ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团 体 标 准

T/CIIA XXXX—XXXX

“数盾”体系总体能力要求

General capability requirements for Data Shield System

（征求意见稿）

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中国信息协会 发布

目 次

前 言 IV

引 言 V

1 范围 1

2 规范性引用文件 1

3 术语和定义 2

4 缩略语 2

5 概述 3

5.1 构建原则 3

5.2 技术特征 3

5.3 体系框架 3

5.3.1 “数盾”总体能力要求框架图 *3*

5.3.2 “数盾”体系两级建设架构 *4*

6 总体要求 5

7 集群级能力要求 5

7.1 总体能力框架 5

7.2 技术能力要求 6

7.2.1 平台层 *6*

7.2.1.1 平应用能力要求 6

7.2.1.2 平台支撑能力要求 9

7.2.1.3 平台总线能力要求 11

7.2.1.4 平台安全管理能力要求 11

7.2.2 组件层 *12*

7.2.2.1 数据中心出口监测组件 12

7.2.2.2 互联网远程监测组件 13

7.2.2.3 集群骨干网监测组件 13

7.2.2.4 安全检查工具组件 13

7.2.2.5 公共基础设施组件 14

7.3 管理能力要求 15
7.3.1 组织架构 15
7.3.2 规章制度 16
7.3.3 运作机制 16
7.4 运营能力要求 16
7.4.1 日常安全运营服务 16
7.4.2 安全数据共享服务 16
7.4.3 安全应急响应服务 17
7.4.4 重大活动保障服务 17
7.4.5 安全检查评价服务 17
7.4.6 演习培训服务 17
8 数据中心能力要求 18
8.1 总体能力框架 18
8.2 技术能力要求 19
8.2.1 平台层 19
8.2.1.1 平台应用能力要求 19
8.2.1.2 平台支撑能力要求 22
8.2.1.3 平台总线接口 24
8.2.1.4 平台安全管理要求 24
8.2.2 组件层 25
8.2.2.1 网络基础设施安全组件 25
8.2.2.2 算力基础设施安全组件 26
8.2.2.3 密码基础设施组件 26
8.2.2.4 应用安全组件 27
8.2.2.5 数据安全组件 27
8.2.2.6 身份认证组件 28
8.3 管理能力要求 29
8.3.1 组织架构 29
8.3.2 规章制度 29
8.3.3 运作机制 29
8.4 运营能力要求 30
8.4.1 日常安全运营服务 30
8.4.2 安全应急响应服务 30

8.4.3 安全监管协同服务 30
8.4.4 重大活动保障服务 31
8.4.5 租户安全服务 31
参 考 文 献 32

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国信息协会提出并归口。

本文件起草单位：国家信息中心、北京大学、北京邮电大学、四川大学、北京工业大学、北京神州绿盟科技有限公司、天翼安全科技有限公司、杭州安恒信息技术股份有限公司、北京思特奇信息技术股份有限公司、北京明朝万达科技股份有限公司、深信服科技股份有限公司、长春吉大正元信息技术股份有限公司、首都信息发展股份有限公司、国科量子通信网络有限公司、联通数字科技有限公司、可信云科（北京）技术有限公司、郑州云智信安安全技术有限公司。

本文件主要起草人：杨绍亮、禄凯、国强、寿贝宁、席斐、肖俊宇、黄卉、张玲、李姗姗、谢安明、高健博、关志、辛阳、高明成、刘斌、陈兴蜀、兰晓、陈良国、胡俊、公备、周觐、叶晓虎、刘嘉奇、郝广宾、刘欢、张鑫、于建鹏、刘佳宁、边赢、周俊、金涛、季宇翔、陈刚刚、郭伟、王世彪、郭立彬、栗文科、赵彬琦、孔勇、俞晓舟、吴坤生、宋晓勇、李健、邢保存、刘丽娟、张晓庆、付跃、左崴东、缪亚军、蒋运平、林海、宋康、刘扬扬、郭翀、岳兴伟、郭宇鸣、彭铭、冯金龙

引　言

2020年12月，国家发展改革委会同中央网信办、工业和信息化部、国家能源局联合发布了《关于加快构建全国一体化大数据中心协同创新体系的指导意见》，提出“加快提升大数据安全水平，强化对算力和数据资源的安全防护，形成‘数盾’体系”的要求。《全国一体化大数据中心协同创新体系算力枢纽实施方案》明确指出，“加强对基础网络、数据中心、云平台、数据和应用的一体化安全保障，提高大数据安全可靠水平。加强对个人隐私等敏感信息的保护，确保基础设施和数据的安全。”2023年12月25日国家发展改革委、国家数据局、中央网信办、工业和信息化部、国家能源局联合印发《关于深入实施“东数西算”工程加快构建全国一体化算力网的实施意见》，推动各类新增算力向国家枢纽节点集聚，并提出完善算网安全保障体系要求：“打造自主创新的技术供给能力，强化国家枢纽节点自主防护能力，统一应急处置、统一安全监测、统一运行监控，构筑全生命周期的安全管控措施，实现集群内网络和数据安全‘可知、可视、可管、可控、可溯’，推动建设国家算力网基础安全服务保障平台，打造一体化的安全保障服务能力。”

2022年12月2日《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》要求：“在落实网络安全等级保护制度的基础上全面加强数据安全保护工作，健全网络和数据安全保护体系，提升纵深防护与综合防御能力。”2023年12月31日国家数据局等部门关于印发《“数据要素×”三年行动计划（2024—2026年）》的通知指出：“完善数据分类分级保护制度，落实网络安全等级保护、关键信息基础设施安全保护等制度，加强个人信息保护，提升数据安全保障水平。”

“数盾”体系提出了国家数据中心集群和集群内数据中心两级一体协同安全总体能力要求框架，分别从集群级和数据中心级两个层面，技术、管理、运营三个维度，指导数据中心集群主管单位、监管部门和数据中心企业构建安全风险监测预警、指挥调度和协同处置能力，实现贯穿基础网络、数据中心、云平台、应用等的安全风险实时动态监管和安全防护能力。指导集群内各数据中心在现有的网络安全防护能力的基础上，构建统一安全技术规范、统一内部数据交换接口和级联接口的一体协同的数据安全保障体系。

本标准是“数盾”体系相关系列规范性文件之一，是编制“数盾”体系其他标准规范文件的基本依据。本标准将“数盾”体系总体能力要求按照集群和数据中心各自特点和需求，分别从技术、管理和运营等三方面提出要求。技术能力要求从平台层和组件层两方面提出相关要求，为数据中心集群安全监督管理和数据中心安全防护提供技术方面指导。管理能力要求从组织架构、规章制度和运作机制三方面提出相关要求，为“数盾”体系的规划、设计和建设提供管理方面指导。运营能力要求分别对集群和数据中心各自主要运营场景提出相关要求，为“数盾”体系相关运营团队提供运营方面指导。

“数盾”体系总体能力要求

1 范围

本文件规定了“数盾”体系应具备的技术、管理和运营三方面的能力要求。

本文件适用于全国一体化算力网国家枢纽节点建设管理单位、承建单位及运营单位开展“数盾”体系的规划、设计、建设及运营等活动，也适用于指引政府、企业等数据安全防护体系建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 50174-2017 数据中心设计规范

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

GB/T 37973-2019 信息安全技术 大数据安全管理指南

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 42453-2023 信息安全技术 网络安全态势感知通用技术要求

GB/T 28827.1-2022 信息技术服务 运行维护

GB/T 32914-2023 信息安全技术 网络安全服务能力要求

T/ISC-0011-2021 数据安全治理能力评估方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

“数盾”体系

“数盾”体系是以提高海量数据流通、汇聚、融合场景下的算网基础设施、应用和数据安全可靠水平为核心目标，通过安全平台及相应安全组件构建的贯穿网络层、计算层、应用层、数据层的一体协同的安全保障能力体系。该体系以“数盾”配套标准规范为指导。

4 缩略语

下列缩略语适用于本文件。

ACK	确认（Acknowledge）
API	应用程序接口（Application Programming Interface）
ATT&CK	对抗策略、技巧与共同认知（Adversarial Tactics, Techniques, and Common Knowledge）
CPU	中央处理器（Central Processing Unit）
CVS	逗号分隔值（Comma-Separated Values）
EDR	端点检测与响应(Endpoint Detection & Response)
FTP	文件传输协议（File Transfer Protocol）
HTTP	超文本传输协议（Hypertext Transfer Protocol）
ICMP	互联网控制报文协议（Internet Control Message Protocol）
IDS	入侵检测系统（Intrusion Detection Systems）
IMAP	互联网消息访问协议（Internet Message Access Protocol）
IO	输入/输出（Input/Output）
IP	网际互连协议（Internet Protocol）
IPS	入侵防御系统（Intrusion Prevention Systems）
JSON	JS对象简谱（JavaScript Object Notation）
POP3	邮局协议第3版（Post Office Protocol version 3）
RDP	远程桌面协议（Remote Desktop Protocol）
SMB	服务器消息块协议（Server Message Block）
SMTP	简单邮件传输协议（Simple Mail Transfer Protocol）
SSH	安全外壳（Secure Shell）
SQL	结构化查询语言（Structured Query Language）
SYN	同步（Synchronization）
Syslog	系统日志(System Log)
UDP	用户数据报协议（User Datagram Protocol）
XSS	跨站脚本（Cross Site Scripting）

5 概述

5.1 构建原则

分层解耦：“数盾”体系把不同的功能模块划分成不同的层面，每个层面各自具有明确的功能定位，便于组织根据不同层面的数据安全需求进行设计、开发和运营。

异构兼容：“数盾”体系定义了各安全平台与组件相应的软硬件适配规范，以实现不同的安全组件与安全平台之间的兼容性和灵活对接，满足安全能力统筹调度协同，安全数据统一关联分析的需要。

按需扩展：“数盾”体系采用模块化设计理念，各安全平台与安全组件可以模块化构建，组织可以根据自身不同发展阶段安全需求，及新兴安全技术发展情况对自身的安全防护能力进行灵活扩展。

