ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1645 (09/2023)

SERIES X: Data networks, open system communications and security

Cloud computing security – Cloud computing security best practices and guidelines

Requirements of network security situational awareness platform for cloud computing

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
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	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
IMT-2020 SECURITY	X.1800-X.1819

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

Recommendation ITU-T X.1645

Requirements of network security situational awareness platform for cloud computing

Summary

Network security situational awareness (NSSA) is derived from situational awareness. It usually includes four processes, data acquisition, security situation analysis, security situation assessment and security situational tendency projection, and it generally has the following capabilities: 1) detection and persistent monitoring of various attack threats, abnormal behaviour and their scope of influence; 2) data mining, threat analysis and tracing abnormal behaviour; 3) security prediction and early warning; 4) visualization of the security situation.

For cloud computing service providers, the NSSA platform plays an important role in improving cloud computing's security protection, the ability to detect security breaches or anomalous behaviours, security decision-making and emergency response ability, and it can even help improve the early warning mechanism for cloud computing.

Recommendation ITU-T X.1645 will first introduce the concept and development of NSSA, analyse the advantages of NSSA coping with the security challenges of cloud computing and document the requirements for the NSSA platform for cloud computing.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1645	2023-09-08	17	11.1002/1000/15527

Keywords

Big data analysis, cloud computing, network security situational awareness, situational awareness.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1645

Requirements of network security situational awareness platform for cloud computing

1 Scope

This Recommendation introduces network security situational awareness (NSSA)and the requirements of the NSSA platform for cloud computing. This Recommendation is applicable to cloud computing service providers.

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 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.4 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 vulnerability [b-NIST-SP-800-30]: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.1.6 threat intelligence [b-ITU-T X.1217]: A collection of organized, analysed, and refined information about potential and current attacks that may threaten an organization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 situational awareness: The ability to assess the current state of elements in a given environment, as well as their relationships over multiple dimensions, including time and space.

NOTE – This is achieved by collecting data from a variety of sources, combining that data and analysing it. The goal of situational awareness is the integration and analysis of information from diverse sources to gain a comprehensive understanding of its meaning.

3.2.2 network security situational awareness (NSSA): The ability to identify and assess key network security elements and categorize them according to rules using temporal and spatial dimensions.

NOTE – This information evaluates the overall security situation of the network and predicts emerging network security trends through techniques such as statistical analysis, data mining and artificial intelligence. The resulting insights can be presented in human-readable formats or as input to network security automation.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Artificial Intelligence
C&C	Command and Control
CRUD	Create, Read, Update and Delete
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
DGA	Domain Generation Algorithm
HBase	Hadoop Database
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
JDBC	Java Database Connectivity
MPP	Massively Parallel Processing
NoSQL	Not only Structured Query Language
NSSA	Network Security Situational Awareness
ODBC	Open Database Connectivity
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall

5 Conventions

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

In this Recommendation and its appendices, the words shall, shall not, should and may appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Introduction of network security situational awareness

Today's, network attacks have been developed towards precise goals, as attackers usually have exact plans, and long-term penetration is common. Correspondingly, the security defence presents a typical 'time confrontation' feature. In traditional security architecture, various security components or products are only deployed with their own protection rules, warning policies, log processing and storage mechanisms, but lack a coordination mechanism between the components and products. This causes an islanding effect, which weakens the defence capability against more secretive and professionally advanced attacks.

Network security situational awareness (NSSA) is derived from situational awareness and is a specific application in network security. It usually includes four processes: data acquisition, security situation perception, security situation assessment and security situation prediction, and generally has the following capabilities:

- Detecting and persistently monitoring various attack threats including abnormal behaviour and their scope of influence;
- Data mining, drilling, threat analysis, and the traceability of abnormal behaviours;
- Security prediction and early warning;
- Visualization of security situation.

In the context of network security, information asymmetry refers to a scenario in which an attacker possesses more knowledge about an organization's systems, network or processes than the organization itself. In such a situation, attackers are in an advantageous position when it comes to strategizing and implementing attacks. NSSA is of great significance in the aim of addressing the information asymmetry between attack and defence, and also for accelerating the incident response and traceability.

In the meantime, the development of big data analysis, cloud computing and artificial intelligence (AI) has brought great opportunities and power to the development of NSSA. For example, NSSA can effectively support massive security log storage, utilizing and mining by big data analysis, to achieve the persistent monitoring of large-scale network security situations; the development of AI can provide more analysis methods and risk prediction capabilities for NSSA, which can effectively improve prediction accuracy; and the development of cloud computing can provide a more flexible and stable infrastructure architecture for NSSA.

The typical framework of an NSSA platform is shown in Figure 6-1.

