Tools and Standards for Cyber Threat Intelligence Projects

Making effective use of cyber threat intelligence is an important component of an organization's security program. Cyber threat intelligence can be obtained internally and from external sources. It must be collected, analyzed, shared and leveraged. This paper considers the context of the 'Develop Project Charter' and 'Scope Definition' processes from the Project Management body of Knowledge (PMBOK). This context is used in performing Product Analysis on leading tools and standards for cyber thr...

Tools and Standards for Cyber Threat Intelligence Projects

GIAC (GCPM) Gold Certification

Author: Greg Farnham
Advisor: Kees Leune

Accepted: October 14th 2013

Abstract

Making effective use of cyber threat intelligence is an important component of an organization's security program. Cyber threat intelligence can be obtained internally and from external sources. It must be collected, analyzed, shared and leveraged. This paper considers the context of the 'Develop Project Charter' and 'Scope Definition' processes from the Project Management body of Knowledge (PMBOK). This context is used in performing Product Analysis on leading tools and standards for cyber threat intelligence systems. Some of the tools and standards considered are the Open Indicators of Compromise (OpenIOC) framework, Vocabulary for Event Recording and Incident Sharing (VERIS), Cyber Observable eXpression (CybOX), Incident Object Description and Exchange Format (IODEF), Trusted Automated eXchange of Indicator Information (TAXII), Structured threat Information Expression (STIX), Traffic Light Protocol (TLP), Open Threat Exchange (OTX) and Collective Intelligence Framework (CIF).

1. Introduction

Effective use of cyber threat intelligence (CTI) is an important tool for defending against malicious actors on the Internet. According to KPMG, "…our experience indicates that many organizations now need to focus on putting in place the fundamentals of intelligence management to gain real value from threat intelligence" (KPMG, 2013). Malicious actors continually use new resources and develop new methods for attacking Internet users. With the rapidly changing nature of the threat, CTI must be acted on quickly to receive its full value. In many cases the value of intelligence can go to zero in days or even hours. At a 2010 conference, Gordon Snow from the FBI Cyber Division put it this way, "Cyber information is unlike any other kind of information. It's perishable. If I don't get it to you in a reasonable period of time, it's useless to you." (Pendergast, 2010). In the last few years increased effort has been placed on managing CTI and sharing it within trusted communities. To enable this level of management and sharing, many standards and tools have been developed. Standards for storing and exchanging CTI data as well as tagging the sharing level can be leveraged for a CTI project. Managing and distributing CTI data can be complex resulting in a complex project to implement the solution. When implementing a complex project it is beneficial to use accepted standards and processes. The Project Management Body of Knowledge (PMBOK) (PMI, 2004) provides standard processes and deliverables for project management that will be applied to a fictitious CTI project. Information regarding CTI tools and standards are provided as well as how PMBOK is leveraged in the fictitious project. To keep the content focused, a few selected components of the PMBOK that are most relevant to CTI tools and standards are used as the context for the CTI project.

2. Project Management

The PMBOK is a comprehensive set of processes and deliverables that can be used to manage projects of all sizes. It can be used to manage large projects that may involve thousands of people and last for dozens of years. The PMBOK is broken down

in to five process groups: Initiating, Planning, Executing, 'Monitoring and Controlling' and Closing. There are also ten knowledge areas that span the different process groups.

A CTI project for a fictitious company, 'ACME Bird Traps' is used a backdrop to analyze cyber threat intelligence standards and tools. The ACME project is following project management processes from the PMBOK. Three selected processes from the PMBOK for a CTI project are considered. These processes are most relevant to evaluating CTI standards and tools. The first process considered is the 'Develop Project Charter' process from the 'Initiating Process Group' process group. The second process considered is the 'Develop Preliminary Project Scope Statement' also from the 'Initiating Process Group'. The third process considered is the 'Scope Definition' process from the 'Planning Process Group'. These processes result in the related outputs of interest, namely the Project Charter, Preliminary Scope Statement and Project Scope Statement (Greene, 2007).

2.1. Project Charter

Projects start with the 'Initiating Process Group' of processes. The first process is 'Develop Project Charter'. The output of this process is the Project Charter. The Project Charter is a very high level description of the objectives of the project. It is the first deliverable used for documenting and managing the project. It also provides a mechanism for the sponsor to authorize the project.

The Project Charter may be the most critical deliverable in the whole project. It is the seed that all other deliverables grow from. Although it may only be a page in length it is important to get it right. Any shortcomings in the Project Charter will be magnified in follow on deliverables. Finding a problem with the Project Charter late in a project means a lot of work was wasted and must be re-done. To ensure a high quality Project Charter, seek additional reviews from other Project Managers or Staff not involved in the project.

Some of the key elements of the Project Charter are the Project Description, Project Requirements, Project Manager, Milestones, Assumptions and the Business Case. They are shown below for the ACME CTI project.

Project Description:

The Cyber Threat Intelligence Management (CTIM) Project will provide ACME a system for collecting, managing, leveraging and sharing cyber threat intelligence. The CTIM system will provide the ability to import threat feeds from public and community sources. It will have the ability to leverage the cyber threat intelligence in existing detective and preventive controls.

