国际电信联盟
电信标准化部门

建议书

ITU-T X.1645 (09/2023)

X系列：数据网、开放系统通信和安全性

云计算安全 – 云计算安全最佳做法和导则

云计算网络安全态势感知平台的要求

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1-X.199
开放系统互连	X.200-X.299
网间互通	X.300-X.399
消息处理系统	X.400-X.499
号码簿	X.500-X.599
OSI组网和系统概貌	X.600-X.699
OSI管理	X.700-X.799
安全	X.800-X.849
OSI应用	X.850-X.899
开放分布式处理	X.900-X.999
信息和网络安全	X.1000-X.1099
安全应用和服务（1）	X.1100-X.1199
网络空间安全	X.1200-X.1299
安全应用和服务（2）	X.1300-X.1499
网络安全信息交换	X.1500-X.1599
云计算安全	X.1600-X.1699
云计算安全概述	X.1600-X.1601
云计算安全设计	X.1602-X.1639
云计算安全最佳做法和指导原则	**X.1640-X.1659**
云计算安全实施方案	X.1660-X.1679
其他云计算安全	X.1680-X.1699
量子通信	X.1700-X.1729
数据安全	X.1750-X.1799
IMT-2020安全	X.1800-X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1645建议书

云计算网络安全态势感知平台的要求

摘要

网络安全态势感知（NSSA）源于“态势感知”，通常包括数据采集、安全态势分析、安全态势评估和安全态势趋势预测四个过程，一般具有以下能力：1) 检测并持续监测各种攻击威胁、异常行为及其影响范围；2) 数据挖掘、威胁分析和追溯异常行为；3) 安全预测和早期预警；4) 安全态势可视化。

对于云计算服务提供商，NSSA平台在提升云计算的安全防护、安全漏洞或异常行为的检测能力、安全决策和应急响应能力方面发挥重要作用，甚至还有助于完善云计算的早期预警机制。

ITU-T X.1645建议书将首先介绍NSSA的概念和发展，分析NSSA在应对云计算的安全挑战方面的优势，以及记载NSSA平台的要求。

历史沿革 *

版本	建议书	批准时间	研究组	唯一ID
1.0	ITU-T X.1645	2023-09-08	17	11.1002/1000/15527

关键词

大数据分析、云计算网络安全态势感知、态势感知

* 欲查阅建议书，请在网络浏览器地址域键入URLhttps://handle.itu.int/，随后输入建议书的唯一识别码。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1645建议书

云计算网络安全态势感知平台的要求

1 范围

本建议书介绍了网络安全态势感知和云计算NSSA平台的要求。本建议书适用于云计算服务提供商。

2 参引

下列ITU-T建议书和其他参考文件的条款，通过在本文本中的引用而构成当前建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文件均面临修订；因此鼓励本建议书的使用者探讨使用下列建议书和其他参考文件最新版本的可能性。当前有效的ITT-T建议书清单定期出版。在本建议书中引用某个独立文件时，并未给予该文件建议书的地位。

无。

3 定义

3.1 他处定义的术语

本建议书使用了以下他处定义的术语：

3.1.1 云计算（cloud computing）[b-ITU-T Y.3500]：有助于网络以按需自助方式调配和管理获取一系列可伸缩和富有弹性的、可共享的物理或虚拟资源的范式。

3.1.2 云服务（cloud service）[b-ITU-T Y.3500]：通过使用定义的接口启动的、由云计算实现的一种或多种功能。

3.1.3 云服务客户（cloud service customer）[b-ITU-T Y.3500]：为使用云服务而具有业务关系的一方。

3.1.4 云服务提供商（cloud service provider）[b-ITU-T Y.3500]：提供云服务的一方。

3.1.5 漏洞（vulnerability） [b-NIST-SP-800-30]：可由威胁来源加以利用的信息系统、系统安全程序、内部控制或实施方案中存在的弱点。

3.1.6 威胁情报（threat intelligence）[b-ITU-T-X.1217]： 是经过组织、分析和提炼的、关于可能威胁某个组织的潜在和当前攻击的信息集合。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 态势感知（situational awareness）：评估给定环境中要素的当前状态以及它们在多个维度（包括时间和空间）上的关系的能力。

注 – 通过从各种来源收集数据、组合这些数据，然后进行分析来实现的。态势感知的目标是整合和分析来自不同来源的信息，以获得全面的理解。

3.2.2 网络安全态势感知（network security situational awareness）（NSSA）：确定和评估关键网络安全要素并使用时间和空间维度作为基础，根据规则对这些要素进行分类的能力。

注 – 这些信息评估网络的整体安全状况并通过采用统计分析、数据挖掘和人工智能等技术来预测新兴的网络安全趋势。获得的见解既可以以人类可读的格式来呈现，也可以作为网络安全自动化的输入。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

