Εργαστήριο 5.1 – Ανάλυση Εικονικού Περιστατικού Ασφαλείας

1. Επισκόπηση Εργαστηρίου

1.1 Περιγραφή Εργαστηρίου

Σε αυτό το εργαστήριο, θα αναλάβεις τον ρόλο του **αναλυτή ασφάλειας που διαχειρίζεται ένα περιστατικό**. Μέσα από ένα προσομοιωμένο σενάριο, θα ακολουθήσεις όλα τα στάδια της **διαχείρισης περιστατικών ασφάλειας**:

- Εξέτασε ειδοποιήσεις και καταγραφές.
- Εντόπισε Δείκτες Παραβίασης (IOCs).
- Περιόρισε, εξάλειψε και ανάκτησε από την απειλή.
- Κατέγραψε τις ενέργειες και τα ευρήματά σου.
- Πραγματοποίησε ανασκόπηση μετά το περιστατικό και εντόπισε τα διδάγματα που προέκυψαν.

Αυτή η άσκηση συνδυάζει τεχνικές δεξιότητες (ανάλυση καταγραφών, ενέργειες απόκρισης) με **κριτική σκέψη και οργανωμένη αναφορά** — ακριβώς όπως λειτουργούν οι επαγγελματικές ομάδες κυβερνοασφάλειας στην αντιμετώπιση επιθέσεων.

1.2 Εκπαιδευτικοί Στόχοι

Μετά την ολοκλήρωση του εργαστηρίου, θα μπορείτε να:

- Αναλύετε καταγραφές για τον εντοπισμό ύποπτων ενεργειών και την επιβεβαίωση περιστατικών.
- Αναγνωρίζετε και καταγράφετε **Δείκτες Παραβίασης (IOCs)**.
- Εφαρμόζετε το μοντέλο απόκρισης **Περιορισμός → Εξάλειψη → Ανάκτηση** .
- Διατηρείτε αποδεικτικά στοιχεία εξασφαλίζοντας τη **συνέχεια της αλυσίδας φύλαξης**.
- Συμπληρώνετε μια **αναφορά απόκρισης σε περιστατικό** (χρονολόγιο, συστήματα, λογαριασμοί, ενέργειες).
- Πραγματοποιείτε **ανασκόπηση μετά το περιστατικό** και προτείνετε βελτιώσεις στην ανίχνευση, τις πολιτικές και την εκπαίδευση.

1.3 Προϋποθέσεις

Πριν ξεκινήσετε το εργαστήριο, θα πρέπει:

- Να έχετε κατανοήσει τα βασικά του **κύκλου ζωής απόκρισης σε συμβάντα** (NIST ή παρόμοιο πρότυπο).

- Νιώστε άνετα να ελέγχετε τα αρχεία καταγραφής συστήματος και να εντοπίζετε ασυνήθιστα μοτίβα.
- Βεβαιωθείτε ότι έχετε στη διάθεσή σας:
    - Ένα **σύνολο δεδομένων αρχείων καταγραφής** (παρέχεται στα υλικά του μαθήματος ή με οδηγίες από τον εκπαιδευτή).
    - Έναν επεξεργαστή κειμένου ή ένα υπολογιστικό φύλλο για να οργανώσετε τα ευρήματά σας.
    - Ένα **πρότυπο αντιμετώπισης περιστατικών** (χρονοδιάγραμμα, ενέργειες, επόμενα βήματα).

Προαιρετικά αλλά συνιστάται: εξοικείωση με βασικές έννοιες SIEM και πρακτικές ψηφιακής ανάλυσης.

1.4 Εκτιμώμενος Χρόνος Ολοκλήρωσης

Δραστηριότητα	**Εκτιμώμενος Χρόνος**
Εισαγωγή σεναρίου & επισκόπηση ειδοποιήσεων	30 λεπτά
Ανάλυση καταγραφών & αναγνώριση IOCs	45 λεπτά
Βήματα αντιμετώπισης περιστατικού	60 λεπτά
Τεκμηρίωση & διαχείριση αποδεικτικών στοιχείων	45 λεπτά
Ανασκόπηση περιστατικού και αποκομισθέντα διδάγματα	30–45 λεπτά
Κλείσιμο και αναστοχασμός	15 λεπτά
Συνολικός Εκτιμώμενος Χρόνος	**~4–4,5 ώρες**

