Research Report
on

"Extensive Analysis on Pervasive Threat-Intel Space Tools"

Submitted By:
Vishakh Lakshmikanth

DEPAUL
UNIVERSITY
COLLEGE OF COMPUTING
AND DIGITAL MEDIA

Under the Guidance of:
Prof., Juan Cortes

Abstract:

Implementing the Cyber-Security intelligence is one of the main fundamentals of an organization’s security program. Cyber threat intelligence can be extracted internally and from various external sources wherein it must be collected, analyzed, shared and leveraged. This report mainly focuses on the analysis of the various threat intel space tools that they are capable to perform and act in case of cyber-threat incidents thus becoming the fundamental component of the security policies.

This respective research report emphasizes on threat intel space tools such as Threat Connect, Threat-Stream, Soltra, MISP, Threat Quotient, Threat Exchange, Maltego and others which forms the baseline of the security analysis.

Introduction:

Effective use of Cyber-Threat Intelligence (CTI) is a fundamental tool for defending against malicious infections from the outer/inner network.

According to Gartner, Cyber-Threat Intelligence is an “Evidence-based knowledge that includes context, mechanism, suitable indicators, related implications and actionable suggestions about an existing or future emergent hazard that can be used to inform decisions regarding the subject’s response to that hazard”.

In general sense, CTI is an elusive concept since it is quite challenging to detect, capture and to recall/retrace the flow of malware. CTI has its key purpose to provide technical developments and security in CyberCrime, Hactivism (illegal hacking) and Cyber Espionage (active/passive spying).

For a threat to exist, there must be a combination of intent, capability and opportunity. Threat Intelligence is often exhibited in the form of Indicators of Compromise (IOC) and performs its actions via its lifecycle: plan, collect, process, produce and disseminate data. Tactical threat intelligence generally deals with attempting to collect right type of network information, analyzing, identifying the threats and responding to it.

There are various threat indicators wherein they indicate the possibility of an attack or some kind of compromise that would be going to happen. Threat indicators includes file hashes/signatures, domains, IP address, malware detectors, web proxy’s and so on.

Basically, there are three types of Cyber-Threat intelligence:

- Operational Intelligence: This is entirely generated by the computers via the help of data identification and collection through to enrichment and analysis.
- Strategic Intelligence: This mainly focuses on much more fundamental and difficult process of identifying and analyzing the threats to an organization’s core assets including customers, employees, products and infrastructure. This form of intelligence can be achieved by highly skilled human analysts thus making a defensive security architecture.
- Tactical Intelligence: This enable the assessment of real-time events, investigations and provides day-to-day operational support such as development of cyber-signatures, IOC’s and so on.

Cyber-Threat Intelligence Tools:

In real-time, we can find hundreds of tools, services and products that helps organizations with teams of all sizes-budgets to combat ongoing threats.

Following a lineup are some essential and effective yet futuristic tools that provides threat detection and incident response teams a powerful toolbox to fight against cybercriminals.

1. Threat Connect:

This tool has a suite of products designed to meet the threat intelligence needs of any organization, no matter the maturity level. Threat Connect arms any organization with the most powerful defense layer against cyber threats and provides the confidence to make more effective strategic business decisions. This suite has been built on the industry's intelligence driven, extensible security platform. Its products are designed to meet the threat intelligence aggregation, analysis and faster yet reliable automation. This results in overall reduction in detection to response time and enhanced asset protection.

Threat Connect provides some unique features such as:

a) Threat Intelligence: This combines external threat data from the trusted sources with the own in-house data to detect and eliminate the false positives and discover relevant threats. It leverages automation more quickly to gain context and enhances the security data with more enrichment tools. Intelligently uses the visualizations to detect any unique patterns and trends to uncover threat actor's capabilities, techniques and effects.

b) Analytics: Provides faster and data-driven decisions. It easily coordinates and prioritizes the entire security operation's identification, prevention and incident response tasks using proprietary analytics. This provides quick view of data that exhibits efforts thus enabling to gain better understanding of the threats that an organization faces.

c) Orchestration: Wherein this creates and acts on the threat intelligence to shorten the analysis time of detection and incident response. This includes intelligence, human analysis and configurable playbooks- all in one thus provides effective, focused and more efficient incident response. This blocks threats more faster by automating effective actions combined with some of the company's existing defensive tools/with cyber-security team's analytical intelligence.

Unique and Futuristic Products suite of Threat Connect are as follows:

a) TC Analyze: It is built on the threat connect platform, this provides a central place to view organization's team tasks, analyzing the threat data and use of all other security tools.

   Benefits of TC Analyze:

   - ✓ Identify
   - ✓ Prioritize
   - ✓ Investigate
   - ✓ Integrate

b) TC Manage: This provides the automation of a single part or for entire processes for managing the threat data including sending the indicators for defensive tools for alerting/blocking/looping of defensive attacks. This includes the features of Orchestration.

   Benefits of TC Manage:

   - ✓ Automate entire tasks
   - ✓ Maximum efficiency
   - ✓ Enhanced Processes
   - ✓ Integration of various tools

c) TC Identify: This provides vetted, actionable threat intelligence from more than 100+ open source feeds, research communities and utilizes the TC Exchange partners.

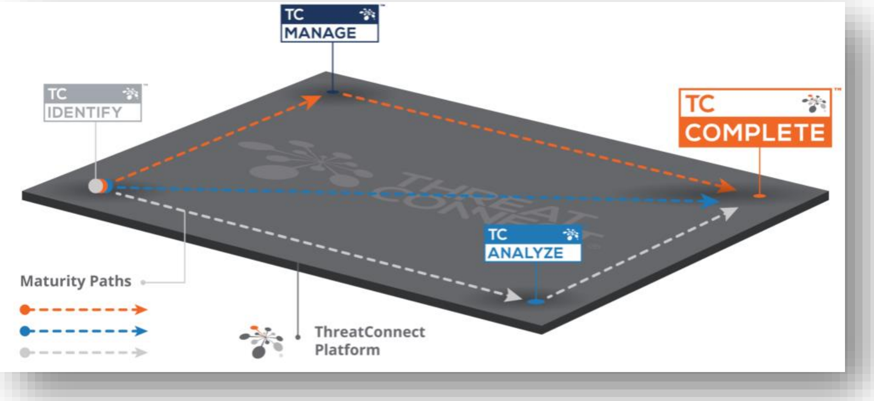
   Benefits of TC Identify:

   - ✓ Enhanced Detection by drastically reduced false positives.
   - ✓ Aggregates all the source feeds in one location.
   - ✓ Unmasked adversaries.

d) TC Complete: This tools acts upon the security operations and analytics platform thus including all the features and security options that Threat Connect offers wherein it allows for informed decision-making based on organization's threat intelligence.

   Benefits of TC Complete:

   - ✓ Gain mores visibility on the attack.
   - ✓ Automates nearly all the security operations thus maximizing the efficiency.
   - ✓ Provides control to the organization's cyber-security officials to configure the platform as per the needs thus proactively hunt threats in the network.