AI 人工智能
C&C 命令和控制
CRUD 创建、读取、更新和删除
CSC 云服务客户
CSP 云服务提供商
DDoS 分布式拒绝服务
DGA 域生成算法
HBase Hadoop数据库
IDS 入侵检测系统
IPS 入侵防御系统
JDBC Java数据库连接
MPP 大规模并行处理
NoSQL 不仅仅是结构化查询语言
NSSA 网络安全态势感知
ODBC 开放式数据库连接
SNMP 简单网络管理协议
SQL 结构化查询语言
VM 虚拟机
VPN 虚拟专用网络
WAF 网络应用防火墙

5 惯例

关键词“**要求**”（**is required to**）指必须严格遵守的要求，若宣称合乎本建议书，则不得有任何偏差。

关键词“**建议**”（**is recommended**）指建议的要求，而非绝对的要求。因此，宣称合规不必包括此项要求。

在本建议书及其附录中，会出现“**须**”（shall）、“**不得**”（shall not）、“**应**”（should）、“**可**”（may）等词语，在这些情况下，这些词语应分别理解为“要求”、“禁止”、“建议”和“可选”。这些短语或关键字出现在附录或明确标记为资料性的材料中时，应解释为没有规范性意图。

6 网络安全态势感知介绍

由于攻击者通常有明确的计划且长期渗透较为常见，因此当前的网络攻击已向精确攻击目标的方向发展。相应地，安全防御呈现出典型的“时间对抗”特征。在传统的安全架构中，各种安全组件或产品仅部署各自的防护规则、警告策略、日志处理和存储机制，而缺乏组件和产品之间的协调机制。这造成孤岛效应，它削弱了防御更隐秘和更专业高级攻击的能力。

网络安全态势感知（NSSA）源于“态势感知”，是网络安全中的一种特定应用，通常包括数据采集、安全态势分析、安全态势评估和安全态势趋势预测四个过程，一般具有以下能力：

– 检测并持续监测各种攻击威胁、包括异常行为及其影响范围；
– 数据挖掘、探究、威胁分析和异常行为溯源；
– 安全预测和早期预警；
– 安全态势可视化。

在网络安全情形下，信息不对称指的是以下场景，即攻击者比组织本身掌握更多关于组织系统、网络或流程的知识。在这种情况下，攻击者在策划和实施攻击时会处于优势地位。从解决攻击和防御之间的信息不对称以及加快事件响应和可追溯性而言，NSSA具有重要意义。

在此同时，大数据分析、云计算和人工智能（AI）的发展为NSSA的发展也带来了巨大的机遇和动力。例如，NSSA可以有效支持海量安全日志存储、借助大数据分析的利用和挖掘，实现对大规模网络安全态势的持续监测；AI的发展可以为NSSA提供更多的分析手段和风险预测能力，这可以有效提高预测精度；云计算的发展可以为NSSA提供更加灵活和稳定的基础架构。

