Ericsson RAN Security Threat Detection

Ericsson enables Communication Service Providers to discover security threats to the RAN using automation and efficient detection algorithms. Threats such as false base stations are responded to with appropriate measures to protect user data, privacy and business operations.

ERICSSON

Networks are obvious targets for threat actors

The threat landscape for mobile networks is ever-changing, with a web of advanced threat actors using increasingly sophisticated tactics and techniques. Diverse motives exist – from theft and fraud, to spying, political protest and sabotage. With networks playing such a vital part in our digital lives, they are now obvious targets for threat actors.

Data breaches are happening constantly. A major data breach is defined as a breach in which more than 30,000 records are lost or stolen.

Verizon's annual report into data breaches recorded 5,258 breaches in 2021. IBM's 2021 report found that the average total cost of a data breach is $4.24M. 287 days was the average time required to identify and contain a data breach. That's more than 9 months.

Data breaches are a very significant problem affecting both telecom service providers and their enterprise customers. When network security breaches occur and data is lost or damaged, there are consequences for service providers. Breaches may also compromise network services, impacting availability for subscribers through outages and loss of mobile service. These outages can last minutes, hours, or even days while the problem is resolved, and normal service resumed.

Outages and data theft result in financial losses for service providers. Penalty payments will be owed to subscribers and enterprise customers to compensate for loss of service, and there may be a possibility of regulatory fines from authorities too.

During this time, service providers are busy with several urgent tasks. They're responding to the incident to fix the network problem, using digital forensics to identify the cause, and communicating with subscribers and the media about the cause of the outage, and the time to restore normal service.

"Hackers attack every 39 seconds"

"Average total cost of a data breach $4.24 million"

"5,258 confirmed data breaches"

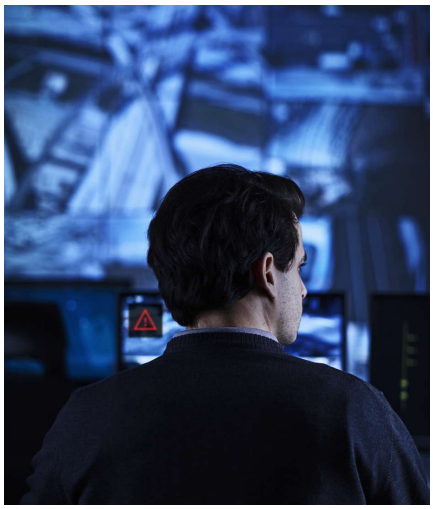
"287 days – average to identify and contain a data breach"

Service providers are challenged by a limited visibility of threat activity in RAN

Tactics and techniques used to breach network security are constantly changing. The use of false base stations is a method for compromising telecom networks. Also known as 'stingrays' or 'IMSI catchers', they are an important type of RAN-specific threat to detect and report."

The Radio Access Network (RAN) is the largest and most accessible part of a CSP's network, with thousands of potential targets. Much radio equipment is placed in public locations with a lower degree of physical protection, compared with other parts of the network, which will generally be located within secured buildings.

Service providers are challenged by limited visibility of RAN threat activity, control of RAN security and timely reports of security breaches. Lack of RAN-specific security automation and detection makes managing security in the RAN domain hard. Without highly tuned RAN-specific detection algorithms and processes, detection turns to laborious manual threat hunting or time-consuming incident response. Manual checking of security compliance and controls is time consuming, taking resources which could be used on higher-value tasks.