5.2 技术特征

标准化：通过在安全技术、安全服务方面标准化，构建“数盾”体系系列标准规范，指导开展安全平台和各安全组件的设计开发工作，以增强安全平台和组件之间的互通性和互操作性。

平台化：依托安全平台统一安全资源调度、统一安全能力编排、统一安全策略控制、统一安全数据分析、统一安全态势感知，实现可知、可视、可管、可控、可溯安全防护目标。

模块化：在标准化的基础上，通过对安全组件及安全平台服务能力原子化，使得安全平台可以快速集成各安全组件并按需扩充新的安全服务能力。

智能化：在安全数据实现统一汇聚的基础上，结合安全大模型的分析能力以及人工智能等创新技术，在大规模算力的支撑下，实现安全事件的快速发现、精准定位、及时响应和有效处置。

5.3 体系框架

5.3.1 “数盾”总体能力要求框架图

“数盾”一体协同的安全保障体系分别由技术能力、管理能力和运营能力三方面组成，每一方面又分为针对集群级和数据中心级的能力要求。

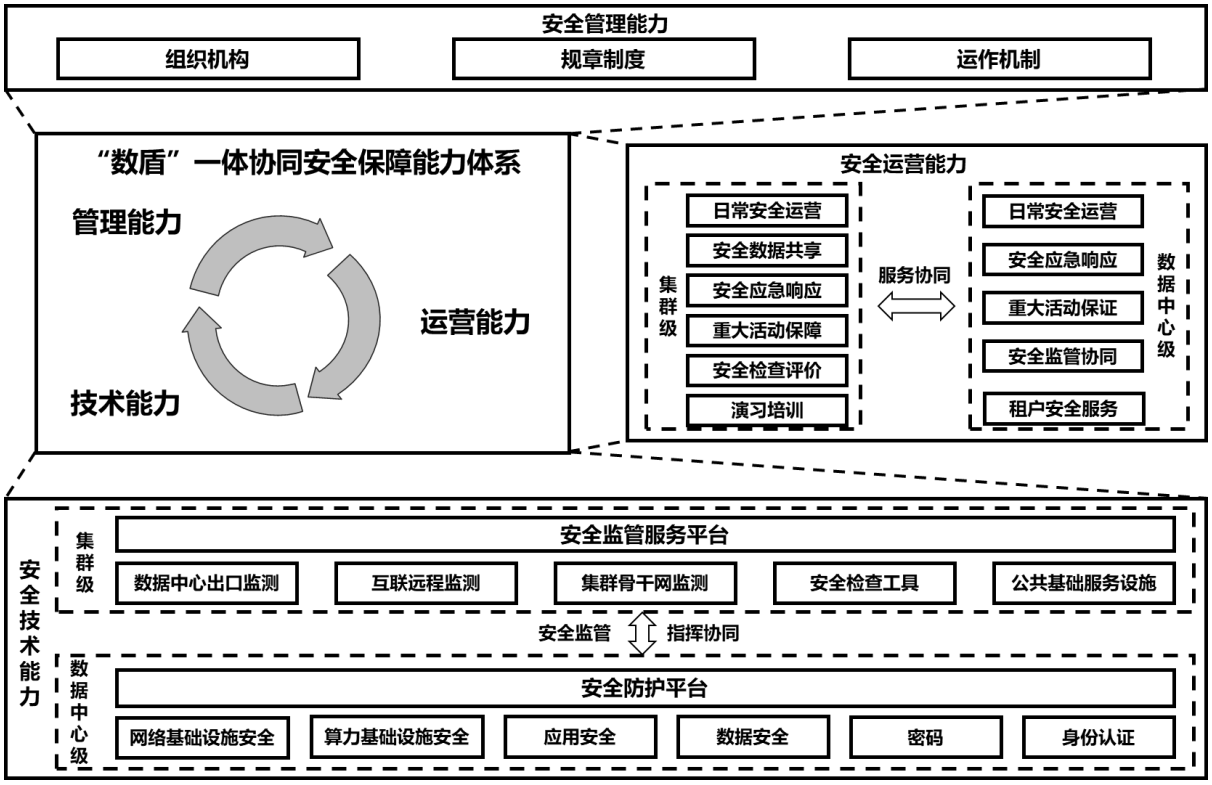

图1 “数盾”总体能力要求框架图

5.3.2 “数盾”体系两级建设架构

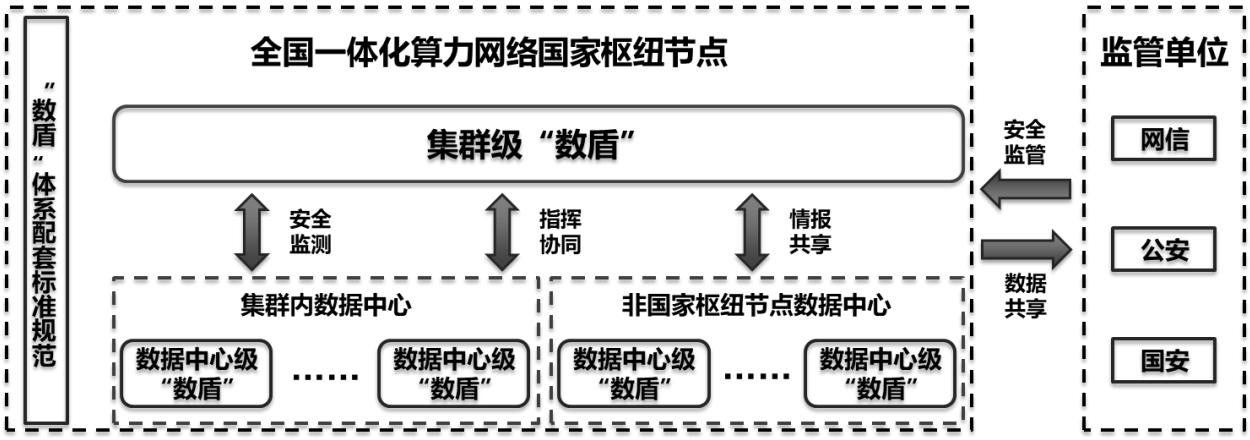

图2 “数盾”体系两级建设架构图

a) **集群级“数盾”：**是以当地数据中心集群建设的主管部门作为建设单位和责任主体，以数据安全体系化协同保护为核心目标，以安全信息共享为导向开展协同联防，统筹调度各所在地数据中心数据安全能力，构建安全监测、统一指挥、协同处置和安全服务共享的区域一体化安全防护能力。

b) **数据中心级“数盾”：**是以数据中心集群所在地各数据中心投资建设单位为责任主体，以数据安全防护能力建设为核心目标，重点从网络基础设施安全、算力基础设施安全、应用安全、

数据安全、身份安全、安全平台建设等维度，构建数据中心自身的安全防护能力和支撑所在集群一体协同的防护能力。

6 总体要求

a) 集群级“数盾”体系建设,参照第7章。数据中心级“数盾”体系建设，参照第8章；

b) 数据中心集群和数据中心的网络及信息系统，应落实国家网络安全等级保护制度相关要求，开展网络和信息系统的定级、备案、安全建设整改和等级测评等工作，并至少满足等级保护3级要求；

c) 运营关键信息基础设施的数据中心应满足关键信息基础设施安全保护要求。

7 集群级能力要求

7.1 总体能力框架

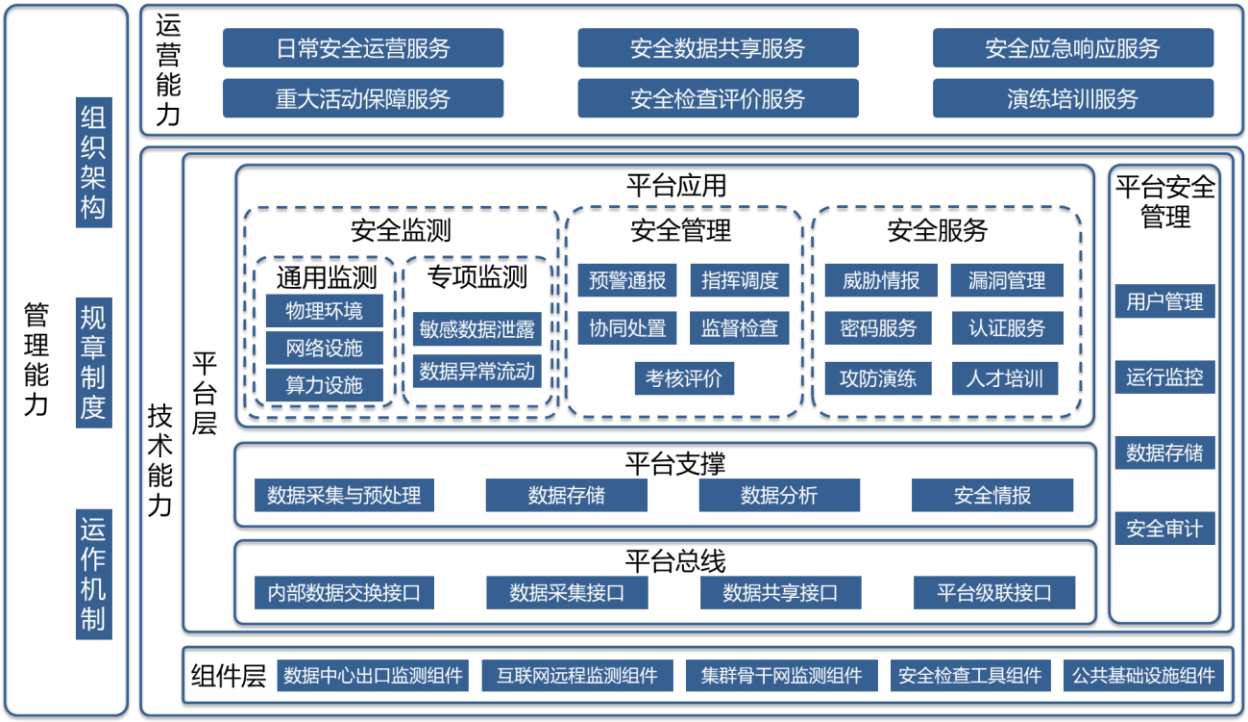

图3 集群级“数盾”总体能力要求框架图

集群级“数盾”体系能力要求由管理能力、技术能力和运营能力三部分要求组成：

a) **管理能力要求：**集群级“数盾”管理能力要求由组织架构、规章制度和运作机制三方面的能力要求构成。

b) **技术能力要求：**技术能力分为平台层和组件层两部分，平台层分别由平台应用、平台支撑、平台总线和平台安全管理四方面的能力构成：

(一) 平台层：

1) **平台应用：**根据集群级安全业务的需要，对数据中心集群各业务系统及所在地数据中心实现安全监测的同时，兼顾安全管理和安全服务；安全管理的同时，优化安全监测和安全服务；安全服务的同时，支撑安全监测和安全管理。

