White Paper

HardenStance

Securing a Utility's Private Wireless Network

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

NOKIA ONELAYER

September 2025

HardenStance
"Trusted Research, Analysis and Insight in IT & Telecom Security"

Executive Summary

- Cyber threats to critical infrastructure have reached new peaks in the last two years. Private wireless networks deployed by water and power companies must protect against threats targeting 4G/5G operators and those targeting their own sector.
- Getting security right from the outset is critical to utilities getting past the pain of operationalizing a private wireless network to the gains from deploying it at scale.
- Simply extending enterprise security tools and processes will not secure a private wireless network properly. Utilities need tools and processes tailored to the unique security requirements of any 4G/5G network. And they need additional protections against risks that arise from the unique ways utilities use a private network.
- Nokia's cybersecurity portfolio – comprising NetGuard EDR, NetGuard Identity Access Manager, NetGuard Certificate Manager, NetGuard Cybersecurity Dome, as well as OneLayer Bridge – is a good fit for the comprehensive security utilities need.

Digital transformation: keeping 'eyes on the prize'

For utilities that have chosen a private 4G/5G network to accelerate their digital transformation, the choice of whether to build and operate your own or lease a telco-built and operated service is pivotal. Among those who choose to self-build, acquiring the right spectrum is another key milestone. Understanding 4G/5G network protocols and how to integrate them into their existing technology stack is another.

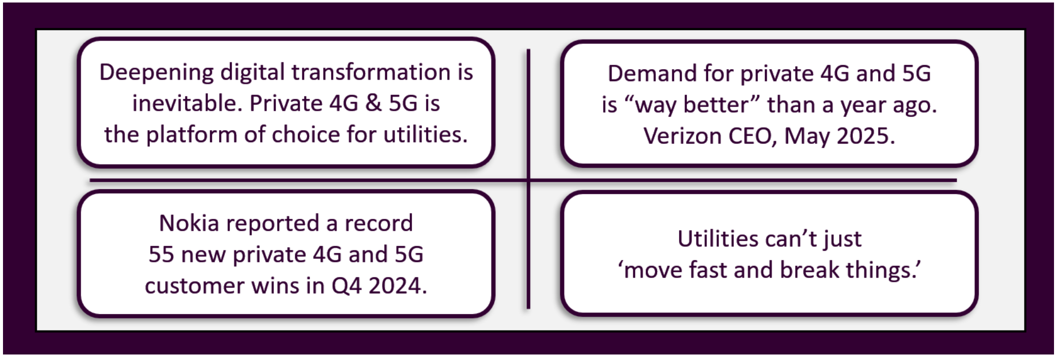
Many power and water companies have completed Proof of Concept (PoC) trials and identified initial use cases like distribution automation and smart metering.

Many power and water companies have completed Proof of Concept (PoC) trials and identified initial use cases like distribution automation and smart metering to deploy on the network at scale. Some advanced use cases also have tremendous long term potential. In the energy sector, Fault Location, Isolation and Service Restoration (FLISR) can keep electricity flowing during disruptive events like storms. Falling Conductor Protection (FCP) can cut the electrical current before a falling power line can hit the ground and start a fire.

Some media and investor sentiment has become impatient with the private 4G/5G market, but there are good reasons for business leaders to keep their 'eye on the prize':

- **Driving the digital transformation roadmap is a non-negotiable business priority**. Things like Distributed energy resources (DER) to better capture renewables and better management of water resources are critical societal goals as well as key opportunities for utilities themselves. The potential of enablers like smart electrical substations and automated water treatment processes is too big to ignore.
- **For utilities, there are no viable alternatives to 4G/5G among network platforms**. Wi-Fi can't provide the extensive wide area coverage they need, including in remote areas. And the only other challenger, WiMAX, is defunct.

Figure 1: **Drivers and momentum in the private wireless networks market**



Deepening digital transformation is inevitable. Private 4G & 5G is the platform of choice for utilities.

Demand for private 4G and 5G is "way better" than a year ago. Verizon CEO, May 2025.

Nokia reported a record 55 new private 4G and 5G customer wins in Q4 2024.

Utilities can't just 'move fast and break things.'

Source: HardenStance

- **A slow rate of change is built into a utility's safety-first culture and operating model**. These are highly regulated businesses. Safety failures in day-to-day operations and supply outages or blackouts can put human life at risk. There are good reasons why utilities can't just 'move fast and break things.'
- **Recent proof points are consistent with a private wireless network market that's scaling steadily rather than spectacularly**. For Q4 2024, Nokia announced a record 55 new private wireless network customer wins. The total has now surpassed 850. Verizon provides another proof point. As well as operating one of the world's largest 4G/5G networks, Verizon also deploys private networks. In May 2025, the company's CEO, Hans Vestberg, told a JP Morgan conference that demand for private wireless networks was "way better" than a year previously.

A utility can't operationalize its wireless network at scale if it can't defend itself and its customers against today's cybersecurity challenges.

Robust security is critical for rolling out at scale

A utility can't operationalize its wireless network at scale if it can't defend itself and its customers against today's cybersecurity challenges. The security architecture needs to be thought all the way through and properly invested in from the outset. Bolting requirements onto a poorly specified security architecture further down the line will invariably cost a lot more than getting it right at the outset. The architecture and operating model must be adaptable to the cyber threat landscape, support future use cases, and take account of the utility's long term compliance obligations.

Before reviewing the escalation in cyber threats to power and water companies, it's notable that attacks on telco-run 4G/5G networks are also escalating (see **Figure 2)**. As will be shown, private operators have advantages and disadvantages compared to telco-run operations when defending a wireless network. Some vulnerabilities and attack vectors are unique to utility-run networks, but others are the same.

