Όνομα: _____ **Ημερομηνία:** _____ **Βαθμολογία:** _____

Λογισμικό antivirus και τερματικά Οδηγός προστασίας

Ανίχνευση υπογραφών, ευρετική ανάλυση, παρακολούθηση συμπεριφοράς, sandboxing, ενημερώσεις

ΕΠΙΣΚΟΠΗΣΗ ΕΚΜΑΘΗΣΗΣ ΛΟΓΙΣΜΙΚΟΥ ANTIVIRUS

ΑΣΦΑΛΙΣΜΕΝΟ
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ
Πρότυπο AES 256 bit

ΣΥΜΦΩΝΟ
ΠΑΓΚΟΣΜΙΑ ΠΡΟΤΥΠΑ
Πλαίσια GDPR και CCPA

ZERO-TRUST
ΠΟΛΙΤΙΚΗ ΠΡΟΣΒΑΣΗΣ
Έλεγχος ταυτότητας πολλαπλών παραγόντων

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στο λογισμικό antivirus και την προστασία τερματικών. Θα εξερευνήσεις βάσεις δεδομένων υπογραφών, ευρετικούς σαρωτές, παρακολούθηση συμπεριφοράς, εικονικά αρχεία sandbox και περιορισμό των ψευδώς θετικών.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- [ ] **Μέρη 1-4: Κατάκτησε την κυβερνοασφάλεια και την πρόληψη απειλών.**
- [ ] **Μέρη 5-7: Λύσε γρίφους σταυρολέξου και αναζήτησης λέξεων.**
- [ ] **Μέρη 8-9: Λύσε μελέτες περίπτωσης και πρόκληση κρυπτογραφημένου μηνύματος.**
- [ ] **Μέρος 10: Εξέτασε τις σελίδες συχνών ερωτήσεων βασικού και προχωρημένου επιπέδου.**
- [ ] **Μέρος 11: Εξερεύνησε 10 ενδιαφέροντα πραγματικά στοιχεία.**
- [ ] **Μπόνους: η πρόκληση Σκέψου γρήγορα.**

Άνοιξε τον Οδηγό του VPN.com για την κυβερνοασφάλεια

URL: https://www.vpn.com/el/kiberasfaleia/antivirus/

Η πορεία μάθησής σου: στρατηγική antivirus

- Διαχώρισε την ανίχνευση κακόβουλου λογισμικού βάσει υπογραφών από την ανίχνευση βάσει ευρετικών μεθόδων.
- Κατανόησε τα πρωτόκολλα παρακολούθησης συμπεριφοράς και απομόνωσης sandbox.
- Αξιολόγησε τις επιπτώσεις των σαρώσεων σε πραγματικό χρόνο στην απόδοση του συστήματος και των τερματικών.
- Μετρίασε τις εσφαλμένες θετικές ταξινομήσεις χρησιμοποιώντας επαλήθευση ψηφιακών πιστοποιητικών.
- Διαχείριση της καθημερινής διανομής ενημερώσεων ορισμών σε εταιρικά τερματικά.

ΟΔΗΓΙΕΣ ΟΔΗΓΟΥ ANTIVIRUS

Απάντησε στις ερωτήσεις πολλαπλής επιλογής και σωστού/λάθους, συμπλήρωσε τα κενά των προτάσεων με την τράπεζα λέξεων, αντιστοίχισε ορισμούς και λύσε το σταυρόλεξο και τον γρίφο αναζήτησης λέξεων. Εφάρμοσε τις γνώσεις σου στην ασφάλεια antivirus των τερματικών. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΠΡΟΣΤΑΣΙΑ ANTIVIRUS ΚΑΙ ΣΑΡΩΣΗ ΥΠΟΓΡΑΦΩΝ (ΕΙΣΑΓΩΓΗ)

Το λογισμικό antivirus προστατεύει τα τερματικά εντοπίζοντας, θέτοντας σε καραντίνα και αφαιρώντας κακόβουλο λογισμικό. Τα σύγχρονα συστήματα συνδυάζουν βάσεις δεδομένων υπογραφών (αντιστοίχιση γνωστών κατακερματισμών απειλών) με ευρετικές μεθόδους (ανάλυση της δομής των αρχείων) και παρακολούθηση συμπεριφοράς για τον εντοπισμό εκμεταλλεύσεων zero-day.

ΔΙΑΒΑΣΕ ΠΡΟΣΕΚΤΙΚΑ ΚΑΘΕ ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ ΚΑΙ ΕΠΙΛΕΞΕ Η ΓΡΑΨΕ ΤΗ ΣΩΣΤΗ

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **Ποιος είναι ένας περιορισμός του εντοπισμού που βασίζεται σε υπογραφές;**
   - A. Δεν μπορεί να εντοπίσει άγνωστο ή τροποποιημένο κακόβουλο λογισμικό
   - B. Παράγει υψηλά ποσοστά ψευδώς θετικών αποτελεσμάτων
   - C. Απαιτεί υψηλή επεξεργαστική ισχύ CPU
   - D. Λειτουργεί μόνο όταν είναι συνδεδεμένο στο διαδίκτυο

2. **Πώς εντοπίζουν οι ευρετικοί σαρωτές νέες παραλλαγές κακόβουλου λογισμικού;**
   - A. Με τον εντοπισμό ύποπτων μοτίβων και δομών κώδικα
   - B. Με την αντιστοίχιση κατακερματισμών αρχείων σε μια βάση δεδομένων απειλών
   - C. Με την αυτόματη διαγραφή όλων των μη υπογεγραμμένων εκτελέσιμων
   - D. Με μεταφόρτωση κάθε αρχείου σε δημόσιο φάκελο cloud

3. **Ποιος είναι ο σκοπός της εκτέλεσης σε sandbox από το antivirus;**
   - A. Απομόνωση και ανάλυση αρχείων σε ασφαλές εικονικό θησαυροφυλάκιο
   - B. Επιτάχυνση της μεταφοράς αντιγράφων ασφαλείας του τοπικού συστήματος αρχείων
   - C. Ενημέρωση των ενημερώσεων ασφαλείας του τοπικού λειτουργικού συστήματος
   - D. Συμπίεση μεγάλων αρχείων εγγράφων για εξοικονόμηση χώρου αποθήκευσης