2) **平台支撑：**通过安全数据采集与预处理、数据存储、数据分析能力，汇集来自集群和集群所在地数据中心的安全数据以及外部权威机构的威胁情报数据，分析处理后为各平台应用提供支撑。

3) **平台总线：**利用内部数据交换接口、数据采集接口、数据共享接口和平台级联接口等实现集群和所在地数据中心之间监管数据的集中采集、转发、共享以及获取外部威胁情报等数据。

4) **平台安全管理：**包括用户管理、运行监控、数据存储和安全审计，为平台自身安全防护提供支撑。

（二）组件层：

是一组具有特定安全能力的基础安全组件的集合，为平台层提供必要的基础安全能力，集群级组件层主要由数据中心出口监测组件、互联网远程监测组件、集群骨干网监测组件、安全检查工具和公共基础设施组件五类安全组件构成。

c) **运营能力要求：**对集群级“数盾”运营中心主要的信息安全运营活动提出要求，包括日常安全运营服务、安全数据共享服务、安全应急响应服务、重大活动保障服务、安全检查评价服务和演习培训服务等。

7.2 技术能力要求

7.2.1 平台层

7.2.1.1 平应用能力要求

7.2.1.1.1 安全监测要求

7.2.1.1.1.1 通用监测

a) 应支持数据中心集群内公共区域物理环境安全风险监测，包括物理访问控制、防盗窃、防破坏、防雷击、防火、防水防潮、防静电、温湿度、电力供应等方面的物理安全风险；

b) 应支持数据中心集群区域内网络设施监测，分析所辖范围内各数据中心核心网络安全状况，识别网络安全风险及威胁，发现网络安全事件；

c) 应支持数据中心集群区域内算力设施监测，通过采集算力基础设施、区域重要单位以及重要单位的信息资产及其运行状态数据，监测算力基础设施安全、云平台、容器、应用等安全风险。

7.2.1.1.1.2 专项监测

a) 应支持敏感数据泄露监测，对互联网公开网站、在线文库、源代码托管平台、黑客交易论坛、暗网资源监控、公网暴露数据库等进行实时监测，发现数据中心集群范围数据泄露风险；

b) 应支持数据异常流通监测，包括但不限于敏感数据未经脱敏、加密跨域明文传输、偏离基线的大批量、异常时间共享交换等异常流动情况。

7.2.1.1.2 安全管理要求

7.2.1.1.2.1 预警通报

a) 应支持事件通报和风险预警能力，通过定制数据接口等方式完成通报预警工作，并持续跟踪和接收本区域内数据中心反馈；

b) 应支持基于数据分析结果和预警规则向通报预警模块推送重点事件，形成分级别通报预警信息；

c) 应支持根据预警级别和预警流程发布预警信息，预警信息内容包括但不限于预警类型、预警级别、威胁方式、涉及对象、影响程度、防范对策等；

d) 应支持按照根据安全事件通报流程进行事件通报，通报内容包括但不限于事件类型、攻击源IP、目的IP、事件级别、事件分析、影响程度和处置建议等；

e) 应支持平台、邮件、短信、即时通讯等预警和通报方式。

7.2.1.1.2.2 指挥调度

a) 应支持跨级“数盾”体系安全平台联动接口，接收上级或公安、网信等区域监管平台的网络及数据安全风险预警事件通报和事件处置的指令，协调网络安全支撑机构的力量共同处理；

b) 应支持跟踪事态发展变化情况、本地区受波及影响情况和处置进展情况，并及时通过系统接口报送至上级或区域监管部门；

c) 应支持数据中心集群重大网络安全保障时期重保人员、值班管理等业务需求，提供实战监控、指挥调度、签到报平安等能力，可实现对重保任务进行展示和统计分析。

7.2.1.1.2.3 协同处置

a) 应支持与区域监管单位、数据中心相关运营方、安全支撑企业等协同处置安全事件的能力；

b) 应支持向数据中心集群节点数据中心运营单位等相关方发送协同处置指令要求协同开展攻击溯源、取证分析、网络服务关停等处置工作，并反馈处置结果。

7.2.1.1.2.4 监督检查

a) 应支持对本区域内数据中心网络及数据安全监督检查任务管理，支持现场检查或单位自查的任务类型模式，将专项检查任务传达到被检查数据中心相关运营方单位闭环处理，监督检查任务支持包括检查单位、执行事件、任务类型、检查任务通告、被检查单位等多个维度进行设定任务；

b) 应支持对数据中心集群网络安全监督检查任务进行展示和统计分析，包括任务状态分布、任务类型分布、以及单位合格率排名。

7.2.1.1.2.5 考核评价

a) 应支持对数据中心集群所辖范围内的网络及数据安全考核评价指标体系的管理和创建，每个指标体系对应多个单项指标，支持设立具体的指标项，指标项应包含至少三级指标，指标中应包含评估内容、评估方式、计分方式、采集方式、分值等；

b) 应支持创建考核评价任务，支持被考核单位填报上传，支持对考核评价任务的跟踪管理，可查看当前任务名称、关联指标体系、考核时间、任务执行的上报进度、任务执行的评估进度。

7.2.1.1.3 安全服务要求

7.2.1.1.3.1 威胁情报

a) 应支持提供多源情报接入、管理和应用等能力，帮助数据中心集群建立自己的情报运营体系，提升威胁检测和响应能力；

b) 应支持提供情报云服务，可提供威胁情报查询服务；

c) 应支持对数据中心集群区域内发生的重大的漏洞、威胁事件，提供及时的威胁通告、详细的技术分析、影响范围、排查方法以及可落地的防护和处置建议；

d) 应支持基于情报的互联网资产核查服务，提供互联网风险监控、资产暴露面核查、移动端资产发现、风险情况监控等能力。

7.2.1.1.3.2 漏洞管理

a) 应支持为数据中心及租户相关系统提供统一的漏洞服务能力；

b) 应支持提供通用漏洞、漏洞事件信息的多源汇聚融合；

c) 应支持与数据中心集群保护对象的资产属性相结合，可以预警保护对象中潜在的资产脆弱性风险，并提供相关风险的漏洞修复建议；

7.2.1.1.3.3 密码服务

a) 应支持为数据中心及租户相关系统提供统一的密码服务能力；

b) 应支持数据中心及租户根据所需要的密码资源情况，在线上申请相应密码服务，并实现密码应用改造；

c) 应支持密码资源平滑扩容，保障各项密码服务满足云上多行业、多类型、多场景的信息系统的密码应用需求；

d) 应支持数据中心及租户实现其下密码资源的统一调度与管理。

7.2.1.1.3.4 认证服务

a) 应支持提供共性认证服务，依托身份认证基础设施资源，提供可信身份认证能力；

b） 应支持为算力设施、网络设施、应用设施、数据设施等提供统一认证门户，实现持续、动态授权控制能力。

7.2.1.1.3.5 攻防演练

a） 应支持围绕数据中心集群关键业务的可持续运行构建各类演练场景，场景以剧本的形式将复杂攻防过程分解成单个攻防技术，用户可在此环境上开展应急演练、战术推演等任务，包括但不限于APT演练场景、应急演练场景等；

b） 应支持根据用户需求生成各类仿真场景，提供攻防工具库、靶标资源、漏洞资源、自动化测试工具、流量仿真工具等能力，可支持用户开展漏洞研究、装备测试，技术验证等任务；

