CBS.LAN
Cyber Security

Prevent.
Detect.
Respond.

Managed Services for Detection
& Response (MSDR)

1. Υπηρεσίες Διαχείρισης Συμβάντων

Οι υπηρεσίες "Managed Services for Detection & Response (MSDR)" της CBSLAN υλοποιούν ένα ολοκληρωμένο Σύστημα Διαχείρισης Συμβάντων Κυβερνοασφάλειας ώστε να τα εντοπίσουν άμεσα προτού αυτά επιφέρουν αρνητικές συνέπειες επιπτώσεις στην λειτουργία του πελάτη. Συνδυάζουν τεχνολογία, ανθρώπους και διαδικασίες έτσι ώστε ο τελικός πελάτης χρησιμοποιώντας τις να εκμεταλλευτεί την πολύ εκτενή εμπειρία και το εύρος της τεχνογνωσίας μας.

Η προτεινόμενη υπηρεσία MSDR λειτουργεί όλο το 24ωρο και έχει σχεδιασθεί με δεδομένο ότι τα εταιρικά δίκτυα κάποια στιγμή στο άμεσο μέλλον θα δεχθούν επίθεση στο πληροφοριακού περιβάλλοντος τους. Φροντίζουμε η υπηρεσία να επικεντρωθεί στην γρήγορη ενημέρωσης και στην άμεση απόκριση σε περίπτωση συμβάντος αναλύοντας την πορείας της επίθεσης είτε από το LAN είτε από το Internet.
Η πλατφόρμα μας είναι πλήρως συμβατή με όλους τους σημαντικούς κατασκευαστές προϊόντων ασφάλειας, αξιοποιώντας τις πληροφορίες που αυτές οι συσκευές προσφέρουν, έτσι ώστε να σχηματιστεί μια ολοκληρωμένη λύση MSDR με τελικό αποτέλεσμα την αντιμετώπιση ενός μεγάλου φάσματος σύνθετων απειλών σε επίσης πολύπλοκα κ σύνθετα περιβάλλοντα πληροφορικής.

Οι προσφερόμενες υπηρεσίες της CBSLAN καλύπτουν τους παρακάτω τομείς:

- Συλλογή και ανάλυση των αρχείων (logs) από τις συσκευές που ορίζονται στο SOW ως log sources (network flows, syslogs, traps, IDS/IPS, vulnerability assessments , κλπ)
- Έλεγχο και διατήρηση των logs για να εντοπιστούν πιθανές αδυναμίες στη λειτουργία τους
- Εφαρμογή της εταιρικής πολιτικής ασφάλειας
- Συσχέτιση πληροφοριών σε πραγματικό χρόνο και ενημέρωση του πελάτη για τα περιστατικά. Η ανάλυση περιστατικών γίνεται από εξειδικευμένο και έμπειρο μηχανικό για να εντοπιστούν τα πραγματικά περιστατικά και να αγνοούνται τα false positives
- Πιθανή η επιτόπια μετάβαση μηχανικού για ανάλυση και αντιμετώπιση κρίσιμων επιθέσεων (On-site Incident Response & forensics)
- Προετοιμασία για συμμόρφωσης με νομικά και κανονιστικά πλαίσια
- Συνεχής ενημέρωση του πελάτη σε περίπτωση εκδήλωσης συμβάντος με δυνατότητα επέμβασης αν το επιθυμεί, ανάλογα με την κρισιμότητα του περιστατικού
- Συλλογή και ανάλυση των αρχείων (logs) από servers, routers, switches, access points, κλπ
- Ενιαία διαχείριση περιστατικών in real time
- Συνεχής παρακολούθηση (24x7) από εξειδικευμένο μηχανικό και σε πραγματικό χρόνο των Alerts που δημιουργούνται από την πλατφόρμα μας, με επιπλέον ανάλυση των events που τα δημιούργησαν
- Καταγραφή ενεργειών διαχείρισης συμβάντος μαζί με αναλυτικές ενέργειες σε ticketing μηχανισμό με πρόσβαση από τον πελάτη για να ενημερωθεί
- Αναλυτικό Reporting με δημιουργία αναφοράς σε ημερήσια, εβδομαδιαία ή και μηνιαία βάση με απεικόνιση του επιπέδου ασφάλειας της υποδομής

2. Scope of Work – Service Commitment

Η ολοκληρωμένη υπηρεσία Managed Services for Detection and Response (MSDR) σε 24ωρη βάση εντοπίζει άμεσα επιθέσεις κ απειλές είτε από Internet είτε από το ευρύτερο εταιρικό LAN. Για την επίτευξη του παραπάνω στόχου η προσέγγισή μας έχει χτισθεί πάνω στις ακόλουθες βασικές αρχές:

Λειτουργεί με συγκεκριμένα «Threat Scenarios» για την παρακολούθηση των συστημάτων βάσει σεναρίων ανεπτυγμένα για την συγκεκριμένη υποδομή. Τα Threat Scenarios σχεδιάζονται για τον εντοπισμό των μορφών απειλών αλλά και των βημάτων επίθεσης. Η υπηρεσία παραμετροποιείται στις απαιτήσεις και τα τεχνικά χαρακτηριστικά του IT περιβάλλοντος για την κάλυψη συγκεκριμένων αναγκών του πελάτη. Για ειδικά Threat Scenarios γίνεται εγκατάσταση security agents στην IT υποδομή για την βελτίωση της αποτελεσματικότητας.