SnapShot 1: *Underlying architecture of ThreatConnect Platform*

2. Threat Stream:

Threat Stream is available as SaaS that operationalizes the threat intelligence, automating collection and integration thus enabling security teams to analyze and respond to the threats. Threat Stream provides some unique features such as:

a) Collection: Threat Stream manages the ingesting intelligence from many trustful-reliable sources including:

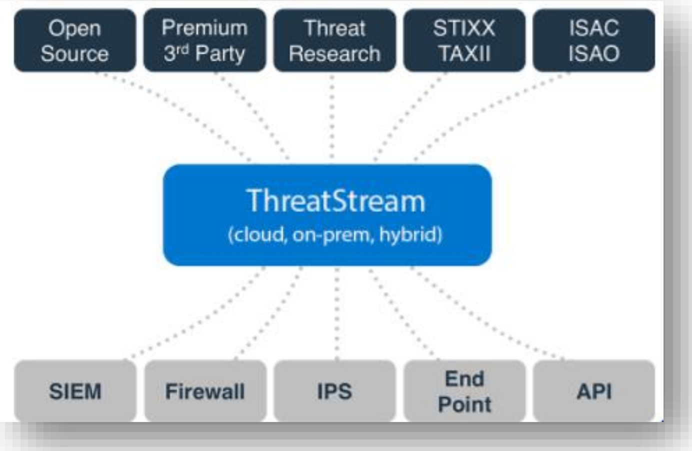
- TAXII/STIX DataSource.
- Commercial threat intelligence provider.
- Unstructured Intelligence: CSV's, Email's
- ISAO/ISAC distributed threat intelligence.
- Open-Source threat feeds.

b) Manage: Threat Stream takes raw threat data the converts into rich, usable and secure intelligence:

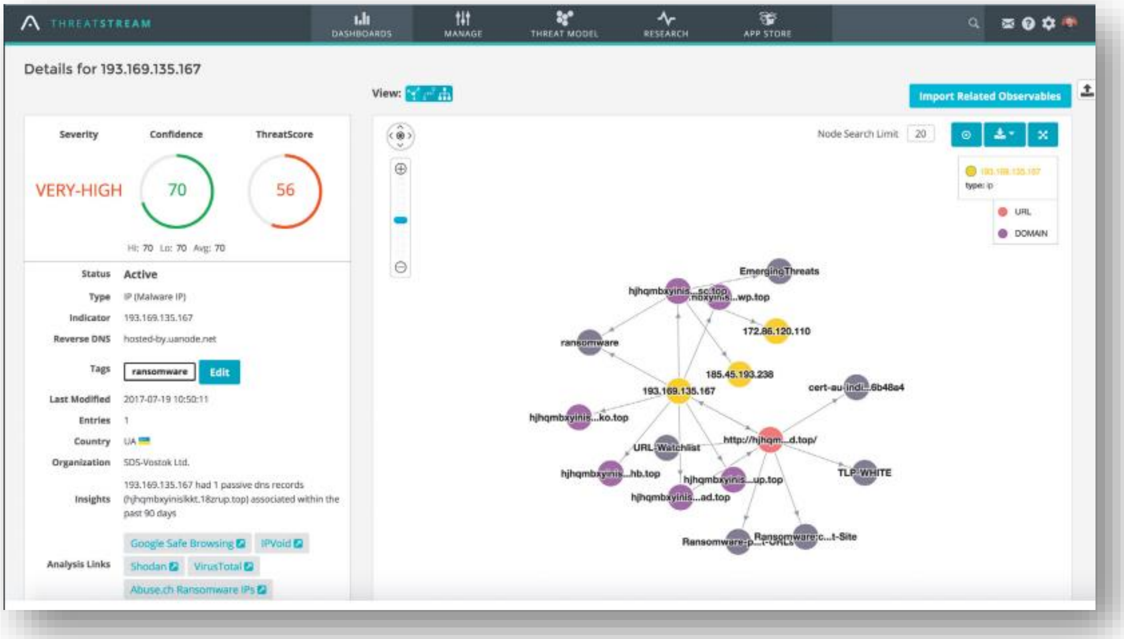
- This enables the normalization of source feeds into a normal taxonomy for ease understandability.
- It has the feature to De-duplicates the data across different and unique source feeds.
- This efficiently removes false positives for more secure and safe environment.
- Enriches data with actor, TTP, campaign and so on
- Upon keen analysis, this associates related threat indicators.

c) Integrate: Threat Stream seamlessly integrates with the internal security systems to make the threat intelligence actionable and efficient to handle any incident response situations.

- This has been deeply integrated with SIEM, FW, IPS, EndPoint.
- It can scaleup to process millions of threat indicators efficiently.
- Risk ranks threats via Machine Learning.
- This includes an additional option for threat bulletins for ease understandability.
- Provides secure 2-way data sharing among trusted and reliable pool.



***SnapShot 2(a)**: Exhibits the connections from external to internal world.*



Details for 193.169.135.167

Severity	Confidence	ThreatScore
VERY-HIGH	70	56

Hi: 70 Lo: 70 Avg: 70

Status	Active
Type	IP (Malware IP)
Indicator	193.169.135.167
Reverse DNS	hosted-by.uanode.net
Tags	ransomware Edit
Last Modified	2017-07-19 10:50:11
Entries	1
Country	UA
Organization	SDS-Vostok Ltd.
Insights	193.169.135.167 had 1 passive dns records (hjhqmbxyinislkkt.18zrup.top) associated within the past 90 days
Analysis Links	Google Safe Browsing IPVoid Shodan VirusTotal Abuse.ch Ransomware IPs

***SnapShot 2(b)**: Displays the sample User-Interface of the ThreatStream Application*

Apart from the above features, threat stream also embeds some analyst-friendly features such as:

- ✓ Association of indicators to Cyber analyst actors.
- ✓ Malicious file analysis within the most secure inbuilt sandbox.
- ✓ Threat investigation engine with analyst's all possible workflow under one roof.
- ✓ Brand Monitoring with detection of brand abuse which includes automatic search for typo-squatted domains and compromised credentials.
- ✓ Easy to collaborate with peers via trusted pool sources.
- ✓ Contextual data includes PassiveDNS, WHOIS and so on.
- ✓ This tool is fully Stix-compatible using the REST API's for easier and secure imports and exports.

Main and immediate advantages of Threat Stream include:

- It enables to centralize all the threat intel data in one secure place.
- Provides the feature to turn any raw indicators into more efficient actionable intelligence.
- This integrates with any existing security investments.
- Enables the security analysts more efficient.

3. Soltra Edge:

Soltra-Edge is a platform for sharing and automating Cyber Threat Intelligence (CTI) within the organization and the outside world. As the central repository for CTI, Soltra-Edge aggregates data from internal and external sources and normalizes it in STIX format.

