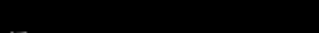
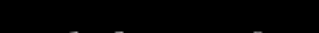
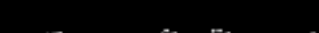
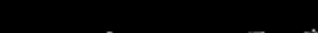
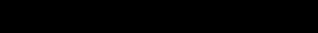
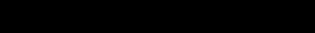
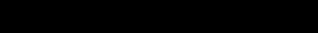
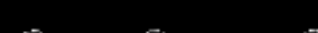




廿和国国家标准 中化人早

~~GB/T 36058—2018~~

security technology—Technical requirements of security—Information management center for classified protection of architecture—main page

2018-12-28-发布

2019-07-01 实施

नीलमणि चन्द्रिका

中國鐵道工程集團有限公司

前言	II	引言	2
1 范围	1	1 范围	2
2 规范性引用文件	1	2 规范性引用文件	2
3 术语和定义	1	3 术语和定义	2
4 缩略语	1	4 缩略语	2
5 安全管理中心概述	2	5 安全管理中心概述	2
5.1 总体说明	2	5.1 总体说明	2
5.2 功能描述	3	5.2 功能描述	3
6 第二级安全管理中心技术要求	3	6 第二级安全管理中心技术要求	3
6.1 功能要求	3	6.1 功能要求	3
6.2 接口要求	7	6.2 接口要求	7
6.3 自身安全要求	7	6.3 自身安全要求	7
7 第三级安全管理中心技术要求	8	7 第三级安全管理中心技术要求	8
7.1 功能要求	8	7.1 功能要求	8
7.2 接口要求	13	7.2 接口要求	13
7.3 自身安全要求	12	7.3 自身安全要求	12
8 第四级安全管理中心技术要求	15	8 第四级安全管理中心技术要求	15
8.1 功能要求	15	8.1 功能要求	15
8.2 接口要求	16	8.2 接口要求	16
8.3 自身安全要求	16	8.3 自身安全要求	16
9 第五级系统安全管理中心技术要求	17	9 第五级系统安全管理中心技术要求	17
9.1 功能要求	17	9.1 功能要求	17
9.2 接口要求	17	9.2 接口要求	17
9.3 自身安全要求	17	9.3 自身安全要求	17

本标准按照 GB/T 1.1—2009 给出的规则起草

研究所、公安部第一研究所、网络信息援本、北京国信安有限公司

引 言

本标准从安全管理中心的功能、接口、自身安全等方面,对GB/T 25070中提出的安全管理中心及

其安全技术和能力进行了进一步细化和补充,提出了安全管理中心的安全要求,并给出了实现

信息安全技术 网络安全等级保护 安全管理中心技术要求

1 范围

本标准规定了网络安全等级保护安全管理中心的技术要求。

本标准适用于指导安全厂商和运营使用单位依据本标准要求设计、建设和运营安全管理中心。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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/T 5271.8—2018 信息安全技术 密码 第8部分:安全

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 25069—2010 信息安全技术 术语

7.0 界定的以及下列术语和定义适用于 GB 17859—1999、GB/T 5271.8、GB/T 25069 和 GB/T 250

4.3.2.3

3.11

数据收集接口 data-collector

3.12 网络安全等级保护安全管理中心接口

3.2.1

3.2.2

采集器 collector

3.2.3 网络安全等级保护安全管理中心接口

3.2.4

3.2.5 网络安全等级保护安全管理中心接口

3.2.6 网络安全等级保护安全管理中心接口

3.2.7 网络安全等级保护安全管理中心接口

3.2.8 网络安全等级保护安全管理中心接口

4 缩略语

下列缩略语适用于本文件。

CPU 中央处理器(Central Processing Unit)

3.2.9 网络安全等级保护安全管理中心接口

3.2.10 网络安全等级保护安全管理中心接口

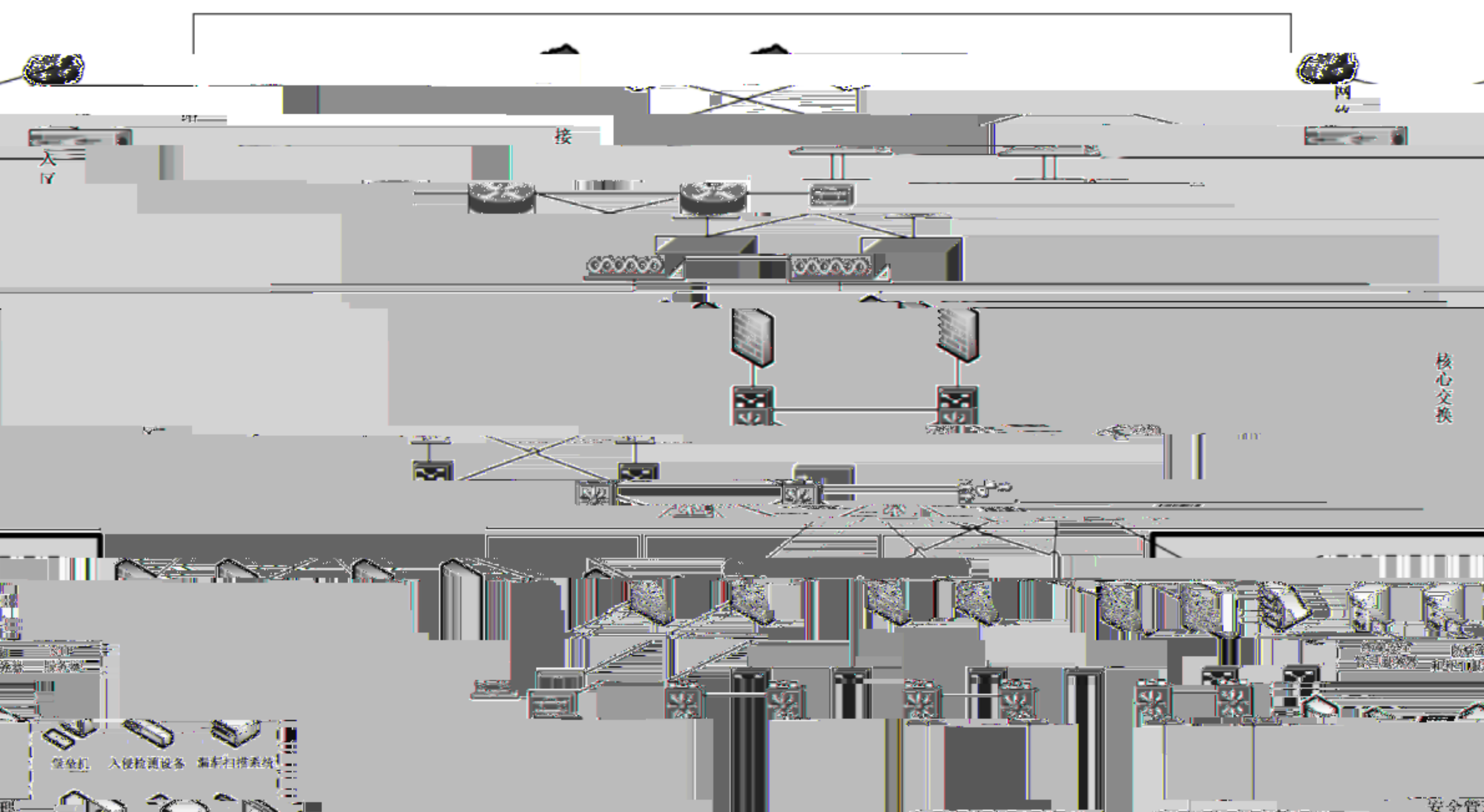
IP 互联网协议(Internet Protocol)