c） 应支持参考国家网络安全保障相关的标准规范创建各类网络对抗场景，并提供相应的工具支撑，方便用户开展各真实环境下的攻防对抗。

7.2.1.1.3.6 人才培训

a） 应支持提供各类网络安全培训课程，包括但不限于网络空间安全基础、专业、前沿技术等方向；

b） 应支持根据人才培养要求定制培养方案，并配套网络安全实训课程和考核；

c） 应支持为竞赛演练提供各类网络安全对抗场景，包括但不限于理论、解题、靶场和混战等比赛模式。

7.2.1.2 平台支撑能力要求

7.2.1.2.1 数据采集要求

a） 应支持多源异构数据的采集与解析，覆盖通信网络、区域边界以及计算环境等范围，包括但不限于数据中心集群区域内各类安全设备组件的监测数据、外部系统数据等；

b） 应支持通过多种方式采集安全数据，包括但不限于主动采集、被动采集、手动导入等方式；

c） 应支持对常见安全数据进行采集，包括但不限于网络流量、安全设备告警、安全日志、资产信息、脆弱性信息、威胁情报、应用日志等。

7.2.1.2.2 数据处理要求

a） 应支持根据数据的类型、来源、内容和格式的不同，执行数据筛选、数据转换、数据归并、数据补全和数据标签等操作；

b） 应支持自定义数据预处理规则，解析JSON、CSV、正则表达式等类型的数据，支持对解析提取的字段进行字段类型、名称、取值规范化。

7.2.1.2.3 数据存储要求

a） 应支持持久化存储各类安全数据，支持存储结构化、半结构化和非结构化等不同格式的数据，包括但不限于文字、样本文件、数据模型、关联规则以及其他二进制数据等类型；

b) 应支持对采集以及处理产生的数据进行分类存储，包括但不限于流量元数据、资产信息、日志数据、告警信息、威胁情报、安全事件、预警信息、知识数据等数据；

c) 应支持根据需要自定义数据存储的时间范围；

d) 应支持对重要数据和敏感数据进行加密存储；

e) 应支持配置策略以管理存储空间的使用情况，包括但不限于磁盘阈值告警策略、磁盘阈值自动清理存储数据策略、自动清理老化数据策略等。

7.2.1.2.4 数据分析要求

a) 应支持资产脆弱性分析的能力，能够发现的脆弱性信息，从不同维度进行统计分析，包括漏洞维度和资产维度：

1) 应支持根据漏洞等级、漏洞对系统、应用、服务的影响程度、威胁类型以及时间等维度进行统计分析，以便全面了解漏洞的分布情况；

2) 应支持根据漏洞影响的资产相关信息，进行多维度统计分析，查看漏洞在不同资产上的分布情况。

b) 应支持网络攻击分析，通过各类规则进行匹配，识别恶意特征，获取攻击属性、攻击路径以及攻击者等网络攻击信息：

1) 应支持识别各种常见网络攻击的能力；

2) 应支持按照网络攻击属性进行多维度进行分析的能力；

3) 应支持从攻击者视角进行攻击路径分析的能力；

4) 应支持建立攻击者画像的能力。

c) 应支持发现用户或实体的异常行为的能力，包括但不限于登录异常、访问异常、操作异常、数据下载异常、可疑域名访问等；

d) 应支持对各类安全事件进行关联分析的能力，对潜在安全事件、安全事件变化趋势等进行预测分析能力；

e) 应支持对数据生命周期内的安全风险分析，包括但不限于数据资源分布分析和流动过程分析、数据泄露风险分析等。

7.2.1.2.5 安全情报要求

a) 应支持多元情报接入：

1) 应支持支持开源情报和第三方商业情报的接入；

2) 应支持通过手工录入、批量导入、自动化接入私有情报数据，生成本地特色情报；

3) 应支持对情报源及情报类型的准确度进行评分；

4) 应支持对本地情报库中的数据进行批量生效/失效/删除等生命周期管理。

b) 应支持威胁情报分析、共享和使用：

1） 应支持对所有情报数据提供附加的情报关联分析能力，为平台应用追踪溯源提供情报支撑；

2） 应支持威胁情报关联检索能力，例如指定IP、域名、URL、漏洞编号、文件哈希等进行精确情报查询；

c） 应支持获取原始样本或数据,并对其进行归类、分析、加工、处理后生成威胁情报。

7.2.1.3 平台总线能力要求

7.2.1.3.1 通用要求

a） 应支持根据数据类型定义数据格式、数据协议和接口调用等；

b） 应支持安全认证及加密传输，保障在数据交换和推送过程中的可用性、完整性和保密性。

7.2.1.3.2 内部数据交换接口要求

应支持与内部不同系统模块之间进行数据共享交换，包括但不限于安全监测、协调指挥、检查评估、演习培训等模块。

7.2.1.3.3 数据采集接口要求

应支持与不同前端数据源组件进行数据交换，实现日志、告警信息、威胁信息、资产信息、用户信息、脆弱性信息、安全事件等安全数据的汇聚；

7.2.1.3.4 数据共享接口要求

a） 应支持与其他网络安全重点企业、技术机构等外部支撑系统的接口对接，获取威胁情报数据等。

b） 应支持与所在区域的相关监管单位进行数据共享，支持数据发送和接收，包括但不限于安全告警、安全事件、预警通报信息、威胁情报、协同指令信息等内容。

7.2.1.3.5 平台级联接口

应支持通过级联接口与上下级 “数盾”体系安全平台对接，支持数据的发送和接收，包括但不限于安全告警、安全事件、预警通报信息、协同指令信息等。

7.2.1.4 平台安全管理能力要求

7.2.1.4.1 用户管理

a） 应支持通过角色分离实现三权分立，包括系统管理员，操作员，审计员等角色；

b） 应支持用户管理能力，包括账户的创建、编辑、启停、注销等；

c） 应支持配置口令安全性策略，包括口令复杂度、口令历史、有效期、错误次数锁定等。

7.2.1.4.2 运行管理

a） 应支持界面可视化监控各节点运行状态，如CPU、内存、磁盘、网络IO等使用率趋势图、节点联通状态等；

b） 应支持配置系统CPU、内存、磁盘使用告警阈值，并支持邮件、SYSLOG告警通知能力。

c） 应支持对平台系统的认证、关键进程、安全策略、核心数据、敏感数据、关键参数进行安全保护。

7.2.1.4.3 数据存储

a） 应支持安全数据的分域隔离存储和在监管下的跨域数据互通。

b） 应支持对数据文件进行分布式存储，支持根据使用场景对热数据和冷数据进行不同方式的存储；

c） 应支持备份机制，部分数据丢失或损坏后可以快速恢复；

d） 应支持数据迁移，包括原始数据、处理结果数据、功能和规则配置数据等；

e） 应支持高可用部署，支持节点扩展，支持负载均衡。

f） 应支持使用加密工具对记录的用户名、口令、SSH用户名和SSH口令等关键信息进行加密。

7.2.1.4.4 日志审计

a） 应支持用户操作审计能力，记录用户的平台操作行为；

b） 应支持记录平台的运行日志；

c） 应支持技术手段保障审计日志不被篡改和删除。

7.2.2 组件层

7.2.2.1 数据中心出口监测组件

7.2.2.1.1 网络安全监测

a） 应支持网络攻击监测，对数据中心流量中的异常协议、网络欺骗、代码执行的攻击监测；

b） 应支持僵木蠕毒监测，包括但不限于HTTP、FTP、SMTP、POP3、IMAP、SMB等协议的安全监测；

c） 应支持拒绝服务攻击监测，包括但不限于对SYN Flood、ICMP Flood、UDP Flood和IP Flood的攻击监测；

d） 应支持威胁情报检测能力，实现基于威胁情报的风险监测。

7.2.2.1.2 应用安全监测

a） 应支持web威胁监测，包括但不限于Web扫描攻击、Webshell后门访问、SQL注入攻击、跨站脚本攻击、命令执行的威胁监测；

b） 应支持脆弱性风险监测，包括但不限于SMB漏洞、RDP漏洞、软件漏洞、系统漏洞等；

c） 应支持邮件威胁监测，包括但不限于垃圾邮件、恶意邮件、钓鱼邮件的安全监测；

d） 应支持异常行为检测，通过动态沙箱和静态沙箱识别恶意行为。

7.2.2.1.3 数据安全监测

a） 应支持数据流转监测，对重要数据流转节点进行安全监测；

b） 应支持数据泄露监测，包括但不限于对协议、文件、数据库传输敏感数据的安全监测。

7.2.2.2 互联网远程监测组件

a） 应支持互联网资产监测，通过IP地址监测发现互联网资产信息；

b） 应支持web脆弱性监测，包括但不限于注入类漏洞、失效身份认证漏洞、敏感信息泄露漏洞、失效访问控制漏洞等主流web应用安全漏洞监测；

c） 应支持安全事件监测，包括但不限于暗链、友情外链、坏链、黑页事件、JS挖矿脚本、网页挂马等安全事件；

d） 应支持可用性监测，包括IPv4和IPv6的可用性监测。

7.2.2.3 集群骨干网监测组件

7.2.2.3.1 异常流量威胁监测

a） 应支持拒绝服务攻击监测，对骨干网边界异常大流量等行为进行检测；

b） 应支持骨干网链路异常流量监测，对流入骨干网业务流量进行检测；

c） 应支持关键业务异常流量监测，对端口、协议、协议端口等组合特征的业务流量进行检测；

d） 应支持重要用户异常流量监测，对预定义源和目的IP地址、源和目的协议端口等组合特征的业务流量进行检测；

e） 应支持黑名单IP异常流量监测，对预定义源IP地址的流量进行检测;

f） 应支持情报生产能力，可根据异常流量进行情报生成及预警。

7.2.2.3.2 异常路由威胁监测

a） 应支持异常路由监测，对不可达的路由条目、路由环路等异常情况进行检测；

b） 应支持路由变化监测，通过路由基线数据来对发生变化的路由条目进行检测；

c） 应支持情报生产能力，可根据异常路由进行情报生成及预警。

7.2.2.3.3 异常 DNS 解析威胁监测

a） 应支持DNS异常解析检测，对无法解析、解析错误、解析响应时间异常缓慢等进行识别；

b） 应支持DNS恶意解析检测，对恶意劫持解析、缓存污染、解析黑洞、误导性解析进行识别；

c） 应支持DGA域名检测，通过深度学习模型来识别恶意域名；

d） 应支持情报生产能力，可根据异常DNS进行情报生成及预警。

7.2.2.4 安全检查工具组件

7.2.2.4.1 数据安全风险检查

a） 应支持基于重要数据规则来识别传输的数据是否存在重要数据，包括但不限于个人敏感信息、商业敏感信息和国家敏感信息等；

b) 应支持网络恶意外联行为检查，包括但不限于主机、云平台、数据库、大数据平台、其他重要数据载体等外联行为检测；

c) 应支持数据接口安全分析检查，包括但不限于数据接口漏洞检测、数据接口有效身份认证、攻击入侵线索分析等。

7.2.2.4.2 网络安全事件检查

a) 应支持解析安全事件发生的重要痕迹、成因，辨析攻击者IP、攻击手法、攻击轨迹，提取关联证据，形成整体的网络安全事件分析报告；

b) 应支持不同类型工具，包括但不限于漏洞扫描工具集、病毒检测工具集、信息采集工具集；

c) 应支持安全事件处置，包括但不限于黑客攻击、木马病毒、异常流量、Web攻击、拒绝服务等。

7.2.2.4.3 网络安全防御评估

a) 应支持从防护设备视角对防火墙、IPS/IDS、web防火墙、EDR等防护能力的验证测试；

b) 应支持从安全区域威胁视角，对高频攻击威胁的模拟验证及防御评估；

c) 应支持从专项威胁视角，对暴力破解、非法外联、勒索病毒等专项威胁进行模拟验证及防御评估。

7.2.2.5 公共基础设施组件

7.2.2.5.1 密码设施

a) 应支持采用多台云密码机建设密码运算资源池，为用户业务系统提供加密解密运算、签名验证运算、摘要值运算等功能；

b) 可使用抗量子计算技术的密码应用系统作为密码基础设施组件；

c) 应支持提供基于密码资源池面向云环境中重要资源如云上应用系统、云平台、云管平台等覆盖认证、传输、存储等机密性、完整性以及不可否认性的要求；

d) 应支持解决不同环节中数据生命周期安全，包括敏感数据加密、数据库加密、大数据加密、密文检索、透明数据加密、数据密钥权限管理服务。

7.2.2.5.2 身份认证

a) 应支持支持统一集中的账号全生命周期管理能力，覆盖账号创建到删除的全生命周期过程；

b) 应支持多认证方式，支持对二次认证链、场景化认证策略进行自定义编排组合；

c) 应支持RBAC、GBAC授权模型，基于用户角色、所在组织进行授权；

d) 应支持按应用分类以及应用名称授予权限。

7.2.2.5.3 威胁情报

a) 应支持基于本地网络流量或安全设备日志，重点监测针对本地关键信息基础设施及重要系统的攻击行为，输出本地专属情报，包含但不限于木马攻击、僵尸网络、蠕虫病毒等线索；