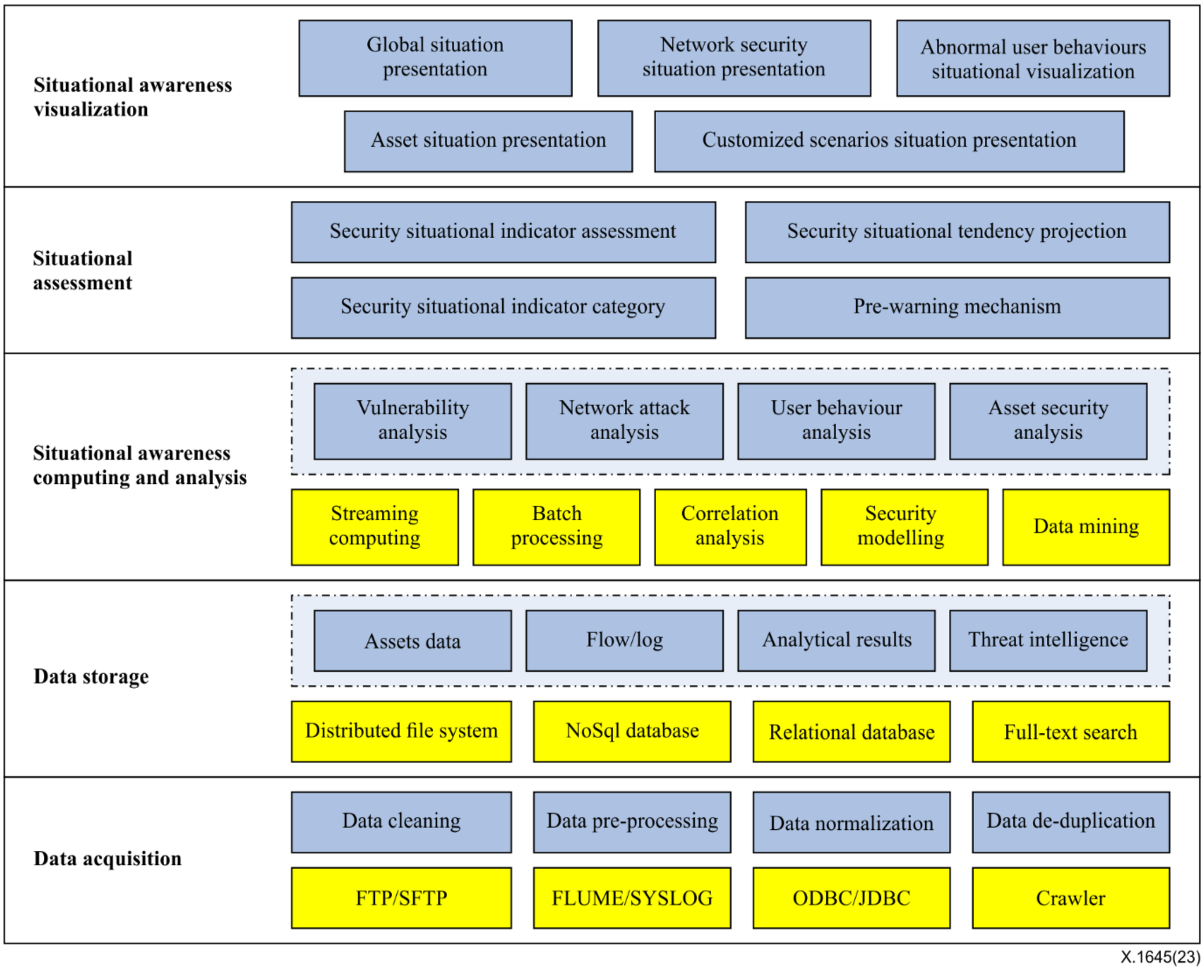

Figure 6-1 – Framework of network security situational awareness platform

7 Analysis

With the fast development of technology and the maturity of its ecosystem, cloud computing represents a new generation of critical information infrastructure. Cloud computing has brought lots of benefits, while also facing much more security issues especially in operation and maintenance, such as the following:

1) With the rapid increase of scale, various kinds of security components deployed in the cloud computing infrastructure involve massive security data and repeated warnings. The scenario makes it difficult for operation and maintenance engineers to deal with in a limited time window.

2) Most security components are isolated from each other, which obviously brings the islanding effect. This makes it hard to provide a well-coordinated defence mechanism in a cloud computing environment.

3) The environment of cloud computing is usually complex and may include public cloud, private cloud and hybrid cloud. This makes it difficult to make reasonable security decisions due to the lack of a macroscopic and entire perspective for cloud computing service providers and even cloud computing users.

NSSA is a suitable approach for solving these problems. Based on big data technology, NSSA can effectively support the storage, usage and data mining of massive, heterogeneous security logs. Further, through correlation analysis of multiple different data, it is possible to effectively organize various different security components, improve the detection ability of threats and increase the efficiency of security engineers. NSSA can also provide a visual capability of the whole security situation awareness for cloud computing. In the meantime, it is convenient to use AI technology in NSSA, which can help improve the detection, diagnosis and prediction capability of security situational awareness for cloud computing.