10. What is the purpose of the "References" section?

10. 五聯網址列表如下 (Table 10.1) :

$\mathbf{S}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

© 2004 Blackwell Publishing Ltd *Journal of Internal Medicine* 255: 103–110



能够对其管理对象的各条管理记录进行再鉴别,并对鉴别结果进行有效跟踪。

数据保护

6.1.1.2 数据保护

6.1.1.2.1 数据保密性

以下要求:

数据保密性应满足

数据保密性应满足以下要求:应能够对其管理对象的各条管理记录进行再鉴别,并对鉴别结果进行有效跟踪。

6.1.1.2.2 数据完整性

数据完整性应满足以下要求:应能够对其管理对象的各条管理记录进行再鉴别,并对鉴别结果进行有效跟踪。

6.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求:

数据备份与恢复应满足以下要求:应能够对其管理对象的各条管理记录进行再鉴别,并对鉴别结果进行有效跟踪。

6.1.1.3 安全事件管理

6.1.1.3.1 安全事件采集

安全事件采集应满足以下要求:

安全事件采集应满足以下要求:应能够对其管理对象的各条管理记录进行再鉴别,并对鉴别结果进行有效跟踪。

6.1.1.3.2 安全事件告警

安全事件告警应具备告警功能。

6.1.1.3.3 安全事件响应

安全事件响应应满足以下要求:

安全事件响应应满足以下要求:应能够对其管理对象的各条管理记录进行再鉴别,并对鉴别结果进行有效跟踪。

6.1.1.3.3 事件管理应支持按照以下规则对事件进行过滤或分类,并支持按位置、时间、内容等维度进行过滤。

6.1.1.3.4 系统应支持以下功能:

6.1.1.3.4.1 系统应支持以下功能:

6.1.1.3.4.2 系统应支持以下功能:

6.1.1.3.4.3 系统应支持以下功能:

- a) 能够按时间、事件类型等条件对安全事件进行查询;
- b) 能够按统计周期和报表生成功能。

6.1.1.4 资产管理

6.1.1.4.1 资产管理

6.1.1.4.1.1 资产管理

6.1.1.4.1.1.1 资产管理

6.1.1.4.1.1.1.1 资产管理

6.1.1.4.1.1.1.2 资产管理

6.1.1.4.1.1.1.3 资产管理

6.1.1.4.1.1.1.4 资产管理

6.1.1.4.1.1.1.5 资产管理

6.1.1.4.2 威胁管理

6.1.1.4.2.1 威胁管理

6.1.1.4.2.1.1 威胁管理

6.1.1.4.2.1.1.1 威胁管理

6.1.1.4.3 脆弱性管理

6.1.1.4.3.1 脆弱性管理

6.1.1.4.3.1.1 脆弱性管理

6.1.1.4.3.1.1.1 脆弱性管理

6.1.1.4.3.1.1.2 脆弱性管理

6.1.1.4.3.1.1.3 脆弱性管理

6.1.1.4.3.1.1.4 脆弱性管理

6.1.1.4.3.1.1.5 脆弱性管理

6.1.1.5 资源监控

6.1.1.5.1 可用性监测

6.1.1.5.1.1 可用性监测

6.1.1.5.1.1.1 可用性监测

6.1.1.5.1.1.1.1 可用性监测

6.1.1.5.1.1.1.2 可用性监测

6.1.1.5.1.1.1.3 可用性监测

设计管理要素

1. 在“数据源”列表框中，单击“数据源”按钮，打开“数据源”对话框。

6.1.2.2.1 审计数据采集

● 2014 年 12 月 1 日

6.1.2.2

—

d) 火灾报警设备(如防火墙入侵监测系统)

审计数据采集方式应满足以下要求:

- a) 支持通过如 Syslog、SNMP 等协议采集各种系统或设备上的审计数据;

