster continuous development in cybersecurity culture, it is imperative for telecom standardization and regulation to keep pace with the rapid evolution of cyberspace. Telecom standards hold significant authority among telecom vendors, shaping the development of telecom equipment and software in adherence to established norms like 3GPP. Ensuring a perpetual evolution of telecom standards aligned with the dynamic changes in cyberspace is crucial.

While local legislation and regulation are adjusting to the transformations witnessed in cyberspace, this adaptation tends to lag behind the rapid evolution of cyberspace. Internet Service Providers (ISPs) find themselves regularly responding to the evolving requirements dictated by local regulations, and concurrently, ISPs are stipulating corresponding prerequisites for telecom vendors.

## 5.2 Proposals, Security Operations, and Network Operations Processes

Internet Service Providers (ISPs) conduct their business and operational activities in accordance with established business processes. Embedding cybersecurity effectively within key business processes is crucial for ensuring an adequate cybersecurity implementation. However, the swift evolution of cyberspace presents a significant

challenge in maintaining the relevance and efficacy of these processes. Our research underscores the profound impact of two specific business processes on the landscape of cybersecurity automation.

1. **Operations Process:** For the facilitation of automation in network security operations, immediate acceptance of network security configuration changes becomes imperative. To circumvent the intricate network change management process, network operations must cultivate a methodology wherein the network security baseline is collaboratively agreed upon by network security specialists and network operation experts. Following this agreement, the security baseline undergoes meticulous network performance verification and approval in staging or laboratory environments before transitioning to the production phase. The objective is to establish a network security baseline recognized for its concurrent high performance and security. This collaborative development involves ongoing collaboration with security specialists and network operation experts to ensure the agreed-upon network security baseline is well-balanced and meets both high-performance and security requirement. A proposed example for a collaborative process can be observed in Figure 3.

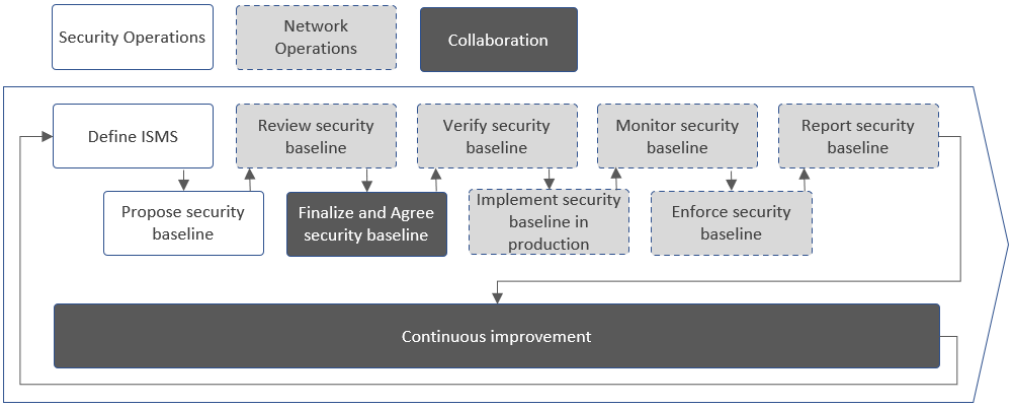


**Figure 3. Collaborative operations process, including Security baseline setup, verification, implementation, monitoring, and automated enforcement and continuous improvement.**

2. **Network Procurement Process:** Achieving a secure network with the desired network security baseline from its inception necessitates clear articulation of security requirements during the network procurement planning phase. As the network procurement planning process commences, it is vital to precisely and professionally define security requirements. This requires the assurance of sufficient cybersecurity competence and a comprehensive understanding of business dynamics. Clear definition of cybersecurity requirements ensures that telecom vendors, responding to requests for pricing, commit to fulfilling these security standards. With a procurement process attuned to security considerations, ISPs exert influence on telecom vendors, compelling them to adopt a security-by-design approach and undertake network asset hardening during the network build process based on the defined network security requirements. However, if an ISP exclusively prioritizes achieving a high-performing network at the lowest possible cost, this inevitably results in the deprioritization of cybersecurity requirements in the procurement process.

## 5.3 Proposals, Tools for Security Operations

The foundation of automation lies in the accessibility of suitable tools. Considering the integral role of telecom networks in society's critical infrastructure, there exists a crucial imperative for steadfast trust and confidence in the ability of machines to execute commands directed at network assets. Our investigative endeavours have revealed that Internet Service Providers (ISPs) need support in two pivotal functional areas.

