HORIZON3.ai

EFFECTIVE SECURITY DEFINED AND REFINED

Horizon3.ai CEO Snehal Antani on Resetting Enterprise Security Expectations

ISMG
INFORMATION SECURITY
MEDIA GROUP

SNEHAL ANTANI

Antani is an entrepreneur, technologist and investor. He is CEO and co-founder of Horizon3.ai, a cybersecurity company using AI to deliver autonomous red teaming and penetration testing. Previously, he was CTO and SVP at Splunk and held multiple CIO roles at GE Capital. Antani started his career as a software engineer at IBM.

At a time when ransomware, zero-day vulnerabilities and supply chain threats are rampant, what is effective security? **Snehal Antani**, CEO of Horizon3.ai, defines it in today's context and describes how enterprises can achieve and maintain it.

In this exclusive video interview with Information Security Media Group, Antani discusses:

- What constitutes effective security;
- Where enterprises are unknowingly deficient;
- Why this isn't a tool problem.

DEFINING EFFECTIVE SECURITY

TOM FIELD: How exactly do you define effective security?

SNEHAL ANTANI: In my own personal experience as a CIO and a CTO, the challenge I had was: I did not know if my security operations center was effective until I was breached. And by then it was too late. I didn't know if I was logging the right data or had configured the right alerts or if my password policies were actually working. My hope and vision was to assess my security posture prior to a breach so that I'd know that my security is effective and I could iron out all those kinks and challenges in the process, versus waiting until I'm already in the news.

“Organizations have not properly assessed their security infrastructure and they’ve over-rotated to just looking at specific CVEs to patch. Meanwhile, the attackers have adapted to all the misconfigurations and defaults and poor passwords.”

ORGANIZATIONS’ SECURITY DEFICIENCIES

FIELD: Where are most organizations unknowingly deficient until they get hit by that breach?

ANTANI: Today, attackers don’t have to hack in using zero-days like in the movies. Often, they’re able to just log into your environments using valid credentials that they found somewhere else. If an attacker is able to find a valid user ID and password from one place and then combine that with a misconfiguration in software that you’ve got in your environment or a dangerous product default, that attacker can go from an unauthenticated user to a domain administrator in the network and not have to use any malware or CVEs. That is effectively how ransomware operates today. Organizations have not properly assessed their security infrastructure and they’ve over-rotated to just looking at specific CVEs to patch. Meanwhile, the attackers have adapted to all the misconfigurations and defaults and poor passwords, and they can combine those together to achieve an effect.

IT’S NOT A TOOL PROBLEM

FIELD: Is it a tool problem?

ANTANI: Absolutely not. On the defensive side, we have more than enough tools. At Horizon3, we do autonomous pentesting, which doesn’t require any humans and has no custom scripts to write and no agents to deploy. We can run as many pen tests as necessary to assess your security posture. Our autonomous pentesting algorithms allowed us, in working with a very high-end bank, to go in 7 minutes and 19 seconds from an unauthenticated user to domain admin on the network. As a domain admin, we had keys to the kingdom. We could destroy all the data, tear down all the clouds and lock out all the users – after 7 minutes and 19 seconds.

This bank had every Gucci security tool you could buy on the market – the flashiest SIEMs, the best MDRs or EDRs and so on – yet not a single security alert had been triggered because those tools were not designed to work together. They were not properly tuned, and the organization had an effectiveness problem. In that scenario, the role of autonomous pentesting is, effectively, as a sparring partner, where you're consistently able to run pen tests, look at what tools and alerts went off and what didn't go off and then use that to tune and improve your effectiveness before you've been actually breached.

