

Odyssey Cybersecurity Engineering Cyber Resilience στην Εποχή του AI

Σε ένα τοπίο όπου οι κυβερνοαπειλές γίνονται ταχύτερες και πιο απρόβλεπτες λόγω AI, η παραδοσιακή άμυνα δεν αρκεί. Η Odyssey επαναπροσδιορίζει την ασφάλεια ως επιχειρησιακή ετοιμότητα, μετατρέποντας τη συμμόρφωση σε στρατηγικό πλεονέκτημα και προσφέροντας στους οργανισμούς τον απόλυτο έλεγχο (Under Ctrl) απέναντι στον ψηφιακό κίνδυνο..

ΤΗΣ ΑΓΓΕΛΙΚΗΣ ΚΟΡΡΕ

2

Η ραγδαία εξέλιξη της Τεχνητής Νοημοσύνης και η αυξανόμενη πολυπλοκότητα των υβριδικών ψηφιακών περιβαλλόντων μεταμορφώνουν το πεδίο της κυβερνοασφάλειας. Οι οργανισμοί σήμερα δεν αναζητούν απλώς περισσότερα εργαλεία ασφάλειας, αλλά έναν στρατηγικό συνεργάτη που θα τους βοηθήσει να διατηρούν συνεχή ορατότητα, να εντοπίζουν έγκαιρα τις απειλές και να ανταποκρίνονται αποτελεσματικά σε πραγματικό χρόνο. Για να παραμείνουν ασφαλείς και ανταγωνιστικοί, χρειάζεται να ξεπεράσουν τα παραδοσιακά μοντέλα άμυνας και να αναπτύξουν την ικανότητα να εντοπίζουν, να κατανοούν και να αντιμετωπίζουν απειλές σε πραγματικό χρόνο, ενισχύοντας έτσι την κυβερνοανθεκτικότητά τους.

Σε αυτή τη συνέντευξη, ο General Manager Ελλάδος της Odyssey Cybersecurity, Απόστολος Πανδρούλας, μιλά για τις νέες προκλήσεις που διαμορφώνουν το τοπίο της κυβερνοασφάλειας το 2026 και εξηγεί πώς η εταιρεία επενδύει συστηματικά στην καινοτομία και στην ανάπτυξη λύσεων που αξιοποιούν την τεχνητή νοημοσύνη. Παρουσιάζει την ολοκληρωμένη προσέγγιση της Odyssey, η οποία συνδυάζει τεχνολογία, διακυβέρνηση και αυτοματοποίηση με τη δύναμη της τεχνητής νοημοσύνης, μέσα από την πλατφόρμα TDIR και τις υπηρεσίες Managed Services. Στόχος είναι να βοηθήσει τους οργανισμούς να ενισχύσουν την κυβερνοανθεκτικότητά τους και να διατηρούν έλεγχο, επιχειρησιακή συνέχεια και εμπιστοσύνη σε ένα ολοένα πιο απαιτητικό ψηφιακό περιβάλλον.

Το 2026 το τοπίο των κυβερνοαπειλών γίνεται πιο σύνθετο, ταχύτερο και πιο απρόβλεπτο, με την AI καθημερινά να ενισχύει και την πλευρά των επιτιθέμενων. Πώς βλέπετε να αλλάζει συνολικά η έννοια της κυβερνοασφάλειας και πώς εξελίσσεται η Odyssey για να ανταποκριθεί σε αυτή τη νέα πραγματικότητα;

Σε μια εποχή όπου οι κυβερνοαπειλές εξελίσσονται και κλιμακώνονται με πρωτοφανή ταχύτητα, συχνά με υψηλό βαθμό αυτονομίας, τα παραδοσιακά εργαλεία κυβερνοασφάλειας δεν επαρκούν πλέον για να αντιμετωπίσουν τη νέα αυτή πολυπλοκότητα. Οι επιθέσεις αξιοποιούν ολοένα και περισσότερο την αυτοματοποίηση και την τεχνητή νοημοσύνη, ενώ περιστατικά όπως identity compromise, ransomware-as-a-service και επιθέσεις στην εφοδιαστική αλυσίδα γίνονται όλο και συχνότερα.

Ο ψηφιακός κίνδυνος έχει πλέον μετατραπεί σε κρίσιμο επιχειρησιακό ζήτημα. Για να παραμείνουν ασφαλείς και ανταγωνιστικοί, οι οργανισμοί χρειάζεται να μπορούν να εντοπίζουν, να κατανοούν και να αντιμετωπίζουν απειλές σε πραγματικό χρόνο, ενισχύοντας την κυβερνοανθεκτικότητά τους.