Soltra, the parent company of Soltra-Edge facilitates a joint venture between the Financial Services Information Sharing and Analysis Center (FS-ISAC), an organization focused on sharing critical cybersecurity threat information worldwide, and The Depository Trust & Clearing Corporation (DTCC), the premier post-trade market infrastructure for the global finance service industry. Soltra-Edge disrupts the cybersecurity status quo by putting safeguards in place to better protect financial organizations of all sizes from cyber-attacks while it leverages deep cyber security expertise from the financial services sector.

Soltra-Edge is a game changer for the security posture of the global financial services sector by leveraging open standards, including Structured Threat Information eXpression (STIX), a uniform format for the threat information, and Trust Automated eXchange of Indicator Information (TAXII), an open standard protocol for routing that threat information.

Soltra-Edge provides some unique features such as:

a) This application shares intelligence with ISAC, ISAO industry associations trusted pools, DHS and so on.
b) Using Soltra-Edge, this filter and control the information that is sent to other application and devices in the organization's cybersecurity stack thus avoiding unnecessary tasks.
c) This has a feature to serve as a router of threat intelligence to the security applications and devices such as SIEMS or firewall.
d) It can easily connect to the leading and trending market players such as Cisco, Intel Security, ThreatQuotient, CarbonBlack, Phantom, Splunk and others.
e) It facilitates two-way sharing with the DHS AIS feed and receipt of the FedGov feed.
f) Has quick setup and configuration procedures for ease operation and migration.
g) Performs robust search and tagging for easy organization and access to the secure cyber threat data.

Benefits of Soltra-Edge includes but not limited to:

- Reduces manual labor required to collect, collate, process and disseminate intelligence data within various environments thus resulting in more efficient/ significant cost saving.
- This enables for private sharing of threat data within the trusted pool and organizations.
- It mainly supports all eight STIX core standard constructs.
- Manages CTI sharing with TLP markings and additional privacy and security controls.
- This has a specialty of operating as both server and a client.
- Provides the facility to run on virtual machines and/or on a physical server.
- Run's on premier NC4 secure data center.
- Provides two factor authentications for additional security.

4. MISP:

MISP stands for ‘Malware Information Sharing Platform’ wherein this enables for information sharing of threat intelligence including the cybersecurity indicators.

This is a threat intelligence platform for sharing, storing and correlating indicators of compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information and even an efficient counter-terrorism information. This embeds a feature to use the IoC’s and information to detect and prevent attacks or threats against ICT infrastructure or organizations.

MISP comprises of some unique features that includes:

a) Has a feature of an efficient IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

b) Provides automatic correlation finding relationships between attributes and indicators from malware, attacks and analysis.

c) This provides a platform for flexible data model where complex objects can be expressed and linked together to express threat intelligence and incidents.

d) Has a built-in sharing functionality for ease data sharing using different model of distributions.

e) MISP can automatically synchronize events and attributes among different MISP platforms. This enables for creation of trusted sharing groups and an attribute distribution level mechanism.

f) MISP embeds an intuitive user-interface for end-users to create, update and collaborate on events and indicators. This graphical interface enables the user to navigate seamlessly between events and their correlations.

g) This stores data in a structured format with an extensive support for cybersecurity indicators along with fraud alerts with respect to financial business domain.

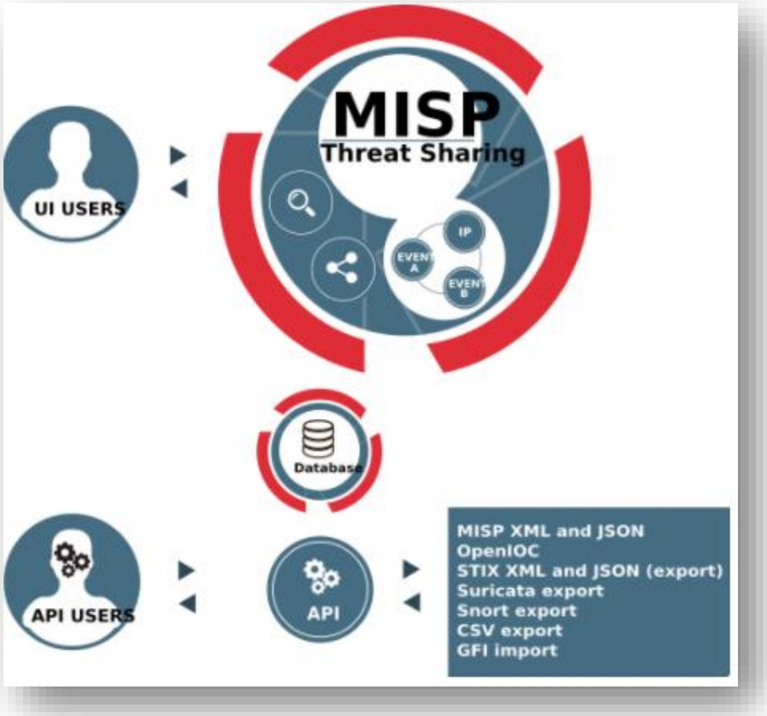
h) MISP generates IDS formats such as Snort-Bro, OpenIoC, CSV, MISP XML, JSON for exporting output which can then be efficiently used to integrate with other systems.

i) As a part of compatibility, MISP enables users to import threat intelligence data in bulk, batch, free-text format, OpenIoC’s, Sandbox, ThreatConnect CSV and other secure formats.

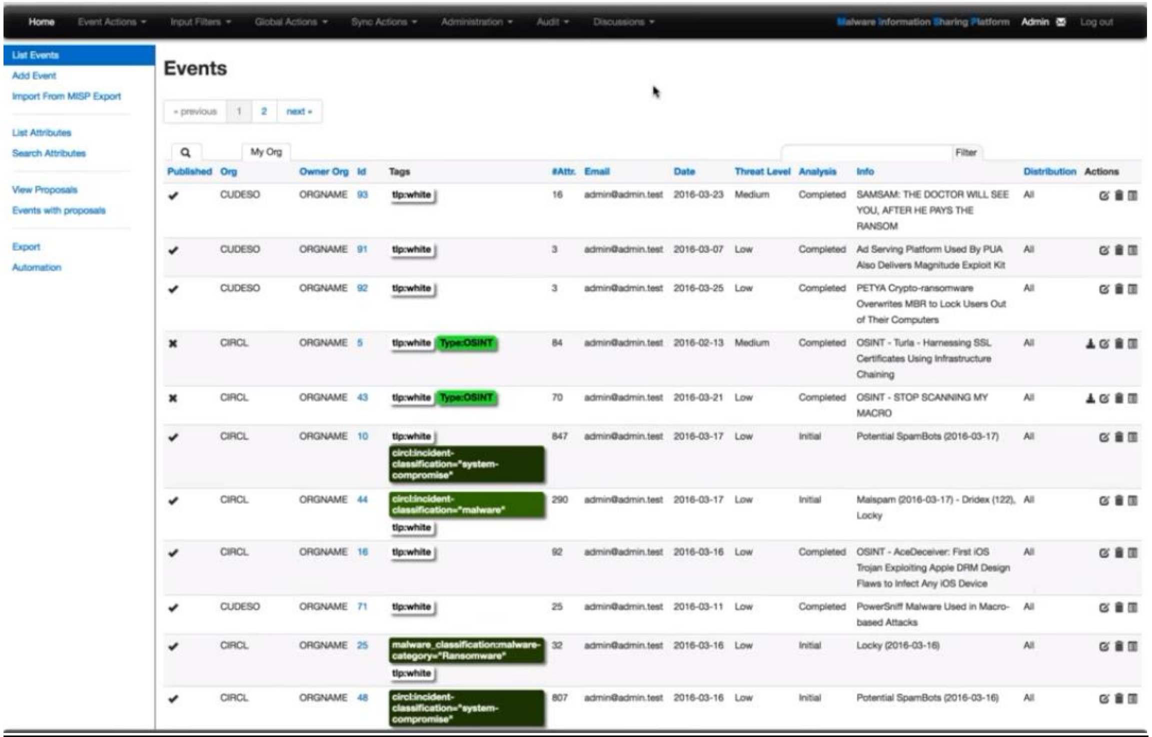
j) Provides flexible free text import tool to ease the integration of any unstructured reports into MISP

