1. Выберите правильный вариант ответа: Что является ключевой целью архитектуры программного обеспечения кибериммунной системы?

2. Выберите правильный вариант ответа: Какое свойство наиболее полно отражает принцип «кибериммунитета»?

3. Какой архитектурный подход чаще всего используется для локализации последствий компрометации отдельных компонентов кибериммунной системы?

4. Какой элемент архитектуры отвечает за формализацию и хранение политик безопасности в кибериммунной системе?

5. Какой уровень архитектуры кибериммунной системы обеспечивает доверенную загрузку (secure boot) и контроль целостности базового ПО?

6. Какой принцип проектирования архитектуры кибериммунной системы минимизирует ущерб от скомпрометированного компонента?

7. Какой тип взаимодействия компонентов предпочтителен для обеспечения наблюдаемости и управляемости в кибериммунной архитектуре?

8. Какое свойство архитектуры позволяет анализировать поведение компонентов и выявлять аномалии для обеспечения кибериммунитета?

9. Какой подход к хранению секретов более соответствует требованиям кибериммунной архитектуры?

10. Какой тип тестирования архитектуры наиболее характерен для проверки свойств кибериммунитета?

11. Какое требование к архитектуре кибериммунной системы является базовым?

12. Какой элемент архитектуры обеспечивает сбор, корреляцию и анализ событий безопасности?

13. Какой подход к обновлению компонентов предпочтителен в кибериммунной архитектуре?

14. Какой архитектурный паттерн улучшает устойчивость к компрометации отдельных экземпляров сервисов?

15. Какой механизм аутентификации предпочтителен для взаимодействия микросервисов в кибериммунной системе?

16. Какой тип контроля доступа наиболее соответствует современным кибериммунным архитектурам?

17. Какой принцип логической сегментации сети рекомендуется в кибериммунной архитектуре?

18. Какой из подходов к проектированию интерфейсов между компонентами более безопасен?

19. Какое свойство архитектуры упрощает формальную верификацию критичных компонентов?

20. Какой вариант лучше описывает доверенную вычислительную базу (TCB) в кибериммунной архитектуре?

21. Какой подход к журналированию событий отвечает требованиям кибериммунитета?

22. Какой тип архитектурной документации особенно важен при проектировании кибериммунной системы?

23. Какое требование к интерфейсам внешних интеграций является ключевым для кибериммунной архитектуры?

24. Какой тип архитектурного контроля позволяет своевременно выявлять отклонения от целевой архитектуры безопасности?

25. Какое требование к конфигурации окружений (dev/test/prod) характерно для кибериммунной архитектуры?

26. Выберите все верные варианты: Какие принципы лежат в основе архитектуры программного обеспечения кибериммунной системы?

27. Какие архитектурные меры повышают устойчивость к атакам на коммуникации между компонентами?

28. Какие компоненты обычно относятся к доверенной вычислительной базе (TCB) в кибериммунной архитектуре?

29. Какие свойства архитектуры обеспечивают ограничение распространения атаки между подсистемами?

30. Какие типы политик безопасности чаще всего реализуются на архитектурном уровне кибериммунной системы?

31. Какие архитектурные решения способствуют обеспечению наблюдаемости (observability) кибериммунной системы?

32. Какие средства архитектуры поддерживают кибериммунитет при отказах аппаратного уровня?

33. Какие требования к API между компонентами важны для кибериммунной архитектуры?

34. Какие практики управления конфигурациями соответствуют принципам кибериммунитета?

35. Какие механизмы помогают проверить неизменность и целостность критичных компонентов?

36. Какие элементы архитектуры отвечают за реакцию на инциденты безопасности?

37. Какие меры повышают устойчивость архитектуры к ошибочным обновлениям?

38. Какие подходы используются для защиты межсервисных взаимодействий?

39. Какие свойства архитектуры важны для анализа поведения и обнаружения аномалий?

40. Какие механизмы минимизируют последствия компрометации учётной записи в кибериммунной архитектуре?

41. Какие подходы к проектированию доменов доверия используются в кибериммунной архитектуре?

42. Какие архитектурные артефакты необходимы для управления безопасностью на уровне жизненного цикла ПО?

43. Какие требования предъявляются к журналам событий в кибериммунной архитектуре?

44. Какие механизмы помогают защитить конфигурации кибериммунной системы от несанкционированных изменений?

45. Какие принципы применяются при проектировании внешних интерфейсов (API) для кибериммунной системы?

46. Какие атрибуты могут использоваться в атрибутной модели контроля доступа (ABAC) в кибериммунной архитектуре?

47. Какие компоненты архитектуры чаще всего интегрируются с SIEM для обеспечения кибериммунитета?

48. Какие типы изоляции могут применяться в архитектуре кибериммунной системы?

49. Какие архитектурные решения помогают снизить риск эксплуатации уязвимостей нулевого дня?

50. Какие меры учитываются при проектировании архитектуры обновлений кибериммунной системы?

51. Расположите этапы проектирования архитектуры кибериммунной системы в правильной последовательности.

52. Упорядочите шаги при обработке инцидента безопасности в кибериммунной архитектуре.

53. Установите правильную последовательность стадий жизненного цикла компонента кибериммунной системы.

54. Расположите шаги процесса управления изменениями архитектуры кибериммунной системы.

55. Определите правильную последовательность действий при внедрении новой политики безопасности.

56. Расположите этапы работы подсистемы мониторинга и корреляции событий.

57. Установите последовательность действий при выпуске обновлений в кибериммунной архитектуре.

58. Определите порядок проектирования доменов доверия в системе.

59. Расположите шаги при проектировании защищённого API между сервисами.

60. Установите последовательность действий при внедрении системы централизованного логирования.

61. Установите соответствие между архитектурным элементом и его ролью в кибериммунной системе.

62. Установите соответствие между архитектурным паттерном и реализуемым свойством кибериммунитета.

63. Установите соответствие между типом политики и её примером.

64. Установите соответствие между типом угроз и архитектурной мерой противодействия.

65. Установите соответствие между уровнем архитектуры и примером компонента.

66. Установите соответствие между задачей и соответствующим архитектурным артефактом.

67. Установите соответствие между типом тестирования и его целью в кибериммунной архитектуре.

68. Установите соответствие между механизмом защиты и уровнем его реализации.

69. Установите соответствие между типом события и предпочтительным источником логов.

70. Установите соответствие между ролью и её ответственностью в кибериммунной архитектуре.