Nesterenko V.R.

Words

1. threat detection - обнаружение угрозы
2. clarification around security analytics - разъяснение об аналитике безопасности
3. security appliances – техника безопасности
4. perimeter-based packet inspection – основанная на периметре проверка пакетов
5. ingress/egress traffic – входной/выходной трафик
6. pervasive service - повсеместная служба
7. cloud-based workloads - облачные рабочие нагрузки
8. distributed enforcement - распределенное правоприменение
9. Endpoint security consolidation - Консолидация безопасности конечной точки
10. amalgamation trend - тенденция к слиянию
11. device coverage – покрытие устройства
12. asset management – управление активами
13. cloud workloads – облачные нагрузки
14. Discourse - речь
15. enterprise cybersecurity professionals – промышленные специалисты в области информационной безопасности
16. Serverless functions – безсерверные функции
17. Prevalent - превалирующий
18. Hook – крюк
19. Temporal – временный
20. absent access – отсутствующий доступ
21. authentication - аутентификация
22. authorization – авторизация
23. encryption – шифрование
24. audit trail – контрольный журнал
25. continuous loop – продолжительный цикл
26. security data lakes – хранилище данных о безопасности
27. threat intelligence platforms – платформы обнаружения угроз
28. interoperate – взаимодействие
29. high-fidelity – высокая точность
30. tremendous - огромный
31. hyperbole - гипербола
32. premises - предпосылки
33. up to – вплоть до
34. takes a village – сложная задача
35. pace of change – темп перемен
36. complement – дополнение
37. loop – цикл
38. instance – экземпляр
39. anomalous – аномальный
40. impact – влияние
41. exploit – вредоносный код
42. privacy-enhancing technologies - технологии повышения конфиденциальности
43. digital cash – цифровые деньги
44. crypto-currency – крипто-ценность
45. sequence of transactions – набор транзакций
46. distributed computing – распределенные вычисления
47. proof-of-work – доказательство работы
48. email spam – спам в электронной почте
49. decentralized – децентрализованный
50. anonymity preserving solution - решение, сохраняющее анонимность
51. double-spending – двойные расходы
52. peer-to-peer setting – пользователь-к-пользователю (распределенный тип сети)
53. remediation mechanisms – механизмы исправления
54. hash-chaining – сцепление с помощью хэша
55. ordering of transfers – заказ переводов
56. transaction ledger – реестр транзакций
57. digital asset – цифровой актив
58. Byzantine quorums – византийский кворум
59. State-machine replication - Репликация конечного автомата
60. immutable sequence of transaction-blocks – неизменяемая последовательность транзакция-блок
61. chain of consensus blocks – цепь блоков консенсуса
62. Byzantine fault tolerance - Византийская отказоустойчивость
63. Smart contracts - смарт-контракт
64. shared data structure – общая структура данных
65. advanced cryptography tools – продвинутые криптографические инструменты
66. programatically facilitate – программно облегчить
67. Distributed protocols – распределенные протоколы
68. Threshold Adversary Model – модель предельного противника
69. Computational Threshold Adversary – вычислительный порог противника
70. Proof-of-Stake – доказательство доли
71. malicious adversary – злоумышленник
72. Public verifiability – возможность публичного потверждения
73. Blockchain replication – подделка блокчейна
74. a growing log of commands – растущий список команд
75. node – узел сети
76. Hybrid Consensus – гибридный консенсус
77. Validity – законность, валидность в сети
78. Agreement - соглашение
79. digital communication – цифровое общение
80. electronic data exchange – электронный обмен данными
81. cyber space – кибер-пространство
82. digital footprint – цифровой отпечаток
83. Integrity -
84. Asymmetrical Cryptography – ассиметричная криптография
85. Symmetrical Cryptography - симетричная криптография
86. Non-Repudiation - неотрекаемость
87. Hash Functions- хэш-функции
88. hash key – хэш-ключ
89. decryption - расшифровка
90. decoded - расшифровка
91. cryptanalysis - криптоанализ
92. distribution of the public key – рассылка открытого ключа
93. cyber criminal – киберпреступник
94. confidential – конфидениальный
95. recipient – получатель
96. cryptology – криптология
97. steganography – стеганография
98. artificial intelligence – искусственный интеллект
99. cognitive dimension – когнитивное измерение
100. fundamental notion – фундаментальное понятие
101. AI-model – модель искусственного интеллекта
102. Structure Mapping Engine - структурно-картографический движок
103. Abstraction - абстракция
104. computational concepts – вычислительные концепции
105. 3D-core – трехмерное ядро
106. Control point – контрольная точка
107. individually unpredictable – индивидуально-непредсказуемый
108. exploratory - поисковый
109. initially perplexed – изначально озадачен
110. Boundary Protection Device – устройство защиты границы
111. Brute Force Password Attack – атака перебором
112. Buffer Overflow – переполнение буфера
113. Bulk Encryption – поточное шифрование
114. Cardholder – разъем для карт
115. Central Services Node – центральный обслуживающий узел
116. Certificate Policy – политика сертификации
117. Chain of Evidence – цепь доказательств
118. Checksum – контрольная сумма
119. Clear Text – открытый текст
120. Closed Security Environment – закрытое защищенное окружение
121. Cloud Computing – облачное вычисление
122. Collision – коллизии(совпадения)
123. Community Risk – общественный риск
124. Computer Forensics – компьютерная криминалистика
125. Continuous Monitoring – продолжительный мониторинг