Therefore, NSSA plays an important role in improving cloud computing's security protection, security decision-making and emergency response capacity, and thus can help improve the early warning mechanism for the cloud computing service providers.

In the meantime, an NSSA platform deployed in cloud computing requires the following particular capabilities as follows:

1) The data acquisition should adapt the dynamic changes of assets in cloud computing, as the assets in cloud computing can be created and removed more flexibly and frequently compared with in a traditional IT architecture.
2) NSSA platform should adapt the character of a cloud computing service such as multitenants' sharing resource use and elastic resource management, which may result in rapid change of data sources. The rapid change of tenants and their service would correspondingly bring the modification of data acquisition for NSSA platform.
3) An NSSA platform should continue to interact and cooperate with the cloud computing management platform to access the various kinds of data such as the running status, and security logs of cloud computing resources to achieve a deep insight view/awareness of the cloud computing resources; for example, NSSA cannot bypass the cloud management platform to observe the network connections between the VMs in the same OSI layer 2 network area.
4) The NSSA platform should support the capability of accessing data from multiple clouds to achieve a unified-asset perspective for users either in hybrid cloud or public cloud.

The application and deployment of NSSA provide possible solutions for the above technical challenges. NSSA can sense various security events and abnormal behaviours comprehensively, accurately and finely in both time and space dimensions, analyse various security elements, understand the whole security situation, and predict its trends, which will help to improve the cloud computing provider' security operation capability, support security decision-making and incident response, and improve the security early warning mechanism.

8 Requirements of security situational awareness platform for cloud computing

8.1 Requirements of data acquisition

8.1.1 Data acquisition mechanism

Acquisition nodes of an NSSA platform should support collecting various types of data, such as network traffic logs, system logs, middleware logs and security logs of cloud computing infrastructure, in an active or passive approach. An active approach collects data by periodically monitoring or scanning targets, whereas a passive approach collects data by mainly receiving or importing data from different data sources.

1) It is required for the data acquisition to support the active approach, such as collecting data by scanning, crawling or simple network management protocol (SNMP).
2) It is required for the data acquisition to support the passive approach, such as by receiving data by syslog protocol or NetFlow channel and importing data manually.

The data acquisition capability should adapt to cloud computing environments in the following ways:

1) It is recommended for the data acquisition to support collecting data across different clouds, such as multiclouds and hybrid clouds.

2) It is recommended for the data acquisition to accommodate dynamic resource changes of cloud computing environments.

3) It is recommended for the data acquisition to support collecting data logs of east–west network traffic of cloud computing platforms.

The acquisition nodes of an NSSA platform should have the following capabilities:

1) It is required for acquisition nodes to perform data filtering and examining data validity, such as data type and value range, and filtering invalid data according to preconfigured policies.

2) It is recommended for acquisition nodes to implement a data re-collection mechanism in case of collection failures.

8.1.2 Data source

An NSSA platform should support applying create, read, update and delete (CRUD) operations to its data and support collecting the following data types:

1) It is required to support collecting asset data of cloud computing platforms, such as asset data of virtual resource pools, network equipment, hosts, security equipment, systems, software and cloud computing management platforms.

2) It is required to support collecting various types of log data, such as web access logs, security logs, business operation logs and login-related logs from multiple sources, such as hosts, middleware and cloud computing management platforms, and support receiving log analysis results from other systems.

3) It is required to support collecting various vulnerability data from multiple equipment and components of cloud computing platforms, such as buffer-overflow vulnerabilities, injection vulnerabilities, business logic vulnerabilities, design vulnerabilities, configuration vulnerabilities, etc.

4) It is required to support collecting data of multiple network attack events, such as DDoS attacks, vulnerability exploit attacks and unauthorized accesses.

5) It is required to support collecting threat intelligence data, such as threat intelligence of IP/domain/URL, malicious samples, command and control (C&C) blacklist and vulnerabilities.

8.1.3 Data preprocessing

In order to satisfy requirements of data quality, the NSSA platform is required to implement data cleaning and filtering, standardization, correlation and completion, merging and de-duplication on collected data, and then store standardized data.

1) Data cleaning: the NSSA platform should support data cleaning if errors, incompleteness, invalidity and other issues exist in collected data, including by means of the following:

   - It is required to support data conversion, processing and filtering for inconsistent data formats, data entry errors and data incompleteness.
   - It is recommended to support data filtering and cleaning based on conditional operations, regular expression matching and expression calculations.
   - It is recommended to support data de-duplication.