4. **Ποια μέθοδος εντοπισμού επισημαίνει συμπεριφορά απειλής σε πραγματικό χρόνο;**
   - A. Συμπεριφορική ανάλυση που παρακολουθεί τις ενέργειες του λογισμικού
   - B. Επιθεώρηση ιστορικών αρχείων καταγραφής που διενεργείται κατά τη διάρκεια της νύχτας
   - C. Χειροκίνητη αναφορά αργών εφαρμογών από τον χρήστη
   - D. Εβδομαδιαίοι χειροκίνητοι έλεγχοι των εγκατεστημένων προγραμμάτων

5. **Γιατί είναι κρίσιμες οι τακτικές ενημερώσεις ορισμών για τα προγράμματα σάρωσης;**
   - A. Για να τροφοδοτεί τις μηχανές υπογραφών με αναγνωριστικά απειλών από βάση δεδομένων
   - B. Για την αύξηση της συχνότητας ρολογιού της CPU κατά τις λειτουργίες
   - C. Για να τροποποιήσεις τους παγκόσμιους χρόνους προσωρινής αποθήκευσης των διακομιστών ονομάτων DNS
   - D. Για έγκριση των ρυθμίσεων cookies του προγράμματος περιήγησης

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση Σωστό/Λάθος 6

6. Η ανίχνευση υπογραφών αντιστοιχίζει κρυπτογραφικούς κατακερματισμούς αρχείων με λίστες βάσεων δεδομένων.

○ Σωστό ○ Λάθος

7 Ερώτηση Σωστό/Λάθος 7

7. Οι ευρετικοί σαρωτές μπορούν να προκαλέσουν ψευδώς θετικές ειδοποιήσεις για ασφαλή αρχεία.

○ Σωστό ○ Λάθος

8 Ερώτηση Σωστό/Λάθος 8

8. Ένα sandbox επιτρέπει στο κακόβουλο λογισμικό να έχει απεριόριστη πρόσβαση σε αρχεία δικτύου.

○ Σωστό ○ Λάθος

9 Ερώτηση Σωστό/Λάθος 9

9. Η σάρωση συμπεριφοράς αποκλείει αρχεία όταν εμφανίζουν κακόβουλες ενέργειες.

○ Σωστό ○ Λάθος

10 Ερώτηση Σωστό/Λάθος 10

10. Το τυπικό λογισμικό antivirus σταματά πλήρως όλες τις επιθέσεις zero-day.

○ Σωστό ○ Λάθος

Σημείο ελέγχου 3: Συμπλήρωση βασικών όρων

Διάβασε κάθε πρόταση παρακάτω και συμπλήρωσε το κενό με τον σωστό όρο από την Τράπεζα Λέξεων.

1. Ένα παραδοσιακό πρόγραμμα σάρωσης αναγνωρίζει γνωστό κακόβουλο λογισμικό αντιστοιχίζοντας την _____ του.

2. Η ανάλυση των μοτίβων κώδικα ενός αρχείου ονομάζεται _____ σάρωση.

3. Τα εργαλεία antivirus απομονώνουν τα ύποπτα αρχεία σε ένα περιβάλλον, το λεγόμενο _____ .

4. Η παρακολούθηση σε πραγματικό χρόνο εξετάζει τη _____ των προγραμμάτων για ύποπτες δραστηριότητες.

5. Τα προγράμματα σάρωσης κατεβάζουν καθημερινά _____ της βάσης δεδομένων για να αναγνωρίζουν νέες απειλές.

6. Τα ασφαλή προγράμματα που επισημαίνονται ως κακόβουλα προκαλούν _____ θετικές ειδοποιήσεις.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΜΜΟΔΟΧΕΙΟ ΑΠΟΜΟΝΩΣΗ ΕΝΗΜΕΡΩΣΕΙΣ ΕΞΑΙΡΕΣΕΙΣ ΕΥΡΙΣΤΙΚΗ
ΣΥΜΠΕΡΙΦΟΡΑ ΥΠΟΓΡΑΦΗ ΨΕΥΔΩΣ

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

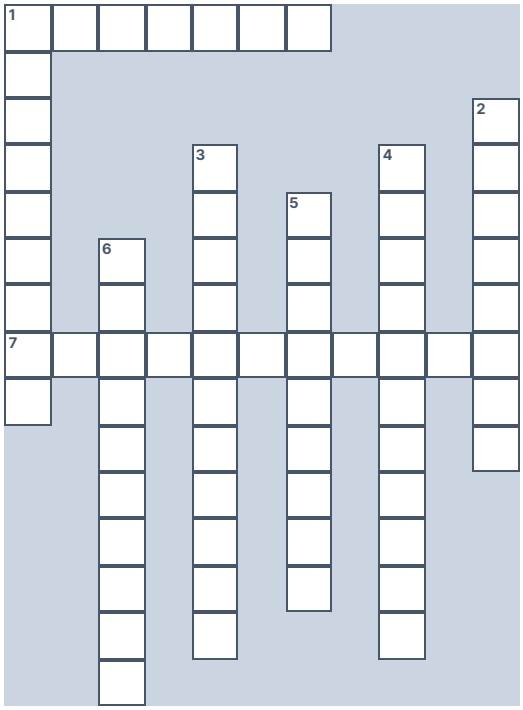
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

Αντιστοίχισε κάθε όρο λεξιλογίου στα αριστερά με τον σωστό ορισμό του στα δεξιά, γράφοντας το αντίστοιχο γράμμα (A-H) στο πλαίσιο εισαγωγής.

