The Evolution and Effectiveness of Threat Intelligence

For Cloud Computing

By Finbarr Bastible

MSc in Cloud Computing

Cork Institute of Technology

Supervisor Dr. J. Creagh

This report is submitted in partial fulfilment of the requirements for the Degree of Master of Science in Cloud Computing at Cork Institute of Technology. It represents substantially the result of my own work except where explicitly indicated in the text. The report may not be copied or distributed without the permission of the author.

March 2015

The Evolution and Effectiveness of Threat Intelligence

For Cloud Computing

Finbarr Bastible

Abstract

This project will research the development of traditional signature based security technologies and the evolution of threat intelligence in cyber security and its effectiveness for cloud computing. The goal of this research is to define the core processes of an effective cyber threat intelligence framework, to conduct a risk assessment of cloud computing security domains and threats and to define core processes for an effective threat intelligence framework for cloud computing.

Acknowledgements

I would like to thank Dr. John Creagh for his guidance and supervision on the research assignment. I would also like to thank my family for their patience and generosity in providing me with time to conduct and write this research assignment.

Chapter 1 - Introduction

The motivation behind this research project is to provide a focus to the topic of threat intelligence as an emerging and developing technology within the information security and cloud computing environments. To this end the goal of this research project is to evaluate current threat intelligence frameworks and to establish their effectiveness for cloud computing,

To achieve this goal, background research is conducted into current cyber security risks and technologies which will provide a context for the scope of malware types, threats, vulnerabilities and risks that exist and the current technologies that are available to defend against them such as firewalls, intrusion detection and prevention systems (IPS/IDS) and system event management systems (SIEM). The depth and complexity of threats that exist and impact our digital and online lives are growing. Technologies, and their use, are evolving to drive paradigms that are specific to this decade such as “consumerization” of the enterprise and the Internet of Things. These developing trends within Web 2.0 and Enterprise 2.0 environments are researched to provide further context to the increasing scope for, and complexity of, cyber threats. The conclusion of the background research addresses the fundamentals of cloud computing in terms of its definition, characteristics and service and deployment models before exploring the key cyber security risks inherent in cloud computing.

Cyber Threat Intelligence (CTI) is evaluated and the relationship between data and intelligence as well as CTI characteristics, uses, limitations and successes are explored before the core processes of an effective CTI framework are presented.

Are current cyber threat intelligence frameworks effective for cloud computing? To establish this, the requirements of a cloud computing threat intelligence framework are developed focusing on the cloud specific challenges and risks that framework would have to meet. Current threat intelligence frameworks are analysed and evaluated against cloud threat intelligence requirements before a design for a threat intelligence framework for cloud computing (TIFCC) is presented. This design develops a set of core processes of an effective threat intelligence framework for cloud computing (TIFCC). The core question of this research is whether current threat intelligence frameworks are effective for cloud computing. To this end the core deliverables of this research project are:

- To establish the requirements of threat intelligence for cloud computing
- To analyse existing threat intelligence frameworks and their effectiveness for cloud computing
- Present a design for core processes of a threat intelligence framework for cloud computing

Chapter 2 - Background Research

Define Cloud Computing

Cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (1).

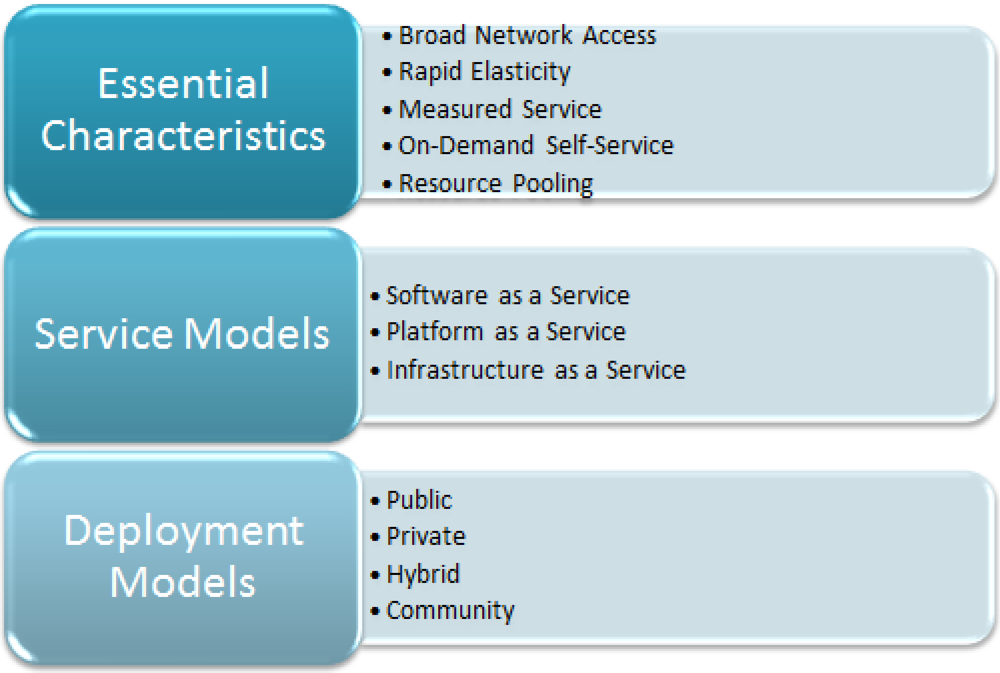


Figure 1: National Institute of Standards and Technology Cloud Computing Definition

This scale of this computing model is enabled by the core elements of virtualized networks and distributed storage.

Cloud computing characteristics are elaborated further as (1):

- Broad Network Access - access is via heterogeneous thick or thin clients
- Rapid Elasticity - the capability to scale rapidly outward and inward in line with demand
- On-Demand Self-Service - unilateral provisioning of computing (server time and storage)
- Resource Pooling - computing resources are pooled using a multi-tenancy model
- Measured Service – usage metering capability

Cloud computing service models (known as the SPI Model) are elaborated as (1):

- SaaS

  The consumer has the capability to use the cloud service provider's applications without the capability to manage or control the underlying cloud computing infrastructure
- PaaS

  The consumer does not have the capability to manage or control the underlying cloud computing infrastructure but deploys, and has control of, applications created using programming, libraries, services and tools supported by the provider
- IaaS

  The consumer does not manage or control the underlying cloud infrastructure but has control over storage, operating systems and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Finally there are 4 cloud computing deployment models which are (1):

- Public – the cloud infrastructure is provisioned for open use by the general public
- Private – the cloud infrastructure is provisioned for exclusive use by a single organization
- Community - the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns
- Hybrid - a composition of two or more of the public, private and community cloud infrastructures that remain unique entities that allow application and data portability

Cyber Security Risks and Technologies

The need for security is seemingly universal. Consumers need and want to be secure in every aspect of the interactions of their lives and enterprises need and want security in the interactions of their operations. Cloud computing is a model that supports the interactions between consumers and enterprises and enables the transaction of information between them. Information security is defined by the SANS Institute as "the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption"(2). Information security is underpinned by three core tenets (3) of:

- Confidentiality – ensuring data is accessed only by authorized users
- Integrity – that information is accurate and complete
- Availability – information is available to users when they need it

The computing systems that enable information flow need to have these fundamental attributes of confidentiality, integrity and availability. In conjunction, there are three independent security goals of (4):

- Prevention
- Detection
- Response

The following sections will address the cyber security risks that exist and the technologies in use to prevent detect and respond to information security threats and attacks.

Cyber Security Risks

Malware Types

The intent of a virus is to infect a host and, once activated, the virus will execute to deliver a payload which can be to connect a command and control server, delete files or cause random reboots. Viruses must replicate and they do this by infecting host applications. Malware types include the following:

- Worms, which reside in memory and self-replicate to infect a network consuming bandwidth and impacting network performance
- Trojans, which have the ability to infect the network once it is executed by a user. Backdoors provide access to a system, Trojans can install backdoors that enable authentication methods to be bypassed and enable remote access.
- Logic bombs are a type of malware that executes at a specific point in time or if a specific application launches. The key sources of risk are from within the organization

through insiders who have malicious intent. As it is an inside threat, the extent of the impact can be significant depending on the access or system privileges the user may have.

- A rootkit is a system level or root level program that resides in memory to hide the malicious code from host based intrusion systems (HIDS) and antivirus software. It poses a particular challenge to antivirus software as the information the operating system is passing to a user or diagnostic tool cannot be trusted (5)
- Botnets is a generic term for automated programs that execute tasks without user intervention and are the most significant threat plaguing the Internet today (5).

It is one thing knowing what these threats are after an attack has occurred but an organization needs to have the signatures and attributes of these malware types in order prevent them getting onto networks in the first place.

Advanced Persistent Threats

Advanced persistent threats (APT) pose the most significant threat to organizations and the biggest challenge to the security industry in terms of prevention, detection and response (6). An APT refers to a specific threat actor. The APT is characterized by (7):

- Having *advanced* computer intrusion capability to use exploits against well-known vulnerabilities or develop custom exploits depending on the target
- Being *persistent* as they are tasked with a formal mission and will maintain the interaction needed to execute their objectives
- The *threat* is organized, funded and motivated. The threat is not a mindless individual utilizing mindless code.

Types of advanced persistent threats include:

- Denial of Service (DoS) where the attack comes from a single source to make a computer unavailable to a user. For example a SYN Flood that affects the TCP handshake process or buffer overflow of a web server.

- Distributed Denial of Service (DDoS) where an attack will come from many sources to create unmanageable network traffic and memory and CPU usage. DDoS is the most common form of DoS in virtualized environments (8).
- Advanced persistent threats use other tactics and techniques that include botnets; spoofing, ARP poisoning, SQL Injection attacks and XML Injection attacks.

The persistent nature of APTs is driving a requirement for cyber security to be more proactive and to mitigate the cost and scale of effort required to root out the APTs within an organization's systems.

The MITRE Corporation have identified six steps in a typical cyber kill chain (9), they are:

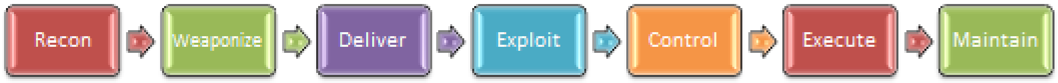


Figure 2: *Cyber Kill Chain*

APTs will dedicate time to planning, developing, and deploying methods to reach their objective. The more time a threat is allowed to prepare and commit an attack, the more potential the threat has for devastating impacts (10). This is put into perspective with data from 2013 that shows the median days that an attacker was present on a victim's network before being detected was 229 days, with the longest presence being 2287 days (11).

Clearly, time now becomes a key variable in APT detection, prevention and response. The faster an organization can identify the tactics, techniques and procedures of an APT the quicker it can take proactive steps to protect its network.

Risks and Vulnerabilities

In terms of information security there are three elements to risk, they are (12):

- Threats, which are events, whether through action or inaction, that lead to an unwanted situation
- Vulnerabilities, which are weaknesses that increase the likelihood of the threat being successful
- Impacts, which are the outcomes of threats that leverage vulnerabilities

A vulnerability is a flaw or weakness that could be exploited resulting in a security breach, a risk is the likelihood a threat will exploit a vulnerability (13). Risk and impact are directly related to the extent of the vulnerability. Examples of vulnerabilities include:

- ICMP Sweeps
- Port scanners and protocols using "well-known ports"
- Vulnerability Scanning tools such as Nmap and Net Cat

As vulnerabilities are reduced then so is risk. So to have an effective security position an organization will have to assess its risk against known vulnerabilities and, based on this, a set of security controls should be implemented. Cloud computing introduces new characteristics, service and deployment models. The risks associated with cloud computing will be outlined later in this research project.

Cyber Security Technologies

Security technology needs to detect, prevent and respond to malicious threats. Signature based security software detects known malware based on signature definitions contained in signature definition files or databases. These files have known patterns of malicious software or malware such as hash and byte signatures. Actions such a deletion or quarantine can be taken against files that have matched the known malware patterns or signatures. Regular updates of signature definition files are key to the effectiveness of this type of cyber security software.

Heuristic software uses behaviour to detect previously unknown malware and addresses the need to detect viruses that are unknown and, thus, do not have known signatures. Heuristic software looks for viral activities through analysis of suspect code, file anomalies and API monitoring.

Anomaly base detection is used in intrusion detection systems and defines patterns of normal behaviour and compares that to current behaviour of the network.

Firewalls

A firewall addresses the first goal of security which is prevention. A firewall is defined as a device that connects two or more networks or network segments together and restricts the flow of information between those networks according to rules configured in a firewall rule base (14). Inherent in this definition is that one of the networks is trusted and the other networks are public or untrusted.

Two key characteristics of firewalls are that they are, firstly, a type of perimeter defence i.e. all traffic from an organization’s LAN to the internet will travel through the firewall and, secondly, they allow or block IP packets to control network traffic. Firewalls use the following prevention methods:

- Port based or packet filtering,
- Stateful packet inspection
- Circuit level gateway
- Application gateway

Packet filtering and port based firewalls use source and destination IP address and TCP/UDP port information contained in TCP/IP packet headers to allow or block packets passing through the firewall. Best practice use of TCP/IP Ports is outlined in the “*Service Name and Transport Protocol Port Number Registry*” (RFC6335). Appendix 1 shows a summary of well-known TCP/IP port number and applications (15). By inspecting the first few bytes of the TCP header in an IP packet the firewall can determine the application protocol, for example:

- Email will utilize port 25
- FTP will use port 20 and 21
- Web traffic will use port 80

From this the firewall will allow or block the packet based on the rules contained within the firewall rules table.

Firewalls are an effective standalone technology within network security but the threat landscape is becoming massively scaled and multi-faceted with firewall evasion techniques being used in web applications. These evasion techniques will be detailed and discussed as part of the Threat Intelligence for Cloud Computing Requirements in chapter 4.

Intrusion Prevention Systems

Gartner defines network intrusion prevention as an inline security control that implements attack detection and mitigation between networks of different trust levels in time (16). Network IPS stands behind the front line network security devices such as firewalls and web and emails gateways. The characteristics of IPS are:

- It is an inline network device
- Network traffic flows through the IPS hardware system
- It can create alerts and block attacks
- It applies protocol anomaly analysis, signature analysis and behaviour analysis
- Unlike a firewall, who permits and blocks packets based on their source, destination and port number regardless of the content on the packet, IPS is designed to permit or block network packets based on the packet's contents. (17)

IPS uses the following detection methods:

- Rule (signature) based detection used for Botnets such as Denial of Service (DoS) attacks
- Anomaly based detection i.e. comparing traffic patterns to "normal" traffic patterns and determining if the traffic is within acceptable patterns or not.
- Stateful Protocol analysis, the observance of network connections to alert or block based on various types of activities.

IPS Sensors are connected to the network in one of three ways:

- Inline behind a firewall, router or switch with network traffic flowing through it
- As a Network Tap to access data flowing across the network
- A Switch Span port i.e. a port on a network switch that monitors network traffic that flows through the switch.

The main functionality you would expect of a network IPS is:

- Vulnerability-based signature production and discovery
- Rapid Signature Updates

Network IPS is now a mature technology. Standalone Network IPS devices offer inline IPS and passive IDS modes, default detection policies and reports, alerts and dashboards while Next Generation IPS (NGIPS) provide the ability to create custom rules and application monitoring of unauthorized applications, operating systems and devices. Virtual IPS sensors are able to protect virtual environments and cloud infrastructure. Next Generation IPS uses the contextual nature of IP traffic, through deep packet inspection, and is becoming more and more important with the "consumerization" of the enterprise network (18). In this context of "consumerization", Next Generation Intrusion Prevention Systems are an important network security technology as they include application awareness i.e. full stack visibility, context awareness using reputational features such as external intelligence and content awareness through advanced malware detection.

System Information and Event Management

SIEM is defined as software systems that collect security-relevant data from a variety of hardware and software products in order to create a unified security dashboard (19). The key characteristics of SIEM are log collection and correlation focusing on informing the threat response as its core objective. The key concepts within SIEM are:

- SIEM is a database of logs
- It parses and normalizes log data
- It enables analysts to deep dive into specific information
- It enables automated searches for events happening on the network

Appendix 2 demonstrates where SIEM is situated within the network to record logs from the systems within the enterprise's infrastructure including:

- Security infrastructure such as IPS/IDS, DLP, Web and email gateways and filters
- Network infrastructure such as routers, switches, application servers
- Network information such as configuration, locations, software inventories

The main functionality you would expect of a SIEM is (20):

- Data Aggregation

- Correlation
- Alerting
- Dashboards
- Compliance
- Retention

So far we have seen that firewalls and IPS/IDS systems will prevent and detect threats based on network traffic and play a pivotal role in detecting security events as perimeter defences. SIEM, though, is different in that it is a system that collects log information from firewalls, IPS/IDS and many other devices and applications with the organizations infrastructure, essentially sitting above the firewall and IPS systems to enable higher level search and correlation using the security event data from the rest of the organization's infrastructure. SIEM is not configured to have the ability to match an IPS in terms of network traffic analysis and is not meant for that reason. Despite the inherent challenges involved in deploying a SIEM solution, due to the amount of systems within an enterprise that can connect to a SIEM IP, it is a progression and bridging technology to real-time log and data gathering and development of threat intelligence.

Chapter 3 - Threat Intelligence in Cyber Security

Gartner's definition of cyber threat intelligence (CTI) states that "threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard"(21).

Thus far, this research project has presented cyber security risks and vulnerabilities and demonstrated how traditional signature based security technologies focus on prevention, detection and response to threats. This chapter will address the following in relation to CTI:

- What threat intelligence is
- Who is using it and examples of it being used
- Case studies of its limitations and success
- How CTI happens and how it works

Defining Data and Intelligence

In addition to traditional signature based security technologies, organizations can adopt an intelligence based approach to security by:

- Analysing their own enterprise environment,
- Analysing open source intelligence feeds
- Analysing vendor intelligence feeds
- Exchanging intelligence with trusted community and industry groups

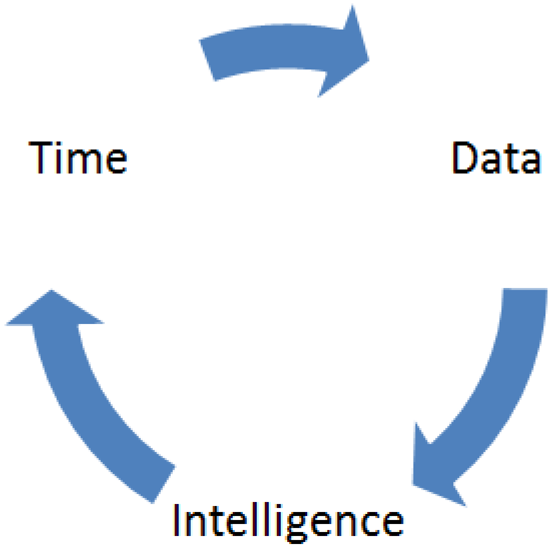


Figure 3: *Actionable Lifecycle of Threat Data*

Receiving petabytes of data feeds from these sources adds little or no value to a Security Operations Centre (SOC) or Computer Security Incident Response Team (CSIRT) unless that data can be transformed into actionable intelligence. This is what cyber threat intelligence frameworks do. They are frameworks that enable data to be converted to intelligence and for that intelligence to be stored and curated to ensure the intelligence is actionable on an ongoing basis. If the intelligence is not managed, updated and curated then its actionable intelligence value will diminish over time and it will inevitably revert back to data with less, or no, actionable value.

