Supported Products List – Jigsaw Security Enterprise

Organization	Product	Description
Attivo Networks, Inc.	BOTsink	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
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
Blue Coat Systems, Inc.	Malware Analysis Appliance	Malware Analysis Appliance can export malware characterization data in STIX format
BrightPoint Security	BrightPoint Sentinel	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."
Bromium Inc.	Bromium LAVA	Endpoint security prodcut leveraging hardware virtualization that automatically creates standardized indicator of compromise reports in STIX/MAEC format for

		collaboration with other security tools
Carbon Black	Carbon Black STIX/TAXII Connector	Carbon Black Enterprise Response and Enterprise Protection - ETDR solutions (Endpoint Threat Detection & Response).
Check Point Software Technology Ltd.	Advanced Threat Prevention	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
Corvil Limited	Corvil Security Analytics	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
Confer Technologies, Inc.	Confer	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
Cosive	STIX Data Generator	Automatically generates STIX content in order to help people learn more about STIX document structures, as well as test their STIX products
Cybermaggedon	Cyberprobe	Cyberprobe is a distributed software architecture for monitoring of networks against attack that includes support for STIX and TAXII
Cyphort	Threat Defense Platform	Cyphort's Advanced Threat Protection solution delivers complete 360 APT defense

		against current and emerging Threats
CyberSponse,Inc.	CyberSponse Security Operations Platform	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
Damballa, Inc.	Damballa Failsafe	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
Deep-Secure	Deep-Secure iXGuard	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
Group-IB	Bot-Trek Intelligence	SaaS-model product, that delivers tailored threat intelligence to specific customers. Information can be accessed and consumed through GUI or through STIX/TAXII API.
Guidance Software, Inc.	EnCase Endpoint Security	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
EclecticIQ	EclecticIQ Platform	EclecticIQ is an applied cyber intelligence technology

		provider, enabling enterprise security programs and governments to mature a Cyber Threat Intelligence (CTI) practice, and empowering analysts to take back control of their threat reality and to mitigate exposure accordingly.
Fox-IT	InTELL Version 3.0	Real-time contextual cyber intelligence
GuardiCore	GuardiCore Centra Security Platform	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
Hail a TAXII	hailataxii.com	Repository of open source cyber threat intelligence feeds in STIX format
HPE Security Threat Central	HPE Security Threat Central	HPE Threat Central enables enterprises to collaborate via a community-sourced security intelligence platform that incorporates dynamic threat analysis scoring to produce relevant, actionable intelligence to combat advanced cyber threats.
IBM	IBM QRadar	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
Infoblox, Inc.	Infoblox Grid	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
Intel Security	McAfee Advanced Threat Defense	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
Intel Security	McAfee Enterprise Security Manager	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 URLï¿½s and Indicators of Compromise (IOCï¿½s) reported via McAfee Advanced Threat Defense providing security operations teams with directly

		readable and usable intelligence for security analytics
Invincea, Inc.	Invincea Advanced Endpoint Protection 5	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
iSIGHT Partners Inc.	iSIGHT Partners ThreatScape API	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
Jigsaw Security Enterprise Inc.	Jigsaw IOC Service	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
Jigsaw Security Enterprise Inc.	Jigsaw Security Enterprise MISP	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
LogRhythm, Inc.	LogRhythm Threat Intelligence Service	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
Netskope, Inc.	Netskope Active Threat Protection	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
Lockheed Martin	Palisade	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
LarkSpear	CATSS	CATSS is a revolutionary CTI platform that consumes and produces CTI in STIX. CATSS also provides data aggregation, advanced analytic processing, predictive analysis and automated machine to machine alerts.
LogRhythm	LogRhythm Threat Intelligence Service	LogRhythm provides the ability to add custom STIX/TAXII compliant providers, such as Soltra Edge, enabling organizations that participate in industry-specific or government-led trusted exchanges to easily incorporate threat intelligence into LogRhythm.
LookingGlass	ScoutVision	ScoutVision is a Threat Intelligence Platform providing identification, classification and pre-emption of cyber security threats targeting commercial companies, critical

		infrastructure, and government organizations. It automates and ingests over 100 threat data feeds including STIX-based feeds over TAXII. Threat information is managed and presented over a continuously updated global Internet topology map that tracks the ownership, interactions, and changes to your public Internet footprint, allowing users to share STIX-based indicators related to the global Internet threats.
Malcovery Security	Protect Your Network	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.
Microsoft Corporation	Interflow	Security and threat information exchange platform
Model Driven Solutions	Threat and risk analytics gateway	We support government and commercial clients enabling a model based approach to aggregating, analyzing and translating information. We also help organizations develop and implement standards.
New Context		
PRODAFT	GPACT	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
Qihoo 360		
RedSocks B.V.	RedSocks Malware Threat Defender	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
ReversingLabs	TitaniumCore Version 2.6	Threat detection and automated static analysis platform
RSA Security	RSA ECAT	RSA ECAT is a continuous endpoint solution providing contextual visibility beyond a single alert to provide incident responders and security analysts a full attack investigation platform to detect and respond in real-time against advanced attacks -- known and unknown, as well as malware and non-malware based threats. RSA ECAT uses behavior analytics to help security analysts determine if a file is malicious. It also provides the ability to check the legitimacy of file certificates and hashes, and to check for known threats by incorporating YARA rules, importing STIX formatted data, leveraging multiple AV engines through OPSWAT Metascan, and other methods.
sleuthkit.org	Autopsy	Digital forensics platform and graphical interface to The Sleuth Kit that includes an ï¿½Indicators of Compromise - Scan a computer using STIXï¿½ module
Soltra	Soltra Edge	Open and scalable threat information platform that uses open standards
Solutionary	Targeted Threat Intelligence Service	Targeted Threat Intelligence Service
Splunk, Inc.	Splunk App for Enterprise Security	Next-generation security intelligence platform that includes integration with STIX/TAXII and OpenIOC to allow access to threat

		intelligence using emerging industry specifications
Splunk, Inc.	SPLICE Version 1.3.1	Correlates Indicators of Compromise (IOCs) from SPLUNK data
ThreatConnect	ThreatConnect	we ingest and export data in stix
TianJi Partners Info Tech Co., LTD.	Alice CTI Sharing & APT Identifying Platform	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
Tanium, Inc.	Endpoint Security	Endpoint security detection and remediation
Tripwire, Inc.	Adaptive Threat Protection Solution	Integrates peer and community threat feeds, leveraging STIX and TAXII standards, and other commercial threat intelligence services
ThreatConnect, Inc.	ThreatConnect	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
ThreatQuotient, Inc.	ThreatQ	On-premise threat intelligence platform (TIP) that automates, structures, and manages intelligence in a central analytical repository
ThreatStream	ThreatStream OPTIC	Threat Intelligence Management platform with full support for STIX and TAXII from both an import and export capacity
threatTRANSFORM	threatTRANSFORM	Open source application designed to streamline the creation, compiling, and publishing of STIX datasets
Tripwire, Inc.	Tripwire Enterprise 8.4	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
VeriSign, Inc.	iDefense	iDefense threat intelligence will support STIX 2.0/TAXII in Q2 2016