



MEDIA RELEASE | FOR IMMEDIATE RELEASE

Singapore, 10 February 2010

Total: 6 pages (including notes to editor)

Start-up licenses high performance traffic analysis engine from Exploit Technologies

Singapore, 10 February 2010 – Niometrics Pte Ltd, a Singapore start-up, had on 5 February 2010 licensed from Exploit Technologies a next-generation, highly accurate traffic recognition engine, developed by the Institute for Infocomm Research (I²R) of the Singapore Agency for Science, Technology and Research (A*STAR).

The licensed technology, codenamed as CUB4, is a home-grown, high-performance, software-based traffic analysis engine. As part of its licensing agreement with Exploit Technologies, the strategic marketing and commercialisation arm of A*STAR, Niometrics will further develop and produce a range of new security products and services. Niometrics' products and services, built around CUB4, are designed with the constantly changing information security landscape in mind, putting strong emphasis on automated protocol learning and a flexible software design that enables fast updates as new protocols and risks emerge. Niometrics' technology can detect more than 4,000 protocols, services and applications, a four-fold improvement over existing products in the market. The new engine allows corporate users to detect IT policy violations and perform fine-grained analysis for potential threats, without enforcing unnecessarily strict blocking policies.

The company is in talks with IT managers in financial institutions, government agencies, and manufacturing companies as well as leading system integrators and service providers in Singapore, Malaysia, Japan, and the US. To this end, the company has already established a partnership with Singapore infocomm security solution provider, GMS Enterprise Pte Ltd, to distribute its products.

Niometrics was founded in May 2009 as a spin-off from I²R, and CUB4 is based on work done by Dr Kostas Anagnostakis, a former research scientist from the institute, and now the founder and CTO of Niometrics.

Dr Anagnostakis said, “We are very excited to license this technology which can help manage risks and tighten enterprise network security, in a landscape of sophisticated malware attacks, high-risk user activities, and insider threats. With the CUB4 engine, we hope to enable network managers to better audit and control their networks. The concerns about Web 2.0 applications and productivity loss are only the tip of the iceberg: there are thousands of other applications and network protocols putting IT infrastructure at risk of misuse or malware infections. The CUB4 engine can already identify more than 4,000 different applications, including a growing number of applications and Trojans that actively try to conceal themselves through encryption or obfuscation. With recent high-profile incidents, and the resulting concerns on attacks and insider threats that slip past traditional defenses, the importance of beefing up the enterprise security arsenal becomes even more evident.”

Commenting on the process of starting the company, Dr Anagnostakis added, “The people from Exploit Technologies have been on our side since day zero, more than two years ago, when we first started testing our early prototype in the lab. They succeeded in teasing us out of the lab, put us in front of real customers, and helped us become more "street smart" and avoid the common pitfalls on the path from raw ideas out to the market.”

Philip Lim, Chief Executive Officer of Exploit Technologies, said, "We are excited to have worked closely with Niometrics to bring A*STAR's technology from concept stage to the commercially viable product we see today. The commercial discussions already underway with key players in the industry position Niometrics well for the future. We are looking forward to having more of such promising and innovative start-ups from A*STAR to embark on the technopreneurship path.”

Prof Lye Kin Mun, Deputy Executive Director (Research) of I²R, said, “This licensing agreement marks another milestone in the transfer of technology developed at I2R to industry. We are happy, of course, that on this occasion, it is going to yet another spin-off company of our institute. We wish Niometrics every success and are confident that they will make their mark globally. They are well poised to provide important security solutions to the rapidly growing Web 2.0 world.”

Niometrics has successfully clinched the Technology Enterprise Commercialisation Scheme (TECS) award, a competitive grant administered by SPRING Singapore. TECS is awarded to start-ups based on strong technology Intellectual Property and a scalable business model. Niometrics was selected as one of the 21 winners from 220 submissions in June 2009.