Nation state and other cyber threat groups are targeting utilities

The targeting of utilities' traditional IT and OT infrastructure has also increased markedly. As shown in **Figure 3** small companies are no more or less vulnerable than large ones. Threat groups sometimes prefer to test new Tactics Techniques and Procedures (TTPs) on smaller operations before going on to target bigger ones. The Colonial Pipeline hack of 2021 arose from a ransomware attack by a criminal gang impacting Colonial's billing and accounting systems. Now heightened geopolitical tensions are driving state-backed groups to take increased risk with increasingly sophisticated attacks on utilities. These pose a genuine threat to national security now.

Figure 2: High impact cyber-attacks on 4G/5G networks 2022 - 2025

Date	Country	Mobile operator	Description
Feb 2022	Portugal	Vodafone	4 million customers suffered outages. Bank ATMs and the national ambulance service were impacted. It took 4 days to restore normal service.
Dec 2023	Ukraine	Kyivstar	Russian state-funded hackers completely wiped the entire mobile core network, including thousands of virtual servers and PCs. Millions of users suffered prolonged outages over days. Costs were estimated at $100 million.
Oct 2024	USA & other	Telecom operators	'Salt Typhoon', penetrated 10 U.S. telco networks including AT&T and Verizon for espionage purposes. They did it by initially exploiting vulnerabilities in these telco organization's network infrastructure.
May 2025	South Korea	SK Telecom	An APT group penetrated SK Telecom (SKT) via a vulnerable VPN. Malware was then dropped onto a Home Subscriber Server (HSS) in SKT's mobile core, allowing exfiltration of critical USIM data of up to 23 million users. Losses due to customers churning to other operators estimated at $5 billion.

Source: HardenStance

Figure 3: High profile cyber-attacks on power and water companies

Date	Country	Sector	Description
April 2022	India	Power	China-backed group intrusion into 5 State Load Despatch Centres that carry out real-time operations for grid control and electricity dispatch in Ladakh.
Nov 2023	USA	Water	Iranian cyber threat group took over Israeli-made water pump or booster station in Aliquippa, Pennsylvania, requiring reversion to manual operations.
Dec 2023	Russia	Water	Ukrainian group deleted over 50TB of Rosvodokanal data (internal document management, email, and backups), resulting in a suspension of operations.
May 2024	Several countries	Water	Russian hacktivists manipulated human machine interfaces throughout North America & Europe causing water pumps and blower equipment to exceed normal operating parameters. Some victims had minor tank overflow events; most reverted to manual controls and quickly restored operations.
March 2025	USA	Power & water	Voltzite, affiliated to Volt Typhoon, did reconnaissance in the systems of LELWD* in Massachusetts for 300 days before detection in November 2023.

Source: HardenStance **The Littleton Electric Light and Water Departments in Littleton, Massachusetts*

In May 2023, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the cyber agencies of several other western countries released guidance on one of these threat groups, 'Volt Typhoon', an Advanced Persistent Threat (APT) cyber threat group funded by the Chinese state. CISA and partners assessed that Volt Typhoon has breached critical infrastructure in the U.S. and other western countries.

The good news is that there are a couple of ways in which securing a 4G/5G network is a bit easier for a private operator than it is for a telco.

Volt Typhoon's aims aren't espionage or IPR theft according to the aims of Chinese threat actors in the past. Instead, Volt Typhoon penetrates critical infrastructure systems to learn as much about them as possible via 'living off the land' techniques. This uses built-in network admin tools by blending in with normal traffic and limiting activity captured in default logging configurations. This makes Volt Typhoon very difficult to detect.

Volt Typhoon learns about critical infrastructure systems in order to then sabotage them in the event of military hostilities with the U.S. Earlier this year, the former head of the UK's National Cyber Security Centre (NCSC), Ciaran Martin, called Volt Typhoon "a direct military grade threat to western infrastructure." Chris Krebs, former head of CISA, called it "the Chinese military preparing for war." In February 2024, CISA further advised that Volt Typhoon has compromised IT environments in the U.S. communications, energy, transportation and water sectors. It has been embedded in some environments for at least five years. In March 2025 it was disclosed that VOLTZITE, a group allied to Volt Typhoon, had been in the network of the Littleton Electric Light and Water Departments in Littleton, Massachusetts for 300 days before detection in November 2023.

Private wireless network security fundamentals

The good news is that there are a couple of ways in which securing a 4G/5G network is a bit easier for a private operator like a utility than it is for a telco:

- **Since a private 4G/5G network is a greenfield network, it is not exposed to legacy 2G/3G vulnerabilities the way most telcos are**. 4G is still vulnerable to things like 'false base station' man-in-the-middle attacks. However, these are harder to pull off in 4G due to features like mutual authentication between base stations and end devices. 5G Stand Alone (5G SA) raises the bar for attackers still higher by encrypting the subscriber identifier over the air whereas 4G leaves the subscriber identifier in plain text.
- **Private 4G/5G networks are less exposed to DDoS attacks than telco-run wireless networks** because, unlike a telco-run network, many or most devices should be configured to prohibit access to the Internet.

- **There is no reason for third parties to sell a utility's subscriber identity modules (SIMs)** as telcos allow Mobile Virtual Network Operators (MVNOs) to do - so none of that risk needs to be borne either.
- **Small networks are less vulnerable** to the complexity that increases cyber risk for larger ones.

In most other respects, though, any cyber-attack that can succeed in a telco-run 4G/5G network can also succeed in a utility's private 4G/5G network. And as will be shown, some vulnerabilities present a greater risk to a utility.

