Mitre Co STIX TAXII List	Copyright 2017 The MITRE Corporation. Legal
Mitre Co STIX TAXII List :	
CybOX	MAEC
Getting Started	
Documentation	
Data Model	
Community	
About	
STIX 2.0 documentation is available here. This site contains archived STIX 1.x documentation. STIX is now maintained by the OASIS CTI TC.	
STIX/TAXII Supporters List (Archive)	
IMPORTANT: The Supporters List has been transitioned to new lists hosted by the OASIS CTI TC. This page has been moved to "Archive" status and will no longer be updated.	
The most up-to-date “STIX, CybOX, and TAXII Supporters” lists are now available on the OASIS website for both Products and Open Source Projects.	
A registration form is available from the OASIS CTI TC to request inclusion on the “STIX/TAXII/CybOX Supporters” lists hosted by the CTI TC.	
(Archive)	
STIX, CybOX, and TAXII are being implemented in many products, services, open source projects, and global communities.	
User Communities (Archive)	
These organizations have publicly announced support for STIX and/or TAXII. (Archive)	

User Community	Organization	Description	STIX	TAXII	Reference
Advanced Cyber Defense Center - Central Clearing House	Advanced Cyber Defense Center (ACDC)	The European ACDC community brings together almost 50 partners, tens of tools and technologies to share cyber risk intelligence, following a European Competitiveness and Innovation Progam from the Policy Support Program of the European Commission under the FP7 program. The platform exchanges threat intelligence on a trustworthy basis amongst the partners, and is open to other future partners	✓	✓	Cited as product feature on website
BrightPoint Security Threat Intelligence Exchange	BrightPoint Security	BrightPoint Security Exchange makes it easier for communities to quickly message and share their data and insight through conversational exchanges, enabling community investigation and remediation recommendations. Informal conversations can begin to identify the elements for a more complete threat picture that can then easily create formal and structured STIX messages to share with ISACs, ISAOs or other Trusted Circle communities automated from within BrightPoint Sentinel	✓	✓	Cited as product features on website, Press Release, Included in white paper, Mentioned in numerous blog articles
Cyber Fed Model (CFM)	Argonne National Laboratory	CFM provides the infrastructure for sharing actionable cyber threat information (CTI) in near real-time. Participating sites are able to mitigate threats, put up defenses via the autonomic machine-to-machine communication of indicators of compromise that are uploaded by one participant site and downloaded/acted upon by subscriber sites. CFM is payload agnostic, supporting XML, CSV, JSON, and STIX	✓	-	Cited as product feature in Brochure
Cyber Threat XChange (CTX)	Health Information Trust Alliance (HITRUST)	Automates process of collecting and analyzing cyber threats and distributing actionable indicators	✓	✓	Press Release
Defense Security Information Exchange (DSIE)	Defense Industrial Base Information Sharing and Analysis Organization (DIB ISAO)	DSIE serves as a member-based cyber information-sharing body focused on protecting and defending DIB critical cyber networks and systems and the information residing thereon. STIX and TAXII are the core foundations of the DSIE ACIX (Automated Cyber-Intelligence Inter-Exchange) initiatives focused on providing “Analyst Driven” automated Inter-Exchange of Actionable Cyber-Threat Intelligence	✓	✓	None available
IBM X-Force Exchange	IBM	IBM X-Force Exchange is a cloud-based platform that allows organizations to easily collaborate on security incidents, as well as benefit from the ongoing contributions of IBM experts and community members. STIX and TAXII are implemented for observables and collections in X-Force Exchange. Public collections are now even more public and can be accessed without connecting to everybody on the Internet. These and other public collections can be easily imported to a security intelligence platform to reduce the time to action by creating a rule to produce an alert when indicators present in the collection are found in the infrastructure being monitored	✓	✓	Blog article
ICS-ISAC	Industrial Control System Information Sharing and Analysis Center (ICS-ISAC)	ICS-ISAC brings together infrastructure stakeholder to improve cybersecurity knowledge sharing. ICS-ISAC’s virtual SoltraEdge server, which includes STIX and TAXII interoperability, provides real-time information sharing for members	✓	✓	Cited as features on website

User Community	Organization	Description	STIX	TAXII	Reference
Information Sharing Architecture (ISA)	Enhance Shared Situational Awareness (ESSA) Initiative	ISA enables machine speed sharing of cyber threat information via STIX and TAXII to promote shared cyber situational awareness among cyber mission partners (U.S. Federal Cyber Centers, other U.S. government, U.S. critical infrastructure owners, and key allies) in accordance with existing policy directives	✓	✓	None available
