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

OASIS Advances Automated Cyber Threat Intelligence Sharing with STIX, TAXII, CybOX

Boeing, Check Point, Cisco, Dell, EMC, eSentire, Fortinet, Fujitsu, IBM, iboss, iSIGHT Partners, NEC, New Context, Palo Alto Networks, Resilient, Securonix, Soltra, TELUS, ThreatQuotient, ThreatStream, TruSTAR, US DHS Office of Cybersecurity and Communications, US NIST, ViaSat, and Others Collaborate on International Standards to Prevent and Defend Against Cyber Attack

16 July 2015 ? Three foundational cyber security specifications, STIX, TAXII, and CybOX, are now being advanced through the international open standards process at OASIS. In a transition headed by the U.S. Department of Homeland Security, a record number of organizations from around the world have come together in the new OASIS Cyber Threat Intelligence (CTI) Technical Committee [1] to develop and promote adoption of standards that enable cyber threat intelligence to be analyzed and shared among trusted partners and communities. The work will support automated information analysis and sharing for cyber security situational awareness, real-time network defense, and sophisticated threat characterization and response.

"Security professionals are overwhelmed and simply don?t have time for analyzing data in disparate formats. STIX, TAXII, and CybOX streamline the process, putting the focus of cyber intelligence where it belongs?on prevention, detection, and remediation," said Jon Oltsik, Senior Principal Analyst at Enterprise Strategy Group. "Using data converted to these standard formats can help security practitioners rapidly identify and access current threats, and determine how they act, who is responsible and what course of action is needed. Threat intelligence standards are also a key building block for fulfilling the vision of ubiquitous threat intelligence sharing."

STIX, TAXII, and CybOX can work in concert or be implemented separately. STIX (Structured Threat Information Expression) is a language for describing cyber threat information so that it can be analyzed and/or exchanged. STIX makes it possible to explicitly characterize a cyber adversary's motivations, capabilities, and activities, and in doing so, determine how to best defend against them. TAXII (Trusted Automated Exchange of Indicator Information) defines services and message exchanges that enable organizations to share the information they choose with the partners they choose. CybOX (Cyber Observable Expression) is a language for specifying, capturing, and communicating events or stateful properties that are observable in system and network operations. Together, STIX, TAXII, and CybOX are instrumental in supporting a wide variety of applications including security event management, malware characterization, intrusion detection, incident response, and digital forensics.

"STIX, TAXII, and CybOX have reached a level of maturity where they will benefit from a more formal collaboration guided by a globally recognized standards development process that ensures transparency, international participation, stability, reciprocity, and perpetual ease of access," said Richard Struse of the U.S. Department of Homeland Security Office of Cybersecurity and Communications, who chairs the OASIS CTI Technical Committee. "OASIS provides all of this, and is an ANSI-accredited developer of American National

Standards as well as an authorized PAS Submitter to ISO. Having these certifications available to STIX, TAXII, and CybOX means they will be implementable by the broadest possible stakeholder community."

OASIS CTI Technical Committee members have formed three Subcommittees to address the specifications individually. The CTI STIX Subcommittee is chaired by Aharon Chernin of Soltra and Sean Barnum of MITRE. The CTI TAXII Subcommittee is chaired by Bret Jordan of Blue Coat and Mark Davidson of MITRE. The CTI CybOX Subcommittee is chaired by Trey Darley of Soltra and Ivan Kirillov of MITRE.

New members are encouraged to join the OASIS CTI Technical Committee and its Subcommittees at any time. Archives are accessible to both members and non-members, and OASIS invites public review and comment on the work.

Support for CTI

Check Point
"Check Point believes that open standards and community sharing are vital components of a successful and effective fight against cybercrime. Our goal is to make Threat Intelligence, from a variety of sources, timely and actionable. We have been working with the STIX/TAXII community for the past three years and are adopting STIX/TAXII in our architectures. We look forward to working with the community to expand the standards to allow for significant sharing between governments, security organizations and vendors, and customers."
--*Dorit Dor, VP, products, Check Point Software Technologies*

eSentire
"Real-time threat intelligence consumption will become more of a reality as these specifications are widely implemented by vendors in all parts of the security ecosystem. Our security intelligence analysts have been affiliated with and advocates of STIX, TAXII and CybOx for quite some time. The introduction of OASIS as an international standards checkpoint will undoubtedly improve threat intelligence sharing amongst partners by facilitating the exchange of computer-readable threat information."
--*David Maxwell, Director of Threat Intelligence, eSentire*

