Antiy’s Next Generation Threat Detection Engine and Innovative Platform "Cyber Ultrabrain"

Founded in 2000 and based in Harbin, China, Antiy is a leading cybersecurity enterprise in the areas of threat detection and defence. Based on our next generation threat detection engine as well as our engineering experience, Antiy has developed a series of products such as Intelligent Endpoint Protection System (IEP), Persistent Threat Detection System (PTD) and Persistent Threat Analysis System (PTA). These products empower customers in endpoint protection, boundary protection, traffic monitoring, threat capture, in-depth analysis and incident responses. We are a core enabler for global supply chain security, chosen by around 100 famous security companies and IT vendors. Our threat detection engines are empowering over 3 million network and security devices and more than 1.5 billion intelligent terminals worldwide.

In the area of cybersecurity, threat detection engine is the main empowerer for security products. Hence, its ability to detect threats and output information is of utter importance. These abilities determine the scalability and detection power of security products, which further determines their threat hunting capability. Traditionally, detection engines aim at files and provide threat detection capability. However, many cyber criminal and APT groups have developed approaches to evade anti-virus engines, which make them an unreliable point in this process. Aiming at solving this emerging problem, Antiy has evolved its next generation detection engine into an integrated supporting node that combines targeted threat

detection, full-format object identification, in-depth preprocessing, vector output, threat information and intelligence output.

AVL, Antiy’s threat detection engine, can detect eight types of malware - including viruses, worms and trojans - of 13 million variants from more than 40,000 families. Its detection ability enables threat mapping to around 10 billion malicious samples. Meanwhile, besides the classification, name, and variant of the detected malware, AVL also outputs other relevant information and tags, especially behavioral capability tags conformed to the ATT&CK Threat Framework. This enables our data output to support higher level ATT&CK-based analysis.

The next generation AVL conducts complete type identification on all input data, with in-depth preprocessing and vector extraction for executables, packages, and compound document files. For executables, the engine can output information on attacking techniques, resources, and attacker identities through analyzing the result from unpacking, decrypting and running in virtual environment. The next generation AVL can also unpack various types of packages, self-extractions and setup programs. It is capable of analyzing and extracting their embedding relations. With compound document files and media files, AVL extracts their embedding content and associated domains. On average, it can extract more than 150 pieces of vector information from a single executable. All these extracted data form a full data set for vector analysis, hence enabling homology analysis, correlation analysis and rule set creation from vectors. With a mechanism of self-defined maintenance of decision tree, we empower our customers to form a vector-based scalable detection rule set.

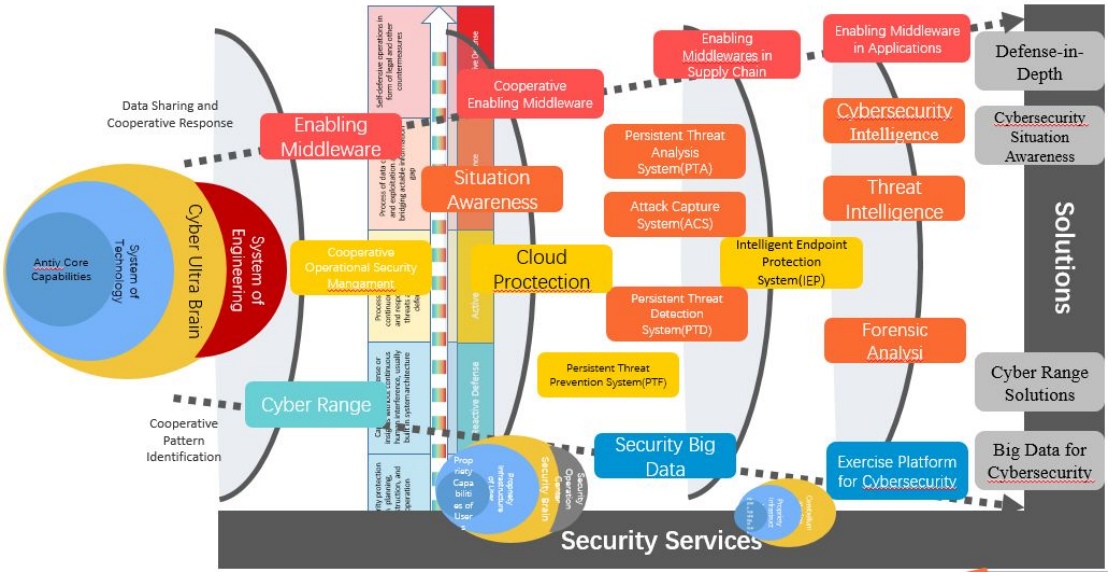
On top of in-depth recognition, preprocessing and

multi-dimensional vector output, AVL engine strengthens detection capacity based on AI-related techniques. With multi-dimensional vector output, AVL empowers users with the capability to analyze attacking tactics, techniques, and procedures. This provides effective support for the production of threat intelligence.

Currently, all of Antiy products —endpoint protection, traffic monitor, threat analysis, and incident response — have been updated to next generation AVL. We have also authorized our core partners with next generation AVL.

Faced with huge amounts of threats, countering these threats requires the ability of systematic analysis and defense. Antiy Cyber Ultrabrain (‘Ultrabrain’ hereafter) is an intelligent cloud-based infrastructure integrating threat capture, threat analysis, intelligence provision and security service management. By deploying sensing techniques such as lure mailbox and honeypots, Antiy is able to capture various threat data, capturing more than 1 million files and hundreds of millions of incident and alert data. These data are fed to Ultrabrain together with open source intelligence, producing efficient trace and analysis of threats and their targets.

Based on Ultrabrain’s threat capture ability, threat analysis ability, intelligence analysis ability, big data analysis capability and AI-related homology correlation analysis ability, our analysts and experts are able to trace, interpret and assess threats efficiently. This enables us to master new trends of cyber criminals and APT groups and help our customers with efficient threat hunting.



Picture 1 Antiy’s Product matrix