TYLER FARRAR

CISO
EXABEAM

exabeam

HEADQUARTERS: Foster City, CA

EMPLOYEES: 669

REVENUE: Private Company

DESCRIBE YOUR ROLE AT EXABEAM?

My role is classified into three major areas. First is more traditional corporate or enterprise cybersecurity – looking internally into the organization and protecting our enterprise infrastructure and the endpoints that our employees use. The second area is within product security, securing the products that we sell to our customers. The third area is related to external engagement and telling the story about myself, our company, the industry, and our product. Because we use the product internally, I am able to share my experience of how Exabeam uses Exabeam.

HOW DO YOU ENSURE SECURITY IS BROUGHT IN AT THE BEGINNING OF THE SDLC?

It's all about building a risk-aware culture. It's a change in mentality with a group that is used to working quickly and deploying software to build a product. There are obviously tools that can do the work of identifying the issues or shoring up various prevention controls, but when those issues arise, it's about teaching and partnership.

So, how do you then engage and try to do it in automated means? Maybe the engineering manager is going to know that the developer didn't clear a specific finding or vulnerability, and they deployed vulnerable code to production. It puts the onus and responsibility on the manager, not just the CISO or the cybersecurity organization, to hold their team members accountable and own their part in securing the organization.

HOW ARE YOU APPROACHING THIRD PARTY RISK?

Our third party risk program spans from being able to inventory all of our vendors to classifying the criticality of these vendors to Exabeam. I'm talking about how vendor dependencies can impact our business operations. It enables us to determine how long we can be down for.

From a security perspective, it's about defining a discrete set of criteria. So when we go through the procurement process, my team is always able to assess the vendor risk to the business. This is executed through the assessment of specific criteria; from compliance certifications to policies to diagrams and system security plans, etc.. We want to uncover: What is the true risk to Exabeam, and are we comfortable with that risk score?

WHAT CONVERSATIONS DO YOU HAVE WITH CUSTOMERS ABOUT THIRD PARTY RISK?

We highly value all aspects of cyber assurance. Just as Exabeam conducts its own third party risk assessments, our customers perform the same on Exabeam. We're not only expected to be able to provide answers to these questions, but also provide the evidence to show that policies and controls have been implemented to manage and mitigate risk. This is all about partnering with our sales teams and assisting with RFPs. We must be able to effectively deliver on requested information, as well as be in tune to what best practice industry standards are and what our customers expect of us. In regards to what we demand of our vendors, we try to have that coalescence

of equality – being able to say that we feel comfortable with the business relationships that we're in.

WHEN YOU'RE SPEAKING TO CUSTOMERS WHAT OTHER CONCERNS DO THEY HAVE?

Ensuring adherence to various regulations and compliance certifications are important to our customers. Outside of that, I've seen a growing number of inquiries around crisis management; how does Exabeam respond when something bad happens? Business disruptions can and will happen. Therefore, Exabeam has prepared for these operational disruptions to ensure continuous availability of our product and our business. So, I see questions come in - What are your SLAs around this? Do you have an incident response plan? Do you know how to manage the business through a crisis? These questions are really centered around business continuity and disaster recovery.

HOW DO YOU APPROACH BUDGET SPEND?

Just like we approach security - it's everyone's responsibility. Security doesn't stop where my team ends from a functional organization perspective. At Exabeam, there are people focused on security within research and engineering, as well as product security and compliance management. They don't have to report to me to do that. We are all responsible for instilling a culture of security.

HOW DO YOU COMMUNICATE EFFECTIVELY WITH EXECUTIVES AND THE BOARD?

It can be broken down into a step by step process. Every month, the core technical metrics are compiled, which conveys key trends and risks. At the end of the quarter, these metrics tell the story; Are we where we want to be in our journey? What are our key risks? I then take all of this information and distill it for the next phase: telling our story to senior Exabeam leadership. We then go meet with the board, ensuring that we are communicating what the overall security posture is across enterprise and product infrastructure, key accomplishments, key risks, and key priorities.

WHAT PREVIOUS EXPERIENCE DO YOU HAVE PRESENTING TO BOARDS?

In my previous role, I presented to the Board Risk Committee. During my military service, I was responsible for leading various cybersecurity operations. Following each operation, I was responsible for conducting a briefing on the result and effectiveness of the operation to senior military leadership. While the military and private sector are different, there are many parallels in how we analyze and present our overall program.