☐	1. Υπογραφή κατακερματισμού	A	Περιορισμός ύποπτων αρχείων για την αποφυγή έκθεσης του τοπικού συστήματος.
☐	2. Ευρετικά κώδικα	B	Σουίτα λογισμικού που σαρώνει και προστατεύει τερματικά από εκμεταλλεύσεις ευπαθειών.
☐	3. Sandbox αρχείων	C	Παρακολούθηση των ενεργειών του λογισμικού που εκτελείται για μοτίβα κακόβουλης λειτουργίας.
☐	4. Σάρωση συμπεριφοράς	D	Μοναδικό κρυπτογραφικό αποτύπωμα βάσης δεδομένων που χρησιμοποιείται για τον εντοπισμό γνωστών απειλών.
☐	5. Καθημερινές ενημερώσεις	E	Ασφαλές εικονικό περιβάλλον δοκιμών που εκτελεί με ασφάλεια μη αξιόπιστο κώδικα.
☐	6. Ψευδώς θετικό	F	Τακτικές λήψεις ορισμών που τροφοδοτούν τη βάση δεδομένων απειλών.
☐	7. Απομόνωση απειλών	G	Ανάλυση βάσει κανόνων που επισημαίνει αρχεία με ύποπτες διατάξεις κώδικα.
☐	8. Εργαλείο antivirus	H	Ειδοποίηση ασφαλείας που ταξινομεί λανθασμένα ασφαλές λογισμικό ως κακόβουλο λογισμικό.

Σημείο ελέγχου 5: Σταυρόλεξο

Λύσε το σταυρόλεξο πληκτρολογώντας γράμματα στα ενεργά λευκά κουτιά. Οι αριθμοί αντιστοιχούν στις οδηγίες παρακάτω.



ΟΡΙΖΟΝΤΙΑ

1. Λογισμικό που σαρώνει και προστατεύει τα τερματικά από εκμεταλλεύσεις ευπαθειών (7)

7. Παρακολούθηση των ενεργειών του λογισμικού που εκτελείται για μοτίβα κακόβουλης λειτουργίας (11)

ΚΑΘΕΤΑ

1. Περιορισμός ύποπτων αρχείων ώστε να αποφεύγεται η έκθεση του τοπικού συστήματος (9)

2. Μοναδικό κρυπτογραφικό αποτύπωμα στη βάση δεδομένων που χρησιμοποιείται για την αναγνώριση γνωστών απειλών (8)

3. Τακτικές λήψεις ορισμών που τροφοδοτούν τη βάση δεδομένων απειλών (11)

4. Ειδοποίηση ασφαλείας που ταξινομεί λανθασμένα ένα ασφαλές λογισμικό ως κακόβουλο (11)

5. Ανάλυση βάσει κανόνων που επισημαίνει αρχεία με ύποπτη διάταξη κώδικα (9)

6. Ασφαλές εικονικό περιβάλλον δοκιμών που εκτελεί με ασφάλεια μη αξιόπιστο κώδικα (10)

Σημείο ελέγχου 5, εναλλακτικά: Προσβάσιμες ενδείξεις σταυρολέξου

Οι χρήστες αναγνώστη οθόνης και πληκτρολογίου μπορούν να πληκτρολογήσουν τις απαντήσεις του σταυρολέξου απευθείας στα πεδία κειμένου παρακάτω. ΟΡΙΖΟΝΤΙΕΣ ΟΔΗΓΙΕΣ ΚΑΘΕΤΕΣ ΟΔΗΓΙΕΣ

ΟΡΙΖΟΝΤΙΑ

1 οριζόντια: Λογισμικό που σαρώνει και προστατεύει τα τερματικά από εκμεταλλεύσεις ευπαθειών (7 γράμματα):

7 οριζόντια: Παρακολούθηση των ενεργειών του λογισμικού που εκτελείται για μοτίβα κακόβουλης λειτουργίας (11 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Περιορισμός ύποπτων αρχείων ώστε να αποφεύγεται η έκθεση του τοπικού συστήματος (9 γράμματα):

2 κάθετα: Μοναδικό κρυπτογραφικό αποτύπωμα στη βάση δεδομένων που χρησιμοποιείται για την αναγνώριση γνωστών απειλών (8 γράμματα):

3 κάθετα: Τακτικές λήψεις ορισμών που τροφοδοτούν τη βάση δεδομένων απειλών (11 γράμματα):

4 κάθετα: Ειδοποίηση ασφαλείας που ταξινομεί λανθασμένα ένα ασφαλές λογισμικό ως κακόβουλο (11 γράμματα):

5 κάθετα: Ανάλυση βάσει κανόνων που επισημαίνει αρχεία με ύποπτη διάταξη κώδικα (9 γράμματα):

6 κάθετα: Ασφαλές εικονικό περιβάλλον δοκιμών που εκτελεί με ασφάλεια μη αξιόπιστο κώδικα (10 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

Βρες τους 8 βασικούς όρους λεξιλογίου που κρύβονται στο παρακάτω πλέγμα. Οι λέξεις μπορεί να είναι οριζόντιες, κάθετες ή διαγώνιες.

Ω Η Δ Ν Δ Π Χ Α Ο Γ Τ Β Α Ω Ν
Σ Σ Δ Λ Α Δ Ξ Μ Δ Ε Ε Η Θ Δ Ρ
Ι Ω Π Μ Ε Θ Ρ Μ Ω Σ Υ Ε Π Υ Ε
Ε Ν Α Α Π Ξ Ν Ο Ο Τ Ρ Χ Π Κ Ρ
Σ Ο Τ Ρ Γ Σ Ν Δ Ψ Β Ι Ζ Ρ Ψ Χ
Ω Μ Φ Ι Α Υ Ρ Ο Ω Ψ Σ Ψ Λ Ε Ζ
Ρ Ο Θ Μ Α Μ Π Χ Κ Μ Τ Μ Σ Υ Ξ
Ε Π Η Ο Ν Π Π Ε Η Ω Ι Α Η Δ Ξ
Μ Α Υ Ζ Τ Ε Υ Ι Β Ψ Κ Ρ Φ Ο Ψ
Η Β Η Μ Ι Ρ Ω Ο Η Κ Η Ξ Α Θ Ο
Ν Ν Χ Γ Ι Ι Μ Ω Ψ Ζ Ψ Ξ Ρ Ε Φ
Ε Υ Λ Υ Κ Φ Ο Β Ν Φ Τ Μ Γ Τ Η
Υ Γ Ψ Υ Ο Ο Κ Ρ Α Χ Ω Ψ Ο Ι Μ
Ρ Π Χ Θ Ξ Ρ Δ Α Γ Κ Π Φ Π Κ Χ
Χ Λ Ι Θ Τ Α Θ Ζ Β Ε Θ Κ Υ Ο Σ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΥΠΟΓΡΑΦΗ ΕΥΡΙΣΤΙΚΗ ΑΜΜΟΔΟΧΕΙΟ ΣΥΜΠΕΡΙΦΟΡΑ ΕΝΗΜΕΡΩΣΕΙΣ
ΨΕΥΔΟΘΕΤΙΚΟ ΑΠΟΜΟΝΩΣΗ ΑΝΤΙΙΚΟ

