eCorner

Stanford eCorner

In Hackers We Trust

07-12-2016

URL: https://stvp.stanford.edu/clips/in-hackers-we-trust

Synack’s Jay Kaplan discusses how the cybersecurity startup he heads mitigates concerns stemming from the practice of using crowdsourced hackers around the world to identify vulnerabilities in the systems of private companies and government agencies that serve as customers. Synack’s safeguards include rigorous vetting and tracking, as well as placing high “bounties” on the most serious vulnerabilities.

Transcript

- But, thinking about solving cyber-security using crowd sourcing? That sounds crazy, right? Well, it sounded crazy to us, too, but we started to ask people, if we created a solution like this, would you actually use it? We asked real potential customers.. We asked people back at the NSA, does this sound even feasible? And they said, you know, it does, but what you have to really think about are all the implications with, as it relates to crowd-sourcing in the consumer space, and you have to address those implications for business.. And so there are five things that we sought to address.. One, trust, right? These are hackers we're talking about.. How the hell do you trust a hacker, right? So we inserted a vetting process, we do background checks, we do ID verification.. We have to do this globally, right? We're in 40 different countries today, and so we had to enlist the help of a lot of third-party companies to help us do that.. We also vet our researchers from a skills perspective.. We only want to work with top people, right? And so we can't just say, I need Joe Shmoe off the street, come work for us.. We put them through a practical exam and a written exam to make sure they meet our minimum bar of skills.. Scale: How do we scale this business? Ultimately, there is, like I mentioned, a shortage of talent in this space, right? And so, for us, we recognize that in order to be a scalable company long-term, we had to turn to technology..

We couldn't just rely on people alone.. And so we decided to create an automation platform, in conjunction with the researchers we would be utilizing, in order to automate some of the low-hanging-fruit attacks that they're throwing at our customers, and that has turned out to be an amazing resource for us, and we've been putting a lot of engineering effort into that technology.. Management: How do you manage hundreds if not thousands of hackers around the world, and how do you enable customers to interface with them on an ongoing basis? Well, we created a platform.. We created a whole online interface where researchers can submit vulnerability data that they find on customers.. We created an interface for customers where they can see what's happening and all the high-impact vulnerabilities coming from our researchers.. And all of that is contained in one easy-to-use online interface.. We even have a function for our own internal team to leverage interacting with both sides.. Engagement: How do you keep researchers, we call them researchers, by the way, it's a little less scary than hacker, but how do you keep researchers engaged, how do you keep them motivated to find these really hard issues? What if they're only looking for the really easy stuff to find? So, what we inserted was actually a bounty-driven approach for conducting vulnerability research.. So we basically said, if you're a hacker and you go through our vetting process, you find a problem on one of our customers, we're only gonna pay you if you exploit that customer, you find a vulnerability on that customer, and we're gonna pay you based on the impact to that organization, right? So it really aligns the economics in a fundamentally better way, so we're not paying them time-and-materials, they don't get paid unless they're finding things, and they're getting paid when they find really serious stuff, a lot of money, we paid up to $25,000 for a single vulnerability so far.. And then intelligence, right? How do we make sure we understand what the researchers are doing, right? It's one thing to say, okay, we're getting lots of vulnerability intelligence coming from the researchers, but how do we actually know what they're doing on a day-to-day basis, and long-term, if a customer is getting more secure, hopefully we're not finding anything anymore, so how do we actually prove to that customer that we're still doing work, right? And so we have a whole analytics and intelligence platform that feeds real-time data to our customers..

So that's how we've addressed all the problems with crowd-sourcing as it relates to the cyber-security space and as it relates to hackers...