Enw: _____ Dyddiad: _____ Sgôr: _____

Ymosodiadau Meddalwedd Wystlo a Busnes Adfer

Gweithredu'r llwyth, amgryptio ffeiliau'n gryptograffig, copïau wrth gefn all-lein, gweithdrefnau cyfyngu ac adfer ar ôl trychineb.

TROSOLWG DYSGU YMOSODIADAU MEDDALWEDD WYSTLO

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 ymosodiadau meddalwedd wystlo ac adfer busnes. Byddwch yn archwilio gweithredu llwythi, amgryptio ffeiliau, copïau wrth gefn all-lein, cyfyngu bygythiadau, taliadau arian cyfred digidol a chynlluniau adfer ar ôl trychineb.

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/ymosodiad-ransomware/

Eich Map Llwybr Dysgu Adfer ar ôl Meddalwedd Wystlo

- Gwahaniaethwch rhwng llwythi Trojan, ransomware a meddalwedd ysbïo.
- Dadansoddwch ffeiliau maleisus y tu mewn i amgylcheddau blwch tywod diogel.
- Lluniwch weithdrefnau cyflym ar gyfer ynysu a chyfyngu ar y rhwydwaith.

CYFARWYDDIADAU'R CANLLAW YMOSODIADAU MEDDALWEDD WYSTLO

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 adfer ar ôl meddalwedd wystlo. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

YMOSODIADAU MEDDALWEDD WYSTLO AC ADFER AR ÔL TRYCHINEB (CYFLWYNIAD)

Mae llwythi meddalwedd wystlo yn cloi storfa'r system yn gryptograffig, gan fynnu taliadau arian cyfred digidol am allweddi dadgryptio. Mae lliniaru'r bygythiad hwn yn cynnwys rheolau ynysu rhwydwaith, dadansoddi maleiswedd mewn blwch tywod, a chopïau wrth gefn oer cadarn wedi'u hynysu'n llwyr (air-gapped).

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

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw prif fecanwaith ymosodiad meddalwedd wystlo?**
   - A. Amgryptio ffeiliau defnyddwyr yn gryptograffig i wrthod mynediad i'r system
   - B. Chwistrellu gorchmynion SQL maleisus i feysydd ffurflenni
   - C. Sniffian pecynnau rhwydwaith ar gysylltiad Wi-Fi cyhoeddus
   - D. Ffugio penawdau e-bost i osgoi dilysu SPF

2. **2. Beth yw copi wrth gefn all-lein (oer)?**
   - A. Copi storio sydd wedi'i ddatgysylltu o'r rhwydwaith i'w ddiogelu rhag lledaeniad maleiswedd
   - B. Copi wrth gefn wedi'i storio ar yriant caled y prif weinydd gwe
   - C. Celc dros dro o logiau cofrestrfa'r system
   - D. Offeryn gweinyddol a ddefnyddir i ailosod cyfrineiriau defnyddwyr

3. **3. Sut dylai timau diogelwch ynysu systemau sydd wedi'u heintio yn ystod ymosodiad meddalwedd wystlo (ransomware)?**
   - A. Datgysylltu ceblau rhwydwaith ac analluogi rhyngwynebau diwifr ar unwaith
   - B. Uwchraddio cronfa ddata llofnodion y gwrthfeirws
   - C. Diffodd y prif weinydd DNS
   - D. Ailenwi estyniadau'r ffeiliau sydd wedi'u cyfaddawdu

4. **4. Pam mae asiantaethau diogelwch yn cynghori yn erbyn talu gofynion meddalwedd wystlo?**
   - A. Mae talu arian yn annog ymosodwyr ac nid yw'n gwarantu y bydd yr allwedd dadgryptio yn cael ei darparu
   - B. Mae'n dirymu holl bolisïau yswiriant y cwmni yn awtomatig
   - C. Mae'n hysbysu pob cwsmer drwy e-bost yn awtomatig
   - D. Mae'n llygru'r ffeiliau wrth gefn sy'n weddill ar y system

5. **5. Beth yw cynllun adfer ar ôl trychineb (DRP)?**
   - A. Proses strwythuredig i adfer gweithrediadau a data ar ôl i system gael ei chyfaddawdu
   - B. Ffurfweddiad wal dân sy'n mapio porthladdoedd rhwydwaith i mewn
   - C. Sgema cronfa ddata sy'n rhestru breintiau gweinyddol defnyddwyr
   - D. Protocol dilysu e-bost sy'n gwrthod parthau ffug

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Gall llwythi meddalwedd wystlo ledaenu'n hawdd i gopïau wrth gefn ar-lein sydd wedi'u cysylltu â'r rhwydwaith.

