Rheoli gweithgareddau fforensig digidol

Trosolwg

Mae'r safon hon yn ymwneud â rheoli prosiectau rheoli cylch bywyd meddalwedd. Mae hyn yn cynnwys sefydlu a goruchwylio polisïau, prosesau a gweithdrefnau fforensig digidol, gan gynnwys yr holl offer a thechnegau a gymeradwywyd i'w defnyddio a'r angen i weithredu'n foesegol ac yn broffesiynol.
Mae'n cynnwys gwneud penderfyniadau technegol strategol i gefnogi galluoedd fforensig digidol y sefydliad, a gwella effeithiolrwydd drwy roi awtomeiddio ar waith fel y bo'n briodol.
Mae'r safon hon ar gyfer y rhai sy'n gorfod rheoli gweithgareddau fforensig digidol yn rhan o'u dyletswyddau.

Meini prawf perfformiad

Rhaid i chi allu:

1. Pennu polisïau a gweithdrefnau’r sefydliad i ddiffinio prosesau fforensig digidol
2. Cynnal y gallu sefydliadol i gyflwyno'r gwasanaethau fforensig digidol gofynnol
3. Ymgynghori ag uwch-randdeiliaid i gytuno ar gyllidebau, blaenoriaethau a metrigau ar gyfer cyflwyno gwasanaethau fforensig digidol
4. Datblygu offer cymeradwy i gefnogi'r gwaith o gaffael data fforensig digidol a'i ddadansoddi
5. Nodi offer a thechnegau newydd a'u rhoi ar waith i gefnogi gwelliannau i brosesau fforensig digidol
6. Arwain ar gasglu data fforensig digidol, brysbennu a dadansoddi ac ymchwilio i achosion fforensig digidol cymhleth
7. Rheoli anghenion hyfforddi tîm fforensig digidol i gynnal lefelau uchel o berfformiad
8. Ennill a chynnal achrediadau perthnasol sy'n dilysu galluoedd fforensig digidol y sefydliad
9. Cynhyrchu a chyfathrebu adroddiadau ar fetrigau fforensig digidol a chanlyniadau ymchwiliadau i randdeiliaid priodol
10. Rhoi tystiolaeth tystion arbenigol fel archwiliwr fforensig digidol ar ran y sefydliad yn ôl yr angen

Gwybodaeth a dealltwriaeth

Mae angen i chi wybod a deall:

1. Y rheoliadau a’r safonau seiberddiogelwch perthnasol ar gyfer gwaith fforensig digidol
2. Pwysigrwydd rhoi arweiniad i ymchwilwyr fforensig digidol ar gynnal cywirdeb y dystiolaeth a’r broses ymchwilio
3. Arfer gorau'r diwydiant o ran methodolegau diogelwch a safonau a meincnodau'r diwydiant
4. Offer a thechnegau fforensig digidol safonol y diwydiant a sut i'w defnyddio
5. Bod dull olrhain fforensig digidol yn gofnod penodol o dystiolaeth ddigidol sy’n nodi cyflawni gweithgareddau digidol penodol, cyfathrebu a/neu storio data penodol
6. Pwysigrwydd cynnal tarddiad a dilysrwydd tystiolaeth ddigidol, o ystyried pa mor hawdd y gellir addasu gwybodaeth ddigidol
7. Ei bod yn bwysig brysbennu targedau digidol posibl yn ystod camau cychwynnol ymchwiliad fforensig digidol i flaenoriaethu ffynonellau data i’w dadansoddi
8. Yr achrediadau sy'n ofynnol i adfer neu ddelweddu data electronig fel darparwr gwasanaethau gwyddoniaeth fforensig digidol
9. Y safonau a'r ardystiadau rhyngwladol a gydnabyddir ar gyfer gwirio ansawdd a thrylwyredd y prosesau a ddilynir wrth gynnal archwiliadau fforensig digidol
10. Bod technegau fforensig digidol hefyd yn cael eu defnyddio i ddiogelu data mewn ymateb i geisiadau mynediad pwnc
11. Bod yn rhaid i feddalwedd caffael data fforensig greu copi cyflawn, heb ei addasu, yn ddibynadwy o'r targedau fforensig y mae wedi'u cynllunio i'w trin
12. Adroddiad terfynol yw canlyniad nodweddiadol ymchwiliad fforensig ac, o bryd i’w gilydd, gall arwain at gyflwyniad mewn ystafell llys.
13. Bod offer fforensig digidol, yn bennaf, yn darparu'r modd i gael tystiolaeth ddigidol o dargedau fforensig, echdynnu ac ail-greu data
14. Y gall nodi'r targedau fforensig perthnasol a'u caffael fod yn broses anodd a hirfaith
15. Mai cael copi lefel bit o'r targed fforensig yw'r canlyniad dymunol o echdynnu data fforensig digidol, a bod modd dadansoddi'r copi hwn wedi hynny gan ddefnyddio gwybodaeth am strwythur a semanteg y cynnwys data
16. Y gall rhywfaint o ddata fod yn ffug a bod wedi'i gynhyrchu gan ddefnyddio offer gwrth-fforensig er mwyn drysu ymchwiliad
17. Bod dilysu offer fforensig yn broses wyddonol sy'n gosod offer penodol ar brawf

systematig er mwyn sefydlu dilysrwydd y canlyniadau a gynhyrchir.
18. Yr ystyriaethau moesegol y mae angen eu defnyddio wrth gynnal ymchwiliadau fforensig digidol i ddata personol

TECDT61251

Rheoli gweithgareddau fforensig digidol

Datblygwyd gan	e-skills
Fersiwn rhif	1
Dyddiad cymeradwyo	30 Maw 2023
Dyddiad Adolygu Dangosol	30 Maw 2026
Dilysrwydd	Ar hyn o bryd
Statws	Gwreiddiol
Sefydliad cychwynnol	ODAG Consultants Ltd.
RCU gwreiddiol	TECDT61251
Galwedigaethau perthnasol	Gweithwyr Technoleg Gwybodaeth a Chyfathrebu Proffesiynol
Cyfres/Set	Gweithiwr TG a Thelathrebu Proffesiynol (procom)
Geiriau Allweddol	seiberddiogelwch, fforenseg ddigidol