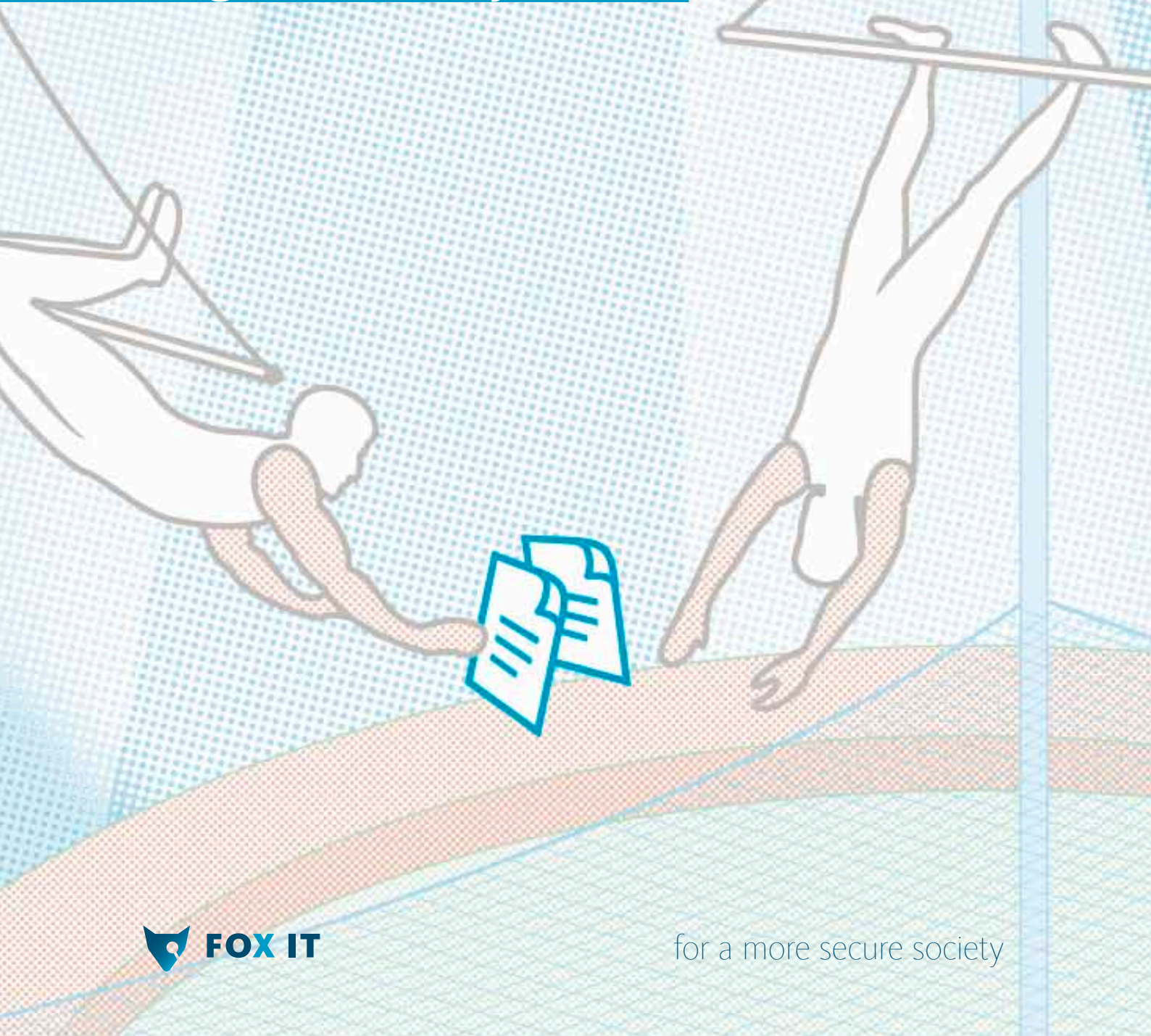


NR 3 NOVEMBER 2012

FOXfiles

Monitoring

What is your
digital safety net?



Smile

In autumn I was in the USA. Sixteen appointments in four days, so I was fairly worn out. However, I flew back from JFK to FOX-IT's headquarters in the Netherlands with a smile.

FOX-IT aspires to achieve innovations which make society safer and to deploy those solutions worldwide. We are now doing this in more than 25 countries and we are proud of it. Not only do we supply our knowledge and solutions to companies and national governments, but also to NASA and NATO. Towards the east of Europe we are also very busy: in 2012 we made a gigantic hydro-electric plant there a whole lot safer. And in India we are working with our partner to protect critical infrastructures and government's networks. FoxCERT – our incident response team – was travelling at the same time: on the other side of the world ten people resolved a gripping cyberattack.

That is all wonderful, of the smile in the aircraft was caused by something else. In America I was investigating whether the market is ready for FOX-IT, and vice versa. Such a trip always provides excellent learning moments. In the US numerous cybersecurity measures were adopted for the critical infrastructures, multinationals and banks many years ago. In that respect they are certainly a step ahead of us. What is notable about the American approach is that the measures are generally responses to legislation which is by definition lagging, and to past experiences. But cybercrime is a dynamic environment, and so by necessity is fighting it. To take the right decisions about arming yourself against cyberattacks, you have to look ahead. In the Netherlands that is exactly what we are world class in. We have the right knowledge and unique experience. When we deploy this broadly in practice, the Netherlands becomes a forerunner.

Oh yes, that smile. We do in fact have an undercover intelligence team which unearths the most exceptional info about new attackers and hackers. Highly secret, so no-one knows them, I thought... Every cyberboss I met in the US said: 'FOX-IT, oh yes, your intel team always has the best "actionable intel" of the entire scene.' I would never have expected that: famous, thanks to the largest undercover club of FOX-IT ;-)

Menno van der Marel, CEO FOX-IT



COLOPHON

Editorial address

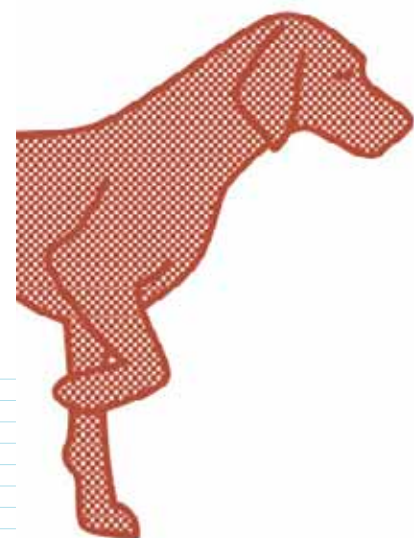
FOX-IT Marketing Department
PO Box 638
2600 AP Delft
+31 (0)15 284 79 99
marketing@fox-it.com
www.fox-it.com

Design

viervier, Rijswijk

Interviews and articles

Sabel Communicatie



04



10



14



20

TOPICAL

04 Monitoring detects cyberthreats

Taking preventive measures against cybercrime is all very well, but it is also necessary to detect digital threats in good time and to prevent worse. Dorifel demonstrated that once more.

PRACTICE

10 Defence experiments

Remote decision-making by commanders requires situational awareness. Which requires high security for networks and data-flows from the field.

MARKET

12 Top Secret

State secrets are secure with the SINA RedFox, developed in a unique international collaboration.

PRACTICE

14 Forensic puzzles

Digital experts work on the most intriguing cases.

OPINION

17 Cyberlegislation on its way

May we hack back as a weapon against cybercrime?

PRACTICE

20 Worth a thousand words

Data visualisation helps to discover links, patterns and incidents in mountains of information.