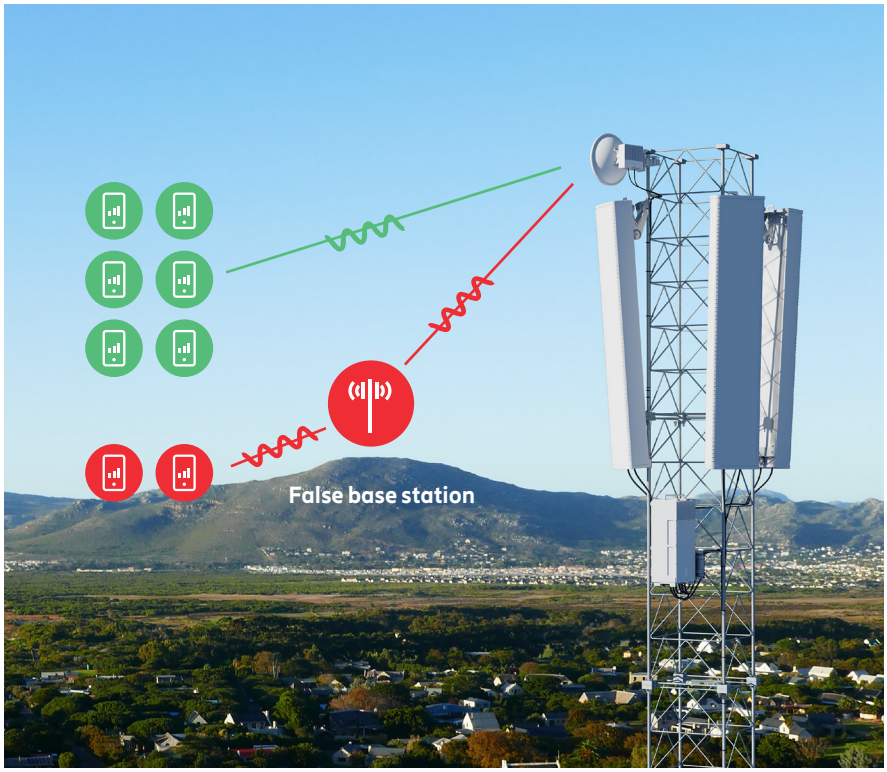


How false base stations operate

False base stations attacks are relatively easy to perform in older generation networks with fewer in-built security mechanisms. The required investment in equipment to create a false base station can be as low as $1,500.

False base stations are small and lightweight. They could be carried in a box or backpack. Therefore, they are highly mobile and can be carried around by one person. Without specialist equipment or sophisticated software, they are relatively hard to detect.

Even if an adversary can mimic a base station, the attack does not scale well and will be limited to the coverage of a false base station. Hence, if the attacker is targeting a specific user, they will already have an approximate understanding of where the victim is geographically located.



Threat detection made possible with Ericsson Security Manager and RAN software

Ericsson Security Manager (ESM) and RAN software, implemented together, make it possible to detect threats to radio access networks.

Ericsson Security Manager already includes Operational and Management (OAM) Detection Logic to detect threats based on real time security event logging (RTSEL). With the introduction of RAN Detection Logic, the threat detection capabilities of ESM are further enhanced with the detection of false base stations.

An ideal detection solution

RAN Security Threat Detection provides improved visibility and control over potential security breaches in the RAN. Continuous monitoring of active threats means service providers can take action to mitigate the consequences early. Security automation with ESM has the potential of cost savings up to 80% and with RAN threat detection there is a greater potential benefit.

Manual threat detection is very resource-intensive and takes skilled security operations staff away from other highly specialized activities. The work is time consuming and challenging. RAN specific detection provides more tuned and focused alerts, reducing the risks of missing threat activities.

RAN Security Threat Detection helps service providers to reduce the risk of potential service loss, regulatory fines and reputational damage which could result from a network being compromised.

Investing in security increases end-user perception of a responsible service provider protecting its subscribers and can therefore strengthen the service provider's brand.

"71% of CMOs believe the biggest cost of a security incident is the loss of brand value"

Source: Data Privacy Manager

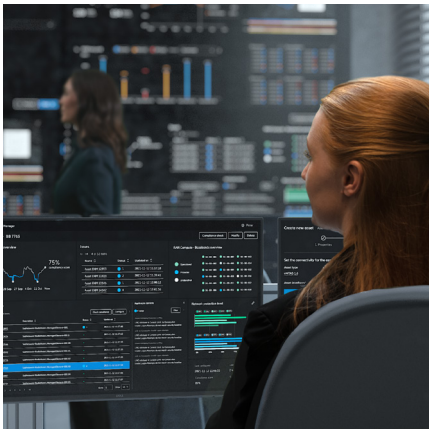
Cost savings up to 80% compared with manual security management

80%

"Ericsson Security Manager has brought security compliance visibility and control to a new level – it is like turning the lights on in a dark cave"

Philippe Vuilleumier,
Head of Group Security, Swisscom

Detect a false base station!



The Ericsson RAN software provides the capabilities required to initiate security-enhanced measurement reporting between the legitimate base stations and the UEs (e.g., mobile phones). These measurements are collected by Ericsson Network Manager (ENM) and then analyzed by ESM, which alerts the Security Operation Center (SOC) if a false base station is detected.