k) Allows simple pseudocode mechanism to delegate publication of threat indicators to other organizations.

l) Provides flexible Python API (PyMISP) to integrate MISP with organizations to handle malware samples and attributes.



***SnapShot 4(a)**: Displays the MISP basic architecture*



Events

Published	Org	Owner Org	Id	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	CUDESO	ORGNAME	93	tlp:white	16	admin@admin.test	2016-03-23	Medium	Completed	SAMSAM: THE DOCTOR WILL SEE YOU, AFTER HE PAYS THE RANSOM	All	
✓	CUDESO	ORGNAME	91	tlp:white	3	admin@admin.test	2016-03-07	Low	Completed	Ad Serving Platform Used By PUA Also Delivers Magnitude Exploit Kit	All	
✓	CUDESO	ORGNAME	92	tlp:white	3	admin@admin.test	2016-03-25	Low	Completed	PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers	All	
✗	CIRCL	ORGNAME	5	tlp:white Type:OSINT	84	admin@admin.test	2016-02-13	Medium	Completed	OSINT - Turla - Harnessing SSL Certificates Using Infrastructure Chaining	All	
✗	CIRCL	ORGNAME	43	tlp:white Type:OSINT	70	admin@admin.test	2016-03-21	Low	Completed	OSINT - STOP SCANNING MY MACRO	All	
✓	CIRCL	ORGNAME	10	tlp:white circl:incident-classification="system-compromise"	847	admin@admin.test	2016-03-17	Low	Initial	Potential SpamBots (2016-03-17)	All	
✓	CIRCL	ORGNAME	44	circl:incident-classification="malware" tlp:white	290	admin@admin.test	2016-03-17	Low	Initial	Malspam (2016-03-17) - Dridex (122), Locky	All	
✓	CIRCL	ORGNAME	16	tlp:white	92	admin@admin.test	2016-03-16	Low	Completed	OSINT - AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device	All	
✓	CUDESO	ORGNAME	71	tlp:white	25	admin@admin.test	2016-03-11	Low	Completed	PowerSniff Malware Used in Macro-based Attacks	All	
✓	CIRCL	ORGNAME	25	malware_classification:malware-category="Ransomware" tlp:white	32	admin@admin.test	2016-03-16	Low	Initial	Locky (2016-03-16)	All	
✓	CIRCL	ORGNAME	48	circl:incident-classification="system-compromise"	807	admin@admin.test	2016-03-16	Low	Initial	Potential SpamBots (2016-03-16)	All	

***SnapShot 4(b)**: Shows the Graphical User-Interface of MISP Application*

5. ThreatQuoitent:

ThreatQ provides an extra bench-power while arming the SOC analysts with a platform that manages and enriches their threat intelligence. With the implementation of ThreatQ, SOC engineers can analyze, organize and utilize their threat intelligence more efficiently and effectively.

ThreatQuoitent embeds some of the main features such as:

a) Self-Tuning Threat Library:

ThreatQ platform equips the cybersecurity professionals with a more efficient threat library that automatically scores and prioritizes threat intelligence based on the parameters. This utilizes both external and internal truth source thus aggregating all the context for better noise removal which in-turn reduces risk of false positives.

Whenever new data or context enters the system, the library will automatically tune and reprioritize threats.

b) Customer-Defined Prioritization:

This feature enables to automatically score and prioritizes threat intelligence based on the customer predefined parameters with organization's cyber regulations.

c) Automate Next Advanced Steps:

When this feature is being enabled, this automatically blocks threats in all of the company's security products. From network to product endpoint, this integrate with SEIMs and incident response systems and automate threat operation processes.

d) StreamLined Teamwork:

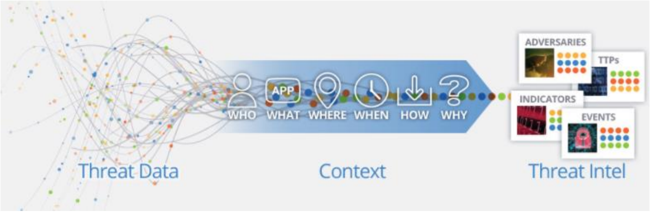
Embeds centralized intelligence sharing, analysis and secure investigation.

e) Open and Transparent:

Includes understandable context, relevance and priority of all ingested threat data.

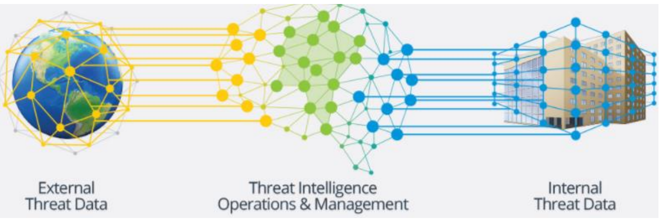
ThreatQ works based on 3 main principles naming:

- Context is Key – Correlates Internal and External Data



- Prioritize threat intelligence for specific environment.

