Enw: _____ Dyddiad: _____ Sgôr: _____

Hanfodion Seiberddiogelwch a Bygythiadau Atal

Bygythiadau seiberddiogelwch, waliau tân rhwydwaith, dilysu aml-ffactor, fframweithiau diogelwch

TROSOLWG DYSGU HANFODION SEIBERDDIOGELWCH

WEDI'I DDIOGELU

AMGRYPTIO DATA

Safon AES 256-did

YN CYDYMFFURFIO

SAFONAU BYD-EANG

Fframweithiau GDPR a CCPA

DIM YMDDIRIEDAETH

POLISI MYNEDIAD

Dilysu Aml-ffactor

Croeso! Mae'r pecyn gweithgareddau hwn yn eich tywys drwy egwyddorion sylfaenol Seiberddiogelwch ac Atal Bygythiadau Ar-lein. Byddwch yn archwilio bygythiadau maleiswedd, dilysu aml-ffactor, waliau tân rhwydwaith a fframweithiau ymateb i ddigwyddiadau.

PWYNTIAU GWIRIO'R DAFLEN WAITH

- [ ] **Rhan 1-4: Meistroli seiberddiogelwch ac atal bygythiadau.**
- [ ] **Rhan 5-7: Datrys posau croesair a chwilair.**
- [ ] **Rhan 8-9: Datrys astudiaethau achos a her y seiffr.**
- [ ] **Rhan 10: Adolygu tudalennau Cwestiynau Cyffredin sylfaenol ac uwch.**
- [ ] **Rhan 11: Archwilio 10 ffaith ddiddorol o'r byd go iawn.**
- [ ] **Bonws: her Meddwl yn Gyflym.**

Agorwch Ganllaw Seiberddiogelwch VPN.com

URL: https://www.vpn.com/cy/diogelwch-seiber/

Eich Map Llwybr Dysgu Hanfodion Seiberddiogelwch

- Nodwch fectorau cyffredin maleiswedd, gwe-rwydo ac ymyrraeth â rhwydweithiau corfforaethol.
- Rhowch reolaethau seiberddiogelwch safonol ar waith, gan gynnwys MFA, waliau tân ac amddiffyn dyfeisiau terfynol.
- Gwerthuso gweithdrefnau ymateb i ddigwyddiadau ar gyfer lliniaru effeithiau tor data.
- Dadansoddwch ffactorau risg sefydliadol ac aliniad diogelwch o dan ganllawiau NIST.
- Ffurfweddwch arferion hylendid diogelwch i liniaru stwffio manylion mewngofnodi awtomataidd.

CYFARWYDDIADAU'R CANLLAW SEIBERDDIOGELWCH

Atebwch y cwestiynau amlddewis a gwir/gau, cwblhewch y brawddegau llenwi bylchau gan ddefnyddio'r banc geiriau, parwch y diffiniadau, a datryswch y posau croesair a chwilair. Cymhwyswch eich gwybodaeth i atal bygythiadau. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

HANFODION SEIBERDDIOGELWCH AC ATAL BYGYTHIADAU (CYFLWYNIAD)

Mae seiberddiogelwch yn diogelu rhwydweithiau, systemau a data rhag ymosodiadau digidol heb awdurdod. Mae datblygu arferion diogelwch cadarn, ffurfweddu waliau tân, mynnu dilysu aml-ffactor, a hyfforddi staff i adnabod bygythiadau yn elfennau hanfodol o amddiffyn rhwydwaith corfforaethol.

DARLLENWCH BOB PWYNT GWIRIO YN OFALUS A DEWISWCH NEU YSGRIFENNWCH YR YMATEB CYWIR.

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw prif amcan ymosodiad gwe-rwydo?**
   - A. Dwyn manylion mewngofnodi a data sensitif defnyddwyr
   - B. Gwella gweledegdd gwefan mewn peiriannau chwilio
   - C. Cynyddu capasiti lled band y rhwydwaith
   - D. Rheoli dyblygu canolfan ddata wrth gefn

2. **2. Pa fecanwaith sy'n darparu'r diogelwch cryfaf i gyfrifon?**
   - A. Dilysu aml-ffactor gan ddefnyddio allweddi caledwedd
   - B. Cyfrineiriau cymhleth a ddiweddarir bob deg diwrnod ar hugain
   - C. Cyfyngu mewngofnodi i'r cyfrif i oriau busnes
   - D. Cuddio enw defnyddiwr y cyfrif rhag cyfeiriaduron cyhoeddus

3. **3. Beth sy'n diffinio llwyth tâl haint meddalwedd wystlo?**
   - A. Amgryptio ffeiliau system a mynnu taliad
   - B. Cofnodi trawiadau bysell yn dawel i weinyddion pell
   - C. Chwistrellu hysbysebion heb awdurdod i borwyr
   - D. Defnyddio adnoddau CPU lleol i gloddio arian cyfred digidol