6.2 接口要求

6.2.1 第三方插件/代理接口协议要求

以及第三方的插

安全管理中心应支持 SNMP Trap、Syslog、Web Service 等常规接口和自定义接口。

在统一安全管理中心部署各组件时，应确保第三方插件/代理的兼容性。

6.2.2 接口安全要求

安全管理中心应提供接口安全要求：

a) 采用安全通信协议，保证接口之间交互数据的完整性；

b) 采用加密技术对敏感信息进行加密传输。

6.3 安全管理要求

6.3.1 身份鉴别

安全管理中心控制台的管理员身份鉴别应满足以下要求：

a) 提供专用的登录控制模块对管理员进行身份标识和鉴别；

b) 提供管理员用户身份标识唯一性和鉴别信息保密性，并应支持多种鉴别方式，如用户名/密码、用户名/证书、用户名/令牌等。

安全管理中心应支持多种鉴别方式。

7 访问控制

6.3.2

安全管理中心控制台访问控制应满足以下要求：

a) 提供安全策略控制模块，能够对安全策略进行配置。

安全管理中心应支持多种安全策略。

安全管理中心应支持多种安全策略，如基于角色的访问控制、基于策略的访问控制等。

安全管理中心应支持多种安全策略。

安全管理中心应支持多种安全策略，如基于角色的访问控制、基于策略的访问控制等。

6.3.3 安全审计

下要求：

安全管理中心控制台的安全审计应满足以下要求：

a) 提供安全审计模块，能够对安全审计数据进行记录。

a) 提供安全审计模块，能够对安全审计数据进行记录。

安全管理中心应支持多种安全策略。

b) 提供无法删除和篡改的记录，无法删除、修改。

安全管理中心应支持多种安全策略，如基于角色的访问控制、基于策略的访问控制等。

c) 提供审计记录数据。

安全管理中心应支持多种安全策略。

d) 提供审计记录数据。

6.3.4 软件容错

安全管理中心控制台应提供软件容错功能，保证系统运行。

安全管理中心控制台应提供软件容错功能，保证系统运行。

输入的数据格式或长度应符合系统设计要求。

6.3.5 资源控制

下要求：

安全管理中心控制台的资源控制应满足以下要求：

a) 对管理员登录地址范围进行限制；

b) 当管理员在一段时间内未作任何动作，

c) 能够对最大并发会话连接数进行限制。

7.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求:

- 提供数据及其他公开执行功能。公开数据及其他至少每天一次。公开4个以外有放

Table 1 Summary of the study variables

7.1.1.2.4 剩余信息

保护

刊例 每行 100 字

[illegible]

1000

100

/// 16 2007 年 10 月 10 日 星期三 16:10 金魚王 11.0

7-13-1 安全事件采集

安全事件采集应满足以下要求:

前 列 腺 癌 的 治 疗 方 案 选 择

— *Journal of the American Medical Association*, 1997

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836. 837. 838. 839. 840.

雅各·格林格

注:安全事件的原因应包括但不限于:时间、地点、设备、媒体类型、连接IP地址、端口等值。

1) 凡在本行系统内办理存款、放款、汇兑、贴现、抵押、担保、租赁、保管、代理、信托、保险、证券、期货、基金、衍生品、贵金属、外汇、国际结算、其他金融业务，均须遵守本行系统内业务操作规程。

《中国地质大学(北京)安全工程本科专业人才培养方案》

4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836. 837. 838. 839. 840. 841. 842. 8

7.1.1.3.2 安全事件告警

安全事件生發應儘量以下要求

© 2004 Blackwell Publishing Ltd *Journal of Internal Medicine* 255: 105–112

Figure 6

二、主要参考文献

Figure 1

1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26



7.3.3 安全配置策略

安全事件响应应满足以下要求:

- b) 能够提供安全通告功能,可以创建或导入安全风险通告,通告中应包含通告内容、描述信息

[illegible]

- 價格和品質在需求上的佔全圖繪景。圖中繪有兩座山，一座山上有許多樹木，另一座山上有許多房屋。圖中還繪有兩條河流，一條河流上有許多小船，另一條河流上有許多房屋。圖中還繪有許多其他景物，如橋樑、道路、樹木等。

4.2.3.4 串仁茨靈參

14. 每段话5分, 每篇话以15分为止。

7.1.1.3.5 统计分析报表

7.1.1.4 风险管理

7.1.1.4.1 资产管理

资产管理应满足以下要求：

- a) 支持资产属性的自定义；
- b) 支持资产属性的预定义；
- c) 支持资产属性的自定义；
- d) 支持资产属性的自定义；

7.1.1.4.3 威胁管理

威胁管理应满足以下要求：

- a) 支持自定义安全威胁分类；
- b) 支持自定义安全威胁分类；
- c) 支持自定义安全威胁分类；
- d) 支持自定义安全威胁分类；

7.1.1.4.5 风险分析

以下要求：

风险分析应满足

- a) 安全风险的计算周期和计算公式能够根据部署环境的实际需要通过对配置的方式进行相应调整；
- b) 安全风险的计算周期和计算公式能够根据部署环境的实际需要通过对配置的方式进行相应调整；

7.1.1.5 资源监控

7.1.1.5.1 可用性监测

可用性监测应满足以下要求：

套可了解其运行状态。

7.1.1.5.1 设备状态监测

在工控系统中,应能够对工控系统设备的运行状态安全地进行实时监测,可对监测指标设置告警阈值,能发告警并记录。

7.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求:

- a) 支持对网络拓扑图进行在线编辑,允许手工添加或删除监测节点或链路;
- b) 能够展现当前网络环境中关键设备(包括网络设备、安全设备、服务器主机等)的状态,如网络流量、网络延迟统计分析等指标。

能够在网络运行出现异常时,能够展现在当前网络拓扑图

7.1.2 安全管理要求

7.1.2.1 安全标记

安全标记应满足以下要求:

在工控系统的安全域中,安全域应包含用户、终端设备、安全设备、服务器、网络设备等;

安全域应具有唯一性,能够准确反映工控系统中安全属性的特征,并具有防止篡改的能力;

安全域应包含安全级别、安全范围等信息,安全级别应可排序进行高低判断,安全范围应可包含判断;

应针对不同安全级别的系统中安全标记与安全属性的单一映射关系。

7.1.2.2 授权管理

应满足以下要求:

对每一个标记所能访问范围的统一管理;

对主体访问权限的统一管理,包括主机访问权限管理、网络访问权限管理、应用访问权限管理;

根据主体标记和客体标记安全级别的不同,制定访问控制策略,控制主体对客体的访问。

7.1.2.3 设备策略管理

7.1.2.3.1 安全策略策略

应制定工控系统的安全策略,并应满足以下要求:

应制定工控系统的安全策略,并应满足以下要求:

7.1.2.3.2 入侵防御

入侵防御应满足以下要求:

