

DETEKTOR



International

Publisher's comment

IoT creates huge security challenges

Security technology market

Video door bells smooth the way to CCTV acceptance

Business news

The latest security industry acquisitions

Product news

Arecont Vision expands Microdome range

The interview

Mahesh Saptharishi, CTO, Avigilon

Security technology industry outlook

Asian manufacturers talk about security technology trends

Security events

Intersec in Dubai successfully kicked off 2017

FOCUS ON

CYBER SECURITY & IP VIDEO SURVEILLANCE

- Hikvision responds to accusations of being a security risk
- Genetec takes action and states that governments are extremely concerned
- Bosch and Axis share their views on cyber security and IP video surveillance
- IT security expert: Some security cameras are completely unprotected

Exhibit at Denmarks biggest security exhibition in 2017



Denmark's biggest security and fire protection exhibition in 2017 will be held from the 27th – 28th of September in Copenhagen.

The theme of the event is "Investment in security and safety makes economic sense" as it is geared towards end users in Scandinavia. But of course all kinds of security services and product suppliers will be gathered during the two SecurityUser Expo days as well.



For stand reservations and more info: www.securityuserexpo.com



Exhibition

The security industry's suppliers of products and services will be gathered together at the SecurityUser Expo on the 27th – 28th of September. More than 100 exhibitors are expected to showcase their latest products in the fields of security and fire protection.



Conference

The SecurityUser Expo Conference will be focused on security for different vertical markets, for example the sectors of retail, transport, educational facilities (schools, universities, public transportation, events and sports arenas) etc.



The SecurityUser Banquet

On the 27th of September, after the first exhibition day, the organiser will host a Security Industry Dinner with entertainment and award presentations at Bella Sky.

Organiser:

armedia
Connecting Security Buyers and Suppliers

In cooperation with:

SikkerhedsBranchen
Den Danske Brancheforening for Sikkerhed og Sikring

Media partners:

DETEKTOR

SECURITY
WORLDHOTEL.COM

SecurityUser.dk



ISSN-1651-3800 published by **armedia**

Head office:

AR Media International AB
Västberga Allé 32 • S-126 30 Hägersten
SWEDEN
Tel: +46 8 556 306 80 • Fax: +46 8 19 10 11
E-mail: info@armedia.se
www.detektor.com
www.armedia.se

Asia Office

Asia office
Asha Chang
AR Media International (Asian Branch)15F,
No 55, Binhai Rd. Sec. 1,
Danshui Dist., New Taipei City 251
Taiwan
Office phone: +(886-2) 2622 1365,
+(886-2) 2622 1385
Office fax: +(886-2) 2622 1305
Mobile: +(886) 922 116272
Email: asha@armediaint.com
ashachang@gmail.com

General Information

- Detektor International is published quarterly.
- No part of this magazine may be reproduced without prior permission from the publisher.
- Detektor International welcomes manuscripts, news, releases and photographs, but cannot be held responsible for loss or damage incurred in transit or in possession.
- News releases can be sent to intnews@securityworldhotel.com

Subscriptions

Marika Thelenius
Rate for four issues is Euro 50
+46 8 556 306 80

Publisher

Lennart Alexandrie
lennart.alexandrie@armediaint.com

Editorial Team

Rachel Ward Owens, Henrik Söderlund,
Jonny Sjöberg, Lennart Alexandrie
info@armedia.se

Art Director

Linn A. Maddern
linn.maddern@armedia.se

Advertisements

Carlos Cisternas
carlos.cisternas@armediaint.com

Printing

Sörmlands Printing Solutions AB, Sweden, 2017



Lennart Alexandrie, Publisher

IoT creates huge security challenges

It is quite obvious to most people that we live in a time where the overall technology trend is the Internet of Things. More and more electronic devices are connected to the internet and provide major cost and efficiency benefits. But what about the safety of these devices? How do we know that they do not cause network attacks, virus attacks or allow opportunities for outsiders to take control? Security devices are no exception when it comes to these risks.

A camera that is being hacked can be used both for network attacks as well as unauthorised monitoring or completely shutting down the video surveillance. So far, it has been relatively quiet regarding this topic, except for some accusations of lack of security in some Chinese camera manufacturers' products. What is the main reason why cameras can easily be hacked? Like everything else, it is often actual operation that is the biggest problem; for example, passwords are often too simple and passwords are not changed. But also, the password procedure itself is a risk. Biometrics and ID solutions will most likely replace typed passwords in the future. Just take a look at how many banks have solved the problem in their network-based payment solutions. Two-factor authentication or multi-factor authentication will certainly also be used for security devices.

In this issue of the Detektor magazine, we place the focus on the problem of securing data in video surveillance applications. The starting point is the big international buzz raised last autumn, namely the accusations made against the world's largest manufacturer of video surveillance equipment – Hikvision.

The IPVM online forum and its charismatic editor, John Honowich, have been engaged in something that might be described as a hunt for Hikvision for a long time. Dumping prices has been a theme, but recently most attention has been put on Hikvision products being a cyber risk. The rhetoric has been fierce and merciless. Hikvision is accused not only of a lack of IT

security, but potentially also of granting the Chinese government access to Hikvision cameras. An article in the British newspaper The Times also supported these arguments.

The attention on Hikvision increased even more when the VMS software manufacturer Genetec decided to disfavour Hikvision cameras by making new customers using Hikvision devices pay a special license fee, and making current customers sign a waiver so that Genetec cannot be held responsible if network problems occur because of Hikvision devices. Genetec's CEO has given an exclusive interview to Detektor on why these measures have been taken. Also, Keen Yao, VP of Hikvision's International Business Centre, responds to both the accusations and insinuations and gives his view on the matter.

Even if the accusations rest heavily on hypotheses or on information from unconfirmed sources and are not necessarily true, they should be seen as an awakening for the physical security industry. Cyber security is often a neglected area. Here, the physical security industry – including all levels of the security camera supply chain, must take responsibility.

"A surveillance system can consist of hundreds of cameras and if one camera fails in security, you may lose the whole surveillance solution", says IT security expert Mikael Simovits, who gives his view on data security and video surveillance in this issue. He is anything but impressed about the data protection in today's IP cameras. He considers them very easy to hack and calls for a much higher level of security.

Cyber security, as well as the development of IoT – are something that will characterise many of this year's upcoming editions of Detektor. There is a great need for information, which we intend to fill, focusing in on security applications.

It seems 2017 is already proving to be an interesting year for the security industry.

- 3 **Publisher's comment.** IoT creates huge security challenges.
- 5 **Security technology market.** Video door bells smooth the way to CCTV acceptance.
- 8 **Business News.** Acquisition fever hits security industry.
- 11 **Focus on.** Cyber security & IP video surveillance.
- 18 **Security technology industry outlook.** Asian manufacturers talk about the market and its trends.
- 22 **The Interview.** Mahesh Saptharishi, CTO, Avigilon.
- 24 **Product News.** Arecont Vision expands Microdome range.
- 29 **Security Buyers Guide.** The directory of important suppliers of security products & services.
- 30 **Security Events Calendar.** The international overview of scheduled security shows.



Focus on: Cyber security & IP video surveillance

Page 11



Mahesh Saptharishi: "Licensing does not always begin smoothly"

Page 22



Asian manufacturers talk about the market trends

Page 18



Arecont Vision expands Microdome range

Page 24

REVIEW



Intersec in Dubai successfully kicked off 2017

With more than 1,300 exhibitors and some 33,501 visitors from 129 countries, Intersec in Dubai (22–24 January) was a 2017 great kick-off for the global security industry.

Page 27

Wireless video surveillance market sees growth ahead

London, UK

Technavio, a tech-focused market research firm, has published a new report on the global Wireless Video Surveillance market, which is expected to grow at a CAGR of close to 21% during the forecast period 2017-2021.

The market researchers have segmented the wireless video surveillance or WVS market into three key geographical regions: The Americas accounting for 43.24% of the market in 2016, the APAC countries 33.18% and the EMEA regions 23.58%.

Analysts found that in the

Americas, the US government has augmented its budget for the deployment of defence and security systems in the country. The US Federal Energy Regulatory Commission is adopting certain standards for the safety of critical infrastructure in the Americas. Therefore, there is increased adoption of the security cameras among commercial, residential, utilities, and government sectors in the Americas to protect people and property.

The WVS market in the EMEA is witnessing growth in

Europe due to the imposition of government regulations such as the European Data Protection Directive. The demand for the security systems among commercial and government sectors is increasing in Europe because of increased security concerns. Besides this, the oil and gas industry has the highest demand for surveillance cameras due to the increasing number of thefts in the industry.

The governments in APAC countries, due to security concerns, have made the implementa-

tion of CCTV cameras mandatory in public places. Moreover, the emergence of retail chains in India will drive the market for better security systems. APAC is an emerging region for global trading and tourist activities, and this further propels the need for advanced wireless cameras in the region. Several factors, such as increased government spending, growing awareness, and an increase in private sector spending, are accelerating the demand for WVS systems in the APAC countries.



Video door bells smooth the way to CCTV acceptance

A new study from IHS Markit suggests there is an increasing demand for integrating video doorbells with home alarm systems. For example, if the two are combined with an electronic lock, this would allow a consumer to grant someone access to his or her home safely from anywhere with a Wifi connection.

London, UK

As the popularity of video doorbells increases, owners are likely to become more comfortable with video cameras in their homes. For many homeowners, a video doorbell is their first experience with an IP camera. Installing it, setting up the app and then later using it to view something remotely all help to build consumers' familiarity with network video cameras. This raises consumer awareness and lowers privacy concerns, two of the main barriers responsible for slowing adoption of video in the home in the past.

A rise in the popularity of video integration with intruder alarm systems potentially creates new product development and marketing opportunities. It enables integrators and installers to upsell cameras as part of their standard offering and gives manufacturers a unique selling point to market.

Cloud storage services offer another opportunity for revenue

generation, which professional monitoring companies could try to integrate with their existing service offerings.

IHS analysts predict that increased consumer preference for video cameras could result in less spending on traditional intrusion equipment like PIR detectors, magnetic contacts or break glass sensors. In the short-term, it seems that video cameras would be adopted as an add-on to the existing system, strengthening the abilities of the traditional equipment and the system overall. However, as video analytics continue to improve, it remains to be seen how this trend could affect demand.

In 2015, 1.1 million (21 percent of) residential connected professional monitoring service contracts included some form of video monitoring service in the American region. This proportion is forecast to increase, particularly with the emergence of facial and

object recognition, promising to further enhance the future functionality of video verification. This functionality offers potential savings both to consumers and providers of monitoring services through lowering false alarm rates.

Professionally installed alarm solution providers such as Vivint, Comcast and Alarm.com are adding video doorbells to their offerings. Currently, however, the typical profile for a buyer of a video doorbell (young and tech-savvy) is also closer to that of one who would purchase a DIY alarm system rather than a professionally installed system. It is therefore likely that in the short-term, the DIY market will feel these proposed effects first if they are to become apparent.

With a global market size of \$78 million in 2015, video doorbells are only just beginning to gain traction among residential consumers. Their adoption is still

largely limited to the US and despite many new entrants; market supply is currently concentrated with a few larger suppliers such as Ring. As competition increases, demand will accelerate and prices will fall. However, the primary barrier today remains price. A normal, non-video-capable doorbell costs less than \$20, while video doorbell costs often exceed \$150. Raising consumer awareness of the benefits will be key to increasing the adoption rate.

IHS Markit forecasts that the global market for video doorbells will experience a 28 percent CAGR over the next five years. As the market continues its rapid ascension, partnering with video doorbell providers could prove lucrative for home alarm manufacturers and service providers.

Another option would be to work with third-party integration software providers like IFTTT and Stringify to build a clean, easy-to-use integrated solution.



See more of Dahua's Penta-brid Video Recorder – XVR



The Dahua XVR, a true Penta-brid video recorder, is a new development based on an industry leading open structure and compatible with multiple access technologies. It is the perfect solution to upgrade existing video surveillance systems.

The XVR supports 4 mainstream analogue camera types on the market, not only traditional CVBS (analogue) cameras, but also HDCVI, AHD and TVI, as well as IP cameras. Moreover, XVR recognises the signal formats from cameras automatically, including both Dahua cameras and third party cameras. True plug & play means operation is more user friendly and convenient.

Compatibility

Support for POC (power over coaxial) helps the XVR to simplify the users' network cable construction, eases the wiring of power cable and maximizes user benefits. In addition, users can switch video channel type from the OSD menu or via the HDCVI UTC controller.

Further, the Dahua VMS,

when partnered with Geutebrück, GeoVision, Heitel, etc., serves as the user interface to command and control Video Surveillance Systems, which consist of imagers, recording devices, extended storage, intelligent analytics, user display and control interfaces (such as monitors, video walls & keyboards).

High performance

The Dahua XVR brings a newly designed chassis with low-noise fan and hive structure heat dissipation. Smart H.264+ Codec is applied to the XVR to save up to 50% bandwidth and storage. The upgrade of power electronics components and interface protection enhances the XVR's quality in terms of anti-cross talk, anti-ESD and anti-surge.

Intelligent functions

Equipped with the intelligent functions such as IVS and face detection, the XVR records and analyses events such as tripwire, intrusion and disappearance from the image. In addition, these intelligent functions meet with

the application requirements of high efficiency and intelligence. The XVR combines the simplicity of analogue systems with rich camera functionality to achieve simple installation and easy operation.

