DTS

SECURITY OPERATIONS CENTER (SOC)

SECURITY OPERATIONS CENTER

Οι κυβερνοεπιθέσεις εξελίσσονται και γίνονται ολοένα και πιο περίπλοκες, ενώ μπορούν να πραγματοποιηθούν ανά πάσα στιγμή. Εκτός από την πολυπλοκότητα των απειλών, η έλλειψη ορατότητας των συσκευών στα δίκτυα, η πληθώρα των ειδοποιήσεων και τέλος η ανεπαρκής εξειδίκευση και ελλιπής γνώση του αντικειμένου εντείνουν τη δυσκολία αντιμετώπισης τους. Ο καλύτερος τρόπος να ανταπεξέλθει κανείς σε αυτές τις αυξημένες απαιτήσεις και να μειώσει τον κίνδυνο από τις επιθέσεις είναι η ύπαρξη ενός Κέντρου Ελέγχου Ασφαλείας (Security Operations Center).

Ένα SOC αποτελείται από αναλυτές και μηχανικούς εξειδικευμένους στην ασφάλεια των πληροφοριακών συστημάτων, που παρακολουθούν συνεχώς τις υποδομές IT. Ωστόσο, είναι δύσκολο για μια επιχείρηση να δημιουργήσει μια τέτοια δική της ομάδα που λειτουργεί αδιάκοπα όλο το 24ωρο, καθώς είναι δαπανηρό και χρονοβόρο.

Η Υπηρεσία SOC της DTS είναι η ιδανική λύση. Το Κέντρο Ελέγχου Ασφάλειας της DTS παρακολουθεί και προστατεύει όλη την IT υποδομή σας συνεχώς, 24/7, 365 μέρες το χρόνο. Παρακολουθούμε, συλλέγουμε δεδομένα, τα επεξεργαζόμαστε και τα αναλύουμε, ανιχνεύουμε πιθανές ανωμαλίες του συστήματος και ενδεχόμενες κυβερνοεπιθέσεις και εφαρμόζουμε μέτρα αντιμετώπισης. Έτσι σας υποστηρίζουμε σε δύο επίπεδα ταυτόχρονα: αφ' ενός προληπτικά, ελέγχοντας συνεχώς τις υποδομές, αφ' ετέρου αποτρεπτικά με τον εντοπισμό και την αντιμετώπιση των απειλών.

- Εξειδικευμένοι μηχανικοί και αναλυτές SOC 24/7/365
- Πιστοποιημένη λειτουργία στην Ευρώπη
- Συνδυασμός τεχνολογίας και ανθρώπινου δυναμικού
- Γρήγορη ανίχνευση ανωμαλιών και προτάσεις αντιμετώπισης
- Αξιοποίηση της εμπειρίας και των γνώσεων της ομάδας SOC της DTS
- Διαφάνεια / Ορατότητα στις υποδομές IT σας
- Προσαρμογές με βάση τα τεκμηριωμένα συμβάντα
- Ανάλυση ευαλωτότητας (vulnerability analysis)
- Ενημέρωση σε τακτά χρονικά διαστήματα
- Συνεχής βελτίωση
- Ελληνόφωνη και αγγλόφωνη ομάδα μηχανικών και αναλυτών