4. **4. Sut mae camfanteisio dim-diwrnod (zero-day) yn effeithio ar amddiffynfeydd diogelwch?**
   - A. Mae'n targedu gwendidau anhysbys heb eu clytio
   - B. Mae'n analluogi wal dân y cwmni yn awtomatig
   - C. Mae'n gorfodi'r system i ailgychwyn yn galed
   - D. Nid oes angen unrhyw gyllideb i'w unioni

5. **5. Pa fframwaith sy'n llywodraethu rheolaethau diogelwch corfforaethol?**
   - A. Canllawiau Fframwaith Seiberddiogelwch NIST
   - B. Manylebau sgema dogfennau W3C HTML5
   - C. Llawlyfrau gosod gyrwyr argraffydd
   - D. Diffiniadau protocol llwybro IETF

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn Gwir/Gau 6

6. Dim ond cyfrifon e-bost personol y mae ymosodiadau gwe-rwydo yn eu targedu.

○ Gwir ○ Gau

7 Cwestiwn Gwir/Gau 7

7. Mae dilysu aml-ffactor yn helpu i rwystro ymosodiadau stwffio manylion mewngofnodi.

○ Gwir ○ Gau

8 Cwestiwn Gwir/Gau 8

8. Mae waliau tân yn archwilio traffig rhwydwaith i rwystro mynediad heb awdurdod at byrth.

○ Gwir ○ Gau

9 Cwestiwn Gwir/Gau 9

9. Mae unioni campau dim-diwrnod yn gofyn am ddiweddariadau diffiniadau gwrthfeirws safonol.

○ Gwir ○ Gau

10 Cwestiwn Gwir/Gau 10

10. Gweinydd abwyd a ddefnyddir i ddenu seiberdroseddwyr yw pot mêl.

○ Gwir ○ Gau

Pwynt Gwirio 3: Mewnosod Termau Allweddol

Darllenwch bob brawddeg isod a llenwch y bwlch gyda'r term cywir o'r Banc Geiriau.

1. Mae gweinyddwyr rhwydwaith yn gosod _____ i hidlo traffig sy'n dod i mewn.

2. Mae ymosodwr yn defnyddio _____ dim diwrnod i osgoi clytiau'r system.

3. Mae ymosodwyr yn anfon e-byst ffug i gynnal ymgyrchoedd _____ yn erbyn gweithwyr.

4. Mae ransomwedd yn ffurf ddinistriol ar feddalwedd o'r enw _____ sy'n cloi data defnyddwyr.

5. Mae sefydlu _____ cyfrineiriau cryf yn lliniaru risgiau dwyn manylion mewngofnodi.

6. I ddiogelu cyfathrebu sensitif, mae defnyddwyr yn cymhwyso protocolau _____ .

BANC GEIRIAU GEIRFA

AMGRYPTIO | AML-FFACTOR | CAMFANTEISIO | GWE-RWYDO | HYLENDID | MALEISWEDD | RANSOMWEDD | WAL DÂN

Ysgrifennwch eich atebion yma:

1.

2.

3.

4.

5.

6.

Pwynt Gwirio 4: Paru Cysyniadau Diogelwch

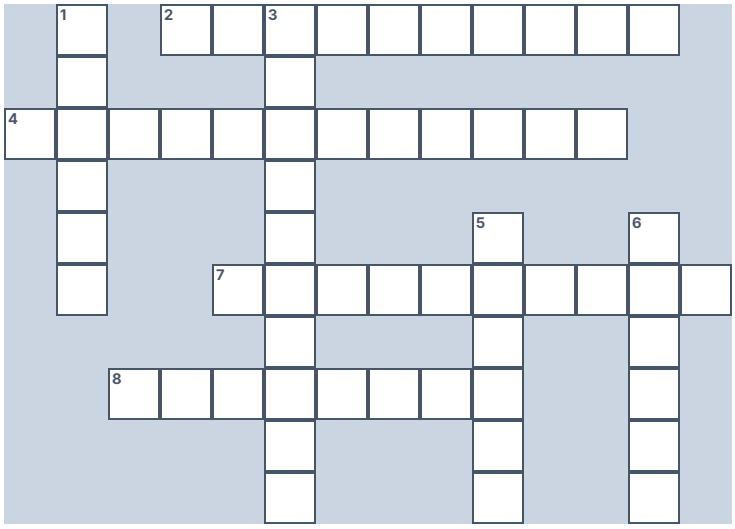
PARU DIFFINIADAU

Parwch bob term geirfa ar y chwith â'i ddiffiniad cywir ar y dde drwy ysgrifennu'r llythyren gyfatebol (A-H) yn y blwch mewnbwn y gellir ei lenwi.

