Security Operation Center Methodology for 5G Networks

Miklós Orsós, Roland Török, Csaba Faragó, Benjamin Antalfia, Eszter Kail, Anna Bánáti

John von Neumann Faculty of Informatics, Óbuda University, Bécsi út 96/b, 1034 Budapest, Hungary, orsosm@stud.uni-obuda.hu, torok.roland@kiber.uni-obuda.hu, csaba.farago@stud.uni-obuda.hu, antalfiabenjamin@stud.uni-obuda.hu, kail.eszter@nik.uni-obuda.hu, banati.anna@nik.uni-obuda.hu

Abstract: The utilization of the recently introduced yet rapidly proliferating new generation of 5G mobile communications offers many new advantages. However, it has also brought with it the introduction of many new services and technologies compared to its predecessors. This, combined with the ever-expanding threat landscape, means that traditional methods of protection are no longer sufficient. Security Operation Centres (SOCs) are not only popular today, they are becoming an essential part of many organisations. Consequently, the development of a 5G SOC methodology for 5G technology has become progressively imperative. This paper presents our 5G SOC methodology. The SOC developed at Óbuda University, designed for monitoring, analyzing, managing data and log data for incident handling has been specifically tailored for 5G-specific usage. The showcased results underscore the utility and success in the pursuit of pioneering a 5G SOC methodology.

Keywords: 5G; Security Operation Centers; Methodology; InfoLab

1 Introduction

Securing a modern IT infrastructure, particularly with the proliferation of mobile devices exceeding billions, poses a formidable challenge. This concern is amplified in the context of 5G networks, the latest mobile telecommunication standard established by 3GPP. Initiated in 2018, the multi-phased deployment of 5G aims to achieve lower latency and superior bandwidth compared to its predecessors. The 5G network is structured with multiple layers, including base stations, control function nodes of the core network and handling of the user equipment [1]. As of today, the network became much more than a regular communication networks with the increase of IoT tools, autonomous cars and healthcare. The critical need for adequate built in security arrangements is clear, although this can be a long and tedious process to implement completely [2].

Addressing the intricate security needs of such a robust infrastructure has led to the growing popularity of Security Operation Centers (SOCs) as well as general cybersecurity in recent years. Setting up a valid environment is apparently quite difficult due to the lacking definition of SOCs as discussed in this report [3].

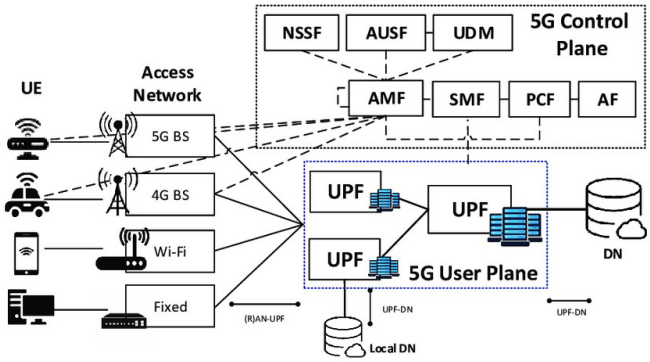

Figure 1
Architecture of 5G network [7]

The absence of documentation about this topic raises an interesting question, as this report [4] states quite a few key elements about improving the implementations of SOCs. The report also arranges a lot of statistics about each skill that an analyst requires. Building such an environment for 5G networks is just as a complex task and is very important because the search for the perfect frameworks seems like a never-ending process [5]. In the subsequent sections of this paper, we present a proposal on the efficiency of integrating a comprehensive SOC methodology on the 5G network, augmenting the inherent security measures already embedded within the network infrastructure.

1.1 5G Networks

The 5G mobile network is spreading more and more widely in industry, public administration, healthcare [6], and everyday life, so it is essential to investigate security issues. The new technology and its deviation from the previous generations also contain new security risks and vulnerabilities, which means that it is necessary to adapt the previous methods on the one hand, and to develop new methods on the other hand. The 5G system uses the same elements as previous generations: the user equipment (UE), which is itself a mobile station, the radio access network (RAN) and the core network (CN), as shown in the Figure 1:

User Equipment (UE): This element is a device connected to the 5G network, which can be a smartphone, tablet, laptop or any other device that supports 5G connection [7]. Each UE communicates with the network through the RAN, thereby accessing the Internet and other services provided by core network.

Radio access network (RAN): Its purpose is to connect the user equipment (UE) and the core network (CN). A RAN includes antennas, base stations, and other equipment that provides wireless coverage in a given area. 5G RAN is designed to operate in three frequency bands (low, medium and high). Low-band spectrum provides wide coverage, while mid-band spectrum provides higher data transfer rates. Broadband spectrum, also known as millimeter wave (mmWave), offers the highest data transfer rates, but with limited coverage [7].

Core network (CN): This element is responsible for the operation and management of traffic between user equipment (UE) and the Internet. This includes such things as: switches, routers, servers, as well as equipment that provides the necessary infrastructure for the 5G network. The 5G core network is designed to support multiple use cases, such as enhanced mobile broadband, mass machine-type communications, and ultra-reliable, low-latency communications [7]. The core network uses a cloud-based service-based architecture (SBA) to support session management, authentication, security, and traffic aggregation of connected devices, which requires a complex interconnection of network functions. The components of the 5G core network are: Application Function (AF), Authentication Server Function (AUSF), Core Access and Mobility Management Function (AMF), Data network (DN), e.g. operator services, Internet access / 3rd party services, Network Exposure Function (NEF), Network Slice Selection Function (NSSF), NF Repository Function (NRF), Policy Control Function (PCF), Session Management Function (SMF), Unified Data Management (UDM), User plane Function (UPF) [7].

Network Function Virtualization (NFV) offers a solution that abstracts and virtualizes network functions from dedicated hardware devices to software-based implementations. This implementation is particularly useful in the context of the 5G core network, where scalability, flexibility and resource efficiency are key. In traditional networks, various network functions are implemented as separate hardware devices, whereas NFV transforms these functions into software-based units, so-called virtualized network functions (VNFs). These VNFs can also be run on general purpose servers. NFV has key components in 5G Core. One is the virtualization layer, which provides the infrastructure to run VNFs. It includes containerization technologies that allow multiple instances to run on the same physical hardware. The other is the NFV Orchestrator, which is important for life cycle management. And if we discuss integration in the 5G Core architecture, we must mention Service Management and Organization. The SMO is responsible for end-to-end service organization and management. It is also linked to NFVO and thus coordinates the deployment and scaling of VNFs in the 5G network. NFV is integrated into various 5G core network functions such as AMF, SMF, UPF, etc. These functions can also be virtualized to increase flexibility and scalability [8].

