CMSGu2017-01

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Cyber Threat Intelligence

CERT–MU

National Computer Board
Mauritius

June 2017

Issue No. 1

Version 1.0

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to give security and business staff an insight on the collection and sharing of cyber threat information.

1.2 Audience

The targeted audience for this document includes security and business staff involved in the collection, analysis and dissemination of cyber threat information.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on sophisticated, well-funded attacks.

Section 3 explains Cyber Threat Intelligence.

Section 4 discusses the different Cyber Threat Intelligence sources.

Section 5 presents the cyber threat information sharing rules.

Section 6 concludes the document.

Section 7 comprises a list of references that have been used in this document.

2.0 Background

A decade ago, IT security professionals were primarily worried about mass attacks. Today these are regarded as secondary threats that only generate “noise” on the network. Security vendors and enterprises normally defend against them successfully by analyzing the first instances discovered and quickly disseminating signatures and indicators of compromise (IOCs). A few initial victims suffer, but almost everyone can detect and block the attacks using appropriate tools. Today, the most serious data breaches and disruptions result from well-planned, complex attacks that target specific companies or industries. Sophisticated, well-funded attackers make detection difficult by:

- Utilizing social engineering techniques and multiphase campaigns that cannot be identified by simple threat indicators or blocked by frontline defenses.
- Constantly adapting their tools, tactics, and procedures to elude even advanced cybersecurity measures.

Criminals have improved their tactics by systematically targeting their victims’ most valuable information assets and business systems.

3.0 Cyber Threat Intelligence Explained

Cyber Threat Intelligence is the collection of information about adversaries and their motivation, intentions and methods, analyzing and sharing this information with security and business staff at all levels in order to protect their critical information.

CTI can be divided into four main categories:

3.1 Adversary based

The types of intelligence we encounter in books, movies, and news reports focus on specific adversaries. Military and political intelligence activities are directed at enemies of the nation. Law enforcement and anti-terrorism intelligence programs probe criminal gangs and terrorist organizations. Sports teams scout upcoming opponents. Competitive analysts compile information on the products, pricing, and plans of rival businesses.

CTI activities are also organized around specific adversaries, especially cybercriminals, cyber espionage agents, and hacktivists. The enterprise that knows its opponents can optimize its defenses to protect against those adversaries and the attacks they employ.

3.2 Risk focused

CTI programs are based on an assessment of the information assets that the enterprise needs to protect. These assets include data, documents, and intellectual property (such as customer databases and engineering drawings), and computing resources (such as websites, applications, source code, and networks).

3.3 Process oriented

From spying, to law enforcement, to competitive analysis, all successful intelligence programs follow the same basic process (Figure 1-1).

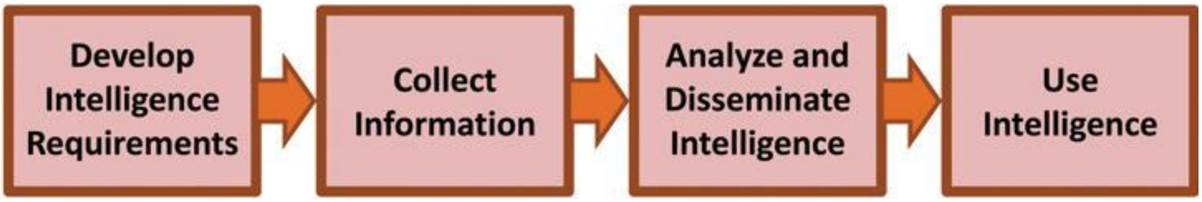
Develop Intelligence Requirements
Collect Information
Analyze and Disseminate Intelligence
Use Intelligence

Figure 1 Steps in an intelligence process

3.4 Tailored for diverse consumers

Another key characteristic of cyber threat intelligence is that it does not stop at distributing raw threat data. Data and analysis must be tailored for each type of intelligence consumer.

For example, in respect to the same alert:

- SOC analysts may want just enough context to know if the alert is worth escalating to the IR team.
- The IR team may want very detailed context to determine if the alert is related to other events observed on the network.
- The CISO might want an evaluation of the risk to the organization and a summary connecting the alert to data breaches recently reported in the press.

