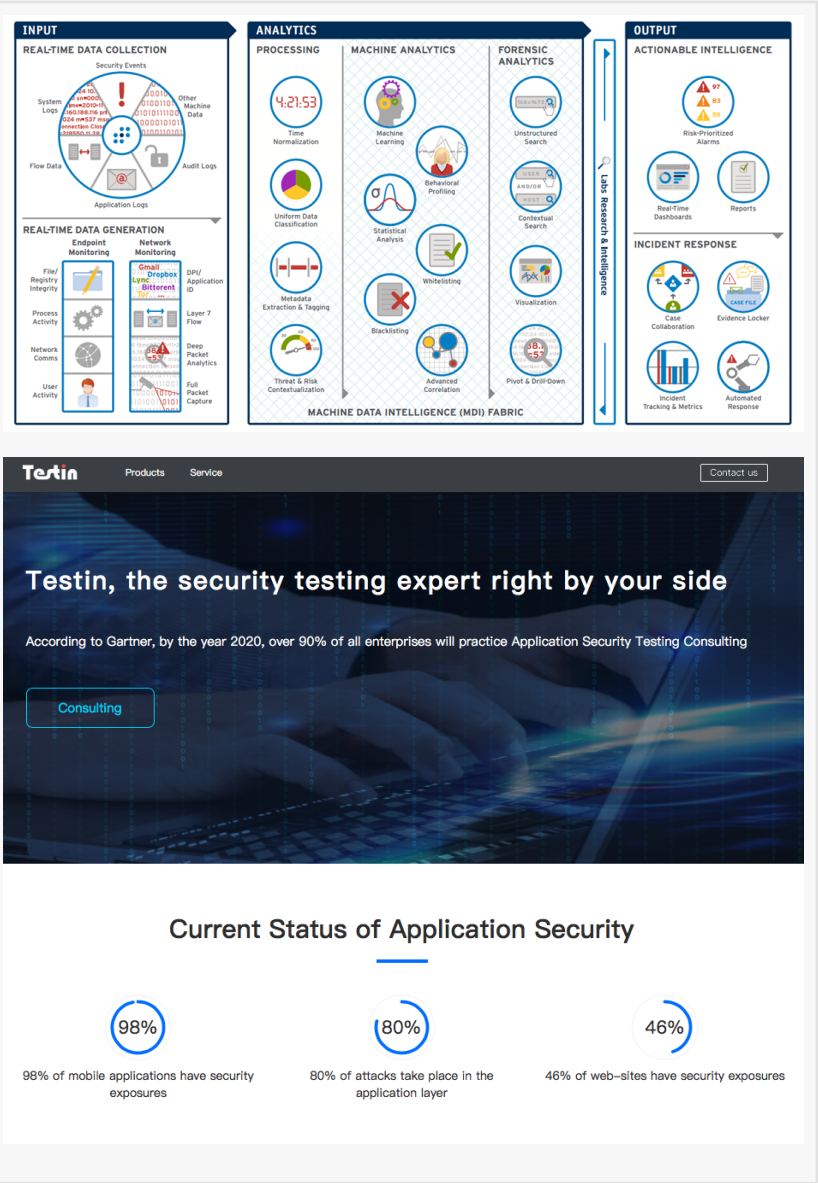
“2017 IT RISK MANAGEMENT”, Testin Predicts The Upcoming Enterprise Security Services Will Be The Merger Of Human And AI

GUANGZHOU, CHINA, December 26, 2017 /EINPresswire.com/ -- “The Upcoming Trend for Enterprise Security Services——Merger Integration of Human and Machine”, Dixon Ho, Chief Security Advisor of Testin, said at the 2017 Canton Tower Science & Technology Conference – Global Mobile Developer Conference and AI Summit Forum. He shared his thoughts and vision on the future of Enterprise Security Services.



In early 2017, with an online alias of “Master” in various international GO Servers, AlphaGo competed against dozens of the top Chinese, Japanese and Korean Go players in a fast-paced version of Go, with a continuous series of 60 victories. Artificial Intelligence (AI) can no longer be considered an objective in the distant event horizon, and pioneering businesses in the artificial intelligence domain are appearing like young bamboo shoots after the Spring rain. Many people are pondering whether Security AI or Security Robot will appear among us. Are we coming into an age of Artificial Intelligence in Security?

