Zelus SOC

Ανίχνευση και Ανάλυση περιστατικών ασφάλειας από εξειδικευμένο προσωπικό

Ιούλιος 2022

www.zelus.gr

Τατοΐου 92, 14452

Μεταμόρφωση, Αθήνα - GR

Σύντομη Περιγραφή

Οι σύγχρονες επιχειρήσεις και οι ψηφιακές τους υποδομές, που χρησιμοποιούνται για την παροχή ολοκληρωμένων, ποιοτικά αναβαθμισμένων, έγκυρων και έγκαιρων πληροφοριών, υπηρεσιών και ηλεκτρονικών συναλλαγών, όλο και περισσότερο στη σημερινή εποχή, αντιμετωπίζουν απειλές για την ασφάλειά τους από ένα ευρύ φάσμα κινδύνων. Πέρα από τις φυσικές απειλές, οι ψηφιακές υποδομές βρίσκονται αντιμέτωπες με απειλές ψηφιακής μορφής, όπως οι ιοί υπολογιστών και οι κυβερνοεπιθέσεις με σκοπό την κλοπή και την απώλεια της δυνατότητας παροχής των ποικίλων αναβαθμισμένων υπηρεσιών που προσφέρουν. Τέτοιες απειλές συναντώνται σε όλο και πιο εξεζητημένες μορφές και έχουν σαν συνέπεια, μεταξύ άλλων, την απώλεια απόρρητης πληροφορίας, τη στέρηση δυνατότητας παροχής υπηρεσιών και τον εκβιασμό.

Προς την κατεύθυνση αυτή, η εταιρεία μας παρέχει το Zelus SOC, που αποτελεί μία ολοκληρωμένη υπηρεσία για την παρακολούθηση του δικτύου και εφαρμογών μίας επιχείρησης και την ανάλυση και αντιμετώπιση συμβάντων ασφάλειας από εξειδικευμένο προσωπικό. Σκοπός της λύσης είναι η έγκαιρη ανίχνευση απειλών και επιθέσεων και η επιτάχυνση των μηχανισμών αντιμετώπισης αυτών για τη διασφάλιση της επιχειρησιακής συνέχειας και ακεραιότητας των διαδικασιών, συστημάτων και πληροφοριών της επιχείρησης.

Προδιαγραφές

Η λύση Zelus SOC αποτελεί μία ολοκληρωμένη υπηρεσία για την αποτελεσματική προστασία της επιχείρησης και την υποστήριξη στον εντοπισμό και την αντιμετώπιση περιστατικών ασφάλειας στον κυβερνοχώρο (threat intelligence). Τα λειτουργικά χαρακτηριστικά της λύσης συνοψίζονται στα ακόλουθα:

- Υποστήριξη από εξειδικευμένο προσωπικό μας για τον εντοπισμό ανωμαλιών στην ψηφιακή δραστηριότητα της επιχείρησης και ενδείξεων απειλών ή/και επιθέσεων στην ψηφιακή υποδομή της.
- Άμεση ενημέρωση με φυσικά και ηλεκτρονικά μέσα του υπεύθυνου της επιχείρησης για κρίσιμα συμβάντα που παρατηρούνται και υποστήριξη στην υλοποίηση μηχανισμών αντιμετώπισης αυτών.
- Συνεχή παρακολούθηση της ψηφιακής δραστηριότητας της επιχείρησης και εφαρμογή μέτρων προστασίας.
- Σύστημα συλλογής και διαχείρισης αρχείων καταγραφής (logs) σχετικά με την εισερχόμενη και εξερχόμενη κίνηση στο δίκτυο μίας επιχείρησης και των ενεργειών στις τερματικές συσκευές και τα εγκατεστημένα λειτουργικά συστήματα και εφαρμογές προστασίας (Security Information and Event Management - SIEM).
- Σύστημα ανίχνευσης περιστατικών ασφάλειας (intrusion detection)
- Ανάλυση, διαχείριση και οπτικοποίηση πιθανών απειλών και συμβάντων, μέσα από μία φιλική προς το χρήση εφαρμογή διαδικτύου (online dashboard).