4.0 Cyber Threat Intelligence Sources

CTI sources can be split in to the following three categories:

4.1 Internal

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

Source	Examples
Network Data Sources	
Router, firewall, remote services (such as remote login or remote command execution), and Dynamic Host Configuration Protocol (DHCP) server logs	Timestamp Source and destination IP address TCP/UDP port numbers Media Access Control (MAC) address Hostname Action (deny/allow) Status code Other protocol information
Diagnostic and monitoring tools (network intrusion detection and prevention system, packet capture & protocol analysis)	Timestamp IP address, port, and other protocol information Packet payloads Application--specific information Type of attack (e.g., SQL injection, buffer overflow) Targeted vulnerability Attack status (success/fail/blocked)

Host Data Sources	
Operating system and application configuration settings, states, and logs	Bound and established network connections and ports Processes and threads Registry settings Configuration file entries Software version and patch level information Hardware information User and groups File attributes (e.g., name, hash value, permissions, timestamp, size) File access System events (e.g., startup, shutdown, failures) Command history
Antivirus products	Hostname IP address MAC address Malware name Malware type (e.g., virus, hacking tool, spyware, remote access) File name File location (i.e., path) File hash Action taken (e.g., quarantine, clean, rename, delete)
Web browsers	Browser histories and caches including: • Sites visited • Objects downloaded • Objects uploaded • Extensions installed or enabled • Cookies

Other Data Sources	
Security Information and Event Management (SIEM)	Summary reports synthesized from a variety of data sources (e.g., operating system, application, and network logs)
Email systems	Email messages: Email header content • Sender/recipient email address • Subject line • Routing information Attachments URLs Embedded graphics
Help desk ticketing systems, incident management/tracking system, and people from within the organization	Analysis reports and observations regarding: • TTPs • Campaigns • Affiliations • Motives • Exploit code and tools • Response and mitigation strategies • Recommended courses of action User screen captures (e.g., error messages or dialog boxes)
Forensic toolkits and dynamic and/or virtual execution environments	Malware samples System artifacts (network, file system, memory)

Table 1 Selected Internal Information Sources

4.2 Community

The community category includes any CTI shared via a trusted relationship with multiple members with a shared interest. This can be an informal group with member organizations that are in the same industry sector or that have other common interests. There are formal community groups such as the Information Sharing and Analysis Centers (ISACs) organized under the National Council of ISACs. ISACs are formed for specific sectors such as higher education or financial services. There are over a dozen ISACs under the National Council of ISACs.

4.3 External

The external category includes CTI from sources outside an organization and not part of a community group. There are two types of external sources. The first is public sources. Public sources are available to anyone and generally there is no cost associated with access. While public feeds can be available at no cost, there can be problems. There can be possible problems with volunteered data as efforts to collect these will always have an issue with guaranteed data quality.

5.0 Cyber Threat Information Sharing Rules

5.1 Threat Information

Threat information is any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include the following:

Indicators

Indicators are technical artifacts or observables that suggest an attack is imminent or is currently underway or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message.

Tactics, techniques, and procedures (TTPs)

TTPs describe the behavior of an actor. Tactics are high-level descriptions of behavior, techniques are detailed descriptions of behavior in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor’s tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit.

Security alerts

Security alerts also known as advisories, bulletins, and vulnerability notes, are brief, usually human-readable, technical notifications regarding current vulnerabilities, exploits, and other security issues. Security alerts originate from sources such as the United States Computer Emergency Readiness Team (US-CERT), Information Sharing and Analysis Centers (ISACs), the National Vulnerability Database (NVD), Product Security Incident Response Teams (PSIRTs), commercial security service providers, and security researchers.

Threat intelligence reports

Threat intelligence reports are generally prose documents that describe TTPs, actors, types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organization. Threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Tool configurations

Tool configurations are recommendations for setting up and using tools (mechanisms) that support the automated collection, exchange, processing, analysis, and use of threat information. For example, tool configuration information could consist of instructions on how to install and use a rootkit detection and removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.

5.2 Information Sensitivity and Privacy

Many organizations handle information that, by regulation, law, or contractual obligation, requires protection. Organizations should identify and properly protect such information. An organization's legal team, privacy officers, auditors, and experts familiar with the various regulatory frameworks should be consulted when developing procedures for identifying and protecting sensitive information.

From a privacy perspective, one of the key challenges with threat information sharing is the potential for disclosure of Personally Identifiable Information (PII). Education and awareness activities are critical to ensure that individuals responsible for handling threat information understand how to recognize and safeguard PII. Internal sharing of information may result in disclosure of PII to people who, by virtue of their job functions, would not typically have routine access to such information.