Σημείο ελέγχου 6, εναλλακτικά: Προσβάσιμη αντιστοίχιση λεξιλογίου

Αντιστοίχισε καθέναν από τους 8 όρους λεξιλογίου του Word Search με τον σωστό ορισμό του, γράφοντας το γράμμα (A-H) στο κενό.

ΟΡΟΙ ΛΕΞΙΛΟΓΙΟΥ

A. ΥΠΟΓΡΑΦΗ

B. ΕΥΡΙΣΤΙΚΗ

C. ΑΜΜΟΔΟΧΕΙΟ

D. ΣΥΜΠΕΡΙΦΟΡΑ

E. ΕΝΗΜΕΡΩΣΕΙΣ

F. ΨΕΥΔΟΘΕΤΙΚΟ

G. ΑΠΟΜΟΝΩΣΗ

H. ΑΝΤΙΙΚΟ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Παρακολούθηση των ενεργειών του λογισμικού που εκτελείται για μοτίβα κακόβουλης λειτουργίας.

2. Λογισμικό που σαρώνει και προστατεύει τα τερματικά από εκμεταλλεύσεις ευπαθειών.

3. Τακτικές λήψεις ορισμών που τροφοδοτούν τη βάση δεδομένων απειλών.

4. Ανάλυση βάσει κανόνων που επισημαίνει αρχεία με ύποπτη διάταξη κώδικα.

5. Περιορισμός ύποπτων αρχείων ώστε να αποφεύγεται η έκθεση του τοπικού συστήματος.

6. Μοναδικό κρυπτογραφικό αποτύπωμα στη βάση δεδομένων που χρησιμοποιείται για την αναγνώριση γνωστών απειλών.

7. Ασφαλές εικονικό περιβάλλον δοκιμών που εκτελεί με ασφάλεια μη αξιόπιστο κώδικα.

8. Ειδοποίηση ασφαλείας που ταξινομεί λανθασμένα ένα ασφαλές λογισμικό ως κακόβουλο.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους της κυβερνοασφάλειας. Γράψε τις απαντήσεις σου στα διαθέσιμα πλαίσια εισαγωγής.

1. **ΦΓΡΥΑΠΗΟ**
2. **ΙΟΑΜΔΟΧΕΟΜ**
3. **ΕΩΡΣΗΝΙΣΕΕΜ**
4. **ΟΗΣΜΩΝΑΠΟ**
5. **ΙΣΥΗΤΙΕΚΡ**
6. **ΕΑΡΦΡΟΣΥΙΜΠ**
7. **ΤΟΨΕΕΟΙΚΥΘΔ**
8. **ΝΙΟΑΚΙΤ**

Δραστηριότητα μπόνους: Σκέψου γρήγορα

3 ΑΠΑΝΤΗΣΕΙΣ ΓΙΑ ΚΑΘΕ ΚΑΤΗΓΟΡΙΑ. ΚΕΡΔΙΖΕΙ ΟΠΟΙΟΣ ΣΥΜΠΛΗΡΩΣΕΙ ΠΡΩΤΟΣ ΤΗ ΛΙΣΤΑ.

1	**Λόγοι για να ενημερώνεις το λογισμικό**			
2	**Άνθρωποι που μπορείς να ρωτήσεις για βοήθεια στην πληροφορική**			
3	**Πράγματα που κάνεις όταν το antivirus βρει κάτι**			
4	**Ενδείξεις ιού υπολογιστή**			
5	**Πράγματα που μπαίνουν σε καραντίνα**			
6	**Μέρη όπου κρύβονται οι ιοί**			
7	**Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι**			
8	**Τύποι κακόβουλου λογισμικού**			
9	**Εργαλεία ασφαλείας που γνωρίζεις**			
10	**Πράγματα που σαρώνει ένα antivirus**			
11	**Πράγματα που παίρνεις αντίγραφο ασφαλείας**			
12	**Συσκευές που μπορούν να παραβιαστούν**			
13	**Προγράμματα antivirus που γνωρίζεις**			
14	**Λόγοι για ψευδείς συναγερμούς**			
15	**Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα**			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

Εφάρμοσε τις έννοιες που έμαθες για να λύσεις τα παρακάτω σενάρια πραγματικού κόσμου.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΣΑΡΩΣΗ ΒΑΣΕΙ ΥΠΟΓΡΑΦΩΝ ΕΝΑΝΤΙ ΕΥΡΕΤΙΚΗΣ ΣΑΡΩΣΗΣ



Σενάριο: Ένας εργαζόμενος κατεβάζει ένα προσαρμοσμένο βοηθητικό πρόγραμμα που έφτιαξε εσωτερικά μια άλλη ομάδα. Ο σαρωτής υπογραφών το αφήνει να περάσει, αλλά ο ευρετικός σαρωτής το επισημαίνει ως ύποπτο.

Ερώτηση συζήτησης: Εξήγησε γιατί συνέβη αυτό και πώς μπορεί να επαληθευτεί αν το αρχείο είναι ασφαλές.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΔΙΑΧΕΙΡΙΣΗ ΨΕΥΔΩΣ ΘΕΤΙΚΩΝ



Σενάριο: Ένας προγραμματιστής λογισμικού μεταγλωττίζει την εφαρμογή του. Το antivirus του συστήματος επισημαίνει το νέο εκτελέσιμο ως κακόβουλο λογισμικό και το βάζει σε καραντίνα.