Πιο συγκεκριμένα, η λύση Zelus SOC παρέχει προστασία και διαχείριση περιστατικών από ενέργειες που υποδηλώνουν πιθανή απειλή ή επίθεση, όπως η εκτέλεση ενός κακόβουλου λογισμικού (malware) ή εντολών που απαιτούν εξειδικευμένα δικαιώματα πρόσβασης (powershell), η δημιουργία ενός νέου χρήστη ή η αλλαγή των δικαιωμάτων πρόσβασης ενός υφιστάμενου χρήστη, η εκτέλεση ασυνήθιστων διεργασιών (unusual processes), η ασυνήθιστη συμπεριφορά χρηστών, όπως η σύνδεση ενός χρήστη

σε μη συνηθισμένες ώρες εργασίας (out-of-office hours login), η διασύνδεση με εξωτερικές συσκευές αποθήκευσης (πχ. συσκευές USB κλπ.), και η μεγάλη κατανάλωση πόρων συστήματος (CPU, RAM, bandwidth) που προκύπτουν από η εξουσιοδοτημένες ενέργειες, όπως η διενέργεια ύποπτων μεταφορών αρχείων.

Η λύση Zelus SOC παρέχει τη δυνατότητα αποθήκευσης της συλλεγόμενης πληροφορίας σε βάση δεδομένων, ακολουθώντας μια προσέγγιση που εγγυάται την ασφάλεια, ακεραιότητα, αποδοτική ανάκτηση και γρήγορη αναζήτησή τους ανά πάσα στιγμή. Επίσης, η ανάκτηση των δεδομένων οδηγεί εύκολα και με κατανοητό τρόπο στην πλήρη καταγραφή και έλεγχο των ενεργειών, ως προς την αντιμετώπιση των συμβάντων ασφάλειας.

Η λύση Zelus SOC έχει αναπτυχθεί με κριτήρια την ανθρωποκεντρική προσέγγιση και την πρόσβαση στις παρεχόμενες υπηρεσίες σε όλους, υιοθετώντας διεθνή πρότυπα, κανόνες και βέλτιστες πρακτικές. Τα βασικά τεχνικά χαρακτηριστικά της λύσης περιλαμβάνουν:

- Υλοποίηση βασισμένη σε μία αρχιτεκτονική πολλαπλών επιπέδων και ανοιχτών προτύπων, με δυνατότητες συνεργασίας με διάφορες μορφές βάσεων δεδομένων, λειτουργικά συστήματα, εξυπηρετητές διαδικτύου & εφαρμογών.
- Παροχή και υποστήριξη συνεργατικών τεχνολογιών.
- Δυνατότητα διαχείρισης χρηστών και απόδοσης διαβαθμισμένης πρόσβασης σε συγκεκριμένες λειτουργίες και πληροφορίες συμβάντων.
- Εύκολη διασύνδεση και ενσωμάτωση με υπάρχοντα πληροφοριακά συστήματα ενός οργανισμού, βάσει διεθνών προτύπων και βέλτιστων πρακτικών, με χρήση ευρέως αποδεκτών τεχνολογιών και δομών μορφοποίησης και μετασχηματισμού δεδομένων και μεθόδων επικοινωνίας.
- Επεκτασιμότητα για την κάλυψη νέων και μελλοντικών υπηρεσιών σχετικά με τη διαχείριση περιπτώσεων ασφάλειας από πιθανές κυβερνοαπειλές.
- Τήρηση του Ελληνικού Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Προτύπων Διαλειτουργικότητας (e-GIF).
- Συμμόρφωση με διεθνή πρότυπα και οδηγίες για την ψηφιακή ασφάλεια δεδομένων, με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), και τον κανονισμό διασφάλισης ιδιωτικότητας (e-Privacy).

Πρόσθετες Παροχές Λύσης

Παρέχεται η δυνατότητα εφαρμογής μέτρων πρόληψης και προστασίας από κυβερνοαπειλές, μέσα από την ασφαλή διαμόρφωση εξοπλισμού και κρίσιμων εφαρμογών προστασίας και τον έλεγχο για τη σωστή παραμετροποίηση της υπάρχουσας υποδομής ασφάλειας. Στην περίπτωση που η υποδομή της επιχείρησης δεν το υποστηρίζει, παρέχεται η δυνατότητα εγκατάστασης και παραμετροποίησης εφαρμογών τείχους προστασίας (firewall) και αντιϊκού προγράμματος (antivirus).