RBL

RETHINK BUSINESS LAB

INNOVATION STRATEGY AGILITY

Ψηφιακή Πλατφόρμα Προστασίας από Κυβερνοκινδύνους

Digital Risk Protection

Ισχυρές, αυτοματοποιημένες λύσεις για να προστατεύετε δεδομένα και πληροφορίες της επιχείρησής σας, όπου και αν βρίσκονται

SKURIO

Ιούνιος 2022

Η Rethink Business Lab – RBL (www.rbl.gr), είναι μια συμβουλευτική και εκπαιδευτική εταιρεία, που προσφέρει υπηρεσίες σε επιχειρήσεις που επιθυμούν να εφαρμόσουν ευέλικτες στρατηγικές μετασχηματισμού με επίκεντρο τη διακυβέρνηση δεδομένων και πληροφοριών.

Χρησιμοποιούμε τα δεδομένα και τις πληροφορίες που παράγονται από αυτά, για να:

- **βελτιστοποιήσουμε λειτουργίες**
- **βελτιστοποιήσουμε την εμπειρία πελάτη**
- **εφαρμόσουμε κανόνες και πολιτικές**
- **εντοπίσουμε και αντιμετωπίσουμε κινδύνους, ενισχύοντας την ασφάλεια των πληροφοριών**
- **επιτύχουμε τη συμμόρφωση με το κανονιστικό και νομοθετικό πλαίσιο**
- **πιστοποιήσουμε την επιχείρηση και τα στελέχη της σύμφωνα με διεθνή πρότυπα**
- **ενισχύσουμε την ανθεκτικότητα**
- **επιταχύνουμε τον ψηφιακό μετασχηματισμό**

Συνεργαζόμαστε με τη SKURIO, την καινοτόμο εταιρεία λογισμικού κυβερνοασφάλειας, που βοηθά επιχειρήσεις να προστατευτούν από ψηφιακούς κινδύνους. Η πλατφόρμα **Digital Risk Protection**, συνδυάζει αυτοματοποιημένη, εικοσιτετράωρη παρακολούθηση του Surface, Deep και Dark Web με ισχυρές δυνατότητες ανάλυσης και εφαρμογής Ευφυΐας στην αντιμετώπιση Κυβερνοαπειλών.

Η Skurio, Ιδρύθηκε το 2011, και έχει την έδρα του στο Ηνωμένο Βασίλειο με ένα διεθνές δίκτυο συνεργατών. Η εξαιρετικά εξειδικευμένη ομάδα των αναλυτών ασφάλειας της Skurio εργάζεται στο κορυφαίο επίπεδο της επιχειρηματικής ευφυΐας και της ψηφιακής προστασίας από κινδύνους, παρέχοντας στους οργανισμούς και επιχειρήσεις την υποστήριξη που χρειάζονται για να αναβαθμίζουν την ασφάλειά τους. Το δίκτυο συνεργατών και διανομής μας εξυπηρετεί εκατοντάδες πελάτες σε 33 χώρες.

Οι ειδήσεις για μια νέα παραβίαση δεδομένων και ασφάλειας πληροφοριών είναι καθημερινό φαινόμενο.

Η ανακάλυψη αν δεδομένα ή επιχειρηματικές πληροφορίες έχουν διαρρεύσει, μπορεί να πάρει μέρες ή ακόμη εβδομάδες και μήνες.
Μέχρι τότε,

Είναι πολύ αργά!

Οι παραβιάσεις που ανακοινώνονται, από εταιρείες κάθε μεγέθους και κλάδου για διαρροή πληροφοριών και δεδομένων, μας υπενθυμίζει την ανάγκη της συνεχούς παρακολούθησης του ψηφιακού αποτυπώματος της εταιρείας μας σχετικά με την έκθεσή της στον κυβερνοχώρο.

Πολλές φορές, οι αποκαλύψεις για παραβίαση δεδομένων μπορεί να είναι αποτέλεσμα παλαιότερων παραβιάσεων που δεν αναγνωρίστηκαν όταν έγιναν.

Η κατανόηση της προέλευσης αυτών των παραβιάσεων μπορεί να βοηθήσει τις εταιρείες να εκτιμήσουν τον κίνδυνο που διατρέχουν, αποφεύγοντας τη σπατάλη πόρων σε περιττές έρευνες καθώς και να βοηθήσει στο να σχεδιάσουν σωστά τα συστήματα πρόληψης διαρροών δεδομένων (DLP- Data Leakage Prevention) και προστασίας από κινδύνους (DRP - Data Risk Protection).