2) Data standardization: the NSSA platform should support uniform formatting of various types of heterogeneous data, and preservation of the original collected data, including by means of the following:

   - It is required to support standardizing data fields based on field rules for each type of data.
   - It is recommended to support uniform formatting of raw content by regular expression.

- It is recommended to support the preservation of original collected data, in order to support subsequent traceability analysis and custom development.

3) Data correlation and completion: it is recommended the NSSA platform support data correlation and completion of standardized data, which includes user information, asset information, geographical location information and threat intelligence information and it is recommended to support selecting particular data and fields to be completed.

4) Data merging: it is recommended the NSSA platform support merging standardized data based on configured rules, and it is recommended to support selecting particular data and fields to merge.

8.1.4 Data acquisition security requirements

1) It is required for the NSSA platform to support access control of acquisition nodes and monitoring the process of data collection with timely alerts in case of abnormal events.

2) It is required to strictly restrict the temporary data storage location during the data-collection process, which cannot be modified arbitrarily.

3) It is required for the NSSA platform to support hierarchical classifications and identifications of collected data and implement security protections such as encryption for sensitive data, for example, asset data, operational data and log data.

4) It is required for the NSSA platform to support data masking and desensitization of sensitive data before preprocessing and analysing, and satisfy security compliance requirements of collected data.

5) It is required for the NSSA platform to maintain a collected and operational log to enable generating timely alerts of abnormal events and auditing, including the following:
   - It is required to audit operations of users and administrators to detect, alert and respond to malicious behaviours such as data misuse.
   - It is recommended to alert for transmission interruptions during data collection.
   - It is recommended to alert if the data storage exceeds a preset threshold during data collection and transmission.

8.2 Requirements of data storage

The data storage of the NSSA platform should apply big data techniques to meet the storage demands of multisource, multidimensional and continuous growth data generated by the cloud computing environment, such as analysis results and external threat intelligence. The NSSA platform should support storage mechanisms according to different domains and classifications of various data types and satisfy the requirements of different data analysis and isolation methods. Meanwhile, the NSSA platform should ensure the availability, integrity and confidentiality of the storage data.

8.2.1 Data storage categorization

It is recommended for the NSSA platform to support the storage of unstructured data, structured data and semi-structured data according to various data sources and support multiple data storage categorizations, including relational data storage, NoSQL (not only structured query language) database, distributed file storage and distributed full-text search.

The data storage categorizations of the NSSA platform are recommended as described in Table 8-1.

Table 8-1 – Data categorization

Data source	Data contents	Data volume	Storage categorization (recommended)
Cloud host/Container/OS	Operation logs, security logs, running status data, configuration files, etc.	Large	Distributed file storage/distributed full-text search/NoSQL database
Cloud management platform	Access logs, operation logs, configuration files, workflow data, etc.	Medium	Distributed file storage/distributed full-text search/NoSQL database
Network equipment	Logs of routers, switches and network platform, routeing table, configuration files, etc.	Large	Distributed file storage/distributed full-text search/NoSQL database
Security equipment	Logs of firewall, intrusion detection system (IDS), intrusion prevention system (IPS), virtual private network (VPN), web application firewall (WAF), configuration files, etc.	Large	Distributed file storage/ distributed full-text search/NoSQL database
Application system	Logs of database, middleware, application systems, configuration files, etc.	Large	Distributed file storage/distributed full-text search/NoSQL database
Basic data	Asset data, account data, IP dictionary, service data, etc.	Medium	Rational database/distributed full-text search/NoSQL database
Network traffic	DPI data, network flow data, etc.	Massive	Distributed file storage
Threat intelligence	Strategic intelligence, tactical intelligence, security information, etc.	Medium	distributed file storage/distributed full-text search/NoSQL database
Analysis results	Security events, compliance data, security index, etc.	Medium	Rational database/distributed full-text retrieval/NoSQL database

8.2.2 Technical requirements of data storage

The NSSA platform should develop an elastic and scalable data storage architecture to satisfy the continuous growth of data volume and the requirements of data classification and hierarchical storage. Also, the data storage lifecycle should be varied according to compliance regulations, business requirements and economic costs.

1) It is recommended for the NSSA platform to support mainstream rational databases. Rational databases are recommended to support a complete relational model access interface, including standard SQL interface, application development standard interface (JDBC, ODBC, etc.).

2) It is recommended for the NSSA platform to support mainstream NoSQL databases.

3) It is recommended for the NSSA platform to support typical big data components, such as Hive, HBase and MPP components, to support extended functionalities.

4) It is recommended for the NSSA platform to adopt full-text search components, which should support keyword retrieval, multi-keyword search, combination search of full text and other fields, and prefix matching, fuzzy matching and other retrieval conditions.

5) It is recommended for the NSSA platform to adopt distributed message bus components, such as Kafka, RabbitMQ and so on. Distributed message bus components should support

functions such as data compression, setting data retained time and deleting expired data automatically.

