Ενότητα 5 – Τελικό Κουίζ: Εντοπισμός Απειλών και Ανταπόκριση σε Περιστατικά

1 - Ποιος είναι ο βασικός σκοπός του εντοπισμού απειλών;

A) Να διασφαλιστεί ότι δεν θα υπάρξουν επιθέσεις
B) Να εντοπιστούν άμεσα πιθανές επιθέσεις και συμβιβασμοί
C) Να αφαιρεθεί αυτόματα κακόβουλο λογισμικό
D) Να κρυπτογραφηθούν όλα τα δεδομένα του συστήματος

2 - Ποιο από τα παρακάτω αποτελεί παράδειγμα Ενδείξεων Παραβίασης (IOC);

A) Ισχυρή πολιτική κωδικών πρόσβασης
B) Ασυνήθιστη εξερχόμενη σύνδεση προς άγνωστη διεύθυνση IP
C) Εκτέλεση προγραμματισμένου αντιγράφου ασφαλείας
D) Εγκατάσταση ενημερώσεων συστήματος

3 - Ποιο εργαλείο έχει σχεδιαστεί για τη συλλογή και ανάλυση μεγάλου όγκου αρχείων καταγραφής ασφαλείας;

A) Αναλυτής πακέτων δικτύου
B) SIEM (Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών)
C) Ανασυγκρότηση δίσκου
D) Καθαριστής μητρώου

4 - Ποιος είναι ο βασικός ρόλος ενός εργαλείου EDR (Εντοπισμός και Απόκριση Τερματικών);

A) Κρυπτογράφηση των δίσκων των τερματικών
B) Εντοπισμός, διερεύνηση και αντιμετώπιση ύποπτων δραστηριοτήτων σε τερματικές συσκευές
C) Βελτιστοποίηση χρήσης CPU
D) Αντικατάσταση των ενσωματωμένων τειχών προστασίας του λειτουργικού συστήματος

5 - Ποια είναι η βασική αρμοδιότητα ενός αναλυτή SOC;

A) Σύνταξη αλγορίθμων κρυπτογράφησης
B) Παρακολούθηση συμβάντων ασφαλείας και άμεση απόκριση σε ειδοποιήσεις
C) Ανάπτυξη νέων λειτουργικών συστημάτων
D) Σχεδίαση ασφαλών μικροκυκλωμάτων

6 - Ποια φάση περιγράφει καλύτερα τον κύκλο ζωής ενός IOC;

A) Δημιουργία → Εντοπισμός → Κοινοποίηση → Λήξη
B) Αντίγραφο ασφαλείας → Ανάκτηση → Ενημέρωση → Αφαίρεση
C) Σάρωση → Κρυπτογράφηση → Κατακερματισμός → Αποθήκευση
D) Αναγνώριση → Φραγή → Διαγραφή → Λήθη

7 - Πού εντοπίζονται συνήθως τα IOCs;

A) Εργαλεία καθαρισμού δίσκου
B) Καταγραφές συστήματος, μνήμη και δικτυακή κίνηση
C) Εφαρμογές συμπίεσης αρχείων
D) Ρυθμίσεις διαχείρισης ενέργειας

8 - Ποια από τα παρακάτω ΔΕΝ αποτελεί συνήθη πηγή δεδομένων για ένα SIEM;

A) Αρχεία καταγραφής firewall
B) Ειδοποιήσεις εντοπισμού εισβολών
C) Αρχεία ελέγχου εφαρμογών
D) Εικόνες φόντου υπολογιστή

9 - Ποιο είναι το πρώτο βήμα στον κύκλο ζωής διαχείρισης περιστατικών ασφάλειας (μοντέλο NIST);

A) Περιορισμός
B) Προετοιμασία
C) Εξάλειψη
D) Ανάκτηση

10 - Ποια ενέργεια αποτελεί μέρος της φάσης περιορισμού κατά την αντιμετώπιση περιστατικών;

A) Επαναφορά των επηρεασμένων συστημάτων σε λειτουργία
B) Απομόνωση των συσκευών που έχουν παραβιαστεί από το δίκτυο
C) Σύνταξη νέων πολιτικών ασφαλείας
D) Διεξαγωγή ανασκόπησης για τα διδάγματα που αποκτήθηκαν

11 - Γιατί θεωρείται η προετοιμασία το πιο σημαντικό βήμα στην αντιμετώπιση περιστατικών;

A) Εξασφαλίζει ότι δεν θα συμβούν ποτέ επιθέσεις
B) Μειώνει τις επιπτώσεις, καθώς υπάρχουν σαφή σχέδια και εργαλεία
C) Καταργεί την ανάγκη για ανίχνευση
D) Αποτρέπει πλήρως τις εσωτερικές απειλές

12 - Ποια από τα παρακάτω στοιχεία πρέπει να περιλαμβάνονται σε μια αναφορά περιστατικού;

A) Συνοπτική περιγραφή της απόδοσης του συστήματος
B) Χρονοδιάγραμμα του περιστατικού, επηρεαζόμενα συστήματα, ενέργειες που πραγματοποιήθηκαν και τελική επίλυση
C) Προγράμματα αδειών των εργαζομένων
D) Αντίγραφα ασφαλείας των κλειδιών κρυπτογράφησης

13 - Γιατί είναι τόσο σημαντική η τεκμηρίωση μετά από ένα περιστατικό;

A) Επιδρά αρνητικά στην απόδοση του συστήματος
B) Βοηθά στη συμμόρφωση, την υπευθυνότητα και την εκπαίδευση για μελλοντικές περιπτώσεις
C) Διευκολύνει την επανάληψη επιθέσεων
D) Αντικαθιστά την ανάγκη για ενημερώσεις λογισμικού

