Ontinue

SOC: Build vs. Buy – When Is It Right?

Ontinue's CEO Geoff Haydon on How to Choose a Reliable SOC Service Provider

ISMG
INFORMATION SECURITY
MEDIA GROUP

Ontinue

Geoff Haydon

Haydon has more than 25 years of experience in the enterprise software and security market. He has held senior executive leadership sales and operations roles at several IT and cybersecurity companies. Haydon is also the executive chairman at Open Systems.

The midsize market encounters many cybersecurity hurdles, including the increasing volume of information that needs to be protected, the shift to hybrid cloud, and limited skilled personnel to build and implement security programs. What does the SOC look like for these organizations?

To create a modern SOC, it's essential to have visibility across the enterprise by using a tool set that allows for ingesting telemetry from various operating environments, said Ontinue CEO **Geoff Haydon**. The ever-evolving cybersecurity landscape poses challenges for organizations to keep up with because "**the cost of acquiring the various tools and architectures is substantial.**"

"**Market prominence is an important consideration. Having a company that has that type of reputation and recognition is important,**" Haydon said. "**You want a company that has excellent people and an excellent technology platform. That combination of technology and talent is a best practice for a security operations center.**"

In this video interview with Information Security Media Group at **RSA Conference 2023**, Haydon also discusses:

- Barriers that prevent organizations from establishing a modern SOC;
- Factors to consider for improving security operations;
- How Ontinue is responding to customer needs and providing a solution.

"It's one thing to stand up tools and technologies, but cybersecurity programs are all about execution and operationalization. So, staffing the SOC with good people is very important. The combination of technology and talent … is a prerequisite to a good operations program."

Midmarket Cybersecurity Challenges

ANNA DELANEY: You cater to the midsize market. What are the unique cybersecurity challenges that these organizations face?

GEOFF HAYDON: The challenges that I'm going to describe aren't necessarily unique to the midmarket, but they tend to be particularly intensive there, and the midmarket is less equipped to deal with them. The growth of information is one. Increasingly, companies are being held to a high standard of accountability around information protection. The volume of that information is increasing. The shift away from on-premises computing to the hybrid cloud expands the virtual attack surface materially. The shift of the workforce from being in the office in a protected environment to anywhere is expanding the physical attack surface. All of these things are making it more difficult to protect information assets.

Also, the midmarket is less well-equipped in terms of the volume and caliber of talent that is building and executing their security programs. There's been a historical tendency to add a lot of tools, which has introduced a lot of cost and complexity. A lot of attacks now leverage the vulnerabilities or seams in between tools, so these complex environments tend to be more vulnerable. The irony is: The more that these companies have invested in tools, the more vulnerable in some cases they've become.

It's hard for any company to find cybersecurity talent right now. And in a midmarket company where there are very few roles and the roles are expected to span a broad variety of cybersecurity domains, it's very difficult to staff the operation centers. So increasingly, and for good reason, they're leveraging services like ours as opposed to opting to build and operate their own security program.

A Modern SOC for the Midsize Market

DELANEY: What does a modern SOC need to look like for these organizations?

HAYDON: The starting point is visibility across the enterprise. You can't secure what you can't see. And you need to have a tool set that allows you to ingest telemetry from across your operating environment, which is the endpoint, the network, the cloud and the OT environment. So, the starting point is getting signal from across the enterprise where emerging threats might be developing. The second component is having an incident and event management architecture

that can ingest that telemetry, apply reason and analytics to it and synthesize it into intelligence or actionable insights. Ideally, on top of that, you have a more sophisticated, purpose-built platform that analyzes the signal and synthesizes it into your highest risk priorities – the things that you organize your cybersecurity program or incident response activities around.

In addition, you need good people to work with these tools, optimize them and interpret what they're telling you, and determine what to act on and what not to act on. There's a lot of noise in the system, so having the expertise to be able to divine what's important and actionable is a priority. And that talent is going to be responsible for operationalizing the program. It's one thing to stand up tools and technologies, but cybersecurity programs are all about execution and operationalization. So, staffing the SOC with good people is very important. The combination of technology and talent in its simplest form is a prerequisite to a good operations program.

Barriers to Building a Modern SOC

DELANEY: What are the barriers preventing these organizations from establishing a truly modern SOC as you described?

HAYDON: A lot of companies, particularly in the midmarket, are struggling with this. Fundamentally, there are financial challenges. The cost of acquiring the various tools and architectures is substantial, and then there's the cost of integrating them, deploying them, deriving value from them and operating them. The operational costs are considerable. Finding and retaining people is difficult. Companies struggle with the staffing dynamic profoundly. One of the other considerations is how dynamic the cybersecurity environment and the attack vector environment are. Increasingly, companies are concluding that even if they're able to build, operationalize and optimize a SOC, by the time they get to that point, the landscape will have changed.