	1. Bygythiad Nwyddau Pridwerth	A	Canllawiau strwythuredig fel NIST a ddefnyddir i reoli risgiau seiber.
	2. Dilysu Aml-Ffactor	B	Cynllun strwythuredig ar gyfer ymdrin â thoriadau diogelwch a'u lliniaru.
	3. Camfanteisio Dim Diwrnod	C	Rhwystr rhwydwaith sy'n hidlo traffig yn seiliedig ar reolau diogelwch.
	4. Pot Mêl Abwyd	D	Maleiswedd sy'n amgryptio data ac yn mynnu taliad ariannol am ei ddadgryptio.
	5. Wal Dân Ymwthiadau	E	Camfanteisio ar wendid a dargedir cyn i'r gwerthwr ryddhau clwt.
	6. Ymateb i Ddigwyddiadau	F	Arferion gorau ar gyfer rheoli manylion mewngofnodi ac allweddi dilysu.
	7. Hylendid Cyfrineiriau	G	Dilysiad diogelwch sy'n gofyn am ddau ffactor dilysu neu fwy.
	8. Fframwaith Diogelwch	H	System abwyd a sefydlwyd i ddenu a dadansoddi actorion maleisus.

Pwynt Gwirio 5: Pos Croesair

Datryswch y croesair drwy deipio llythrennau yn y blychau gwyn gweithredol. Mae'r rhifau'n cyfateb i'r cliwiau isod.



CLIWIAU AR DRAWS

2. Canllawiau strwythuredig fel NIST a ddefnyddir i reoli risgiau seiber (10)

4. Ymosodiad ar wendid sy'n cael ei dargedu cyn i'r gwerthwr ryddhau clwt (12)

7. Dilysiad diogelwch sy'n gofyn am ddau ddull dilysu neu fwy (10)

8. Arferion gorau ar gyfer rheoli manylion mewngofnodi ac allweddi dilysu (8)

CLIWIAU I LAWR

1. Cynllun strwythuredig ar gyfer delio â thoriadau diogelwch a'u lliniaru (6)

3. Maleiswedd sy'n amgryptio data ac yn mynnu taliad ariannol i'w ddadgryptio (10)

5. Rhwystr rhwydwaith sy'n hidlo traffig ar sail rheolau diogelwch (6)

6. System ffug a sefydlir i ddenu a dadansoddi actorion maleisus (6)

Pwynt Gwirio 5, dewis arall: Cliwiau Croesair Hygyrch

Gall defnyddwyr darllenwyr sgrin a bysellfwrdd deipio atebion y croesair yn uniongyrchol yn y meysydd testun isod.

CLIWIAU AR DRAWS

2 ar draws: Canllawiau strwythuredig fel NIST a ddefnyddir i reoli risgiau seiber (10 llythyren):

4 ar draws: Ymosodiad ar wendid sy'n cael ei dargedu cyn i'r gwerthwr ryddhau clwt (12 llythyren):

7 ar draws: Dilysiad diogelwch sy'n gofyn am ddau ddull dilysu neu fwy (10 llythyren):

8 ar draws: Arferion gorau ar gyfer rheoli manylion mewngofnodi ac allweddi dilysu (8 llythyren):

CLIWIAU I LAWR

1 i lawr: Cynllun strwythuredig ar gyfer delio â thoriadau diogelwch a'u lliniaru (6 llythyren):

3 i lawr: Maleiswedd sy'n amgryptio data ac yn mynnu taliad ariannol i'w ddadgryptio (10 llythyren):

5 i lawr: Rhwystr rhwydwaith sy'n hidlo traffig ar sail rheolau diogelwch (6 llythyren):

6 i lawr: System ffug a sefydlir i ddenu a dadansoddi actorion maleisus (6 llythyren):

Pwynt Gwirio 6: Chwilair Geiriau Cudd

Dewch o hyd i'r 8 term geirfa allweddol sydd wedi'u cuddio yn y grid isod. Gall geiriau fod yn llorweddol, yn fertigol neu'n groeslinol.

S Z L V C Z W F F K H Z D N D
Q X E P C U B F A Z H N D K A
D D M O D F H R I D Y R Q M E
D N T I R Z S A F Q L V F A A
E A O Q O N P M T X E Q K A R
W D P U S D N W Y B N F S M X
M L W J A R Z A Y Y D L G L I
O A M R J M L I T O I H Q F Q
S W H Z A O V T G U D B Y F R
N Y B H L Z G H J O P N W A C
A C A M F A N T E I S I O C M
R Z Y G Y O W U K V P B N T V
T M Y M A T E B G V D Y U O K
R B X Z Y M R Q X I P D A R D
J Q V W W L J H T H G B E I K

RHESTR GEIRIAU GEIRFA

RANSOMWEDD AMLFFACTOR CAMFANTEISIO POTMEL WALDAN YMATEB HYLENDID FFRAMWAITH

Pwynt Gwirio 6, dewis arall: Paru Geirfa Hygyrch

Parwch bob un o'r 8 term geirfa o'r Chwilair â'i ddiffiniad cywir drwy ysgrifennu'r llythyren (A-H) yn y bwlch.