Περιορισμός κινδύνων μέσω Στοχευμένων Αναζητήσεων

Από τη στιγμή που τα δεδομένα σας βρίσκονται σε πολλούς τόπους εκτίθενται σε κινδύνους και το ρολόι χτυπάει για τη διαρροή ή παραβίαση.
Με τόσο μεγάλο όγκο δεδομένων έξω από τον έλεγχό σας πως θα ξέρετε αν κινδυνεύουν;

Οι σύνθετες, ψηφιακές αλυσίδες εφοδιασμού (digital supply chain), οι αυξημένες κυβερνοεπιθέσεις και οι νέοι κανονισμοί προστασίας δεδομένων μπορεί να αφήνουν την επιχείρησή σας ευάλωτη.
Η διαχείριση της κυβερνοασφάλειας μόνο στο δίκτυό σας δεν είναι πλέον αρκετή, όταν κρίσιμα δεδομένα μοιράζονται με συνεργάτες της εφοδιαστικής αλυσίδας.

Την ίδια στιγμή, terabyte δεδομένων, που παραβιάζονται, είναι σε κοινή θέα (στο Surface, Deep και Dark Web.) και αποτελούν αντικείμενο συναλλαγής μεταξύ απατεώνων, δημιουργώντας μεγάλες απειλές και κινδύνους. Όπως, κίνδυνος επιχειρηματικής αναστάτωσης και διακοπής εργασιών, απώλεια ταυτότητας, διαρροή ευαίσθητων δεδομένων, απώλεια εσόδων, πλήγμα στη φήμη, και πολλά άλλα.
Η έρευνα και η εύρεση των δεδομένων σας με χειροκίνητους τρόπους – σε κακόβουλες περιοχές του διαδικτύου- χρειάζεται σημαντικό χρόνο και προσπάθεια. Η μη αυτοματοποιημένη έρευνα μπορεί επίσης να αφήσει το αποτύπωμά της και να εκθέσει τις ομάδες ασφαλείας σας σε παράνομο ή ενοχλητικό περιεχόμενο - ακόμη και στους τύπους κακόβουλου λογισμικού που προσπαθούσαν να αποφύγουν.

Η παρακολούθηση με την πλατφόρμα RBL-Skurio Digital Risk Protection, ο εντοπισμός παραβιάσεων δεδομένων και οι λύσεις πληροφοριών κυβερνοαπειλών αποκαλύπτουν με ασφάλεια τις απειλές που υπάρχουν έξω από το δίκτυό σας, φωτίζοντας τις πηγές του ψηφιακού κινδύνου έτσι ώστε να μπορείτε να ενεργήσετε γρηγορότερα για να τον αντιμετωπίσετε και να τον μειώσετε.

Πώς χρησιμοποιούν οι απατεώνες το Dark Web;

Ως επαγγελματίας, πιθανότατα έχετε ακούσει για το Dark Web (Σκοτεινό Διαδίκτυο), αλλά ίσως δεν είστε αρκετά σίγουροι πώς σχετίζεται με την εταιρεία σας ή τα σχέδιά σας για την ασφάλεια σας στον κυβερνοχώρο.

Η εικόνα με το παγόβουνο δείχνει τα διαφορετικά επίπεδα για το τι βλέπουμε και σε τι υπάρχει πρόσβαση στο διαδίκτυο στο σύνολό του. Η επιφάνεια (surface web) αλλά και περιοχές που βρίσκονται κάτω από αυτήν (deep web) είναι οι πιο συχνά προσβάσιμες.

Το Dark Web είναι μια περιοχή του διαδικτύου, σε μεγαλύτερα «βάθη», που δεν βρίσκεται όπως συνήθως από το Google ή από άλλες μηχανές αναζήτησης.
Δεν είναι καν προσβάσιμο μέσω ενός κανονικού προγράμματος περιήγησης στο διαδίκτυο.

Ένας συγκεκριμένος τύπος προγράμματος περιήγησης, όπως ένα πρόγραμμα περιήγησης Tor, απαιτείται για την πρόσβαση σε αυτό το τμήμα του διαδικτύου και συνήθως, ο χρήστης πρέπει να γνωρίζει ακριβώς πού θέλει να πάει. Χρειάζεται κάποιος τη συγκεκριμένη διεύθυνση για αυτό που θέλει να βρει. Δεν υπάρχει μηχανή αναζήτησης που θα τον οδηγήσει εκεί.

Το πρόγραμμα περιήγησης Tor, για παράδειγμα, χρησιμοποιεί πολλά πολύπλοκα συστήματα και VPNs για να συγκαλύψει τη διεύθυνση IP του χρήστη προέλευσης, ανωνυμοποιώντας την τοποθεσία και τα μεταδεδομένα που συνήθως σχετίζονται με την περιήγηση στο διαδίκτυο.

Εξαιτίας αυτού, έχει κάνει το Dark Web το σύγχρονο τόπο συνάντησης για παράνομες συναλλαγές και παράνομο εμπόριο αγαθών.

Είναι μια κοινή παρανόηση ότι τα έσοδα/κέρδη του Σκοτεινού Διαδικτύου προέρχονται μόνο από όπλα, ναρκωτικά και πορνογραφία.

Τα αγαθά προς πώληση, στις μέρες μας, είναι εξίσου πιθανό να περιλαμβάνουν τα στοιχεία από τη δική σας εταιρείας, τα δεδομένα της, κωδικούς πρόσβασης, τα emails, στοιχεία πιστωτικών καρτών και άλλα.