TRAINING

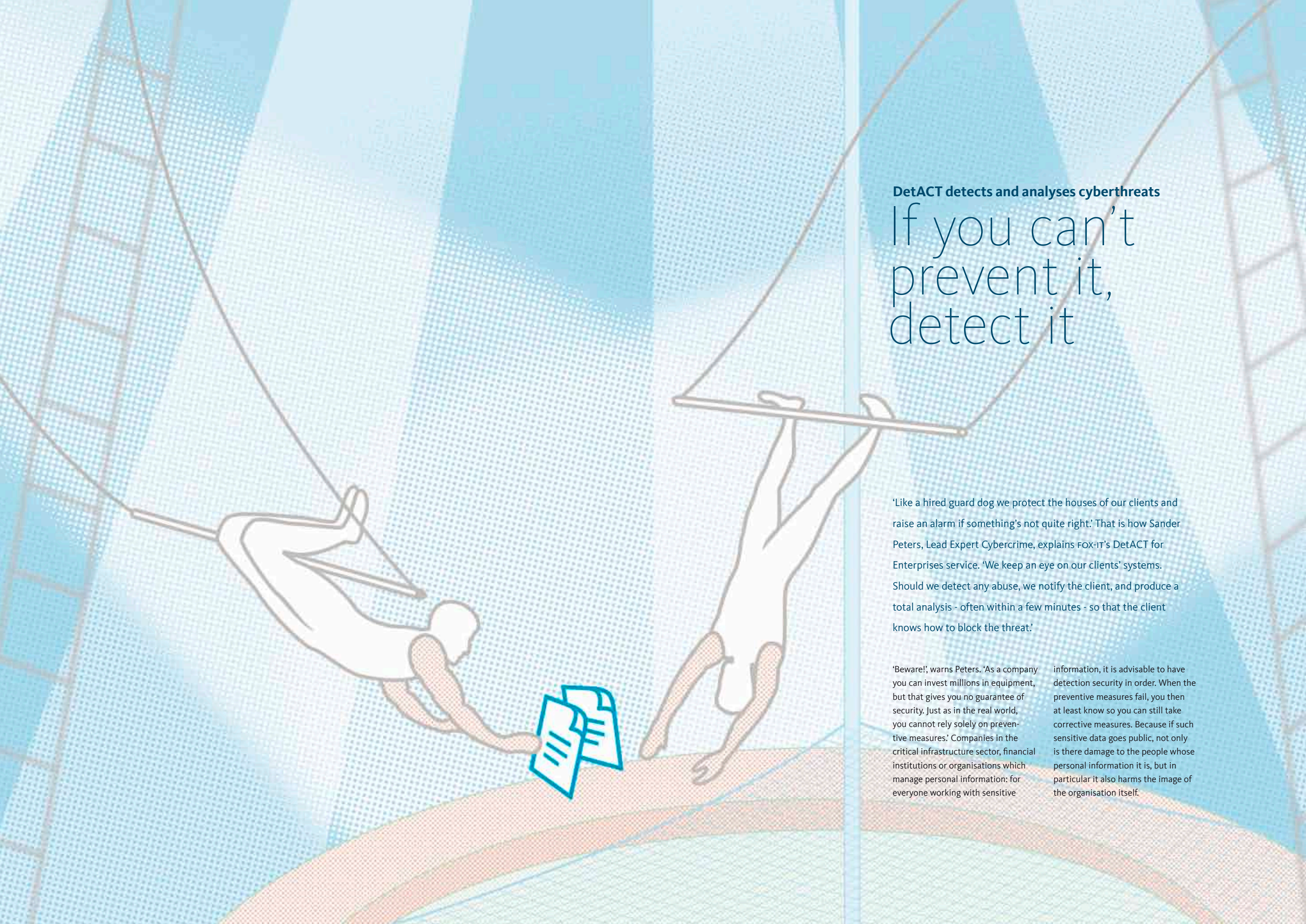
22 To school

The Forensics Summer School was a huge success. And new training courses are in the pipeline.

NEWS

24 Bits

FOX-IT has been selected as one of the best employers in the Netherlands. And is sponsoring the OHM2013 hacker camp and the Hack42 hacker space.

An illustration of two white, stylized figures walking a tightrope. The figure on the left is in a crouched position, holding a small stack of papers. The figure on the right is in a more upright position, balancing on the wire. The background consists of large, curved, blue and green shapes with a halftone dot pattern, suggesting a stylized landscape or sky. The tightrope is a thin, dark line.

DetACT detects and analyses cyberthreats

If you can't prevent it, detect it

'Like a hired guard dog we protect the houses of our clients and raise an alarm if something's not quite right.' That is how Sander Peters, Lead Expert Cybercrime, explains FOX-IT's DetACT for Enterprises service. 'We keep an eye on our clients' systems. Should we detect any abuse, we notify the client, and produce a total analysis - often within a few minutes - so that the client knows how to block the threat.'

'Beware!', warns Peters. 'As a company you can invest millions in equipment, but that gives you no guarantee of security. Just as in the real world, you cannot rely solely on preventive measures.' Companies in the critical infrastructure sector, financial institutions or organisations which manage personal information: for everyone working with sensitive

information, it is advisable to have detection security in order. When the preventive measures fail, you then at least know so you can still take corrective measures. Because if such sensitive data goes public, not only is there damage to the people whose personal information it is, but in particular it also harms the image of the organisation itself.

DORIFEL

Increasingly often instances of cybercrime have hit the headlines in recent months. For example, the Dorifel virus was able to spread harmful software onto thousands of infected computers, and the Dutch news site nu.nl was abused to spread infecting malware. In both instances FOX-IT was able to identify the threat, almost in real time, and to notify the parties concerned. Peters: 'We have been investigating botnets and trojans for banks since 2006. What we learn there we then translate to our DetACT services, which enables us to detect these types of threats automatically.'

Dorifel ended up on networks through the existing communication channels of the banking trojan Citadel which, without people knowing about it, had already installed itself into scores of company networks. 'We had already analysed Citadel in detail many months before. So with DetACT we were already keeping a very close watch on any Citadel-related activities, and clients were notified accordingly so that they could take corrective measures. This enabled us to prevent any outbreak of the Dorifel virus among our clients long before less fortunate organisations started cleaning up.'

realise what the consequences could be, should a drastic security incident occur despite the presence of preventive measures.

'You cannot trust technology entirely, without the human factor. Consider the approach in the physical security world: there too, specialists in control rooms monitor the output from security cameras. Technology does indeed help to track down suspicious activities, but ultimately it's people who assess whether something is a threat or not. Systems work purely with the data they have available; there is no equipment which reports that it has missed something. Because otherwise it would not have missed it! That's what people are needed for, experts who monitor the security process.'

SEPARATING SENSE FROM NONSENSE

A monitoring system which generates daily and hefty generic reports is not effective', concludes Herlaar: 'There's a danger that events which are not really threats, "pollute" the list every day. Eventually, the long list of events is simply not read, at least not on time. That's why human analysis is so valuable and necessary.'

Peters: 'When DetACT generates an alert and our analysts determine that it is not an actual attack, a false positive, then we don't report this to the client unless it is part of a larger attack. So we only report genuinely relevant incidents. Once we have identified an alert as a false positive, we feed this back to our systems so that identical scenarios are automatically flagged as false positives the next time. This so-called "tuning" is an important part of our work and essential to keeping the detection effective.'

With DetACT, FOX-IT offers the digital equivalent of physical detection security like cameras in shopping streets, alarm sensors in shops or burglar alarms in homes. Peters: 'We are the eyes and ears in our client's infrastructure. Among other things we inspect network traffic and log files for suspicious activities which could lead to damage. Once an alert is raised, we conduct a complete analysis. In many cases our client is notified of the extent of the threat within minutes, so they can implement countermeasures. Hacking attempts, data leaks, virus outbreaks, Denial of Service or other cyberthreats can thus be headed off at the pass.'

An important yardstick for the effectiveness of DetACT is the role of the Intelligence department. Here information is collected on the Internet about the threats to our clients. The digital underworld is kept under close watch. For instance, our experts deliberately let systems get infected in a controlled environment to

T-Mobile: 'The entire world depends on our network''

T-Mobile Nederland outsources the monitoring of its network to FOX-IT. Ton van Ginkel, Manager Security and Compliance Management: 'T-Mobile is a major communications company where telephone traffic has not been the only focus for a long time. Through our networks clients access websites, they communicate through Facebook, they have Twitter accounts... Almost five million people, all connected to us, so that

ultimately links the entire world to our network. You can't take any risks with this. No matter how good our preventive measures are, one small fault can let a hacker in. Naturally we can do our own monitoring – we're big enough for that. But the advantage of outsourcing is that FOX-IT can deploy the knowledge they have discovered at other firms, for us. When for example the monitoring service identified the infection at nu.nl and FOX-IT immediately notified all its clients, our damage was limited to just thirty workstations.'