Project Requirements:

The successful completion of the CTIM Project will result in the following:

- A system for collecting, managing, leveraging and sharing cyber threat intelligence.

- Automated integration to receive cyber threat intelligence from public and community sources.

- Automated integration to leverage cyber threat intelligence in existing detective and preventive controls.

Assigned Project Manager and Authority Level:

Scott Moore has been assigned as the Project Manager.

Internal project management number 409522002 has been assigned for accounting of project related expenses.

Summary Milestone Schedule:

January 1, 2014 Project Kickoff

December 1, 2014 Production Release

External Assumptions and Constraints:

It is assumed that external cyber threat intelligence source will have an Application Program Interface (API) for accessing the data programmatically.

Business Case:

ACME is subjected to a high level of threat when using the Internet. In order to quickly react to the ever changing threats on the Internet, ACME must leverage cyber threat intelligence. By deploying a Cyber Threat Intelligence Management system, ACME will be able to more quickly prevent or detect Internet based threats.

Once a Project Charter is completed, the next step is to use it as input to the 'Develop Preliminary Project Scope' process.

Greg Farnham

2.2. Preliminary Project Scope

The 'Develop Preliminary Project Scope' process is also part of the 'Initiating Process Group' of processes. The Project Charter and other inputs are used to create the Preliminary Scope Statement. This statement identifies elements of scope for the project. This continues the progressive elaboration that is fundamental part of the PMBOK. With progressive elaboration more details are added as the project progresses. This process is analogous to carving a statue from ice. First an outline is defined from a block of ice using very coarse cuts from a chain saw. Then a large chisel is used to define major features such as arms and legs. Finally, a small chisel is used to define the detail. Consider the level of detail when defining the Preliminary Scope Statement. It needs more detail than the Project Charter, but will not have as much detail as the resulting Project Scope Statement. Do not spend energy defining requirement details in this process. Only define enough detail required for the next step in the process which is Scope Definition. Review each requirement and ask the question, 'Is this too detailed?'

Key Elements of the Preliminary Scope Statement include the project objectives, requirements, acceptance criteria, boundaries, deliverables, constraints, organization, risks, milestones and cost. They are shown below for the ACME CTIM project.

Project and product objectives:

Completion of the project by December 15, 2014. The CTIM system will result in 20% fewer incidents that require investigation.

Product or service requirements and characteristics:

R1 - Capability to Import/Export indicator details to/from other systems in a standard format.
R2 - Capability to Import/Export structured incident data to/from other systems in a standard format.
R3 - Capability to Query, Import, Export and Manage CTI data through a user interface.
R4 - Capability to enforce data sharing based on an attribute attached to CTI data.
R5 - Capability to automate the import and export of CTI data.
R6 - Capability to provide authentication and confidentiality when sharing data.
R7 - Capability to export data that can be used in detective and preventive controls.
R8 - Capability to select data for export based on creation dates of CTI data.
R9 - Capability to measure the efficacy of CTI feeds.

Product acceptance criteria:

The project test team successfully completes all of the User Acceptance Tests.

Project boundaries:

The project only manages cyber threat intelligence data. Other security data such as vulnerability scanning data and security event data is out of scope.

Project deliverables:

- Cyber Threat Intelligence Management System
- Policies created and approved to manage and operate the CTIM system
- Documentation on the system design and use.
- Training materials for administrators and end users.
- Procedures to be followed by administrators and end users.

Project constraints and assumptions:

Any required servers will use a corporate standard operating system and configuration.

Initial project organization:

Project Manager, Business Analyst, Developer

Initial defined risks:

Public cyber threat intelligence feeds offer no service level agreement and could be shut down at any time.

Schedule milestones:

January 1, 2014 Project Kickoff

February 1, 2014 Project Staffing complete

April 1, 2014 Completed Acquisition of all hardware and software

October 1, 2014 Beta Test

December 1, 2014 Production Release

Order of magnitude cost estimate:

Hardware and Software, $250,000
External Consulting, $40,000
Internal Man Hours, 4,000

The Preliminary Scope Statement will be used as an input to the Scope Definition process which is part of the 'Planning Process Group' in the PMBOK. In this process, additional detail will be added to the scope. The Scope Definition process is discussed next.

2.3. Scope Definition

The Scope Definition is executed as part of the 'Planning Process Group'. This process is used to define the scope of the project. It is part of the 'Project Scope Management' knowledge area. Defining the scope is critical to being able to manage it and managing the scope is critical to project success. The Scope Definition has multiple inputs. Two of the inputs were previously discussed. They are the Project charter and the Preliminary Scope Statement. The main output will be the Project Scope Statement.

Scope changes are inevitable, but they can be reduced by starting with a well defined scope. To avoid high cost changes late in a project, personally discuss the project scope with all stake holders. Scope changes happen on every project. In fact 'Project Scope Management', one of the knowledge areas of the PMBOK all about managing changes to the scope.

