International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1216

(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Requirements for collection and preservation of cybersecurity incident evidence

Recommendation ITU-T X.1216

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	**X.1200–X.1229**
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1216

Requirements for collection and preservation of cybersecurity incident evidence

Summary

Recommendation ITU-T X.1216 describes a general procedure for cybersecurity incident response and investigation. It also analyses sources of cybersecurity incident evidence and specifies capability requirements for tools used for collection and preservation of such evidence in an investigative process. This Recommendation also specifies reliability assurance requirements for these tools as guidelines to developers who design tools for such purpose.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1216	2020-09-03	17	11.1002/1000/14259

Keywords

Cybersecurity, cybersecurity incident evidence, incident response and investigation.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T X.1216

Requirements for collection and preservation of cybersecurity incident evidence

1 Scope

This Recommendation describes a general procedure for cybersecurity incident response and investigation. It also analyses sources of cybersecurity incident evidence and specifies capability requirements for tools used for collection and preservation of such evidence in an investigative process. This Recommendation also specifies reliability assurance requirements for these tools as guidelines to developers who design tools for such purpose.

This Recommendation does not include privacy issues and regulations related to gathering cybersecurity incident data, legal proceedings, disciplinary procedures and other related actions in handling potential cybersecurity incident evidence. These elements are considered outside the scope of "collection and preservation".

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 collection [b-ISO/IEC 27037]: Process of gathering the physical items that contain potential digital evidence.

3.1.2 evidence [b-ITU-T X.813]: Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute.

3.1.3 investigation [b-ISO/IEC 27042]: Application of examinations, analyses, and interpretation to aid understanding of an incident.

3.1.4 preservation [b-ITU-R BR.1351]: The maintenance operations that must be performed to ensure proper preservation of the archived materials, like periodic checking of the state of deterioration of the media and regeneration of the content on new media when needed.

3.1.5 security incident [b-ITU-T E.409], [b-IETF RFC 2828]: Any adverse event whereby some aspect of security could be threatened.

3.1.6 timestamp [b-ISO/IEC 27037]: Time variant parameter which denotes a point in time with respect to a common time reference.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cybersecurity incident evidence: Information or data stored or transmitted in binary form, which has been determined, through the process of analysis, to be relevant to the investigation of a cybersecurity incident.

NOTE – This definition is based on definition of 'digital evidence' in [b-ISO/IEC 27037].

3.2.2 moving target defence: Mechanisms that automatically change one or more system attributes in order to make a system's attack surface unpredictable to adversaries.

NOTE – This definition is based on [b-Jajodia14].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
DLL	Dynamic Linked Library
IP	Internet Protocol
MAC	Media Access Control
MTD	Moving Target Defence
PE File	Portable Executable File
PII	Personally Identifiable Information
WORM	Write Once Read Many

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "should" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Overview of cybersecurity incident evidence

6.1 General procedure for incident response and investigation

When analysing the cause of a cybersecurity incident, the collection and preservation of evidence related to the incident is a critical component of an incident response and investigation because cybersecurity incident data analysed could become potential evidence in court trial cases. Furthermore, cybersecurity incident evidence gathered can be used to examine vulnerabilities to enhance an organization's cybersecurity.

The incident investigation procedure shown in Figure 1 includes the following sequential phases:

– Preparation: in this phase, preliminary preparations should be made for incident investigation.

– Detection: in this phase, an unauthorized event, i.e., incident, is observed. According to the severity of the incident, decision should be made on how to respond to the incident besides collecting data.

- Collection: data should be acquired from the tools used to collect the traffic data. This phase is very important. As traffic data are exchanged at a rapid speed, it is not possible to generate the same network traffic data at a later time.
- Preservation: the original network traffic data obtained should be stored on a backup device, and a hash of all data should be also preserved.
- Investigation: in this phase, all traces gathered should be integrated. The evidence is searched to identify attack artefacts. The indicators are classified and correlated to deduce important observations using the existing attack patterns. The attack path may be determined, and attribution may establish the identity of the attacker by iteratively performing analysis in this phase to arrive at a conclusion.
- Report: the observations and explanation of the investigation should be presented in an understandable language for legal personnel.