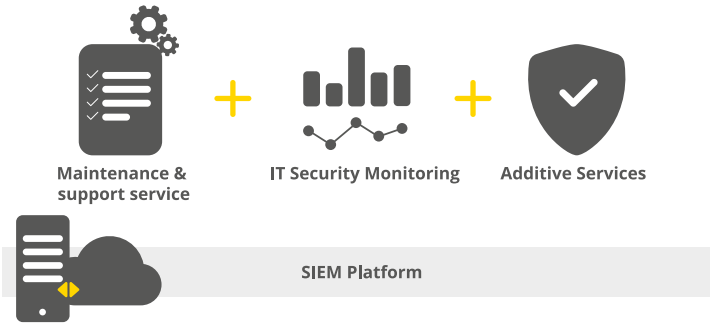
Η παρακολούθηση του IT περιβάλλοντος μιας επιχείρησης από ένα Κέντρου Ελέγχου Ασφαλείας (SOC) είναι πολύ σημαντικός παράγοντας για την ασφάλεια αυτού. Ανεξαρτήτως της μορφής και της κλίμακας μιας κυβερνοεπίθεσης, αν εντοπιστεί αργά μια επίθεση, μπορεί να προκληθεί τεράστια ζημιά. Επιπλέον, οι επιτιθέμενοι έχουν πάντα τη δυνατότητα να επαναχρησιμοποιούν στοιχεία πρόσβασης και δεδομένα και να επαναλάβουν τις επιθέσεις σε άλλη χρονική στιγμή. Για το λόγο αυτό είναι πολύ σημαντικό να υπάρχει ένας συνδυασμός εμπειρίας στην κυβερνοασφάλεια, ορατότητας των δικτύων, διάγνωσης, ανάλυσης και γνώσεις των κατάλληλων τρόπων αντιμετώπισης. Επιπλέον, θα πρέπει πάντα να λαμβάνεται υπόψη όλες οι ιδιαιτερότητες της εκάστοτε υποδομής IT, οπότε άλλος πολύ σημαντικός παράγοντας είναι η τεχνική επάρκεια των αναλυτών που παρακολουθούν και εποπτεύουν στο Κέντρο Ελέγχου Ασφαλείας. Οι επιθέσεις μπορούν να πραγματοποιηθούν όλο το 24ώρο και συνεπώς η διασφάλιση της συνεχούς λειτουργίας ενός SOC για την αντιμετώπιση δυνητικών απειλών, αποτελεί πάντα μια δύσκολη πρόκληση για κάθε επιχείρηση.

Η εξειδικευμένη ομάδα του DTS SOC βρίσκεται πάντα σε επιφυλακή. Με αυτόματη ανίχνευση των επιθέσεων, ενεργή παρακολούθηση από ειδικούς στην κυβερνοασφάλεια, ταχεία ανάλυση και διερεύνηση των κινδύνων και έγκαιρη αντιμετώπιση των απειλών λαμβάνετε υπηρεσίες υψηλού επιπέδου SOC 24/7/365, σε χαμηλό κόστος και χωρίς να εμπλέκεστε με την πολυπλοκότητα και τις δυσκολίες που σχετίζονται με τη δημιουργία, τη σωστή στελέχωση και τη λειτουργία του δικού σας Κέντρου Ελέγχου Ασφαλείας (SOC). Έτσι να μπορείτε να επικεντρωθείτε στις δικές σας κύριες δραστηριότητές. Εμείς αναλαμβάνουμε σαν managed services την παρακολούθηση και την ανάλυση των IT συστημάτων σας, την ανίχνευση και την αντιμετώπιση των κενών ασφαλείας, τη διαχείριση της ασφάλειας κεντρικά, τη διαχείριση των alerts και την καταγραφή αυτών, τους τακτικούς ελέγχους, τη συμμόρφωση με τους κανονισμούς, την ενημέρωση σας και πολλά ακόμη.

Οι υπηρεσίες που παρέχει το SOC της DTS καλύπτουν ένα ευρύ φάσμα ενεργειών, ώστε να παρέχουμε τη σιγουριά στους πελάτες μας, ότι τα πληροφοριακά τους συστήματα είναι ασφαλή. Παρέχονται δε σε μηνιαία βάση, μετά από έναν αρχικό σχεδιασμό και την φάση ενεργοποίησης. Ανάλογα με τις απαιτήσεις σας, προσφέρουμε διάφορες μεθόδους παροχής: αφενός, παρακολούθηση ασφάλειας IT (με βάση το SIEM), αφετέρου μέσω υπηρεσιών MDR (με βάση το Cortex XDR).

