Enw: _____ **Dyddiad:** _____ **Sgôr:** _____

Meddalwedd Gwrthfeirws a Dyfeisiau Terfyn Canllaw Diogelu

Canfod llofnodion, hewristeg, monitro ymddygiad, blwch tywod, diweddariadau

TROSOLWG DYSGU MEDDALWEDD GWRTHFEIRWS

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 feddalwedd gwrthfeirws a diogelu pwyntiau terfyn. Byddwch yn archwilio cronfeydd data llofnodion, sganwyr hewristig, monitro ymddygiad, ffeiliau rhithwir mewn blwch tywod a lliniaru canlyniadau positif ffug.

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/gwrthfeirws/

Eich Map Llwybr Dysgu Strategaeth Gwrthfeirws

- Gwahaniaethwch rhwng canfod maleiswedd sy'n seiliedig ar lofnodion a chanfod sy'n seiliedig ar hewristeg.
- Deall protocolau monitro ymddygiad ac ynysu mewn blwch tywod.
- Gwerthuso effeithiau sganio amser real ar berfformiad systemau a dyfeisiau terfynol.
- Lliniaru dosbarthiadau positif ffug gan ddefnyddio dilysu tystysgrifau digidol.
- Rheoli dosbarthiad diweddariadau diffiniadau dyddiol ar draws pwyntiau terfyn corfforaethol.

CYFARWYDDIADAU CANLLAW GWRTHFEIRWS

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 ddiogelwch gwrthfeirws ar ddyfeisiau terfyn. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

DIOGELWCH GWRTHFEIRWS A SGANIO LLOFNODION (CYFLWYNIAD)

Mae meddalwedd gwrthfeirws yn diogelu dyfeisiau terfyn drwy adnabod, cwarantinio a chael gwared ar faleiswedd. Mae systemau modern yn cyfuno cronfeydd data llofnodion (sy'n paru hashes bygythiadau hysbys) â hewristeg (dadansoddi strwythur ffeiliau) a monitro ymddygiad i ganfod campau dim-diwrnod.

DARLLENWCH BOB PWYNT GWIRIO YN OFALUS A DEWISWCH NEU YSGRIFENNWCH YR

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw un o gyfyngiadau canfod ar sail llofnodion?**
   - A. Ni all adnabod maleiswedd anhysbys neu wedi'i haddasu
   - B. Mae'n cynhyrchu cyfraddau uchel o bositifau ffug
   - C. Mae angen pŵer prosesu CPU uchel arno
   - D. Dim ond pan fydd wedi'i gysylltu â'r rhyngrwyd y mae'n gweithio

2. **2. Sut mae sganwyr hewristig yn canfod amrywiolion maleiswedd newydd?**
   - A. Drwy nodi patrymau a strwythurau cod amheus
   - B. Drwy baru hashes ffeiliau â chronfa ddata o fygythiadau
   - C. Drwy ddileu pob ffeil weithredadwy heb ei llofnodi yn awtomatig
   - D. Drwy lanlwytho pob ffeil i ffolder cwmwl cyhoeddus

3. **3. Beth yw diben gweithredu mewn blwch tywod gwrthfeirws?**
   - A. Ynysu a dadansoddi ffeiliau mewn cladgell rithwir ddiogel
   - B. Cyflymu trosglwyddiad copi wrth gefn y system ffeiliau leol
   - C. Diweddaru clytiau diogelwch y system weithredu leol
   - D. Cywasgu ffeiliau dogfen mawr i arbed storfa

4. **4. Pa ddull canfod sy'n tynnu sylw at ymddygiad bygythiadau mewn amser real?**
   - A. Dadansoddi ymddygiad sy'n monitro gweithredoedd meddalwedd
   - B. Archwilio logiau hanesyddol dros nos
   - C. Ymyriad llaw gan ddefnyddwyr yn adrodd am apiau araf
   - D. Adolygiadau llaw wythnosol o raglenni sydd wedi'u gosod

5. **5. Pam mae diweddariadau diffiniadau rheolaidd yn hanfodol i sganwyr?**
   - A. I fwydo dynodwyr bygythiadau i gronfa ddata peiriannau llofnodion
   - B. Cynyddu cyflymder cloc y CPU yn ystod gweithrediadau
   - C. Er mwyn addasu amseroedd storio gweinyddion enwau DNS byd-eang mewn celc
   - D. Er mwyn awdurdodi gosodiadau cwcis y porwr gwe

