

SPECIAL FEATURE

ΜΗΝΙΑΙΑ ΕΚΔΟΣΗ ΓΙΑ ΤΗΝ ΚΥΠΡΙΑΚΗ  
ΑΓΟΡΑ & ΤΑ ΣΤΕΛΕΧΗ | ΤΕΥΧΟΣ 201  
ΝΟΕΜΒΡΙΟΣ 2022  
ΤΙΜΗ €2.00

# IN Business

**20** YEARS **ODYSSEY™**  
cybersecurity

**20**  
**YEARS**  
**AHEAD**



Εμπειρία, καινοτομία και εξειδίκευση στην κυβερνοασφάλεια



5291295000102  
www.inbusinessnews.com

ODYSSEY

# 20 ΧΡΟΝΙΑ

---

εμπειρίας, καινοτομίας και εξειδίκευσης στην κυβερνοασφάλεια

---

Με 140 άτομα προσωπικό σε τέσσερις χώρες, εκ των οποίων το 70% να αποτελεί εξειδικευμένους μηχανικούς, σύμβουλους και αναλυτές στην κυβερνοασφάλεια, η Odyssey αποτελεί τον μεγαλύτερο, και πιθανώς παλαιότερο, οργανισμό στην ευρύτερη περιοχή με ξεκάθαρη εξειδίκευση και 20ετή εμπειρία στον τομέα της.

TASPRO

## ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΣ ΣΕ ΕΝΑ ΣΥΝΕΧΩΣ ΜΕΤΑΒΑΛΛΟΜΕΝΟ ΤΟΠΙΟ ΑΠΕΙΛΩΝ

Ο κόσμος αλλάζει συνεχώς, με απρόβλεπτες αλλαγές που χαρακτηρίζονται από αστάθεια, αβεβαιότητα, πολυπλοκότητα αλλά και ασάφεια. Τα θέματα κυβερνοασφάλειας, η προστασία και η ανθεκτικότητα των πληροφοριακών συστημάτων, απέναντι στις συνεχώς εξελισσόμενες απειλές του σύγχρονου κυβερνοχώρου, είναι πλέον πιο επίκαιρα από ποτέ. Οι οργανισμοί αναζητούν τρόπους για να διασφαλίσουν την ικανότητά τους όχι μόνο να προβλέπουν και να ανταποκρίνονται σε αναδυόμενες απειλές αλλά και να μπορούν να ανακάμπτουν γρήγορα με στόχο την κυβερνοανθεκτικότητα. Την ίδια στιγμή, η στρατηγική κάθε σύγχρονου οργανισμού εστιάζεται στην ψηφιακή μεταρρύθμιση, η οποία αποτελεί επιβλητική ανάγκη. Ανάμεσα στις μεγάλες προκλήσεις που εμπεριέχει ένα έργο τέτοιου μεγέθους, σημαντικότητας αλλά και διάρκειας, βρίσκεται και η ασφάλεια της πληροφορίας ενός οργανισμού. Η πολυπλοκότητα που δημιουργείται στο IT οικοσύστημα από την όλο και μεγαλύτερη εξάρτηση σε τρίτους παράγοντες, όπως πάροχους υπηρεσιών Cloud και τεχνολογικών εφαρμογών, καθώς και η εδραίωση της τηλεργασίας, δημιουργούν ένα καινούργιο φάσμα ψηφιακών κινδύνων.

## ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΚΑΙ ΚΛΙΜΑΚΩΣΗ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