Μια διαφορετική προσέγγιση για την ασφάλεια στον κυβερνοχώρο

Δεν είναι πλέον απαραίτητο για τους χάκερς και τους απατεώνες να επιτίθενται στο δίκτυό σας προκειμένου να αποσπάσουν κρίσιμα δεδομένα σας.

Είτε πρόκειται για μια προσεκτικά προετοιμασμένη επίθεση εστιασμένης στόχευσης είτε απλά για έναν δυσαρεστημένο εργαζόμενο που θέτει σε απειλή εμπιστευτικές πληροφορίες - τα δεδομένα σας μπορούν να καταλήξουν να μοιράζονται ή να πωλούνται σε σκοτεινά μέρη του Διαδικτύου τα οποία είναι αόρατα στα εσωτερικά συστήματα ασφαλείας σας.

Η αναζήτηση των δεδομένων σας εκτός του τείχους προστασίας της επιχείρησής σας με ασφαλή και αυτοματοποιημένο τρόπο είναι το επόμενο βήμα στο ταξίδι σας προς την ωριμότητα και αναβάθμιση του επιπέδου κυβερνοασφάλειας.

Ενισχύστε την ασφάλεια σας σε ένα συνδεδεμένο οικοσύστημα με την πλατφόρμα Digital Risk Protection, με σαφή οφέλη.

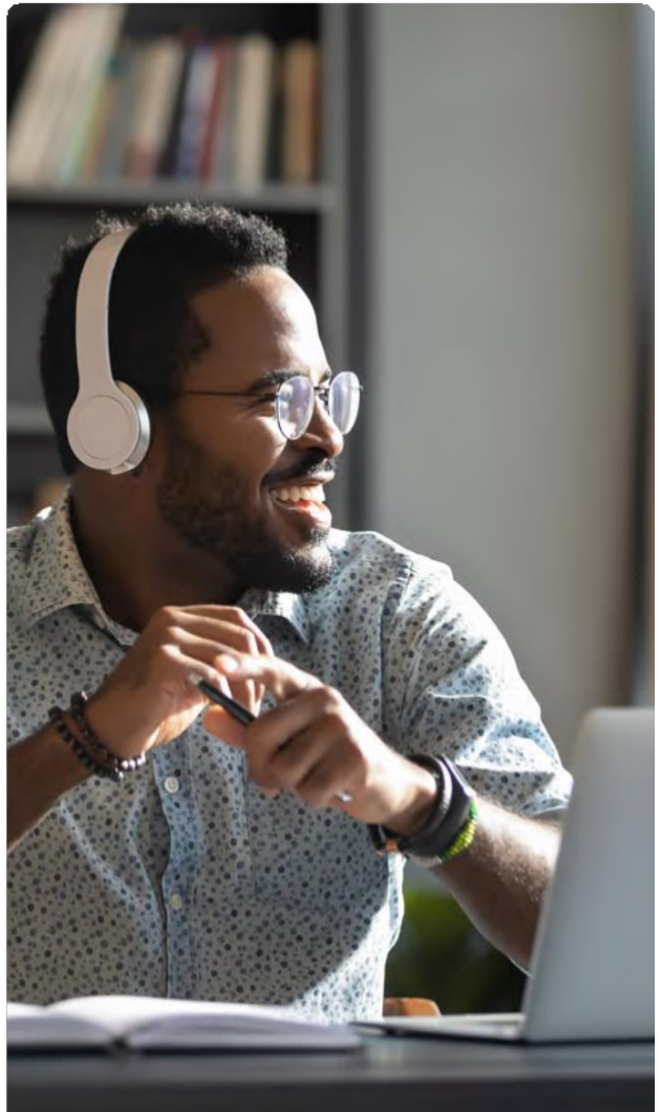
Για να βελτιώσετε τη στρατηγική σας στον κυβερνοχώρο, πρέπει να κοιτάξετε πέρα από την περίμετρο του δικτύου σας για να φωτίσετε αθέατες περιοχές που δεν ελέγχονται από εσάς. Ανακαλύψτε πώς η Ψηφιακή Προστασία από Κινδύνους μπορεί να σας βοηθήσει να ευθυγραμμίσετε τη στρατηγική ασφαλείας σας με τους επιχειρησιακούς σας στόχους.

- **Υπερασπιστείτε τη λειτουργία σας:** Ανακαλύψτε τις κρυμμένες απειλές για την επωνυμία σας, τα έσοδα και τα στελέχη σας, παρακολουθώντας για διαρροή σε ευαίσθητα και κρίσιμα δεδομένα της εταιρείας σας όλο το εικοσιτετράωρο.
- **Προστατέψτε την ψηφιακή αλυσίδα τροφοδοσίας σας:** με την τεχνική του μαρκαρίσματος (υδατογράφημα - breach marker) των δεδομένων σας και συνεχή παρακολούθηση αν (π.χ.) δεδομένα πελατών σας έχουν διαρρεύσει.
- **Αποφύγετε τη διακοπή εργασιών:** Χρησιμοποιήστε άμεσες ειδοποιήσεις, προηγμένη αυτοματοποίηση και αποτελεσματική ολοκλήρωση (integration) στο δικό σας περιβάλλον, για να ελαχιστοποιήσετε τις επιπτώσεις οποιουδήποτε περιστατικού παραβίασης και να επιτύχετε να τη γρηγορότερη αποκατάσταση.