KNOWLEDGE EXCHANGE

During one of the regular security meetings, in which the so-called feedback

loop is a vital part, FOX-IT and T-Mobile exchanged recently acquired knowledge and there were enthusiastic discussions. Van Ginkel: 'There is a dual advantage to this knowledge exchange. Through FOX-IT's experiences we learn for example how we need to modify our organisation to limit any damage. On the other hand they learn from us: because there is so much traffic on our network, the FOX-IT monitoring staff can use the knowledge they glean from us about threats, for their other clients.'

A monitoring system which generates daily and hefty generic reports is not effective.

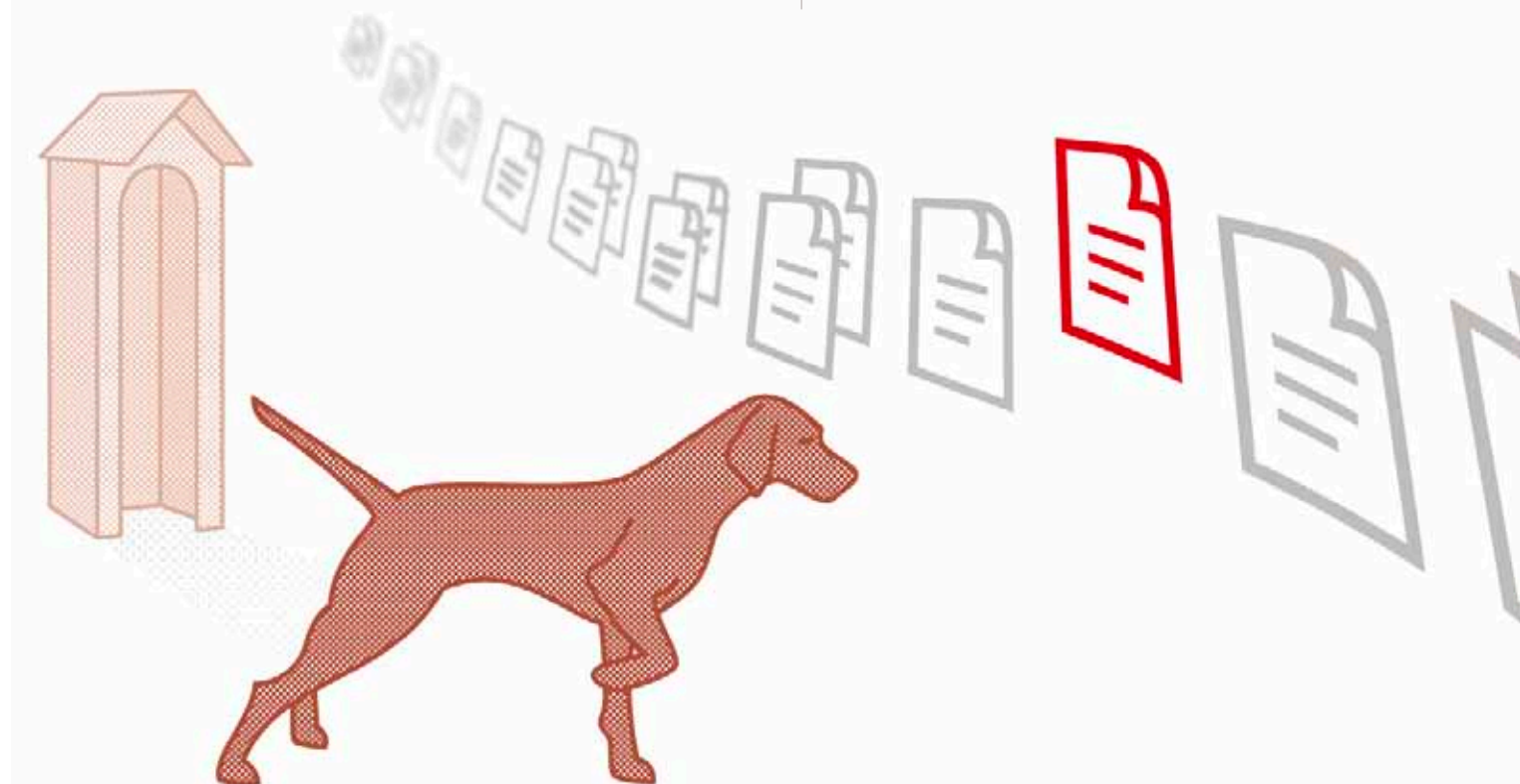
24/7

Analysis is a labour-intensive process with which FOX-IT's cybercrime fighters are permanently occupied. Peters: 'You can't blame organisation specialists for not investing as much time in this as we do, because it's not their primary task. They also don't have the benefits of scale which we do. That's why it's so important that companies working with sensitive information assign monitoring to a specialist party which does this 24/7.'

HUMAN INTERPRETATION OF SIGNALS

'Just look around you,' notes colleague Jeroen Herlaar, Business Unit Manager Cybercrime with FOX-IT. 'Increasing numbers of companies and organisations appear to have the security of their infrastructure not in order. Most of them are aware of the dangers and want to invest in security, but they often allocate their security budgets inefficiently. The major question is whether companies

Monitoring is a crucial
part of forensic readiness



investigate how specific malware works and how its presence in infrastructures can be detected. This knowledge is then implemented in DetACT to enable detection amongst our clients.

DETECT WHAT YOU CANNOT AVOID

To implement good security measures, it is customary to conduct a risk analysis. The threat then becomes apparent as do the most important measures to take against it. Often these are in accordance with best practices from the industry. These measures keep the bestknown threats at bay.

What makes matters much more difficult is when you do not exactly know what threats are involved so that you cannot determine what preventive measures you need to

take. Then it is sensible to at least be ready for the moment you are faced with an incident. Herlaar: 'Monitoring is a crucial part of forensic readiness; ensuring that you are ready for an incident and that you can investigate directly rather than searching.'

LEARNING FROM INCIDENTS

'We are an independent external party not influenced by the interests of an internal IT organisation or an external IT supplier,' emphasises Peters. 'We assess security incidents independently and on the facts. Ultimately this delivers the greatest value to our clients. We also monitor many different types of environment and we apply the lessons learned from one environment to others. During the regular security meetings we communicate our findings and actions back to the client. Practical solutions

are discussed to prevent certain incidents in the future, so that the intrinsic security level of the client's environment improves. Conversely, the client tells us of his experiences. We really learn a lot from each other during such discussions!' ▼