NSSA平台的典型框架如图6-1所示：

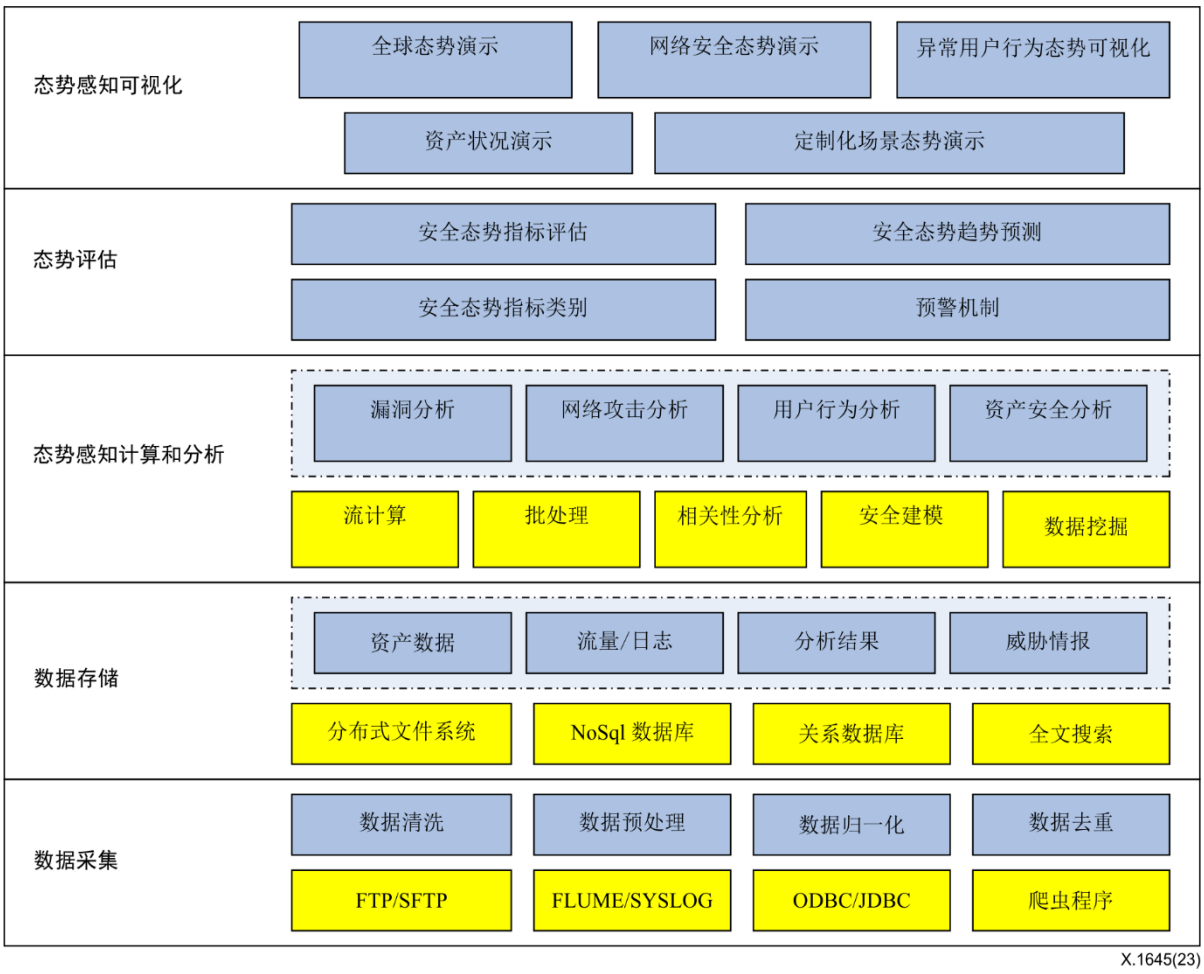

图6-1 – 网络安全态势感知平台的框架

7 分析

随着技术的快速发展和生态系统的成熟，云计算推出了新一代的关键信息基础设施。云计算带来了诸多好处，同时也面临下文所述的更多安全问题，尤其在运营和维护方面：

1) 随着规模的快速增长，部署在云计算基础设施中的各种安全组件涉及到海量的安全数据和重复的警告。这种场景使得操作和维护工程师难以在有限的时间窗口内进行处置。

2) 大多数安全组件相互隔离，这带来了明显的孤岛效应。这使得在云计算环境中很难提供良好协调的防御机制。

3) 云计算环境通常很复杂，并可能包括公共云、私有云以及混合云。因缺乏宏观的、整体的视角，这使得云计算服务提供商甚至云计算用户很难做出合理的安全决策。

NSSA是适合解决这些问题得一种技术。基于大数据技术，NSSA可以有效支持海量、异构安全日志的存储、使用和数据挖掘。进一步地，通过多个不同数据的相关性分析，可以有效地组织各种不同的安全组件，提高威胁的检测能力，并增加安全工程师的效率。NSSA还可以为云计算提供可视化的整体安全态势感知能力。同时，在NSSA使用AI技术非常方便，这有助于提高云计算安全态势感知的检测、诊断和预测能力。

因此，NSSA在提升云计算的安全防护、安全决策和应急响应能力方面发挥重要作用，甚至还有助于完善云计算服务提供商的早期预警机制。

同时，部署在云计算中的NSSA平台需要以下特定能力：

1) 数据采集应适应云计算中资产的动态变化，因为与传统IT架构相比，对云计算中的资产可以更灵活、更频繁地创建和移除。

2) NSSA平台应适应云计算服务的多租户共享资源使用和弹性资源管理等特点，这可能导致数据源的快速变化。租户及其服务的快速变化将相应地带来NSSA平台数据采集的变化。

3) NSSA平台应继续与云计算管理平台保持互动和协作，以访问云计算资源的运行状况、安全日志等各种数据，从而实现对云计算资源的深入洞察/感知，例如，NSSA不能绕过云管理平台来观察同一OSI第二层网络区域中虚拟机之间的网络连接。

4) NSSA平台应支持从多个云中访问数据的能力，以便为混合云或公共云中的用户提供统一的资产视角。

NSSA的应用和部署为上述技术挑战提供了可能的解决方案。NSSA能够从时间和空间两个维度全面、准确、精细地感知各种安全事件和异常行为，分析各种安全要素，了解整体安全态势，并预测其趋势，这将有助于提高云计算提供商的安全运营能力，支持安全决策和事件响应，并完善安全早期预警机制。

8 云计算网络安全态势感知平台的要求

8.1 数据采集的要求

8.1.1 数据采集机制

NSSA平台的采集节点应支持以主动或被动的方式收集各种类型的数据，如网络流量日志、系统日志、中间件日志、云计算基础设施的安全日志等。主动方式通过定期监测或扫描目标来收集数据，而被动方式主要通过从不同的数据源接收或导入数据来收集数据。