14 - Τι σημαίνει η αλυσίδα φύλαξης ψηφιακών αποδεικτικών στοιχείων στην ψηφιακή εγκληματολογία;

A) Ένα αρχείο που καταγράφει ποιος είχε πρόσβαση και χειρίστηκε τα αποδεικτικά στοιχεία, ώστε να διασφαλιστεί η νομική εγκυρότητα
B) Μία λίστα με όλους τους αλγόριθμους κρυπτογράφησης που χρησιμοποιήθηκαν
C) Ένα αντίγραφο ασφαλείας των εργαλείων ψηφιακής ανάλυσης
D) Η χρονολογική σειρά των επιθέσεων

15 - Ποιο από τα παρακάτω είναι ένα εργαλείο ψηφιακής εγκληματολογίας που χρησιμοποιείται συχνά σε έρευνες;

A) Wireshark
B) Photoshop
C) Εκκαθάριση Δίσκου
D) Excel

Εργαστήριο 5.1 – Ανάλυση Προσομοιωμένου Περιστατικού Ασφαλείας

16 - Κατά τον έλεγχο των αρχείων καταγραφής, ποιο από τα παρακάτω θα μπορούσε να είναι ένδειξη πιθανής παραβίασης;

A) Επιτυχής σύνδεση από ασυνήθιστη γεωγραφική τοποθεσία σε περίεργες ώρες
B) Άνοιγμα εγγράφου Word από έναν χρήστη
C) Ολοκλήρωση προγραμματισμένου αντιγράφου ασφαλείας
D) Κανονικό αίτημα DNS

17 - Ποιο είναι το πρώτο βήμα αντίδρασης μετά την επιβεβαίωση ενός περιστατικού;

A) Ανάκτηση
B) Περιορισμός
C) Εξάλειψη
D) Καταγραφή

18 - Γιατί είναι σημαντική η διατήρηση αρχείων καταγραφής και πτητικών δεδομένων;

A) Μειώνει τα προβλήματα απόδοσης του συστήματος
B) Διασφαλίζει ότι τα αποδεικτικά στοιχεία παραμένουν έγκυρα για έρευνα και νομική χρήση
C) Επιταχύνει τη λειτουργία του υλικού
D) Αντικαθιστά την ανάγκη για αντίγραφα ασφαλείας

19 - Ποιος είναι ο σκοπός της ανασκόπησης μετά από ένα περιστατικό;

A) Να αποδοθούν ευθύνες στους εργαζομένους
B) Να εντοπιστούν τα διδάγματα και να βελτιωθούν οι διαδικασίες
C) Να αντικατασταθεί το λογισμικό προστασίας από ιούς
D) Να γίνει επανεγκατάσταση του λειτουργικού συστήματος

20 - Ποιο από τα παρακάτω θεωρείται συχνό λάθος κατά την αντιμετώπιση περιστατικών;

A) Η παράλειψη καταγραφής κάθε βήματος κατά τη διαχείριση του περιστατικού
B) Η εφαρμογή στρατηγικής περιορισμού
C) Η διατήρηση της αλυσίδας φύλαξης
D) Η υλοποίηση συνόδου ανασκόπησης και συμπερασμάτων

Κλειδιά Απαντήσεων

1. **B** – Ανίχνευση = έγκαιρη αναγνώριση παραβιάσεων, όχι μόνο πρόληψη.
2. **B** – Ασυνήθιστες εξερχόμενες IP αποτελούν ισχυρούς δείκτες συμβάντων.
3. **B** – Τα SIEM συγκεντρώνουν και αναλύουν δεδομένα καταγραφών.
4. **B** – Το EDR εντοπίζει και αντιδρά στα endpoints.
5. **B** – Οι αναλυτές SOC επιτηρούν και ανταποκρίνονται σε ειδοποιήσεις.
6. **A** – Ο κύκλος ζωής IOC περιλαμβάνει δημιουργία, ανίχνευση, διαμοιρασμό, λήξη.
7. **B** – Εντοπίζονται σε αρχεία καταγραφής, μνήμη και δικτυακή κίνηση.
8. **D** – Τα wallpapers δεν αποτελούν πηγή δεδομένων για SIEM.
9. **B** – Πρώτο βήμα είναι η προετοιμασία.
10. **B** – Περιορισμός = απομόνωση των προσβεβλημένων συστημάτων.
11. **B** – Η σωστή προετοιμασία διασφαλίζει ετοιμότητα και μειώνει τον αντίκτυπο.
12. **B** – Οι αναφορές πρέπει να περιλαμβάνουν χρονολόγιο, πόρους, ενέργειες και επίλυση.
13. **B** – Η τεκμηρίωση διευκολύνει τη συμμόρφωση και τη μάθηση από τα περιστατικά.
14. **A** – Η αλυσίδα φύλαξης διασφαλίζει την ακεραιότητα των αποδεικτικών στοιχείων.
15. **A** – Το Wireshark είναι εργαλείο ανάλυσης και έρευνας.
16. **A** – Ασυνήθιστες συνδέσεις αποτελούν προειδοποιητικό σημάδι.
17. **B** – Ο περιορισμός εφαρμόζεται άμεσα μετά την επιβεβαίωση.
18. **B** – Η διατήρηση των αποδεικτικών στοιχείων διασφαλίζει την αξιοπιστία και την αποδοχή τους.
19. **B** – Οι ανασκοπήσεις μετά το συμβάν βελτιώνουν την απόκριση στο μέλλον.
20. **A** – Η ελλιπής τεκμηρίωση αποτελεί σοβαρό σφάλμα.