TERMAU GEIRFA
A. RANSOMWEDD
B. AMLFFACTOR
C. CAMFANTEISIO
D. POTMEL
E. WALDAN
F. YMATEB
G. HYLENDID
H. FFRAMWAITH

	DIFFINIADAU A MEYSYDD PARU
	1. Rhwystr rhwydwaith sy'n hidlo traffig ar sail rheolau diogelwch.
	2. Cynllun strwythuredig ar gyfer delio â thoriadau diogelwch a'u lliniaru.
	3. Maleiswedd sy'n amgryptio data ac yn mynnu taliad ariannol i'w ddadgryptio.
	4. Dilysiad diogelwch sy'n gofyn am ddau ddull dilysu neu fwy.
	5. Arferion gorau ar gyfer rheoli manylion mewngofnodi ac allweddi dilysu.
	6. Canllawiau strwythuredig fel NIST a ddefnyddir i reoli risgiau seiber.
	7. Ymosodiad ar wendid sy'n cael ei dargedu cyn i'r gwerthwr ryddhau clwt.
	8. System ffug a sefydlir i ddenu a dadansoddi actorion maleisus.

Pwynt Gwirio 7: Her Geiriau Cymysg

Dad-sgramblwch y llythrennau isod i ddatgelu cysyniadau a thermau allweddol seiberddiogelwch. Ysgrifennwch eich atebion yn y blychau mewnbwn a ddarperir.

1. DWMOAREDSN
2. OAANCSIMEITF
3. WLDNAA
4. EIDDNHYL
5. TARMFCFAOL
6. EMPTLO
7. EYTBAM
8. TAWHFMFAIR

Gweithgaredd Bonws: Meddwl yn Gyflym

3 ATEB YM MHOB CATEGORI. Y PERSON CYNTAF I GWBLHAU'R RHESTR SY'N ENNILL.

1	Swyddi ym maes seiberddiogelwch			
2	Rhesymau dros ddiweddaru meddalwedd			
3	Pethau y gall wal dân eu rhwystro			
4	Arwyddion rhybudd mewn e-bost			
5	Pethau rydych chi'n gwneud copi wrth gefn ohonynt			
6	Mathau adnabyddus o seiberymosodiad			
7	Pethau y gall pot mêl (honeypot) eu denu			
8	Gwybodaeth na ddylech byth ei rhannu			
9	Arwyddion bod cyfrifiadur wedi'i heintio			
10	Ffilmiau neu raglenni am hacwyr			
11	Haenau diogelwch y gallwch eu hadeiladu			
12	Pethau i'w hymarfer mewn ymarfer diogelwch			
13	Offer diogelwch rydych chi'n eu hadnabod			
14	Pobl y gallwch ofyn iddynt am help TG			
15	Geiriau sy'n dechrau â 'seiber'			

Pwynt Gwirio 8: Astudiaethau Achos Seiberddiogelwch

Cymhwyswch y cysyniadau rydych wedi'u dysgu i ddatrys y senarios go iawn isod.

ASTUDIAETH ACHOS 1: STRATEGAETH ADFER AR ÔL MEDDALWEDD PRIDWERTH

👷

Senario: Mae rhwydwaith corfforaethol wedi'i heintio â nwyddau pridwerth, gan gloi cronfeydd data hanfodol. Mae'r ymosodwyr yn mynnu taliad o $100,000 mewn arian cyfred digidol. Mae gan y cwmni gopïau wrth gefn all-lein o 24 awr yn ôl.

Cwestiwn Trafod: Dadansoddwch risgiau talu, a gwerthuswch y strategaeth adfer.

ASTUDIAETH ACHOS 2: AMDDIFFYN RHAG STWFFIO MANYLION MEWNGOFNODI

👷

Senario: Mae gwasanaeth ar-lein yn profi ymosodiad stwffio manylion mewngofnodi, gyda hacwyr yn profi miliynau o barau enw defnyddiwr/cyfrinair a ddygwyd o wefannau eraill.

Cwestiwn Trafod: Disgrifiwch fecanwaith yr ymosodiad hwn yn fanwl, ac amlinellwch ddwy system amddiffyn.

Pwynt Gwirio 9: Dadgryptio'r Seiffr

Mae gweithiwr proffesiynol seiberddiogelwch yn diogelu asedau rhwydwaith rhag actorion bygythiad ar-lein. Defnyddiwch yr allwedd Llythyren-i-Rif isod i ddadgryptio'r neges drwy ysgrifennu'r llythrennau cyfatebol yn y bylchau gwag.

ALLWEDD AMGRYPTIO LLYTHRENNAU-I-RIFAU

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

4	9	15	7	5	12	23	3	8		5	9	3	8		19	25	19	20	5	13
			7	25	4	1		4	9	12	25	19	21		1	13	12			
							6	6	1	3	20	15	18							

Neges wedi'i datgodio:

AWGRYM: MAE POB RHIF YN CYNRYCHIOLI SAFLE'R LLYTHYREN HONNO YN YR WYDDOR (E.E. 1 = A, 2 = B, 26 = Z).

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am Seiberddiogelwch (Rhan A)

Adolygwch gwestiynau ac atebion cyffredin am liniaru bygythiadau ar-lein.

Q1: Beth yw prif amcan seiberddiogelwch?

Y prif nod yw diogelu rhwydweithiau, dyfeisiau a data rhag mynediad heb awdurdod, ymosodiadau a difrod damweiniol.