ΥΠΗΡΕΣΙΕΣ SOC ΒΑΣΙΣΜΕΝΕΣ ΣΤΟ SIEM ΤΗΣ LOGRHYTHM

Οι υπηρεσίες SOC με βάση το SIEM στηρίζονται σε αυτήν την περίπτωση στο XDR της LogRhythm. Οι δυνητικά επικίνδυνες ανωμαλίες του συστήματος εντοπίζονται, τεκμηριώνονται και καταγράφονται μέσω αυτής της τεχνολογίας σε μια κεντρική κονσόλα. Αυτό παρέχει στις εταιρείες μια ολιστική άποψη της κατάστασης ασφάλειάς τους. Επιπλέον, οι λύσεις SIEM βοηθούν να αποδειχθεί η συμμόρφωση με τις νομοθετικές και κανονιστικές απαιτήσεις ενώ παράλληλα παρακολουθούνται όλα τα συμβάντα. Με βάση το SIEM προσφέρονται διάφορες εναλλακτικές για να χαρτογραφήσουμε τις ανάγκες σας με τον καλύτερο δυνατό τρόπο. Από την αρχική ενεργοποίηση, τη διαχείριση του SIEM σαν managed service, την παροχή υπηρεσίας SOC έως και την τελική αντιμετώπιση των τρωτών σημείων των συστημάτων σας. Με αυτόν τον τρόπο η DTS έχει πάντα την κατάλληλη λύση, για να σας προσφέρει τη βέλτιστη δυνατή υποστήριξη.



ΠΛΕΟΝΕΚΤΗΜΑΤΑ

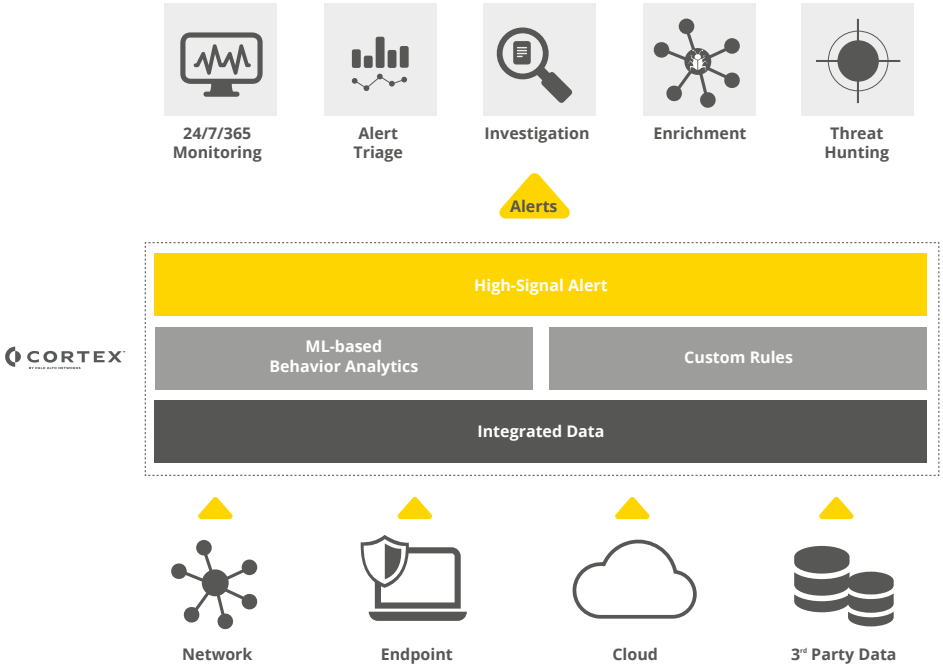
- Υπηρεσία 24/7/365
- Διαχείριση πλατφόρμας on-premises ή στο cloud
- Αξιολόγηση απειλών & κινδύνων από ιστορικά αρχεία καταγραφής
- Χρήση των βέλτιστων πρακτικών της DTS στις ανάγκες του πελάτη
- Ανίχνευση περιστατικών ασφαλείας από τους πιστοποιημένους αναλυτές του SOC της DTS
- Άμεση ενημέρωση για συμβάντα μέσω προκαθορισμένων καναλιών επικοινωνίας στην οποία περιλαμβάνονται αναφορές, πληροφορίες για τα συμβάντα, συστάσεις για ανάκτηση δεδομένων και περιορισμό της ενδεχόμενης βλάβης
- Μηνιαία συνάντηση για αξιολόγηση των αναγκαίων προσαρμογών
- Ενημερώσεις για εναρμόνιση με κανονισμούς και ελέγχους
- Τριμηνιαίες αναφορές σχετικά με την ανάλυση της εικόνας των απειλών και παρουσίαση προτάσεων για την αντιμετώπιση αυτών
- Τακτικές αναφορές για τις απειλές που ανιχνεύτηκαν
- Τακτικές αναφορές για τις ενέργειες που ακολούθησαν και προτάσεις βελτίωσης

ΚΥΡΙΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΗΣ ΥΠΗΡΕΣΙΑΣ SOC ΒΑΣΙΣΜΕΝΗ ΣΤΟ LOGRHYTHM SIEM

- Διαχείριση μέσω κεντρικής πλατφόρμας SIEM
- Παρακολούθηση της ασφάλειας των IT συστημάτων
- Πληροφόρηση σχετικά με το επίπεδο συμμόρφωσης με κανονισμούς
- Πλήρης εικόνα της επιχειρησιακής κατάστασης των συστημάτων

ΥΠΗΡΕΣΙΑ MDR ΒΑΣΙΣΜΕΝΗ ΣΤΟ CORTEX XDR

Η υπηρεσία DTS Managed Detection and Response (MDR) αυξάνει σημαντικά την αποτελεσματικότητα για την ανίχνευση και την αντιμετώπιση κυβερνοαπειλών. Για τη γρήγορη ανίχνευση πιθανών απειλών σε ολόκληρο το IT περιβάλλον σας, βασικός παράγοντας είναι ο συνδυασμός υψηλής εξειδίκευσης προσωπικού και η χρήση κορυφαίας τεχνολογίας. Οι άρτια εκπαιδευμένοι αναλυτές και μηχανικοί που αποτελούν το SOC της DTS, παρακολουθούν ενεργά 24/7/365 τις δυνητικές απειλές και τις αντιμετωπίζουν βασιζόμενοι στην πλατφόρμα Cortex XDR της Palo Alto Networks. Συνδυάζουμε την αυτόματη ανίχνευση, την ανάλυση και την αντιμετώπιση, βασιζόμενοι σε τεχνολογίες αιχμής, με συνεχή προληπτικό έλεγχο, ανάλυση δεδομένων και άμεση αντιμετώπιση των απειλών.



ΠΛΕΟΝΕΚΤΗΜΑΤΑ

- 24/7/365 ανίχνευση, παρακολούθηση, δράση μέσω της πλατφόρμας Cortex XDR
- Συνεχείς προληπτικές ανιχνεύσεις δυνητικών απειλών
- Αυτοματοποιημένη ανάλυση με τη χρήση κορυφαίας τεχνολογίας
- Root cause ανάλυση, έλεγχος και αποκατάσταση
- Χρήση πληθώρας βάσεων δεδομένων σχετικών με κυβερνοαπειλές
- Ψηφιακή ανάλυση δεδομένων
- Ursachenanalyse, Prozesseingrenzung & -behebung
- Bedrohungserkennung auf Basis der Informationen führender Threat Intelligence Plattformenn

ΚΥΡΙΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΗΣ ΥΠΗΡΕΣΙΑΣ MDR ΒΑΣΙΣΜΕΝΗ ΣΤΟ CORTEX XDR

- Ανίχνευση & ανάλυση βασιζόμενες σε πληροφορίες από τερματικά
- Αντιμετώπιση περιστατικών μέσω της πλατφόρμας Cortex XDR
- Ανίχνευση & ανάλυση απειλών για την ασφάλεια του IT περιβάλλοντος

DTS Cloud Security MonEPE - Athens
+30 211 1040-711

dts.de
info@dts-cloudsecurity.gr