

RSA 2017 Features Huge Demonstration of Support for Cyber Threat Intelligence, Encryption, and Cryptography Standards as 24 OASIS Member Companies Collaborate

Bay Dynamics, DFLabs, EclecticIQ, Fujitsu, IBM, LookingGlass, New Context, NC4, ThreatConnect, ThreatQuotient, TruSTAR, and Verisign Demo STIX and TAXII Support. Cryptsoft, Feitan, Fonetix, Hancore Secure, Hewlett Packard Enterprise (HPE), IBM, Kryptus, Oracle, Quintessence Labs, SafeNet, Utimaco, and Watchdata Demo KMIP Interoperability and/or PKCS #11 Support.

San Francisco, CA; 13 February 2017 ? One of the largest showings of support for security standards in RSA Conference history is happening this week. The nonprofit OASIS open standards consortium has brought together 24 companies to demonstrate support for the STIX and TAXII cyber threat intelligence standards, Key Management Interoperability Protocol (KMIP) standard, and the Public-Key Cryptography Standard (PKCS) #11. The demos are being held in Booths 2121 and 2115 from 13-16 February.

"This year's RSA Conference enables us to demonstrate both the latest work of the Technical Committees and the depth of capabilities within products that implement these standards," said Tony Cox of Cryptsoft, co-chair of the OASIS KMIP Technical Committee and KMIP Interop Lead. "Demonstrating interoperability between these products live at the RSA Conference reinforces the reality of choice of vendor solutions for CIOs, CSOs and CTOs, enabling products from multiple vendors to be deployed as a single enterprise security solution that addresses both current and future requirements."

STIX and TAXII

Twelve companies stand together at RSA to show attendees why STIX and TAXII are recognized as the definitive standards for automated cyber threat intelligence sharing. Products from Bay Dynamics, DFLabs, EclecticIQ, Fujitsu, IBM, LookingGlass, New Context, NC4, ThreatConnect, ThreatQuotient, TruSTAR, and Verisign demonstrate how STIX and TAXII are being used to prevent and defend against cyber attack by enabling threat intelligence to be analyzed and shared among trusted partners and communities.

KMIP

RSA attendees also are witnessing live demonstrations of encryption key and security object management interchange between Cryptsoft, Fornetix, Hancorn Secure, HPE, IBM, Kryptus, Oracle, Quintessence Labs and SafeNet. The demonstration shows how KMIP enables both the interchange of security objects as well as the provision of encryption keys and cryptographic services across a common interface. Client and server implementations cover the full key management lifecycle including creating, registering, locating, retrieving, deleting, and transferring symmetric and asymmetric keys and certificates between vendor systems.

The latest KMIP release, version 1.4, is being demonstrated publicly for the first time at RSA, along with KMIP versions 1.3 and 1.2, which are ratified OASIS Standards.

PKCS #11

One of the most widely deployed cryptography standards, PKCS#11, is being showcased by Cryptsoft, Feitian, Fornetix, Oracle, Quintessence Labs, Utimaco, and Watchdata. Their implementations show how cryptographic objects with combinations of one or more symmetric keys, asymmetric keys, or certificates between vendor systems can be generated and found. Key and certificate usage within the implementations also are being displayed.

The demos feature two versions of PKCS#11—the current, well established 2.4 version as well as the new 3.0 version under development.

Support for STIX and TAXII

Bay Dynamics co-founder and CTO, Ryan Stolte, said, "Understanding how much cyber risk an organization faces depends on high-quality information. By marrying cyber threat intelligence with information about an organization's valuable assets and security posture, organizations can achieve an accurate and actionable picture of which threats could cause the greatest financial harm. We're excited to showcase at this year's OASIS Interop Demo how Risk Fabric leverages the STIX and TAXII standards as an important part of determining enterprises' cyber value at risk."

EclecticIQ CEO & Founder, Joep Gommers, said, "The OASIS STIX/TAXII standards have accelerated and driven the adoption of actionable Cyber Threat Intelligence throughout enterprises and governments. At the RSA Conference 2017, EclecticIQ will showcase its STIX/TAXII-based Threat Intelligence Platform at the OASIS booth."

DFLabs CEO & Founder, Dario Forte, said, "DFLabs IncMan 4.0, Security Automation and Orchestration for incident response can be enriched with actionable intelligence to provide effective direction to your SOC team. DFLabs will demonstrate how IncMan supports industry-standard threat intelligence exchange formats like STIX as well as integration with commercial threat intelligence feeds. Visualizing the correlation between incidents and artifacts allows analysts to promptly apply industry recognized response and mitigation actions."

Fujitsu Director Marketing & Sales Div. (Cyber Systems) Defense Systems Unit, Hitoshi Habe, said, "Fujitsu will demonstrate CTIM (Cyber Threat Intelligence Management System) proto-type. This system includes a function to display an overview of the constituent elements of cyber-attacks recorded in CTI information, including essential details, and displays a diagram of the relationships between these elements. CTIM also offers CTI sharing function that enables secure and easy CTI sharing between organizations. Fujitsu has been a member since the OASIS CTI Technical Committee's establishment, and CTIM supports the STIX format."