Αυτοματοποιημένη παρακολούθηση Dark Web και εντοπισμός παραβίασης δεδομένων

- **Η πλατφόρμα Digital Risk Protection είναι μια ασφαλής λύση SaaS (Software as a Service) που σας βοηθά να εντοπίσετε εξωτερικές απειλές και παραβιάσεις ειδικά για την επιχείρησή σας. Η πλατφόρμα περιέχει πρακτικά χαρακτηριστικά που σας παρέχουν ψηφιακή προστασία από κινδύνους για τα δεδομένα και τους πόρους σας:**

- Εξαλείψτε τα ψευδείς ειδοποιήσεις, εξοικονομήστε χρόνο και εστιάστε αναζητώντας περιεχόμενο συγκεκριμένο για την επιχείρησή σας
- Δημιουργήστε απλές ή σύνθετες ειδοποιήσεις χρησιμοποιώντας λέξεις-κλειδιά, email domains, διαπιστευτήρια (κωδικούς χρηστών) σύνδεσης χρηστών, διευθύνσεις IP, διευθύνσεις email και άλλα
- Αποκτήστε πρόσβαση σε πολυετή ιστορική βάση πληροφοριών σχετικά με παραβίασεις
- Παρακολουθήστε το surface, deep και dark web για διαρροές δεδομένων σας, 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα, συμπεριλαμβανομένων των Social Media, των IRC chat rooms και των τοποθεσιών απόθεσης πληροφοριών με τη μορφή κειμένου όπως το Pastebin
- Μείνετε ενημερωμένοι για απειλές ή παραβιάσεις που εμφανίζονται έξω από την περίμετρό σας μέσω SMS, email, Slack ή API, μέσα σε λίγα λεπτά που τα δεδομένα σας θα εμφανιστούν οπουδήποτε που δεν θα έπρεπε



- Μειώστε τον αντίκτυπο και το κόστος με ταχύτερη ανίχνευση παραβίασης μέσω αυτοματοποίησης, εξοικονομώντας χρόνο και προσπάθεια
- Συνεργαστείτε και βελτιώστε την παραγωγικότητα με τη δημιουργία προσαρμοσμένων φακέλων, τη διαχείριση τρόπων απόκρισης και τη συγκέντρωση ευρημάτων και σχολίων
- Διαχειριστείτε τις έρευνες και λάβετε πληροφορίες χρησιμοποιώντας σύνθετες αναλύσεις
- Παρακολουθήστε για παραβιάσεις των δεδομένων πελατών σε ολόκληρη την αλυσίδα προμήθειας σας χρησιμοποιώντας 5 προηγμένες τεχνικές
- Χρησιμοποιήστε τον προηγμένο εντοπισμό για παραπλανητικά sites με βάση την επωνυμία σας (typosquatting) για να εντοπίσετε πηγές απάτης ή πηγές ηλεκτρονικού ψαρέματος (phishing)
- Λάβετε συμβουλές και βοηθηθείτε στην κατανόηση ειδοποιήσεων με τη δυνατότητα "Ask an Analyst"
- Ζητήστε το κατέβασμα posts ή sites που είναι βλαπτικά για την επιχείρησή σας, χρησιμοποιώντας τις εξειδικευμένες υπηρεσίες μας

Cyber Threat Intelligence

Τα χαρακτηριστικά της υπηρεσίας Cyber Threat Intelligence, συλλέγουν και συνδυάζουν πολλαπλές πηγές απειλών στο surface, deep και dark web σε μια ενιαία συγκεντρωτική αναφορά, η οποία παρέχει στους αναλυτές απειλών ισχυρές δυνατότητες αναζήτησης, ανάλυσης και εξαγωγής αποτελεσμάτων.

Η πλατφόρμα είναι βελτιστοποιημένη για την εύρεση απειλών σε μεγάλο όγκο αταξινόμητων και άναρχων δεδομένων, ικανή να αναγνωρίζει και να επιλέγει τις αξιοποιήσιμες πληροφορίες που μπορούν να μετατρέπονται στη συνέχεια σε ενέργειες περαιτέρω έρευνας και αντιμετώπισης απειλών, κινδύνων και ευπαθειών με βάση το ψηφιακό τους αποτύπωμα.

Η πλατφόρμα λειτουργεί στο cloud και δεν απαιτεί εγκατάσταση. Παρέχει ισχυρές δυνατότητες παραμετροποίησης και εφαρμογής κριτηρίων που ρυθμίζονται κατάλληλα ώστε να βρίσκετε γρήγορα τα αποτελέσματα που αφορούν τη δική σας επιχείρηση.