Scope changes get more expensive as a project progresses. While actual values are very dependent on project size and type, Boehm (Boehm, 1981) found that for large software projects, the cost to fix an issue late in a project could be 100 times the cost of fixing it early. Consider an extreme example of a change to a car design late in the project. If the car has been designed and the factory built, consider the impact of a change to the wheel base. It would require changing the suspension, the body, the interior and the assembly line to build it. If the same change happened in the concept phase it would be inexpensive since components had not yet been designed let alone building the factory to make them.

There is a notable tool within the Scope Definition process. It is Product Analysis. Product Analysis involves analyzing products that will be used as part of the project deliverables and how they affect the scope of the work for the project. This tool is used to review and analyze available cyber threat intelligence tools and standards. The use of this tool begins with a discussion of cyber threat intelligence (CTI).

3. Cyber Threat Intelligence

Cyber threat intelligence (CTI) is threat intelligence related to computers, networks and information technology. It is instructive to consider definitions for classic intelligence. Intelligence as defined by Edward Waltz is, "the information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding, is the product that provides battlespace awareness" (Waltz, 1998). Another definition is provided by Robert Clark, "Writers therefore describe intelligence as being actionable information" (Clark, 2010). There are two key takeaways from these definitions that also apply to CTI. First, intelligence is not just information or data it is information that has been analyzed. Second, intelligence must be actionable. If it is not actionable, there is no benefit to having it. Additionally, cyber threat intelligence can be strategic or tactical. Strategic intelligence includes things like motivation of adversaries. Tactical intelligence includes things like 'tactics, tehniques and procedures (TTP)' and 'indicators of compromise (IOCs)'. IOCs are one of the most easily actionable types of CTI and are often the focus standards and tools. Some of the most commonly used IOCs are IP addresses, domain names, uniform resource locators (URLs) and file hashes. With a clear definition of CTI the drivers for CTI management are considered next.

3.1. Cyber Threat Intelligence Management Drivers

The threats against an organization's assets are the main drivers for managing cyber threat intelligence. Use of the Internet is required to do business for most companies and the threats come with the territory. There continues to be an ever changing threat landscape that organizations must defend against. Adversaries are very creative in coming up with new attacks to defeat yesterday's and today's defenses. The ability to manage CTI and share with others in an automated fashion is needed to respond

to these attacks. CTI standards and tools are required to accomplish this automation. One of the first steps in managing CTI is the collection of cyber threat intelligence through available sources.

3.2. Cyber Threat Intelligence Sources

CTI sources can be split in to three categories internal, community and external.

3.2.1. Internal

The internal threat category encompasses any CTI that is collected from within the organization. This can included reported information from security tools such as firewalls, intrusion prevention systems (IPS) and host security systems like anti-virus. A valuable source of threat intelligence information comes from computer forensic analysis. The analysis can yield intelligence that is not readily visible and may be very useful in detection of other attacks. Analysis can yield intelligence to identify tools or TTP which are harder for attackers to change compared to things like IP addresses and domain names.

3.2.2. Community

The community category includes any CTI shared via a trusted relationship with multiple members with a shared interest. This can be an informal group with member organizations that are in the same industry sector or that have other common interests. There are formal community groups such as the Information Sharing and Analysis Centers (ISACs) organized under the National Council of ISACs (NCI, 2013). ISACs are formed for specific sectors such as higher education or financial services. There are over a dozen ISACs under the National Council of ISACs. One example of a community sharing group is Research and Education Networking (REN) ISAC. REN-ISAC is a trusted community for research and higher education. They are the main organization behind the Collective Intelligence Framework covered in section 3.4.7. Another example of a community group is the Defense Industrial Base Collaborative Information Sharing Environment (DCSIE). This group provides a hub for CTI sharing between U.S. government defense contractors.

3.2.3. External

The external category includes CTI from sources outside an organization and not part of a community group. There are two types of external sources. The first is public sources. Public sources are available to anyone and generally there is no cost associated with access. While public feeds can be available at no cost, there can be problems. Amoroso points out possible problems with volunteered data, "…efforts to collect volunteered data will always have an issue with guaranteed data quality" (Amoroso, 2011). An example of a public CTI feeds is MalwareDomains (MalwareDomains, 2013). MalwareDomains provides a list of domains known to be involved in malicious activity. The list available in multiple formats and can be used to block access to the malicious domains.

The other type of an external CTI source is private. Private sources are typically only available on a paid basis. An organization can subscribe to a threat feed from a vendor to receive regularly updated CTI. These feeds have the advantage in that there may be a service level agreement on data quality. Many security products include some type of cyber threat intelligence update mechanism. CTI services can also be purchased separately. One example is the Emerging Threats ETPro Ruleset (EmergingThreats, 2013). Emerging threats offers subscription services for IDS rules and IP reputation.

3.3. Cyber Threat Intelligence Requirements

CTI requirements can vary based on the organization and the objectives of their projects. For the ACME CTI management project, the requirements are defined in section 2.2. Requirements have been labeled R1 through R9. The following standards and tools are evaluated against these requirements.