Malware Information Sharing Platform (MISP)	Computer Incident Response Center Luxembourg (CIRCL) MISP Community	MISP allows organizations to share, store, and correlate information about malware and threats and their indicators, including STIX export	✓	-	Cited as product feature on website
NH-ISAC National Health Cybersecurity Intelligence Platform	National Health Information Sharing & Analysis Center (NH-ISAC)	Automating cybersecurity “actionable” threat intelligence, with STIX and TAXII interoperability, powered by Soltra-Edge and Vorstack	✓	✓	Press Release
Open Threat Exchange (OTX) 2.0	AlienVault, Inc.	OTX is an open threat information sharing and analysis network, upon which the latest threat intelligence will automatically update local security products into open formats such as STIX, JSON, OpenIoC, MAEC, and CSV	✓	-	Press release
Retail Cyber Intelligence Sharing Center (R-CISC) Intelligence Sharing Portal	Retail Information Sharing and Analysis Center (Retail-ISAC)	Intelligence Sharing Portal managed by the Financial Services Information Sharing and Analysis Center (FS-ISAC)	✓	✓	Press Release, News Article
Products and Services (Archive)					
Many vendors have implemented STIX and TAXII in their product and service offerings. (Archive)					
Offering	Vendor	Description	STIX	TAXII	Reference
Adaptive Threat Protection Solution	Tripwire, Inc.	Integrates peer and community threat feeds, leveraging STIX and TAXII standards, and other commercial threat intelligence services	✓	✓	Press Release
Advanced Threat Prevention	Check Point Software Technology Ltd.	ATP allows users to import indicators into threat prevention technologies, anti-bot, anti-virus, with an interface to upload STIX-formatted messages containing indicators into threat indicator database	✓	-	Cited as product feature in “Threat Prevention R77 Versions Administration Guide”
Alice CTI Sharing & APT Identifying Platform	TianJi Partners Info Tech Co., LTD.	Chinese-developed CTI sharing platform, integrating the feeds from over 10 security companies and two individual CTI communities locally, to provide CTI exchanging and ATP identifying services; STIX format and TAXII protocol are the basic instruments for Alice platform users interconnecting	✓	✓	Product web page
Autopsy	sleuthkit.org	Digital forensics platform and graphical interface to The Sleuth Kit that includes an “Indicators of Compromise - Scan a computer using STIX” module	✓	-	Cited as product feature on website, Dedicated “STIX” page in user documentation

User Community	Organization	Description	STIX	TAXII	Reference
BOTsink	Attivo Networks, Inc.	BOTsink deception server is designed to detect APTs, HTTPS, zero-day, and stolen credential attacks. Attivo AMR engine captures and analyzes attacker IPs, methods, and actions that can then be viewed in the Attivo Threat Intelligence Dashboard, can be exported in IOC, PCAP, STIX, CSV formats	✓	-	Cited as product feature on website, Cited as product feature in magazine product review article
BrightPoint Sentinel	BrightPoint Security	Automated threat intelligence analysis and collaboration platform that "supports many intelligence feeds and other standards, including STIX, TAXII, CybOX, and the Lockheed Martin Kill Chain framework."	✓	✓	Cited as product features on website, Press Release, Included in white paper, Mentioned in numerous blog articles
Bromium LAVA	Bromium Inc.	Endpoint security prodcut leveraging hardware virtualization that automatically creates standardized indicator of compromise reports in STIX/MAEC format for collaboration with other security tools	✓	-	Data Sheet
Cabby	EclecticIQ	A TAXII client implementation designed to act as a Python library and a command line tool supporting all TAXII services according to TAXII specification v1.0 and v1.1	-	✓	Cited as product feature on website, Dedicated STIX/TAXII page on website
Carbon Black	Bit9 + Carbon Black	Endpoint threat detection and response product that collects endpoint activity in which STIX/TAXII data feeds can be matched up against event activity to find when particular indicators or observables occur	✓	✓	Blog article, Github
CATSS	LarkSpear	CATSS (Cyber Automated Threat Sharing System) provides unparalleled cyber threat information sharing solutions to community based ecosystems. CATSS implements TAXII services and ingests STIX formatted data to analyze, report and share threat intelligence	✓	✓	Cited on paper product sheet
ce1sus	GovCERT.lu	ce1sus is an open source threat information database based on STIX	✓	-	README