Δυνατότητες του Cyber Threat Intelligence

- Η έρευνα και αναζήτηση πληροφοριών σε περιοχές κοινωνικών σχολίων, όπου συλλέγονται χρήσιμες πληροφορίες από sites συμπεριλαμβανομένων των Reddit και Telegram. Αυτό παρέχει μια πολύτιμη ιστορική βάση δεδομένων για χρήση σε έρευνες καθώς και ειδοποιήσεις δεδομένων ή αναφορές σχετικές με την επωνυμία, τα προϊόντα, τα ανώτερα στελέχη της εταιρείας σας και πολλά άλλα
- Με βάση τις προηγούμενες αναζητήσεις, η έρευνα επεκτείνεται και σε ένα ευρύ φάσμα δημοφιλών κοινωνικών δικτύων για να αντληθούν ακόμη περισσότερες πληροφορίες σχετικά με την επιχείρησή σας
- Η λειτουργία Insights σας βοηθά να αναλύετε και να φιλτράρετε χιλιάδες μηνύματα σε μία ενιαία εικόνα, να εντοπίζετε γρήγορα τις απειλές χωρίς περιττές ή άσχετες πληροφορίες στην έρευνά σας
- Οπτικοποίηση των αποτελεσμάτων σε χρονοδιαγράμματα για να σας βοηθά να διερευνήσετε την πηγή ενός συμβάντος και να εντοπίσετε τους κακόβουλους επιτιθέμενους με συνεχή παρακολούθηση
- Dashboard με αυτοματοποιημένες αναφορές που σας βοηθούν να παρακολουθείτε την εξέλιξη των ερευνών και τις ενέργειες που καταβάλει η ομάδα σας

Προηγμένες δυνατότητες προστασίας από ψηφιακούς κινδύνους

Τεχνολογία BreachMarker

- Βάλτε ένα ψηφιακό υδατογράφημα (breachmarker) στα δεδομένα σας, το οποίο θα τα ακολουθεί, έτσι ώστε να γίνεται εύκολη η ανίχνευση παραβιάσεων σε ολόκληρη την ψηφιακή σας αλυσίδα (digital supply chain)
- Δημιουργείστε σύνθετα διαφορετικά ταυτοτικά στοιχεία ώστε να διευκολύνεται η παρακολούθηση διαφορετικών περιοχών που εσείς θα επιλέγετε
- Συνδυάστε διαφορετικά ψηφιακά υδατογραφήματα παραβίασης (breachmarker) για να ανιχνεύσετε την πηγή και το χρόνο μιας διαρροής δεδομένων
- Εντοπίστε παραβιάσεις που προέρχονται από συστήματα τρίτων ή συνεργατών σας και εντοπίστε το σημείο όπου πραγματοποιήθηκαν με τη χρήση των σύνθετων ταυτοτικών στοιχείων σας
- Χρησιμοποιήστε απλές λέξεις-κλειδιά για την αποφυγή εσφαλμένων ειδοποιήσεων απειλών, που μοιάζουν με αληθινές, και δώστε βάση μόνο σε αξιόπιστες πηγές
- Αποτρέψτε τις παραβιάσεις δεδομένων από τις κυβερνοεπιθέσεις πριν αυτές πάρουν μεγάλες διαστάσεις, μειώνοντας έτσι τους κινδύνους και το κόστος διαχείρισης

Δυνατότητες Integration

- Χρησιμοποιήστε τα REST APIs της πλατφόρμας μας, για ενσωματώσετε αποτελέσματα και ειδοποιήσεις στις SIEM, SOAR, ITSM και άλλες εφαρμογές ασφάλειας που χρησιμοποιείτε
- Δημιουργήστε τα δικά σας work-flows και αυτοματοποιήστε τις ενέργειες παραβιάσεων
- Αποφύγετε εσφαλμένες ειδοποιήσεις απειλών, που μοιάζουν με αληθινές, εντοπίζοντας γρήγορα τις παραβιάσεις κωδικών χρηστών κρίσιμης σημασίας σε ενεργούς λογαριασμούς τους, κατανοώντας τους τύπους των χρηστών που αποτελούν στόχο
- Ενημερωθείτε για τις εγγραφές εργαζομένων (sign-ups) σε υπηρεσίες διαφόρων τρίτων παρόχων, που έχουν παραβιαστεί με πρόσθετη πληροφόρηση εάν έχουν παραβιαστεί και passwords
- Βελτιώστε τις πολιτικές ασφάλειας στον κυβερνοχώρο και σχεδιάστε στοχευμένες εκπαιδεύσεις, ενισχύοντας την ευαισθητοποίηση του προσωπικού σας σαν μέτρο πρόληψης
- Βελτιώστε την αποτελεσματικότητα του περιβάλλοντος SOC μέσω της έξυπνης αυτοματοποίησης και δώστε στους αναλυτές απειλών τη δυνατότητα να επικεντρωθούν στις απειλές υψηλού κινδύνου