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn Gwir/Gau 6

6. Mae canfod llofnodion yn paru stwnshiadau ffeiliau cryptograffig â rhestrau cronfa ddata.

○ Gwir ○ Gau

7 Cwestiwn Gwir/Gau 7

7. Gall sganwyr hewristig sbarduno rhybuddion positif ffug ar ffeiliau diogel.

○ Gwir ○ Gau

8 Cwestiwn Gwir/Gau 8

8. Mae blwch tywod yn caniatáu i faleiswedd gyrchu ffeiliau rhwydwaith heb derfynau.

○ Gwir ○ Gau

9 Cwestiwn Gwir/Gau 9

9. Mae sganio ymddygiadol yn rhwystro ffeiliau pan fyddant yn dangos gweithredoedd maleisus.

○ Gwir ○ Gau

10 Cwestiwn Gwir/Gau 10

10. Mae meddalwedd gwrthfeirws safonol yn atal pob ymosodiad dim diwrnod yn llwyr.

○ 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 sganiwr traddodiadol yn dibynnu ar baru _____ i adnabod maleiswedd hysbys.

2. Yr enw ar ddadansoddi patrymau cod ffeiliau yw sganio ar sail _____ .

3. Mae offer gwrthfeirws yn ynysu ffeiliau amheus mewn amgylchedd _____ .

4. Mae monitro amser real yn gwylio _____ rhaglenni am weithgarwch amheus.

5. Mae sganwyr yn lawrlwytho _____ i'r gronfa ddata bob dydd i adnabod bygythiadau newydd.

6. Mae rhaglenni diogel sy'n cael eu nodi fel maleiswedd yn sbarduno rhybuddion positif _____ .

BANC GEIRIAU GEIRFA

BLWCH TYWOD DIWEDDARIADAU FFUG HEURISTEG LLOFNODION OFFERYN GWRTHFEIRWS YMDDYGIAD YNYSU

Ysgrifennwch eich atebion yma:

