Surveillance

Search the site ...

Trovicor: The Black Panther of Surveillance

March 24, 2015

On the Prowl for Terrorists

Of all the symbols in the surveillance industry, few resonate like the black panther of Trovicor. Pound for pound scarcely larger than a man, the panther is a silent stalker that strikes with speed, cunning and astounding strength. Size is irrelevant when counted against the assets of intelligence, stealth and – where prey are cornered — jaws as powerful as a lion's.

Similar attributes explain Trovicor's popularity with law enforcement and government agencies worldwide. When it comes to putting the bite on criminals and terrorists, few can top the black panther.

Like the big cat, Trovicor is in a class by itself, not to be lumped with single-play vendors that provide just a mediation device, or a probe, or mobile location, or deep packet inspection (DPI) or semantic technologies that separate meaning from data, or intrusive zero days that take over a target's device, or social media tracking or analytics. What *do* they offer? Answer: all of the above, depending on the client's specific need. Note that while Trovicor might not makes all such tools itself, its platform integrates with any intelligence device, software or app made by third parties.

Trovicor's approach to intelligence gathering and analysis is thus strategic and comprehensive, with the focus on providing "end to end" solutions versus piece parts. Solutions leverage the company's own strengths, and also incorporate "best-in-class" tools of other market leaders. The end result: systems that evolve quickly with the needs of the marketplace.

From Many Systems to One

Trovicor traces its roots to German multinational conglomerate Siemens, and to a subsequent joint venture with Nokia Siemens Networks (NSN), the latter now better known as Nokia Networks.

Beginning in the early 1990s the company that would become Trovicor was part of the Siemens Intelligence Solutions group's seminal Voice and Data unit. With the rise of the Internet and creation of diverse new communications mediums, the surveillance end of the business quickly took off. While many in the business began churning out boxes or software, Siemens adopted a more holistic approach with its unique Intelligence Platform. Built on a monitoring center developed by NSN, the Intelligence Platform was among the first Big Data analytics plays designed to incorporate feeds from multiple sources.

Make no mistake: Classic lawful intercept of content and metadata, together with mobile location were included. But Siemens opted to go further, adding intelligence modules that could incorporate and apply analytics to data feeds from a wide variety of sources: financial transactions, flights, car rental, voice recognition, fingerprints, DNA, police and criminal records, to name a few.

With this platform, agents in many lands could for the first time develop a layered view of the target. Heuristic analytics created target profiles and patterns. Link analysis revealed connections to other potential members of a criminal or terrorist cell. Predictive analytics pointed to near-term threats. Real-time analytics brought threats into the present, providing "next best actions" for tactical preemption.

For agents that up until this time had been forced to rely on multiple tools that at best delivered a fragmented picture, the idea of gaining a complete detailed view in a single solution was mind-bending. Siemens' Intelligence Platform quickly picked up customers in Europe, the CIS, the Middle East, Africa and the Asia Pacific.

For reasons that still remain unexplained but subsequently proved a blessing for the company, Siemens management steered clear of the lucrative North American marketplace and — with the exception of the UK — instead focused on Tier II and Tier III markets.

By 2007, Siemens Intelligence Solutions and their novel Intelligence Platform were "on a roll." Government agencies that had struggled to manage multiple challenges — not just terrorism and organized crime, but also smuggling, illegal immigration and threats to critical nuclear or energy infrastructure — now had access to one system that could handle them all.

Then, one might say, "life happened."

Siemens and NSN Take Heat

In 2005, German investigators began to explore rumors that Siemens was involved in the bribery of government officials to obtain contracts. Because the company is traded on the New York Stock Exchange, the investigation in 2006 spread to the U.S., involving the Securities & Exchange Commission and Department of Justice.

Reviewing millions of documents, criminal investigators discovered that since at least 2002, Siemens had operated a bribery unit that annually doled out $US millions in payoffs. The purse was staggering. Between 2001 and 2007 Siemens reputedly made $US 1.4 billion in illegal payments, with the principal recipients being China, Russia, Argentina, Israel and Venezuela, but also including Greece, Norway, Nigeria and other countries.