Q2: Sut mae gwe-rwydo'n wahanol i we-rwydo wedi'i dargedu (spear phishing)?

Ymgyrch e-bost eang sy'n targedu defnyddwyr ar hap yw gwe-rwydo, tra bod gwe-rwydo wedi'i dargedu (spear phishing) yn targedu unigolion penodol gan ddefnyddio data personol.

Q3: Beth yw wal dân rhwydwaith?

System diogelwch rhwydwaith yw wal dân sy'n monitro ac yn hidlo traffig sy'n dod i mewn ac yn mynd allan yn seiliedig ar reolau diogelwch a ddiffiniwyd ymlaen llaw.

Q4: Pam mae dilysu aml-ffactor (MFA) yn angenrheidiol?

Mae MFA yn ychwanegu haen hanfodol o amddiffyniad, gan atal mynediad hyd yn oed os bydd ymosodwyr yn dwyn neu'n cracio'r prif fanylion cyfrinair.

Q5: Beth sy'n diffinio feirws cyfrifiadurol?

Maleiswedd hunanddyblygol yw firws sy'n ei glymu ei hun wrth ffeiliau glân ac yn lledaenu ar draws systemau unwaith y caiff ei weithredu.

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am Seiberddiogelwch (Rhan B)

Adolygwch gwestiynau ac atebion cyffredin am liniaru bygythiadau ar-lein.

Q6: Sut mae meddalwedd wystlo yn cloi data lleol?

Mae meddalwedd wystlo yn defnyddio algorithmau cryptograffig i amgryptio ffeiliau defnyddwyr, gan eu gwneud yn annarllenadwy nes bod allwedd ddadgryptio'n cael ei chymhwyso.

Q7: Beth yw gwendid dim diwrnod (zero-day)?

Diffyg diogelwch mewn meddalwedd nad yw'r gwerthwr yn gwybod amdano yw zero-day, gan adael dim amser i ddatblygu clwt cyn iddo gael ei gamfanteisio.

Q8: Beth yw rôl fframwaith NIST?

Mae fframwaith NIST yn darparu canllawiau a safonau gwirfoddol i helpu sefydliadau i reoli a lleihau risgiau seiberddiogelwch.

Q9: Beth yw cynllun ymateb i ddigwyddiadau diogelwch?

Mae'n set o weithdrefnau wedi'u dogfennu ar gyfer canfod, cyfyngu ac adfer ar ôl achosion o dorri diogelwch a pheryglu rhwydwaith.

Q10: Sut mae peirianneg gymdeithasol yn manteisio ar ddefnyddwyr?

Mae peirianneg gymdeithasol yn defnyddio triniaeth seicolegol i dwyllo gweithwyr i ddatgelu cyfrineiriau neu lawrlwytho ffeiliau maleisus.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am Ddiogelwch (Rhan C)

Archwilio agweddau technegol uwch ar fframweithiau diogelwch, dadansoddi maleiswedd, a chydymffurfiaeth data.

Q1: Sut mae ymosodiad DDoS yn gorlethu gweinyddion gwe?

Mae ymosodiad DDoS yn cydlynu miliynau o ddyfeisiau botrwyd sydd wedi'u cyfaddawdu i foddi gweinydd â thraffig, gan ddihysbyddu terfynau lled band a CPU.

Q2: Beth yw'r gwahaniaeth rhwng amgryptio cymesur ac anghymesur?

Mae amgryptio cymesur yn defnyddio un allwedd ar gyfer amgryptio a dadgryptio, tra bo amgryptio anghymesur yn defnyddio pâr o allweddi cyhoeddus a phreifat.

Q3: Sut mae hacwyr yn cyflawni ymosodiadau chwistrellu SQL?

Mae ymosodwyr yn mewnbynnu gorchmynion SQL maleisus i feysydd ffurflenni, gan dwyllo'r gronfa ddata gefn i ryddhau cofnodion defnyddwyr heb awdurdod.

Q4: Beth yw symud ochrol mewn ymwthiadau rhwydwaith?

Dyma'r dechneg lle mae ymosodwyr yn manteisio ar fynediad cychwynnol i weinydd i beryglu systemau rhyng-gysylltiedig eraill ar y rhwydwaith mewnol.

Q5: Sut mae ffugio DNS yn ailgyfeirio traffig gwe?

Mae ffugio DNS yn newid cofnodion storfa gweinyddion enwau, gan lwybro defnyddwyr dilys i wefannau maleisus sy'n edrych yn debyg yn hytrach na'r parthau targed.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am Ddiogelwch (Rhan D)

Archwilio agweddau technegol uwch ar fframweithiau diogelwch, dadansoddi maleiswedd, a chydymffurfiaeth data.

Q6: Beth yw tocyn diogelwch caledwedd?

Mae'n ddyfais ffisegol (fel YubiKey) sy'n cynhyrchu proflenni dilysu cryptograffig, gan gynnig yr amddiffyniad mwyaf posibl rhag gwe-rwydo o bell.

Q7: Sut mae timau diogelwch yn defnyddio potiau mêl ffug?