An organization should have information sharing policies and procedures in place that provide guidance for the handling of PII. These policies and procedures should include steps for identifying incident data types that are likely to contain PII. Policies should describe proper safeguards for managing the privacy risks associated with sharing such data. A common practice is to focus on the exchange of indicators to the maximum extent possible. Some indicators, such as file hashes, network port numbers, registry key values, and other data elements, are largely free of PII. Where PII is identified, however, organizations should redact fields containing PII that are not relevant to investigating or addressing threats before sharing. The type and degree of protection applied should be based on the intended use of the information, the sensitivity of the information, and the intended recipient. Where practical, organizations are encouraged to use automated methods rather than human-oriented methods to identify and protect PII. Manual identification, extraction, and obfuscation of PII can be a slow, error-prone, and resource-intensive process. Automated methods may include field-level data validation using permitted values lists, searching for PII using pattern matching techniques such as regular expressions, and performing operations that de-identify, mask, and anonymize data containing PII. The degree of automation that can be achieved will vary based on factors such as the structure, complexity, and sensitivity of the information.

Organizations should also implement safeguards to protect intellectual property and other proprietary information from unauthorized disclosure. The disclosure of such information could result in financial loss, violate NDAs or other sharing agreements, be cause for legal action, or damage an organization's reputation. Organizations should have a plan in place to address the unauthorized or inadvertent disclosure of CUI. The plan should cover containment, control, and recovery procedures; breach notification requirements, and post-incident activities such as capturing lessons learned.

The table below introduces selected types of threat information, provides examples of sensitive data that may be present in these types of threat information, and offers general recommendations for handling such data.

Type of Threat Information	**Examples of Sensitive Data Elements**	**Recommendations**
Network Indicators	Any single network indicator can be sensitive, but network indicators in the aggregate are often more sensitive because they can reveal relationships between network entities. By studying these relationships it may be possible to infer the identity of users, gather information about the posture of devices,	Focus on the exchange of network indicators such as destination IP addresses associated with an actor's command and control infrastructure, malicious URLs/domains, and staging servers. Before sharing, anonymize or sanitize network indicators

	perform network reconnaissance, and characterize the security safeguards and tools that an organization uses.	that contain IP or MAC addresses of target systems or addresses registered to your organization. Also anonymize or sanitize indicators that may reveal the structure of internal networks, or ports or protocols that identify particular products.
Packet Capture (PCAP)	In addition to the network indicators previously discussed, unencrypted or decrypted packets may contain authentication credentials and sensitive organization information, such as PII, CUI or other types of sensitive information.	PCAP files can be challenging because network indicators may be present within both the packet header and the payload. For example, PCAP files may show protocols (e.g., DHCP, Address Resolution Protocol (ARP), File Transfer Protocol (FTP), DNS) and applications operating at multiple layers within the network stack. These protocols and applications generate network information that may be captured within PCAP files and may require sanitization or anonymization to prevent sensitive information leakage. Filter PCAP files before sharing by extracting only those packets that are related

		to the investigation of a specific incident or pattern of events: •Related to a particular network conversation (i.e., exchange of information between specific IP addresses of interest); •Occurring during a chosen time period; •Destined for, or originating from, a specific port; or •Use of a particular network protocol. Redact payload content that contains PII, CUI or other types of sensitive information that is not relevant for characterizing the incident or event of interest. When anonymizing or redacting network information, use a strategy that preserves enough information to support meaningful analysis of the resulting PCAP file contents.
Network Flow Data	Network flow data contains information such as: •Source IP address (i.e., thesender), •Destination IP address (i.e.,	Before sharing network flow data, organizations should consider redacting portions of session histories using cryptography-based, prefix-

	the recipient), •Port and protocol information, •Byte counts, and •Timestamps. If not effectively anonymized, network flow data may make identification of specific users possible, provide insights into user behavior (e.g., web sites visited), expose application and service usage patterns, or reveal network routing information and data volumes.	preserving, IP address anonymization techniques to prevent network identification or to conceal specific fields within the session trace (e.g., time stamps, ports, protocols, or byte counts). To gain the greatest value from the information, use a tool that transforms network flow data without breaking referential integrity. Network flow analysis and correlation operations often require that IP address replacement and transformation operations are performed consistently within and sometimes across multiple files. Anonymization techniques that do not use a consistent replacement strategy may reduce or eliminate the value of sharing this type of information.
Phishing Email Samples	Email headers may contain information such as: • Mail agent IP addresses, • Host or domain names, and • Email addresses. An email message body may also contain PII, CUI, or other types of sensitive	Organizations should anonymize email samples and remove any sensitive information that is not necessary for describing an incident or event of interest.

