STIX and TAXII

Automated Sharing of Threat Intelligence

Cybersecurity Showcase | South Hall, Booth #1701

The OASIS Cybersecurity Showcase brings together nine members of the OASIS Cyber Threat Intelligence Technical Committee to demonstrate how to share threat data safely by using the widely adopted, open specifications; STIX and TAXII. Anomali, EclecticIQ, Fujitsu, Hitachi, IBM Security, New Context, NC4, Threat Quotient, and TruSTAR will show how STIX and TAXII is being deployed in their products.

In addition to seeing the demonstrations, RSA attendees are learning more about how the latest public releases of STIX and TAXII are making it easier to automate cyber threat intelligence sharing.

Cybersecurity standards at OASIS:

STIX

A structured language for threat intelligence that enables organizations to share intelligence in a consistent, machine-readable way. **STIX lets you anticipate computer-based attacks and respond faster and more effectively.**

Learn about STIX 2.0: cti-tc.github.io

TAXII

A transport mechanism for communicating cyber threat information over HTTPS in a simple, scalable way. TAXII defines an API that aligns with common sharing models. It's designed to support exchanges represented in STIX.

CSAF

A format for disclosing cyber vulnerabilities so that machine-readable security advisories can be produced and consumed. CSAF makes it easier to identify and address known vulnerabilities within your networks, regardless of platform.

OpenC2

A standardized language for automated defense against cyber-attacks that enables machine-to-machine exchange of commands for investigating or mitigating against attacks. OpenC2 supports real-time, machine-speed response as well as interoperable coordination between domains.

For details on how to get involved in any of these initiatives or to bring your cybersecurity project to OASIS, contact join@oasis-open.org.

STIX & TAXII Showcase Participants

ANOMALI™

The Anomali suite of threat intelligence solutions empowers organizations to detect, investigate and respond to active cybersecurity threats. The award-winning ThreatStream threat intelligence platform aggregates and optimizes millions of threat indicators, creating a "cyber no-fly list." Anomali integrates with internal infrastructure to identify new attacks, or search forensically over the past year to discover existing breaches, and enables security teams to quickly understand and contain threats. Anomali also offers STAXX, a free tool to collect and share threat intelligence, and provides a free, out of the box intelligence feed, Anomali Limo. Follow us on Twitter: @anomali. **www.anomali.com**

eclectic iq

EclecticIQ helps organizations turn cyber threat intelligence into business value with a suite of products built for cyber security professionals in threat intelligence, threat hunting, SOC, and Incident Response roles. EclecticIQ Platform is the analyst-centric threat intelligence platform based on STIX/TAXII that meets the full spectrum of intelligence needs. EclecticIQ Fusion Center enables the acquisition of thematic bundles of human-qualified cyber threat intelligence from leading suppliers with a single contract. **www.eclecticiq.com**

FUJITSU

Fujitsu is a leading Japanese information and communication technology (ICT) company, offering a full range of technology products, solutions, and services. Approximately 156,000 Fujitsu people support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers. **www.fujitsu.com**

IBM Security

Cybercriminals are growing in number and sophistication, rendering traditional perimeter solutions power-less against today's advanced threats. IBM Security, with 7,500 dedicated professionals in more than 130 countries, delivers next-generation intelligent, integrated security technology and services to out-think cybercriminals, detect threats and respond quickly to breaches. We focus on the most critical needs of more than 12,000 clients: transforming security programs; optimizing and automating security operations and incident response systems; and protecting their most critical and valuable information. **www.ibm.com**

NC4

NC4 delivers safety and security solutions for both business and government organizations. We revolutionize how organizations and communities collect, manage, share and disseminate information to reduce cyber threats, fight crime, mitigate risks, and manage incidents. NC4 also provides cyber threat sharing solutions both through secure collaboration services and recently (via Soltra Edge), through automated, structured, and standardized (STIX/TAXII) mechanisms. **www.NC4.com**

NEW CONTEXT

New Context protects people's security and privacy by designing and building secure, scalable systems to accelerate the digital transformation of critical infrastructure and the industrial internet. Our Lean Security methodology allows for a focus on innovation by fully integrating security into software development, architecture, and infrastructure management. We are a team of highly skilled experts in the areas of product development, operations, security, compliance, and cyber risk management. **www.newcontext.com**

THREATQUOTIENT

ThreatQuotient delivers an open and extensible threat intelligence platform (TIP) to provide defenders the context, customization and collaboration needed for increased security effectiveness and efficient threat operations and management. ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders unmatched control through a threat library, an adaptive workbench and an open exchange to ensure that intelligence is accurate, relevant and timely to their business. **www.threatq.com**

TRUSTAR TECHNOLOGY

TruSTAR's intelligence exchange platform incentivizes information exchange among peers, partners, and groups. As companies see data relevant to them they can easily submit, sanitize, and share data to discover how cyber incidents relate to other companies. **www.trustar.co**