CYFIRMA

Bringing Threat Visibility and Predictive Intelligence into Cybersecurity

Historians credit Greece's victory in the Trojan War to the Greek Army's intelligent tactic to use the Trojan Horse. The unbreachable walls of Troy would not have fallen if the Trojans stationed at the gates had inspected the horse before letting it into the city. Today, in a similar case, cybersecurity solutions fail to protect enterprise networks not because of the integrity of their firewalls and other security controls, but due to the lack of proper intelligence and timely threat visibility. This challenge is resulting in the demand for smarter solutions that can monitor, detect, and prevent incoming cyber attacks. Singapore/Tokyo based CYFIRMA offers AI and machine learning-powered cybersecurity solutions that deliver accurate, predictive cyber intelligence across all aspects of an organization to ensure unparalleled protection. "CYFIRMA's contextual intelligence technology predicts and simulate cyberattacks and breaches before they happens, enhancing an enterprises' ability to proactively identify the threats and address the risks in their cybersecurity posture better safeguarding corporate data and reputation," says Kumar Ritesh, chairman and CEO of CYFIRMA.

The core challenge in today's cyberspace is an organization's reactive approach toward cybersecurity. Ritesh, with his extensive expertise of working in the cybersecurity realm, believes that organizations have to assess their cybersecurity posture from an external viewpoint in order to tackle the current and future threats that the ever-evolving cybercriminals pose. "CYFIRMA offers their clients with a hacker's point-of-view and informs organizations on the vulnerabilities in their system, and the motivations and maturity level of a hacker group, to aid enterprises in understanding the type of potential attacks that could be targeted at them," adds Ritesh.

Kumar Ritesh
Chairman and CEO

The company offers two types of solution for organizations with not very mature and mature cybersecurity posture. 1) 360°cyber services tailored daily and weekly intelligence reports for not very mature cybersecurity organization, and 2) For mature cybersecurity organizations, they offer cloud-based AI-powered Cyber threat visibility and intelligence (CAP) product, which organizations can use to perform threat hunting, correlation and attribution. The 360° services have a subscription model where clients receive daily and weekly intelligence reports offering detailed insights into who the hackers are, why they are interested in an organization, their background, what are they interested in, their motivation, how ready they are to launch an attack and how they can potentially attack. Additionally, the company's intelligence-driven brand and executive monitoring, cyber risk scoring, cyber vulnerability analytics, and cyber education solutions provide a more focused product portfolio for clients to utilize in order to strengthen the security of their brand, asset, networks and more importantly people.

CYFIRMA delivers unmatched predictive cyber threat visibility and intelligence through their cloud-based platform by employing the most advanced and cutting-edge AI and ML technology using data mining and analytics techniques to help proactively identify, quantify and prioritize potential cybersecurity threats. CAP collects threat data from thousands of different and discrete sources that include open source, closed source, government intelligence, CERT, ISAC, CIRT, commercial forum, social platforms, news forums and peer to peer channel. The unique value proposition of their technology offering is the ability to embed itself into Dark Web channels that are typically used by hackers to communicate with each other and plan an attack. CYFIRMA's technology silently monitors conversations over a hundred forums without interacting with the perpetrators to avoid detection. Subsequently, when the solution detects the name of a client in a discussion, it starts to capture conversation-level information and brings it into CYFIRMA's Cyber Intelligence Analytics Platform (CAP). CAP applies five layers of AI and ML engines to filter the data and structure the information to aid organizations in understanding the profile of hackers, their reason for breaching a client business, and assesses the perpetrators' arsenal of potential attack methodologies to predict the timeline for a potential attack.

The company delivers the information gathered from the CAP analysis to the customer in three different segments—Strategic Intelligence, Management Intelligence, and Tactical Cyber Intelligence. The Strategic Intelligence segment informs clients about the "whos" and "whys" of a potential cyber attack and helps businesses gain an understanding of the vulnerabilities in their cybersecurity to ensure effective protection. With Management Intelligence, enterprises gain an idea on how to integrate CYFIRMA's insights into their system and make the necessary changes: policy revisions, incorporation of newer cyber threats into the current incident response processes, and more. Finally, the Tactical Intelligence supports customers in the day-to-day detection of active threats to improve their cyber posture.

> "CYFIRMA's contextual intelligence technology predicts and simulate cyberattacks and breaches before they happens, enhancing an enterprises' ability to proactively identify the threats and address the risks in their cybersecurity posture better safeguarding corporate data and reputation"

In the coming years, the traditional approach of deploying data security such as building stronger firewalls will put businesses at risk because hackers and perpetrators will continue to find newer and more innovative ways to break into an enterprise network. CYFIRMA, with their predictive threat visibility, is spreading awareness of the need for cyber intelligence and helping organizations cope with the increasing threat of cyber attacks. "Cyber intelligence will become the center of cybersecurity to ensure effective protection of enterprise networks in the future of cyberspace," concludes Ritesh. ES