Designed to be fully intelligent, the Dahua XVR is able to provide end users with the simplicity of an analogue system, with flexibility and a wide selection of cameras. Significant savings on total system cost is achieved by ease of installation and reuse of existing coaxial cabling. Therefore, it is ideal for a wide range of applications such as public safety, retail stores, transportation, stadiums, recreation centres, home surveillance and education, etc.

Models:

XVR41/4200 Series 720P

- Full channels 720P real-time recording
- HDCVI/AHD/TVI/CVBS self-adaptive plug and play
- 1/2/2 extra IP channels
- Powerful network performance
- Up to 6TB capacity for each SATA

XVR51/5200 Series 1080P-Lite

- Full channels 1080P non-real-time/720P real-time recording
- HDCVI/AHD/TVI/CVBS self-adaptive plug and play
- 2/4/8 extra IP channels
- Powerful network performance
- IVS, Face detection, Smart H.264+

XVR71/7200 Series 1080P

- Full channels 1080P real-time recording
- HDCVI/AHD/TVI/CVBS self-adaptive plug and play
- 2/4/8 extra IP channels
- Powerful network performance
- IVS, Face detection, Smart H.264+

About Dahua Technology

Dahua Technology Co., Ltd. is a world-leading manufacturer of professional security and surveillance equipment. Over the past 15 years, Dahua Technology has invested heavily into the Research and Development of innovative solutions that improve public safety. Dahua's solutions are designed to be scalable and modular to provide flexible configuration options. The company is ranked 4th in the Security 50 rankings from A&S International for 2016. Dahua enjoys the world's second largest market share according to the IHS 2016 report. Visit www.dahuasecurity.com to learn more.

XVR

— Industry's leading full - compatible platform

Highlights

- Penta-brid: HDCVI/AHD/TVI/IP/CVBS
- User-friendly GUI, plug & play
- Optimized transmission distance & image performance
- Enhanced quality: component & interface protection, anti - crosstalk



Available products:
—XVR 7000/5000/4000 Series



Acquisition fever hits security industry

The consolidation of the security industry has continued over recent years. In this issue of *Detektor* we have compiled the details of several acquisitions, made during the last 3 months (December 2016–February 2017), as a simple overview of the acquisition activity in the security industry.

G4S sells off British and Israeli business

G4S has completed the sale of G4S Utility Services, its UK multi-utility metering services business, to First Reserve, the majority shareholder in Morrison Utility Services Group, for £52 million paid in cash. G4S Utility Services comprises G4S Utility and Outsourcing Services (UK) Limited; G4S Assessment Services (UK) Limited; G4S Locks & Alarms (UK) Limited.

G4S Israel has been sold to FIMI Opportunity Funds (FIMI) for an estimated net consideration of NIS425m (approximately £88m). FIMI is a premier Israeli private equity fund. G4S will retain a presence in Israel through ownership and continued investment in the flagship national police training centre Policity in partnership with FIMI and Shikun & Binui, a major Israeli infrastructure and real estate group.

In the year to 2015, G4S Israel generated profit before taxation of around £8m and had estimated gross assets of around £56m.

Allegion acquires Republic Doors & Frames

Republic manufactures hollow metal doors and frames, complementing Allegion's Steelcraft brand and core business in the Americas region. Republic generated approximately \$20 million in net sales for 2015. Additionally, Republic's footprint includes five regional service centres in Atlanta, Dallas, Orlando, Houston and Seattle that provide for faster servicing of local customers in these key markets. Republic's president, Mike Taylor, will remain in a consulting capacity and focus on a smooth integration.

Veracity acquires I-Comply

I-Comply is a UK software provider of integrated command and control security solutions. The agreement includes all operational staff, software, intellectual property, on-going business and also I-Comply's sales and support subsidiary in India. Veracity will maintain I-Comply as a separate business and will immediately expand its operations including an imminent move to larger premises near Leeds.

The modular software solution supports a range of access control, CCTV, fire, alarm and other security equipment vendors, including Veracity, Bosch, Honeywell, Paxton, Axis, Hanwha Techwin and Milestone. Michael Gallagher will remain in charge of I-Comply business development and will also be responsible for running sales, support and operations for the business.

EC clears Smiths acquisition of Morpho

Further to the announcement last April that Safran had reached an agreement to sell Morpho Detection, to Smiths Group plc for an enterprise value of \$710 million, Smiths has now confirmed that the European Commission has finally given clearance for the proposed acquisition which it was originally anticipated would be closed during the first quarter of 2017.

In order to secure approval in Phase I of the EU merger review process, Smiths Group proposed the divestment of Morpho Detection's explosive trace detection business. This divestment is conditional on the successful closing of Smiths Group's acquisition of Morpho Detection and on the European Commission's approval of the purchaser of the Trace business as a suitable purchaser. Completion of the acquisition of Morpho Detection by Smiths Group remains conditional upon

approval from the relevant authorities in the United States and certain other territories, among other conditions.

ALSO acquires Internet Smartsec

The IT product distributor Also has acquired Internet Smartsec. A Finnish importer and value-added distributor of security and network products. Its portfolio encompasses secure e-commerce solutions, VPN routers, user identification equipment, smart cards, encryption technology, IDS and filtering products, as well as various firewall devices. The company also provides consultation and training in data security and data networks. In 2016, Internet Smartsec's net sales reached €4.5 million, a 61 per cent increase compared to the previous year. The company has eleven employees.

Assa Abloy acquires in Poland and the US

Southeastern Dock & Door, with 70 employees, is an industrial and commercial door and docking solutions distributor headquartered in South Carolina, now acquired by Assa Abloy. Sales for 2017 are expected to reach USD 19 million.

Assa Abloy has also acquired LOB in Poland, a producer of locks, cylinders and padlocks. LOB is headquartered in Leszno, Poland and has some 440 employees. Sales for 2017 are expected to reach some PLN 96 million. The transaction is conditional on regulatory approval and is expected to close during the second quarter of 2017. bloy and Head of the EMEA division.

Pinkerton merges with Secredo

The Swedish risk and security consulting service provider, Secredo, has been acquired by Pinkerton, the global American risk management consulting company. However, both companies are fully owned subsidiaries of Securitas, so the deal is to be considered more as a merger between two sister companies.

Jack Zahran, President at Pinkerton.



GJD acquires Embsec technology



Mark Tibbenham, GJD (right) and Erik Lindstein, Embsec shake hands.

GJD has signed an agreement to acquire from Embsec AB, a Swedish R&D house, all of their internet protocol and laser technology plus all related intellectual property rights. The IP technology will be integrated into GJD's D-Tect detector and Clarius LED illuminator product ranges to provide automated and digitally connectable security solutions.

The purchase of Embsec's IP products, software and technology allows GJD to offer a fully integrated IP solution, with all products being manufactured in-house at GJD's head office in Heywood, Greater Manchester.

"This strategic acquisition will enable the company to substantially develop and

grow in terms of technology innovation. There is a high demand for IP security products to complement the rise in smart home and building management systems”, commented Mark Tibbenham, Managing Director of GJD when the acquisition was announced.

Flir acquires Prox Dynamics

Flir pays 134 million dollars for Prox Dynamics AS, a developer and manufacturer of nano-class unmanned aerial systems (UAS) for military and paramilitary intelligence, surveillance, and reconnaissance applications. Based in Oslo, Norway and founded in 2007, Prox Dynamics develops, manufactures, and distributes aerial sensors that are small, light, and covert surveillance systems.

Prox Dynamics’ Personal Reconnaissance System (PRS) features their Black Hornet aerial sensor and a hand controller, a system that is pocket sized and hand-launched by a soldier in the field, enabling a significant advantage in situational awareness and mission planning. The Black Hornet aerial sensor utilises Flir’s Lepton micro thermal camera, visible spectrum cameras, advanced low-power rotor technology, and proprietary software for flight control, stabilisation, and communications. The business will become Flir’s Unmanned Aerial Systems (UAS) line of business operating within the surveillance segment.

ACRE acquires Comnet

ACRE, LLC, is the holding company that owns Vanderbilt Industries, Mercury Security and recently acquired ACT in Ireland. Comnet offers a line of fibre optic, copper, and wireless video and data transmission equipment that is designed to meet the needs of security and surveil-

lance in the intelligent transportation systems, utility and industrial markets.

“In line with our mission, the Comnet acquisition, with their extensive offerings in the communication and data transmission technologies, continues to round out the product portfolio provided by the ACRE family of companies”, stated ACRE CEO Joe Grillo.



Joe Grillo, ACRE, CEO.

Genua acquires Protect

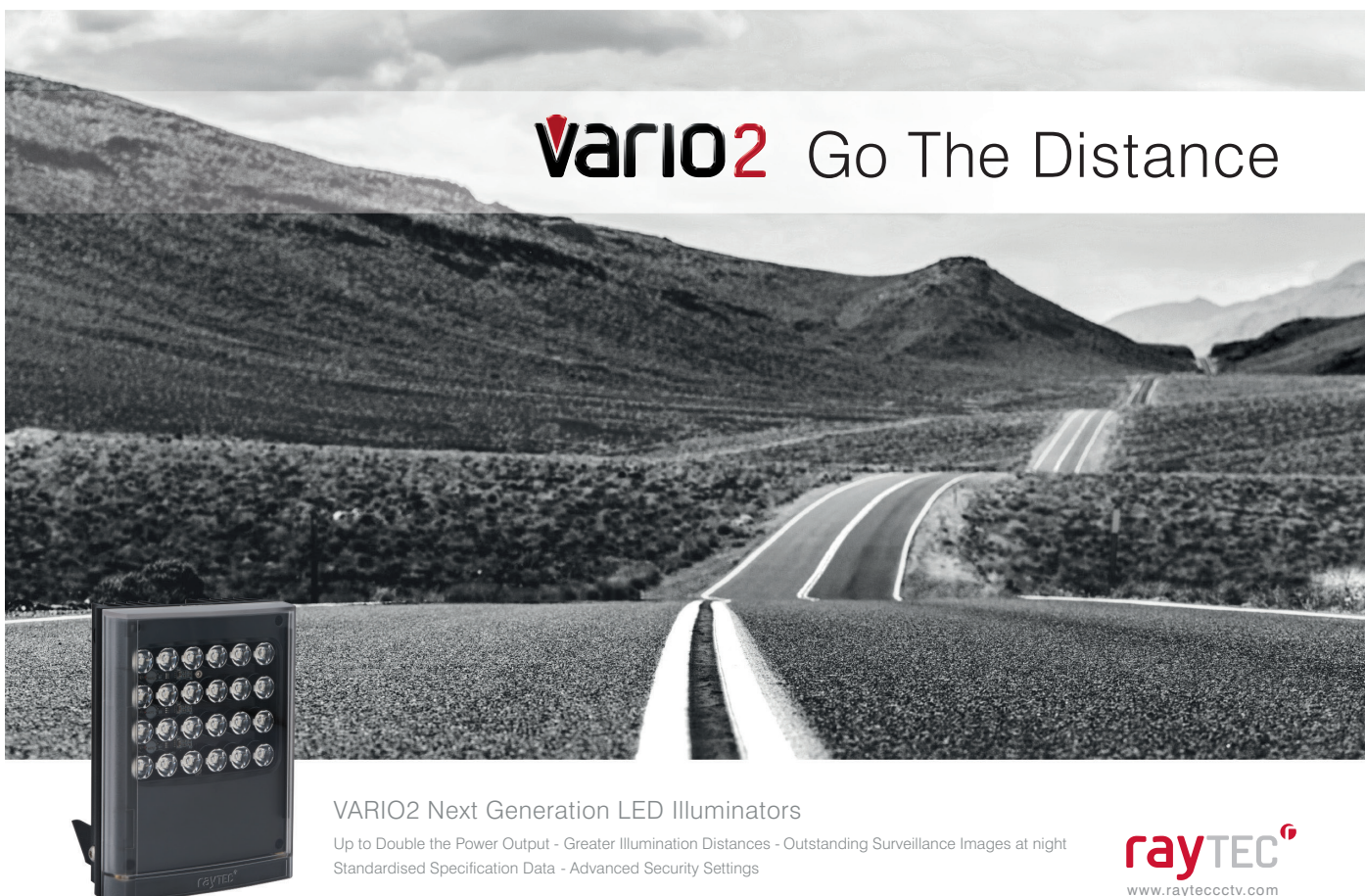
The Danish investment company Genua A / S has just taken over Protect A / S, the world’s largest manufacturer of fog cannons for protection of businesses and homes.. 90 percent of Protect’s production is exported to more than 50 countries.

HID acquires Bluvision

Bluvision is a complete IoT ecosystem provider, offering real-time location system technology, presence and proximity-based location capabilities and condition monitoring solutions as well as cloud infrastructure, gateways, beacons and software as a service (SaaS).

The Bluvision team will report to Marc Biemann, VP & MD of the Identification Technologies business within HID Global. The addition of Bluvision’s products expands HID Global’s “component continuum” from high-end, passive RFID components (LF/HF/UHF) to active BLE.

Bluvision will continue to maintain its operations in Fort Lauderdale, Florida.



