Cyflwyno gwasanaethau fforensig digidol

Trosolwg

Mae'r safon hon yn ymwneud â chyflwyno gwasanaethau fforensig digidol.
Mae twf yn y defnydd o ddyfeisiau digidol at ddibenion sefydliadol a chymdeithasol wedi arwain at ymddygiadau y gallai fod angen ymchwilio iddynt o ran ymddygiad proffesiynol neu gyfreithlondeb.
Mae hyn yn cynnwys nodi ac ail-greu mewn modd moesegol y dilyniant perthnasol o ddigwyddiadau sydd wedi arwain at ymchwilio i system TG darged neu ddyfeisiau digidol a phwysigrwydd tystiolaeth ddigidol. Mae hyn yn cynnwys nodi, casglu a dadansoddi gwybodaeth ddigidol yn ofalus i gefnogi ymchwiliadau er mwyn pennu amgylchiadau digwyddiadau sy'n peri pryder i sefydliad tra'n cynnal cywirdeb tystiolaethol.
Mae'r safon hon yn cwmpasu'r cymwyseddau sydd eu hangen i gyflwyno gwasanaethau fforensig digidol. Mae ar gyfer y rhai sy'n gorfod cyflwyno gwasanaethau fforensig digidol yn rhan o'u dyletswyddau.

Meini prawf perfformiad

Rhaid i chi allu:

1. Mynd i leoliadau digwyddiadau i chwilio am ddata digidol, gan sicrhau parhad priodol yn y dystiolaeth
2. Cynnal archwiliadau ffisegol o ddyfeisiau digidol, gan gynnwys dadosod ac ailosod
3. Cynnal dadansoddiad fforensig rhagarweiniol i nodi manylebau dyfeisiau storio, a mathau o systemau a ffeiliau
4. Brysbennu systemau gwybodaeth a dyfeisiau digidol pan fo angen i flaenoriaethu a chynllunio gwaith adfer a dadansoddi data
5. Caffael data fforensig yn unol â chanllawiau sefydliadol
6. Dod o hyd i logiau system perthnasol a'u dehongli, i nodi anghysondebau neu dystiolaeth o beryglu gan gynnwys o waliau tân, dirprwyon, gweinyddwyr gwe, ffeiliau system, a dadansoddi pecynnau
7. Cynnal dadansoddiad fforensig manwl o ddata i adrodd hanes y gweithgaredd digidol ar gyfer senario'r defnyddwyr o dan sylw
8. Paratoi data tystiolaethol i'w ddefnyddio mewn ymchwiliadau pellach ac achosion cyfreithiol posibl
9. Cofnodi pob gweithgaredd fforensig digidol a chanlyniadau yn unol â safonau sefydliadol
10. Paratoi adroddiadau ar weithgareddau a chanfyddiadau fforensig digidol
11. Cyflwyno canfyddiadau fforensig digidol i randdeiliaid rheoli, cyfreithiol a rhanddeiliaid eraill

Gwybodaeth a dealltwriaeth

Mae angen i chi wybod a deall:

1. Y gall yr angen am ddadansoddiad fforensig digidol ddeillio o ddigwyddiadau, amheuaeth o fynediad diawdurdod at ddata, dwyn eiddo deallusol, ymchwiliadau i fygythiadau mewnol, twyll a cham-drin, camddefnyddio asedau, a thorri polisi sefydliadol
2. Cipolwg ar gyflwr y system o ddiddordeb yw'r man cychwyn ar gyfer dadansoddiad fforensig digidol o ddata. Mae hyn yn cynnwys yr hyn a gedwir ar hyn o bryd ar yriannau storio data, storio cwmwl, data system neu gyfrwng storio arall.
3. Sut i echdynnu a chynhyrchu delwedd ddrych o ddata, tra'n cynnal ei gyfanrwydd
4. Bod system weithredu yn cynnal amrywiaeth o gofnodion monitro sy'n gallu rhoi gwybodaeth ddefnyddiol am weithgarwch defnyddwyr cyfrifon unigol
5. Pensaernïaeth gyfrifiadurol, gweithrediad, cysylltedd a rhwydweithio sefydlog a rhithwir
6. Y ddeddfwriaeth mewn perthynas â Chamddefnyddio Cyfrifiaduron a Seiberdroseddu
7. Y Ddeddf Diogelu Data, y Ddeddf Rhyddid Gwybodaeth, a'r Ddeddf Gweithdrefn ac Ymchwiliadau Troseddol
8. Sut i reoli prosiectau fforensig digidol yn effeithiol i sicrhau bod gofynion a disgwyliadau rhanddeiliaid yn cael eu bodloni
9. Sut i gael mynediad at ddyfeisiau digidol a'u harchwilio, gan gynnwys gyriannau disg caled, gyriannau cyflwr solet, cardiau SIM ffôn symudol a chyfryngau storio eraill
10. Offer a thechnegau delweddu a dadansoddi fforensig digidol safonol y diwydiant a sut i'w defnyddio
11. Sut i chwilio a hidlo ffynonellau data i nodi data o ddiddordeb
12. Sut i ddarllen ac echdynnu data i nodi ffeithiau a pherthnasoedd unigol a all ategu neu wrthbrofi rhagdybiaeth sy'n cael ei hymchwilio
13. Y camau sy'n gysylltiedig â chynnal archwiliad fforensig o ddyfeisiadau neu systemau digidol yn unol â pholisïau a gweithdrefnau sefydliadol
14. Wrth i ddyfeisiadau storio ddatblygu, ei bod yn fwyfwy anodd cael copi ffisegol gwirioneddol o'r cyfryngau ac efallai mai caffaeliad rhesymegol neu rannol yw'r unig bosibilrwydd.
15. Sut i ddefnyddio dadansoddiad fforensig sy'n gallu esbonio'r dystiolaeth data

digidol a gafwyd

16. Sut i adrodd ar archwiliadau fforensig i ddweud hanes y data o weithgareddau digidol defnyddwyr yr ymchwilir iddynt

17. Yr angen i gynnal gwybodaeth fforensig ddigidol i barhau i fod yn ymwybodol o ddyfeisiau digidol newydd a thechnolegau storio data

18. Y gallai fod angen cyflwyno canlyniadau ymchwiliad fforensig ar ffurf sy'n dderbyniol mewn llys barn

19. Gwybod pryd i weithredu a phryd i beidio â gweithredu

20. Yr angen i weithredu'n foesegol wrth ymdrin â data personol

Cyflwyno gwasanaethau 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	TECDT61241
Galwedigaethau perthnasol	Gweithwyr Technoleg Gwybodaeth a Chyfathrebu Proffesiynol
Cyfres/Set	Gweithiwr TG a Thelathrebu Proffesiynol (procom)
Geiriau Allweddol	seiberddiogelwch, fforenseg ddigidol