Ερώτηση συζήτησης: Περίγραψε συνοπτικά τους κινδύνους της προσθήκης σε λίστα εξαιρέσεων και περίγραψε τη σωστή διαδρομή επίλυσης.

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Ένας επαγγελματίας κυβερνοασφάλειας προστατεύει τα περιουσιακά στοιχεία του δικτύου από διαδικτυακούς φορείς απειλών. Χρησιμοποίησε το παρακάτω κλειδί Γράμμα-Αριθμός για να αποκρυπτογραφήσεις το μήνυμα γράφοντας τα αντίστοιχα γράμματα στα κενά.

ΚΛΕΙΔΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΓΡΑΜΜΑΤΟΣ ΣΕ ΑΡΙΘΜΟ

Α=1 Β=2 Γ=3 Δ=4 Ε=5 Ζ=6 Η=7 Θ=8

Ι=9 Κ=10 Λ=11 Μ=12 Ν=13 Ξ=14 Ο=15 Π=16

Ρ=17 Σ=18 Τ=19 Υ=20 Φ=21 Χ=22 Ψ=23 Ω=24



Αποκρυπτογραφημένο μήνυμα:

ΣΥΜΒΟΥΛΗ: ΚΑΘΕ ΑΡΙΘΜΟΣ ΕΚΠΡΟΣΩΠΕΙ ΤΗ ΘΕΣΗ ΤΟΥ ΓΡΑΜΜΑΤΟΣ ΣΤΟ ΑΛΦΑΒΗΤΟ (Π.Χ. 1 = Α, 2 = Β, 24 = Ω).

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Α)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q1: Πώς εντοπίζει το λογισμικό antivirus το κακόβουλο λογισμικό;

Εντοπίζει κακόβουλο λογισμικό με αντιστοίχιση υπογραφών βάσης δεδομένων, ευρετική ανάλυση της διάταξης του κώδικα και παρακολούθηση συμπεριφοράς σε πραγματικό χρόνο.

Q2: Τι είναι ο εντοπισμός βάσει υπογραφών;

Είναι μια μέθοδος σάρωσης που αντιστοιχίζει κρυπτογραφικούς κατακερματισμούς αρχείων με λίστες βάσεων δεδομένων γνωστών απειλών κακόβουλου λογισμικού.

Q3: Τι είναι ένας ευρετικός σαρωτής (heuristic scanner);

Οι ευρετικές μέθοδοι αναλύουν τη δομή και τις εντολές κώδικα ενός αρχείου, επισημαίνοντας ύποπτα μοτίβα που είναι κοινά σε παραλλαγές κακόβουλου λογισμικού.

Q4: Τι σημαίνει όταν ένα αρχείο τίθεται σε καραντίνα;

Το antivirus μετακινεί το αρχείο σε έναν ασφαλή, απομονωμένο φάκελο, αποκλείοντας την εκτέλεσή του για να προστατεύσει το λειτουργικό σύστημα.

Q5: Τι είναι ένα ψευδώς θετικό αποτέλεσμα antivirus;

Είναι ένα σφάλμα όπου νόμιμο, ασφαλές λογισμικό επισημαίνεται εσφαλμένα ως κακόβουλο από τους αλγορίθμους σάρωσης.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Β)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q6: Πώς προστατεύει τα συστήματα η παρακολούθηση συμπεριφοράς;

Παρακολουθεί το λογισμικό που εκτελείται σε πραγματικό χρόνο, αποκλείοντας διεργασίες που επιχειρούν ύποπτες αλλαγές, όπως έγχυση κώδικα.

Q7: Γιατί είναι σημαντικές οι δοκιμές σε sandbox;

Το sandboxing εκτελεί μη αξιόπιστα αρχεία σε απομονωμένη εικονική μηχανή, παρατηρώντας με ασφάλεια τις ενέργειες χωρίς έκθεση του συστήματος.

Q8: Πόσο συχνά πρέπει να ενημερώνονται οι ορισμοί του antivirus;

Οι σαρωτές πρέπει να ενημερώνουν τους ορισμούς καθημερινά ή ωριαία για να αναγνωρίζουν νεοανακαλυφθέντα στελέχη κακόβουλου λογισμικού.

Q9: Ποια είναι η διαφορά μεταξύ antivirus και EDR;

Το antivirus εστιάζει στη σάρωση αρχείων, ενώ η Ανίχνευση και Απόκριση στα Τερματικά (EDR) παρέχει παρακολούθηση και περιορισμό των απειλών σε όλο το δίκτυο.

Q10: Μπορώ να εκτελώ δύο προγράμματα antivirus μαζί;

Όχι. Η λειτουργία δύο ενεργών σαρωτών προκαλεί συγκρούσεις στο σύστημα, επιβραδύνει την απόδοση και μπορεί να εμποδίζουν ο ένας τις λειτουργίες του άλλου.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q1: Πώς ελαχιστοποιούν οι ευρετικοί κανόνες την παράκαμψη απειλών;

Οι ευρετικές μέθοδοι αναλύουν γενικά μοτίβα απειλών αντί για συγκεκριμένες υπογραφές, εντοπίζοντας τροποποιημένες παραλλαγές γνωστών οικογενειών κακόβουλου λογισμικού.

Q2: Τι είναι ένας πολυμορφικός ιός;

Είναι κακόβουλο λογισμικό που αλλάζει τη διάταξη των αρχείων και τη ρουτίνα αποκρυπτογράφησής του σε κάθε εκτέλεση, καθιστώντας αναποτελεσματικές τις σαρώσεις υπογραφών.

Q3: Πώς εντοπίζουν τα sandbox την παράκαμψη εικονικών μηχανών (VM);

Τα σύγχρονα sandbox προσομοιώνουν κλικ του ποντικιού και χρόνο λειτουργίας του συστήματος, ξεγελώντας το κακόβουλο λογισμικό που έχει σχεδιαστεί να κρύβεται όταν τρέχει σε εικονικές μηχανές.

