TECIS60631

Cyfrannu at weithgareddau canfod a dadansoddi ymyriadau i ddiogelwch gwybodaeth

Trosolwg

Mae dadansoddi ymyriadau yn ymwneud â chanfod materion diogelwch gwybodaeth, gan gynnwys torri diogelwch rhwydwaith. Gellir adolygu unrhyw faterion a nodir a'u huwchgyfeirio at dimau ymateb i ddigwyddiadau. Mae canfod ymyriadau yn golygu defnyddio ystod o gyfarpar awtomataidd i fonitro systemau a rhwydweithiau gwybodaeth mewn amser real, a bydd prosesau dadansoddi ymyriadau yn dehongli'r rhybuddion a gynhyrchir gan y cyfarpar hynny. Mae hyn yn cynnwys cyfatebu gwybodaeth o amrywiaeth o ffynonellau cyn penderfynu a yw'r rhybudd yn dynodi toriad diogelwch ai peidio. Os canfyddir toriad diogelwch, caiff hwn ei uwchgyfeirio at dîm ymateb i ddigwyddiadau, gan roi hysbysiad o'r toriad a thystiolaeth gysylltiedig bod toriad wedi digwydd.

Mae'r safon hon yn diffinio'r cymwyseddau sydd eu hangen i helpu i ganfod achosion o doriadau mewn systemau gwybodaeth a systemau diogelwch rhwydwaith. Mae hyn yn cynnwys yr angen i ddehongli'r rhybuddion a gynhyrchir mewn amser real gan gyfarpar canfod awtomataidd, i benderfynu a yw'r rhybudd yn dynodi toriad diogelwch ai peidio. Mae'n cynnwys dadansoddi'r mater diogelwch gwybodaeth i'w uwchgyfeirio at y tîm ymateb i ddigwyddiad.

Meini prawf perfformiad

Rhaid i chi allu:

1. adolygu ffeiliau log a gynhyrchir gan weinyddion, gweinyddion rhithwir, waliau tân a llwybryddion er mwyn canfod anghysondebau o ran diogelwch gwybodaeth
2. ymateb i rybuddion amser real o gyfarpar dadansoddi rhwydwaith a chyfarpar canfod materion systemau gwybodaeth er mwyn nodi anghysondebau o ran diogelwch gwybodaeth
3. cynorthwyo'r gwaith o gyfateb anomaleddau diogelwch gwybodaeth a chymharu â data am fygythiadau a gwendidau hysbys i benderfynu a yw anghysondeb yn dynodi toriad diogelwch gwybodaeth
4. ffurfweddu systemau gwybodaeth a chyfarpar monitro a dadansoddi rhwydwaith i greu rhybuddion awtomataidd i wendidau
5. diweddaru cronfeydd data am fygythiadau a gwendidau i nodi anghysondebau o ran diogelwch gwybodaeth yn erbyn bygythiadau a gwendidau hysbys
6. cyfathrebu'n effeithiol â'r timau ymateb i ddigwyddiadau i uwchgyfeirio digwyddiadau posibl a chynnwys tystiolaeth ategol
7. cofnodi gwybodaeth yn gywir am anomaleddau diogelwch gwybodaeth a ganfuwyd a pharatoi adroddiadau cryno yn unol â safonau sefydliadol

Gwybodaeth a dealltwriaeth

Mae angen i chi wybod a deall:

1. sut i adolygu systemau ffeiliau log i nodi anghysondebau o ran diogelwch gwybodaeth
2. sut i ddehongli rhybuddion a chynghorion a ddarperir gan gyfarpar canfod bygythiadau a gwendidau awtomataidd
3. sut i gysylltu rhybuddion ag ymddygiad a arsylwyd mewn systemau gwybodaeth a rhwydweithiau
4. sut i gyfatebu data am anomaleddau diogelwch gwybodaeth â data am fygythiadau a gwendidau hysbys
5. sut i ddadansoddi anomaleddau diogelwch gwybodaeth i benderfynu a fu digwyddiad
6. sut i gymharu anghysondebau o ran diogelwch gwybodaeth â bygythiadau a gwendidau hysbys i ganfod yr achos
7. sut i weithredu yn unol â chytundebau lefel gwasanaeth neu feini prawf perfformiad a ddiffinnir gan y cyflogwr
8. sut i gyfathrebu'n effeithiol â'r tîm ymateb i ddigwyddiad pan ddynodir ymyriadau fel digwyddiadau diogelwch gwybodaeth
9. sut i ffurfweddu cyfarpar dadansoddi a monitro rhwydweithiau
10. sut i gynnal ymchwil i ddod o hyd i wybodaeth am fygythiad a gwendid
11. sut i ddiweddaru cronfeydd data am fygythiadau a gwendidau i gadw golwg ar fygythiadau a gwendidau hysbys

TECIS60631

Cyfrannu at weithgareddau canfod a dadansoddi ymyriadau i ddiogelwch 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	TECIS60631
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, dadansoddi ymyriadau, canfod ymyriadau