Κατά τον σχεδιασμού της μεθοδολογίας των MSDR υπηρεσιών μας αναλύουμε και συμπεριλαμβάνουμε πληροφορίες που αφορούν το προφίλ απειλών και ευπαθειών από το LAN & Internet. Με τον τρόπο αυτό η λύση μας λαμβάνει συνεχώς χρήσιμα στοιχεία για νέες απειλές από διάφορους παρόχους σχετικών πληροφοριών στο Διαδίκτυο. Για κάθε επιβεβαιωμένο περιστατικό επίθεσης γίνεται αναλυτική επεξεργασία των χαρακτηριστικών της και αυτά μετά ενσωματώνονται στους γενικούς κανόνες ανάλυσης και συσχέτισης των logs.

Βασιζόμαστε ιδιαίτερα στην αυτοματοποιημένη διαδικασία αντιμετώπισης των πραγματικών περιστατικών (δηλ. για το Incident Response) ώστε να επιτυγχάνεται η ταχεία επιβεβαίωση τους για την επιλογή των βέλτιστων ενεργειών αντιμετώπισης από τους ειδικούς Incident Responders και την ομάδα αντιμετώπισης συμβάντων ασφάλειας (Security Incident Response Team-SIRT) της CBS LAN.

3. Ανταγωνιστικά πλεονεκτήματα

Η υπηρεσία παρακολούθησης ασφάλειας και απειλών σε 24ωρη βάση της CBS LAN, έχει ως σκοπό την προσφορά υψηλού επιπέδου υπηρεσιών προσαρμοσμένων στις ανάγκες του πελάτη με κινητήρια δύναμη το εξειδικευμένο ανθρώπινο δυναμικό μηχανικών της.

Η CBS LAN είναι θυγατρική των δύο από τους μεγαλύτερους παρόχους υπηρεσιών πληροφορικής (Cosmos Business Systems & LANCOM) με κυρίαρχη ελληνική παρουσία και εξειδικευμένες υπηρεσίες διαχείρισης ασφάλειας (MSSDR) που καθιστούν την CBS LAN τον πιο έμπιστο συνεργάτη για να ανταποκριθεί άμεσα σε ανάγκη ασφάλειας.
Στον πίνακα που ακολουθεί παρουσιάζονται συνοπτικά τα βασικά σημεία διαφοροποίησης της CBS LAN ως παρόχου υπηρεσιών 24x7 MSDR σε σχέση με τον ανταγωνισμό.
Βασικά Σημεία Διαφοροποίησης:

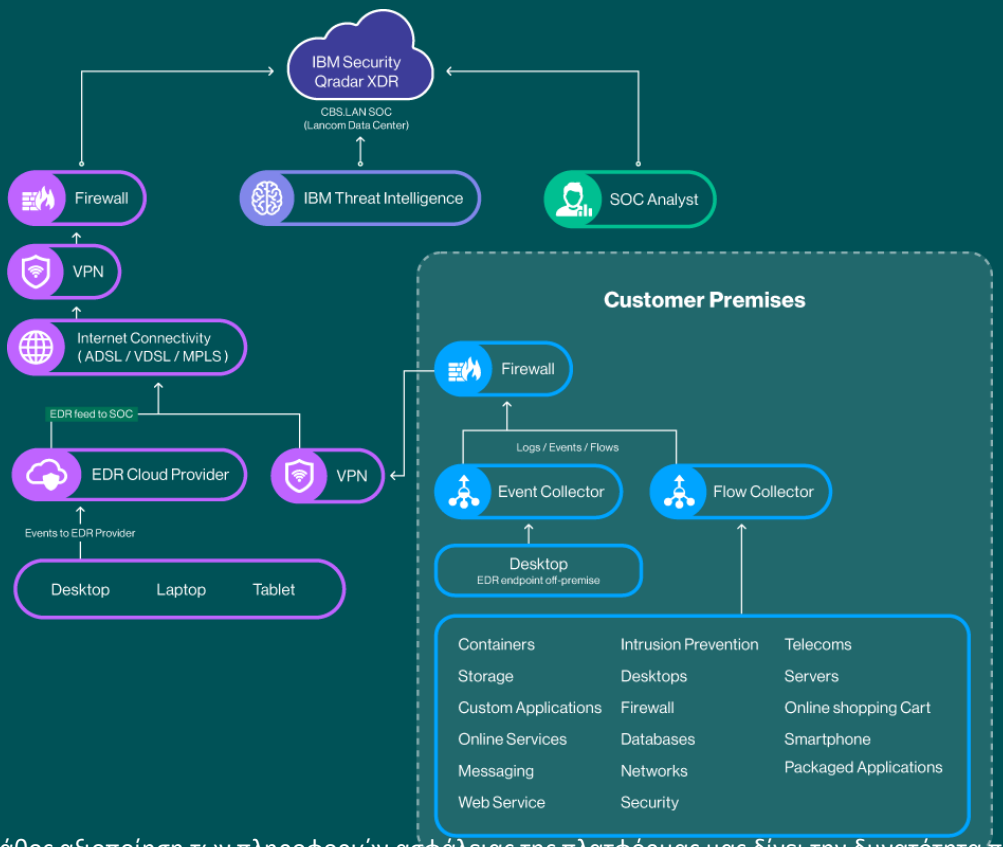
Μοναδική Τεχνογνωσία	Θυγατρική των 2 κορυφαίων παρόχων Managed Services στον Ελληνικό Χώρο με το τεράστιο δυνητικό πελατολόγιο τους (CBS & Lancom) και την εμπειρία στον σχεδιασμό και υλοποίηση έργων υποδομής Το 90% των μηχανικών της CBS LAN διαθέτει πιστοποίηση/μεταπτυχιακό τίτλο στην Ασφάλεια Πληροφοριών Πολλαπλές πιστοποιήσεις ασφάλειας
Κορυφαία Τεχνολογική Πλατφόρμα	MSDR SIEM: IBM Qradar, SOAR & Advisor Add Ons Εφαρμογή ειδικών τεχνικών-μηχανισμών όπως: • Deep packet inspection • Advanced malware analysis • Advanced Endpoint protection (EDR/XDR) • Active response • Threat intelligence feeds • Continuous endpoint monitoring
Προσαρμοσμένη διαχείριση υποδομής	Υλοποίηση Security Audit & Risk Assessment κατά την αρχική φάση σχεδιασμού για κάθε πελάτη

Incident Response και διαχείριση εξοπλισμού πελάτη	Εκτεταμένη τεχνογνωσία σε πολλές πλατφόρμες κατασκευαστών όπως : • Fortinet • Cisco • Microsoft Defender • ESET
Κατάρτιση Τεχνικής ομάδας MSDR (Analyst & SIRT)	Μεταπτυχιακός τίτλος στην Ασφάλεια Πληροφοριών (SOC Analysts) Εξειδίκευση στις στοχευμένες επιθέσεις Μοναδική τεχνογνωσία-εμπειρία πάνω στις στοχευμένες επιθέσεις Advanced Cyber Threats (APTs, Cyber-Insider, etc.) Συμμετοχή σε πολυάριθμα έργα διερεύνησης & αντιμετώπισης περιστατικών ασφάλειας (Incident Response & Digital Forensics investigations)
Σημεία παρουσίας	Κάλυψη με επιτόπου παρουσία SOC Responder Engineer σε Αθήνα & Θεσσαλονίκη σε συνδυασμό με την υφιστάμενη πανελλαδική κάλυψη της Cosmos Business Systems.

4. Τεχνολογική Πλατφόρμα

Βασιζόμαστε στην κορυφαία πλατφόρμα διαχείρισης ασφάλειας της IBM (Qradar SIEM) η οποία παρέχει προηγμένες δυνατότητες διαχείρισης συμβάντων. Η τεχνική πλατφόρμα έχει σχεδιασθεί με βάση την ευελιξία και επεκτασιμότητα ώστε να προσαρμόζεται στις απαιτήσεις του κάθε πελάτη και της υποδομής του. Διαχειρίζοντας τα logs με τις προηγμένες δυνατότητες ανίχνευσης απειλών, η πλατφόρμα MSSDR της CBS LAN αποτελεί μια αποτελεσματική SOC λύση που επιτρέπει την αξιοποίηση των πληροφοριών ασφάλειας.

Με την πλατφόρμα της CBS LAN διευρύνετε η ορατότητα της δικτυακής κίνησης χρηστών και εφαρμογών στην υποδομή παρέχοντας πληροφορίες για πιθανές πηγές απειλών στο ευρύτερο εταιρικό δίκτυο (on premise & cloud). Η πλατφόρμα συλλέγει, επεξεργάζεται και συσχετίζει πληροφορίες ασφάλειας από το δίκτυο και τα συστήματα αναλύοντας την δραστηριότητα για τον εντοπισμό και την ιεράρχηση συμβάντων. Η αρχιτεκτονική της MSSDR υπηρεσίας ακολουθεί συγκεκριμένη αρχιτεκτονική ώστε ολόκληρη η πλατφόρμα μαζί με τα δεδομένα κ τα alerts βρίσκονται στις εγκαταστάσεις μας και η ανάλυση τους γίνεται on premise από το SOC.