Προηγμένες Δυνατότητες Digital Risk Protection διαφόρων κατηγοριών σε μια ενιαία πλατφόρμα

Καθορίστε γρήγορα και εύκολα πολλαπλά κριτήρια αναζητήσεων απειλών, διαρροών και παραβιάσεων για όλες τις κατηγορίες δεδομένων που μπορούν να απασχολούν την επιχείρησή σας

Προστασία του Προσωπικού

Που και τι ψάχνουμε:

Data dumps
Credentials
PII /fullz
Credit cards
Mobile numbers Domains
Email addresses

Απειλές που αποφεύγουμε

- Phishing
- Smishing
- Account takeover
- Identity theft

Προστασία των Υποδομών

Που και τι ψάχνουμε:

IP addresses
Infrastructure details
Device details
Forum mentions
Port scans
3rd party supplier mentions

Απειλές που αποφεύγουμε

- Attack Planning
- Vulnerabilities
- Supply chain Attacks
- Open port scan attacks

Προστασία των Πελατών

Που και τι ψάχνουμε:

BreachMarker IDs
Customer data
Customer emails
'Regex' pattern matches

Απειλές που αποφεύγουμε

- Data sale or dump
- Spam, scams and fraud
- Phishing
- Account takeover

Προστασία της Εταιρικής Ταυτότητας

Που και τι ψάχνουμε:

Brand names
URLs
Domain registrations

Απειλές που αποφεύγουμε

- Typosquatting
- Brand impersonation
- Customer phishing
- Activist targeting

Προστασία Κερδών και Εσόδων

Που και τι ψάχνουμε:

Products
Loyalty card details
Pattern matches

Απειλές που αποφεύγουμε

- Discount abuse
- Contract loopholes
- Voucher abuse
- Free downloads

Προστασία Αγαθών και Υπηρεσιών

Που και τι ψάχνουμε:

Product codes
Brands
Intellectual property

Απειλές που αποφεύγουμε

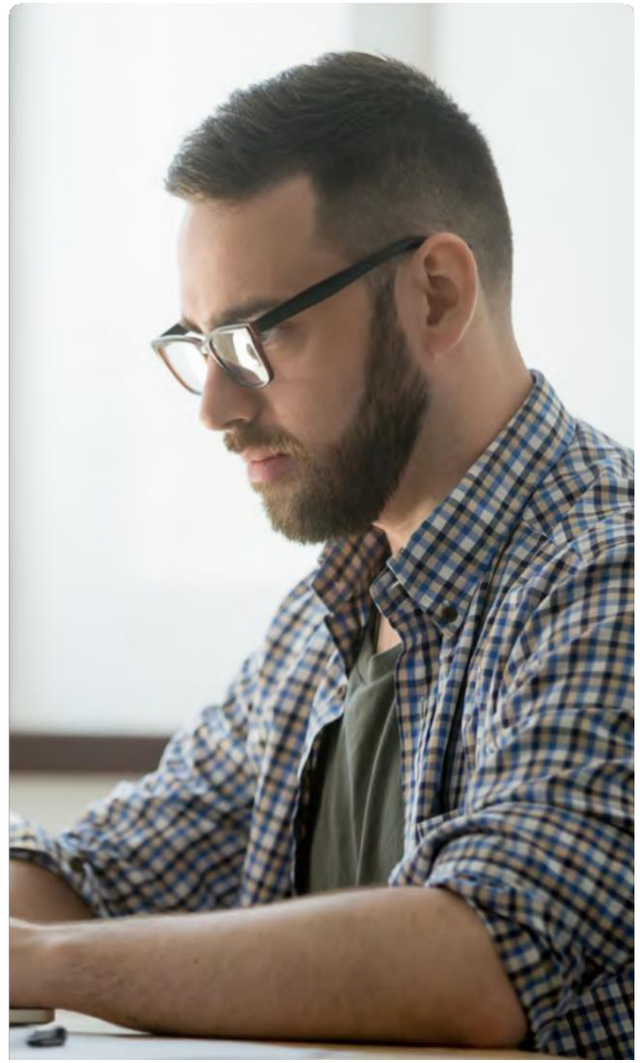
- Intellectual property leak
- Trademark Infringement
- Source Code theft
- Counterfeit goods

Προηγμένες Υπηρεσίες προστασίας πληροφοριών - όταν τις χρειάζεστε

Η πλατφόρμα Digital Risk Protection παρέχει τα υψηλότερα επίπεδα εντοπισμού των παραβιάσεων δεδομένων μέσω αυτοματοποιημένης παρακολούθησης του Surface, Deep και Dark web. Προσθέτοντας αυτές τις υπηρεσίες στη συνδρομής σας, έχτε τέσσερα βασικά πλεονεκτήματα