1. **2.**

3. **4.**

5. **6.**

Pwynt Gwirio 4: Paru Cysyniadau Diogelwch

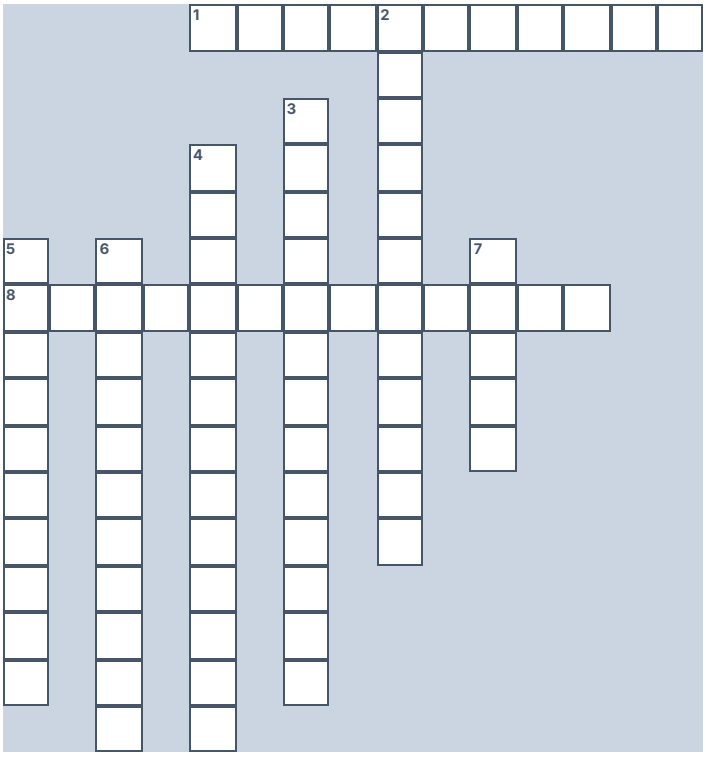
PARU DIFFINIADAU

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. Llofnod Hash	A	Cyfyngu ffeiliau amheus i atal datgelu'r system leol.
	2. Heuristeg Cod	B	Cyfres feddalwedd sy'n sganio ac yn diogelu pwyntiau terfyn rhag campau.
	3. Blwch Tywod Ffeiliau	C	Monitro gweithredoedd meddalwedd sy'n rhedeg am batrymau gweithredu maleisus.
	4. Sgan Ymddygiad	D	Ôl troed cronfa ddata cryptograffig unigryw a ddefnyddir i adnabod bygythiadau hysbys.
	5. Diweddariadau Dyddiol	E	Amgylchedd prawf rhithwir diogel sy'n rhedeg cod nad oes modd ymddiried ynddo'n ddiogel.
	6. Positif Ffug	F	Lawrlwythiadau diffiniadau rheolaidd sy'n bwydo'r gronfa ddata bygythiadau.
	7. Ynysu Bygythiadau	G	Dadansoddiad ar sail rheolau sy'n nodi ffeiliau â chynlluniau cod amheus.
	8. Offeryn Gwrthfeirws	H	Rhybudd diogelwch sy'n dosbarthu meddalwedd ddiogel yn anghywir fel maleiswedd.

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

1. Cyfres feddalwedd sy'n sganio ac yn diogelu dyfeisiau terfynol rhag campau manteisio (11)

8. Ôl troed cryptograffig unigryw mewn cronfa ddata a ddefnyddir i adnabod bygythiadau hysbys (13)

CLIWIAU I LAWR

2. Dadansoddiad ar sail rheolau sy'n tynnu sylw at ffeiliau â chynllun cod amheus (12)

3. Lawrlwythiadau diffiniadau rheolaidd sy'n bwydo'r gronfa ddata bygythiadau (13)

4. Monitro gweithredoedd meddalwedd sy'n rhedeg am batrymau gweithredu maleisus (13)

5. Amgylchedd prawf rhithwir diogel sy'n rhedeg cod nad oes modd ymddiried ynddo yn ddiogel (10)

6. Rhybudd diogelwch sy'n dosbarthu meddalwedd ddiogel fel maleiswedd ar gam (11)

7. Cyfyngu ffeiliau amheus er mwyn atal amlygu'r system leol (5)

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 CLIWIAU I LAWR

CLIWIAU AR DRAWS

1 ar draws: Cyfres feddalwedd sy'n sganio ac yn diogelu dyfeisiau terfynol rhag campau manteisio (11 llythyren):

8 ar draws: Ôl troed cryptograffig unigryw mewn cronfa ddata a ddefnyddir i adnabod bygythiadau hysbys (13 llythyren):

CLIWIAU I LAWR

2 i lawr: Dadansoddiad ar sail rheolau sy'n tynnu sylw at ffeiliau â chynllun cod amheus (12 llythyren):

3 i lawr: Lawrlwythiadau diffiniadau rheolaidd sy'n bwydo'r gronfa ddata bygythiadau (13 llythyren):

4 i lawr: Monitro gweithredoedd meddalwedd sy'n rhedeg am batrymau gweithredu maleisus (13 llythyren):

5 i lawr: Amgylchedd prawf rhithwir diogel sy'n rhedeg cod nad oes modd ymddiried ynddo yn ddiogel (10 llythyren):

6 i lawr: Rhybudd diogelwch sy'n dosbarthu meddalwedd ddiogel fel maleiswedd ar gam (11 llythyren):

7 i lawr: Cyfyngu ffeiliau amheus er mwyn atal amlygu'r system leol (5 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.