Small networks are less vulnerable to the complexity that increases cyber risk for larger ones.

High level recommendations for a utility's security team

HardenStance recommends that the following five core principles should form the backbone of a strategy for securing a utility's private wireless network:

1. Comply with relevant standards, guidelines and frameworks.
2. Recognize the limitations of enterprise security and 3GPP security.
3. Invest in device visibility.
4. Monitor the infrastructure within an XDR framework.
5. Collaborate intensively with peers and partners.

1. Comply with relevant standards, guidelines and frameworks

As discussed below, the requirements of multiple standards bodies, industry guidelines and compliance frameworks spanning different sectors need to be embraced and complied with (and in some cases reconciled).

Aligning with standards and guidelines of multiple sectors

3GPP, the cellular industry's standardization body, bakes advanced security into the specifications for the 4G/5G core, RAN and transport infrastructure. It also specifies the Subscriber Identity Module (SIM) for authenticating users and devices. These should all be complied with but they're only a baseline.

Generic IT/OCS frameworks should be embraced, like the NIST SO 800-82 Guide to Industrial Control Systems Security and the Purdue Model for network segmentation (see **Figure 6**). Generic Zero Trust IT security frameworks should also be followed, like CISA's Zero Trust Maturity Model. This defines Zero Trust as a set of concepts "to minimize uncertainty in enforcing accurate, least privilege per-request access decisions….in a network viewed as [already] compromised." 4G/5G operators world-wide are adopting CISA's model as well as the NIST Zero Trust Architecture.

Conflicts need to be navigated and reconciled

Sector-specific regulations also need to be complied with. For the energy sector, two of the most important are NERC CIP in the U.S, which specifies safety and cybersecurity standards for the production and transmission of electricity and IEC 62351 which protects the integrity and confidentiality of energy-related data. The security architecture and operations must also navigate and reconcile conflicts between different standards and frameworks. One example is NERC CIP's adherence to an Electronic Security Perimeter (ESP) whereas Zero Trust drives cybersecurity strategy away from perimeter-based security.

2. Recognize the limitations of enterprise security and 3GPP security

As will be shown, best practice enterprise security principles, 3GPP's 4G/5G security specifications, and even some enterprise security software licences, can all be re-used for securing a utility's wireless network. But security teams can't rely on these alone:

- **3GPP, the cellular industry standardization body, has its limitations**. Utilities should make full use of the outstanding suite of authentication, encryption, integrity protection and other security specifications 3GPP provides. But 3GPP doesn't provide guidance on how to operationalize security. For example, it provides no guidance with respect to how to do network security monitoring, orchestration, detection or response. As shown in the section on device visibility on this page, 3GPP also has significant limitations with respect to a utility's IoT security model.
- **The security architecture must take full account of just how different a 4G/5G network is from an enterprise IT environment**. Normal and abnormal behaviours of unique 4G/5G protocols like GPRS Tunnelling Protocols (GTP) and Stream Control Transmission Protocol (SCTP) must be understood. The dependencies - and the good and bad behaviours - of different 4G and 5G network functions are also very different to IT applications

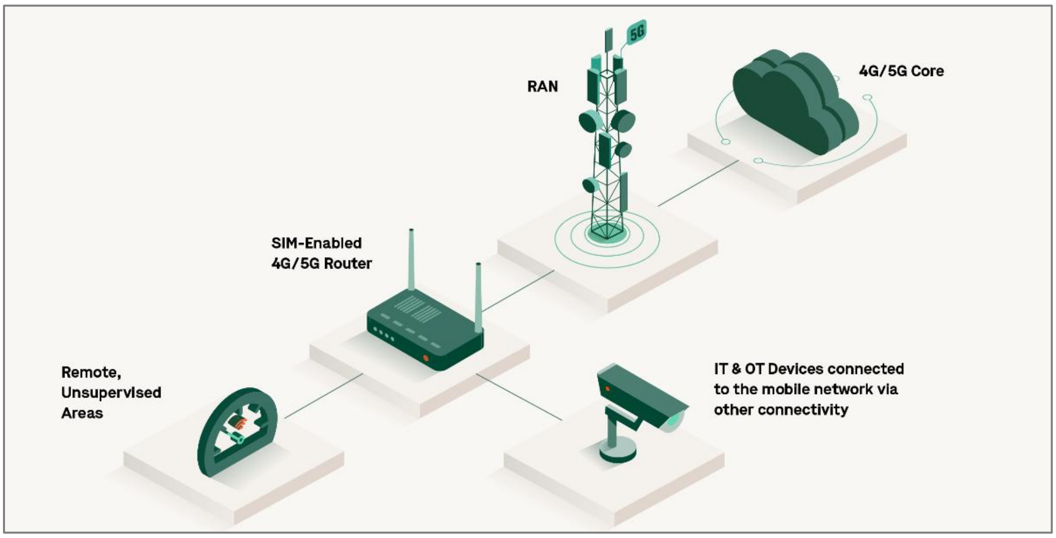
It's often not possible to patch some OT devices; even when it is, patching is nowhere near as frequent or automated as it is in IT.

- **OT security is chronically immature. Many of a utility's OT devices can't support standard IT protections** like Endpoint Detection and Response (EDR) software. It's often not possible to patch some OT devices; even when it is, patching is nowhere near as frequent or automated as it is in IT. A lot of OT/ICS protocols tend not to have good security built into them, either. And where fixes exist, they're often not universally implemented (or they're implemented but poorly).
- **A current NGFW licence can be extended to cover private wireless traffic – but only if it supports key 4G/5G protocols like GTP and SCTP**. As will be shown, current EDR and Privilege Access Management (PAM) solutions can also be extended into the wireless domain, but security teams should be aware that alternatives may be better tailored to a 4G/5G network run by a critical industry.