6) It is recommended for the NSSA platform to support online storage and backup mechanisms to guarantee data availability.

7) It is recommended for the NSSA platform to support metadata storage, mainly including:

   - Technical metadata and use for data maintenance, such as how data is stored to achieve efficient data access.
   - Management metadata, such as data access control policy and data processing results.

8.2.3 Security requirements of data storage

1) It is required for the NSSA platform to develop data access control mechanisms, such as role-based data storage access control, to prevent unauthorized accesses.

2) It is required for the NSSA platform to support data storage encryption for important or sensitive data. It is recommended to clarify storage encryption requirements of various data types based on data classification and hierarchical definition, such as requirements for data encryption algorithms and encryption key management.

3) It is required for the NSSA platform to implement appropriate techniques and control measures to ensure the effectiveness of data storage integrity and multicopy data consistency.

4) It is required for the NSSA platform to implement appropriate techniques and control measures to ensure data storage availability. Based on principles of data classification, it is recommended to clarify the backup and recovery policies of various data, such as backup modes, requirements of storage period and recovery time.

5) It is recommended for the NSSA platform to test data storage mechanisms periodically to verify abilities of data fault identification and backup reconstruction.

6) It is required for the NSSA platform to generate all processing logs of data storage, to ensure the traceability of the data storage processes, and provide warning capabilities for abnormal behaviours.

8.3 Requirements of situational computing and analysis

The situational computing and analysis of the NSSA platform mainly includes the computing and analysis engine and situational analysis functional modules.

1) The computing and analysis engine provides threat modelling and analysis computing capabilities for situational analysis function modules. The computing and analysis engine includes security modelling and big data computing frameworks, such as the offline computing engine, and real-time computing.

2) Situational analysis function modules mainly achieve the network security situational analysis in the cloud computing environment based on data mining, drilling and threat analysis over various aggregated asset data, such as security events, log data and network traffic data.

3) To improve the efficiency of calculation and analysis, it is required to build a unified representation of various security events and asset information before security modelling, which can be achieved by vectorization of context. The method of vectorization maps the context to a Euclidean space, and usually is a premise to adopt various AI algorithms for similarity calculation and correlation calculation.

8.3.1 Requirements of computing and analysis engine

8.3.1.1 Security modelling

Security modelling is required to include correlation modelling, statistical modelling, threat intelligence correlation modelling and AI modelling, providing in-depth analysis and mining capabilities of basic situational data.

1) **Correlation modelling**: A rule-based matching method is used to perform logical association and feature matching analysis on heterogeneous and heterogeneous events.
   - It is required to support logical correlation analysis based on the causality of security incidents.
   - It is required to support the correlation of multi-source heterogeneous data from multiple aspects, such as time and space.
   - It is recommended to support clustering of alert information according to dynamic situations of network security, to reduce the number of alerts and improve responding efficiency.
2) **Statistical modelling**: use statistical methods to compute the quantitative characteristics of various events, such as frequency and occurrence period, and obtain the distribution of event data, main characteristics, trend of time series, whether there are abnormal values and event summary results.
   - It is recommended to support performing statistical analysis of security events, security behaviours, security threats and other characteristics, and discover important statistical characteristics of security threats from various data sources.
3) **Threat intelligence association**: It is recommended to support integrating threat intelligence capabilities to discover accurate intelligence events based on threat intelligence in the cloud computing environment.
4) **AI modelling**: It is recommended to support various built-in artificial intelligence algorithms, including timing algorithm, classification algorithm, clustering algorithm and other algorithm prototypes, providing users with learning and analysis capabilities for arbitrary data, and to analyse advanced security threats and unknown threats.
   - It is recommended to support mainstream algorithms, such as cluster analysis, association analysis, decision tree analysis, regression analysis and other AI/machine learning analysis algorithms.
   - It is recommended for the NSSA platform to support the centralized management of security modelling and policy to facilitate effective execution and rapid deployment.

8.3.1.2 Big data computing framework

It is required to support both offline and real-time computing frameworks, to achieve batch processing of static data and real-time analysis of dynamic data (streaming data).

1) **Offline computing framework**: it is required to support deployments of offline algorithms, training models and machine learning scenarios. Analysts can use the offline analysis engine to mine data in depth, having immediate feedback on the output results of the algorithm, providing model training capabilities.
2) **Real-time streaming computing framework**: it is recommended that the real-time computing framework support a distributed architecture, and that the storage capacity can be dynamically adjusted. High availability and separation of read and write policies can ensure separate data reading and writing on offline data analysis.

8.3.2 Requirements of situational analysis functional modules

Based on the computing and analysis engine, the situational analysis function modules establish scenario-based analysis capabilities for various asset data, security events, log data, traffic data and other data, and provide security analysis scenarios based on multiple data to achieve scenario-based security alerts and early warning capabilities. The situational analysis functional modules include network security analysis, asset security analysis and high-risk user behaviour analysis in the cloud computing environment.