Together with Ericsson Security Manager (ESM), the Ericsson RAN Security Threat Detection software offers timely detection using automation and advanced detection algorithms. It's flexible and can be set to constant alert, reducing manual probing and testing, and freeing up security operations resources to reduce Opex.

Unique values for Service Providers

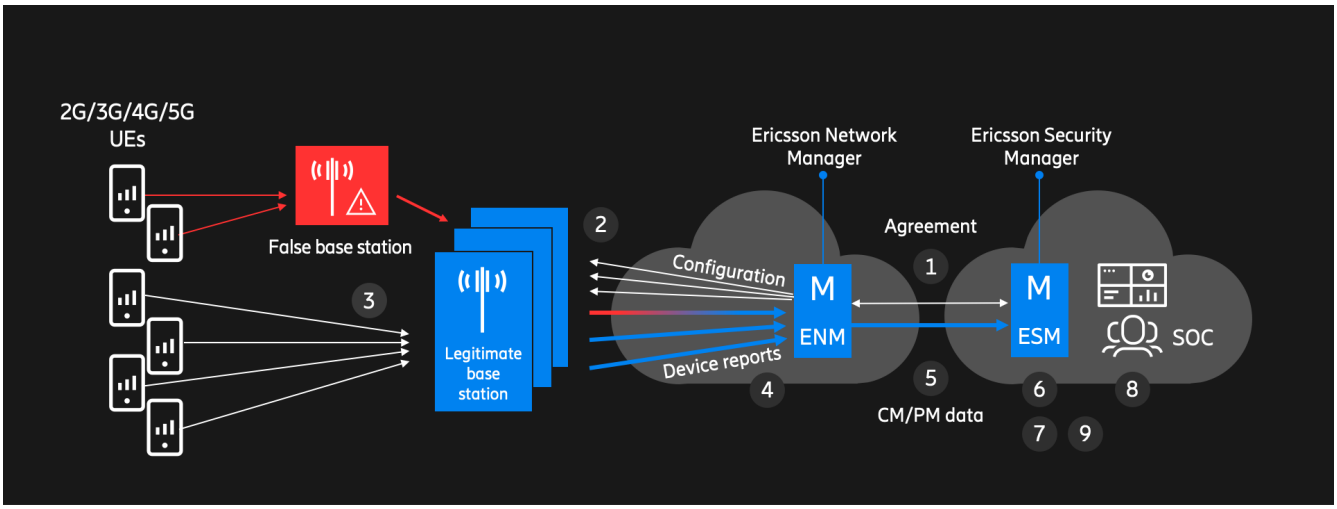
The Ericsson RAN Security Threat Detection solution is powerful and innovative, with unique values for telecom deployments. This is how false base station detection works.

RAN-specific threat detection enables communication service providers to promptly discover threats to the RAN, including false base stations. They can then take appropriate measures to protect user data, privacy and business operations. Detection is better performed by using intelligence from within the RAN itself, and with deep telecom know-how to understand threats and potential weaknesses. An enterprise/IT-focused solution will not be sufficient or effective.

Network-centric intelligence

It is a software-only automated solution leveraging intelligence from within the network. Measurements are made by the UEs, controlled by the RAN and analyzed by ESM. Efficient and innovative detection algorithms build on deep Ericsson radio expertise. Automated detection is constantly active, and false base stations are promptly reported. Detection can be customized to focus on at-risk locations or times. The solution combines both 3GPP standards and Ericsson analytics innovation.

"Detection can be customized to focus on at-risk locations or times."



Meeting all specific requirements

"You can be confident when a detection is reported that the threat is real."

The solution has smart analytics capabilities with dependable and timely reports. Alerts of false base stations are highly precise with minimal false positives, meaning you can be almost certain when a detection is reported that the threat is real.

It is a cost-effective software-only solution with no need for any network probes or other air interface measuring devices. No drive testing or other manual processes are required, and threat detection activities are easily scaled to cover a large percentage of the RAN.

Ericsson is a world leader in communications technology and services with headquarters in Stockholm, Sweden. Our organization consists of more than 111,000 experts who provide customers in 180 countries with innovative solutions and services. Together we are building a more connected future where anyone and any industry is empowered to reach their full potential. Net sales in 2016 were SEK 222.6 billion (USD 24.5 billion). The Ericsson stock is listed on Nasdaq Stockholm and on NASDAQ in New York.

Ericsson.com

2/28701-FGB 101 0781 Uen