3. Invest in device visibility

A utility's cyber-attack surface increases as volumes of IT and OT devices like sensors, actuators, Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs) as well as smartphones and tablets are onboarded onto the wireless network. Many of these IoT 'things', including Remote Terminal Units (RTUs), are deployed in remote areas like remote substations or on poles.

Figure 4: **SIM-free devices deployed in remote areas present a major new risk**



These devices are very vulnerable to physical tampering by unsupervised employees and contractors, or unauthorized individuals passing by. There's often nothing to stop them being moved, swapped out or even reconfigured. The challenge is that these same IoT 'things' that cannot support an EDR client also cannot support 3GPP's proven security mechanisms for identifying and authenticating devices. They can't support an International Mobile Equipment Identity (IMEI) number which is an important device identifier (although vulnerable to being spoofed). They can't support a Subscriber Identity Module (SIM) either. And since an International Mobile Subscriber Identity (IMSI) number is stored on a SIM, these devices also can't support an IMSI.

As shown in **Figure 4,** a utility's IoT model has to depend in part on devices connecting via another wired or wireless connection to SIM-enabled cellular routers. Unless additional measures are taken, a utility's security team will lack proper visibility into what types of devices are sending and receiving exactly what types of traffic. Since a solution must be tightly integrated with the 4G/5G network, there is no choice but to look beyond both 3GPP and the enterprise security product market for a solution.

4. Monitor the infrastructure within an XDR framework

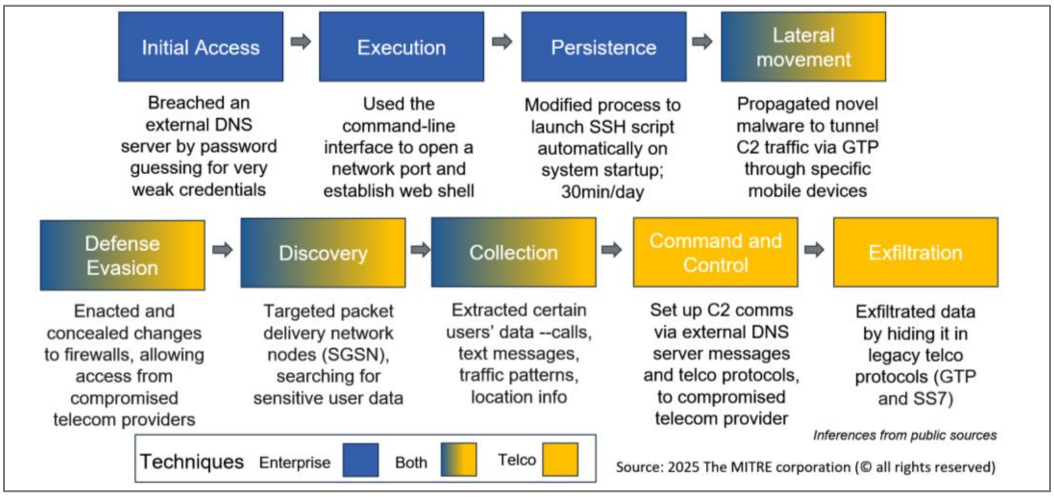
Advanced threat groups execute attacks on 4G/5G networks in multiple distinct phases over weeks, months, even years. Since some of the obfuscation techniques used are so effective, security operations needs to be able to detect suspicious behaviours among 4G/5G network functions during any one of those different phases at any point in time.

In some respects, the value of pre-integrated XDR can be greater in a private wireless context.

Figure 5 depicts the detailed TTPs of Liminal Panda, a group that has targeted 4G/5G networks via their external DNS (eDNS) servers which are part of the GPRS network. As also shown in **Figure 2,** the group that breached the South Korean 4G/5G operator, SK Telecom, earlier this year exfiltrated data by dropping malware onto a Home Subscriber Server (HSS). Both examples show that utilities need to be able to protect their own 4G/5G network functions against these types of breach by monitoring the network infrastructure for anomalies, raising alerts and remediating threats.

Utilities should also be open to an Extended Detection and Response (XDR) approach to securing the 4G/5G network and all the IT and OT devices connected to it. The value proposition of pre-integrated visibility and control across all assets and security tools is the same for private wireless as for enterprise IT. But in some respects, the value of pre-integrated XDR can be greater in a private wireless context. Pre-integration with a suite of security tools that is tailored to 4G/5G security requirements relieves utility teams of a substantial and specialized workload. Tendering RFQs, selecting security vendors, and then testing, deploying and integrating them all are tasks that security teams should be open to outsourcing to a trusted vendor with a compelling portfolio.

Figure 5: How Liminal Panda extracts sensitive data from mobile operators



Initial Access: Breached an external DNS server by password guessing for very weak credentials

Execution: Used the command-line interface to open a network port and establish web shell

Persistence: Modified process to launch SSH script automatically on system startup; 30min/day

Lateral movement: Propagated novel malware to tunnel C2 traffic via GTP through specific mobile devices

Defense Evasion: Enacted and concealed changes to firewalls, allowing access from compromised telecom providers

Discovery: Targeted packet delivery network nodes (SGSN), searching for sensitive user data

Collection: Extracted certain users' data --calls, text messages, traffic patterns, location info

Command and Control: Set up C2 comms via external DNS server messages and telco protocols, to compromised telecom provider

Exfiltration: Exfiltrated data by hiding it in legacy telco protocols (GTP and SS7)

Inferences from public sources

Source: 2025 The MITRE corporation (© all rights reserved)

5. Collaborate intensively with peers and partners

Left to itself, the market may not ensure the supply of appropriately skilled personnel to staff a utility's security operations. It won't drive cyber threat intel sharing on the latest TTPs of threat actors targeting other businesses like theirs either. Utilities should drive these outcomes themselves through intense collaboration with peers and partners.