3.4. Threat Intelligence Standards and Tools

There are a number of different CTI standards and tools. Many of the available ones are analyzed for their applicability to the ACME CTI management project.

3.4.1. Traffic Light Protocol (TLP)

The Traffic Light Protocol (TLP) is a very straight forward and simple protocol. It comes from the United States Computer Emergency History (US-CERT, 2013). TLP

is used to control what can be done with shared information. Shared information is tagged with one of four colors white, green, amber or red. The color designates what can be done with the shared information. Information tagged white can be distributed without restriction. Information tagged green can be shared within the sector or community, but not publicly. Information tagged amber may only be shared with members of their own organization. Information tagged red may not be shared. Given its simplicity TLP can be used verbally, with email or incorporated in to an overall system.

The ability to tag and control sharing of information is requirement R4 for the ACME project. TLP supports requirement R4, but does not address any other requirements.

3.4.2. Managed Incident Lightweight Exchange

The Managed Incident Lightweight Exchange (MILE) Working Group is working on standards for exchanging incident data. The group works on the data format to define indicators and incidents. It also works on standards for exchanging data. This group has defined a package of standards for CTI which includes Incident Object Description and Exchange Format (IODEF), IODEF for Structured Cyber Security Information (IODEF-SCI) and Real-time Inter-network Defense (RID).

3.4.2.1. Incident Object Description and Exchange Format

Incident Object Description and Exchange Format (IODEF) is a standard defined by Request For Comments (RFC) 5070 (Danyliw, 2007). Incident Object Description Exchange Format (IODEF) was proposed in December of 2007 after discussions began with RFC3067 in Feb 2001. IODEF is an XML based standard used to share incident information by Computer Security Incident Response Teams (CSIRTs).

The IODEF Data Model includes over 30 classes and sub classes used to define incident data. The classes cover a wide range of information including Contact, Monetary Impact, Time, Operating System and Application. It includes data handling labels such as sensitivity and confidence. Examples of IODEF are included in section 7 of the RFC (Danyliw, 2007).

IODEF is used in a number of projects and vendor products. A successful implementation of IODEF is used by the Anti-Phishing Working Group. They have extended the IODEF standard to support the reporting of phishing and other email incidents. It is used as a storage format in the Collective Intelligence Framework (CIF). IODEF is also used in products from DFLabs, Arcsite and Foundstone (Moriarty, 2013).

3.4.2.2. IODEF for Structured Cyber Security Information

'IODEF for Structured Cyber security Information" (IODEF-SCI) is an extension to the IODEF standard that adds support for additional data. It is a standard proposed by the MILE working group (Takahashi, 2013). The additional information includes: attack pattern, platform information, vulnerability, weakness, countermeasure instruction, computer event log, and severity. IODEF-SCI supports the additional data by embedding existing standards within the IODEF document. The following standards are proposed to be included in IODEF-SCI: Common Attack Pattern Enumeration and Classification (CAPEC), Common Event Expression (CEE), Common Platform Enumeration (CPE), Common Vulnerability and Exposures (CVE), Common Vulnerability Reporting Format (CVRF), Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), Common Weakness Scoring System (CWSS), Open Checklist Interactive Language (OCIL), Open Vulnerability and Assessment Language (OVAL), Extensible Configuration Checklist Description Format (XCCDF), Distributed Audit Service (XDAS) and ISO/IEC 19770. An example of IODEF-SCI is included in section 5 of the draft (Takahashi, 2013).

3.4.2.3. Real time Inter-network Defense (RID)

Real time Inter-network Defense (RID) is a standard for communicating CTI. RID is defined in RFC 6545 (Moriarty, 2012) and the transport of RID messages over HTTP/TLS is defined in RFC 6546 (Trammell, 2012). RFC 6545 states, "Real-time Inter-network Defense outlines a proactive inter-network communication method to facilitate sharing incident handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution." The RID schema is built off of the off of the IODEF model and also adds a Boolean data type. RID functions via five message types: Request, Acknowledgement,

Result, Report and Query. The RID standard includes a Policy Class which would allow different policies to be applied based on the relationship with the sharing parties. Some of the relationships considered are ClientToSP (Service Provider), SPToClient, IntraConsortium, PeerToPeer and BetweenConsortiums. This flexibility would allow for direct organization to organization sharing via the PeerToPeer relationship or within a community using the IntraConsortium relationship.

3.4.2.1. Managed Lightweight Incident Exchange Summary

The MILE working group has defined a package of standards using IODEF, IODEF-SCI (draft) and RID for CTI sharing. The IODEF standard supports the R1 requirement for using a standard data format. The IODEF-SCI supports the R2 requirement. The RID standard provides for secure sharing mechanisms with multiple policies which supports requirements R5 and R6.

3.4.3. Open Indicators of Compromise (OpenIOC) framework

OpenIOC was introduced by Mandiant in 2011 (OpenIOC, 2011). It is used in Mandiant products, but has also been released as an open standard. OpenIOC is primarily for tactical CTI. OpenIOC provides definitions for specific technical details including over 500 indicator terms. New terms are easily added because the terms are separate for the main schema. Most of the terms are host centric with titles beginning with file, driver, disk, system, process or registry. A couple of simple examples are 'File Name' and 'File MD5 Hash'. IOC definitions are stored as an XML schema.

