**No.65**
*March 8th 2023*

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/ NOT SPONSORED**

# MWC23: Taking Stock of Telco Security

*HardenStance absorbed the vibes within and beyond the Fira Barcelona at MWC last week. This snapshot review of telco security includes notes from meetings with Accedian, Allot, Enea AdaptiveMobile Security, Ericsson, F5, Fortinet, Juniper Networks, MEF, Mobileum, Nokia, Palo Alto Networks, Titanium Software and Viavi Solutions.*

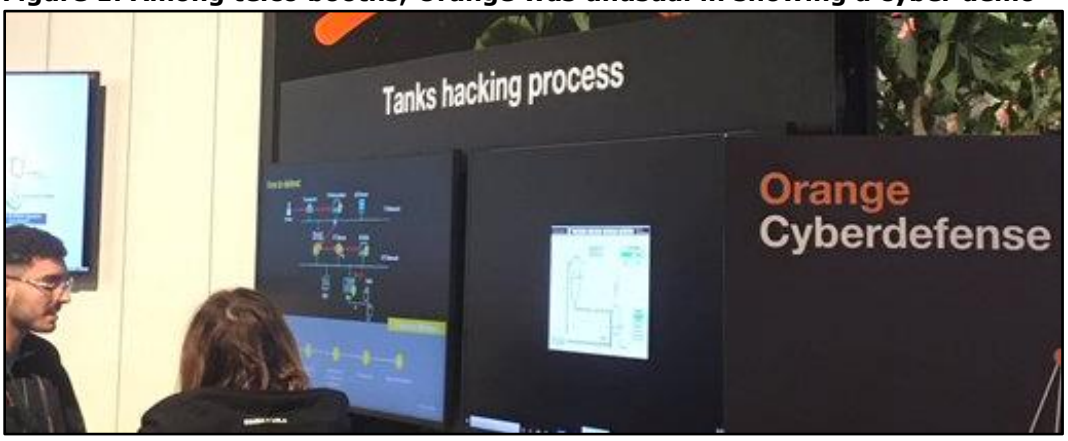
- Major delays in 5G SA rollouts mean leading telcos are only just starting to invest in cyber security solutions that are cloud-centric and that map to the emerging 5G attack surface and threat landscape. Vendors aren't shipping much new stuff.
- An informal HardenStance poll shows security vendors are hopeful new telecom security regulations can help drive incremental demand but this will take a couple of years to materialise. In MWC meetings, HardenStance pointed out a new $150 billion programme of ICT security funding that literally no-one had even heard of.
- There was evidence of ongoing and new investment in securing cloud native 5G development and operations; news on SEPP platforms; even OpenRAN security. But commercial proof-points were thin in the ground. Yes, it's still very early days.

It was great going onto the telco exhibition stands in Barcelona last week. Vodafone, Telefonica, Orange, Deutsche Telekom, Verizon. They all had demo pod after demo pod depicting their progress against the 1 – 5 scale of the cyber security maturity model; talks on the lessons learnt from so many telco breaches of the last 12 months that we've lost count of them; and commitments to increasing the frequency with which they rehearse their internal cyber incident response plans to two or three times a year. It was heartening to see such leadership in cybersecurity - baked in, not an afterthought.

*Among the telco exhibition stands, only Orange had a cybersecurity demo of any kind.*

And – the four words every school child gets to use at least once at the very end of a creative writing assignment – "then I woke up." I saw none of the above in Barcelona, of course. Rather, and in keeping with MWC tradition, what I actually saw on these big telco stands was a couple of references to cybersecurity – one slide in a presentation here, one bullet on a slide there. Among them, only Orange had a cybersecurity demo of any kind. Moreover, aligned with the company targeting €1.3 billion in cybersecurity

**Figure 1: Among telco booths, Orange was unusual in showing a cyber demo**




*Source: HardenStance*

revenues by 2025, that demo showed how Orange makes money selling cybersecurity services to organizations whose cybersecurity capabilities are inferior to its own. Meantime, last Tuesday, thousands of miles from Barcelona, in an FCC filing, Dish Network attributed the six days of disruption it had endured up to that point to "a cyber security incident" during which "certain data was extracted". Yes, six days.

In cybersecurity, as in many things, context is everything. And HardenStance's MWC meetings with network security vendors at the Fira Barcelona took place against the backdrop of a telecom sector's outlook on cybersecurity which is inconsistent, conflicted, and far from satisfactory. If it wasn't these things, governments wouldn't be as motivated as they clearly are now to prescribe stricter regulations for telcos in the belief that only government mandates can raise the sector's cybersecurity posture to the level required for such a critical industry that all others are so dependent on (see page 7).

*It's not that telcos don't care about cybersecurity. They do – sort of. It's more that they haven't found the right way of updating how they care about it in the modern world.*

## Telcos need to think and communicate differently on cybersecurity

It's not that telcos don't care about cybersecurity. They do – sort of. It's more that they haven't found the right way of updating how they care about it in the modern world, how they build and implement strategy, and how they talk about it. Unfortunately, Dish itself serves as a good (or bad) example. Coming up on two years ago, Dish released a White Paper describing its blueprint for securing its 5G network and how it was partnering Nokia, Palo Alto Networks and Allot to execute on it. It was unusually bold.

Line that paper up alongside last week's 6 days of disruption now and the two don't fit together well. Here's why: in its SEC Filing the Thursday before MWC, Dish stated that "DISH, Sling and our wireless and data networks remain operational; however the Corporation's internal communications, customer call centres and internet sites have been affected." Speculating on the causes of an incident from afar is always perilous but it does seem pretty reasonable to conclude from Dish's filing that the 5G network itself, and the contributions to its security by the three mentioned vendors, were not affected by the breach and that a failure of 5G security was not the cause of it.

No, just like so many telcos security incidents, including the many high profile breaches at T-Mobile USA, and the major recent one at Optus in Australia, the Dish filing is clear that it was the company's internal IT systems that were affected. In other words, with its 5G security positioning two years ago, Dish stuck its neck out as a cybersecurity leader by promoting the security of its doors but didn't properly secure its windows.

And here's the key thing: the impact of a telco breach tends to feel much the same from a customer or investor perspective no matter what side of the house gets hacked. They don't know – or care to know – the difference. The telecom sector as a whole has yet to properly reflect and act on its lopsided approach to cybersecurity. There needs to be a rebalancing of the effort that goes into securing internal enterprise IT (which telcos still view mostly as a cost) and the effort that goes into securing their telecom network (their source of revenue). That doesn't mean spending any less time and money on securing the telecom network but rather raising the level of internal IT security.

