PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SELIM AISSI
CISO, ELLIE MAE

HEADQUARTERS: Pleasanton, California
EMPLOYEES: 1,500
ANNUAL REVENUE: $417 Million

About three years ago, Selim Aissi embarked on building a security program from the ground up as CISO of Ellie Mae, the leading cloud-based platform provider for the mortgage finance industry. Leveraging his extensive experience in financial and technology security, along with thought-leadership acumen, Aissi developed a strong security and risk management and worked hard to bridge the gap between Ellie Mae's board of directors, executives, engineers, customers, and partners.

TOP STRATEGIC GOALS AT ELLIE MAE

Aissi leads with four specific, strategic goals to continually ensure he aligns security with the business and makes an impact on the overall organization.

Protecting customer data. For Aissi, this means implementing necessary controls, accessing and understanding risk, and making the right investments to protect customer data.

Automation. Aissi says, "It's key in this space that whatever can be automated, is automated. A lot of the things CISOs do are based on workflows (e.g., incident management, vulnerability management, and patching). All these workflows should be automated. One of my strategic goals has been to automate any security-workflows that could be automated."

Innovation. Pushing limits in terms of detection, monitoring, and remediation are key for Aissi when it comes to innovation. He has deployed many of these innovations and his team continues to be at the cutting edge.

Customer-orientation. "This means continuously talking to customers, understanding their challenges, helping them out when they need help, and learning from them. We have thousands of financial customers and a lot of what they do and what they see is very relevant to us. So, I've started a lot of engagement with our customers' CxOs to share learnings and help them succeed. Since we work in the same space, we're targeted by the same adversaries, and we want to be able to share as much as we can," explains Aissi.

STRATEGY TO COMBAT THREATS

Aissi implements core tenets to continually and proactively combat threats impacting Ellie Mae. The first one is solidifying a strong cyber threat intelligence program. He comments, "The purpose of having a cyber threat intelligence program is to be able to predict most

of the attacks, and to correlate many incidents so that similar attacks can be avoided in the future. This program also helps to quickly collect indicators of compromise and to effectively use them for prevention, monitoring, and forensics."

Aissi also believes that having a strong insider threat program to manage threats is critical. He values building a threat management program based on risk since not all threats are created equal. This type of program enables quick assessment and evaluation of threats, as well as making decisions about the criticality of an incident.

Another important aspect of a threat program is having a strong and effective Security Operations Center (SOC). He says, "When there's a threat, any related alerts should feed into the SOC in real-time. The SOC should analyze it and quickly react to it. Having an effective SOC team and process are key. It's also important to have automation when it comes to threat management. When an incident happens, the whole workflow should be automated including threat hunting, mitigation, investigation, forensics, all the way to the closure of that incident."

The last tenet of Aissi's approach is making sure incident management is proactive and practiced. He believes that security teams should constantly practice this to know whether their workflows work. For him, he says a strong process and meticulous fine-tuning as well as enrichment ensure that incident management is effective.

THE REALITY OF PHISHING THREATS

"The biggest threat we see is phishing. These types of campaigns are massive and they're getting more sophisticated and more targeted. They're coming with new weaponized payloads and new credential-harvesting techniques," explains Aissi.

He continues, "The thing about phishing is that it's a "gateway." It provides an attacker access to many different valuable assets in a very unique approach that leverages human weakness. Social engineering will continue to be an effective method for adversaries. Many years ago, I used to see a lot of targeted attacks where the attacker would go straight to a database. However, today that's not even necessary because if an attacker can launch a very targeted spear-phishing attack that is based on exhaustive reconnaissance, their chances of stealing sensitive information from their specific victim are much higher. They don't need to spend two or three months getting into a database because social engineering is a much easier approach and it's more cost-effective for the attackers."

To combat these types of attacks, Aissi relies on having necessary cybersecurity controls at different levels. While educating and training employees also plays a major role, he says it should be a balanced approach.

For internal education, Aissi focuses on awareness and simulated phishing attacks so employees learn to pay attention to details. In his experience, most phishing emails can be detected visually if employees are well-trained.

When it comes to available commercial security tools, Aissi says many of those can drastically reduce the number of known phishing attacks, however many technologies and processes need to be built internally and continuously fine-tuned and enriched. He comments, "These tools, if they're not self-learning, need to be fine-tuned all the time because you don't want to block good email. The number of false positives needs to be reduced to near-zero, otherwise it's not an effective cybersecurity tool. This is where it's important to be able to have an effective security program and not block the business since legitimate emails still need to go through. Fine-tuning and adding intelligence to these products and solutions is really important when it comes to spear-phishing. I call this ensuring that all cybersecurity controls get the necessary TLC!"

What advice do you have for other CISOs?

"CISOs cannot speak buzzwords, they must understand security technology and innovation trends to make decisions about what solutions to deploy and how to address operational and business risks. They must also be a credible partner to the business and to customers. A CISO should partner with all executives to make decisions together and should aspire to be an enabler to the business. Last, CISOs must be practical but also strategic. They should be able to build an effective security program and describe all of the components of that program in business terms. My last piece of advice for other CISOs: never stop learning!"