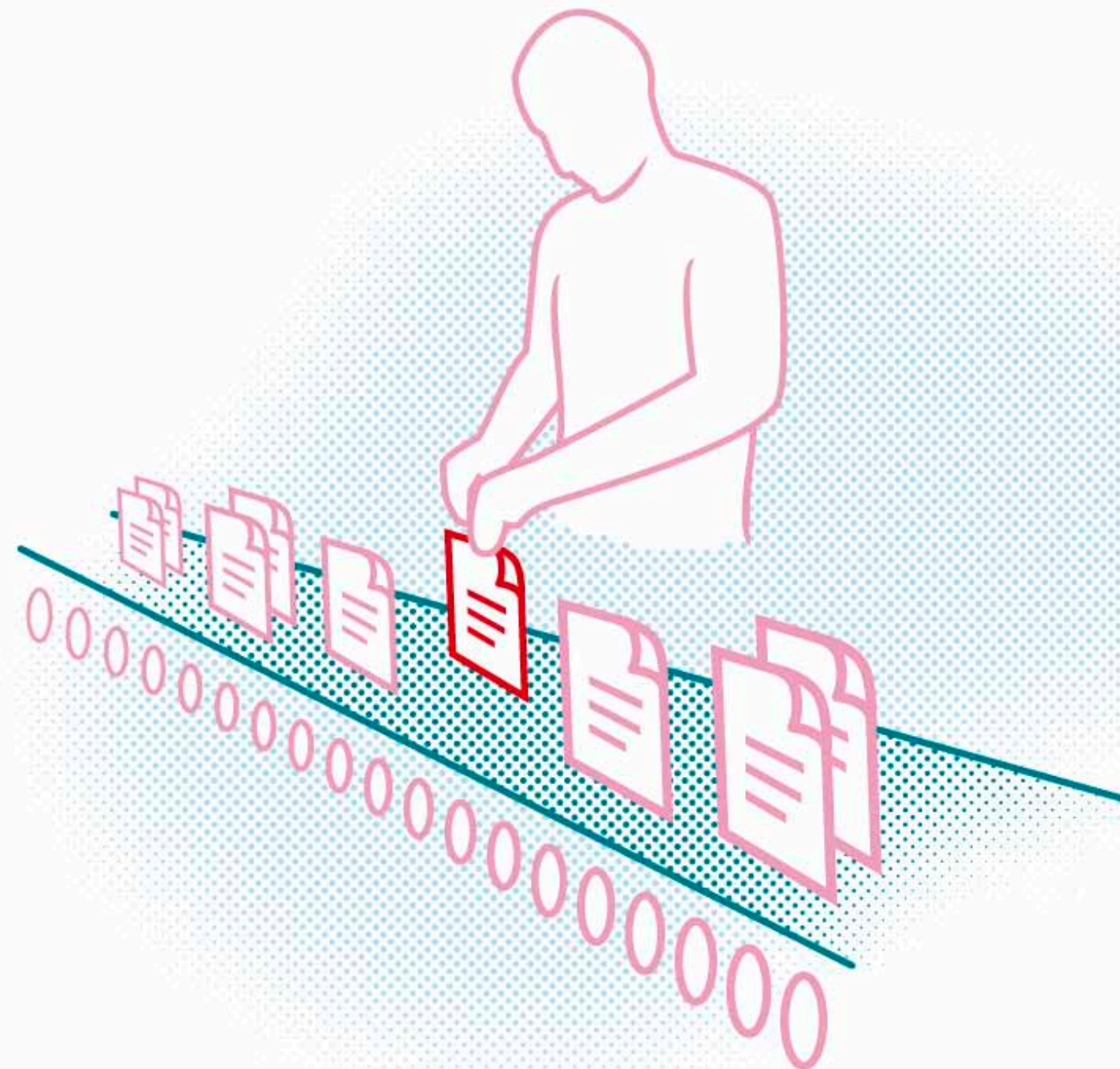
MALWARE QUICKLY DETECTED ON NU.NL

In March this year a hacker placed a link to an exploit kit on an adserver which shows advertising on the Dutch news site nu.nl. This exploit kit detected whether the website visitor's computer was vulnerable enough to have malware placed on it. If so, the malware was then transferred.

Peters: 'That entire process, the infection of vulnerable systems, occurred on the networks of clients we monitor. Within five minutes the dash boards of our Security Operation Center (SOC) lit up like a Christmas tree. Because

so many events were happening, colleagues were told to drop everything they were doing to reinforce our on-duty monitoring team.

'Within five minutes we had analysed a few of the incidents, all of them leading back to nu.nl, reported the hack to nu.nl, immediately notified our infected clients and warned all our other clients and then – once nu.nl was notified – we placed a warning on Twitter.' FOX-IT was the first to identify the infection and was thus partly responsible for minimising a large-scale and full infection among our clients, as well as in the rest of the Netherlands.



MORE THAN JUST

SIGNATURE-BASED DETECTION

With DetACT for Enterprises, FOX-IT does not restrict itself to just one technology, but detects the three M's (misuse, misconfiguration and misbehaviour) in a variety of ways:

Signature-based
Heuristic
Blacklisting

Not only network traffic is studied, but also log files and activity on workstations, for instance.

DIFFERENT VARIANTS OF DETACT

DetACT is the collective name for the services from FOX-IT where the emphasis is on detection. DetACT stands for Detection of Active Cyber Threats. This article considers the DetACT for Enterprises service. This service keeps an eye on networks, log files and IT environment hosts within an organisation, and sounds the alarm should there be security incidents. With DetACT for Online Banking, online banking traffic is inspected for fraud. DetACT for Critical Infrastructure maintains a watch over the specific SCADA networks of power stations and other industrial networks.

For more information about DetACT visit fox-it.com or call our Cybercrime account managers on +31(0)15 284 79 99

Defence: experimenting in major Peregrine Sword exercise

Situational awareness important in command post



Precise operational information is essential for Defence. It is the basis for commanders to be able to take better decisions. During the Peregrine Sword exercise of the first German-Dutch army corps in September, improved information exchange technology was tested within the 11 Airborne Brigade (11 LMB), with a major role for the Fox DataDiode and SkyTale.

Some six thousand people from a variety of NATO countries participated in Peregrine Sword from 13 to 27 September in Germany. In essence this was a so-called validation exercise for 11 LMB. The supporting Purple NECtar experimental platform was constructed for optimum information exchange within 11 LMB. Innovation in technologies and networks offers new possibilities, which Defence is testing in exercises like Peregrine Sword. One of the objectives this year was to obtain a better 'situational awareness': the best possible insight into the current situation 'in the field'. After all, command posts always work with limited information from operational units. By improving this information provision, commanders acquire a better picture of the situation and – remotely from the command post – they can take better decisions.

DEPLOYMENT OF FOX DATADIODE

An example is the use of blue force tracking: around 250 people, vehicles and helicopters were equipped with GPS trackers the size of a smartphone. Thanks to this device the command post could see all the units on a digital map. FOX-IT's DataDiode was also deployed here. This is a data valve which guarantees that information can only flow in one direction. The product has a Common Criteria EAL7+ certificate and the AIVD (Dutch General Intelligence and Security Service) has approved it up to and including the SECRET classification level. NATO has accepted the Fox DataDiode for use up to the NATO SECRET level. Lieutenant-colonel and senior operational architect Duco Brongers: 'The Fox DataDiode was chosen because it's the only accredited tool with which information can flow from unclassified sources to the "secret" level. The information from the trackers comes into our secret command network through the Internet. The web cannot be trusted, and of course we do not want information from our secret network within the command post to go back to the Internet. The DataDiode prevents this.' Defence has amassed considerable experience with the Fox DataDiode and is very satisfied with it, according to Brongers.

ENCRYPTING RECONNAISSANCE IMAGES

For a different experiment called sensor-to-effector, two Fennek reconnaissance vehicles were equipped with sensors like infra-red cameras. The Fenneks could also place separate sensors like cameras and radars out in the field. 'The information from these sensors formerly stayed in the vehicle. Or it was brought back to the command post indirectly and with considerable delay, for example by a batman,' explained lieutenant-colonel and project leader Siegmund van Iwaarden. 'In our test we forwarded the information directly to the command post. With virtually real-time photos from the field, the commander could make a better assessment of the situation.'

'PLE [SkyTale] was chosen because it requires little to no overhead, thus little bandwidth, and the quality of service is extremely convenient.' Siegmund van Iwaarden, Defensie

MAINTAINING SECRECY

Because such operational information has a secrecy status, it is necessary to apply state-of-the-art encryption to the data. FOX-IT's SkyTale was deployed for this – a robust hardware IP-crypto solution for information at the NATO and national confidential level. SkyTale was developed for use in MANETs (mobile ad hoc networks) and combines an optimised network protocol and high network performance with extremely low overhead and multicast support. Because both IPv4 and IPv6 are supported, SkyTale can be integrated in existing systems largely without reconfiguration.

Defence uses SkyTale under the name Payload Encryptor (PLE), in combination with an ad-hoc router. 'We use the encryptor on both sides of the connection with the reconnaissance vehicles,' explains Van Iwaarden. 'With the special ad-hoc router on board the armoured vehicles, you can choose which communication channels you use, for example the one with the fastest transfer. One of the Fenneks also had a SatCom on board; the second vehicle could make use of it via Wi-Fi.'

INNOVATION SPEARHEAD

Defence's intention is to continue with experiments as in Purple NECtar. Innovation is also one of the Defence leadership's spearheads. 'Here Purple NECtar offers an excellent platform to achieve pragmatic solutions together with all the sections of the armed forces, public order and security, and along with the commercial world,' says Duco Brongers. 'Converting a successful experiment into implementation certainly bears challenges, but these can also be resolved if we put our heads together.'





