No.50
October 2021

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/SPONSORED

Using Threat Intelligence in Telecoms

On October 20th 2021, HardenStance hosted the first virtual half-day "Telecom Threat Intelligence Summit". This report shares HardenStance's summary of the key takeaways from the event as well as a link to the event recording.

- Bridging the gap with the enterprise IT security world in the way mobile network threats are described and shared is a key priority for cyber security in telecoms.
- Good use of threat intelligence can improve an organization's cyber security posture and competitiveness. But threat intelligence sharing is no panacea – moreover some of it is hard. Telcos need realistic expectations of what it takes to generate an ROI.
- Investment in using threat intelligence should focus on specialist threat analyst personnel as well as automation tools and features.

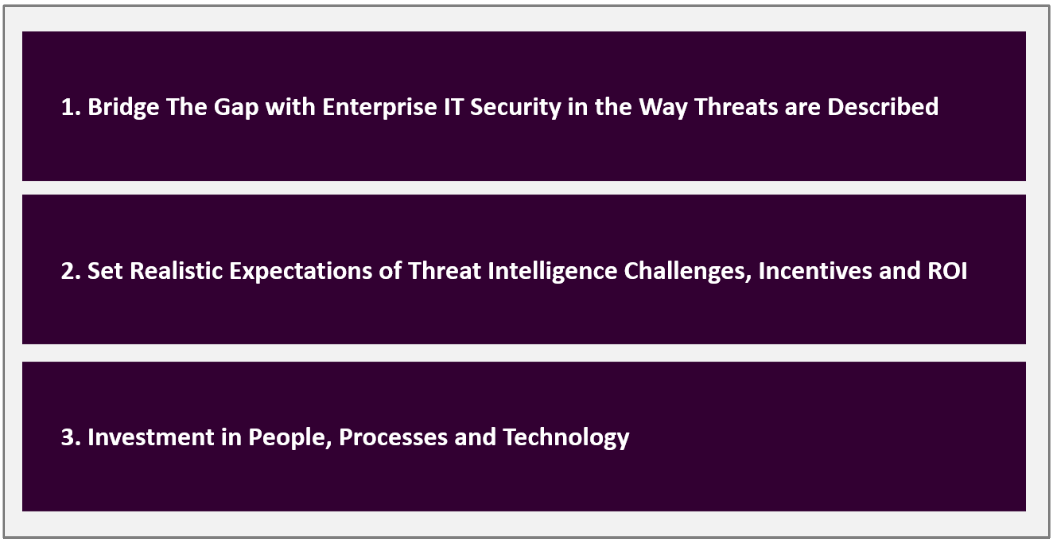
For brevity, the speakers cited in this report are referred to as follows: David (GSMA); Thomas (Deutsche Telekom); Les (Telus); Tristan (BT); Michael (Cyber Threat Alliance – CTA); Ciaran (Blavatnik School); Ed (Tag Cyber); Cathal (AdaptiveMobile Security); Tyler (EclecticIQ); Kevin (Nokia); Derek (Fortinet); Umair (Ericsson) and Roland (NETSCOUT). Their full names and job titles are featured at the end of this report.

Bridging The Gap with Enterprise IT Security

The overriding conclusion of HardenStance's half-day TTIS2021 event was that while the telecom sector is doing pretty well in terms of sharing and using threat intelligence compared with most other sectors of industry, it can do a great deal better. Michael (Cyber Threat Alliance) and Tyler (EclecticIQ) were representative of most speakers in stating that many telco security teams are good at sharing with other telco security teams. They nevertheless pointed to significant shortfalls in terms of how a lot of telcos use and share threat intelligence internally with business leaders and other stakeholders

There are significant shortfalls in how a lot of telcos share threat intelligence internally in their own organization, as well as with other sectors of industry.

Figure 1: Threat Intel Priorities for Telcos: Key Take-Aways from TTIS2021



1. Bridge The Gap with Enterprise IT Security in the Way Threats are Described

2. Set Realistic Expectations of Threat Intelligence Challenges, Incentives and ROI

3. Investment in People, Processes and Technology

Source: HardenStance

in their own organization, as well as with other sectors of industry. One of the critical gaps identified during TTIS2021 is in the way mobile network threats are described and shared in the relatively small telecom world and the way cyber threats are described and shared in the much larger world of enterprise IT security.