In the case of threat intelligence collaboration, the Mitre ATT&CK Framework is widely used for tracking advanced nation state threat groups. Mitre's 5G Hierarchy of Threats (FiGHT) Framework, launched two years ago, focuses on 4G and 5G threats. These frameworks serve as inputs into assessing security posture, identify TTPs, and mapping adversary behaviours. They also enable threat hunting, and threat detection and response operations using attack and defence playbooks.

Nokia's 4G/5G security portfolio for utilities

The NetGuard portfolio is natively integrated with Nokia's 4G/5G networks portfolio as well as with the company's own security orchestration platform.

The second half of this paper describes Nokia's NetGuard cybersecurity portfolio for private wireless networks. It addresses the portfolio's suitability for securing a utility's private wireless network, spanning the full range of IT and OT devices connecting to it.

The NetGuard portfolio is natively integrated with Nokia's 4G/5G networks portfolio as well as with the company's own security orchestration platform, making it highly modular. The portfolio can also be integrated with a utility's existing SIEM platform. The device asset management solution is provided by Nokia's partner, OneLayer Bridge.

The full portfolio line-up is described in the following 5 sections.

1 Identity and access management: NetGuard IAM

2 Device asset management: OneLayer Bridge

3 Infrastructure monitoring: NetGuard EDR

4 LCM: NetGuard Certificate Management

5 Orchestration: NetGuard Cybersecurity Dome

Links to the individual product pages are provided in the 'More Information' section.

1. Identity & access management: NetGuard IAM

Privilege escalation to gain elevated access to computer systems is a very common tactic used by nation state and criminal cyber threat groups. It can take the form of credential exploitation via phishing emails; other social engineering whereby employees are manipulated into volunteering access credentials; or by exploiting software vulnerabilities, exploits and misconfigurations.

Salt Typhoon, which has so far penetrated at least ten telcos in the U.S., one in Canada and some in other western countries, has exploited at least two different privilege escalation vulnerabilities. One is in Windows Server Message Block (SMB), for networking and file-sharing and Windows Management Instrumentation (WMI) for accessing and managing system components. Salt Typhoon has also exploited a privilege escalation vulnerability in the web UI feature of Cisco IOS XE.

CISA recommends Privilege Access Management (PAM)

In its February 2024 Advisory on Volt Typhoon for IT and OT administrators and defenders, CISA encourages providers of U.S. critical national infrastructure to consider using a Privileged Access Management (PAM) solution. This has been standard best practice for many years for centrally monitoring and managing privileged access accounts throughout an organization's estate and alerting against suspicious or unauthorized activities.

Ten of CISA’s recommendations against Volt Typhoon

This is a subset of CISA’s extensive recommendations for critical infrastructure businesses from its February 7th, 2024, Advisory on China state-sponsored cyber threat actors in U.S critical infrastructure.

1. Apply patches for internet-facing systems. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
2. Document a list of threats and cyber actor TTPs relevant to your organization
3. Consider using a privileged access management (PAM) solution.
4. Segment OT assets from IT environments.
5. Enforce strict access policies for accessing OT networks.
6. Ensure logging is turned on for application, access, and security logs.
7. Closely monitor all connections into OT networks for misuse, anomalous activity, or OT protocols.
8. Monitor for unauthorized controller change attempts.
9. Tune log alerting to reduce noise while ensuring there are alerts for high-risk activities.
10. Tailor the training to network IT personnel/administrators and other key staff based on relevant organizational cyber threats and TTPs, such as Volt Typhoon.

If a utility already has a PAM, extending their vendor’s software licence to cover users that need access to the wireless network is typically the lowest cost, least disruptive, approach. But this can leave the wireless network exposed to unnecessary risk. Most popular PAM solutions can manage and enforce access rights to a wireless network’s network functions according to the roles of different types of user - for example, those who manage the operational environment; those who only need to pull statistics from a network function; and those who oversee the actual deployment of network functions and new cell sites. However, most popular PAM solutions typically do this by exposing each network function’s access credentials to users.

Users only ever need to log in to NetGuard IAM; they need never directly log in to a specific network function.

The actual credentials of network functions can be concealed

This is a risk that NetGuard Identity Access Manager (NetGuard IAM), Nokia’s Identity and Privileged Access Management solution, can close off by introducing an intermediary layer or proxy between the user and the wireless network. Users only ever need to log in to NetGuard IAM; they need never directly log in to a specific network function. The solution maps the access rights of users to specific network functions according to their role. The actual credentials of the network functions are always concealed. This reduces the risk of passwords being shared and malicious actors getting access to them.

2. Device asset management: OneLayer Bridge

Lack of visibility into exactly which devices are doing what in the network – and whether each of those device behaviours is normal or anomalous – is addressed by OneLayer's device asset management solution using device identifiers and network segmentation.

i. A unique device identifier per device

OneLayer allocates each device a unique, agentless device identifier at the point it is onboarded. It records details about the device such as the modem, device manufacturer, model, firmware, and software versions. This allows security operations to know exactly where that device is and what it's doing in real time. If a device somehow appears on the network without a device identifier, it can be disconnected.

ii. Granular network segmentation

Onboarding current use cases that are currently running on multiple single-purpose FANs – as well as enabling new ones - is the express purpose of deploying a multiservice 4G/5G network. But unless security policies prevent it, any onboarded IT or OT device could potentially access any of a utility's IT or OT resources. This can compound the risk of cyber threat actors leveraging an initial breach of IT to move laterally into OT, which is a threat vector power and water companies are already vulnerable to.