## MWC's cybersecurity focus was on the telecom network

Maybe MWC will evolve in this direction someday, but last week certainly wasn't the occasion for it, no more than any of the previous MWCs were. The rest of this report is a summary of HardenStance's learnings and take-aways from what MWC23 actually offered from a cybersecurity perspective rather than what it might have offered. And in keeping with tradition, the event that was focused unapologetically on telecom networks and services. It was also one at which cybersecurity certainly did feature, albeit not all that prominently.

## Vendors aren't shipping much new stuff

Sometimes you go to MWC and vendors tell you that the product they launched 12 or 18 months ago is flying off the shelves. Or they'll tell you that telco customers are falling over themselves to trial something brand new that's being announced at the show. This wasn't one of those years. Couched in varying degrees of impatience, a common theme of HardenStance's MWC meetings was that network security vendors are mostly shipping old stuff. That stuff might have been enhanced a bit with the odd new feature, but pretty much anything new that was launched in the last year or two seems to be shifting slowly.

The main reason for this is the extended delays in 5G standalone (5G SA) rollouts. This is what so much vendor R&D on network security targeting the telecom sector was pegged to in the 2018-2020 timeframe. That was before the pandemic hit, before it had started to truly dawn on telcos just how challenging a shift to cloud native operations really is, and before Russia's invasion of Ukraine had driven up energy costs.

*There's an extra twist to this specific market space that threatens to push demand for SEPP out even further than the other headwinds are already doing.*

### More new features than new products

Fortinet and Palo Alto Networks have both invested significant R&D in telco-specific 5G security products. Palo Alto Networks had a couple of 5G-oriented customer announcements to share this year but no new product announcements. Fortinet reported that 5G rollouts are progressing faster with Global System Integrator (GSI) partners ATOS and Cap Gemini on the private 5G side than what it is seeing from most of its telco customers. There were no new product announcements from Fortinet either. Ericsson and Nokia did have new features to announce for Ericsson Security Manager (ESM) and the NetGuard portfolio respectively. However ESM is five years old. Nokia only announced the new Cybersecurity Dome at last year's MWC but it has its origins in the previous Nokia Security Management Centre (SMC) announced at the end of 2017.

It was the same with signaling security vendors. They're shipping SS7 and Diameter firewalls as well as other products like SMS firewalls in volume. But as for the new Security Edge Protection Proxy (SEPP) for 5G, that's only just been launched in the last few weeks with one customer. And is it Generally Available (GA)? Most vendors gave an answer along the lines of "Err, yeah, I think so. Yes. Sort of. Pretty much. Yes."

There's an extra twist to the signaling security space that threatens to push demand for SEPP even further out than the other headwinds are already doing. As HardenStance covered in a White Paper supported by Orange, Deutsche Telekom and NetNumber, and published a year ago, the GSMA's 5G Mobile Roaming Revisited (5GMRR) Task Force is seeking to bridge the gap between industry stakeholders around how – or whether – to adopt PRotocol for N32 INternet Security (PRINS). This is the new 3GPP application layer security protocol that allows a subset of signaling data to be exposed, inspected and modified where intermediary IPX carriers are in the path of 5G roaming traffic.

### Extraordinarily toxic email exchanges

As this comes down to a vote within GSMA, several sources in Barcelona stated that some opposing email exchanges between interested parties have been extraordinarily toxic; so much so that there is real concern over whether outcomes can even be reached in line with conventional best practise. This in-fighting has very little to do with the geopolitical conflicts that are pulling at the threads of global Internet and mobile networks standardization more generally. The rifts in the 5GMRR Task Force are more about conflicts of interest between different business models and competing technology philosophies. In the true spirit of our times, compromise and convergence are apparently proving worryingly elusive. In the meantime, consistent with the 5GMRR's work to date, all vendors' first SEPP releases support TLS. Uncertainty remains around PRINS.

## MWC Poll #1: The $150 billion ICT Security Fund No-One's Heard Of

*Literally none of the 16 security vendors HardenStance met at MWC had heard of a $150 billion market opportunity in ICT security - one which specifically promises billions of funding for 5G and 6G security*.

The Global Partnership for Infrastructure Investment (GPII) must be the best kept secret in telecoms. Announced as a G7 commitment last June, the GPII is the western world's competitive response to China's 'Belt and Road Initiative'. It aims to mobilize $600 billion in funding by 2027. The developing world's appetite for GPII should certainly be sharpening now that a number of countries like Sri Lanka are going through various stages of buyer's remorse upon having China-built strategic assets like new ports seized by China when they can't make the repayments. Better late than never, as they say.

The GPII is targeting four specific funding areas, of which ICT security is one. Divvy that up roughly four ways and that's around $150 billion to be earmarked for ICT security over the next four years. The text of the announcement specifically calls out the importance of "open, interoperable, secure, and reliable internet and mobile networks with sound cybersecurity." That's pretty savvy as a value proposition for the many developing countries that don't trust China. The Snowden revelations of the NSA spying on Germany's Chancellor Merkel is a reminder that the U.S, the leading partner in the G7, has a mixed record itself in terms of how trusted it is not to spy on allies, let alone neutral countries. Nonetheless, geopolitically speaking, these are very rapidly changing times and the GPII should be very welcome indeed to western and western-leaning companies that are leaders in telecom security.

It's ironic, then, that literally not one of the individuals HardenStance me with at MWC last week had heard of the GPII. It's seemingly a $150 billion ICT security opportunity no-one's ever heard of. Is it "just" a G7 commitment? Couldn't it be watered down like some other G7 commitments? Maybe. But what does a watered down $150 billion commitment look like? I don't know, maybe a $75 billion commitment? Companies that want to lead in telco security over the next decade should get out in front of this. Rather than wait to see if it gets side-lined, they should engage in making damn sure it doesn't.

### 5G RAN supply diversity is mostly about Samsung

*Vodafone went all-in and announced Samsung as its chosen partner throughout Europe.*

From a 5G network supply diversity perspective – something that only came to the fore when Chinese vendors ceased to be trusted by western governments – announcements during MWC mostly reaffirmed an existing trend. It's long been HardenStance's view that among the world's big 'bellwether' telcos, the priority as regards diversifying 5G RAN suppliers is Samsung. The main goal is place enough orders with Samsung to incentivize the company to commit long term to being a number three RAN vendor behind Ericsson and Nokia. HardenStance's view is that those big telcos do want opener (yes open-er) RAN. Nevertheless, beefing up Samsung irrespective of its product architecture or partner ecosystem is a greater priority than realizing a fully OpenRAN vision supported by a much larger sub supplier ecosystem than in the past. If they can have both, that's of interest. But if one risks jeopardising the other, ensuring Samsung's long term commitment to the market comes first.