1) 需要数据采集支持主动方式，例如，通过扫描、爬取或简单网络管理协议（SNMP）等方式收集数据。

2) 需要数据采集支持被动方式，例如，通过syslog协议或NetFlow信道等接收数据，并手动导入数据。

数据采集能力应采用如下方式适应云计算环境：

1) 建议数据采集支持跨不同云收集数据，例如，多云和混合云。

2) 建议数据采集适应云计算环境的动态资源变化。

3) 建议数据采集支持收集云计算平台东西向网络流量的数据日志。

NSSA平台的采集节点还应具备以下能力：

1) 需要采集节点执行数据过滤和检查数据的有效性，例如，数据类型、取值范围等，并根据预先配置的策略过滤无效数据。

2) 建议采集节点在收集失败的情况下执行数据重新收集机制。

8.1.2 数据源

NSSA平台应支持对其数据采用创建、读取、更新和删除（CRUD）操作，并支持收集以下数据类型：

1) 需要支持收集云计算平台的资产数据，例如，虚拟资源池、网络设备、主机、安全设备、系统、软件和云计算管理平台的资产数据。

2) 需要支持收集各种类型的日志数据，例如，万维网访问日志、安全日志、业务操作日志和登录相关日志等，它们来自多个源，例如，主机、中间件和云计算管理平台等，并支持从其他系统接收日志分析结果。

3) 需要支持从云计算平台的多个设备和组件收集各种漏洞数据，例如，缓冲区溢出漏洞、注入漏洞、业务逻辑漏洞、设计漏洞、配置漏洞。

4) 需要支持收集多种网络攻击事件的数据，例如，DDoS攻击、漏洞利用攻击和未经授权的访问。

5) 需要支持收集威胁情报数据，例如，IP/域/URL的威胁情报、恶意样本、命令和控制（C&C）黑名单和漏洞。

8.1.3 数据预处理

为了满足数据质量的要求，NSSA平台需要对采集的数据进行数据清洗和过滤、标准化、关联和补全、合并和去重，然后存储标准化的数据。

1) 数据清洗：如果收集的数据中存在错误、不完整、无效等问题，则NSSA平台应支持通过以下方式进行数据清洗，包括：
   - 需要支持对数据格式不一致、数据录入错误和数据不完整的数据转换、处理和过滤。
   - 建议支持基于条件操作、正则表达式匹配和表达式计算的数据过滤和清洗。
   - 建议支持数据去重。

2) 数据标准化：NSSA平台应支持通过以下方式对各类异构数据进行统一格式化，并保存最初收集的数据，包括：
   - 需要支持基于每种数据类型的字段规则来标准化数据字段。
   - 建议通过正则表达式来支持对原始内容的统一格式化。
   - 建议支持保存初始收集的数据，以便支持后续的可追溯性分析和定制开发。

3) 数据关联和补全：建议NSSA平台支持标准化数据的数据关联和补全，包括用户信息、资产信息、地理位置信息和威胁情报信息，并建议支持选择特定的数据和字段来完成。

4) 数据合并：建议NSSA平台支持基于配置的规则来合并标准化数据，并建议支持选择特定的数据和字段来合并。

8.1.4 数据采集安全要求

1) 需要NSSA平台支持采集节点的访问控制，并监测数据采集过程，在出现异常事件的情况下及时告警。

2) 需要在数据收集过程中严格限制临时数据存储位置，不能随意修改。

3) 需要NSSA平台支持收集数据的分级分类和标识，并对敏感数据实施加密等安全保护，例如，资产数据、运营数据、日志数据等。

4) 需要NSSA平台支持在预处理和分析之前对敏感数据的数据屏蔽和脱敏，并满足收集数据的安全合规性要求。

5) 需要NSSA平台维护收集的运行日志，以便及时对异常事件和审计发出告警，包括以下内容：

- 需要审计用户和管理员的操作，以检测、告警和响应恶意行为，例如，数据滥用。
- 建议在数据收集期间对传输中断发出告警。
- 建议在数据收集和传输期间，若出现数据存储超过预设阈值，则发出告警。

8.2 数据存储要求

NSSA平台的数据存储应采用大数据技术，以满足云计算环境下产生的多源、多维和持续增长的数据存储需求，例如，分析结果和外部威胁情报。NSSA平台应支持根据不同领域和不同数据类型分类的存储机制，并满足不同数据分析和隔离方法的要求。同时，NSSA平台应确保存储数据的可用性、完整性和机密性。

8.2.1 数据存储分类

建议NSSA平台根据不同的数据源支持非结构化数据、结构化数据和半结构化数据的存储，并支持多种数据存储分类，包括关系数据存储、NoSQL（不仅仅是结构化查询语言）数据库、分布式文件存储和分布式全文搜索。