8.3.2.1 Network security analysis

The network security analysis module is required to have the ability to analyse various network attack situations, such as abnormal network traffic, malicious program propagation and malicious domain name access in the cloud computing environment, as well as the ability to trace their variation tendencies.

1) It is recommended to support the detection and statistical analysis of the general situation of common attacks and analyse the variation trends of the current attack situation.
   - It is recommended to support network attack detection and analysis functions based on multi-source data, which includes network intrusions, web attacks, malware, DdoS attacks, network reconnaissance, suspicious activities and other types of network attacks.
   - It is recommended to support the statistical analysis of various types of network attacks, and the analysis of trend variation in various types of attacks.
2) It is recommended to support the detection and statistical analysis of the overall situation of abnormal network traffic in the cloud computing environment and analyse the trend variation of current abnormal network traffic.
   - It is recommended to support the abnormal identification of network traffic, and to be able to detect and analyse abnormal traffic of protocols based on common virus ports.
   - It is recommended to support the statistical analysis of abnormal network traffic and the merging and statistics of protocol abnormal traffic, and analyse the trend of abnormal traffic.
3) It is recommended to support the analysis of the overall situation of the spread of malicious programs such as viruses, worms and trojans in the cloud computing environment, and analyse the current trends in the spread of malicious programs.
4) It is recommended to support the detection and statistical analysis of botnet C&C hosts and zombie hosts and support the analysis of the spread and trend variation of botnets.
5) It is recommended to support the analysis of the access statistical and propagation of malicious domain names, C&C IP addresses and domain generation algorithm (DGA) domain names.
6) It is recommended to support the attack chain model to trace the source of attack events by classifying the generated security events according to the attack process, which includes information collection, network intrusion, C&C, horizontal penetration, target achievement and evidence cleaning.
7) It is recommended to support the analysis of attacker information based on threat intelligence.

8.3.2.2 Asset security analysis

It is required to support the analysis of the security status of various assets of the cloud computing platform. It is recommended to analyse the security status of the cloud computing infrastructure, virtual machines, containers and business systems through security equipment logs, system logs, vulnerability scanning results and other data. The analysis types include system attacks analysis and system vulnerability analysis.

8.3.2.3 Asset information analysis

1) It is required to support asset statistical analysis, including analysis based on asset classifications, categorizations and priorities, and asset status updates, such as adding or removing assets.

2) It is required to support asset distribution analysis, including analysis based on asset geographical information, department belongings and important web applications.

3) It is required to support searching and displaying asset information according to asset IP addresses, categorizations, priorities and geographical information.

8.3.2.4 Asset threat analysis

1) It is required to support system attack threat analysis, including log destruction detection, system privilege escalation detection, error log detection and brute force attack. The analysis can be implemented based on the correlation analysis of asset data, device logs, host system logs, security system data and threat intelligence.

2) It is required to support the statistical analysis and trend analysis of asset threats.

8.3.2.5 Asset vulnerability analysis

1) It is required to support the correlation analysis of asset vulnerability scanning results and security device detection logs to perform vulnerability utilization analysis, including host machine/VM/container vulnerability analysis and application vulnerability analysis, and the statistical analysis of assets at risk of vulnerability exploitation according to time, business system, vulnerability level and other dimensions data.

8.3.2.6 Compliance analysis of asset configurations

1) It is required to support the analysis of the configuration compliance results of operating systems, virtualization software, databases, network equipment and middleware in the cloud computing environment.

2) It is required to support the statistical analysis of non-compliant items had been discovered, and support the risk analysis of attackers using non-compliant items to attack assets.

8.3.2.7 User behaviour analysis

It is recommended to support the detection and analysis of abnormal behaviours of internal users accessing the cloud computing platform, and abnormal behaviours of assets and business systems as well as profiling analysis of user behaviours.

1) It is recommended to support the analysis of abnormal user operation behaviours including abnormal operations of sensitive data, expired account login, illegal outreach, sensitive command execution, brute force attack and abnormal address login.

2) It is recommended to support profiling based on internal user behaviours, including individual behaviour characteristics of users and group characteristics.

3) It is recommended to support the customization of abnormal behaviour rules and behaviour models.

4) It is recommended to support abnormal behaviour analysis based on user profiles, and compare individual or group single-day behaviours with historical behaviour data to mine abnormalities

5) It is recommended to support the abnormal behaviour analysis of various cloud computing resources, and to be able to identify abnormal behaviours that may occur in cloud computing environment, such as abnormal behaviours of cloud hosts, abnormal calling system tools, abnormal network behaviours and illegal out-communication.