Σε αυτή την κατεύθυνση, η Odyssey επενδύει διαρκώς στην εξέλιξη της πλατφόρμας TDIR (Threat Detection, Investigation & Response), αξιοποιώντας τεχνολογία, αυτοματοποίηση, τεχνητή νοημοσύνη και ανθρώπινη εξειδίκευση. Στόχος μας είναι να βοηθάμε τους οργανισμούς να διατηρούν έλεγχο, ταχύτητα λήψης αποφάσεων και επιχειρησιακή συνέχεια σε ένα ολοένα πιο απαιτητικό περιβάλλον απειλών.

Μέσα σε αυτό το περιβάλλον, η Odyssey έχει καταφέρει να ξεχωρίσει και διεθνώς. Ποια είναι τα βασικά στοιχεία της προσέγγισής σας που σας διαφοροποιούν και τι σημαίνει στην πράξη για έναν οργανισμό το μοντέλο που προωθείτε;

Η βασική μας διαφοροποίηση είναι ότι δεν αντιμετωπίζουμε την κυβερνοασφάλεια ως άθροισμα τεχνολογιών, αλλά ως ζήτημα επιχειρησιακής ετοιμότητας και διαχείρισης κινδύνου.

Πολλοί οργανισμοί επενδύουν σε εργαλεία χωρίς να τα εντάσσουν σε ένα ενιαίο λειτουργικό μοντέλο. Αυτό οδηγεί σε κατακερματισμένη ορατότητα, καθυστερημένες



Απόστολος Πανδρούλα

3

αντιδράσεις και δυσκολία κατανόησης του πραγματικού κινδύνου.

Η προσέγγιση της Odyssey βασίζεται στην ενοποίηση τεχνολογίας, διαδικασιών και ανθρώπινης εμπειρίας ώστε τα δεδομένα ασφάλειας να μετατρέπονται σε πραγματική επιχειρησιακή εικόνα κινδύνου.

Στην πράξη αυτό σημαίνει για έναν οργανισμό, καλύτερη και πιο ολοκληρωμένη ορατότητα, ταχύτερη και πιο στοχευμένη απόκριση σε περιστατικά, πιο καθαρές προτεραιότητες σε επίπεδο κινδύνου και ένα ώριμο λειτουργικό πλαίσιο για να αντιμετωπίζει απειλές χωρίς να λειτουργεί διαρκώς αντιδραστικά.

Σε ένα περιβάλλον όπου οι επιθέσεις εξελίσσονται συνεχώς, η πραγματική αξία ενός συνεργάτη δεν βρίσκεται μόνο στην τεχνολογία που διαθέτει, αλλά στην ικανότητά του να βοηθά έναν οργανισμό να λειτουργεί με σταθερότητα, σαφήνεια και πραγματικό επιχειρησιακό έλεγχο. Να διατηρεί, δηλαδή, την ασφάλεια και τις κρίσιμες λειτουργίες του οργανισμού υπό έλεγχο (Under Ctrl) ακόμη και όταν το περιβάλλον γίνεται πιο ασταθές.

Πολλοί οργανισμοί αναζητούν σήμερα όχι απλώς τεχνολογία, αλλά λειτουργική υποστήριξη, ταχύτητα και εξειδικευμένο ανθρώπινο δυναμικό. Πώς καταφέρνει

η Odyssey να λειτουργεί ως πραγματική προέκταση της ομάδας του πελάτη;

Οι οργανισμοί σήμερα λειτουργούν σε ένα περιβάλλον όπου οι απειλές αυξάνονται, τα τεχνολογικά περιβάλλοντα γίνονται πιο σύνθετα και η εξειδικευμένη γνώση στον τομέα της κυβερνοασφάλειας παραμένει περιορισμένη.

Η Odyssey λειτουργεί ως προέκταση της ομάδας του πελάτη γιατί προσαρμόζει το μοντέλο υπηρεσιών της στις ανάγκες, στις προτεραιότητες και στο επίπεδο ωριμότητας κάθε οργανισμού. Αυτό μεταφράζεται σε 24/7 παρακολούθηση και συνεχή ανίχνευση απειλών, γρήγορη αξιολόγηση συμβάντων, σαφείς διαδικασίες απόκρισης και άμεση πρόσβαση σε εξειδικευμένους αναλυτές. Για τον πελάτη, η διαφορά είναι ουσιαστική. Δεν συνεργάζεται απλώς με έναν εξωτερικό πάροχο, αλλά με μια ομάδα που ενσωματώνεται στην καθημερινή του λειτουργία και ενισχύει ουσιαστικά την ετοιμότητα, την ταχύτητα αντίδρασης και τη συνολική ανθεκτικότητα του οργανισμού.