D I W E D D A R I A D A U U K

A G U F F F I T I S O P R Y B

I X Z Y M R Q X I P D A N D J

G Q V W W L J H T H G Y B E I

Y K T S V R Z E H E S S C A L

D Q C Z M K V R U U A S W J M

D M H H N H R F K T L R W H B

M U F Y D O W Y T H C W L B O

Y Y W S H T X A P U N N Z O I

N S W R I E F H T R W G Q T I

A L L O F N O D S T W N S H P

G V U O U U K A E P M K A N V

S G H E U R I S T E G C O D G

P Q X Y J K V J Y W Y P J I Z

I J N A E I A S A J F W E K Z

RHESTR GEIRIAU GEIRFA

LLOFNODSTWNSH HEURISTEGCOD BLWCHTYWOD SGANYMDDYGIAD

DIWEDDARIADAU POSITIFFFUG YNYSU GWRTHFEIRWS

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. LLOFNODSTWNSH

B. HEURISTEGCOD

C. BLWCHTYWOD

D. SGANYMDDYGIAD

E. DIWEDDARIADAU

F. POSITIFFFUG

G. YNYSU

H. GWRTHFEIRWS

DIFFINIADAU A MEYSYDD PARU

1. Monitro gweithredoedd meddalwedd sy'n rhedeg am batrymau gweithredu maleisus.

2. Cyfres feddalwedd sy'n sganio ac yn diogelu dyfeisiau terfynol rhag campau manteisio.

3. Lawrlwythiadau diffiniadau rheolaidd sy'n bwydo'r gronfa ddata bygythiadau.

4. Dadansoddiad ar sail rheolau sy'n tynnu sylw at ffeiliau â chynllun cod amheus.

5. Cyfyngu ffeiliau amheus er mwyn atal amlygu'r system leol.

6. Ôl troed cryptograffig unigryw mewn cronfa ddata a ddefnyddir i adnabod bygythiadau hysbys.

7. Amgylchedd prawf rhithwir diogel sy'n rhedeg cod nad oes modd ymddiried ynddo yn ddiogel.

8. Rhybudd diogelwch sy'n dosbarthu meddalwedd ddiogel fel maleiswedd ar gam.

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. DOTSOLSWLNHNF
2. OCBLHDYWTW
3. IDRAIAUWADDDE
4. YUSYN
5. ECETDUIGSHOR
6. YGDMIAAYSGDDN
7. FTPOFGFUSII
8. RESFRGHWWIT

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Rhesymau dros ddiweddaru meddalwedd			
2	Pobl y gallwch ofyn iddynt am help TG			
3	Pethau i'w gwneud pan fydd gwrthfeirws yn canfod rhywbeth			
4	Arwyddion o feirws cyfrifiadurol			
5	Pethau sy'n cael eu rhoi mewn cwarantin			
6	Mannau lle mae feirysau'n cuddio			
7	Gwybodaeth na ddylech byth ei rhannu			
8	Mathau o feddalwedd faleisus			
9	Offer diogelwch rydych chi'n eu hadnabod			
10	Pethau y mae gwrthfeirws yn eu sganio			
11	Pethau rydych chi'n gwneud copi wrth gefn ohonynt			
12	Dyfeisiau y gellir eu hacio			
13	Rhaglenni gwrthfeirws rydych chi'n eu hadnabod			
14	Rhesymau dros rybuddion ffug			
15	Arferion diogel y gallwch eu dechrau heddiw			

Pwynt Gwirio 8: Astudiaethau Achos Seiberddiogelwch

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

ASTUDIAETH ACHOS 1: SGANIO AR SAIL LLOFNOD NEU SGANIO HEWRISTIG



Senario: Mae gweithiwr yn lawrlwytho cyfleuster pwrpasol a adeiladwyd yn fewnol gan dîm arall. Mae'r sganiwr llofnodion yn ei basio, ond mae'r sganiwr hewristig yn ei nodi'n amheus.

Cwestiwn Trafod: Esboniwch pam y digwyddodd hyn, a sut i wirio a yw'r ffeil yn ddiogel.

ASTUDIAETH ACHOS 2: YMDRIN Â POSITIFAU FFUG



Senario: Mae datblygwr meddalwedd yn crynhoi ei raglen. Mae gwrthfeirws y system yn nodi'r ffeil weithredadwy newydd fel maleiswedd ac yn ei rhoi mewn cwarantin.

Cwestiwn Trafod: Amlinellwch risgiau rhestru gwyn, a disgrifiwch y llwybr datrys cywir.

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

3	1	14	6	15	4		13	1	12	5	9	19	23	5	4	4

14	5	23	25	4	4		7	25	4	1		8	5	21	18	9	19	20	5	7

3	15	4

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: Sut mae meddalwedd gwrthfeirws yn adnabod maleiswedd?

Mae'n adnabod maleiswedd drwy baru llofnodion cronfa ddata, dadansoddi strwythur cod yn hewristig, a monitro ymddygiad mewn amser real.

Q2: Beth yw canfod ar sail llofnodion?