VARIO2 Go The Distance

VARIO2 Next Generation LED Illuminators

Up to Double the Power Output - Greater Illumination Distances - Outstanding Surveillance Images at night

Standardised Specification Data - Advanced Security Settings

rayTEC[®]

www.raytecctv.com

Raytec lighting transforms security for national bank

Ashington, Northumberland (UK) and Bucharest, Romania

As part of a large upgrade to an IP surveillance system, the National Bank of Romania, has deployed, both infrared and white-light LED lighting solutions from Raytec, at its multi-site locations to deliver a huge improvement to surveillance image quality at night, and to create a safer, more effective working environment.

Security at the bank is strict, especially at the headquarters. The perimeter and access corridors are monitored by the bank's camera system 24/7, but previously they were much more vulnerable during the hours of darkness.

The previous surveillance system, using analogue cameras, had no professional lighting – making use of street lighting where possible. The images were dark and grainy with an uneven light coverage making facial recognition totally impossible. It was also very difficult to raise accurate alarms based on the poor information in the images.

Leading and managing the upgrade project was distributor Lantec, who urged the move towards the Raytec LED surveillance lighting and Mobotix MP IP cameras. "We have worked with Raytec for over ten years", comments Radu

Cristea, Lantec General Manager, "and we knew that their LED lighting would be the best solution to help the new IP cameras deliver a very high level of detail at night. Having never used video surveillance lighting before, the customer was also very attracted to the fact that the Raytec illuminators offered a ten year life and needed zero maintenance".

Working together, Lantec and system integrator Rasirom specified Raytec's Raymax infrared illuminators for use around the perimeter and both internal and external access ways. The final night-time images are a vast improvement. Every image is evenly illuminated and shows exceptional clarity and detail - with no bright or dark spots. The detailed images are also helping the cameras' inbuilt analytics to detect and analyse incidents more

accurately, resulting in fewer false alarms.

"The bank is very satisfied with the night time images and reliability of the information generated by the infrared lighting" confirms Radu. "They are especially pleased that they can zoom in on any subject anywhere in the image in great detail. It's also an added benefit that the IR is invisible and does not cause additional light pollution".

Lantec also recognised that they could solve some of the bank's additional security needs that extended beyond surveillance, by introducing some of Raytec's specialist visible white-light solutions.

In particular, some of the branch cash processing centres and under vehicle check areas suffered from poor visibility as a result of little natural lighting. This made operations and inspection very difficult. To address this weakness, Raytec's ceiling mounted Urban Bay lighting was installed in the cashing areas, along with simple low-voltage Vario lighting



The detailed images are helping the cameras' inbuilt analytics to detect and analyse incidents more accurately.

mounted at ground level in the vehicle inspection bays. The result is a highly targeted illumination delivering a brighter, more natural lighting environment which makes it easier and quicker to perform tasks more accurately.

David Lambert, Raytec MD (joint) comments: "We're delighted that with the help of our long-term partner, Lantec, we've been able to help the bank to solve so many different security issues with LED lighting. Whilst good camera lighting is essential for night-time surveillance, lighting for people is just as important for ensuring the best safety, productivity and operational effectiveness at all times."

Birmingham Uni stays safe with wireless access control

Birmingham, West Midlands (UK)



The Chamberlain student accommodation at Edgbaston, Birmingham University, secures access with Aperio.

When the University of Birmingham opened its newest accommodation block, it required an access control system to meet the unique needs of a student population. Now, over 1400 students housed

at Edgbaston's Vale Village site are protected with Aperio wireless access control.

University halls of residence have a complex set of access control requirements. Accommodation blocks often house large numbers of students, whose population is in a constant state of change. Physical keys can be frequently lost, compromising site security and causing time and money to be wasted every time mechanical locks must be changed. Electronic access control with real-time monitoring enables security managers to stay in control of the site.

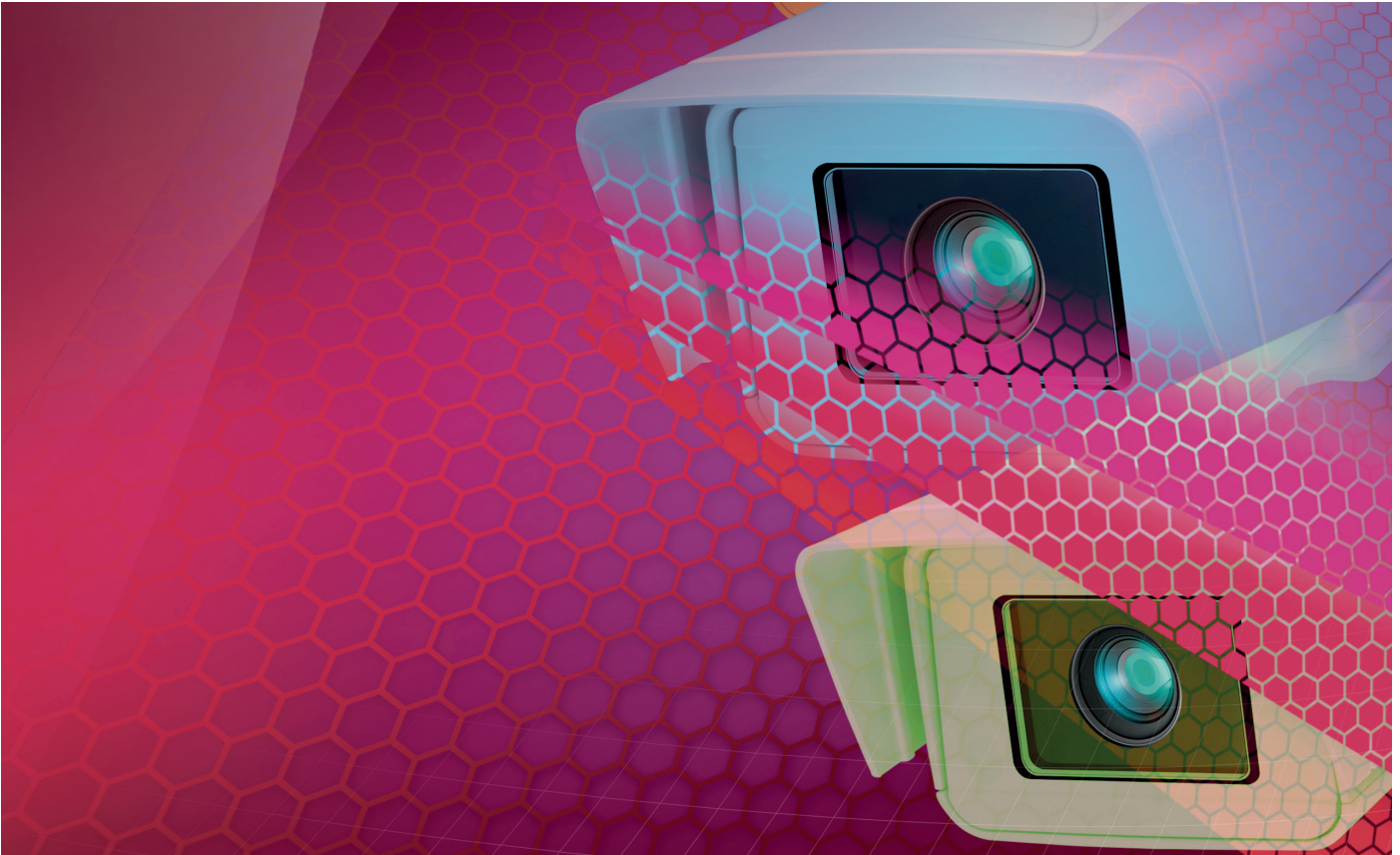
Student rooms and entrance doors at both Chamberlain and Mason halls have been fitted with Aperio wireless devices. All door locks are fully integrated with Gallagher Command Centre software. Because Aperio components are built using open standards, integration with Gallagher's security system is seamless, and provides security staff with a single point of control over the site.

A mix of online escutcheons and cylinders, for both Euro and Scandinavian profile doors, have been installed. Installation was wire-free, and locks are powered by standard lithium-ion batteries,

which guarantees the university a low-cost security solution. It also removes the need for mechanical keys.

Birmingham joins many other Universities who have chosen Aperio to protect their students while improving the overall student experience.

"Our extensive experience within the education sector has enabled us to provide the University of Birmingham with a seamless integrated solution," says David Hodgkiss, National Sales Manager at Assa Abloy access control. "The university already has plans to roll Aperio out to other residences."



Cyber security has become an increasing issue for the video surveillance industry. Now, Hikvision – the world's biggest manufacturer of video surveillance equipment – is being accused of lacking of security.

Hikvision's products accused of being a security risk

Products from Hikvision – the world's biggest manufacturer of video surveillance equipment – are being accused of lacking in security. Various media sources – mainly the website IPVM.com and the British newspaper The Times – have claimed that the Chinese government may have access to footage from Hikvision cameras. Furthermore, the market leading VMS company Genetec has introduced restrictions against Hikvision products and this has increased the air of mistrust.

By Henrik Söderlund /Lennart Alexandrie

In 2014, hacking attacks were reported on Hikvision products. After that, Hikvision established a security response centre in order to manage security-related vulnerabilities. In 2015, a new structure was devised meaning that anyone setting up a Hikvision device now has to use more complicated software when launching the product.

Back door

In 2016, new accusations were directed towards Hikvision: this time allegations that Hikvision may have built-in, so called, back doors into their devices which

would grant the Chinese government access to cameras, and thus to the networks and the sites where they are installed. The high-profile physical security blogger John Honowich and his website www.ipvm.com has been the main driver behind this criticism and still is.

Controversial article

Hikvision is publicly listed and the fact that its biggest shareholder is a Chinese state owned company is the very source of concern. The British newspaper The Times published an article last autumn

” The high-profile IP-video surveillance blogger John Honowich and his website www.ipvm.com has been the main driver behind this criticism and still is.

where unnamed former officials and security officers from the British intelligence service MI6 claimed that Hikvisions cameras could be hacked by the Chinese government.

Genetec disclaims responsibility

Now, the Canadian VMS-company, Genetec, has started requiring new customers to pay for a special

license if connecting Hikvision products to the Genetec VMS platform. And furthermore, existing customers need to sign a waiver in order to release Genetec from any responsibility if their network or other networks are hacked via a Hikvision device.

In this issue of Detektor, both Hikvision and Genetec will give their views on this controversial matter.

Genetec has recently started requiring their customers to sign a waiver so that Genetec cannot be held responsible if their network or networks of their neighbours are hacked via Hikvision or Huawei devices.

"Governments have told us they are extremely concerned about the origins of these products", says Genetec CEO Pierre Racz.

By Henrik Söderlund



"Governments have told us they are extremely concerned about the origins of these products", says Genetec CEO Pierre Racz.

Pierre Racz, CEO of Genetec, about Hikvision: **"Governments are extremely concerned"**

Genetec will continue to support devices from Huawei and Hikvision, but new customers using these devices will need to sign the waiver and pay a special 250 USD connection license in addition to standard license fees.

As a background to this decision, a report from the Commission on the Theft of American Intellectual Property from 2013, which states that China is the world's largest source of IP theft and the annual losses for the Amer-

ican economy because of international IP theft is estimated to over 300 billion USD – comparable to the annual level of US exports to Asia. Also, the New York Times has revealed a secret backdoor in some Huawei cell phones in the US. A software transmitted the full contents of text messages, contact lists, call logs, location information and other data to a Chinese server every 72 hours. This has worried Genetec and its customers. However, there is no such evidence regarding Hikvision.

"Certainly the hacking of the US election brought it to the forefront so everyone knows the danger and the threat cyber criminals can pose to our freedom and democracy."

About half of Hikvision is owned by a Chinese state-owned enterprise and this is a problem according to Pierre Racz. "Government ownership of a company is a critical factor in individual risk assessments made by the

end-user", stated Pierre Racz. "Such risk assessments are made by the end-user based on the end-users' circumstances."

He also adds that Genetec sheds light on obfuscated origins of equipment – so customers can make an enlightened and informed risk assessment, depending on their circumstances.

According to www.ipvm.com, the Chinese government gave Hikvision a 6 billion-dollar subsidy and this has raised concern.

"The question you have to pose is: clearly its motivation is not profit, so what is it then?" says Pierre Racz.

How difficult was this waiver decision?

"It was hard but we have this ethos where we would rather lose the sale than the relationship."

So it is not a commercial consideration?

"No. Since we are aware of the origin of these devices, our customers told us it would be hypocritical not to disclose it publicly."

Are Hikvision products trustworthy?

"It is in the eye of the beholder. If you are a Chinese government

organisation, the answer is yes. If you are an American governmental organisation, the answer is definitely no. If the risk factor is between 0 and 1, I can guarantee it is not 0. It is somewhere in between 0 and 1. A simple, hypothetical risk assessment question could be: if a Western power were to go to war with China, would you apply a security update patch to your Hikvision cameras?"

Do you think Hikvision has put backdoors in their cameras?

"Hikvision has publicly made it known that they have a password recovery mechanism for their hardware. And by default, the cameras phone home. But, in some versions of the software, an end-user can opt out."

What about Western companies, can they not be a security risk too?

"Yes, but the difference between a democratic and an authoritarian state is that we agree there are limits to the power of government. If a western government tells a security camera manufacturer to put a backdoor in their cameras, the company can say no and take it to court. Hikvision explicitly says in its manuals, they cannot be sued if their devices are used to attack your network. And even if that was not put in the manual, you cannot sue the Chinese government."

What about Dahua, the other big Chinese manufacturer of video surveillance equipment?

"Dahua is a private company and you can sue them and they are motivated by the risk of losing the trust of their customer base. The risk is not zero, but less than with a company that is owned by the government and has been given a 6-billion-dollar subsidy."