b) 应支持提供对命中的情报进行深度分析，如威胁类型命中分析等，可提供详情数据供用户进行多维度深入分析；

c) 应支持情报源接入与管理，提供插件式多源接入能力；

7.2.2.5.4 漏洞管理

a) 应支持调度所纳管的扫描设备，进行对应类型扫描任务的执行，完成对目标资产的漏洞扫描、资产发现、弱口令扫描、配置核查等检查工作；

b) 应支持不同厂商、不同类型、不同来源方式的各类脆弱性数据格式化、标准化、融合处理；

c) 应支持对于扫描发现的脆弱性问题按照顺序依次进行相关评估，计算分析业务域脆弱性值。

7.3 管理能力要求

7.3.1 组织架构

a) 应在数据中心集群所在地成立“数盾”建设管理领导机构，由集群当地主要领导担任第一责任人，负责集群“数盾”体系建设管理的整体规划和统筹协调：

1) 对“数盾”体系建设进行整体规划，统筹数据中心集群安全需求，明确“数盾”体系建设管理的主要目标、基本要求、工作任务；

2) 对“数盾”体系建设进行统筹协调，明确各部门职责分工、落实主体责任，构建全方位、多层级、一体化安全防护体系，形成跨部门、跨层级、跨行业的协同联动机制，加大人力、物力、财力的支持和保障力度。

b) “数盾”建设领导小组应授权当地数据中心集群建设管理单位负责集群级“数盾”体系建设管理的具体工作：

1) 对所在地的各数据中心级“数盾”建设管理单位的“数盾”体系相关规划、制度和建设落实情况进行监督检查；

2) 对所在地的各数据中心级“数盾”建设管理单位发生的信息安全事件或问题进行协同处置；

3) 对所在地的各数据中心级“数盾”建设管理单位的安全能力建设情况进行考核评估；

4) 对所在地的各数据中心级“数盾”建设管理单位的违反相关规定和政策的行为进行定责问责；

5) 对本集群其它集群级业务建设管理单位提供安全合规保障和按需安全服务。

c) 应成立集群级的“数盾”运营单位，在集群级“数盾”建设管理单位的指导下，进行具体的集群级“数盾”安全建设和安全运营，整合集群安全资源，控制集群安全风险以及最佳安全实践的推广，以保障集群级“数盾”的安全运营。

7.3.2 规章制度

应结合数据中心集群所在地的实际情况，编制适合当地的《“数盾”体系管理办法》，并在此框架下，制定相应的规章制度：

a) 明确项目建设预算中安全经费的比例，制定“数盾”体系资金保障制度；
b) 保障安全人员的数量、质量和培训等，制定“数盾”体系人才保障制度；
c) 明确联动协同工作的范围、内容、流程，制定“数盾”体系协同运作制度；
d) 明确考核评估标准以及办法，制定“数盾”体系考核评估制度；
e) 明确建设方的工作和职责，从对技术规范、质量管理、验收交付等方面对建设提出要求，制定“数盾”体系建设项目管理制度；
f) 明确“数盾”体系运营方的工作和职责，对“数盾”体系的运营服务管理提出要求，制定“数盾”体系运营管理制度。

7.3.3 运作机制

a) 应建立通报预警机制，发生重大安全事件时对上下各方进行通报和预警；
b) 应建立指挥协同机制，为相关方建立完善的沟通协作机制，如建立完善的沟通渠道和平台等。
c) 应建立监督检查机制，实现事前审批、事中留痕、事后可追溯的安全运行监管机制；
d) 应建立考核评估机制，统筹优化考核标准、推动安全风险认定标准化并增强考核执行力；
e) 应建立追因问责机制，明确数据流转全流程中的各方权利义务和法律责任，按照“谁管理，谁负责”和“谁使用，谁负责”的原则进行追责。

7.4 运营能力要求

7.4.1 日常安全运营服务

a) 应设置数据中心集群日常安全运营团队，包括管理人员和技术人员，明确岗位职责和人员要求；
b) 应制定数据中心集群日常安全运营总体方针，并形成配套的制度、标准、操作规程等；
c) 应建立数据中心集群日常安全监测预警机制，监测集群及各数据中心节点物理环境、网络设施、算力设施、数据及应用系统状态信息,及时发现安全风险,并向相关单位通报。

7.4.2 安全数据共享服务

a) 应提供共享支撑服务，结合上级监管机关要求，完成数据梳理上报工作，包括但不限于资产数据、网络安全事件数据、安全报告数据等；
b) 应支持结合安全防护需求，梳理数据中心集群相关威胁情报数据，为数据中心级“数盾”体系安全平台提供网络安全情报数据共享服务。

7.4.3 安全应急响应服务

a) 应设置数据中心集群安全应急响应团队，包括应急指挥小组和应急处置小组，明确职责和人员要求；
b) 应制定数据中心集群级应急预案，并定期开展应急预案演练，应当按照事件发生后的危害程度、影响范围等因素对安全事件进行分级，并规定相应的应急处置措施；
c) 应建立数据中心集群级安全应急处置机制，发生安全事件时，及时启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向相关单位公布有关信息；
d) 应建立安全事件协同处置机制，发生集群级或涉及多个数据中心的安全事件后，及时协调各方资源，开展应急响应处置；
e) 应当在安全事件处置完毕后五个工作日内向上级主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。

7.4.4 重大活动保障服务

a) 应设置数据中心集群重保运营团队，并指定接口人与各数据中心对接，建立集群与数据中心之间的沟通协调机制，在重保服务期间，可根据需要对各数据中心进行统一协调指挥；
b) 应制定数据中心集群重保服务方案，明确保护目标、范围、人员安排、重保阶段划分、值班计划及预案等事宜；
c) 应在重保活动结束后开展重保活动总结评价，提供集群级重保服务总结报告，并对各数据中心的保障活动进行评价。

7.4.5 安全检查评价服务

a) 应建立数据中心集群安全检查评价机制，定期对集群内部及各数据中心安全工作开展情况进行合规检查，提出改进优化意见，并监督跟进改进结果；
b) 应依据相关国家安全标准与政策要求制定数据中心集群安全检查评价标准，确保考核评价工作有法可依、规范科学。

7.4.6 演习培训服务

a) 应制定数据中心集群攻防演习方案，明确攻防演习的目标、流程、资源保障等内容，并定期或根据需要开展实战攻防演习，对演习结果进行总结评价；
b) 应支持安全培训服务，培训对象包括但不限于数据中心集群内部人员、外部用户，培训内容包括但不限于安全意识培训、安全技能培训、安全事件应急处置专项培训等。

8 数据中心能力要求

8.1 总体能力框架

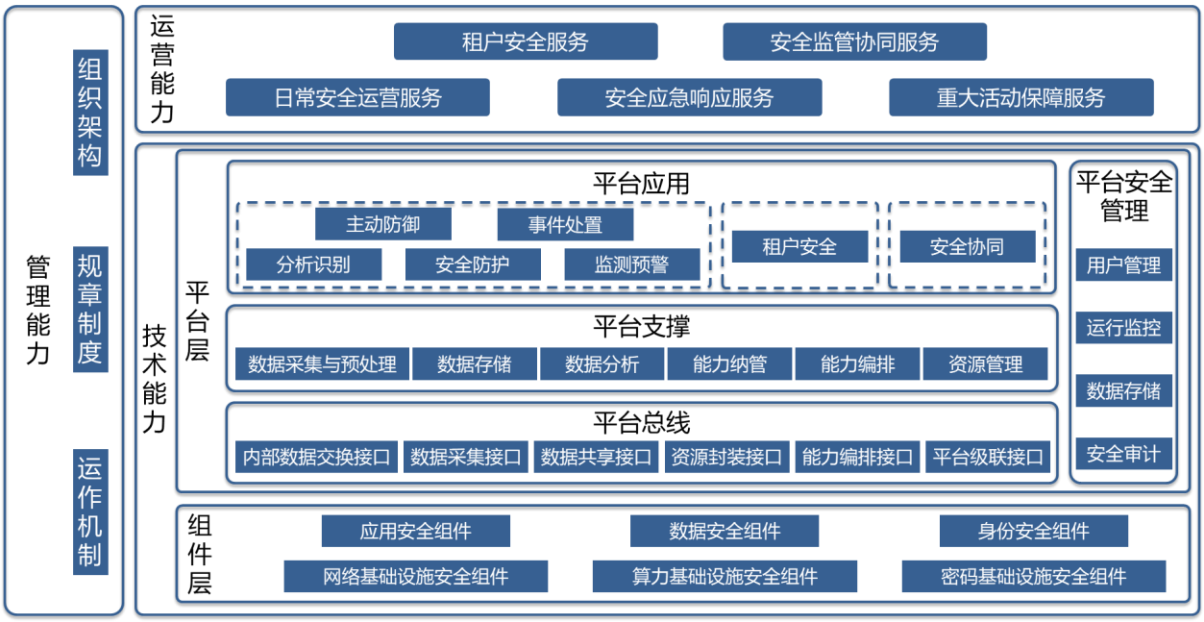

图4 数据中心级“数盾”总体能力要求框架图

数据中心级“数盾”体系能力要求由管理能力、技术能力和运营能力三部分要求组成：

a) **管理能力要求：**数据中心级“数盾”管理能力要求由组织架构、规章制度和运作机制三方面的能力要求构成。

b) **技术能力要求：**技术能力分为平台层和组件层两部分，平台层分别由平台应用、平台支撑、平台总线和平台安全管理四方面能力构成：

（一）平台层：

1) **平台应用：**根据数据中心级安全业务的需要，对所在数据中心实现资产和脆弱性分析识别、安全防护、监测预警、主动防御、安全事件处置和租户安全，并对所属集群的安全监管要求提供一体化协同支撑。

