

CYBER SECURITY

THE CRITICAL ROLE OF BUSINESS ENGAGEMENT



ΧΟΡΗΓΙΑ ΕΚΔΟΣΗΣ



BOUSSIAS
media

ΔΙΑΣΦΑΛΙΣΗ ΕΝΟΣ ΚΥΒΕΡΝΟΑΝΘΕΚΤΙΚΟΥ ΜΕΛΛΟΝΤΟΣ ΜΕ ΛΥΣΕΙΣ ΥΠΟΣΤΗΡΙΖΟΜΕΝΕΣ ΑΠΟ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Το τοπίο των κυβερνοαπειλών έχει αλλάξει ριζικά την τελευταία δεκαετία, μετατρέποντας την κυβερνοασφάλεια σε έναν από τους πιο κρίσιμους τομείς για τους σύγχρονους οργανισμούς.

Με την αυξανόμενη εξάρτηση από ψηφιακές πλατφόρμες, την εκτεταμένη χρήση του cloud computing και τη ραγδαία ανάπτυξη του Internet of Things (IoT), η επιφάνεια επιθέσεων έχει επεκταθεί σε ανησυχητικά επίπεδα. Η διεύρυνσή αυτή έχει προσφέρει στους κυβερνοεγκληματίες περισσότερες ευκαιρίες, αφού πλέον διαθέτουν εξειδικευμένα εργαλεία και στρατηγικές για την εκμετάλλευση των αδυναμιών ασφαλείας. Απειλές όπως οι Προηγμένες επίμονες απειλές (APTs), επιθέσεις που υποστηρίζονται από Τεχνητή Νοημοσύνη, και οι zero-day ευπάθειες έχουν γίνει πλέον συχνότερες και πιο περίπλοκες.

Οι Προηγμένες Επίμονες Απειλές (APTs) έχουν εξελιχθεί, χρησιμοποιώντας σύνθετες τακτικές για να ξεπερνούν τις παραδοσιακές άμυνες. Η Τεχνητή Νοημοσύνη (TN) στα χέρια των επιτιθέμενων καθιστά τις επιθέσεις πιο στοχευμένες και δύσκολα ανιχνεύσιμες. Οι zero-day ευπάθειες – ανακαλυπτόμενες πριν υπάρξουν patches – είναι πλέον πιο συχνές και επικίνδυνες, καθιστώντας την άμεση αντίδραση ζωτικής σημασίας. Το νέο τοπίο απαιτεί στρατηγικές που ανταποκρίνονται στην πολυπλοκότητα των σύγχρονων απειλών.

ΓΙΑΤΙ ΟΙ ΠΑΡΑΔΟΣΙΑΚΕΣ ΜΕΘΟΔΟΙ ΔΕΝ ΜΠΟΡΟΥΝ ΝΑ ΑΝΤΑΠΟΚΡΙΘΟΥΝ ΣΤΙΣ ΣΥΓΧΡΟΝΕΣ ΠΡΟΚΛΗΣΕΙΣ

Για χρόνια, οι οργανισμοί στηρίζονταν σε παραδοσιακά εργαλεία κυβερνοασφάλειας τα οποία ήταν σχεδιασμένα να εντοπίζουν γνωστές απειλές. Ωστόσο, αυτά τα συστήματα δυσκολεύονται να ανιχνεύσουν τις νέες, σύνθετες και συνεχώς εξελισσόμενες απειλές.

Ένα από τα κύρια προβλήματα αυτών των συστημάτων έγκειται ότι λειτουργούν με βάση την αντίδραση (reactive) και όχι την πρόληψη (proactive). Περιμένουν πρώτα να εκδηλωθεί μια απειλή ή επίθεση και στη

συνέχεια αντιδρούν για να την αντιμετωπίσουν, αντί να την εντοπίζουν και να την αποτρέπουν εκ των προτέρων. Αυτό έχει ως αποτέλεσμα οι κακόβουλες ενέργειες να μην ανιχνεύονται εγκαίρως, αφήνοντας τα συστήματα εύλωτα σε νέες, εξελισσόμενες επιθέσεις. Την ίδια στιγμή, καθώς αυξάνεται ο όγκος των επιθέσεων, τα παραδοσιακά εργαλεία παράγουν ένα υπερβολικό αριθμό ειδοποιήσεων, οδηγώντας σε αυτό που αποκαλείται «κόπωση από τις ειδοποιήσεις» (alert fatigue). Οι ομάδες ασφαλείας, κατακλυζόμενες από ειδοποιήσεις, δυσκολεύονται να ξεχωρίσουν τις πραγματικές απειλές από τις ψευδείς συναγερμούς.