One announcement at MWC gave this direction another strong push. Having selected Samsung first for the UK and then Germany, Vodafone announced its' selection of Samsung "to deploy OpenRAN" throughout Europe. Deutsche Telekom, however, went off-script (or at least off HardenStance's script). Rather than add to Samsung's order book, DT announced that, seemingly truer to OpenRAN goals, it has chosen Nokia, Fujitsu and Mavenir. That said, just how "progressive" this proves will depend heavily on the total amount of spend by DT and the share of it that goes to Nokia rather than the two smaller players. If most of it ends up going to Nokia, this could potentially have a more "regressive" effect from a supply diversity perspective than picking Samsung.

## Some evidence of innovation – it wasn't all gloom

It is HardenStance's view that the domain where most 5G security innovation and investment will be needed on top of 3GPP security standards is in cloud native development and operations. Every mobile operator on the planet is going to have to evolve towards cloud native development and operations. There's no avoiding the major expansion of the attack surface that this entails, including the opportunity that automation creates to increase cyber security risk as well as reduce it. Visibility, monitoring, anomaly detection, threat detection and mitigation throughout a telco's cloud native development and operations (or devops) environments is where the single biggest 5G security challenge lies and where the most investment is going to be needed – in people, processes and technology.

Here, then, are some of the highlights of what vendors shared with HardenStance at MWC in terms of new security capabilities for development and operations environments.

- **Accedian**: Having launched it at RSA last year, Accedian showed up at MWC showcasing its new network security capabilities at MWC for the first time. Its Network Detection and Response (NDR) software is branded 'Interceptor', available from the same Skylight platform that drives Accedian's core performance optimization solutions.

*The Ericsson Security Manager (ESM) is able to monitor Cloud Native Network Functions and spot deviations from expected behaviours now.*

- **Ericsson:** Having launched an asset discovery capability 18 months ago, the latest release of Ericsson Security Manager (ESM) now fully automates this. ESM is also able to monitor Cloud Native Network Functions (CNFs) and spot deviations from expected behaviours now. Among some of the detection features recently added to ESM are OAM log threat detection and RAN Detection Logic. In conjunction with Advanced RAN Defence software in Ericsson's baseband products and the Ericsson Network Management (ENM) system, ESM's RAN Detection Logic supports the detection of false base stations that are used in 'IMSI catcher' attacks.
- **F5:** F5's portfolio of CNFs is now Generally Available (GA). BIG-IP Next Edge Firewall CNF, BIG-IP Next Policy Enforcer CNF, BIG-IP Next DNS CNF, and BIG-IP Next CGNAT CNF support several use cases for securing and enhancing 5G deployments.
- **Nokia:** Whereas the established feature set in Nokia's NetGuard EDR offer protects subscriber endpoints like smartphones according to a network-based or agentless approach, the new EDR feature announced at MWC does something different but complementary. The new EDR feature uses an agent to protect an operator's CNFs against things like unauthorized privilege escalation, deletion of logs and root access. Strictly speaking, CNFs aren't 'endpoints'. Nokia's explanation for using the term is that it finds itself pitching this part of its security portfolio against EDR/XDR vendors like CrowdStrike, so has had to align its branding accordingly.
- **Palo Alto Networks:** As part of Palo Alto Networks' promotion of continuous security visibility, detection and prevention with 5G subscriber-ID and equipment-ID granularity across all layers, all locations, all attack vectors, and all software lifecycle stages, deployment of Prisma Cloud, the company's cloud native security platform (CNSP) is ongoing in Globe Telecom in the Philippines. This includes different modules including Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP) and microsegmentation.
- **Three other vendors:** HardenStance's meetings with two other vendors (one large, one small, neither profiled in this report) yielded further evidence of new investment already going into new telco security operations products. The meeting with **Juniper Networks** also yielded enough to suggest that investment in some segment of this broad product space is possible, perhaps likely.

## SEPP platforms are (more or less) Generally Available

Despite the lag in rolling out 5G SA roaming, it was good to see Enea AdaptiveMobile Security, Mobileum and Titanium Software all pointing to having their initial 5G SEPP releases in deployment. All vendors support TLS in the first instance. As discussed on page 3, they are all awaiting the outcome of the 5GMRR Task Force's deliberations regarding the fate of the PRINS protocol. Being able to support a high level of integration with mobile roaming value added services providers is going to be important in evaluating any SEPP platform. The greater the flexibility in these vendors' architectures, the easier it will be to make whatever adaptations are needed over time.

## Some vendors promoted security solutions for OpenRAN

OpenRAN already has, and will continue to have, one of the lowest say/do ratios of any mobile network technology ever. It's not as bad as WiMAX - it won't die. But it is up there with WAP, 3G and the first small cell boom that never was in that it won't deliver anything remotely close to its original, grossly overhyped, promise. At this point in time, security isn't a priority with OpenRAN deployments. Most operators that are deploying it are still investing a lot of time – oh so much time – trying to make different components talk to one another and get the performance metrics up to required levels within an acceptable cost envelope. Security will come later (in many cases, much later).

*Consistent with its commitment to its RIC roadmap for OpenRAN, Juniper is positioning several features from its portfolio into the OpenRAN security space.*

Hence it was good to hear OpenRAN security come up in three conversations last week:

- **Fortinet** is bringing its portfolio of interface encryption, cloud/container platform protection, Zero Trust Network Access (ZTNA), Endpoint Detection and Response (EDR) and API gateway capabilities to bear to secure OpenRAN deployments.
- **Juniper:** Consistent with its commitment to its RAN Intelligent Controller (RIC) roadmap, Juniper is positioning several features from its portfolio into the OpenRAN security space. Specifically these are encrypted traffic analysis; malware detection; cloud based threat correlation; northbound interface protection and IPsec protection on OpenRAN interfaces.
- **Viavi Solutions:** With some of its key Next Gen Firewall (NGFW) customers now positioning their portfolios for the OpenRAN opportunity, VIAVI is being led by them into the RAN space and by extension the broader network security testing space. Exploring the security implications of extending disaggregation and new open interfaces into the RAN in a cloud native environment has been driving new dialogue between Viavi and some operators. This points to operators preparing to be less satisfied with a tick box, compliance-driven, approach to security testing. Conversations have also yielded some evidence of emerging demand from operators for more rigorous attention to ensuring products are adequately designed from a security perspective. According to Viavi, some operators are now asking their vendors to provide them with actual demos that attest to that.