IBM Security VP of Product Management and Strategy, Jason Corbin, said, "Standardizing the language of shared threat intelligence is one of the single most important steps that organizations can take to defend against

future cyberattacks. With the ultimate goal of making the security community stronger and more prepared, IBM proudly supports the development of the STIX and TAXII standards and will continue to incorporate them into our security offerings."

LookingGlass Cyber Solutions CTO, Allan Thomson, said, "LookingGlass is a strong advocate for standards to support an open ecosystem and sharing within the cyber threat Intelligence community. We are proud to be an active participant in the OASIS Technical Committee that is introducing STIX/TAXII 2.0, which we believe results in increased and more timely sharing of threat intelligence."

NC4 Cyber Security Group VP, George Johnson, said, "This year NC4 plans to showcase CTX/Soltra Edge which is a premier Communications Platform that allows for the aggregation of Cyber Threat Intelligence (CTI). CTX/Soltra Edge facilitates ingestion and distribution of CTI in one common format that allows analysts to get out of the business of data normalization and refocus on the business of analysis. CTX/Soltra Edge uses open standards (STIX/TAXII) to empower an end-to-end community defense model."

New Context CEO, Daniel Riedel, said, "As a proud sponsor and member of the OASIS CTI Technical Committee, we believe strongly in transparent standards as well as continuous improvement. Over the past year, a tremendous amount of work and collaboration went into developing STIX 2.0, and we look forward to its release because automation and machine-readable standards for threat intel truly are the future."

ThreatQuotient Director, Threat Intelligence Engineers, Chris Jacob, said, "The STIX/TAXII standard has become a critical element in the exchange of Threat Intelligence amongst industry groups. There is a lot of importance in having a dependable and experienced organization at the helm when defining its evolution. ThreatQ is excited to work with OASIS and the other industry professionals as the standard continues to grow."

TruSTAR Co-Founder & CEO, Paul Kurtz, said, "Companies realize there is an urgent need to have situational awareness of cyber incidents. The TruSTAR platform offers real-time correlation with events in the broader community without market and reputational risk. Cyber threat intelligence standards such as CybOX, STIX, and TAXII are central to TruSTAR's mission of building the most robust intelligence exchange platform on the market."

Support for KMIP and PKCS #11

Cryptsoft CTO, Tim Hudson, said, "Reliable storage, availability and lifecycle management of security objects has become a focus for enterprises; interoperability between key management, security, and encryption systems is no longer 'nice-to-have' but essential. The OASIS KMIP and PKCS #11 standards provide mechanisms to address the fundamental interoperability requirement enabling migration from single point ad-hoc products to full enterprise security solutions. As a major OEM technology supplier, supplying OASIS conformant solutions ensures interoperability is a reality for our customers."

Hancom Secure Senior Researcher of R&D Center, Sun-ho Lee, said, "We are very pleased to participate in the OASIS KMIP Interop for the first time and demonstrate our KMIP Server and Client interoperability at the showcase in RSA 2017. Hancom Secure is a leading company in the security software field to create security standards in Korea. As a KMIP TC member, we are proud to introduce HancomSecure KeyManager offering our customers a centralized key management and an easy and quick KMIP application with Client SDK."

Hewlett Packard Enterprise HPE Security VP & GM, Albert Biketi, said, "Customer adoption of key management integration using OASIS KMIP further enables encryption to be embedded into more mainstream applications and systems to simplify interoperability. Industry standards are of the utmost importance to HPE

and today we have one of the most robust partner integration portfolios available. Our HPE ESKM solution supports FIPS 140-2 and Common Criteria EAL2+ standards."

Kryptus CEO, Roberto Gallo, said, "Kryptus provides cryptographic hardware with secure execution of client applications and algorithms along with client-oriented features, reducing operational and infrastructure costs without the loss of security, performance, and reliability. Kryptus is specialized in the protection of highly-sensitive information for more than 10 years with leading edge products and advanced hardware protection features."

Oracle VP Solaris, Markus Flierl, said, "As cryptography is becoming an expected part of on-premise, cloud and ZFS SA storage deployments, we are excited by the benefits of enterprise key management interoperability to make enterprise administration easier and safer. We support the OASIS PKCS11 standard efforts to create a vendor-neutral cryptographic services API and are excited about making your data more secure."

SafeNet product manager for data protection, Stephen Kingston, said, "With more than 45 documented KMIP integrations, SafeNet KeySecure helps protect data in the most widely deployed IT products and services across the cloud, backup, big data, and storage including IBM DB2, Nutanix, MongoDB, Centrify and Commvault. Enterprises benefit from our broad ecosystem of technology partner product integrations that help unify the control of data and improve compliance, all from a centralized key management solution."

Additional information:

OASIS Cyber Threat Intelligence Technical Committee
<http://www.oasis-open.org/committees/cti/>

OASIS KMIP Technical Committee
<http://www.oasis-open.org/committees/kmip/>

OASIS PKCS 11 Technical Committee
<http://www.oasis-open.org/committees/pkcs11/>

About OASIS:

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-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, cloud computing, Web services, the Smart Grid, content technologies, business transactions, emergency management, and other applications. 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 100 countries. <http://www.oasis-open.org>

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