How concerned is the market about Hikvision and Huawei products?

"The concern is directly proportional to the sophistication of the organisation. Large organisations that are more sophisticated are more concerned. Governments have told us they are extremely concerned."

You are the only manufacturer that has taken this action. What is your message to other VMS manufacturers?

"They should rethink. I would like to remind them they are not only responsible to their shareholders, but also to their employees and most importantly to their customers and the countries that support them with infrastructure."

Why do you think data security has become a hot topic of conversation in the security industry?

"There are a couple of reasons for why this is becoming public interest; certainly the hacking of the US election brought it to the forefront so everyone knows the danger and the threat cyber criminals can pose to our freedom and democracy."

Keen Yao, Hikvision, on the accusations:

"It's time to move away from outdated Cold War stereotypes"

Keen Yao, VP of Hikvision's International Business Centre, stresses that the negative news about the company is based on biased information and Genetec's actions are politically motivated.

"Of course, Hikvision has never intentionally put a backdoor into firmware or software, and it never will", he says.

By Lennart Alexandrie

Keen Yao has given an exclusive interview to Detektor due to the recent accusations and the critical articles in the press.

What is your reaction to the accusations that Hikvision cameras can be hacked by the Chinese government?

"It's important to consider the source and motivation of anyone who would make this kind of baseless allegation. These are not people who care about security and public safety. They care about their personal financial and political agendas. They certainly do not display an understanding of physical security technology. It is time to move away from outdated Cold War stereotypes and concentrate on solving the serious problems our global society faces today."

Is it possible to put a "backdoor" in a Hikvision or other manufacturer's device?

"Any manufacturer, including those who develop or support software, has the technical ability to put a "backdoor" into firmware. Of course, Hikvision has never intentionally put a backdoor into firmware or software, and it never will."

Genetec has decided to make their customers sign a waiver so as not to be able to hold Genetec responsible if their network or their neighbours' networks are attacked via a Hikvision device. Genetec is also worried about Chinese government control over Hikvision. Can you comment on that?

"We believe this is an unfortunate move by Genetec, which purports to be Onvif-compliant and an "open" platform. It is also unfortunate for integrators and end-users. Genetec has not produced any evidence that this decision is based on product technology. We believe it is politically motivated and designed to negatively influence perceptions about Hikvision's approach to cyber security. We have been in touch with our partners and customers about Genetec's decision and are available to answer any questions, and to discuss options."

Is Hikvision a division of the Chinese government? What is the ownership structure of Hikvision?

"Hikvision is a commercial entity; it is not a division of the Chinese government.

The ownership structure of Hikvision, like many global, publicly traded companies, is complex, and includes a diverse set of private and public shareholders. As of June 30, 2016, 41.88 percent of Hikvision's shares are jointly owned by China Electronics Technology HIK Group Co., Ltd. (CETHIK) and CETC No. 52 Research Institute, both are part of CETC, a state-owned enterprise; 18.28 percent is privately owned by Mr. Kung Hung Ka (a Hong Kong permanent resident); 8.48 percent is owned by the company's founders and executives; and the remaining 31.36 percent is owned by A-shares investors; International institutional investors such as UBS AG and JP Morgan are

among Hikvision's top 10 shareholders.

The Shenzhen-Hong Kong Stock Connect, which launched at the end of 2016 is enabling more foreign investors to buy Hikvi-

"Genetec has not produced any evidence."

sion stock, which will make the shareholder structure even more diversified."

Who is in charge of managing Hikvision?

"Hikvision's management team, led by CEO, Mr. Hu Yangzhong, is responsible for the daily management and business operations of the global company, its long-term business plan and implementation of that plan."

What did you think of the Times of London story in September, focusing on the possibility that the Chinese government has access to Hikvision cameras?

"Unfortunately, this particular Times of London story contained errors and omissions. Much of the reporting – and speculative quotes – were based on biased information supplied by an American blogger site that engages in name-calling and ridicule, publishes an inordinate amount of commentary from anonymous sources, and otherwise does not observe standard journalistic practices."

How do you handle this negative news?

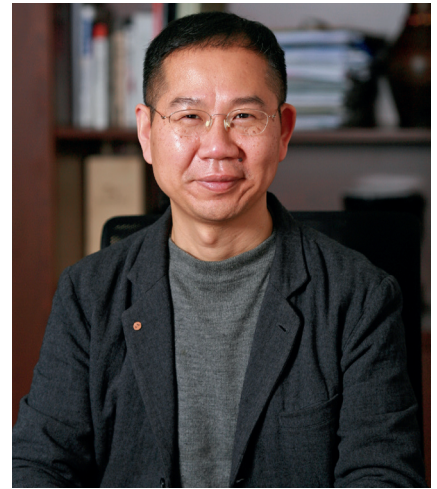
"As the No. 1 video surveillance

provider, we expect occasional negative, sensationalist or biased reports. Of course, we try to answer any questions that may arise from this kind of article from legitimate news outlets such as

yours, but mainly we are focused on running our business. We have created thousands of good jobs around the world in the regions where we do business and we have made significant, positive contributions to the communities where we do business. Helping security professionals combat terrorism and criminal behaviour is why we are in this business.

Is cyber security a major concern for Hikvision?

"Cyber security is a major concern for all physical security manufacturers. Hikvision has established a sustainable and reliable cyber security assurance system that encompasses the company's policies, organisational and operational procedures, technology and regulations. For example, we have a special task force at Hikvision headquarters, the Network and Information Security Lab, which sets Hikvision's security standards, performs security evaluations and testing, and responds to security issues. We continue to take steps to improve our products, including having them tested by leading third-party cybersecurity firms to minimize any potential security risks."



Keen Yao, VP of Hikvision's International Business Centre.

Michael Simovits, IT security expert:

“Many manufacturers skip the encryption”

Security cameras are easy to hack because encryption is not a priority, software updates are lagging behind and the cameras are connected to general IT networks, argues IT security expert Michael Simovits.

“Some cameras are completely unprotected”, he says.

By Henrik Söderlund

Mikael Simovits is the founder of the Stockholm based Simovits Consulting, specialising in information and IT security services. He has taught cryptography at Chalmers University of Technology and has been named one of the best security experts in Sweden. Since 2004–2005, he has worked with high-end security solutions where cameras have been included.

“The camera processors are not always so powerful and encryption takes a lot of energy from image processing. If you are using high resolution and want to encrypt, the product will become more expensive to manufacture. Therefore, many manufacturers skip the encryption”, he says.

“If someone steals your camera, you have to keep in mind that the thief might carry out an attack later.”

How important is data security for security cameras?

“It depends what they are used for. If it is just about monitoring a construction site in order to show how fast things are being built, it is not the most important feature, even though it would be embarrassing if anyone in the world could go online and look at the hacked cameras. However, if you add intelligence, for example by allowing the cameras to react to motion and connecting them to an alarm system, then the entire infrastructure should be secured; it is not enough only securing the cameras because threats are directed towards the whole surveillance system.”

How do you secure the whole infrastructure?

“You must implement a concept that covers everything from cameras to the network equipment, servers and firewalls and have a clear policy on which device should

initiate which communication. A surveillance system can consist of hundreds of cameras and if one camera fails in security, you may lose the whole surveillance solution. A camera should not initiate contact with a server and transfer video; instead the server should initiate communication with the camera and download video. However, when we scrutinise high-end security solutions, they cannot always keep up with all the security requirements because it simply prevents the function of the cameras. If you have 300 cameras, it is not always easy to constantly update and be on watch, it requires a lot of resources.”

How often do security cameras get hacked?

“It is very common and there are a number of websites that have links to hacked cameras. Usually it is not cameras in high-end security applications, but for example cameras on highways, in cities or cameras in people’s private homes.”

How secure are security cameras?

“This might sound a bit harsh, but the cameras have the same kind of security issues as IoT devices. They have a small, usually Linux-based operating system which is customised and – just as IoT devices – tend to fail in the way that there is no good solution for patching and updating the cameras in a simple and efficient way. So, I equate security cameras with IoT devices.”

... which you can buy off the shelf in retail?

“Again, it might sound a bit harsh, but in general, yes.”

How can the update problem be solved?

“You must be online in order to get the patches quickly into the cameras but if you do so, another security issue that must be handled arises. Some of our customers have solved this by sending out security watchmen as soon as a camera has been stolen, if the image goes black or becomes blurry or if there are any other indications of tampering. If someone steals your camera, you have to keep in mind that the thief might carry out an attack later. Often, all cameras in a setup are configured to have the same encryption key and very conveniently, the same password. So if it happens, you directly have to change all the encryption keys.”

What can happen if someone hacks into the system?

“The attacker could disable the entire system, freeze the image, or turn off alarms. If you get in, you can do anything and it is not certain that anyone will even notice that there has been an attack.”

What responsibilities should be put upon the camera manufacturers?

“They may have to change their threat scenarios when designing their cameras, because security systems were previously isolated islands and were not connected to anything else. Today, I see more examples of security networks being connected to the general IT network, and even if there is a firewall between them, that changes the whole foundation of security. The isolation of networks has also led to software updates lagging behind.”

Why has this issue not been discussed earlier?

“Customers see, for example, the benefits of being able to watch video footage directly on a smart phone when there is an alarm, and



Mikael Simovits is the founder of the Stockholm based Simovits Consulting.

therefore they have to be connected to the internet. This means that security networks are sewn together with the general networks and the internet, and that, consequently, forces security companies to market themselves in a completely new way when it comes to IT security.”

If an end customer wants to be able to view live video on a smart phone, what is your solution?

“Do not use the existing network in order to send the video without first building a separate network with an internet connection of its own. In this way, the vulnerability area will decrease: if the mail server is hacked, the video surveillance system will not be affected. Ideally, video should only be able to be seen from a dedicated device and therefore, encryption keys have to be installed in that device and a VPN tunnel must be built between the customer’s network and the device so username and password will not be enough in order to get connected.”

Has the end customer’s awareness of IT security increased?

“Well, I think they do not have a choice but to follow and secure. IP cameras are here to stay, and the camera’s level of security must be adapted so they can withstand the environment they are in.”

Are they not today?

“No, not really.”

Bosch is one of a few IP camera manufacturers that place emphasis on data security when selling cameras. The reason is that cameras are easy targets for hackers.

“Manufacturers do not want to talk about this before they have a good solution, but I would be very surprised if several manufacturers are not highlighting data security at the upcoming security exhibition ISC West in Las Vegas”, says Anders Karlsson, Bosch Security Systems.

By Henrik Söderlund

Anders Karlsson, Bosch Security Systems:

“Manufacturers do not want to talk about this before they have a good solution”

After several notable distributed denial-of-service (DDoS) attacks with security cameras, the lack of security in cameras has become an increasingly hot topic of conversation.

“The biggest and most common problem today is that the passwords and user management systems are weak, or if the firmware is old and has not been updated and so the products might have open ports. It does not matter how safe your products are if you do not handle these fundamental things correctly”, says Anders Karlsson, Bosch’s Product Marketing Manager in Northern Europe.

He believes that the security of

Now, there are many indications that more importance will be placed on how the cameras can be protected from hacker attacks.

“Those responsible for IT security will not allow manufacturers to bring their security products with their own security solution, and add them to their secured networks without question”, says Anders Karlsson.

Many large surveillance systems are and have been sealed and not connected to the internet, but when the software needs to be updated, they are exposed to risks, for example if the update is put on a USB stick or it is downloaded online.



Anders Karlsson, Bosch’s Product Marketing Manager in Northern Europe.

it can be both about blackmailing and pressures of various kinds”, says Anders Karlsson.

Another risk is that someone installs software or infects cameras with malware in order to shut down the system or manipulate it.

A major problem is that cameras are not being updated. According to Anders Karlsson, most manufacturers have ways to inform the camera, the storage solution or the software that it needs to be updated but often the technician is not used to programming it.

“It is a matter of education. Some technicians become upset because we make their job more difficult: they must educate themselves and keep track of passwords, but on the other hand, those who make demands on system security will become more satisfied. However, for IT technicians, this is not a disadvantage because they will be working more with tools, protocols and services that they are already familiar with.”

IP cameras normally have had many open ports to configure products and universal plug-and-play functionality.

“A year ago, we had lots of open ports, but today they are considered as risks rather than opportunities and they are being closed down. Instead, one refers to secure ports with certificate management and encryption in order to communicate with the product”, says Anders Karlsson.

Another reason for why safety has not been a priority for IP cameras is that the system’s performance will decrease if, for

example, a virus scan is conducted at the same time as video is being recorded.

Anders Karlsson believes that stories about IP cameras being hacked, and the rumour that the Chinese government has access to video footage from for example Hikvision cameras, have had a major impact on the market – no matter whether it is true or not – and not least for the manufacturers.

He says: “We, who claim that our cameras are safer, want to quickly develop the security and those whose cameras are not safe become very eager to change them. More resources are devoted to camera security than before, perhaps this may even result in other performance enhancing features being less prioritised.”

Firewalls and VPN tunnels

In 2016, Bosch began to put emphasis on data security and the company has added security both to software and hardware, and equipped its cameras with a Trusted Platform Module to safely store certificates needed for authentication and encryption. Anders Karlsson says there is also a type of firewall in the system, which studies behaviour: where is the login taking place, is it a known user/unit that has logged in before or is it a new one? Depending on this, the logins are sorted into different categories.