Gwir Gau

7 Cwestiwn 7

7. Mae talu'r pridwerth arian cripto yn gwarantu y caiff ffeiliau eu dadgryptio'n llwyddiannus.

Gwir Gau

8 Cwestiwn 8

8. Mae datgysylltu systemau heintiedig o'r rhwydwaith yn helpu i atal nwyddau pridwerth rhag lledaenu i systemau cyfagos.

Gwir Gau

9 Cwestiwn 9

9. Nid yw meddalwedd wystlo byth yn defnyddio cryptograffeg gymesur i amgryptio storfa'r system.

Gwir Gau

10 Cwestiwn 10

10. Mae profi gweithdrefnau adfer data'n rheolaidd yn rhan hanfodol o adfer ar ôl trychineb.

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 gwrthod mynediad at ffeiliau lleol yn defnyddio _____ cryptograffig.

2. Y cod maleisus gweithredol sy'n cael ei redeg ar system yw'r _____ .

3. Yr enw ar gopïau storio oddi ar y safle sydd wedi'u datgysylltu yw _____ diogel.

4. Mae atal maleiswedd rhag lledaenu yn golygu bod angen _____ rhwydwaith ar ddyfeisiau terfynol.

5. Y taliad arian cripto y mae seiberdroseddwyr yn ei fynnu yw'r _____ .

6. Mae dychwelyd ffeiliau data gweithredol yn rhan o _____ ar ôl trychineb.

BANC GEIRIAU GEIRFA

ADFER | AMGRYPTIO | CEFFYL PREN TRYCHINEB | COPI OER YNYSU | LLWYTH | PRIDWERTH

Ysgrifennwch eich atebion yma:

1.
2.
3.
4.
5.
6.

Pwynt Gwirio 4: Paru Cysyniadau Diogelwch

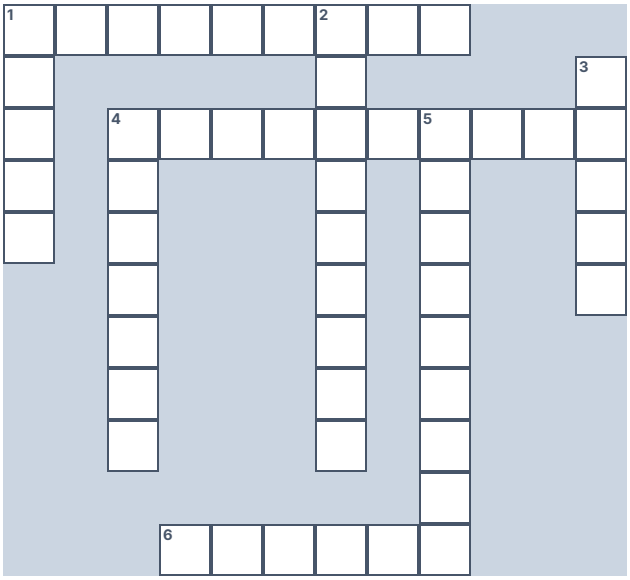
PARU DIFFINIADAU

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. AMGRYPTIO	A	Datgysylltu systemau rhwydwaith heintiedig.
☐	2. LLWYTH	B	Ffeil faleisus wedi'i chuddio fel un lân.
☐	3. COPI WRTH GEFN OER	C	Cloi ffeiliau'n gryptograffig.
☐	4. YNYSU	D	Digwyddiad tarfu mawr ar y system.
☐	5. PRIDWERTH	E	Rhedeg meddalwedd maleisus.
☐	6. ADFER	F	Copi all-lein wedi'i ddatgysylltu.
☐	7. TRYCHINEB	G	Adfer cronfa ddata o gopi wrth gefn.
☐	8. CEFFYL PREN	H	Cais am daliad allwedd gryptograffig.