## Edge deployments featured at the edge of MWC

Having only targeted security vendors, HardenStance may well have missed some high profile communication around edge deployments at MWC. In terms of the security vendors, however, securing edge deployments barely came up. That may be because they are seen as a little way off. For sure, environmental hardening of equipment and measures to protect against physical tampering certainly isn't where it needs to be yet.

The one memorable conversation that did crop up on this was with Fortinet. On day one of MWC, NEC published the results of a lab evaluation. This concluded that Fortinet appliances for SecGW and CGNAT scenarios can achieve up to 452% energy savings and 528% rack-space savings when compared to equivalent virtualized solutions. Fortinet is leveraging these results to position its prowess in ASIC-driven hardware acceleration for the 5G edge where operators are wrestling with trade-offs between limited space, costly power consumption, performance and security.

## MWC Poll #2: New Regulation will be Good-ish for Telecom Security

*HardenStance asked 14 individuals representing vendors – including 11 of those listed in the meeting reports - whether new cybersecurity regulations for the telecom sector will improve telecom security, make no difference, or make it worse. 50% (7 individuals) thought new regulations will improve telco security; 29% (4 individuals) thought it will make things worse; 21% (3 individuals) thought it will make no difference. Some of the anonymized responses are featured below:*

- "Ultimately it will be down to enforcement but it's a fantastic thing in principle."
- "Regardless of regulations, I think telcos will go in this direction anyway."
- "I hope it will be positive. I think it will. It goes in the right direction."
- "It depends on an operator's strategy – approaching it the right way or as a tick box exercise."
- "It will improve things. Anything like that which raises the profile and drives engagement is good."
- "It will be good. Look at GDPR - everyone rushes to comply due to the fines and the publicity."
- "It won't necessarily have positive outcomes. Regulators can make things unnecessarily complex."
- "It's inevitable, positive, and a differentiator for telcos. They're used to doing this; AWS isn't."
- "Bringing security to the forefront like this invokes positive conversation. That trumps everything."
- "Regulators don't understand their own mandates. It'll make no difference or make things worse."
- "It may not be the best way to do security but it's the best way to secure budget. It's positive."

## Where telco security spending goes from here

Three of the key factors that are going to drive the direction and shape of telecom security spending over the next two to three years are the pace of 5G SA deployment; the agility with which telcos can change their organizations and retrain their people; and new government cybersecurity regulations targeting the telecom sector.

*Hopes of a breakthrough in 5G SA deployment momentum are probably better pinned on 2024.*

- **The pace of 5G SA rollout** will be a key factor but not one that HardenStance is able to predict very dependably. With a wet finger in the air, the odds on continued slow-ish progress through the rest of 2023 must be fairly high. Hopes of a breakthrough in 5G SA deployment momentum are probably better pinned on 2024.
- **Organizational rigidity and the resulting slow pace of change** – with respect to optimizing their organizations for security or indeed anything else – came up in several conversations at MWC. Those with MEF and Accedian focused on the difficulty of getting network and security organizations to talk to each other on a strategic rather than transactional level - let alone explore areas where elements of convergence that could be advantageous with appropriate segmentation. A couple of other meetings yielded other statements along these same lines. These, however, were unprintable even as anonymized comments; let alone as statements directly attributable to the impatient individuals who spat them out.
- **New government intervention to regulate and fund cybersecurity in the telecom sector**. Although other participants got there first in some cases, HardenStance raised the likely impact of new and upcoming cybersecurity regulation of the telecom sector in each and every meeting in Barcelona. Examples include the UK's new Telecommunications (Security) Act, the EU's NIS Directive, even two new Notices of Proposed Rule Making from the FCC in the U.S. As shown in MWC Poll #2 on this page, HardenStance undertook an informal survey of several meeting participants.


The balance of opinion among those network security vendors surveyed believes new regulations will be positive for cybersecurity in the telecom sector. As shown, 50% of respondents reckoned it will be positive; 21% though it will make no difference and 29% thought it will make things worse. The anonymized statements individuals made in response are also captured. HardenStance agrees with the majority opinion. In HardenStance's view the clinching argument is the assistance regulation gives to signing-off on increased cybersecurity spending. New regulations take time to bed in and drive significant changes in behaviour and spending, though. So they will take a year or two to work their way through on the ground.

As depicted in the banner ad above, On April 20th, HardenStance is hosting *"The End of Laissez Faire in Telecom Cyber Security Regulation"* a webinar sponsored by Nokia and featuring Peter Haigh, Principal Director, Telecoms, the UK's National Cyber Security Centre (NCSC); Gerry McQuaid, Director of Telecoms and Internet Security, Ofcom; Nils Ahrlich, Head of Security Consulting, Nokia; and Patrick Donegan, Principal Analyst, HardenStance. You can register for this webinar here.

*Accedian admits to finding the cybersecurity sale with Skylight Interceptor challenging into telcos.*

As shown in MWC Poll #1 at the top of page 4, the G7 is also aiming to assemble in the region of $150 billion by 2027 to fund ICT security as part of the Global Partnership for Infrastructure Investment (GPII). Given that this effort explicitly calls for funding of security for 5G mobile networks, the fact that literally no-one HardenStance spoke to all week had heart of it was a little bit baffling.

## One-on-one meeting reports with vendors

### 1. Accedian

*Meeting with Sergio Bea, Global Enterprise and Channels and Kaela Loffler, VP Marketing.*

At RSA Conference last June, Accedian announced the launch of a new value proposition from its core 'Skylight' platform. As well as seeing 100% of traffic and monitoring it solely from a performance perspective, Accedian announced it had added a new Network Detection and Response (NDR) engine, branding it as Skylight Interceptor. This puts a cyber security lens on the traffic Skylight sees as well as a performance lens – both viewable within the same pane of glass.

Accedian serves both the internal or 'in house' network operations side of a telco organization and the business services organization. For now, Accedian is initially targeting the business services organizations with its NDR offering, many of which are already using Accedian to deliver performance optimization services like performance troubleshooting and SLA assurance. Accedian reports telco customers being quicker to capitalize on leveraging its new security features to monetize them than they are deploying them harden their own internal environments.