Confer	Confer Technologies, Inc.	Confer, an advanced threat prevention and incident response solution, can import and export threat data in STIX format using TAXII, allowing customers to operationalize their intelligence across the endpoint	✓	✓	Cited as product features on website, Included in FAQs on website
Corvil Security Analytics	Corvil Limited	Corvil Security Analytics provides full network visibility in real-time and retrospect to enable rapid understanding of the bigger picture of covert attack activity; Corvil brings real-time STIX based indicator detection down to the wire, auto-matching against all network flows and decoded network data	✓	✓	Cited as product features on data sheet, Cited in blog article
Cyberprobe	Cybermaggedon	Cyberprobe is a distributed software architecture for monitoring of networks against attack that includes support for STIX and TAXII	✓	✓	Cited as product features on website
Cyphort	Threat Defense Platform	Cyphort's Advanced Threat Protection solution delivers complete 360º APT defense against current and emerging Threats	✓	✓	Cited as product features on website

User Community	Organization	Description	STIX	TAXII	Reference
CyberSponse Security Operations Platform	CyberSponse,Inc.	CSOP, which provides a central hub for an organization’s security operations and enables automated efforts, has a built-in TAXII server or can use Soltra Edge to both ingest and send STIX packages	✓	✓	Cited as product feature on website
Damballa Failsafe	Damballa, Inc.	Damballa Failsafe analyzes network traffic and automatically detects infected devices after other security controls have failed; security teams receive actionable and prioritized intelligence so they can take immediate action to prevent data theft	✓	-	None available
Deep-Secure iXGuard	Deep-Secure	Deep-Secure iXGuard enables secure information exchange by carefully controlling the content that is shared such that it does not present a risk to the system that it is protecting, including STIX content	✓	✓	Data Sheet
EclecticIQ Platform	EclecticIQ	Powered by STIX and TAXII and enables users to consolidate, enrich, analyze, integrate, and collaborate on intelligence from multiple sources	✓	✓	Cited as product features on website, Dedicated STIX/TAXII page on website
EnCase Endpoint Security	Guidance Software, Inc.	In EnCase Endpoint Security Version 5.12, Structured Threat Information eXpression (STIX) definitions can now be imported globally and used as filtering criteria in any investigation. Customers will be able to root out indicators no matter how well they might be hidden from other technologies, reducing the time it takes to detect and respond security to breaches in their network	✓	-	Cited as product feature in press release
Endpoint Security	Tanium, Inc.	Endpoint security detection and remediation	✓	-	Cited as product features on website, “Tanium IOC Detect” Data Sheet
FLARE - Near Real Time Messaging System	Business Computers Management Consulting Group, LLC (BCMC)	FLARE is used for exchanging messages in a publish/subscribe model, and includes support for STIX and TAXII	✓	✓	Cited in installation guide
FreeSTIX	FreeSTIX	A set of APIs written in Go for generating JSON based STIX messages	✓	-	Cited as product feature on website
FreeTAXII	FreeTAXII	A set of APIs written in Go for generating JSON based TAXII messages	-	✓	Cited as product feature on website
GuardiCore Centra Security Platform	GuardiCore	GuardiCore provides real-time detection and response of advanced attacks in the data center. Once GuardiCore detects a breach inside the data center, it provides Indicators of Compromise (IOC) to its Check Point Security Gateways using the STIX API, allowing security administrators to block future attacks in the data center and at the perimeter	✓	-	Cited as product feature on data sheet, Press release
GPACT	PRODAFT	PRODAFT’s G-PACT Threat Sharing enables real-time sharing of threat details among public and private organizations in an inter-industrial and intra-industrial structure inside a standardized (Human Readable + STIX) format	✓	✓	Cited as product feature on website
hailataxii.com Repository of Open Source Cyber Threat Intelligence Feeds in STIX Format	Hail a TAXII	Repository of open source cyber threat intelligence feeds in STIX format	✓	✓	Cited as product features on website

User Community	Organization	Description	STIX	TAXII	Reference
IBM QRadar	IBM	IBM Security QRadar SIEM consolidates log source event data from thousands of devices endpoints and applications distributed throughout a network. Via the optional Threat Intelligence application, QRadar allows ingestion of threat feeds containing cyber observables, expressed in STIX format via the TAXII protocol. These ingested threat feeds can be monitored for use in real-time correlation rules, as well as used in reports and searches of either log or flow data. QRadar also allows the real-time publishing of newly discovered cyber observables in QRadar, to any TAXII server	✓	✓	Web page, Blog article