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. Cloi ffeiliau'n gryptograffig. (9)

4. Ffeil faleisus wedi'i chuddio fel un lân. (10)

6. Rhedeg meddalwedd faleisus. (6)

CLIWIAU I LAWR

1. Dychwelyd cronfa ddata o gopi wrth gefn. (5)

2. Digwyddiad tarfu mawr ar systemau. (9)

3. Datgysylltu systemau rhwydwaith heintiedig. (5)

4. Copi all-lein wedi'i ddatgysylltu. (7)

5. Cais am daliad yn gyfnewid am allwedd gryptograffig. (9)

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

1 ar draws: Cloi ffeiliau'n gryptograffig. (9 llythyren):

4 ar draws: Ffeil faleisus wedi'i chuddio fel un lân. (10 llythyren):

6 ar draws: Rhedeg meddalwedd faleisus. (6 llythyren):

CLIWIAU I LAWR

1 i lawr: Dychwelyd cronfa ddata o gopi wrth gefn. (5 llythyren):

2 i lawr: Digwyddiad tarfu mawr ar systemau. (9 llythyren):

3 i lawr: Datgysylltu systemau rhwydwaith heintiedig. (5 llythyren):

4 i lawr: Copi all-lein wedi'i ddatgysylltu. (7 llythyren):

5 i lawr: Cais am daliad yn gyfnewid am allwedd gryptograffig. (9 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.

C R I G N R M C P X Q O C U S

T E U L J B A O B C L P X L K

Y K S X T K D P Q M L J D I N

O N Y K Q P G I M M W Q R S T

I T N G C C S O Q O Y H S P B

T W Y D S E Z E V C T Z W R F

P K H Z D F N R T D H Q X I P

Y C U B A F Z N R D K A D D O

R D F H I Y D R Y Q M E I W R

G Z S F Q L A V C F A A Q E O

M N P T X P D Q H K R U S R D

A N Y B F R F S I X W J A T R

Z Y Y L G E E I N M R J M H L

T O H Q Q N R H E Z A O V G U

B Y R Y B H L Z B G J O P N W

RHESTR GEIRIAU GEIRFA

AMGRYPTIO, LLWYTH, COPIOER, YNYSU CEFFYLPREN, PRIDWERTH, ADFER, TRYCHINEB

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. AMGRYPTIO
B. LLWYTH
C. COPIOER
D. YNYSU
E. PRIDWERTH
F. ADFER
G. TRYCHINEB
H. CEFFYLPREN

	DIFFINIADAU A MEYSYDD PARU
	1. Copi all-lein wedi'i ddatgysylltu.
	2. Ffeil faleisus wedi'i chuddio fel un lân.
	3. Cloi ffeiliau'n gryptograffig.
	4. Cais am daliad yn gyfnewid am allwedd gryptograffig.
	5. Datgysylltu systemau rhwydwaith heintiedig.
	6. Digwyddiad tarfu mawr ar systemau.
	7. Rhedeg meddalwedd faleisus.
	8. Dychwelyd cronfa ddata o gopi wrth gefn.

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. **PYRMATIOG** _____
2. **CPREOIO** _____
3. **PEWRRHDTI** _____
4. **HBECNITRY** _____
5. **YWHLTL** _____
6. **SYYUN** _____
7. **ERAFD** _____
8. **EFLNCYEPRF** _____

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Gwybodaeth na ddylech byth ei rhannu			
2	Dyfeisiau y gellir eu hacio			
3	Rhesymau dros beidio â thalu pridwerth			
4	Arferion diogel y gallwch eu dechrau heddiw			
5	Offer diogelwch rydych chi'n eu hadnabod			
6	Ffyrdd o ddiogelu eich cyfrifon			
7	Arwyddion bod cyfrifiadur wedi'i heintio			
8	Mannau i gadw copi wrth gefn			
9	Ffeiliau nad ydych chi byth eisiau eu colli			
10	Ffyrdd y mae nwyddau pridwerth yn lledaenu			
11	Pethau i'w gwneud yn awr gyntaf ymosodiad			
12	Pobl i gysylltu â nhw yn ystod ymosodiad			
13	Pethau y gall nwyddau pridwerth eu cloi			
14	Geiriau sy'n ymwneud â seiberddiogelwch			
15	Sefydliadau sy'n cael eu targedu'n aml			

