



N° and issue date : 204 - 01/10/2011

Circulation : 75438

Frequency : Monthly

Web Site: <http://www.pcpro.co.uk>

Page : 68

Size : 95 %

905 cm2

## CAREERS

# So you want to be a security researcher?

Davey Winder reveals how you can get started in one of the most exciting careers the IT industry has to offer

**I**T careers don't get more exhilarating than fighting cybercrime, which is pretty much the job description of a security researcher. But before considering a career as one, you'll naturally want to find out exactly what the job entails.

Eddy Willems, security evangelist at G Data, admits that pinning down a precise job description isn't easy, because the role of a security researcher is so varied. "They'll look into and investigate problems relating to security, but they usually specialise in a specific domain, such as malware or network security," he says.

"The cyber-security industry is reactive, and a researcher has to be on top of what's going on," Willems continues. "Social media can play an important role in their day, since news often surfaces there first. Forums are another important tool for security researchers, especially internal forums that provide a secure outlet for the research community to communicate relevant information."

A security researcher can also spend a considerable amount of time in the labs looking at how malware behaves. "It's important to

note that security researcher is a high-level position that requires the trust of the industry," Willems says. "Writing white papers and giving presentations to other industry professionals is usually part of the package."

If all this leaves you wanting to know more, you'll probably be wondering what

qualifications are required to break into the industry. Yuval Ben-Itzhak, AVG's chief technology officer, told *PC Pro* that security research isn't really studied at university, so "many of the security researchers are 'self-taught' people".

"They're multi-skilled in many computer-science topics, and a good security researcher is one that knows how to mix these topics together, as well as being keen to seek holes and vulnerabilities left by programmers in their software," he adds.

Indeed, a thorough knowledge of how operating systems and networks function is

necessary, since this is how most "black hat" hackers launch their attacks. A computer science degree is a good starting point, and there are a number of certified courses that might also be valuable, but none is a passport to this particular career choice. Courses such as Certified Information Systems

**"Cybercrime threats are on the rise, so the security market is in need of good researchers"**

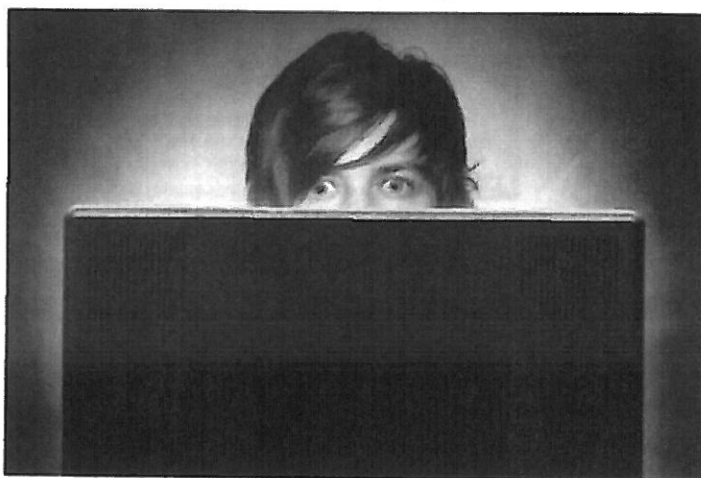
Security Professional (CISSP), Licensed Penetration Tester (LPT) and Certified Ethical Hacker (CEH) will certainly improve your job prospects, however.

While a degree in computing, electrical engineering, mathematics or physics can provide a strong indication that a person may become a good security researcher, it's by no means a prerequisite. Vanja Svajcer, principal virus researcher with SophosLabs, insists that the most important characteristics of good security researchers are simply an inquisitive mind, the ability to learn quickly, and an inherent interest in the area of computer or network security. "Many of the best security researchers don't have a formal education but started working on security alone, purely out of interest," Svajcer explains, adding that "self-starters are often very motivated to find new vulnerabilities, analyse the latest malware, and develop new techniques for fighting cybercrime."

Guillaume Lover, senior manager with Fortinet's Threat Response Team, agrees, adding that there's "a perception that those who've learned all they know from books won't be able to do the job without experience".

### Salary expectations

If you do get a foothold on the security research ladder, what kind of money can you expect to make? Sophos' Vanja Svajcer warns that the starting salary is likely to be in line with an





N° and issue date : 204 - 01/10/2011

Circulation : 75438

Frequency : Monthly

Web Site : <http://www.pcpro.co.uk>

Page : 69

Size : 95 %  
905 cm2

average junior software engineer or technical support analyst. "However, as your experience grows, the money you earn will significantly increase," he says. "The top security researchers in some companies earn six-figure salaries, but that often includes some management responsibilities."