State secrets secure with SINA RedFox

For years FOX-IT has been protecting the state secrets of the Dutch government with its own products and those of others, such as the SINA products from the German company secunet. With the self-developed RedFox and the integration of this encryption module in SINA, FOX-IT and secunet together are taking the lead for the security of state secrets at the very highest level. A unique instance of collaboration between two countries.

An international collaboration at the highest level has always been 'a bridge too far'. Countries prefer to develop their own encryption products. 'Here we're talking about securing state secrets, and the national interest is extremely high,' explains Ronald Westerlaken, Product Manager with FOX-IT. 'Espionage by other countries lies in wait and thus constitutes a very serious risk. Certainly because these countries will invest a great deal of time and money in accessing the highly secret information. Historically, countries would prefer to work independently on this type of product. In an industry based entirely on trust, collaboration is difficult.'

EUROPEAN COLLABORATION

This changed in Europe thanks to the so-called 'second country evaluations'; security bodies from different countries check one another's encryption products. 'This certainly helped to improve mutual trust,' says Martijn Verschoor, Lead Developer at

FOX-IT. 'But things can and should go a step further. Now for the first time there has been a combined development of a new product at this level, by FOX-IT and secunet. It is exceptional that both countries have dared to be so open with each other. At the same time, the development of SINA RedFox closely meets the desire within the EU to create a European encryption industry.'

COLLABORATING ON BETTER PRODUCTS

The first good step has been taken with the SINA RedFox, but further 'pan-European' collaboration is needed. Verschoor: 'Alongside integrating products, countries will also develop entirely new products, in which they will combine budgets and development capacities. This will lead to products which are more appropriate for the increasingly demanding requirements of the clients, and which can be brought to market more quickly.'

SINA BECOMES SINA REDFOX

The summer of 2013 will see the first combined product appearing in the market from FOX-IT and secunet, the SINA RedFox Box – a further integration in the entire SINA line is possible. At its encryption heart this VPN box has the RedFox from FOX-IT (see the other sidebar) making it possible to link state secret networks via the Internet. Secret networks in the Netherlands will thus become SINA RedFox networks. Alongside the secret networks of the Netherlands, it is also suitable for securing European and NATO networks. For other networks, a special variant of the RedFox has been developed which may be deployed worldwide.

WHAT SINA REDFOX OFFERS

The most recent status of the technology has been incorporated into the RedFox. It meets the Dutch and

European requirements for the State Secret SECRET classification level. For the deployment of the SINA RedFox this means better protection, performance and simpler physical transportation compared to other products in the market. Westerlaken: 'We achieved this latter feature through a so-called declassification token; the box without a token can be transported without any special measures.' SINA RedFox is also based on the most recent version of the SINA software, so that clients can benefit from the latest features.

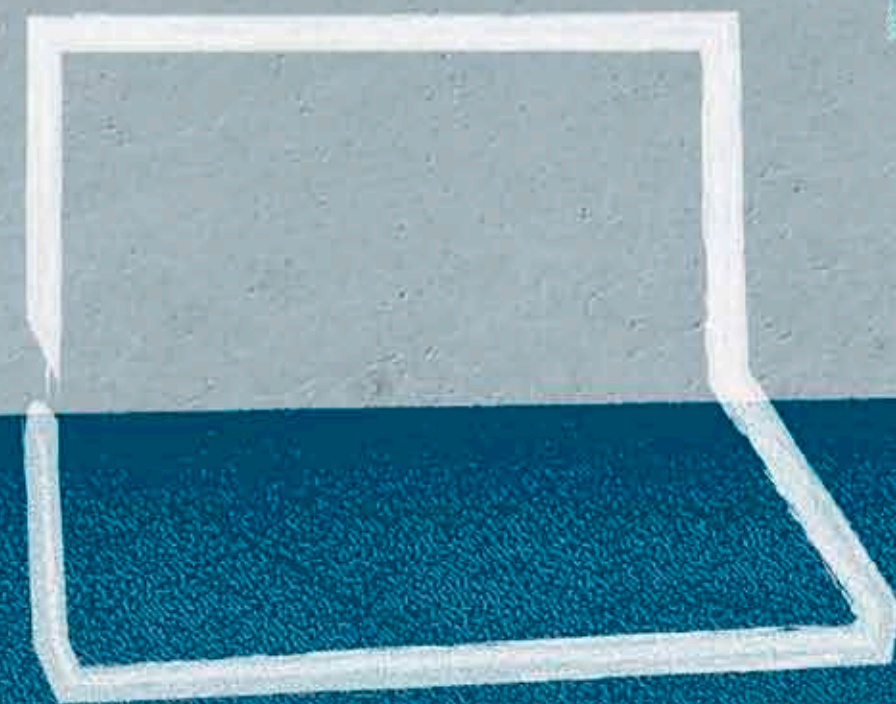
Organisations which already use SINA can easily upgrade this to SINA RedFox in a step by step procedure.

FURTHER INFORMATION

Ronald Westerlaken, Product Manager, westerlaken@fox-it.com
+31 (0)15 284 79 99

REDFOX

The FOX-IT RedFox module, also known as Mystique, is a hardware encryption module developed in close cooperation with the Dutch government, to secure information at secret level. The RedFox is the successor to the current generation of encryption chips and offers a higher degree of security and high performance. The module can be deployed for securing Dutch, EU and NATO secrets and is a building block which is eminently suitable for integration within other products. This makes it relatively easy to develop high-end security products, such as VPN solutions (for example SINA RedFox), harddisk encryption and hardware security modules (HSMs).



2



Forensic puzzles

Are you also an NCIS fan? And are you intrigued by Abby Sciuto's digital skills. The lives of FOX-IT's forensic experts sometimes seem very similar. Here is a glimpse at three cases.

1
CASE

MANIPULATION WITH GOOGLE ADWORDS

From abroad, an employee of a webshop googles his own company name and discovers a Google Adwords advert which looks a little different than normal. The advert leads to his webshop via an intermediary. That is strange, because the company runs its AdWords campaign directly. The intermediary has indeed been commissioned to generate extra clicks to the website, but in terms of

the agreement it may not use any AdWords for this. The affiliate is paid per click. Things become even odder when it turns out that colleagues back in the office can't reproduce the suspicious ad, but get to see their own, correct, advertisement.

FOX-IT investigates what is going on. With Google AdWords you can deploy advertisements exclusively for specific regions, and whoever pays the highest price gets his advert at the top of the Google page. The FOX-IT experts only have access to the webshop's log files, and analyse them thoroughly. Using a so-called 'heatmap', they chart just when the clicks to the webshop occur and where they come from. It becomes clear that the AdWords campaign is being manipulated. By day – when most of the traffic to the webshop occurs – most clicks

via Google AdWords originate from the company's region. But outside the region the webshop's visitors arrive via the intermediary. Outside office hours the hits come from the whole of the Netherlands via Google AdWords.

It appears that the intermediary – in contravention of the agreement – has offered more for the same search terms than the webshop itself and has created an almost look-alike advert to show up. In this way the intermediary hijacked the ad-campaign of the webshop and made them pay a higher price per click than Google would have charged them. To this end every effort was made to avoid discovery; the timing indicates that employees should not chance across the false advertisement from the office by day, or in the evenings from home. FOX-IT's investigation paved the way for further investigation.

2
CASE

DATABASE GOES PUBLIC

Friday evening 9 o'clock, Foxers are barbecuing and the emergency phone rings. The manager of a webshop reveals in panic that a database with client details may have been offered to a competitor. That alone would be bad enough, but the uncertainty of the situation makes it worse: was the company hacked from outside, or is one of their own employees channelling out company secrets? Who is it and what is the scope? Speed is needed. Tracks must not be erased and on Monday morning all the staff must be able to use a fully functioning company network again.

Saturday morning, a team of five Foxers turns up at the company's doorstep. First they draw up all the possible scenarios in which the database might have left the

premises. They compile an inventory of the entire network and investigate the database for digital tracks. The experts use a combination of standard forensic tools like FTK and Encase, and they write supplementary software on-site. At the same time the e-mail and FTP servers are secured and investigated.