126. Cookie – куки(информация клиента в браузере)
127. Critical Infrastructure – критическая инфраструктура
128. Cross Site Scripting – межсайтовый скриптинг
129. Cryptographic Strength – криптографическая стойкость
130. Cryptographic Token – криптографический токен
131. Cyber Incident – кибер-инидент
132. Data Encryption Standard – стандарт шифрования данных
133. Data Encryption Algorithm – алгоритм шифрования данных
134. Data Loss – потеря данных
135. Digital Signature – цифровая подпись
136. Digital Signature Algorithm – алгоритм цифровой подписи
137. Domain – домен
138. Exploit Code – вредоносный код
139. Exploitable Channel – канал исполнения вредоносного кода
140. External Network – внешняя сеть
141. External Security Testing - внешние тесты безопасности
142. False Acceptance Rate – коэффициент ложного принятия
143. False Positive – Ложный позитив
144. False Rejection –ложный отказ
145. False Rejection Rate – коэффициент ложного отказа
146. Firewall - фаерволл
147. Firewall Control Proxy – управляющий фаерволом прокси
148. Full Disk Encryption – полнодисковое шифрование
149. Functional Testing – функциональное тестирование
150. Gateway – шлюз
151. Gray Box Testing – Тестирование серым ящиком
152. Identity Verification – верификация личности
153. Identity Validation – валидация личности
154. Identity Token – токен личности
155. Image - образ
156. Information Security Architecture – архитектура ИБ
157. Information Security Risk – Риск ИБ
158. Information System Life Cycle – жизненный цикл ИС
159. Information System Owner – владелец ИС
160. Initialize - инииализировать
161. Intranet – внутренняя сеть
162. Intrusion Detection Systems – система обнаружения вторжения
163. Intrusion Prevention System – система предотвращения вторжения
164. Key Expansion – расширение ключа
165. Key Logger – кейлогер(программа, записывающая нажатия клавиш)
166. Key Management – менеджмент ключа
167. Key Loader – загрузчик ключа
168. Key Pair – пара ключей
169. Key Stream – ключевой поток
170. Key Recovery – восстановление ключа
171. Key Updating – обновление ключа
172. Logic Bomb – логическая бомба
173. Malicious Code – вредоносный код
174. Malware – вредоносное ПО
175. Man-in-the-middle Attack – атака Человек в середине
176. Manual Cryptosystem – ручная криптосистема
177. Message Digest – дайджест сообщений
178. Spoofing - спуфинг
179. Mutual Authentication –ручная аутентификация
180. National Security System – система национальной безопасности
181. Network Sniffing – перехват пакетов в сети
182. Non-deterministic Random Bit Generator – недетерминированный генератор случайных битовых последовательностей
183. Nonce - нонс
184. Packet Sniffer
185. Passive Attack – пассивная атака
186. Passive Security Testing – пассивное тестирование безопасности
187. Password Cracking – взлом пароля
188. Payload - нагрузка
189. Penetration Testing – тестирование проникновением
190. Phishing - фишинг
191. Port Scanning – санирование портов
192. Public Seed – публичное семя для генерации последовательности
193. Quarantine - карантин
194. Radio Frequency Identification – радиочастотная идентификация
195. Random Number Generator – генератор случайных чисел
196. Random Bit Generator – случайный генератор битовых последовательностей
197. RBAC – доступ по модели разделения ролей
198. Remote Access – удаленный доступ
199. Repository - хранилище
200. Responder - ответчик
201. Risk Analysis - анализрисков
202. Risk Assessment – оценка рисков
203. Risk Assessment Methodology – методология оценки рисков
204. Risk Management – менеджмент рисков
205. Risk Model – модель рисков
206. Risk Monitoring – мониторинг рисков
207. Risk Tolerance – принятие риска
208. Round Key – Ключ раунда
209. Secure Communication Protocol – протокол защищенного сообщения
210. Secure Hash Algorithm – алгоритм защищенного хэширования
211. Secure Subsystem – подсистема безопасности
212. Security Category – категория безопасности
213. Security Domain – домен безопасности
214. Security Incident –инцидент безопасности
215. Security Inspection – инспекция безопасности
216. Security Kernel - ядро безопасности
217. Security Label – слой безопасности
218. Security Level – уровень безопасности
219. Security Perimeter – перметр безопасности
220. Security Plan – план безопасности
221. Security Policy – политика безопасности
222. Security Requirements – требования безопасности
223. Security Specification - спецификация безопасности
224. Shared Secret – распределенный секрет
225. Signature – подпись
226. Signature Certificate – сертификат подписи
227. Social Engineering – социальная инженерия
228. Technical Vulnerability Information – информация о технических уязвимостях
229. Threat - угроза
230. Threat Analysis – анализ угрозы
231. Threat Monitoring – мониторинг угрозы
232. Threat Source – источник угрозы
233. Traffic Analysis – анализ трафика
234. Trojan Horse – троянский конь
235. Triple DES – тройной стандарт шифрования данных
236. Trusted Certificate – заверенный сертификат
237. Trusted Agent – доверенный агент
238. Trusted Channel – доверенный канал
239. Unsigned data – неподписанные данные
240. Validation – валидация
241. Verification – верфикация
242. Virtual Private Network – Виртуальная частная сеть
243. Virtual Machine – виртуальная машина
244. Vulnerability Analysis – анализ уязвимостей
245. Web Bug – баг Веба
246. Wireless Access Point – беспроводная точка доступа
247. Zone Of Control - зона контроля
248. Initialization Vector – инициализирующий вектор
249. Intellectual Property – интеллектуальная собственность
250. Internal Network – внутренняя сеть