Mr. Dixon Ho had served as the Chief Security Officer for Microsoft Hong Kong and security director for Microsoft Greater China, as well as Chief Security Advisor for the 2008 Beijing Olympics and the 2005 Sixth Ministerial Conference of the World Trade Organization (WTO MC6). Now he has dedicated most of his career and professional life, to lead Testin Security Services team to serve mobile application enterprises’ concerns for quality and security. At the summit, Dixon narrated from the 3 different viewpoints of the past, present and future of the security domain, the greatest challenges to enterprise security, and the security strategy for the future.

Future Direction of the IT Security Domain

In his judgement, Dixon believes future direction of the IT security domain should encompass the dimensions of Human, Security Artificial Intelligence and Software Security Robotics. A large number of large enterprises in the contemporary world are already leveraging AI in the implementation of their business tactics. It is estimated that, in the coming 2 to 4 years, high accuracy security protection applications in the field of information security using AI technology will become increasingly mature, and the use of software security robotics in cross-disciplinary cooperation will become more stabilised in the next 3 to 5 years.

Within the Security Artificial Intelligence (S.A.I.) framework, the responsibilities of the 3 elements can be structured as:

1. Leveraging the cumulation of past experiences, the human element can be responsible to design, define and manage the security tasks, as well as the subsequent monitoring, auditing and quality assurance duties;

2. Security Artificial Intelligence can be tasked with the learning and “activation” of new experiences. To achieve this, it must be capable of self-learning and analysis, or what is commonly referred to as machine learning, and through the processes of self-learning, founding, extracting and integrating, assemble the Security Decision Making Knowledge Base (SecDMKB).

3. Software Security Robotics can be used as the executor of the security tasks. This would include such real world duties as patrolling and watch duty. Furthermore, through the utilisation and integration of S.A.I. application programmatic interface (API) and Software Defined Security (SDSec) within the IT infrastructural cross disciplinary cooperation, protecting the multi-tier information asset in synchronisation to attain the security standards with intelligent automation.

The Greatest Enterprise Security Challenges of Today

The high speed development of the Internet, the ubiquity of intelligent mobile phones and the explosion of mobile Internet applications not only brings unbounded conveniences to the users, but also a profusion of potential security hazards. Consequently, the enterprise security concerns are also shifting from PC security, web security to mobile security.

As shown by authoritative statistics in PRC, roughly one in every ten Android mobile phones on average have been infected by virus during 2016 – an infection rate of up to 10%.

According to Alibaba JAQ 2016 Annual Security Report, 3284524 new virus samples were added to the Alibaba JAQ Security mobile virus sample database during 2016, averaging about 9,000 per day.

Of the top 10 apps from 18 industries analysed, security loopholes were found in 98% of the apps for a total of 14798 cases, or an average of 82 loopholes per app. Data from the internationally acclaimed Gartner Group showed that 80% of the attacks took place in the application layer, and 95% of security violations were at the endpoint devices. At the same time, AV-Test.org pointed out that new malicious software was growing at a incredible rate of 390 thousand per day. The traditional anti-virus (AV) solution can ill cope with the enterprise security problems and challenges. Enterprise security problem has now reached a critical stage.

From the perspective of the DevSecOps practitioners, a similar challenge is also being faced today in the overall security integration. Within PRC, most of the research and development (R&D) teams are short on application security professionals. For the testing stage, commonly found application security testing (AST) tools are unable to root out all the security loopholes. Data from IDC indicated that the popular AST tools are only capable of discovering about 67% of the loopholes, and are unable to carry out detection of security loopholes in the business logic. The fiercely competitive market environment of PRC causes many enterprise R&D teams to release new applications or versions before the security loopholes have been fully addressed in order to meet the business timelines. At the operations stage, attacks such as Zero-Day Exploits (0 Day) and Advanced Persistent Threat (APT) through file-based channels are particularly difficult to defend against. Data is the core asset of enterprises, and security will determine the lifeline of enterprise development. Consequently, irrespective of whether the enterprise is engaged in traditional business or centred around the Internet, there is the necessity to re-think and re-strategise on security and threat counter measures.

The Future of Enterprise Security: Integration of Human and Artificial Intelligence

It is the opinion of Dixon that in the near future of the next few years, the security hierarchy will be constituted of an amalgamation of human, tools and learning machines to result in rigorously comprehensive security testing and security protection systems. Security Development Lifecycle (SDL) will continue to be necessary at the R&D stage. The technology today is still distance from full automation in business logic loopholes detection for the test and release stage. Experts and specialised tools are still the status quo for comprehensive security flaw detection, penetration testing and hardening. At the final operations stage, intelligent security protection framework of breath and depth will be necessary, so as to establish an overarching, multi-disciplinary security environment.