应制定工控系统的安全策略,并应满足以下要求:

a) 提供统一接口,实现对网络入侵防御和主机入侵防御

计,应通过运维审计系统对管理员的运维行为进行安全审计,应通过租户隔离机制,确保审计数据隔离的有效性;

7.1.3.2.3 审计数据采集方式

- a) 通过部署在设备端的数据采集探针;
- b) 通过部署在Hadoop、SAP等数据仓库设备上的审计数据;
- c) 通过统一接口向设备管理运维的安全可信应用;

7.1.3.2.4 审计数据关联分析

7.2 接口要求

7.2.1 第三方插件/代理接口协议要求

接口协议要求应满足以下要求:

7.2.2 接口安全要求

下要求:

- a) 采用安全的接口协议,保证接口之间交互数据的完整性;
- b) 采用加密技术保证接口之间交互数据的保密性;

接口安全要求应满足以

7.3 自身安全要求

7.3.1 身份鉴别

的管理员身份鉴别应满足以下要求:

安全管理中心控制台

- a) 采用非对称加密技术或双向认证技术实现身份鉴别,应支持多种认证方式;
- b) 应采用可信计算技术实现身份鉴别;

7.3.2 访问控制

安全管理中心控制台的访问控制应满足以下要求:

- a) 应具备自主访问控制功能,能够安全策略配置及策略动态调整;
- b) 自主访问控制应支持细粒度访问控制策略配置,能够支持任意访问策略;

- c) 应具备基于角色的访问控制功能,能够支持任意角色配置;

- d) 实现特权用户的权限分离,应授予不同特权用户完成各自承担任务所需的最低

7.3.3 安全审计

控制台的安全审计应满足以下要求：

— 对操作和安全事件进行审计；

— 对时间、发起者信息、资源、描述和结果进行

— 对安全事件审计结果的访问控制策略进行审计。

— 安全管理中心控制台的安全审计应满足以下要求：

a) — 提供覆盖到每个管理员工的安全审计功能，记录所有管理员工的操作；

b) — 保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

c) — 审计记录的结果至少应包括事件类型、

7.3.4 剩余信息保护

安全管理中心控制台的剩余信息保护应满足管理员工对敏感信息所有权的完整控制权分配给

其他管理员工或用户前得到完全清除，若该信息是存储在设备中，还应进行备份。

7.3.5 软件容错

安全管理中心控制台应提供容错产品为要求。

a) — 能够对输入数据进行校验，保证输入数据和输出数据的完整性；

系统应要求：

— 提供冗余备份功能，防止数据丢失。

7.3.6 资源控制

安全管理中心控制台的资源控制应满足以下要求：

a) — 管理端资源应进行限制；

b) — 当管理员工一段时间内未作任何动作，应自动结束会话；

c) — 能够对最大会话数连接数进行限制；

d) — 能够对管理端资源的使用情况进行实时监控；

— 能够对资源使用情况进行检测和报警；

e) — 能够对资源使用情况进行实时监控，并能将资源使用率降低到预设阈值；

— 7.3.7 入侵检测

安全管理中心控制台的安全防范应满足以下要求：

— 安全管理中心控制台应能对入侵行为进行检测和报警；

— 报警信息应能及时通知相关人员；

7.3.8 数据安全

安全管理中心控制台的数据安全应满足以下要求：

a) — 应能对数据进行加密存储和传输，并能对数据进行备份和恢复，并能对数据进行完整性验证；

— 在发生数据丢失或损坏时，能及时采取必要的恢复措施；

8 第四级安全管理中心技术要求

8.1 功能要求

8.1.1 系统管理要求

8.1.1.1 用户身份管理

用户身份管理应满足以下要求：

- a) 能够对被管理对象环境中的主体进行标识；

8.1.1.2 数据保护

8.1.1.2.1 数据保密性

数据保密性应满足以下要求：

数据保密性应满足以下要求：

- a) 能够检测到被管理对象敏感信息，对管理操作不安全的敏感信息能够及时识别和完整告警提示并采取必要的恢复措施；
- b) 能够检测到被管理对象敏感信息，对管理操作不安全的敏感信息能够及时识别和完整告警提示并采取必要的恢复措施；
- c) 对重要通信提供专用通信协议或安全通信协议服务，避免来自通用通信协议的攻击破坏。

8.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求：

- a) 提供数据备份与恢复功能，安全数据备份至少每天一次，备份介质异地存放；
- b) 提供数据恢复功能，安全数据恢复至少每天一次，恢复介质异地存放；
- c) 提供异地备份功能，利用通信网络将数据备份到异地备份设备。

中华人民共和国境内 禁止从境外对境内云计算平台的运维

[illegible]

可信路径应满足以下要求：

- a) 在对主体进行身份鉴别时,应能够建立一条安全的信息传输路径;

卷一 詩經



8.1.1.2.5 剩余信息保护

各站沿途主销主体前得到完

[illegible]

Abstract

8.1.1.3 安全事件管理

8.1.1.3.1 安全事件采集

安全事件采集应满足以下要求：

- a) 支持安全事件监测采集功能,及时发现和采集发生的安全事件;
- b) 能够提供与第三方系统的数据采集接口,发送或接收安全事件;

Abstract

——“当能够完全掌握汉语时，在位置上的最后阶段，不属于进入‘语言习得’的范围”
——在语言习得中，

[illegible]

安全事件通报及处理流程表

Figure 1. The structure of the proposed model.

8.1.1.3.2 安全事件告警

安全事件告警应满足以下要求:

- a) 具备告警功能,在发现异常时可根据预先设定的阈值产生告警;

一、二、三、四、五、六、七、八、九、十、十一、十二、十三、十四、十五、十六、十七、十八、十九、二十、二十一、二十二、二十三、二十四、二十五、二十六、二十七、二十八、二十九、三十、三十一、三十二、三十三、三十四、三十五、三十六、三十七、三十八、三十九、四十、四十一、四十二、四十三、四十四、四十五、四十六、四十七、四十八、四十九、五十、五十一、五十二、五十三、五十四、五十五、五十六、五十七、五十八、五十九、六十、六十一、六十二、六十三、六十四、六十五、六十六、六十七、六十八、六十九、七十、七十一、七十二、七十三、七十四、七十五、七十六、七十七、七十八、七十九、八十、八十一、八十二、八十三、八十四、八十五、八十六、八十七、八十八、八十九、九十、九十一、九十二、九十三、九十四、九十五、九十六、九十七、九十八、九十九、一百

Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was plotted against the number of trials for each condition. The number of correct responses increased with the number of trials for all conditions. The number of correct responses was highest for the condition with the highest number of trials (10 trials) and lowest for the condition with the lowest number of trials (2 trials).