Mae'n ddull sganio sy'n paru stwnshiau ffeiliau cryptograffig â rhestrau cronfa ddata o fygythiadau maleiswedd hysbys.

Q3: Beth yw sganiwr hewristig?

Mae hewristeg yn dadansoddi strwythur a chyfarwyddiadau cod ffeil, gan nodi patrymau amheus sy'n gyffredin i amrywiolion maleiswedd.

Q4: Beth mae'n ei olygu pan fydd ffeil wedi'i rhoi mewn cwarantin?

Mae'r gwrthfeirws yn symud y ffeil i ffolder diogel ar wahân, gan rwystro ei gweithredu er mwyn diogelu'r system weithredu.

Q5: Beth yw positif ffug gwrthfeirws?

Mae'n wall lle mae meddalwedd ddilys a diogel yn cael ei nodi'n anghywir fel maleiswedd gan algorithmau sganio.

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

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

Q6: Sut mae monitro ymddygiad yn diogelu systemau?

Mae'n monitro meddalwedd sy'n rhedeg mewn amser real, gan rwystro prosesau sy'n ceisio gwneud newidiadau amheus fel chwistrellu cod.

Q7: Pam mae profi mewn blwch tywod yn bwysig?

Mae blychau tywod yn rhedeg ffeiliau nad ymddiriedir ynddynt mewn peiriant rhithwir ynysig, gan arsylwi ar weithredoedd yn ddiogel heb amlygu'r system.

Q8: Pa mor aml y dylai diffiniadau gwrthfeirws ddiweddaru?

Dylai sganwyr ddiweddaru diffiniadau bob dydd neu bob awr i adnabod mathau o faleiswedd sydd newydd eu darganfod.

Q9: Beth yw'r gwahaniaeth rhwng gwrthfeirws ac EDR?

Mae gwrthfeirws yn canolbwyntio ar sganio ffeiliau, tra bo Endpoint Detection and Response (EDR) yn darparu olrhain a chyfyngu bygythiadau ar draws y rhwydwaith cyfan.

Q10: A allaf redeg dwy raglen wrthfeirws gyda'i gilydd?

Na. Mae rhedeg dau sganiwr gweithredol yn achosi gwrthdaro yn y system, yn arafu perfformiad, a gallant rwystro gweithrediadau ei gilydd.

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 rheolau hewristig yn lleihau'r bygythiadau sy'n llwyddo i osgoi'r amddiffynfeydd?

Mae hewristeg yn dadansoddi patrymau bygythiadau cyffredinol yn hytrach na llofnodion penodol, gan ddal amrywiolion wedi'u haddasu o deuluoedd maleiswedd hysbys.

Q2: Beth yw feirws amlffurf?

Maleiswedd yw hon sy'n newid strwythur ei ffeil a'i threfn ddadgryptio bob tro y caiff ei gweithredu, gan wneud sganiau llofnod yn aneffeithiol.

Q3: Sut mae blychau tywod yn canfod osgoi peiriannau rhithwir?

Mae blychau tywod modern yn efelychu cliciau llygoden ac amser rhedeg y system, gan dwyllo maleiswedd a gynlluniwyd i guddio wrth redeg mewn peiriannau rhithwir.

Q4: Beth yw fformatau llwytho i lawr diweddariadau llofnodion?

Fel arfer mae diweddariadau'n ffeiliau gwahaniaeth deuaidd cynyddrannol ysgafn, gan leihau'r defnydd o led band rhwydwaith y cleient.

Q5: Sut mae asiantau pwyntiau terfyn yn rheoli sganiau lleol?

Mae asiantau'n cynnal gwiriadau cefndir ysgafn, gan drosglwyddo chwiliadau stwnsh cryptograffig dwfn i gronfeydd data bygythiadau yn y cwmwl.

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 sganio i ganfod rootkits?

Mae'n sganio tablau cof ar lefel y cnewyllyn, gan osgoi'r APIs system weithredu y mae rootkits yn ymglymu wrthynt i guddio eu hedafedd gweithredol.

Q7: Sut mae sganio ymddygiad yn rhwystro meddalwedd wystlo?

Mae'n canfod dolenni amgryptio ffeiliau torfol awtomataidd, gan derfynu proses y gwesteiwr cyn i gronfeydd data'r system gael eu cloi.