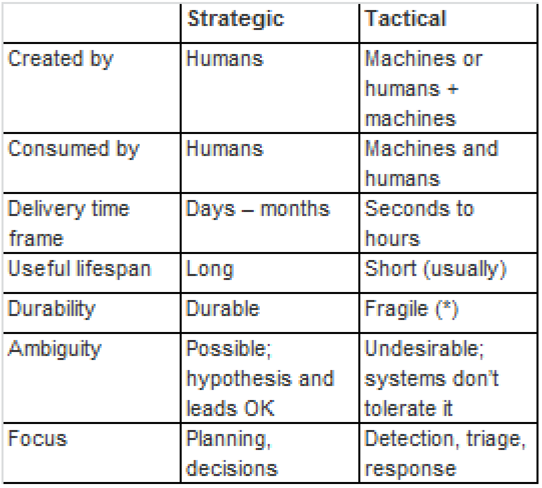
A key term within cyber threat intelligence is an Indicator of Compromise (IOC). An indicator of compromise is an intrusion signature and types of IOCs have been categorized as follows: (22)

- Host Indicators such as:
    - MD5 hashes, filenames, file sizes, file extensions, file compile times, registry keys, mutex, directory path
- Network Indicators such as:
    - IPv4 address, IPv6 address, URLs, domain names, communication protocols
- Host and Network Indicators which can be found on hosts and networks such as:
    - File name, text string
- Static Indicators, of which there are three:
    - Atomic i.e. those that cannot be broken down into smaller components such as IP address, hostname
    - Computed i.e. derived from incident data such as hash value, regular expressions
    - Behavioural i.e. collections of atomic and computational indicators paired to provide useful context

Essentially IOCs are artefacts that indicate where threat actors are, or have been. Traditionally organizations managed these indicators using flat files or their own databases. The core focus of IOCs is to enable organizations to focus on threats that are most significant to their organization's assets and leave antivirus software to deal with standard malware detection and prevention. IOCs provide context to data and transform it into intelligence, only information with its associated context can be considered intelligence (23).

Types of Cyber Threat Intelligence

The two types of CTI are strategic and tactical. The IOCs noted above are tactical CTI, defined as "*system-level or network-level artefacts that can be matched to what is observed on information systems*" whereas strategic threat intelligence are "*reports and other human readable products on threat actors and (their) intentions, goals and capabilities*" (21).



	Strategic	Tactical
Created by	Humans	Machines or humans + machines
Consumed by	Humans	Machines and humans
Delivery time frame	Days – months	Seconds to hours
Useful lifespan	Long	Short (usually)
Durability	Durable	Fragile (*)
Ambiguity	Possible; hypothesis and leads OK	Undesirable; systems don't tolerate it
Focus	Planning, decisions	Detection, triage, response

Table 1 *Characteristics of Strategic and Tactical Intelligence* (21)

Sources of Cyber Threat Intelligence

There are 3 sources of CTI (24), they are:

- Internal sources of cyber threat intelligence i.e. data collected from an organization's security devices firewalls, IPS/IDS etc.
- Community sources of cyber threat intelligence i.e. information based on trust relationships within communities of shared interest. Community threat intelligence sources can be either an Information Exchange (IE) or an Information Security Advisory Centre (ISAC) (25). One example of an ISAC is the Research and Education Networking Information Sharing and Analysis Centre (REN-ISAC) which is a trusted community for higher education groups and institutes.

  The European Agency for Network and Information Security has published a Good Practice Guide for Network Security Information Exchanges (26), the objectives of which are:

  - To protect against attack and to acquire early evidence of its likelihood, rather than damage recovery
  - Identify emerging threats and analyse their potential impact on communications networks and information systems

    - Assess the impact of incidents (security breaches, network failures, service interruptions)
    - Identify, analyse, and adopt appropriate coordinated preparedness measures to mitigate such threats and risks
    - Set up internal and joint procedures to continually review the implementation of adopted measures
- The final type of CTI source is External sources, which are:
    - Public sources available at no cost but have quality risks
    - Private vendor provided commercial threat feeds

Cyber Threat Intelligence Use Cases

Tactical threat intelligence frameworks and their effectiveness in cloud computing are the core focus of this research project. Though strategic threat intelligence is broadly out of scope it is important to note that tactical threat intelligence is a critical input to strategic intelligence in terms of identifying the tactics, techniques and procedures (TTPs) of threat actors. This is clearly evidenced in the seven use cases identified for strategic and tactical threat intelligence (27). These are:

1. Planning
    - Strategic - Security architecture planning based on long-term threats and relevant actor capabilities
    - Tactical - Historical trends across TI feeds and environment match history
2. Prevention
    - Strategic - Better align security spending based on human intelligence derived from TI
    - Tactical - Block bad IPs, URLs, domains, emails, files, etc.

3. Detection
    - Strategic - Review reports on threat actor tools to find ways to better detect them

- Tactical - Use TI feeds to create NIDS signatures, SIEM and endpoint threat detection and response (ETDR) alerting rules

4. Triage
    - Strategic - Define incident response policies based on indicator types
    - Tactical - Use TI feeds as context for enriching alerts, link alerts together into incidents, automated triage by escalating alerts linked to specific threats
5. Incident Response
    - Strategic - Understand the business
    - Tactical - "Pulling the thread" to find all compromised assets and all attacker traces
6. Threat Assessment
    - Strategic - Assess overall threat level for your organization; report to management
    - Tactical - Assess the risk to customers (internal or external) and fraud risk assessment
7. TI Fusion
    - Strategic and Tactical - Increase value of TI feeds by validating, correlating, enriching context, tying to local observations and attribution; enrich tactical TI by linking to strategic TI

The pyramid of pain is a specific model that graphically articulates the use case of cyber threat intelligence (28). The model outlines the levels of threat intelligence and the pain that each will cause threat actors. The ideal is to have intelligence about the threat actor's tactics, techniques and procedures. This ultimate use case of threat intelligence provides the threat actor with two choices; give-up or re-invent themselves from scratch. The former eliminates the threat to the organization while the latter is the most costly and most impactful to the threat actor. Given the commercial motivation of attackers it is likely that they will not take this option but just give up and move on. Both outcomes represent the optimum use case for threat intelligence.

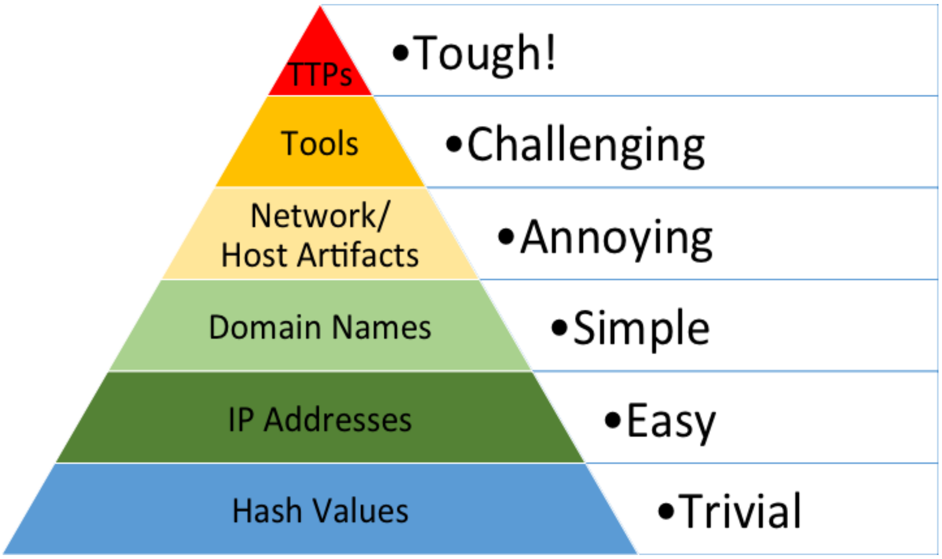


Figure 4: *The Pyramid of Pain (28)*

Cyber Threat Intelligence Frameworks

*"Cyber intelligence seeks to understand and characterize things like: what sort of attack actions have occurred and are likely to occur; how can these actions be detected and recognized; how can they be mitigated; who are the relevant threat actors; what are they trying to achieve; what are their capabilities, in the form of tactics, techniques, and procedures (TTP) they have leveraged over time and are likely to leverage in the future; what sort of vulnerabilities, misconfigurations, or weaknesses they are likely to target; what actions have they taken in the past; etc."(*9). This is an extensive and comprehensive definition of cyber threat intelligence from which the core processes of an effective CTI can be distilled.

Processes of an Effective Cyber Threat Intelligence Framework

The three core processes required for an effective CTI framework are:

- Collaboration
  - The ability of the framework to support sharing of threat intelligence between communities whether trusted or public.
  - The usability of the framework and the ability to share intelligence using secure transport protocols.
- Context
  - The ability of the framework to address tactical or strategic information.

  - The level of the "Pyramid of Pain" where the CTI framework will provide intelligence.
  - The quantity and structure of the IOCs (attributes and classes) the framework supports.
  - The flexibility of the framework and the extent the framework can parse, normalize and index the data fed into it.
- Curation
  - The effectivity of the framework as a data-store or repository of threat intelligence.
  - The efficiency, machine readability and real-time processing capability of the framework to manage the actionable lifecycle of threat data (Figure 4)

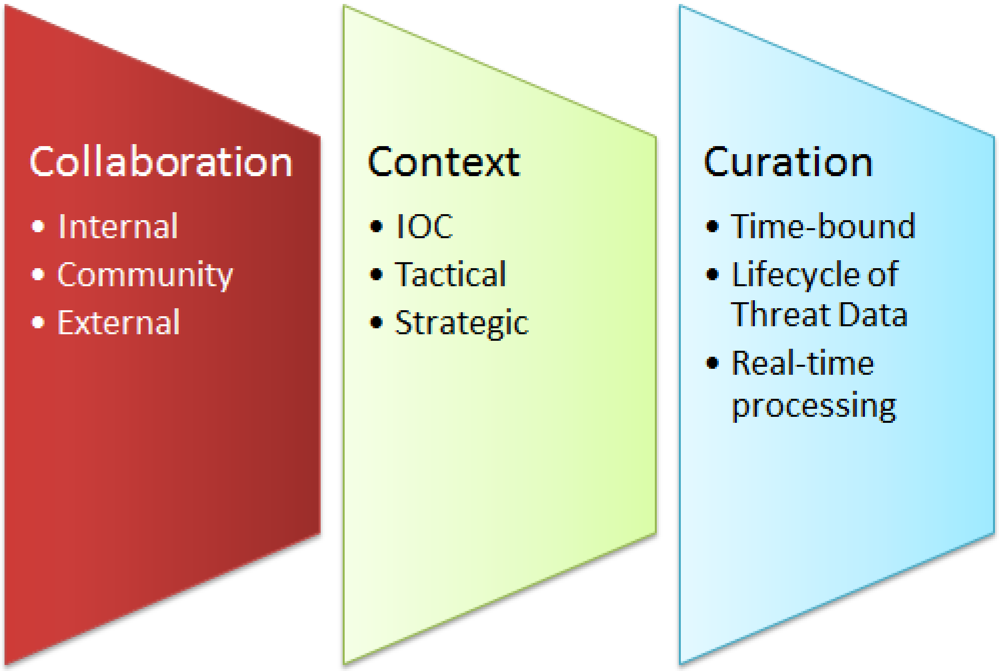


Figure 5: *The core processes of an effective CTI framework - Collaboration, Context and Curation*

Limitations of Cyber Threat Intelligence

Case Study - Heartbleed vulnerability

The Heartbleed vulnerability (CVE-2014-0160) is described by the Common Vulnerabilities and Exposures Standard as "*the (1) TLS and (2) DTLS implementations in Open SSL 1.0.1 before*

1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug" (29). It is claimed that the vulnerability was known of, and used by, the US National Security Agency (NSA) for over two years prior to its discovery (30). The scope of the Heartbleed Vulnerability is evidenced by:

- Open SSL being the most widespread implementation of the Transport Layer Security (TLS) protocol
- Open SSL being used to protect for example email servers (SMTP, POP and IMAP protocols), chat servers (XMPP protocol), virtual private networks (SSL VPNs) (31)
- Open SSL used by over half of the webservers of active sites on the Internet (32), see appendix 4 for the NetCraft graph of active webservers on the internet

The impact of the Heartbleed Vulnerability was demonstrated by Hack Labs (33) who used the exploit code and retrieved username, passwords and session cookies for banking customers in the tests they carried out.

Critically, the Heartbleed Vulnerability demonstrates a limitation of CTI in that the exploitation of this bug does not leave any trace of anything abnormal happening to the logs (31).

Case Study - BASH vulnerability

The Bash vulnerability (CVE-2014-6271) is described by the Common Vulnerabilities and Exposures Standard as the GNU Bash Remote Code Execution Vulnerability. BASH is the acronym for the Bourne Again Shell used by system administrators and developers for string processing and system information management in Linux and UNIX environments. Webservers using Common Gateway Interface and Linux and UNIX operating systems using BASH are vulnerable.

The examples and tactics of the BASH vulnerability exploits varied from: (34)

- Exploits including Perl.Shellbot and Bckdoor.Trojan
- Tactics included:
    - Ping probes by scanners indexing vulnerable web servers

  - Shell commands that gathered “uname” and “id” and dummy files on the files system
  - Serious exploits to deploy Kaiten.bot to make the servers part of a DDoS program

Exploits of the BASH vulnerability demonstrate the limitation of CTI in terms of vulnerability exploits. The shell commands that exploited the BASH vulnerability contained code to remove traces of the exploit by deleting the executable or downloaded bots directly form a server which was loaded into memory and immediately removed (34).

The Heartbleed and BASH vulnerabilities are both examples of “1 day” vulnerabilities where attackers rush to exploit vulnerability once it is made public. Tactical CTI certainly cannot eliminate “zero day” or “1 day” exploits as the vulnerabilities are programming errors in the original code. It is important to note, though, that CTI’s quick standards based response to the Heartbleed bug does demonstrate one of the successes of CTI. The standards defined for Heartbleed include:

- The Common Vulnerability Enumeration CVE-2014-0160
- The Common Weakness Enumeration, CWE-125 and CWE-130, that identified the programming weaknesses of “out of bounds reads” and “Improper Handling of Parameter Inconsistency”
- The Common Attack Pattern Enumeration and Classification used for identifying and understanding attacks that defined CAPEC-540 “Over-read Buffers”

The use of these CTI standards, of behavioural (atomic and computational) indicators and sharing of human intelligence derived from strategic threat intelligence is an effective way to identify, contextualize and minimize the effect of these “zero day” and “1 day” vulnerabilities.

Chapter 4 - Threat Intelligence for Cloud Computing – Requirements

Chapter 3 treated data and intelligence; it identified the types, sources and use cases of cyber threat intelligence before presenting the core processes of an effective CTI and the limitations and successes of CTI. This chapter will present the challenges and requirements cloud computing presents for CTI will be defined. Cloud Security Domains will be analysed for risk and five core cloud security domains will be identified where a threat intelligence framework for cloud computing needs to effective.

Web 2.0 and Enterprise 2.0 challenges

In terms of Web 2.0, "*there is no single, commonly accepted definition, nor is there likely to ever be one*" (35) but it can be understood as the evolution of first generation web based technologies such as Blogging, RSS and messaging to Web 2.0 tools like SharePoint, Facebook, Twitter, YouTube, and cloud based services such as Salesforce, WebEx and the suite of Google cloud based applications.

A related concept, and one that is core to the cloud technology landscape, is that of "consumerization" of the enterprise, otherwise known as Enterprise 2.0. This is where employee interactions and engagement go beyond the corporate boundaries (36) and corporate infrastructures are populated by personal technologies and applications. Consumerization is defined by Gartner as *"the specific impact that consumer-originated technologies can have on enterprises*" (37).

A recent study by Intel confirmed the lines are being blurred between employee's personal and work spaces and that enterprises should adopt "*a user experience-centric approach that includes a security-minded Bring Your Own Device (BYOD) initiative*" (35). The study showed the following key trends:

- 78% of employees use their personal devices for work-related activities
- 79% conduct personal online activities on company-issued devices
- 77% feel their employer is taking the necessary steps to protect all important data

In essence the consumer is bringing applications into the enterprise domain but expecting the enterprise to be robust enough to protect the data that is being exchanged by them on enterprise networks. At the same time, developers are designing consumer applications with the objective for them to be ubiquitous. To achieve this, as an example, they are using techniques such as HTTP and SSL tunnelling to enable their applications to get past standard firewalls that would normally block the application (38).These evasion methods are used by benign application developers but of course by malicious attackers and threat actors also.

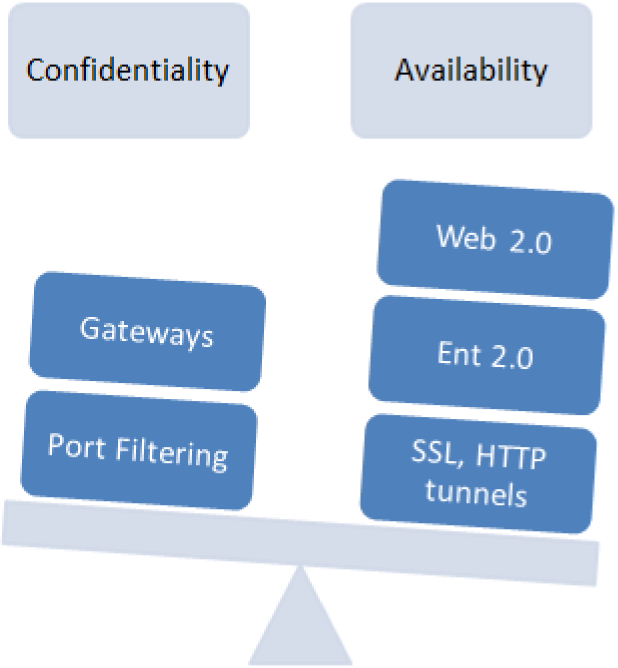


Figure 6: Weighting of *Availability over Confidentiality in Web 2.0 Application Development*

The implication of this is that an enterprise now needs to be prepared for the added complexity of threat detection, driven by application evasion techniques such as:

- Port hopping
- Use of non-standard ports
- Tunnelling
- SSL encryption

Equally a threat intelligence framework for cloud computing (TIFCC) has to recognize that Web 2.0 and Enterprise 2.0 threats are moving to the application layer where these techniques are being used. The notion that enterprises can be protected by perimeter defences such as firewalls is not adequate as the traditional network perimeter is circumvented by Web 2.0 and Enterprise 2.0 applications. Traditional firewall capabilities are limited by their inability to extract intelligence about potential threats beyond the inspection of the IP packet header and port number and the inference that has for the service the traffic is associated with. To manage the challenge of Web 2.0 an organization has to implement the following security requirements (39):

- Control communications and content in real time
- Identify and prevent malware and data leakage incidents
- Discriminate between acceptable and unacceptable Web 2.0 sources
- Enforce a policy which includes all IT communication devices
- Provide monitoring, activity and performance reports

From this overview of Web 2.0 and Enterprise 2.0 it can be determined that there are three significant points of note for threat intelligence for cloud computing:

- The network perimeter has changed and traditional perimeter defences are no longer adequate
- The application layer is a key threat vector
- Confidentiality (ensuring data is accessed only by authorized users)has suffered as a consequence of the focus on application availability

Requirements of a Threat Intelligence Framework for Cloud Computing

An objective of this chapter is to identify the top five cloud security domains where a TIFCC needs to effective. The Open Security Architecture's (OSA) Cloud Computing Pattern (36) states that an organization should conduct *" assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties)".*

For TIFCC, a risk assessment will be carried out focusing on threats, vulnerabilities, likelihood of occurrence, impact and controls (12) on the following 15 Cloud Security Domains (40).

1. Cloud Computing Architecture
2. Governance and Enterprise Risk Management
3. Legal Issues: Contracts and Electronic Discovery

4. Compliance and Audit Management
5. Information Management and Data Security
6. Portability and Interoperability
7. Traditional Security, Business Continuity and Disaster Recovery
8. Data Centre Operations
9. Incident Response, Notification and Response
10. Application Security
11. Encryption and Key Management
12. Identity and Access Management
13. Virtualization
14. Security as a Service

Nine top threats have been identified for Cloud Computing (41), they are:

1. Data Breaches
2. Data Loss
3. Account or Service Traffic Hijacking
4. Insecure Interfaces and APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Vulnerabilities

To understand the likelihood and impact of these threats each individual threat has been plotted on an actual and perceived risk graph.

