

Cyber Security Innovators: Orange Polska

Service Providers #3

Network Traffic Analysis

A custom report sponsored by:



Patrick Donegan, Principal Analyst, HardenStance

February 2019



HardenStance

*"Trusted Research, Analysis & Insight in IT &
Telecom Security"*

The final content of this paper was approved and signed-off by Przemyslaw Deba, CISO, Orange Polska; Gilad Peleg, CEO, SecBI; and Patrick Donegan, Founder & Principal Analyst, HardenStance.

Executive Summary

- By comparison with most incumbent telcos, Orange Polska is unusually well placed to be a cyber security leader in its national market.
- Orange Polska has found that SecBI's Network Traffic Analysis (NTA) is capable of detecting banking and crypto-jacking malware, internal data exfiltration and other high-risk threats that the company's other defences couldn't spot.
- Orange Polska has built up significant internal expertise deriving the high value security outcomes that can come from applying machine learning to NTA use cases.
- Less than a year into the deployment, Orange Polska's focus is now turning to accelerating the automation of its responses to SecBI's detection capabilities.

Market Context

In large part because of its geopolitical location, Poland has been subjected to similar nation-state funded cyber attacks to those inflicted on other East European countries such as Estonia and Ukraine. With a population of 38 million, Poland is also a large enough market to justify investment by both global and local criminal hackers in targeted Polish-language attacks on businesses and consumers.

The Polish market in cyber security products and services is still fairly immature. This can be seen from the data points shown in **Figure 1**. These are among the responses of 127 Polish cyber security experts to the 5th issue of PwC's "Global State of Information Security" survey conducted in the autumn of 2017. The dedication of just 3% of total IT budget to cyber security by Polish companies is half the global average of around 6%. This lack of maturity in demand is still mirrored on the supply side. Relatively few of the world's largest cyber security players have their own facilities – or even dedicated sales offices – in Poland.

The Polish government is recruiting a 1,000-strong "Cyber Army"

The market is nevertheless showing some signs of maturing. On July 5th 2018, the Polish Parliament passed the Act on the National Cyber Security System (ANCS) which ensures Poland's compliance with the EU's Network and Information Security (NIS) Directive. Also, arising from a 2017 government initiative, PLN 2 billion (€465 million) is being invested in recruiting and equipping a one thousand-person strong "cyber army" to protect the country's critical infrastructure and wider economy. Among key security vendors, IBM Security opened a local X-Force Command Centre in Wroclaw in June 2017.

Figure 1: 2017 Enterprise Security Metrics in Poland

Metric	Percentage
Average share of company IT budget dedicated to cyber security	3%
Companies defined as "cyber mature" by PwC	8%
Companies that have deployed a WAF / have deployed IDS/IPS	53% / 52%
Companies that recorded a security breach	65%
Companies that suffered financial loss due to a cyber attack	44%
Companies that were victims of ransomware	21%

Source: PwC

The dedication of just 3% of total IT budget to cyber security by Polish companies is around half the global average of around 6%.

Cyber Security Strategy

Orange Polska is the incumbent telecom operator in Poland. The company arrived at this position via the former France Telecom's acquisition of a controlling stake in the former state-owned telecom operator, TPSA. This was then followed by the re-branding of France Telecom and its affiliate companies as Orange. As an Orange affiliate, Orange Polska draws on the global resources of Orange Business Services (OBS). It also leverages Orange Cyberdefense (OCD), the group's 1,200-strong cyber security business unit that provides MSSP services worldwide.

Orange Polska's first and foremost responsibilities to its customers and shareholders are to protect its own telecom and IT infrastructure, including the data that it holds on its customers. Its obligations as a provider of national critical infrastructure have also been ramped up with Poland's new ANCS legislation.

Orange Polska already has its own Computer Emergency Response Team (CERT) which operates out of its Security Operations Centre (SOC) in Warsaw. To grow its own cyber security competence, Orange Polska is focused on growing its in-house skill-sets; partnering established cyber security vendors; and partnering innovative new companies according to a model that also drives the development of internal know-how.