Onboarding current use cases that are currently running on multiple single-purpose FANs – as well as enabling new ones - is the express purpose of deploying a multiservice wireless network.

It's one thing to have visibility into the profile of a device but understanding whether it is doing what it should be doing – and no more than that – requires network segmentation. To mitigate the risk of so many different devices and use cases sharing the same multiservice network, each device connected to the wireless network needs to be assigned to those subnets – and only those – that it needs access to.

It's not just IT and OT that need their own subnet. IT needs separating into employees and visitors. Static OT devices need separating from those that need mobility. Sensitive use cases need their own dedicated subnet; non-sensitive ones might even need their own too. Ultimately the smaller the subnet, the smaller the 'blast radius' when an incident occurs.

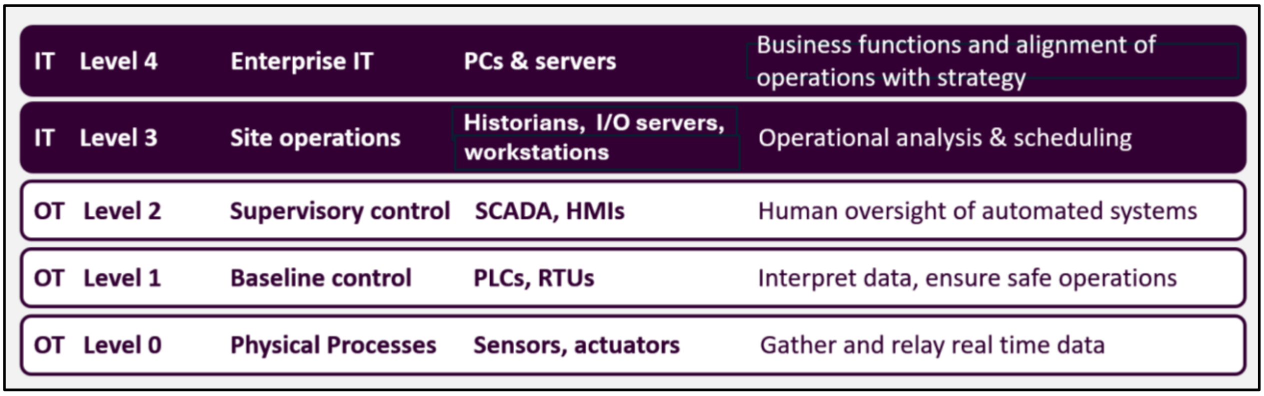
Borrowing from enterprise security – but adapting too

Telcos routinely use Access Point Names (APNs) and Virtual LANs (VLANs) in their 4G/5G network segmentation plan. However, these are typically for differentiating QoS, not segmenting for security.

Utilities should use APNs and VLANs too, but they need to be aware of their limitations.

- APNs rely on SIM authorization to connect a device to a subnet. Hence, they lack visibility into those among a utility's OT devices that sit behind a router.
- In private networks, APNs typically use static IP addresses and are designed to be configured once and then left alone in telco-run networks. They're not designed to be dynamically updated to keep up with operational risk in a utility's private network. Manual updates get increasingly complex as the network scales up.
- It is built into the standardization of cellular networks that IP addresses have to be dynamically shared between devices using Network Address Translation (NAT). This is in order to reuse the limited number of available IPv4 addresses and applies to private mobile networks as much as public networks. Hence in a mobile network IP addresses are not correlated to specific devices.

Figure 6: The Purdue Model is a good basis for a network segmentation plan



IT	Level 4	Enterprise IT	PCs & servers	Business functions and alignment of operations with strategy
IT	Level 3	Site operations	Historians, I/O servers, workstations	Operational analysis & scheduling
OT	Level 2	Supervisory control	SCADA, HMIs	Human oversight of automated systems
OT	Level 1	Baseline control	PLCs, RTUs	Interpret data, ensure safe operations
OT	Level 0	Physical Processes	Sensors, actuators	Gather and relay real time data

Source: HardenStance

Enriching APNs and IP addresses with other identifiers like GPS-based location and OneLayer's device identifier helps security teams align with their segmentation plan. Without that, the risk of policy violations increases. Real time access to all these network and device identifiers gives a persistent and accurate view of device behaviours in the wireless network in spite of all the dynamic and potentially anomalous changes that are occurring. Segmentation plans should leverage one or more established models such as the Purdue Model for ICS security (see **Figure 6**) or one of the Zero Trust frameworks. In some cases, a hybrid model borrowing from both may be advisable.

As well as a device asset management solution, OneLayer Bridge provides one half of Nokia's approach to EDR.

The device - side of the EDR solution

As well as a device asset management solution, OneLayer Bridge provides one half of Nokia's approach to EDR. As shown in the next section, NetGuard EDR combines agent-based and agentless approaches to identifying and responding to threats within the network infrastructure. By providing real-time monitoring and anomaly detection in the context of device visibility and network segmentation, OneLayer augments this with an agentless approach to EDR for end devices. Examples of the sorts of real-time alerts security operations teams can expect to see from OneLayer Bridge are as follows:

- A device connected to an intermediary cellular router has been swapped out without this being pre-authorized.
- A device has connected from an unauthorized location or has undergone handover from one cell site to another when it shouldn't (i.e. a violation of a geofencing policy)
- A change in the traffic profile coming from of an end device or a cellular router.
- A device is escalating (or has repeatedly tried to escalate) its access privileges, such as by trying to get onto a subnet it is not authorized to access.
- A device is using a protocol it should not be using.
- A device has connected which has an embedded component that violates supply chain security policy.