Επιπλέον, τα παραδοσιακά εργαλεία ασφαλείας αποτυγχάνουν να προσφέρουν κρίσιμες πληροφορίες σχετικά με το **πλαίσιο μιας απειλής**. Χωρίς την απαραίτητη γνώση για την προέλευση ή τις πιθανές συνέπειες μιας επίθεσης, οι αναλυτές ασφαλείας αναγκάζονται να λαμβάνουν κρίσιμες αποφάσεις υπό πίεση, πολλές φορές χωρίς επαρκή δεδομένα για να υποστηρίξουν τις ενέργειες τους.

Ένα ακόμη κρίσιμο πρόβλημα είναι οι **αργοί χρόνοι απόκρισης**. Οι παραδοσιακές μέθοδοι ανίχνευσης συχνά χρειάζονται υπερβολικά πολύ χρόνο για να εντοπίσουν, να αναλύσουν και να αντιμετωπίσουν τις επιθέσεις. Μέχρι να αναληφθεί δράση, η ζημιά μπορεί ήδη να έχει γίνει, ενώ οι χάκερ δρουν με ολοένα μεγαλύτερη ταχύτητα και πολυπλοκότητα.

ΠΩΣ Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΜΕΤΑΜΟΡΦΩΝΕΙ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ - ΓΙΑΤΙ ΤΟ ΑΙ ΑΠΟΤΕΛΕΙ ΟΡΟΣΗΜΟ ΣΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΥΒΕΡΝΟΑΠΕΙΛΩΝ

Η Τεχνητή Νοημοσύνη (TN) δεν αποτελεί απλώς μια τεχνολογική καινοτομία στον τομέα της κυβερνοασφάλειας, αλλά μια θεμελιώδη αλλαγή στον τρόπο

που οι οργανισμοί αντιμετωπίζουν τις σύγχρονες απειλές. Το πλεονέκτημα της TN έχει τη δυνατότητα να γεφυρώσει τα κενά που αφήνουν οι παραδοσιακές τεχνολογίες, παρέχοντας ταχύτερες, ακριβέστερες και πιο προορατικές άμυνες.

Ένα από τα μεγαλύτερα πλεονεκτήματα της TN είναι η ασύγκριτη ταχύτητα ανίχνευσης. Σε αντίθεση με τις συμβατικές τεχνολογίες, μπορεί να εντοπίσει σε πραγματικό χρόνο ύποπτες δραστηριότητες, όπως ασυνήθιστες μεταφορές δεδομένων ή μη εξουσιοδοτημένες προσπάθειες σύνδεσης, δίνοντας στους οργανισμούς τη δυνατότητα να σταματήσουν μια επίθεση πριν αυτή εξελιχθεί.

Η TN συμβάλλει επίσης στην αντιμετώπιση ενός από τα μεγαλύτερα προβλήματα στην κυβερνοασφάλεια: τους ψευδείς συναγερμούς (false positives). Με τη συνεχή μάθηση και βελτίωσή της, η TN μπορεί να φιλτράρει τις ασήμαντες ειδοποιήσεις και να επικεντρωθεί στις πραγματικές απειλές. Αυτό επιτρέπει στις ομάδες ασφαλείας να διαχειρίζονται πιο αποτελεσματικά το φορτίο τους, επικεντρώνοντας τις προσπάθειές τους στους σοβαρούς κινδύνους αντί για καθημερινές λειτουργικές ανωμαλίες.

Τέλος, μπορεί να μπλοκάρει άμεσα την πρόσβαση, να απομονώσει κρίσιμα συστήματα ή να εφαρμόσει άλλες προληπτικές ενέργειες. Αυτή η αυτοματοποίηση μειώνει την πιθανότητα εξάπλωσης μιας επίθεσης και εξασφαλίζει ότι οι οργανισμοί είναι καλύτερα προετοιμασμένοι.