It quickly becomes clear that the company has not been hacked. The experts find the leaked database and discover that the dataset originates from a test database, which was accidentally filled with production data. It is accessible to everyone within the company. All the local machines are searched for traces of this database. The investigation is completed on Sunday evening; all the traces are secured, and the company can take further steps with the results.

3 SEARCHING IN AUDIO FILES

New facts come to light in an investigation. It is important to know whether certain keywords also occur in audio recordings. During the investiga-

tion hundreds of hours of conversations were recorded, of which only a very small proportion have been transcribed literally. Because the new keywords were not sought in this, all audio recordings have to be listened to again. There is a need for speed, so FOX-IT is asked to find an automated way to search for the keywords.

An interesting challenge, because at the beginning of the investigation FOX-IT was not familiar with searching in audio files. So FOX-IT drafts in extra expertise in the form of a Dutch company which specialises in audio mining. This technology uses fuzzy matching. The technique does not produce grammatically correct transcriptions, but does recognise sounds and patterns based on a phonetic dictionary and applies them to a word. The object is to find as many keywords as possible.

First FOX-IT tests this technology. A random test shows with 95% certainty that the audio-mining software will find between 70% and 80% of the keywords. This result is good enough to get started on 25 GB of

recorded material. Within two and a half days the software has 'cut out' around 20 thousand recognised fragments and these have been listened to by people. Ultimately around fifty recognitions turn out to be correct. The total investigation by FOX-IT takes fourteen days; with the experience and techniques acquired, comparable research could be completed in a few days in future.

If all the recordings had been listened to by people, the investigation would have taken at least forty days. Certainly people are always better at recognising words than machines, but listening endlessly to conversations for multiple keywords increases the chance of omissions.

Alongside the time savings, this audio-mining technique also has the advantage of being able to integrate the output of the audio recordings with the output of Internet taps, for instance. Searching for keywords could then occur in both the Internet data and the audio of the tapped conversations or VOIP traffic. ▼

Dutch government produces cyberlegislation

Are we allowed to fight back?

Hacking back as a weapon against cybercrime is not permitted without a legal basis.

It certainly does work, if it is used in the right conditions and only as an extreme measure, to protect citizens against cybercriminals. Now is the right time for politicians to map out problems and solutions in cyberspace and to move towards an 'admiralty law' for the Internet, believes FOX-IT CEO Ronald Prins. Here is his opinion.

Since the appointment of Minister Ivo Opstelten of Security and Justice in 2010, the services responsible for tracking down and prosecuting cybercrime have been exerting pressure to obtain more powers to tackle foreign Internet criminals. Now, exactly two years later, the currently demissionary minister has announced in a letter to the Lower House that cyberlegislation is on its way.¹ At FOX-IT we are anticipating this new law with interest. Because although we often know where to find the foreign servers used in cyberattacks, we can do nothing without a legal basis. The Netherlands experiences considerable trouble because of cybercrime. The current arrangements for tackling this growing form of crime are limited and not effective enough to stop the criminals and protect the citizens. By definition, the Internet is an area which is separate from national boundaries and we also need to keep it that way. But this should not mean that punishable offences may be perpetrated without consequences. After all, the victims are real people, suffering actual damage,

and not virtual figures in a virtual world. Legislation, comparable to the international admiralty law, will help to protect citizens and make cybercrime less attractive to perpetrators.

WAITING FOR COLLABORATION

The Bredolab botnet, 2010: through the servers of a company in the Netherlands, some 30 million infected computers were controlled by a criminal from abroad. The Dutch police were able to bring this botnet to a halt by breaking into the Dutch servers, and using the functionality of the botnet itself to clean up the infected computers.

Things were different during the recent outbreak of the Dorifel virus; the suspects could not be apprehended directly. The reason: the police did not have the authority to break into the foreign computers of the cybercriminals, to collect evidence and to render the command and control servers harmless.

¹The minister's bill had not yet been revealed as this edition was going to press. The formation of a new cabinet was also underway.



Striking back immediately
if there is a cyberattack
against national security

With more powers to counteract the acute threat posed by the Dorifel virus by taking it offline, the police would have been able to achieve this within a few hours. At the moment, stopping new infections requires days. As a society we think it is unacceptable that municipalities, companies and government agencies can no longer work because the Dorifel virus was able to continue spreading. All this happened simply because a hosting provider abroad would not cooperate directly in resolving the problem.

A request to a foreign country can take weeks if not months, and that's just one step in the investigation. Information is often already gone because any random party in any random country can institute a notice and takedown, or because the criminal himself has erased his tracks. The data on a server is increasingly stored encrypted, so that a copy of a server has little or no value. Certainly the details of what information the perpetrator has stolen and what may have been used or abused are only available on the attacker's systems. Tracks pointing to the perpetrator can often only be retrieved by breaking into his infrastructure.

Minister Opstelten acknowledges the need for new rules for cross-border fighting and preventing cybercrime. He also confirms that legislation and international agreements are lagging. So it's good to note that the previous cabinet wanted to strengthen collaboration with countries which are at the forefront in cybersecurity. These include a number of European countries, the United States, Australia and in Asia, for example, Singapore. However, concrete solutions are not yet in sight. That's perhaps not all that odd if you consider the sensitivity of the principle of national sovereignty in some nations. Because how could we even

consider dabbling in computers situated in other countries?

I believe the fear is rooted in just how you view the Internet and its boundaries. If a server is located in Ukraine, focuses only on Dutch victims, solely has an impact in the Netherlands and can be accessed from the Netherlands, then the Dutch judiciary has more say on it than the country which just happens to provide the electricity for the server. This is certainly an issue you need to consider carefully for each incident. If what's involved, for instance, is a hacked server of a respectable Ukrainian company, then you have to be a lot more careful in your dealings. In such a case there's even a good chance that after calling, the company immediately takes the server down.

Conversely, should we tolerate that foreign police services be allowed to search computers in the Netherlands? This would be a logical consequence. If, for example, what's involved is a rented virtual private server at around 20 euros a month, rented by an Eastern European criminal organisation, then it makes sense that the other country conducts the investigation independently. Certainly it would be ideal if at least a notification was sent to the authorities, that an online "house search" is taking place.

REQUESTING LEGAL ASSISTANCE

At issue are powers which apply not just for the Netherlands, but which also offer the scope to access "non-identifiable" computers abroad. The Netherlands is the first country which wishes to provide this so explicitly and extensively through legislation. Why is being able to hack back so important? Because many digital offences only leave digital traces behind. So you need to be able

"to search past the Internet" to eventually establish a real identity and to be able to apprehend a suspect. If it's a Dutch trace we can achieve a great deal. But as soon as a row of linked proxy servers is involved which eventually terminates in Ukraine for example, that's when you will certainly need several weeks of working with requests for legal assistance.

