Patrowl

SECURITY ENGINEER

A MULTI-FUNCTIONAL POSITION THAT IS RUNNING OUT OF STEAM

Expert opinion by Sébastien Coll, Pentester - Lead Dev and Marius Vinaschi, Pentester - Backend Dev at PatrOwl

THE SECURITY ENGINEER OF A SMALL BUSINESS, A ONE-MAN BAND

Ideally, a security engineer should spend his days looking for solutions to the problems he encounters and implementing them. It is a high value intellectual work, the one for which he (and she, to a lesser extent, still and unfortunately) has been trained and recruited.
The job is conceived as a succession of extremely diverse issues, to the point that be versatile is required: pentester, trainer, network expert, at least, to embrace as broadly as possible the constantly expanding field of cyber risk. But what else? Author and prescriber of backup policies, identity manager, often a bit of a developer himself, etc., in an SME, expertise is not measured by the success rate, but rather by the unsuspected range of skills of the security engineer.

This is perhaps also what you would find in a job description, the frantic search for a rare bird who knows how to speak Python, Ruby, Perl, shell, powershell, ASM x86 and x64, C/C++, German and Portuguese (not essential), knowledges in software and hardware, and a keen sense of teaching. And yet, this would still not be a tour of the huge amusement park that today's attackers visit every day.

MAKING CHOICES IS STILL A BAD CHOICE

It is always expected that the defensive missions of an engineer do not have the effect of slowing down the work of the business team and by extension their potential creative effort. The maximum security level of some inevitably clashes with the desire of others to free themselves from constraints, leading to the perception that protective measures are a burden, or even an obstacle to activity.

> *"Today, this natural prioritization reveals serious flaws at all levels and make organizations to accumulate major delays in risk prevention, training and in the implementation of solutions."*

In their defense, companies have always missed time, budget and skills, for too long to work in parallel on security and service availability, which are closely linked.

Moreover, if the example of a small company seems too caricatural, let's remember that a larger company does not have more cybersecurity personnel than others, despite the presence of teams of developers, for example, dedicated to the creation of digital products. Then, insecurity grows and new risks appear everyday and its problems are declining and opening perspectives of ever widening risks.

THE AUTOMATION OPTION IS NO MORE AN OPTION

Given the cost of a security engineer, of a complex recruitment process, but also a more restrictive regulatory framing and pressure from the ecosystem for more security, an effective strategy would be to free up more and more time for employees so that they can concentrate on the missions that cannot be carried out without them.

In particular, they can do security awareness with business employees to better fight phishing, but also with developers, so that they can definitively integrate security by design into their job. The acquisition of skills in this area will never be self-evident without the repeated and forceful intervention of the CISO and his team, which is both indispensable and time-consuming.

One of the areas in which the company can act by relieving its engineers of tasks that are both difficult and unpleasant is the set of assets that the company exposes on the Internet.

Databases, websites, applications, APIs, servers, services, it is very common for companies to poorly secure their assets or even simply ignore what they expose, especially if they are prone to shadow IT. By definition, a forgotten server is not updated and offers a golden opportunity to penetrate the company's systems. While this attack vector represent 60% of compromise (the other main vector is social engineering through phishing), after social engineering through phishing, it is also the area that is best covered by automated monitoring.

if you can’t increase the size of you security team, it's your tools that need to be enhanced. Automated solutions are not just about saving precious time. They free employees from the burden of activities that are so repetitive that they cause weariness and distraction. Let's remember that it will always be more difficult for an engineer to defend an entire system than for an attacker to find the vulnerability that will allow him to compromise the company.