Despite being very well known, and generally well liked, as a performance assurance player in the telco space, Accedian admits to finding the cybersecurity sale with Skylight Interceptor challenging into telcos. As ever, organizational challenges within the telco loom large. Except for perhaps the very largest ones, it's a lot easier to converge network

and security in enterprise organizations. In a telco, the idea of converging network and security monitoring into a single platform still has a tendency to trigger powerful departmental resistance – sometimes but not always for good reasons.

From a feature perspective, Skylight Interceptor needs to be competitive in an NDR market with well-established leaders. These include Vectra, DarkTrace and ExtraHop Networks. Combining performance analytics and user experience solutions with network security monitoring in the same platform is a differentiator against these and other competitors. Purely from an NDR perspective, though, one of the most powerful competitive proof-points for any vendor is the extent to which it can minimise false positive alerts. Accedian doesn't have a hardened metric for that yet but expects to have a compelling one with which to go out to market before the end of the year. The intended metric will be one that measures reduction in false positives as a specific percentage.

A new release of Skylight Interceptor targeted for April this year will support a number of new features. These will include a honeypot/deception capability; support for Suricata rules for mapping threat intelligence to network traffic; and SIEM/SOAR integration by embedding Workato, the Integration Platform as a Service (iPaas), into Skylight rather than via multiple adapters.

## 2. Allot

*Meeting with Angel Fernandez, VP, Cybersecurity, Product Sales & Strategic Partnerships*

No major portfolio or feature changes to report at MWC. Angel did point to one significant change in buying behaviours, though. The mix of telco deployments is changing. The tendency among telcos to leverage Allot to offer premium security services to a subset of premium customers is declining. The tendency to deploy Allot universally to protect all customers is increasing. Certainly this what Allot wants to see happen – what any vendor wants to see happen – but Angel insisted Allot is seeing this playing out in the marketplace now.

## 3. Enea AdaptiveMobile Security

*Meeting with Cathal Mc Daid, CTO, AdaptiveMobile Security and Tomas Hedqvist, Product Marketing, Enea.*

*The war in Ukraine has been a key driver of how AdaptiveMobile communicates the value of its mobile network signaling and messaging security portfolio.*

I last met Cathal Mc Daid at MWC 2022, six days after troops and tanks first entered Ukraine, marking the start of Russia's invasion. I didn't anticipate then – maybe he didn't either – just how much this war would shape Enea AdaptiveMobile Security's market positioning in the next twelve months. Since then, the war in Ukraine has been a key driver of how the company communicates the value of its mobile network signaling and messaging security portfolio to telecom operators, governments and regulators.

Throughout the last year, AdaptiveMobile Security has been openly sharing intelligence on the Ukrainian networks themselves, as well as on Russian threat actors in the mobile signaling space. It has done this on a scale and with a level of detail that continues to differentiate it from competitors. The fundamental message is that mobile networks and mobile network services and applications are the new digital front in modern warfare. By extension, in the interests of national security, governments, regulators and the operators need to up their game when it comes to protecting the networks themselves and the services and applications that run on them. And that applies across all three pillars of the 'CIA' triad of cybersecurity – Confidentiality, Integrity and Availability.

Cathal reported continued solid business in both signaling and messaging security. An initial SEPP release supporting TLS has been deployed with a first customer. Eighteen months after being acquired by Enea, Cathal said that he and his team are "still evaluating the options" regarding potential use cases for integrating Enea's Qosmos ixEngine DPI technology into the AdaptiveMobile portfolio.

Threat intelligence-driven correlation between what AdaptiveMobile sees from GTP-U inspection across 4G and 5G with what it can already see from inspecting GTP-C on the telco network side in 4G and HTTP/2 in 5G may have seemed like a direction AdaptiveMobile's roadmap should take soon after becoming part of Enea. In practise – perhaps due in part to 5G SA rollout delays – it would seem that the right use case has yet to present itself.

## 4. Ericsson

*Meeting with Keijo Mononen, General Manager, Security Solutions*

Ericsson Security Manager (ESM) is the company's security automation and orchestration platform. One of its first public customer references, Swisscom, was announced four years ago at MWC 2019. Given the slowness with which telcos are adjusting to new security requirements, the fact that ESM took until a year ago to achieve double digits in customer references feels like progress on a par with the rate of market development – no more, no less. The most recent new customer reference released in the public domain was Vodafone Turkey at the end of last year.

*Having launched an asset discovery capability 18 months ago, the latest release of Ericsson Security Manager now fully automates this.*

Keijo said that demand for ESM is "taking off now" driven by 5G acceleration, enterprise customer requirements and new cybersecurity regulation of the telecom sector. A big challenge for a multi-vendor security orchestration and automation solution like ESM is racking up the number of integrations with third party vendors. The value that can be derived from ESM is at least partially determined by the visibility the platform has across the diverse array of vendors and software solutions that are scattered throughout a telco's environment – in addition to Ericsson's own portfolio.

Keijo rattled off a few big brand name vendors from the worlds of telecom networking; Next Gen Firewalls; and Identity and Access Management (IAM) that Ericsson has integrated with ESM. This still leaves a sizable list still to go to in order to give operators the fully comprehensive coverage they want from a solution like ESM. This nevertheless presents respectable progress. It has likely been a factor in growing the customer reference list as far as it has got to until now – and will continue to be a factor determining how much longer that list of customer reference grows and how fast.

Having launched an asset discovery capability 18 months ago, the latest release of ESM now fully automates this. In Kubernetes-based cloud deployments, ESM is also able to monitor CNFs and spot deviations from expected behaviours. Among some of the detection features recently added to ESM are OAM log threat detection and RAN Detection Logic. In conjunction with Advanced RAN Defence software in Ericsson's baseband products and the Ericsson Network Management (ENM) system, ESM's RAN Detection Logic supports the detection of false base station or 'IMSI catcher' attacks.

One of Keijo's other messages resonated well with me. He cautioned against operators thinking of the Extended Detection and Response (XDR) or Managed Detection and Response (MDR) market spaces as any kind of 'silver bullet'. Okay, Ericsson doesn't offer its own XDR solution. Hence his message was in part competitive positioning against enterprise IT vendors pushing XDR, not to mention Nokia's aggressive promotion of XDR over the last twelve months (and in the next door Hall 3 of the Fira). But his point was nevertheless well made: operators should focus as much on what Keijo called "fixing the basics" of cybersecurity risk via security orchestration automation in development and operations aligned with telco lifecycle management requirements. This is as important as investing in detection and response solutions as defined by the 'sexier' XDR product category which is attracting quite a lot more attention and investment.