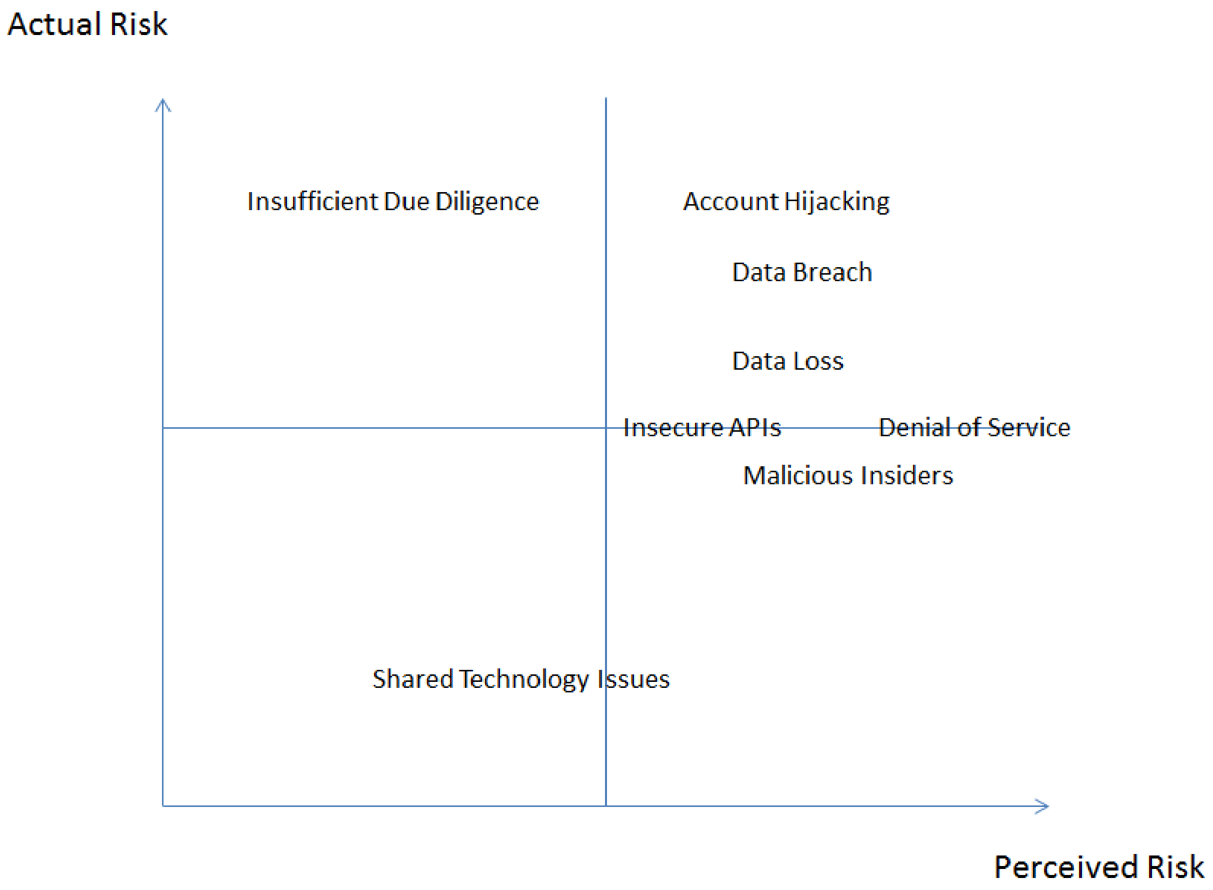
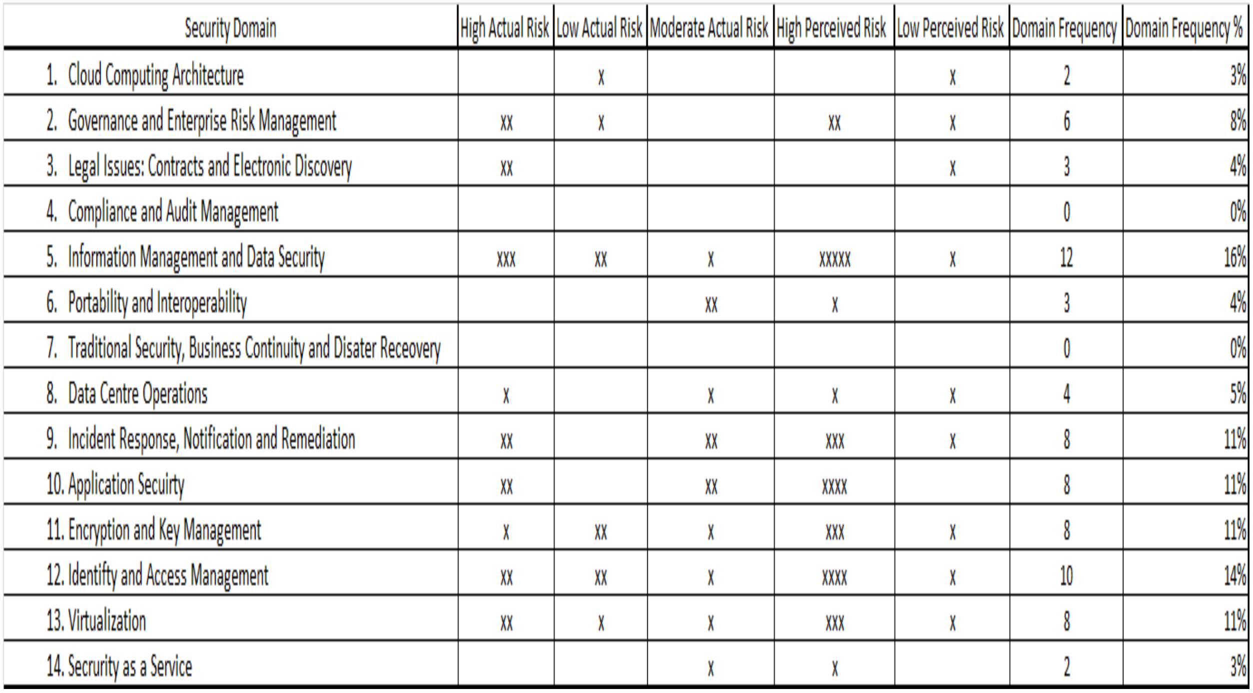


Figure 7: Composite of Actual and Perceived Risk for Cloud Threats derived from Cloud Security Alliance Cloud Computing Top Threats (41)

Figure 11 demonstrates that when each of the security domains are assessed in terms of frequency of actual risk and perceived risk, Domain 5, Information Management and Data Security has the highest actual risk frequency and highest perceived risk frequency; it also has the highest frequency of risk with 16% risk frequency as demonstrated in Table 2.

Domain 12, Identity and Access Management, has the second highest, and equal, actual and perceived risk to Domain 10, Application Security, but has slightly higher overall risk frequency with 14% compared to 11% for Application Security.



Security Domain	High Actual Risk	Low Actual Risk	Moderate Actual Risk	High Perceived Risk	Low Perceived Risk	Domain Frequency	Domain Frequency %
1. Cloud Computing Architecture		x			x	2	3%
2. Governance and Enterprise Risk Management	xx	x		xx	x	6	8%
3. Legal Issues: Contracts and Electronic Discovery	xx				x	3	4%
4. Compliance and Audit Management						0	0%
5. Information Management and Data Security	xxx	xx	x	xxxxx	x	12	16%
6. Portability and Interoperability			xx	x		3	4%
7. Traditional Security, Business Continuity and Disater Receovery						0	0%
8. Data Centre Operations	x		x	x	x	4	5%
9. Incident Response, Notification and Remediation	xx		xx	xxx	x	8	11%
10. Application Secuirty	xx		xx	xxxx		8	11%
11. Encryption and Key Management	x	xx	x	xxx	x	8	11%
12. Identifty and Access Management	xx	xx	x	xxxx	x	10	14%
13. Virtualization	xx	x	x	xxx	x	8	11%
14. Secrurity as a Service			x	x		2	3%

Table 2: Cloud Security Domain Risk Frequency, analysis derived from Cloud Security Alliance Cloud Computing Top Threats (41)

Domain 13, Virtualization, and Domain 9, Incident Response, Notification and Remediation have the third highest actual and perceived risk frequency with equal overall risk frequency of 11% each.

The core cloud security domains based on this actual and perceived risk assessment of cloud threats are:

1. Information Management and Data Security
2. Identity and Access Management
3. Application Security
4. Virtualization
5. Incident Response, Notification and Remediation

A TIFCC needs to be effective and provide actionable intelligence to enable computer security incident response teams (CSIRTs) and security operations centres (SOCs) to control the risks in these top five cloud security domains and to protect their organizational assets that interact with these core cloud security domains.

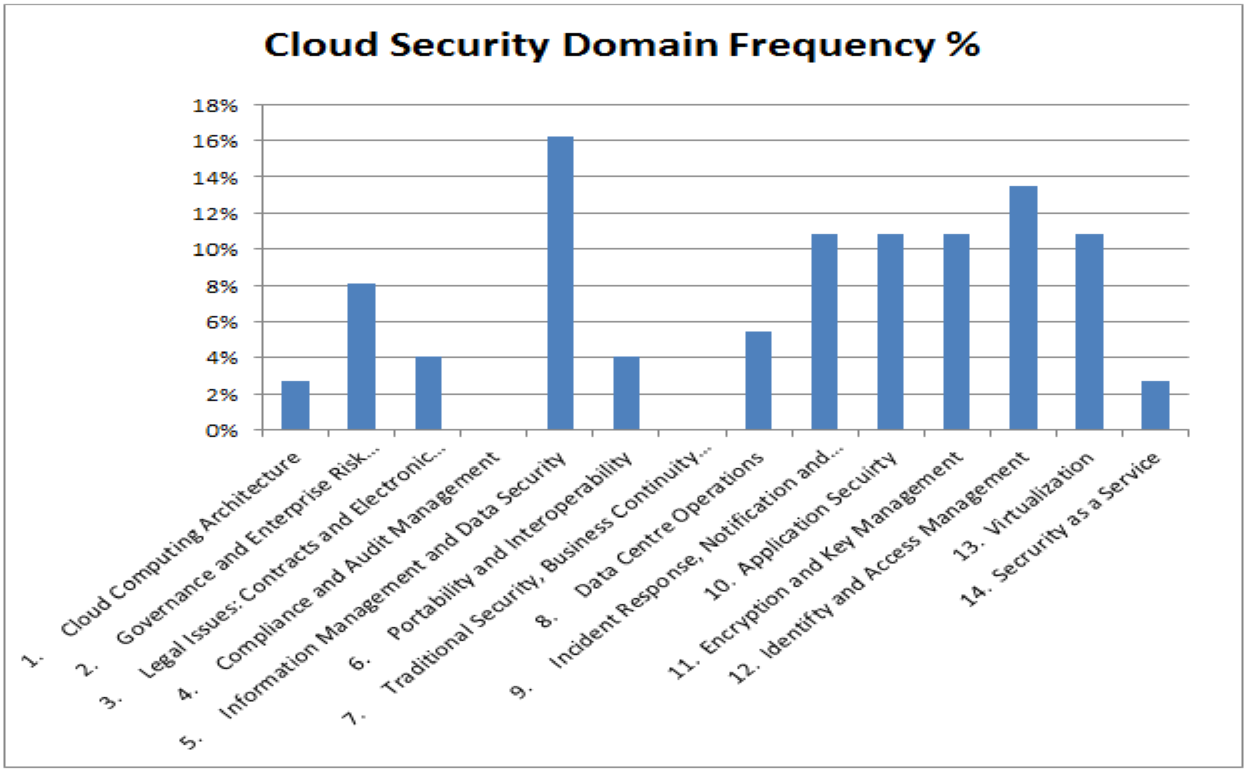


Figure 8: *Cloud Security Domain Risk Frequency, analysis derived from Cloud Security Alliance Cloud Computing Top Threats (41)*

A TIFCC will also need to be effective in terms of the confidentiality, integrity and availability (CIA) triad. A TIFCC will have to have processes and indicators to:

- Protect confidentiality and the risks associated with virtualized environments, multi-tenancy and co-resident virtual machines e.g. side-channel attacks and other virtualization threats such as “Man-in-the-Middle” and ARP Poisoning.
- Recognise the proliferation of easy to access passwords and the tactics this such as phishing and social engineering.
- Identify the weaknesses of applications and single sign on APIs that are developed for convenience of use and availability over security and confidentiality
- Be aware of techniques like cross site scripting for accessing user logon credential

- Be able to have forensic capability and indicators to identify network and application layer DoS and DDoS attacks.

Chapter 5 - Threat Intelligence for Cloud Computing – Analysis

The most comprehensive comparative analysis of CTI Frameworks is by Farnham (24). He reviewed CTI frameworks in the context of the Project Management Institute's "*Project Management Book of Knowledge*" (PMBOK) process groups for a hypothetical case study where a company had 9 specific service requirements for a threat intelligence framework. The requirements he specified were:

- 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.

Cyber Threat Intelligence Framework analysis

The frameworks identified by Farnham will now be defined, analysed and assessed in the context of a TIFCC. The frameworks that will be reviewed are:

- Open Indicators of Compromise (Open IOC)
- VERIS
- Traffic Light Protocol (TLP)
- Mitre Standards for CTI Management

    - Structured Threat Information eXpression (STIX)
    - Cyber Observable Expression (CyboX)
    - Trusted Automated Exchange of Indicator Information (TAXII)
- Managed Lightweight Exchange (MILE)
    - Incident Object Description Exchange Format (IODEF)
    - IODEF for structured cybersecurity information (IODEF-SCI)
    - Real time Inter-network Defence (RID)
- Open Threat Exchange (OTX)
- Collective Intelligence Framework (CIF)
- Other supporting tools

Open Indicators of Compromise

Open Indicators of Compromise (Open IOC) is an extensible XML schema for the description of technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise (42). Open IOC is a tactical threat intelligence tool available as open source since 2011. It has developed into a commercial tool as part of the Mandiant Corporation, now part of Fire Eye Security. Open IOC's functionality develops intelligence from signatures to discover threat actor behaviours. The functionality of Open IOC is as follows (43):

- Signatures
    - Files specifics – MD5 hash, file size, file name etc.
    - Memory entities – services, processes, handles, mutex
    - Registry entities – unique entries, persistence mechanisms
- Increasing Complexity
    - Combine signatures together logically to create powerful searches
    - Identify commonality on groups of malware
    - Use on collections of data to identify anomalies
- Methodology
    - Focus on what attacker does instead of what malware is
    - Look for behaviours beyond compromise and exploits

  - Staging locations, naming conventions, recurring behaviours

An example and notable Open IOC deployment is in Trend Micro's *Deep Discovery Advisor* log, file sample, storage, and visualization and investigation tool.

The key findings from the analysis of Open IOC are that it:

- Is designed to be a collaborative tool with key use to enable automated sharing of threat intelligence
- Is open Source but with strength and resources of Mandiant and Fire Eye as demonstrated by Mandiant releasing more than 3,000 indicators to bolster defences against APT1 (6) Operations
- Is highly contextual with over 500 attributes
- Is implemented at scale in external private threat intelligence as part of Mandiant's Intelligent Response product
- Enables investigation of tactics, techniques and procedures through Redline functionality

Veris

VERIS is a strategic threat intelligence framework available for public use and designed to provide metrics for risk management. It is defined as *"a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner*" (44).

VERIS has 5 categories within its schema, they are:

- Incident Tracking
- Victim Demographics
- Incident Description
- Discovery and Response
- Impact Assessment

Each of these main categories has sub elements e.g. incident description has 4 sub categories of:

- Actors
- Actions
- Assets
- Attributes

The actor's category has sub elements of external, internal and partners each with motive, variety and origin. Indicators of compromise are very limited in VERIS, it provides for question text, user notes, question type, variable name, purpose, developer notes and miscellaneous information. VERIS does, though, note that this data can be exported to more suitable schemas such as STIX (44).

The key findings from the analysis of VERIS are:

- It is a strategic framework and context is provided at an aggregate level more to inform enterprise risk management than tactical context sharing with CSIRTs and SOCs
- It curates incident data with VERISDB, a database of actual events and post-incident analysis and data visualization at an aggregate level.
- It has limited collaboration with a contribution pool of just 19 organizations supplying information , and weighted to incidents from the healthcare sector

MITRE standards for CTI Management

The MITRE standards for CTI management incorporate:

- STIX
- CybOX
- TAXII

STIX is specifically designed for automation and is defined as *”a language, being developed in collaboration with any and all interested parties, for the specification, capture, characterization* *and communication of standardized cyber threat information"*(9). It does so in a structured fashion to support more effective cyber threat management processes and application of automation.

CybOX is defined as "*a language for encoding and communicating standardized high-fidelity information about cyber observables, whether dynamic events or stateful measures that are observable in the operational cyber domain"* (45). STIX is a higher level schema than Cybox and uses CybOX language to describe "observables" which are essentially host and network indicators of compromise.

TAXII is the exchange used to securely share this cyber threat intelligence. It is a community driven effort and seeks to standardize trusted automated information exchange.

A notable deployment is in Microsoft's Interflow security automation platform which has adopted the STIX, TAXII and CybOX specifications to enable structured, automated machine to machine information exchange.

The key findings from the analysis of Mitre Standards for CTI Management are:

- CybOX
    - Supports automation and has big data database (MongoDB)
    - Has data visualization
- TAXII
    - Contextual and application aware
    - Uses Python and XML
    - Supports collaboration with TAXII service, hosted by a server and listens for connections
        - Discovery Service – Advertise available TAXII Services
        - Inbox Service – Accept pushed data from producers
        - Poll Service – Offer information for consumers to poll
        - Collection Management Service – Advertise available Data Collections; Manage Subscriptions (Create, delete, pause, resume)

    - Supports collaboration with TAXII client , used by a client to use a TAXII service
        - Discovery Client – Learn which TAXII Services are available
        - Inbox Client – Push data to consumers
        - Poll Client – Poll data from producers
        - Collection Management Client – Learn available Data Collections; Manage Subscriptions
- STIX
    - Incorporates other schemas such as IODEF as part of its "integrate not duplicate approach"
    - Has repeated patterns, supports automation and uses live feeds
    - Extensible Schema and supports the conversion of content between STIX and other formats e.g. Open IOC XML to STIX
    - Flexible, can use XML or JSON
    - Enables Visualization through STIXViz: graphical visualization and knowledge graphs
    - Can be used for both tactical and strategic threat intelligence

STIX, CybOX and TAXII deliver collaboration, context and curation in their respective languages and protocols, enabling automation, standardization and real-time feeds and storage of threat indicators.

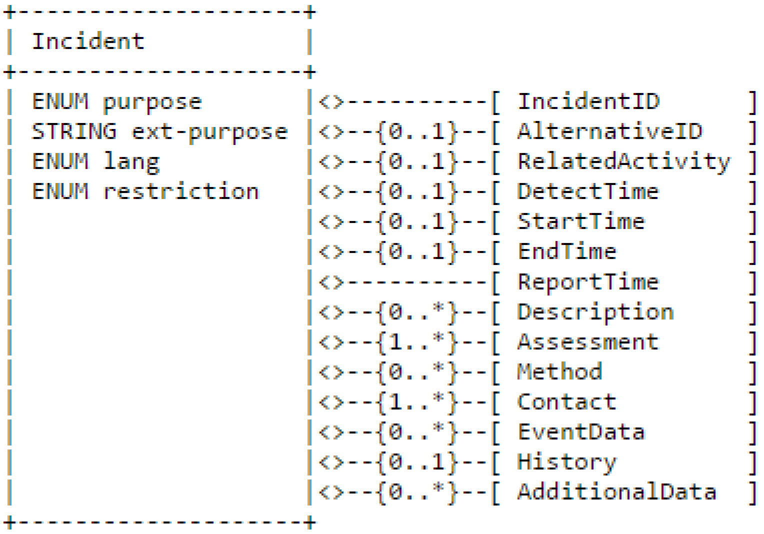
Managed Incident Lightweight Exchange

MILE is made up of three elements:

- Incident Object Description Exchange Format (IODEF)
- IODEF for structured cybersecurity information (IODEF-SCI)
- Real time Inter-network Defence (RID)

"The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incident." (46).

