Published on *OASIS* (https://www.oasis-open.org)

International Community Comes Together at OASIS to Advance OpenC2 Standard for Automated Defense Against Cyber-Attacks

Anomali, Arbor Networks, Centripetal, Cisco, Cryptsoft, EclecticIQ, FireEye, ForeScout, Fornetix, FS-ISAC, G2, IBM, LookingGlass, McAfee, NC4, NEC, New Context, Phantom, Swimlane, Tanium, ThreatQuotient, U.S. DoD, U.S. NSA, U.S. NIST, and Others Define Open Command and Control (OpenC2)

5 Sept 2017 ? Organizations and government agencies from Asia, Australia, Europe, and the U.S. are joining forces to advance a standardized language for cyber operations command and control. The work of the new OASIS OpenC2 Technical Committee enables defenders to respond to cyber-attacks in machine-speed. It also helps ensure greater interoperability among products.

Cyber threats are realized in seconds while human responses can take weeks. By providing a common language for machine-to-machine communication, OpenC2 makes it possible for defenders to conduct automated, coordinated, tactical threat responses more accurately and at speeds greater than those previously possible.

Most environments include hundreds of types of systems and devices. Without OpenC2, every device needs to be manually configured or sent commands in real time. This not only slows down incident response, it introduces the potential for human error. With OpenC2, defensive actions can be applied automatically to vulnerable devices in the environment.

"As cyber threats continue to proliferate and accelerate, the community needs foundational mechanisms for coordinating, exchanging, and executing defensive responses at machine speed," said Neal Ziring, Technical Director, Capabilities Directorate, U.S. National Security Agency (NSA). "OpenC2 will fill a critical gap in our standards landscape, and drive interoperability that will be critical for cyber defense."

OpenC2 is platform- and product-agnostic. It complements active cyber defense approaches. Using OpenC2, organizations can devise ways of preventing specific threats and share those methods with others in precise, machine-readable terms. Receiving organizations can apply the mitigation directly to their environments without concern about interoperability.

"Moving OpenC2 to the OASIS international standards body is a major milestone and has had a very positive impact on the effort," said Joe Brule of the NSA, co-chair of the OASIS OpenC2 Technical Committee. "OpenC2 now has in excess of 100 members representing 54 organizations from industry, government, academia, the financial sector, power grid and other major stakeholders. Broad participation will facilitate the development and deployment of OpenC2."

"We are in strong support of OpenC2 adoption, and we encourage the community of practitioners and vendors to work together to establish and implement this standard so that we can reduce the complexity of our integrated

systems and increase the speed at which we can respond to attacks," added Sounil Yu of Bank of America, who co-chairs the OASIS OpenC2 Technical Committee along with Brule.

Laurent Liscia, CEO and executive director of OASIS, said, "We?re excited to have OpenC2 at OASIS. It's a strong specification, with solid industry support. OpenC2 is a welcome addition to our cybersecurity portfolio. Many members of the OASIS Cyber Threat Intelligence (CTI) Technical Committee, which advances the STIX and TAXII standards, are also involved in OpenC2."

Support for OpenC2

ForeScout Chief Strategy Officer, Pedro Abreu, said, "OpenC2 and ForeScout benefit from each other in a unique manner. ForeScout's device identification and classification engine provides the much needed, fine grained distinction between devices all the way from legacy server systems to modern IoT gadgets and anything in between. OpenC2?s action framework through actuators provides the capability to define an abstract course of action for incident response. With the combination of both, organizations can take a quick contextual action at machine speed to reduce their attack surface."

G2, Inc. President, Paul Green, said, "G2 is thrilled OpenC2 is gaining more traction in the OASIS community. Early on, we recognized the critical need for vendor-agnostic command and control in support of cyber defense and are proud that our design principles and early work on the syntax and vocabulary have been enthusiastically received. The wide adoption of OpenC2 will make it significantly easier for defensive systems to orchestrate their activities to address cyber threats in real time."

LookingGlass CTO, Allan Thomson, said, "Cyber threats continue to increase in sophistication and speed, forcing cyber defenders to look for technologies that provide coordinated real-time detection and response. LookingGlass is excited to contribute our expertise and background to integrate threat intelligence and threat mitigation technologies in the new OpenC2 standard."

NC4 Soltra Development Manager, Mark Davidson, said "Moving the standardization of interfaces and protocols for machine-to-machine, automated threat detection under Oasis? Open Command and Control (OpenC2) technical committee will help ensure vendor interoperability. In the long run, the ability to quickly provide cyber-defenders the action part in the cybersecurity equation, will strengthen and support cyber defenses."

NEC General Manager, Cyber Security Strategy Division, Toshiyuki Ishii, said, "NEC is very pleased to be part of the OpenC2 Technical Committee and continues to drive OpenC2 adoption with industry partnerships to benefit customers. NEC believes that a common language for defensive actions is crucial for proactively countering the cyber threat in real time. We are excited about the formation of OpenC2 TC and support its efforts through its contributing to and promotion of this global standard."

New Context CEO, Daniel Riedel, said, "Our vulnerable attack surface is increasing, as are the adversaries targeting our systems and networks. Security automation is a force multiplier for defenders. New Context is committed to the development of OpenC2 as we are convinced that an open, vendor-neutral standard for driving interoperable machine-driven mitigation and incident response is essential in order to enable organizations to cope with the rising challenges and growing numbers of increasingly sophisticated cyber threats."

Phantom CTO & Co-founder, Sourabh Satish, said, "Phantom's partnership with the OpenC2 Forum began several years ago. The adversaries are using automation against us, so the only way to mitigate attacks at cyber-speed is with automation. With a strong specification and support from industry leaders like Phantom, the OASIS OpenC2 Technical Committee will make great progress in defining a standardized language for cyber

operations command and control."

Swimlane Founder and CEO, Cody Cornell, said, "The future of security is going to require high levels of interoperability, and the only way we get there is through open standards. That is why we are so excited about the work being done collectively by the federal government, security vendors, and the OpenC2 Technical Committee."

Tanium Chief Security Officer, David Damato, said, "As the number of connected devices rapidly multiplies and the cyber threat grows, it's become clear we need a common language for technologies to automatically communicate with each other, both within and across networks. This interoperability will help organizations operate at the speed needed to stop attacks. We support the development of the OpenC2 standard and applaud OASIS for bringing businesses and government agencies together to develop it."

ThreatQuotient CTO, Ryan Trost, said, "Operationalization and use of cyber threat intelligence (CTI) across all tools within the infrastructure serves as the glue to accelerate detection and response. The adoption of open standards like OpenC2 to effectively use CTI and automate response is critical to achieve an integrated defense."

More information

OpenC2 Technical Committee [1]

Video: Introduction to OpenC2 [2]

About OASIS

OASIS is a non-profit, international consortium that drives the development, convergence, and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for cyber security, privacy, cloud computing, IoT, SmartGrid, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. OASIS members broadly represent the marketplace of public and private sector technology leaders, users, and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in 65+ countries.

Media inquiries: communications@oasis-open.org; +1.941.284.0403

Links:
[1] https://www.oasis-open.org/committees/openc2/
[2] https://www.youtube.com/watch?v=kCooyNJoOrU