Mae timau'n defnyddio gweinyddion abwyd nad ydynt yn rhai cynhyrchu i ganfod ymyriadau'n gynnar a dadansoddi patrymau ymosod actorion heb awdurdod.

Q8: Beth yw egwyddor y fraint leiaf?

Dyma'r safon ddiogelwch o gyfyngu hawliau mynediad defnyddwyr i'r lleiafswm absoliwt sydd ei angen i gyflawni eu rolau gwaith.

Q9: Sut mae ymosodiad Dyn-yn-y-Canol yn camfanteisio ar gysylltiadau?

Mae ymosodwr yn rhyng-gipio ac yn newid cyfathrebiadau rhwng dwy ddyfais ar rwydweithiau heb eu hamgryptio, gan ddwyn tocynnau sesiwn a manylion mewngofnodi.

Q10: Beth yw dangosyddion cyfaddawdu (IOCs)?

Cliwiau data fforensig yw IOCs, fel addasiadau anarferol i'r gofrestrfa neu draffig IP twyllodrus, sy'n dangos bod system wedi'i thorri.

Rhan 11: 10 Ffaith a Mewnwelediad Seiberddiogelwch o'r Byd Go Iawn

Adolygwch ffeithiau o'r byd go iawn am dor-diogelwch, mecanweithiau amddiffyn, a safonau cydymffurfio.

1. CIPOLWG AR DDIOGELWCH

Mae ymosodwyr yn sganio'r rhyngrwyd yn gyson am weinyddion agored i niwed ac yn anfon negeseuon e-bost gwe-rwydo i fewnflychau gweithwyr.

2. CIPOLWG AR DDIOGELWCH

Mae gwall dynol, fel clicio ar ddolenni gwe-rwydo, yn ffactor cyffredin mewn achosion o dorri data, a dyna pam mae hyfforddiant yn bwysig.

3. CIPOLWG AR DDIOGELWCH

Mae costau tor data yn cynnwys dirwyon cyfreithiol, colli cwsmeriaid, ymchwilio a thrwsio, a gallant gyrraedd miliynau o ddoleri.

4. CIPOLWG AR DDIOGELWCH

MFA sy'n gwrthsefyll gwe-rwydo, fel allweddi diogelwch caledwedd, yw'r math cryfaf o MFA a'r safon y mae CISA yn ei hannog. [2]

5. CIPOLWG AR DDIOGELWCH

Mae meddalwedd wystlo yn parhau i fod yn fygythiad mawr i rwydweithiau menter, ac mae CISA yn annog copïau wrth gefn all-lein wedi'u hamgryptio fel amddiffyniad allweddol. [4]

6. CIPOLWG AR DDIOGELWCH

Mae gan Fframwaith Seiberddiogelwch NIST 2.0 (2024) chwe swyddogaeth graidd: Llywodraethu, Nodi, Diogelu, Canfod, Ymateb, Adfer. [1]

7. MEWNWELEDIAD DIOGELWCH

Mae botiau stwffio manylion mewngofnodi yn profi parau enw defnyddiwr a chyfrinair a ddatgelwyd ar raddfa fawr yn erbyn pyrth mewngofnodi bancio ac e-fasnach.

8. MEWNWELEDIAD DIOGELWCH

Mae marchnadoedd campau diwrnod sero yn bodoli ledled y byd, lle gall gwendidau difrifol iawn werthu am symiau mawr cyn iddynt gael eu clytio.

9. MEWNWELEDIAD DIOGELWCH

Mae system abwyd pot mêl yn adrodd rhybuddion ymyrraeth ar unwaith gan nad oes gan ddefnyddwyr dilys unrhyw reswm i'w chyrchu.

10. CIPOLWG AR DDIOGELWCH

Mae Transport Layer Security (TLS) yn amgryptio sesiynau porwr, gan atal sniffian pecynnau ar rwydweithiau Wi-Fi cyhoeddus.

Cyfeiriadau a Ffynonellau Technegol

Mae'r canllaw astudio a'r posau rhyngweithiol wedi'u llunio o safonau byd-eang NIST, OWASP a chydymffurfio â phreifatrwydd data.

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Ymosodiadau Gwe-rwydo** GWE-RWYDO — **Ateb Cywir: A**

NODYN ADDYSGU

Mae ymgyrchoedd gwe-rwydo yn ceisio dwyn manylion mewngofnodi a data sensitif defnyddwyr gan ddefnyddio e-byst ffug. Ffynhonnell: OWASP Secure Configuration.

2 **Diogelu Cyfrif** ALLWEDD MFA — **Ateb Cywir: A**

NODYN ADDYSGU

Dilysu aml-ffactor (MFA) sy'n defnyddio tocynnau caledwedd sy'n darparu'r amddiffyniad cryfaf ar gyfer mynediad at gyfrifon. Ffynhonnell: NIST Digital Identity.

3 **Bygythiad Meddalwedd Wystlo** MEDDALWEDD WYSTLO — **Ateb Cywir: A**

NODYN ADDYSGU

Mae meddalwedd wystlo yn amgryptio systemau a data hanfodol, gan fynnu taliad mewn arian cyfred digidol am allweddi dadgryptio. Dyfyniad: Center for Internet Security (CIS).