IODEF-SCI (RFC 7203) extends IODEF for structured cybersecurity information and embeds identifiers from structured data representation types such as Common Vulnerabilities and Exposures (CVE) and Open Vulnerability and Assessment Language (OVAL) (47).



```
+--------------------+
| Incident           |
+--------------------+
| ENUM purpose       |<>----------[ IncidentID      ]
| STRING ext-purpose |<>--{0..1}--[ AlternativeID   ]
| ENUM lang          |<>--{0..1}--[ RelatedActivity ]
| ENUM restriction   |<>--{0..1}--[ DetectTime      ]
|                    |<>--{0..1}--[ StartTime       ]
|                    |<>--{0..1}--[ EndTime         ]
|                    |<>----------[ ReportTime      ]
|                    |<>--{0..*}--[ Description     ]
|                    |<>--{1..*}--[ Assessment      ]
|                    |<>--{0..*}--[ Method          ]
|                    |<>--{1..*}--[ Contact         ]
|                    |<>--{0..*}--[ EventData       ]
|                    |<>--{0..1}--[ History         ]
|                    |<>--{0..*}--[ AdditionalData  ]
+--------------------+
```

Figure 9: *Incident Class in IODEF (48)*

Real time Inter-network Defence (RID) protocol is "*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*." (49). RID is a separate schema to IODEF and acts like an envelope for secure transportation of IODEF –RID XML enabling sharing of incident data, mitigation and insight between service providers and CSIRTs.

A notable deployment of IODEF is its use by the Anti-Phishing Working Group (APWG) as a message format. RFC5901 extends the IODEF document class for reporting phishing.

The key findings from the analysis of MILE are:

- It delivers context with incident, port list, URL , impact type and severity
- It efficiently curates threat intelligence by increased machine readability and automation

- It incorporates a separate standardized security transport protocol RID and enables real-time messaging and collaboration
- IODEF-SCI uses structured descriptions e.g. CAPEC, CVE, CVRF, CCE, MAEC, OVAL
- It supports collaboration models of P2P, Source/subscriber and Hub and Spoke
- IODEF-SCI is application aware
- Is used in External Private (Commercial) threat intelligence
- By definition IODEF-SCI is only a transport format and not designed for storage or archiving

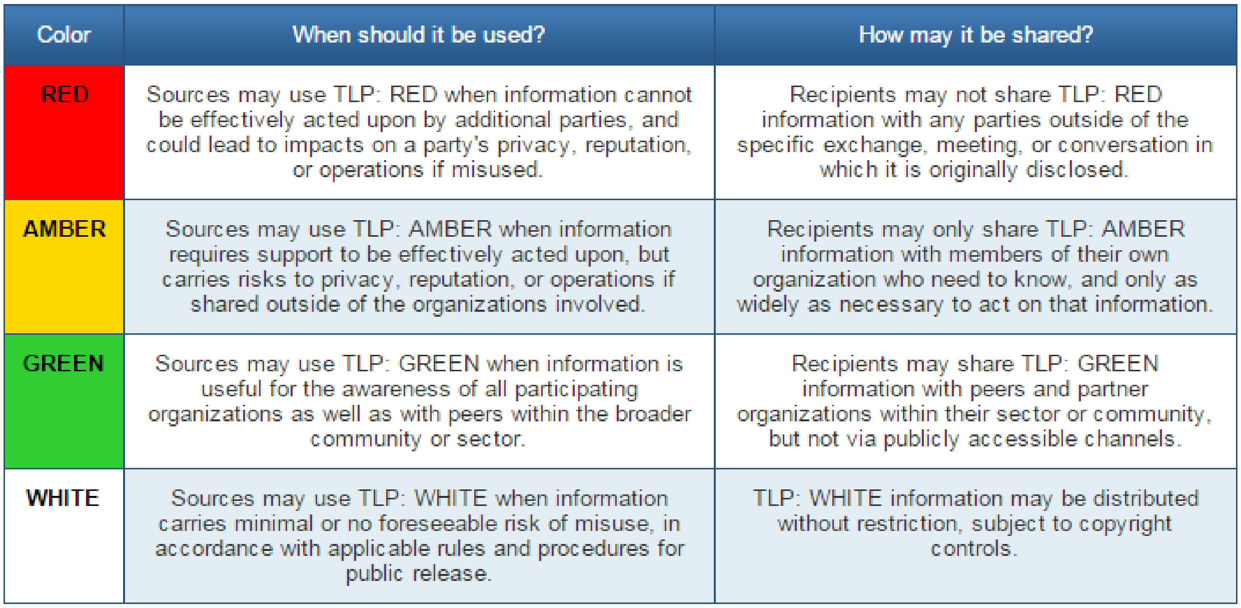
Traffic Light Protocol

"The Traffic Light Protocol (TLP) is a set of designations used to ensure sensitive information is shared with the correct audience. It employs four colours to indicate different degrees of sensitivity and the corresponding sharing considerations, to be applied by the recipient(s)" (50).

TLP is a US Computer Emergency Readiness Team (US-CERT) initiative. It is a very simple schema to categorize sensitive information for the purpose of appropriate information exchange and used as a data marking extension in STIX

The key findings from the analysis of TLP are:

- This schema has no automated functionality for collaboration or curation
- Provides basic human-readable schema for information exchange and context
- Has use in categorizing and controlling information for trusted and public sharing communities



Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Figure 10: *TLP Model* (50)

OTX

OTX is an open threat intelligence sharing and analysis service focused on providing threat data to the public. It utilizes Alien Vault's Open Source SIEM system to collect, validate and share data to Alien Vault's Open Threat Exchange. OTX is available as a feed in the Collective Intelligence Framework (CIF).

The key findings from the analysis of OTX are:

- OTX is essentially an aggregation of a global SIEM network i.e. those using the Alien vault Open Source SIEM (OSSIM), this limits the context to this single SIEM sensor network
- Has limitations in terms of collaboration as it has limited use for community based or trust based exchanges and does not have controls in terms of who can access submitted data
- OTX has scale and delivers curated threat intelligence through real-time feeds
- OTX is an external private (commercial) CTI framework

Collective Intelligence Framework

Collective Intelligence Framework (CIF) is a Research and Education Networking Information Sharing and Analysis Centre (REN-ISAC) project. It is defined as a cyber threat intelligence management system that *"allows you to combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route)"* (51).

CIF is a tactical threat intelligence framework used by CSIRTS for response and forensic analysis. It ingests data from open source intelligence (OSINT), parses, normalizes and indexes the data from those feeds and makes it available for outbound feeds using output plugins.

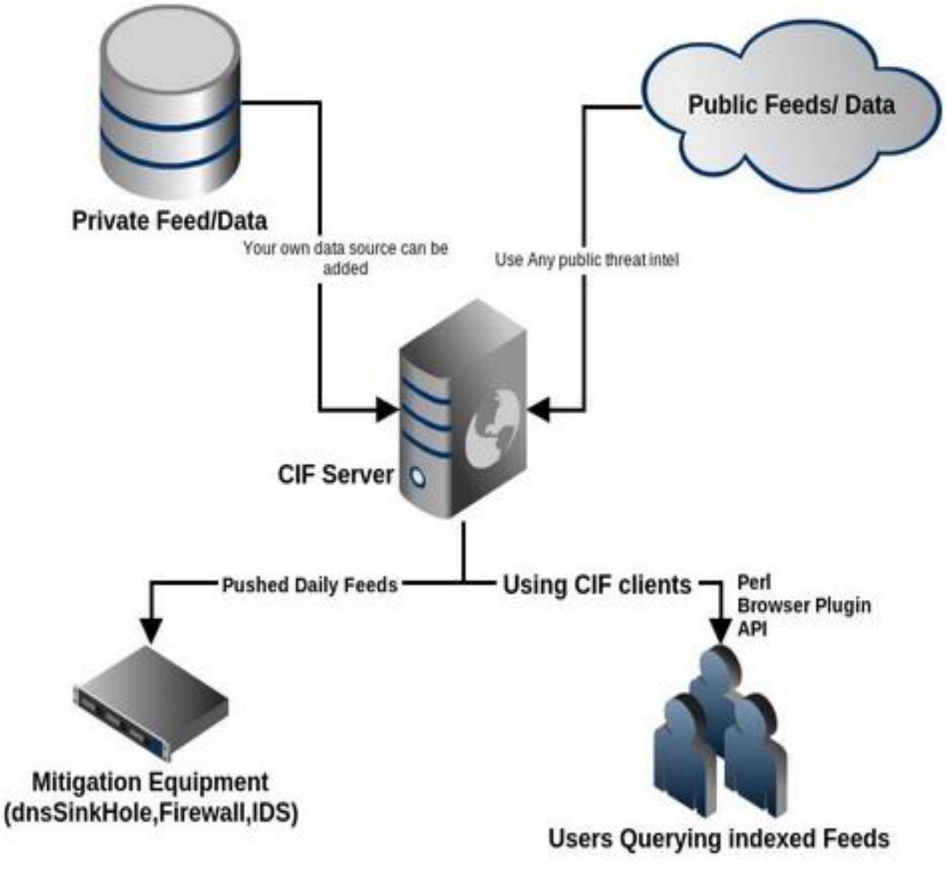


Figure 11: *CIF feed flow (51)*

CIF utilizes a 7 step process to:

- Parse
- Normalize
- Store
- Post process
- Query
- Share
- Produce data sets

CIF has widespread use for Open Source Intelligence (OSINT) and automated host and network threat feeds e.g. REN-ISAC, STIX, and Bro Network Monitor.

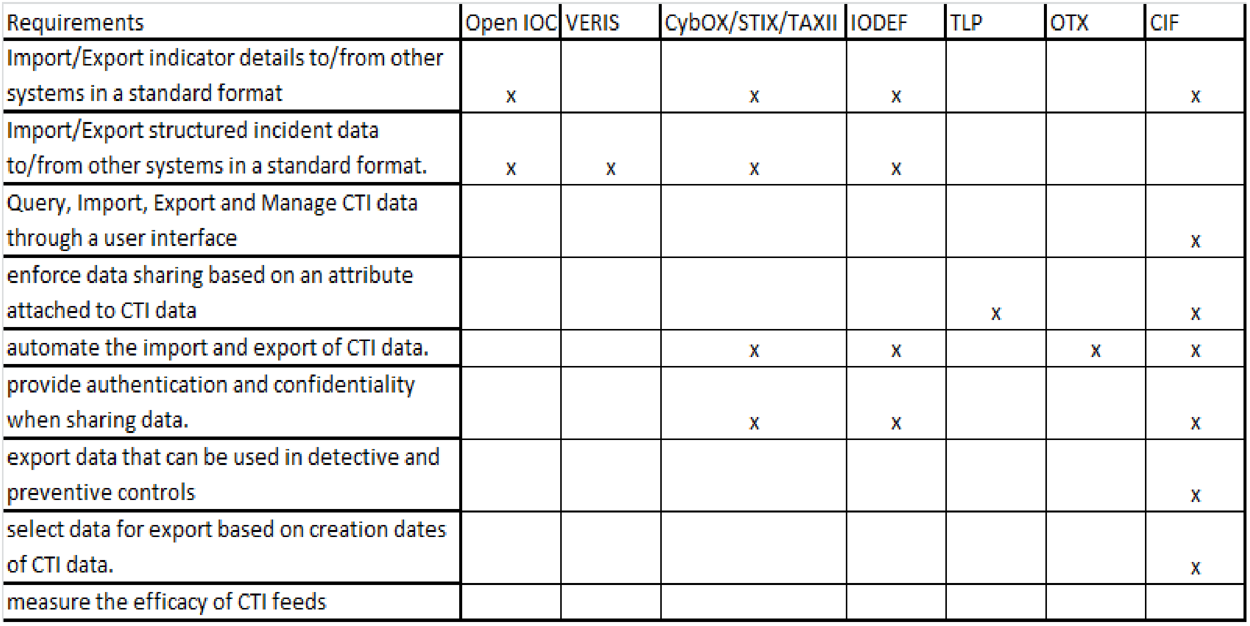
The key findings from the analysis of CIF are:

- It is a collaborative Open Source community based framework configured with multiple open source intelligence sources such as Spamhaus, Zeus Tracker and Shadowserver
- Focuses mainly on tactical threat types such as IP addresses, URLs and domains but does include concepts of *severity* and *confidence* as well as *privilege* which do add contextual capability
- Contextualizes threats and normalizes the data into Botnets, Malware, Phishing, Fast Flux, Scanner, Spam, Suspicious and Whitelist
- Delivers curation with CIF v1 using a schema-less storage with RDBMS (PostgreSQL), and HBase proposed for CIF v2
- CIF can be queried via web-browser, native client and API

Other Supporting Tools

There are a number of supporting tools that are widely used within cyber threat intelligence. They do not have the complexity to meet the core processes requirements of an effective CTI but do have broad use and value to the CTI frameworks contained within this research. Examples of these tools are:

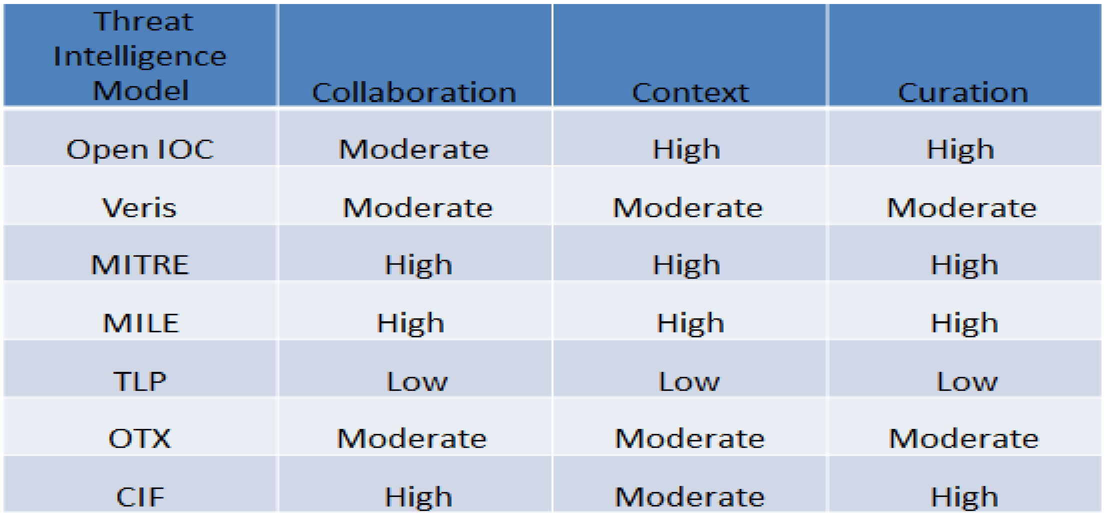
- YARA - https://github.com/plusvic/yara . A custom text based tool to create rules to identify and classify malware using strings and Boolean expression.
- Snort - https://snort.org/ - A set of rules designed for use in Intrusion Detection Systems. Rules focus on IP and HTTP headers and packet payload patterns.
- Splunk - http://www.splunk.com/ Splunk is a log management and analysis platform for use by CSIRTs and SOCs.
- Bro - https://www.bro.org/ Bro Network security monitor is an open source network traffic analysis framework.



Requirements	Open IOC	VERIS	CybOX/STIX/TAXII	IODEF	TLP	OTX	CIF
Import/Export indicator details to/from other systems in a standard format	x		x	x			x
Import/Export structured incident data to/from other systems in a standard format.	x	x	x	x			
Query, Import, Export and Manage CTI data through a user interface							x
enforce data sharing based on an attribute attached to CTI data					x		x
automate the import and export of CTI data.			x	x		x	x
provide authentication and confidentiality when sharing data.			x	x			x
export data that can be used in detective and preventive controls							x
select data for export based on creation dates of CTI data.							x
measure the efficacy of CTI feeds							

Table 3 *“Tools and Standards for Cyber Threat Intelligence Projects” (24)*

Farnham finds that CIF meets the most criteria defined by him for his assessment of threat intelligence frameworks. It does not though meet his second requirement which is the “Capability to Import/Export structured incident data to/from other systems in a standard format” and consequently has been evaluated as moderate in the core CTI process of Context. Figure 12 provides a comparative illustration of these frameworks and shows Open IOC is moderate in the core process of Collaboration due to its lack of a dedicated transport protocol. Mitre and MILE packages score high in all core processes with high level schemas, languages for incidents and observables and dedicated transport protocols. OTX and VERIS have moderate performance in all three CTI processes and TLP has a low performance in each process.



Threat Intelligence Model	Collaboration	Context	Curation
Open IOC	Moderate	High	High
Veris	Moderate	Moderate	Moderate
MITRE	High	High	High
MILE	High	High	High
TLP	Low	Low	Low
OTX	Moderate	Moderate	Moderate
CIF	High	Moderate	High

Figure 12: *Comparative assessment of CTI frameworks for core processes of an effective CTI*

Chapter 6 - Threat Intelligence for Cloud Computing - Design

The information and assets that an enterprise has within either one, or all, of the SPI cloud service models represent the cyber security priorities for that enterprise. An effective TIFCC design will need to support the protection of those assets in the core cloud security domains of:

- Incident and Access Management
- Virtualization
- Application Security
- Incident Response
- Notification and Remediation and Information Management and Data security

To do this a TIFCC has to have the core processes of an effective CTI (Collaboration, Context and Curation) to support Strategic and Tactical Threat Intelligence. In addition, though, a TIFCC will have to deliver processes that are specific to cloud computing and these will be outlined in detail in this chapter.

Design for an effective Threat Intelligence Framework for Cloud Computing

Cloud computing has specific characteristics, service models and deployment models (1).To support this cloud computing architecture an effective threat intelligence framework needs to have processes that are over and above the design processes of standard cyber threat intelligence frameworks. The processes for an effective Threat Intelligence Framework for Cloud Computing are:

- Scale
- Sharing
- Speed
- Structure
- Standardization

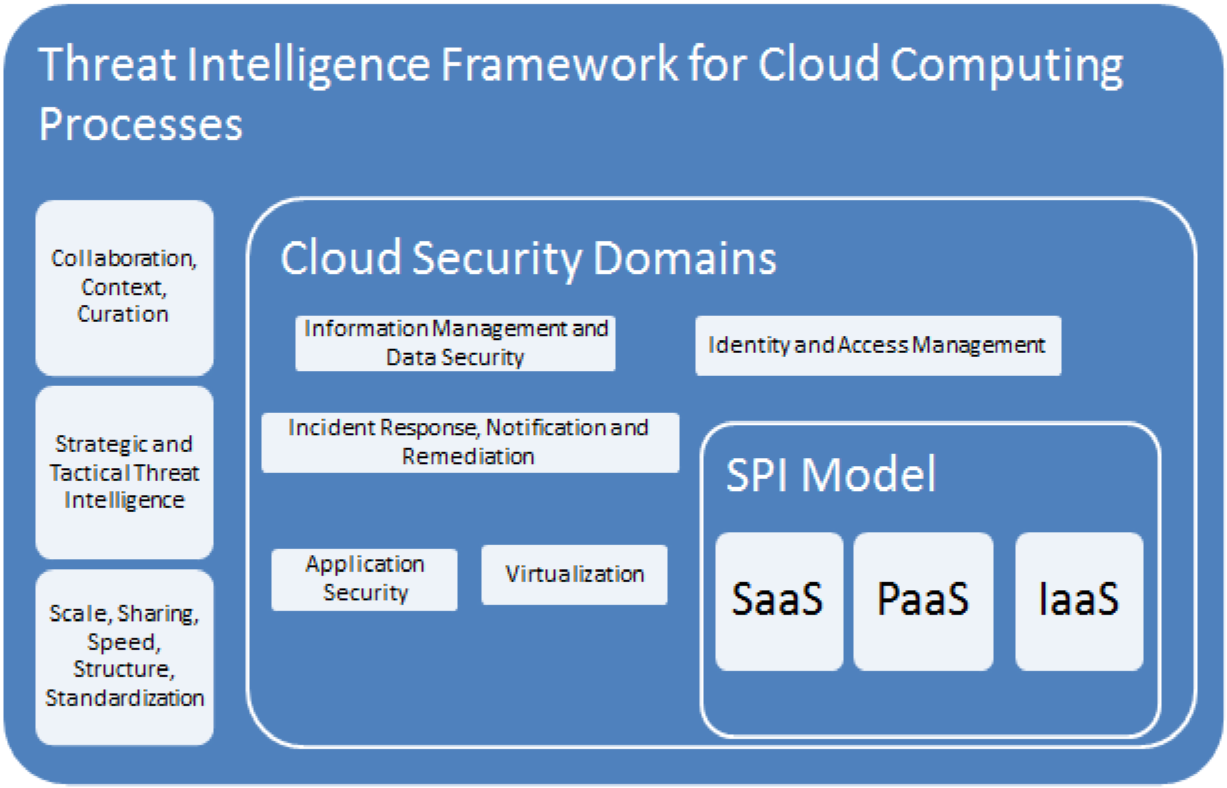

Threat Intelligence Framework for Cloud Computing Processes
Collaboration, Context, Curation
Strategic and Tactical Threat Intelligence
Scale, Sharing, Speed, Structure, Standardization
Cloud Security Domains
Information Management and Data Security
Identity and Access Management
Incident Response, Notification and Remediation
Application Security
Virtualization
SPI Model
SaaS
PaaS
IaaS

Figure 13: *Processes of an effective Threat Intelligence Framework for Cloud Computing*

Scale

Cloud computing is a distributed computing model. The National Institute of Standards and Technology (NIST 800-145) defines rapid elasticity, on-demand self-service and resource pooling as characteristics of cloud computing (1) and all of these characteristics are explicitly linked to the scalability of cloud computing. Cloud scaling enables software to adjust and add resources in an organization's infrastructure without interactive involvement. The cloud will scale capacity dynamically, proactively or reactively to support availability requirements (52). Thus an effective threat intelligence framework for Cloud Computing will have:

- The capability to receive threat data feeds from a vast amount of data sources within this dynamically scaling infrastructure
- Will have a NoSQL ("Not Only SQL") database engine to process and map the data from the cloud architecture

The requirement for a NoSQL database is that relational databases will struggle in terms of I/O and processing speed required to support the volume of threat data that cloud computing will produce.

