Cybersecurity Metrics

DAT-E1 [Essential] Implement data security by selecting appropriate cryptographic procedures, algorithms, and tools based on security policy and level of risk in an organization. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-E2 [Essential] Discuss forensically sound collection and acquisition of digital evidence. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-E3 [Essential] Apply principles, processes, tools and techniques used in mitigating security threats and responding to security incidents. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-E4 [Essential] Use appropriate levels of authentication, authorization, and access control to ensure data integrity and security for information systems and networks. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-E5 [Essential] Infer gaps in data security considering current and emerging technologies and the current state and prevailing trends in cybercrime. [Understanding]

Emerging Standard
DAT-S1 [Supplemental] Perform a forensic analysis on a local network, on stored data within a system as well as mobile devices for an enterprise environment. [Applying]

DAT-S2 [Supplemental] Outline complex technical concepts to technical and non-technical audiences as they relate to data security. [Analyzing]

DAT-LO-E01 [Essential] Analyze which cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation. [Analyzing]

DAT-LO-E02 [Essential] Apply symmetric and asymmetric algorithms as appropriate for a given scenario. [Applying]

DAT-LO-E03 [Essential] Investigate hash functions for checking integrity and protecting authentication data. [Applying]
Explain hash functions for checking integrity and protecting authentication data. [Understanding]

Developed Standard
Investigate hash functions for checking integrity and protecting authentication data. [Applying]

Highly Developed Standard
Examine hash functions for checking integrity and protecting authentication data. [Analyzing]

DAT-LO-E04 [Essential] Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher, and Enigma machine simulator, to encrypt and decrypt data. [Applying]

Emerging Standard
Describe some historical ciphers. [Understanding]

Developed Standard
Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher, and Enigma machine simulator, to encrypt and decrypt data. [Applying]

Highly Developed Standard
Contrast historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher, and Enigma machine, for encrypting and decrypting data. [Analyzing]

DAT-LO-S01 [Supplemental] Compare the benefits and drawbacks of applying cryptography in hardware vs software. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S02 [Supplemental] Demonstrate the importance of mathematical theory in the application of cryptography. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S03 [Supplemental] Deduce minimum key strength for symmetric algorithms to be effective. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S04 [Supplemental] Contrast trust models in PKI, such as hierarchical, distributed, bridge, and web of trust. [Analyzing]
DAT-LO-S05 [Supplemental] Explain how symmetric and asymmetric encryption are used in tandem to secure electronic communications and transactions, such as cryptocurrencies and other crypto assets. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S06 [Supplemental] Apply symmetric and asymmetric cryptography, such as DES, Twofish, AES, RSA, ECC, and DSA for a given scenario. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-E05 [Essential] Discuss the concept, need, and value of digital forensics. [Understanding]

Emerging Standard
Define the concept of digital forensics. [Remembering]
Developed Standard
Discuss the concept, need, and value of digital forensics. [Understanding]
Highly Developed Standard
Illustrate the concept, need, and value of digital forensics. [Applying]


Emerging Standard
Recognize components of a digital investigation, sources of digital evidence, and limitations of forensics. [Remembering]
Developed Standard
Describe components of a digital investigation, sources of digital evidence, limitations of forensics, and ethical considerations. [Understanding]
Highly Developed Standard
Debate sources of digital evidence, limitations of forensics, and ethical considerations. [Evaluating]

DAT-LO-E07 [Essential] Discuss key rules, laws, policies, and procedures that impact digital forensics. [Understanding]

Emerging Standard
List key rules, laws, policies, and procedures that impact digital forensics. [Remembering]
Developed Standard
Discuss key rules, laws, policies, and procedures that impact digital forensics. [Understanding]
Highly Developed Standard
Debate key rules, laws, policies, and procedures that impact digital forensics. [Evaluating]

DAT-LO-E08 [Essential] Explain how to preserve the chain of custody for digital evidence. [Understanding]
Emerging Standard
State the purpose of the chain of custody for digital evidence. [Remembering]
Developed Standard
Explain how to preserve the chain of custody for digital evidence. [Understanding]
Highly Developed Standard
Carry out the steps necessary to preserve the chain of custody for digital evidence. [Applying]

DAT-LO-E09 [Essential] Perform fundamental incident response functions including detecting, responding, and recovering from security incidents. [Applying]
Emerging Standard
Describe fundamental incident response functions including detecting, responding, and recovering from security incidents. [Understanding]
Developed Standard
Perform fundamental incident response functions including detecting, responding, and recovering from security incidents. [Applying]
Highly Developed Standard
Integrate fundamental incident response functions including detecting, responding, and recovering from security incidents. [Analyzing]

DAT-LO-S07 [Supplemental] Demonstrate the benefits of digital forensic readiness and planning. [Understanding]
Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S08 [Supplemental] Examine legal issues, authorities, and processes related to digital evidence. [Analyzing]
Emerging Standard
Developed Standard
Highly Developed Standard
DAT-LO-S09 [Supplemental] Describe the role and ethical responsibilities of a forensic examiner. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S10 [Supplemental] Outline a variety of digital forensic tools (open source vs. closed source) and their limits. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S11 [Supplemental] Describe digital forensics investigative procedures, such as identification of evidence, collection and preservation of evidence, timelines, reporting, chain of custody, and authentication of evidence. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S12 [Supplemental] Carry out forensically sound acquiring and handling of digital evidence following chain of custody best practices. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S13 [Supplemental] Analyze digital evidence from non-PC devices, such as smartphones, tablets, GPS, game consoles, Smart TVs, and IoT devices. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S14 [Supplemental] Apply documentation techniques and reporting of findings using industry standard and technically accurate terminology and format. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard
DAT-LO-S15 [Supplemental] Outline complex technical concepts and processes so that they are easily understood by non-technical audiences. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S16 [Supplemental] Carry out verification and validation of evidence during forensic acquisition, preservation, and analysis, including the use of hashes. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

DAT-LO-S17 [Supplemental] Summarize the best practices in collecting and isolating mobile devices when part of digital evidence. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

SOF-E1 [Essential] Write secure code with appropriate documentation for a software system and its related data. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

SOF-E2 [Essential] Analyze security and ethical considerations at each phase of the software development lifecycle. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

SOF-S1 [Supplemental] Implement isolation to secure a process or application. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard
SOF-LO-E02 [Essential] Execute access decisions and permissions based on explicit need. [Applying]

Emerging Standard
Classify access decisions and permissions based on explicit need. [Understanding]
Developed Standard
Execute access decisions and permissions based on explicit need. [Applying]
Highly Developed Standard
Analyze access decisions and permissions based on explicit need. [Analyzing]

SOF-LO-E01 [Essential] Apply fundamental design principles, including least privilege, open design, and abstraction, to system and application software. [Applying]

Emerging Standard
Describe fundamental design principles for system and application software. [Understanding]
Developed Standard
Apply fundamental design principles, including least privilege, open design, and abstraction, to system and application software. [Applying]
Highly Developed Standard
Evaluate the fundamental design principles used, including least privilege, open design, and abstraction, for a given software development scenario. [Evaluating]

SOF-LO-S01 [Supplemental] Test authorization and access control for a given class. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

Association for Computing Machinery

- Login
- Acceptable Use
- Privacy Policy

Copyright © 2020 ACM CCECC