1.2 Security Operation Center

In traditional computer networks, a Security Operations Center (SOC) is a centralized solution within an organization responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents. It's a critical component of an organization's cybersecurity strategy and infrastructure. The primary goal of a SOC is to enhance an organization's security posture by rapidly detecting and responding to cybersecurity threats, minimizing the impact of incidents, and continuously improving security measures based on insights gained from incident analysis and threat intelligence. A SOC traditionally consists of three main components:

People: In a traditional SOC, tasks are assigned according to tiers, which is a measure of an individual person's knowledge. A Tier 1 analyst i.e. 'First Responder' needs basic programming and networking knowledge. The Tier 2 analyst needs a higher level of technical knowledge as he/she should be able to handle incident response. Tier 3 is already the threat hunter level, here a deep data analyst and penetration testing background is expected.

Process: The average shift of a security analyst starts with checking the security alert queues, for which they mostly use some kind of ticketing system. It is common that the SIEM, the software that generates the alarms, can cause false positives, which is why the security analyst's task is primarily to confirm whether the alarm is a real security incident or not. If a positive result has been confirmed based on the inspection of the incident, it should be forwarded to the investigators or relevant security officials for action. Otherwise, the message may be ignored as a false positive finding. If the security analyst cannot resolve the given ticket, the task will be forwarded to a level 2 employee for investigation. There is also a level 3 incident investigator if the task requires further escalation. They already have extensive expertise and threat hunting knowledge.

Technology: Every SOC needs a security information and event management system (SIEM) that combines data from multiple systems. SIEM systems are generally used to collect and filter data, detect and classify threats, analyze and investigate threats, and manage resources to implement preventive measures and properly address future threats. SOC technologies may include: Log Management; Event collection, correlation and analysis; Security check; Security supervision; Threat analysis; Vulnerability assessment; Vulnerability tracking. These tools support the work of security analysts in monitoring, analyzing, investigating and responding to security incidents. The main components may also include elements such as: monitoring system, IDP/IPS, firewall, log management, vulnerability scanning, honeypot or endpoint protection [9].

2 Related Work

Despite the ever-engaging need to develop a security solution for larger networks, the clear, overall definition of a SOC is still not defined very well. The vast majority of research done on this subject agrees on a lot of similar facts, however, the components of a specific implementation aren't defined explicitly [3], [10]. It's important to mention that network monitoring is already very much present in similar solutions [11], [12], [13], [14], but these don't necessarily engage the concept of SOCs in detail. Our work originates from the need to combine secure network monitoring with every other aspect that a regular SOC and especially a 5G SOC should offer. Researchers from University of Regensburg [15] propose another interesting evaluation about integrating an extra layer of security between the SOC and analysis in the form of digital twins. These digital representations of real world assets help make simulations even more advanced for future work. Basing our methodology around this, we attempt to build one of the first 5G SOC environments supporting ease of operation.

When it comes to experiencing abnormalities on a 5G network, several studies show that even simple forms of attacks could pose a serious threat [16], [17]. Therefore, it's relevant to implement effective attack simulations as part of our SOC. Designing a robust system capable of replicating various attacks like spoofing, jamming, battery/downgrade attacks, etc. requires a great deal of planning. The most sensitive pieces of information on a 5G network that could compromise a subscriber are the location and identity [18]. Attempts to fight the theft of such assets are ongoing as well, however, most of them aren't built into the actual network because of regulations or other causes [19]. To create a well functioning 5G SOC lab environment, we studied similar implementations (partly from previous networks, such as LTE) and gathered adequate information about key vulnerabilities that could be set up on a test environment [17]. We found that most attempts for implementations like this were not focused on going into detail or they were done on previous versions of the network. In our research, we attempt to take a step further as literature about building a SOC environment on 5G networks is significantly limited.

For the actual implementation, we found that open source software and other publicly available information in general could be a great approach to build a solid foundation [20]. The usage of ELK stack in monitoring and data processing is a possibility very welcomed for, however, we are modifying a few parts [21]. In addition to finding that Opensearch could be a more suitable solution and why other organizations would opt for it [22], the authors of these articles [23] do a great job pointing out why a Grafana Loki [24] and Prometheus [25], [26] setup could also be a very solid choice now. Visualizing returned data properly is always a crucial point and will make for better, more human readable results.

3 Background

3.1 Security Operation Center

At Óbuda University, we are developing a Security Operation Center (SOC) specified for 5G networks. The development is based on open source solutions that fit the educational approach and usage [20]. During the development, the involved computer science students have the opportunity experiment with the system and fine-tune it with their own solutions. The university SOC is based on several, widely used open source solutions, such as Opensearch, Prometheus and Grafana, which together allow easy and flexible implementation of data collection, log management, Security Information and Event Management (SIEM), and visualization of log data. In addition, it is able to interoperate with many other SOC components such as Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, vulnerability scanning tools, or honeypots. As various "Beat" (Filebeat, Packetbeat, Winlogbeat) applications send log data from the test endpoints to Opensearch, other tools such as Prometheus handle metrics management on the system by sending data to alert managers to generate reports about attacks in the 5G environment and send logs to Grafana for advanced data visualization.

Figure 2
Architecture of Test 5G site provided by Nokia

3.2 5G Test Environments

At the Kálmán Kandó Faculty of Electrical Engineering of Óbuda University, we are creating the 5G test network in the 4G LTE Vodafone laboratory. The test network is Stand Alone (SA) 5G, with the RAN components supplied by NOKIA and time synchronization provided by a GPS receiver. The test network includes

four Pico RRH (Remote Radio Head) units and one Micro RRH unit with an operating frequency of 3.4 GHz and a bandwidth of 40 MHz. The infrastructure of the test environment can be seen in Figure 2.

3.3 5G Simulated Environments

In addition to the physical test network, we also have developed a virtualised, open source environment for more detailed simulations and comprehensive analyses. The high-level architecture of simulated 5G network can be seen in Figure 3.

