ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Πληροφορικής

Εικόνα που περιέχει ορθογώνιο παραλληλόγραμμο, σχεδίαση

Το περιεχόμενο που δημιουργείται από τεχνολογία AI ενδέχεται να είναι εσφαλμένο.

Εργασία Μαθήματος ***Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων***

|  |  |
| --- | --- |
| Αρ. Άσκησης - Τίτλος Άσκησης | ***Ανάλυση και Διαχείριση Επικινδυνότητας*** |
| Όνομα φοιτητή - Αρ. Μητρώου  (όλων σε περίπτωση ομαδικής εργασίας) | Γιαννίκος Παναγιώτης – ΜΠΚΕΔ24007 |
| Μπαλτζής Δημήτρης – ΜΠΚΕΔ24026 |
| Ραυτόπουλος Μάριος – ΜΠΚΕΔ24034 |
| Ημερομηνία παράδοσης | 25/02/25 |

**Εργασία B: Ανάλυσης και Διαχείρισης Επικινδυνότητας**

Περιγραφή:

Επιλέξτε ένα οργανισμό/εταιρεία/φορέα που φιλοξενεί πληροφοριακό σύστημα ή περιγράψτε τα πληροφοριακά αγαθά που εμπλέκονται στην παροχή μιας Υπηρεσίας Εφοδιαστικής Αλυσίδας  και πραγματοποιήστε:

1. Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας η οποία θα πρέπει να περιλαμβάνει:
   * Περιγραφή της Μεθοδολογίας
   * Περιγραφή του Οργανισμού/ Εταιρίας/ Φορέα / Εφοδιαστικής Υπηρεσίας
   * Απαιτήσεις Ασφάλειας - Νομικές Απαιτήσεις
   * Χαρτογράφηση ΠΣ / αγαθών (Cartography)
   * Αποτίμηση Επιπτώσεων (Impact Assessment)
   * Αποτίμηση Απειλών (Threat Assessment)
   * Αποτίμηση Αδυναμιών (Vulnerability Assessment)
   * Αποτίμηση Κινδύνων (Risk Analysis)
   * Προτεινόμενα Μέτρα Προστασίας (Proposed Security Countermeasures)
   * Σχέδιο Υλοποίησης Μέτρων Προστασίας (Risk Treatment Plan)
2. Κατανομή οργανωτικών δομών και αρμοδιοτήτων ασφάλειας (Security Roles and Responsibilities)
3. Βασικές Πολιτικές Ασφάλειας (Access Control Policy, Password Policy, Logging Policy, Backup Policy)
4. Βασικές Διαδικασίες (Διαδικασία αντιμετώπισης περιστατικών ασφάλειας, Διαδικασία Backup, Διαδικασία Δημιουργίας / Διαγραφής Χρήστη)

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

[1. Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας 4](#_Toc189833661)

[1.1 Περιγραφή της Μεθοδολογίας 4](#_Toc189833662)

[1.2 Περιγραφή του Οργανισμού/ Εταιρίας/ Φορέα / Εφοδιαστικής Υπηρεσίας 5](#_Toc189833663)

[1.3 Απαιτήσεις Ασφαλείας & Νομικές Απαιτήσεις για την Υπηρεσία SOC 6](#_Toc189833664)

[1.5 Χαρτογράφηση Αγαθών 7](#_Toc189833665)

[1.6 Αποτίμηση Επιπτώσεων (Impact Assessment) 11](#_Toc189833666)

[1.7 Αποτίμηση Απειλών (Threat Assessment) 11](#_Toc189833667)

[1.8 Αποτίμηση Αδυναμιών 11](#_Toc189833668)

[1.9 Αποτίμηση Κινδύνων (Risk Assessment) 12](#_Toc189833669)

[1.10 Προτεινόμενα Μέτρα Προστασίας (Proposed Security Countermeasures) 12](#_Toc189833670)

[1.11 Σχέδιο Υλοποίησης Μέτρων Προστασίας 13](#_Toc189833671)

[2. Κατανομή οργανωτικών δομών και αρμοδιοτήτων ασφάλειας (Security Roles and Responsibilities) 14](#_Toc189833672)

[3. Βασικές Πολιτικές Ασφάλειας (Access Control Policy, Password Policy, Logging Policy, Backup Policy) 14](#_Toc189833673)

[4. Βασικές Διαδικασίες (Διαδικασία αντιμετώπισης περιστατικών ασφάλειας, Διαδικασία Backup, Διαδικασία Δημιουργίας / Διαγραφής Χρήστη) 15](#_Toc189833674)

# 1. Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας

## 1.1 Περιγραφή της Μεθοδολογίας

Η μεθοδολογία που ακολουθείται βασίζεται στις πρακτικές ISO 27005 για τη διαχείριση και αποτίμηση κινδύνων. Η ανάλυση επικεντρώνεται στα πληροφοριακά αγαθά που σχετίζονται με την υπηρεσία Managed SIEM που παρέχει το Security Operations Center (SOC).

Μια υπηρεσία Managed SIEM είναι ιδανική γιατί:

* Συλλέγει, αποθηκεύει, επεξεργάζεται και αναλύει πληροφοριακά δεδομένα.
* Διαχειρίζεται logs, ειδοποιήσεις ασφαλείας, network traffic, threat intelligence data.
* Εμπλέκει πολλές κατηγορίες πληροφοριακών αγαθών, όπως πελατειακά δεδομένα, λειτουργικά δεδομένα και δεδομένα ασφαλείας.
* Είναι κρίσιμη για τη λειτουργία επιχειρήσεων που θέλουν να εντοπίζουν και να αποκρίνονται σε απειλές.

Αρχικά, πραγματοποιείται ταυτοποίηση και αποτίμηση της αξίας των πληροφοριακών αγαθών, συμπεριλαμβανομένων των δεδομένων, των λογισμικών, του υλικού εξοπλισμού και των φυσικών υποδομών που εμπλέκονται στην υπηρεσία. Η αξία των πληροφοριακών αγαθών καθορίζει και την αξία των αγαθών στα οποία συμπεριλαμβάνεται.

Στη συνέχεια, εκτελείται Impact Assessment, όπου αξιολογούνται οι πιθανές επιπτώσεις από απώλεια εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας των αγαθών. Σε αυτή τη διαδικασία, υιοθετείται η προσέγγιση worst-case scenario, καταγράφοντας τη μέγιστη δυνατή επίδραση που θα μπορούσε να προκύψει.

Ακολουθεί Threat & Vulnerability Assessment, όπου εντοπίζονται οι πιθανές απειλές και αδυναμίες που θα μπορούσαν να επηρεάσουν την υπηρεσία SOC, βασισμένες σε διεθνή πρότυπα, στατιστικά στοιχεία κυβερνοεπιθέσεων (π.χ., ENISA Threat Landscape, MITRE ATT&CK) και security controls που εφαρμόζονται σε SOCs.

Τέλος, πραγματοποιείται Risk Analysis, όπου εκτιμάται το συνολικό ρίσκο, και διαμορφώνεται ένα Risk Treatment Plan. Το σχέδιο αυτό περιλαμβάνει προτεινόμενα μέτρα προστασίας και στρατηγικές μετριασμού των κινδύνων, διασφαλίζοντας τη συνέχεια και την ασφαλή λειτουργία του SOC.

## 1.2 Περιγραφή του Οργανισμού/ Εταιρίας/ Φορέα / Εφοδιαστικής Υπηρεσίας

Η ανάλυση επικεντρώνεται στην υπηρεσία managed SIEM, η οποία διασφαλίζει την συνεχιζόμενη παρακολούθηση και ασφάλεια των πληροφοριακών συστημάτων ενός οργανισμού ή υπηρεσίας.

Το Managed SIEM παρέχει ανίχνευση και ανάλυση απειλών σε πραγματικό χρόνο. Για παράδειγμα, αν ένας πελάτης δέχεται brute-force attack, το SIEM καταγράφει πολλαπλές αποτυχημένες συνδέσεις. Αυτό δημιουργεί alert στο SOC, όπου ένας SOC Analyst (L1) το αξιολογεί και, αν απαιτείται, το κλιμακώνει σε L2/L3. Η ομάδα incident response ενεργοποιεί containment policies, π.χ., αποκλεισμό IP ή forced password reset, αποτρέποντας περαιτέρω επιθέσεις.

Οι βασικές λειτουργίες περιλαμβάνουν:

**Παρακολούθηση Δικτύου (Network Monitoring):**

Ανίχνευση Νέων Συσκευών:

Παρακολούθηση του δικτύου για την αναγνώριση νέων συσκευών που συνδέονται με το δίκτυο.

Διαχείριση Καταγραφών Δικτύου (Network Logs):

Ανάλυση των καταγραφών του δικτύου για την ανίχνευση ανωμαλιών και παραβιάσεων.

Μοτίβα Επικοινωνίας Συσκευών (Device Communication Patterns):

Εξετάζονται τα πρότυπα επικοινωνίας των συσκευών για τον εντοπισμό ύποπτης δραστηριότητας.

Ανατροφοδότηση Απειλών (Threat Intelligence Feeds):

Χρήση feeds από αξιόπιστες πηγές για τη λήψη ενημερώσεων σχετικά με νέες απειλές ή κακόβουλο λογισμικό.

Αναγνώριση Ευπαθειών (Vulnerabilities) και Ενημερώσεις Λογισμικού (Patches):

Παρακολούθηση και εφαρμογή των τελευταίων ενημερώσεων και διορθώσεων ασφάλειας.

**Ανίχνευση και Αντιμετώπιση Περιστατικών (Incident Detection and Response):**

Αντιμετώπιση Σοβαρών Περιστατικών:

Χρησιμοποιούνται manuals και πρωτόκολλα αντίδρασης σε περιστατικά (incident response protocols) για την άμεση και οργανωμένη διαχείριση σοβαρών περιστατικών ασφαλείας.

Ενημερώσεις για Ενημέρωση Λογισμικού (Updates for Software Patches):

Διαχείριση και εφαρμογή ενημερώσεων για το λογισμικό, εξασφαλίζοντας ότι το σύστημα παραμένει προστατευμένο από νέες απειλές.

Ασφαλής Χρήση Πρωτοκόλλων και Κωδικών Πρόσβασης:

Ενημέρωση για την αποφυγή χρήσης ανασφαλών πρωτοκόλλων και κωδικών πρόσβασης και την προώθηση ασφαλών πρακτικών, όπως η υιοθέτηση MFA (Multi-Factor Authentication).

Έρευνα Πιθανών Κινδύνων:

Διαρκής ανάλυση της ασφάλειας για να εντοπιστούν και να αντιμετωπιστούν πιθανοί κίνδυνοι πριν επηρεάσουν τα συστήματα ή τα δεδομένα.

## Απαιτήσεις Ασφαλείας & Νομικές Απαιτήσεις για την Υπηρεσία SOC

Ελεγχόμενη Πρόσβαση:

Χρήση συστημάτων ελέγχου πρόσβασης για την ασφαλή πρόσβαση στους χώρους όπου πραγματοποιείται η παρακολούθηση και διαχείριση των δεδομένων (π.χ., SOC rooms).

Εφαρμογή καρτών ή άλλων μέσων ασφαλούς πρόσβασης για να διασφαλιστεί ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε κρίσιμα δεδομένα και εργαλεία παρακολούθησης.

Εκπαίδευση Προσωπικού:

Συνεχής εκπαίδευση του προσωπικού του SOC σε θέματα κυβερνοασφάλειας, αντιμετώπισης περιστατικών και κοινωνικής μηχανικής για να διασφαλιστεί ότι μπορούν να αναγνωρίζουν και να αντιδρούν σε νέες και εξελισσόμενες απειλές.

Αντιμετώπιση Περιστατικών Ασφαλείας:

Ορισμός σαφών διαδικασιών και πρωτοκόλλων αντίδρασης για την άμεση και αποτελεσματική διαχείριση περιστατικών ασφαλείας που εντοπίζονται μέσω του SOC.

Τεκμηρίωση και εφαρμογή των διαδικασιών για να διασφαλιστεί η ταχεία και σωστή ανταπόκριση σε περιστατικά και η ενημέρωση για αλλαγές, όπως ενημερώσεις λογισμικού ή αδυναμίες πρωτοκόλλων.

Ασφαλής Πρόσβαση:

Χρήση Multi-Factor Authentication (MFA) και Role-Based Access Control (RBAC) για να περιορίζεται η πρόσβαση στα δεδομένα και τα εργαλεία παρακολούθησης του SOC μόνο σε εξουσιοδοτημένο προσωπικό.

Κρυπτογράφηση:

Εφαρμογή κρυπτογράφησης τόσο σε δεδομένα που μεταφέρονται όσο και σε δεδομένα που αποθηκεύονται, για να διασφαλιστεί η προστασία της εμπιστευτικότητας των δεδομένων που διαχειρίζεται η υπηρεσία SOC.

Προστασία Δικτύου:

Εφαρμογή firewall, Intrusion Detection Systems (IDS) και Intrusion Prevention Systems (IPS) για τη διαρκή παρακολούθηση και προστασία των δικτύων που χρησιμοποιούνται από την υπηρεσία SOC, αναγνωρίζοντας και εμποδίζοντας ενδεχόμενες επιθέσεις.

Προστασία Δεδομένων Προσωπικού Χαρακτήρα (GDPR):

Εξασφάλιση της συναίνεσης από τα υποκείμενα των δεδομένων πριν από την επεξεργασία τους για σκοπούς ασφάλειας.

Διασφάλιση των δικαιωμάτων των υποκειμένων δεδομένων, όπως το δικαίωμα στη διαγραφή και το δικαίωμα στη φορητότητα των δεδομένων, για όλα τα δεδομένα που επεξεργάζεται η υπηρεσία SOC.

Συμμόρφωση με Διεθνή Πρότυπα Ασφαλείας:

Η υπηρεσία SOC πρέπει να συμμορφώνεται με διεθνή πρότυπα ασφάλειας, όπως το ISO 27001, για τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων που παρακολουθούνται και προστατεύονται μέσω του SOC.

Εφαρμογή διαδικασιών και πρωτοκόλλων για την αποδοχή και εφαρμογή των προτύπων ασφαλείας που σχετίζονται με τη διαχείριση των δεδομένων στον τομέα της κυβερνοασφάλειας.

## 1.5 Χαρτογράφηση Αγαθών

**1. Δεδομένα Πελατών (Customer Data)**

**Περιγραφή:** Τα δεδομένα των πελατών περιλαμβάνουν προσωπικά και οργανωτικά δεδομένα που δίνονται στην υπηρεσία SOC κατά την έναρξη και τη συνεχή παροχή της υπηρεσίας.

**Παραδείγματα:**

* Προσωπικά δεδομένα (ονόματα, διευθύνσεις, στοιχεία επικοινωνίας).
* Δεδομένα υποδομής (τοπολογία δικτύου, συσκευές, endpoints, δικτυακές ρυθμίσεις).
* Πληροφορίες πρόσβασης χρηστών (authentication logs, δικαιώματα πρόσβασης).
* Πολιτικές ασφαλείας και compliance requirements (ISO 27001, GDPR, NIST).
* **Threat Intelligence Feeds** (δεδομένα από εξωτερικές πηγές όπως VirusTotal, AbuseIPDB, CVEs).
* **Asset Inventory** (λίστα με συσκευές και υπηρεσίες που προστατεύει το SOC).

**Ασφάλεια:** Τα δεδομένα πρέπει να προστατεύονται μέσω κρυπτογράφησης, ελέγχου πρόσβασης και συμμόρφωσης με νομικά και κανονιστικά πλαίσια (GDPR, ISO 27001).

**2. Εσωτερικά Δεδομένα (SOC Internal Data)**

**Περιγραφή:** Δεδομένα που αφορούν το εσωτερικό περιβάλλον του SOC, όπως στοιχεία εργαζομένων και αρχεία ελέγχου.

**Παραδείγματα:**

* Προσωπικά δεδομένα SOC analysts (user credentials, επίπεδα πρόσβασης).
* **Logins των SOC Analysts** (ποιος συνδέθηκε και πότε).
* **Audit Logs** (ενέργειες των SOC analysts στο SIEM, αλλαγές σε correlation rules, response actions).
* Πολιτικές πρόσβασης και διαχείρισης χρηστών.

**Ασφάλεια:** Η πρόσβαση πρέπει να περιορίζεται με Role-Based Access Control (RBAC) και να καταγράφεται κάθε ενέργεια για forensic ανάλυση και auditing.

**3. Operational Data (Monitoring, Analysis Data)**

**Περιγραφή:** Δεδομένα που συλλέγονται από το SIEM και άλλες πηγές παρακολούθησης για την ανίχνευση και αντιμετώπιση απειλών.

**Παραδείγματα:**

* Δεδομένα κίνησης δικτύου (NetFlow, DNS queries, firewall logs).
* Συναγερμοί ασφαλείας (SIEM alerts, IDS/IPS detections).
* Logs από endpoints, servers, firewalls, cloud services.
* **Threat Intelligence Data** (κακόβουλες IP, hash κακόβουλων αρχείων, phishing URLs).
* **Correlation Rules** (κανόνες που εφαρμόζει το SIEM για την αναγνώριση επιθέσεων).

**Ασφάλεια:** Τα δεδομένα πρέπει να παρακολουθούνται συνεχώς, να αναλύονται σε πραγματικό χρόνο και να διασφαλίζεται η ακεραιότητά τους μέσω hashing και immutable storage.

**4. Backup/Historical Data (Backup και Ιστορικά Δεδομένα)**

**Περιγραφή:** Δεδομένα που σχετίζονται με τη διατήρηση ιστορικών καταγραφών και την αποκατάσταση μετά από περιστατικά ασφαλείας.

**Παραδείγματα:**

* Αποθηκευμένα logs από SIEM, firewall, IDS/IPS.
* **Log Retention Policies** (κανόνες για τη διατήρηση logs, π.χ. 6 μήνες, 1 έτος).
* **Forensic Data** (ψηφιακά ίχνη, ιστορικά alerts, memory dumps για ανάλυση περιστατικών).

**Ασφάλεια:** Απαιτείται κρυπτογράφηση των backup, χρήση immutable storage και τακτικός έλεγχος της δυνατότητας

**5. Documentation (Έγγραφα και Πολιτικές)**

**Περιγραφή:** Τεκμηρίωση που αφορά τη λειτουργία του SOC και τις διαδικασίες απόκρισης σε περιστατικά ασφαλείας.

**Παραδείγματα:**

* Security Policies & Compliance Documents (ISO 27001, NIST, GDPR).
* **SOC Playbooks** (καθορισμένες διαδικασίες για αντιμετώπιση περιστατικών, π.χ. phishing response, malware analysis).
* Οδηγίες χρήσης εργαλείων (SIEM, SOAR, EDR).
* Εκπαιδευτικά υλικά για τους SOC Analysts.

**Ασφάλεια:** Πρέπει να υπάρχει περιορισμός πρόσβασης μέσω RBAC, καταγραφή αλλαγών (version control) και αποθήκευση σε ασφαλή τοποθεσία.

**Λογισμικά( Software Assets):**

Community-driven and Accessible platforms (Free-tier tools):

Περιγραφή: Τα εργαλεία αυτά, όπως το GitHub και τα threat intelligence platforms, χρησιμοποιούνται για τη συνεργασία, την ανάλυση απειλών, και την ανάπτυξη εργαλείων ασφαλείας και στρατηγικών.

Ασφάλεια: Η χρήση αυτών των εργαλείων πρέπει να συνοδεύεται από τη συνεχή παρακολούθηση των ενημερώσεων ασφαλείας και την εφαρμογή πρακτικών διαχείρισης ευπαθειών για να εξασφαλιστεί ότι δεν εισάγονται νέοι κίνδυνοι από ανασφαλή εργαλεία.

Operational Software (Επιχειρησιακά Λογισμικά):

Περιγραφή: Αυτά τα εργαλεία περιλαμβάνουν συστήματα παρακολούθησης δικτύου, SIEM, και άλλα συστήματα που χρησιμοποιούνται για την ανάλυση, ανίχνευση, και ανταπόκριση σε απειλές. Αυτά τα εργαλεία είναι κρίσιμα για την παροχή της υπηρεσίας SOC.

Ασφάλεια: Η προστασία αυτών των συστημάτων περιλαμβάνει τη χρήση πολιτικών ασφαλείας, τη διασφάλιση της διαθεσιμότητας και ακεραιότητας των δεδομένων και την κατάλληλη εκπαίδευση του προσωπικού για τη σωστή χρήση τους.

Microsoft Office Suite:

Θα πρέπει να υπάρχουν και πολιτικές για την προστασία των δεδομένων που διαχειρίζονται μέσω αυτών των εργαλείων, όπως μέσω κρυπτογράφησης αρχείων ή ασφαλούς αποθήκευσης.

Λειτουργικά Συστήματα(Operational Systems):

Η ασφάλεια των λειτουργικών συστημάτων Windows και Linux πρέπει να είναι σε υψηλά επίπεδα, καθώς είναι τα βασικά περιβάλλοντα για τα εργαλεία SOC.

**Υλικό (Hardware Assets):**

Συσκευές Χρηστών:

Περιγραφή: Περιλαμβάνουν συσκευές όπως κινητά τηλέφωνα, laptops, workstations που χρησιμοποιούνται για την πρόσβαση και εκτέλεση των καθηκόντων της υπηρεσίας SOC.

Ασφάλεια: Πρέπει να εφαρμόζονται αυστηρές πολιτικές για την ασφαλή πρόσβαση στις συσκευές (π.χ. χρήση MFA, συστήματα απομακρυσμένης διαχείρισης για την προστασία των συσκευών).

Συσκευές Δικτύου:

Περιγραφή: Αυτές οι συσκευές περιλαμβάνουν servers, firewalls, routers, και άλλα δικτυακά εξαρτήματα που χρησιμοποιούνται για την παρακολούθηση και διαχείριση της δικτυακής υποδομής.

Ασφάλεια: Η προστασία των συσκευών αυτών περιλαμβάνει την εφαρμογή πολιτικών παρακολούθησης για την ανίχνευση επιθέσεων, τη διασφάλιση της διαθεσιμότητας του δικτύου και την ασφαλή διαχείριση των διαμορφώσεων.

Συσκευές Αποθηκευτικού Χώρου:

Περιγραφή: Αφορά διακομιστές αρχείων και συστήματα NAS που χρησιμοποιούνται για την αποθήκευση δεδομένων.

Ασφάλεια: Η κρυπτογράφηση των δεδομένων αποθήκευσης και η διαχείριση δικαιωμάτων πρόσβασης σε αυτά τα συστήματα είναι κρίσιμες για την αποφυγή της μη εξουσιοδοτημένης πρόσβασης.

**Φυσικά Αγαθά (Physical Assets)** (Αναφερόμαστε στα παρακάτω ως ένα αγαθό που τα περιλαμβάνει όλα -> **Headquarters**) όπου περιλαμβάνονται τα:

Offices (Computer Rooms, Conference Room, …):

Περιγραφή: Περιλαμβάνει τα γραφεία, τα δωμάτια υπολογιστών και άλλους χώρους όπου διεξάγεται η εργασία της υπηρεσίας SOC.

Ασφάλεια: Η φυσική προστασία αυτών των χώρων περιλαμβάνει την πρόσβαση με κάρτες ασφαλείας, την καταγραφή της φυσικής πρόσβασης και την εγκατάσταση συστημάτων ασφαλείας (κάμερες, συναγερμοί).

Data Center (Network and Storage Equipment):

Περιγραφή: Τα κέντρα δεδομένων που φιλοξενούν τους servers, τα συστήματα δικτύου και την υποδομή αποθήκευσης.

Ασφάλεια: Χρειάζεται αυστηρός έλεγχος πρόσβασης και κανονιστικά πλαίσια για την προστασία της υποδομής και την ασφαλή αποθήκευση των δεδομένων.

Security Systems (Cameras, Physical Cards, Alarms):

Περιγραφή: Περιλαμβάνει τα συστήματα φυσικής ασφαλείας που χρησιμοποιούνται για την προστασία των χώρων και των υποδομών.

Ασφάλεια: Η φυσική ασφάλεια πρέπει να συνδυάζεται με ψηφιακά συστήματα παρακολούθησης για να εξασφαλίζεται η προστασία σε όλους τους τομείς της υπηρεσίας.

## 1.6 Αποτίμηση Επιπτώσεων (Impact Assessment)

Θα εκτιμήσουμε τι επιπτώσεις θα είχε μια παραβίαση ή διαρροή στα πληροφοριακά αγαθά που ορίσαμε. Μπορούμε να τις κατηγοριοποιήσουμε βάσει **εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας (CIA Triad)**.

**Ιmpact levels:**

low=0

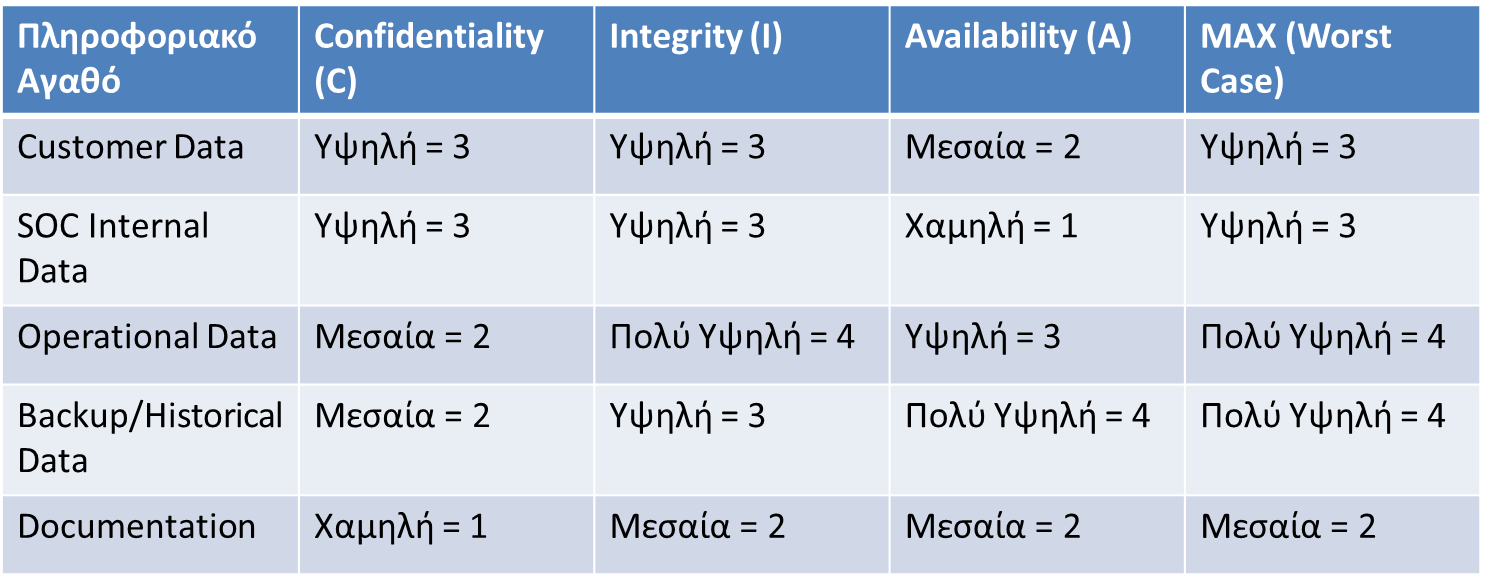
very low=1

med=2

high=3

very high=4

Για παράδειγμα:



**Συμπέρασμα**:

* Τα **Δεδομένα Πελατών, Operational Data και Backup Data** έχουν τον υψηλότερο αντίκτυπο και πρέπει να προστατευτούν περισσότερο.
* Τα **Εσωτερικά Δεδομένα** είναι επίσης κρίσιμα, αλλά δεν επηρεάζουν άμεσα την ασφάλεια των πελατών.
* Τα **Documentation Data** έχουν χαμηλότερο ρίσκο, αλλά μπορούν να βελτιώσουν ή να αποτρέψουν λάθη στη λειτουργία του SOC.

## 1.7 Αποτίμηση Απειλών (Threat Assessment) και Ευπαθειών ( Vulnerability Assessment)

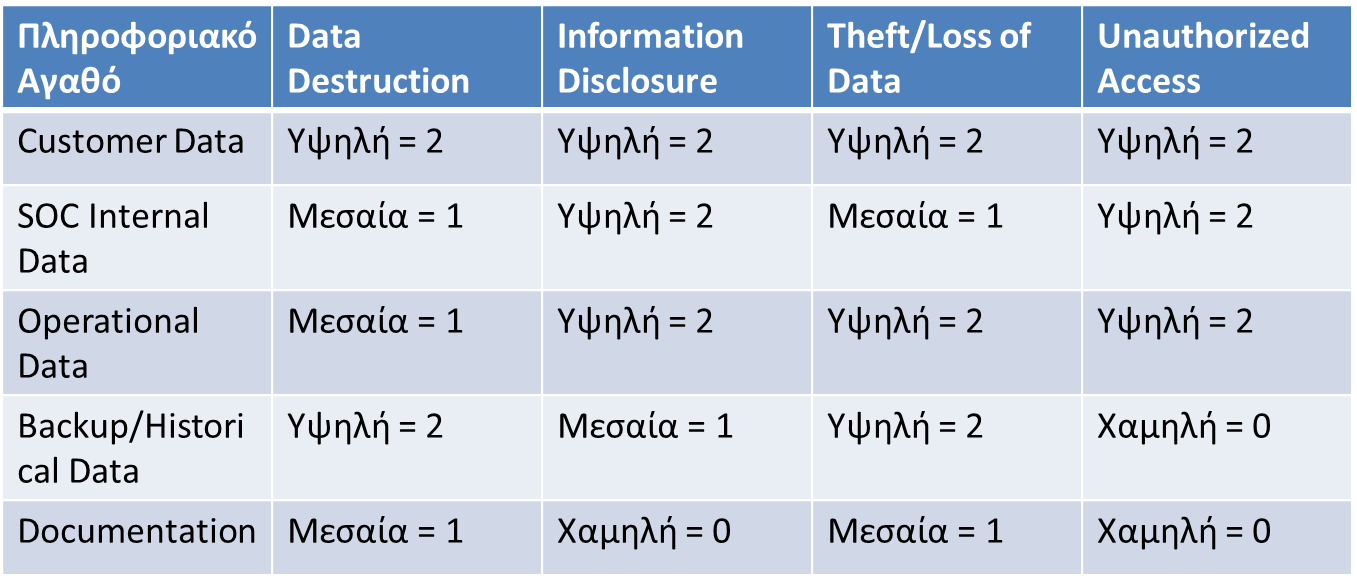
Για κάθε πληροφοριακό αγαθό, αναλύουμε τις πιθανές απειλές.

**Τhreat levels:**

0=low= once every 10 years

1=medium=once every 3 years

2=high=once a year

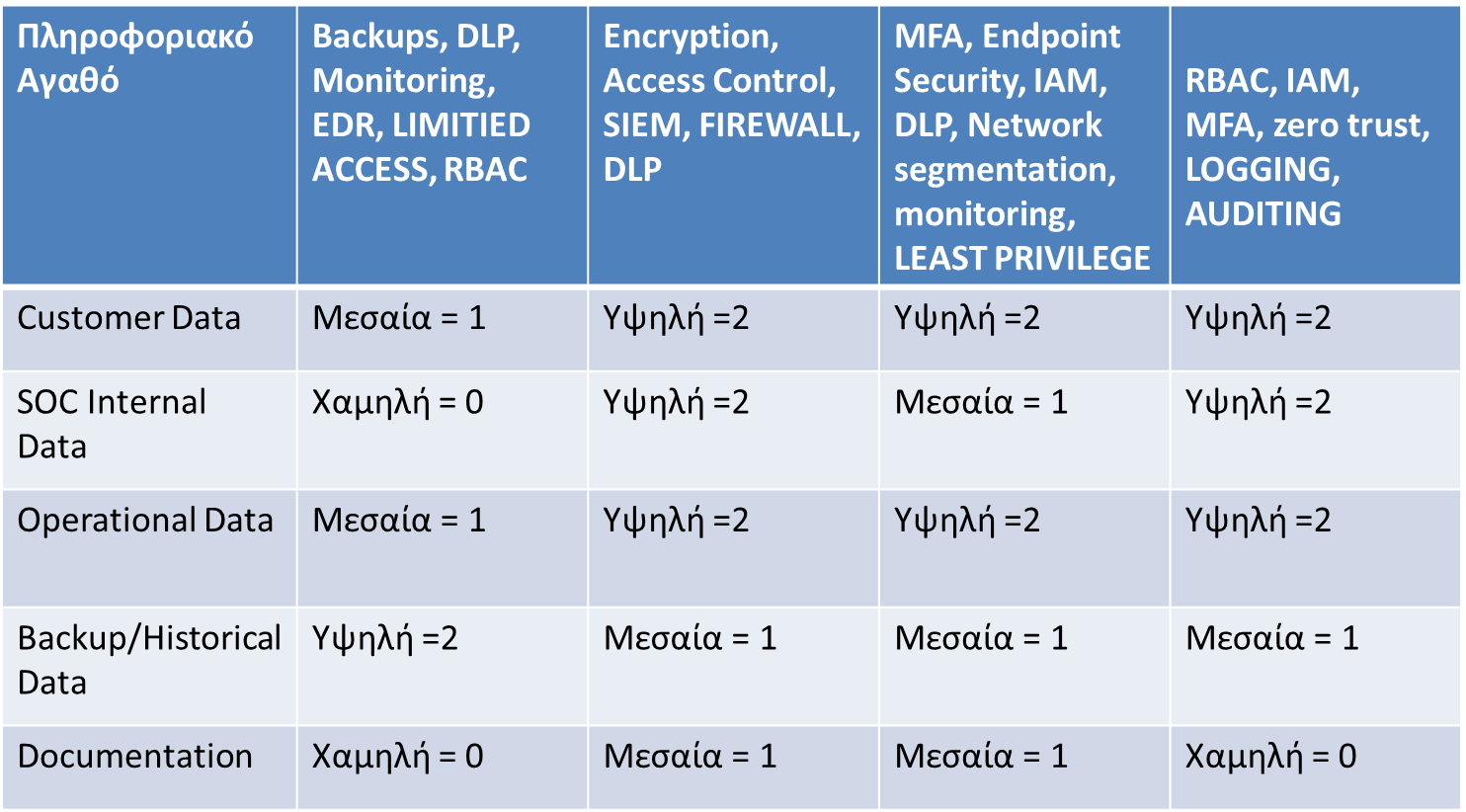


**Vulnerability levels:**

0=low= <33% πιθανότητα να συμβεί το χειρότερο σενάριο

1=med= 33 % < πιθανότητα να συμβεί το χειρότερο σενάριο < 66%

2=high= πιθανότητα να συμβεί το χειρότερο σενάριο > 66%



## 1.9 Αποτίμηση Κινδύνων (Risk Assessment)

Η αποτίμηση του κινδύνου για κάθε asset γίνεται προσθέτοντας το impact value, threat value, vulnerability value (ή αλλιώς impact + likelihood).

threat + value =likelihood of an incident

**Likelihood levels:**

0=low= very unlikely

1=low= unlikely

2=medium= possible

3=high= likely

4=very high= frequent

Οπότε η κλίμακα του συνολικού κινδύνου κυμαίνεται από 0 έως 8.

**Risk Levels:**

0-2=low risk

3-5=med risk

6-8=high risk

| **Πληροφοριακό Αγαθό** | **Πιθανότητα Απειλής** | **Σοβαρότητα Επιπτώσεων** | **Συνολικό Ρίσκο** |
| --- | --- | --- | --- |
| **Customer Data** | Υψηλή | Υψηλή | Υψηλό |
| **SOC Internal Data** | Μεσαία | Υψηλή | Υψηλό |
| **Operational Data** | Υψηλή | Υψηλή | Υψηλό |
| **Backup Data** | Μεσαία | Υψηλή | Υψηλό |
| **Documentation** | Χαμηλή | Μεσαία | Μεσαίο |

**Υψηλότερο ρίσκο → Customer Data, Operational Data & Backup Data.**

**Συμπεράσματα:**

* Τα **Δεδομένα Πελατών, Operational Data και Backup Data** έχουν το **μεγαλύτερο ρίσκο** και χρειάζονται αυστηρή προστασία.
* Τα **Εσωτερικά Δεδομένα** έχουν υψηλό ρίσκο λόγω compliance, αλλά χαμηλότερη πιθανότητα επίθεσης.
* Τα **Documentation Data** έχουν το χαμηλότερο ρίσκο, αλλά πρέπει να προστατεύονται για ομαλή λειτουργία.

## 1.10 Προτεινόμενα Μέτρα Προστασίας (Proposed Security Countermeasures)

Ανάλογα με το επίπεδο ρίσκου, προτείνουμε λύσεις για να **μειώσουμε τις πιθανότητες επιτυχημένης επίθεσης** και να **περιορίσουμε τις συνέπειες**.

**Σκοπός:** Αντιστοίχιση **κάθε απειλής** με τα βασικά **μέτρα προστασίας** για μείωση του κινδύνου.

| **Threat** | **Protection Measures (Μέτρα Προστασίας)** |
| --- | --- |
| **Data Destruction** | Immutable Backups (μη τροποποιήσιμα αντίγραφα)   Redundant storage (RAID, Cloud replication)   SIEM monitoring για ανίχνευση διαγραφών |
| **Accidental/Intentional Disclosure** | Data Loss Prevention (DLP)   Data Classification & Encryption   Awareness training για προσωπικό |
| **Theft/Loss of Data** | Endpoint Protection (EDR/XDR)   Strong authentication (MFA, biometrics)   USB/Device control policies |
| **Unauthorized Access** | Role-Based Access Control (RBAC)   Multi-Factor Authentication (MFA)   Zero Trust Security Model |

**Τα πιο κρίσιμα μέτρα είναι τα:** **RBAC, MFA, SIEM monitoring, DLP & Immutable Backups**  
**Με αυτά τα μέτρα, μειώνουμε το συνολικό ρίσκο σε όλα τα πληροφοριακά αγαθά.**

## 1.11 Σχέδιο Υλοποίησης Μέτρων Προστασίας

**Υψηλού ρίσκου πληροφοριακά αγαθά** απαιτούν **άμεσες ενέργειες** με κρυπτογράφηση, περιορισμό πρόσβασης και συνεχές monitoring.  
**Μεσαίου ρίσκου** απαιτούν **βελτιώσεις στο IAM και auditing**.  
**Χαμηλού ρίσκου** απαιτούν **καλύτερη κατηγοριοποίηση και πρόσβαση**.

Ως προτεραιότητα θα αντιμετωπίσουμε τους κινδύνους που αποτιμάμε με βαθμολογία 5-8 , την τελευταία βαθμίδα της μεσαίας επικινδυνότητας και όλες τις υψηλές.

Θα προχωρήσουμε σε αποδοχή κινδύνου από την βαθμολογία 0-4.

# Κατανομή οργανωτικών δομών και αρμοδιοτήτων ασφάλειας (Security Roles and Responsibilities)

Στην υπηρεσία SOC, η ασφάλεια των πληροφοριακών αγαθών απαιτεί διακριτούς ρόλους με σαφείς ευθύνες. Παρακάτω περιγράφουμε τα βασικά security roles και τις αρμοδιότητές τους.

**Chief Information Security Officer (CISO**)

Ρόλος: Ο CISO είναι υπεύθυνος για την ολοκληρωμένη στρατηγική κυβερνοασφάλειας του SOC.

Αρμοδιότητες:

Καθορίζει τις πολιτικές και διαδικασίες ασφαλείας.

Ελέγχει τη συμμόρφωση με πρότυπα (ISO 27001, NIST, GDPR).

Αναπτύσσει σχέδιο αντιμετώπισης κινδύνων.

Ενημερώνει τη διοίκηση για απειλές και επιθέσεις.

**Security Operations Center (SOC) Manager**

Ρόλος: Επικεφαλής του SOC, επιβλέπει τη λειτουργία του και συντονίζει τις ομάδες ασφαλείας.

Αρμοδιότητες:

Επιβλέπει το SIEM, monitoring tools και threat intelligence.

Συντονίζει την ανταπόκριση σε περιστατικά (Incident Response).

Διαχειρίζεται τη ροή πληροφοριών μεταξύ ομάδων.

Εκπαιδεύει την ομάδα SOC και αναπτύσσει playbooks.

**SOC Analysts (L1, L2, L3)**

L1 (Tier 1) SOC Analyst

Ρόλος: Πρώτη γραμμή άμυνας, αναλύει alerts και κάνει triage περιστατικών.

Αρμοδιότητες:

Παρακολουθεί το SIEM για alerts.

Κάνει αρχική ανάλυση απειλών (malware, phishing, network intrusions).

Ανοίγει tickets και τα κλιμακώνει σε L2/L3 αν απαιτείται.

L2 (Tier 2) SOC Analyst

Ρόλος: Εμβαθύνει στα περιστατικά και εκτελεί ενεργή απόκριση.

Αρμοδιότητες:

Αναλύει δικτυακή κίνηση, logs και endpoints.

Χρησιμοποιεί Threat Intelligence για ταυτοποίηση επιθέσεων.

Εφαρμόζει μείωση απειλών (containment, eradication).

L3 (Tier 3) SOC Analyst

Ρόλος: Ειδικός σε Advanced Persistent Threats (APT) και forensic investigations.

Αρμοδιότητες:

Εκτελεί forensic ανάλυση και reverse engineering malware.

Αναπτύσσει νέους κανόνες SIEM (correlation rules).

Συνεργάζεται με Threat Hunting και Red Teams.

**Incident Response Team (IRT)**

Ρόλος: Αναλαμβάνει την αντιμετώπιση σοβαρών περιστατικών και την αποκατάσταση.

Αρμοδιότητες:

Δημιουργεί Incident Response Playbooks.

Διερευνά επιθέσεις και εκτελεί containment & recovery.

Συνεργάζεται με νομικά τμήματα για compliance & breach notifications.

**Threat Intelligence Team**

Ρόλος: Συλλέγει πληροφορίες για επιθέσεις και προσαρμόζει την άμυνα του SOC.

Αρμοδιότητες:

Αναλύει νέα exploits και IoCs (Indicators of Compromise).

Τροφοδοτεί το SIEM με Threat Feeds.

Συνεργάζεται με εθνικές αρχές και cybersecurity communities.

**Security Engineers**

Ρόλος: Υπεύθυνοι για τη σχεδίαση, υλοποίηση και διαχείριση των συστημάτων ασφαλείας.

Αρμοδιότητες:

Ρυθμίζουν και βελτιστοποιούν SIEM, IDS/IPS, Firewalls.

Διαχειρίζονται Endpoint Detection & Response (EDR) λύσεις.

Εφαρμόζουν Zero Trust Architecture και Network Segmentation.

**Compliance & Governance Team**

Ρόλος: Επιβλέπει τη συμμόρφωση με τα κανονιστικά πλαίσια και τα security policies.

Αρμοδιότητες:

Διενεργεί εσωτερικούς και εξωτερικούς ελέγχους (audits).

Βεβαιώνει ότι τηρούνται GDPR, ISO 27001, NIST, SOC 2.

Συνεργάζεται με νομικές υπηρεσίες για data breach notifications.

# Βασικές Πολιτικές Ασφάλειας (Access Control Policy, Password Policy, Logging Policy, Backup Policy)

Στην υπηρεσία SOC, η ύπαρξη σαφών πολιτικών ασφαλείας είναι κρίσιμη για τη διαχείριση κινδύνων και τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών αγαθών.

**Access Control Policy (Πολιτική Ελέγχου Πρόσβασης)**

Σκοπός:

Καθορίζει τους κανόνες πρόσβασης στα πληροφοριακά συστήματα και δεδομένα του SOC, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες έχουν τη σωστή πρόσβαση.

Κύριες Αρχές:

Least Privilege Principle: Κάθε χρήστης έχει μόνο τα απολύτως απαραίτητα δικαιώματα για την εργασία του.

Role-Based Access Control (RBAC): Τα δικαιώματα χορηγούνται βάσει ρόλων (π.χ. SOC Analyst, Incident Responder).

Multi-Factor Authentication (MFA): Υποχρεωτικό για όλους τους χρήστες με πρόσβαση σε κρίσιμα συστήματα.

Segregation of Duties: Οι κρίσιμες λειτουργίες κατανέμονται σε διαφορετικά άτομα για την αποφυγή καταχρήσεων.

Παραδείγματα Κανόνων:

Οι SOC Analysts δεν έχουν άμεση πρόσβαση σε συστήματα παραγωγής.

Οι Security Engineers μπορούν να τροποποιούν ρυθμίσεις ασφαλείας, αλλά όχι να εγκρίνουν αλλαγές.

Οι λογαριασμοί διαχειριστών είναι ξεχωριστοί από τους προσωπικούς λογαριασμούς εργασίας.

**Password Policy (Πολιτική Κωδικών Πρόσβασης)**

Σκοπός:

Διασφαλίζει ότι οι κωδικοί πρόσβασης είναι ισχυροί και προστατεύονται από μη εξουσιοδοτημένη πρόσβαση.

Κύριες Αρχές:

Μήκος & Πολυπλοκότητα: Ελάχιστο μήκος: 14 χαρακτήρες

Περιλαμβάνει κεφαλαία, πεζά, αριθμούς και ειδικούς χαρακτήρες

Διαχείριση & Ανανέωση: Αλλαγή κωδικού κάθε 90 ημέρες

Δεν επιτρέπεται η χρήση των τελευταίων 5 κωδικών

Αποθήκευση:

Οι κωδικοί δεν αποθηκεύονται σε απλό κείμενο, αλλά με PBKDF2, bcrypt ή Argon2

MFA Υποχρεωτικό:

Για όλους τους λογαριασμούς με πρόσβαση σε ευαίσθητα δεδομένα

Παραδείγματα Κανόνων:

Οι χρήστες δεν μπορούν να χρησιμοποιούν κοινά passwords (π.χ. P@ssw0rd!).

Απαγορεύεται η αποστολή κωδικών μέσω email ή η καταγραφή τους σε μη ασφαλείς τοποθεσίες.

Η πρόσβαση σε ευαίσθητα δεδομένα απαιτεί MFA + password.

**Logging & Monitoring Policy (Πολιτική Καταγραφής & Παρακολούθησης)**

Σκοπός:

Καθορίζει ποιες δραστηριότητες καταγράφονται και πώς παρακολουθούνται για την ανίχνευση επιθέσεων και την απόκριση σε περιστατικά ασφαλείας.

Κύριες Αρχές:

Καταγραφή Όλων των Κρίσιμων Συμβάντων:

Επιτυχημένες & αποτυχημένες προσπάθειες πρόσβασης

Αλλαγές ρυθμίσεων ασφάλειας

Δραστηριότητα διαχειριστών και χρηστών υψηλών δικαιωμάτων

Συγκέντρωση Δεδομένων στο SIEM:

Τα logs αποστέλλονται σε SIEM για ανάλυση και ανίχνευση απειλών

Πολιτική Διατήρησης:

Τα logs αποθηκεύονται για τουλάχιστον 1 έτος για forensic ανάλυση

Προστασία των Καταγραφών:

Κρυπτογράφηση των logs (AES-256)

Role-Based Access για πρόσβαση μόνο από εξουσιοδοτημένους χρήστες

Παραδείγματα Κανόνων:

Όλοι οι χρήστες του SOC υπόκεινται σε 24/7 monitoring.

Οι κρίσιμες αλλαγές στα συστήματα SIEM, Firewalls και EDR πρέπει να καταγράφονται και να ελέγχονται.

Τα logs αποθηκεύονται σε ξεχωριστή ασφαλή τοποθεσία (log server).

**Backup & Recovery Policy (Πολιτική Αντιγράφων Ασφαλείας & Ανάκαμψης)**

Σκοπός:

Διασφαλίζει ότι τα δεδομένα του SOC προστατεύονται από απώλεια και μπορούν να ανακτηθούν σε περίπτωση καταστροφής ή κυβερνοεπίθεσης.

Κύριες Αρχές:

Πολιτική 3-2-1 για αντίγραφα ασφαλείας:

3 αντίγραφα των δεδομένων

2 διαφορετικά μέσα αποθήκευσης

1 αντίγραφο εκτός τοποθεσίας (offsite/cloud)

Κρυπτογράφηση Backup Data:

Όλα τα backups προστατεύονται με AES-256 encryption

Δοκιμές Ανάκαμψης:

Τα backups ελέγχονται με restore tests κάθε 3 μήνες

Χρόνος Διατήρησης:

Τα κρίσιμα backups διατηρούνται για 1-3 έτη, ανάλογα με τις νομικές απαιτήσεις

Παραδείγματα Κανόνων:

Όλα τα δεδομένα SIEM & forensic logs υποστηρίζονται με ημερήσια incremental backups και μηνιαία full backups.

Τα backups αποθηκεύονται σε air-gapped αποθήκευση για προστασία από ransomware.

Μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση στα αρχεία backup.

# 4. Βασικές Διαδικασίες (Διαδικασία αντιμετώπισης περιστατικών ασφάλειας, Διαδικασία Backup, Διαδικασία Δημιουργίας / Διαγραφής Χρήστη)

**1. Διαδικασία Αντιμετώπισης Περιστατικών Ασφάλειας (Incident Response Process)**

**Σκοπός:**  
Εξασφαλίζει ότι κάθε κυβερνοεπίθεση ή περιστατικό ασφαλείας **αντιμετωπίζεται άμεσα και αποτελεσματικά**, μειώνοντας τον αντίκτυπο στο SOC και στην επιχείρηση.

**Βήματα της Διαδικασίας:**

**Αναγνώριση (Detection & Identification)**

Συλλογή ειδοποιήσεων από SIEM, IDS/IPS, EDR, Firewalls.  
Κατηγοριοποίηση των περιστατικών (π.χ., phishing, malware, data breach).

**Ανάλυση & Επιβεβαίωση (Analysis & Classification)**

Εξέταση των logs και δικτυακής κίνησης.  
Κατηγοριοποίηση βάσει σοβαρότητας:

* **Low:** Δεν απαιτεί άμεση ενέργεια.
* **Medium:** Χρειάζεται παρακολούθηση.
* **High:** Άμεση απόκριση απαιτείται.  
  Χρήση Threat Intelligence για συσχέτιση με γνωστές επιθέσεις.

**Αντίδραση & Απομόνωση (Containment & Mitigation)**

Αποσύνδεση μολυσμένων endpoints ή χρηστών από το δίκτυο.  
Εφαρμογή **firewall rules** για περιορισμό κακόβουλης κυκλοφορίας.  
Καθαρισμός και αποκατάσταση επηρεασμένων συστημάτων.

**Ανάκαμψη (Eradication & Recovery)**

Επαναφορά από **καθαρό backup**.  
Αναβάθμιση συστημάτων και εφαρμογή patches.  
Δοκιμές για επαλήθευση ότι το σύστημα είναι καθαρό.

**Αναφορά & Βελτίωση (Reporting & Lessons Learned)**

Δημιουργία **αναφοράς περιστατικού**.  
Αναθεώρηση πολιτικών και διαδικασιών ασφαλείας.  
Εκπαίδευση προσωπικού για αποφυγή παρόμοιων επιθέσεων.

**Παράδειγμα Αντίδρασης σε Ransomware Attack:**

**1️⃣ Αναγνώριση: SIEM alert για μαζική κρυπτογράφηση αρχείων σε endpoint.**

**2️⃣ Ανάλυση: Ο SOC Analyst (L1) βλέπει ότι ο χρήστης "User123" εκτελεί άγνωστα PowerShell scripts.**

**3️⃣ Αντίδραση: Ο SOC Analyst (L2) αποσυνδέει το endpoint από το δίκτυο.**

**4️⃣ Ανάκτηση: Ο SOC Manager (L3) εφαρμόζει immutable backup restore για ανάκτηση αρχείων.**

**5️⃣ Αναφορά & Lessons Learned: Εφαρμόζονται επιπλέον EDR rules για ανίχνευση κακόβουλων PowerShell εκτελέσεων στο μέλλον.**

**2. Διαδικασία Backup (Backup & Recovery Process)**

**Σκοπός:**  
Εξασφαλίζει ότι τα δεδομένα διατηρούνται ασφαλή και μπορούν να ανακτηθούν σε περίπτωση καταστροφής ή κυβερνοεπίθεσης.

**Βήματα της Διαδικασίας:**

**Δημιουργία Backup**

Καθημερινά **incremental backups** και εβδομαδιαία **full backups**.  
Αποθήκευση backup σε **τρία διαφορετικά μέσα** (τοπικό NAS, cloud, offline air-gapped).  
Κρυπτογράφηση των backup (AES-256).

**Αποθήκευση & Διατήρηση**

Τα backup αρχεία αποθηκεύονται για **τουλάχιστον 1-3 έτη**.  
Τα κρίσιμα δεδομένα αποθηκεύονται σε **air-gapped συστήματα** για προστασία από ransomware.  
Μόνο **εξουσιοδοτημένοι χρήστες** έχουν πρόσβαση.

**Δοκιμή Ανάκτησης (Restore Testing)**

Κάθε **3 μήνες**, γίνεται δοκιμή ανάκτησης δεδομένων.  
Επαλήθευση ότι το backup είναι **λειτουργικό** και δεν έχει διαφθαρεί.

**Ανάκτηση Δεδομένων (Disaster Recovery)**

Αν υπάρχει **data breach ή ransomware**, γίνεται αποκατάσταση από το τελευταίο **καθαρό backup**.  
Σε περίπτωση φυσικής καταστροφής, τα δεδομένα αποκαθίστανται από **cloud backups**.

**Παράδειγμα:** Αν ένας server καταστραφεί, η ομάδα SOC ανακτά τα δεδομένα από το backup και επαναφέρει τη λειτουργία χωρίς απώλειες.

**3. Διαδικασία Δημιουργίας & Διαγραφής Χρήστη (User Account Management Process)**

**Σκοπός:**  
Εξασφαλίζει ότι οι λογαριασμοί χρηστών δημιουργούνται, διαχειρίζονται και διαγράφονται με **ασφαλή και ελεγχόμενο τρόπο**.

**Βήματα της Διαδικασίας:**

**Δημιουργία Νέου Χρήστη (User Onboarding)**

Ο διαχειριστής λαμβάνει **αίτημα δημιουργίας χρήστη** από τον υπεύθυνο τμήματος.  
Εξουσιοδοτημένος διαχειριστής δημιουργεί τον λογαριασμό με **role-based access control (RBAC)**.  
Υποχρεωτική **MFA ενεργοποίηση**.  
Ο νέος χρήστης ενημερώνεται και λαμβάνει προσωρινό κωδικό **(πρέπει να αλλάξει κατά την πρώτη σύνδεση)**.

**Αλλαγή Δικαιωμάτων (User Modification)**

Αιτήματα αλλαγής πρόσβασης εξετάζονται και εγκρίνονται από ανώτερο υπάλληλο.  
Οι αλλαγές καταγράφονται στο **SIEM για auditing**.

**Διαγραφή Χρήστη (User Offboarding)**

Απενεργοποίηση λογαριασμού εντός **24 ωρών από την αποχώρηση**.  
Αφαίρεση πρόσβασης από όλα τα συστήματα (SIEM, VPN, email).  
Διατήρηση των logs του χρήστη για **1-3 έτη** για forensic ανάλυση.

**Παράδειγμα:** Όταν ένας υπάλληλος αποχωρεί, ο λογαριασμός του απενεργοποιείται, τα credentials διαγράφονται και η πρόσβασή του αποκόπτεται από το σύστημα.