Q8: Beth yw gwirio tystysgrifau llofnodi cod?

Mae sganwyr yn gwirio llofnodion digidol cod yn erbyn awdurdodau tystysgrifau gwraidd dibynadwy, gan ddilysu hunaniaeth datblygwr y feddalwedd.

Q9: Sut mae pacwyr (packers) yn effeithio ar beiriannau sganio?

Mae pacwyr yn cywasgu neu'n amgryptio llwythi maleiswedd. Rhaid i sganwyr ddadbacio'r ffeil yn y cof cyn i wiriadau llofnod redeg.

Q10: Sut mae offer EDR yn awtomeiddio ynysu?

Mae asiantau EDR yn rhoi pwyntiau terfyn sydd wedi'u peryglu mewn cwarantin ar lefel y rhwydwaith, gan rwystro symudiad ochrol tra'n caniatáu mynediad i ddadansoddwyr.

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 cronfeydd data llofnodion yn storio stwnshiadau maleiswedd hysbys, felly caiff ffeiliau cwbl newydd neu wedi'u newid eu methu nes bod diffiniadau'n diweddaru.

2. CIPOLWG AR DDIOGELWCH

Gall peiriannau hewristig nodi rhai amrywiolion maleiswedd newydd cyn bod llofnodion yn bodoli, ar draul mwy o bethau positif ffug.

3. CIPOLWG AR DDIOGELWCH

Mae rhybuddion positif ffug yn costio amser i dimau TG wrth ddilysu ac adfer ffeiliau a roddwyd mewn cwarantin ar gam.

4. CIPOLWG AR DDIOGELWCH

Mae maleiswedd amlffurf yn newid ei god gyda phob copi, felly mae amddiffynwyr yn cyfuno llofnodion â gwiriadau hewristig ac ymddygiad.

6. CIPOLWG AR DDIOGELWCH

Mae awduron maleiswedd yn ysgrifennu cod pwrpasol sydd wedi'i gynllunio i wirio amgylcheddau blwch tywod, gan oedi gweithredu i osgoi amseryddion.

5. CIPOLWG AR DDIOGELWCH

Mae peiriannau gwrthfeirws yn y cwmwl yn gwirio stwnsh ffeiliau amheus yn erbyn cronfeydd data bygythiadau ar-lein mawr bron mewn amser real.

7. MEWNWELEDIAD DIOGELWCH

Mae gwerthwyr yn gwthio diweddariadau diffiniadau i bwyntiau terfyn yn rheolaidd fel bod sganwyr yn gallu adnabod bygythiadau sydd newydd eu cadarnhau.

8. MEWNWELEDIAD DIOGELWCH

Mae monitorau ymddygiad meddalwedd wystlo yn targedu galwadau API Win32 penodol sy'n gysylltiedig ag amgryptio ffeiliau a dileu copïau cysgodol.

9. MEWNWELEDIAD DIOGELWCH

Gall llofnodion cod dilys leihau'r risg o bositif ffug, ond caiff ffeiliau wedi'u llofnodi eu sganio o hyd, gan y gellir llofnodi maleiswedd hefyd.

10. CIPOLWG AR DDIOGELWCH

Mae rootkits yn addasu strwythurau cnewyllyn y system, gan ei gwneud yn ofynnol defnyddio sganwyr amser cychwyn arbenigol i'w canfod a'u glanhau.

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 DIWYDIANNOL

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

https://csrc.nist.gov/pubs/sp/800/83/r1/final

[2] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[3] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] 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

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Cwestiwn 1** LLOFNODION **Ateb Cywir: A**

NODYN ADDYSGU

Mae sganio llofnodion yn dibynnu ar stwnsh cronfa ddata hysbys, gan fethu canfod maleiswedd anhysbys neu wedi'i haddasu. Ffynhonnell: OWASP Secure Configuration.

2 **Cwestiwn 2** HEWRISTEG **Ateb Cywir: A**

NODYN ADDYSGU

Mae hewristeg yn dadansoddi cynllun cod a gorchmynion i nodi nodweddion amheus amrywiadau bygythiadau newydd. Ffynhonnell: Center for Internet Security (CIS).