3.1.1 Core Network

We found two solutions for simulating 5G mobile networks. Through experimenting with both of them, we got closer to develop the necessary and accessible log management during the construction of a physical 5G network. In the following, we will compare the two, and as a result choose the solution that will be used for our virtualized network in the future.

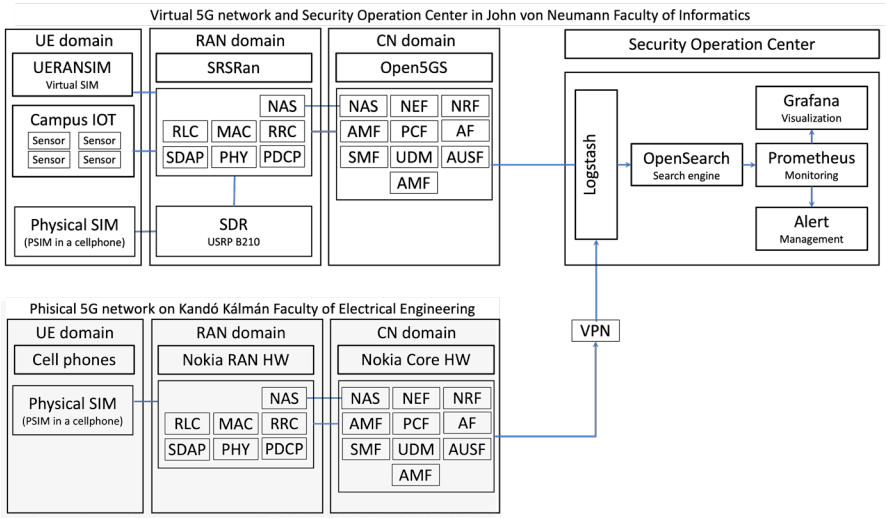

Figure 3
High level architecture of the simulated 5G network

Free5GC [27] is a simulated environment of the 5G core. It was originally based on the other possible solution while also keeping a great deal of performance. It supports user and network function management. The other option is Open5GS [28], which is also an implementation of the core network written in the C language. It is compatible with the most widely used Linux distributions and supports a handful of important features, e.g. Voice over LTE (VoLTE). Open5GS is capable of sending application and operating system level logs as well. Both projects are

open-source and do not require large resources. They can be run easily, as a matter of fact they are known for their ease of installation. However, Open5GS has already been tested with more physical devices, proving it's versatile compatibility [29], [30]. We use an USRP B210 type Software Defined Radio (SDR) in our system where stability is critical, so that's why we opted for Open5GS.

3.1.2 Radio Access Network (RAN)

The Radio Access Network (RAN) is composed of mainly two solutions. SrsRAN [31] (formerly srsLTE) and UERANSIM [32] are both free and open-source software packages capable of simulating endpoints and base stations. They can be used with third-party core network solutions to build complete end-to-end wireless private mobile networks.

UERANSIM is a 5G User Equipment (UE) and RAN (gNodeB) implementation. It's still under development, but the UE and gNodeB components are ready for use. UERANSIM is important in our research, as it forms a connection with the core network to create virtual endpoints and base stations. It can be used to monitor the entire connection process of a UE, and the log files generated during the process can be sent to the SOC for further analysis. On the other hand, srsRAN is a software tool simulating RAN networks with real radio device support. This allows for a realistic, physical radio link, enhancing attack simulations. Software Defined Radios (SDR) are connected to each host running the srsRAN service to provide a physical hardware endpoint for the core network.

3.1.3 UE Domain

In our SOC, we use virtual user endpoints (UE) provided by UERANSIM, real phones equipped with programmable Subscriber Identity Module (SIM) cards and IoT devices as well, including sensors. The phones are connected to the Open5GS core through the International Mobile Subscriber Identity (IMSI) number. They require both the srsRAN service as well as the SDRs for a successful connection.

Software Defined Radio (SDR) uses wireless communication technology, in contrast to traditional wired radios. SDR's software implementation allows flexibility in adjusting frequency, modulation, and output power. It's adaptability supports multiple protocols concurrently, making it easily integrated into various systems. Our SDRs are connected to the hosts running the srsRAN service via USB. The progress of registration can be observed on real time output [33].

4 The Security Operation Center Methodology for 5G Networks

Setting up the technical pillar of a Security Operations Center (SOC) specialized for 5G networks involves implementing the infrastructure, tools, and processes necessary for effective security monitoring, attack simulation, incident detection, and response handling. The key steps and phases include ensuring the sufficient hardware/software support and that accessing the system is secure. The SOC should also have a well setup logging and analytic system to handle threat detection, as well as some form of automation to free analysts from tedious, repetitive work. On the other hand, orchestration and container management can be integrated for improved long-term scalability. With these in mind, the environment still needs to be regularly tested and adjusted so that it's always up-to-date and ready for the newest security concerns.

4.1 Infrastructure

As Figure 4 shows, throughout our research, we are fortunate to have access to two distinct research environments that provide unique perspectives on 5G network simulations. The first environment, located within the John von Neumann Faculty of Informatics, is a virtual network where we simulate the 5G network within what is commonly referred to as a "closed system." In this controlled setting, we have employed a software-based approach to eliminate any disruptive factors, allowing for a focused security examination of the 5G networks.

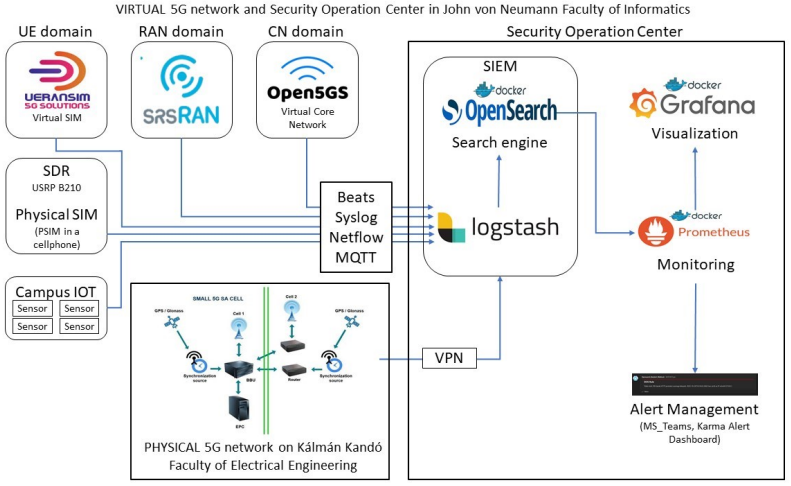

Figure 4
Research environment

On the other hand, our second testing environment is hosted at the Kálmán Kandó Faculty of Electrical Engineering, offering a contrasting setup. Here, each component of the 5G network exists as physical hardware, providing a tangible and realworld simulation of the 5G network infrastructure. Accessing the Kandó Campus is facilitated through a VPN connection, enabling us to establish remote connections to this environment and ensuring seamless analysis of the physical components of the 5G network.