Devices behaving suspiciously can be quarantined, de-registered or even removed from the network altogether. Policies for specific subnets or specific devices can be updated. A subset of devices can also be patched.

3. Infrastructure monitoring: NetGuard EDR

In enterprise security, the traditional centrepiece of threat monitoring is EDR. As already noted, EDR clients can't run on many IT and OT devices. It can certainly be a good idea to extend the organization's existing EDR agents onto laptops and smartphones when they are onboarded onto the 4G/5G network. But extending enterprise-grade EDR to the servers that 4G and 5G network functions run on carries risk.

With any security solution, proper account needs to be taken of the impact on system performance. This is especially true in a 4G/5G network that supports critical national infrastructure where high availability and low latency need to be assured. Enterprise EDR agents often run in kernel space requiring elevated privileges. They can also draw heavily on CPU resources. There may be little or no risk from a laptop or workstation temporarily foregoing access to a large part of its CPU during a scan. But there is much more risk in expecting the same from a server running a Serving GPRS Support Node (SGSN), HSS or other 4G/5G network function.

With any security solution, proper account needs to be taken of the impact on system performance. This is especially true in a 4G/5G network that supports critical national infrastructure.

Complementary agent-based and agent-less components

NetGuard EDR is uniquely tailored to security monitoring requirements for 4G/5G network functions. It compromises agents deployed on the utility's servers as well as an agent-less component.

- **An agent based layer**: Lightweight agents on network servers monitor and raise alarms against events like suspicious file changes, unknown software installations, and container image deviations within the network functions. They are designed to accommodate the performance requirements of 4G/5G network functions. They don't run in kernel space, so they don't need elevated access privileges.
- **An agent-less layer**: A network sensor appliance monitors and alerts against malicious behaviours in the OA&M and control plane traffic between the network functions. As well as augmenting the monitoring provided by the agents, this protects against blind spots by providing security monitoring and alerting for elements of the network infrastructure that can't support the EDR agents.

In common with enterprise EDR systems, NetGuard EDR can trigger automated responses to events as well as support proactive threat hunting.

4. LCM: NetGuard Certificate Management

A wireless network uses Public Key Infrastructure (PKI) to securely authenticate cellular base stations or eNode Bs to the 4G/5G core as well as authenticate end devices to the base stations. No organization wants to run separate PKI infrastructures for IT and OT so if an existing solution is adequately future-proofed, it can be extended to the wireless network domain. If it can't, another solution should be considered. The history of large-scale outages arising from misconfiguration or other mismanagement of PKI certificates shows how complex and error-prone certificate management can be. **Figure 7** lists some real-world examples of the major outages this has caused.

Figure 7: Examples of major network disruption arising from PKI certificate outages and other issues

Year	Company	Country	Impact
2018	Softbank and O2	Japan and UK	Certificate expiry in the SGSN-MME network function in the mobile core network left millions of mobile users without service for several hours.
2023	Cisco	Global	Widespread customer outages arising from the expiry of certifications on Cisco Viptela vEdge 1000, vEdge 2000 and Edge 1000 SD-WAN hardware.
2023	Apple	Global	A widespread outage caused by SSL certificate issues affected Apple services, including the App Store, Apple Music, and Apple News.

Source: HardenStance

As shown, even experienced telco leaders like O2 and Softbank are among the tech sector's leaders that have learnt this from their own first-hand, experience. The standard approach to reducing risk in this domain is to reduce dependence on manual updates and configuration changes through automated lifecycle management of certificates. This has been best practice for secure 4G/5G network operations for some years. This whole environment is set to become still more dynamic, as illustrated by these examples:

NetGuard Cybersecurity Dome aggregates and correlates telemetry from a wide variety of sources for comprehensive visibility, monitoring, detection and response.

- The Certification Authority Browser Forum (CA Browser Forum), the consortium of Certification Authorities (CAs) and vendors of browser and other PKI-enabled applications, is seeking to shorten the lifecycles of some certificates to 47 days.
- Leading CAs like Let's Encrypt are seeking to retire or phase out certificate attributes like widely used TLS.
- To defend public key encryption against the power of quantum computers, the U.S. National Institute of Science and technology (NIST) announced in December 2024 that as well as disallowing them for federal use from 2035, it will begin the process of retiring RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA) by 2030.