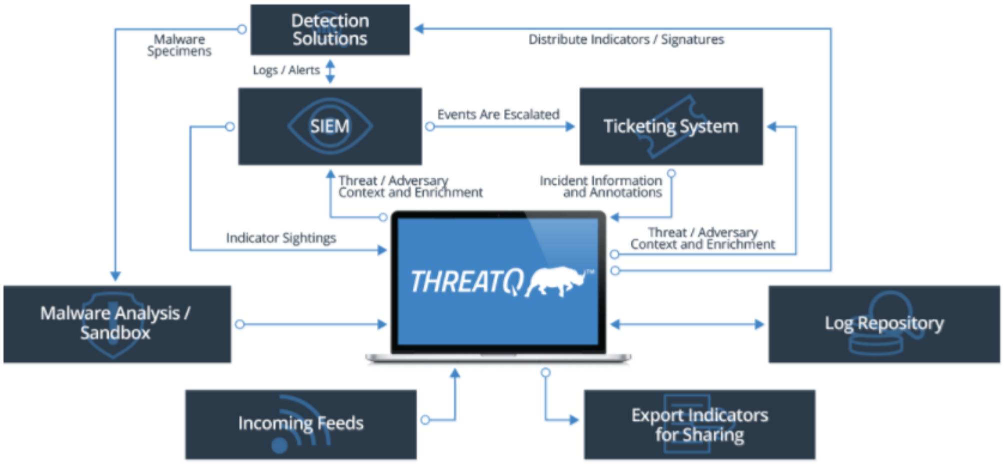
- Accelerate Detection and response



ThreatQuotient obeys a rule “Understanding and Analyzing the Past is as important as living in future”. Based on this principle, ThreatQ embeds a unique feature of Threat Intelligence Statistics wherein this includes: Data Preparation, Data Classification, Data Validation, Data Correlation and Data Scoring. Based on the Statistics scores, security professionals must quick and accurate in decision making thus drastically reduces the false positives and noisy datasets hence threat intelligence teams should consider statistics tool to improve their findings.

Some of the notable benefits of ThreatQ includes:

- ✓ Single source of truth for threat intelligence.
- ✓ Automatic copy/transfer of threat data from emails/other formats.
- ✓ No more multi-window third-party indicator research.
- ✓ Automatic threat data lookup and further analysis.
- ✓ Automatic detection and handle of false positives and threat noises.
- ✓ Quick and ease understandability of contexts about any threats.



***SnapShot 5**: Exhibits the underlying ThreatQ working principle*

6. Threat-Exchange:

ThreatExchange platform aids the participating organizations to share the threat data mutually using a convenient, structured and easy-to-use API that proves to provide privacy controls to enable sharing with only desired groups. ThreatExchange characterizes previous means of communication between professionals as “inconsistent” and “difficult” resigned to emails or spreadsheets.

ThreatExchange acts as a strong-secure framework that stored cyberthreat information for analysis by security pros.

FaceBook’s ThreatExchange API serves as a centralized repository to which members can contribute information with the entire network of participating members thus implementing the rating system that will let members of ThreatExchange can provide feedback on the incoming threat data. Based on the rating response, members can decide whether the information is useful or outdated. But as a contrary, some of the organizations feel that the cyberthreat data is highly sensitive and confidential and they are reluctant to revel their security breach data.

Best practices to be followed while implementing ThreatExchange includes:

- Tag the data.

  By tagging the data, it makes easy for others to find any particular indicator.
- Be descriptive with the tags.

  Provide as much information as possible to create more clear view about the threat.
- Consider the Privacy Rules.

  Threat tags are visible based on the Privacy-Type (Pubic/Private) of the tagged data.
- Paging the Response Data.

  Enables the functionalities of Graph API.
- Use Batch Requests for improved throughput.

  This allows to make multiple requests for Graph API using single HTTP call.
- Include Nested fields and Objects in the Result Data.

  Nested fields/indicator objects helps to pull all of its descriptors without any additional API calls.

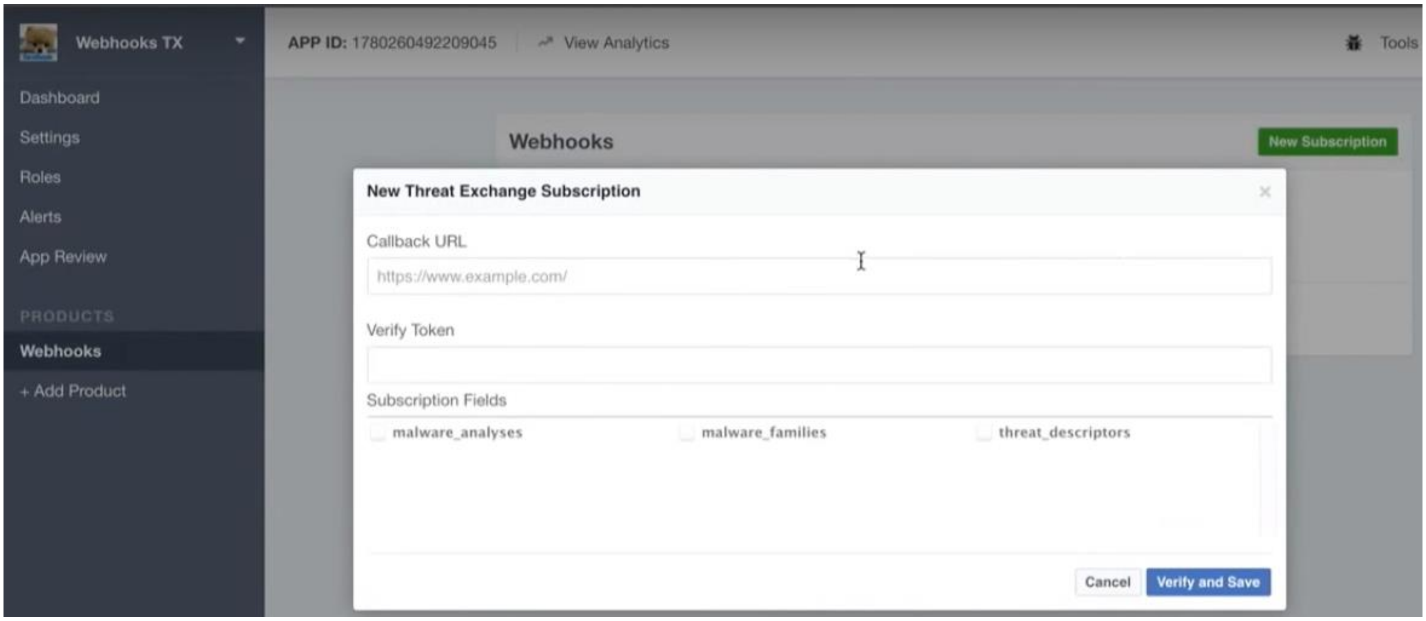
ThreatExchange is a subset of API endpoints within the larger ecosystem of Facebook’s Graph.

This tool embeds a webhook, wherein this allows the members to receive real-time push notification for indicators, descriptors, tags, analyzers and other malware families.

Benefits of ThreatExchange API's:

- ✓ Field Validation.
- ✓ Persistence to Facebook's Graphs.
- ✓ Type Checking.
- ✓ Everyone can use what you share and be protected.

ThreatExchange API's allows to create connections/bridges between ThreatIndicator objects to express relationship for ease understandability and identification.



