TECIS60652

Rheoli gweithgareddau 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 datblygu'r safonau ar gyfer canfod, ymchwilio a rheoli digwyddiadau diogelwch, a'r gallu i ymchwilio a rheoli diogelwch yn llawn.

Meini prawf perfformiad

Rhaid i chi allu:

1. diffinio a rhoi ar waith y polisïau, y safonau a'r gweithdrefnau ar gyfer canfod, ymchwilio a rheoli digwyddiadau diogelwch gwybodaeth
2. arwain y tîm ymchwilio a rheoli digwyddiad yn unol â safonau sefydliadol
3. rheoli anghenion y tîm ymchwilio a rheoli digwyddiad diogelwch gwybodaeth o ran adnoddau, hyfforddiant a datblygiad yn unol â gofynion sefydliadol
4. rheoli'r cynlluniau ymateb i ddigwyddiadau diogelwch gwybodaeth gan gynnwys paratoi'r adroddiad terfynol yn unol â safonau sefydliadol
5. cydlynu'r dadansoddiad o achosion sylfaenol digwyddiadau yn unol â safonau sefydliadol
6. asesu’r angen am weithgarwch fforensig digidol, ac uwchgyfeirio digwyddiadau at dimau fforensig digidol yn ôl yr angen
7. paratoi adroddiadau am ddigwyddiadau a chyfathrebu â rhanddeiliaid i sicrhau yr eir i'r afael â'r holl risgiau uniongyrchol
8. rhoi diweddariadau cywir ar statws digwyddiadau diogelwch gwybodaeth
9. cynnal ymarferion i brofi, gwirio a gwella perfformiad o ran ymateb i ddigwyddiadau diogelwch gwybodaeth a diweddaru polisïau a gweithdrefnau yn ôl yr angen
10. cyfathrebu gallu parhaus y tîm ymchwilio a rheoli digwyddiad yn unol â gofynion y sefydliad

Gwybodaeth a dealltwriaeth

Mae angen i chi wybod a deall:

1. sut i arwain tîm sy'n cynnal ymchwiliadau i ddigwyddiadau diogelwch gwybodaeth i nodi gwybodaeth am ddigwyddiadau a'i dadansoddi
2. sut i gynnal pob cam sy'n gysylltiedig ag ymateb i ddigwyddiadau diogelwch gwybodaeth a'u rheoli
3. sut i asesu gallu'r tîm ymateb i ddigwyddiadau diogelwch gwybodaeth
4. sut i ddatblygu'r polisïau a'r safon sy'n ofynnol ar gyfer ymchwilio i ddigwyddiadau diogelwch gwybodaeth a'u rheoli
5. sut i bennu hyd a lled toriad diogelwch posibl drwy dechnegau ymchwilio i ddigwyddiad
6. sut i gydlynu dadansoddiad o achosion sylfaenol digwyddiadau diogelwch gwybodaeth
7. sut i adrodd a chyflwyno canfyddiadau o ymchwiliad i ddigwyddiad diogelwch gwybodaeth i noddwyr a rhanddeiliaid
8. bod angen dilyn prosesau ymateb cyflym ar gyfer digwyddiadau diogelwch gwybodaeth
9. sut i greu a chynnal profion digwyddiad diogelwch gwybodaeth gan gynyddu soffistigeiddrwydd ar draws yr holl systemau gwybodaeth hanfodol i wirio perfformiad o ran ymateb i ddigwyddiad
10. pwysigrwydd meithrin perthnasoedd cryf yn fewnol ac yn allanol yn rhan o'r tîm ymateb i ddigwyddiadau diogelwch gwybodaeth
11. yr angen i nodi ffynonellau arferion gorau ar gyfer rheoli ac ymchwilio i ddigwyddiadau diogelwch gwybodaeth a sut i wneud y defnydd gorau o'r rhain

TECIS60652

Rheoli gweithgareddau 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	TECIS60652
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