8.4 Requirements of situational assessment

The situational assessment of the NSSA platform is recommended to support dynamic situational assessment of the overall security status in the cloud computing environment, predicting the situational tendency, based on analysing multidimensional security data, security analysis results of the cloud computing platform and evaluation modelling of the situational index category. It supports issuing early warnings and interacting with the security decision-making and emergency response mechanisms of the cloud service provider (CSP) / cloud service customer (CSC).

8.4.1 Situational assessment

The scope of the security situational assessment includes the comprehensive situation of the cloud platform, the security situation of cloud assets, threats, vulnerabilities, network attack and the availability status of the cloud platform and its components.

1) It is required to collect the asset information as a data source to build a security situational assessment index category. The asset information should include the specific version of operation systems, middleware, application and database, the network topology location, the value of asset, etc., which would help in generating reasonable assessment indicators.

2) It is required to support a security situational assessment index category of the cloud computing platform by creating general metrics in a unified scale for security situational measurements and quantifying various elements of the network security situation.

   - It is recommended to create both qualitative and quantitative indicators for network situational assessment. Qualitative indicators are subjective assessments based on professional security analysers. For example, security analysers can assign severity levels given vulnerabilities or network attacks based on their experiences. Quantitative indicators come from collections and analysis of raw data.
   - It is recommended to support similarity calculation and correlation calculation in dealing with threat indicators, including the following:
     - ➢ It is recommended to use the similarity calculation of threat context to recognize the easily surging threats such as scanning, brute force cracking and DDoS attacks, so as to avoid drastic changes of a specific indicator caused by a large number of repeated alarms.
     - ➢ It is recommended to use the correlation analysis between threat and asset information to recognize threats of blind attack and massive attempting, which would help the security personnel quickly find the high-risk indicators that really need their responses.
     - ➢ It is recommended to adopt a unified algorithm framework to realize correlation analysis and similarity analysis, such as angle cosine. The unified algorithm framework could obviously reduce the maintenance cost of utilizing the algorithms.
   - It is recommended to create the general indicator and subdivision indicators for network security situational assessment. The general indicator reflects the overall characteristics of cloud computing platform security assessment; the subdivision indicators can be decomposed for different components or systems, which reflects the differences of situational assessment results for various components/systems.
   - It is recommended to support creating situational indictor categories, including the following:
     - ➢ It is recommended to support creating operational indicators for cloud computing platforms, such as utilizations of cloud resource pools and business access delays.
     - ➢ It is recommended to support creating indicators of network security threats, including various network security incidents, which can be further computed and evaluated in terms of their frequencies and severities.

- ➢ It is recommended to support creating indicators for cloud assets security assessment, such as asset threats and asset vulnerabilities, including vulnerability severity, and whether vulnerabilities have been patched.
- ➢ It is recommended to support creating indicators for user behaviour security, such as whether users have abnormal accesses, login and malware download behaviours. It is also required to adopt user privacy protection techniques, such as data desensitization and data anonymization to protect user privacy.

3) It is recommended to support constructing a comprehensive security situational assessment mechanism or modelling based on a hierarchical, multidimensional indicator categories.

- It is required to support standardizations of different subdivision indicators, including both qualitative and quantitative indicators, to avoid biased evaluation results due to unit and magnitude differences. It is recommended to adopt conversion techniques to convert qualitative indicators to numerical values for further computing or analysing.
- It is recommended to support multidimensional situational assessment mechanisms, including risk-oriented assessment, threat-oriented assessment or modelling based on time series data.
- It is recommended to support various evaluation models, including models based on mathematical theoretical models or knowledge-based reasoning.
- It is recommended to support a bottom-up hierarchical assessment method by comprehensively processing situation indicators of lower layers and then computing the situational assessment results of upper layers and progressively computing the overall assessment of the security situation.
- In hierarchical assessment methods, it is recommended to support similarity calculation to interpretability of a specific situation assessment value, comparing it with the historical and nearby values. For a final assessment value, a multidimensional vector can be constructed by choosing its precedent results of a specific level, and it can be used to calculate the similarity of the historical nearby values by angles cosine, space vector distance and other algorithms. The similarity calculation can help security personnel to find the anomaly more easily and understand the situational awareness more accurately.

4) It is recommended to support abilities to trace historical security situation assessments of the cloud platform efficiently by implementing log preprocessing, key field indexing, full-text search and fuzzy query.

8.4.2 Situational tendency projection

On the basis of acquiring and tracing the security status of the cloud computing environment, extracting the security elements and key indicators that can cause changes in the network situation, the NSSA platform is recommended to support predicting the overall security tendency, subdivision component security tendency and potential security risks based on cloud platform-oriented security situational projection models.

1) It is required to support constructing a hierarchical and multidimensional indicators category based on collected data and analysed results and predict the situational tendency by relevant forecasting models.

2) It is recommended to support mainstream prediction models, including machine learning based regression prediction models, deep learning models and prediction models based on differential equations in professional fields.

