ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

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

Εκφώνηση Εργασίας

Εργασία Β: 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

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:

- 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.

Περιγραφή Μεθοδολογίας:
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 ανάλυση γίνεται με επίκεντρο τα πληροφοριακά αγαθά που συμμετέχουν στην συγκεκριμένη υπηρεσία οπότε και 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.

ΒΑΣΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΔΙΚΤΥΟΥ (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.
ΑΝΙΧΝΕΥΣΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ (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.

1.3 Απαιτήσεις Ασφαλείας & Νομικές Απαιτήσεις για την Υπηρεσία SOC

ΑΠΑΙΤΗΣΕΙΣ	
ΑΣΦΑΛΕΙΑΣ	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.
	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.
ΝΟΜΙΚΕΣ	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.

1.4 Χαρτογράφηση Αγαθών

ΑΓΑΘΑ	ΠΕΡΙΓΡΑΦΗ	ΠΑΡΑΔΕΙΓΜΑΤΑ	ΑΣΦΑΛΕΙΑ
ΔΕΔΟΜΕΝΑ ΠΕΛΑΤΩΝ (CUSTOMER DATA)	Τα δεδομένα των πελατών περιλαμβάνουν προσωπικά και οργανωτικά δεδομένα που δίνονται στην υπηρεσία SOC κατά την έναρξη και τη συνεχή παροχή της υπηρεσίας.	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	Τα δεδομένα πρέπει να προστατεύονται μέσω κρυπτογράφησης, ελέγχου πρόσβασης και συμμόρφωσης με νομικά και κανονιστικά πλαίσια (GDPR, ISO 27001).
ΕΣΩΤΕΡΙΚΑ ΔΕΔΟΜΕΝΑ (SOC INTERNAL DATA)	Δεδομένα που αφορούν το εσωτερικό περιβάλλον του SOC, όπως στοιχεία εργαζομένων και αρχεία ελέγχου.	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	Η πρόσβαση πρέπει να περιορίζεται με Role-Based Access Control (RBAC) και να καταγράφεται κάθε ενέργεια για forensic ανάλυση και auditing.
OPERATIONAL DATA (MONITORING, ANALYSIS DATA)	Δεδομένα που συλλέγονται από το SIEM και άλλες πηγές παρακολούθησης για την ανίχνευση και αντιμετώπιση απειλών.	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	Τα δεδομένα πρέπει να παρακολουθούνται συνεχώς, να αναλύονται σε πραγματικό χρόνο και να διασφαλίζεται η ακεραιότητά τους μέσω hashing και immutable storage.
BACKUP/HISTORICAL DATA (BACKUP ΚΑΙ ΙΣΤΟΡΙΚΑ ΔΕΔΟΜΕΝΑ)	Δεδομένα που σχετίζονται με τη διατήρηση ιστορικών καταγραφών και την αποκατάσταση μετά από περιστατικά ασφαλείας.	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	Απαιτείται κρυπτογράφηση των backup, χρήση immutable storage και τακτικός έλεγχος της δυνατότητας

DOCUMENTATION (ΕΓΓΡΑΦΑ ΚΑΙ ΠΟΛΙΤΙΚΕΣ)	Τεκμηρίωση που αφορά τη λειτουργία του SOC και τις διαδικασίες απόκρισης σε περιστατικά ασφαλείας.	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	Πρέπει να υπάρχει περιορισμός πρόσβασης μέσω RBAC, καταγραφή αλλαγών (version control) και αποθήκευση σε ασφαλή τοποθεσία.

ΛΟΓΙΣΜΙΚΑ (SOFTWARE ASSETS)	**ΠΕΡΙΓΡΑΦΗ**	**ΑΣΦΑΛΕΙΑ**
COMMUNITY-DRIVEN AND ACCESSIBLE PLATFORMS (FREE-TIER TOOLS)	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.	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 (ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΛΟΓΙΣΜΙΚΑ)	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.	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.	
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ (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.	

ΥΛΙΚΟ (HARDWARE ASSETS)	ΠΕΡΙΓΡΑΦΗ	ΑΣΦΑΛΕΙΑ
ΣΥΣΚΕΥΕΣ ΧΡΗΣΤΩΝ	Περιλαμβάνουν συσκευές όπως κινητά τηλέφωνα, laptops, workstations που χρησιμοποιούνται για την πρόσβαση και εκτέλεση των καθηκόντων της υπηρεσίας SOC.	Πρέπει να εφαρμόζονται αυστηρές πολιτικές για την ασφαλή πρόσβαση στις συσκευές (π.χ. χρήση MFA, συστήματα απομακρυσμένης διαχείρισης για την προστασία των συσκευών).
ΣΥΣΚΕΥΕΣ ΔΙΚΤΥΟΥ	Αυτές οι συσκευές περιλαμβάνουν servers, firewalls, routers, και άλλα δικτυακά εξαρτήματα που χρησιμοποιούνται για την παρακολούθηση και διαχείριση της δικτυακής υποδομής.	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.
ΣΥΣΚΕΥΕΣ ΑΠΟΘΗΚΕΥΤΙΚΟΥ ΧΩΡΟΥ	Αφορά διακομιστές αρχείων και συστήματα NAS που χρησιμοποιούνται για την αποθήκευση δεδομένων.	Η κρυπτογράφηση των δεδομένων αποθήκευσης και η διαχείριση δικαιωμάτων πρόσβασης σε αυτά τα συστήματα είναι κρίσιμες για την αποφυγή της μη εξουσιοδοτημένης πρόσβασης.

Τα φυσικά αγαθά αντιμετωπίζονται ως ένα ενιαίο, το Headquarters, το οποίο περιλαμβάνει τα παρακάτω:

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)	ΠΕΡΙΓΡΑΦΗ	ΑΣΦΑΛΕΙΑ
OFFICES (COMPUTER ROOMS, CONFERENCE ROOM, …):	Περιλαμβάνει τα γραφεία, τα δωμάτια υπολογιστών και άλλους χώρους όπου διεξάγεται η εργασία της υπηρεσίας SOC.	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):	Τα κέντρα δεδομένων που φιλοξενούν τους servers, τα συστήματα δικτύου και την υποδομή αποθήκευσης.	Χρειάζεται αυστηρός έλεγχος πρόσβασης και κανονιστικά πλαίσια για την προστασία της υποδομής και την ασφαλή αποθήκευση των δεδομένων.
SECURITY SYSTEMS (CAMERAS, PHYSICAL CARDS, ALARMS):	Περιλαμβάνει τα συστήματα φυσικής ασφαλείας που χρησιμοποιούνται για την προστασία των χώρων και των υποδομών.	Η φυσική ασφάλεια πρέπει να συνδυάζεται με ψηφιακά συστήματα παρακολούθησης για να εξασφαλίζεται η προστασία σε όλους τους τομείς της υπηρεσίας.

1.5 Αποτίμηση Επιπτώσεων (Impact Assessment)

Οι επιπτώσεις που προκύπτουν από μια επικείμενη παραβίαση ή διαρροή στα πληροφοριακά αγαθά που ορίστηκαν παραπάνω, κατηγοριοποιούνται βάσει **εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας (CIA Triad)** και λαμβάνουν τις παρακάτω τιμές:

IMPACT ASSESSMENT

#	Asset	Asset Category	A	I	C	MAX
A1	Customer Data	Information	3	4	4	**4**
A2	SOC Internal Data	Information	2	3	4	**4**
A3	Operational Data	Information	4	4	3	**4**

A4	Backup/Historical Data	Information	4	4	3	**4**
A5	Documentation	Information	2	3	2	**3**

Όπου: Πολύ Χαμηλή = 0, Χαμηλή = 1, Μεσαία = 2, Υψηλή = 3, Πολύ Υψηλή = 4

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.

1.6 Αποτίμηση Απειλών (Threat Assessment) και Ευπαθειών (Vulnerability Assessment)

THREAT ASSESSMENT (INFORMATION ASSETS)

#	Asset	Threat Name	Threat Level	Threat Value	Security Controls	Vulnerability Level	Vulnerability Value
A1	Customer Data	Data Destruction	MEDIUM (M)	1	A system exists that conducts backup, Security Awareness Trianing program for all the mebmers of the company is in place, Access control policies, Malware protection systems(antivirus), firewall	HIGH (H)	2
		Information Disclosure	HIGH (H)	2		HIGH (H)	2
		Theft/Loss of data	HIGH (H)	2		MEDIUM (M)	1
		Unauthorised Access. E.g Hacking	HIGH (H)	2		HIGH (H)	2
A2	SOC Internal Data	Data Destruction	LOW (L)	0		MEDIUM (M)	1
		Information Disclosure	HIGH (H)	2		HIGH (H)	2
		Theft/Loss of data	MEDIUM (M)	1		MEDIUM (M)	1
		Unauthorised Access. E.g Hacking	HIGH (H)	2		MEDIUM (M)	1
A3	Operational Data	Data Destruction	MEDIUM (M)	1		HIGH (H)	2
		Information Disclosure	HIGH (H)	2		MEDIUM (M)	1
		Theft/Loss of data	HIGH (H)	2		HIGH (H)	2
		Unauthorised Access. E.g Hacking	HIGH (H)	2		HIGH (H)	2
A4	Backup/Historical Data	Data Destruction	HIGH (H)	2		MEDIUM (M)	1
		Information Disclosure	MEDIUM (M)	1		MEDIUM (M)	1
		Theft/Loss of data	MEDIUM (M)	1		LOW (L)	0
		Unauthorised Access. E.g Hacking	MEDIUM (M)	1		LOW (L)	0
A5	Documentation	Data Destruction	LOW (L)	0		LOW (L)	0
		Accidental/Intentional disclosure of information	MEDIUM (M)	1		LOW (L)	0
		Theft/Loss of data	MEDIUM (M)	1		LOW (L)	0
		Unauthorised Access. E.g Hacking	LOW (L)	0		LOW (L)	0

1.7 Αποτίμηση Κινδύνων (Risk Assessment)

Η αποτίμηση του κινδύνου για κάθε asset γίνεται προσθέτοντας τα impact value, threat value και vulnerability value, συμπεριλαμβάνοντας και το risk treatment plan.

ASSET	A	I	C	THREAT	THREAT VALUE	VULNERABILITY VALUE	R-A	R-I	R-C	RISK VALUE	RISK LEVEL	STRATEGY (ACCEPTANCE, AVOIDANCE, TRANSFERENCE, MITIGATION)	CONTROL IMPLENTATION	IMPLEMENTATION DATE (WITHIN THE NEXT COUPLE OF WEEKS, WITHIN THE NEXT SIX MONTHS, WITHIN THE NEXT 12 MONTHS)	RESIDUAL RISK
CUSTOMER DATA	3	4	4	Data Destruction (Ransomware attacks, insider threats, hardware/software failure)	1	2	6	7	7	7	HIGH	Mitigation	Data Loss Prevetion policy, Backup policy	within the next weeks	MEDIUM
SOC INTERNAL DATA	2	3	4	Accidental/Intentional disclosure of information	0	1	3	4	5	5	MEDIUM	Acceptance			MEDIUM
OPERATIONAL DATA	4	4	3	Theft/Loss of data	1	2	7	7	6	7	HIGH	Mitigation	Data Loss Prevetion policy, Backup policy	within the next weeks	MEDIUM
BACKUP/HISTORICAL DATA	4	4	3	Unauthorised Access. E.g Hacking	2	1	7	7	6	7	HIGH	Mitigation			MEDIUM
DOCUMENTATION	2	3	2	Data Destruction	0	0	2	3	2	3	MEDIUM	Acceptance			MEDIUM
CUSTOMER DATA	3	4	4	Accidental/Intentional disclosure of information (phishing, misconfigured oermissions, insider threats)	2	2	7	8	8	8	HIGH	Mitigation	Εσωτερικές επιθεωρήσεις και log auditing. Cyber Security Awareness Training programs, Identity Access Mangement	within the next weeks	MEDIUM
SOC INTERNAL DATA	2	3	4	Theft/Loss of data	2	2	6	7	8	8	HIGH	Mitigation			MEDIUM
OPERATIONAL DATA	4	4	3	Unauthorised Access. E.g Hacking	2	1	7	7	6	7	HIGH	Mitigation			MEDIUM
BACKUP/HISTORICAL DATA	4	4	3	Data Destruction	1	1	4	4	5	5	MEDIUM	Acceptance			MEDIUM
DOCUMENTATION	2	3	2	Accidental/Intentional disclosure of information	1	0	3	4	3	4	MEDIUM	Acceptance			MEDIUM
CUSTOMER DATA	3	4	4	Theft/Loss of data (malware, lost/stolen devices, unauthorized API access)	2	1	6	7	7	7	HIGH	Mitigation		within the next weeks	MEDIUM
SOC INTERNAL DATA	2	3	4	Unauthorised Access. E.g Hacking	1	1	4	5	6	6	HIGH	Mitigation	Endpoint Security, USB blocking, encryption		MEDIUM
OPERATIONAL DATA	4	4	3	Data Destruction	2	2	8	8	7	8	HIGH	Mitigation			MEDIUM
BACKUP/HISTORICAL DATA	4	4	3	Accidental/Intentional disclosure of information	1	0	5	5	3	5	MEDIUM	Acceptance			MEDIUM
DOCUMENTATION	2	3	2	Theft/Loss of data	1	0	3	4	3	4	MEDIUM	Acceptance			MEDIUM
CUSTOMER DATA	3	4	4	Unauthorized Access. E.g Hacking (brute force attacks, default credentials, privilege escalation)	2	2	7	8	8	8	HIGH	Mitigation	MFA everywhere, least privilege policy, Cyber Security Awareness Training	within the next weeks	MEDIUM
SOC INTERNAL DATA	2	3	4	Data Destruction	2	2	6	7	8	8	HIGH	Mitigation			MEDIUM
OPERATIONAL DATA	4	4	3	Accidental/Intentional disclosure of information	2	2	8	8	7	8	HIGH	Mitigation			MEDIUM
BACKUP/HISTORICAL DATA	4	4	3	Theft/Loss of data	1	0	5	5	4	5	MEDIUM	Acceptance			MEDIUM
DOCUMENTATION	2	3	2	Unauthorised Access. E.g Hacking	0	0	2	3	2	3	MEDIUM	Acceptance			MEDIUM

Επεξήγηση των βαθμολογιών:

Impact Assessment:
Very Low=0
Low=1
Medium=2
High=3
Very High=4

Impact Value	Impact Lelel
0	VERY LOW (VL)
1	LOW (L)
2	MEDIUM (M)
3	HIGH (H)
4	HIGH (H)

Threat and Vulnerability Assessment:
Low=1
Medium=2
High=3

Κλίμακα Αποτίμησης Απειλών

Επίπεδο Απειλής	Βαθμός Απειλής	Περιγραφή
LOW (L)	0	αναμένεται να συμβούν το πολύ μέχρι μία φορά κάθε 10 χρόνια
MEDIUM (M)	1	αναμένεται να συμβούν κατά μέσο όρο μία φορά τα 3 χρόνια.
HIGH (H)	2	αναμένεται να συμβούν κατά μέσο όρο μία φορά το χρόνο

Κλίμακα Αποτίμησης Αδυναμιών

Επίπεδο Αδυναμίας	Βαθμός Αδυναμίας	Περιγραφή
LOW (L)	0	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι < 33%
MEDIUM (M)	1	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι 33% - 66%
HIGH (H)	2	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι > 66%

Ο συνδυασμός της απειλής με την ευπάθεια, μας δίνει την πιθανότητα να συμβεί η απειλή=likelihood.

Likelihood Matrix									
Likelihood of Threat	Low			Medium			High		
	0	0	0	1	1	1	2	2	2
Vulnerability Level	L	M	H	L	M	H	L	M	H
	0	1	2	0	1	2	0	1	2
Likelihood Value of an incident scenario	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**

Likelihood Level	Likelihood Value
Very Low (Very Unlikely)	**0**
Low (Unlikely)	**1**
Medium (Possible)	**2**
High (Likely)	**3**
Very High (Frequent)	**4**

Risk Assessment:
Low=0-2
Medium=3-5
High=6-8

Κλίμακα Επικινδυνότητας	
Risk Level	**Risk Value**
Low	0 - 2
Medium	3 - 5
High	6 - 8

Ο αναλυτικός πίνακας:

Risk Scale Matrix						
Likelihood Value of an incident scenario		**0**	**1**	**2**	**3**	**4**
Likelihood Level		**Very Low (Very Unlikely)**	**Low (Unlikely)**	**Medium (Possible)**	**High (Likely)**	**Very High (Frequent)**
Very Low Business Impact	**0**	0	1	2	3	4
Low Business Impact	**1**	1	2	3	4	5
Medium Business Impact	**2**	2	3	4	5	6
High Business Impact	**3**	3	4	5	6	7
Very High Business Impact	**4**	4	5	6	7	8

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.

1.8 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 (ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ)
DATA DESTRUCTION	• Immutable Backups, Redundant storage (RAID, Cloud replication), SIEM monitoring για ανίχνευση διαγραφών
ACCIDENTAL INTENTIONAL DISCLOSURE	• Εσωτερικές επιθεωρήσεις και log auditing. Cyber Security Awareness Training programs, Identity Access Mangement
THEFT/LOSS OF DATA	• Endpoint Security, USB/Device control policies
UNAUTHORIZED ACCESS	• MFA everywhere, least privilege policy, Cyber Security Awareness Training

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.

1.9 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 6-8.

Θα προχωρήσουμε σε αποδοχή κινδύνου από την βαθμολογία 0-5.

2. 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.

SECURITY ROLES	ΡΟΛΟΣ	ΑΡΜΟΔΙΟΤΗΤΕΣ
CHIEF INFORMATION SECURITY OFFICER (CISO)	Υπεύθυνος για την ολοκληρωμένη στρατηγική κυβερνοασφάλειας του SOC	• 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	Επικεφαλής του SOC, επιβλέπει τη λειτουργία του και συντονίζει τις ομάδες ασφαλείας	• 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 ANALYST (L1 TIER)	Πρώτη γραμμή άμυνας, αναλύει alerts και κάνει triage περιστατικών	• Παρακολουθεί το SIEM για alerts • Κάνει αρχική ανάλυση απειλών (malware, phishing, network intrusions) • Ανοίγει tickets και τα κλιμακώνει σε L2/L3 αν απαιτείται
SOC ANALYST (L2 TIER)	Εμβαθύνει στα περιστατικά και εκτελεί ενεργή απόκριση	• Αναλύει δικτυακή κίνηση, logs και endpoints • Χρησιμοποιεί Threat Intelligence για ταυτοποίηση επιθέσεων • Εφαρμόζει μείωση απειλών (containment, eradication)
SOC ANALYST (L3 TIER)	Ειδικός σε Advanced Persistent Threats (APT) και forensic investigations	• Εκτελεί forensic ανάλυση και reverse engineering malware • Αναπτύσσει νέους κανόνες SIEM (correlation rules) • Συνεργάζεται με Threat Hunting και Red Teams
INCIDENT RESPONSE TEAM (IRT)	Αναλαμβάνει την αντιμετώπιση σοβαρών περιστατικών και την αποκατάσταση	• Δημιουργεί Incident Response Playbooks • Διερευνά επιθέσεις και εκτελεί containment & recovery • Συνεργάζεται με νομικά τμήματα για compliance & breach notifications
THREAT INTELLIGENCE TEAM	Συλλέγει πληροφορίες για επιθέσεις και προσαρμόζει την άμυνα του SOC	• Αναλύει νέα exploits και IoCs (Indicators of Compromise) • Τροφοδοτεί το SIEM με Threat Feeds • Συνεργάζεται με εθνικές αρχές και cybersecurity communities
SECURITY ENGINEERS	Υπεύθυνοι για τη σχεδίαση, υλοποίηση και διαχείριση των συστημάτων ασφαλείας	• Ρυθμίζουν και βελτιστοποιούν SIEM, IDS/IPS, Firewalls • Διαχειρίζονται Endpoint Detection & Response (EDR) λύσεις • Εφαρμόζουν Zero Trust Architecture και Network Segmentation
COMPLIANCE & GOVERNANCE TEAM	Επιβλέπει τη συμμόρφωση με τα κανονιστικά πλαίσια και τα security policies	• Διενεργεί εσωτερικούς και εξωτερικούς ελέγχους (audits) • Βεβαιώνει ότι τηρούνται GDPR, ISO 27001, NIST, SOC 2 • Συνεργάζεται με νομικές υπηρεσίες για data breach notifications

3. 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.

ΒΑΣΙΚΕΣ ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ	ΣΚΟΠΟΣ	ΚΥΡΙΕΣ ΑΡΧΕΣ	ΠΑΡΑΔΕΙΓΜΑΤΑ ΚΑΝΟΝΩΝ
ACCESS CONTROL POLICY (ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ)	Καθορίζει τους κανόνες πρόσβασης στα πληροφοριακά συστήματα και δεδομένα του SOC, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες έχουν τη σωστή πρόσβαση	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	• 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 (ΠΟΛΙΤΙΚΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ)	Διασφαλίζει ότι οι κωδικοί πρόσβασης είναι ισχυροί και προστατεύονται από μη εξουσιοδοτημένη πρόσβαση	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	• 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 (ΠΟΛΙΤΙΚΗ ΚΑΤΑΓΡΑΦΗΣ & ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ)	Καθορίζει ποιες δραστηριότητες καταγράφονται και πώς παρακολουθούνται για την ανίχνευση επιθέσεων και την απόκριση σε περιστατικά ασφαλείας	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)	• 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).

		Role-Based Access για πρόσβαση μόνο από εξουσιοδοτημένους χρήστες	
BACKUP & RECOVERY POLICY (ΠΟΛΙΤΙΚΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ & ΑΝΑΚΑΜΨΗΣ)	Διασφαλίζει ότι τα δεδομένα του SOC προστατεύονται από απώλεια και μπορούν να ανακτηθούν σε περίπτωση καταστροφής ή κυβερνοεπίθεσης	Πολιτική 3-2-1 για αντίγραφα ασφαλείας: τρία αντίγραφα των δεδομένων δυο διαφορετικά μέσα αποθήκευσης ένα 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	• 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)

ΒΑΣΙΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ	ΣΚΟΠΟΣ	ΒΗΜΑΤΑ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ		ΠΑΡΑΔΕΙΓΜΑ
ΔΙΑΔΙΚΑΣΙΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ (INCIDENT RESPONSE PROCESS)	Εξασφαλίζει ότι κάθε κυβερνοεπίθεση ή περιστατικό ασφαλείας αντιμετωπίζεται άμεσα και αποτελεσματικά, μειώνοντας τον αντίκτυπο στο SOC και στην επιχείρηση.	**1. 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. **2. Κατηγοριοποίηση βάσει σοβαρότητας:** Low: Δεν απαιτεί άμεση ενέργεια. Medium: Χρειάζεται παρακολούθηση. High: Άμεση απόκριση απαιτείται. Χρήση Threat Intelligence για συσχέτιση με γνωστές επιθέσεις. **3. Αντίδραση & Απομόνωση (Containment & Mitigation)** Αποσύνδεση μολυσμένων endpoints ή χρηστών από το δίκτυο. Εφαρμογή firewall rules για περιορισμό κακόβουλης κυκλοφορίας. Καθαρισμός και αποκατάσταση επηρεασμένων συστημάτων.	**4.Ανάκαμψη (Eradication & Recovery)** Επαναφορά από καθαρό backup. Αναβάθμιση συστημάτων και εφαρμογή patches. Δοκιμές για επαλήθευση ότι το σύστημα είναι καθαρό. **5. Αναφορά & Βελτίωση (Reporting & Lessons Learned)** Δημιουργία αναφοράς περιστατικού. Αναθεώρηση πολιτικών και διαδικασιών ασφαλείας. Εκπαίδευση προσωπικού για αποφυγή παρόμοιων επιθέσεων.	Αντίδραση σε Ransomware Attack: Αναγνώριση: SIEM alert για μαζική κρυπτογράφηση αρχείων σε endpoint Ανάλυση: Ο SOC Analyst (L1) βλέπει ότι ο χρήστης "User123" εκτελεί άγνωστα PowerShell scripts. Αντίδραση: Ο SOC Analyst (L2) αποσυνδέει το endpoint από το δίκτυο. Ανάκτηση: Ο SOC Manager (L3) εφαρμόζει immutable backup restore για ανάκτηση αρχείων. Αναφορά & Lessons Learned: Εφαρμόζονται επιπλέον EDR rules για ανίχνευση κακόβουλων PowerShell εκτελέσεων στο μέλλον.
ΔΙΑΔΙΚΑΣΙΑ BACKUP	Εξασφαλίζει ότι τα δεδομένα διατηρούνται ασφαλή και μπορούν να	**1. Δημιουργία Backup** Καθημερινά incremental backups και εβδομαδιαία full backups.	**3. Δοκιμή Ανάκτησης (Restore Testing)** Κάθε 3 μήνες, γίνεται δοκιμή ανάκτησης δεδομένων.	Αν ένας server καταστραφεί, η ομάδα SOC ανακτά τα δεδομένα από το backup και επαναφέρει τη λειτουργία χωρίς απώλειες.

	ανακτηθούν σε περίπτωση καταστροφής ή κυβερνοεπίθεσης.	Αποθήκευση backup σε τρία διαφορετικά μέσα (τοπικό NAS, cloud, offline air-gapped). Κρυπτογράφηση των backup (AES-256). **2. 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	Επαλήθευση ότι το backup είναι λειτουργικό και δεν έχει διαφθαρεί. **4. 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.	
ΔΙΑΔΙΚΑΣΙΑ ΔΗΜΙΟΥΡΓΙΑΣ / ΔΙΑΓΡΑΦΗΣ ΧΡΗΣΤΗ	Εξασφαλίζει ότι οι λογαριασμοί χρηστών δημιουργούνται, διαχειρίζονται και διαγράφονται με ασφαλή και ελεγχόμενο τρόπο.	**1. 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). **2. Αλλαγή Δικαιωμάτων (User Modification)** Αιτήματα αλλαγής πρόσβασης εξετάζονται και εγκρίνονται από ανώτερο υπάλληλο. Οι αλλαγές καταγράφονται στο SIEM για auditing.	**3. 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.	Όταν ένας υπάλληλος αποχωρεί, ο λογαριασμός του απενεργοποιείται, τα credentials διαγράφονται και η πρόσβασή του αποκόπτεται από το σύστημα.