deepwatch

Deepwatch is redefining the SOC and how customers protect their brand, reputation and digital assets

Charlie Thomas, CEO

Businesses of all sizes are migrating applications and data to the cloud and are thereby creating larger online footprints as they transform into digital enterprises. This creates greater conveniences for their customers, but it also increases their security risk profile. As a result, companies are focusing on improving their overall security posture.

In parallel, security tools and technologies continue to advance. This proliferation of security solutions can be overwhelming for security teams, but can also drive significant benefits in terms of automation, increased collaboration and improved reporting and transparency for them.

Developing and implementing a security strategy that adopts best of breed technology solutions, while allowing flexibility to add and remove solutions as the threat landscape rapidly evolves, all while balancing a combination of internal and external resources is extremely challenging.

In light of the foregoing, we're thrilled to present Deepwatch.

Deepwatch's innovative cloud SecOps platform and relentless customer focus are redefining the managed security services industry. Deepwatch provides highly tailored managed security services driven by its unique IP which is tightly integrated with best of breed technologies and a world-class team of engineers and analysts. Its advanced maturity model automatically indexes and benchmarks each customer's overall security posture and charts a course for steady improvement.

Charlie Thomas is the CEO of Deepwatch He spoke about the company in an exclusive interview with The Silicon Review. Below is an excerpt.

What motivated you to establish Deepwatch?

I've been a long-time entrepreneur involved in leading and advising numerous start-up and growth stage technology companies. I'm passionate about building and growing companies, and I have an infinite amount of respect for all entrepreneurs, whether a 1 person company or a 1000+ person company. I love working with passionate, smart people and it's rewarding to watch our team members grow and prosper individually and collectively.

In 2015, Justin Moorehouse and his partners at Guidepoint Security had the idea to launch a game changing Managed Security Service (MSS) to address significant gaps it was seeing from its customers. After a lot of research and customer input Guidepoint's vSOC (Virtual Security Operations Center) was created. I had been a Board member at GuidePoint since inception and became CEO of the vSOC business in 2018. We spun out vSOC as an independent company named Deepwatch in 2019. We've been fortunate to have an amazing team that is growing the business by over 100% annually the last five years.

Explain your services in brief.

We currently offer three services. Our Managed Detection and Response Service (MDR) provides 24/7/365 threat detection, alerting, validation, and proactive threat hunting. Second, our Managed Endpoint Detection & Response Service (EDR) provides management of endpoint detection solutions and, finally our Vulnerability Management solution provides the people, process, and technologies to fully or partially administer vulnerability management programs for our customers.

Overall our customers leverage our services to free their teams from the time-consuming tasks and high costs of implementing, hosting, administering, and integrating their cybersecurity technologies while achieving their desired security outcomes.

How are you changing the MSS/MDR game and how are you different from other providers?

Back in 2015 when we were looking at the MSS Provider (MSSP) market, there was a one size fits all approach. MSSP's were serving all customers in the same manner - essentially as numbers on a list. Customers didn't know the analysts on the other side that were doing the work. In security, contextual knowledge is essential. Deepwatch developed a unique approach called our **Squad Delivery Model**. We assign a named team of seasoned security experts to collaborate closely with each customer. These security experts become intimately familiar with the uniqueness of each customer's environment, their teams, and their business and security objectives.

From a technology perspective, MSSPs say they support a broad range of technologies. If you think about it, developing core competence across a wide set of technologies is not achievable. There isn't enough security or engineering talent available to hire dozens of engineers who are expert with Splunk, Nitro, Exabeam, LogRhythm, ArcSight, etc. So we carefully analyzed and vetted the best-of-breed technologies in each NIST category and picked the best with our relentless focus on outcomes to our customers. We built our **Security Operations (SecOps)** platform to provide comprehensive coverage for every aspect of our customers' security operations by seamlessly integrating industry-leading technologies tightly integrated with our own IP.

Deepwatch has developed its own unique content distribution and management platform — we call this our **Content Management & Distribution Platform**. This unique data and platform enables us to manage, manipulate, and measure hundreds of SIEM instances at scale from a single solution in a highly automated fashion. This platform consists of proprietary metadata which is unique to every customer, every log source and every use case which are correlated to industry standards, frameworks, and compliance regulations.

This property metadata combined with our proprietary scoring mechanism enables us to generate automated security posture indexing - scoring - which we call our **Maturity Model** - for every customer. Our Maturity Model indexing is used by customers at the Board Level to measure and manage progress against their security objectives. It is the driver of their entire security program. Our customers know they are proactively protected with security best practices, teams that work around the clock, and a rapid response to mitigate against threats.

You mentioned that you work with your customers to mature their security operations. How do you work with your customers to evolve your offerings?

Our Squad Delivery Model allows us to stay in constant communication with our customers via Slack, Zoom, email, etc. We collect real-time feedback from our customers via these communications and our ticketing system on a daily basis. This data is analyzed and used to produce significant metrics and dashboards. We also collect data from engineering tickets and all of this goes into our formal vetting process to inform our R&D team and roadmap based on these insights.

In addition, our Customer Advisory Board (CAB) made up of strategic customers and business partners provides guidance on corporate strategy, delivers guidance on products and services, and helps us create solutions to key industry

challenges. The overall objective of the CAB is to develop strategic plans to ensure long-term performance, growth, and ensuring our service offerings remain innovative and advanced for the benefit of our customers.

What is your take on automation and machine learning in the cyber security industry?

Automation and machine learning hold extraordinary promise. Most often, folks use the terms freely and so it's very important to be precise when considering the overall impact of both. We are seeing significant gains in efficiency, efficacy and overall success in threat identification and containment resultant from automation and the proactive insights derived from machine learning. That said, I don't think the talent shortage will ever go away. There aren't enough qualified engineers and analysts to backfill the talent shortage we face today. So we're doing what good technology companies do. We are investing in technology and automating fundamental tasks so that our highly skilled analysts can focus their time on the most significant events and incidents.

We were a very early adopter of **Security Orchestration, Automation and Response (SOAR) technology**, and our partner Palo Alto Networks, stated that our deployment of Cortex XSOAR, formerly Demisto, is one of the most sophisticated in the world. We invested in SOAR to maximize the effectiveness and efficiency of our analysts with a sole focus on improving outcomes for our customers. Coupled with our **Content Management & Distribution Platform**, a unique repository of custom security use cases developed by Deepwatch, we have substantially automated threat detection and analysis. Our analysts automatically receive information required to validate alerts faster and with more precision. We have built a large use case and run book repository that contain threat detection signatures, risky authentication behavior searches, automated response workflows, anomalous network activity and more.

Do you have any new services planned for launch?

We have an unyielding commitment to innovation and a relentless passion for changing the game of SOC management. We will maintain our differentiation and innovative approach through an increased investment in R&D and by continuing our close partnership with our customers. Our 2020 roadmap is more exciting than ever, and we are rolling out several exciting new products as core components of our platform. I'm not ready to go into the specifics just yet, however, we are working on a second generation of our Maturity Model, a net new service offering, as well as a customer application that helps CISOs understand and report on their security posture on a real-time basis.

Do you have any plans for future growth?

We are very bullish on our growth prospects. We are extremely differentiated in a large, global and growing market. Our customer retention rate is world class - over 120% net retention and as an example, we recently had a renewing customer request a six-year contract extension. Now that we are investing in marketing and growing our partner ecosystem, we expect continued expansion in North America with an eye toward global expansion in 2021 and beyond. SR

"With our cloud SecOps platform and relentless customer focus, we are redefining the managed security services industry."