- **Expert on-boarding** - αξιοποιήστε στο έπακρο την επένδυσή σας από την πρώτη ημέρα, αναβαθμίζοντας τις δυνατότητες της ομάδας ασφάλειας σας, ώστε να διαμορφώνουν λύσεις για κάθε περίπτωση
- **Προσαρμοσμένες υπηρεσίες στις δικές σας ανάγκες** – Συνεργαζόμαστε μαζί σας καθορίζοντας ένα μηνιαίο πρόγραμμα ενεργειών, με τη βοήθεια των ειδικών αναλυτών μας, που θα εστιάζει στους κινδύνους που αφορούν τη δική σας επιχείρηση
- **Μελέτες περιπτώσεων (use cases)** – λαμβάνετε βοήθεια από τους εξειδικευμένους αναλυτές που συγκεντρώνουν στοιχεία από διάφορες περιπτώσεις απειλών και παραβιάσεων, για να μάθετε να προστατεύετε συγκεκριμένους τύπους δεδομένων ή να εντοπίζετε συγκεκριμένες απειλές χωρίς την πολυπλοκότητα και το κόστος διαχείρισης που απαιτείται εάν όλα γίνονται εσωτερικά στην επιχείρησή σας
- **Υποστήριξη σε περίπτωση παραβίασης** - θα είμαστε εκεί όταν χρειαστείτε βοήθεια στη διερεύνηση περιστατικών παραβίασης και θα σας υποστηρίξουμε σε νομικά, επιχειρησιακά θέματα καθώς και σε θέματα ασφάλειας πληροφοριών, συμπεριλαμβανομένων των υποχρεώσεων αναφοράς της παραβίασης στην Αρχή Προστασίας Δεδομένων και στα φυσικά πρόσωπα όταν απαιτείται

Η ομάδα των συμβούλων μας έχει εκτενή εμπειρία και κορυφαία τεχνογνωσία. Αποτελεί την ιδανική ομάδα για να υποστηρίξει τα δικά σας στελέχη, παρέχοντας προγραμματισμένες υπηρεσίες ελέγχων του επιπέδου ασφάλειας αλλά και βοήθεια για την αντιμετώπιση περιστατικών παραβίασης όταν θα τη χρειαστείτε.



Ενισχύστε τη συμμόρφωσή σας με τον GDPR

Οι παραβιάσεις δεδομένων μπορεί να έχουν σαν συνέπεια σοβαρά πρόστιμα σύμφωνα με τον GDPR

Ο GDPR απαιτεί να έχετε εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ελαχιστοποίηση των κινδύνων παραβίασης προσωπικών δεδομένων. Σε περίπτωση σημαντικής παραβίασης, ο νόμος απαιτεί να ενημερώσετε την Αρχή Προστασίας Δεδομένων και τα φυσικά πρόσωπα που επηρεάζονται εάν κριθεί απαραίτητο.

Η κατάλληλη προετοιμασία είναι τα πάντα!

Χάρη στους αυτοματισμούς και την ενσωματωμένη ευφυία της πλατφόρμας Digital Risk Protection, έναντι απειλών και με τη δυνατότητα έγκαιρης ανίχνευσης, είναι ευκολότερο να αποδείξετε στην Αρχή Προστασίας Δεδομένων ότι έχετε κάνει τις εύλογες ενέργειες.

Μπορεί να αυξήσει την ικανότητά σας να παρέχετε στην Αρχή Προστασίας Δεδομένων, μια ολοκληρωμένη εικόνα του τι συνέβη, τι έχετε κάνει και τι ενέργειες θα κάνετε στη συνέχεια.

Όλα αυτά μπορούν να κάνουν τις επικοινωνίες σας με την Αρχή Προστασίας Δεδομένων, λιγότερο χρονοβόρες, δαπανηρές και αγχωτικές.

Η υπηρεσία Digital Risk Protection, θεωρείται σαν ένα «τεχνικό και οργανωτικό μέτρο», σύμφωνα με τον GDPR, και μπορείτε να τη συμπεριλάβετε στο Σχέδιο Αντιμετώπισης Περιστατικών Παραβιάσεων που υποχρεούστε να έχετε στην επιχείρησή σας.

Προτεινόμενες Λύσεις Digital Risk Protection και Σύγκρισή τους

Συνοπτικά Χαρακτηριστικά	SKURIO-DRP Bronze	SKURIO-DRP Silver	SKURIO-DRP Gold
Παραμετροποίηση & Αρχική Εκπαίδευση	◉	◉	◉
Ιστορικές Αναζητήσεις διαρροής δεδομένων	◉	◉	◉
Οδηγός Αντιμετώπισης Παραβιάσεων	◉	◉	◉
Corporate Email Domain	◉	◉	◉
Corporate URL Monitoring		◉	◉
IP addresses		◉	◉
Παραποιημένα URLs, Προϊόντα, κλπ. (Typosquatting)		◉	◉
Individual email addresses		◉	◉
Αναζητήσεις με λέξεις κλειδιά (Keywords) – για την επιχείρηση. (Brand Monitoring)			◉
Αναζητήσεις με λέξεις κλειδιά (Keywords) - για δεδομένα στελεχών, διοίκησης, κλπ., VIP Monitoring			◉
Αναζητήσεις με λέξεις κλειδιά (Keywords) – για κρίσιμα επιχειρηματικά δεδομένα, όπως προσωπικό, προϊόντα, δεδομένα πελατών, πνευματική ιδιοκτησία, επιχειρηματικά μυστικά, κλπ.(Business Critical Info)			◉