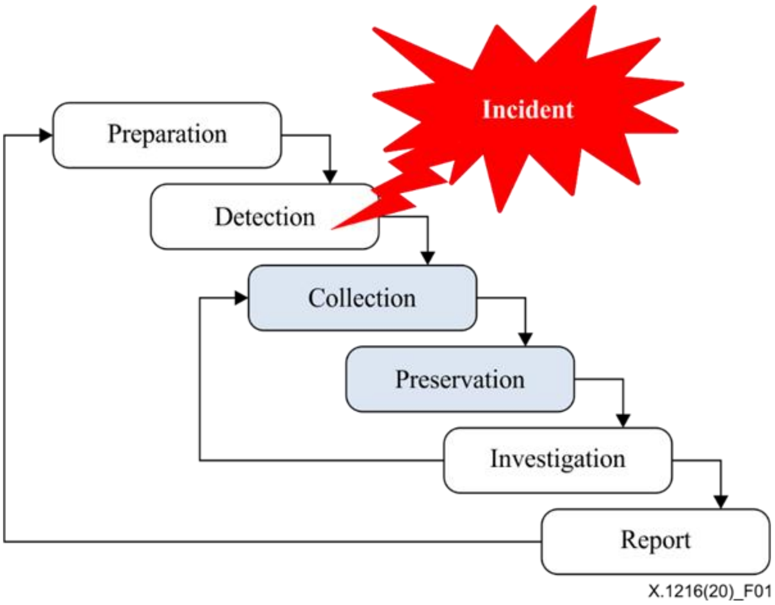

Figure 1 – General procedure for incident investigation

Various ISO/IEC guidelines related to digital investigation and incident response are standardized in [b-ISO/IEC 27035-3], [b-ISO/IEC 27037], [b-ISO/IEC 27041], [b-ISO/IEC 27042] and [b-ISO/IEC 27043]. These guidelines primarily focus on providing best practices and handling of digital evidence throughout the incident investigation procedure. [b-IETF RFC 3227] also gives guidelines for evidence collection and archiving, such as preparations and considerations for collection steps; selection of archive media and documentation for chain of custody; set of tools to be required for evidence collection and archiving. However, the guideline for selection or development of the investigation tools is not clearly described.

6.2 Data sources of cybersecurity incidents

Typical data sources related to cybersecurity incidents are host devices, network security devices, network devices and networks. Figure 2 depicts the categorized information available from the data sources.

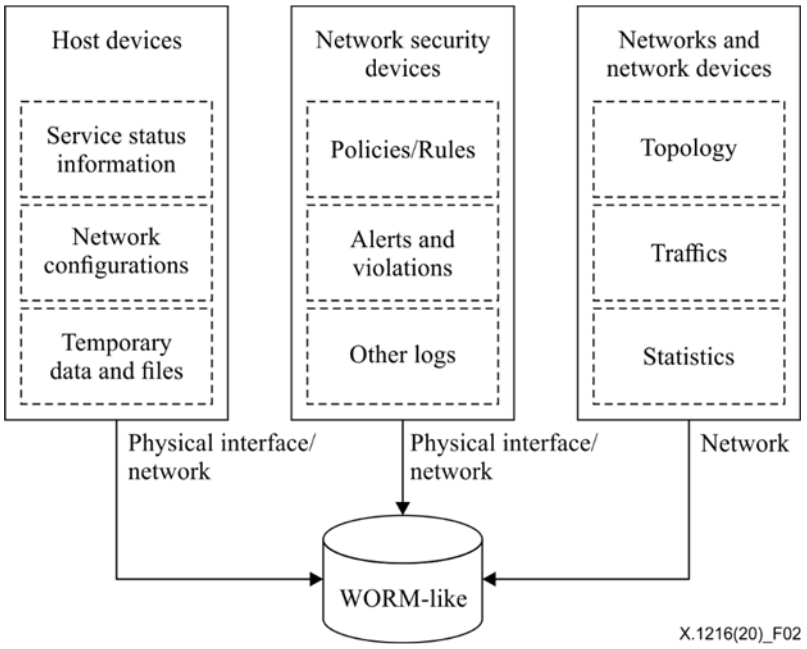

Figure 2 – Various sources for obtaining cybersecurity incident data

6.2.1 Host devices

Generally, a host device provides various kinds of data related to cybersecurity incidents. Data collecting tools should gather these data carefully as some of them are volatile and can easily be destroyed. The types of data that can be collected from the host device are as follows:

(1) System status related:

- General information (host name, user account information, system date and time, last bootup time, current time zone, boot device);
- Operating system information (manufacturer, name, architecture, version, serial number, installation date);
- Application programs (installed programs, patch status, environment variables);
- Processes (process table, automatically running processes, scheduled services);
- Logon session;
- Other registry data.

(2) Data and storage related:

- Memory data;
- Temporary file systems (recently used or executed files including dynamic linked library (DLL) and handles);
- Hidden files, executable files, opened files, deleted files, unallocated area;
- Archival media;
- Shared data (shared folders, network devices).

(3) Networking related:

- Routing table, address resolution protocol (ARP) cache, kernel statistics;
- Network configurations (IP addresses, media access control (MAC) addresses, open ports, network interfaces);
- Internet browser related information (Internet browser history, recently accessed Internet objects, cookies).

6.2.2 Network security devices

Data related to attack activities should be gathered from network security devices, such as intrusion detection systems and firewalls.

- Security policies (access control, detection rules);
- Security events and logs (alerts, alarms, warnings, errors);
- Statistical information.

6.2.3 Networks and network devices

Gathering data from networks is important when investigating cyberattacks. In particular, network topology information can help cyber incident investigators understand an enterprise network's components and configurations, discover attack paths, and estimate the extent of damage. Especially when network configuration changes dynamically as cloud computing, virtual machine, bring your own device (BYOD), and moving target defence (MTD)-based security technologies are deployed these days. Typical examples of network and network devices data are:

- Network topology configuration;
- Router logs;
- Networked services;
- Networked host related information (open ports, internally operating services, state);
- Traffic traces including a header and data;
- Session flow data (source IP address/port number, destination IP address/port number, protocol, other TCP header information);
- Files transferred through the network;
- Network traffic statistics.

7 Requirements for collection of cybersecurity incident data

Just as important as deciding what data need to be collected when a cyber-security incident happens, is deciding how to collect, preserve and analyse these data. This clause describes capabilities to collect cybersecurity incident data from the three types of data sources presented in clause 6.

Logging and other incident data that is collected from data sources may include personally identifiable information (PII). Implementers should minimize the collection of any PII to only what is strictly necessary for incidence reporting and response, and protect PII in accordance with relevant and applicable laws and regulations.

7.1 Cybersecurity incident data collection from host devices

Host devices are typically the main data source for cybersecurity incident analysis. They provide data related to the registries, logs and files loaded by the system. When a more precise analysis is required, a memory dump from the host device should be collected.

In order to support this, the collection tool should have capabilities such as those listed below:

- to examine processes and collect process information;
- to gather system status;
- to do bit-to-bit copies;
- to generate core images;
- to automate a collection process;
- to import and export collected data;
- to support various operating systems of host devices;

- to provide libraries required for collecting data and not to use any libraries in the host devices;
- to collect volatile data while the system is running; and
- to gather the network status of the current connection and opened socket.

7.2 Cybersecurity incident data collection from network security devices

A lot of data useful for cybersecurity incident analysis should be obtained from network security devices, such as intrusion protection systems, intrusion detection systems, intrusion prevention systems, firewall systems, security information and event management systems.

In order to support this, the collection tool should have capabilities such as the following:

- to collect event logs from network security devices;
- to collect alerts and violation logs from network security devices;
- to collect user authentication logs from network security devices;
- to gather security policies and rules of network security devices.