Sharing

Sharing develops the core CTI process of collaboration. Nearly two-thirds of organizations have stated that threat intelligence could have prevented the cyberattacks they had experienced in the previous 12 months (53), so for effective threat intelligence, data and intelligence has to be shared. Three basic sharing models support threat intelligence sharing, they are Source and Subscriber, Hub and Spoke and Peer to Peer (54).

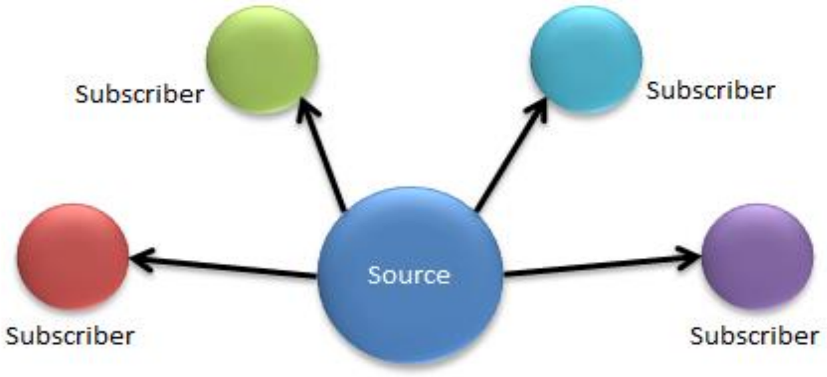


Figure 14: *Source and Subscriber Sharing Model (54)*

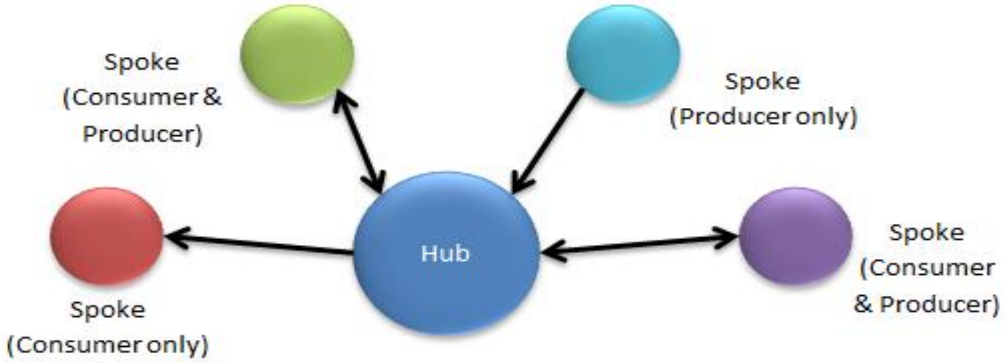


Figure 15: *Hub and Spoke Sharing Model (54)*

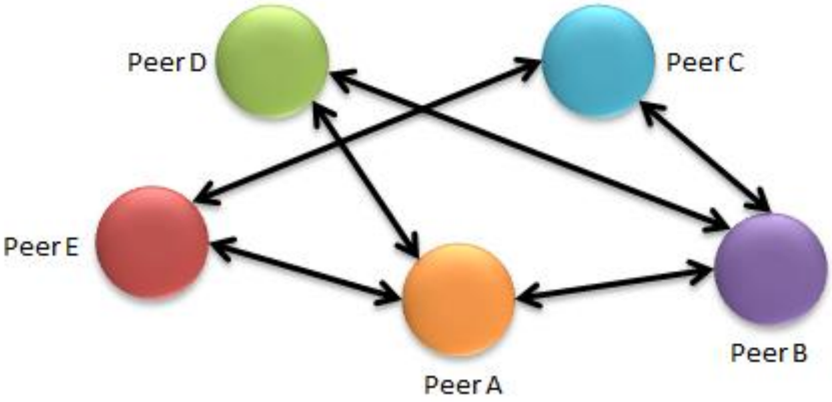


Figure 16: *Peer to Peer Sharing Model (54)*

In addition due to the volume of threat data in cloud computing an effective TIFCC will have to:

- Share data in machine readable formats
- Be a framework that support automation
- Have a secure transport protocol
- Have a data visualization component

Speed

Speed develops the core CTI process of curation. Close to 70% of organizations say that threat intelligence expires within seconds or minutes, and more than half say they get that information in days, weeks, or months after its discovery, rendering much of it useless (6). The

Actionable Lifecycle of Threat Data (Figure 4) demonstrates the inherent time sensitivity of data and intelligence, and the risk that intelligence can revert back to data if it is not processed quickly.

An effective CTI needs to be able to manage the velocity of threat data that is associated with cloud computing. The key elements required are:

- Have real-time processing component
- Receive live threat data feeds

Structure

Getting context from threat information enables TTPs to be determined and ultimately knowledge of the behaviours embedded in cyberattacks. The TIFCC design process of Scale outlined that cloud computing, and the vast amounts of threat intelligence data it produces, will require the use of NoSQL databases. To provide context from structured and unstructured threat data a TIFCC will require the NoSQL database to provide rich querying ability.

Column databases such as HBASE and Cassandra are a good design fit for a TIFCC in terms of the speed of processing required for a cloud computing threat intelligence data. The volume of threat intelligence data sets is demonstrated by big data analytics experiments conducted by HP Labs which used 2 billion HTTP requests, 1 billion DNS requests and 35 billion NIDS alerts (55). The key advantages that column databases provide for TIFCC is that they offer performance through reduction in I/O bottlenecks and offer scalability which is a particular advantage compared to relational databases. Despite these advantages there are relative downsides also, for instance, it should be noted that column databases do not offer rich querying capabilities relative to RDBMS, though “bolt-ons” such as Hive do address this relative deficiency. Key Value databases are another type of NoSQL database and examples are Dynamo DB and Riak. These are similar to column databases in that they do not require a schema and provide flexibility and scalability which are required to meet the threat data volumes associated with a TIFCC.

Standardization

It is recognized (56) that as late as 2013 there is no generally accepted standard data format for security operations teams to share IOCs and there are a multitude of different enumerations, languages and repositories for threat intelligence (57). For TIFCC to be effective it needs to have as many standardized elements as possible. Making Security Measurable (MSM) is a collection of Information Security Community Standardization Activities and Initiatives (58). Its objectives are:

- Create registries of baseline security data
- Provide standardized languages
- Establish community approaches for standardized process

MSM identifies 15 areas where security needs to be standardized and measured. A TIFCC needs to incorporate relevant standards from the following areas:

- Software Assurance – CWE, CWSS
- Application Security – CWE, CAPEC,OWASP
- Asset Management – ARF, ASR, OVAL, CCE, CPE, XCCDF, OCIL
- Supply Chain Risk Management - OWASP
- Cyber Intelligence Threat Analysis – STIX, Cybox, CVE, CPE, MAEC
- Cyber Threat Intelligence Sharing – STIX, TAXII
- Vulnerability Management – CVRF, CVSS, CVE, CWE, OVAL
- Patch Management – OVAL, CVE, CCE, CPE, XCCDF, OCIL, SCAP
- Configuration Management – CEE, CPE, OVAL, SCAP, FDCC, USGCB
- Malware Protection – MAEC
- Intrusion Detection – CVE, CVSS, CAPEC, MAEC, OVAL, XCCDF, OCIL, SCAP
- System Assessment – CVE, CWE, CWSS, CWRAF, CCE, CPE, OVAL, MAEC, CVSS, SWID, FDCC, USGCB, STIGS, CIS, SCAP
- Incident co-ordination – STIX, TAXII, IODEF, RID
- Enterprise Reporting – ASR, ARF, OVAL, XCCDF, OCIL
- Remediation – OVAL, CVE, CCE, CPE, XCCDF, OCIL, SCAP

Appendix 7 provides a full and expanded list of each of these standards.

The research thus far has demonstrated that an effective TIFCC must have the core CTI processes of:

- Collaboration
- Context
- Curation

A TIFCC also needs to be effective in the five core cloud security domains of:

- Information Management and Data Security
- Identity and Access Management
- Application Security
- Virtualization
- Incident Response, Notification and Remediation

Finally, a TIFCC needs to demonstrate the design capability to meet the core cloud specific processes of:

- Scale
- Sharing
- Speed
- Structure
- Standardization

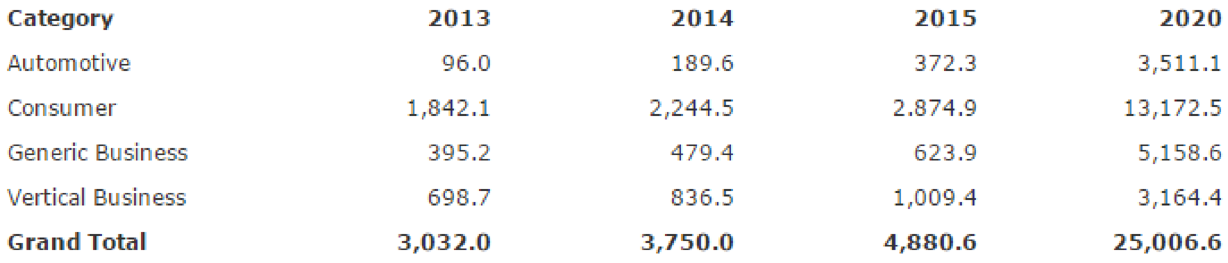
All of these elements will be addressed in the next chapter *Threat Intelligence Framework for Cloud Computing – Discussion.*

Chapter 7 - Threat Intelligence Framework for Cloud Computing - Discussion

Threat Intelligence Frameworks for Cloud Computing

Claims have been made that 90% of all threat intelligence is redundant from feed-to-feed (59). It is logical that when the quantity of data exceeds the quality of data the risk of false positives increases. An effective TIFCC will need to derive quality intelligence out of this abundant and redundant threat data, driving less false positives and in turn more dependable and effective intelligence.

A TIFCC will also need to meet the scale of technology trends such as the Internet of Things (IOT). Gartner's (59) analysis shows that there are 4.9 billion connected devices in use in 2015 and project that number will increase to 25 billion devices by 2020.

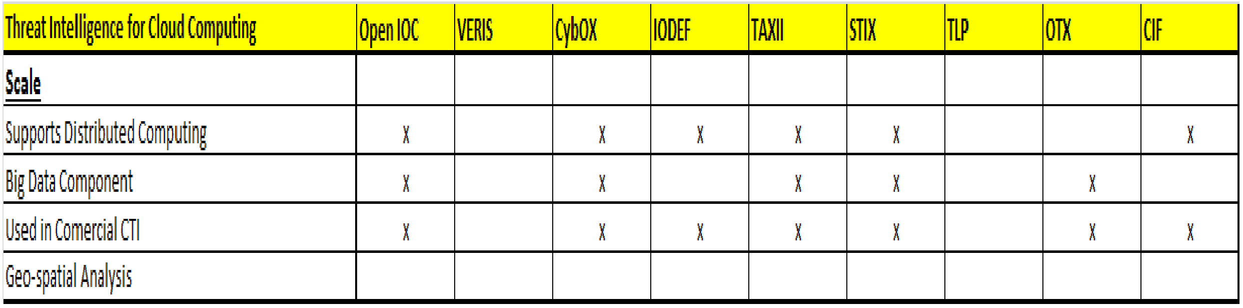


Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Figure 17: *Internet of Things Units Installed Base by Category (71)*

This data demonstrates that the volume, variety and velocity of IOT data will increase five-fold in the next five years and will have an inevitable and disruptive effect on the data that feeds into threat intelligence frameworks for cloud computing.

- There will be more logs, more events and alerts and these will be more challenging to parse and normalize.
- Treat intelligence attributes and IOCs will increase in variety. A TIFCC will need to have geo-spatial analysis (36) and build spatial NoSQL databases into the framework such as Neo4j. To date none of the frameworks analysed possess this capability.
- The IOT also presents a challenge for threat intelligence as IOT devices may introduce new vulnerabilities such as those presented by the Bash vulnerability (60). This is an established blind-spot for TIFCC where to date it has not been effective and increases the risk of DDoS attacks as IOT devices grow in number.
- XML is the most common language of all used in CTIs, there remains a question over how efficient and scalable XML will be to meet the 500% growth in IOT devices.



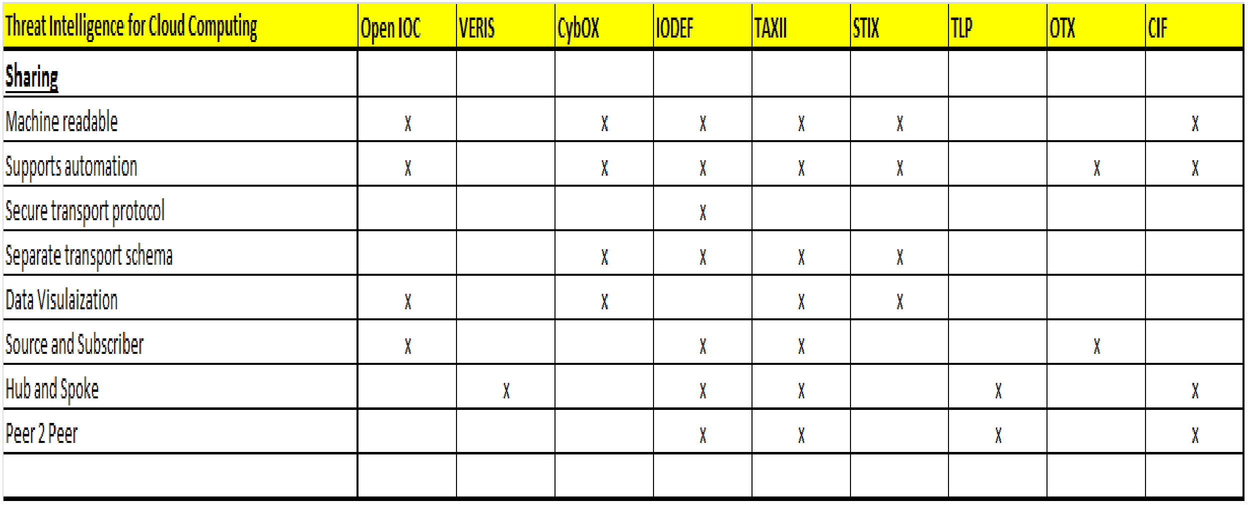
Threat Intelligence for Cloud Computing	Open IOC	VERIS	CybOX	IODEF	TAXII	STIX	TLP	OTX	CIF
Scale									
Supports Distributed Computing	X		X	X	X	X			X
Big Data Component	X		X		X	X		X	
Used in Comercial CTI	X		X	X	X	X		X	X
Geo-spatial Analysis									

Table 4: *Evaluation of scale process in a TIFCC*

A TIFCC needs to share intelligence effectively, to do this it needs to have:

- A language architecture for intelligence information
- A protocol for transporting the information
- A data-store of indicators of compromise

MILE (IODEF, IODEF-SCI and RID) and Mitre (Cybox, TAXII and STIX) standout as the threat intelligence frameworks that possess these characteristics.



Threat Intelligence for Cloud Computing	Open IOC	VERIS	CybOX	IODEF	TAXII	STIX	TLP	OTX	CIF
Sharing									
Machine readable	X		X	X	X	X			X
Supports automation	X		X	X	X	X		X	X
Secure transport protocol				X					
Separate transport schema			X	X	X	X			
Data Visulaization	X		X		X	X			
Source and Subscriber	X			X	X			X	
Hub and Spoke		X		X	X		X		X
Peer 2 Peer				X	X		X		X

Table 5: *Evaluation of sharing process in a TIFCC*

Table 5 identifies the sharing processes required in an effective TIFCC. Intelligence sharing will be an ongoing challenge for TIFCC's, exacerbated by legal, trust and competitive worries that will continue to impede the sharing process between organizations (6). Despite this, sharing is fundamental to an effective TIFCC and will be required for intelligence sharing between ISACs, sharing communities, commercial threat intelligence and Security as a Service (SaaS) products.

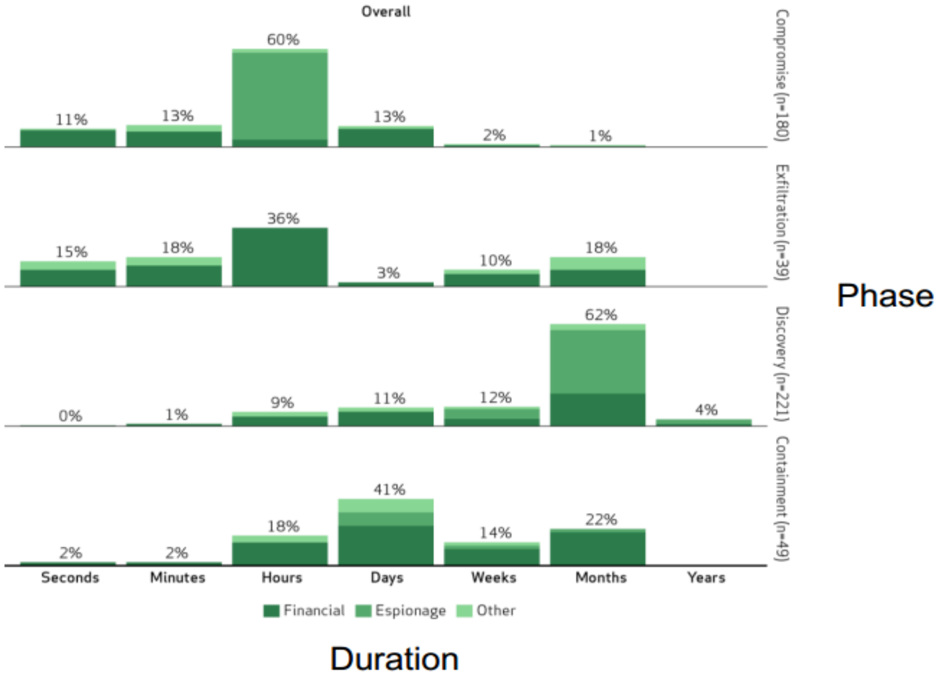


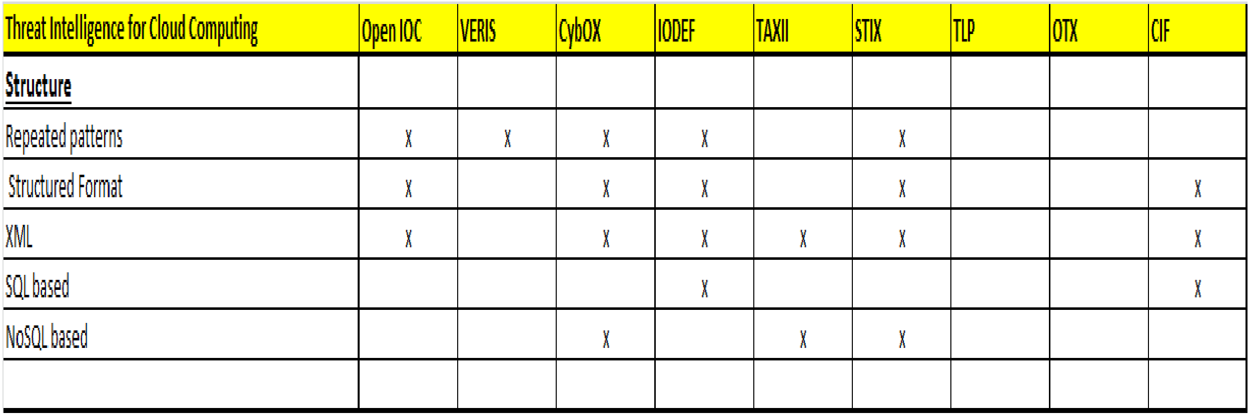
Figure 17: *Demonstrates "Breaches happen quickly but are discovered slowly" (61)*

Appendix 5 shows a visualization of the scale of the world's biggest data breaches in the last two years. This speed and scale demonstrates that cloud computing expands the threat footprint with increased volume and velocity of logs and alerts emanating from cloud sensor networks. To be effective a TIFCC will need to parse and normalize this data and create actionable intelligence as fast as possible to reduce the duration taken to discover and mitigate cloud computing threats.