Most glaringly, telecom sector stakeholders don't have anything that compares with the MITRE ATT&CK Framework's open source model for standardizing and updating information on threat actors and their Tactics, Techniques and Procedures (TTPs). Several speakers stated how important it is for the mobile networks industry to bridge this gap. As many speakers noted, however, this is challenging for two main reasons:

- Knowledge of telecom protocols is heavily concentrated in the telecom sector. As Cathal (AdaptiveMobile Security) put it, "people from an IT background have as good a chance of speaking Klingon as they have of speaking SS7 or Diameter."
- Telcos are also subject to unique privacy regulations. This makes sharing data in a way that is both compliant with telecom privacy regulations and able to map usefully to a shared framework "a tall order", Cathal said.

Telcos are subject to unique privacy regulations. This makes sharing data in a way that is both compliant with telecom privacy regulations and able to map usefully to a shared framework a tall order.

Attendees from MITRE Seemed to Like What They Heard

A number of speakers chimed in on this issue, which in turn prompted several MITRE attendees to respond and interact enthusiastically in the event chat function:

- David (GSMA) said the Fraud and Security Group (FASG) he chairs is actively supporting collaboration with MITRE. At the outset of the 5G era, he said Indicators of Compromise (IoCs) and ways of describing threats "have got to be universal."
- Roland (NETSCOUT) referred to the three 'CIA' security pillars of Confidentiality, Integrity and Availability. While ATT&CK is weighted towards confidentiality and integrity, he noted that it's availability that matters most to telcos "since without availability they don't have a business." Roland reckoned a customized "ATT&CK-like" framework with a strong availability component which has equal weighting with confidentiality and integrity "would be a real boon for the industry."
- Derek (Fortinet) saw additional opportunities from aligning with MITRE in terms of playbook integration for red team and blue team wargaming in telecoms.

Other speakers pointed out additional ways that the telecom sector pays a price for its exceptionalism. Cathal noted the irony that researchers leading the recent Pegasus Project engaged a variety of stakeholders to investigate abuse of NSO Group's spyware. But rather than thinking of the mobile operator community as a first port of call to share intelligence with, they did not seem to engage with mobile operators much at all.

Want to Argue with The Regulator? You Might Need Good Threat Data

Les (Telus) showed how threat intelligence can be used to push back against aspects of the way telcos are regulated. He suggested that the long history regulators have of regulating telcos can be an all-too-familiar, all-too-comfortable "crutch" that they lean on. Hence, he said, it can be an "an impediment to targeting intervention against other actors" such as makers of cheap, poorly secured, IoT devices.

In recent engagements with the Canadian government arguing for a less telco-centric approach to dealing with botnets, Telus found itself hampered by lacking the right kind of detailed threat data with which to reinforce its case. Les used TTIS2021 to share a high-level subset of the threat data that Telus sees relating to attack vectors like DDoS, phishing and SMS attacks. He invited other operators to join Telus in building a community for normalizing these measurements on a regional basis.

A Realistic View of Challenges, Incentives & ROI

Ed (Tag Cyber) and Ciaran (Blavatnik School) brought their many years of experience at AT&T and the UK's National Cyber Security Centre (NCSC) respectively to bear in guiding attendees not to buy into what Ed called the "sophomoric" idea that threat intelligence sharing is inherently useful, that we just need a lot more of it, and that with enough of it we can solve everything.

These "hopes and prayers" around threat intelligence sharing go back many years, even decades. Despite both of them showing how these expectations are demonstrably unrealistic, Ed argued that this outdated thinking is still present in the Biden Administration's May 2021 Executive Order on Improving the Nation's Cybersecurity. Attributing this to politicians understanding information sharing very much better than they understand cyber security, Ed doubted that anyone in telecom security is craving more data, arguing that "if anything, there's too much." In a spirit of airing it so that it has visibility among key stakeholders, Ed also asserted that even in a relatively collaborative sector like telecoms, there are a subset of circumstances in which competitive rivalries can still potentially erode incentives to share threat intel.

An ROI is attainable from threat intelligence sharing programs so long as they are underpinned by four key components.

Threat Intelligence Sharing is Really Hard

Michael (Cyber Threat Alliance) stated that "sometimes people expect threat intelligence sharing to be easy but it's actually really hard and requires investment. Connecting the pipes doesn't guarantee success." Ciaran expressed this as "the absence of a common language for digesting information between organizations means the efficiency of threat intelligence sharing between them being less effective than it could be". (One attendee pointed to the STIX and TAXII standards here – see a link to a HardenStance Briefing at the end of this report).

Even if a common language is used, Tyler (EclecticIQ) showed how the value of threat intelligence can go unrealized for lack of internal collaboration. He pointed to examples of European telcos where a security team and business leaders "struggle to communicate around what threats they're seeing or around changes in business strategy." People "often don't realize the value of certain information to other teams", he said.