According to Lovet, the average salary ranges between £37,000 and £50,000 in the UK, while in the US you could expect to earn between \$50,000 and \$100,000. Many security researchers will ultimately establish their own security companies and the rewards there can be greater.

And don't forget the freelance option, as Robert McArdle, senior advanced threat researcher at the Trend Micro Forward Looking Threat Research team explains. "There are several well-known people in security who are quite successful in this regard, such as Dancho Danchev or Bruce Schneier," he says. "With the internet today, people can promote themselves better than ever before. A person can raise their profile via a personal blog, Twitter, speaking at conferences and local security events, and so on. That promotion helps to increase their contacts, and those contacts get them better offers for work."

Opting for a freelance career might look like an attractive option, but remember that the high-profile names mentioned above are leaders in their field. Getting such a profile doesn't occur overnight, unless you happen to stumble across a major security problem that makes the media sit up and beg for your attention. As Lovet admits, there's little or no job security if you're a freelancer, and your work is done on an ad hoc basis.

So joining a large security vendor is probably the best approach if you want to be exposed to the broadest variety of threats, in order to get the best possible grounding in the research field. "It's also an excellent way of learning about the security needs of large and complex organisations, such as banks and some of the world's most renowned financial clearing houses, or large governmental or educational institutions," says Lovet. "This isn't to say that experience with a smaller organisation won't be valuable, but working with one of the leading security vendors in the world does open your eyes to the enormous scale and impact of cybercrime in everyday life."

On the downside, you'll find you're bound by stringent non-disclosure agreements. "Intellectual property is taken very seriously by vendors, as you'd expect," says Lovet. "I there was a recent high profile case of a security researcher being prevented from boarding a plane by the US Government because he was a



## A day in the life of a security researcher

**Name:** Orla Cox

**Job title:** Senior security operations manager

**Experience:** 14 years with Symantec, holds MCST and CISSP certificates

PROFILE

Typically, I arrive at our Dublin-based research centre at 8am. The first thing I do is join a call with the Symantec Tokyo team, which has been working throughout the night, scanning email traffic to protect against malicious activity and identifying anything suspicious. During this call, we review all threats or unusual activity that's come in, so we can take over any work that needs to be continued

to get a deeper understanding of the threats we're dealing with, or any unusual activity we've picked up on.

No two days are the same, and the way we try to identify these threats varies. My role may range from setting up "honeypot" systems to gathering new threats for analysis, to monitoring discussions on the Internet to identify new trends and methodologies.

## "My role may range from setting up 'honeypot' systems to gathering new threats I can then analyse"

when the Asia team clocks off. This ranges from monitoring and analysing potential threats to getting websites shut down, it can be fairly unpredictable.

Our team in Dublin then meets to review the issues of the day and how we're going to research, analyse and tackle any big threats that have been identified. We'll spend the rest of the day carrying out our research in order

In the afternoon, we have a virtual meeting with the US team that's based in California, which will be responsible for taking over from us once our office closes for the day. In this meeting, we review what we've been working on throughout the day and hand over anything the Californian team needs to take on, before signing off for the evening.

friend of somebody who volunteered for the WikiLeaks website." An extreme case, perhaps, but it does demonstrate what a sensitive area this is to be working in. You need to be prepared for such incidents if you decide to pursue a career in security.

### A move from the Dark Side?

What about if you're an ex-hacker, or have been involved in the "dark side" of security: should you even bother applying to the security vendors for a job? Mikko Hyppönen, chief research officer at T-Secure, thinks not.

insisting: "If you're a virus writer, that makes you a criminal.

Most security companies don't want to hire criminals. I'd hate to have to explain why we're hiring criminals. I just don't need the grief."

It's true that ex-hackers usually possess a wealth of knowledge on security issues. "However, they lack the trust of the research community,

which is crucial to becoming a security researcher," says G Data's Eddy Willems. "Many companies view it as unethical and hypocritical to hire them, and are concerned that it could damage the company's reputation. Therefore, security companies such as G Data absolutely don't hire malware writers."

It's important to distinguish between black and white-hat hackers, though, so it really does depend on what you've done and what you're prepared to admit to. As Yuval Ben-Itzhak concludes: "Anyone with the right skills and curiosity should apply, including ex-hackers who would like to come back from the dark side."

And, finally, what's the job market like? "As businesses continue to see that IT security enables them to work more efficiently and effectively, security products will become more popular and drive demand," says Carl Leonard, senior research manager at Websense Security Labs. "The cybercrime threats are increasing, so the security market is on the ascendancy at the moment, and is therefore in need of good researchers to keep the protection going."

**Vacancies**  
The best place to find vacancies for security researchers is the websites of the security firms themselves. At the time of writing, Websense was recruiting for a researcher at [www.pcpro.co.uk/links/204careers](http://www.pcpro.co.uk/links/204careers)