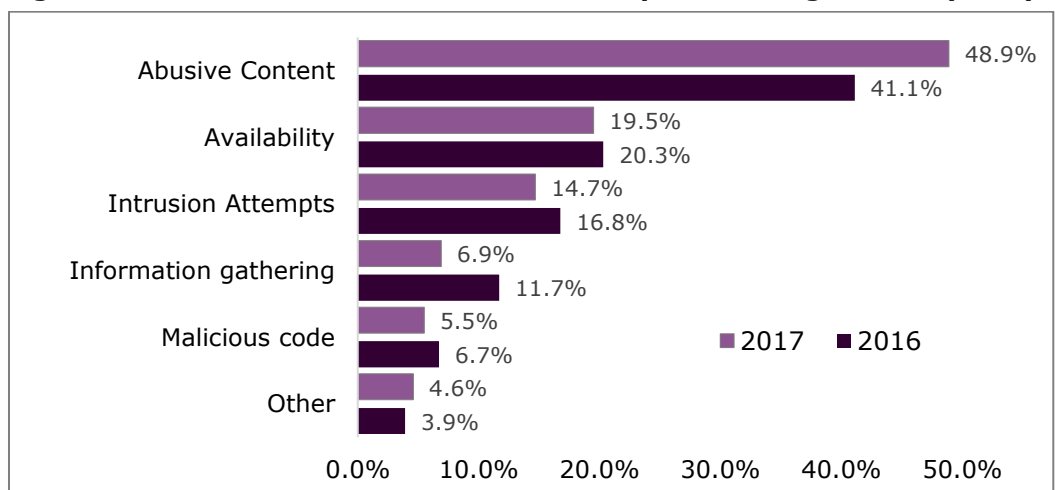
Having tested and proved cyber security solutions within its own network environment, Orange Polska looks to roll those out to Polish businesses. Whereas a local incumbent telco offering cyber security is often a couple of steps behind the cyber security leaders in mature markets, Orange Polska can lay claim to being a cyber security leader in Poland. It also serves as a centre of cyber security excellence within the Orange Group.

As an Orange affiliate, Orange Polska draws on the global resources of Orange Business Services as well as Orange Cyberdefense.

A large MSSP portfolio and leadership in Managed DDoS Services

Four years ago, the company began rolling out an enterprise security services portfolio around "clean pipes" principles. The company's portfolio comprises a variety of services including secure DNS; code audit; audit of security policy; performance tests; sensitivity scanning; malware analysis; DDoS protection; threat feed as a service; firewall audit and management automation among others. In the case of the nascent market in managed DDoS protection, Orange Polska is very well positioned and currently serves several hundred customers. The focus is increasingly on weaning customers off physical appliances towards consuming software-based solutions from the cloud.

Figure 2: Distribution of Incidents Processed by CERT Orange Polska (2017)



Source: CERT Orange Polska

In addition to either leading or being among the leaders in established cyber security products and services, Orange Polska is seeking to break new ground in key areas. As an MSSP in a relatively immature market, it recognizes that it can only expect to lead in

new, differentiated, products and services rather than with traditional approaches. One area the company wants to lead in is Network Traffic Analysis (NTA) on client to server traffic between its data centres and the external Internet. This serves as a means of detecting threats across the cyber security kill chain.

Looking to Lead in Machine Learning and Network Traffic Analysis

To that end, Orange Polska is partnering SecBI, a company which Orange Digital Ventures has invested in. SecBI is an Israel-based start-up whose Autonomous Investigation software detects suspicious activity using a combination of cluster analysis and machine learning. The machine learning comprises a core of unsupervised machine learning supplemented with supervised machine learning.

Orange Polska cut over SecBI's software to commercial service in the first quarter of 2018. The rest of this "Cyber Security Innovators" paper describes Orange Polska's experience with, and learnings from, the deployment to date. It also looks at a gap analysis and considers potential next steps.

Progress Report

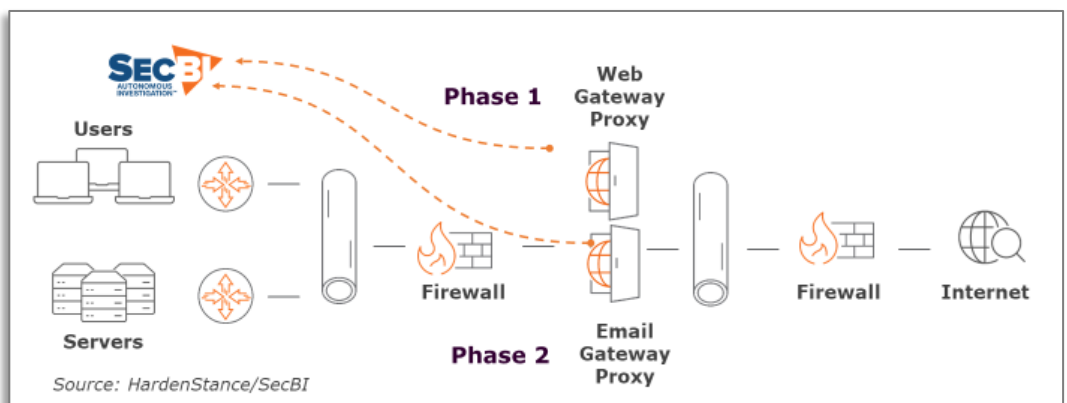
Orange Polska has deployed SecBI's software as an enterprise security solution within its own network. Consistent with its obligations under the new ANCS legislation and GDPR, Orange Polska wants to protect its own data assets and those of its customers that it stores in its network from misuse or abuse by employees, third party partners and external attackers. Neither the user traffic nor the end devices of Orange Polska's fixed and mobile communications customers are directly protected by this deployment.