2) **平台支撑：**通过安全数据采集与预处理、数据存储、数据分析、能力纳管、能力编排和资源管理能力，汇集数据中心安全数据、纳管数据中心各安全组件，为各平台应用提供支撑。

3) **平台总线：**通过内部数据交换接口、数据采集接口、数据共享接口实现本数据中心安全数据的集中采集、转发、共享，通过资源封装接口、能力编排接口实现本数据中心对各安全组件纳管、编排，通过平台级联接口实现对所属集群监管数据的共享。

4) **平台安全管理：**包括用户管理、运行监控、数据存储和安全审计，为平台自身安全防护提供支撑。

（二）组件层：

是一组具有特定安全能力的基础安全组件的集合，为平台层提供必要的基础安全能力，数据中心级组件层主要由网络基础设施安全组件、算力基础设施安全组件、密码基础设施安全组件、应用安全组件、数据安全组件和身份安全组件六类安全组件构成。

c） **运营能力要求：**对数据中心级“数盾”运营中心主要的信息安全运营活动提出要求，包括日常安全运营服务、安全应急响应服务、重大活动保障服务、租户安全服务和安全监管协同服务等。

8.2 技术能力要求

8.2.1 平台层

8.2.1.1 平台应用能力要求

8.2.1.1.1 分析识别要求

8.2.1.1.1.1 资产管理

a） 应支持资产管理的功能，支持对通过“数盾”组件资产识别能力或采用人工添加方式获取IT资产和数据资产信息进行管理，建立资产基础信息库；

b） 应支持记录资产的属性信息，支持按照属性对资产进行分组管理；

c） 应支持资产的入库、变更、退库等生命周期管理；

d） 应支持资产画像，包括但不限于资产的漏洞信息、弱口令信息、不合规信息、威胁信息、安全事件信息、指纹信息、属性信息等。

8.2.1.1.1.2 脆弱性管理

a） 应支持脆弱性管理的功能，支持对通过“数盾”组件脆弱性识别能力或采用人工添加方式获取的系统漏洞、web漏洞、不合规配置等脆弱性信息进行管理，建立资产脆弱性信息库；

b） 应支持脆弱性的生命周期管理，支持通过工单派发、漏洞验证、调用“数盾”组件防护能力等方式对脆弱性进行闭环处置。

8.2.1.1.2 安全防护要求

8.2.1.1.2.1 安全策略

应支持统一的安全策略管理，实现安全策略的创建、变更、同步、删除等操作，包括但不限于以下安全策略配置要求；

a） 应支持数据安全防护的策略管理，包括但不限于数据库防护策略、数据传输安全策略、数据防泄露策略、数据加密策略、数据脱敏策略、数据容灾备份策略；

b） 应支持网络防护策略的管理，包括但不限于流量过滤策略、流量监控策略、流量阻断策略；

c） 应支持主机防护策略的管理，包括但不限于各类终端、服务器、云主机等主机防护策略；

d) 应支持密码基础策略的管理，包括但不限于加密通信策略、身份鉴别策略、完整性鉴别策略、非否认性鉴别策略；

e) 应支持云原生安全策略的管理，包括但不限于容器安全策略、服务器安全策略、日志安全策略、开发安全策略；

f) 应支持身份与访问控制策略的管理，包括但不限于用户管理策略、认证管理策略、权限管理策略；

g) 应支持应用安全策略的管理，包括但不限于Web、邮件等应用服务防护策略。

8.2.1.1.3 监测告警要求

8.2.1.1.3.1 安全监测

a) 应支持基于监测策略，指定监测对象范围和监测内容对数据中心的安全风险状况进行监测，包括但不限于资产风险、网络攻击、异常流量、脆弱性、异常行为、数据安全风险等；

b) 应支持监测对象范围基于资产的属性进行筛选，包括但不限于所属安全区域、所属业务系统、资产重要程度、物理位置等；

c) 应支持监测结果体现相关安全风险的关键属性，例如关联资产、攻击链阶段、ATT&CK映射、关联情报、载荷信息、关联流量上下文信息、原始告警日志、开始结束时间等；

8.2.1.1.3.2 态势展示

a) 态势展示方式要求

1) 应支持对整体安全状况用分值或等级等方式进行评估和展示；

2) 应支持对不同时间段的整体网络安全状况进行评估和展示；

3) 应支持采用多种视图展示整体安全状况，包括雷达图、地理信息图、关联关系图、威胁路径图、趋势图、同/环比图、柱状图等；

4) 应支持根据应用场景进行不同类型专题态势的评估和展示。

b) 态势展示内容要求

1) 预警展示内容应满足GB/T 42453-2023中6.3.2的要求；

2) 应支持资产画像展示能力，评估和展示资产的安全状况和风险等级；

3) 应支持数据安全态势展示，包括数据资产的总体情况、数据安全事件总体情况和数据安全合规情况等。

8.2.1.1.4 主动防御要求

8.2.1.1.4.1 溯源取证

a) 应支持对安全事件进行调查取证，取证信息包括告警溯源信息和关联的原始日志等；

b） 应支持攻击者画像，包括攻击者基础信息、攻击者浏览器指纹、攻击者地理信息、攻击者社交信息、攻击者关联情报信息和攻击者攻击轨迹信息，支持对攻击者进行封堵、加入白名单、手动通告等处置；