Pwynt Gwirio 8: Astudiaethau Achos Seiberddiogelwch

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

ASTUDIAETH ACHOS 1: CYFYNGU AR LWYTH MEDDALWEDD PRIDWERTH MEWN MENTER

👷

Senario: Mae rhwydwaith ardal leol corfforaethol wedi cael ei dorri gan feddalwedd wystlo weithredol. Mae gweinyddion ffeiliau allweddol wedi dechrau dangos estyniadau ffeil gyda .locked.

Cwestiwn Trafod: Disgrifiwch y camau cyfyngu yn fanwl, ac amlinellwch y protocol adfer data.

ASTUDIAETH ACHOS 2: GWERTHUSO PENSAERNÏAETHAU COPÏAU WRTH GEFN ALL-LEIN

👷

Senario: Mae menter am ddylunio strategaeth gwneud copïau wrth gefn o ddata sy'n lleihau'r risg y gellir peryglu'r copïau wrth gefn, hyd yn oed os caiff y prif rwydwaith lleol ei herwgipio'n llwyr gan nwyddau pridwerth.

Cwestiwn Trafod: Lluniwch system claddgell storio copïau wrth gefn all-lein a diogel.

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

1	4	6	5	18	23	3	8		4	4	1	20	1		23	5	4	9	
5	9		1	13	7	18	25	16	20	9	15		15		7	15	16	9	
								15	5	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 meddalwedd wystlo?

Meddalwedd faleisus yw meddalwedd wystlo sydd wedi'i chynllunio i rwystro mynediad i systemau cyfrifiadurol neu ffeiliau nes bod swm pridwerth yn cael ei dalu.

Q2: Sut mae meddalwedd wystlo'n lledaenu?

Drwy atodiadau e-byst gwe-rwydo, gwendidau meddalwedd heb eu clytio, a systemau mynediad o bell sydd wedi'u cyfaddawdu. [1]

Q3: Pam mae taliad yn cael ei ofyn mewn arian cyfred digidol?

Mae arian cyfred digidol fel Bitcoin yn cynnig anhysbysrwydd cymharol, gan ei gwneud yn anodd i orfodi'r gyfraith olrhain yr arian.

Q4: A yw gwrthfeirws yn rhwystro meddalwedd wystlo?

Ydy, ond gall gwrthfeirws ar sail llofnodion fethu yn erbyn llwythi tâl meddalwedd wystlo dim diwrnod sydd newydd eu creu.

Q5: Beth yw copi wrth gefn wedi'i ynysu'n llwyr (air-gapped)?

Copi wrth gefn nad oes ganddo unrhyw gysylltiad ffisegol na rhesymegol â'r prif rwydwaith, gan ei ddiogelu rhag lledaeniad.

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

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

Q6: Beth yw cribddeiliaeth ddwbl?

Pan fydd ymosodwyr nid yn unig yn amgryptio ffeiliau ond hefyd yn dwyn data sensitif i fygwth ei ollwng yn gyhoeddus os na thelir.

Q7: Beth yw dadgryptiwr?

Cyfleuster meddalwedd sy'n cynnwys yr allwedd gryptograffig sydd ei hangen i adfer ffeiliau wedi'u cloi i destun plaen.

Q8: Sut ydych chi'n canfod meddalwedd wystlo yn gynnar?

Drwy fonitro systemau ffeiliau am weithgarwch sydyn ac enfawr o addasu ac ailenwi ffeiliau.

Q9: Beth yw rôl yswiriant?

Gall yswiriant seiber helpu i dalu costau adfer, ond mae telerau'r yswiriant a'r rheolau ar dalu pridwerth yn amrywio o bolisi i bolisi.

Q10: A ddylwn i ailgychwyn system sydd wedi'i heintio?