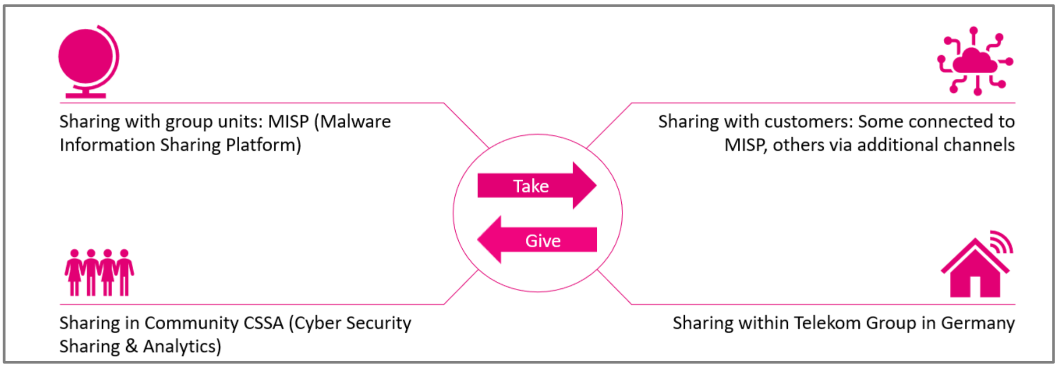
Drawing on many years' experience, Michael stated that a Return on Investment (ROI) is attainable from threat intelligence sharing programs so long as they are underpinned by four key components:

- **Trust** – that recipients will use the intelligence to deliver better security outcomes;
- **Money** – to maintain and update technology enablers like protocols and databases;
- **Time** – effort can't be put into a threat sharing sporadically;
- **Attention** – key stakeholders need awareness and appreciation of the added value.

Some examples of best practice threat intelligence sharing in the telecom sector were highlighted during the event. Going back twenty years, Roland (NETSCOUT) pointed to excellent progress in threat sharing for DDoS protection amongst telcos at the peering level. He went as far as to argue that collaboration has even reached "stupendous, almost unbelievable" levels in the last five years.

Thomas (Deutsche Telekom) and Tristan (BT) both celebrated the value their companies get from sharing on the Malware Information Sharing Platform (MISP), now re-branded the Open Source Threat Intelligence and Sharing Platform. Deutsche Telekom uses MISP to share information with group units, partners, customers and security communities. Thomas described MISP as DT's "most important" sharing platform.

Figure 2: Deutsche Telekom's Commitment to Threat Intelligence Sharing


Sharing with group units: MISP (Malware Information Sharing Platform)

Sharing with customers: Some connected to MISP, others via additional channels

Sharing in Community CSSA (Cyber Security Sharing & Analytics)

Sharing within Telekom Group in Germany

Source: Deutsche Telekom

In the case of Germany's Cyber Security Sharing and Analytics (CSSA) group which Deutsche Telekom participates in, Thomas discussed how the group is governed. He mentioned the way participants only access and use the platform if they themselves contribute to it and the way the privacy of the data shared within CSSA has to be protected. Separately, via its open source 'teapot' cyber security project, DT has extended its footprint of honeypots to more than 3,000, due to participation by a number of organizations world-wide. These include universities in Japan, South America and Africa. DT also shares threat intel with the U.S. Department of Homeland Security (DHS).

In terms of threat sharing by telcos within the FASG, however, David (GSMA) pointed to a legacy of trusted person-to-person phone calls that responds to threats far too slowly and is no longer fit for purpose. Through what he called "reform and revolution", this legacy model is being updated to respond to today's dynamic threat landscape.

Via its open source 'teapot' project, Deutsche Telekom has managed to extend its footprint of honeypots to more than 3,000, thanks to participation by a number of organizations throughout the world.

No-one Gets Close to the Financial Services Sector

A couple of speakers flagged that no industry comes close to financial services in terms of investment in large scale, industry-focused, threat sharing platforms that are well resourced, extensively used by a great many stakeholders, and used to such good effect in terms of improving security outcomes.

Ciaran (Blavatnik School) built on this to show how investment incentives play a key role in determining how an industry applies threat intelligence and threat intelligence sharing to its cyber security model. In that context, he suggested that the UK's new Telecom Security Bill – which gives government powers to mandate new telecom security measures – has strong potential to usher in positive change.

Ciaran said this can help reform what he called today's "broken" telecom model in which regulation has been focused on driving down consumer prices without pricing in adequate investment in cyber security. Ciaran alluded to a meeting of telco executives on cyber security strategy during his tenure as head of the NCSC. During that meeting one telco CEO said he assumed "we've reached the limits of you [i.e. government] asking us nicely." More stringent government requirements – or the threat of them – should sharpen telco incentives to make better use of threat intelligence.