Σημείο Ελέγχου

Πριν προχωρήσετε, βεβαιωθείτε ότι:

- Κατανοείτε το σκοπό της προσομοίωσης (εξάσκηση στη διαχείριση περιστατικού από την αρχή ως το τέλος).
- Έχετε έτοιμα τα αρχεία καταγραφής, το πρότυπο και τα εργαλεία σημειώσεων.
- Μπορείτε να αφιερώσετε περίπου **4–4,5 ώρες** για να ολοκληρώσετε το εργαστήριο πλήρως.

2. Στήσιμο Σεναρίου – Η Αρχική Ειδοποίηση

2.1 Ιστορικό

Είναι περασμένα μεσάνυχτα — **2:41 π.μ.** — όταν το σύστημα της εταιρείας σας για **Διαχείριση Πληροφοριών Ασφαλείας**
και Συμβάντων (SIEM) εκδίδει μια ειδοποίηση. Ως ο αναλυτής που βρίσκεται σε ετοιμότητα, πρέπει να αποφασίσετε αν πρόκειται για:

- Μια αθώα ανωμαλία, ή
- Ένα πραγματικό **περιστατικό ασφάλειας σε εξέλιξη**;

2.2 Λεπτομέρειες ειδοποίησης

Η ειδοποίηση από το SIEM περιλαμβάνει τα εξής ύποπτα στοιχεία:

- **Δραστηριότητα σύνδεσης**: Επιτυχής σύνδεση από τη διεύθυνση IP 203.0.113.41.
- **Λογαριασμός χρήστη**: Η σύνδεση πραγματοποιήθηκε με τον **dbadmin** λογαριασμό, ο οποίος συνήθως χρησιμοποιείται μόνο εντός ωραρίου.
- **Ώρα σύνδεσης**: **2:41 π.μ.**, εντελώς εκτός συνηθισμένων προτύπων χρήσης.
- **Επόμενη δραστηριότητα**: Ξαφνική αύξηση σε **εκροή δικτυακής κυκλοφορίας** από τον διακομιστή HR της εταιρείας προς εξωτερικό FTP server.

2.3 Ο Ρόλος σας

Αναλαμβάνετε τη θέση του **Υπεύθυνου Αντιμετώπισης Περιστατικών**. Οι αρμοδιότητές σας είναι οι εξής:

1. **Εξετάστε προσεκτικά την ειδοποίηση** .
2. **Συλλέξτε επιπλέον αποδεικτικά στοιχεία** από τα αρχεία καταγραφής και τη δικτυακή δραστηριότητα.
3. **Αποφασίστε** αν πρόκειται για ψευδώς θετικό συμβάν ή για πραγματικό περιστατικό.
4. **Δράστε** όποτε χρειάζεται.

Συμβουλή: Μην βγάζετε βιαστικά συμπεράσματα μόνο από την ειδοποίηση — αντιμετωπίστε την ως αφετηρία για περαιτέρω διερεύνηση.

2.4 Στόχοι Έρευνας

Σε αυτό το στάδιο, οι στόχοι σας είναι οι εξής:

- Επαληθεύστε αν η σύνδεση ήταν νόμιμη.
- Εξετάστε αν η εξαγωγή δεδομένων ήταν **εξουσιοδοτημένη** ή **κακόβουλη**.
- Εντοπίστε τυχόν αρχικά **σημάδια παραβίασης (IOCs)** για πιο ενδελεχή έρευνα στα επόμενα βήματα.

Σημείο Ελέγχου

Πριν προχωρήσετε:

- Έχετε κατανοήσει τις λεπτομέρειες του αρχικού ειδοποιητηρίου (ώρα, λογαριασμός, IP, μεταφορά δεδομένων);
- Έχετε κάποιον τρόπο να κρατήσετε σημειώσεις όσο εξετάζετε τα logs και δημιουργείτε το χρονολόγιό σας;
- Είστε έτοιμοι να ξεκινήσετε **τον έλεγχο των logs και την αναγνώριση IOCs**;

3. Έλεγχος Καταγραφών και Εντοπισμός Δεικτών Συμβάντων (IOC)

3.1 Ανασκόπηση Καταγραφών Ταυτοποίησης

Το πρώτο σας βήμα είναι να εξετάσετε τις **καταγραφές ταυτοποίησης** για λεπτομέρειες σχετικά με τη ύποπτη είσοδο.

Στις καταγραφές εμφανίζονται:

```
2025-09-21 02:41:06 ΕΠΙΤΥΧΗΣ ΕΙΣΟΔΟΣ χρήστης=dbadmin ip=203.0.113.41

2025-09-21 09:15:42 ΕΠΙΤΥΧΗΣ ΕΙΣΟΔΟΣ χρήστης=dbadmin ip=10.0.2.15

2025-09-20 14:05:33 ΕΠΙΤΥΧΗΣ ΕΙΣΟΔΟΣ χρήστης=dbadmin ip=10.0.2.15
```

Παρατηρήσεις:

- Η **σύνδεση στις 2:41 π.μ.** ξεχωρίζει ως ασυνήθιστη.
- Οι προηγούμενες συνδέσεις πραγματοποιήθηκαν από μια **εσωτερική διεύθυνση IP (10.0.2.15)** κατά τη διάρκεια των εργάσιμων ωρών.
- Η ύποπτη σύνδεση προήλθε από **εξωτερική διεύθυνση IP εξωτερικού (203.0.113.41)**.

3.2 Καταγραφές Πρόσβασης Αρχείων

Στη συνέχεια, ελέγχετε τα αρχεία καταγραφής πρόσβασης στο HR database server.

```
2025-09-21 02:43:11 FILE ACCESS user=dbadmin /HR/employee_records.xlsx

2025-09-21 02:44:27 FILE ACCESS user=dbadmin /HR/salary_data.csv

2025-09-21 02:45:03 FILE ACCESS user=dbadmin /HR/benefits.docx
```

Παρατηρήσεις:

- Άμεσα μετά τη μη αναμενόμενη είσοδο, υπήρξε πρόσβαση σε ευαίσθητα αρχεία του τμήματος Ανθρώπινου Δυναμικού.
- Αυτά τα αρχεία συνήθως ανοίγονται μόνο κατά την περίοδο εκκαθάρισης μισθοδοσίας κάθε μήνα.

3.3 Καταγραφές Δραστηριότητας Δικτύου

Τέλος, προχωράτε στον έλεγχο των καταγραφών κίνησης δικτύου.

```
2025-09-21 02:46:10 ΕΞΕΡΧΟΜΕΝΗ ΜΕΤΑΦΟΡΑ χρήστης=dbadmin διακομιστής=203.0.113.50 πρωτόκολλο=FTP μέγεθος=1.2GB 2025-09-21

02:49:55 ΕΞΕΡΧΟΜΕΝΗ ΜΕΤΑΦΟΡΑ χρήστης=dbadmin διακομιστής=203.0.113.50 πρωτόκολλο=FTP μέγεθος=850MB
```

Παρατηρήσεις:

- Μεγάλος όγκος δεδομένων μεταφέρθηκε εκτός δικτύου σε **εξωτερικό FTP server**.
- Η συνήθης κίνηση της βάσης δεδομένων γίνεται μέσω **SQL στην θύρα 1433** και όχι μέσω FTP.

3.4 Εντοπισμός Δεικτών Παραβίασης (IOCs)

Από την ανάλυση των καταγραφών σας, εντοπίσατε τους παρακάτω δείκτες παραβίασης:

- **Ύποπτη διεύθυνση IP**: 203.0.113.41 (πηγή σύνδεσης).
- **Ασυνήθιστη ώρα σύνδεσης**: 2:41 π.μ.
- **Χρησιμοποιήθηκε λογαριασμός**: dbadmin (πιθανή παραβίαση).
- **Πρόσβαση σε ευαίσθητα αρχεία**: αρχεία HR και δεδομένα μισθοδοσίας.
- **Εξερχόμενη κίνηση**: Μεγάλη μεταφορά αρχείων μέσω FTP προς 203.0.113.50.

3.5 Επιβεβαίωση του περιστατικού

Σε αυτό το σημείο, τα στοιχεία δείχνουν ότι πρόκειται για **επιβεβαιωμένο περιστατικό**:

- Εξωτερική σύνδεση από ασυνήθιστη IP → **Μη εξουσιοδοτημένη πρόσβαση**.
- Πρόσβαση σε αρχεία HR → **Ευαίσθητες πληροφορίες σε κίνδυνο**.
- Μεγάλες εξερχόμενες μεταφορές FTP → **Επιβεβαιωμένη εξαγωγή δεδομένων**.

Συμπέρασμα: Αυτή η περίπτωση **δεν είναι ψευδώς θετική** — πρέπει άμεσα να ξεκινήσουν ενέργειες περιορισμού.

Σημείο Ελέγχου

Πριν συνεχίσετε:

- Εντοπίσατε τουλάχιστον **τρεις δείκτες παραβίασης** στα αρχεία καταγραφής;
- Καταλαβαίνετε γιατί πρόκειται για επιβεβαιωμένη παραβίαση;
- Είστε έτοιμοι να προχωρήσετε σε **ενέργειες αντιμετώπισης περιστατικού**;

4. Ενέργειες Αντιμετώπισης Περιστατικών

4.1 Περιορισμός

Η πρώτη προτεραιότητα είναι να **διακοπεί άμεσα η επίθεση**.

Ενέργειες που πρέπει να γίνουν άμεσα:

1. **Απενεργοποιήστε τον παραβιασμένο λογαριασμό** (dbadmin).
2. **Απομονώστε τον επηρεασμένο διακομιστή** από το δίκτυο για να αποτραπεί περαιτέρω διαρροή δεδομένων.
3. Ενημερώστε τον **επικεφαλής της Ομάδας Αντιμετώπισης Περιστατικών (IR)** και ακολουθήστε τη διαδικασία κλιμάκωσης σύμφωνα με την πολιτική.

Στόχος: Να περιοριστεί η απειλή πριν εξαπλωθεί περαιτέρω.

4.2 Εξάλειψη

Όταν η απειλή περιοριστεί, η προσοχή στρέφεται στην **απομάκρυνση της παρουσίας του εισβολέα**.

Τα βήματα περιλαμβάνουν:

- Ελέγξτε το επηρεασμένο σύστημα για **κακόβουλο λογισμικό, rootkits ή backdoors**.
- Αφαιρέστε όλα τα κακόβουλα αρχεία ή μη εξουσιοδοτημένες προγραμματισμένες εργασίες.
- Εξετάστε για **δευτερεύοντες παραβιασμένους λογαριασμούς** που μπορεί να έχουν δημιουργηθεί από τον εισβολέα.

Στόχος: Να διασφαλιστεί ότι ο εισβολέας δεν έχει πλέον πρόσβαση.

4.3 Ανάκτηση

Αφού εξαλειφθεί η απειλή, προχωρήστε στην **αποκατάσταση της κανονικής λειτουργίας**:

1. Επαναφέρετε το παραβιασμένο σύστημα από ένα **αξιόπιστο καθαρό αντίγραφο ασφαλείας**.
2. Εφαρμόστε **ενημερώσεις ασφαλείας** και ανανεώστε τις ρυθμίσεις πριν το επαναφέρετε στο δίκτυο.
3. Παρακολουθήστε στενά το σύστημα για ενδείξεις επαναλαμβανόμενης κακόβουλης δραστηριότητας.

Στόχος: Να επιστρέψει η επιχείρηση σε κανονικούς ρυθμούς με ενισχυμένα μέτρα προστασίας.

4.4 Καταγραφή Ενεργειών Ανταπόκρισης

Καθώς προχωράτε από Περιορισμό → Εξάλειψη → Ανάκαμψη:

- Καταγράψτε **την ημερομηνία και ώρα** κάθε ενέργειας.
- Σημειώστε **ποιος εκτέλεσε την ενέργεια**.
- Βεβαιωθείτε ότι οι ενέργειες έχουν καταχωρηθεί στην επίσημη **αναφορά ανταπόκρισης περιστατικού**.

Αυτή η τεκμηρίωση είναι απαραίτητη για τη συμμόρφωση, την αναφορά και τη συλλογή γνώσης.

Σημείο ελέγχου

Πριν συνεχίσετε:

- Κατέγραψες και τις τρεις φάσεις (Περιορισμός → Εξάλειψη → Ανάκαμψη);
- Έχεις ξεκινήσει να σημειώνεις κάθε ενέργεια με χρόνο και λεπτομέρειες;
- Γνωρίζεις γιατί η παρακολούθηση είναι απαραίτητη στη φάση της ανάκαμψης;

5. Τεκμηρίωση και Διαχείριση Αποδεικτικών Στοιχείων

5.1 Γιατί Είναι Σημαντική η Τεκμηρίωση

Κάθε ενέργεια κατά τη διάρκεια ενός περιστατικού πρέπει να **καταγράφεται και να φέρει χρονοσφραγίδα**.

- Διαμορφώνει ένα **σαφές χρονολόγιο** γεγονότων και χρόνων.
- Παρέχει αποδεικτικά στοιχεία για **αποτίμηση μετά το συμβάν** και νομικούς ελέγχους.
- Εξασφαλίζει συμμόρφωση με **πολιτικές και πρότυπα του οργανισμού** (π.χ., ISO 27001, NIST, GDPR).

5.2 Διαφύλαξη Καταγραφών

Τα αρχεία καταγραφής αποτελούν το βασικό σας αποδεικτικό υλικό. Φροντίστε να τα ασφαλίσετε πριν διαγραφούν ή αντικατασταθούν.

- Εξάγετε τα αρχεία ειδοποιήσεων του SIEM.
- Αντιγράψτε τα αρχεία καταγραφής ταυτοποίησης συστήματος.
- Αποθηκεύστε τα αρχεία καταγραφής κίνησης δικτύου.
- Βεβαιωθείτε ότι τα αντίγραφα ασφαλείας διατηρούνται σε **τοποθεσία μόνο για ανάγνωση**.

Συμβουλή: Διατηρείτε πάντα **το αρχικό αντίγραφο ανέπαφο** — εργάζεστε μόνο με αντίγραφα.

5.3 Συλλογή Πτητικών Δεδομένων

Ορισμένα αποδεικτικά στοιχεία χάνονται γρήγορα αν δεν καταγραφούν άμεσα.

- Αποτύπωση της μνήμης του παραβιασμένου διακομιστή (περιεχόμενα RAM).
- Καταγραφή των ενεργών διεργασιών και των τρεχουσών συνδέσεων δικτύου.
- Λήψη στιγμιότυπων οθόνης ύποπτων συνεδριών.

5.4 Αλυσίδα Διαφύλαξης Αποδεικτικών Στοιχείων

Για να διατηρηθεί η ακεραιότητα, ακολουθήστε τη **διαδικασία αλυσίδας διαφύλαξης** των αποδεικτικών στοιχείων:

1. Καταγράψτε **ποιος συνέλεξε τα αποδεικτικά στοιχεία**, **πότε** και **με ποιον τρόπο**.

2. Αποθηκεύστε τα αποδεικτικά στοιχεία με ασφάλεια (π.χ. σε κρυπτογραφημένο δίσκο ή ειδικό θησαυροφυλάκιο).

3. Καταγράψτε κάθε μεταβίβαση όταν τα αποδεικτικά στοιχεία αλλάζουν χέρια.

Με αυτόν τον τρόπο διασφαλίζεται ότι τα αποδεικτικά στοιχεία είναι **νομικά έγκυρα** και προστατευμένα από παραποίηση.

5.5 Ολοκλήρωση της Αναφοράς Περιστατικού

Το πρότυπο ανταπόκρισης σε περιστατικά θα πρέπει να περιλαμβάνει:

- **Χρονολόγιο συμβάντων** (ενημέρωση, εντοπισμός, αντιμετώπιση).
- **Επηρεασμένα συστήματα**.
- **Εμπλεκόμενοι λογαριασμοί**.
- **Ενέργειες που πραγματοποιήθηκαν**.
- **Εκκρεμείς επόμενες κινήσεις**.

Σημείο Ελέγχου

Πριν προχωρήσετε:

- Έχετε εξάγει και διασφαλίσει όλα τα σχετικά αρχεία καταγραφής;
- Συλλέξατε οποιαδήποτε πτητικά στοιχεία πριν χαθούν;
- Καταγράψατε τις ενέργειές σας στην αναφορά περιστατικού με χρονικές σημάνσεις;
- Διατηρήσατε την αλυσίδα φύλαξης για οποιοδήποτε κρίσιμο αποδεικτικό υλικό;

6. Ανασκόπηση Μετά το Περιστατικό και Συμπεράσματα

6.1 Η Σημασία της Ανασκόπησης Μετά το Περιστατικό

Η επίλυση ενός περιστατικού δεν είναι το τέλος — είναι η **αφετηρία για βελτίωση**. Μια οργανωμένη ανασκόπηση διασφαλίζει ότι:

- Εντοπίζονται οι πραγματικές αιτίες.
- Οι κανόνες ανίχνευσης ανανεώνονται.
- Οι ομάδες μαθαίνουν από τα λάθη και τις επιτυχίες τους.
- Ο οργανισμός ενισχύει την ανθεκτικότητά του.

6.2 Επισκόπηση Συμπερασμάτων

Μετά τον περιορισμό και την αποκατάσταση, συγκεντρώστε την ομάδα διαχείρισης περιστατικών για να εξετάσετε:

- **Χρονολόγιο γεγονότων** (ειδοποίηση → διερεύνηση → περιορισμός → αποκατάσταση).
- **Ταχύτητα ανταπόκρισης της ομάδας**.
- **Ποια σημεία λειτούργησαν σωστά** (π.χ. άμεση ανίχνευση, σωστή κλιμάκωση).
- **Πού υπήρξαν αδυναμίες** (π.χ. ανεπαρκής παρακολούθηση, καθυστερημένη επικοινωνία).

Καταγράψτε αυτά τα συμπεράσματα στην επίσημη αναφορά.

6.3 Βελτιώσεις προς Εφαρμογή

Με βάση τα συμπεράσματά σας, προχωρήστε σε ενέργειες για την ενίσχυση της ασφάλειας:

- **Κανόνες ανίχνευσης** → Ενημερώστε το SIEM ώστε να εντοπίζει ασυνήθιστες ώρες συνδέσεων ή μεταφορές μέσω FTP.
- **Τείχη προστασίας** → Αποκλείστε ύποπτες διευθύνσεις IP και περιορίστε την εξερχόμενη κίνηση FTP.
- **Εκπαίδευση χρηστών** → Οργανώστε ενημερωτικές συνεδρίες για ορθή διαχείριση λογαριασμών και αναφορά ύποπτων ενεργειών.
- **Εγχειρίδια αντιμετώπισης περιστατικών** → Ενσωματώστε αυτό το σενάριο στα runbooks σας για ταχύτερη αντίδραση στο μέλλον.

6.4 Εκπαίδευση της Ομάδας

Η ανασκόπηση μετά από ένα περιστατικό είναι ταυτόχρονα και μια **ευκαιρία για μάθηση**:

- Μοιραστείτε τα διδάγματα με τις ομάδες IT, ασφάλειας και διοίκησης.
- Πραγματοποιήστε μια **άσκηση προσομοίωσης** για να εξασκηθείτε στο ίδιο σενάριο.
- Ενημερώστε τη διαδικασία ένταξης νέων μελών με όσα διδαχθήκατε από αυτό το περιστατικό.

Κάθε περιστατικό είναι μια ευκαιρία να ενισχύσετε τις δεξιότητες της ομάδας.

6.5 Παραδείγματα Διδάγματων (Από αυτό το σενάριο εργαστηρίου)

- Η κοινή χρήση διαχειριστικών λογαριασμών (dbadmin) ενέχει κίνδυνο → Εφαρμόστε πολιτική ελάχιστων δικαιωμάτων και παρακολούθηση.
- Η εξερχόμενη FTP κίνηση πρέπει να είναι **υπό παρακολούθηση ή περιορισμό**.
- Οι συνδέσεις εκτός ωραρίου πρέπει να ενεργοποιούν **προειδοποιήσεις αυτόματα**.
- Η τεκμηρίωση των περιστατικών οφείλει να είναι τυποποιημένη και να αναθεωρείται συστηματικά.

Σημείο Ελέγχου

Πριν συνεχίσετε:

- Καταγράψατε τι λειτούργησε και τι όχι σε αυτό το περιστατικό;
- Προτείνατε τουλάχιστον **δύο βελτιώσεις** σε εργαλεία, πολιτικές ή εκπαίδευση;
- Σημειώσατε τα διδάγματα για μελλοντικά περιστατικά και τα μοιραστήκατε με την ομάδα σας;

7. Συνοψίζοντας

7.1 Βασικά Σημεία

Σε αυτό το εργαστήριο ολοκληρώσατε μια **προσομοιωμένη άσκηση διαχείρισης περιστατικού** που σας οδήγησε σε όλα τα στάδια της ανταπόκρισης στον κυβερνοχώρο. Ειδικότερα:

Εξετάσατε μια ειδοποίηση από το SIEM.

Εντοπίσατε Δείκτες Παραβίασης (IOCs) σε αρχεία καταγραφής και δικτυακά δεδομένα.

Εφαρμόσατε το πλαίσιο ανταπόκρισης **Περιορισμός → Εξάλειψη → Ανάκτηση** .

Διατηρήσατε τα αποδεικτικά στοιχεία και εξασφαλίσατε σωστή διαχείριση της αλυσίδας φύλαξης.

Καταγράψατε τη χρονική σειρά του περιστατικού και τις ενέργειες σε επίσημη αναφορά.

Πραγματοποιήσατε αξιολόγηση μετά το συμβάν και εντοπίσατε πολύτιμα διδάγματα.

7.2 Δεξιότητες που αποκτήσατε

Ολοκληρώνοντας αυτό το εργαστήριο, πλέον μπορείτε να:

- Αναλύετε αρχεία καταγραφής για να επιβεβαιώνετε ή να απορρίπτετε ύποπτες δραστηριότητες.
- Ανταποκρίνεστε οργανωμένα σε περιστατικά εφαρμόζοντας βέλτιστες πρακτικές.
- Συντάσσετε επαγγελματικές **αναφορές περιστατικών** με χρονολογική σειρά, ενέργειες και αποδεικτικά στοιχεία.
- Προτείνετε ουσιαστικές **βελτιώσεις** στην ανίχνευση, την ανταπόκριση και την εκπαίδευση των χρηστών.

7.3 Επόμενο Βήμα: Τελικό Κουίζ Ενότητας 5

Ολοκληρώσατε με επιτυχία το **πρακτικό εργαστήριο αποκορύφωσης της Ενότητας 5: Ανίχνευση Απειλών και Αντιμετώπιση Περιστατικών**.

Το επόμενο βήμα είναι να συμμετάσχετε στο **Τελικό Κουίζ Ενότητας 5**, το οποίο περιλαμβάνει:

- Έννοιες ανίχνευσης απειλών (ειδοποιήσεις, IOCs, βασικά στοιχεία SIEM).
- Κύκλος ζωής αντιμετώπισης περιστατικών (Περιορισμός, Εξάλειψη, Αποκατάσταση).
- Διαχείριση αποδεικτικών στοιχείων και αλυσίδα φύλαξης.
- Επανεξέταση του περιστατικού και συνεχής βελτίωση.

Τελικό Σημείο Ελέγχου

Πριν προχωρήσετε στο κουίζ:

- Έχετε ολοκληρώσει και αποθηκεύσει την αναφορά σας για την αντιμετώπιση του περιστατικού;
- Μπορείτε να εξηγήσετε με σαφήνεια τι οδήγησε το περιστατικό στο να χαρακτηριστεί ως **επιβεβαιωμένη παραβίαση**;
- Μπορείτε να συνοψίσετε **τρεις βασικές γνώσεις** που αποκομίσατε από αυτό το εργαστήριο;

Αν ναι — είστε έτοιμοι για το κουίζ!

8. Παράρτημα

8.1 Υπόδειγμα Φόρμας Αντιμετώπισης Περιστατικού

Χρησιμοποιήστε αυτό το υπόδειγμα για να οργανώσετε την καταγραφή ενός περιστατικού:

Πεδίο	**Λεπτομέρειες**
Κωδικός Περιστατικού	[Μοναδικός αναγνωριστικός αριθμός]
Ημερομηνία/Ώρα Εντοπισμού	[π.χ., 2025-09-21 02:41 π.μ.]
Αναφορά από	[SIEM / Αναλυτής / Χρήστης]
Επηρεαζόμενα Συστήματα	[Διακομιστής βάσης δεδομένων, αρχεία HR]
Εμπλεκόμενοι Λογαριασμοί	[dbadmin]
Δείκτες Παραβίασης (IOCs)	[Υποπτες διευθύνσεις IP, ασυνήθιστες συνδέσεις, μεταφορές μέσω FTP]
Ενέργειες Περιορισμού	[Απενεργοποίηση λογαριασμού, απομόνωση διακομιστή]
Ενέργειες Εξάλειψης	[Έλεγχος για κακόβουλο λογισμικό, αφαίρεση backdoors]
Ενέργειες Ανάκτησης	[Επαναφορά από καθαρό αντίγραφο ασφαλείας]
Συλλεχθέντα στοιχεία	[Αρχεία καταγραφής, απόσπασμα μνήμης, έντυπο αλυσίδας φύλαξης]
Επόμενα βήματα	[Αποκλεισμός διευθύνσεων IP, ενημέρωση κανόνων SIEM, εκπαίδευση χρηστών]
Κατάσταση	[Σε εξέλιξη / Ολοκληρώθηκε]

8.2 Λίστα Αναφοράς Δεικτών Παραβίασης (IOC)

Συνήθεις κατηγορίες IOC για παρακολούθηση:

- **Αρχεία σύνδεσης** → Ασυνήθιστες ώρες εισόδου, ξένες διευθύνσεις IP, επαναλαμβανόμενες αποτυχίες που ακολουθούνται από επιτυχή είσοδο.
- **Δραστηριότητα αρχείων** → Ασυνήθιστη πρόσβαση σε ευαίσθητους φακέλους, μεγάλες μεταφορές αρχείων.
- **Δικτυακή κίνηση** → Εξερχόμενες συνδέσεις σε άγνωστες διευθύνσεις IP, ασυνήθιστα πρωτόκολλα (π.χ. FTP αντί για HTTPS).

- **Δραστηριότητα διεργασιών** → Απροσδόκητες υπηρεσίες, προγραμματισμένες εργασίες ή εκτέλεση εντολών.

Συμβουλή: Πάντα να διασταυρώνετε τα IOCs με **αξιόπιστες πηγές ανάλυσης απειλών** για επιβεβαίωση.

8.3 Συνήθη λάθη στην απόκριση περιστατικών

- **Άμεση μετάβαση σε περιορισμό** χωρίς πρώτα να επιβεβαιωθεί το περιστατικό.
- **Παράλειψη καταγραφής ενεργειών** τη στιγμή που εκτελούνται.
- **Μη διατήρηση πτητικών αποδεικτικών στοιχείων** (RAM, ενεργές συνδέσεις).
- **Αγνόηση της αλυσίδας διαχείρισης αποδεικτικών στοιχείων** — κάτι που μπορεί να ακυρώσει τη χρήση των στοιχείων σε νομικό πλαίσιο.
- **Παράλειψη αξιολόγησης μετά το περιστατικό**, χάνοντας έτσι ευκαιρίες ενίσχυσης της ασφάλειας.

8.4 Πρόσθετη Βιβλιογραφία & Πηγές

- **Οδηγός Διαχείρισης Περιστατικών Ασφάλειας Υπολογιστικών Συστημάτων NIST (SP 800-61r2)** https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- **SANS Εγχειρίδιο Διαχείρισης Περιστατικών** https://www.sans.org/white-papers/33901/
- **FIRST (Forum Απάντησης σε Περιστατικά και Ομάδων Ασφάλειας)** Βέλτιστες Πρακτικές https://www.first.org/
- **Πλαίσιο MITRE ATT&CK** – Για χαρτογράφηση τεχνικών και συμπεριφορών επιτιθέμενων https://attack.mitre.org/

Προτεινόμενη Βιβλιογραφία: *Αντιμετώπιση Περιστατικών & Ψηφιακή Εγκληματολογία* (Luttgens, Pepe, Mandia).