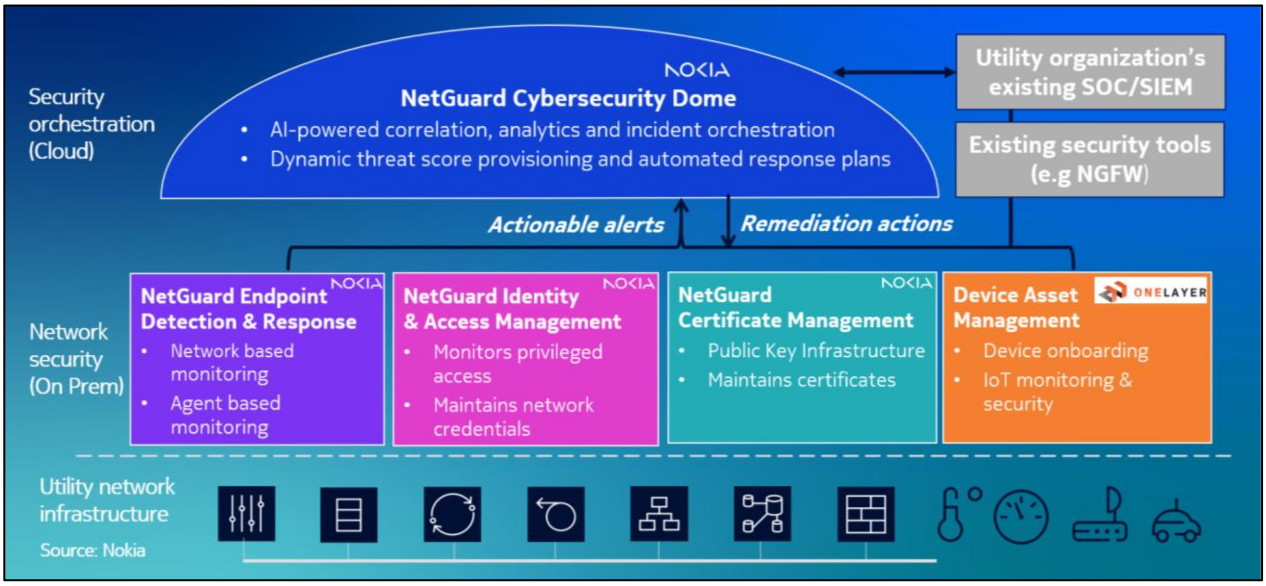
This additional dynamism will make certificate management still more vulnerable to error than it already is. That should serve as an additional impetus to plans for migrating to automated solutions like NetGuard Certificate Management.

5. Orchestration: NetGuard Cybersecurity Dome

NetGuard Cybersecurity Dome is Nokia's SaaS-based XDR platform for security orchestration and incident response in 4G/5G networks. Covering network, cloud and endpoints, it's designed for SOC analysts defending wireless networks for telcos, utilities and other critical infrastructure providers.

As shown in **Figure 8**, NetGuard Cybersecurity Dome aggregates and correlates telemetry from a wide variety of sources for comprehensive visibility, monitoring, detection and response across the network. Depending on requirements, these can include the NetGuard portfolio of EDR, IAM and Certificate Management products as well as OneLayer Bridge. It also supports integration with a utility's existing SOC/SIEM and with other security tools like Next Gen Firewalls. An initial level of filtering and normalization of the data is done on premises. Only a small subset of clearly suspicious traffic needs to be processed in the cloud.

Figure 8: Nokia's private wireless network security solution overview


Security orchestration (Cloud)
NOKIA
NetGuard Cybersecurity Dome
• AI-powered correlation, analytics and incident orchestration
• Dynamic threat score provisioning and automated response plans
Utility organization's existing SOC/SIEM
Existing security tools (e.g NGFW)
Actionable alerts
Remediation actions
Network security (On Prem)
NetGuard Endpoint Detection & Response
• Network based monitoring
• Agent based monitoring
NetGuard Identity & Access Management
• Monitors privileged access
• Maintains network credentials
NetGuard Certificate Management
• Public Key Infrastructure
• Maintains certificates
Device Asset Management
ONELAYER
• Device onboarding
• IoT monitoring & security
Utility network infrastructure
Source: Nokia

Correlation across all these sources using AI-enhanced analytics means that security teams should be able to have more confidence in risk scores accorded to patterns and events than they have in alerts from point products. The solution builds threat signatures it can recognize and respond to, including with defensive playbooks. Examples of responses include disconnecting comprised users, terminating a compromised network function and spinning up a new one, and blocking malicious command and control traffic.

Nokia has trained OpenAI's algorithms on 4G/5G network topologies spanning RAN, transport and core networks.

Cybersecurity Dome leverages parts of Microsoft's cloud, AI and cybersecurity portfolios. It is hosted in Azure and leverages 'Sentinel', Microsoft's SIEM. Nokia has also integrated a GenAI Assistant that uses Azure OpenAI Service which powers Microsoft Copilot, including Copilot for Security. Nokia has trained OpenAI's algorithms on 4G/5G network topologies spanning RAN, transport and core networks as well as on telecom threat intelligence and attack and defensive playbooks from multiple sources. These include Nokia's own threat intel derived from working with customers worldwide as well as from the MITRE ATT&CK framework and MITRE's FiGHT framework for 4G/5G threats. ■

More Information

About Nokia

Nokia is an industry leader for its private 5G/LTE network solutions that drive industrial digital transformation. Utilizing advanced technologies such as Nokia Digital Automation Cloud (DAC), Modular Private Wireless (MPW) and NetGuard Security suite, Nokia delivers secure, scalable, and high-performance connectivity tailored for Industry 4.0 applications.

By addressing complex operational challenges through reliable, low-latency connectivity, AI-driven automation, and robust data security, Nokia empowers enterprises to optimize efficiency, enhance automation, and foster sustainability.

With deployments across over 795+ enterprise customers and 1,500 mission-critical networks, Nokia's innovative private wireless solutions are setting new standards for connectivity, security, operational excellence, and industrial growth worldwide.

Details of each of the products in Nokia's NetGuard portfolio can be viewed here:

- NetGuard Certificate Manager
- NetGuard Cybersecurity Dome
- NetGuard EDR
- NetGuard Identity Access Manager

About OneLayer

OneLayer provides advanced asset management, operational intelligence, and zero trust security for private LTE and 5G networks. Its solutions empower organizations to manage and secure cellular networks, all without deep cellular expertise. For more, information visit www.onelayer.com.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, ETSI and TM Forum. To learn more visit www.hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, non-infringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.