CHRIS BATES

CISO
SENTINELONE

SentinelOne

HEADQUARTERS: Mountain View, CA

EMPLOYEES: 2,100+

REVENUE: $422 Million

HOW WOULD YOU DESCRIBE YOUR JOB?

My job is to protect SentinelOne's employees, systems, and fleet from attackers and misuse, and I am also responsible for building trust through proactive transparency with our customers.

I just took on a new role as Chief Security and Trust Officer, and will be enhancing our trust program to drive greater transparency around how we use, store and access data and proactive, honest communications with key stakeholders.

HOW DOES SENTINELONE PROTECT CUSTOMER DATA?

We have a very robust insider threat program through which we monitor usage, and a very robust security program overall. Data is stored in a way of least privilege, and it's encrypted. We monitor all access and there are a lot of trips and gates that allow us to detect abnormal usage in real time. We use a lot of automation to handle responding to and investigating possible malicious activity.

HOW DO YOU ENSURE SECURITY IS BAKED INTO THE SDLC?

I run a team called Application Security and their sole job is to partner with the R&D teams as they're designing things. They start from teaching how to write secure code to actually enforcing the SSDLC, which includes security reviews and how we develop code in a secure way. They also man all of the gateways and checkpoints to make sure that when code is checked in, it's got a threat model applied to it. We have tooling that scans code at commit and blocks it if it has issues. Once the code is deployed via the pipelines into production, then I bring in a Production Security Team to make sure that the only things running in production come from the approved pipelines, from the approved code, and are configured in the approved way. They monitor to make sure nothing running in production is modified in a way that it shouldn't be.

WHAT HAS YOUR EXPERIENCE BEEN LIKE WORKING ON BOTH THE VENDOR AND END USER SIDE?

Since I've worked on both sides, I look for vendors who are going to be partners with us. Vendors can tell you whatever they want, but when stuff goes sideways - and it always goes sideways - are they going to be the people standing next to you to fix it?

I work for a data company, so I ingest a lot of data and I can do a lot of cutting-edge things. For instance, I think right now, 80% of my tickets are fully automated. The SOC never even sees them. From the time it fires to the time it's resolved, the SOC never touches it and it gets into user validation and interaction. And that's pretty cool from an efficiency and productivity standpoint.

HOW DOES SENTINELONE'S SECURITY BUDGET COMPARE TO END USER ORGANIZATIONS?

I report to the CEO and the board. And we receive the funding we need to do what we need to do. We scale the budget by breaking it down per team. For example, the GRC team is based on compliance and sales needs, the security engineering team is based on data and automation. Appsec is scaled with the CTPO's

organization. Each team has its own specific alignment to a business driver, and as that business driver scales up or scales down, we scale the budget.

IS THERE ANYTHING ELSE YOU WANTED TO SHARE ABOUT WHAT YOU ARE DOING AT SENTINELONE?

We've just announced new generative AI capabilities within our threat hunting platform that are going to transform security. Essentially, we're putting the power of AI in the hands of security teams to help them detect and respond to threats at machine speed. And they don't need to know detailed query languages to do it. Through our platform, they can ask a native language question, and not only will the system return the data, it will suggest other questions they may not have thought about and recommend four or five actions they should consider. It's going to change the way people in the SOC and security work.