Investment in People, Processes and Technology

Investment in people, processes and technology is central to cyber security. When it comes to the threat intelligence component, Thomas shared that Deutsche Telekom has grown its team of threat intelligence specialists from just two a couple of years ago to a double-digit number today. He said that the biggest challenge he faces in getting the most from using threat intelligence in his role is the shortage of skilled people.

In light of the high salaries threat intelligence analysts can command (and the difficulty of retaining them) Thomas told TTIS2021 that telcos that are serious about leveraging threat intelligence must invest in training their own people to fill that gap. He also specified how important it is to motivate them by giving them the freedom and the tools to do research leveraging the breadth of available data as part of their role. “If you only offer them 24/7 grunt work”, he said, “you won’t be able to attract them.”

A different dimension of the people side of the equation is business advisory groups that draw on both the public and private sectors. Pointing to his time at the NCSC, Ciaran observed that in the UK, businesses looking to get advice on 5G security threats can convene with groups of highly trusted, open and authoritative experts from government and the private sector to help them scope 5G risk. Ciaran referred to this as “a big intangible asset” and pointed to government agencies in Singapore, Canada and the U.S. as other innovators in this area.

Business Decision Makers Need to Engage Threat Intel Teams

In terms of optimizing processes, the fundamental problem of an organization being unable to ingest threat intelligence and make effective use of it internally was addressed by Tyler (EclecticIQ) in his talk on ‘Collaborative Threat Modelling’. This isn’t just about improving the way threat intelligence is used and shared within the cyber security team. Business decision makers also need to engage those same threat intel people early in the cycle of launching a new product, entering a new market, or engaging with a new business partner. That allows the way threat intelligence is sourced curated and shared to be adjusted to the upcoming change in the organization’s security posture.

In the context of detecting mobile malware out in an operator’s telecom infrastructure, Kevin (Nokia) provided additional insight into how layering different types of threat intelligence together adds value to an operator’s detection efficacy – “that way, you earn interest on the investment, so to speak.”

If your basic cyber hygiene is inadequate, all the threat intelligence data in the world isn’t going to help you much – whether it’s curated or un-curated, understandable or incomprehensible.

Umair (Ericsson) noted that different industries are at varying maturity levels in the way cyber threat intelligence is shared. In relation to 5G threats, he recognized the value of building on existing threat sharing groups. Umair nevertheless recognized that where there is strong interest in dedicated 5G networks, but threat sharing is currently lacking or poorly developed, there may be a case for Ericsson to help with convening the right group and start working towards threat intelligence sharing across industries.

Thomas (Deutsche Telekom) was clear on the paramount importance of robust cyber security processes. He stated that often, when an attack gets through, it’s because defenders are “lazy” – by which he meant they neglected basic aspects of routine cyber security processes like patching. This struck a similar note to Ed and Ciaran’s warning that threat intelligence in itself is no panacea. If your basic cyber hygiene is inadequate, all the threat intelligence in the world isn’t going to help you much – whether it’s understandable or incomprehensible, curated or un-curated.

Defenders Should be Automating at least as Fast as Attackers

The pace of investment in automating security shouldn’t be set by a telco organization’s own trajectory of being able to adopt it. It should be set by the trajectory at which attackers are automating their attacks – which is increasingly common and increasingly fast now. Thomas pointed out that when Microsoft recently released a software update to fix a critical vulnerability, it took just two hours for Deutsche Telekom to see attackers use intelligence and reverse engineering in fully automated scans across the Internet looking for vulnerable systems.

Although Roland (NETSCOUT) referred to some aspects of DDOS threat intelligence sharing between telcos as “stupendous”, he nevertheless recognized that too much of is still ‘”ad hoc”. Islands of automated threat intelligence sharing have emerged among some leading telcos in recent years but he said there is still a long way to go. Combining home grown and community-driven threat intelligence to make real time decisions on whether a given packet should be forwarded or dropped is the roadmap that telecom operators need to be aligning with now, he said.

As part of his "reform and revolution" agenda for the FASG, David (GSMA) also emphasized the need for more automation. GSMA now has an on-line threat reporting mechanism for members which also feeds into how plenary sessions are managed. Pointing to one of FASG's mottos - "one organization's detection is another's prevention" - David said he also has in mind potentially defining universal APIs for operators and other stakeholders. The GSMA could potentially host them too, he added.

