

Decurity, with some flagship accounts under its belt, branches out

Analyst: Nick Selby

Decurity, founded by a former **ArcSight** managed services leader with an intelligence background and a long-time enterprise IT consultant, provides enterprise security information management (ESIM) content creation and security operations center and intelligence operations center consulting services for enterprise and government.

The 451 Take

Decurity's approach to the business is mission-driven and consultative, with its continuing engagements in the areas of push-based content updates and co-sourcing of its ESIM and log management offerings. We are intrigued by Decurity's leveraging its organization capabilities with its varied experience in security operations centers in government and enterprise. Inevitably, a discussion about Decurity brings up its closest philosophical rival, Vigilant. We feel that while the companies benefit from one another being in similar spaces, there is enough different about their approaches that they complement each other more than they might recognize.

Context

Tampa, Florida-based Decurity was founded in October 2007 by Rocky DeStefano and Paul Davis. DeStefano, who had served in the **US Air Force** doing intelligence work, was an early employee at ArcSight, where he was a leader in professional services. Davis is an industry veteran, having worked at **EDS** and **Unisys**, among other IT shops (the pair met at EDS). Decurity was set up with what DeStefano refers to as 'a couple hundred thousand dollars,' and has been cash-flow positive and US GAAP profitable since its first year of operation. It currently employs around ten staffers, mainly in the Washington DC and Boston areas. Its more than 10 customers include a Fortune 100 manufacturing firm and a large US federal agency. Its average deal sizes are around \$75,000.

Products

Decurity is focused on the security operations aspects of delivering a security in a business environment. Based on its experience and knowledge, it helps organizations with the process of 'operationalizing' the tools and teams involved so that the solution delivers meaningful information to the business and data owners. It provides these services through traditional consulting engagement models or through a partnership model that can provide these

capabilities on an ongoing basis, as well as enhanced services such as remote systems management, tuning, updates and performance monitoring.

Decurity assists customers in understanding the requirements of their desired 'to be' state and then consults on what are the best sources of events within the enterprise to support it. Decurity can assist the company in buying ESIM products or deploying the one it already owns. Based on its corporate heritage, Decurity may be seen as being guilty of bias toward ArcSight. However, we know firsthand from a mutual customer, which is not an ArcSight customer, that Decurity is platform-agnostic.

Decurity authors ESIM content, including correlation rules that help the ESIM produce alerts and associate workflows that are most relevant to the organization, and provides regular updates to, for example, ArcSight Active Lists and the corresponding equivalent in other ESIM products. Decurity also provides expertise in areas of intelligence gathering and correlation for enterprise and government and helps manage security operation centers once established.

Technology

Decurity, like **Vigilant** and several consultants, has a set of its best practices and experience-driven correlation rules in its library. Decurity insists that this is not the core of its offering and that it differentiates by working to capture first what it is that customers need to accomplish and then tailoring the Decurity rule set to the customer's infrastructure to make the rule set mold to the suited purpose.

After setup, Decurity will work to create regular – daily or better – content updates, feeding correlation engines the equivalent of ArcSight's Active Lists or **Symantec's** GIN-fed correlation rules. As a high-level example, a Decurity customer coming under attack by a specific botnet would need information about that botnet, like proxy and DNS information and other crucial descriptive content, which would then be fed to Decurity customers in the form of premade correlation rules. Decurity also offers its clients 'on demand' content generation, which can use a support portal to define the use case, and its experts will configure, test and help the customer implement the content in the customer environment.

Its Trusted Advisor service provides advice related to security operations. This helps clients improve their security service delivery capabilities and respond to business and IT changes and threats, leveraging a partnership in order to enable the secure sharing of information and access to their trusted advisors.

Competition

Like Vigilant, Decurity competes on many levels with the ESIM vendors themselves, other firms like Decurity, managed service providers (like EDS, where DeStefano and Davis met) and consultants. In addition to direct competition from Vigilant, competition comes from the professional-services wings of ESIM vendors – including ArcSight, **IBM**, **RSA**, **Novell** and Symantec – and from log management vendors, including **Splunk Inc**, **LogLogic** and **Tenable Network Security**. Decurity competes against large managed security service

provider players, including **AT&T, BT Counterpane, Verizon/Cybertrust** and the aforementioned EDS, as well as other large managed security services vendors. Competition from consultants comes from **Knowledge Consulting Group, Deloitte** and **PricewaterhouseCoopers**.

SWOT analysis

| Strengths | Weaknesses |
|--|---|
| Lean but sufficient funding, frugal and experienced management, and some powerhouse early customers (and at least one large government contract) put Decurity into the agile, fast-moving crowd. | That lean funding and agility of having a virtual office could strike some customers as groovy or even flighty. |
| Opportunities | Threats |
| Decurity has some excellent ideas about how security operations centers need to adapt for the next five years that we've not heard others speak of. | Vigilant is similarly lean, agile, self-funded and frugal, but is growing faster. ArcSight is getting extremely aggressive with its professional services play. |

Reproduced by permission of The 451 Group; copyright 2009. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to: www.the451group.com