Threat Intelligence for Cloud Computing	Open IOC	VERIS	CybOX	IODEF	TAXII	STIX	TLP	OTX	CIF
Speed									
Realtime Components				X		X		X	X
Live feeds				X		X		X	X
Machine readable	X		X	X	X	X			X
Supports automation	X		X	X	X	X		X	X

Table 6: *Evaluation of Speed process in a TIFCC*

Of course the inherent challenge is that *"information is not always timely enough or in a format that can be translated quickly into a machine-readable state for security tools"* (6). As the machine-to-machine vector becomes increasingly critical for real-time intelligence sharing so too will it become a vector for new attacks. The two frameworks that stand out in terms of real-time components are the MILE and MITRE frameworks which support automation and enable intelligence to be machine readable. The importance of real-time components in a TIFCC is demonstrated by data from 2013 that showed the median time an attacker was present on a victim network was 243 days, despite this being a 40% reduction from 416 days in 2011 it still demonstrates that data needs to be converted to intelligence and actioned as quickly as possible to further reduce this median (6). Appendix 6 demonstrates the data, information, knowledge, wisdom hierarchy in the context of threat intelligence operations (62).



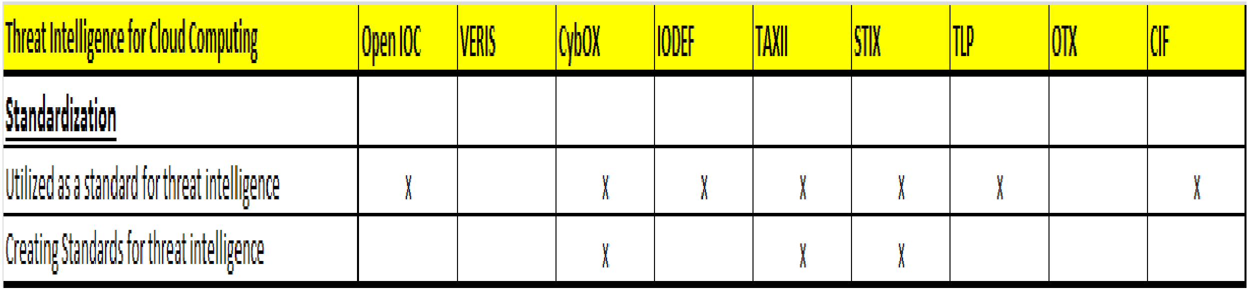
Threat Intelligence for Cloud Computing	Open IOC	VERIS	CybOX	IODEF	TAXII	STIX	TLP	OTX	CIF
Structure									
Repeated patterns	X	X	X	X		X			
Structured Format	X		X	X		X			X
XML	X		X	X	X	X			X
SQL based				X					X
NoSQL based			X		X	X			

Table 7: *Evaluation of structure process in a TIFCC*

Almost 50% of organizations share intelligence IP addresses, file hashes, URLs, and email addresses used in attacks in an unstructured format via email, phone, or in-person meetings (63). Human language and free text methods used for manual communication of threat intelligence such as that used in the TLP protocol do not scale and will not be effective for a TIFCC. All of the frameworks examined with the exception of TLP use a structured language for intelligence exchange e.g. XML, Python, JSON and R.

TIFCCs will need data stores capable of scaling to meet the volume and variety of threat intelligence. STIX use of Mongo DB demonstrates its positioning to meet the data analytics requirement of a TIFCC. Frameworks such as CIF are inherently positioned as host based tools to pull data into IPS/IDS and SIEM systems but lack the data storage capability to be an effective TIFCC. Veris with its bespoke Veris Community Database (VCDB) is designed to support a strategic threat intelligence framework and cannot scale to meet the volume requirements of a tactical TIFCC. To meet the structured and unstructured data analytics requirements of threat intelligence for cloud computing a TIFCC will need to utilize NoSQL data-stores where a SOC can leverage Hadoop, Map Reduce and data access libraries such as Pig, Hive and Mahout to develop analytics and methods to impact the tactics, techniques and procedures of attackers. This data science and analytics will enable a SOC to do:

- Data modelling, analysis and validation (false positives, bias)
- Application and modelling to present the data attributes, parameters and constraints of Threat Intelligence
- Development of Intelligence Metrics
- Statistical Modelling (validation of accuracy, data normalization)



Threat Intelligence for Cloud Computing	Open IOC	VERIS	CybOX	IODEF	TAXII	STIX	TLP	OTX	CIF
Standardization									
Utilized as a standard for threat intelligence	X		X	X	X	X	X		X
Creating Standards for threat intelligence			X		X	X			

Table 8: *Evaluation of standardization process in a TIFCC*

Underpinning an effective TIFCC is standardization; this critical process enables machine readability to achieve faster, real-time and standardized exchange of threat intelligence. There are various standards for structured descriptions of threat information and Appendix 7 contains a comprehensive list of these Threat Intelligence Standards. As we have seen IODEF-SCI embeds XMLs of CVE and OVAL identifiers and is illustrated in figure 18. IODEF, MILE and MITRE packages are the threat intelligence frameworks that demonstrate effective use of standards that can support a TIFCC.

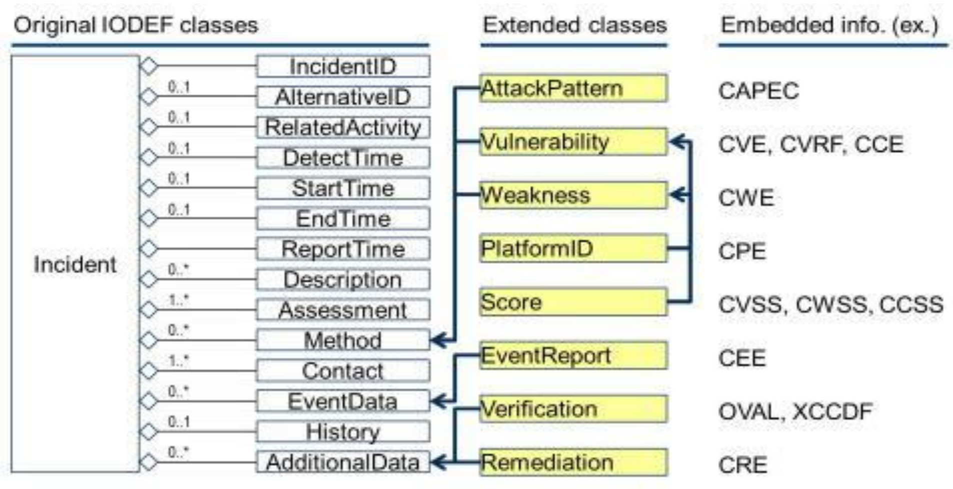


Figure 18: *IODEF Classes and embedded standards (64)*

Bringing it all together

A TIFCC needs to enable security operations centres and computer incident response teams to proactively protect organizational assets in the core cloud security domains of Information Management and Data Security, Identity and Access Management, Application Security, Virtualization and Incident Response, Notification and Remediation.

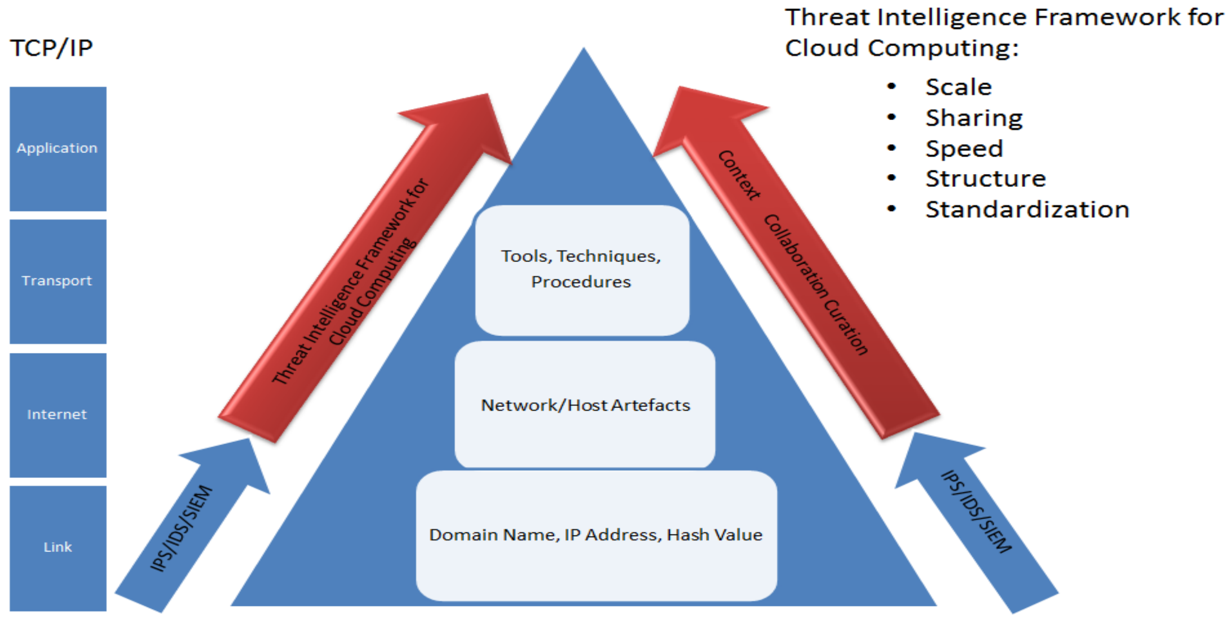

TCP/IP
Application
Transport
Internet
Link
IPS/IDS/SIEM
Threat Intelligence Framework for Cloud Computing
Tools, Techniques, Procedures
Network/Host Artefacts
Domain Name, IP Address, Hash Value
Context Collaboration Curation
IPS/IDS/SIEM
Threat Intelligence Framework for Cloud Computing:
Scale
Sharing
Speed
Structure
Standardization

Figure 19: *TCP/IP Stack, Pyramid of Pain, Cyber Threat Detection, Prevention and Response Technologies and Threat Intelligence Frameworks for Cloud Computing*

The effectiveness of cyber threat detection, prevention and response technologies differ at the various levels of the TCP/IP stack and the Pyramid of Pain. To affect the behaviour of threat actors and attackers, CTI frameworks and a TIFCC framework need to efficiently exchange data and intelligence feeds and have the capability to identify and impact the tactics, techniques and procedures of attackers.

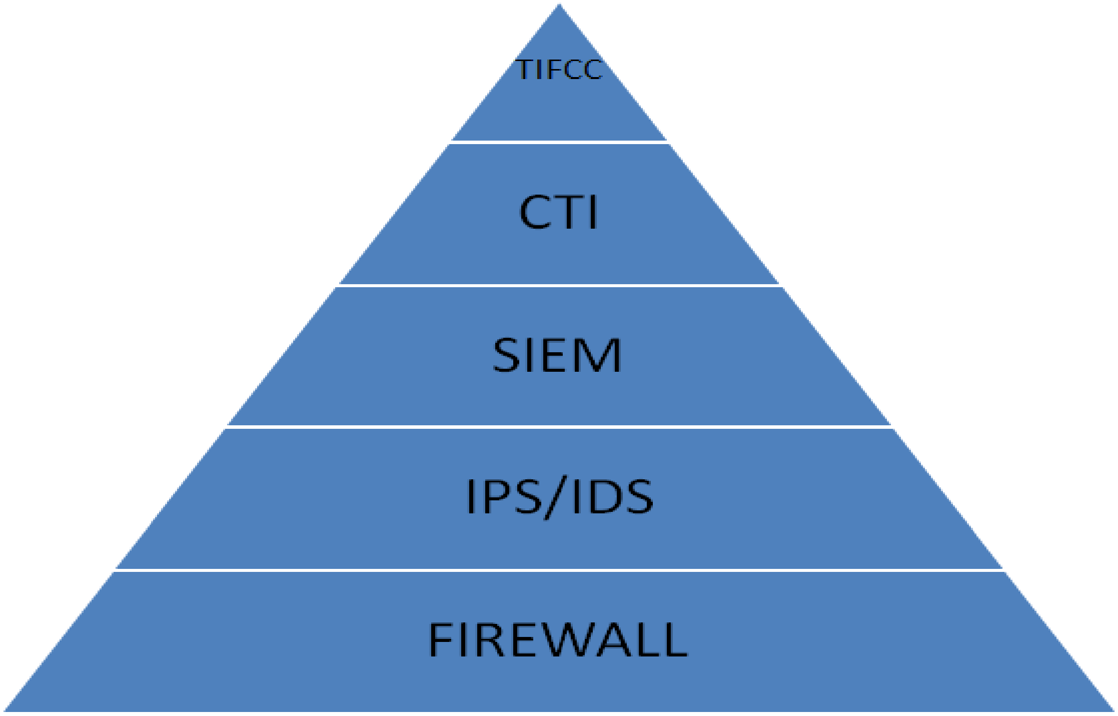


Figure 20: *Cloud Computing Security Intelligence Pyramid*

TIFCC sits at the highest layer of a cloud computing security intelligence pyramid. Firewalls do the blocking and tackling with “allow or block” rules based on signatures in the firewall tables , IPS and IDS sits behind the firewall doing packet inspection while SIEM, in turn, sits at a higher level in the network logging, correlating and distilling data and initiating the conversion of network data to threat intelligence. The value of the intelligence is then concentrated by core CTI processes that are fed by SIEM, sensor networks and threat feeds. TIFCC is then deployed at the highest level to automate the exchange of intelligence and protect assets in core cloud security domains.

This research paper has demonstrated that Web 2.0 and Enterprise 2.0 have opened up the application layer of the TCP/IP stack as a critical threat vector for cloud computing. It is an area of weakness in traditional security technologies and a key area where a TIFCC needs to develop IOCs and standard enumerations of application layer vulnerabilities. The ten most critical web application security risks in 2013 have been identified as (65) (61):

1. Injection
2. Broken Authentication and Session Management
3. Cross-Site Scripting
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery
9. Using Known Vulnerable Components
10. Un-validated Redirects and Forwards

These risks are accentuated by the evasion techniques of Web 2.0 applications such as port hopping, tunnelling and use of non-standard ports and Enterprise 2.0's move to the application layer, through trends such "bring-your-own-device" (BYOD), is causing further risk of data loss, leakage and noncompliance.

The network is fundamental to standard network computing and cloud computing alike. A TIFCC will need to deliver effective network indicators of compromise and host based intelligence also. A SOC will rely on a TIFCC to deliver effective intelligence that is derived from network artefacts such as communication time stamps and intervals, parallel or simultaneous network events, correlation between IP address, DNS servers and domain names. A SOC will equally need a TIFCC to deliver host based intelligence such as that delivered by the Collective Intelligence framework with session data that provides information about when the host communication happened, what ports were used, the packet information and the services and applications that were used.

The conclusion to be drawn is that the network and host artefacts may remain largely the same for a CTI and TIFCC but it is the elastic characteristic of cloud computing that requires a TIFCC to be more scalable, faster and contextual than standard cyber threat intelligence frameworks.

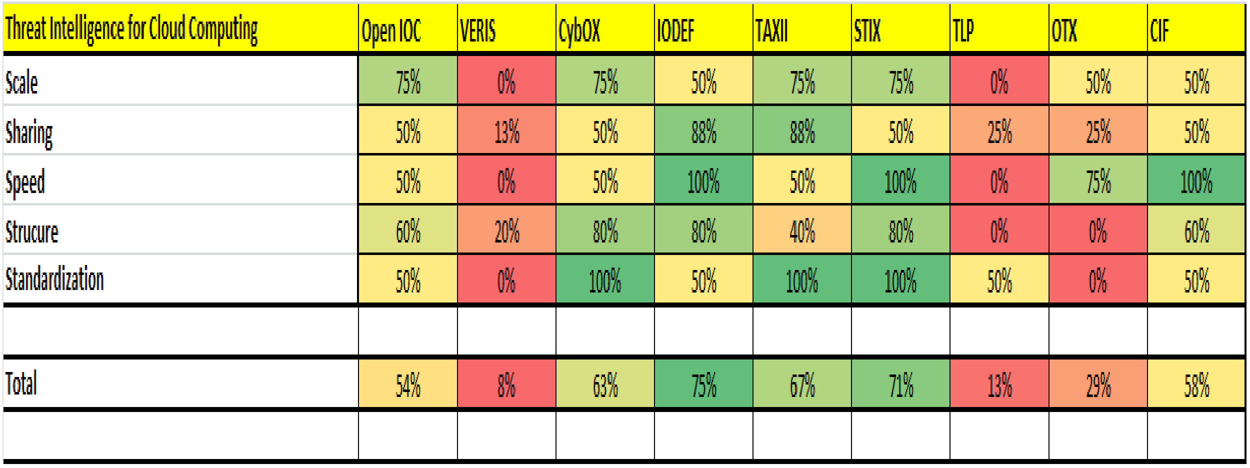
Virtualization is a core cloud security domain and cloud computing characteristic that presents additional forensic challenges for a TIFCC. Protecting the traditional network perimeter with firewalls and the concept of "perimeterization"(66) have become too one dimensional, as threat vectors, applications and business models have developed and the challenge of finding malicious traffic now involve virtual machine migration and management, inter-host communications and hypervisor security. For a TIFCC to be fully effective an organization will have to control the policies relating to VM instantiation, orchestration and log viewing and all other policies associated a cloud computing environment. The Open Security Architecture's (OSA) Cloud Computing Pattern (67) provides controls for security services, provisioning and configuration management, infrastructure, monitoring, logging, load and performance testing, platforms, applications, cloud architects and business management. The policies of the Cloud Computing Pattern should be implemented as part of a TIFCC deployment in a virtualized or cloud environment.

It is important to remember that threat intelligence is about contextualizing the artefacts of malicious activity to ultimately change the TTPs of attackers. TIFCC will not be a panacea for all security risks and threats; for example it will not in itself be able to combat Dynamic DNS techniques such as Fast Flux. It will though, through use of standard language, vulnerability libraries and real-time processing of threat intelligence, enable faster median and meantime discovery of malicious activity on a cloud network.

TIFCC is an element in the overall security posture of an organization that has a SaaS, PaaS or IaaS cloud service model. Traditional and existing network security devices such as firewalls, IPS/IDS protect the perimeter against known signatures, while SIEM bridges the gap to provide log and system information to develop a body of data to enable threat intelligence frameworks to establish the context of events and if any artefacts map to established standards for vulnerabilities and threats. It is from this point that the CSIRTs and SOCs can add value from a human intelligence perspective using data science and analytics to take remediation or pre-emptive steps to disrupt the tactics, techniques and procedures used by attackers.

