JANUARY 2020

Cybersecurity and the Problem of Interoperability

William D. Crumpler and James A. Lewis

Organizations face a growing threat from malicious cyber activity. Nation-states are becoming more aggressive, and criminals are growing in sophistication. The spread of poorly secured "Internet of Things" devices increases the attack surface, and AI-enabled hacking tools and cybercrime-as-a-service intensifies the competition between defenders and attackers. These threats have driven companies to build layers of defenses, resorting to a variety of products and services developed by different cybersecurity vendors.

According to AttackIQ and the Ponemon Institute, large organizations use an average of 47 different cybersecurity tools across their networks, and research firm ESG estimates that firms source their tools from an average of 10 different vendors.[1] Coordinating the implementation of all these products is a challenge of its own. Moreover, this complex mixture of cybersecurity products and services creates interoperability problems that work against the efficient use of these tools.

Integrating different products is a major challenge for security teams.[2] When new tools are introduced but are unable to communicate with other platforms, it is hard to get a useful picture of the threat landscape. Some may be ineffective because they are not being fed data from complementary systems. The pace of cyberattacks is accelerating too quickly for organizations to rely on manual threat analysis and response, and a multiplicity of tools can provide contradictory information. In the face of these inconveniences, purchased tools may be left languishing.

[1] Charlie Osborne, "Over half of enterprise firms don't have a clue if their cybersecurity solutions are working," ZDNet, July 30, 2019, https://www.zdnet.com/article/over-half-of-enterprise-firms-dont-measure-the-performance-of-their-cybersecurity-tools/; Jessica Lyons Hardcastle, "IBM Security, McAfee Spearhead Open Cybersecurity Alliance," SDxCentral, October 8, 2019, https://www.sdxcentral.com/articles/news/ibm-security-mcafee-spearhead-open-cybersecurity-alliance/2019/10/.

[2] "The Top Challenges in Network security for 2019," Bricata, December 14, 2018, https://www.slideshare.net/Bricata/the-top-challenges-to-expect-in-network-security-in-2019-survey-report.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Even when cybersecurity teams manage to integrate their cyber defense toolkits, the time and effort required to do so can create a significant resource drain. Instead of spending their time responding to threats, cyber professionals are occupied with managing a complex web of products and services that was supposed to make their jobs easier.

A common set of standards, protocols, taxonomies, and open-source software that can tie cybersecurity tools together could help ease this burden. If tools used shared methods for identifying and classifying threat intelligence, communicating anomalies, and automating response actions, it would be significantly easier to take advantage of new cybersecurity solutions.

The Organization for the Advancement of Structured Information Standards (OASIS) has launched a new Open Project called the Open Cybersecurity Alliance (OCA). The OCA brings together interested stakeholders intended to provide a solution to the described problem. It is attempting to do so through two ongoing programs. One will develop an interoperable messaging format for cybersecurity tools, while the other will develop standardized data models and libraries to classify threats in a way that can be analyzed by any cybersecurity tool.[3]

Adopting open standards for cybersecurity tools will take time, and cybersecurity customers can encourage interoperability. The federal government, for instance, can play an important role. Projects like the Continuous Diagnostics and Mitigation (CDM) "Dynamic Evolving Federal Enterprise Network Defense" from the Department of Homeland Security can promote interoperability and the widespread adoption of common standards. It is also in companies' best interest to push for the adoption of common standards. Even with an expert staff and all the latest tools, security teams will continue to face challenges as long as security architectures work against integration. By prioritizing the construction of a more open, interoperable cyber ecosystem, companies can be leaders in building a more effective, more sustainable cyber defense.

One thing we have learned in cybersecurity is that speed is crucial, to identify, to block, and to respond. Things that make a defender slower give advantage to the attacker. Thus, it is particularly undesirable that the very investment intended to strengthen defense can sometimes weaken it. Improving interoperability returns some of the advantage to defenders.

William Crumpler *is a research assistant for the Technology Policy Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***James Andrew Lewis*** *is a senior vice president at CSIS.*

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

[3] Hardcastle, "Open Cybersecurity Alliance."