Figure 1. The effect of the number of iterations on the accuracy of the proposed algorithm. The accuracy of the proposed algorithm increases with the number of iterations. The accuracy of the proposed algorithm is 0.95 when the number of iterations is 1000.

8.1.1.3.3 安全事件响应

一、安全事件响应应满足以下要求：

- [illegible]

[illegible]

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836. 837. 838. 839. 840.

11. *Journal of the American Medical Association*, 1997; 277: 1039-1043.

8.1.1.3.4 事件关联分析

事件关联分析应满足以下要求：

——能关联事件序列，关联规则配置灵活；

——能关联事件的上下文信息和关联事件的时间信息；

——能关联事件的地理位置信息和关联事件的网络信息；

——能关联事件的时间信息和关联事件的空间信息；

——能关联事件的事件类型和关联事件的事件等级；

——能关联事件的事件发生时间和关联事件的事件持续时间；

8.1.1.3.5 统计分析报表

统计分析报表应满足以下要求：

——能关联事件的时间信息和关联事件的空间信息；

——能关联事件的事件类型和关联事件的事件等级；

——能关联事件的事件发生时间和关联事件的事件持续时间；

——能关联事件的事件发生时间和关联事件的事件持续时间；

8.1.1.4 风险管理

——能关联事件的事件发生时间和关联事件的事件持续时间；

8.1.1.4.1 资产管理

资产管理应满足以下要求：

——能关联事件的事件发生时间和关联事件的事件持续时间；

——能关联事件的事件发生时间和关联事件的事件持续时间；

——能关联事件的事件发生时间和关联事件的事件持续时间；

——能关联事件的事件发生时间和关联事件的事件持续时间；

——支持资产属性的自定义；

——支持自定义资产记录或基于模板的批量资产导入；

——支持对资产的自动发现，并能够将其自动添加到资产库中；

8.1.1.4.2 资产业务价值评估

——能关联事件的事件发生时间和关联事件的事件持续时间；

——能关联事件的事件发生时间和关联事件的事件持续时间；

8.1.1.4.3 威胁管理

威胁管理应满足以下要求：

——能关联事件的事件发生时间和关联事件的事件持续时间；

a) 具备预定义的安全威胁分类；

b) 支持自定义安全威胁分类，并将已发生的按安全风险评估的威胁源安全资产关联的威胁；

8.1.1.4.4 脆弱性管理

脆弱性管理应满足以下要求：

——能关联事件的事件发生时间和关联事件的事件持续时间；

——能关联事件的事件发生时间和关联事件的事件持续时间；

——能关联事件的事件发生时间和关联事件的事件持续时间；

8.1.1.4.5 风险分析

风险等级应满足以下要求：

- a) 能够根据攻击事件发生概率、攻击后果的严重性和资源可承受的安全风险等级对资产的安全等级进行划分；

风险等级应满足以下要求：

8.1.1.5 资源监控

8.1.1.5.1 可用性监测

可用性监测应满足以下要求：

- a) 支持通过监测网络设备、安全设备、

主机操作系统、数据库、中间件、应用系统等重要性能指标，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

8.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求：

- a) 支持对网络拓扑图进行在线编辑，允许手工添加或删除监测节点或链路；

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

8.1.2 安全管理要求

8.1.2.1 安全标记

安全标记应满足以下要求：

- a) 能够对主/客体的安全标记统一管理，主体标记范围包括用户、代理进程、终端等，客体标记范

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

在操作系统、数据库、中间件、应用系统等重要性能指标中，

8.1.2.2 授权管理

授权管理应满足以下要求：

- a) 实现对每一个标记所能访问范围的统一管理；
- b) 实现主体对客体访问权限的统一管理，包括主机访问权限管理、网络访问权限管理、应用访问权限管理；
- c) 实现根据主体标记和客体标记安全级别的不同，制定访问控制策略，控制主体对客体的访问，

8.1.2.3 设备策略管理

8.1.2.3.1 安全配置策略

设备管理应满足以下要求：

- a) 实现对主机操作系统、数据库系统、网络设备、安

8.1.2.3.2 入侵防御

入侵防御应满足以下要求：

8.1.2.3.3 恶意代码防范

8.1.2.4 密码保障

8.1.3.1 审计策略集中管理

审计策略集中管理应满足以下要求：

- a) 能够查看主机操作系统、数据库系统、网络设备、安全设备的审计策略配置情况，有权策略

8.1.3 审计管理要求

8.1.3.2 审计数据集中管理

2.1.3.2.1 网站数据备份

审计数据采集应满足以下要求：

- a) 能够实现审计数据的归一化处理,内容应涵盖日期、时间、主体标识、客体标识、类型、结果、IP

2.2 审计数据采集对象

审计数据采集对象应满足以下要求:

- a) 支持安全设备(如防火墙、入侵检测系统、数据库审计设备、入侵防御系统、防病毒系统、邮件安全网关、网络控制系统等)与信息安全管理系统集成,实现安全设备与信息安全系统的联动。

计数据采集方式

采集方式应满足以下要求:

通过如 Syslog、SNMP 等协议采集各种系统或设备上的审计数据；

《中国南方民族关系史论》(三卷本)出版。

9.1.3.2.4 数据采集组件要求

边缘存和断点续传,在网络通信发生故障时,能够在数据采集任务对数据进行

以后,信息采集组将重新恢复向安全管理中心上报航网期间采集的数据。

9 1 3 2 5_ 审计数据关联分析

审计数据关联分析应满足以下要求：

④ 应提供规则关联规则自定义功能；

8.2 接口要求

8.2.1 第三方插件/代理接口协议要求

接口协议要求应满足以下要求：

- a) 安全管理中心应实现对 IPv4 及 IPv6 双协议环境的支持(包括 IPv4 环境、IPv6 环境等)；

8.2.2 接口安全要求

接口安全要求应满足以下要求：

- a) 采用安全的接口协议,保证接口之间交互数据的安全性；
- b) 采用加密和认证机制对接口数据进行保护；
- c) 各接口之间进行通信时,应通过身份验证机制相互验证对方身份；

8.3 自身安全要求

8.3.1 身份鉴别

安全管理中心控制台的管理员身份鉴别应满足以下要求：

- a) 提供专用的登录控制模块对管理员进行身份标识和鉴别,防止非法用户登录；
- b) 采用强身份鉴别技术,如密码鉴别、生物特征鉴别、数字证书鉴别等；
- c) 对同一管理员用户采用两种或两种以上身份鉴别技术；
- d) 对同一管理员用户采用两种或两种以上身份鉴别技术；

8.3.2 访问控制

8.3.3 可信路径

安全管理中心控制台的可信路径应满足以下要求：

及时采取必要的恢复措施，防止数据丢失和篡改。

通信系统应满足以下要求：

- a) 应能支持系统安全通信，防止数据丢失和篡改。
- b) 应能支持系统安全通信，防止数据丢失和篡改。

系统应满足以下要求：

系统应满足以下要求。

第五级安全管理

10 跨定级系统安全管理中心技术要求

跨定级系统安全管理中心应满足以下要求：

- a) 应能支持系统安全通信，防止数据丢失和篡改。
- b) 应能支持系统安全通信，防止数据丢失和篡改。
- c) 应能支持系统安全通信，防止数据丢失和篡改。
- d) 应能支持系统安全通信，防止数据丢失和篡改。

系统应满足以下要求：

系统应满足以下要求。

系统应满足以下要求。

系统应满足以下要求。

系统应满足以下要求。

系统应满足以下要求。

附录 A
(规范性附录)

保护对象等级对应关系

安全管理中心与网络安全等级保护

见表 A.1。

安全管理中心与网络安全等级保护对象等级对应关系

表 A.1 安全管理中心与网络安全等级

表 A.1 安全管理中心与网络安全等级

| 级别 | 网络安全等级保护对象等级 | 安全管理中心 |
|-----|--------------|--------|
| 第二级 | 第二级 | |
| 第三级 | 第三级 | |
| 第四级 | 第四级 | |
| 第五级 | 第五级 | |

附 录 B
(规范性附录)