Με τις απαιτήσεις όπως η NIS2 και το DORA να ανεβάζουν τον πήχη, πώς βοηθάτε τους οργανισμούς να μετατρέψουν τη συμμόρφωση από αποσπασματική υποχρέωση σε πιο ώριμο μοντέλο ανθεκτικότητας, διακυβέρνησης και ετοιμότητας;

Οι νέες ευρωπαϊκές οδηγίες όπως η NIS2 και η DORA αλλάζουν σημαντικά τη φιλοσοφία της κυβερνοασφάλειας. Δεν περιορίζονται σε τεχνικές απαιτήσεις, αλλά δίνουν έμφαση στη λειτουργική ανθεκτικότητα και στη διακυβέρνηση κινδύνου.

Στην πράξη αυτό σημαίνει ότι οι οργανισμοί πρέπει να μπορούν να αποδείξουν πως διαθέτουν σαφείς διαδικασίες, επαρκή ορατότητα, δομημένη διαχείριση κινδύνου και ικανότητα αποτελεσματικής απόκρισης σε περιστατικά.

Ο ρόλος της Odyssey είναι να βοηθά τους οργανισμούς να μετατρέπουν αυτές τις απαιτήσεις σε ένα πρακτικό και εφαρμόσιμο operational model. Αυτό σημαίνει να υποστηρίζουμε τους οργανισμούς στην σαφή αποτύπωση και αξιολόγηση του κινδύνου, στον καθορισμό ξεκάθαρων ρόλων και διαδικασιών, στη συνεχή παρακολούθηση και ανίχνευση απειλών, καθώς και στην ενεργή εμπλοκή της διοίκησης στη διαχείριση των κυβερνοκινδύνων.

Όταν αυτή η προσέγγιση εφαρμοστεί σωστά, η συμμόρφωση παύει να αποτελεί απλώς μια κανονιστική υποχρέωση και μετατρέπεται σε έναν ουσιαστικό μηχανισμό ωρίμανσης του οργανισμού, ενισχύοντας τη διακυβέρνηση, τη λειτουργική πειθαρχία και τη συνολική ανθεκτικότητά του.

αποτελεσματική δυνατότητα πρόληψης, ανίχνευσης και απόκρισης, τότε η κυβερνοασφάλεια παύει να αντιμετωπίζεται ως κόστος και μετατρέπεται σε παράγοντα ανάπτυξης και ψηφιακής ωριμότητας.

Συχνά η ασφάλεια αντιμετωπίζεται ως κόστος. Μπορείτε να μας δώσετε παραδείγματα όπου οι επενδύσεις στην κυβερνοασφάλεια μέσω της Odyssey λειτούργησαν ως καταλύτης για τον ψηφιακό μετασχηματισμό και την ανάπτυξη μιας εταιρείας;

Στην πραγματικότητα, η κυβερνοασφάλεια δεν είναι απλώς ένα λειτουργικό κόστος. Είναι βασική προϋπόθεση για να μπορέσει ένας οργανισμός να προχωρήσει στον ψηφιακό του μετασχηματισμό με ασφάλεια και αυτοπεποίθηση.

Έχουμε δει αρκετές περιπτώσεις όπου η επένδυση σε ένα πιο ώριμο μοντέλο ασφάλειας λειτούργησε ως επιταχυντής αλλαγής. Για παράδειγμα, οργανισμοί που σχεδίαζαν να μεταφέρουν κρίσιμες λειτουργίες στο cloud δεν μπορούσαν να προχωρήσουν χωρίς επαρκή ορατότητα και δυνατότητα συνεχούς monitoring. Με

Χτίζουμε ένα μοντέλο ψηφιακής ανθεκτικότητας που μετασχηματίζει τον κίνδυνο σε πλεονέκτημα και προσφέρει πραγματικό έλεγχο σε κάθε επιχείρηση

Καθώς οι επιχειρήσεις επιταχύνουν τον ψηφιακό τους μετασχηματισμό, μεταφέρουν workloads στο cloud και λειτουργούν σε όλο και πιο υβριδικά περιβάλλοντα, πώς μπορεί η κυβερνοασφάλεια να λειτουργήσει όχι ως φρένο, αλλά ως καταλύτης ευελιξίας, ανάπτυξης και εμπιστοσύνης;

Για πολλά χρόνια υπήρχε η αντίληψη ότι η ασφάλεια επιβραδύνει την πρόοδο. Στην πράξη, σήμερα ισχύει το αντίθετο. Καθώς οι οργανισμοί μεταφέρουν υποδομές στο cloud, συνεργάζονται με τρίτους παρόχους και λειτουργούν σε ολοένα και πιο διασυνδεδεμένα οικοσυστήματα, η κυβερνοασφάλεια γίνεται προϋπόθεση για βιώσιμο ψηφιακό μετασχηματισμό.