## 5. F5

*Meeting with James Feger, Senior Vice President and General Manager, Service Provider Alix Leconte, VP, EMEA, Service Provider; Bart Salaets, EMEA CTO.*

The big news from F5 at MWC was that the portfolio of CNFs that it deployed in Rakuten Symphony's Symworld marketplace is now Generally Available (GA). BIG-IP Next Edge Firewall CNF, BIG-IP Next Policy Enforcer CNF, BIG-IP Next DNS CNF, and BIG-IP Next CGNAT CNF support a variety of use cases for securing and enhancing 5G deployments.

It's early days as regards the company's big bet on the F5 Distributed Cloud Platform. A couple of customer logos are already showing on the sales board but the organizational change required to support the model are inevitably proving challenging at this early point in the sales cycle. The F5 Distributed Cloud Platform was announced just over a year ago, combining technology from F5 itself as well as from two of its acquisitions – Volterra and Shape Security. A lot of F5, Shape, and Volterra security services have been renamed as F5 Distributed Cloud Services. These include F5 Distributed Cloud Bot Defense, F5 Distributed Cloud DDoS Mitigation, F5 Distributed Cloud WAF, and F5 Distributed Cloud API Security.

## 6. Fortinet

*Meeting with Ronen Shpirer, Director, 4G and 5G Solutions Marketing*

Fortinet continues to enjoy solid sales into the telecom sector. This continues to be driven primarily by traditional demand for 3G and 4G network firewalls and 3GPP-defined Security Gateways (SEG or SecGWs), albeit those requirements also extend into 5G Non Stand Alone (5G NSA) networks. The company has invested in security capabilities tailored to the needs of the 5G SA core – such as in the API security space – but demand for that has yet to take off.

*Fortinet technology is a key enabler of the 5G SOC service being built out by Cap Gemini.*

While it remains focused on the carriers as by far the largest 5G SA market opportunity in the medium and long term, Fortinet is seeing quite a bit more private 5G momentum with what it calls the Global Systems Integrators (GSIs). The week before MWC, ATOS, a global player in technology services, consulting and managed services, announced a new '5G Guard' managed security service for private 5G operators and public telecom operators. This features Fortinet under the hood. Fortinet technology is also a key enabler of the 5G SOC service being built out by Cap Gemini.

Fortinet had plenty to thank one of its partners, NEC, for in Barcelona. On day one of MWC, NEC published the results of a lab evaluation which concluded that Fortinet appliances for SecGW and CGNAT scenarios, can achieve up to 452% energy savings and 528% rack-space savings when compared to equivalent virtualized solutions. Fortinet is leveraging these results to position its prowess in ASIC-driven hardware acceleration for the opportunity at the 5G edge.

In these edge deployments, operators are wrestling with very challenging trade-offs that have to be made between limited space, expensive power consumption, performance and security. Fortinet is keeping an eye on the OpenRAN security opportunity too. It brings its portfolio of interface encryption, cloud/container platform protection, Zero Trust Network Access (ZTNA), Endpoint Detection and Response (EDR) and API gateway capabilities to bear to secure OpenRAN security as and when the OpenRAN ecosystem turns to prioritising security.

## 7. Juniper Networks

*Meeting with Samantha Madrid, VP, Security*

For the calendar year 2017, Juniper's security business recorded revenues of $293 million. Samantha Madrid joined as VP Security in August 2018. By calendar year 2022, Juniper's security revenues had hit $629 million. Neither Samantha nor anyone from Juniper told me that when we sat down at MWC. Or before we sat down. Or ever,

actually. They're just the facts – I sought them out all by myself. They're pertinent facts at the outset of this meeting report. They will be pertinent again towards the end too.

In the telco network itself, Juniper continues to support telco customers with the SRX firewall portfolio and security features in the MX router series. The company also has an extensive SD-WAN, SASE and SSE portfolio for channel partners including telco MSSPs.

Juniper launched its first ever push into the RAN market at last year's MWC with its announcement of a commitment to a RAN Intelligent Controller (RIC) product for the OpenRAN market space. Shortly before MWC Juniper announced a RIC trial with Vodafone. Given Juniper is still very new to the RAN market, it was good to see the company already positioning its OpenRAN security capabilities on the Juniper booth, branded as 'Zero Trust ORAN Security'. Five features are to the fore of this approach, many/most of which are driven by the Juniper SRX. These are:

- Encrypted traffic analysis (enhanced with machine learning, Juniper reckons it can spot bad SSL flows in the ORAN cloud with an accuracy in excess of 95%.
- Malware detection.
- Correlation of threat activity in the ORAN cloud with threat activity in a telco's other domains via the Advanced Threat Protection Cloud (ATP Cloud).
- SRX protection at Northbound interfaces.
- IPsec protection of ORAN interfaces according to the same principle as traditional applied by many operators to protect 4G backhaul interfaces.

*It's not a racing certainty Juniper will be talking about a new mobile network security product come MWC 2024 but it's more likely than not.*

Besides applying its existing portfolio to the ORAN space, Juniper hasn't done much new custom development specifically for the 5G SA market as bigger competitors like Fortinet and Palo Alto Networks have done. Whether by luck, or judgement, or just being focused on other things, this lag has served Juniper well because the delays in 5G SA rollout mean the market is still some way from taking off.

I suspect Juniper is going to put that right and do something tailored for 5G mobile network security requirements before long. I'm pretty sure Samantha wants to. During our meeting, I asked her about a very specific type of mobile network security product I thought could work well for Juniper. For the first time in an otherwise very animated conversation she clammed up and declined to comment. I asked her the same question in a different way. Same answer: "no comment". Followed by the discrete smiles and chuckles that are conventionally triggered when you reach that point in a conversation.

My take-way is that it's not a racing certainty that Juniper will be talking about a new mobile network security product come MWC 2024 but I suspect it's more likely than not. Why? So long as you can make a half-decent business case, doubling the revenues of your business unit from ~$300 million to ~$600 million in 5 years makes you pretty difficult to say 'No' to. Let's see how Samantha's CEO, Rami Rahim, gets on.

## 8. MEF

*Meeting with Dan Bar Lev, VP Strategic Programs, EMEA*

MEF is an operator-driven industry standards organization that has traditionally driven networking standards - Colt, Verizon Business, Comcast Business, Orange Business Services are all represented on MEF's Board. These days MEF is undergoing a pretty substantial transformation, specifying network security standards and advancing the convergence of networking and cybersecurity in communications services. There are already the MEF 117 SASE Service Attributes and Service Framework and the MEF 118 Zero Trust Framework for MEF Services of October 2022 to show for it.

