Full name: Changming Liu
Position: CEO and co-founder

1. Tell us a little bit about your history. How did Stellar Cyber originate?

Stellar Cyber was founded in 2015 by Changming Liu and Aimei Wei. Changming, CEO and co-founder, previously founded Aerohive and Trustgo, and was an early employee and a key architect at Netscreen, which was acquired by Juniper in 2004 for $4 billion. Aimei, CTO and co-founder, had worked for both early stage startups (Nuera, SS8 Networks, and Kineto Wireless) and well-established companies including Nortel, Ciena, and Cisco.

Aimei knew first-hand the frustration security analysts have in trying to combat cyberthreats with collections of stand-alone tools. With stand-alone tools, analysts must manually correlate alerts from various tools to gain a complete picture of evolving cyberattacks, but the volume of alerts makes it nearly impossible for them to do so. Aimei's idea was to build a central console with core cybersecurity capabilities that could ingest and correlate data from other, stand-alone tools to provide a 360-degree view of the threat landscape.

2. Can you tell us a little bit about what you do? What issues do you mainly focus on?

The Stellar Cyber Open XDR Platform solves the problem of siloed security tools by ingesting data from its own and third-party tools to present a complete picture of evolving cyberthreats while protecting existing investments in other security tools. Stellar Cyber's platform was the first Open XDR solution, and it not only ingests data, but it correlates and analyses that data and then offers contextual, prioritized incidents with recommendations for how analysts can address them.

3. What types of technology do you use to detect threats before it is too late?

Stellar Cyber's platform incorporates AI and machine learning to evaluate alerts from disparate tools and group them into incidents. The platform also includes NDR (network detection and response), next-generation SIEM (security incident and event management), and TIP (a threat information platform) to monitor network traffic and evaluate security incidents, and integrates with any EDR to add to investment protection and ensure everything detection and response.

4. How do you think the pandemic influenced the ways in which threat actors operate?

With many employees working from home, hackers have seen their attack possibilities increase significantly. Hackers are more likely to target home-working employees' computers to obtain access to corporate networks.

5. In the age of frequent cyberattacks, do you think small businesses and big enterprises should rely on the same security measures?

Yes, but the way they go about using those measures is different. Enterprises can afford a staff of security analysts and will use security tools and an XDR platform to manage threats.

Small businesses can't afford teams of analysts or the most sophisticated security tools, so they should work with an MSSP (managed security services provider) to offload the security function. Many MSSPs use Stellar Cyber's Open XDR platform as the core of their offerings.

6. As XDR solutions are starting to gain popularity, some still might not be familiar with this topic. Could you briefly explain how is it different from traditional detection and response?

Traditional detection and response involves analysts chasing threats without proper context. An analyst might use several different tools that report security alerts, and then he or she must chase down those alerts one at a time. Often, analysts miss sophisticated attacks because they are reported as relatively benign incidents in several different tools, and the analyst can't effectively correlate those incidents to see the big picture.

Stellar Cyber's Open XDR platform automatically correlates data from multiple tools, groups related alerts from multiple tools, and then reports contextual incidents that can be immediately acted upon.

7. With remote work becoming the new normal, what are some of the worst cybersecurity habits that can lead to serious attacks or breaches?

One of the worst habits is clicking on links in emails. These phishing attacks are a common way of installing malware on user computers. Users should always make sure an email's Send domain matches the content of the email. For example, a Send domain support@locklife.com doesn't match the actual company, Lifelock.com. Text messages have the same issue, and users need to remember that large vendors like AT&T or Bank of America never send texts about account blocking or giveaways.

Remote workers should use virtual private network (VPN) connections to secure and encrypt traffic between their systems and the corporate network. Otherwise, the traffic is open to snooping and login passwords are vulnerable.

Many remote workers forget about maintaining adequate backup and recovery systems. Backups are critical for recovering data in the event of a breach.

Enterprises should train their workers on all these techniques, and they should adopt XDR security systems to protect against breaches based on the behavior summarized above.

8. What new threats do you think the public should be ready to take on in the next few years? What security tools should be implemented?

Siloed security tools look at individual "trees" in the forest, rather than the whole forest. Hackers will always look to get in between the trees. XDR systems look across tools and block hackers' newer strategies. Machine Learning adds context, so while seemingly authentic transactions alone may look authentic, when look at in context as a cluster of events, analysts can see the "forest" to spot complex, multi-layered attacks.

Hackers continue to advance and so will XDR thinking. Hackers will get deeper into the

applications, deeper into the hardware and deeper into the data that defines who we are. XDR will continue to advance as well by making the existing protection better through better intelligence, and by advancing AI and Big Data sciences purpose built for cyber security

9. Share with us, what's next for Stellar Cyber?

Stellar Cyber recently completed a $38 million Series B funding round that included Samsung, Highland Capital Partners, and all existing investors because the company has demonstrated its leadership in the XDR markets with 3x year-over-year growth and nearly 1,000 customers globally. Cyberattacks grow more numerous and sophisticated continually, and Stellar Cyber continues to innovate with its platform to offer the most comprehensive solution to this threat. The combination of accelerated migration to the cloud and the need to provide security for remote workers is increasing demand for more powerful and streamlined solutions. As the enterprise security industry matures, Stellar Cyber is going to be a leader in the $20 billion XDR market.