Some manufacturers use a VPN tunnel to protect themselves against DDoS attacks, while some do not protect the data at all.

“A year ago, we had lots of open ports, but today they are considered as risks rather than opportunities and they are being closed down.”

an average IP video surveillance system is mainly based on the username and their chosen password.

“In this industry, we do not have very strict requirements on how to set the username and password. There are still not many systems that require the user to change the original password.”

Instead, many end customers rely on suppliers of infrastructure and IT equipment to handle safety.

Improvement is needed

Since IP cameras broke through into the market, most of the debate has been focused on improved image resolution, ease of use, light sensitivity and intelligent features.

“The security industry has made a journey to a connected world, and the new type of users and installers which originate from the world of IT will set demands. The implementation of penetration tests is becoming much more common”, says Anders Karlsson.

More aware of risks

There are several risks associated with IP cameras. For example, someone might want to hack into a surveillance system in order to watch recorded video or live footage.

“The purpose may be to access critical business information, or to violate an individuals’ privacy,

It is impossible to completely protect oneself against hackers. But you may limit the risk by carrying out a risk analysis and reflect on what is most important to protect.

“To be able to feel secure with your security solution, suppliers and manufacturers must also have expertise and communication strategies for IT security. Unfortunately this is not always the case”, says Jimmy Ek, Nordic Sales Manager, Axis Communications

By Henrik Söderlund

Jimmy Ek, Axis Communications:

How to safeguard the IP camera system

The number of online gadgets is reaching new records by the minute and this increases vulnerability. How can you minimize the risk of data breach in security applications and protect security cameras from hackers?

Jimmy Ek stresses that threats must be handled at a system level, and the responsibility for securing the network with its online devices and services lies with the whole chain, from suppliers to installation engineers, administrators and system users.

Protect what is most important

According to Jimmy Ek, at a basic level, IT security is about risk management, and it is impossible to eliminate all risks. Therefore, it is wise to start by identifying what is most important to the end customer.

“Identify your crown jewels and protect them thoroughly. Estimate the acceptable level of risk for your company. Also consider how you can mitigate the effects of certain risks and transfer other risks via different types of insurance”, says Jimmy Ek.

IP cameras can not only be hacked, they can also be stolen and tampered with, or physically damaged. Jimmy Ek says that both the camera's physical security and their cyber vulnerabilities

demand a strategy and you can apply the same principles on both.

First, assets and resources must be identified. According to Jimmy Ek, when it comes to security cameras on your network, apart from the physical camera, the most

important assets are the video stream and the video material that is stored locally in the camera or on an external server.

“This video is, in most cases, very valuable to your company but of little use to anybody else. However, you should carefully consider why an intruder might be interested in access to your video material”, he says.

Review passwords

Another important action is to identify the most likely threats.

Jimmy Ek elaborates: “Are there are any potential threats to your IP camera system: physical sabotage (of the cameras themselves or the location the cameras monitor); access to the video material; or using a device (camera) as a point of intrusion in order to gain access to other parts of your network.”

It is also important to identify vulnerability: no system in the world is completely invulnerable.

“In order to be effective, devices and networks have to be exposed to the outside world. But some vulnerability can be prevented. The physical exposure of a camera can make it vulnerable to sabotage and therefore the quality of the camera is of utmost importance – to ensure that the camera should withstand extreme physical conditions. Secondly, it is about revealing passwords and allowing access to video management systems, as well as unsatisfactory practices in the operation and maintenance of the network”, says Jimmy Ek.

The cost of an attack

The end customer must identify



Jimmy Ek, Nordic Sales Manager, Axis Communications.

“Identify your crown jewels and protect them thoroughly. Estimate the acceptable level of risk for your company. Also consider how you can mitigate the effects of certain risks and transfer other risks via different types of insurance.”

the anticipated cost of an attack in order to know how much to invest to safeguard the system.

“If the cameras are used in an everyday environment and there is no chance of them being used as a gateway to the rest of the network, you can expect the cost of an intrusion in the camera to be quite low. But if your situation is more sensitive and an intrusion in your network could expose your company to financial losses or loss of confidence then the costs will be much higher, and you will probably want to invest more time and energy in safeguarding your security system”, Jimmy Ek concludes.

Axis' top 10 recommendations for securing a security application:

1. Conduct a risk analysis in accordance with the strategies above (identify assets and resources, identify the most likely threats, identify vulnerability and identify the anticipated cost of an attack)
2. Compile all available knowledge on how you can protect your system and work closely with your dealer, installation engineer and supplier.
3. Secure your network. If the

network is hacked then it increases the risk of access to sensitive information and attacks on individual servers and network devices

4. Use strong, unique passwords and change them at regular intervals
5. Don't rely on a network device's “factory default setting”
 - a. Change default passwords
 - b. Activate and configure a device's cyber security functions
 - c. Deactivate functions that are not used
6. Use an encrypted connection when possible, even on a local network
7. The user should not be allowed access to a camera if not required by the design of the system. The user should only have access to video via a VMS or via a media proxy
8. Check the access log on a regular basis to detect any attempts to hack the system
9. Check your network devices on a regular basis. Activate system notification whenever possible
10. Always upgrade to the latest firmware because the manufacturer may have closed security gaps.



IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

20-22 JUNE 2017 EXCEL LONDON UK

THE ONLY LARGE SCALE SECURITY EVENT IN EUROPE THIS YEAR



Over 10,000 security products to test & trial

- Find your perfect solution from over 600 leading security suppliers
- Pre-book 1-2-1 meetings with the suppliers you want to work with
- Discover future trends with free education seminars & discussion panels
- Grow your network with over 27,000 other security professionals
- Get discounted air travel & accommodation exclusively for IFSEC visitors

REGISTER TO GET YOUR **FREE** BADGE TODAY AT IFSEC.EVENTS

Supported by:



Your badge also gives you entry to:



Asian manufacturers talk about the market and its trends

Asian video surveillance product manufacturers continue to gain global market share. Detektor has interviewed management representatives from three of them, all with slightly different orientation.

Dahua, from China – the second biggest video surveillance manufacturer in the world – has an expansive growth plan while Idis, from South Korea is fighting to reach the top 10 manufacturers list and focuses on becoming a one-solution company. Finally Lilin, that has moved away from the traditional market and found a new home in the automation market.

Idis sees advances in ANPR and intelligent analytics

Idis, the biggest South Korean video surveillance manufacturer, is continuing to grow and is placing great emphasis on international presence. After increasing its business in Europe, the Middle East and the US, the next step for Idis is to establish itself among the global top 10 video surveillance manufacturers.

By Henrik Söderlund



Brian Song, Managing Director for Idis Europe.

Idis has previously been named as one of the biggest DVR manufacturers in the world. Today, Idis wants to be a manufacturer that provides end-to-end solutions for its customers. Brian Song, Man-

aging Director for Idis Europe, believes that the reason why the industry has seen a lot of acquisitions lately is that companies are preparing for the next business step: becoming a one solution company. Installers and integrators want to find an end-to-end provider who has a reliable solution and that can be a trusted supplier, so that the end user can choose one company, which will meet their needs and demands and supply everything.

Global market share means a lot to us and we are trying to get into top 10. That is our goal.

“Many surveillance manufacturers have now also added or acquired VMS to become strong end-to-end solution vendors and that is a key to their success, while others are moving into more sophisticated analytics such

as people counting, heat mapping and queue management so users can learn more about their customers’ behaviours, needs and demands,” says Brian Song.

In 2015, you said your plan was to increase your business in North America and Europe. How is it going?

“Idis America was launched in 2015 and is now a twenty person operation and still growing. We are attracting a lot of interest from the market and we offer an end-to-end solution.”

What about Europe?

“Currently, Benelux is our biggest market in Europe and we are rapidly growing in the UK, particularly in retail, education, local government and various commercial sectors. We have also signed deals with leading integrators and distributors in Germany, Russia and Spain.”

How much of your revenue comes from international sales?

“Our domestic market is strong and takes a large portion of our sales with a market share of around 40 per cent. Year by year, our overseas sales are increasing. Overall I would say it is about 50-50 but the overseas business is certainly accelerating.”

What other aims do you have?

“Global market share means a lot to us and we are trying to get into top 10. That is our goal. In a recent IHS report, Idis was ranked as number fifteen in the global video surveillance market and number six in the recorder market. We want to be among the top ten, and top three in the recorder market.”

What is the top trend in the security industry today?

“Video analytics is one: there is much more operability today since video surveillance can be used in combination with commercial purposes. The demand for intelligent platforms has increased and the need to derive intelligence from big data. Another trend is ANPR (Automatic Number Plate Recogni-

tion) for car parks, petrol stations, small hotels, shopping malls among many more commercial applications.

What is your view on the Internet of Things?

“There is a lot of discussion in the industry and all players are doing something. In terms of surveillance, there are more and more devices and more and more sensors and that means more complexity. We believe our NVRs can be a main IoT hub, because NVRs and previously DVRs, have functioned as hubs.”

What is the main problem with IoT?

“It is still quite complex to configure sensors into a traditional NVR. NVRs used to be the hub in the surveillance system. However, to install it, set it up and maintain is often very complex, but we believe surveillance is very much part of IoT and we have simplified configuration and maintenance through patented zero configuration that goes beyond plug-and-play and thus removed that complexity.”

Commoditisation leads Lilin to home automation

Merit Lilin has turned to new markets and particularly to the smart home automation market as a response to the commoditisation of the market. "We have achieved a presence in this sector within 4 years that we never would have in security", says Jason Hill, Vice President of Merit Lilin.

By Henrik Söderlund



Jason Hill, Vice President of Merit Lilin.

Founded in 1980, Lilin has a long history in the video surveillance market. However, in recent years the company has taken a new path after anticipating the consolidation of the market, with more standardisation and lower prices. Lilin's main focus has shifted from security installations to home automation in many markets.

Only two SDKs

"Four years ago, we started to work with some American home automation manufacturers and we discovered that we were very suitable for this market", says Jason Hill.

The major reason for that is that Lilin only has two SDKs in all their products – one for all the cameras and encoders, and another for the recording systems (i.e. NVRs) and decoders – which means only two drivers have to be written in order to make all products compatible with the automation system.

"Our competitors have many different SDKs and when they release a new product, they will write a new SDK for it. Therefore it will not work with the driver that was written two years ago, whereas we are consistent in the fact that when we release a new product, it is compatible with our current SDK", he says.

Lilin started doing deep integration of cameras and its video recording system with home automation systems in order to let the end user control the CCTV

system from his or her automation platform.

Wider adoption

"The US is leading in the world of adoption of smart homes. Europe and the US are growing at the same rate, but the American market is more advanced and potentially bigger", says Jason Hill.

"Europe is also growing and if you look at the graphs of growth of smart homes in Europe and America you will see a very sharp increase for the European market".

He claims that more awareness of smart home technology and the fact that the cost of the technology is coming down and making it more accessible, contributes to wider adoption.

"In 3–5 years time, the average British home will have a camera in it, and another two or three smart devices. Once you get to 3–4 smart devices that act independently, homeowners are going to ask how the devices can work together and that is where automation will become interesting. Sometimes our cameras will go in before the automation system, but usually they are going in as part of automation system," says Jason Hill.

Security is the main driver

According to Lilin, the user's key driver for purchasing a home automation system is security, not lighting, or any other clever gadgets. The reason for this is psychological and Jason Hill argues that it follows Maslow's hierarchy

of needs where the basic needs for human beings are food and shelter and then security.

"There are so many things that are high up in that hierarchy: luxury goods like being able to listen to music in the whole house, etc., but further down is safety and security and that is why you

as they have in their house. These people are not so concerned about which is the cheapest, they want the best", says Jason Hill.

All about integration

Today, more and more of Lilin's product development is focused on the home automation and inte-

In 3–5 years time, the average British home will have a camera in it, and another two or three smart devices.

can get an alert from the home automation system and be able to look at the cameras from your phone, it improves people's sense of security", he says.

More cameras than expected

Jason Hill also stresses that many of the projects are bigger and contain more cameras than many people and other IP camera manufacturers think. Some are using server based

VMS platforms, which Lilin also integrate into home automation and Lilin also target the high-end residential market.

"Some people own more than one property or one business. When they see our products in their homes, they want those products in their businesses and in their other properties too and it leads on and on. They might have a yacht and then they want the same automation system there

gration market, and the company has also gone into the IP video door phone and marine camera markets.

Jason Hill says: "We are all about integration now. Home automation will certainly be a cornerstone for our business for the next five years. In nearly every single case, when a home automation system is installed in the house, cameras will go into that system."

He argues that Lilin has achieved a presence in the home automation sector within 4 years that they never would have done in the traditional security industry and they will move on to more sectors ahead.

"It is very refreshing. I have been in the security industry for 30 years, and I am so passionate and excited about what we are doing now in automation. It has completely reinvigorated me as a manager in this business."

The CEO of Dahua, Fu Lique, believes the company will be able to continue to grow at the same rate for another 3–5 years due to more intelligent functions at the edge.

“CCTV has not hit the ceiling, there is still a lot of room for growth”, he says.

By Henrik Söderlund



“CCTV has not hit the ceiling, there is still a lot of room for growth”, says Dahua CEO Fu Lique.

Video analytics will sustain Dahua’s growth

Dahua is the world’s second biggest video surveillance manufacturer with more than 10,000 employees and was ranked as the fourth biggest security company in the world in the A&S Security 50 report 2016.