CENTRIC AI: ΤΟ ΜΕΛΛΟΝ ΕΙΝΑΙ ΗΔΗ ΕΔΩ

Η εποχή της Τεχνητής Νοημοσύνης μπορεί να θεωρείται από πολλούς ως μια αχατογράφητη περιοχή γεμάτη προκλήσεις, αλλά η Odyssey βλέπει την ευκαιρία να ηγηθεί αυτής της μετάβασης με την τεχνογνωσία της και την εμπειρία της στο συνεχώς εξελισσόμενο τοπίο των απειλών. Χάρη

στη δέσμευσή της για καινοτομία και τη συνεχή επένδυση στην Έρευνα και Ανάπτυξη (R&D), η Odyssey προχωρά δυναμικά με την παρουσίαση της πλατφόρμας **ClearSkies Centric AI TDIR**, που φέρνει την τεχνολογία της TN στο προσκήνιο της κυβερνοασφάλειας.

Ενσωματώνοντας τις πιο προηγμένες δυνατότητες που προσφέρει η TN, αυτή η πλατφόρμα επαναπροσδιορίζει ολόκληρο τον κύκλο διαχείρισης απειλών, προσφέροντας **ταχύτερη** και **ακριβέστερη** ανίχνευση, **βαθύτερες** και πιο **ολοκληρωμένες** αναλύσεις, καθώς και **άμεσες** και **αποτελεσματικές** αντιδράσεις. Το **ClearSkies Centric AI TDIR** δεν συμβαδίζει απλώς με την παγκόσμια αγορά SIEM/TDIR· την επαναπροσδιορίζει. Εισάγει λύσεις βασισμένες στην AI που ενισχύουν τις εσωτερικές λειτουργίες ασφάλειας και επιτρέπουν στους οργανισμούς να παραμένουν μπροστά από τους κυβερνοεγκληματίες, οι οποίοι επίσης χρησιμοποιούν AI για να ενισχύσουν τις επιθέσεις τους. Με το **Centric AI Fabric στην βάση της**, η πλατφόρμα μαθαίνει συνεχώς από νέα δεδομένα, προηγούμενα περιστατικά, και το εξελισσόμενο τοπίο των απειλών, βελτιώνοντας διαρκώς την ακρίβεια και προσαρμόζοντας τις στρατηγικές ασφάλειας στις πιο σύγχρονες μεθόδους επίθεσης.

Με την ενσωμάτωση πληροφοριών απειλών σε πραγματικό χρόνο από πολλαπλές πηγές και προσαρμοσμένα playbooks, η πλατφόρμα ενισχύει σημαντικά τη διαδικασία λήψης αποφάσεων, μειώνει τα λειτουργικά κόστη και αυξάνει την αποδοτικότητα των οργανισμών. Με την επεκτασιμότητα, την ευελιξία και την ευχρηστία της, το ClearSkies Centric AI TDIR ενισχύει την ασφάλεια του οργανισμού σας, εφοδιάζοντας την ομάδα SecOps με τα κατάλληλα εργαλεία για ανίχνευση, διερεύνηση και αντιμετώπιση σύνθετων απειλών. Σε μια εποχή

όπου η ταχύτητα και η ακρίβεια είναι καθοριστικές, η πλατφόρμα προσφέρει μια προσαρμοστική και συνεχώς εξελισσόμενη άμυνα, εξασφαλίζοντας ότι οι οργανισμοί παραμένουν ασφαλείς καθώς προχωρούν στην νέα εποχή της TN.

AI POWERED MANAGED SERVICES: ΣΥΝΔΥΑΖΟΝΤΑΣ ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΑΝΘΡΩΠΙΝΗ ΕΞΕΙΔΙΚΕΥΣΗ

Συνδυάζοντας τις επαναστατική πλατφόρμα **ClearSkies Centric AI TDIR** με τη απαραίτητη εξειδίκευση των αναλυτών της Odyssey, προσφέρει μια εξαιρετικά ανταγωνιστική, έξυπνη και οικονομικά αποδοτική υπηρεσία διαχειριζόμενης ασφάλειας (Managed Services). Αυτή η προσέγγιση συνδυάζει τις προηγμένες δυνατότητες της Τεχνητής Νοημοσύνης με την ανθρώπινη τεχνογνωσία, παρέχοντας εξατομικευμένες Υπηρεσίες Λειτουργίας Ασφάλειας (SOC) προσαρμοσμένες στις μοναδικές απαιτήσεις κάθε οργανισμού, ανεξάρτητα από το μέγεθος, τον κλάδο ή την πολυπλοκότητα του.