4 **Gwendid Diwrnod Sero** DIWRNOD SERO — **Ateb Cywir: A**

NODYN ADDYSGU

Mae bygythiadau diwrnod sero yn manteisio ar wendidau diogelwch anhysbys heb eu clytio cyn bod clwt gan y gwerthwr ar gael. Ffynhonnell: OWASP Secure Configuration.

5 **Fframweithiau Diogelwch** FFRAMWAITHIAU — **Ateb Cywir: A**

NODYN ADDYSGU

Mae fframweithiau fel NIST yn darparu canllawiau strwythuredig i helpu sefydliadau i reoli a lleihau risgiau seiber. Ffynhonnell: NIST Digital Identity.

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Gwe-rwydo wedi'i Dargedu** GWE-RWYDO — **Ateb Cywir: Gau**

NODYN ADDYSGU

Mae ymosodiadau gwe-rwydo yn targedu rhwydweithiau corfforaethol a chyfrifon personol i ehangu fectorau ymosod. Ffynhonnell: OWASP Secure Configuration.

7 **Cwestiwn 7** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae MFA yn gofyn am ail ffactor, felly fel arfer nid yw cyfrinair wedi'i ddwyn ar ei ben ei hun yn ddigon i fewngofnodi.

8 **Wal Dân Traffig** WAL DÂN — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae waliau tân yn archwilio ac yn rhwystro traffig ar byrth rhwydwaith penodol i hidlo cysylltiadau heb awdurdod. Ffynhonnell: Center for Internet Security (CIS).

9 **Ymateb Diwrnod Sero** DIWRNOD SERO — **Ateb Cywir: Gau**

NODYN ADDYSGU

Mae unioni diffygion dim-diwrnod yn gofyn am glytiau cod a hidlo WAF gan nad oes llofnodion yn bodoli eto. Ffynhonnell: OWASP Secure Configuration.

10 **Potiau Mêl Abwyd** POT MÊL — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gweinyddion twyllodrus yw potiau mêl (honeypots) a ddefnyddir gan dimau diogelwch i ddenu actorion maleisus, rhybuddio amdanynt, a'u hastudio. Ffynhonnell: Center for Internet Security (CIS).

Allweddi Geirfa a Chyfarwyddyd Marcio

Cyfarwyddyd Marcio i Athrawon: Rhowch 1 pwynt am bob paru cywir (8 pwynt i gyd) a phob term cyd-destun (6 phwynt i gyd).

PWYNT GWIRIO 4: ALLWEDD PARU CYSYNIADAU

D 1. Bygythiad Nwyddau Pridwerth	G 2. Dilysu Aml-Ffactor	E 3. Camfanteisio Dim Diwrnod	H 4. Pot Mêl Abwyd
C 5. Wal Dân Ymwthiadau	B 6. Ymateb i Ddigwyddiadau	F 7. Hylendid Cyfrineiriau	A 8. Fframwaith Diogelwch

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 WAL DÂN	2 CAMFANTEISIO	3 GWE-RWYDO	4 MALEISWEDD
5 HYLENDID	6 AMGRYPTIO		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 E – WALDAN	2 F – YMATEB	3 A – RANSOMWEDD	4 B – AMLFFACTOR
5 G – HYLENDID	6 H – FFRAMWAITH	7 C – CAMFANTEISIO	8 D – POTMEL

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio Bygythiad Nwyddau Pridwerth, Dilysu Aml-Ffactor a Camfanteisio Dim Diwrnod yn eu geiriau eu hunain a rhoi enghraifft o bob un.

Astudiaethau Achos:
Gofynnwch i fyfyrwyr gefnogi eu hargymhellion â ffeithiau o'r daflen waith yn hytrach na thybiaethau.

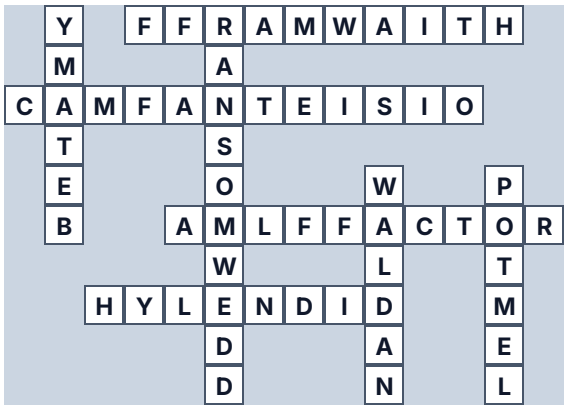
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