Evolving and adapting your program, tools and talent to that evolving landscape is very difficult for a small to medium-sized company, and a lot of them are concluding that their core business isn't executing cybersecurity programs. They're in the manufacturing business or the healthcare business. The center of gravity that develops around the cybersecurity program ultimately becomes quite costly and distracting to execute in their core mission. So, many of them are deciding not to do this on their own.

I don't understand why any midmarket company would opt to build and operate their own security operations center. There's so much data now on the cost and consequence of trying to do so and business cases around why it's more economical to lean on a domain expert but also more effective in terms of improving the efficacy and the performance of your security program and your ongoing and evolving maturity as the cybersecurity landscape evolves. We're seeing an epidemic shift toward leaning on a domain expert – a company that does nothing other than this – particularly in the midmarket.

Factors to Consider When 'Buying' a SOC

DELANEY: I want to talk more about build versus buy. What factors should an organization consider to make the right decision for them?

HAYDON: Fundamentally, market prominence is an important consideration. You want a company that is reputable and that has some mass and experience. Size matters when it comes to cybersecurity because your perspective across multiple customers and across the market broadly is very important in terms of improving your understanding of emerging threats. Prominence is important. So is having strong relationships with other cybersecurity leaders. Microsoft is a very prominent partner of ours. We were recognized as the MSSP of the year last year. Having a company with that type of reputation and recognition is important. You want a company that has excellent people and an excellent technology platform. That combination of technology and talent is a best practice for a security operations center.

The technology component is going to become increasingly important for operation centers. The speed at which the threat landscape is evolving requires a level of sophistication that only technology, data science and automation can bring. Companies that are looking at either building or adopting an operation center service should consider a number of factors.

Automation is very important. Being able to sift through the sheer volume and velocity of telemetry that's being captured across an organization and synthesize it into something that matters is becoming increasingly difficult for people to do. So, being able to automate – to filter it without the involvement of a human – is very important. We've invested very heavily in it. Ontinue acquired a data science company a few years ago, and we bought a company in December who's renowned for their automation capabilities. Automation improves the speed, accuracy and efficacy of the detection and response effort, and it reduces your dependence on people and frees them up to focus on more meaningful incidents.

Collaboration is another key factor that is important in a service like ours. Cybersecurity is no longer about simply detecting and responding. It's about operationalizing a security program. You need to be able to manage an incident. You need to be able to contain or remediate an incident or respond to it if it represents a breach scenario. That requires a high degree of collaboration between a customer and its service provider and across functions within a customer – across the security and IT function and across the business units that might be affected by a breach. So, having a collaboration platform is very important. We built our service

"Going beyond detection and response into understanding a customer's environment … and getting ahead of attacks – not just chasing them but preventing them from happening in the first place – is an integral part of the next generation of cybersecurity services."

on Microsoft Teams. We've embedded security functionality in Teams and stood it up as a security killer app. That's unique.

Localization is something we also talk a lot about. It's one thing for a security provider or a company to understand the threat vectors, but it's much more powerful and valuable to understand how those threat vectors intersect with an enterprise's operating environment – understanding your users, devices, applications and information. You associate different values with these different attributes and levels of risk. For example, a laptop that's stolen out of a restaurant – versus one stolen out of your CEO's or CFO's office that might contain confidential information or information on an acquisition – would have different levels of value associated with them. Having context on that is very important.

We invest a tremendous amount of time and money in understanding customer environments more intimately, and we do that through a team of people. We have an advisory function that interacts with our customers regularly and understands continuous changes in their operating environment. We've also invested very heavily in data science capabilities that monitor and enrich our understanding of an operating environment. The localization piece is important.

Assessment and ultimately prevention is the next domain of managed cybersecurity services. For years, we've been talking about detection and response. Even today, most of the cybersecurity services focus on improving your detection capabilities. Response is still quite nascent and immature. Through the collaboration and automation capabilities, we're introducing generational improvements in these areas. But going beyond detection and response into understanding a customer's environment, where the vulnerabilities are, and getting ahead of attacks – not just chasing them but preventing them from happening in the first place – is an integral part of the next generation of cybersecurity services and an area of great focus for us.

Ontinue

Our Story of Nonstop Security

Born in the cloud, built to be the best, engineered to deliver, and backed by the newest technology and the sharpest minds. Ontinue is all of this … and so much more.

Visit www.ontinue.com to learn more.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organisation 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 Just for Credit Unions INFO SECURITY® 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