Multiple IOCs can be combined using Boolean logic to define a specific malware sample or family. The combined logic can be used to look for items that should not be there as well as verifying expected items. For example, if a service runs a dynamic link library (DLL) file that is normally signed, finding a DLL file but not finding a valid signature could be an IOC. Examples are available for known malware.

An example of the Nettraveler malware originally reported by Kaspersky is available on the Mandiant Blog (Gibb, 2013) as an IOC formatted XML file. Examples of FileName, File Hash, IP Address and portable executable (PE) exports are included.

OpenIOC is primarily used in Mandiant products, but some other sources are making use of it. The web site ioc.forensicarftifacts.com (Churchill, 2012) provides a community resource to submit and share OpenIOC files. McAfee has released OpenIOC files for operation Troy (Walter, 2013). They also list several McAfee products that can consume OpenIOC files. An example of an open source project for OpenIOC files is also available. The project is pyioc, "pyioc is a set of tools to handle IOC files" (Bryner, 2013).

OpenIOC's comprehensive set of terms and standard file format allows it to meet several of the requirements for the ACME CTI management project. OpenIOC provides the richest set of terms for defining indicators. With over 500 terms it can be used to define IOCs in great detail. These features allow it to support requirements R1 and R2. The draft version 1.1 adds the ability to include user defined parameters with an IOC (Wilson, 2013). This would allow tagging for different levels of sharing which would meet requirement R4. Other requirements would have to be met by other standards or tools.

3.4.4. Vocabulary for Event Recording and Incident Sharing (VERIS)

The VERIS framework was released by Verizon in March of 2010. As the name implies VERIS provides a standard way for defining and sharing incident information. Verizon releases an annual 'Data Breach Investigation Report' (DBIR) that leverages VERIS. With the VERIS framework, other organizations can contribute data in a standard format and vocabulary. These data can then be incorporated and used as a larger data set for analysis and reporting. As stated on the community page, "VERIS is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. The overall goal is to lay a foundation on which we can constructively and cooperatively learn from our experiences to better manage risk." (VERIS, 2010).

The VERIS schema is divided in to five sections: Incident tracking, Victim demographics, Incident description, 'Discovery & response' and Impact assessment. Each of the sections has multiple elements with specific data types and variables names. Some of the elements included are 'Incident summary', 'Confidence rating', 'Primary

industry' and 'hacking variety'. Some of these elements contain enumerated lists. For example 'hacking variety' is made up of an enumerated list of 46 hacking varieties. The varieties include things like 'brute force', buffer overflow', 'cache poisoning' etc. VERIS does have a limited ability to include Indicators of Compromise (IOC). This is done via a simple IOC element that stores an indicator and a comment about it. VERIS is intended for strategic and risk based information as opposed to tactical information.

A community database for VERIS data is available from Verizon. The database contains over 1,200 incidents from the department of health and human services (HHS) as well as other public incidents (Widup, 2013). The database is publicly available in JSON format. VERIS example files can be downloaded from the community site (VERIS 2010). There is also a Tableau based interactive graph site available to view the data.

VERIS is in use by Verizon as part of the methodology for generating the DBIR (Verizon, 2013). For the 2013 report there were a total of 19 organizations supplying incident details. These organizations collected data using one of three methods: VERIS directly, re-entered in a VERIS application or converted data from another schema.

VERIS is capable of storing data in a format that can be automatically shared which supports requirement R2. It is designed for strategic information and an aggregate view of incidents. It does not fit as well for sharing tactical data.

3.4.5. Mitre Standards CybOX, STIX, TAXII

Mitre has developed three standards that each fill different needs for a CTI management system. The first is Cyber Observable eXpression (CybOX) which provides a standard for defining indicator details known as observables (Mitre, 2013c). The second is Structured threat Information Expression (STIX) which provides a standard to define patterns of observables in context (Mitre, 2013a). The third is Trusted Automated eXchange of Indicator Information (TAXII) which provides a standard to exchange CTI (Mitre, 2013b). These standards are treated as a package since they were designed to work together. The first one discussed is CybOX.

3.4.5.1. Cyber Observable eXpression (CybOX)

CybOX is used for defining details regarding measurable events and stateful properties. The objects that can be defined in CybOX can be used in higher level schemas like STIX. CybOX was first discussed in 2009 with the first schema draft being released in 2010.

The goal of CybOX is to enable the ability to automate sharing of security information such as CTI. It does this by providing over 70 defined objects that can be used to define measurable events or stateful properties. Examples of objects are File, HTTP Session, Mutex, Network Connection, Network Flow and X509 Certificate. An example using the Network Connection object is available on the CybOX project site (Wunder, 2013a).