4.2 Tools and Technologies

As Figure 3 shows, our implementation collects log data in Logstash. This tool can perform some basic filtering and expansion of the logs, so we can store the filtered or enriched data in a format that is convenient for us. Opensearch, a very efficient search engine, is also available in our environment, which can index the logs at the moment of arrival. This indexing makes it possible to run quick queries later. Another important feature of the device is its ability to handle large amounts of data. We use Grafana, an open-source monitoring platform, to display individual information and visualize dashboards, which is an ideal choice for displaying metrics, logs and traces collected from applications. Grafana can be connected too many data sources, our choice is Prometheus, which connects the aforementioned visualization platform with the Opensearch search engine. Those visible on the Grafana visualization platform also facilitate the work of security analysts, but we use many additional tools to discover the background of the incident, such as Wireshark to analyze network traffic or Cyber Chef to reverse encryption. In addition to these, we often use additional tools found in the following distributions, such as Kali Linux, Remnux, FlareVM, to facilitate the analysis.

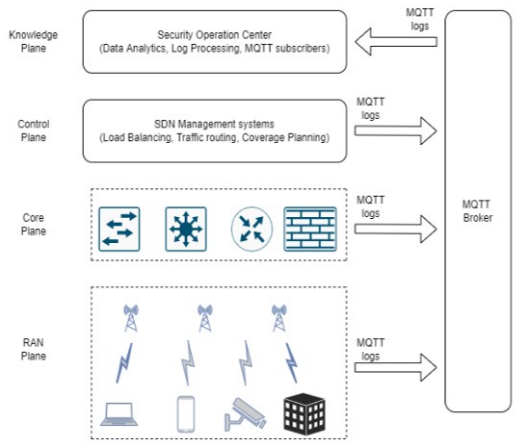

Figure 5
Implementation of SDN and MQTT [34]

During our research, we used a software technology - Software Defined Radio (SDR) - which is capable of receiving and transmitting radio signals. We created a Fake Base Station (FBS) that disguises itself as a real base station and tricks nearby phones, computers, 5G-capable IoT devices to connect to it instead of the original station. This allows us not only to eavesdrop on the traffic of the devices connected to the given FBS, but also to change/modify the original messages, thus building a series of further attack steps. Our goal with this is to run and analyze attacks, and we would also investigate the possibility of whether this is suitable for a kind of "honeypot"-like operation.

One of the characteristics of 5G technology is the use of Software Defined Networking (SDN), which is a new type of approach in the world of telecommunication networks, as it represents a new approach to network separation. It consists of three layers (Application Layer, Control Layer, Infrastructure Layer), but from the point of view of our research, another stratification plays a much more important role. The system we use consists of four levels (Figure 5), which expand the well-known SDN architecture. These are the following: RAN plan (which is responsible for the wireless connection of end users), core plane (functional elements of which are virtualized using NFV), control plane (which consists of an SDN controller, which is responsible for routing, load distribution and other network functions) and the knowledge plane (which means creating/managing knowledge using data analysis). We built our SOC system based on the latter, which collects the log events of individual network devices, endpoints, and other SOC components (honeypot, firewall) for analysis. The RAN plane connect user devices such as mobile phones, computers, and IoT to the core network via a radio connection. The core plane - located between the RAN plane and the control plane - can aggregate the traffic of all base stations. The main function of the control plane - located between knowledge plane and core plane - is to provide information about the network. The "SOC plan" should also be highlighted, the task of which is to plan an automated threat response based on the information collected from the log data. It identifies patterns based on traffic passing through the network and events on individual communication channels, on the basis of which different rules can be created. Alerts can be generated in the event of any result that is different from normal, so even today’s increasingly widespread and sophisticated attacks can be effectively detected [34].

Security Operation teams (SecOps) must also keep up with the 5G technological transformation and prepare to coordinate security detection and incident response. The most important of these is having the right skills and knowledge to implement and secure virtual or container-based applications and network functions. Some examples of these:

Network-based threats: DDOS is a very serious threat to any network, but it is especially dangerous for next-generation radio access networks (ngRAN) that support broadband frequencies, making 5G an even bigger attack surface for malicious actors. An example is when Rogue Base Stations (RBS) send an

overwhelming number of false authentication or authorization requests to the Access and Mobility Management Function (AMF). These devices are also capable of broadcasting stronger signals, which may be preferred by unsuspecting or targeted user equipment (UE), such as mobile phones. This attack differs from the classic DOS attack in several ways, as the RBS tool can view and record UE identification data, such as the International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), and even location data. [35]

Threats affecting virtualization: In a 5G network, virtual and containerized network functions have separated the core functions, thereby introducing a flexible, scalable and programmable approach. This is a useful approach, but it requires new security controls to be inserted at the appropriate points or interfaces in the 5G ecosystem. This implementation provides visibility of user, control and management plane traffic, thus ensuring adequate coverage and remediation of attacks against the 5G network. At the container level, using tools that monitor communication paths between service-based functions is key to system security. Another important function is the authentication and authorization of transactions and ensuring the appropriate level of encryption. [35]

4.3 Monitoring and Alerting

4.3.1 Log Collection

Collecting logs is a very important part of operating a SOC. Log files contain valuable information about security incidents, operating system level errors, etc. We try to focus primarily when and why security incidents happen and what are the main causes [36]. Multiple logging solutions are already available in the ELK stack (the solution we based our implementation on) to provide the confidentiality and integrity of log data.