One significant continuing challenge is that threat intelligence, in general, is prone to vague and unclear definition. Intelligence is frequently used as a misnomer for data and, though data plays a key part as the initial feed into the threat intelligence cycle, poor and probably deliberate misuse of *intelligence* as a marketing term by commercial security vendors impedes the development of threat intelligence as a defined discipline. For the uninitiated, cloud computing is a difficult model to conceptualize and adding threat intelligence to that computing model can be a further challenge for individuals to comprehend.

The core cyber threat intelligence framework (CTI) processes and the core threat intelligence framework for cloud computing (TIFCC) processes that have been presented in this paper demonstrate that there are specific processes that constitute the discipline of threat intelligence for both conventional computing and cloud computing. At this time, no single framework presently delivers all the relevant core TIFCC processes.



Threat Intelligence for Cloud Computing	Open IOC	VERIS	CybOX	IODEF	TAXII	STIX	TLP	OTX	CIF
Scale	75%	0%	75%	50%	75%	75%	0%	50%	50%
Sharing	50%	13%	50%	88%	88%	50%	25%	25%	50%
Speed	50%	0%	50%	100%	50%	100%	0%	75%	100%
Strucure	60%	20%	80%	80%	40%	80%	0%	0%	60%
Standardization	50%	0%	100%	50%	100%	100%	50%	0%	50%
Total	54%	8%	63%	75%	67%	71%	13%	29%	58%

Figure 21: *Effectiveness of current Cyber Threat Intelligence (CTI) frameworks as Threat Intelligence Frameworks for Cloud Computing (TIFCC)*

The key process that will enable TIFCC to make advances will be standardization. That will enable SOCs and CSIRTs to have common language, architecture and enumeration of threats and vulnerabilities and to enable threat actor behaviour to be automatically identified and mitigated as quickly as possible. The combined Mitre package of STIX, Cybox and TAXII standout as the most developed Threat Intelligence Framework for Cloud Computing at this time.

The future for TIFCC is dependent on a number of factors:

- Continued Open Source development of CTI frameworks but using common standards for threat, weakness and vulnerabilities
- The development of TIFCC as a Security as a Service (SECaaS) certainly for small and medium enterprises who do not have the resources to manage the volume of threat intelligence and require a service provider to provide correlation, behaviour analysis and intelligence on tactics, techniques and procedures.
- Broad and significant adoption of a single framework, or reduced number of frameworks, and standards to support TIFCC as a specific discipline. Microsoft's adoption of STIX into its Azure incident responders cloud platform (63) is a positive indicator toward the industry centring on a preferred framework and set of standards.
- Continued academic, industry, ISAC and government organization research into CTI and TIFCC. Such as the list of almost seventy different types of information sharing standards, transport and serialization and information management tools for exchange and processing of actionable information published by the European Agency for Network and Information Security (68).
- CTI and TIFCC are focussed on the highest level of the Cloud Computing Security Intelligence Pyramid and need to provide actionable intelligence against the most significant cyber threats such as Advanced Persistent Threats. The inherent geo-political nature of APTs in locations such as China (6) point to a continued challenge for the adoption of a global TIFCC framework and the continued disparate development of frameworks on a regional basis i.e. US, European, Russian and Chinese.

Chapter 8 – Conclusion

Organizations need to detect, prevent and respond to threats using traditional network security technology. Organizations also need to ensure the confidentiality, integrity and availability of their assets with effective tactical and strategic threat intelligence. Cloud Computing has introduced new computing service and deployment models that require existing security technologies and approaches to adapt to this new distributed computing model.

This research paper has found that the area of cyber threat intelligence is still developing. Many organizations utilize cyber threat intelligence as simply data feeds to their existing IPS/IDS systems. The relative immaturity of cyber threat intelligence frameworks correlates to emergence of Advanced Persistent Threats as critical challenges for organizations; it also correlates to the emergence of the application layer as a key area of threats for organizations using a cloud computing model.

Cyber Threat Intelligence frameworks and Threat Intelligence Frameworks for Cloud Computing have different core processes and attributes but there is no defined single standard at this time. This research has defined three core processes of collaboration, context and curation as a requirement for an effective cyber threat intelligence framework. Cloud Computing presents specific requirements for a threat intelligence framework in the areas of Information Management and Data Security, Identity and Access Management, Application Security, Virtualization and Incident Response, Notification and Remediation. This research paper presents five core processes of Scale, Sharing, Speed, Structure and Standardization as a requirement for an effective threat intelligence framework for cloud computing.

Big data variables of volume, variety and velocity, driven by expansion of sensor networks through trends such as the Internet of Things, will multiply the data footprint that threat intelligence frameworks need to manage. Big Data technologies such as NoSQL and the Hadoop ecosystem will have to be a part of an effective TIFCC.

TIFCC is part of the overall security of an organization's cloud computing deployment and sits at the top of the Cloud Computing Security Intelligence Pyramid, best placed of all security technologies to mitigate threats that are inherent to cloud computing such as distributed denial of service and advanced persistent threats.

To look at CTI and TIFCC in the context of Tuckman's "Storming, Norming and Performing" developmental process (69), the emergence of a preferred TIFCC and integrated standards may represent the "norming" phase of development for CTI and TIFCC where ISACs, governments, open source developers, and security industry providers settle on a standard architecture for sharing threat intelligence. Sharing underpins all aspects of effective threat intelligence and the degree to which these players can trust each other, collaborate on and implement an agreed framework and standards will determine how effective a Threat Intelligence Framework for Cloud Computing will perform into the future.

Bibliography

1 Mell, P., and Grance, T., (2011) “The NIST Definition of Cloud Computing” USA, National Institute of Standards and Technology [Online] available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

2 Definition of Information Security, SANS Institute [Online] available at http://www.sans.org/information-security/

3 Srinivasan, A., (2014),”Cloud Computing”, India, Dorling Kindersley

4 Winkler, V., (2011), “Securing the Cloud”, USA, Syngress

5 Elisan, C., (2012) “Malware, Rootkits & Botnets: A Beginner’s Guide”, USA, McGraw Hill

6 Mandiant.com, (2013) “M-Trends 2013 Threat Report”, [Online] available at https://www.mandiant.com/resources/mandiant-reports

7 Bejtlich, R., (2010) “Understanding the Advanced Persistent Threat” [Online] available at http://searchsecurity.techtarget.com/magazineContent/Understanding-the-advanced-persistent-threat

8 Prowell, S., Kraus, R., Borkin, M., (2010) “Seven Deadliest Network Attacks”, USA, Syngress

9 Barnum, S., (2012), “Standardizing Cyber Threat Intelligence with Structured Threat Information eXpression (STIX)” USA, Mitre Corporation [Online] available at https://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0_(Draft).pdf

10 Mateski, M., Trevino, C., Veitch, C., Michalski, J., Harris, M., Marouka, Scott., Frye, J., (2012) “Cyber Threat Metrics”, USA, Sandia National Laboratories [Online] available at http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-065.pdf

11 Mandiant.com, (2014) “M-Trends 2014 Threat Report”, [Online] available at https://www.mandiant.com/resources/mandiant-reports

12 Talabis, M. and Martin, J. (2012) “Information Security Risk Assessment Toolkit”, USA, Syngress

13 Gibson, D., (2011), “Security +, Get Certified Get Ahead”, USA, CreateSpace

14 Sequeira, A., (2012) “ CCNP Security Firewall 642-618 Quick Reference”, USA , Cisco Press

15 Kozierok, C., (2005), “TCP/IP Guide”, USA, No Starch Press

16 Young, G. and Pescatore, J. (2012) “Magic Quadrant for Intrusion Prevention Systems”, USA, Gartner

17 Piper, S., (2011) “Intrusion Prevention Systems for Dummies”, USA, Wiley Publishing Inc.

18 Young, G. and Pescatore, J. (2011) “Defining Next Generation Intrusion Prevention Systems”, USA, Gartner

19 Pfleeger, C., Pfleeger, S., Margulies, J., (2015) “Security in Computing, 5th edition” USA, Pearson Education

20 Vacca, J., (2013) “Network and System Security, 2nd Edition”, USA, Syngress

21 Chuvakin, A., (2014) “On Broad Types of Threat Intelligence” [Online] available at http://blogs.gartner.com/anton-chuvakin/2014/01/30/on-broad-types-of-threat-intelligence/

22 Sanders, C. and Smith, J., (2013) “Applied Network Security Monitoring”, USA, Syngress

23 Goldfarb, J., (2014, July) “How to Source Cyber Threat Intelligence” [Online] available at

http://www.computerweekly.com/opinion/How-to-source-cyber-threat-intelligence

24 Farnham, G., (2013) “Tools and Standards for Cyber Threat Intelligence Projects”, SANS Institute

25 Theron, P., Bologna, S., (2013) “Critical Information Infrastructure Protection and Resilience in the ICT Sector”, USA, IGI Global

26 Ouzounis, V., (2009) “Good Practice Guide Network Security Information Exchanges”, European Network and Information Security Agency

27 Chuvakin, A., (2014) “On Threat Intelligence Use Cases” [Online] available at http://blogs.gartner.com/anton-chuvakin/2014/02/04/on-threat-intelligence-use-cases/

28 Bianco, D., (2013) “The Pyramid of Pain” [Online] available at http://detect-respond.blogspot.co.uk/2013/03/the-pyramid-of-pain.html

29 Heartbleed CVE-2014-0160 [Online] available at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

30 Nolan, C., Wilson, A., (2014) “The Audacity to Spy”, USA, Technics Publications

31 “The Heartbleed Bug”, [Online] available at http://heartbleed.com/

32 Netcraft, “April 2014 Web Server Survey”, [Online] available at http://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html

33 HackLabs, “Testing for the TLS Heartbleed Vulnerability” [Online] available at http://www.hacklabs.com/team-penetration-testing/2014/4/8/testing-for-the-tls-heartbleed-vulnerability.html

34 Elisyan, O., Zavodchik, M., (2014) “Threat Intelligence Shellshock” [Online] available at https://f5.com/Portals/1/PDF/Reports/shellshock-threat-intelligence-report.pdf

35 Worley, C., (2015) "Protect yourself by Protecting Others" [Online] available at http://www.darkreading.com/partner-perspectives/intel/protect-yourself-by-protecting-others/a/d-id/1318725

36 Wilson, J., et al, (2014, June) "Using Big Data Analytics to Amplify Security Intelligence" [Online] available at https://www.youtube.com/watch?v=cIGdM36OsRw

37 Gartner IT Glossary [Online] available at http://www.gartner.com/it-glossary/consumerization

38 Gourley, D., et al, (2002) "HTTP – A Definitive Guide", USA, O'Reilly Media

39 Kendrick, R., (2010) "Cyber Risks for Business Professionals", USA, IT Governance Ltd

40 Simmonds, P., et al (2011) "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0" USA, Cloud Security Alliance [Online] available at https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

41 Los, R., Et al (2013) "The Notorious Nine: Cloud Computing Top Threats in 2013", USA, Cloud Security Alliance [Online] available at http://www.cloudsecurityalliance.org/topthreats

42 Open IOC, "An Open Framework for Sharing Threat Intelligence" [Online] available at http://www.openioc.org/

43 Wilson, D. and Gibb, w., (2012) "Fresh Prints of Malware – IOCing Red" [Online] available at https://dl.mandiant.com/EE/assets/FP_041912_Final.pdf

44 VERIS Overview [Online] available at http://veriscommunity.net/veris-overview.html

45 Cyber Observable eXpression, A Structured Language for Cyber Observables [Online] available at https://cybox.mitre.org/

46 Danyliw, R., Meijer, J., Demchenko, Y., (2007) "RFC 5070 The Incident Object Description Exchange Format" [Online] available at https://tools.ietf.org/html/rfc5070

47 Common Vulnerabilities and Exposures, "The Standard for Information Security Vulnerability Names" [Online] available at https://cve.mitre.org/

48 Takahashi, T., et al (2014) "An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information", RFC 7203 [Online] available at https://tools.ietf.org/html/rfc7203

49 Moriarty, K., (2012) "RFC 6545 Real-Time Inter-Network Defence (RID)" [Online] available at https://tools.ietf.org/html/rfc6545

50 Traffic Light Protocol (TLP) Matrix [Online] available at https://www.us-cert.gov/tlp

51 Collective Intelligence Framework [Online] available at https://code.google.com/p/collective-intelligence-framework/wiki/WhatisCIF

52 Reese, G., (2009) “Cloud Application Architectures” USA, O’Reilly Media

53 Higgins, K., (2014) “Intelligence-Sharing Suffers Growing Pains” [Online] available at http://www.darkreading.com/analytics/intelligence-sharing-suffers-growing-pains/d/d-id/1234823

54 Mitre Corporation, (2013) “TAXII: An Overview” [Online] available at http://taxii.mitre.org/about/documents/TAXII_Overview_briefing_July_2013.pdf

55 Cardenas, A., (2013) “Big Data Analytics for Security Intelligence”, Cloud Security Alliance [Online] available at https://cloudsecurityalliance.org/download/big-data-analytics-for-security-intelligence/

56 Harrington, C., (2013) “Sharing Indicators of Compromise: An Overview of Standards and Formats” [Online] available at https://www.rsaconference.com/writable/presentations/file_upload/dsp-w25a.pdf

57 Martin, R., (2008) “Making Security Measurable and Manageable” USA, Mitre Corporation [Online] available at https://buildsecurityin.us-cert.gov/sites/default/files/publications/Making_Security_Measurable_and_Manageable_White%20Paper.pdf

58 Mitre Corporation, “Making Security Measurable, A collection of Information Security Standardization Activities and Initiatives” [Online] available at http://makingsecuritymeasurable.mitre.org/about/index.html

59 “Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015” [Online] available at http://www.gartner.com/newsroom/id/2905717

60 “Shellshock: All you need to know about the Bash Bug Vulnerability” (2014) [Online] available at http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability

61 Maxwell, K., (2013) “Open Source Threat Intelligence” [Online] available at

https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Open-Source-Threat-Intelligence-Kyle-Maxwell.pdf

62 Hartley, M., (2014) “Cyber Threats: Information versus Intelligence”[Online] available at http://www.darkreading.com/analytics/threat-intelligence/cyber-threats-information-vs-intelligence/a/d-id/1316851

63 Higgins, K., (2014)“Microsoft Unveils New Intelligence-Sharing Platform” [Online] available at http://www.darkreading.com/analytics/threat-intelligence/microsoft-unveils-new-intelligence-sharing-platform/d/d-id/1278781

64 NICT- Cybex Forum [Online] available at http://cybex.nict.go.jp/iodef-sci_en.html

65 Williams, J. and Wichers, D., (2013) “The Open Web Application Security Project”OWASP Top Ten 2013, The Ten most critical Web Application Security Risks” USA, OWASP Foundation [Online] available at https://www.owasp.org/index.php/Top_10_2013-Risk

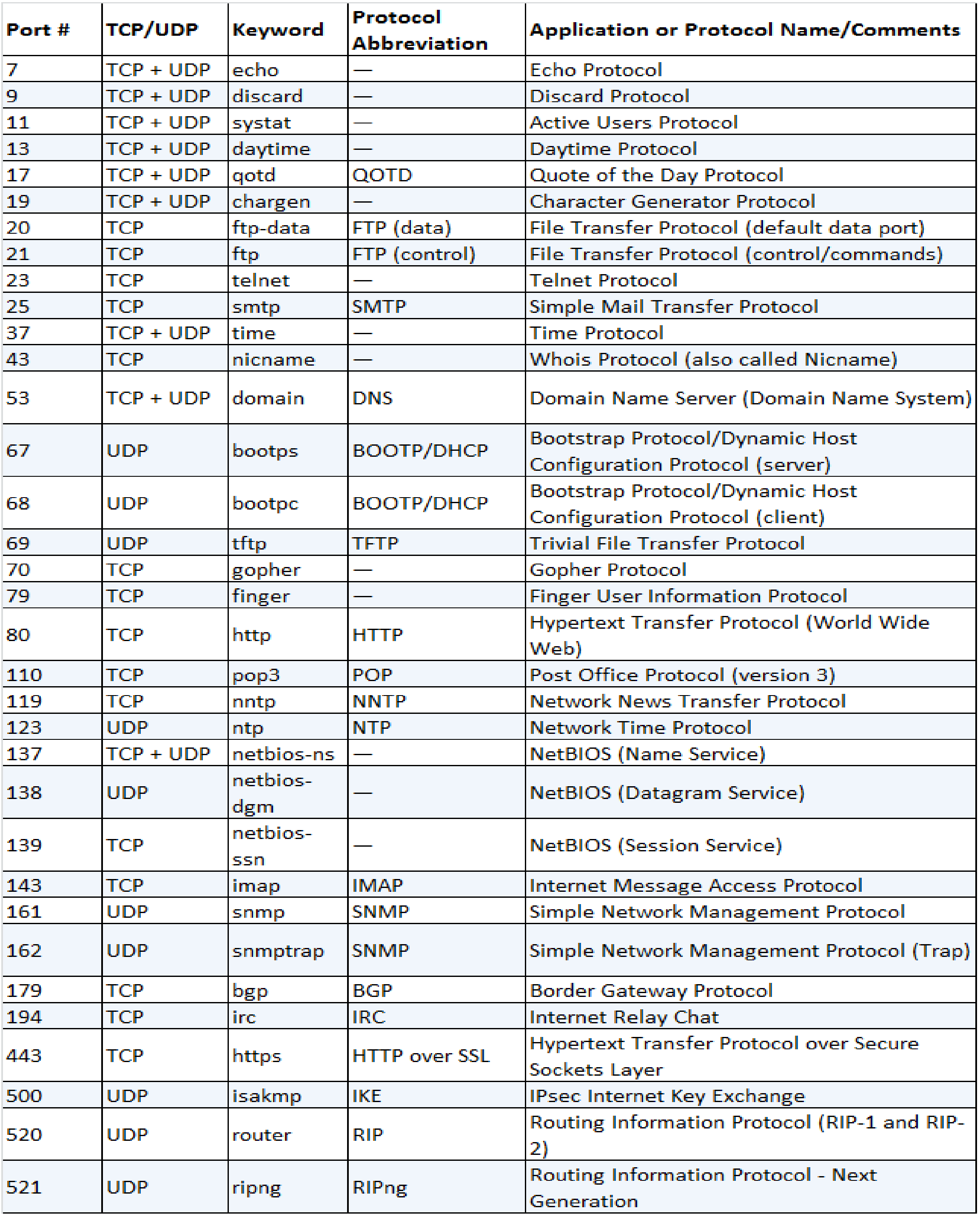
66 Dubrawsky, I., (2007) “The “De-perimeterization” of Networks”, [Online] available at https://technet.microsoft.com/en-us/library/cc512604.aspx

67 Open Security Architecture, “SP-011: Cloud Computing Pattern” [Online] available at http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing

68 Dandurand, L., Et al, (2014) “Standards and tools for exchange and processing of actionable information”, European Union Agency for Network and Information Security (ENISA)