Χωρίς επαρκή ορατότητα και έλεγχο, κάθε νέο ψηφιακό βήμα αυξάνει εκθετικά την έκθεση σε κίνδυνο.

Όταν όμως η ασφάλεια έχει σχεδιαστεί σωστά, λειτουργεί ως enabling layer για τον οργανισμό. Δημιουργεί τις προϋποθέσεις ώστε η διοίκηση να μπορεί να λαμβάνει πιο φιλόδοξες στρατηγικές αποφάσεις, οι ομάδες να υλοποιούν πιο γρήγορα πρωτοβουλίες και ο οργανισμός να επεκτείνεται ή να μετασχηματίζεται χωρίς να θυσιάζει την εμπιστοσύνη, τη συμμόρφωση και τη συνέχεια των λειτουργιών του.

Έχουμε δει στην πράξη ότι όταν ένας οργανισμός αποκτά καλύτερη ορατότητα, ώριμη διακυβέρνηση και

την υλοποίηση ολοκληρωμένων δυνατοτήτων Security Operations και Threat Detection & Response απέκτησαν συνεχή εποπτεία του περιβάλλοντός τους και μπόρεσαν να επιταχύνουν την υιοθέτηση cloud υπηρεσιών και νέων ψηφιακών εφαρμογών.

Αντίστοιχα, σε οργανισμούς που δραστηριοποιούνται σε υψηλά ρυθμιζόμενους κλάδους, η ενίσχυση της διακυβέρνησης κινδύνου και των δυνατοτήτων detection και response αποτέλεσε προϋπόθεση για την ανάπτυξη νέων ψηφιακών υπηρεσιών και τη συνεργασία με διεθνείς εταίρους. Σε αυτές τις περιπτώσεις η κυβερνοασφάλεια δεν λειτουργεί ως περιορισμός. Λειτουργεί ως καταλύτης εμπιστοσύνης και ανάπτυξης.

Διατηρείτε ισχυρή παρουσία σε πολλές χώρες. Ποιες ιδιαίτερες προκλήσεις εντοπίζετε στην ελληνική αγορά σε σύγκριση με το εξωτερικό και πού πρέπει να εστιάσουν οι ελληνικές εταιρείες τους επόμενους 12 μήνες;

Η ελληνική αγορά έχει σημειώσει σημαντική πρόοδο τα τελευταία χρόνια, ωστόσο εξακολουθεί να παρουσιάζει διαφορετικό επίπεδο ωριμότητας σε σχέση με πιο ώριμες αγορές του εξωτερικού. Σε αρκετές περιπτώσεις η κυβερνοασφάλεια εξακολουθεί να αντιμετωπίζεται κυρίως ως τεχνικό ζήτημα και όχι ως επιχειρησιακός κίνδυνος



Απόστολος Πανδρούλας, General Manager Greece, Ηλίας Σαλπέας, Sales Manager Government, Defense & Space, Μαριλένα Νίκου, Head of Marketing, ClearSkies, Γιώργος Δρεπανιώτης, Sales Manager, Biku Σιγούρου, Head of Marketing Odyssey

που αφορά τη διοίκηση και τη συνολική λειτουργία ενός οργανισμού.

Παράλληλα, πολλές εταιρείες έχουν επενδύσει σε εργαλεία ασφάλειας χωρίς να διαθέτουν ένα ενιαίο λειτουργικό μοντέλο διαχείρισης κινδύνου, συνεχούς παρακολούθησης και αποτελεσματικής απόκρισης σε περιστατικά.

Τους επόμενους 12 μήνες οι ελληνικές εταιρείες θα χρειαστεί να εστιάσουν στην ενίσχυση των δυνατοτήτων detection και response, στην ουσιαστική ενσωμάτωση της κυβερνοασφάλειας στη στρατηγική και στη διακυβέρνηση του οργανισμού και στην προσαρμογή στα νέα κανονιστικά πλαίσια όπως η NIS2.