Q4: Ποιες είναι οι μορφές λήψης των ενημερώσεων υπογραφών;

Οι ενημερώσεις είναι συνήθως ελαφριά αρχεία αυξητικών δυαδικών διαφορών, που ελαχιστοποιούν την κατανάλωση εύρους ζώνης δικτύου του πελάτη.

Q5: Πώς διαχειρίζονται οι πράκτορες τερματικών (endpoint agents) τις τοπικές σαρώσεις;

Οι πράκτορες εκτελούν ελαφρείς ελέγχους παρασκηνίου, μεταθέτοντας τις βαθιές αναζητήσεις κρυπτογραφικών κατακερματισμών σε βάσεις δεδομένων απειλών στο cloud.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q6: Τι είναι η σάρωση ανίχνευσης rootkit;

Σαρώνει πίνακες μνήμης σε επίπεδο πυρήνα, παρακάμπτοντας τα API του λειτουργικού συστήματος που τα rootkit «αγκιστρώνουν» για να κρύψουν τα ενεργά νήματά τους.

Q7: Πώς αποκλείει η σάρωση συμπεριφοράς το ransomware;

Εντοπίζει αυτοματοποιημένους βρόχους μαζικής κρυπτογράφησης αρχείων, τερματίζοντας τη διεργασία του οικοδεσπότη πριν κλειδωθούν οι βάσεις δεδομένων του συστήματος.

Q8: Τι είναι η επαλήθευση πιστοποιητικού υπογραφής κώδικα;

Οι σαρωτές ελέγχουν τις ψηφιακές υπογραφές του κώδικα με αξιόπιστες αρχές πιστοποίησης ρίζας, επικυρώνοντας την ταυτότητα του προγραμματιστή του λογισμικού.

Q9: Πώς επηρεάζουν οι packers τις μηχανές σάρωσης;

Οι packers συμπιέζουν ή κρυπτογραφούν το κακόβουλο φορτίο. Οι σαρωτές πρέπει να αποσυμπιέσουν το αρχείο στη μνήμη πριν εκτελεστούν οι αντιστοιχίσεις υπογραφών.

Q10: Πώς αυτοματοποιούν την απομόνωση τα εργαλεία EDR;

Οι πράκτορες EDR θέτουν σε καραντίνα τα παραβιασμένα τερματικά σημεία σε επίπεδο δικτύου, αποκλείοντας την πλευρική κίνηση ενώ επιτρέπουν την πρόσβαση στους αναλυτές.

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για την κυβερνοασφάλεια

Εξέτασε πραγματικά στοιχεία για τις παραβιάσεις ασφαλείας, τους μηχανισμούς άμυνας και τα πρότυπα συμμόρφωσης.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι βάσεις δεδομένων υπογραφών αποθηκεύουν κατακερματισμούς γνωστού κακόβουλου λογισμικού, επομένως τα εντελώς νέα ή τροποποιημένα αρχεία διαφεύγουν μέχρι να ενημερωθούν οι ορισμοί.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι ευρετικές μηχανές μπορούν να επισημάνουν ορισμένες νέες παραλλαγές κακόβουλου λογισμικού πριν υπάρξουν υπογραφές, με το κόστος περισσότερων ψευδώς θετικών.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι ψευδώς θετικές ειδοποιήσεις κοστίζουν στις ομάδες πληροφορικής χρόνο για την επαλήθευση και την επαναφορά αρχείων που τέθηκαν λανθασμένα σε καραντίνα.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το πολυμορφικό κακόβουλο λογισμικό αλλάζει τον κώδικά του με κάθε αντίγραφο, γι' αυτό οι υπερασπιστές συνδυάζουν υπογραφές με ευρετικούς ελέγχους και ελέγχους συμπεριφοράς.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι δημιουργοί κακόβουλου λογισμικού γράφουν προσαρμοσμένους κώδικες που ελέγχουν τα περιβάλλοντα sandbox και καθυστερούν την εκτέλεση ώστε να παρακάμπτουν τους χρονομετρητές.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι μηχανές antivirus που βασίζονται στο cloud ελέγχουν τα hash ύποπτων αρχείων με μεγάλες διαδικτυακές βάσεις δεδομένων απειλών σχεδόν σε πραγματικό χρόνο.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι πάροχοι στέλνουν τακτικά ενημερώσεις ορισμών στα τερματικά ώστε οι σαρωτές να αναγνωρίζουν πρόσφατα επιβεβαιωμένες απειλές.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι μηχανισμοί παρακολούθησης συμπεριφοράς για ransomware στοχεύουν συγκεκριμένες κλήσεις Win32 API που σχετίζονται με την κρυπτογράφηση αρχείων και τη διαγραφή στιγμιοτύπων σκιάς.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι έγκυρες υπογραφές κώδικα μπορούν να μειώσουν τον κίνδυνο ψευδώς θετικών, αλλά τα υπογεγραμμένα αρχεία σαρώνονται και πάλι, καθώς και το κακόβουλο λογισμικό μπορεί να είναι υπογεγραμμένο.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα rootkit τροποποιούν τις δομές του πυρήνα του συστήματος, απαιτώντας εξειδικευμένους σαρωτές χρόνου εκκίνησης για τον εντοπισμό και τον καθαρισμό τους.

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα διαδραστικά παζλ έχουν συνταχθεί από παγκόσμια πρότυπα NIST, OWASP και συμμόρφωσης με την ιδιωτικότητα των δεδομένων. ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[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

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Ερώτηση 1** ΥΠΟΓΡΑΦΕΣ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η σάρωση υπογραφών βασίζεται σε γνωστά hash της βάσης δεδομένων και αποτυγχάνει να εντοπίσει άγνωστο ή τροποποιημένο κακόβουλο λογισμικό. Παραπομπή: OWASP Secure Configuration.

2 **Ερώτηση 2** ΕΥΡΕΤΙΚΕΣ ΜΕΘΟΔΟΙ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η ευρετική ανάλυση αναλύει τη διάταξη του κώδικα και τις εντολές για να εντοπίσει ύποπτα χαρακτηριστικά νέων παραλλαγών απειλών. Παραπομπή: Center for Internet Security (CIS).