NSSA平台的数据存储分类建议如表8-1所述。

表8-1 – 数据分类

数据源	数据内容	数据量	存储分类 （建议）
云主机/容器/操作系统	操作日志、安全日志、运行状态数据、配置文件等	大	分布式文件存储/分布式全文搜索/ NoSQL数据库
云管理平台	访问日志、操作日志、配置文件、工作流数据等	中	分布式文件存储/分布式全文搜索/ NoSQL数据库
网络设备	路由器、交换机和网络平台的日志、路由表、配置文件等	大	分布式文件存储/分布式全文搜索/ NoSQL数据库
安全设备	防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）、虚拟专用网络（VPN）、网络应用防火墙（WAF）的日志、配置文件等	大	分布式文件存储/分布式全文搜索/ NoSQL数据库
应用系统	数据库、中间件、应用系统的日志、配置文件等	大	分布式文件存储/分布式全文搜索/ NoSQL数据库
基本数据	资产数据、账户数据、IP字典、服务数据等	中	关系数据库/分布式全文搜索/NoSQL数据库
网络流量	DPI数据、网络流量数据等	大	分布式文件存储
威胁情报	战略情报、战术情报、安全信息等	中	分布式文件存储/分布式全文搜索/ NoSQL数据库
分析结果	安全事件、合规性数据、安全指数等	中	关系数据库/分布式全文搜索/NoSQL数据库

8.2.2 数据存储的技术要求

NSSA平台应开发一个有弹性和可扩展的数据存储架构，以满足数据量的持续增长，以及数据分类和分级存储的需求。此外，数据存储生命周期应根据合规性规则、业务需求和经济成本而有所不同。

1) 建议NSSA平台支持主流关系数据库。建议关系数据库支持完整的关系模型访问接口，包括标准SQL接口、应用开发标准接口（JDBC、ODBC等）。

2) 建议NSSA平台支持主流NoSQL数据库。

3) 建议NSSA平台支持典型的大数据组件，例如，Hive、HBase和MPP组件，以支持扩展功能。

4) 建议NSSA平台采用全文检索组件，应支持关键词检索、多关键词检索、全文和其他字段的组合检索，以及前缀匹配、模糊匹配和其他检索条件。

5) 建议NSSA平台采用分布式消息总线组件，例如，Kafka、RabbitMQ等。分布式消息总线组件应支持数据压缩、设置数据保留时间和自动删除过期数据功能。

6) 建议NSSA平台支持在线存储和备份机制，以保证数据的可用性。

7) 建议NSSA平台支持元数据存储，主要包括：

   - 技术元数据并用于数据维护，例如，如何存储数据以实现高效的数据访问。
   - 管理元数据，例如，数据访问控制策略和数据处理结果。

8.2.3 数据存储的安全要求

1) 需要NSSA平台开发数据访问控制机制，例如，基于角色的数据存储访问控制，以防止未经授权的访问。

2) 需要NSSA平台支持对重要或敏感数据的数据存储加密。建议基于数据分类和分层定义，澄清各种数据类型的存储加密要求，例如，数据加密算法和加密密钥管理的要求。

3) 需要NSSA平台实施适当的技术和控制措施，以确保数据存储完整性和多副本数据一致性的有效性。

4) 需要NSSA平台实施适当的技术和控制措施，以确保数据存储的可用性。基于数据分类的原则，建议澄清各种数据的备份和恢复策略，例如备份模式、存储期限和恢复时间的要求。

5) 建议NSSA平台定期测试数据存储机制，以验证数据故障识别和备份重建能力。

6) 需要NSSA平台生成数据存储的所有处理日志，以确保数据存储过程的可追溯性，并提供对异常行为的预警能力。

8.3 态势计算和分析的要求

NSSA平台的态势计算和分析主要包括计算和分析引擎以及态势分析功能模块。

1) 计算和分析引擎为态势分析功能模块提供威胁建模和分析计算能力。计算和分析引擎包括安全建模和大数据计算框架，例如，离线计算引擎和实时计算。

2) 态势分析功能模块主要实现云计算环境下的网络安全态势分析，它基于对各种聚合资产数据的数据挖掘、探究和威胁分析，例如，安全事件、日志数据和网络流量数据。

3) 为了提高计算和分析的效率，需要在安全建模之前建立各种安全事件和资产信息的统一表示，这可以通过对背景的量化来实现。量化方法将背景映射到一个欧氏空间，这通常是采用各种人工智能算法进行相似性计算和相关性计算的一个前提。