Η έλλειψη εξειδικευμένων στελεχών παραμένει το νούμερο ένα πρόβλημα των CISOs. Πώς το μοντέλο των MSSP (Managed Security Service Provider) της Odyssey έρχεται να καλύψει αυτό το κενό, λειτουργώντας ως προέκταση της ομάδας του πελάτη;

Η έλλειψη εξειδικευμένων στελεχών αποτελεί σήμερα μία από τις μεγαλύτερες προκλήσεις για τους CISOs παγκοσμίως. Το κενό ταλέντων στην κυβερνοασφάλεια είναι δεδομένο και δεν μπορεί να καλυφθεί απλώς με πε-

ρισσότερες προσλήψεις. Γι' αυτό και η προσέγγιση αλλάζει: η λύση βρίσκεται στον συνδυασμό ανθρώπινης εξειδίκευσης, αυτοματοποίησης και πιο ώριμων μοντέλων security operations.

Το μοντέλο MSSP της Odyssey έχει σχεδιαστεί ακριβώς με αυτή τη λογική. Μέσα από τα Managed Security Services, οι οργανισμοί αποκτούν άμεση πρόσβαση σε μια έμπειρη ομάδα αναλυτών, σε ώριμες διαδικασίες και σε τεχνολογίες ανίχνευσης και απόκρισης που λειτουργούν σε συνεχή βάση.

Παράλληλα, αξιοποιούμε αυτοματοποίηση και τεχνητή νοημοσύνη ώστε να περιορίζεται ο όγκος των ειδοποιήσεων και των επαναλαμβανόμενων εργασιών που επιβαρύνουν τις ομάδες ασφάλειας. Αυτό επιτρέπει στους εξειδικευμένους αναλυτές να επικεντρώνονται σε αυτό που έχει πραγματική αξία: στην εις βάθος ανάλυση απειλών, στο threat hunting και στη στρατηγική αντιμετώπιση σύνθετων κινδύνων.

Για τον οργανισμό, το αποτέλεσμα είναι ουσιαστικό. Αντί να προσπαθεί να δημιουργήσει μόνος του μια πλήρη ομάδα ασφάλειας σε μια αγορά με περιορισμένο ταλέντο, αποκτά άμεσα πρόσβαση σε εξειδικευμένες δυνατότητες, συνεχή παρακολούθηση και γρήγορη απόκριση σε περιστατικά. Με αυτόν τον τρόπο ενισχύεται η συνολική ανθεκτικότητα του οργανισμού και δημιουργείται ένα πιο αποτελεσματικό μοντέλο ασφάλειας, όπου οι άνθρωποι επικεντρώνονται στις κρίσιμες αποφάσεις και όχι στη διαχείριση ατελείωτων alerts.

Κλείνοντας, αν έπρεπε να συνοψίσετε τη φιλοσοφία της Odyssey σε μία φράση για το cover story μας, ποια θα ήταν αυτή; Τι να περιμένουμε από εσάς στο άμεσο μέλλον;

Κλείνοντας, η φιλοσοφία της Odyssey συνοψίζεται σε μια απλή αρχή: η κυβερνοασφάλεια δεν είναι απλώς άμυνα απέναντι στις επιθέσεις, αλλά ένα δυναμικό σύστημα προστασίας που εξελίσσεται συνεχώς μαζί με τις απειλές. Καθώς η τεχνητή νοημοσύνη αλλάζει ριζικά το τοπίο της κυβερνοασφάλειας, η πραγματική πρόκληση είναι να περάσουμε από τη λογική της αντίδρασης σε ένα μοντέλο προληπτικής και όλο και πιο αυτόνομης άμυνας.

Στην Odyssey πιστεύουμε ότι το μέλλον της ασφάλειας βρίσκεται σε συστήματα που μπορούν να ανιχνεύουν, να συσχετίζουν και να ανταποκρίνονται σε απειλές σε πραγματικό χρόνο, αξιοποιώντας τεχνητή νοημοσύνη, αυτοματοποίηση και την εμπειρία των ανθρώπων μας. Σε ένα περιβάλλον όπου οι επιθέσεις γίνονται ολοένα και πιο αυτοματοποιημένες, ο στόχος μας είναι να βοηθάμε τους οργανισμούς να προσαρμόζονται ταχύτερα και να λειτουργούν με μεγαλύτερη ανθεκτικότητα.

Θα συνεχίσουμε να επενδύουμε σε πιο εξελιγμένες δυνατότητες detection, investigation και response και σε μοντέλα security operations που αξιοποιούν την τεχνητή νοημοσύνη για να προβλέπουν και να περιορίζουν απειλές πριν εξελιχθούν σε κρίσεις. Με απλά λόγια, θέλουμε να βοηθάμε τους οργανισμούς να κινούνται με σιγουριά σε ένα περιβάλλον όπου το ψηφιακό ρίσκο αυξάνεται συνεχώς, διατηρώντας τον κυβερνοκίνδυνο πραγματικά Under Ctrl. **nw**