Cyber Security and versaSRS

Beyond the Perimiter

Delta Technology Solutions provides Server Management, Health Monitoring and Cyber Threat Security Analysis services as a subscription based, fully managed service and framework, to a broad range of SME and Corporate clients globally.

Learn more at versaSRS.com

The power of AI and advanced analytics is the computing equivalent to harnessing the wind.

It's about making sense of the vast amounts and many different types of customer information that stream in at unrelenting speed. From consumer transactions to social media trends, every online click is grist to the mill. Collecting data is the endless pursuit of big business. Finding its value is the key. Businesses are using data analytics to inform their decision making and generate competitive advantage.

Cyber-attacks occur daily across the globe by hackers who are increasingly advanced and persistent. Their aim to interrupt, damage, destroy or steal confidential information inflicts a massive financial wound. As the cost of malicious attacks goes up, so too does the spend to prevent them. In 2018, upward of US$97 Billion was spent on SIEM (Security Information and Event Management) alone, and according to the founding Director of Delta Technology Solutions, Rick Mulford "the bad guys are still breaking in".

It's a grim reality that the motivation to use data analytics for good is equal to the motivation for using it for evil. It all depends on the algorithm. For the good guys, the battle is keeping up with the vulnerabilities and reducing the risk, which begs the question: who's actually winning? Rick Mulford points to the disparity in the cyber security industry as a genuine constraint. "Product vendors are competing for work in the same space. It creates a lot of confusion", he says, "and that's only helping the bad guys."

So, who are they, and what are they doing? At the big end of town are the state-sponsored cyber operations with China and Russia topping the list by a fair margin. The number of malicious organisations and skilled individuals dotted throughout the globe are much harder to quantify. Malware, ransomware and social engineering are among the most common types of threats with so many variants, it's impossible to keep count. The entry point for the vast majority of these attacks: the ubiquitous email. Simply clicking on a link can be all it takes to give access to a network. In Australia, health and finance make up almost half of the data breaches that are occurring. The risk to individuals is largely in the form of identity theft whereas to companies, industrial espionage and the risk to intellectual property is outweighed only by the loss of trust and damage to reputation. As a recent attack on Australia's Federal Parliament attests, even governments, with arguably the most to lose, are not impenetrable.

Delta Technology Solutions entered market in the early 2000's with their flagship product, Delta iManager, a full analytics, SIEM and threat analysis solution. "When we embarked on this mission, we realised we had a choice, we could create another fantastic set of tools to meet our requirements and then compete in this space, or create a process and analysis framework to complement the existing range of tools and systems available; therefore creating a new global service opportunity that complements the industry and product vendors rather than competing with them", says Rick. In essence, the framework relies on good partnerships.

Since its inception, iManager was built to compile information from existing technology leaders such as Microsoft, HP and IBM. The software also includes tools and services from other leading service providers such as GFI, Paessler and LogicNow. But it's not all about household names or global reputations. Great partnerships are borne out of a synergy of complementary skills and capabilities. Regarded as one of the keystone products in Delta's information framework is versaSRS developed by VersaDev. "All communication is done through the Versa interface", says Rick. "We looked at a number of other products and solutions but Versa gave us a strong client facing portal and interface. It also gave us the ability to get an alert out really quickly with a ticket number so it was fully trackable and auditable."

Systems monitoring is known for being an exceptionally complex area to operate in thanks to the sheer volume of data and number of sources involved. To put this into context, a single device can potentially generate millions of events per day. This creates a lot of 'noise' in terms of the information to be deciphered and condensed into something that is clear and usable. Then when you consider that a ransomware infection can encrypt hundreds of files in a matter of seconds, response time is critical. It's a paradox, like the immovable object meeting the unstoppable force. Surely something's gotta give?

Re-enter: data analytics. Rather than just monitoring for malicious activity, Delta are looking for patterns of normality. "By using data analytics, we can establish what's 'normal good' or 'normal bad' and where those patterns are stemming from", says Rick, "we also track it to regions so we can see a pattern." They can then correlate all of this information into a single event. Instead of hundreds or even thousands of security-based alerts being sent to the support team via email, Delta can consolidate them into actionable data within minutes.

Learn More About
versaSRS & Business Transformation

Ph: +61 8 8463 1914
versasrs@versadev.com

This is where the synergy with Versa really comes into play, by getting the information out to the right people, in a rapid space of time. "We initiate an event and escalate that via the Versa interface. The value-add proposition that versaSRS brings to us is we are able to coordinate clients into groups and underneath that, subsets of skill-groups. So, we make sure that the right information automatically gets distributed to the right people all the time, who are responsible for looking after specific areas of the network. And we track that event all the way through to completion before closing the ticket", says Rick. "The beauty of it is it saves mistakes. It's really easy for a person to click on the wrong button but if we force that process, it allows us to do that."

To have any hope of detecting and averting malicious behaviour requires security defence by layers. "One of our key points of difference is we're monitoring not only the perimeter but the end point", says Rick. The perimeter being a firewall device or intrusion detection system and the end point being the hardware such as servers, computers and smart phones. Conficker, considered one of the most serious malware outbreaks of all time, provides a genuine case in point for two defences being better than one. The computer worm, which emerged in 2008 is still active today, having infected millions of computers world-wide with the clean-up estimated to be around $9 Billion. One instance of a large organisation in New Zealand being infected with conficker occurred during patching via a USB. Over a period of several hours, everything was slowing down and eventually ground to a halt. It was discovered that conficker had been introduced to the network and bypassed all their system protections. It affected over 2000 devices and almost every server had to be rebuilt. By comparison, a client of Delta's was inadvertently infected with the exact same variant of conficker via a USB. "We spotted it within minutes of it going live before it got off that one computer. We couldn't get hold of the support team so we turned that computer off to stop it from propagating", says Rick. "That's the key point of difference, and we've stopped about 25 outbreaks of that calibre."

Delta, and indeed their entire industry, are witnessing threats that are getting faster, stronger and more sophisticated. In a complex environment, simplicity becomes all the more important. Despite the power of what analytics can do with big data, people still need information that is granular and systems that are user friendly. "That's where Versa is a vital piece of our information management", says Rick. "We look at so much information, having a single interface is really important. If we can present that in a very nice and user-friendly fashion, the longer-term relationship we have with our clients as well." Delta's clients are spread across the globe and use the client facing portal SRSConnect. This gives them consolidated access to all current and historical tickets in the system instead of having to trawl through emails to locate a particular incident. "Having a portal that people can interact with is a lot more secure" says Rick, "and by having a simple web interface, it takes away all the complexities of a full IT management solution but they get all the features of that through our interaction."

The future of data analytics is a measure of comparison. "We believe that this next wave of security threats is going to be bigger and worse than what we've seen today", says Rick. "And we're working with our channels to make sure we're ahead of the game to be able to help mitigate those risks." VersaDev and Delta provide intelligent and highly scalable software. The combination of these unique offerings creates a powerful and highly functional solution.