New Threat Exchange Subscription

Callback URL

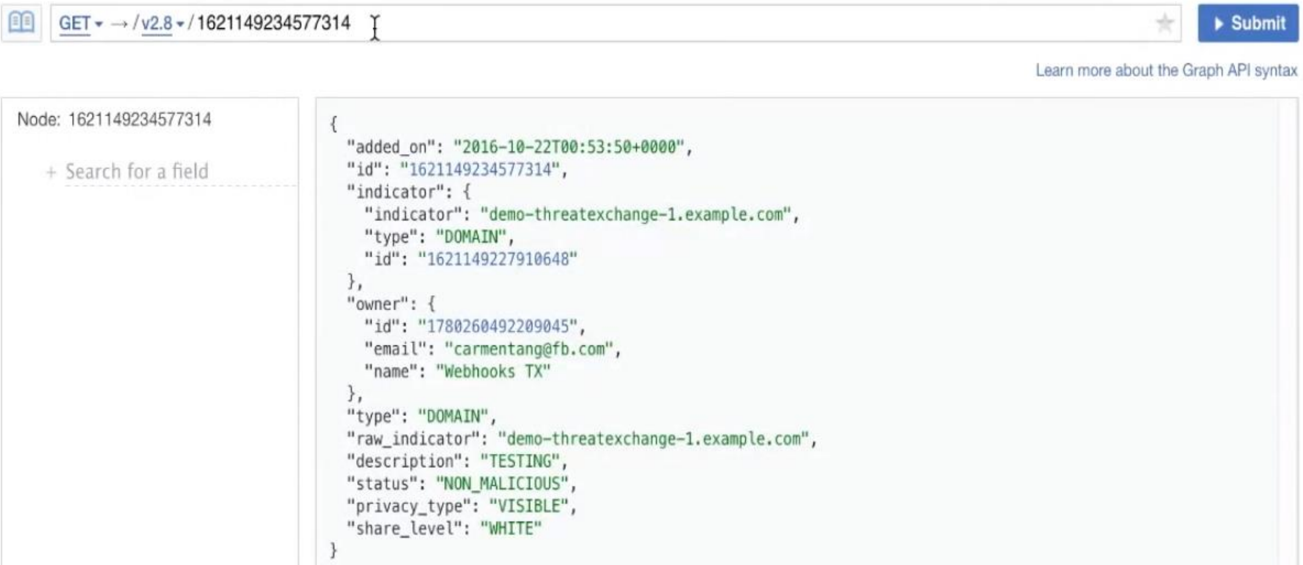
https://www.example.com/

Verify Token

Subscription Fields

□ malware_analyses □ malware_families □ threat_descriptors

SnapShot 6(a): *Shows the working of WebHook API for subscribing to receive push notifications*



GET → /v2.8 / 1621149234577314

Node: 1621149234577314

```
{
  "added_on": "2016-10-22T00:53:50+0000",
  "id": "1621149234577314",
  "indicator": {
    "indicator": "demo-threatexchange-1.example.com",
    "type": "DOMAIN",
    "id": "1621149227910648"
  },
  "owner": {
    "id": "1780260492209045",
    "email": "carmentang@fb.com",
    "name": "Webhooks TX"
  },
  "type": "DOMAIN",
  "raw_indicator": "demo-threatexchange-1.example.com",
  "description": "TESTING",
  "status": "NON_MALICIOUS",
  "privacy_type": "VISIBLE",
  "share_level": "WHITE"
}
```

SnapShot 6(b): *Exhibits the code snippet for posting the threat data onto the ThreatExchange Platform.*

7. Maltego:

Maltego is an interactive, visual data mining and link analysis tool used to conduct online investigation through plugin libraries called ‘transforms’.

Maltego allows security professionals to retrieve information on the target of interest such as infrastructure or companies using an efficient and powerful graph visualizations. There are around 26 Maltego Transform API’s.

Maltego can be used to analyze:

- Whois information
- Historical DNS Records
- Associated Malware File Hashes
- Detected suspicious
- Malicious URL’s
- SSL Certificate information

Maltego tools enables to investigate relationships between pieces of information from various sources located on the internet thus using the ideology of transforms to automate the process of querying from different data sources. After in-depth analyses, the information is then displayed on a node-based graph suited for performing link analysis.

Types of Maltego tools:

a) Maltego Classic:

Maltego Classic is the professional cersion of Maltego and provides extended functionality and capabilities when compared with other community versions. This tool must be used in a commercial environment thus includes a range of different formats that your graphs can be exported.

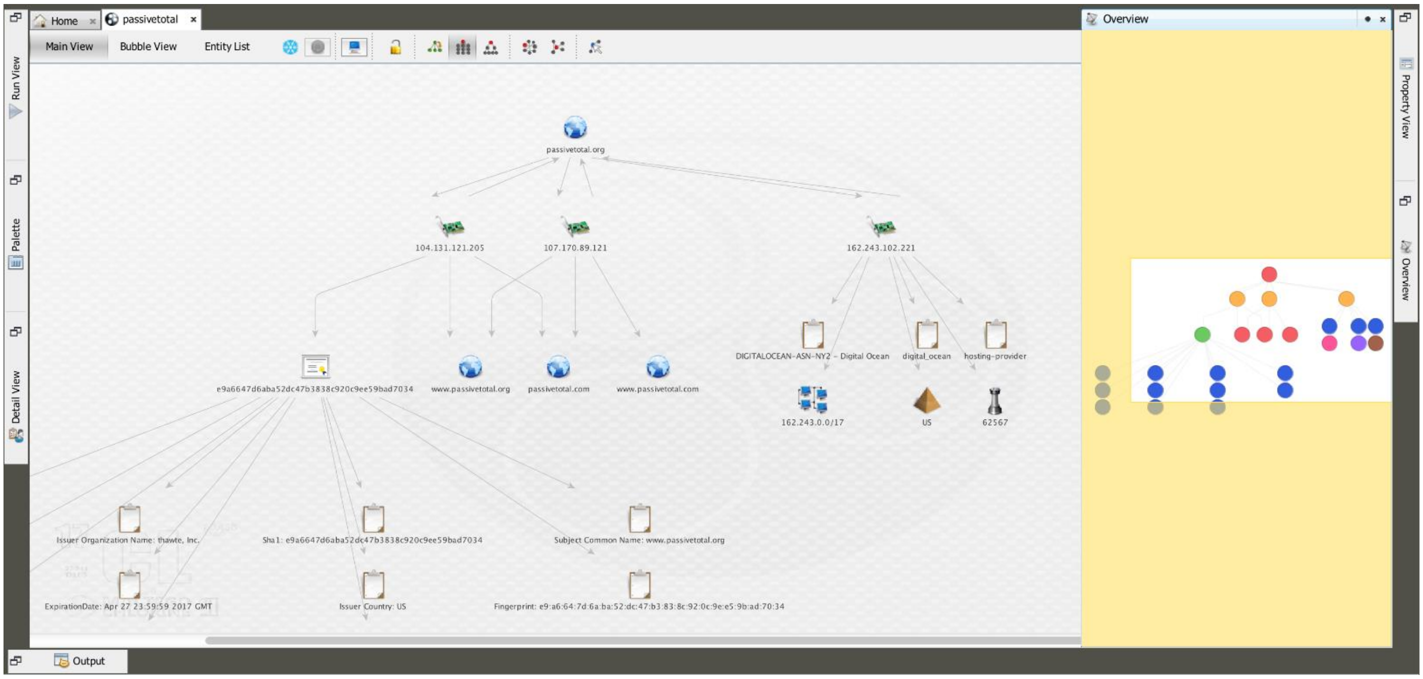
Maltego offers the user unprecedented information.