Τεχνικές Προδιαγραφές

Platform features

- Domain and email monitoring
- Infrastructure information monitoring
- Financial and personal information monitoring
- Keyword monitoring
- BreachMarkers - synthetic watermarking
- Automated monitoring of surface, deep and Dark Web sources for your data 24x7
- Unique historic breached data library of 3.5 billion post, dump and web page records
- Assign messages, add comments, status & priority
- 'Ask an Analyst' direct line to help and advice
- Post takedown and optional* site takedowns

CTI features*

- Specialist pattern matching/REGEX searching
- Point-and-click filters to identify threats easily
- Zoom in on author, site, or channel and track authors or sites of interest to spot threats
- Visualise and analyse results
- Discover trends that could affect your business

* With CTI / enterprise packages

Core data sources

- Dark Web: TOR (.onion) marketplaces and sites
- IRC: Internet Relay Chat rooms
- Bins: anonymous text dump sites used for leaking and marketing data
- Derived Sources: unlisted and private dump sites
- Curated Sources: content from hard-to-reach sites gathered by our analyst team
- Data Dumps: credentials from large data breaches
- Hacker forums
- Typosquatting: domain registration feeds

CTI data sources

- Reddit, Telegram and news
- YouTube, Flickr and VK
- Custom market place and social media sources*

Integration

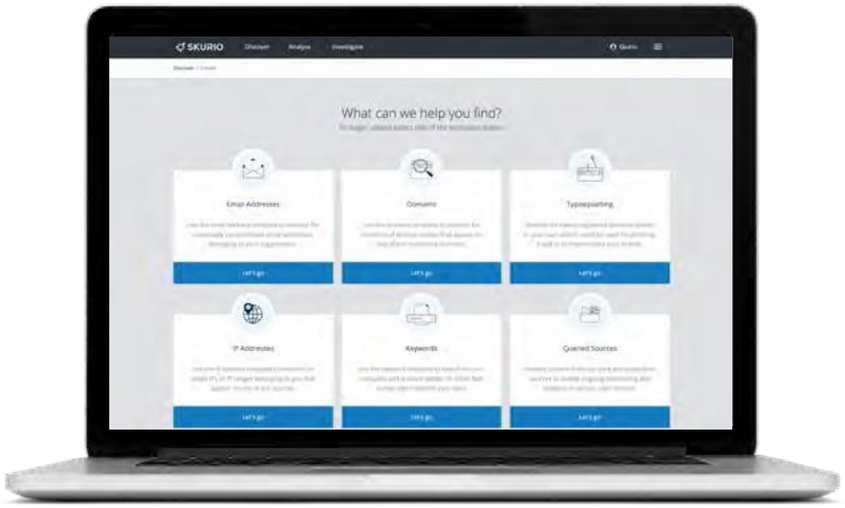
- REST Application Programming Interface (API) access for integration SOC solution integration including Splunk, Microsoft, ServiceNow and Microsoft connectors*

Platform

- SaaS solution, EU based application & data hosting
- Multi-factor authentication including SMS option
- In-app help, knowledge base and how-to videos
- REST API integration to any SOC application*

Instant alerts

- In-app, email, Teams, SMS and Slack notifications



RBL - Data Protection Service Center

Διεθνής Εμπειρία / Βέλτιστες Πρακτικές

CX + Privacy

Ευαισθητοποίηση & Εκπαίδευση

ATTACK SIMULATOR

Συμβουλευτικές Υπηρεσίες

Θεματική Εκπαίδευση

The DPO Academy

Certification

Εξειδικευμένες Νομικές Υπηρεσίες

Digital Risk Protection

SKURIO

Βελτιστοποίηση Λειτουργιών / Διαδικασιών

Vulnerability Assessment

Ανθεκτικότητα & Ανάκτηση

Αντιμετώπιση Περιστατικών Παραβίασης

Cyber Insurance

ISO Standards

IT Security

RBL

RETHINK BUSINESS LAB

INNOVATION STRATEGY AGILITY

The DPO Academy

SKURIO

ATTACK SIMULATOR

info@rbl.gr

www.rbl.gr

+30 215 560 0411

ΕΛΛΗΝΙΚΟ ΙΝΣΤΙΤΟΥΤΟ ΕΞΥΠΗΡΕΤΗΣΗΣ ΠΕΛΑΤΩΝ ΕΙΕΠ

CSR: ΟΜΑΔΑ ΑΙΓΑΙΟΥ