There are resources available for working with CybOX. First, there are Python bindings. These are Python libraries that providing a mapping to Python data types. Second there are Helper Application Programmer Interfaces (APIs). The Helper APIs provide a higher level of abstraction and can be used for parsing, creating and editing CybOX objects. CybOX is used in STIX which is covered next.

3.4.5.2. Structured threat Information Expression (STIX)

Mitre has developed several complimentary standards related to CTI. Structured Threat Information Expression (STIX) is for defining threat information including threat details as well as the context of the threat. The first draft for STIX was released in 2012. The 1.0 version was released in April, 2013 with the 1.1 version currently in the planning state.

STIX is designed to support four cyber threat use cases: analyzing cyber threats, specifying indicator patterns, managing response activities and sharing threat information (Mitre, 2013a). It uses XML to define threat related constructs such as campaign, exploit target, incident, indicator, threat actor and TTP. In addition, extensions have been defined with other standards such as TLP, OpenIOC, Snort and YARA. The structured nature of the STIX architecture allows it to define relationship between constructs. For example the TTP used can be related to a specific threat actor.

An example of a malicious domain watch list using the indictor construct is available on the STIX project site (Wunder, 2013b).

Although under heavy development, a python library for parsing and generating STIX files is available. STIX is being accepted by industry leaders. According to a Microsoft blog posting, "STIX and TAXII are starting to see broad adoption" (Bryant, 2013) . In a blog post, Charles Smutz comments on the momentum of the Mitre package of standards, "Momentum is snowballing for adoption of specific standards for intel sharing, the foremost of which is the Mitre suite of STIX/TAXII/MAEC." MAEC is Malware Attribute Enumeration and Characterization and is outside the scope of this paper.

3.4.5.3. Trusted Automated eXchange of Indicator Information

Mitre has developed several complimentary standards related to CTI. Trusted Automated eXchange of Indicator Information (TAXII) supports sharing of CTI data. The Mitre definition for TAXII states, "Defines a set of services and message exchanges for exchanging cyber threat information" (Mitre, 2013b). The first draft of the TAXII specification was proposed in 2012.

TAXII was designed to be flexible. It supports multiple sharing models including variations of 'hub and spoke' as well as 'peer to peer'. These models allow for push or pull transfer of CTI data. The models are supported by four core services: discovery, feed management, inbox and poll.

The four services each provide pieces of the overall functionality. The Feed Management Service has the following request types: subscribe, unsubscribe, pause delivery, resume delivery, modify subscription, status query. The Inbox is a listener to receive content from feeds. The Poll service is a service hosted by data producers that data consumers can request data based on a timestamp range. It is used when a customer pulls data from a producer. Lastly, Discovery Service is for identifying existing services and how they work. A given sharing model will make use of one or more of the core services.

TAXII uses XML and HTTP for message content and transport. It also allows for custom formats and protocols. TAXII includes standard mechanisms for confidentiality, integrity and attribution

TAXII has a few high profile groups using it. TAXII has been adopted as a planned standard by Microsoft as part of its 'Microsoft Active Protections Program' (MAPP) (Bryant, 2013). It will be used to share CTI data with MAPP members. TAXII is also in use by Financial Services Information Sharing Analysis Center (FS-ISAC) (Connolly, 2013). FS-ISAC members can leverage STIX and TAXII to access CTI. APIs are available for Discover and Pull for the current FS-ISAC deployment (FSISAC, 2013).

3.4.5.4. Mitre Standards Summary

Taken as a package, the Mitre standards cover many of the requirements for the ACME CTI project. The CybOX and STIX standards support the data formatting requirements such as R1 and R2. The TAXII standard supports R5 for automated sharing and R6 for confidentiality and authentication.

3.4.6. Open Threat Exchange

Open Threat Exchange (OTX) is a publicly available service created by Alien Vault for sharing threat data. The first public announcement for OTX was February of 2012. According to the press release, "AV-OTX cleanses aggregates, validates and publishes threat data streaming in from the broadest range of security devices across a community of more than 18,000 OSSIM and AlienVault deployments." (Nellums, 2012). OTX is a centralized system for collecting CTI. It is provided by AlienVault and interoperates with their Open Source SIEM (OSSIM) system, where SIEM is Security Event and Information Management. OSSIM is free to use. OSSIM users can configure their system to upload their threat data to OTX. Collected data is validated by AlienVault. The CTI is then delivered to all OSSIM users that subscribe to OTX. OTX Threat Intelligence is also available in the Collective Intelligence Framework (CIF) system.

The AlienVault web site hosts publicly available feeds with reputation data (AlienVault, 2013). Example records are shown below.

```
64.202.163.216 # Malware Domain US,Scottsdale,33.6119003296,-111.890602112
50.22.225.203 # Scanning Host US,Dallas,32.929901123,-96.8352966309
189.4.93.167 # Scanning Host „,32.929901123,-96.8352966309
217.107.219.76 # Malware IP RU„,60.0,100.0
198.56.193.26 # Scanning Host US„,38.0,-97.0
174.122.148.162 # C&C US,Houston,29.7523002625,-95.3669967651
75.127.114.52 # C&C;Malware IP US,Atlanta,33.7257003784,-84.4309005737
```

OTX is used by any OSSIM users that have enabled it as well as any CIF users accessing the system. As of February 22, 2012 there are more than 18,000 OSSIM deployments (Nellums, 2012).