8.3.1 计算和分析引擎的要求

8.3.1.1 安全建模

安全建模需要包括相关性建模、统计建模、威胁情报相关性建模和人工智能建模，提供对基本态势数据的深入分析和挖掘能力。

1) **相关性建模：**使用基于规则的匹配方法对异构和异质事件进行逻辑关联和特征匹配分析。
   - 需要支持基于安全事件因果关系的逻辑相关性分析。
   - 需要从多个方面支持多源异构数据的关联，例如，时间和空间。
   - 建议支持根据网络安全动态态势对告警信息进行聚类，以减少告警数量并提高响应效率。
2) **统计建模：**使用统计方法计算各种事件的定量特性，例如，频率和发生周期，并获取事件数据的分布、主要特性、时间序列的趋势、是否存在异常值和事件汇总结果。
   - 建议支持对安全事件、安全行为、安全威胁和其他特性进行统计分析，并从各种数据源中发现安全威胁的重要统计特性。
3) **威胁情报关联：**建议支持整合威胁情报能力，以在云计算环境中基于威胁情报发现准确的情报事件。
4) **人工智能建模：**建议支持各种内置的人工智能算法，包括时序算法、分类算法、聚类算法等算法原型，为用户提供对任意数据的学习和分析能力，并分析高级安全威胁和未知威胁。
   - 建议支持主流算法，例如，聚类分析、相关性分析、决策树分析、回归分析等人工智能/机器学习分析算法。
   - 建议NSSA平台支持集中管理安全建模和策略，以利于有效执行和快速部署。

8.3.1.2 大数据计算框架

需要同时支持离线和实时计算框架，以实现对静态数据的批处理和对动态数据（流数据）的实时分析。

1) **离线计算框架：**需要支持部署离线算法、训练模型和机器学习场景。分析师可以使用离线分析引擎来深入挖掘数据，对算法的输出结果进行即时反馈，提供模型训练能力。
2) **实时流计算框架：**建议实时计算框架支持分布式架构，并对存储容量可以动态进行调整。高可用性和读写分离策略可以确保离线数据分析时数据读写分离。

8.3.2 态势分析功能模块的要求

基于计算和分析引擎，态势分析功能模块针对各种资产数据、安全事件、日志数据、流量数据等数据建立基于场景的分析能力，并提供基于多种数据的安全分析场景，以实现基于场景的安全告警和早期预警能力。态势分析功能模块包括云计算环境下的网络安全分析、资产安全分析和高风险用户行为分析。

8.3.2.1 网络安全分析

需要网络安全分析模块具备分析云计算环境中各种网络攻击情况的能力，例如，异常网络流量、恶意程序传播和恶意域名访问，以及跟踪其变化趋势的能力。

1) 建议支持常见攻击总体态势的检测和统计分析，并分析当前攻击态势的变化趋势。
   - 建议支持基于多源数据的网络攻击检测和分析功能，包括网络入侵、万维网攻击、恶意软件、DdoS攻击、网络侦察、可疑活动和其他类型的网络攻击。
   - 建议支持对各类网络攻击的统计分析，以及对各类攻击趋势变化的分析。
2) 建议支持对云计算环境下异常网络流量总体态势的检测和统计分析，并分析当前异常网络流量的趋势变化。
   - 建议支持网络流量异常识别，可以基于常见病毒端口检测和分析协议异常流量。
   - 建议支持网络异常流量的统计分析以及协议异常流量的合并和统计，以及异常流量的趋势分析。
3) 建议支持对云计算环境下病毒、蠕虫和木马等恶意程序传播的整体态势进行分析，并分析当前恶意程序传播的趋势。
4) 建议支持对僵尸网络C&C主机和僵尸主机进行检测和统计分析，并支持对僵尸网络的传播和趋势变化进行分析。
5) 建议支持对恶意域名、C&CIP地址和域生成算法（DGA）域名的访问统计和传播进行分析。
6) 建议支持攻击链模型，以追踪攻击事件源。根据攻击过程对生成的安全事件进行分类，包括信息收集、网络入侵、C&C、水平渗透、目标实现和证据清洗。
7) 建议支持基于威胁情报对攻击者信息进行分析。

8.3.2.2 资产安全分析

需要支持对云计算平台各种资产的安全状况进行分析。建议通过安全设备日志、系统日志、漏洞扫描结果等数据，来分析云计算基础设施、虚拟机、容器和业务系统的安全状况。分析类型包括系统攻击分析和系统漏洞分析。

8.3.2.3 资产信息分析

1) 需要支持资产统计分析，包括基于资产分类、类别、优先级等的分析，以及资产状况更新，例如，添加或删除资产。
2) 需要支持资产分布分析，包括基于资产地理信息、部门财产和重要的万维网应用等的分析。
3) 需要支持根据资产IP地址、分类、优先级和地理信息等搜索和显示资产信息。

8.3.2.4 资产威胁分析

1) 需要支持对系统攻击威胁进行分析，包括日志破坏检测、系统权限提升检测、错误日志检测和暴力攻击。分析可以基于资产数据、设备日志、主机系统日志、安全系统数据和威胁情报的相关性分析来实施。
2) 需要支持对资产威胁进行统计分析和趋势分析。

8.3.2.5 资产漏洞分析

1) 需要支持对资产漏洞扫描结果和安全设备检测日志进行相关性分析，以执行漏洞利用分析，包括主机/虚拟机/容器漏洞分析和应用程序漏洞分析，并根据时间、业务系统、漏洞等级和其他维度数据对存在漏洞利用风险的资产进行统计分析。