4.3.2 Logging Methods

Before we continue, we have to mention two important methods of logging and the differences between them [34]. First, agent-based logging, which is the method of log forwarding through an extra service provider called an agent. It is typically running on the client to collect and forward logs to the server, e.g. Logstash in the ELK stack. Ont the contrary to agent-based logging, an agentless method - as the name suggests - doesn’t require an agent to run and handle log collection/forwarding. Either the server fetches the logs periodically or the client sends messages to the server every once in a while.

Our implementation uses various "beat" utilities, such as FileBeat [37], which are agent-based packages operating together to ship logs. For reference, the logs written by the Open5GS core are carried over to Logstash via FileBeat. Logstash then does the additional parsing, filtering and forwarding of logs to the Opensearch daemon.

Once ready, the logs are sent to a metrics (numerical measurements) handling system, e.g. Prometheus to export data for appropriate visualization in a tool called Grafana [38], which is used to create dashboards. As an important SOC functionality, the system also has an alert manager. which is shown in Figure 3. We use the embedded alert manager in Opensearch to create alerts from specific events, however, Prometheus could also be further improved by using Karma [39], i.e. an advanced alert dashboard providing extended functionality.

4.3.3 Traditional Monitoring Techniques

Network monitoring techniques use various protocols to collect and process data from the device [40]. The syslog protocol is a standard that supports the sending of log information in a predefined format about the operation and performance indicators of user equipment, network devices and other network system components. Packet analysis usually involves a SPAN port originating from a switch or network branch, extracting information from each packet and usually sending it to an intrusion detection/prevention system. IDS/IPS usually looks for signatures in packets indicating malicious/harmful traffic. Log analysis is a solution that collects the data generated by the machine, typically in the form of log files (syslog) and presents a database of them. Correlate events between different types of systems (for example, routers, firewalls, servers, load balancers).

4.3.4 5G Specific Techniques

It is possible to extend the monitoring of traditional IoT devices with logging via an MQTT broker. MQTT (Message Queuing Telemetry Transport) is a TCP-based lightweight logging protocol designed for IoT sensors/devices featuring small overhead and versatile support. The functionality of MQTT can be combined with Software Defined Networking (SDN) and IoT devices in a layered architecture. The broker will act as a hub and collect logs from every individual layer. After collection, the logs are sent to the SOC for further analysis [34]. The architecture of this model is shown in Figure 5.

4.4 Incident Response and Investigation

Incident response is an organization’s process of reacting to IT threats such as cyberattack, security breach, and server downtime.

The incident response life cycle is the organization’s step-by-step framework for identifying and reacting to a service outage or security threat. The National Institute of Standards and Technology (NIST) provides guidelines and standards for various aspects of information security, including incident response. The NIST incident response life cycle is a systematic approach to managing and responding to cybersecurity incidents.

The NIST Framework for cybersecurity [41] includes five key phases to ensure a comprehensive and effective approach. The initial "Preparation" phase involves laying the groundwork for cybersecurity measures. The subsequent "Detection and Analysis" stage focuses on identifying and analyzing potential threats. In the event of a security incident, the "Containment, Eradication, and Recovery" phase outlines actions to mitigate the impact, eliminate the threat, and restore normal operations. Following an incident, the "Post-Event Activity" involves assessing the aftermath and implementing necessary improvements. Lastly, the "Review and Update" phase emphasizes the importance of regularly reviewing and updating the cybersecurity framework to adapt to evolving threats and technologies.

4.5 Security Orchestration, Automation and Response (SOAR)

It is a comprehensive solution that combines security orchestration and automation to streamline and improve the efficiency of security operations. This technology is designed to help security teams manage and respond to security incidents more effectively by integrating and automating various security processes. SOAR platforms have three main components. The Security Orchestration component facilitates the integration of different security tools, ensuring they can share information and work collaboratively. This includes integration with SIEM (Security Information and Event Management), threat intelligence feeds, and endpoint protection systems. The Automation component involves using technology to perform repetitive and routine tasks without human intervention. In a SOC, automation is applied to various security processes to increase speed, accuracy, and consistency. We can create automated playbooks for incident response that include tasks like gathering additional information, isolating affected systems, or blocking malicious activities. The Response capabilities in SOAR involve the actions taken by the security team to address and mitigate security incidents. This can include both automated responses and human-guided responses based on the context of the incident. For example, automatically blocking a suspicious IP address, notifying relevant stakeholders, and initiating a predefined incident response playbook.

Benefits of Using SOAR: it provides fast reaction time and incident detection and the security orchestration combines multiple related alerts from different systems into a single incident. To save even more time, security automation allows the system to respond to alarms without human intervention whenever possible. Contextualising textual data and automating the decision making process allows for faster incident handling. Another important benefit is providing better threat context. SOC analysts are constantly dealing with information overload. The best SOAR platforms can ingest threat intelligence and automatically correlate it with events in real-time. This takes the burden off of SOC analysts and provides immediately actionable information for incident response teams. It is also making Analysts more productive by making SOAR enables automation of lower-level

threats. This frees up resources and time for analysts to work on larger and more complex projects, resulting in greater productivity and efficiency. All elements of SOAR contribute to simplifying security operations. Security orchestration aggregates data from different sources. Security automation can easily handle low priority alerts and incidents using automated playbooks. Incident response takes the guesswork out of incident management, limiting the latency of cyberattacks and the overall impact on business.

Security orchestration and automation are used to offload low-priority and repetitive tasks, allowing SOC analysts to do higher-value work that further improves incident response. With security automation and incident response playbooks, SOAR can build workflows that require minimal, if any, human intervention.

5 Metrics and Key Performance Indicators

Measuring the qualitative and quantitative aspects of Security Operations Center (SOC) processes is an indispensable step in formulating a comprehensive operational strategy. Key Performance Indicators (KPIs) can be used to monitor the efficiency of SOC operations and identify deficiencies in processes and technologies.