3 **Ερώτηση 3** ΕΚΤΕΛΕΣΗ ΣΕ SANDBOX **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ένα sandbox εκτελεί ύποπτα αρχεία σε απομονωμένη εικονική μηχανή για να παρατηρεί με ασφάλεια τη συμπεριφορά εκτέλεσης. Παραπομπή: NIST Digital Identity.

4 **Ερώτηση 4** ΣΥΜΠΕΡΙΦΟΡΙΚΗ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η σάρωση συμπεριφοράς παρακολουθεί τα προγράμματα που τρέχουν σε πραγματικό χρόνο για να αποκλείει μη εξουσιοδοτημένες αλλαγές στο σύστημα. Παραπομπή: Center for Internet Security (CIS).

5 **Ερώτηση 5** ΕΝΗΜΕΡΩΣΕΙΣ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι σαρωτές κατεβάζουν καθημερινές σταδιακές ενημερώσεις ορισμών για να παραμένουν συγχρονισμένοι με το τοπίο των απειλών. Παραπομπή: OWASP Secure Configuration.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Ερώτηση 6** ΥΠΟΓΡΑΦΕΣ **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα εργαλεία υπογραφών υπολογίζουν κρυπτογραφικά hash και τα αντιστοιχίζουν με μια βάση δεδομένων γνωστών hash απειλών. Παραπομπή: OWASP Secure Configuration.

7 **Ερώτηση 7** ΕΥΡΕΤΙΚΕΣ ΜΕΘΟΔΟΙ **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι ευρετικές μηχανές εφαρμόζουν διατάξεις βάσει κανόνων που μπορεί να επισημάνουν ως ύποπτα νόμιμα, ασφαλή αρχεία. Παραπομπή: Center for Internet Security (CIS).

8 **Ερώτηση 8** ΕΚΤΕΛΕΣΗ ΣΕ SANDBOX **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ένα sandbox εκτελεί κώδικα σε εικονικό container, αποκλείοντας αυστηρά την πρόσβαση σε κοινόχρηστους πόρους δικτύου. Παραπομπή: NIST Digital Identity.

9 **Ερώτηση 9** ΣΥΜΠΕΡΙΦΟΡΙΚΗ **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η παρακολούθηση σε πραγματικό χρόνο επισημαίνει τις διεργασίες που τρέχουν και επιχειρούν παράνομες εγγραφές ή κλείδωμα αρχείων. Παραπομπή: Center for Internet Security (CIS).

10 **Ερώτηση 10** **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Κανένα antivirus δεν σταματά κάθε επίθεση zero-day· άγνωστες απειλές μπορούν να παρακάμψουν τις υπογραφές και την ευρετική ανάλυση.

Λύσεις λεξιλογίου και κριτήρια βαθμολόγησης

Κριτήρια βαθμολόγησης για τον εκπαιδευτικό: Δώσε 1 μονάδα για κάθε σωστή αντιστοίχιση (σύνολο 8 μονάδες) και για κάθε όρο περιεχομένου (σύνολο 6 μονάδες).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 4: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΕΝΝΟΙΩΝ

D 1. Υπογραφή κατακερματισμού	G 2. Ευρετικά κώδικα	E 3. Sandbox αρχείων	C 4. Σάρωση συμπεριφοράς
F 5. Καθημερινές ενημερώσεις	H 6. Ψευδώς θετικό	A 7. Απομόνωση απειλών	B 8. Εργαλείο antivirus

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΥΠΟΓΡΑΦΗ	2 ΕΥΡΙΣΤΙΚΗ	3 ΑΜΜΟΔΟΧΕΙΟ	4 ΣΥΜΠΕΡΙΦΟΡΑ
5 ΕΝΗΜΕΡΩΣΕΙΣ	6 ΨΕΥΔΩΣ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 D – ΣΥΜΠΕΡΙΦΟΡΑ	2 H – ΑΝΤΙΙΚΟ	3 E – ΕΝΗΜΕΡΩΣΕΙΣ	4 B – ΕΥΡΙΣΤΙΚΗ
5 G – ΑΠΟΜΟΝΩΣΗ	6 A – ΥΠΟΓΡΑΦΗ	7 C – ΑΜΜΟΔΟΧΕΙΟ	8 F – ΨΕΥΔΟΘΕΤΙΚΟ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

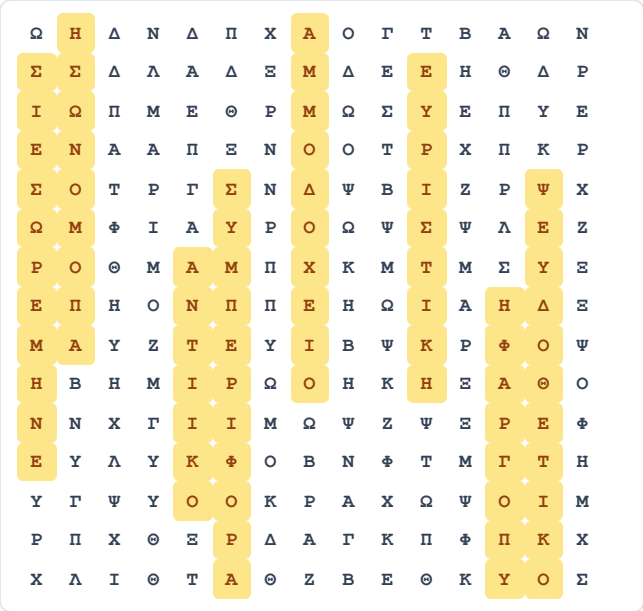
Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους Υπογραφή κατακερματισμού, Ευρετικά κώδικα και Sandbox αρχείων και να δώσουν ένα παράδειγμα για τον καθένα.

Μελέτες περίπτωσης:
Ζήτησε από τους μαθητές να στηρίζουν τις προτάσεις τους σε στοιχεία του φύλλου εργασίας και όχι σε υποθέσεις.

