BRIEF
New Zealand's leading source of security and threat news

TAGS

Managed services, Cybersecurity, RedShield

RedShield's CTO on the iSANZ win – and why he wants your security problems

DECEMBER 06, 2016 9AM / SARA BARKER

RedShield is a Kiwi-owned fully managed service cybersecurity provider that has just won big at the latest iSANZ Awards. With a continuous find-manage-fix-monitor programme, the company says it can fix almost all detected issues, including logic flaws. They do this by fixing old, new or third party applications without clients' developers writing a single line of code.

Sam Pickles, RedShield's co-founder and CTO, talks to Techday about the company, its win and plans for the future.

Pickles has spent more than 15 years experience in protecting companies and governments around the world in the event of cyber attacks. He runs a team of developers and security engineers to build, maintain and monitor customers' shields.

"Our experts develop, deploy, maintain, monitor and report on the effectiveness of the fixes on an ongoing basis and highlight any security incidents that we have prevented, so we become your advanced security team. The fixes are rented and can be added, changed, removed very rapidly. So we solve more problems than the competitors, but more importantly we solve *your* problems. We communicate with business level risk reporting including our patented incident report," he says.

The company recently won Best Security Company of the Year at the 2016 iSANZ Awards, and Pickles says it's a validation of the dream they set out on five years ago.

"Back then the founders were in different areas of the security community, with half of the team coming from security testing where similar security issues were discovered between organisations and then rarely fixed in a timely manner. The other half came from the security protection tools community, and had observed failed deployment after failed deployment, where the common characteristic was lack of skill and process."

The company saw an opportunity to combine all of these skills and use them for real problem solving. The company has now grown to include more than 1800 applications from a wide variety of organisations, it shows that the approach has value.

"This award is recognition from the industry that we are indeed solving a real problem, and doing it exceptionally well," Pickles says.

The iSANZ judges made special mention that the company addresses global needs rather than just security consulting services, and Pickles says this is all about fixes based on all individual, public-facing security problems.

"We believe in test centric security, where it is important continually search for issues and then fix them. If they are exploitable then they aren't fixed. The criminals are highly organised and so are we. Our team does the basics of weekly scanning, log reviews, continuous monitoring, which then allows us to perform advanced actions when required."

Pickles says RedShield differentiates its services in four key areas:

1) We are the only company in this sector that we are aware of that actively pursues customer specific issues to address. The competition very much uses a toolbox approach where they fix a defined list of issues and only those issues.

2) We believe 99% fixed is still 100% vulnerable and hence are the only company that promotes virtual code patching to address logic flaws in applications in additional to technical vulnerability fixes. The competition only proposes technical vulnerability fixes and leaves the more difficult software logic flaws to the software developer community. This means we can solve many more issues than our competitors. The market estimates that the issues are 50/50 between technical and logic.

3) We are highly pragmatic when it comes to deploying security controls, we ensure that the controls are both required and effective plus that processes are efficient end to end to deal with incidents, both attacks and mistakes. The competition filters traffic that the tool has categorised as a threat. Using this approach we are currently operating at a false positive ratio (blocking customer traffic by mistake) that is 1/1000th what the industry states as best practise.

4) We believe that expertise and mature process are required along with advanced tools to be effective against and organised and skilled adversary. Criminal gangs accounted for 80% of the 455 billion USD of cyber crime in 2015, these organisations are highly organised, motivated and skilled. The Cyber crime industry is highly profitable and now costs society more than the drug trade ($380 billionUSD 2015).

Pickles believes that IT security investments are too focused on legacy network tools, meaning applications, skills and processes are left unaddressed. He says IBM analysts have pointed out that cybercriminals are the most organised; and HP research has shown that 87% of SoCs don't meet the minimum acceptable level of process maturity, and it will take five years for organisations to get to that point.

With presences in New Zealand, Australia, the United States and the United Kingdom, the company is rapidly growing in all territories. So what lies in the company's future? Opportunity and investment.

"New Zealand and Australia are our most mature markets, but in 2017 we plan to add headcount and investment in other territories to address the growing opportunities further abroad. We have a number of early wins, and discussions with Fortune 500 companies that we are progressing," Pickles concludes.

Are you keen to hear more? We can get you in contact with RedShield. Click here

RELATED

WatchGuard's global reseller survey finds ransomware top customer fear for 2017

ESET walks away with 100th industry accolade in 'monumental milestone' for security

CipherCloud promoted to Dropbox Premier Partner as security services skyrocket

ISACA provides cyber governance roadmap for enterprise security

FOLLOW US

SPONSORED

> **The 2017 National Disaster Recovery Survey - win $200** Disaster Recovery, Data, Cyber Attacks, Survey, Westcon-Comstor, Veritas

> **EXCLUSIVE: Expert tips for protecting your crucial data** Disaster Recovery, Data security, Veritas, Backup, Digital transformation

FEATURED

Our lax attitude to passwords is 'leaving the front door open' to trouble

Behind the WhatsApp 'backdoor' allegations: An expert's opinion

Can you ever be truly anonymous online?

OUR ASIAN NETWORK

SecurityBrief Asia
DataCenterNews Asia
EnterpriseChannel Asia

OUR AUSTRALIAN NETWORK

IT Brief Australia
SecurityBrief Australia
ChannelLife Australia

OUR NEW ZEALAND NETWORK

NetGuide NZ
Educators NZ
IT Brief NZ
SecurityBrief NZ
Techday
bizEDGE NZ
ChannelLife NZ

ABOUT TECHDAY

About Us
FAQ
Terms of Use
Meet the Team
Advertise
Contact Us

SOCIAL

Facebook
LinkedIn
Twitter
RSS

New Zealand's leading source of security and threat news

Singapore
+65 3 159 0565
Australia
+61 1300 092 195
New Zealand
+64 9 376 8121