###

Enc: Notes to the editor

For **media enquiries**, please contact:

Kostas Anagnostakis (Dr)
Founder and Chief Technology Officer
Niometrics Pte Ltd
Mobile: (65) 8186 9464
Email: kostas@niometrics.com

Seeto Wei Peng (Ms)
Vice President, Corporate Marketing and Communications
Exploit Technologies Pte Ltd (A member of A*STAR)
DID : (65) 6478 8443
Mobile: (65) 9711 9001
Email : weipeng@exploit-tech.com

Andrew Yap (Mr)
Acting Manager, Corporate Communications
Institute for Infocomm Research (I²R)
DID: (65) 6419 1143
Fax: (65) 6466 7716
Email: yapjt@scei.a-star.edu.sg

About Niometrics Pte Ltd

Founded in May 2009, Niometrics is a fast growing networking and security company with a strong focus on R&D and innovation. Our core expertise is in layer-7 network traffic analysis technology, with applications in enterprise network audit, policy enforcement, traffic management, and data leakage prevention. Niometrics' mission is to help security-conscious organizations protect their networks in an ever-evolving landscape of external as well as internal security risks. Niometrics also partners with vendors and customers in sensitive industries in R&D to deliver tailored security and traffic analysis solutions.

For more information, please visit www.niometrics.com.

About Exploit Technologies Pte Ltd

Exploit Technologies is the strategic marketing and commercialisation arm of the Agency for Science, Technology and Research (A*STAR). Its mission is to support A*STAR in transforming the economy through commercialising R&D. Exploit Technologies enhances the research output of A*STAR scientists by translating their inventions into marketable products or processes.

Through licensing deals with industry partners and spin offs, Exploit Technologies is a key driver of technology transfer in Singapore. It actively engages industry leaders and players to commercialise A*STAR's technologies and capabilities, bridging the gap from Mind to Market. Exploit Technologies' charter is to identify, protect and exploit promising intellectual property (IP) created by A*STAR's research institutes.

For more information, please visit www.exploit-tech.com.

About Institute for Infocomm Research (I²R)

The Institute for Infocomm Research (I²R - pronounced as i-squared-r) is a member of the Agency for Science, Technology and Research (A*STAR) family. Established in 2002, our mission is to be the globally preferred source of innovations in 'Interactive Secured Information, Content and Services Anytime Anywhere' through research by passionate people dedicated to Singapore's economic success. I²R performs R&D in information, communications and media (ICM) technologies to develop holistic solutions across the ICM value chain. Our research capabilities are in information technology, wireless and optical communication networks, interactive and digital media; signal processing and computing. We seek to be the infocomm and media value creator that keeps Singapore ahead. Website: www.I2R.a-star.edu.sg.

NOTES TO THE EDITOR

The problem: IT managers losing control

On an average day, there are more than 500 different applications peddling packets over a typical enterprise network, and overall, many thousands of network applications have been seen “in the wild”. While some applications are essential to an organization’s mission, many more are installed by employees for productivity or leisure. It is not easy to tell which applications are safe and reliable, which ones are well-maintained by reputable vendors, and which ones are counter-productive, risky, or malicious. Unfortunately, existing traffic shaping, content filtering, and firewall solutions are oblivious to most of these applications. IT managers cannot see them, and therefore can also not act on them in terms of setting a policy to shield their network.

Niometrics Products and Services

Niometrics’ flagship product, the NWOW Policy Enforcer, is a layer-7 analysis and filtering system that allows IT managers to audit their networks and enforce corporate use and security policies. With close to 100% traffic detection performance, the NWOW enables tighter control, while at the same time being able to monitor a much broader set of potential risk vectors.

Niometrics’ flagship service, the Deep Network Audit (DNA), is the first to use layer-7 protocol recognition to provide IT managers with a comprehensive risk profile based on observed behavior in the network over the duration of the audit. The Deep Network Audit complements the raw power of the NWOW engine with the knowledge and insights of an experienced team of analysts to help identify and interpret the most mysterious and potentially harmful network behaviors

Customized solutions include application-specific passive traffic analyzers, a high-performance traffic capture and forensics toolkit, and tailored detection modules for DPI and WAN optimization solutions.

Technology

Our technology was designed for change, putting strong emphasis on automated protocol learning and a flexible software design to enable fast updates as new protocols and risks emerge. Our products and services are built around CUB4, a home-grown, high-performance, software-based traffic analysis engine. Our software-centric strategy accelerates the time-to-market for new functions, minimizes vulnerability windows, closes functionality gaps, and allows us to evolve and stay ahead of competitors.

Our technology can detect more than 4,000 protocols, services and applications, a 4x improvement over other products. With excellent detection performance, our engine can transparently look out for policy violations and perform fine-grained analysis for potential threats rather than turning a blind eye to the problem or enforcing unnecessarily heavy-handed blocking policies.