8.3.2.6 资产配置的合规性分析

1) 需要支持在云计算环境中对操作系统、虚拟化软件、数据库、网络设备和中间件的配置合规性结果进行分析。

2) 需要支持对已发现的非合规项进行统计分析，并支持对利用非合规项攻击资产的攻击者进行风险分析。

8.3.2.7 用户行为分析

建议支持对访问云计算平台的内部用户的异常行为、对资产和业务系统的异常行为进行检测和分析，以及对用户行为的画像分析。

1) 建议支持对异常用户操作行为进行分析，包括对敏感数据的异常操作、过期账号登录、非法外联、敏感命令执行、暴力攻击和异常地址登录等。

2) 建议支持基于内部用户行为对用户进行画像，包括用户的个体行为特性和群体特性。

3) 建议支持对异常行为规则和行为模型进行定制。

4) 建议支持基于用户配置文件的异常行为分析，并将个人或群组的单日行为与历史行为数据进行对比，以挖掘异常。

5) 建议支持对各种云计算资源的异常行为进行分析，并可识别云计算环境中可能发生的异常行为，例如，云主机异常行为、异常调用系统工具、异常网络行为和非法对外通信等。

8.4 态势评估的要求

建议NSSA平台的态势评估支持对云计算环境中整体安全状况进行动态态势评估，在分析多维安全数据、云计算平台安全分析结果和态势指标类别评估建模的基础上，预测态势趋势。它支持发布早期预警，并与云服务提供商（CSP）/云服务客户（CSC）的安全决策和应急响应机制进行交互。

8.4.1 态势评估

安全态势评估的范围包括云平台的综合态势、云资产的安全态势、威胁、漏洞、网络攻击以及云平台及其组件的可用性状况等。

1) 需要收集资产信息作为数据源，以建立安全态势评估指标类别。资产信息应包括操作系统、中间件、应用程序和数据库的具体版本、网络拓扑位置、资产价值等，这将有助于生成合理的评估指标。

2) 需要通过创建统一尺度的安全态势测量通用指标，来支持云计算平台的安全态势评估指标类别，并量化网络安全态势的各种要素。

   - 建议为网络态势评估创建定性和定量指标。定性指标是基于专业安全分析师的主观评估。例如，安全分析师可以基于其经验为给定的漏洞或网络攻击指定严重性等级。定量指标来自原始数据的收集和分析。
   - 建议在处理威胁指标时支持相似性计算和相关性计算，包括以下内容：

- 建议使用威胁背景的相似性计算来识别容易激增的威胁，例如，扫描、暴力破解和DDoS攻击等，以便避免因大量重复告警而导致的特定指标的剧烈变化。
- 建议使用威胁和资产信息之间的相关性分析来识别盲目攻击和大规模尝试的威胁，这将有助于安全人员快速找到真正需要他们做出响应的高风险指标。
- 建议采用统一的算法框架来实现相关性分析和相似性分析，例如，角度余弦等。统一的算法框架可明显降低使用算法的维护成本。

- 建议创建网络安全态势评估的通用指标和细分指标。通用指标反映云计算平台安全评估的总体特性；细分指标可以分解为不同的组件或系统，反映不同组件/系统的态势评估结果的差异。
- 建议支持创建态势指标类别，包括以下内容：
  - 建议支持创建云计算平台的运营指标，例如，云资源池利用率和业务访问延迟等。
  - 建议支持创建网络安全威胁指标，包括各种网络安全事件，对这可以做进一步计算并在其频度和严重性方面进行评估。
  - 建议支持创建云资产安全评估的指标，例如，资产威胁和资产漏洞，包括漏洞严重性以及漏洞是否已修补等。
  - 建议支持创建用户行为安全指标，例如，用户是否有异常访问、登录、恶意软件下载行为等。还需要采用如数据脱敏和数据匿名等用户隐私保护技术来保护用户隐私。

3) 建议支持构建一个全面的安全态势评估机制或者基于分级、多维指标类别进行建模。
   - 需要支持不同细分指标的标准化，包括定性指标和定量指标，以避免因单位和幅度差异而导致评价结果的偏差。建议采用转换技术将定性指标转换为数值，以便做进一步计算或分析。
   - 建议支持多维态势评估机制，包括面向风险的评估、面向威胁的评估或基于时间序列数据的建模等。
   - 建议支持各种评估模型，包括基于数学理论模型的模型、基于知识的推理等。
   - 建议通过综合处理下层的态势指标来支持自下而上的分级评估方法，然后计算上层的态势评估结果；并逐步计算安全态势的总体评估。
   - 在分级评估方法中，建议通过与历史值和邻近值的比较，来支持对特定态势评估值可解释性的相似性计算。对于最终的评估值，可以通过选择其特定级别的先例结果来构建多维向量，并可使用该多维向量，通过角度余弦、空间向量距离等算法，来计算历史邻近值的相似性。相似性计算可以帮助安全人员更容易地发现异常，以及更准确地理解态势感知。
4) 建议通过实施日志预处理、关键字段索引、全文搜索和模糊查询等，来支持高效追溯云平台历史安全态势评估的能力。