7.3 Cybersecurity incident data collection from networks and network devices

The organization collects evidence and conducts network monitoring to identify suspicious points of internal conspirators. If host-based monitoring is not effective, network monitoring can increase the effectiveness of the evidence. Network monitoring is not intended to prevent attacks, but rather to collect relevant information in the event of an incident, and it also provides much more evidence for analysis. To gather security incident data from networks and network devices, the data collection tools should provide the following capabilities:

- to collect network traffic without loss;
- to extract session flow from network trace and gather session flow information such as source IP address and port number, destination IP address and port number, IP protocol and service information, start and end time of the session, the number and size of incoming packets, the number and size of outgoing packets;
- to collect portable executable (PE) files transferred over the network and extract file information such as file name, file size, time the file was collected, source IP address and port number of the session containing the portable executable file (PE File), destination IP address and port number of the session containing the PE file, IP protocol;
- to collect logs of network devices, such as routers, switches, network monitoring systems.

8 Requirements for preservation of cybersecurity incident data

To analyse the causes of cybersecurity incidents, it is necessary to preserve the collected original data and avoid its potential damage. In particular, when considering legal cases, it is necessary to preserve collected data so that the integrity and legitimacy of the evidence remains. In order to support this, the preservation tools should support the following capabilities:

- to generate checksums and digital signatures;
- to validate that collected data is preserved without loss;
- to generate timestamp (in ms) for the time of data collection and preservation;
- to record collected data on a write once read many (WORM) like device;
- to provide a profile of data retention policies that should be maintained accordingly;
- to ensure that the collected data is preserved for the duration of the policy;
- to preserve the collected data and metadata in a formalized form (various considerations on this matter are specified in [b-ITU-T X.1215] and [b-ITU-T X.1541]).

9 Requirements for collection and preservation tool to ensure reliability

The data collected and preserved by a collection and preservation tool can be used to investigate the cause of the cybersecurity incidents and as evidence to identify the responsibility for the incident.

Therefore, the tool for collecting and preserving data for cybersecurity incident analysis should provide the following capabilities for reliability assurance that consist of user management and data management:

– the tool should provide a means to limit and control user access to the tool itself and to stored data;

– the tool should not allow attempts to overwrite, alter or delete retention data without proper authorization;

– the tool should provide security management functions that authorized administrators can configure and manage security functions, security policies and important data;

– when transmitting collected data between physically separated devices, data must be encrypted to ensure confidentiality and integrity;

– all communication means associated with the tool should use a secure encrypted communication protocol;

– the tool should provide a backup function for the preserved data;

– the tool should provide capabilities for logging, error reporting and auditing;

– the tool should provide capabilities for processing metadata and formalized content and sharing it according to existing policies (as specified in [b-ITU-T X.1550] and [b-ITU-T X.1582]).

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

[b-ITU-T X.1215] Recommendation ITU-T X.1215 (2019), *Use cases for structured threat information exchange*.

[b-ITU-T X.1541] Recommendation ITU-T X.1541 (2017), *Incident object description exchange format 2*.

[b-ITU-T X.1550] Recommendation ITU-T X.1550 (2017), *Access control models for incident exchange networks*.

[b-ITU-T X.1582] Recommendation ITU-T X.1582 (2014), *Transport protocols supporting cybersecurity information exchange*.

[b-ITU-R BR.1351] Recommendation ITU-R BR.1351 (1998) *Requirements for the application of digital technology to audio archiving systems for radio broadcasting*.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary*.

[b-IETF RFC 3227] IETF RFC 3227 (2002), *Guidelines for Evidence Collection and Archiving.*

[b-ISO/IEC 27035-3] ISO/IEC 27035-3, *Information technology – Security techniques – Information security incident management – Part 3: Guidelines for incident response operations.*

[b-ISO/IEC 27037] ISO/IEC 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.*

[b-ISO/IEC 27041] ISO/IEC 27041:2015, *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method.*

[b-ISO/IEC 27042] ISO/IEC 27042:2015 *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence.*

[b-ISO/IEC 27043] ISO/IEC 27043: 2015, *Information technology – Security techniques – Incident investigation principles and processes.*

[b-Jajodia14] Jajodia, Sushil, and Kun Sun. "MTD 2014: First ACM workshop on moving target defense." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020