iDefense	VeriSign, Inc.	iDefense threat intelligence will support STIX 2.0/TAXII in Q2 2016	✓	✓	TBA
Infoblox Grid	Infoblox, Inc.	Infoblox Grid ingests third-party threat intelligence in STIX format using our fully integrated TAXII server. This allows customers to automatically create a blacklist of domains and IP addresses in Infoblox, enabling them to respond to threats faster using their local threat intelligence	✓	✓	Blog article
InTELL Version 3.0	Fox-IT	Real-time contextual cyber intelligence	✓	✓	Cited as product features on website, Press Release
Interflow	Microsoft Corporation	Security and threat information exchange platform	✓	✓	Cited as product features on website, Included in FAQ answers on website, Press Release
Invincea Advanced Endpoint Protection 5	Invincea, Inc.	Uniquely combines containerization technology with advanced endpoint visibility, analysis, and control to provide superior compromise detection and elimination; allows selective publication of threats to trusted communities in standard STIX format	✓	-	Press release
iSIGHT Partners ThreatScape API	iSIGHT Partners Inc.	ThreatScape API extends iSIGHT Partners cyber threat intelligence products and associated technical indicators to easily match indicators to rich intelligence context, ingest indicator data associated with intelligence reporting, and collect and consume intelligence reports including those in STIX format	✓	-	Cited as product feature on website, Included in FAQ answers on website, Press Release, Blog article
Jigsaw IOC Service	Jigsaw Security Enterprise Inc.	We offer feeds in STIX and TAXII as well as many other common formats. We offer a complete big data solution for importing and exporting STIX and TAXII data. We integrate with all products that support the standards	✓	✓	Cited as product feature on website, Blog article
Jigsaw Security Enterprise MISP	Jigsaw Security Enterprise Inc.	We provide feeds in STIX and TAXII format for use in our intelligence products to include our MISP host intrusion detection client, our IDS appliances, as well as our Threat Intelligence Platforms	✓	✓	Cited as product features on website, Blog article, included in FAQ answer

User Community	Organization	Description	STIX	TAXII	Reference
LogRhythm Threat Intelligence Service	LogRhythm, Inc.	LogRhythm seamlessly incorporates threat intelligence from STIX/TAXII-compliant providers, commercial and open source feeds, and internal honeypots, all via an integrated threat intelligence ecosystem. The platform uses this data to reduce false-positives, detect hidden threats, and help prioritize alarms	✓	✓	Cited as product features on website, Cited in blog article
Malware Analysis Appliance	Blue Coat Systems, Inc.	Malware Analysis Appliance can export malware characterization data in STIX format	✓	-	Cited in user guide
Malware Information Sharing Platform (MISP)	Computer Incident Response Center Luxembourg (CIRCL) MISP Community	MISP allows organizations to share, store, and correlate information about malware and threats and their indicators, including STIX export	✓	-	Cited as product feature on website
McAfee Advanced Threat Defense	Intel Security	McAfee ATD finds advanced malware and integrates with McAfee security solutions to freeze the threat, identify vulnerable machines, and initiate fix or remediation actions; When McAfee ATD identifies a malicious file or executable, it funnels CybOX STIX-formatted IoC artifacts to McAfee Enterprise Security Manager to interpret and act on them	✓	-	Data Sheet
McAfee Enterprise Security Manager	Intel Security	McAfee Enterprise Security Manager (ESM) version 9.5 and above has taken the cyber threat management to a new level by collecting and translating suspicious or confirmed threat information into actionable intelligence for security operations teams. McAfee ESM 9.5 can import a wealth of security threat data including STIX/TAXII feeds; third party URL's and Indicators of Compromise (IOC's) reported via McAfee Advanced Threat Defense providing security operations teams with directly readable and usable intelligence for security analytics	✓	✓	Blog article
Netskope Active Threat Protection	Netskope, Inc.	Netskope Active Threat Protection, which combines threat intelligence, static and dynamic analysis, and machine-learning based anomaly detection to enable real-time detection, prioritized analysis, and remediation of threats, communicates using STIX/TAXII or OpenIOC standards to exchange threat context and detection information	✓	✓	Cited as product features on website, Press Release
OpenTAXII	EclecticIQ	A Python implementation of TAXII Services that delivers a rich feature set and friendly pythonic API; Implements all TAXII services according to TAXII specification v1.0 and v1.1	-	✓	Cited as product feature on website, Dedicated STIX/TAXII page on website
