



# CYBER-SAFETY IN AN EVER-SHIFTING LANDSCAPE

*The threat of infection looms large in the digital world, but a team of University of Malta (UM) alumni have taken it upon themselves to create a cybersecurity system that acts quickly and responds dynamically. **Teodor Reljic** learns about CyberSift.*



When it comes to cybersecurity, the adage 'survival of the fittest'

gains an even sharper—almost crystalline—technological edge. The nature of the beast makes it so. The cybernetic universe is infinitely adaptable, expanding or contracting its borders based on the latest innovations. With this broad canvas of potential open to all, 'innovations' could either mean something positive and wholly beneficial, or it can signal new and destructive ways for cyberattacks to worm their way through a system. Any system.

This is where cybersecurity comes in. How can businesses feel entirely safe on the web, given all of the digital landscape's attendant vulnerabilities and the obvious dangers of tech-savvy attackers who would always be

*The cybernetic universe is infinitely adaptable, expanding or contracting its borders based on the latest innovations.*

tweaking their methods to beat the 'good guys' at their game?

Well, while they do not claim to have all of the solutions, a new cybersecurity venture appears to be able and willing to give it their all when it comes to addressing some of the industry's key lacunae.

## AI FOR SECURITY

CyberSift was founded by Brian Zarb Adami and David Vassallo in an attempt to address some rather large elephants in the realm of cybersecurity. The idea to take their own shot at shaping this scene first came about while the duo were still employees within the ranks of another company, tackling a particularly tough project. The project was successfully brought forward, but Vassallo was left frustrated with the cybersecurity mechanics available at the time.

Throughout the course of the assignment, it became painfully clear that large security systems raised the biggest red flags. Not only were they unable to detect new threats released daily, but they also lacked integration of modern data mining techniques.


'This was alarming, given how organisations worldwide are always shoring up vast amounts of data—hence the term 'Big Data'. In reality, they rarely use that data to its full potential,' Sirly Raavel, CyberSift's Marketing and Communications Executive explains, as she guides us through the company's journey. An enhanced security mechanism is one

of the ways in which such data could be employed to more beneficial ends.

This starting point would grow to form the backbone of the entire CyberSift initiative, which, Raavel hastens to add, not only includes its founders, but also a dedicated team of IT developers, IT infrastructure engineers, 'and, of course, marketing.'

'We wanted to create a system that was quick and easy to deploy and incorporated modern AI and machine learning techniques to glean valuable insights from all the data that's being gathered. These insights help the customer's security analysts be more effective and basically helps in automating away the boring aspects of these analysts' jobs. This approach allows a customer to increase their level of security with a smaller upfront cost,' Raavel adds, before delving into the logic behind how CyberSift evolved from a concept to what it is today.

'The AI and machine learning algorithms were a product of David's studies and research while pursuing his Masters in Computer Security (University of Liverpool), and they continue to be improved and used in CyberSift to this day. Brian handled the business side—raising investment, identifying customers both locally and abroad, all while managing operations and marketing.'

Going back even further, Vassallo is very quick to emphasise the importance of the University of Malta (UM) to their overall project. Having met as students in that institution (though at that )



**Brian Zarb Adami**



**David Vassallo**

time, enjoying widely divergent academic paths) both Vassallo and Zarb Adami pride themselves in being able to creatively apply their early academic experience in ways that have now yielded substantial tangible benefits.

'The most important impact that the UM has had is that it taught us how to research, how to think, and how to solve problems that are not necessarily part of the course curriculum or career that you are pursuing,' Vassallo says. This is directly reflected in the duo's eclectic research backgrounds. Case in point: CyberSift is an IT company; however Vassallo graduated from the UM as an electrical engineer, and even more dramatically, Zarb Adami graduated as a pharmacist. While both disciplines appear to be entirely at odds with the nature of the CyberSift project, Vassallo firmly believes that their university experience contributed to making them great all-rounders, capable of internalising

the knowledge required for any task, and creatively dealing with issues.

### **SOME CYBER-GAPS**

All of this paints a picture of a company put together by a couple of dynamic and well-informed professionals itching to address what they deem to be some of the industry's most glaring imperfections. CyberSift's efforts become all the more important to consider when you remember that 'imperfections' tend to equal 'gaps' in the fields of cybersecurity. Gaps through which crippling attacks can worm their way.

