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

Cybersecurity Companies Demo Support for STIX and TAXII Standards for Automated Threat Intelligence Sharing at RSA 2018

Anomali, EclecticIQ, Fujitsu, Hitachi, IBM Security, New Context, NC4, ThreatQuotient, and TruSTAR Demo STIX and TAXII Support

16 April 2018 -- Nine companies from around the world come together at the RSA 2018 conference this week to demonstrate automated cyber threat intelligence sharing in action. Members of the nonprofit OASIS standards consortium will showcase an array of products that support the STIX? and TAXII? standards. The demos are being held from 16-19 April, in Booth 1701.

The STIX standard enables organizations to share cyber threat intelligence in a consistent, machine-readable manner, allowing companies to anticipate and respond to attacks faster and more effectively. TAXII is the transportation protocol specifically designed to support the exchange of STIX data.

Products from Anomali, EclecticIQ, Fujitsu, Hitachi, IBM Security, New Context, NC4, ThreatQuotient, and TruSTAR are demonstrating how STIX and TAXII are being used to prevent and defend against cyberattack by enabling threat intelligence to be analyzed and shared among trusted partners and communities. In addition to seeing the demos, RSA attendees are learning more about how the major new version of STIX and TAXII making it much easier to automate cyber threat intelligence sharing.

Support for STIX and TAXII

Anomali CTO, Wei Huang, said, "Anomali is the first company to provide Limo?a free TAXII service, compliant with both STIX/TAXII 2.0 and 1.0?to enable interoperability testing, validation, and adoption for vendors and customers. This service includes threat intelligence and threat bulletins from Anomali Labs, Modern Honey Net, and open source feeds. Anomali's free STIX/TAXII client?Anomali STAXX, can be used with Limo or any other STIX/TAXII threat intelligence source."

EclecticIQ CEO & Founder, Joep Gommers, said, "STIX is the foundation of the data model of EclecticIQ Platform. Its analyst-centricity has helped to enable and transform the threat intelligence community in a relatively short time span. At the OASIS booth, we will demonstrate how our Threat Intelligence Platform utilizes STIX & TAXII to meet the full spectrum of intelligence needs."

Fujitsu Director of Marketing & Sales (Cyber Systems) Defense Systems Unit, Hitoshi Habe, said, "Fujitsu will demonstrate S-TIP (Seamless - Threat Intelligence Platform) prototype. This platform merges human (SNS, email) and system (STIX/TAXII) CTI sharing seamlessly to help reveal 5Ws1H of cyber-attacks (such as threat actors, time periods, objectives, attack targets, intrusion paths, methods) with its capabilities like CTI graph analytics engine. Fujitsu has been an OASIS CTI Technical Committee member since the TC?s establishment."

Hitachi, Ltd. Director of Security Innovation Promotion Department, Akihito Sawada, said, "Hitachi will demonstrate the prototype of information sharing service. This will be a part of security service of Hitachi Systems that gathers threat-related information in cyberspace and provides discussion place among analysts, operators. The information is provided to its users after it has been converted to STIX and TAXII format, ranked, classified and grouped. We are honored to introduce STIX and TAXII as prototype."

NC4 Vice President, Andrew Blumberg, said, "As an early leader in bringing sharing of CTI to scale, NC4 is maturing the model for collective cyber defense by integrating person-to-person collaboration with machine-to-machine sharing. Unifying teams across industries and government, NC4 brings scale to the human factor of collaboration. Leveraging the STIX/TAXII standards to increase the immediacy of awareness and action also enables more effective use of core standard constructs like TTPs and COAs."

New Context CEO, Daniel Riedel, said, "We?re proud to continue collaborating with OASIS as both a sponsor and contributor to the OASIS CTI Technical Committee. New Context is committed to the advancement of threat intel because we?re convinced that an open, vendor-neutral standard for driving interoperable machine-driven mitigation and incident response protects our data. Standards are an important part of the New Context Design Principles and to answering future challenges of the cyber threat landscape."

ThreatQuotient Co-Founder and CTO, Ryan Trost, said, "ThreatQuotient is committed to advancing the state of security operations by enabling greater collaboration across an organization, and by upholding the standards and integrations that are key elements of a strong security program. We look forward to this opportunity to demo the ThreatQ threat intelligence platform with partners of OASIS at RSA, and continuing to play a role in helping organizations get more out of cyber threat intelligence."

TruSTAR Co-Founder & CEO, Paul Kurtz, said: "Too often security and risk teams silo event data into multiple categories like fraud, phishing, malware, DDoS, insider threats, and physical breaches. At TruSTAR we believe companies must take a unified approach to security operations. Interoperable ingest tools championed by OASIS help TruSTAR customers leverage multiple intelligence sources and enrich them with their own event data."

About OASIS

OASIS is a nonprofit, 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 key management, cryptography, cybersecurity, privacy, cloud computing, IoT, 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.

Press contact:

communications @oasis-open.org