Palisade	Lockheed Martin	Palisade supports comprehensive threat data collection, analysis, collaboration, and expertise in a single platform. Palisade supports the exchange of intelligence via STIX and CSV for import and export of indicators and observables	✓	-	Cited as product feature on website
pan-stix	Palo Alto Networks, Inc.	pan-stix is a python package for converting Palo Alto Networks Wildfire threat information into STIX/MAEC format	✓	-	Cited as product feature on website

User Community	Organization	Description	STIX	TAXII	Reference
Protect Your Network	Malcovery Security	Machine-readable threat intelligence (MRTI) delivers human-confirmed indicators of current malware infrastructure in near-real time via our API in STIX and other formats for your automated consumption by your SIEM, proxy, firewall, etc.	✓	-	Cited as product feature on website
RedSocks Malware Threat Defender	RedSocks B.V.	RedSocks Malware Threat Defender is a network appliance that analyses digital traffic flows in real-time based on algorithms and lists of malicious indicators; it includes the ability to import malware intelligence that is structured according to the STIX and TAXII format	✓	✓	Press Release
RSA Enterprise Compromise Assessment Tool (ECAT)	RSA Security	RSA ECAT performs checks to help security analysts determine if a file is malicious, including the ability to check the legitimacy of file certificates and hashes, check for known threats by incorporating YARA rules, importing STIX data, and leveraging multiple AV engines through OPSWAT Metascan, identify any code modifications made by malware, and more	✓	-	Cited as product feature on data sheet
Soltra Edge	Soltra	Open and scalable threat information platform that uses open standards	✓	✓	Cited as product features on website, Included in FAQ answers on website, Press Release
SPLICE Version 1.3.1	Splunk, Inc.	Correlates Indicators of Compromise (IOCs) from SPLUNK data	✓	✓	Cited as product features on website
Splunk App for Enterprise Security	Splunk, Inc.	Next-generation security intelligence platform that includes integration with STIX/TAXII and OpenIOC to allow access to threat intelligence using emerging industry specifications	✓	✓	Press release
STIX Data Generator	Cosive	Automatically generates STIX content in order to help people learn more about STIX document structures, as well as test their STIX products	✓	-	Cited as product features on website
Targeted Threat Intelligence Service	Solutionary	Targeted Threat Intelligence Service	✓	-	Cited as product feature on website, Press Release
TAXII Directory	EclecticIQ	A sort of a phone book, listing organizations and available cyber threat intelligence servers and feeds	✓	✓	Cited as product features on website, Dedicated STIX/TAXII page on website
TAXII stand	EclecticIQ B.V.	We host TAXII servers; all currently hosted TAXII Server are listed in our directory server for discoverability	-	✓	Cited as product feature on website
Threat Central	Hewlett Packard	Threat Central is an open, automated, cloud-based platform for security intelligence that enables customers to consume and share community-driven intelligence. With support for open threat intelligence standards such as STIX and TAXII, we are product agnostic, enabling any customer to connect to our platform via API for machine-to-machine communication	✓	✓	Datasheet

User Community	Organization	Description	STIX	TAXII	Reference
ThreatConnect	ThreatConnect, Inc.	Available both on-premises and in the cloud, ThreatConnect is a threat intelligence platform that allows you to aggregate, analyze, and act on threat intelligence data, including STIX documents via TAXII	✓	✓	Cited as product features on website, Press Release
ThreatQ	ThreatQuotient, Inc.	On-premise threat intelligence platform (TIP) that automates, structures, and manages intelligence in a central analytical repository	✓	✓	"ThreatQuotient Battle Rhythm Workflow" Data Sheet
ThreatStream OPTIC	ThreatStream	Threat Intelligence Management platform with full support for STIX and TAXII from both an import and export capacity	✓	✓	Cited as product feature on website
threatTRANSFORM	threatTRANSFORM	Open source application designed to streamline the creation, compiling, and publishing of STIX datasets	✓	-	Cited as product features on website, Press Release
TitaniumCore Version 2.6	ReversingLabs	Threat detection and automated static analysis platform	✓	-	Data Sheet
Tripwire Enterprise 8.4	Tripwire, Inc.	Incorporates automated feed of Indicators of Compromise (IoC) from TAXII servers, which receive IoC from industry-specific Information Sharing and Analysis Centers and other providers of open source threat intelligence; Also integrates feeds from tailored commercial threat intelligence services	-	✓	Press Release, Blog article