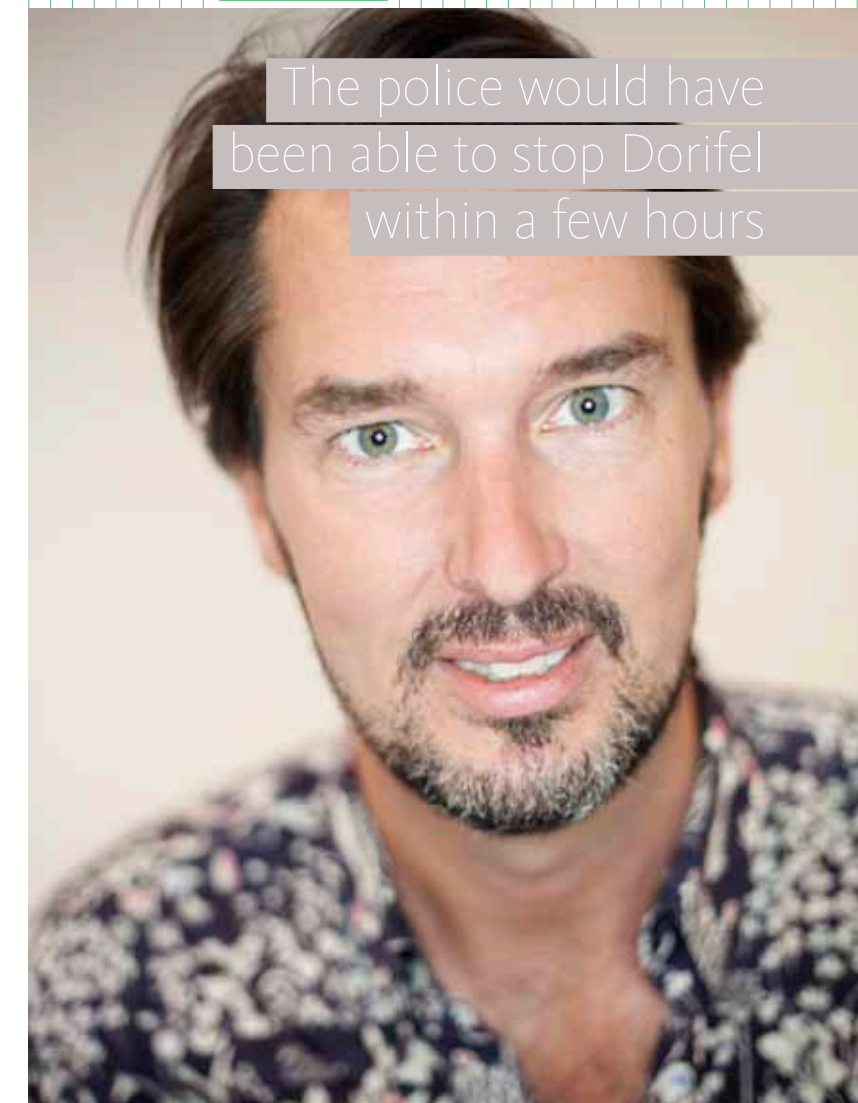
Should there be an attack on national security, for example on the critical infrastructures in the Netherlands, I believe that it is sometimes necessary to "hack back" without the permission of foreign authorities.

NO ROUGH REMEDIES

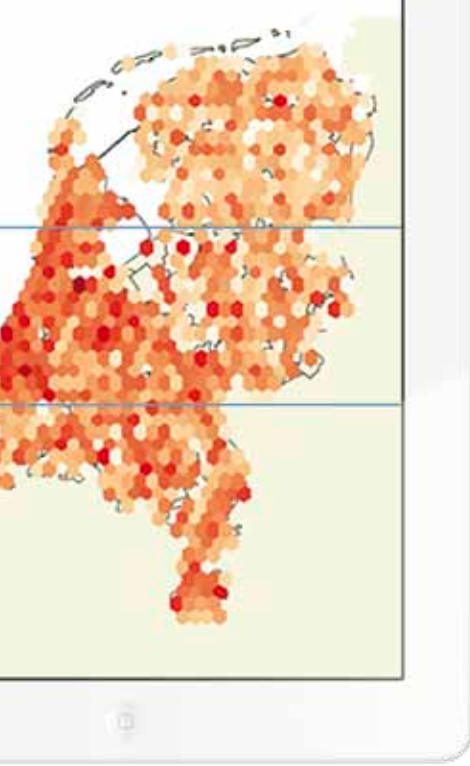
I realise that this is a very exceptional power. Violating privacy and violating the sovereignty of other countries are both matters of concern. Therefore I also hope that good account of this matter will be taken in definitively framing the law. In my opinion, the police should not simply be able to deploy this rough remedy for every investigation where it might appear to be "useful". It may only be deployed after consideration that less drastic measures really do not work, and that there is the necessity for rapid intervention.

It should be possible, after all, to reach agreements on fighting cybercrime in an international context. Compare it to the international admiralty law: if a Dutch ship is attacked in international waters, our navy goes into action. This should also be the case in international Internet territories. ▼

Ronald Prins
CEO FOX-IT



The police would have
been able to stop Dorifel
within a few hours



Data visualisation helps with analysing information

A PICTURE IS WORTH A THOUSAND WORDS

Data traffic volumes are increasing. With large volumes of information it is difficult to establish links and patterns. Digital forensic investigation deploys data visualisation during the analysis and to clarify the result. But beware: do not lose sight of the context.

The exponential increase in data has brought a greater need for visualisation. This helps people to understand substantial quantities of complex data better. Data visualisation is an interdisciplinary field between graphic design, informatics and knowledge theory. Digital forensic researchers use it in a variety of ways, for example as an analysis aid during an investigation, or as an end-product to clarify investigation results.

DATA VISUALISATION AS AN END-PRODUCT

Within IT, data visualisation frequently appears as an end-product in network monitoring and various software packages for system management. A good example of this is the Daedalus system from the Japanese National Institute of Information and Communica-

tions Technology. The system charts the real-time traffic of a variety of networks and visualises it three-dimensionally. In this way network administrators can quickly see where unusual activities are occurring in the network.

A TOOL FOR FORENSIC ANALYSIS

Data visualisation is a welcome addition to digital forensic investigations. It helps the reader to understand a complex problem. In many instances, for example, a digital forensic investigator may be reviewing various log files. Consider a bank's transaction data, or websites which someone concerned may have visited. Reading these log files from top to bottom (one-dimensional analysis) often offers little solace. The investigator's interests lie in recognising

patterns, because it is on this basis that he can identify individual incidents more easily. To this end he poses several essential questions, such as: On which days do we see an increase in the number of login attempts after six o'clock in the evening? Have the skimmed payment cards been used at precisely the same location during a specific day? In which countries do we note an increase in payment activities after the moment of skimming?

Each of these questions requires a multidimensional approach. Data visualisation offers this, and converts data into histograms, line graphs, pie charts, motion charts, geo charts or heat maps, for instance, each revealing patterns. By layering datasets over each other, you can zoom deeper into a problem.

DO NOT OVERLOOK THE CONTEXT

Data visualisation needs context. This may take the form of an accompanying text, reproducing the variables which have been omitted from consideration, or choosing the appropriate time periods during which the incident occurs. Reproducing visualisations without context is asking for faulty interpretations and thus faulty decisions, sometimes with far-reaching consequences. ▼

Krijn de Mik, Forensic IT Expert

DIY TOOLS FOR DATA VISUALISATION

TOOL	ADVANTAGES AND DISADVANTAGES
Microsoft Excel	Flexible, with various visualisation abilities. A limiting factor is that the log may only be a maximum of 1 million lines.
Google Code Playground	Many new visualisation abilities. Lots of manual work. More suitable for the end result than as an analysis tool.
Google Fusion	Advantages are Google's computing power and the possibility of using data shared by others for your analysis. A disadvantage is that possibly confidential data ends up on a Google server.
D3.js Prefuse InfoVis	All three tools offer very many fine visualisation abilities. They do however require programming/scripting experience.

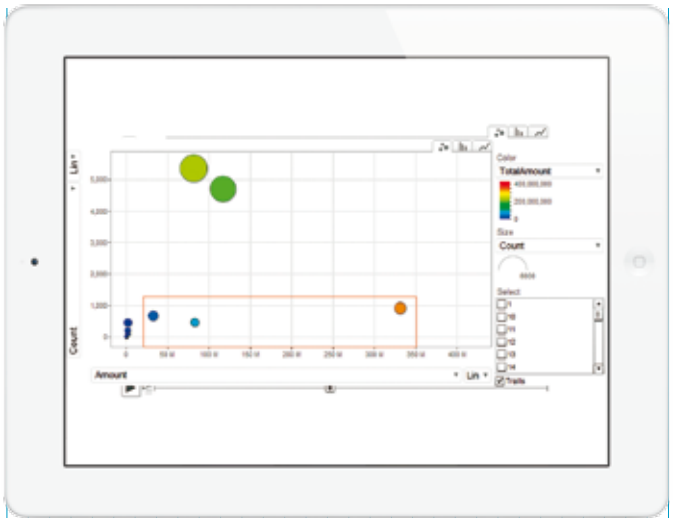
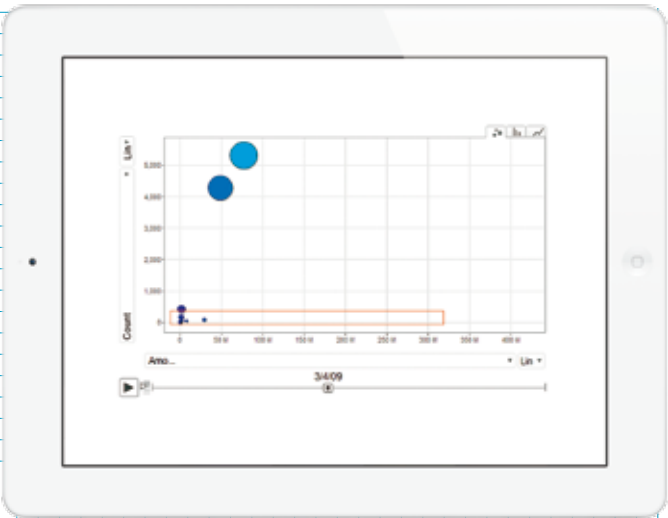
CASE: SKIMMERS IDENTIFIED

A bank notices an increase in fraudulent transactions. The payment cards linked to the accounts have been skimmed. The assignment for the digital forensic investigator is to identify the four different phases of skimming: skimming, distribution, quality (balance) check and cashing out.