69 Tuckman, B.W., (1965) “Developmental Sequence in Small Groups” Psychological Bulletin, 63

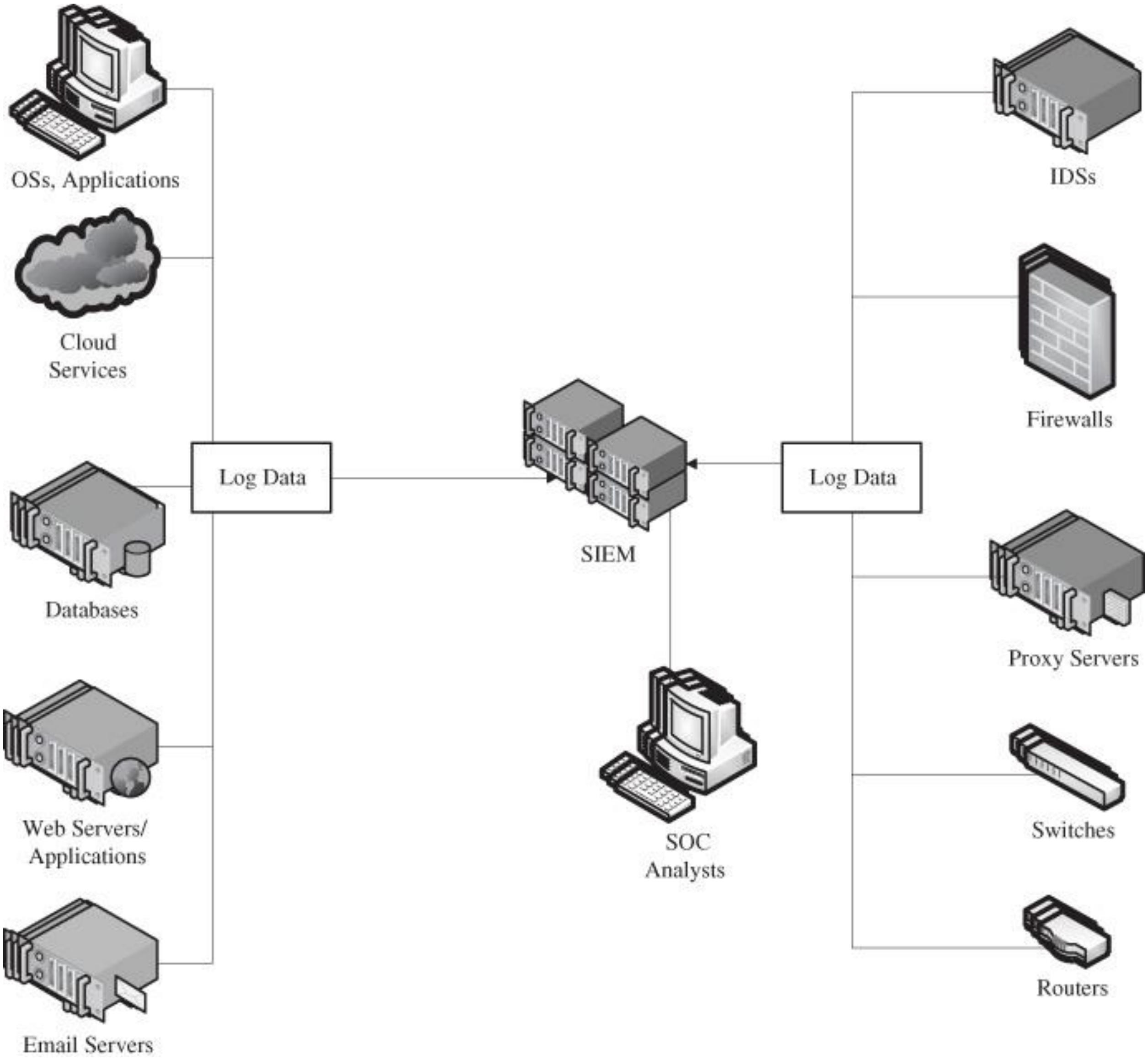
Appendix 1: Common TCP/IP Well-known port number and applications



Port #	TCP/UDP	Keyword	Protocol Abbreviation	Application or Protocol Name/Comments
7	TCP + UDP	echo	—	Echo Protocol
9	TCP + UDP	discard	—	Discard Protocol
11	TCP + UDP	systat	—	Active Users Protocol
13	TCP + UDP	daytime	—	Daytime Protocol
17	TCP + UDP	qotd	QOTD	Quote of the Day Protocol
19	TCP + UDP	chargen	—	Character Generator Protocol
20	TCP	ftp-data	FTP (data)	File Transfer Protocol (default data port)
21	TCP	ftp	FTP (control)	File Transfer Protocol (control/commands)
23	TCP	telnet	—	Telnet Protocol
25	TCP	smtp	SMTP	Simple Mail Transfer Protocol
37	TCP + UDP	time	—	Time Protocol
43	TCP	nicname	—	Whois Protocol (also called Nicname)
53	TCP + UDP	domain	DNS	Domain Name Server (Domain Name System)
67	UDP	bootps	BOOTP/DHCP	Bootstrap Protocol/Dynamic Host Configuration Protocol (server)
68	UDP	bootpc	BOOTP/DHCP	Bootstrap Protocol/Dynamic Host Configuration Protocol (client)
69	UDP	tftp	TFTP	Trivial File Transfer Protocol
70	TCP	gopher	—	Gopher Protocol
79	TCP	finger	—	Finger User Information Protocol
80	TCP	http	HTTP	Hypertext Transfer Protocol (World Wide Web)
110	TCP	pop3	POP	Post Office Protocol (version 3)
119	TCP	nntp	NNTP	Network News Transfer Protocol
123	UDP	ntp	NTP	Network Time Protocol
137	TCP + UDP	netbios-ns	—	NetBIOS (Name Service)
138	UDP	netbios-dgm	—	NetBIOS (Datagram Service)
139	TCP	netbios-ssn	—	NetBIOS (Session Service)
143	TCP	imap	IMAP	Internet Message Access Protocol
161	UDP	snmp	SNMP	Simple Network Management Protocol
162	UDP	snmptrap	SNMP	Simple Network Management Protocol (Trap)
179	TCP	bgp	BGP	Border Gateway Protocol
194	TCP	irc	IRC	Internet Relay Chat
443	TCP	https	HTTP over SSL	Hypertext Transfer Protocol over Secure Sockets Layer
500	UDP	isakmp	IKE	IPsec Internet Key Exchange
520	UDP	router	RIP	Routing Information Protocol (RIP-1 and RIP-2)
521	UDP	ripng	RIPng	Routing Information Protocol - Next Generation

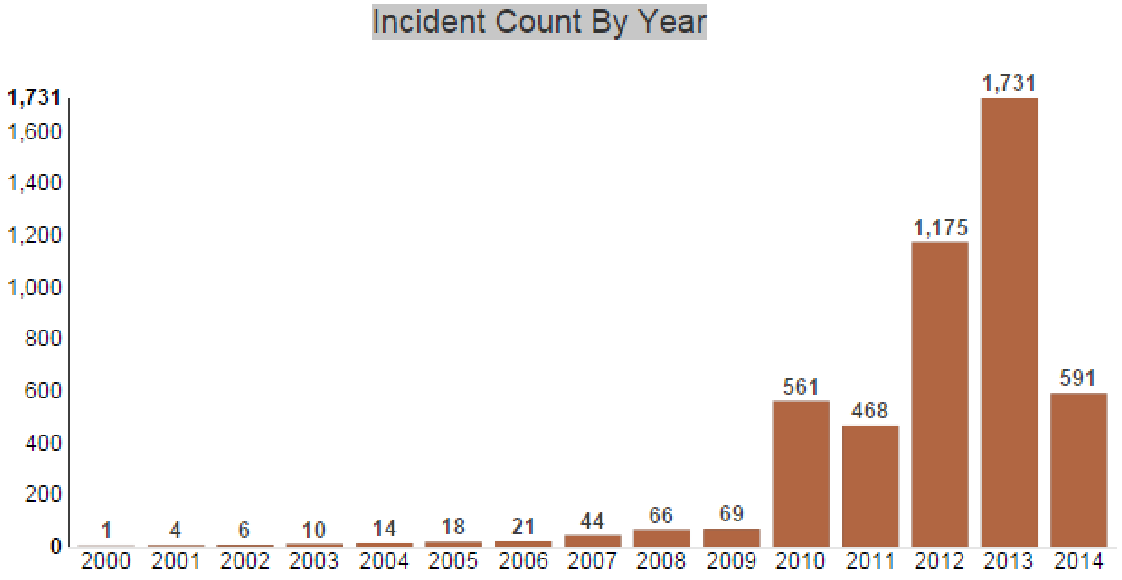
Common TCP/IP Well-known port number and applications (15)

Appendix 2: How SIEM systems are connected to the network

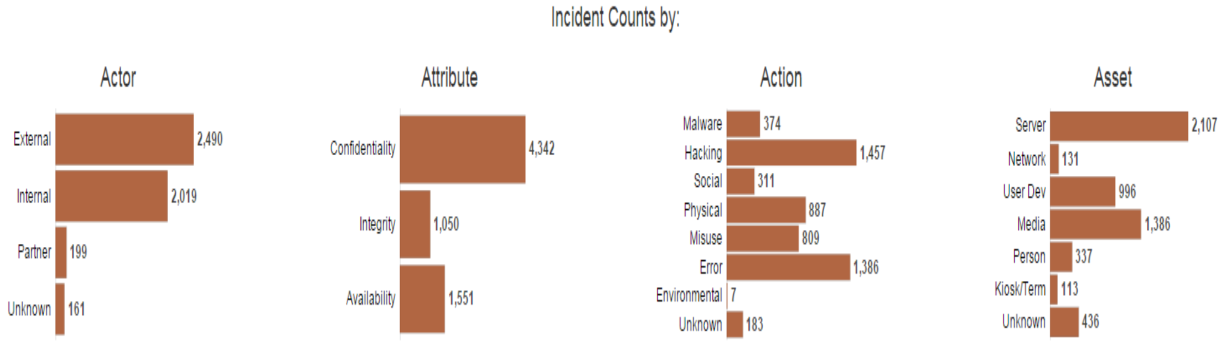


How SIEM systems are connected to the network (19)

Appendix 3: VERIS Incident Metrics

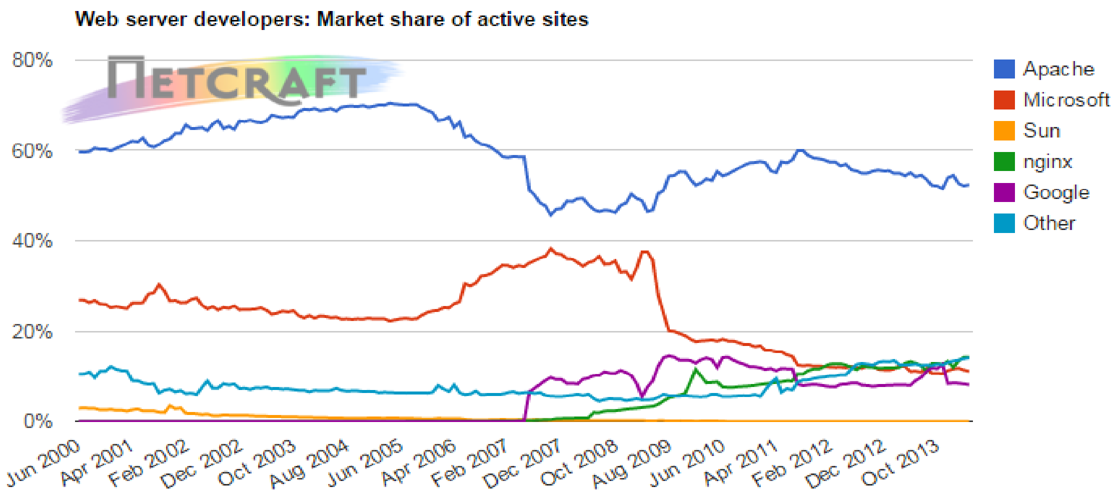


VERIS Incident Metric (44)



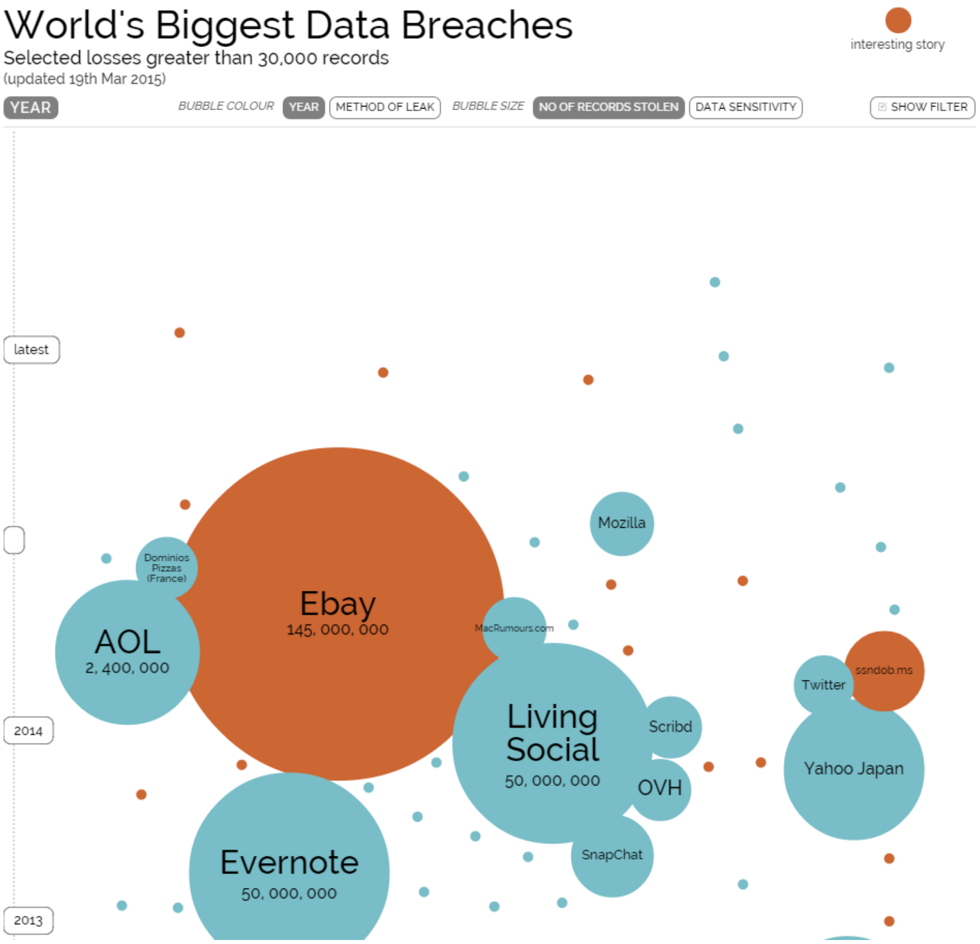
VERIS Incident Description Count with sub elements (44)

Appendix 4: Active web servers on the Internet



Active web servers on the Internet (32)

Appendix 5: World’s Biggest Data Breaches



World's Biggest Data Breaches

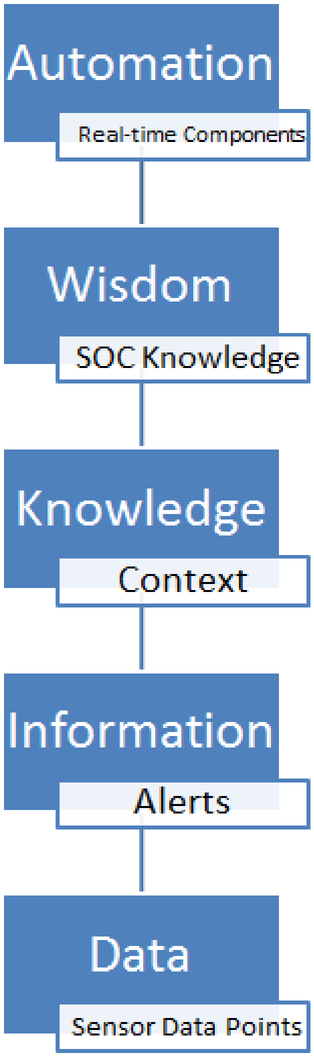
Selected losses greater than 30,000 records

(updated 19th Mar 2015)

Dynamic Data Visualization available at

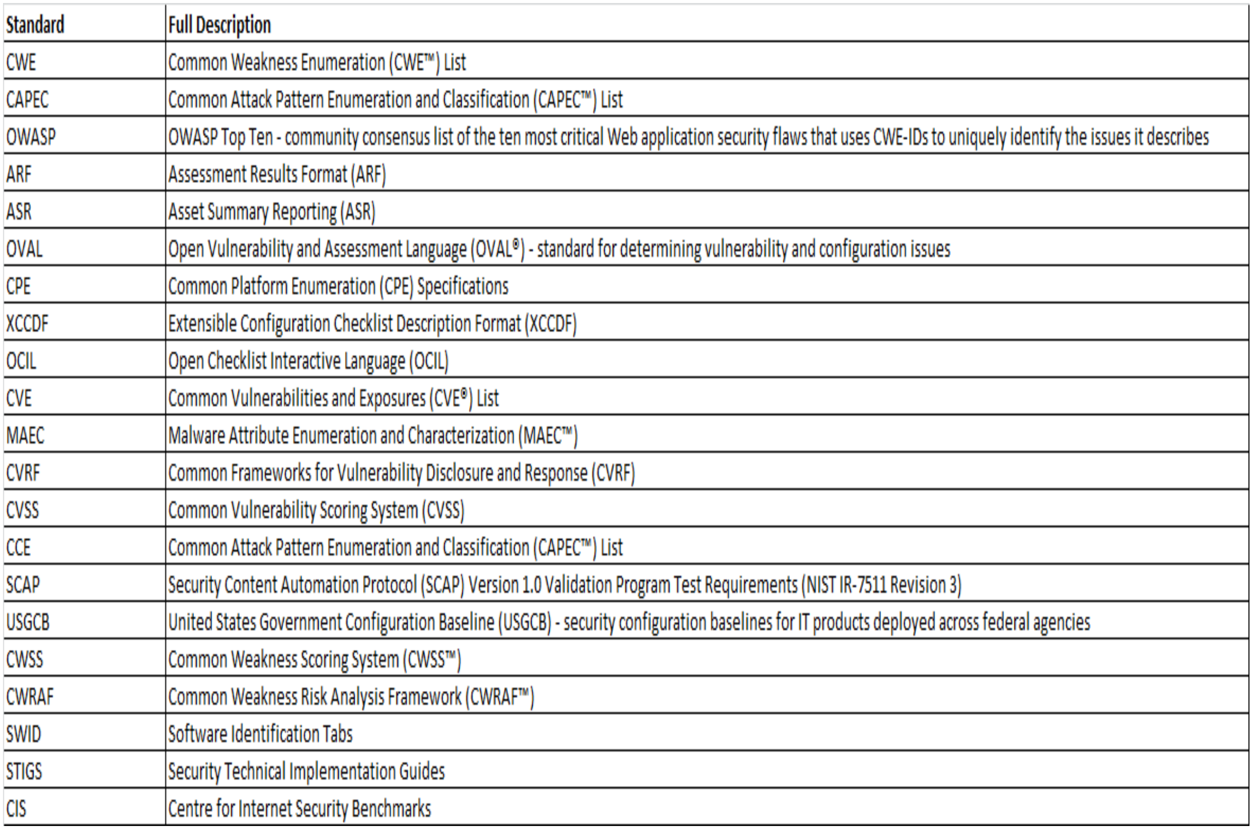
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Appendix 6: Data, Information, Knowledge, Wisdom Hierarchy for Threat Intelligence Operations



Graphical interpretation of Data, Information, Knowledge, Wisdom (DIKW) hierarchy (62)

Appendix 7: Threat Intelligence Standards



Standard	Full Description
CWE	Common Weakness Enumeration (CWE™) List
CAPEC	Common Attack Pattern Enumeration and Classification (CAPEC™) List
OWASP	OWASP Top Ten - community consensus list of the ten most critical Web application security flaws that uses CWE-IDs to uniquely identify the issues it describes
ARF	Assessment Results Format (ARF)
ASR	Asset Summary Reporting (ASR)
OVAL	Open Vulnerability and Assessment Language (OVAL®) - standard for determining vulnerability and configuration issues
CPE	Common Platform Enumeration (CPE) Specifications
XCCDF	Extensible Configuration Checklist Description Format (XCCDF)
OCIL	Open Checklist Interactive Language (OCIL)
CVE	Common Vulnerabilities and Exposures (CVE®) List
MAEC	Malware Attribute Enumeration and Characterization (MAEC™)
CVRF	Common Frameworks for Vulnerability Disclosure and Response (CVRF)
CVSS	Common Vulnerability Scoring System (CVSS)
CCE	Common Attack Pattern Enumeration and Classification (CAPEC™) List
SCAP	Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements (NIST IR-7511 Revision 3)
USGCB	United States Government Configuration Baseline (USGCB) - security configuration baselines for IT products deployed across federal agencies
CWSS	Common Weakness Scoring System (CWSS™)
CWRAF	Common Weakness Risk Analysis Framework (CWRAF™)
SWID	Software Identification Tabs
STIGS	Security Technical Implementation Guides
CIS	Centre for Internet Security Benchmarks