### *5.3.1 Network Security Configuration*

Within the domain of monitoring network security configuration, ISPs require a tool proficient in establishing communication with network assets and presenting a visual representation of the adherence to network security requirements. The effectiveness of this tool in enforcing network security configuration hinges on its capability to compare the existing network security configuration with the desired baseline. Subsequently, it should establish a connection with the network asset and execute the relevant configuration operations. To facilitate this functionality, the tool must incorporate the collectively agreed-upon network security configuration baseline and execute pertinent commands through scripts on the network assets. Importantly, this same tool

can be judiciously employed for monitoring security hardening procedures and, additionally, for the implementation of security hardening measures. The specific procedural phases that an automated tool for network security configuration should encompass are highlighted in Figure 4.

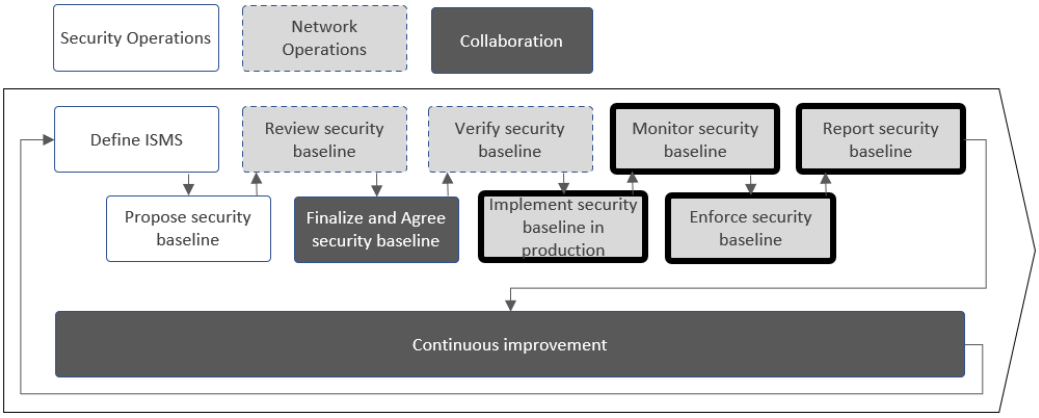


**Figure 4. Here are highlighted the procedural phases that can utilize an automated tool for network security configuration.**

### *5.3.2 Network Software Patch Management*

In an ideal scenario, Network Software Patch Management tools should be provided either directly by network vendors or, if supplied by a third-party partner, seamless integration with the mobile network vendor's software catalogue is a necessity. This integration is crucial, establishing a unified and interconnected methodology for managing network software patches, thereby enhancing the network's capacity to promptly address vulnerabilities. The automated administration of network software patches is a pivotal element in ensuring the security and resilience of a network. This process encompasses three comprehensive functions: Inventory and Asset Management, Software Patch Deployment, and Integrations.

1. **Inventory and Asset Management:** Involves maintaining a precise inventory of all software within the network per vendor, a crucial aspect for identifying systems requiring patching. Continuous monitoring of software levels is essential.
2. **Patch Deployment:** Utilizes patch management tools, this phase involves deploying software patches across the network. Automation within this process ensures uniformity and reduces the time between patch release and deployment. Before deploying patches to the production network, a verification process is employed in a test environment to identify potential problems, preventing unintended disruptions to critical services. Implementation of a patch deployment schedule is crucial to minimize disruption to business operations, scheduling patches during maintenance windows or low-traffic periods to reduce the impact on users. A predefined rollback plan is in place in case a patch causes unexpected issues, ensuring swift reversion to a stable state if problems arise.
3. **Integrations:** To receive information for Network Software patch management these integrations are needed.
    - Integration with a Security Incident and Event Management (SIEM) solution correlates patching activities with security events, enhancing the organization's ability to detect and respond to potential threats.
    - Vendor integration is necessary to stay informed about patch releases by subscribing to vendor notifications and security alerts, ensuring the organization promptly addresses critical vulnerabilities.
    - Integration with an endpoint protection solution is required to provide a layered defence against security threats, ensuring comprehensive addressing of both vulnerabilities and active threats.