RED, BLUE AND PURPLE TEAMS

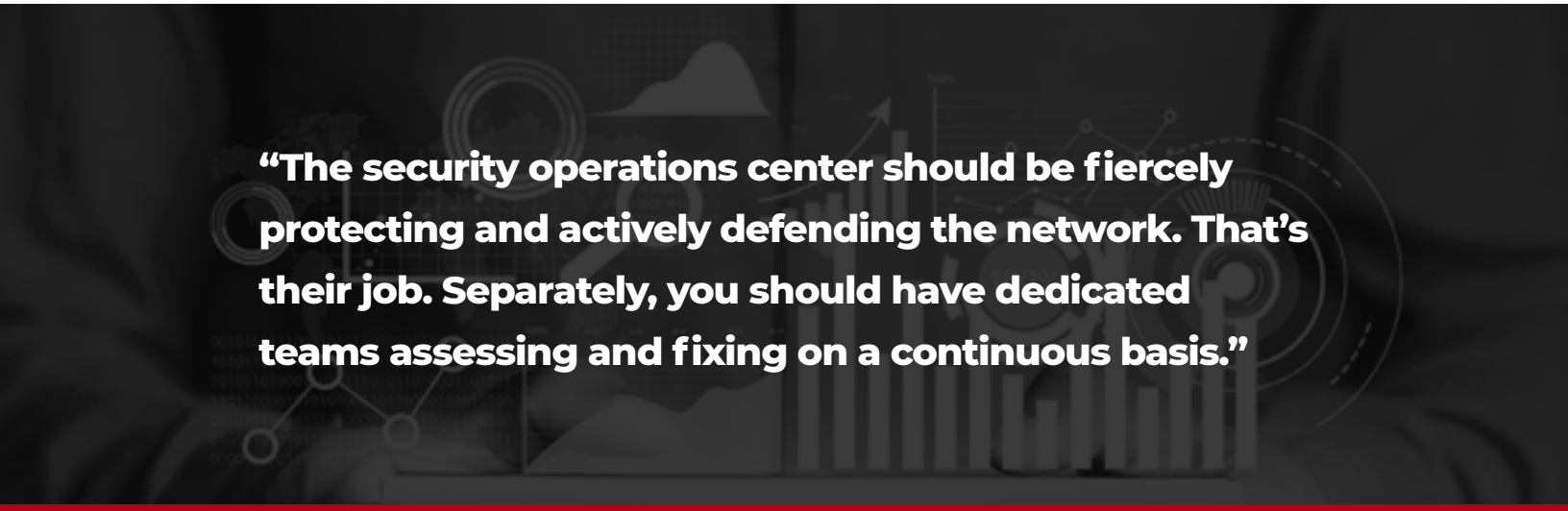
FIELD: Isn't this what red, blue and purple teams ought to be doing? Where are they going wrong?

ANTANI: There are a couple of interesting dynamics there. Purple teaming is much more a culture than it is a particular organizational structure. Today, the red team often consists of consultants that show up once a year, poke you in the eye, embarrass your team and then disappear. Then the blue team is left scrambling with a PDF with 100 pages of random problems to fix and as they fix them, they have no way to properly verify that they have been fixed. So, the relationship between the red and blue teams is very adversarial, number one, and number two, very transactional, where it's a one and done. As a result, they never properly work together. You need to set conditions where the red and the blue teams work together and share the goals of proactively finding and fixing problems. As the red team is continuously finding problems, the blue team can go fix them and then the red team can verify that the problems have truly been remediated. This cycle of find, fix, verify – on a continuous basis – sets the conditions for a purple team culture.

EFFECTIVE SECURITY IS CONTINUOUS

FIELD: So effective security clearly can't be one and done. How do organizations ensure ongoing efficacy?

ANTANI: You need to continuously assess and continuously fix, and that should be separate and distinct from continuously defending. The security operations center should be fiercely protecting and actively defending the network. That's their job. Separately, you should have dedicated teams assessing and fixing on a continuous basis.



That allows you to not have teams dilute their focus: You've got one team focused on assessment, one focused on fixing and one focused on defending.

THE HORIZON3.AI APPROACH

FIELD: How does Horizon3.ai help its customers to redefine and maintain effective security?

ANTANI: We consistently see two big use cases. Number one is serving as that sparring partner for the security operations center, to make sure that its tools are working properly and have been tuned properly, and that it knows that its security posture can actually work prior to the breach. It's all about proactively verifying and improving that posture. The second use case is enabling the red and blue teams to work together in this find-fix-verify loop. You run our autonomous pentesting product to find your problems, and then the blue team fixes them and then you rerun our product to verify that those problems have been fixed.

Finding talented red team members is a big challenge for organizations. They're few and far between, and they tend to be unstandardized in terms of their skills. They all tend to be artists applying their own techniques. The really large banks can afford to hire a few, but the rest of the market can't. So our product was not designed for security people. Most of our users are IT administrators, network engineers and security tools admins. They are not pentesters but with three clicks, they're able to behave like a pentester with 20 years of experience. We've enabled those fixer teams to have the red team on their fingertips.

THE FUTURE OF SECURITY: OUR VISION

The future of cyber warfare will run at machine speed – algorithm vs. algorithm – with humans by exception.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® (Just for Credit Unions) GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY (Prevention. Response. Notification.) CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io