3) It is recommended to support computing prediction results by fusing different prediction models to improve prediction accuracy, specifically by:

- Monitoring the accuracy of each model by computing the loss function values between prediction and data results.

- Combining results of each model through weights, making adaptive adjustments to weights between models. For example, the weight of each model can be adaptively adjusted based on the monitoring result of the loss function; offline training of the latest data can also be automatically triggered to update the model and improve accuracy.

8.4.3 Pre-warning mechanisms

The NSSA platform should provide early warning mechanisms for potential security risks in the cloud computing environment, based on the results of security analysis, situational assessment and situational predictions.

1) It is recommended to provide early warnings of asset vulnerabilities by correlating vulnerabilities to threat intelligence data, related security event data, etc., and analysing the vulnerability of cloud platform assets.

2) It is recommended to support early warnings of potential network attacks based on the prediction tendency, including malicious scanning, web attacks, DDoS attacks, password guessing attacks and system vulnerability attacks.

3) It is recommended to support early warnings of potential user abnormal behaviours based on tendency prediction, including abnormal sensitive data operations, expired account logins and high-risk command execution, etc. Before issuing warnings, it is required to use data desensitization and data anonymization techniques to protect user privacy.

4) It is recommended to support early warnings of undetected security threats by associating detected abnormal behaviours, threat intelligence and original logs, etc.

5) The early warning mechanisms include the following:
   - It is recommended to support issuing early warnings based on preconfigure policies which can be customized accordingly.
   - It is recommended to support the hierarchical management of early warnings and categorizing warning levels according to importance and severity.
   - It is recommended to support issuing warnings through APIs by which third party systems can receive warnings and response accordingly.

8.5 Requirements of situational visualization

The NSSA platform is required to support displaying security situation of multiple scenarios, including global security situation, network security situation, asset security situation and customize security situation. At the same time, it is recommended to support using multiple types of views to display the detailed information of the security situation, such as radar chart, correlation information map and threat path map, and to support drilling the detailed security information.

8.5.1 Global security situational visualization

1) It is recommended to support presenting evaluation statuses of the global security of the cloud computing platform by means of scores or grades.

2) It is recommended to support presenting the global security situation of the cloud computing platform graphically, including the risk ranking, tendency of network attacks, vulnerabilities and high-risk user behaviours.

3) It is recommended to support presenting the security situation of different tenants, different business operations and different assets, etc. in the cloud computing platform and comparing with historical data to show trends.

4) It is recommended to support presenting real-time aggregated alarms of network security events, abnormal user behaviours and asset security status in the cloud computing platform, and support drilling details of these alarms graphically.

8.5.2 Network security situational visualization

1) It is recommended to support presenting the network security risks of the cloud computing platform graphically in multidimensions, including statistical analysis results of network attacks, network attack types, geographical distribution of network attacks, abnormal network traffic, source IP and destination IP of attacks.

2) It is recommended to support presenting real-time security alarms of the cloud computing platform, such as network attacks, abnormal network traffic and malicious programs. The alarm information includes timestamp, security type, severity level, source IP and destination IP of attacks.

3) It is recommended to support drilling detailed information of the network security situation information.

8.5.3 Asset security situational visualization

1) It is recommended to support presenting asset information of the cloud computing platform graphically, such as assets scales, asset types, asset ownership and asset distributions.

2) It is recommended to support presenting various statistical analysis results of the cloud computing platform graphically, including asset vulnerabilities, network attacks and configuration errors.

3) It is recommended to support real-time security risks of various assets of the cloud computing platform in multidimensions, including asset name, asset IPs, attack types, vulnerability types, number of vulnerabilities and configurations errors.

4) It is recommended to support drilling detailed information on the asset security situation.

8.5.4 Abnormal user behaviours situational visualization

1) It is recommended to support presenting abnormal user behaviours of cloud computing platforms in multidimensions, including abnormal behaviour types, abnormal behaviour tendency and abnormal users (accounts or IPs).

2) It is recommended to support presenting real-time security alarms of abnormal user behaviours of the cloud computing platform, including alarm time, alarm types, severity levels and abnormal user (account).

3) It is recommended to support the drilling details of user abnormal behaviour information.

8.5.5 Customized security situational visualization

It is recommended to support configuring customized situational views of specific business scenarios, and support importing configurations graphically or by scripts, according to the business requirements, management roles and other individual requirements of the cloud computing platform.

Bibliography

[b-ITU-T X.1217] Recommendation ITU-T X.1217 (2021), *Guidelines for applying threat intelligence in telecommunication network operation.*

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2016), *Security framework for cloud computing.*

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-NIST-SP-800-30] NIST Special Publication 1800-30 Revision 1 (2012), *Guide for Conducting Risk Assessments*.

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

Published in Switzerland
Geneva, 2023