## 6. Conclusion

Security permeates every aspect of an organization, impacting each individual within it. A holistic perspective is essential for the successful implementation of security measures throughout the organization. The strength of

security is inherently linked to its weakest point; should a vulnerability exist, a determined hacker will inevitably exploit it, and this exploitation is only a matter of time. Our research emphasizes that the successful automation of network security operations necessitates concerted efforts across three essential domains: Security Culture, Operational Processes, and Tools. Disregarding any of these domains results in suboptimal outcomes due to a lack of alignment. When prioritizing these domains, our findings indicate that Security Culture takes precedence, as it constitutes a pivotal factor for success. Well-implemented security protocols are grounded in the actions of individuals and their collective will. A strategically defined security direction, complemented by individuals possessing competence, collaboration skills, and motivation, plays a pivotal role in guiding the organization toward the envisioned outcomes. The desired results materialize when there is a collective commitment to achieving them. Given the heightened emphasis on network performance, it is imperative to elevate the prioritization of security through regulatory guidance. This involves a proactive approach by local regulatory bodies in each country, necessitating the revision and enhancement of their existing security requirements. Subsequently, these refined security standards should be explicitly communicated and mandated for adherence by Internet Service Providers (ISPs). This strategic regulatory intervention is essential for reinforcing the security landscape within the telecommunications infrastructure, aligning with the prevailing imperative to enhance security in tandem with the prioritized focus on network performance.

## References


Pejanović-Djurišić, M. and Kuklinski, S. (2022). 5G Security Landscape: Concept and Remaining Challenges. *30th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, 2022, pp. 1-4, https://doi.org/10.1109/TELFOR56187.2022.9983722.

Teng, C. C., Chen, M. C., Hung, M. H. and Chen, H. J. (2022). End-to-end Service Assurance in 5G Crosshaul Networks. *21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Daegu, South Korea, 2022, pp. 306-309, https://doi.org/10.23919/APNOMS50412.2020.9236977.

Suhaily Maizan, A. M., Nurul Husna, A. A. K. and Wan, A. S. (2021). Determinants of Profitability on Listed Telecommunications Service Providers Companies: Evidence in Bursa Malaysia. *Journal of Research in Business and Management Volume 9 ~ Issue 1 (2021)* pp: 22-28, ISSN(Online):2347-3002. Available at https://www.questjournals.org/jrbm/papers/vol9-issue1/4/C09012228.pdf

Anirban, D., Asif Imran, A. T. M. and Chinmay, B. (2023). Network Automation: Enhancing Operational Efficiency Across the Network Environment, *INTERNATIONAL CENTER FOR RESEARCH AND RESOURCES DEVELOPMENT*, ISSN Number: 2773-5958, https://doi.org/10.53272/icrrd

Lee, S., Levanti, K. and Kim, H. S. (2014). Network monitoring: Present and future, *Computer Networks*, Volume 65, 2014, pp. 84 – 98, ISSN 1289-1286, https://doi.org/10.1016/j.comnet.2014.03.007.

Shetty, R. S. (2021). 5G Mobile Core Network: Design, Deployment, Automation, and Testing Strategies. Apress Skillsoft version, Available at https://2masteritezproxy.skillport.com/skillportfe/main.action?assetid=154626

Homeland Security, (2015). Communications Sector-Specific Plan, An Annex to the NIPP 2013, Available at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf

Creswell, J. (2014). Research design; qualitative, quantitative, and mixed methods approaches. 4th ed. United Kingdom: SAGE Publications

Creswell, J. (2013). Qualitative Inquiry and Research Design: Choosing Among Five Approaches. 3rd ed. United Kingdom: SAGE Publications

Dawson, J. and Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. Frontiers in psychology, https://doi.org/10.3389/fpsyg.2018.00744

Aykurt, K. and Kellerer, W. (2023), Autonomous Network Management in Multi-Domain 6G Networks based on Graph Neural Networks, *2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*, Madrid, Spain, 2023, pp. 338-341, doi: https://doi.org/10.1109/NetSoft57336.2023.10175480

Steinke, M. and Hommel, W. (2018). Overcoming Network and Security Management Platform Gaps in Federated Software Networks," *2018 14th International Conference on Network and Service Management (CNSM)*, Rome, Italy, 2018, pp. 295-299. https://ieeexplore-ieee-org.ezproxy.jamk.fi:2443/stamp/stamp.jsp?tp=&arnumber=8584959

Drvodelić Cvitak, L. D. and Car, Ž. (2010). Impact of agile development implementation on configuration and change management in telecom domain, *The 33rd International Convention MIPRO*, Opatija, Croatia, 2010, pp. 377-381. https://ieeexplore-ieee-org.ezproxy.jamk.fi:2443/stamp/stamp.jsp?tp=&arnumber=5533407

Aaltola, K., Ruoslahti, H. and Heinonen, J. (2022), Desired Cybersecurity Skills and Skills Acquisition Methods in the Organizations, *21st European Conference on Cyber Warfare and Security, Chester, UK, 2022, pp. 1-9,* https://papers.academic-conferences.org/index.php/eccws/issue/view/7/8