Την ίδια στιγμή, ο κυβερνοπόλεμος στην Ουκρανία με βασικό παράγοντα τις κυβερνοεπιθέσεις σε κρίσιμους τομείς υποδομών και κατ' επέκταση την εκμετάλλευση πληροφοριών και χρήση τους για επιθέσεις ή εκβιασμούς, ήρθε να συμβάλει στην περαιτέρω διεύρυνση του τοπίου απειλών. Συγκεκριμένα, από τα τέλη Φεβρουαρίου μέχρι και πρόσφατα, έχει παρατηρηθεί κλιμάκωση στον αριθμό των αναφερόμενων κυβερνοεπιθέσεων εναντίον ουκρανικών ιδρυμάτων, οργανισμών αλλά και του γενικού πληθυσμού. Οι state-sponsored hackers, που στην ουσία αντιπροσωπεύουν τους καλύτερους στο είδος τους, χρησιμοποιούν τις πιο εξελιγμένες τεχνικές επιθέσεων εναντίον των κρατών, τις οποίες εκμεταλλεύονται και αντιγράφουν κυβερνοεγκληματίες, στοχεύοντας με τη σειρά τους οργανισμούς ανά την υφήλιο με άνωτερο στόχο το οικονομικό όφελος. Μάλιστα, σε κάποιες περιπτώσεις είναι τόσο καινοτόμες αυτές οι τεχνικές, που χαρακτηρίζονται πρωτόγνωρες. Η εν λόγω γεωπολιτική κατάσταση έκανε την παγκόσμια κοινότητα να συνειδητοποιήσει την αναγκαιότητα και τη σημαντικότητα της κυβερνοασφάλειας στην προστασία των πληροφοριακών συστημάτων και στη διατήρηση της ακεραιότητας των υποδομών.

## ΔΙΑΣΦΑΛΙΖΟΝΤΑΣ ΤΗΝ ΑΝΘΕΚΤΙΚΟΤΗΤΑ ΤΗΣ ΥΠΟΔΟΜΗΣ ΚΑΙ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Στο νέο αυτό περιβάλλον, το πλαίσιο διαχείρισης κινδύνου αλλάζει δραματικά, ενώ η έννοια της αρχιτεκτονικής περιμετρικής ασφάλειας, όπως τη γνωρίζουμε, δεν είναι πλέον επαρκής. Ταυτόχρονα, η ελάχιστη εμπειρία ή ακόμα και η άγνοια ως προς τους ψηφιακούς κινδύνους που αναδύονται, ενδέχεται να εκθέσουν έναν οργανισμό σε νέους τύπους απειλών, αυξάνοντας έτσι σημαντικά τον κίνδυνο παραβίασης της ασφάλειας των υποδομών του.

«Όραμα μας είναι να παρέχουμε πραγματική αξία στους εργαζομένους και στους πελάτες μας, με εξειδικευμένες λύσεις, υπηρεσίες και προϊόντα, παραμένοντας πάντα ένα βήμα μπροστά από την εποχή και το συνεχώς μεταβαλλόμενο τοπίο απειλών.»

ΕΛΕΥΘΕΡΙΟΣ ΑΝΤΩΝΙΑΔΗΣ,  
CTO & FOUNDER, ODYSSEY





Για να αντιμετωπιστούν αυτές οι προκλήσεις, ένας οργανισμός δεν πρέπει να διαχειρίζεται μεμονωμένα ή τη στιγμή που προκύπτουν τα θέματα που αφορούν στην ασφάλεια και στη διαθεσιμότητα. Η κυβερνοασφάλεια δεν αφορά μόνο το τμήμα τεχνολογίας αλλά πρέπει να αναγνωρίζεται και να τυγχάνει χειρισμού κατά τον καθορισμό των εταιρικών στόχων του οργανισμού και τη διαμόρφωση της στρατηγικής του.