c） 应支持通过“数盾”组件的安全检测能力，获取原始流量信息进行流量取证。

8.2.1.1.4.2 情报支撑

a） 应支持威胁情报与资产、漏洞、威胁的关联；

b） 应支持主动模式和被动模式自动获取威胁情报数据，支持手动导入离线威胁情报文件；

c） 应支持威胁情报接入后的本地化存储与查询，可在线查询情报，支持情报预警。

8.2.1.1.5 事件处置要求

8.2.1.1.5.1 响应处置

a） 应支持通过“数盾”组件相关安全能力进行事件响应的能力，支持IP封堵、主机隔离、流量清洗等；

b） 应支持基于分析研判结果进行安全编排和调度，支持预置或自定义自动化脚本进行闭环处置；

c） 应支持多种策略编排动作，包括但不限于封堵、通知、工单等，同时支持编排动作的灵活扩展机制。

8.2.1.1.5.2 工单管理

应支持工单管理的功能，支持基于告警响应动作创建工单的工作流程。

8.2.1.1.6 租户安全要求

8.2.1.1.6.1 服务发布

a） 应支持服务目录能力，“数盾”运营者可在服务目录中注册“数盾”运营服务，设置服务规格与相应的计费规则，并关联涉及的安全组件；

b） 应支持服务发布能力，“数盾”运营者可发布服务目录中相关服务。

8.2.1.1.6.2 订阅运营

a） 应支持服务订阅能力，“数盾”服务对象可按需订阅“数盾”发布的服务或产品；

b） 应支持根据“数盾”服务对象订阅的服务提供相应的安全运营能力，包括但不限于资产管理、事件管理、产品与服务管理等能力。

8.2.1.1.7 安全协同要求

8.2.1.1.7.1 信息共享

a） 应支持纵向与数据中心集群级“数盾”体系安全平台的安全数据贯通和安全业务协同，横向与监管部门、安全技术支撑单位的安全数据共享；

b） 应支持提供自动化的注册管理接口和数据传输接口，以便实现各部门之间的信息共享交换。

8.2.1.1.7.2 协同支撑

a) 应支持接收、处理数据中心集群等监督管理部门下发的协同处置指令，协同处置安全事件；

b) 应支持攻击事件应急处置，开展攻击溯源、取证分析、网络服务关停等处置工作并反馈处置结果，完成协同任务处置。

8.2.1.2 平台支撑能力要求

8.2.1.2.1 数据采集要求

a) 应支持多源异构数据的采集与解析，覆盖通信网络、区域边界以及计算环境等范围，包括但不限于网络空间内各类安全设备组件的监测数据、外部系统数据等；

b) 应支持通过多种方式采集安全数据，包括但不限于主动采集、被动采集、手动导入等方式；

c) 应支持对常见安全数据进行采集，包括但不限于网络流量、安全设备告警、安全日志、资产信息、脆弱性信息、威胁情报、应用日志等。

8.2.1.2.2 数据处理要求

a) 应支持根据数据的类型、来源、内容和格式的不同，执行数据筛选、数据转换、数据归并、数据补全和数据标签等操作；

b) 应支持自定义数据预处理规则，解析JSON、CSV、正则表达式等类型的数据，支持对解析提取的字段进行字段类型、名称、取值规范化。

8.2.1.2.3 数据存储要求

a) 应支持持久化存储各类安全数据，支持存储结构化、半结构化和非结构化等不同格式的数据，包括但不限于文字、样本文件、数据模型、关联规则以及其他二进制数据等类型；

b) 应支持对采集以及处理产生的数据进行分类存储，包括但不限于流量元数据、资产信息、日志数据、告警信息、威胁情报、安全事件、预警信息、知识数据等数据；

c) 应支持根据需要自定义数据存储的时间范围；

d) 应支持对重要数据和敏感数据进行加密存储；

e) 应支持配置策略以管理存储空间的使用情况，包括但不限于磁盘阈值告警策略、磁盘阈值自动清理存储数据策略、自动清理老化数据策略等。

8.2.1.2.4 数据分析要求

a) 应支持资产脆弱性分析的能力，能够发现的脆弱性信息，从不同维度进行统计分析，包括漏洞维度和资产维度：

1) 应支持根据漏洞等级、漏洞对系统、应用、服务的影响程度、威胁类型以及时间等维度进行统计分析，以便全面了解漏洞的分布情况；

2) 应支持根据漏洞影响的资产相关信息，进行多维度统计分析，查看漏洞在不同资产上的分布情况。

b) 应支持网络攻击分析，通过各类规则进行匹配，识别恶意特征，获取攻击属性、攻击路径以及攻击者等网络攻击信息：

1) 应支持识别各种常见网络攻击的能力；

2) 应支持按照网络攻击属性进行多维度进行分析的能力；

3) 应支持从攻击者视角进行攻击路径分析的能力；

4) 应支持建立攻击者画像的能力。

c) 应支持发现用户或实体的异常行为的能力，包括但不限于登录异常、访问异常、操作异常、数据下载异常、可疑域名访问等；

d) 应支持对各类安全事件进行关联分析的能力，对潜在安全事件、安全事件变化趋势等进行预测分析能力；

e) 应支持对数据生命周期内的安全风险分析，包括但不限于数据资源分布分析和流动过程分析、数据泄露风险分析等。

8.2.1.2.5 资源管理要求

a) 应支持根据安全组件的使用需求，对安全资源进行统一调度；

b) 应支持对已纳管安全组件对应的安全资源的运行状态进行监测，包括但不限于CPU使用率、内存使用率、硬盘使用率、设备在线时长、设备在线/离线情况等；

c) 应支持对监测到的安全资源的异常运行情况进行告警，包括但不限于CPU、内存、硬盘占用过高、设备离线等；

d) 应支持对安全资源的故障诊断，包括但不限于运行日志查询、抓包分析等；

e) 应支持对各类安全组件的容量进行监控，并对容量异常情况进行告警。

8.2.1.2.6 能力编排要求

a) 应支持可视化编排的方式支撑安全运营中心的自动化响应策略；

b) 应支持将安全组件能力的接口调用进行组合设置为编排动作；

c) 应支持编排动作的管理，包括查询、增加、修改、删除等；

d) 应支持安全事件精确匹配以及模糊匹配的编排触发条件，包括事件名称、事件类型、攻击结果、事件等级等；

e) 应支持基于攻击者时间、事件以及命中事件类型、攻击次数等的编排触发条件；

f) 应支持特征提取、通用流程、逻辑判定、自定义脚本、API以及数据合并等编排过程动作；

g) 应支持IP/域名/会话封堵、流量牵引、主机隔离、工单、通报预警等编排结果动作。

8.2.1.2.7 能力纳管要求

a) 应支持安全组件能力的注册与分类，组件分类包括但不限于数据安全、网络防护、主机防护、密码基础、云原生安全、身份与访问控制、应用安全等；

b） 应支持安全组件与安全资源的关联，从接口上建立安全组件的安全能力与安全资源的安全功能之间的对应关系；

c） 应支持接收安全运营中心的下发的安全策略，并向关联安全资源下发、更新安全规则。

8.2.1.3 平台总线接口

8.2.1.3.1 通用要求

a） 应支持根据数据类型定义数据格式、数据协议和接口调用等；

b） 应支持安全认证及加密传输，保障在数据交换和推送过程中的可用性、完整性和保密性。

8.2.1.3.2 内部数据交换接口

应支持与内部不同系统模块之间进行数据共享交换，包括但不限于分析识别、安全防护、监测告警、事件处置等系统；

8.2.1.3.3 数据采集接口

应支持与不同前端数据源组件进行数据交换，实现日志、告警信息、威胁信息、资产信息、用户信息、脆弱性信息、安全事件等安全数据的汇聚；

8.2.1.3.4 数据共享接口

应支持与其他网络安全重点企业、技术机构等外部支撑系统的接口对接，获取威胁情报数据等。

8.2.1.3.5 资源封装接口

应支持能力纳管和安全组件之间的控制通讯，实现“数盾”组件的应用安全组件、数据安全组件、身份安全组件、网络基础设施安全组件、算力基础设施安全组件、密码基础设施安全组件的调用。