8.4.2 态势趋势预测

在采集和跟踪云计算环境的安全状况、提取能够引起网络态势变化的安全要素和关键指标的基础上，建议NSSA平台支持基于面向云平台的安全态势预测模型来预测整体安全趋势、细分组件安全趋势和潜在安全风险。

1) 需要支持基于收集的数据和分析的结果构建一个分层、多维的指标类别，并通过相关的预测模型预测态势趋势。

2) 建议支持主流预测模型，包括专业领域中基于机器学习的回归预测模型、深度学习模型和基于微分方程的预测模型等。

3) 建议通过融合不同的预测模型，来支持计算预测结果，以提高预测精度，具体如下：

- 通过计算预测和数据结果之间的损失函数值，来监测每个模型的精度。
- 通过权重合并每个模型的结果，对模型之间的权重进行自适应调整。例如，可以基于损失函数的监测结果来自适应地调整每个模型的权重；还可以自动触发最新数据的离线训练，以更新模型和提高精度。

8.4.3 预警机制

NSSA平台应基于安全分析、态势评估和态势预测的结果，为云计算环境中的潜在安全风险提供早期预警机制。

1) 建议通过将漏洞与威胁情报数据、相关安全事件数据等相关联来提供资产漏洞的早期预警，并分析云平台资产的漏洞。

2) 建议支持基于预测趋势的潜在网络攻击早期预警，包括恶意扫描、万维网攻击、DDoS攻击、密码猜测攻击和系统漏洞攻击等。

3) 建议支持基于趋势预测的潜在用户异常行为早期预警，包括异常敏感数据操作、过期账户登录、高风险命令执行等。在发布预警前，需要使用数据脱敏和数据匿名技术来保护用户隐私。

4) 建议通过关联检测到的异常行为、威胁情报和原始日志等，来支持对未检测到的安全威胁的早期预警。

5) 早期预警机制包括以下内容：

- 建议支持基于预配置策略发出可相应定制的早期预警。
- 建议支持早期预警的分级管理，并根据重要性和严重性对预警级别进行分类。
- 建议支持通过API发出预警，第三方系统可以通过API接收预警并做出相应的响应。

8.5 态势可视化的要求

需要NSSA平台支持显示多种场景的安全态势，包括全球安全态势、网络安全态势、资产安全态势、定制安全态势等。同时，建议支持使用多种类型的视图来显示安全态势的详细信息，例如，雷达图、相关性信息图和威胁路径图等，并支持探究详细的安全信息。

8.5.1 全球安全态势可视化

1) 建议支持以分数或等级的方式呈现云计算平台全球安全的评估状况。

2) 建议支持图形化展现云计算平台的全球安全态势，包括风险排名、网络攻击趋势、漏洞和高风险用户行为等。

3) 建议支持呈现云计算平台中不同租户、不同业务运营和不同资产等的安全态势，并与历史数据进行比较，以显示趋势。

4) 建议支持对云计算平台中的网络安全事件、异常用户行为和资产安全状况发出实时聚合告警，并支持图形化探究这些告警的细节。

8.5.2 网络安全态势可视化

1) 建议支持多维度图形化呈现云计算平台的网络安全风险，包括网络攻击的统计分析结果、网络攻击类型、网络攻击的地理分布、异常网络流量、攻击的源IP和目的IP等。

2) 建议支持呈现云计算平台的实时安全告警，例如，网络攻击、异常网络流量和恶意程序等。告警信息包括时间戳、安全类型、严重程度、攻击的源IP和目的IP等。

3) 建议支持探究有关网络安全态势信息的细节。

8.5.3 资产安全态势可视化

1) 建议支持图形化呈现云计算平台的资产信息，例如，资产规模、资产类型、资产所有权和资产分布等。

2) 建议支持图形化呈现云计算平台的各种统计分析结果，包括资产漏洞、网络攻击和配置错误等。

3) 建议多维度支持云计算平台各类资产的实时安全风险，包括资产名称、资产IP、攻击类型、漏洞类型、漏洞数量、配置错误等。

4) 建议支持探究资产安全态势的详细信息。

8.5.4 异常用户行为态势可视化

1) 建议支持多维度呈现云计算平台的异常用户行为，包括异常行为类型、异常行为趋势和异常用户（账号或IP）等。

2) 建议支持提供云计算平台用户异常行为的实时安全告警，包括告警时间、告警类型、严重程度、异常用户（账号）等。

3) 建议支持探究有关用户异常行为信息的细节。

8.5.5 定制化安全态势可视化

建议根据云计算平台的业务要求、管理角色和其他个性化需求，支持配置特定业务场景的定制化态势视图，并支持图形化或脚本化导入配置。

参考文献

[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 onducting* Risk Assessments.

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2024年，日内瓦