b) Maltego CE:

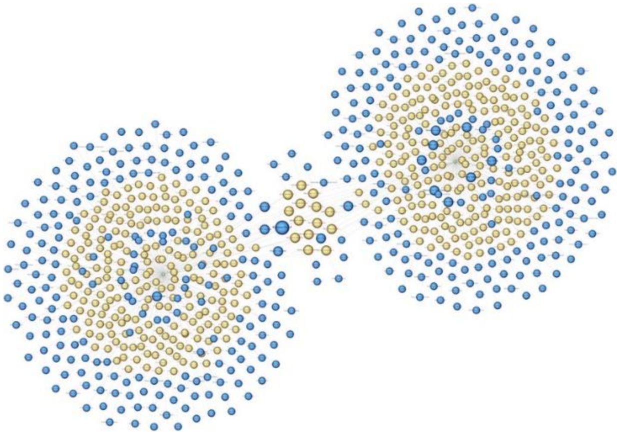
This is used by security professionals worldwide. It belongs to the community version of Maltego. The main limitation with the community version is that the application cannot be used for commercial purpose and there is a restriction on the maximum number of entities that can returned from a single transform.

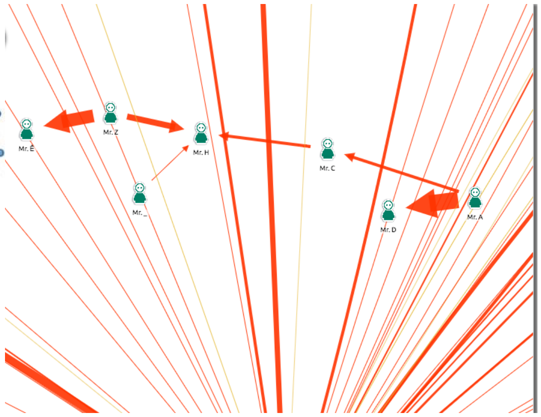
c) Maltgo XL:

Maltego XL is an eXtra Large, premier edition of the three Maltego clients since this includes the capabilities and features of Maltego Classic but with enhanced capability of executing instructions on the extremely large complex graphs. Maltego XL allows the threat predictors to map out clear threat picture of the entire company's network thus making it easy to identify its weak points and drawbacks.


Home
passivetotal
Main View
Bubble View
Entity List
Run View
Palette
Detail View
Overview
Property View
Output
passivetotal.org
104.131.121.205
107.170.89.121
162.243.102.221
e9a6647d6aba52dc47b3838c920c9ee59bad7034
www.passivetotal.org
passivetotal.com
www.passivetotal.com
DIGITALOCEAN-ASN-NY2 - Digital Ocean
digital_ocean
hosting-provider
162.243.0.0/17
US
62567
Issuer Organization Name: thawte, Inc.
Sha1: e9a6647d6aba52dc47b3838c920c9ee59bad7034
Subject Common Name: www.passivetotal.org
ExpirationDate: Apr 27 23:59:59 2017 GMT
Issuer Country: US
Fingerprint: e9:a6:64:7d:6a:ba:52:dc:47:b3:83:8c:92:0c:9e:e5:9b:ad:70:34

SnapShot 7(a): *Shows the graphical user interface of Maltego application.*





SnapShot 7(b): *Graphical analysis of Social Networks*

Snapshot 7(c): *Visualization of Bitcoin network*

8. Splunk:

Splunk delivers real-time answers and business values from machine data so the respective company can make better decisions.

Different variations of Splunk:

a) Splunk Enterprise: In-organization solution to aggregate, analyze and get solutions from company’s own machines. Enables to ask any questions to company’s data.

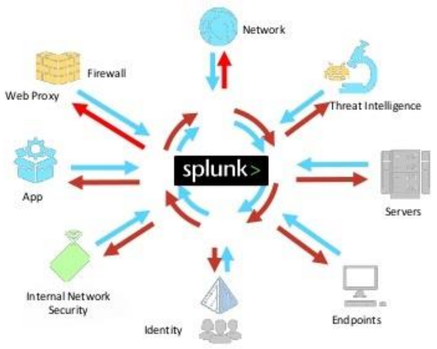
b) Splunk Cloud: Enables scalability and service thus without needing the infrastructure and its relevant components thus provisioning end-to-end visibility.

c) Splunk Light: Comprehensive solution for small IT environments thus automating log search and analysis.

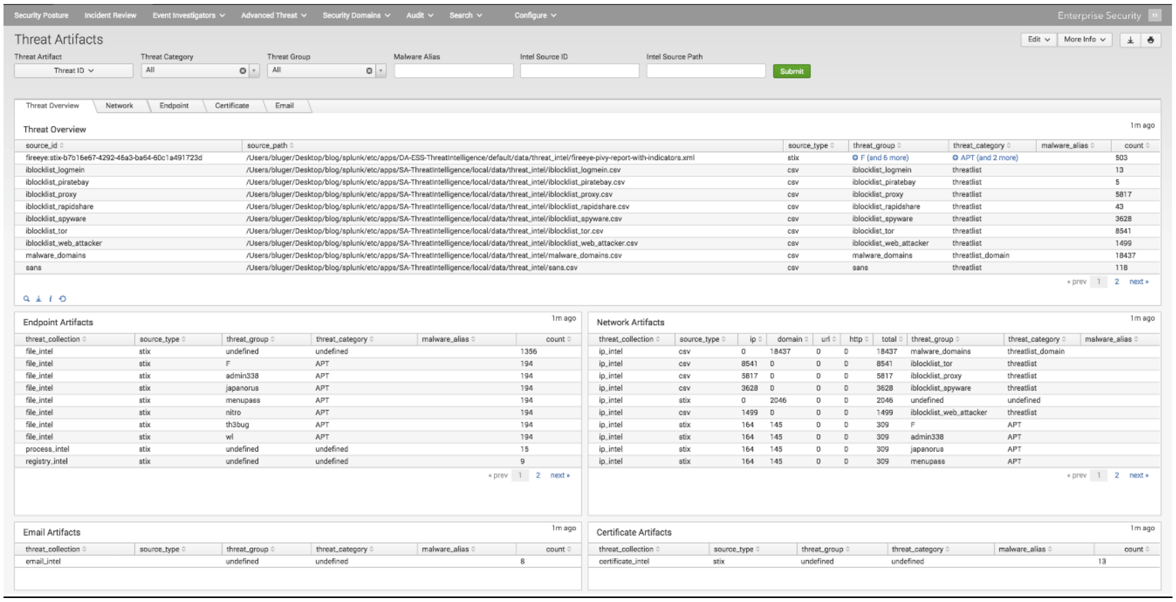
Some of the unique services of Splunk includes: User Behavior Analytics, Enterprise Security, IT service intelligence and many more.

