No.28
August 7th 2019

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/UN-SPONSORED

A New Window Onto an OpenC2 World

- The OpenC2 Technical Committee has approved its first technical specifications.
- The promise of accelerating multi-vendor security orchestration and automation makes OpenC2 an important new cyber security standard. User support is needed to scale the ecosystem beyond the limited capability set that is initially available.
- While Symantec is an early adopter, a lot of incumbent vendors are conflicted about OpenC2. For new entrant security vendors, early adoption looks like a no-brainer.

The Technical Committee (TC) of the OpenC2 Forum – part of OASIS – broke through the key milestone of approving its first specifications on Monday this week. OpenC2 is a suite of open command and control specifications designed to enable faster orchestration and automation in cyber security operations. This milestone finally puts the standard on a footing with which it can scale out into commercial deployments.

The specifications approved comprise the OpenC2 language itself as well as the first examples of an actuator profile and a transport spec.

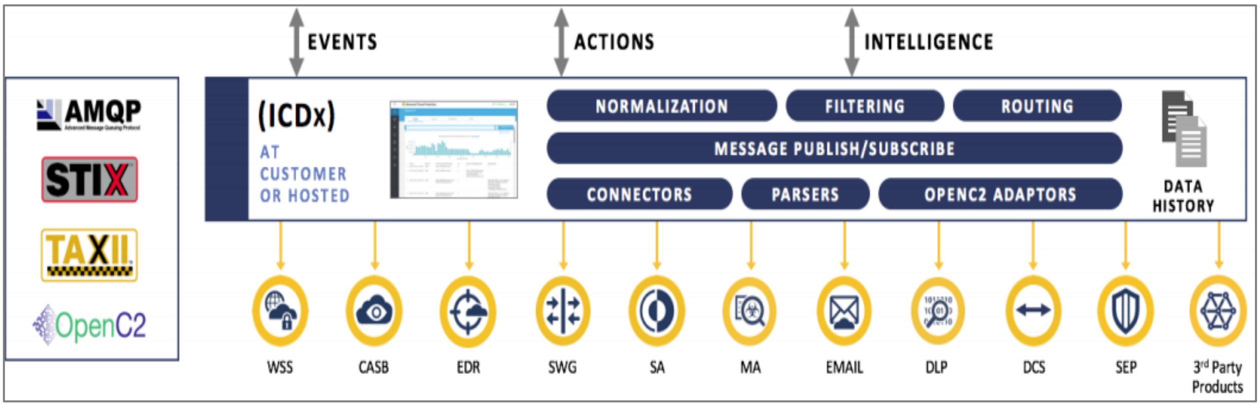
To affect an orchestrated response to a security incident in today's complex, multi-vendor, security operations environment, the security team typically needs to know the syntax of each different product that's involved in the response; go to a web based application; use an API or connect remotely to input commands. The value proposition of OpenC2 is that commoditizing the command and control interface on all those same product types allows security teams to automate an orchestrated response a lot more reliably and a lot faster. By extension, it also allows competition between security vendors to focus more on product performance.

Three pillars of specifications

The specifications approved last week by the TC comprise the core OpenC2 language itself, together with the first examples of the two other components that are needed for initial real world-deployments. These are:

- the first OpenC2 actuator profile allowing a stateless packet filter to be commanded or orchestrated by another security product.
- the first OpenC2 transport specification, an https API.

Figure 1: Symantec's ICDx supports OpenC2



Source: Symantec

For OpenC2 to scale up beyond this initial tool set, a library of additional actuator profiles will be needed to describe other objects or product types in the security operations environment besides packet filters. In the case of other transport specs, other variants could include protocols developed by particular vendors such as McAfee's OpenDXL.

As shown in **Figure 1**, motivated by the lead role in driving OpenC2 that has been played by major customers such as AT&T, Bank of America and the US National Security Agency (NSA), Symantec is at the forefront of implementing OpenC2 in parts of its portfolio. Specifically, Symantec has an initial implementation of OpenC2 in its Integrated Cyber Defense Exchange (ICDx).

Symantec's Implementation of OpenC2 in ICDx

Physically, ICDx uses adaptors to represent OpenC2 actuators. Specific adaptors are implemented per product, which translate standard calls to product-specific calls. Product termination points are categorized by standard OpenC2 targets. Using this pattern, a common action call can be routed to product termination points and invoked in the context of each product. Actions supported by Symantec ICDx are allow, deny, contain, query, and remediate. Targets include device, file, process, URL, directory, email message, registry key, and others.

Users that are early adopters should be willing to go the extra mile and support new entrants with joint marketing efforts.

A lot of incumbent vendors are conflicted about OpenC2. In terms of protecting existing business, widespread adoption of the new specification risks undermining the de facto lock-in they have with the kinds of legacy platforms and footprint that make them the primary strategic vendor in some accounts. On the other hand, the current rush into the Security Orchestration Automation and Response (SOAR) space – witness the recent acquisition of Demisto by Palo Alto Networks – can help create new opportunities for incumbents in accounts where their competitors are best positioned.

From a start-up or new entrant perspective, OpenC2 looks like a no-brainer, promising easier, faster integration and operation in multi-vendor environments. To help drive the ecosystem, leading users of OpenC2 should therefore be willing to go the extra mile and support new entrants that support OpenC2 with joint marketing efforts.

Voting Members on the Technical Committee

As of August 7th, the following companies are showing as voting members on the Open C2 Technical Committee website: AT&T; Bank of America; Darklight Inc; FS-ISAC; FireEye; G2; LookingGlass; National Security Agency (NSA); NEC Corporation; New Context Services Inc; NineFxInc; Northrop Grumman; sFractal Consulting LLC; Symantec; Trend Micro; and University of North Carolina at Chapel Hill.

A number of other companies, including a number of other well-known vendors, are members – rather than voting members - of the TC. If you are interested in learning more or participating in OpenC2 please contact: openc2-chair@lists.oasis-open.org

More Information

- Contact HardenStance's Principal Analyst: patrick.donegan@hardenstance.com
- Register for free email notifications when HardenStance publishes new content.
- www.hardenstance.com
- HardenStance received no payment for publishing this Briefing.

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.