Cyfrannu at weithgareddau ymchwilio a rheoli digwyddiadau diogelwch gwybodaeth

Trosolwg

Pan fydd digwyddiadau diogelwch gwybodaeth, rhaid i sefydliadau ymateb yn gyflym ac yn effeithiol i amddiffyn eu hunain rhag ymosodiadau a chyfyngu ar ddifrod a chwmpas ymosodiadau. Er mwyn gwneud hyn mae angen iddynt sefydlu timau ymateb i ddigwyddiadau a diffinio'r polisïau a'r safonau sy'n ymwneud â datblygu, gweithredu a gwella galluoedd rheoli digwyddiadau.
Mae'r safon hon yn diffinio'r cymwyseddau sy'n gysylltiedig â chyfrannu at ddadansoddi a gwerthuso digwyddiad o ddiddordeb a allai ddatblygu i fod yn broblemau a'u huwchgyfeirio at dimau rheoli digwyddiadau fel y bo'n briodol.

Meini prawf perfformiad

Rhaid i chi allu:

1. rhoi ymateb cychwynnol i ddigwyddiadau diogelwch gwybodaeth yr adroddwyd amdanynt, yn unol â safonau sefydliadol
2. uwchgyfeirio materion diogelwch gwybodaeth at uwch-ymchwilwyr yn unol â meini prawf uwchgyfeirio digwyddiadau sefydliadol
3. cynorthwyo i gynnal cyfweliadau, dadansoddi systemau gwybodaeth, adolygu dogfennau a dadansoddi systemau monitro amddiffynnol yn ystod

ymchwiliadau i ddigwyddiadau diogelwch gwybodaeth

1. dilyn gweithdrefnau a safonau sefydliadol yn gywir mewn perthynas â gweithgareddau rheoli digwyddiadau diogelwch gwybodaeth
2. defnyddio offer rheoli digwyddiadau diogelwch gwybodaeth yn unol â safonau sefydliadol
3. gweithredu gydag gonestrwydd a chyfrinachedd yn ystod gweithgareddau ymchwilio i ddigwyddiadau diogelwch gwybodaeth yn unol â safonau sefydliadol
4. ceisio cyngor ac arweiniad priodol yn ôl yr angen yn ystod gweithgareddau ymchwilio i ddigwyddiadau diogelwch gwybodaeth
5. nodi'r angen am archwiliad fforensig manwl yn rhan o ymchwiliad i ddigwyddiad diogelwch gwybodaeth
6. dogfennu'r holl ganfyddiadau ymchwiliadau i ddigwyddiadau diogelwch gwybodaeth ac adrodd arnynt yn unol â safonau sefydliadol

Gwybodaeth a dealltwriaeth

Mae angen i chi wybod a deall:

1. beth yw ystyr digwyddiad diogelwch gwybodaeth
2. beth yw pwrpas rheoli digwyddiadau a'i rôl ym maes diogelwch gwybodaeth
3. pryd i alw am archwiliad fforensig manwl yn rhan o ymchwiliad
4. sut i roi gwybod am ddigwyddiad diogelwch yn eu maes gwaith eu hunain
5. sut y gall graddfa digwyddiad diogelwch gwybodaeth effeithio ar y busnes ac ysgogi ymateb sy'n seiliedig ar barhad busnes
6. sut i gofnodi a chadw tystiolaeth i allu ei defnyddio i ategu achos ffurfiol
7. prif gamau rheoli digwyddiadau; e.e. nodi, cadw, glanhau, adfer, cau'r
8. prosesau, gweithdrefnau, dulliau, offer a thechnegau sy'n ymwneud â gweithgareddau rheoli digwyddiadau diogelwch gwybodaeth a'r amcanion i'w cyflawni
9. y ddeddfwriaeth a'r rheoliadau allanol, y polisïau mewnol a'r safonau mewnol ac allanol sy'n berthnasol i weithgareddau rheoli digwyddiadau diogelwch gwybodaeth
10. sut y gall effaith digwyddiadau diogelwch ar fusnes ddylanwadu
11. ar yr angen am gyfrinachedd, gonestrwydd, argaeledd ac enw da yn eu maes gwaith
12. sut y gall rheoli digwyddiadau diogelwch liniaru goblygiadau digwyddiadau diogelwch
13. yr angen i gadw tystiolaeth i gynorthwyo achosion ffurfiol
14. yr angen i weithgareddau rheoli digwyddiadau gael eu cynnal yn unol ag unrhyw godau ymddygiad a safonau sefydliadol

TECIS60632

Cyfrannu at weithgareddau ymchwilio a rheoli digwyddiadau diogelwch gwybodaeth

Datblygwyd gan	e-skills
Fersiwn rhif	1
Dyddiad cymeradwyo	01 Maw 2016
Dyddiad Adolygu Dangosol	01 Ebr 2019
Dilysrwydd	Ar hyn o bryd
Statws	Gwreiddiol
Sefydliad cychwynnol	The Tech Partnership
RCU gwreiddiol	TECIS60632
Galwedigaethau perthnasol	Swyddog Technoleg Gwybodaeth a Chyfathrebu, Technoleg Gwybodaeth a Chyfathrebu, Gweithwyr Proffesiynol Technoleg Gwybodaeth a Chyfathrebu
Cyfres/Set	Diogelwch Gwybodaeth
Geiriau Allweddol	Diogelwch gwybodaeth, seiberddiogelwch, rheoli digwyddiadau, ymchwilio i ddigwyddiadau