Στον πυρήνα των υπηρεσιών της βρίσκεται η απόλυτη συνεργασία μεταξύ της TN και της ανθρώπινης διορατικότητας. Η τεχνολογία, που ενισχύεται από την Τεχνητή Νοημοσύνη συνδυάζεται άμεσα με την ανάλυση των ειδικών της Odyssey, προσφέροντας αξιόπιστες και προσαρμοστικές λύσεις. Είτε πρόκειται για μικρή επιχείρηση είτε για μεγάλο οργανισμό, οι επεκτάσιμες λύσεις της Odyssey αναπτύσσονται παράλληλα με τις ανάγκες του εκάστοτε οργανισμού, προσφέροντας υπηρεσίες που παραμένουν σταθερά επικεντρωμένες στις συνεχώς εξελισσόμενες απειλές.

Η πλατφόρμα, εξοπλισμένη με αυτοματοποιημένη ακρίβεια μέσω AI και υποστηριζόμενη από τη μηχανική μάθηση, διασφαλίζει ταχύτητα και ακριβή αντα-

πόκριση σε περιστατικά. Παράλληλα, οι ειδικοί μας επιβλέπουν προσεκτικά κάθε περιστατικό, προσφέροντας την προσοχή και τη φροντίδα που απαιτείται. Με αυτόν τον συνδυασμό τεχνολογίας και εμπειρίας, διασφαλίζουμε ότι ο οργανισμός σας βρίσκεται διαρκώς ένα βήμα μπροστά από τις κυβερνοαπειλές, εξασφαλίζοντας την ασφάλειά του σε κάθε επίπεδο.

ΑΓΚΑΛΙΑΖΟΝΤΑΣ ΤΟ ΜΕΛΛΟΝ ΜΕ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Η πλατφόρμα ClearSkies Centric AI της Odyssey και η νέα γενιά των Managed Services διαμορφώνουν το μέλλον της κυβερνοασφάλειας, παρέχοντας στους οργανισμούς την προηγμένη προστασία που απαιτείται στο συνεχώς εξελισσόμενο ψηφιακό τοπίο. Καθώς οι κυβερνοαπειλές γίνονται ολοένα πιο πολύπλοκες, η Τεχνητή Νοημοσύνη (TN) αποτελεί τον καταλύτη για την αντιμετώπισή τους. Οι επιχειρήσεις που υιοθετούν αυτές τις τεχνολογίες είναι σε θέση να εξασφαλίσουν την προστασία των δεδομένων τους και να πλοηγηθούν με αυτοπεποίθηση στη νέα εποχή των ψηφιακών προκλήσεων. Με περισσότερα από 20 χρόνια εμπειρίας, η Odyssey παραμένει στην πρώτη γραμμή της κυβερνοασφάλειας, αφοσιωμένη στην ασφάλεια των ψηφιακών υποδομών των οργανισμών. Συνδυάζοντας βαθιά τεχνογνωσία, καινοτόμες λύσεις και δέσμευση να βοηθήσει τους οργανισμούς να μπορούν να προβλέπουν, να αντιστέκονται, να προσαρμόζονται και να ανακάμπτουν στις συνεχώς εξελισσόμενες κυβερνοαπειλές, διασφαλίζοντας παράλληλα την συμμόρφωση με τις κανονιστικές τους υποχρεώσεις.

Με την Odyssey, οι οργανισμοί δεν αποκτούν απλώς μια λύση ασφάλειας· αποκτούν έναν στρατηγικό συνεργάτη για ένα ασφαλές και βιώσιμο μέλλον.



INFO

Λ. Μεσογείων 237, Νέο Ψυχικό
E: info@odysseycs.com
W: www.odysseycs.com



FUTURE-PROOF YOUR CYBERSECURITY WITH AI-POWERED **MANAGED SERVICES**

In today's fast-paced cybersecurity landscape, integrating AI is not just an option—it's a imperative. Empower your organization with our advanced AI-powered Managed Services, designed to keep you ahead of ever-evolving threats.

WHY AI-POWERED **MANAGED** **SERVICES?**



**Intelligent Security,
Human Expertise**



**Scalable Solutions
for Every Business**



**Automated Precision,
Expert Oversight**



**Enhanced Security Posture
with Continuous Learning**



www.odysseycs.com

Offices: GREECE, CYPRUS (HQ), KSA, UK