While neither Nokia Siemens Networks nor the Siemens Intelligence Solutions unit were specifically referenced in the suit, bribes were aimed principally at winning deals in the aligned field of telecommunications equipment. Bribes funneled through offshore bank accounts typically cost Siemens five percent of the contract value, though in some instances the payoff figure went much higher.

One German investigator characterized the company's offshore operations as follows: "Bribery was Siemens's business model." He may have been playing to the media. While the evidence against Siemens was strong, it's just as likely that the company was simply dealing in the realities of many of the markets it entered, where the practice of "baksheesh" is part and parcel of all business dealings for centuries.

Regardless, when the suit came to settlement in late 2008, Siemens ended up paying $US 1.6 billion in fines — at the time, the largest ever penalty of its kind — and $1.0 billion as reimbursement for government investigations in the U.S. and Germany. The cost of restructuring and cleaning house at Siemens was estimated at another $US 1.0 billion. Siemens paid up, cleared the decks and moved on.

Then in mid-2009 came the first hint of troubles in the Arab world. Reports surfaced that NSN technology was deployed in Iran to monitor protesters. The company abruptly halted all work related to its monitoring center in that country.

In 2011, North Africa exploded with the Arab Spring. Appended to that story: the revelation that NSN tech was used by regimes throughout North Africa and the Middle East.

NSN didn't wait around for an investigation. They quickly spun off their intelligence unit to an investment group based in the Channel Islands.

Return of the Black Panther

That entity is now Trovicor, providing the same technologies and services before, still under the sign of the

black panther.

The company's Monitoring Center and Intelligence Platform, variously billed as the "Fusion System," remain top sellers in the same global markets, which Trovicor supports from its Munich HQ, as well as branch offices in Dubai, Islamabad, Kiev, Prague and Kuala Lumpur. Several of these cities overlap with the sites of ISS World conferences where Trovicor often contributes as lead sponsor and a program participant.

The company is also active at ISS World shows in Johannesburg and Mexico City. But understandably, given the events of 2008 – 2010, Mexico and points south are likely as close to the U.S. as they wish to come.

Final Thoughts

Today Trovicor makes a point of promoting its social responsibility agenda, which includes measures to ensure that the company conducts business "in a respective manner by obeying the law in all countries where we sell."

Granted, that is the kind of statement that critics in the privacy arena like to latch on to and exploit. But let's put it in perspective.

Critics of surveillance tend to thrive under the umbrella of Western democracies that for reasons of national security, public safety and expediency ally themselves with authoritarian regimes. Saudi Arabia is one. Jordan, another. And Dubai. And Singapore. Etc. On the flip side, many of these same nations point an accusing finger at Western alliances with Israel, raising questions about support for a country with a questionable record on the treatment of Palestinians.

In the business arena, tech industry leaders like to descry surveillance as an impingement of privacy. Never mind that in many cases these companies' entire business models are based on the capture and exploitation of customers' personal data for purely commercial gain. Tech companies such as Google, Facebook and Apple are every bit as intrusive as the surveillance companies they condemn — arguably more so.

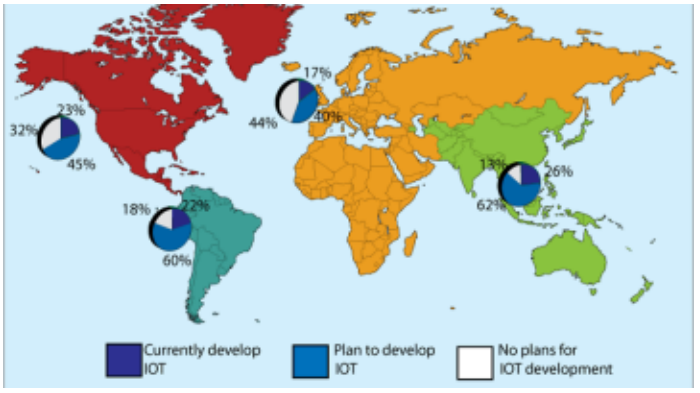
When Trovicor says that its primary mission is "to make the world a safer place," we take them at their word.

Insider Surveillance rating for Trovicor: 5 Stars.