3 **Cwestiwn 3** BLYCHA TYWOD **Ateb Cywir: A**

NODYN ADDYSGU

Mae blwch tywod yn rhedeg ffeiliau amheus mewn peiriant rhithwir ynysig i arsylwi ar eu hymddygiad gweithredu yn ddiogel. Ffynhonnell: NIST Digital Identity.

4 **Cwestiwn 4** YMDDYGIADOL **Ateb Cywir: A**

NODYN ADDYSGU

Mae sganio ymddygiad yn monitro rhaglenni sy'n rhedeg mewn amser real i rwystro newidiadau anawdurdodedig i'r system. Ffynhonnell: Center for Internet Security (CIS).

5 **Cwestiwn 5** DIWEDDARIADAU **Ateb Cywir: A**

NODYN ADDYSGU

Mae sganwyr yn lawrlwytho diweddariadau diffiniadau cynyddrannol dyddiol i aros yn gydamserol â thirweddau bygythiadau. Ffynhonnell: OWASP Secure Configuration.

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Cwestiwn 6** LLOFNODION **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae offer llofnodion yn cyfrifo stwnsh cryptograffig ac yn eu cyfateb yn erbyn cronfa ddata o stwnsh bygythiadau hysbys. Ffynhonnell: OWASP Secure Configuration.

7 **Cwestiwn 7** HEWRISTEG **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae peiriannau hewristig yn rhedeg cynlluniau ar sail rheolau a all nodi ffeiliau dilys, diogel fel rhai amheus. Ffynhonnell: Center for Internet Security (CIS).

8 **Cwestiwn 8** BLYCHA TYWOD **Ateb Cywir: Gau**

NODYN ADDYSGU

Mae blwch tywod yn rhedeg cod mewn cynhwysydd rhithwir, gan rwystro mynediad at gyfrannau rhwydwaith yn llym. Ffynhonnell: NIST Digital Identity.

9 **Cwestiwn 9** YMDDYGIADOL **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae monitro amser real yn nodi prosesau rhedeg sy'n ceisio ysgrifennu'n anghyfreithlon neu gloi ffeiliau. Ffynhonnell: Center for Internet Security (CIS).

10 **Cwestiwn 10** **Ateb Cywir: Gau**

NODYN ADDYSGU

Nid oes unrhyw wrthfeirws yn atal pob ymosodiad dim diwrnod; gall bygythiadau anhysbys osgoi llofnodion a dulliau hewristig.

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. Llofnod Hash	G 2. Heuristeg Cod	E 3. Blwch Tywod Ffeiliau	C 4. Sgan Ymddygiad
F 5. Diweddariadau Dyddiol	H 6. Positif Ffug	A 7. Ynysu Bygythiadau	B 8. Offeryn Gwrthfeirws

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 LLOFNODION	2 HEURISTEG	3 BLWCH TYWOD	4 YMDDYGIAD
5 DIWEDDARIADAU	6 FFUG		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 D – SGANYMDDYGIAD	2 H – GWRTHFEIRWS	3 E – DIWEDDARIADAU	4 B – HEURISTEGCOD
5 G – YNYSU	6 A – LLOFNODSTWNSH	7 C – BLWCHTYWOD	8 F – POSITIFFFUG

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio Llofnod Hash, Heuristeg Cod a Blwch Tywod Ffeiliau 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.

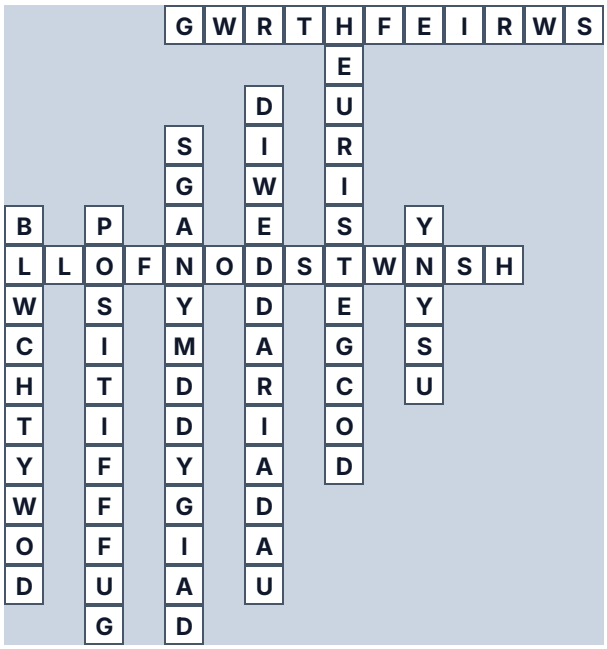
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CLIWIAU AR DRAWS