主 D.1 内人等理由心社书西书八知主

| 级 | 技术要求 | 第二级 | 第三级 | 第四级 |
|--------------|----------|-------------|--------------|--------------|
| 8.1.1.1+ | 用户身份管理 | 6.1.1.1 | 7.1.1.1+ | 8.1.1.1+ |
| 8.1.2.1+ | 数据保密性 | 6.1.1.2.1 | 7.1.1.2.1+ | 8.1.1.2.1+ |
| 8.1.1.3.1+ | 数据完整性 | 6.1.1.3.1 | 7.1.1.3.1+ | 8.1.1.3.1+ |
| 6.1.1.2.3.1+ | 数据保护 | 6.1.1.2.3.1 | 7.1.1.2.3.1+ | 8.1.1.2.3.1+ |
| 8.1.1.2.4+ | 可信路径 | 6.1.1.2.4 | 7.1.1.2.4+ | 8.1.1.2.4+ |
| 7.1.1.0.4+ | 融合信息保护 | 7.1.1.0.4 | 8.1.1.0.4+ | 9.1.1.0.4+ |
| 6.1.1.3.1 | 安全事件采集 | 6.1.1.3.1 | 7.1.1.3.1+ | 8.1.1.3.1+ |
| 6.1.1.3.2 | 安全事件告警 | 6.1.1.3.2 | 7.1.1.3.2+ | 8.1.1.3.2+ |
| 6.1.1.3.3 | 安全事件响应 | 6.1.1.3.3 | 7.1.1.3.3+ | 8.1.1.3.3+ |
| 7.1.1.3.4 | 数据关联分析 | 7.1.1.3.4 | 8.1.1.3.4+ | 9.1.1.3.4+ |
| 6.1.1.3.5 | 统计分析报表 | 6.1.1.3.5 | 7.1.1.3.5+ | 8.1.1.3.5+ |
| 6.1.1.4.1 | 资产管理 | 6.1.1.4.1 | 7.1.1.4.1+ | 8.1.1.4.1+ |
| 7.1.1.4.2 | 资产业务价值评估 | 7.1.1.4.2 | 8.1.1.4.2+ | 9.1.1.4.2+ |
| 6.1.1.4.3 | 威胁管理 | 6.1.1.4.3 | 7.1.1.4.3+ | 8.1.1.4.3+ |
| 6.1.1.4.4 | 脆弱性管理 | 6.1.1.4.4 | 7.1.1.4.4+ | 8.1.1.4.4+ |
| 6.1.1.4.5 | 风险分析 | 6.1.1.4.5 | 7.1.1.4.5+ | 8.1.1.4.5+ |
| 6.1.1.5.1 | 资源监控 | 6.1.1.5.1 | 7.1.1.5.1+ | 8.1.1.5.1+ |
| 6.1.1.5.2 | 网络拓扑监测 | 6.1.1.5.2 | 7.1.1.5.2+ | 8.1.1.5.2+ |
| 7.1.2.1 | 安全标记 | 7.1.2.1 | 8.1.2.1+ | 9.1.2.1+ |
| 7.1.2.2 | 授权管理 | 7.1.2.2 | 8.1.2.2+ | 9.1.2.2+ |
| 7.1.2.3 | 安全策略管理 | 7.1.2.3 | 8.1.2.3+ | 9.1.2.3+ |
| 7.1.2.4 | 恶意代码防范 | 7.1.2.4 | 8.1.2.4+ | 9.1.2.4+ |
| 7.1.2.5 | 密码保障 | 7.1.2.5 | 8.1.2.5+ | 9.1.2.5+ |
| 7.1.2.6 | 数据备份与恢复 | 7.1.2.6 | 8.1.2.6+ | 9.1.2.6+ |
| 7.1.2.7 | 数据关联分析 | 7.1.2.7 | 8.1.2.7+ | 9.1.2.7+ |
| 7.1.2.8 | 数据关联分析 | 7.1.2.8 | 8.1.2.8+ | 9.1.2.8+ |
| 7.1.2.9 | 数据关联分析 | 7.1.2.9 | 8.1.2.9+ | 9.1.2.9+ |
| 7.1.2.10 | 数据关联分析 | 7.1.2.10 | 8.1.2.10+ | 9.1.2.10+ |
| 7.1.2.11 | 数据关联分析 | 7.1.2.11 | 8.1.2.11+ | 9.1.2.11+ |
| 7.1.2.12 | 数据关联分析 | 7.1.2.12 | 8.1.2.12+ | 9.1.2.12+ |
| 7.1.2.13 | 数据关联分析 | 7.1.2.13 | 8.1.2.13+ | 9.1.2.13+ |
| 7.1.2.14 | 数据关联分析 | 7.1.2.14 | 8.1.2.14+ | 9.1.2.14+ |
| 7.1.2.15 | 数据关联分析 | 7.1.2.15 | 8.1.2.15+ | 9.1.2.15+ |
| 7.1.2.16 | 数据关联分析 | 7.1.2.16 | 8.1.2.16+ | 9.1.2.16+ |
| 7.1.2.17 | 数据关联分析 | 7.1.2.17 | 8.1.2.17+ | 9.1.2.17+ |
| 7.1.2.18 | 数据关联分析 | 7.1.2.18 | 8.1.2.18+ | 9.1.2.18+ |
| 7.1.2.19 | 数据关联分析 | 7.1.2.19 | 8.1.2.19+ | 9.1.2.19+ |
| 7.1.2.20 | 数据关联分析 | 7.1.2.20 | 8.1.2.20+ | 9.1.2.20+ |
| 7.1.2.21 | 数据关联分析 | 7.1.2.21 | 8.1.2.21+ | 9.1.2.21+ |
| 7.1.2.22 | 数据关联分析 | 7.1.2.22 | 8.1.2.22+ | 9.1.2.22+ |
| 7.1.2.23 | 数据关联分析 | 7.1.2.23 | 8.1.2.23+ | 9.1.2.23+ |
| 7.1.2.24 | 数据关联分析 | 7.1.2.24 | 8.1.2.24+ | 9.1.2.24+ |
| 7.1.2.25 | 数据关联分析 | 7.1.2.25 | 8.1.2.25+ | 9.1.2.25+ |
| 7.1.2.26 | 数据关联分析 | 7.1.2.26 | 8.1.2.26+ | 9.1.2.26+ |
| 7.1.2.27 | 数据关联分析 | 7.1.2.27 | 8.1.2.27+ | 9.1.2.27+ |
| 7.1.2.28 | 数据关联分析 | 7.1.2.28 | 8.1.2.28+ | 9.1.2.28+ |
| 7.1.2.29 | 数据关联分析 | 7.1.2.29 | 8.1.2.29+ | 9.1.2.29+ |
| 7.1.2.30 | 数据关联分析 | 7.1.2.30 | 8.1.2.30+ | 9.1.2.30+ |
| 7.1.2.31 | 数据关联分析 | 7.1.2.31 | 8.1.2.31+ | 9.1.2.31+ |
| 7.1.2.32 | 数据关联分析 | 7.1.2.32 | 8.1.2.32+ | 9.1.2.32+ |
| 7.1.2.33 | 数据关联分析 | 7.1.2.33 | 8.1.2.33+ | 9.1.2.33+ |
| 7.1.2.34 | 数据关联分析 | 7.1.2.34 | 8.1.2.34+ | 9.1.2.34+ |
| 7.1.2.35 | 数据关联分析 | 7.1.2.35 | 8.1.2.35+ | 9.1.2.35+ |
| 7.1.2.36 | 数据关联分析 | 7.1.2.36 | 8.1.2.36+ | 9.1.2.36+ |
| 7.1.2.37 | 数据关联分析 | 7.1.2.37 | 8.1.2.37+ | 9.1.2.37+ |
| 7.1.2.38 | 数据关联分析 | 7.1.2.38 | 8.1.2.38+ | 9.1.2.38+ |
| 7.1.2.39 | 数据关联分析 | 7.1.2.39 | 8.1.2.39+ | 9.1.2.39+ |
| 7.1.2.40 | 数据关联分析 | 7.1.2.40 | 8.1.2.40+ | 9.1.2.40+ |
| 7.1.2.41 | 数据关联分析 | 7.1.2.41 | 8.1.2.41+ | 9.1.2.41+ |
| 7.1.2.42 | 数据关联分析 | 7.1.2.42 | 8.1.2.42+ | 9.1.2.42+ |
| 7.1.2.43 | 数据关联分析 | 7.1.2.43 | 8.1.2.43+ | 9.1. |

表 B.1 (续)

[illegible]