SecBI's Autonomous Investigation software can be deployed on bare metal, in a virtualized environment or in any one of the major public clouds. Orange Polska's initial internal deployment is on VMware ESX. When it was cut over in a production environment a little under a year ago, Orange Polska deployed the SecBI solution to ingest traffic from the company's web gateways. At the very end of 2018, the integration was extended to its email gateways.

Orange Polska cites three specific aspects of the SecBI solution that have delivered the greatest value to the company so far:

- The simplicity of the deployment architecture. The Autonomous Investigation software runs on a standard server that's plugged into a gateway proxy. There are no specialized appliances or agents. This delivers value to the user very quickly.
- Significantly lower TCO than the big name cyber security vendors.
- Proven ability to detect threats that the company's other security tools cannot.

Figure 3: The SecBI Deployment Architecture in Orange Polska



When it was cut over in a production environment a little under a year ago, Orange Polska deployed the SecBI solution to ingest traffic from the company's web gateways.

Orange Polska cites the following specific examples of high-risk threats discovered by SecBI during 2018 that would otherwise have gone unspotted.

- **Detection of banking malware.** Banking malware is a significant threat in the Polish market. Orange Polska has successfully leveraged SecBI to detect banking malware which it wasn't able to spot with the rest of its cyber security defences. The malware was able to bypass other security controls that use threat feeds and signatures by means of techniques like encryption and sandbox obfuscation.
- **Detection of Crypto-Jacking.** The dependence of crypto mining malware on frequent communications to receive, calculate and re-distribute hashes gives any NTA solution a key advantage for detection. The exact security efficacy of an NTA solution is then down to how accurately a given vendor's software can distinguish crypto mining messages based on factors like their length and frequency. SecBI has proven effective at spotting crypto mining malware and helping Orange Polska protect against the abuse of its IT and power resources.
- **Detection of attempted data exfiltration and risky behaviour by employees.** Aware of internal security threats posed by a company's own employees, Orange Polska has undertaken separate tests under controlled conditions simulating an internal user accessing high risk websites and another attempting unauthorized data exfiltration. In both cases, the SecBI solution rapidly notified the security team of the behaviour. Again, none of the company's other security controls flagged this.

Orange Polska has successfully leveraged SecBI to detect banking malware which it wasn't able to spot with the rest of its cyber security defences.

Some of the value derived from the SecBI deployment goes beyond just a binary comparison of the solution's ability to detect compared to another's inability to do so. Since deploying SecBI, Orange Polska has seen cases where its IDS/IPS products do spot a threat just as quickly as SecBI. Here the value of SecBI has been in ongoing traffic monitoring and the discovery of instances of the same threat that made it into the network before the IDS/IPS started blocking any further instances from entering.

An important learning for Orange Polska is that deriving value from an NTA solution like SecBI's does require skilled people. SecBI outputs can certainly be fed into a SIEM and used more broadly across security operations for lower level security tasks. But leveraging SecBI's machine learning capabilities and using them to arrive at the high value detection outcomes cited above requires highly skilled people with a deep understanding of attack playbooks across the cyber kill-chain.

Orange Polska has recently started to automate some of its responses

Having spent less than a year learning how best to leverage the solution to augment its security posture in its live production networks, it's perhaps not surprising that Orange Polska has only recently started to automate some of its responses to SecBI's insights.

Until very recently, the Orange Polska team would receive SecBI insights and then manually determine next steps. Automation is being introduced in two ways. The first is internally by feeding SecBI discoveries into Hive collaboration software to help automate investigations. The team is also starting to leverage SecBI's own user interactive automation capabilities. When SecBI flags an issue, the engine recommends a course of action and gives the user a push-button option to execute on that course of action.