Ed (Tag Cyber) said he was excited about the momentum behind intelligence-driven automation in cyber security and especially bullish about the potential in the telecoms sector. Whenever people speak reluctantly or fearfully about security automation he points them to the bygone days of the first URL filtering solutions when everyone insisted on manually checking policy updates rather than allowing them to be automated. Today, he said, we're wholly comfortable with that being automated – even if there's an error from time to time, we recognize that we'd have made errors manually ourselves anyway.

If we can get to the point where the feeds that come in become data, and we learn from that data, that seems like the perfect connection. Feed, intelligence, platform and then auto-updates – this can happen in telecom.

Ed was also very bullish about the value of Threat Intelligence Platforms (TIPs), especially when supported by a rich toolset that organizations can use to configure them themselves. Ed said, though, that he had "not seen any one in telecom deploy TIPs properly across the whole business. There's still some distance between state of the art and state of the practise."

Hardly any of the speakers at TTIS2021 spoke directly about the value of Artificial Intelligence (AI). Ed (Tag Cyber) and Thomas (Deutsche Telekom) both said that they prefer talking about the real world value of machine learning. In his concluding comments, Ed was fulsome in his enthusiasm for what machine learning algorithms can contribute to cyber security. "If we can get to the point where the feeds that come in become data, and we learn from that data, that seems like the perfect connection", he said. "Feed, intelligence, platform and then auto-updates – this can happen in telecom. I'm not as convinced about other sectors but the telecom industry gets this. That's where I think the contribution can be most meaningful from the telecom community."

Heroics from the Telecom Sector? There's a Recent Precedent

Ciaran (Blavatnik School) also expressed confidence in the telecom sector's ability to adapt to new challenges. Reflecting on the "occasionally heroic" achievements of the telecom sector at the start of the coronavirus pandemic, Ciaran reflected that if he'd been told the whole of the UK was going to have to move to remote working within a few days without a plan, he said he "would have assumed the consequences – including the cybersecurity consequences –would be a lot worse than they actually were."

Perhaps the right concluding takeaway for TTIS2021 is that if it can raise its game so effectively to mitigate the effects of the pandemic, the telecom sector can indeed do so again to meet new cyber security challenges. ■

View the TTIS2021 Event Recording

TTIS2021 was sponsored by AdaptiveMobile Security, Nokia, EclecticIQ, NETSCOUT, Ericsson and Fortinet as well as co-sponsored by The Cyber Threat Alliance. You can register to view the full four and a half hour recording of the event here:

https://events.adaptivemobile.com/hardenstance-ttsi2021

Each speaker and their start-time in the recording is listed here:

- **0.04.16** David Rogers (Chairman, GSMA's Fraud and Security Group – FASG)
- **0.24.15** Thomas Tschersich (Chief Security Officer, Deutsche Telekom)
- **0.51.00** Tyler Oliver (XDR Product Manager, EclecticIQ)
- **1.15.00** Professor Ciaran Martin (Blavatnik School of Govt & Ex-Head, UK's NCSC)

- **1.32.00** Panel: “Threat Intelligence in the Telco Business Model”
  Derek Manky (Chief, Security Insights & Global Threat Alliances, Fortinet)
  Umair Bakhari (Head of PSIRT, Ericsson)
  Cathal Mc Daid (CTO, AdaptiveMobile Security)
  Roland Dobbins (Principal Engineer, NETSCOUT)
- **2.12.45** Michael Daniel (President and CEO, Cyber Threat Alliance – CTA)
- **2.30.55** Cathal Mc Daid (CTO, AdaptiveMobile Security)
- **2.56.30** Les Wong, (Director of the Cyber Defense Centre, Telus)
- **3.21.22** Kevin McNamee, (Security Product Manager, Nokia)
- **3.42.44** Dr Ed Amoroso (CEO, Tag Cyber and Former Chief Security Officer, AT&T)
- **4.02.33** Tristan Morgan (Director, Security Advisory Services, BT)

More Information

- Deutsche Telekom's 'Teapot' honeypot threat intel sharing project
- “Telus Security Ecosystem Report”. Contact les.wong@telus.com
- HardenStance Briefing: "An ATT&CK-Like Framework for Telcos" (September 2020)
- HardenStance Briefing: "Ericsson and Nokia Complete 5G Cyber Hack" (Feb 2020)
- HardenStance Briefing: "New STIX & TAXII Releases Approved (April 2020)
- Register to receive public domain HardenStance reports when they're released

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 and is the organizer and host of the Telecom Threat Intelligence Summit. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The GSM Association, MEF, OASIS, ETSI. The Cyber Threat Alliance. HardenStance is also a recognized Cyber Threat Alliance ‘Champion’.