Na, gall ailgychwyn ddinistrio tystiolaeth yn y cof anweddol; ynyswch ef o'r rhwydwaith yn lle hynny. [1]

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 meddalwedd wystlo'n defnyddio amgryptio anghymesur?

Mae'n defnyddio allwedd gyhoeddus sydd wedi'i hymgorffori yn y maleiswedd i amgryptio ffeiliau, gan ofyn am allwedd breifat yr ymosodwr i'w dadgryptio.

Q2: Pam mae amgryptio cymesur hefyd yn cael ei ddefnyddio?

Mae amgryptio cymesur (fel AES) yn gyflym a gall gloi cronfeydd data enfawr mewn munudau, tra bo allweddi anghymesur yn diogelu'r allwedd AES.

Q3: Beth yw segmentu rhesymegol?

Rhannu rhwydweithiau'n barthau ynysig, gan atal maleiswedd rhag lledaenu'n ochrol o nodau gweithfannau i weinyddion craidd.

Q4: Beth yw storfa WORM?

Cyfryngau Ysgrifennu-Unwaith, Darllen-Sawl-Gwaith, sy'n atal data wrth gefn rhag cael ei olygu, ei drosysgrifo neu ei ddileu gan lwythi tâl meddalwedd wystlo.

Q5: Beth yw copïau cysgodol (shadow copies)?

Cipluniau wrth gefn lleol a grëwyd gan Windows; mae nwyddau pridwerth fel arfer yn dileu'r rhain yn gyntaf gan ddefnyddio offer gweinyddol.

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

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

Q6: Sut mae dwyn manylion mewngofnodi yn galluogi meddalwedd wystlo?

Mae ymosodwyr yn prynu manylion mewngofnodi gweinyddwyr a ddatgelwyd er mwyn mewngofnodi drwy benbyrddau o bell, gan weithredu ransomware â llaw ar draws y rhwydwaith.

Q7: Beth yw profi adfer ar ffurf ymarfer (dry-run)?

Adfer cronfeydd data wrth gefn yn rheolaidd i amgylcheddau prawf ynysig i wirio bod cyflymder adfer a chywirdeb data'n bodloni metrigau trychineb.

Q8: Sut mae canfod pwyntiau terfyn (EDR) yn atal meddalwedd wystlo?

Drwy ddadansoddi ymddygiad prosesau (e.e., amgryptio cyflym) ac atal y rhaglen dwyllodrus yn gyflym.

Q9: Beth yw model meddalwedd wystlo fel gwasanaeth (RaaS)?

Model masnachfraint lle mae datblygwyr maleiswedd yn prydlesu adeiladwyr nwyddau pridwerth i gysylltiedigion yn gyfnewid am ganran o'r taliadau.

Q10: Sut mae RDP heb ei ddiweddaru yn sbarduno meddalwedd wystlo?

Mae pyrth Remote Desktop Protocol agored heb eu clytio yn caniatáu i ymosodwyr dorri mewngofnodion drwy rym ysgrublaidd a lansio maleiswedd â llaw.

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 actorion meddalwedd wystlo yn aml yn defnyddio offer fel vssadmin.exe i ddileu copïau cysgodol Windows a rhwystro adfer lleol. [1]

2. CIPOLWG AR DDIOGELWCH

Fel arfer, defnyddir allweddi AES-256 cymesur i amgryptio llwythi ffeiliau, sydd wedyn yn cael eu cloi gan ddefnyddio allweddi RSA cyhoeddus.

3. CIPOLWG AR DDIOGELWCH

Gall adfer ar ôl ymosodiad nwyddau pridwerth llwyddiannus gymryd wythnosau, a dyna pam mae copïau wrth gefn all-lein wedi'u profi yn bwysig.

4. CIPOLWG AR DDIOGELWCH

Nid yw'r FBI yn cefnogi talu pridwerth ac mae'n rhybuddio nad yw talu'n gwarantu y cewch unrhyw ddata yn ôl. [2]

5. CIPOLWG AR DDIOGELWCH

Dylai cynlluniau adfer ar ôl trychineb (DRP) ddiffinio Amcan Amser Adfer (RTO) ac Amcan Pwynt Adfer (RPO).