8.2.1.3.6 能力编排接口

应支持平台应用和能力编排模块之间的控制通讯，实现安全策略下发，包括但不限于快速封堵调度支撑、策略编排调度支撑、工单调度支撑等。

8.2.1.3.7 平台级联接口

应支持通过级联接口与上下级 “数盾”体系安全平台对接，支持数据的发送和接收，包括但不限于安全告警、安全事件、预警通报信息、协同指令信息等。

8.2.1.4 平台安全管理要求

8.2.1.4.1 用户管理

a） 应支持通过角色分离实现三权分立，包括系统管理员，操作员，审计员等角色；

b） 应支持用户的分权分域，划分可进行操作和访问的资产、脆弱性、威胁、事件等数据；

c） 应支持用户管理能力，包括账户的创建、编辑、启停、注销等；

d） 应支持配置口令安全性策略，包括口令复杂度、口令历史、有效期、错误次数锁定等。

8.2.1.4.2 运行管理

a) 应支持界面可视化监控各节点运行状态，如CPU、内存、磁盘、网络IO等使用率趋势图、节点联通状态等；

b) 应支持配置系统CPU、内存、磁盘使用告警阈值，并支持邮件、SYSLOG告警通知能力。

c) 应支持对平台系统的认证、关键进程、安全策略、核心数据、敏感数据、关键参数进行安全保护。

8.2.1.4.3 数据存储

a) 应支持对数据文件进行分布式存储，支持根据使用场景对热数据和冷数据进行不同方式的存储；

b) 应支持备份机制，部分数据丢失或损坏后可以快速恢复；

c) 应支持数据迁移，包括原始数据、处理结果数据、功能和规则配置数据等；

d) 应支持高可用部署，支持节点扩展，支持负载均衡。

e) 应支持使用加密工具对记录的用户名、口令、SSH用户名和SSH口令等关键信息进行加密。

8.2.1.4.4 日志审计

a) 应支持用户操作审计能力，记录用户的平台操作行为；

b) 应支持记录平台的运行日志；

c) 应支持技术手段保障审计日志不被篡改和删除。

8.2.2 组件层

8.2.2.1 网络基础设施安全组件

8.2.2.1.1 边界防护

a) 应支持边界防护能力，对跨越数据中心边界的访问和数据流通提供受控接口进行通信；

b) 应支持对外部非授权设备联到数据中心网络的行为进行检查或限制；

c) 应支持对数据中心内部用户非授权联到外部网络的行为进行检查或限制。

8.2.2.1.2 访问控制

a) 应支持网络访问控制能力，对源IP、目的IP、端口、黑白名单等进行访问控制；

b) 应支持网络隔离交换能力，对传输的数据实现协议剥离、格式检查和内容过滤。

8.2.2.1.3 入侵防御

a) 应支持网络入侵防御能力，通过协议解码、内容检测、规则匹配及威胁情报分析等技术手段，阻断入侵行为；

b) 应支持网络威胁检测能力，对网络流量和加密流量的检测分析；

c) 应支持网络攻击溯源能力，通过对攻击信息片段进行综合分析和场景还原，重构攻击者的攻击路径、攻击手法、攻击意图。

8.2.2.1.4 拒绝服务防护

a) 应支持拒绝服务攻击防护能力，包括但不限于SYN/ACK Flood、ICMP Flood等攻击防护；

b) 应支持阈值限制能力，通过流量限制、报文限制、连接限制等方式保障带宽有效使用。

8.2.2.2 算力基础设施安全组件

8.2.2.2.1 主机安全

a) 应支持访问控制能力，对身份、流量、协议、操作行为等进行访问控制；

b) 应支持入侵防御能力，对出入主机的流量进行检测识别，防御网络攻击及入侵行为；

c) 应支持恶意代码查杀能力，对恶意代码进行检测和清除；

d) 应支持漏洞扫描能力，对保护对象的漏洞检测；

e) 应支持安全补丁能力，为保护对象提供安全补丁服务；

f) 应支持安全审计能力，对重要的主机行为和重要事件进行审计。

8.2.2.2.2 云原生安全

a) 应支持访问控制能力，阻断南北向和东西向流量攻击；

b) 应支持入侵行为检测能力，包括但不限于基于Pod的流量检测和恶意镜像检测；

c) 应支持基线扫描能力，对编排工具、运行时组件和镜像中的配置文件进行扫描；

d) 应支持镜像完整性保障机制能力，禁止对未通过完整性校验的镜像部署到容器中；

e) 应支持运行异常行为监控能力，对容器的异常启动进行监控；

f) 应支持入侵行为响应，支持在确认收到入侵后容器可快速响应处置。

8.2.2.2.3 可信计算

a) 应提供可信度量与报告等技术，达成对平台特定节点可信状况的验证与报告能力；

b) 应将可信验证与报告的结果用于系统其它安全功能的执行过程；

c) 应提供TEE、可信密码、可信访控等安全可信机制，达成数据在存储、处理和传输过程中，对非授权对象的保密能力；

d) 应提供可信签名、可信认证等安全可信机制，达成对数据内容完整性和自身属性的验证能力；

e) 应提供区块链、CA、可信认证等安全可信机制，实现多用户、多节点场景下关键操作的可信记账机制，并提供对数据共享过程中智能合约等功能的支持。

8.2.2.3 密码基础设施组件

8.2.2.3.1 网络和通信安全

a) 应支持密码技术保证通信过程中重要数据的完整性；

b) 应支持密码技术保证通信过程中重要数据的机密性；

c) 应支持密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

d) 可使用抗量子计算技术的密码应用系统作为密码基础设施组件。

8.2.2.3.2 设备和计算安全

a) 应支持密码技术建立远程管理设备的信息传输通道；

b) 应支持密码技术保证系统资源访问控制信息的完整性；

c) 应支持密码技术保证日志记录的完整性；

d) 应支持密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；

e) 应支持密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。

8.2.2.3.3 应用和数据安全

a) 应支持密码技术保证信息系统应用的访问控制信息的完整性；

b) 应支持密码技术保证信息系统应用的重要数据在存储过程中的机密性；

c) 应支持密码技术保证信息系统应用的重要数据在存储过程中的完整性；

d) 应支持密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

e) 应支持密码技术保证信息系统应用的重要数据在传输过程中的机密性；

f) 应支持密码技术保证信息系统应用的重要数据在传输过程中的完整性；

g) 应支持密码技术确保数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性，

8.2.2.4 应用安全组件

8.2.2.4.1 Web 安全防护

a) 应支持web访问控制能力，包括但不限于对访问主体、访问权限、访问行为等进行访问控制；

b) 应支持web安全防护能力，包括但不限于SQL注入、XSS跨站、爬虫、黑链的攻击防护；

c) 应支持网页漏洞扫描能力，包括但不限于SQL注入、敏感信息泄露、跨站脚本、越权等行为检测；

d) 应支持防篡改能力，对网页实时监控并对篡改文件及时恢复。

8.2.2.4.2 API 接口安全防护

a) 应支持API接口资产识别能力，自动识别流量中的API接口，形成API接口台账；

b) 应支持API接口防护能力，包括但不限于身份认证、数据加密、安全审计等安全措施。

8.2.2.5 数据安全组件

8.2.2.5.1 数据采集安全

a) 应支持数据资产识别能力，识别数据存储位置、数据格式、数据类别、数据级别等主要信息。

b) 应支持身份鉴别能力，对采集对象进行身份鉴别和访问控制；

c) 应支持数据分类分级能力，对数据进行自动化分类分级；

d) 应支持数据安全审计能力，对采集的数据进行记录和审计。

8.2.2.5.2 数据传输安全

a) 应支持数据加密能力，采用国产密码算法对关键的数据传输通道加密以及对传输数据内容进行加密；

b) 应支持数据完整性检测能力，对传输数据完整性进行检测，并具备数据容错或恢复的技术手段。

8.2.2.5.3 数据存储安全

a) 应支持脆弱性扫描能力，对数据存储系统的漏洞、安全配置进行扫描；

b) 应支持数据加密能力，对存储的数据进行基于国产密码算法的加密，支持对数据库进行字段级、表级或库级加密；

c) 应支持备份存储能力，提供数据库系统快照的存储和检索功能；

d) 应支持数据安全审计能力，对数据存储行为进行记录和审计。

8.2.2.5.4 数据处理安全

a) 应支持数据访问控制能力，对访问主机、访问工具、数据库账号等进行访问控制；

b) 应支持数据脱敏能力，对数据处理过程中的敏感数据进行数据脱敏；

c) 应支持数据泄漏防护能力，对数据处理过程中的敏感数据进行泄漏监测和数据保护；

d) 应支持数据安全审计能力，提供对数据处理过程的操作进行记录和审计。

8.2.2.5.5 数据交换安全

a) 应支持数据水印能力，在数据交换过程中进行水印标记；

b) 应支持数据接口异常处理能力，对数据接口不安全输入参数进行限制或过滤；

c) 应支持数据安全审计能力，对数据的交换行为进行记录和审计。

8.2.2.5.6 数据销毁安全

应支持数据销毁能力，通过物理损毁、消磁等方式实现硬盘、光盘等存储介质的有效销毁。

8.2.2.6 身份认证组件

8.2.2.6.1 身份鉴别

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登陆次数和当登录连接超时自动退出等相关措施；

c) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

8.2.2.6.2 访问控制

a) 应支持配置访问控制策略，访问控制策略规定主体对客体的访问规则；

b) 访问控制主体的粒度应支持用户级或进程级；

c) 应支持对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

8.3 管理能力要求

8.3.1 组织架构

a) 应成立由数据中心所属单位主要负责人担任领导职务的“数盾”体系管理组织部门，负责数据中心“数盾”体系的规划、建设、管理和运营工作；

b) 在委员会或领导小组下，应针对“数盾”体系各项活动设立不同的组织部门，明确各自的角色以及职责，确保“数盾”体系建设的规划、设计和运营等工作顺利开展，如：

1) 应根据“数盾”体系建设方的需求进行整体规划和设计；

2) 应对“数盾”体系建设和运营过程中对人员录转调离等工作进行管理；

3) 应对“数盾”体系的建设过程中产品选购以及项目验收等工作进行审核；

4) 应对“数盾”体系建设和运营过程中的突发事件制定应急预案并快速采取措施；

5) 应在“数盾”体系运行时进行系统监控和故障排除等工作；

6) 应对“数盾”体系运营过程中的人员培训教育。

8.3.2 规章制度

a) 应根据所属集群的《“数盾”体系管理办法》，制定数据中心内部的“数盾”体系管理办法；

b) 应针对“数盾”体系建设和运营过程中涉及到人员的相关方面制定规章制度，包括但不限于人员的录转调离、能力要求、生产操作、账号管理、出入管理、保密协议等方面；

c) 应针对“数盾”体系建设和运营过程中涉及到设备的相关方面制定规章制度，包括但不限于设备的物理环境、维护保养、运营运维等方面；

d) 应针对“数盾”体系的建设和运营过程中的各项活动制定相应规章制度，如项目的生命周期、产品的生命周期、安全活动、沟通交流、考核评估等方面的相关活动。

8.3.3 运作机制

a) 应具备合理的沟通协作机制，加强数据中心级“数盾”体系内部的合作沟通；

b) 应具备完善的宣传培训机制，对“数盾”体系内的各项管理制度进行宣传培训以确保下达，以及对人员进行技能培训、操作流程培训等；

c) 应具备完善的考核评估机制，包括但不限于对宣传培训的效果、规划设计的内容、安全事件的处理、风险的处理、资产的情况等方面进行评估；

d) 应具备完善的计划管理机制，为“数盾”体系建设过程中的各项活动制定计划，保证各项活动的如期进行；

e) 应具备完善的质量管理机制，保证“数盾”体系建设过程中出现的产品和服务符合相应的标准；

f) 应具备完善的风险管理机制，能够识别各种风险并制定策略应对，以及对风险进行通报；

g) 应具备完善的供应链管理机制，包括对供应链合作伙伴的评估选择和安全审计监督等。

8.4 运营能力要求

8.4.1 日常安全运营服务

a) 应根据数据中心运营保障要求，组建日常安全运营团队，明确不同岗位职责和人员要求；

b) 应制定数据中心日常安全运营体系，并形成相应的制度、流程、操作规范等；

c) 应提供威胁监测、事件分析与处置、漏洞信息分析等服务，确保可以解决不同情况下的日常安全问题，并能够将处置进展上报集群；

d) 应使用有效运营工具监控和管理日常运营服务，为安全运营工作提供有效的支撑与保障。

8.4.2 安全应急响应服务

a) 应组建数据中心应急响应团队，包括应急指挥小组和应急处置小组，明确相关职责，配齐管理人员，开展突发事件的监测、分析和应急处置工作；

b) 应构建完整的应急响应预案和应急响应流程体系，并定期开展应急预案演练，能够准确分析攻击行为，有效处置安全事件，及时控制和消除各类突发事件的危害及影响，全面提升应急处置和快速响应能力；

c) 应建立应急宣教机制，组织专家开展专业咨询、培训演练和课题研究，开展安全应急指挥人员和应急处置人员技能与心理素质培训，实现各单位培训全覆盖；

d) 应建立安全事件联动处置机制，强化实战化应急能力，遇到突发事件后，能够快速有效联动各单位沟通渠道，开展应急响应处置，并将处置进展及时反馈；

e) 应构建各阶段能力提升评估机制，制定应急处置能力提升方案、应急处置能力提升方案实施评估、应急响应处置工作执行情况评估、安全突发事件应急处置事件后评估工作等。

8.4.3 安全监管协同服务

a) 应根据数据中心安全服务要求，组建安全监管协同团队，明确不同的岗位职责和人员要求；

b) 应构建数据中心安全监管协同体系，并形成相应的制度、流程、操作规范等；

c) 应支持实时监管数据中心区域内的安全状况，及时发现网络或数据安全事件，识别网络或数据安全隐患及威胁，并能上报集群；

d) 应支持接收数据中心集群下发送协同处置指令，能够快速开展协同处置工作，确保安全风险的可控和安全事件的处置响应。

8.4.4 重大活动保障服务

a) 应组建数据中心级重保服务团队，重保任务期间提供相应运营服务，并指定接口人与集群进行对接，建立快速有效的沟通渠道；
b) 应提供重保任务的全生命周期管理服务保障，包含重保筹备阶段、临战阶段、实战阶段和总结阶段；
c) 应具备将产生的告警及时显示在重保任务工作台中，为值班的重保安全专家推送预警通报信息；
d) 应提供重保活动总结服务，提供总结报告并统计保障活动中数据中心节点相关数据。

8.4.5 租户安全服务

a) 应根据数据中心租户安全服务需求编制服务目录，由租户运营团队统一发布、集中管理；
b) 应构建数据中心租户安全服务流程体系，明确开通、试用、交易、回访、结束等租户服务流程；
c) 应组建租户运营团队，明确不同的岗位职责，并制定租户服务人员的操作规范和管理制度等；
d) 应使用有效运营工具监控和管理租户安全服务，为安全运营工作提供有效的支撑与保障。

参 考 文 献

[1] 《党委（党组）网络安全工作责任制实施办法》（中共中央办公厅2017年8月15日发布执行）

[2] 《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》（2021年3月11日第十三届全国人民代表大会第四次会议通过）

[3] 《数字中国建设整体布局规划》（中共中央、国务院2023年印发）

[4] 《国务院关于印发“十四五”数字经济发展规划的通知》（国发〔2021〕29号）

[5]《“十四五”国家信息化规划》（2021年12月27日中央网络安全和信息化委员会印发）

[6]《“十四五”推进国家政务信息化规划》（发改高技〔2021〕1898号）

[7]《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号）

[8]《全国一体化政务大数据体系建设指南》（国办函〔2022〕102号）

[9]《关于加快构建全国一体化大数据中心协同创新体系的指导意见》（发改高技〔2020〕1922号）

[10]《全国一体化大数据中心协同创新体系算力枢纽实施方案》（发改高技〔2021〕709号）

[11]《国务院关于印发促进大数据发展行动纲要的通知》（国发〔2015〕50号）

[12]《“数盾”体系技术架构研究》（国家信息中心信息与网络安全部“数盾”研究小组编著 2022年11月2日评审通过）