OTX can successfully provide data to the public, but lacks the ability to restrict access for community use. OTX does provide an automated mechanism for sharing CTI data, thus it supports requirement R5. The focus of OTX is to provide data to the public. As such, there does not appear to be any way to control who can access submitted data. OTX does provide a valuable service, but its functionality is limited to publicly sharing data.

3.4.7. Collective Intelligence Framework (CIF).

The Collective Intelligence Framework (CIF) is client/server system for sharing threat intelligence data. CIF was developed out of the Research and Education Network Information Sharing and Analysis Center (REN-ISAC) (CIF Project, 2009a). Available documentation first appeared in 2009. CIF includes a server component which collects and stores CTI data. Data can be IP addresses, ASN numbers, email addresses, domain names and uniform resource locators (URLs) and other attributes. These data can be accessed via various client programs. The standard client is a Perl command line utility. A browser plugin is also available. CIF data also includes information on the type of threat, severity of an attack and the confidence of the data. CIF provides the ability to control access through the use of an API-Key and the ability to place restriction levels on the data. Internally, CIF stores data using the IODEF format. CIF is also capable of exporting CTI for specific security tools. CIF can output data as Snort rules or iptables rules as well as other formats.

An example query using the command line client for malicious uniform resource locators (URLs) with a medium severity is shown below (CIF Project, 2009b). The output has been truncated.

```
$ cif -q url/malware -s medium
restriction |severity|address
need-to-know|medium  |http://derts3563d.net/old_files/root/bin/config.bin
need-to-know|medium  |http://yyyaanve.ru/b.bin
```

CIF is in use by REN-ISAC members and at least one large Managed Security Service Provider (MSSP).

CIF has a robust set of features. It supports all the required data types. Its script based command line client can be easily leveraged for automating use of the data. CIF stores data in a defined standard format (IODEF). It also has features for labeling data and access control. CIF meets supports R1, R3, R4, R5, R6, R7 and R8.

4. Conclusions

Several conclusions can be drawn from the content of this paper. The conclusions can be offered from different viewpoints.

From a project management viewpoint, the PMBOK is a useful tool for managing CTI projects. A CTI project can be complex and having an accepted standard for project management will improve the odds for success.

From a security community viewpoint, CTI management is a recognized problem and there is a lot of activity to solve it. There is a large number of standards defined or under development for CTI. There is some overlap between some of the standards, but many of them have a specific focus. In addition to the standards there are groups actively sharing CTI and tools being developed to support CTI sharing.

From an ACME viewpoint, there are a large number of tools and standards to choose from. The best standard or tool is driven by the specific objectives of a CTI project and which groups with which you will be sharing CTI data. In many cases, the best solution may include more than one of the standards or tools available. For the requirements considered all could be supported by at least one tool or standard except R9,

"Capability to measure the efficacy of CTI feeds." This is an advanced requirement would require custom development for a solution. Some of the requirements such as R3, R7 and R8 could only be met by a tool and not a standard. These requirements were only met by the one tool considered, CIF.

Many of the standards fit will for organizations with specific needs. If an organization wants to share incident data and be part of the analysis of a broad data set, then VERIS would be the best choice. If an organization wants to share indicator details in a completely public system, then OTX would be a reasonably choice. If an organization is using tools that support OpenIOC, then of course OpenIOC would be the best choice. If an organization is looking for a package of industry standards then the MILE package (IODEF, IODEF-SCI, RID) or the Mitre package (CybOX, STIX, TAXII) would be suitable. Both have the capability to represent a broad array of data and support sharing of that data.

For the ACME CTIM project several requirements were defined. Based on these requirements the MILE package or the Mitre package both offer standards that would support many requirements. Both packages meet the same set of requirements: R1, R2, R5 and R6. In addition to standards, the only system considered in the product analysis is the Collective Intelligence Framework (CIF). CIF would support the most number of requirements of all standards and tools considered.

Requirements Supported

	R1	R2	R3	R4	R5	R6	R7	R8	R9
TLP				X					
IODEF/IODEF-SCI/RID	X	X			X	X			
OpenIOC	X	X							
VERIS		X							
CybOX/STIX/TAXII	X	X			X	X			
OTX					X				
CIF	X		X	X	X	X	X	X	

Table 1.

Based on the high level view of the requirements CIF is a solution that should be considered for the project. If an organization has similar requirements and is looking for an open source existing system, CIF would be worth a look.

Greg Farnham

5. References

AlienVault. (2013). *Reputation data*. Retrieved from https://reputation.alienvault.com/reputation.data

Amoroso, E. (2011). Cyber attacks: protection national infrastructure. Burlington, MA: Elsevier.

Boehm, B. (1981). Software engineering economics. Upper Saddle River, New Jersey: Prentice Hall PTR.