The accompanying illustrations are an example of a motion chart, from which one can deduce the country in which the 'quality' of the skimmed cards has been tested and where the money has been withdrawn. In the visualisation, each dot represents a country. The Y axis indicates the number of transactions which have been carried out with the skimmed payment cards. The X axis indicates the associated overall amount of money which has been

withdrawn. Criminals first check the balances of the skimmed cards to learn how much money can be withdrawn and the category into which the card falls in the black market. These checks can be identified in the transaction log files as a zero transaction, because no money is withdrawn.

By comparing the details above against the time, and then running the motion chart, the animation very quickly shows the countries in which major shifts occurred. The three red-boxed dots indicate the countries which rapidly 'overtake' the other countries bottom-left. This indicates a huge increase in transactions and cash withdrawals. It is also highly probable that these are the three countries where balance checks were conducted and the money was withdrawn.



Training

NEW TRAINING COURSES CONTINUALLY EVOLVING

FOX-IT has incorporated a number of new training courses into the programme. Additionally, last summer the highly popular Forensics Summer School was organised for the first time.

RUSH FOR THE FORENSICS SUMMER SCHOOL
FOX-IT organised the Forensics Summer School from 27 to 31 August 2012. For a whole week there were two workshops daily on an aspect of digital forensic investigation, conducted by a **FOX-IT** expert. In total 73 participants followed one or more workshops. Students were able to take part at a special rate.

'This was a wonderful method for extra training,' recalls Renny ter Veer of Waterleiding Maatschappij Drenthe. 'Many aspects were covered in a short time and I have refreshed my knowledge well again.' Student Sander Swuste (Open University) was also an enthusiastic participant: 'The workshops were a good way of meeting **FOX-IT**'s professionals and things were put together very well.'



SEARCHING IN RELATIONAL DATABASES – NEW!

Traces in databases are extremely important for investigation teams. To avoid confiscating whole servers and thus restricting the use of other databases hosted on them, the FIOD (Dutch Fiscal Information and Investigation Service) and **FOX-IT** worked together on finding a solution. The customised training session 'Digital forensic investigation in relational databases' was developed, highlighting advanced technologies to secure, analyse and report data, and thereby making an important contribution to a larger investigation into data leaks, for example. The training course is now also offered as a regular three-day training session, and is on the programme for 19 to 21 November. Among the target groups are digital investigators with government services and fraud investigators for banks and insurers. 'This is an excellent course which fitted well with our practice,' recalls Bert Ooms (IT auditor, FIOD). 'We gained a lot of practical knowledge from the extremely good lecturer who had a lot of expert knowledge and provided clear explanations.'

DIGITAL FORENSICS ACADEMY – NEW!

Do you actually have enough digital forensic experts in-house? How do you ensure that new employees, without experience in digital forensic investigation, quickly learn the tools of the trade? **FOX-IT** is offering a complete Digital Forensics course to this end, which will get your employee ready for the real work in six weeks.

MASTER CLASS MOBILE DEVICE MALWARE & INVESTIGATION – NEW!

Mobile devices and malware are becoming increasingly important within digital investigations. Problems are often the various types of devices and their operating systems. During the Mobile Device Malware & Investigation training course, intended for digital investigators with both the government and the commercial sector, attention is devoted to the most common operating systems such as iOS and Android. Participants learn to analyse malware themselves, and to investigate a mobile device. The next master class is planned for 30 and 31 January 2013.

INVESTIGATING VIA SOCIAL MEDIA – NEW!

The use of social media is now an integral part of our daily lives. It is also becoming increasingly important for investigations and law enforcement. Social media can deliver a good indication of where people are, what they are doing and with whom. A recent example of this is Project X in Haren (NL). To learn how you can use social media in an investigation, from 14 November 2012 **FOX-IT** will be offering a one-day in-depth training on tracking via social media.

CISSP® PREPARATION COURSE – NEW!

For professionals with at least five years of work experience in IT security, **FOX-IT** will be offering training for CISSP – Certified Information Systems Security Professional - in 2013. For more information see fox-it.com

TRAINING CALENDAR 2012/2013

14 Nov	ROI Social Media – NEW!
19-21 Nov	DFO Relational Databases - NEW!
26-30 Nov	DFO Basic
10-11 Dec	ROI Continued
12-14 Dec	iRN part 2
17-20 Dec	ROI Basic
15-16 Jan	Online Facts Research for Lawyers
22 Jan	ROI Social Media – NEW!
24 Jan	ROI Search Strategies – NEW!
30-31 Jan	Masterclass Mobile Device Malware & Investigation – NEW!
6-8 Feb	DFO Relational Databases – NEW!
13-14 Feb	DFO Essentials - NEW!
26 Feb-23 Apr	CISSP® preparation course (1 day per week) – NEW!
6-7 Mar	ROI Basic (day 1 and 2)
11-15 Mar	DFO Basic
21-22 Mar	ROI Basic (day 3 and 4)
27-28 Mar	iRN part 1
29-31 May	iRN part 2

GLOSSARY OF DUTCH ACRONYMS

iRN	Internet Research Network
ROI	Investigation on the Internet
DFO	Digital Forensic Investigation
More info on	www.fox-it.com/training

Bits

STRONGEST CLIMBER

Working for FOX-IT is great. Foxers have long known that themselves, but now it is official. In the 2012 Best Employer Awards, FOX-IT took fifth place and was awarded as 'Strongest Climber' among companies with up to a thousand employees. 'That's because we choose the right people extremely carefully, people who match our type of work,' according to contented CEO Menno van der Marel.

The general satisfaction of Foxers has grown further, partly influenced by improved clarity about roles, progression possibilities and communication about developments and changes. Foxers also believe that management is guiding the organisation well.

The pleasure and involvement of Foxers is also attributable to the social relevance: 'We are doing innovative and useful work.' Effectory and VNU Media (Intermediair) organise the Best Employer

The scope to assume responsibility

Awards, the largest employer survey in the Netherlands. To this end, Effectory conducts a thorough and anonymous investigation among employees to obtain an objective opinion on what constitutes being a good employer.



OHM2013 HACKER CAMP

FOX-IT is the proud sponsor of OHM2013, the forthcoming edition of the renowned four-yearly Dutch outdoor technology and security conference. OHM2013 (Observe. Hack. Make.) will be held from 31 July to 4 August 2013 in Geestmerambacht near Alkmaar. Hacker camps feature a unique atmosphere, with inspiring lectures, workshops and hands-on tinkering, with drones to 3-D printing. The non-profit event is organised by and for the hacker community, a varied collection of creative, curious and critical individuals. The event also

attracts security experts from around the world. Several Foxers assist the organisation in their free time.

ohm2013.org



HACK42 IN ARNHEM

Hacker spaces are meeting places, extended living rooms, for technophiles and creative people. As social place with a low threshold, they offer the 'tinkerers' a space to work and to share specialist knowledge. The best hackers turn their hobby into a career, and the other way around. FOX-IT has recently sponsored the new teaching area of Hacker

space Hack42 in Arnhem with workstations and furniture, so courses such as Arduino hacking can soon be followed there.

hack42.nl
hackerspaces.nl