Fortinet
"Information sharing is crucial to building a more secure infrastructure across the global ecosystem. Creating a common language, a methodology for how that language is communicated, rating systems, and other standards are going to be required for efficiency and clarity to combat the speed of new threat creation. STIX and TAXII in particular are important initiatives towards next generation threat intelligence. Using the same terms, data streams, and threat modeling methods will help researchers, vendors, and law enforcement alike share information back and forth to stay abreast or even ahead of threat actor groups. We are pleased to contribute to this and more through OASIS."
--*Derek Manky, Global Security Strategist, Fortinet*

IBM
"IBM has long supported industry standards to solve the world?s most pressing challenges. Cybersecurity is one of the greatest challenges our modern society faces and requires a coordinated approach to succeed. Under OASIS leadership, we see an opportunity to better organize the good guys to fight cybercriminals by sharing cyber threat intelligence data in an automated and efficient data standard."
--*Peter Allor, Senior Security Strategist, IBM*

iboss
"We have long been committed to any advances that can better enable the sharing of threat intelligence among security professionals. Until now, organizations have been hampered by a lack of common standards and the tendency for security information to be siloed. We strongly support this important endeavor and look forward to

contributing to the standardization being led by OASIS."
--*Paul Martini, Co-founder and CEO, iboss Cybersecurity*

iSIGHT Partners
"iSIGHT Partners, creator of the commercial cyber threat intelligence category, understands how security organizations can gain the advantage over adversaries by using threat intelligence across their security and risk management program. As an early contributor and enabler of STIX, we welcome the opportunity to join with OASIS to further develop CTI standards and accelerate the adoption of context rich threat intelligence."
--*Robert Huber, VP Community, iSIGHT Partners*

NEC
"NEC is very pleased to be part of the CTI Technical Committee and continues to drive CTI adoption with industry partnerships to benefit customers. NEC believes that threat intelligence standards are crucial for proactively countering the cyber threat. We are excited about the formation of CTI TC and support its efforts through its contributing to and promotion of this global standard."
--*Kozo Matsuo, General Manager, Cyber Security Strategy Division, NEC Corporation*

New Context
"Development of an industry-wide standards framework for cyber threat intelligence is crucial for the information security industry to be able to define and share threats. New Context is a proud sponsor of OASIS and believes strongly in open and transparent standards frameworks development. We look forward to collaborating on the next standards for STIX, CybOX and TAXII."
--*Daniel Riedel, CEO, New Context*

Resilient
"As a Sponsor of the OASIS CTI Technical Committee, we are delighted to be at the forefront of advancing critically important standards like STIX, TAXII and CybOX. By creating protocols that address how to best model, analyze, and share cyber threat intelligence, we can provide greater support to overwhelmed security professionals."
--*John Bruce, CEO and co-founder, Resilient Systems*

Soltra
"Soltra is proud to be a member of the OASIS CTI Technical Committee. Our threat information sharing solution, Soltra Edge, was built leveraging STIX, TAXII, and Cybox ? key standards within the industry. We look forward to contributing to CTI as we continue to establish and maintain open standards, while improving cyber security capabilities and reducing workload."
--*Aharon Chernin, CTO, Soltra, a DTCC and FS-ISAC Company*

TruSTAR
"We are proud to support the work OASIS is doing to advance their cybersecurity specifications and promote information sharing, a critical factor in today's security posture. By sharing details about malicious incidents quickly, not only between the public and private sectors, but across industry lines within the private sector as well, we can work together to better defend ourselves and stay ahead of the hackers."
--*Paul Kurtz, founder and CEO, TruSTAR Technology*

ViaSat
"Focusing on standardizing threat intelligence technologies to keep sensitive government and corporate information secure is paramount to the mission of OASIS and its members. At ViaSat, we take a comprehensive approach to cybersecurity, from identifying potential cyber and physical security vulnerabilities to designing and implementing a plan that leverages big data analytics, intuitive visualization and intelligent automation to

keep pace with evolving threats no matter where data resides on the network or how it is accessed."
--*Jerry Goodwin, VP, Secure Network Systems, ViaSat*

Additional information
OASIS CTI Technical Committee [1]

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 security, privacy, cloud computing, IoT, content technologies, digital experiences, 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. http://www.oasis-open.org

Press contact: Carol Geyer, carol.geyer@oasis-open.org, +1.941.284.0403

Links:
[1] https://www.oasis-open.org/committees/cti/