### ODYSSEY: ΣΤΡΑΤΗΓΙΚΟΣ ΣΥΝΕΡΓΑΤΗΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟ CLOUD

Η Odyssey ιδρύθηκε πριν από 20 χρόνια, σε ένα τομέα τότε άγνωστο στον περισσότερο κόσμο, με το διαδίκτυο να βρίσκεται ακόμη σε νηπιακή μορφή. Στόχος της είναι να παρέχει εξειδικευμένες και ολιστικές υπηρεσίες ανίχνευσης και διαχείρισης κινδύνου στην ασφάλεια πληροφοριών, διασφαλίζοντας έτσι τη βιωσιμότητα και εξέλιξη των οργανισμών. Σε ένα τοπίο απειλών που διευρύνεται και αλλάζει με τρομερά γρήγορους ρυθμούς, που δημιουργεί καινούριες προκλήσεις και απαιτεί εξειδικευμένη γνώση και εμπειρία, η Odyssey με 20ετή πορεία στον χώρο της κυβερνοασφάλειας έχει αποδείξει ότι μπορεί να αποτελέσει τον στρατηγικό συνεργάτη των οργανισμών που έχουν ως στόχο την κυβερνοανθεκτικότητα. Διαθέτοντας την απαραίτητη τεχνογνωσία, εμπειρία και ανθρώπινο δυναμικό, αλλά και εφαρμόζοντας μια ολιστική προσέγγιση, υποστηρίζει τους οργανισμούς στη στρατηγική ασφάλειας της πληροφορίας τους, στον σχεδιασμό, την εφαρμογή, την παρακολούθηση, τη διατήρηση αλλά και τη συνεχή ενημέρωση των αναγκών τεχνολογιών και διαδικασιών. Μέσω της ολιστικής προσέγγισης, υποστηρίζει τους οργανισμούς με τις απαραίτητες λύσεις και υπηρεσίες για την αποτελεσματική διαχείριση των Ψηφιακών Κινδύνων σε όλες τις λειτουργικές πτυχές ενός οργανισμού (ανθρώπους, διαδικασίες, τεχνολογία).

Η ολιστική αυτή προσέγγιση συμπεριλαμβάνει έξι πυλώνες με λύσεις, υπηρεσίες αλλά και προϊόντα, όπως: ClearSkies™ Threat & Vulnerability Management Platform, Managed Security/Managed Detection & Response Services, Governance, Risk & Compliance, Threat Risk Assessment services, Cloud Security και Integrated Solutions. Κάθε ένας απ' αυτούς, χωριστά ή σε συνδυασμό, συμβάλλει επίσης στην αποτελεσματική διαχείριση του Λειτουργικού Κινδύνου ενός οργανισμού, δημιουργώντας έναν ανθεκτικό οργανισμό που μπορεί να προβλέπει αποτελεσματικά, να ανταποκρίνεται, να ανακάμπτει γρήγορα και να προσαρμόζεται σε αναδυόμενες απειλές, διασφαλίζοντας έτσι την επιχειρησιακή του συνέχεια.

### ΠΑΓΚΟΣΜΙΑ ΑΝΑΓΝΩΡΙΣΗ

Η Odyssey έχει αναγνωριστεί από την Gartner, στο Magic Quadrant του 2021, για το προϊόν της ClearSkies™, ως ένα από τα 20 καλύτερα παγκοσμίως στην κατηγορία Security Information and Event Management. Επίσης, κέρδισε το Βραβείο Καινοτομίας της OEB τόσο το 2018 όσο και το 2021, το Παγκόσμιο Data Impact Award αλλά και τα Business IT Excellence (BITE) Awards το 2015. Η πλατφόρμα αυτή, προσφέρει ορατότητα σε πραγματικό χρόνο της κατάστασης ετοιμότητας σχετικά με την ασφάλεια ενός οργανισμού. Η εταιρεία είναι επίσης πιστοποιημένη με ISO 27001, ISO 9001, SOC 2 Type 2 και ISO 22301 και διαπιστευμένη ως Qualified Security Assessor (QSA) από το Payment Card Industry Security Standards Council (PCI SSC). Παράλληλα, έχει διακριθεί ανάμεσα στις κορυφαίες εταιρείες στον κόσμο όσον αφορά το καλύτερο εργασιακό περιβάλλον, με το πιστοποιητικό Great Place to Work. Η εταιρεία έχει γραφεία σε Ελλάδα, Κύπρο, Σαουδική Αραβία και Ηνωμένο Βασίλειο, ενώ το πελατολόγιό της αποτελείται από οργανισμούς διαφορετικού μεγέθους, τομέα και πολυπλοκότητας, σε 35 χώρες.

«Όσο παρατηρούμε το πεδίο απειλών να διευρύνεται τόσο προσπαθούμε να βγαινουμε εκτός των ορίων μας. Στόχος μας η περαιτέρω εξάπλωσή μας στην Ευρώπη και η είσοδός μας στην αγορά των ΗΠΑ».

ΧΡΙΣΤΟΣ ΟΝΟΥΦΡΙΟΥ,  
ODYSSEY CEO







# YEARS AHEAD

Working Together to make the World a Cyber Safer Place

OFFICES CYPRUS | GREECE | USA | UK | GULF REGION  
[www.odysseycs.com](http://www.odysseycs.com)