S	Z	L	V	C	Z	W	F	F	K	H	Z	D	N	D
Q	X	E	P	C	U	B	F	A	Z	H	N	D	K	A
D	D	M	O	D	F	H	R	I	D	Y	R	Q	M	E
D	N	T	I	R	Z	S	A	F	Q	L	V	F	A	A
E	A	O	Q	O	N	P	M	T	X	E	Q	K	A	R
W	D	P	U	S	D	N	W	Y	B	N	F	S	M	X
M	L	W	J	A	R	Z	A	Y	Y	D	L	G	L	I
O	A	M	R	J	M	L	I	T	O	I	H	Q	F	Q
S	W	H	Z	A	O	V	T	G	U	D	B	Y	F	R
N	Y	B	H	L	Z	G	H	J	O	P	N	W	A	C
A	C	A	M	F	A	N	T	E	I	S	I	O	C	M
R	Z	Y	G	Y	O	W	U	K	V	P	B	N	T	V
T	M	Y	M	A	T	E	B	G	V	D	Y	U	O	K
R	B	X	Z	Y	M	R	Q	X	I	P	D	A	R	D
J	Q	V	W	W	L	J	H	T	H	G	B	E	I	K

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

2 ar draws: FFRAMWAITH Canllawiau strwythuredig fel NIST a ddefnyddir i reoli risgiau seiber (10 llythyren)

4 ar draws: CAMFANTEISIO Ymosodiad ar wendid sy'n cael ei dargedu cyn i'r gwerthwr ryddhau clwt (12 llythyren)

7 ar draws: AMLFFACTOR Dilysiad diogelwch sy'n gofyn am ddau ddull dilysu neu fwy (10 llythyren)

8 ar draws: HYLENDID Arferion gorau ar gyfer rheoli manylion mewngofnodi ac allweddi dilysu (8 llythyren)

CLIWIAU I LAWR

1 i lawr: YMATEB Cynllun strwythuredig ar gyfer delio â thoriadau diogelwch a'u lliniaru (6 llythyren)

3 i lawr: RANSOMWEDD Maleiswedd sy'n amgryptio data ac yn mynnu taliad ariannol i'w ddadgryptio (10 llythyren)

5 i lawr: WALDAN Rhwystr rhwydwaith sy'n hidlo traffig ar sail rheolau diogelwch (6 llythyren)

6 i lawr: POTMEL System ffug a sefydlir i ddenu a dadansoddi actorion maleisus (6 llythyren)

Allwedd Datrys Geiriau Cymysg a Seiffr

Allwedd marcio ar gyfer y gweithgaredd dad-sgramblo geirfa a'r Her Seiffr Gyfrinachol.

ALLWEDD DATRYS GEIRIAU CYMYSG

1.	D W M O A R E D S N	RANSOMWEDD	5.	T A R M F C F A O L	AMLFFACTOR
2.	O A A N C S I M E I T F	CAMFANTEISIO	6.	E M P T L O	POTMEL
3.	W L D N A A	WALDAN	7.	E Y T B A M	YMATEB
4.	E I D D N H Y L	HYLENDID	8.	T A W H F M F A I R	FFRAMWAITH

ALLWEDD HER Y SEIFFR CYFRINACHOL

"DIOGELWCH EICH SYSTEM GYDA DILYSU AML FFACTOR"

Allwedd Atebion yr Astudiaethau Achos

A Astudiaeth Achos 1: Strategaeth Adfer ar ôl Meddalwedd Pridwerth

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae rhwydwaith corfforaethol wedi'i heintio â nwyddau pridwerth, sy'n cloi cronfeydd data hanfodol. Mae'r ymosodwyr yn mynnu taliad o $100,000 mewn arian cripto. Mae gan y cwmni gopïau wrth gefn all-lein o 24 awr yn ôl.
- Strategaeth ac Ateb a Argymhellir: Risgiau Talu: Nid yw talu'n gwarantu dadgryptio ffeiliau, mae'n labelu'r cwmni fel targed sy'n talu, ac mae'n ariannu gweithgarwch troseddol. Strategaeth Adfer: Dylai'r tîm ynysu'r gwesteiwyr sydd wedi'u heintio, sychu'r gweinyddion sydd wedi'u cyfaddawdu, ac adfer data o gopïau wrth gefn all-lein. Rhaid iddynt glytio'r fector mynediad cychwynnol (gwe-rwydo neu gamfanteisio) i atal ailheintio ar unwaith.

B Astudiaeth Achos 2: Amddiffyn rhag Stwffio Manylion Mewngofnodi

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae gwasanaeth ar-lein yn profi ymosodiad stwffio manylion mewngofnodi, gyda hacwyr yn profi miliynau o barau enw defnyddiwr/cyfrinair a ddygwyd o wefannau eraill.
- Strategaeth ac Ateb a Argymhellir: Mecanwaith: Mae ymosodwyr yn manteisio ar ailddefnyddio cyfrineiriau ar draws gwefannau, gan ddefnyddio botiau awtomataidd i fewngofnodi i gyfrifon defnyddwyr. Amddiffynfeydd: 1. Mae dilysu aml-ffactor (MFA) yn rhwystro ymdrechion mewngofnodi hyd yn oed os yw'r cyfrinair yn gywir. 2. Mae gweithredu cyfyngu cyfradd a CAPTCHAs yn rhwystro traffig botiau awtomataidd rhag sbamio pwyntiau terfyn mewngofnodi.