6. CIPOLWG AR DDIOGELWCH

Mae'r FBI yn argymell copïau wrth gefn sydd wedi'u hamgryptio ac yn ddigyfnewid, sy'n golygu na ellir eu newid na'u dileu. [3]

7. MEWNWELEDIAD DIOGELWCH

Mae datblygwyr meddalwedd wystlo yn defnyddio technegau cuddio datblygedig i osgoi sganwyr gwrthfeirws traddodiadol sy'n seiliedig ar lofnodion.

8. MEWNWELEDIAD DIOGELWCH

Mae segmentu rhwydwaith yn cyfyngu ar symud ochrol, gan helpu i atal nwyddau pridwerth rhag lledaenu y tu hwnt i'r gwesteiwr heintiedig cyntaf. [3]

9. MEWNWELEDIAD DIOGELWCH

Mae gwasanaethau o bell sy'n agored ac wedi'u diogelu'n wael, fel Remote Desktop Protocol (RDP), yn fan mynediad cyffredin i ransomware. [1]

10. CIPOLWG AR DDIOGELWCH

Mae CISA yn cynghori cadw copïau wrth gefn wedi'u hamgryptio all-lein, gan fod llawer o amrywiadau meddalwedd pridwerth yn chwilio am gopïau wrth gefn y gellir eu cyrraedd ac yn eu dileu. [1]

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] CISA. (2023). #StopRansomware Guide.

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

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

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

[5] 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

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Cwestiwn 1** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw prif fecanwaith ymosodiad meddalwedd wystlo? → Amgryptio ffeiliau defnyddwyr yn gryptograffig i wrthod mynediad i'r system

2 **Cwestiwn 2** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw copi wrth gefn all-lein (oer)? → Copi storio sydd wedi'i ddatgysylltu o'r rhwydwaith i'w ddiogelu rhag lledaeniad maleiswedd

3 **Cwestiwn 3** — **Ateb Cywir: A**

NODYN ADDYSGU

Sut dylai timau diogelwch ynysu systemau sydd wedi'u heintio yn ystod ymosodiad meddalwedd wystlo (ransomware)? → Datgysylltu ceblau rhwydwaith ac analluogi rhyngwynebau diwifr ar unwaith

4 **Cwestiwn 4** — **Ateb Cywir: A**

NODYN ADDYSGU

Pam mae asiantaethau diogelwch yn cynghori yn erbyn talu gofynion meddalwedd wystlo? → Mae talu arian yn annog ymosodwyr ac nid yw'n gwarantu y bydd yr allwedd dadgryptio yn cael ei darparu

5 **Cwestiwn 5** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw cynllun adfer ar ôl trychineb (DRP)? → Proses strwythuredig i adfer gweithrediadau a data ar ôl i system gael ei chyfaddawdu

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Cwestiwn 6** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gall llwythi meddalwedd wystlo ledaenu'n hawdd i gopïau wrth gefn ar-lein sydd wedi'u cysylltu â'r rhwydwaith.

7 **Cwestiwn 7** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae'r FBI yn rhybuddio nad yw talu yn gwarantu y cewch unrhyw ddata yn ôl. [2]

8 **Cwestiwn 8** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gwir: mae CISA yn cynghori datgysylltu gwesteiwyr heintiedig neu dynnu'r rhwydwaith all-lein i gyfyngu ar y lledaenu.

9 **Cwestiwn 9** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae nwyddau pridwerth fel arfer yn amgryptio ffeiliau â seiffrau cymesur cyflym fel AES.

10 **Cwestiwn 10** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae profi gweithdrefnau adfer data'n rheolaidd yn rhan hanfodol o adfer ar ôl trychineb.

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

C 1. AMGRYPTIO	E 2. LLWYTH	F 3. COPI WRTH GEFN OER	A 4. YNYSU
H 5. PRIDWERTH	G 6. ADFER	D 7. TRYCHINEB	B 8. CEFFYL PREN

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 AMGRYPTIO	2 LLWYTH	3 COPI OER	4 YNYSU
5 PRIDWERTH	6 ADFER		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 C – COPIOER	2 H – CEFFYLPREN	3 A – AMGRYPTIO	4 E – PRIDWERTH
5 D – YNYSU	6 G – TRYCHINEB	7 B – LLWYTH	8 F – ADFER

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio AMGRYPTIO, LLWYTH a COPI WRTH GEFN OER 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.