1 ar draws: GWRTHFEIRWS Cyfres feddalwedd sy'n sganio ac yn diogelu dyfeisiau terfynol rhag campau manteisio (11 llythyren)

8 ar draws: LLOFNODSTWNSH Ôl troed cryptograffig unigryw mewn cronfa ddata a ddefnyddir i adnabod bygythiadau hysbys (13 llythyren)

CLIWIAU I LAWR

2 i lawr: HEURISTEGCOD Dadansoddiad ar sail rheolau sy'n tynnu sylw at ffeiliau â chynllun cod amheus (12 llythyren)

3 i lawr: DIWEDDARIADAU Lawrlwythiadau diffiniadau rheolaidd sy'n bwydo'r gronfa ddata bygythiadau (13 llythyren)

4 i lawr: SGANYMDDYGIAD Monitro gweithredoedd meddalwedd sy'n rhedeg am batrymau gweithredu maleisus (13 llythyren)

5 i lawr: BLWCHTYWOD Amgylchedd prawf rhithwir diogel sy'n rhedeg cod nad oes modd ymddiried ynddo yn ddiogel (10 llythyren)

6 i lawr: POSITIFFFUG Rhybudd diogelwch sy'n dosbarthu meddalwedd ddiogel fel maleiswedd ar gam (11 llythyren)

7 i lawr: YNYSU Cyfyngu ffeiliau amheus er mwyn atal amlygu'r system leol (5 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.	DOTSOLSWLNHNF	LLOFNODSTWNSH	5.	ECETDUIGSHOR	HEURISTEGCOD
2.	OCBLHDYWTW	BLWCHTYWOD	6.	YGDMIAAYSGDDN	SGANYMDDYGIAD
3.	IDRAIAUWADDDE	DIWEDDARIADAU	7.	FTPOFGFUSII	POSITIFFFUG
4.	YUSYN	YNYSU	8.	RESFRGHWWIT	GWRTHFEIRWS

ALLWEDD HER Y SEIFFR CYFRINACHOL

"CANFOD MALEISWEDD NEWYDD GYDA HEURISTEG COD"

Allwedd Atebion yr Astudiaethau Achos

A Astudiaeth Achos 1: Sganio ar Sail Llofnod neu Sganio Hewristig

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae gweithiwr yn lawrlwytho cyfleuster pwrpasol a adeiladwyd yn fewnol gan dîm arall. Mae'r sganiwr llofnodion yn ei basio, ond mae'r sganiwr hewristig yn ei nodi fel un amheus.
- Strategaeth ac Ateb a Argymhellir: Pam y Digwyddodd: Mae sganio llofnodion yn gwirio hashes ffeiliau; gan ei bod yn bwrpasol, nid yw yn y gronfa ddata bygythiadau. Mae hewristeg yn dadansoddi strwythur ac yn nodi gweithredoedd amheus (e.e. ysgrifennu i'r gofrestrfa). Dilysu: Rhedwch y ffeil mewn blwch tywod i arsylwi ar ei gweithredoedd, gwiriwch lofnodion digidol, a chyflwynwch yr hash i byrth cudd-wybodaeth am fygythiadau.

B Astudiaeth Achos 2: Ymdrin â Positifau Ffug

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae datblygwr meddalwedd yn crynhoi ei raglen. Mae gwrthfeirws y system yn nodi'r ffeil weithredadwy newydd fel maleiswedd ac yn ei rhoi mewn cwarantin.
- Strategaeth ac Ateb a Argymhellir: Risgiau Rhestr Ganiatáu: Gall osgoi sganwyr ganiatáu i god go iawn sydd wedi'i heintio redeg. Llwybr Datrys: Cyflwynwch y ffeil i werthwr y gwrthfeirws i'w dadansoddi, llofnodwch y cod yn ddigidol gan ddefnyddio awdurdodau tystysgrifau, a ffurfweddwch eithriadau ffolder penodol dros dro yn hytrach na diffodd y gwrthfeirws.