The ultimate goal of these efforts, in keeping with MEF's operating model, is to deliver MEF-certified solutions into the market so an enterprise customer can have certainty that when they're evaluating a given SASE or Zero Trust service from a telecom

operator, they can know with certainty that if it is MEF-certified then it supports a given list of MEF-compliant features and capabilities.

Take the business services or MSSP arms of large telecom operators that are very, very keen on delivering standards-based SASE and Zero Trust services to business customers. Then take the many cyber security vendors that are likewise very, very keen to use those same telcos as channels to market for their SASE or Zero Trust services. You might assume then that the vendor community must be falling over itself to beat a path to MEF's door and lead from the front on MEF's SASE and Zero Trust specifications work. MEF is certainly going through the gears with SASE and Zero Trust now and the cybersecurity vendor community has started engaging. However cybersecurity vendors are not yet engaging with anything like the same energy that they are committing to pitching the proprietary products they have available into the telco channel.

In our conversation, I wondered whether maybe the cybersecurity vendor community doesn't get it at all. Or, more likely, perhaps the cybersecurity community does get it but is engaging with MEF far more slowly than it should. Dan was more sanguine. MEF has been here before, he said. The organization used to be driven by architects and engineers. Pivoting towards Life Cycle Orchestration (LSO) required embracing operations people. Bridging that gap, attracting the participation of enough of the right operations people, took a lot of time.

*Mobileum pointed to a significant uptick in sales of SMS firewalls as well as to an acceleration in cross selling of signaling firewalls, SMS firewalls and voice firewalls into the same customers.*

Evolving in the direction of security and the convergence of networking and security will also take time, he said. That's because for the most part today – in the telecom world more so than other sectors of industry – the security and network operations teams are discrete and tend to interface with one another at the margins. In many cases they don't actually know one another all that well. Dan compared the challenge of converging network operations and security thinking within MEF to the 'Bell Heads vs Net Heads' challenges of the past. From a technology perspective, what's in MEF's favour is that whereas the original SDWAN model is heavily dependent on deploying endpoints at customer premises, the SASE and SSE models are cloud-based. This will require standards-based interoperability and automation across multiple vendor components at scale. But, again, it will take time.

## 9. Mobileum

*Meeting with Stephen Ornadel, Senior VP, Security Solutions*

The main talking point emerging from Mobileum was that its' SEPP is GA and in deployment with at least one IPX carrier. The main features are multi-tenancy, availability in both standalone mode and integrated with a 5G firewall, as well as a high level of integration with mobile roaming value added services providers. In line with progress in the GSMA's 5G Mobile Roaming Revisited (5GMRR) specs, Mobileum's SEPP supports TLS with potential to support PRINS at a later date.

Mobileum expects that legislation such as the UK's new Telecommunications (Security) Act will drive demand from customers to use its' signaling related threat intelligence data. This is on the basis that they will increasingly want to be updating the platform in the context of the latest threat intelligence – and be seen to be doing so by their regulator. Mobileum pointed to a significant uptick in sales of SMS firewalls as well as an acceleration in cross selling of signaling firewalls, SMS firewalls and voice firewalls into the same customers.

## 10. Nokia

*Meeting with Gerald Reddig, Portfolio Marketing Director, Cyber Security; Rodrigo Brito, Head of Cyber Security BL; and Alex Pavlovic, Director of Product Marketing (Deepfield)*

Along with the established identity and access management (IAM); audit compliance and certificate management product lines, the two stars of Nokia's NetGuard Security portfolio are its Endpoint Detection and Response (EDR) product line and the new Cybersecurity Dome that was launched at MWC 2022 last year.

The most important development discussed at MWC was the much-anticipated evolution of Nokia's EDR roadmap. Whereas the established EDR feature set protects subscriber endpoints like smartphones according to a network-based or agentless approach, the new EDR feature, which is GA now, does something different but complementary. The new EDR feature uses an agent-based approach to protect an operator's CNFs against things like unauthorized privilege escalation, deletion of logs and root access.

*Nokia's new EDR feature uses an agent-based approach to protect an operator's CNFs against things like unauthorized privilege escalation, deletion of logs and root access.*

Strictly speaking, CNFs aren't 'endpoints'. Nokia's explanation for using the term is that it finds itself pitching this part of its security portfolio against EDR/XDR vendors like CrowdStrike, so has had to align its branding accordingly. Nokia wants to create a strong roadmap differentiator against XDR competitors from the enterprise IT security space by assuring that this new agent has virtually no impact on network performance.

Much of the XDR solution development, leveraging both NetGuard EDR and Cybersecurity Dome, is done at Nokia's Advanced Security Testing and Research (ASTaR) labs in Dallas. Here Nokia carries out penetration testing on its 5G network facilities, including with third party red team partners. Telemetry from sources like logs from Kubernetes, 5G Network Functions and NetGuard EDR, are monitored and correlated to build threat signatures that Cybersecurity Dome can recognize and act on.

Also in the mix is Nokia Bell Labs' Bhadra framework. Nokia defines this as "a structured way to talk about security events (e.g., attacks, incidents, or threats) using a common language and reference framework describing adversary behaviours in telecom networks…which takes inspiration from the MITRE ATT&CK framework." Nokia states it is collaborating on Bhadra with MITRE, including on MITRE's 5G 'FiGHT' threat intelligence framework – the 'FIve G Hierarchy of Threats'. Forming part of what looks like a substantial relationship with Microsoft in the cybersecurity space, Cybersecurity Dome now leverages Microsoft's 'Sentinel' Security Incident and Event Management (SIEM) platform running in Azure.

Nokia was also demonstrating the embedded DDoS protection and 'AnySec' encryption service capabilities of the 7750 SR routing platform on its stand in Barcelona. The 7750's roadmap seeks to make it more competitive with more expensive DDoS vendor specialists like NETSCOUT and its Arbor portfolio. Rather than being used just to block a small subset of the most straightforward DDoS attacks, as is the most common DDoS use case for network routers, Nokia is seeing to grow the share of DDoS traffic that operators can leave to the 7750 to block – and at lower cost compared with detection and mitigation by specialist vendors. Using the additional security context obtained from the cloud based Deepfield Secure Genome, and Deepfield Defender's security analytics, these days Nokia is able to go deeper into a packet to view some of the DNS and other information needed to identify and stop more complex attacks.