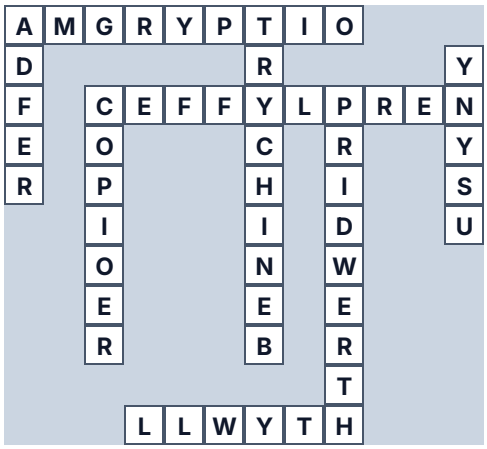
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

1 ar draws: AMGRYPTIO Cloi ffeiliau'n gryptograffig. (9 llythyren)

4 ar draws: CEFFYLPREN Ffeil faleisus wedi'i chuddio fel un lân. (10 llythyren)

6 ar draws: LLWYTH Rhedeg meddalwedd faleisus. (6 llythyren)

CLIWIAU I LAWR

1 i lawr: ADFER Dychwelyd cronfa ddata o gopi wrth gefn. (5 llythyren)

2 i lawr: TRYCHINEB Digwyddiad tarfu mawr ar systemau. (9 llythyren)

3 i lawr: YNYSU Datgysylltu systemau rhwydwaith heintiedig. (5 llythyren)

4 i lawr: COPIOER Copi all-lein wedi'i ddatgysylltu. (7 llythyren)

5 i lawr: PRIDWERTH Cais am daliad yn gyfnewid am allwedd gryptograffig. (9 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.	PYRMATIOG	AMGRYPTIO	5.	YWHLTL	LLWYTH
2.	CPREOIO	COPIOER	6.	SYYUN	YNYSU
3.	PEWRRHDTI	PRIDWERTH	7.	ERAFD	ADFER
4.	HBECNITRY	TRYCHINEB	8.	EFLNCYEPRF	CEFFYLPREN

ALLWEDD HER Y SEIFFR CYFRINACHOL

"ADFERWCH DDATA WEDI EI AMGRYPTIO O GOPI OER"

Allwedd Atebion yr Astudiaethau Achos

A Astudiaeth Achos 1: Cyfyngu ar Lwyth Meddalwedd Pridwerth mewn Menter

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae nwyddau pridwerth gweithredol wedi torri i mewn i rwydwaith ardal leol corfforaethol. Mae gweinyddion ffeiliau allweddol wedi dechrau dangos estyniadau ffeil .locked.
- Strategaeth a Datrysiad a Argymhellir: Datgysylltwch yr holl weinyddion yr effeithiwyd arnynt o'r rhwydwaith ardal leol. Terfynwch sesiynau gweinyddol gweithredol. Adferwch ffeiliau heb eu cyfaddawdu o system copïau wrth gefn all-lein ddiogel sydd wedi'i chloi rhag ysgrifennu.

B Astudiaeth Achos 2: Gwerthuso Pensaernïaethau Copïau Wrth Gefn All-lein

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae menter am ddylunio strategaeth gwneud copïau wrth gefn o ddata sy'n lleihau'r risg y caiff copïau wrth gefn eu peryglu hyd yn oed os caiff y prif rwydwaith lleol ei herwgipio'n llwyr gan feddalwedd wystlo.
- Strategaeth ac Ateb a Argymhellir: Gweithredwch storfa ysgrifennu-unwaith-darllen-sawl-gwaith (WORM). Crëwch fwlch aer rhesymegol drwy ddatgysylltu'r system wrth gefn o bob rhwydwaith, a gorfodwch gylchdroi cyfryngau ffisegol bob dydd.