In cybersecurity, gaps are normally linked to complacency. As Raavel succinctly puts it, 'businesses tend to think of cybersecurity the same way they do about insurance. They don't think they really need it until they get hit by a security incident, by which time it's usually already way too late.' Despite this issue, CyberSift

still needed to elbow its way through the market during its early stages.

'The first steps were to understand the demand [from companies]. We had to answer questions like: how much would a customer be willing to pay for such a system? What would be the major pain points they were likely to encounter when using the product? Once we had a handle on these questions, the next challenge was to build a working proof of concept that we could deploy to a friendly customer to make sure our idea worked. Users should be able to interact with the system without needing an advanced degree in mathematics,' Vassallo says.

One of CyberSift's key innovations is its speed of implementation. The sluggishness of previous systems was always a bugbear of Vassallo's, so unsurprisingly then, this was one of the first things to be addressed by the team when bringing this new system to life.



*CyberSift in particular is a behaviour-based system, though Raavel is quick to add that even this niche includes a diversified range of products.*

'To this end, the tech team's main concern was to make sure that CyberSift would be able to 'slot in' to an existing customer network without any large disruptions, or causing a bottleneck,' Zarb Adami recalls, filling us in on some of the nitty-gritty details of how CyberSift works in practice.

'Almost any client already has some sort of security infrastructure in place, be it an antivirus, firewalls, and so on,' Zarb Adami says.

All these products generally generate logs. What CyberSift does is simply 'ingest' these logs in a variety of ways, 'offering flexibility to the customer,' and then applies its AI and machine-learning algorithms to digest and absorb them, highlighting those logs and sequences which are anomalous.

'So in reality, once a client buys CyberSift—which is either a server on-premises, or a server in the cloud—they simply tell their existing security tools to send their logs to CyberSift,' Zarb Adami adds.

Raavel then goes on to outline just how CyberSift differs from other security mechanisms out there.

In general terms, Raavel explains, there are two types of security products, each of which has their niche in the security ecosystem.

'There are 'signature-based' products—for example your antivirus—

which downloads a set of rules and flags a file or event as suspicious if it matches any of those rules. Then there are 'behaviour-based' systems which take the time to sit back and build a baseline of your network to get a better idea of what normally happens on there,' Raavel says. After a certain amount of 'training,' these systems can highlight any behaviour which deviates from this baseline. This approach is advantageous, since these behaviour-based systems are actually capable of detecting previous unseen malware as they do not require any rules—a big plus in today's security landscape.

CyberSift in particular is a behaviour-based system, though Raavel is quick to add that even this niche includes a diversified range of products. 'These differences are mostly due to the type of AI we use in our systems. AI is a vast and interesting field, with sub-categories such as neural networks, genetic algorithms, and pure statistical-based methods,' Raavel says, adding that, 'Naturally, each approach has its own pros and cons.'

'For example, some algorithms may be very quick to train, but have a lower accuracy—while other algorithms may take a very long time to train, but offer much greater accuracy. Other algorithms may be fantastically accurate but require so many resources

that they are impractical,' Raavel says. She continues, 'Like any good barista would tell you—the trick is choosing the right blend.' In CyberSift's case, 'We need the right blend of algorithms to make CyberSift accurate while remaining responsive and not breaking the bank in terms of resources required.'

## THE PERPETUAL FIGHT

Asked to single out some of the most urgent cyber-security issues right now, Vassallo says that the biggest problem is 'helping defenders keep up with the attackers'. For this reason, CyberSift favours a behaviour-based approach, because it can 'highlight those events which look suspicious even if they are brand new, or 'zero-day' in industry terms.'

Favouring a rapidly responsive and dynamic system appears to be a 'common-sense approach to battling the constant threat of 'infection' in the digital world,' Vassallo explains.

'The challenge of the cybersecurity industry is that you can never just 'fire-up-and-forget' a product [...] it's not a good job for people who don't like learning new things, or being outside their comfort zone on a regular basis. But if you have the right people, then it actually becomes a thoroughly rewarding experience.' 