Common metrics are already in use in many organisations and are selected based on the following factors: Organisational goals, industry expectations, maturity of the security programme. Organisational goals may include Mean Time to Detect (MTTD), which is the average time it takes the SOC team to detect an incident or security event; Mean Time to Resolution (MTTR), which is the average time from incident detection to full resolution; Average Time to Attend and Analyse (MTTAA), which is very similar to the previous measure, but different, MTTA measures the time taken by the SOC team from incident detection through the prioritisation process to deciding how an incident affects the organisation and how it can be resolved; Number of Security Incidents by measuring the number of security incidents detected and reported by the SOC team within a given time frame, and False Positive Rates (FPR) and False Negative Rates (FNR). In the area of industry expectations, metrics may include Escalation Effectiveness, which refers to meeting industry expectations for hierarchical incident response and escalation; Benchmarking Against Industry Incidents Metrics, to ensure comparability of SOC performance metrics with industry benchmarks; and Threat Intelligence Integration Rate, to measure the extent to which threat intelligence is integrated into SOC operations. From the perspective of security programme maturity, training and skills development effectiveness, incident trend analysis and learning can provide some useful KPIs.

At Óbuda University's 5G Security Operations Center (SOC), our objective is to enhance the aforementioned Key Performance Indicators (KPIs): To improve

organisational KPIs, it is imperative to accelerate the detection and identification of incidents. This can be achieved by developing a tailored monitoring and alerting system. Regular vulnerability and penetration testing is essential to assess the security posture of our system and ensure it is up to date. In addition, the creation of automated tools using machine learning techniques for incident classification and prioritisation is advocated, in line with industry standards in the context of our research SOC. Such tools and methodologies have the potential to significantly reduce both detection and remediation times. To meet industry expectations, careful documentation of issues, best practices, guidelines and successful incident handling is paramount. In parallel, we have initiated the development of a knowledge graph to aggregate publicly available threat and remediation knowledge. This repository, in conjunction with 5G security-related tweets and blog information on social media platforms, aims to accelerate the implementation of proactive defence methods. The knowledge graph will include 5G-specific threat information, remediation techniques and defence strategies. Concerning the maturity of our safety program, the regular training of our employees, especially students, is an established practice. In addition, promoting knowledge sharing through collaborative tools and enhancing communication skills, supported by instant messaging platforms and dedicated communication and incident response channels, contributes to refining the maturity of our security programme.

6 Test Cases and Results

6.1 Registration Tracking

This section is based on the gap-filling work of the team led by Lucas Baleeiro Dominato Silveira, entitled "Tutorial on communication between access networks and 5G core". [42] It helps understand the communication between network segments and architecture components. The tutorial provides a comprehensive overview of the communication between User Equipment (UE), Radio Access Network (RAN) and 5G Core (5GC). Throughfollowing the initial registration process, we can show how our SOC implementation can report on the state of the virtualized test 5G network.

In the first message, the UE sends a registration request to the 5GC. This message contains different types of information, such as initial registration, mobility registration update, etc. The UE does not have a valid context during the initial registration, so it must provide a 5GS mobile ID during the first registration on the network. Examples of such identifiers are SUCI (Subscription Concealed Identifier) or GUTI (Globally Unique Temporary Identity).

The status graph in Figure 6 shows the stages of the registration process. Below is a table summarizing how much we know about the status of our 5G network based

on the log entries. In the scope of this article, we will look at a total of 12 registration flows, see which flow has progressed, and try to resolve failed registrations based on the log entries. A summary of the registrations examined is shown in Figure 6.

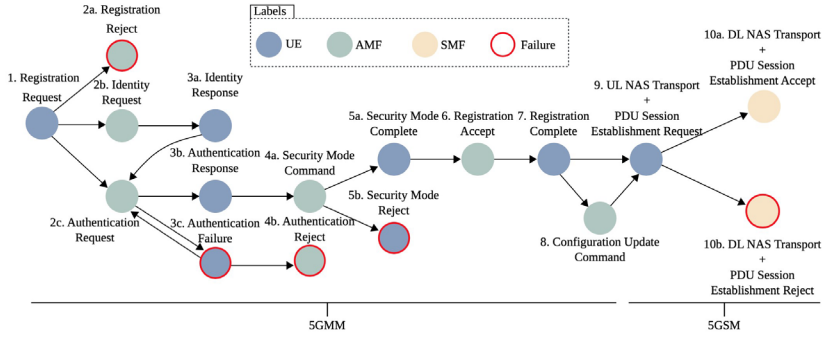

Figure 6
Non-Access Stratum (NAS) message flows [42]

The AMF processes the registration request based on three possible messages: Registration Denied (2a), Identity Request (2b) or Authentication Request (2c). In my SOC solution there was only one case where the registration request was rejected (2a). When this response is received, the error message informs the UE about problems encountered during the processing of the registration request, such as protocol errors or invalid values.

In case of authentication failure, the UE sends an authentication failure (3c) message, which allows to synchronise the serial number (SQN) and send a new challenge. In this case, the 5GC authentication reject (4b) message is sent to complete the primary authentication. The most common errors are related to the different keys used during the primary authentication, which cause problems in the verification of the message authentication code (MAC). The SOC found 9 errors in this category. It is important to note that in this case, the process can step back one level to the Authentication Request (2c) state, after which another authentication error can be avoided.

After the exchange of authentication, primary authentication and key agreement messages, the UE and AMF shall establish a security context in the NAS messages. We found that in the test environment 11 devices reached this stage, i.e. all of them support the selected NAS algorithm. Otherwise, a Security Mode Reject (5b) message is returned.

We observed that all devices that reached this point without exception reach the PDU Session Establishment Accept status (10a). Thus, the registration process (7) is completed. In this state, the 5GC knows the UE location, the NAS connection and the security settings. So, if the 5GC provides the PDU session, the selected SMF sends the PDU Session Establishment Accept (10a) message to the AMF. The PDU

Session Establishment Accepted state includes the PDU address, the QoS rules and the Session Aggregate Maximum Bit Rate (AMBR).

State	*SOC data / number of UE in stage*	*Information of the network*
Registration Request (1)	12	How many UE want to register
Registration Rejected (2a)	1	Protocol error or invalid values
Authentication Failure (3c)	9	Could be an attack undergoing
Authentication Rejection (4b)	0	Number of UE unable to connect
Security Mode Reject (5a)	0	Not supported security level
Registration Complete (7)	11	Number of active UEs
PDU Session Establishment Accept (10a)	11	Number of active UEs

Figure 7
State of 5G network in some stages of the registration procedure

6.2 Traffic Capture and Correlation

As 5G networks are expected to deliver higher data transfer speeds, lower latency, and numerous new functionalities, we employ unique protocols and technologies specific to 5G for capturing 5G network traffic. In our environment, we analyze these using software solutions. Our solutions include Netflow and Packetbeat, ensuring continuous monitoring and analysis of the network. Additionally, we use the Wireshark traffic analyzer offline for comprehensive analysis.