Bryant, J. (2013, July). New mapp initiatives. Retrieved from http://blogs.technet.com/b/bluehat/archive/2013/07/29/new-mapp-initiatives.aspx

Bryner, J. (2013, February). Python tools for ioc (indicator of compromise) handling. Retrieved from https://github.com/jeffbryner/pyioc

Churchill, M. (2012). About forensicartifacts.com. Retrieved from http://ioc.forensicartifacts.com/about/

CIF Project. (2009a). collective-intelligence-framework. Retrieved from https://code.google.com/p/collective-intelligence-framework/

CIF Project. (2009b). collective-intelligence-framework. Retrieved from https://code.google.com/p/collective-intelligence-framework/wiki/ClientExamples

Clark, R. (2010). Intelligence analysis: A target-centric approach. (Third ed.). Washington, DC: CQ Press.

Connolly, J. (2013, July). The trusted automated exchange of indicator information (taxii). Retrieved from http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_July_2013.pdf

Danyliw, R. (2007, December). The incident object description exchange format. Retrieved from http://www.ietf.org/rfc/rfc5070.txt

EmergingThreats. (2013). *Enhance your intrusion detection system with etpro™ ruleset*. Retrieved from http://www.emergingthreats.net/solutions/etpro-ruleset/

FSISAC. (2013, June). Cyber intelligence repository. Retrieved from https://www.fsisac.com/sites/default/files/Cyber Intelligence Repository One-Sheet Handout 10Jun2013.pdf

Gibb, W. (2013, June 18). Nettraveler in openioc format. Retrieved from https://www.mandiant.com/blog/nettraveler-openioc/

Greene, J. (2007). Head first pmp. (First ed.). Sebastopol, CA, USA: O'Reilly.

KPMG. (2013, May). Cyber threat intelligence and the lessons from law enforcement. Retrieved from www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-threat-intelligence-final3.pdf

MalwareDomains. (2013). *Dns-bh – malware domain blocklist*. Retrieved from http://www.malwaredomains.com/

Mitre. (2013a, May). Use cases (STIX). Retrieved from http://stix.mitre.org/language/usecases.html

Mitre. (2013b, July). Taxii: An overview. Retrieved from http://taxii.mitre.org/about/documents/TAXII_Overview_briefing_July_2013.pdf

Mitre. (2013c, September). cyber observable expression. Retrieved from http://cybox.mitre.org/

Moriarty, K. (2012, April). Real-time inter-network defense (rid) rfc 6545. Retrieved from http://datatracker.ietf.org/doc/rfc6545/

Moriarty, K. (2013). Implementations on incident object description exchange format. Retrieved from http://siis.realmv6.org/implementations/

NCI. (2013). National council of isacs. Retrieved from http://www.isaccouncil.org/home.html

Nellums , K. (2012, February). Alienvault launches open threat exchange, largest community-sourced information security threat feed. Retrieved from http://www.alienvault.com/about/press-releases/alienvault-launches-open-threat-exchange-largest-community-sourced-informat

OpenIOC. (2011, October). An introduction to openioc. Retrieved from http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf

Pendergast, G. (2010, October). Review: Mandiant's incident response conference (mircon) day 2. Retrieved from http://computer-forensics.sans.org/blog/2010/10/15/review-mandiants-incident-response-conference-mircon-day-2

PMI. (2004). A guide to the project management body of knowledge: Pmbok guide. (3rd ed.). Newton Square, Pennsylvania: Project Management Institute, Inc.

Takahashi, T. (2013, July 4). Iodef-extension for structured cybersecurity information. Retrieved from http://tools.ietf.org/html/draft-ietf-mile-sci-08

Trammell, B. (2012, April). Transport of real-time inter-network defnse (rid) messages over http/tls rfc 6546. Retrieved from https://datatracker.ietf.org/doc/rfc6546/

US-CERT. (2013). Traffic light protocol (tlp) matrix and frequently asked questions. Retrieved from http://www.us-cert.gov/tlp

VERIS, Community. (2010, March). Veris overview. Retrieved from http://www.veriscommunity.net/doku.php?id=overview

Verizon, Risk Team. (2013, April). *2013 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdfhttp://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Walter, J. (2013, July). *Operation troy: Openioc release*. Retrieved from http://blogs.mcafee.com/executive-perspectives/operation-troy-openioc-release

Waltz, E. (1998). Information warfare principles and operations. Norwood, MA: Artech House, Inc.

Widup, S. (2013, July 25). The veris community database. Retrieved from http://www.verizonenterprise.com/security/blog/index.xml?postid=4642

Wilson, D. (2013, September). The history of openioc. Retrieved from https://www.mandiant.com/blog/history-openioc/

Wunder, J. (2013a, September). Cybox_network_connection_http_pattern.xml. Retrieved from https://github.com/CybOXProject/schemas/blob/master/samples/CybOX_Network_Connection_HTTP_Pattern.xml

Wunder, J. (2013b, October). Retrieved from https://github.com/STIXProject/schemas/blob/master/samples/STIX_Domain_Watchlist.xml

Last Updated: November 24th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS London November 2017	OnlineGB	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced