

CADMUS-SGTTX-20

Cyber Crisis Leadership Challenge (Serious Games)

Σας προσκαλούμε να παρακολουθήσετε τα διαδικτυακά μαθήματα που προσφέρονται μέσω της πλατφόρμας CADMUS (<https://cadmus.uom.gr/>) της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ). Η πλατφόρμα CADMUS προσφέρει ένα οικοσύστημα εκπαίδευσης και κατάρτισης στην Κυβερνοασφάλεια, σε πλήρη συμβατότητα με το Ευρωπαϊκό Πλαίσιο ECSF. Τα προσφερόμενα μαθήματα ακολουθούν ποικίλες δομές, όπως Bootcamps, Cyber Ranges, Serious Games και Tabletop Exercises.

Άμεσα, μπορείτε να εγγραφείτε στο μάθημα **CADMUS-SGTTX-20** (<https://cadmus.uom.gr/moodle/course/view.php?id=44>), με τίτλο **Cyber Crisis Leadership Challenge (Serious Game)**, το οποίο προσφέρεται από 21/09/2026 έως 16/10/2026, και να μελετήσετε το πολύ ενδιαφέρον περιεχόμενό του. Πρόκειται για ένα ολοκληρωμένο μάθημα που περιέχει ένα διαδραστικό εκπαιδευτικό παιχνίδι (Serious Game), το απαραίτητο θεωρητικό μέρος και διαδραστικές ασκήσεις. Το εκπαιδευτικό παιχνίδι είναι σχεδιασμένο για την ανάπτυξη δεξιοτήτων ηγεσίας σε περιστατικά κυβερνοασφάλειας, ιεράρχησης κινδύνων, λήψης τεκμηριωμένων αποφάσεων και αποτελεσματικής επικοινωνίας με τα ενδιαφερόμενα μέρη.

Στο εκπαιδευτικό παιχνίδι αναλαμβάνετε το ρόλο ενός νεοδιορισμένου Chief Information Security Officer (CISO) στο δικτυακό περιβάλλον ενός οργανισμού, με τα βασικά του στοιχεία όπως servers, routers, σταθμούς εργασίας και Policy Centers. Στον οργανισμό δεν έχει πραγματοποιηθεί συνολική αξιολόγηση κυβερνοασφάλειας τα τελευταία χρόνια. Ξεκινάτε με περιορισμένο προϋπολογισμό, αυστηρούς χρονικούς περιορισμούς και Action Points, δηλαδή την ικανότητά σας να εκτελείτε ενέργειες.

Το σενάριο του παιχνιδι περιλαμβάνει προκλήσεις, καθώς δεν είναι δυνατόν να πραγματοποιήσετε όλες τις διαθέσιμες ενέργειες: θα πρέπει να επιθεωρήσετε τα συστήματα, να ιεραρχήσετε τις λύσεις θωράκισης του οργανισμού, να επιλέξετε ενέργειες και να αιτιολογήσετε τις αποφάσεις σας. Οι επιλογές σας επηρεάζουν την κατάσταση κυβερνοασφάλειας του οργανισμού (Cybersecurity State), τον επιχειρησιακό αντίκτυπο (Business Impact), την εμπιστοσύνη των ενδιαφερόμενων μερών (Stakeholder Trust) και τους διαθέσιμους οικονομικούς πόρους.

Ιδιαίτερη έμφαση δίνεται στη μετάβαση από την απλή αντιμετώπιση μεμονωμένων τεχνικών προβλημάτων προς μια περισσότερο ώριμη και συστηματική προσέγγιση κυβερνοασφάλειας. Το σενάριο συνδέει στην πράξη έννοιες, όπως Cybersecurity Maturity, Risk Management, Governance, Asset Management και Continuous Improvement.

Κατά την εκτέλεση του παιχνιδιού, προσπαθήστε να μην εστιάζετε αποκλειστικά στο ερώτημα «ποια ευπάθεια μπορώ να διορθώσω;», αλλά στα ερωτήματα: «ποια υπηρεσία είναι σημαντικότερη για τον οργανισμό;», «ποιος είναι ο πραγματικός κίνδυνος;», «ποια ενέργεια προσφέρει τη μεγαλύτερη αξία με τους διαθέσιμους πόρους;», «ποια στοιχεία υποστηρίζουν την απόφασή σας και πώς θα την εξηγήσετε στη διοίκηση;».

Το εκπαιδευτικό παιχνίδι έχει στόχο να σας εκπαιδεύσει να σκέφτεστε όχι μόνο ως τεχνικός επαγγελματίας κυβερνοασφάλειας, αλλά ως ηγέτης κυβερνοασφάλειας και μελλοντικός CISO, ικανός να συνδέει την τεχνική κατάσταση με τον επιχειρησιακό κίνδυνο, να κατανέμει περιορισμένους πόρους, να τεκμηριώνει αποφάσεις και να καθοδηγεί τη συνεχή βελτίωση της κυβερνοασφάλειας του οργανισμού.

Το μάθημα είναι πλήρως ασύγχρονο και ολοκληρώνεται με τελική αξιολόγηση. Χορηγούνται Πιστοποιητικό Συμμετοχής και Πιστοποιητικό Επιτυχούς Ολοκλήρωσης, με κατώφλι επιτυχίας 50%.

Σχετικές οδηγίες για την εγγραφή σας στην πλατφόρμα και στο μάθημα θα βρείτε στο συνημμένο έγγραφο.

Για οποιαδήποτε απορία ή βοήθεια, μπορείτε να απευθυνθείτε στο email: notas@uom.edu.gr και στο τηλέφωνο 2310891839.