Filed Under: Analytics, Intelligence Community, Law Enforcement
Tagged With: Analytics, Big Data, Intelligence, lawful intercept

RECENT POSTS

CYBER



Internet of Things: The Map of Cyber Intrusion Vulnerability

July 27, 2015

The Web is alive with a new report by Evans Data Corporation showing rapid expansion of the Internet of Things (IoT). The report cites North …
Continue Reading

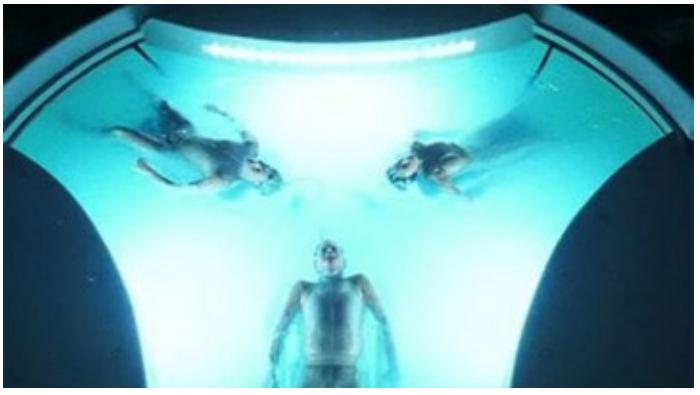
MOBILE LOCATION

Persistent Systems: Mobile Location for Lawful Intercept

July 31, 2015

Insider Surveillance reviews Persistent Systems, a provider of mobile location products for lawful intercept -- plus Big Data analytics apps …
Continue Reading

LAW ENFORCEMENT

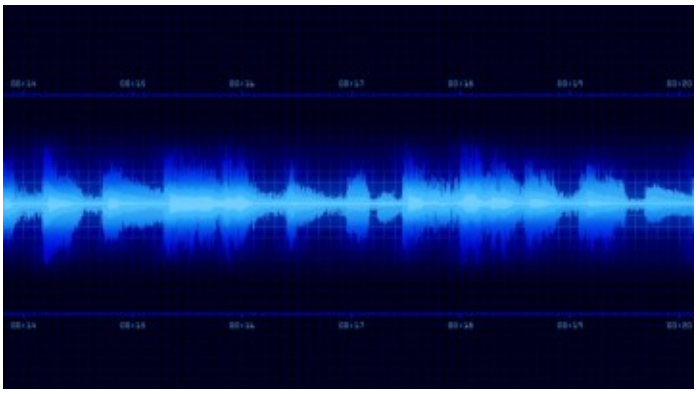


Don't Confuse Pre-Crime with Predictive Analytics

August 19, 2015

Insider Surveillance examines how rampant media hype leverages Hollywood's "Minority Report"? to distort the capabilities of pre-crime … Continue Reading

ANALYTICS

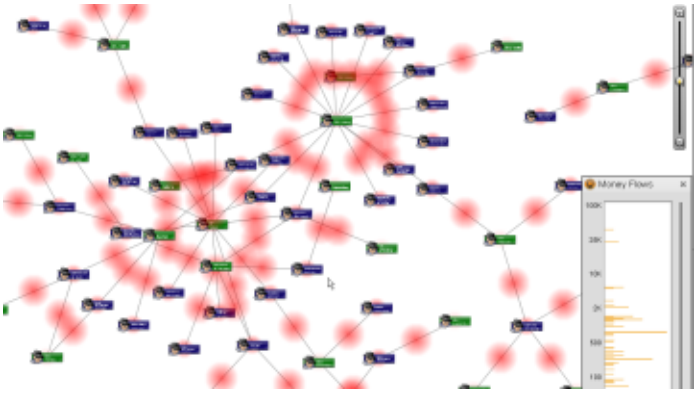


Auraya Systems Voice Biometrics: Security, Yes. Homeland Security, No.

August 4, 2015

Insider Surveillance reviews the Auraya Systems ArmorVox System, designed to prevent fraud and improve security – but not as a tool for law … Continue Reading

MILITARY



Raytheon Visual Analytics: Opting Out of War Games

August 11, 2015

Insider Surveillance reviews Raytheon's venture into visual analytics and asks: Why did Raytheon and the Pentagon pass on embracing … Continue Reading

VIEWPOINT

Central Asia – The Next Flash Point for Radical Islam

July 22, 2015

Perceptions of Central Asia terrorism run black or white. The five republics -- Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and … Continue Reading