“We have a plan until 2018, but we cannot reveal any details. But before 2008, our CAGR (Compound Annual Growth Rate) was 37 per cent. From 2008 to 2014 we have experienced rapid growth of 47 per cent and we wish to keep that”, says Fu Lique.

He believes there are many reasons for Dahua being able to sustain this rapid growth.

“Because of the technology and high functionality, like video analytics, people counting and others, we can fulfil or solve customer requirements and increase the business intelligence. Therefore, for us, CCTV has not yet hit the ceiling; there is still a lot of room for growth. I believe we still have 3–5 years or more with this level of high growth.”

Increased marketing budget

Dahua is now growing faster abroad than in China. Domestically it holds the second position but the company stresses that there are markets where it is leading, like in the Guangxi province and in Brazil for example.

Fu Lique says that Africa is Dahua’s fastest growing market in terms of percentages, but there are also good growth opportunities in Europe.

“We have been selling individual hardware products, and in the future there will be more solutions. This will drive the growth in Europe”, says Fu Lique.

Dahua admits it has previously been too conservative with marketing, and that it now places greater emphasis on personnel training and localisation in the individual markets. The company is also more involved in project solutions and government projects than before. All this together will increase growth, Fu Lique believes.

“After many years of working hard in Europe, we have already entered the top three in multiple markets”, he says.

The Dahua CEO mentions the UK as a market where HD-CVI has been very successful.

“We first introduced HD-CVI into this market three years ago and it has been a great success. In many cases, one cannot change the cabling and according to the research, 50 per cent of the replacement market is changing from analogue to high definition.”

The major trends

Fu Lique sees three major trends in the video surveillance industry. The first one is HD 24/7:

“No matter if it is daytime or night time, the picture should always be clear with high resolution.”

The second trend is artificial intelligence and the fact that the hardware is able to learn through

experience. The longer the usage, the more data it can process. Finally what Fu Lique refers to as technology fusion: cameras with video analytics combined with other digital sensors.

“This kind of technology will fulfil market demands and it is the future”, says Fu Lique.

He believes that the Internet of Things can bring value and success eventually, but it is still at an early stage.

“Google indicates that IoT is coming. Video surveillance cameras are one of the sensors and combined with other sensors, it

“That is a market that combines a great deal of technology, for example floor management, PA systems and other technologies. When brought into the building, technology can make building management much easier, more intelligent, and it can bring more convenience to the building users. This is a market that will grow.”

Looking for acquisitions

While, for example, Canon has acquired Axis and Milestone, Chinese companies within the physical security industry have been very cautious when it comes

“This kind of technology will fulfil market demands and it is the future.”

can create more value within our everyday lives. We began with people counting in 2001 and looking at the flow of big data and analysis up to now, we think it has created some value for the human life and therefore IoT is definitely something to expect in the future”, Fu Lique says.

Smart buildings

According to Dahua, the market for smart buildings and the market for smart homes are both in an early phase in China, and therefore it is hard to say how big the markets might be. However, Fu Lique sees growth potential in the smart buildings market.

to acquiring western companies. However, this year Hikvision acquired Pyronix.

“We are also looking for and would welcome an opportunity, to work with a quality company. However, we are still looking...”, Fu Lique says.

Dahua’s biggest challenge lies inside the business according to its CEO.

“I think market competition is always there and that is not always a bad thing, sometimes it makes you grow. But the biggest challenge for Dahua always comes from inside; to become better and much more advanced. This always comes from inside the company.”

Two important reports

for anyone interested in developing their security business

The Physical Security Business 2016 to 2021

The new 2016 definitive resource for access control, intruder alarms, video surveillance market research & investment analysis.



The Internet of Things Smart Commercial Buildings 2016 to 2021

Market prospects, impacts & opportunities.



This report analyses the techno & commercial changes that are impacting the business and the role that mergers and acquisitions, investment and alliances are playing in changing the competitive landscape.

The information is geared towards all those engaged in managing, operating and investing in physical security companies (and their advisers) around the world. In particular those wishing to acquire, merge, sell or find alliance partners will find it especially useful.

Starting at only USD \$1,500 this report provides valuable information on how Physical Security companies can develop their business through Merger, Acquisition and Alliance.



Order the report on www.armediaint.com
or email to: info@armedia.se

This new 2016 Study from Memoori makes an objective assessment of the market for Internet of Things technologies, networks and services in buildings 2016 to 2021. The focus is on market sizing and opportunities for smart commercial buildings, providing a fresh market assessment based upon the latest information. Regions for this edition of the study are split into 5 categories representing the international markets of North America, Latin America, Europe, Asia Pacific and The Middle East & Africa.

The information contained in this report will be of value to all those engaged in managing, operating and investing in Commercial Smart Buildings (and their advisers) around the world. In particular those wishing to acquire, merge, sell or find alliance partners will find it especially useful.



Order the report on www.armediaint.com
or email to: info@armedia.se

armedia

Connecting Security Buyers and Suppliers

AR Media International AB, Västberga Allé 32, S 126 30 Hägersten, Sweden
Phone: +46 8 556 306 80, www.armediaint.com

Mahesh Saptharishi, Avigilon CTO:

"Licensing does not al

Avigilon continues to grow rapidly and believes that video analytics and artificial intelligence will be an important part of the surveillance industry's future. Detektor met up with Mahesh Saptharishi, Avigilon's CTO, to discuss technical trends and Avigilon's patent licensing programme.

"We have an aggressive roadmap when it comes to video analytics, so the acquisition of the Object Video patent portfolio was an important aspect of that," he says.

By Henrik Söderlund

Alexander Fernandes founded Avigilon in 2004 and he is still its President, CEO and Chairman of the Board. The company designs, develops, and manufactures video analytics, network video management software and hardware, surveillance cameras, and access control solutions, and in 2015, the turnover was 369 million dollars – a 36 per cent increase compared to 2014.

Mahesh Saptharishi co-founded VideoIQ, but joined Avigilon in 2014 when Avigilon acquired VideoIQ. He argues that the

introduction of Appearance search, it is really taking this to the next step and making it more of a complete solution and that is what is propelling us forward."

How do you plan to sustain your high growth rate?

"The phase that we are entering right now is really the platform going forward. We believe that the number of cameras that are being deployed is increasing. As a result of this increase, the conversation is suddenly changing from how many cameras you deploy and



Avigilon CTO, Mahesh Saptharishi co-founded VideoIQ, but joined Avigilon in 2014 when Avigilon acquired VideoIQ.

alignment between the expectations of what video analytics can do and what the industry at large can deliver. We have gone through ups and downs on that as I mentioned previously and, in terms of it taking off, I think video analytics is going to become a required component of most large security system sales at this point."

At the end of 2014, you acquired Object Video with all its patents. What is your aim with your patent licensing programme and how can it be a part of your business model?

"We have an aggressive roadmap when it comes to video analytics, so the acquisition of the Object Video patent portfolio was an important aspect of that. We believe analytics and artificial intelligence are the future of the industry. That said, we are introducing a huge array of products that are geared towards really bringing video analytics and artificial intelligence to the industry in new ways. We also believe that the industry at large could benefit from the intellectual property that we have in our portfolio today. There are going to be others in the industry who will be interested in seeing this in their own products and we want to encourage that, and so our patent licensing programme will be a key part of that as well."

What impact would a more competitive view on patents have on the security industry and for

integrators and end users?

"I think it should have a positive impact because we hold the largest number of foundational patents in video analytics in this industry at this point. I believe our patent licensing programme complements and encourages industry growth in video analytics, so from that standpoint I think we see this being a positive step for the industry at large."

Many companies were concerned about what you would do as Object Video was behaving so aggressively.

"Licensing does not always have the smoothest of starts and I think Object Video experienced some of that. But at the end of the day, our interest in video analytics is really driving our strategy in holding the key patents necessary for us to build our own products, and develop video analytics, but also to allow others to do so as well."

What is the top trend in the physical security industry today?

"I would say probably two things; the first is smart codecs and I would link it to video analytics. One of the features that we have in our products is called Idle scene mode, where we can control compression based upon what the cameras actually see. It is using video analytics not only for alarms, but also to really look at the value of the information that you are compressing, transmitting

“I think we are entering the third phase right now with our introduction of Appearance search.

video surveillance industry has gone through three large growth phases. The first was the transition from analogue to IP, where HD resolution was a big driver.

"The second phase was taking advantage of high resolution and bringing video analytics to the mix. Video analytics has had an up and down cycle, but when Avigilon introduced video analytics it was all self-learning and not something that required a great deal of calibration, providing the customer with the value of having a full end-to-end solution", he says.

And the third phase?

"I think we are entering the third phase right now with our

how much coverage you have across your facility, to dealing with information overload. It becomes a question of how many operators you have to actually look at that live video across the many cameras you have installed. And in order for us to make that a scalable solution, we have to change this from operators looking at video to where operators are instead being asked by the system to focus on certain areas where there might be activity. That is really where the artificial intelligence and video analytics come in, helping drive further growth."

Is video analytics finally taking off?

"I believe there is finally an

ways begin smoothly"

and storing, and based on that value, allocate the right amount of storage or bandwidth to that content."

starting to come to the forefront of many practical applications and in fact it is the video analytics more useful."

“I believe there is finally an alignment between the expectations of what video analytics can do and what the industry at large can deliver.

And the second trend?

"If you look at the rate at which processor technology in cameras and in servers is increasing its capability, this is naturally leading to bigger and better video analytics being implemented. So, video analytics technology that our industry previously could not consider implementing because it was so computationally intensive and as a result, too expensive, are now

What will the market look like in the future?

"I think a few years from now, what we do with the video will be a greater topic of conversation than resolutions, bandwidth and how many cameras you have on site. I think security operations people will no longer be watching video on a video wall. There are going to be more wearable technologies and the security force will be more of

a mobile force. Enterprise security will not be limited to the high end of the market, because targeted applications where you can afford a mobile security force is going to make security technology more accessible to a wider swath of the market."

Chinese security camera manufacturers are selling a lot of cameras. How do you tackle the commoditisation of the market?

"I think commoditisation is a very natural part of the industry. Think of the cell phone market: in the beginning of the 2000s it was all about smaller, cheaper phones and eventually cell phone companies were giving away phones as a part of a subscription model. They became commoditised, but then suddenly you had smart phones and today you pay 500 dollars for

them. I think our industry is going through a very similar trend where cameras that are just plain, old video sensors are going through a natural trend of commoditisation and I believe for the industry at large, that is a good thing because it beckons newer innovations that are forthcoming and that means the industry will go through a bit of technology bump at this point where you will see new camera technology and we believe it is largely going to be video analytics driven. So, what is happening with the Asian manufacturers is perfectly natural and a technology company like ours is always thinking about the next thing and how to both take advantage of the fact that certain sensors and cameras are being commoditised right now and also what is next when it comes to camera technologies."

D-TECT® External Detectors

Wired and wireless
Advanced IP connectivity
Precision Laser

FEATURES

Programmable detection range up to 50m
Adjustable pan and tilt detector module
Covert sensor module
500m wireless communication



Clarius® LED Illuminators

Visible White-Light
Covert Infra-Red
PoE Variants

FEATURES

Interchangeable lens diffuser system 10° - 120°
Configurable lighting for IP and standard cameras
CleanLITE® self cleaning lens coating technology
Lighting design service now available



Unit 2, Birch Business Park, Whittle Lane, Heywood,
Greater Manchester, OL10 2SX, UK
gjd.co.uk | info@gjd.co.uk | +44 (0) 1706 363 998



AWARD WINNING
BRITISH MANUFACTURER

The first universal access credential

Austin, Tx (USA)

HID Global is launching what is believed to be the industry's first end-to-end identity access management solution that enables government agencies and other organisations requiring higher security to use a single credential for accessing doors, IT systems, networks and data.

The company's new *HID PIV* (Personal Identity Verification) solution provides complete identity lifecycle management – from identity proofing plus secure credential issuance and use, to deprovisioning of these credentials. Organisations

are now able to unify physical and IT security systems to create a far more seamless experience for users, while also offering strong authentication applying trusted credential and other advanced security capabilities that are easier to procure, deploy and maintain.

"HID PIV represents the industry's first comprehensive IAM solution that provides trusted identities for accessing both IT and physical domains," said Brad Jarvis, Vice President and Managing Director of IAM Solutions with HID Global. "HID Global con-

tinues to develop fully integrated solutions across our portfolio of products and provide a convenient and trusted experience for our customers."

HID PIV helps government agencies and other regulated industries such as banking, healthcare, and transportation to improve their overall security posture and consolidate physical and IT security. The company's PIV-based solution allows organisations to use strong cryptographic credentials for users to digitally sign emails or documents, decrypt emails or

files, use full disk encryption and boot protection to secure laptops, protect sensitive print jobs with secure printing and leverage many other security capabilities.

The HID PIV solution is available in two options – Express and Enterprise. HID PIV Express provides a complete high-assurance multi-factor authentication solution. The solution covers the complete lifecycle of the identity: from identity proofing, secure credential issuance, usage in IT systems and facilities access, and credential retirement.

Dallmeier 4K ultra HD camera

Regensburg, Germany

With the *DDF5400HDV-DN* **Dallmeier** presents a 4K camera with ultra HD resolution. Owing to their extremely high resolution the cameras within the Ultraline series provide even sharper images with more details.