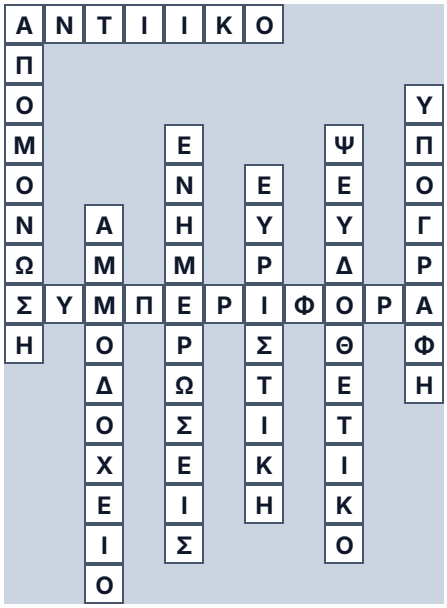
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ



ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΡΙΖΟΝΤΙΑ

1 οριζόντια: ΑΝΤΙΙΚΟ Λογισμικό που σαρώνει και προστατεύει τα τερματικά από εκμεταλλεύσεις ευπαθειών (7 γράμματα)

7 οριζόντια: ΣΥΜΠΕΡΙΦΟΡΑ Παρακολούθηση των ενεργειών του λογισμικού που εκτελείται για μοτίβα κακόβουλης λειτουργίας (11 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΑΠΟΜΟΝΩΣΗ Περιορισμός ύποπτων αρχείων ώστε να αποφεύγεται η έκθεση του τοπικού συστήματος (9 γράμματα)

2 κάθετα: ΥΠΟΓΡΑΦΗ Μοναδικό κρυπτογραφικό αποτύπωμα στη βάση δεδομένων που χρησιμοποιείται για την αναγνώριση γνωστών απειλών (8 γράμματα)

3 κάθετα: ΕΝΗΜΕΡΩΣΕΙΣ Τακτικές λήψεις ορισμών που τροφοδοτούν τη βάση δεδομένων απειλών (11 γράμματα)

4 κάθετα: ΨΕΥΔΟΘΕΤΙΚΟ Ειδοποίηση ασφαλείας που ταξινομεί λανθασμένα ένα ασφαλές λογισμικό ως κακόβουλο (11 γράμματα)

5 κάθετα: ΕΥΡΙΣΤΙΚΗ Ανάλυση βάσει κανόνων που επισημαίνει αρχεία με ύποπτη διάταξη κώδικα (9 γράμματα)

6 κάθετα: ΑΜΜΟΔΟΧΕΙΟ Ασφαλές εικονικό περιβάλλον δοκιμών που εκτελεί με ασφάλεια μη αξιόπιστο κώδικα (10 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

Κλειδί βαθμολόγησης για τη δραστηριότητα αποκωδικοποίησης λέξεων λεξιλογίου και την πρόκληση Secret Cipher.

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΦΓΡΥΑΠΗΟ — **ΥΠΟΓΡΑΦΗ**
2. ΙΟΑΜΔΟΧΕΟΜ — **ΑΜΜΟΔΟΧΕΙΟ**
3. ΕΩΡΣΗΝΙΣΕΕΜ — **ΕΝΗΜΕΡΩΣΕΙΣ**
4. ΟΗΣΜΩΝΑΠΟ — **ΑΠΟΜΟΝΩΣΗ**
5. ΙΣΥΗΤΙΕΚΡ — **ΕΥΡΙΣΤΙΚΗ**
6. ΕΑΡΦΡΟΣΥΙΜΠ — **ΣΥΜΠΕΡΙΦΟΡΑ**
7. ΤΟΨΕΕΟΙΚΥΘΔ — **ΨΕΥΔΟΘΕΤΙΚΟ**
8. ΝΙΟΑΚΙΤ — **ΑΝΤΙΙΚΟ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΑΝΙΧΝΕΥΣΕ ΝΕΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΜΕ ΕΥΡΙΣΤΙΚΗ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Σάρωση βάσει υπογραφών έναντι ευρετικής σάρωσης

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας υπάλληλος κατεβάζει ένα προσαρμοσμένο βοηθητικό πρόγραμμα που δημιουργήθηκε εσωτερικά από άλλη ομάδα. Ο σαρωτής υπογραφών το αφήνει να περάσει, αλλά ο ευρετικός σαρωτής το επισημαίνει ως ύποπτο.
- Προτεινόμενη στρατηγική και λύση: Γιατί συνέβη: Η σάρωση υπογραφών ελέγχει κατακερματισμούς αρχείων· επειδή είναι προσαρμοσμένο, δεν υπάρχει στη βάση δεδομένων απειλών. Η ευρετική ανάλυση εξετάζει τη δομή και επισήμανε ύποπτες ενέργειες (π.χ. εγγραφές στο μητρώο). Επαλήθευση: Εκτέλεσε το αρχείο σε sandbox για να παρατηρήσεις τις ενέργειες, έλεγξε τις ψηφιακές υπογραφές και υπέβαλε τον κατακερματισμό σε πύλες πληροφοριών απειλών.

B Μελέτη περίπτωσης 2: Διαχείριση ψευδώς θετικών

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας προγραμματιστής λογισμικού μεταγλωττίζει την εφαρμογή του. Το antivirus του συστήματος επισημαίνει το νέο εκτελέσιμο ως κακόβουλο λογισμικό και το θέτει σε καραντίνα.
- Προτεινόμενη στρατηγική και λύση: Κίνδυνοι λίστας επιτρεπόμενων: Η παράκαμψη των σαρωτών μπορεί να επιτρέψει την εκτέλεση πραγματικού, μολυσμένου κώδικα. Διαδρομή επίλυσης: Υπέβαλε το αρχείο στον προμηθευτή antivirus για ανάλυση, υπόγραψε ψηφιακά τον κώδικα μέσω αρχών πιστοποίησης και ρύθμισε προσωρινά εξαιρέσεις για συγκεκριμένους φακέλους αντί να απενεργοποιήσεις το antivirus.