Let me show the examination of network traffic with a simple example in Figure 7. The registration part is measured through two key metrics: the first is related to Accepted registrations, indicating successful registrations, and the second focuses on Registration requests, representing the total number of registration attempts.

An anomaly becomes apparent in the data where there are 3 accepted registrations but only 2 registration requests, signaling a potential irregularity that requires investigation. Additionally, a pie chart illustrates the Severity levels, where an increase in warnings or errors could indicate anomalies within the system. This serves as a visual indicator for potential issues that merit attention.

Furthermore, a chart depicting the amount of traffic on a specific interface is presented. The dotted line in the chart serves as a threshold, representing a standard level of traffic. Deviations above this threshold may signify abnormal levels of network activity, prompting further investigation.

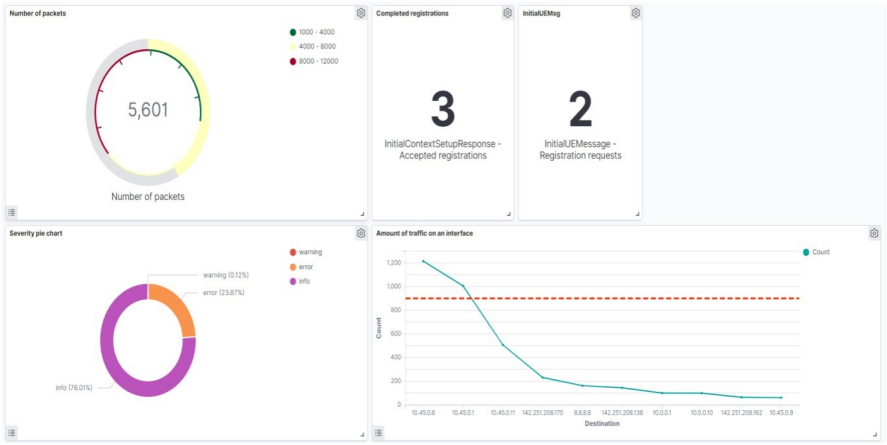

Figure 8
Simple Dashboard

7 Future Work

Relying on the findings of this study, future research could focus on expanding important SOC operations. While our study provided specific information about registration tracking and traffic capture, other aspects, such as incident response and threat intelligence analysis could benefit from further investigation. We are planning to extend our present 5G infrastructure by conducting a thorough evaluation of the current hardware, software, and network components.

This assessment should focus on performance bottlenecks, hardware obsolescence, software compatibility issues, and network capacity constraints specific to the high demands of 5G technology. Updating the infrastructure involves boosting network capacity, upgrading to state-of-the-art hardware, integrating commercial off-the-shelf (COTS) endpoints, and leveraging cloud integration for scalable and flexible resource management.

For proactive defensive strategies, it is essential to identify specific threat intelligence sources that are pertinent to 5G networks, especially for the Radio Access Network (RAN). Ensuring complete security coverage and safeguarding devices against advanced attacks require implementing Endpoint Detection and Response (EDR) solutions like Wazuh and strengthening endpoint security through strong device management.

Finally, we intend to investigate the application of 5G-specific intrusion detection techniques, such as including honeypots into our SOC. We would like to examine the use of all-in-one solutions (such as T-Pot), as well as honeypots with specialized

applications (telecommunications, IoT, and OT). We're also looking forward to cooperating in another honeypot research and development project at Óbuda University.

Conclusion

The endeavor to pioneer one of the initial Security Operations Center (SOC) environments tailored specifically for 5G networks presented an unmatched opportunity. The biggest challenge of this aim lied in the newly introduced and mostly virtualised nature of 5G protocols. In this paper, at its core, we explored and introduced a methodology developed for crafting a 5G SOC environment. Leveraging several open-source software components, we have formulated a system that represents a prototype implementation in 5G SOC design. By offering an overview of existing research in closely aligned domains, we not only contribute to a field with limited existing literature but also introduce novel solutions. Emphasis has also been placed on the identification and analysis of key performance indicators (KPIs) pivotal for enhancing SOC performance. Based on our methodology we have demosntrated the results. Several processes interacting with each other we have succeeded in detecting 5G attacks implemented in a simulation environment with a dedicated SIEM and alerting system. Looking ahead, our primary focus is on the practical extension of the outlined methodology. This will not only further refine our system, but will also position the SOC for more advanced simulations and heightened data processing capabilities.

Acknowledgment

The research was supported by the Ministry of Culture and Innovation NRDI Office within the framework of the Infocommunication and Information Technology National Laboratory Program.

References

[1] J. A. Khan, M. M. Chowdhury, “Security Analysis of 5G Network,” in 2021 IEEE International Conference on Electro Information Technology (EIT), 001-006, 2021, doi:10.1109/EIT51626.2021.9491923

[2] P. Schneider, G. Horn, “Towards 5G Security,” in 2015 IEEE Trustcom/BigDataSE/ISPA, volume 1, 1165-1170, 2015, doi:10.1109/Trustcom.2015.499

[3] M. Vielberth, F. Böhm, I. Fichtinger, G. Pernul, “Security Operations Center: A Systematic Study and Open Challenges,” IEEE Access, 8, 227756-227779, 2020, doi: 10.1109/ACCESS.2020.3045514

[4] E. Hinchy, “Voice of the SOC 2023,” https://www.tines.com/reports/voice-of-the-soc2023, 2023

[5] M. Bogdanoski, T. Shuminoski, M. Hadji-Janev, A. Risteski, T. Janevski, “Future 5G Mobile Broadband Networks Using Cloud-based Services with

Advanced Security and QoS Framework," Acta Polytechnica Hungarica, 17(10), 20, 2020

[6] V. Rajasekar, J. Premalatha, K. Sathya, M. Saracevi˘ c, "Secure remote user authentica-´ tion scheme on health care, IoT and cloud applications: a multilayer systematic survey," Acta Polytechnica Hungarica, 18(3), 87-106, 2021