The DDF5400HD Ultraline camera series has been designed especially for applications requiring very high resolution images in real time. The camera is available with an integrated lens in a vandal-resistant dome housing. It can be conventionally supplied with an external power supply unit or conveniently with Power

over Ethernet (PoE Class 0, IEEE 802.3af).

The high resolution of the sensor and the sophisticated image processing enable real-time recordings with UHD resolution at a frame rate of up to 25/30 fps (2160p/30) with excellent quality. Thus, the camera is ideally suited when capturing the finest details in real time is required.

The camera is equipped with an ambient light sensor and a removable IR cut filter and can automatically switch between day and night mode. In addition, different day and night presets for the

exposure settings can be defined and adjusted.

The camera has a motor-driven megapixel varifocal lens that is tuned to the image sensor. The adjustment of zoom, focus and iris is made conveniently using a web browser. The manual lens setting directly at the installation site of the camera is not required.

The P-Iris control provides precise and automatic setting of the optimum aperture. Thus, the camera achieves a much better depth of field than with conventional DC auto iris lenses under almost any lighting conditions.



With the DDF5400HDV-DN Dallmeier presents a 4K camera with ultra HD resolution.

It is also equipped with a RAM memory that is used by the Edgestorage function for storing the video stream in case of a network failure. When the network is restored, the Smartbackfill function ensures a fast transmission to the Smavia recording system. This stores the video stream with high speed and then seamlessly continues the recording of the live stream.

swh

Camera series with Hanwha's "most important component" embedded

Chertsey, Surrey (UK)

Hanwha Techwin is launching the *Wisenet X series* with an embedded proprietary chipset that the company believes is the most important component to date developed by Hanwha Techwin's core technologies.

"Wisenet 5, our latest chipset, offers extremely high performance. It's at the core of Hanwha Techwin's competitiveness," said Lee Man-Seob, President & CEO

of the Hanwha Techwin Security Business Group. "The Wisenet X series is our first product range to use this single chip solution. As a result, our new 5 megapixel and 2 megapixel camera lineups will redefine industry standards, not only with exceptionally sharp images, but also with much faster image processing and upgraded functions."

The Wisenet X series offers

150dB WDR, image stabilisation using gyro sensors and boasts razor sharp images 24/7 with improved low-light performance. Using Wisestream II, the second generation of Hanwha Techwin's unique compression technology, the Wisenet X series delivers a highly efficient bandwidth friendly camera range. There



By adding the Wisenet X series to the recently released Wisenet Q and P series, Hanwha Techwin has now established a full line-up.

are also many other notable key benefits, including a variety of on-board analytics.

swh



Business & Product News – Every Day!

www.securityworldhotel.com

Flir launches United VMS update

Wilsonville, Or (USA)



Flir is releasing a *United VMS 7.0 software update* with exciting new

features and enhancements to Latitude, Horizon and Meridian products.

The version update focuses on tighter integration and superior user experience with Flir's thermal security cameras.

The inclusion of advanced integration with Flir security cameras means that the new version offers the ability to configure thermal settings from the United VMS

and a FLIR PT-Series picture in picture (PiP) is available in United VMS client applications. There is also support for analytics and radiometric events sent from FC-Series ID, FC-Series R and A310-PT cameras.

The update provides Improved robustness for enterprise deployments and large customers with complex, high-availability requirements will be able to take

advantage of new backup and failover facilities. There are also improved forensic tools and EZ client web interface enhancements, support for digital PTZ in EZ client web interface and an adaptive thumbnail view in EZ client. The mechanism for Fast Forward (FF) playback has been improved along with the improvement in image quality with 4K cameras utilising the 'de-jittering' filter. swih

Explosion-proof camera from Hikvision

Hangzhou, China

Providing a safe camera solution for video surveillance applications within hazardous areas, **Hikvision** has launched three new ATEX & IECEx certified standard network cameras, including bullet and PTZ dome style models.

Hikvision's latest *explosion-proof cameras* utilise 304 and 316L stainless steel housings for maximum corrosion and explosion resistance, and are IP68 water/dust ingress rated. For any surveillance requirement within hazardous environments, or environments where the camera is required to operate within areas with combustible sources, the new explosion proof cameras provide a high-performance and safe imaging solution. Typical applications are for poten-

tially hazardous or explosion risk areas, such as gas & oil processing and storage plants, chemical plants, industrial sites, deep mines, or marine applications.

Hikvision's range of ultra-low-light explosion-proof camera models boast Hikvision Darkfighter technology, providing minimum illumination as low as to 0.005Lux in colour mode and 0.0005Lux in B/W mode. The result is crystal-clear colour and monochrome images in conditions that would defeat conventional low-light models. The range also comes with progressive scan 2MP and 4MP CMOS image sensors, full HD 1080p video at up to 60 fps, triple video streams, 3D DNR and 120dB WDR.

Greatly reducing the required video bitrate to reduce bandwidth and associated storage costs, the new cameras support the latest Hikvision H.265+ smart

codec technology. An intelligent algorithm developed by Hikvision, H.265+ is an encoding technology based on the H.265/HEVC (High Efficiency Video Coding) standard, with the benefit of being able to greatly decrease the bitrate of surveillance video through three core technologies, namely: Prediction Encoding, Noise Suppression and Bitrate Control.

Accepting 100v - 240V AC and PoE input power, video performance is enhanced via Smart features such as Smart detection, Smart tracking, ANPR etc, the



Hikvision's latest explosion-proof cameras.

new explosion-proof camera range delivers a robust video surveillance camera solution for use within any harsh/critical operational environment. The cameras also support on-board storage up to 128Gb via SD card.

Hikvision explosion-proof cameras include the DS-2XE6222F-IS 2MP explosion-proof network bullet camera, DS-2XE6242F-IS 4MP explosion-proof network bullet camera and DS-2DF6223-CX (W) 2MP explosion-proof network speed dome. swih

■ For more info about the products, contact the suppliers directly by looking in the Security Buyers Guide on page 30

swih The suppliers web site is linked to the global security web portal, www.securityworldhotel.com

One-stop service for innovative RFID products

125KHz / 13.56MHz / 433.5MHz / 915MHz / 2.45GHz



- Biometric (Fingerprint)
- Bluetooth / NFC Access Controller
- Passive / Active RFID System
- Reader / Writer Programmer for LF / HF / UHF frequency
- Car Parking System / Lift Access Control System
- Single / Multi-Door Access Controller / ESD Access Control System
- Electric Strike / Electric Deadbolt / Electromagnetic Lock
- Exit Button / Contactless Infrared Sensor Exit Button

Module Series

- Compact with Dual, triple, quadruple decoding by single module.
- With multi-selectable output formats. (ABA, Wiegand, UART, RS-232, RS-485)
- Low power consumption modules with sleep mode supported.
- OEM / ODM available.




PONGEE INDUSTRIES CO., LTD.

www.pongee.com

pongee@pongee.com.tw

Made In Taiwan

Mobotix kicks off 2017 with intelligent 3D detection

Langmeil, Germany

Mobotix is kicking off 2017 with new innovative developments including the *Mxactivitysensor 2.0* a proprietary network switch that is ideally suited for installing small systems, as well as an update to the MxMC 1.3 video management software.

The Mxactivitysensor has been integrated in to the camera since 2013, differentiates between events that are relevant and irrelevant to alarms and thereby reduces the number of false alarms. This motion analysis reliably detects moving objects and does not trigger any false alarms in the event of

interference such as rain, snowfall or moving trees or poles.

Mobotix has taken this idea one step further with the Mxactivitysensor 2.0, as it includes intelligent 3D motion detection that also reduces false alarms triggered in conventional motion detection (for example, in response to the movement of birds or small wild animals). This means that the camera always keeps an eye on the essentials and only triggers an alarm for security-relevant events. A practical example is the monitoring of the flat roof of a warehouse. With Mxactivitysensor 2.0 in

place, intruders trigger an alarm wherever they might be on the roof, while a bird would not. Persons at the fence do not go undetected, either. If someone enters the premises, an alarm is triggered, whereas with a watchdog (such as the one pictured above), no alarm is triggered.

Alongside Mxactivitysensor 2.0, which is available in the latest firmware version (4.4.2.34), Mobotix now offers a new four-way sensor: Mxmultisense. This sensor records information such as



Mxactivitysensor 2.0 includes intelligent 3D motion detection built in to reduce false alarms.

the noise level, movement (PIR), temperature and brightness and is an inexpensive supplement to camera installations. It also monitors areas that cannot be captured by cameras.

 **CCTV** 

Arecont Vision expands Microdome range

Glendale, Ca (USA)



Microdome Duo is designed with an extremely compact and advanced twin sensor omnidirectional camera.

Arecont Vision is expanding the compact Microdome ultra-low profile true day/night camera family with the release of its dual-sensor *Microdome Duo* series.

Microdome Duo is designed with an extremely compact and advanced twin sensor omnidirectional camera. Both sensors feature independent remote focus modules, mounted on 3-axis gimbals for outstanding viewing coverage.

“Customers around the world will benefit from the small size, advanced cyber security protection, future-proof design, and unique capabilities of the new Microdome Duo,” said Sanjit Bardhan, Vice President of Sales, Middle East, Africa, and India

(MEAI) for Arecont Vision. “Microdome Duo reduces the number of cameras required for a wide range of applications by providing high definition video of two areas at once, and its many, installer-friendly features cut down on installation time and expense.”

A single compact Microdome Duo camera can be mounted on a wall or ceiling to cover two different views simultaneously. This results in enhanced coverage and improved situational awareness over a multitude of scenes, particularly those in need of low-profile, high resolution indoor/outdoor surveillance. Such areas include hallways, walkways, ATMs, and POS terminals.

Microdome Duo offers fast frame rates and a choice of 4, 6, or 10-megapixel resolution models. Each camera is available with lens options ranging from 2.1 to 16mm, providing the widest possible application requirements. Snapstream (smart noise adaptation and processing) technology reduces camera bandwidth consumption in all Microdome Duo models without impacting image quality.

At the core of Microdome

Duo is an Arecont Vision FPGA (field programmable gate array) integrated circuit. Arecont Vision cameras are designed and built in the USA to run an in-house developed, massively parallel image processing architecture (MPIPA) on the FPGA. All core features and technologies are developed by Arecont Vision, allowing installed cameras to be upgraded with new capabilities, thereby extending the useful life of the device.

By employing the unique MPIPA architecture on the FPGA, Arecont Vision cameras do not require the use of common operating systems. This approach eliminates the risk of a cyber hacker repurposing an Arecont Vision camera for use in distributed denial of service (DDoS) robotic actions or other increasingly common cyber attacks.

The Microdome Duo series is designed for applications with challenging lighting conditions, featuring integrated, dual, day/night mechanical IR cut filters. For applications with strong backlighting, reflections from wet flooring, streets or puddles, or contrast due to fog, mist, or glare, optional wide dynamic range

(WDR) equipped 4- and 6-megapixel models are also available. Built-in Corridorview technology provides better coverage of hallways, corridors, and other narrow spaces without wasting pixels on unchanging areas.

Each Microdome Duo camera offers independent remote focus capability to simplify set-up and significantly reduce installation time. Installers can simply select short range focus or full range focus for rapid setup, or they can adjust the view remotely as required by the application.

The Microdome Duo is a compact (71.9mm/2.83” height by 103mm/4.06” width by 163mm/6.42” length), light weight (0.88kg/1.95lbs) surveillance camera series. It is built on Arecont Vision’s new installer-friendly enclosure design to further simplify positioning and installation. A single PoE IP connection is required, reducing wiring time and expense.

The rugged, tamper-resistant, die-cast aluminum housing features two polycarbonate dome bubbles that are both IK-10 impact-resistant and IP66 weather-proof rated. The Microdome Duo is ONVIF Series S compliant. 

 For more info about the products, contact the suppliers directly by looking in the Security Buyers Guide on page 30

 The suppliers web site is linked to the global security web portal, www.securityworldhotel.com



Some 33,501 visitors from 129 countries came to Intersec Dubai.



The vast majority of visitors came from the United Arab Emirates.

More than 33,000 came to Intersec in Dubai

With more than 1,300 exhibitors and some 33,501 visitors from 129 countries, Intersec in Dubai (22–24 January) was a 2017 great kick-off for the global security industry.

The event took place over 56,000 square metres in the Dubai International Convention and Exhibition Centre – a huge area – and most of the large companies in the physical security were represented.

According to organiser Messe Frankfurt Middle East GmbH, almost half of the visitors came from the United Arab Emirates. Saudi Arabia was second

with more than 3,000 visitors, followed by Iran and India with close to 1,800 and more than 1,000 visitors. Other countries with large representation were Pakistan, Qatar, Kuwait, Egypt, United Kingdom and Oman.

Detektor and AR Media were represented by Carlos Cisternas, on the company's own booth at the fair.

"It has been a good show and

people from all over the world have been here. We have many followers in the Persian Gulf area and it is important for us to be present here", says Carlos Cisternas.

Regarding exhibitors, China dominated with 241 exhibitors, followed by the United Arab Emirates (210), United Kingdom (150), USA (85), Germany (84), Taiwan (55) and Italy (51).



Access Control provider Assa Abloy had many visitors to their stand.



Nedap, the Dutch access control provider, was represented on their stand by Jan Hofman and Lars Lensink.