## 11. Palo Alto Networks

*Meeting with Lenny Burakovsky, Senior Director, Product Management*

Palo Alto Networks has assembled one of the most comprehensive cybersecurity portfolios for securing network interfaces, development and operations environments. Telco MSSP businesses have long been major sell-through customers. The company was early to spot the opportunity 5G represents to grow its sell-to business to help telcos protect their 5G networks as well as its sell-through business securing the private 5G or 5G slice-enabled deployments of those telcos' 5G business customers. That hoped-for breakthrough has been kicked down the road, in step with delays in 5G SA deployments.

There wasn't a lot to report by way of recent portfolio evolution at MWC, but that's in large part because the company arrived at a relatively advanced set of cloud native, 5G-oriented, capabilities some way ahead of market demand. The messaging at the show centred on the same staple value proposition Palo Alto Networks has been communicating for the last couple of years: the need for continuous security visibility, detection and prevention with 5G subscriber-ID and equipment-ID granularity across all layers, all locations, all attack vectors, and all software lifecycle stages.

*The Singtel announcement feels like progress in the sense of a leading operator seemingly putting security front and centre in its initial deployment of 5G network slicing.*

Having invested on the way into the 'peak of inflated expectations' of the 5G hype-cycle, Palo Alto Networks is impatient for the 'slope of enlightenment' that 5G SA at scale promises. There is, though, some evidence of 'green shoots' of 5G-oriented investment:

- **Globe Telecom** (The Philippines). Globe is using the company's Next Generation Firewalls (NGFWs) for corporate perimeter security, data center perimeter, as well as RAN Layer 7 protection. Deployment of Prisma Cloud – the company's cloud native security platform (CNSP) – is also ongoing, with enhancements being implemented on different modules including Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP) and microsegmentation.
- **Singtel:** what the operator itself refers to in its own press release as "the world's first 5G Security as a Slice (SecaaS) capability", enabled by Palo Alto Networks. If you can get past the fact that the term 'SecaaS' is far more commonly used to mean 'Security as a Service', then this announcement was welcome. Most of the telco marketing on 5G network slicing to date has either given security a single perfunctory tick-box mention - or no mention at all. Hence, this announcement feels like progress in the sense of a leading operator seemingly putting security front and centre in its initial deployment of 5G network slicing. As to what the deployment will actually amount to in practice – what the specific security value proposition will be and to whom – this announcement is too high level to be able to gauge that. Besides which, the notion of network slicing presupposes each network slice being configured with its own unique mix of supporting security features. The explanation of quite how a 'security slice' as a dedicated entity in its own right fits with multiple slices tailored to unique customers or use cases will need more explanation down the road.

## 12. Titanium Software

*Meeting with Olivier de Rocquigny, SVP, Global Carrier Sales*

Titanium Software is a new company spun out from NetNumber and is now in the process of being acquired by Lumine Group. Titanium is gearing up for the 5G roaming market and has its SEPP solution in a POC with an IPX carrier. The company is counting on the flexibility of the Titanium architecture being a differentiator when it comes to enabling interoperability with other SEPP vendors. In particular Titanium is designed to be able to extract any parameter from the signalling traffic, and then route adapt and modify it in a way that provides additional flexibility while also being standards compliant.

## 13. Viavi Solutions

*Meeting with Stephen Hire, Vice President Wireless Marketing*

One of the few security 'needles' HardenStance found worth extracting from the Omnipresent 'haystack' of endless OpenRAN babble in Barcelona was the impact it has had on network testing solutions vendor, Viavi. In the security testing space, a large part of Viavi's business in the telecom space is with Next Gen Firewall vendors, whose products are deployed to protect the mobile core.

With these key customers now positioning their portfolios for the OpenRAN opportunity (see the Juniper Networks and Fortinet examples in this report), VIAVI is being led by them into the RAN space and by extension the broader network security testing space. Exploring the security implications of extending disaggregation and new open interfaces into the RAN in a cloud native environment has been driving some new dialogue with operators. This points to operators preparing to be less satisfied with a tick box, compliance-driven, approach to security testing. It has also yielded some evidence of emerging demand from operators for more rigorous attention to ensuring that products deployed in the network are adequately designed from a security perspective. Some operators are now asking vendors to provide them with actual demos that attest to that.

*Viavi sees potential for performance and security requirements to converge over time and wants its portfolio to evolve to align with those requirements.*

Viavi sees potential for network performance and security requirements to converge over time and wants its portfolio to evolve to align with those requirements. A key principle underlying this thinking is that in a much more multi-vendor environment in both core and RAN, operators will increasingly wean themselves off having a single 'throat to choke', whether that's Ericsson or Nokia or another big systems vendor. Hence, they will need to take more responsibility themselves for security testing the different components in their network.

That's certainly consistent with the OpenRAN zeitgeist (such as it is). That said, too big a bet on that direction could also backfire if – when? – operators decide that, despite more multi-vendor disaggregation and virtualization, they still want their big system vendors to take the lead in testing and integrating their different hardware and software components. ■

# Register to receive HardenStance reports

To receive those HardenStance reports that are released free of charge in the public domain – such as this one – you can register here or at www.hardenstance.com. There are only 4 fields and HardenStance will never share your data with third parties.

Contact: Founder & Principal Analyst patrick.donegan@hardenstance.com

# HardenStance reports & upcoming virtual events

- **Webinar**: Register for HardenStance's "The End of Laissez Faire in Telecom Cyber Security Regulation" taking place on April 20th 2023, featuring speakers from Nokia, Ofcom and the UK's National Cyber Security Centre (NCSC).
- **Virtual Event**: Register for HardenStance's "Telecom Threat Intelligence Summit 2023", taking place on June 6th and 7th 2023.
- **Briefing**: "Intelligence-Driven DDoS Defence" (February 2023)
- **Briefing**: "Streamlining Telco SOC Operations" (November 2022)
- **Cybersecurity Innovators**: "Gamma" (September 2022)
- **Briefing**: "Threat Intel in Telecoms (TTIS 2022)" (July 2022)
- **White Paper**: "Defending Telecoms against Nation State Cyber Threats" (June 2022)

- **Briefing**: "Securing IP Services in Router Silicon" (March 2022)
- **White Paper**: "A Service-Based Security Posture for 5G" (February 2022)
- **White Paper**: "5G Roaming Drives Security by Redesign" (February 2022)

## About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. 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, MEF OASIS, ETSI and TM Forum. www.hardenstance.com.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): Registration Link

## HardenStance Disclaimer