Advantages of Splunk includes:

- ✓ Inheritance of BigData implementation.
- ✓ Efficient and unsupervised Machine Learning feature.
- ✓ Custom threat generation.
- ✓ Anomaly suppression & scoring.
- ✓ Detection of compromised Endpoint.
- ✓ Operationalize threat intelligence.
- ✓ Aggregates everything in the business context.
- ✓ Deploys within hours.



***SnapShot 8(a)**: Displays the security overview of Splunk*



Threat Artifacts

Threat Artifact	Threat Category	Threat Group	Malware Alias	Intel Source ID	Intel Source Path
Threat ID	All	All			

Threat Overview

source_id	source_path	source_type	threat_group	threat_category	malware_alias	count
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/Users/bluger/Desktop/blog/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F (and 6 more)	APT (and 2 more)		503
iblocklist_logmein	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	csv	iblocklist_logmein	threatlist		13
iblocklist_piratebay	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_piratebay.csv	csv	iblocklist_piratebay	threatlist		5
iblocklist_proxy	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.csv	csv	iblocklist_proxy	threatlist		5817
iblocklist_rapidshare	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_rapidshare.csv	csv	iblocklist_rapidshare	threatlist		43
iblocklist_spyware	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.csv	csv	iblocklist_spyware	threatlist		3628
iblocklist_tor	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_tor.csv	csv	iblocklist_tor	threatlist		8541
iblocklist_web_attacker	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_web_attacker.csv	csv	iblocklist_web_attacker	threatlist		1499
malware_domains	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/malware_domains.csv	csv	malware_domains	threatlist_domain		18437
sans	/Users/bluger/Desktop/blog/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/sans.csv	csv	sans	threatlist		118

Endpoint Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
file_intel	stix	undefined	undefined		1356
file_intel	stix	F	APT		194
file_intel	stix	admin338	APT		194
file_intel	stix	japanorus	APT		194
file_intel	stix	menupass	APT		194
file_intel	stix	nitro	APT		194
file_intel	stix	th3bug	APT		194
file_intel	stix	wl	APT		194
process_intel	stix	undefined	undefined		15
registry_intel	stix	undefined	undefined		9

Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category	malware_alias
ip_intel	csv	0	18437	0	0	18437	malware_domains	threatlist_domain	
ip_intel	csv	8541	0	0	0	8541	iblocklist_tor	threatlist	
ip_intel	csv	5817	0	0	0	5817	iblocklist_proxy	threatlist	
ip_intel	csv	3628	0	0	0	3628	iblocklist_spyware	threatlist	
ip_intel	stix	0	2046	0	0	2046	undefined	undefined	
ip_intel	csv	1499	0	0	0	1499	iblocklist_web_attacker	threatlist	
ip_intel	stix	164	145	0	0	309	F	APT	
ip_intel	stix	164	145	0	0	309	admin338	APT	
ip_intel	stix	164	145	0	0	309	japanorus	APT	
ip_intel	stix	164	145	0	0	309	menupass	APT	

Email Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
email_intel		undefined	undefined		8

Certificate Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
certificate_intel	stix	undefined	undefined		13

SnapShot 8(b): Shows the user-interface with captured security threat artifacts within the organization.

Drawbacks of Splunk includes:

- ✓ Overall cost to implement the solution is quite high and its also expensive to maintain the product/service license.
- ✓ Splunk doesn’t offer an appliance version of the solution. Organizations needs to work with trusted partners to implement the integration on supported hardware.
- ✓ Splunk UBA is visible on shortlists of splunk users seeking to add UEBA features hence users must validate the degree of integration of the solution and trusted vendors for continuous integration.

Conclusion:

Enterprises are striving hard to keep up with the current threat landscape with too many manual processes while struggling with the lack of resources-budget. As a key point to notice, organizations risk investing large amounts of time and money on threat intel with little positive effect on security. Its clear that the effective threat intelligence focuses on the questions that an organization wants to get answered rather than simply attempting to collect, process and act on huge amount of data. In order to get actionable threat intelligence, it has to be captured from variety of trusted sources, analyze, classify and publish in real-time as a consumable product.

Finally, threat intelligence needs to be simpler to integrate in a manner that best suites the organization and its client’s environment, with an ability to expand inputs as needed to meet the needs of the organization.

Bibliography:

1. https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/
2. http://resources.infosecinstitute.com/open-source-threat-intelligence-tools-techniques/#gref
3. https://www.cio.com/article/2973027/security/8-new-threat-intelligence-products-to-make-you-bulletproof.html#slide1
4. https://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375
5. https://www.threatconnect.com/blog/7-threat-intelligence-tools-your-cybersecurity-team-needs/
6. https://www.threatconnect.com/
7. https://www.recordedfuture.com/threat-intelligence-definition/
8. https://www.crunchbase.com/organization/threatconnect-inc-#section-overview
9. https://www.threatconnect.com/press-releases/threatconnect-provides-enhanced-intelligence-global-context-threatassess-cal/
10. https://www.itcentralstation.com/products/comparisons/threatconnect_vs_threatstream
11. https://www.anomali.com/
12. https://anomali.cdn.rackfoundry.net/files/ThreatStream-Datasheet.pdf
13. https://www.scmagazine.com/anomali-threatstream/review/9329/
14. https://www.cloudera.com/solutions/gallery/anomali-threatstream.html
15. https://www.esecurityplanet.com/products/anomali-threatstream.html
16. https://www.circl.lu/services/misp-training-materials/
17. http://www.misp-project.org/features.html
18. https://www.threatq.com/
19. https://developers.facebook.com/tools-and-support/
20. https://developers.facebook.com/docs/threat-exchange/v2.12
21. https://mashable.com/2015/02/11/threatexchange-facebook/#sgchI6srlZqE
22. http://fortune.com/2016/07/19/facebook-threatexchange-ratings/
23. https://groupsense.io/blog/how-to-use-maltego-to-conduct-threat-research/
24. https://www.crowdstrike.com/blog/operational-threat-intelligence-with-maltego-transform-hub/
25. https://www.paterva.com/web7/services/training.php
26. https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php
27. https://www.blackhat.com/us-16/training/threat-intelligence-using-maltego.html
28. https://www.threatconnect.com/blog/threatconnect-maltego-integration/
29. https://www.anomali.com/blog/threatstream-optic-maltego-integration
30. https://go.recordedfuture.com/maltego-integration-webinar
31. https://www.lookingglasscyber.com/blog/virustotal-maltego-visualizing-actionable-malware-iocs/
32. www.splunk.com
33. https://www.gartner.com/document/3834578?ref=solrAll&refval=200037320&qid=937f7d6aed8e846bda
34. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf
35. https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf
36. https://cryptome.org/2015/09/cti-guide.pdf