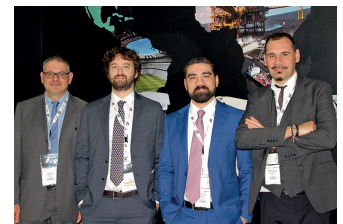
Intrusion Alarm provider Optex was present with Gaurav Mahajan, Division Manager and Aude Desbrerie, Marketing Director for Optex Europe.



Paxton was present with fr left Nick Lawden Int. Sales & Accounts, Dan Drayton Sales Manager.



Salto Systems was present during the event: Carlos Elosequi, Marketing Manager, Roger Birch, Regional Technical Lead, Ali Ahsan, Regional Sales.



The team from Italian CCTV manufacturer Videotec were present during the event. From left: Nicola Risi, Alberto Zulian, Davide Boschetti, Alessandro Franchini.



German CCTV provider ASP AG Grundig had Yalcin Demirak, Ludwig Bergschneider (CEO) and Tristram Borgmann meeting up with visitor in the stand.



Andy Jackson from CQR and John Angel from Takex were happy to display their products.



IDL Fastlane were present during the fair fr left Tony Smith, Stephen Short and Shane Naish.



The team from Austrian based access control provider EVVA had busy days.

intersec

SAVE THE DATE

January 21 – 23, 2018

Dubai, UAE

**The world's leading trade fair for
Security, Safety & Fire Protection**

7 Show Sections

Commercial Security

Information Security

Fire & Rescue

Safety & Health

Homeland Security & Policing

Smart Home

Perimeter & Physical Security

www.intersecexpo.com



messe frankfurt

Security User Expo cuts off one day

The Danish security event offers more efficient format

Security User Expo is Denmark's largest security exhibition – and Scandinavia's second largest, surpassed only by the Skydd fair in Stockholm. And the event is in constantly evolving. This year the organisers have reduced it by one day.

The third Security User Expo will take place in Copenhagen on the 27th and 28th of September 2017 and is organised by AR Media International in collaboration with Sikkerhedsbranchen (the Danish Security Industry Association). The event will once again be held at the Bella Center's East hall, just 100 metres from the Bella Center metro station.

– This year Security User Expo will be over two days rather than the three days of previous events. This step is taken as we strive to create an even more effective trade show. Two days means more visitors per day, a higher intensity and better utilisation of the exhibition resources with reduced

costs for all concerned, says AR Media International's CEO, Lennart Alexandrie.

Two intensive days

Otherwise, the show will have the same profile as before, with end user oriented conferences held alongside the exhibition, where suppliers will display the latest security products and services, whether it comes to protection against fire, burglary or other adverse events.

Target group – professionals

Both the exhibition area and conferences are designed to show the benefits of investing in security – whether it is for private or public



Security User Expo is Denmark's largest security exhibition.

organisations. The target audience for Security User Expo is professionals that deal with security in their organisation, full time or part time, as buyers or users, but also as representatives from the supply chain, including manufacturers, distributors, wholesalers, system integrators, installers and consultants.

1.5 million security cameras

The organiser of Security User Expo has already booked up more than 50 percent of the exhibition space. The confirmed exhibitors

come from Denmark, but also from other European countries and Asia. Denmark may be a small country but is also an attractive market for exporters

– The security market in Denmark is very interesting. The awareness of the benefits that security technology offers is very high. For example, Denmark with its 5.7 million inhabitants, has 1.5 million cameras installed. This equates to one camera for every 4 people in Denmark – maybe a world record, states Lennart Alexandrie.

Security buyers guide

Alarm Communication



Tel +44 (0)1895 474474
sales@csldual.com
www.csldual.com

Access Control



Box: 3042, 443 03 Stenkullen
Tel: 0302 680 600
Fax: 0302 680 640
Epost: info@cardkeep.se
Webb: www.cardkeep.se



mobility
solutions

Nedap Security Management

Parallelweg 2, 7141 DC, Groenlo
PO BOX 103, 7140 AC, Groenlo
The Netherlands
Tel + 31 544 471 111
www.nedapsecurity.com
info@nedapsecurity.com



Touchless Biometric Systems AG

Rietbrunnen 2, Pfaffikon SZ,
CH 8808, Switzerland
Tel +41 (0)55 533 20 00
tbs@tbs-biometrics.com
www.tbs-biometrics.com

CCTV



Security Tech Germany

ABUS Security-Center GmbH & Co. KG

Linker Kreuthweg 5
86444 Affing (Germany)
Tel +49 82 07 959 90-833
Fax +49 82 07 959 90-180
export@abus-sc.com
www.abus.com

Perimeter Protection



Forteza, JSC

Tilzes str. 38, 91112 Klaipeda
Lithuania
Phone +370 46 441195
Fax +370 46 412231
forteza@forteza.com
www.forteza.com



outdoor protection
our profession

Via Gadames 91, 20151 Milan, ITALY
Tel +39 02 380 701
Fax +39 02 308 80 67
www.sicurit.com, export@sicurit.it



TAKEX Europe Ltd.

Aviary Court, Wade Rd, Basings-
toke, Hampshire RG24 8PE, UK
Tel +44 1256 475555
Fax +44 1256 466268
sales@takex.com • www.takex.com

Security Events Calendar

March

 **15–16 March**
Sectech Norge –
Lillestrøm, Norway
Venue: Norges Varemesse
Organiser: AR Media International AB
Tel: +46 8 556 306 80
Fax: +46 8 19 10 11
Email: deniz.baykal@armedia.se
Website: www.sectech.nu

Visit AR Media at Sectech Norge

 **15–17 March**
SecurityExpo 2017 –
Sofia, Bulgaria
Venue: Expo Center
Organiser: BCCI
Tel: +359 2 981 66 26
Fax: +359 2 8117 428
Email: fairs@bccibg
Website: www.securityexpo.bg

 **15–17 March**
SECON 2017 –
Seoul, South Korea
Venue: KINTEX
Organiser: SECON 2017 OFFICE
Tel: +82-2-6715-5406
Email: global@seconexpo.com
Website: www.seconexpo.com

 **21–23 March**
Securex West Africa 2017 –
Lagos, Nigeria
Venue: Landmark Centre
Organiser: Montex
Tel: +44 207 886 3048
Email: joleen.sibley@montex.co.uk
Website: www.securexwestafrica.com

 **21–24 March**
Securika Mips 2017 – Moscow, Russia
Venue: Expocentre Fairgrounds
Organiser: ITE GROUP
Tel: +44 (0) 207 596 5079
Email: Dmitrijs.Syatchikhins@ite-exhibitions.com
Website: www.securika-moscow.ru

April

 **4 April–4 April**
Milipol Asia-Pacific –
Singapore, Singapore
Venue: Sands Expo and Convention Centre
Organiser: Comexposium Singapore
Tel: +65 6392 5328
Fax: +65 6392 3098
Email: andrew.marriott@comexposium-sg.com
Website: www.milipolasiapacific.com

 **5–7 April**
ISC West Expo 2017 –
Las Vegas, United States
Venue: Sands Expo Center
Organiser: Reed Exhibitions
Tel: +1 203.840.5602
Email: inquiry@isc.reedexpo.com
Website: www.iscwest.com

 **26 April**
Trygghetskamerans dag –
Stockholm, Sweden
Venue: Clarion Hotel Stockholm
Organiser: AR Media International AB
Tel: +46 8 556 306 80
Email: deniz.baykal@armedia.se
Website: www.trygghetskameransdag.se

Visit AR Media at Trygghetskamerans dag

May

 **3–4 May**
Security & Counter Terror Expo –
London, United Kingdom
Venue: Olympia
Organiser: Clarion Events
Tel: +44 20 7384 7894
Email: sophie.mckimm@clarionevents.com
Website: www.counterterrorexpo.com

 **17–18 May**
Security Forum 2017 – Barcelona, Spain
Venue: Centro de Convenciones Int. de Barcelona
Organiser: Peldañó
Tel: +34 914 768 000
Email: info@securityforum.es
Website: www.securityforum.es

 **23–25 May**
Exposec – Sao Paulo, Brazil
Venue: Sao Pulo Expo
Organiser: Fiera Milano
Tel: +55 (11) 5585-4355
Email: comercial@fieramilano.com.br
Website: www.exposec.tmp.br

 **30 May – 1 June**
Securex West Africa –
Johannesburg, South Africa
Venue: Centro de Convenciones Int. de Barcelona
Organiser: Peldañó
Tel: +34 914 768 000
Email: info@securityforum.es
Website: www.securityforum.es

June

 **20–22 June**
Ifsec 2017 – London, United Kingdom
Venue: Excel Exhibition Ground
Organiser: UBM
Tel: +44 20 7921 5000
Email: info@ubm.com
Website: www.ifsec.co.uk

September

 **27–28 September**
SecurityUserExpo 2017 –
Copenhagen, Denmark
Venue: Bella Center
Organiser: Ar Media International
Tel: +46 8 556 30 680
Fax: +46 8 19 10 11
Email: info@securityuserexpo.com
Website: www.securityuserexpo.com

November

 **6 Nov–9 November**
Defense & Security 2017 –
Bangkok, Thailand
Venue: Impact Exhibition and Convention Center
Organiser: GML Co., Ltd
Tel: +66 (0) 2642 6911
Email: yaowalak@asiandefense.com
Website: www.asiandefense.com

 **15–17 November**
Sicurezza 2017 –
Milano, Italy
Venue: Fiera Milano (RHO)
Organiser: Fiera Milano
Tel: +39 02 4997.6241
Fax: +39 02.4997.6252
Email: areatecnica1@fieramilano.it
Website: www.sicurezza.it

 **21–22 November**
Sectech Sverige –
Stockholm, Sweden
Venue: Stockholmsmässan
Organiser: AR Media International AB
Tel: +46 8 556 306 80
Fax: +46 8 19 10 11
Email: deniz.baykal@armedia.se
Website: www.sectech.nu

Visit AR Media at Sectech Sverige

 **22–24 November**
ALL- OVER- IP Expo 2017 –
Moscow, Russia
Venue: Sokolniki Expo
Organiser: Groteck
Tel: +7 (495) 647-0442
Email: aldushina@groteck.ru
Website: www.all-over-ip.ru

 **29–30 November**
UK SECURITY EXPO –
London, United Kingdom
Venue: Olympia
Organiser: Nineteen Event
Tel: +44 (0) 20 8947 9177
Email: mluis@nineteen-events.com
Website: www.uksecurityexpo.com

2018

 **16–18 January**
Perimeter Protection –
Nurnberg, Germany
Venue: Exhibition Centre Nuremberg
Organiser: Nurnberg Messe GmbH
Tel: +49 911 8606 – 8386
Email: perimeter-protection@nuernbergmesse.de
Website: www.perimeter-protection.de

 **21–23 January**
Intersec – Dubai, United Arab Emirates
Venue: World Trade Centre Arena
Organiser: Messe Frankfurt Middle East GmbH
Tel: +971 4 389 4500
Email: intersec@uae.messefrankfurt.com
Website: www.intersecexpo.com

Detektor International takes no responsibility for any changes to the details of the above mentioned events. Please always contact the organisers in each case to confirm the dates and venues.
www.securityworldhotel.com/int/Security-Events

Business & Product News
– Every Day!

www.securityworldhotel.com

SECTECH

EXPO & CONFERENCES / SWEDEN

Sectech Sweden 21-22 November, 2017
Stockholmsmässan/Stockholm

Be a part of the compact
success event in Sweden

Book
your stand
- before it's
too late

Reserve a stand at the most important security technology-focused event in Sweden 2017 – to be held in Stockholm on the 21 – 22 November at the International Stockholm Fair.

The compact Sectech event is an exhibition with seminars that will once again gather suppliers and buyers of security technology based products and services during two hectic days.

The technology focus at the exhibition is video surveillance, access control and all kinds of alarm and integrated systems for physical security applications. The seminars are focusing on technology trends and include topics like , Internet of Things, data security, the benefits and threats that come with drones.

The compact format means limited exhibition space – be part of the success in 2017 – book your stand now.

• EXHIBITION • SEMINARS • SECURITY BANQUET •



WWW.SECTECH.NU

Organizers:

ar media
Connecting Security Buyers and Suppliers



Stockholmsmässan

Media partners:

DETEKTOR
SÖDERSTRÖM

SECURITY
WORLDHOTEL.COM

Entrance sponsor:

nexus

Enabling
trusted
identities

AR Media International AB, Västberga Allé 32, S 126 30 HÄGERSTEN Sweden, Tel +46 8 556 306 80, www.armedia.se, www.sectech.nu



HIKVISION®



LET THERMAL TECHNOLOGY ALERT YOU!

Hikvision thermal cameras capture sharp images in the distance

Hikvision Thermal Cameras provide superior long-range Smart behavior analyses including line-crossing detection and intrusion detection in open and expansive areas, delivering vivid images at resolutions of up to 640 x 512 pixels. These powerful features make it the perfect solution for 24/7 perimeter protection, unhindered by any weather or light condition. Its temperature-anomaly and fire detection effectively prevent emergencies in critical infrastructure and many other applications.

Hikvision thermal products come with various styles for different application needs, including bullet, PTZ dome, handheld models and positioning system, dual-lens model with thermal and optical imaging in one unit is available as well.



Hikvision Headquarters
No.555 Qianmo Road, Binjiang District
Hangzhou 310052, China
T +86 571 88075998
F +86 571 89935635
overseasbusiness@hikvision.com

www.hikvision.com