[7] I. Leyva-Pupo, A. Santoyo-González, C. Cervelló-Pastor, "A framework for the joint placement of edge service infrastructure and user plane functions for 5G," Sensors, 19(18), 3975, 2019

[8] Y. Zhang, Network Function Virtualization: Concepts and Applicability in 5G Networks, John Wiley & Sons, 2018

[9] M. V. Kecskés, M. Orsós, E. Kail, A. Bánáti, "Monitoring 5g networks in security operation center," in 2021 IEEE 21st International Symposium on Computational Intelligence and Informatics (CINTI), 000223-000228, IEEE, 2021

[10] D. Shahjee, N. Ware, "Integrated Network and Security Operation Center: A Systematic Analysis," IEEE Access, 10, 27881-27898, 2022, doi: 10.1109/ACCESS.2022.3157738

[11] D. Giannopoulos, P. Papaioannou, C. Tranoris, S. Denazis, "Monitoring as a Service over a 5G Network Slice," in 2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit), 329-334, 2021, doi: 10.1109/EuCNC/6GSummit51104.2021.9482534

[12] M. Mekki, S. Arora, A. Ksentini, "A Scalable Monitoring Framework for Network Slicing in 5G and Beyond Mobile Networks," IEEE Transactions on Network and Service Management, 19(1), 413-423, 2022, doi:10.1109/TNSM.2021.3119433

[13] I. Angelopoulos, E. Trouva, G. Xilouris, "A monitoring framework for 5G service deployments," in 2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 1-6, 2017, doi: 10.1109/CAMAD.2017.8031617

[14] S. R. Chowdhury, M. F. Bari, R. Ahmed, R. Boutaba, "PayLess: A low cost network monitoring framework for Software Defined Networks," in 2014 IEEE Network Operations and Management Symposium (NOMS), 1-9, 2014

[15] M. Dietz, M. Vielberth, G. Pernul, "Integrating digital twin security simulations in the security operations center," in Proceedings of the 15th International Conference on Availability, Reliability and Security, 1-9, 2020

[16] Y. Arjoune, S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 1010-1015, 2020

[17] A. Shaik, R. Borgaonkar, "New vulnerabilities in 5G networks," in Black Hat USA Conference, 2019

[18] G. Holtrup, W. Lacube, D. P. David, A. Mermoud, G. Bovet, V. Lenders, "5g system security analysis," arXiv preprint arXiv:2108.08700, 2021

[19] K. Norrman, M. Näslund, E. Dubrova, "Protecting IMSI and user privacy in 5G networks," in Proceedings of the 9th EAI international conference on mobile multimedia communications, 159-166, 2016

[20] A. Szarvák, V. Póser, "Review of using Open Source Software for SOC for education purposes–a case study," in 2021 IEEE 25th International Conference on Intelligent Engineering Systems (INES), 000209-000214, IEEE, 2021

[21] R. Stoleriu, A. Puncioiu, I. Bica, "Cyber Attacks Detection Using Open Source ELK Stack," in 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 1-6, 2021

[22] S. Papadopoulos, P. Saiz, U. Schwickerath, E. Kleszcz, "Architecting the OpenSearch service at CERN,"

[23] E. Bautista, N. Sukhija, S. Deng, "Shasta Log Aggregation, Monitoring and Alerting in HPC Environments with Grafana Loki and ServiceNow," in 2022 IEEE International Conference on Cluster Computing (CLUSTER), 602-610

[24] "Grafana Loki: Log aggregation system," https://grafana.com/oss/loki/, accessed: 2024-02-02

[25] "Prometheus: Metrics management system," https://prometheus.io, accessed: 2024-02-02

[26] M. Hadded, G. Lauras, J. Letailleur, Y. Petiot, A. Dubois, "An Assessment Platform of Cybersecurity Attacks against the MQTT Protocol using SIEM," in 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 1-6, 2022

[27] "Free5GC: Opensource 5G Core Implementation," https://free5gc.org/, accessed: 2024-02-02

[28] "Open5GS: Open source implementation for 5G Core and EPC ," https://open5gs.org, accessed: 2024-02-02

[29] G. Lando, L. A. F. Schierholt, M. P. Milesi, J. A. Wickboldt, "Evaluating the performance of open source software implementations of the 5G network core," in NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, 1-7, 2023, doi:10.1109/NOMS56928.2023.10154399

[30] L. Bonati, M. Polese, S. D'Oro, S. Basagni, T. Melodia, "Open, programmable, and virtualized 5G networks: State-of-the-art and the road ahead," Computer Networks, 182, 107516, 2020

[31] “SrsRAN: Complete 5G RAN solution,” https://www.srsran.com/5g, accessed: 202402-02

[32] “UERANSIM: Open source state-of-the-art 5G UE and RAN (gNodeB) simulator,” https://github.com/aligungr/UERANSIM, accessed: 2024-02-02

[33] T. Bakhshi, et al., “State of the art and recent research advances in software defined networking,” Wireless Communications and Mobile Computing, 2017

[34] M. Orsós, M. Kecskés, E. Kail, A. Bánáti, “Log collection and SIEM for 5G SOC,” in 2022 IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI), 000147-000152, IEEE, 2022

[35] R. Evangelista, “Security Operations in a 5G World,” 2020

[36] K. Schmidt, C. Phillips, A. Chuvakin, Logging and log management: the authoritative guide to understanding the concepts surrounding logging and log management, Newnes, 2012

[37] “FileBeat: Lightweight shipper for logs,” https://www.elastic.co/beats/filebeat, accessed: 2024-02-02

[38] “Grafana: The open observability platform,” https://grafana.com, accessed: 2024-0202

[39] “Karma: Alert dashboard for Prometheus Alertmanager,” https://github.com/prymitive/karma, accessed: 2024-02-02

[40] C. Carthern, W. Wilson, N. Rivera, “Effective Network Management,” in Cisco Networks: Engineers’ Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA, 705-730, Springer, 2021

[41] P. Cichonski, T. Millar, T. Grance, K. Scarfone, “Computer Security Incident Handling Guide,” 2012, doi:https://doi.org/10.6028/NIST.SP.800-61r2

[42] L. B. Dominato, H. C. de Resende, C. B. Both, J. M. Marquez-Barja, B. O. Silvestre, K. V. Cardoso, “Tutorial on communication between access networks and the 5G core,” 2021