	information.	
System, Network, and Application Logs	Log files may contain PII, CUI or other types of sensitive information. Log data may reveal IP addresses, ports, protocols, services, and URLs, as well as connection strings, logon credentials, portions of financial transactions, or other activities captured in URL parameters.	Organizations should perform IP address, timestamp, port, and protocol anonymization and remove any sensitive information that is not necessary for describing an incident or event of interest. Before sharing log data, it may also be necessary to sanitize URLs that contain identifying information such as session or user identifiers. Application logs may require redaction and anonymizing operations that are specific to particular application log formats.
Malware Indicators and Samples	Although organizations are unlikely to encounter sensitive information in malware indicators or samples, sensitive information may be present depending on how targeted the malware is and what collection methods were used to gather a sample.	Organizations should remove PII, CUI, and other types of sensitive information that is not necessary for describing an incident or event of interest.

Table 2 Handling Recommendations for Selected Types of Sensitive Data

5.3 Sharing Designations

A variety of methods exist to designate handling requirements for shared threat information. These designations identify unclassified information that may not be suitable for public release and that may require special handling. A designation applied to threat information can communicate specific handling requirements and identify data elements that are considered sensitive and should be redacted prior to sharing. Organizations are encouraged to provide clear handling guidance for any shared threat information. Likewise, recipients of threat information should observe the handling, attribution, dissemination, and storage requirements expressed in the source organization's handling guidance.

The Traffic Light Protocol (TLP), depicted in the below table, provides a framework for expressing sharing designations.

Colour	When should it be used?	How may it be used?
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.

Table 3 Traffic Light Protocol, Version 1.0

The TLP specifies a color-coded set of restrictions that indicate which restrictions apply to a particular record. In the TLP, red specifies the most restrictive rule, with information sharable only in a particular exchange or meeting, not even within a participant's own organization. The amber, green, and white color codes specify successively relaxed restrictions.

For some threat information, collection methods may be considered confidential or proprietary, but the actual indicators observed may be shareable. In such cases, an organization may want to use *tear line reporting*, an approach where reports are organized such that information of differing sensitivity is not intermingled (e.g., the indicator information is presented in a separate part of the document than the collection methods). Organizing a report in this manner allows an organization to readily produce a report containing only information that designated recipients are authorized to receive.

An organization should carefully choose, or formulate, an approach for expressing sharing designations. Regardless of how an organization expresses sharing designations, the procedures for applying designations to threat information should be documented and approved, and the personnel responsible for assigning such designations properly trained.

5.4 Cyber Threat Information Sharing and Tracking Procedures

Over time, an organization's cybersecurity activities can result in the accumulation of large quantities of threat information from various sources, both internal and external. Though challenging, tracking of data sources is important both for protecting information owners and for ensuring that consuming organizations can meet their legal or regulatory commitments for data protection. Organizations should also preserve the provenance of data by tracking who provided the information and how the information was collected, transformed, or processed, information that is important for drawing conclusions from shared information.

An organization should formulate procedures that allow prompt sharing of threat information while at the same time satisfying its obligations for protecting potentially sensitive data. The procedures should, to the extent possible, balance the risks of possibly ineffective sharing against the risks of possibly flawed protection. An organization's information sharing and tracking procedures should:

- Identify threat information that can be readily shared with trusted parties.
- Establish processes for reviewing, sanitizing, and protecting threat information that is likely to contain sensitive information.
- Develop plan for addressing leakage of sensitive data.
- Automate the processing and exchange of threat information where possible.
- Describe how information handling designations are applied, monitored, and enforced.
- Accommodate non-attributed information exchange, when needed.
- Track internal and external sources of threat information.

The procedures should describe the roles, responsibilities, and authorities (both scope and duration) of all stakeholders. The procedures should allow for the effective transfer of authority and flow of shared information to key decision makers and should enable collaboration with approved external communities when needed.

6.0 Conclusion

The effective usage of CTI is instrumental for defending against continually changing threats. CTI simply refers to the information about adversaries and their motivation, intentions and methods which is collected, analyzed and disseminated in ways that help security and business staff at all levels protect critical assets of their organizations. However, with the rapidly changing threat landscape, CTI must be acted on quickly to receive its full value.

7.0 References

- **www.nist.gov**
- **www.fireeye.com**
- **www.sans.org**