附录 C
(资料性附录)
归一化安全事件属性

表 C.1 归一化安全事件属性

| 序号 | 属性 | 描述 |
|-----|-----------|------------|
| 1 | 采集器 IP | 事件的采集器地址 |
| 2 | 采集器名称 | 事件的采集器名称 |
| 3 | 设备 IP | 产生该事件的设备地址 |
| 4 | 设备类型 | 该设备的设备类型 |
| 5 | 设备名称 | 设备名称 |
| 6 | 接收事件时间 | 事件采集时间 |
| 7 | 归并数量 | 归并事件的数目 |
| 8 | 事件源 IP | 事件源 IP 地址 |
| 9 | 事件源名称 | 事件源名称 |
| 10 | 事件源 IP 地址 | 事件源 IP 地址 |
| 11 | 事件内容 | 事件原始信息 |
| 12 | 事件源 IP | 事件源 IP 地址 |
| 13 | 事件源名称 | 事件源名称 |
| 14 | 事件源 IP 地址 | 事件源 IP 地址 |
| 15 | 事件源名称 | 事件源名称 |
| 16 | 事件源 IP 地址 | 事件源 IP 地址 |
| 17 | 事件源名称 | 事件源名称 |
| 18 | 事件源 IP 地址 | 事件源 IP 地址 |
| 19 | 事件源名称 | 事件源名称 |
| 20 | 事件源 IP 地址 | 事件源 IP 地址 |
| 21 | 事件源名称 | 事件源名称 |
| 22 | 事件源 IP 地址 | 事件源 IP 地址 |
| 23 | 事件源名称 | 事件源名称 |
| 24 | 事件源 IP 地址 | 事件源 IP 地址 |
| 25 | 事件源名称 | 事件源名称 |
| 26 | 事件源 IP 地址 | 事件源 IP 地址 |
| 27 | 事件源名称 | 事件源名称 |
| 28 | 事件源 IP 地址 | 事件源 IP 地址 |
| 29 | 事件源名称 | 事件源名称 |
| 30 | 事件源 IP 地址 | 事件源 IP 地址 |
| 31 | 事件源名称 | 事件源名称 |
| 32 | 事件源 IP 地址 | 事件源 IP 地址 |
| 33 | 事件源名称 | 事件源名称 |
| 34 | 事件源 IP 地址 | 事件源 IP 地址 |
| 35 | 事件源名称 | 事件源名称 |
| 36 | 事件源 IP 地址 | 事件源 IP 地址 |
| 37 | 事件源名称 | 事件源名称 |
| 38 | 事件源 IP 地址 | 事件源 IP 地址 |
| 39 | 事件源名称 | 事件源名称 |
| 40 | 事件源 IP 地址 | 事件源 IP 地址 |
| 41 | 事件源名称 | 事件源名称 |
| 42 | 事件源 IP 地址 | 事件源 IP 地址 |
| 43 | 事件源名称 | 事件源名称 |
| 44 | 事件源 IP 地址 | 事件源 IP 地址 |
| 45 | 事件源名称 | 事件源名称 |
| 46 | 事件源 IP 地址 | 事件源 IP 地址 |
| 47 | 事件源名称 | 事件源名称 |
| 48 | 事件源 IP 地址 | 事件源 IP 地址 |
| 49 | 事件源名称 | 事件源名称 |
| 50 | 事件源 IP 地址 | 事件源 IP 地址 |
| 51 | 事件源名称 | 事件源名称 |
| 52 | 事件源 IP 地址 | 事件源 IP 地址 |
| 53 | 事件源名称 | 事件源名称 |
| 54 | 事件源 IP 地址 | 事件源 IP 地址 |
| 55 | 事件源名称 | 事件源名称 |
| 56 | 事件源 IP 地址 | 事件源 IP 地址 |
| 57 | 事件源名称 | 事件源名称 |
| 58 | 事件源 IP 地址 | 事件源 IP 地址 |
| 59 | 事件源名称 | 事件源名称 |
| 60 | 事件源 IP 地址 | 事件源 IP 地址 |
| 61 | 事件源名称 | 事件源名称 |
| 62 | 事件源 IP 地址 | 事件源 IP 地址 |
| 63 | 事件源名称 | 事件源名称 |
| 64 | 事件源 IP 地址 | 事件源 IP 地址 |
| 65 | 事件源名称 | 事件源名称 |
| 66 | 事件源 IP 地址 | 事件源 IP 地址 |
| 67 | 事件源名称 | 事件源名称 |
| 68 | 事件源 IP 地址 | 事件源 IP 地址 |
| 69 | 事件源名称 | 事件源名称 |
| 70 | 事件源 IP 地址 | 事件源 IP 地址 |
| 71 | 事件源名称 | 事件源名称 |
| 72 | 事件源 IP 地址 | 事件源 IP 地址 |
| 73 | 事件源名称 | 事件源名称 |
| 74 | 事件源 IP 地址 | 事件源 IP 地址 |
| 75 | 事件源名称 | 事件源名称 |
| 76 | 事件源 IP 地址 | 事件源 IP 地址 |
| 77 | 事件源名称 | 事件源名称 |
| 78 | 事件源 IP 地址 | 事件源 IP 地址 |
| 79 | 事件源名称 | 事件源名称 |
| 80 | 事件源 IP 地址 | 事件源 IP 地址 |
| 81 | 事件源名称 | 事件源名称 |
| 82 | 事件源 IP 地址 | 事件源 IP 地址 |
| 83 | 事件源名称 | 事件源名称 |
| 84 | 事件源 IP 地址 | 事件源 IP 地址 |
| 85 | 事件源名称 | 事件源名称 |
| 86 | 事件源 IP 地址 | 事件源 IP 地址 |
| 87 | 事件源名称 | 事件源名称 |
| 88 | 事件源 IP 地址 | 事件源 IP 地址 |
| 89 | 事件源名称 | 事件源名称 |
| 90 | 事件源 IP 地址 | 事件源 IP 地址 |
| 91 | 事件源名称 | 事件源名称 |
| 92 | 事件源 IP 地址 | 事件源 IP 地址 |
| 93 | 事件源名称 | 事件源名称 |
| 94 | 事件源 IP 地址 | 事件源 IP 地址 |
| 95 | 事件源名称 | 事件源名称 |
| 96 | 事件源 IP 地址 | 事件源 IP 地址 |
| 97 | 事件源名称 | 事件源名称 |
| 98 | 事件源 IP 地址 | 事件源 IP 地址 |
| 99 | 事件源名称 | 事件源名称 |
| 100 | 事件源 IP 地址 | 事件源 IP 地址 |

中华人民共和国国家标准

信息安全技术 网络安全等级保护

信息安全技术 网络安全等级保护

安全管理中心技术要求

GB/T 36958—2018

中国标准出版社出版发行

北京市朝阳区和平里西街甲2号(100029)

北京市西城区三里河北街16号(100045)

网址: www.spc.org.cn

服务热线: 400-168-0010

2018年11月第一版

*

书号: 155066 · 1-61703

版权专有 侵权必究



GB/T 36958-2018