The security infrastructure of intelligent terminals must be able to defend against all kinds of attacks, including traditional, advanced persistent threat and zero-day exploits. Dixon has presented the leading worldwide “one stop mobile cloud application testing service” provider – Testin, and the jointly introduced S1 endpoint device intelligent security detection and protection scheme with the strategic US Silicon Valley security partners. Through a tri-dimensional monitoring and safeguarding strategy, S1 can help enterprises to deal with different levels of security challenges, including:

– Real-time dynamic cloud intelligence, utilising known malicious program hashes, IP addresses, network or host characteristics etc. to minimise the exposure to attacks;

– Advanced static monitoring and safeguarding, based on machine learning, exhaustive file inspection engine, to unearth known and unknown (0-day exploit) malicious software;

– Advanced dynamic monitoring and safeguarding, based on machine learning, to detect the unusual behaviours of different types of attackers and prevent attacks that use automate scripts, dynamic contents, null files and other techniques, to aid the enterprises to implement behavioural risk monitor and control so as to realise 360-degree comprehensive dynamic monitoring to protect the enterprise security.

It has been reported that cloud testing can provide S1 endpoint intelligent detection and protection and can be implemented without undue complexity to establish real-time viewable evidence. This will enable not only automated multi-tier monitoring against security threats, but can also protect against 0-day exploit and advanced persistent threat attacks, thereby resolving the security issues and challenges that cannot be handled by traditional AV software.

It is estimated that in the top10 applications of 18 industries, 98% of them have loopholes. Testin application security scanning assists customers to find them and provide the complete solution which further ensures business security.

The function of Testin's security product is based on T-leading security core technology, through the automatic way to detect the security risks and loop hole in Android application. We also give suggestions on how to solve the security issues discovered. It helps the enterprise understands and improves the security of the application, and avoid low level potential risk after it is in production.

The advantage of application security scanning (Compared with the traditional test)

Use static and dynamic scanning, malicious analysis and other technologies to locate code issues precisely.
Efficient automated scanning can issue security scanning report in 10 minute. Test process is completely recorded.
The code scanning tool of independent intellectual property rights, scanning checkpoints include configuration security, code security, component security, data security, encryption security, communication security, etc. Internal risk of application is detected comprehensively.
The issues and challenges being faced by IT management of the enterprises, in Dixon's opinion, will surely multiple in the future. The present day security strategy and tactics are already unable to satisfy the wants and needs of security management, and cannot accomplish the necessary seamless platform integration. In conclusion, the positioning of intelligence in enterprise IT security will invariably become an integral part of the critical core infrastructure. Enterprise must take the initiative to plan for the future and lay the next generation strategic groundwork to safeguard the invaluable data and informational asset in the age of artificial intelligence.

About Testin

Testin (http://www.testin.net) is the global leader in One-Stop-Application cloud testing services for applications such as web, mobile web, H5, native mobile APP, Lite APP, mobile games, VR/AR, wearable, AI, smart home, smart driving, IoT and industrial APP developers to provide the necessary one-stop testing services and quality assurance. Testin is the disruptor of the traditional software testing service mode, combine AI automated real device SaaS testing, crowdsourcing testing, full stack security testing and continuous big data analysis, succeeded not only in capturing the domestic market of China but also in sett its foot of the global arena, has now continued to serve more than 800,000 developers with their 2.3+ million APPs, branding clients including most tier 1 internet entities and McDonald's, Nestle, Starbucks, Daimler, BMW, Philips and Kabam, etc. Testin has been certified by ISO9000 , ISO27001 , ISO20000 , ISO17025, CMMI3 and CNAS, aim to help developers build confidence in their applications and ensure a good user experience. Testin has secured US$84.9 million in 3 rounds of IDG, Banyan, Haiyin, and CEL. Testin has been recognized as 2015 and 2016 Deloitte High-Tech & Growth Top 50 China, Red Herring Finalist 2014 Asia 100, 2015 Global 100 and 2017 Red Herring Global 100 Winner.

For more information about Testin please visit http://www.Testin.net, or contact +852-2392-6880 (Asia) or +1-516-277-6800 (U.S.)

Jerry Wang
Testin
+1 (516) 277-6800
email us here