Based on the initial deployment in Orange Polska, Orange is now starting to roll out the SecBI solution as part of its MSSP portfolio. Orange Polska has already been instrumental in persuading another Orange affiliate to replicate its deployment model for internal security. The experience in Poland has also been leveraged to secure a first large MSSP customer for the Orange group in the form of a large financial institution headquartered in France. Orange Polska will begin reselling SecBI in Poland during 2019, initially targeting larger, well-resourced, organizations facing the most advanced threats.

Gap Analysis and Next Steps

Orange Polska's cyber security priorities for 2019 and 2020 are to further expand its internal cyber security capabilities; evolve partnerships with existing innovation partners and engage in new ones. The near term priority for the MSSP business is to accelerate sales of its existing portfolio. The medium term priority is to expand upon and drive sales of its managed security services delivered from the Orange Polska SOC.

Between them, SecBI and the Orange Polska security team are no closer to eliminating false positives altogether than any other user/vendor partnership. Compared with many legacy security products, Orange Polska's experience with SecBI is relatively good but like any user, Orange Polska still wants to go further here to reduce inefficiencies.

In terms of how it evolves its current use of the SecBI solution, two specific possibilities present themselves to the company. The first is to integrate other cyber security solution domains into SecBI in addition to the current web and email gateway integrations. A potential candidate here is to forward data from Orange Polska's endpoint protection products into SecBI.

A related option would be to integrate SecBI into the East-West traffic between servers in Orange Polska's data centres. This would provide better visibility into lateral attack vectors, complementing the North-South visibility that SecBI is already providing. Less than a year in to the initial SecBI deployment, a decision on whether to move forward in either or both these directions is pending.

At a broader level, Orange Polska's main cyber security priority over the next couple of years is to accelerate the level of automation of its security operations. Consistent with what security teams the world over are targeting, the company wants to implement a series of steps towards a highly orchestrated, highly automated SOC environment.

The End Goal is to Share Intelligence across Siloed Domains

The end goal is to enable intelligence to be shared and action taken across currently siloed security domains via open APIs, with high levels of orchestration and automation enabling dynamic adjustments to the company's security posture. Orange Polska is targeting that end goal for its own SOC and network infrastructure. Via its MSSP business, it also wants to deliver that same capability to its enterprise customers.

Three options present themselves as the core engine for driving orchestration and automation throughout the company's security operations.

- As shown, Orange Polska has already experimented with implementing automation itself through Hive. The company may consider itself big enough to justify further expanding this internal effort.
- Some of Orange Polska's current vendor partners - including SecBI - have capabilities through open APIs which position them to serve as a primary security automation and orchestration engine for large networks.
- A third option is to choose an entirely new security automation and orchestration vendor.

At this time, Orange Polska is considering all of the above options for taking its next steps towards greater automation. It could choose just one or it could assemble a solution from two or all three approaches. There's a debate to be had around the right way forward in terms of its own internal network. The outcome won't necessarily dictate the path the company chooses for serving enterprise customers as an MSSP. ■

Orange Polska's main priority over the next couple of years is to accelerate the level of automation of its security operations.

About Orange Polska S.A

Orange Polska S.A, a joint stock company, was incorporated and commenced its operations on 4 December 1991. The Orange Polska Group comprises Orange Polska and its subsidiaries. Orange Polska shares are listed on the Warsaw Stock Exchange. The Group is the principal provider of telecommunications services in Poland. The Group provides mobile and fixed telecommunications services, including calls, messaging, content, access to the Internet and TV. In addition, the Group provides ICT (Information and Communications Technology) services, leased lines and other telecommunications value added services, sells telecommunications equipment, provides data transmission, constructs telecommunications infrastructure, sells electrical energy and financial services. www.orange.pl

About SecBI

SecBI has developed a revolutionary approach to network traffic analysis (NTA) to deliver automated threat detection and investigation for Security Operations Centres (SOCs) and Managed Security Service Providers (MSSPs). Our value is best understood in contrast to solutions that generate sporadic alerts and anomalies requiring manual correlation and investigation. Our Autonomous Investigation™ technology incorporates machine learning to uncover the full scope on every suspicious incident, including all affected entities within minutes. Without the need to deploy special appliances or agents, the solution can be deployed on premise or in the cloud, and is currently used by financial institutions, telecoms, retailers, and manufacturing enterprises worldwide. For more information, visit: www.secbi.com or write to: info@secbi.com

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. www.hardenstance.com