Η σε βάθος αξιοποίηση των πληροφοριών ασφάλειας της πλατφόρμας μας δίνει την δυνατότητα πλήρους ανάλυσης τόσο πριν όσο κατά τη διάρκεια αλλά και μετά από ένα σημαντικό συμβάν. Άλλες παρωχημένες πλατφόρμες διαχείρισης απειλών συλλέγουν στοιχεία κατά τη διάρκεια της επίθεσης και δεν έχουν πολλές δυνατότητες για την προληπτική δράση και την δημιουργία νέων profiles (play books). Επίσης έχουν περιορισμένες δυνατότητες forensics. Αυτό σημαίνει καλύτερη πρόληψη, εύρεση και διερεύνηση των συμβάντων ασφάλειας.

5. Incident Response Management

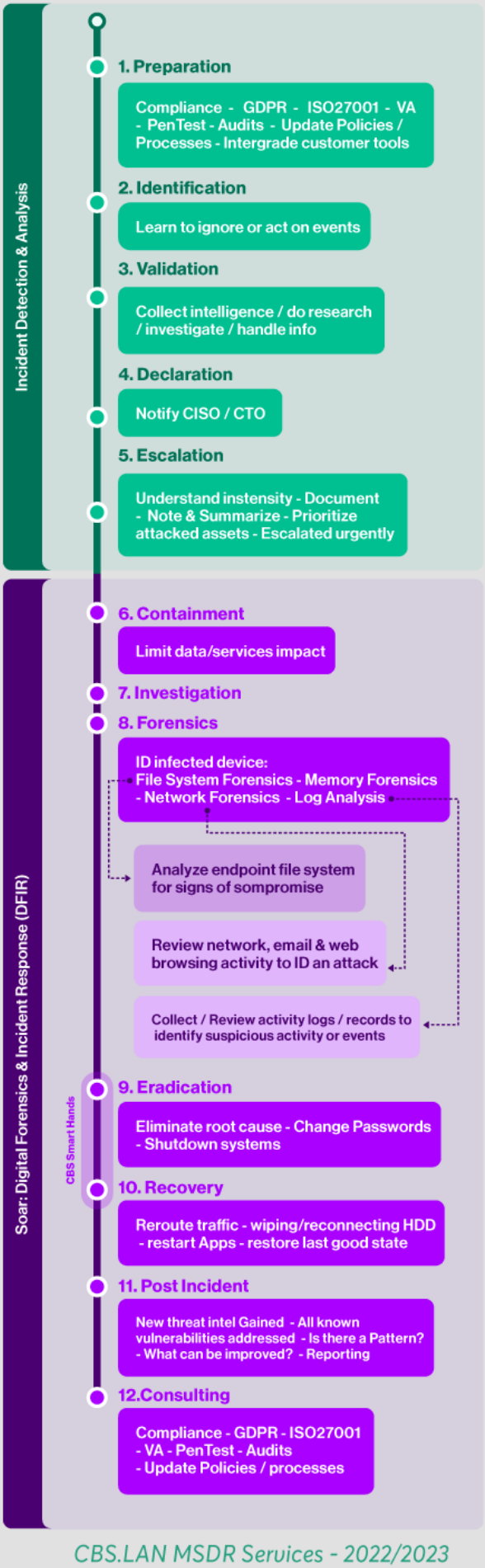
Η αντιμετώπιση των Security Incidents επιβάλλει άμεσα διαθέσιμη εξειδικευμένη ομάδα μηχανικών (SIRT) είτε εξ αποστάσεως είτε με επιτόπια επέμβαση για να αντιμετωπιστεί οποιοδήποτε κρίσιμο περιστατικό και να επανέλθει το δίκτυο σε κανονική λειτουργία άμεσα.
Η CBS LAN σε συνεργασία με το IT team του πελάτη θα εφαρμόσει διαδικασία διαχείρισης συμβάντος με βάση τις βέλτιστες πρακτικές.
Τα βήματα δράσης θα εφαρμόζονται σε πιθανά ή επιβεβαιωμένα περιστατικά καλύπτοντας συνοπτικά:

1. **Ταυτοποίηση Συμβάντος**
2. **Δράσεις για περιορισμό των Επιπτώσεων**
3. **Αφαίρεση των αιτιών που οδήγησαν στο συμβάν**
4. **Επανάκαμψη των IT συστημάτων**
5. **Καταγραφή περιστατικού με σχετική τεκμηρίωση**

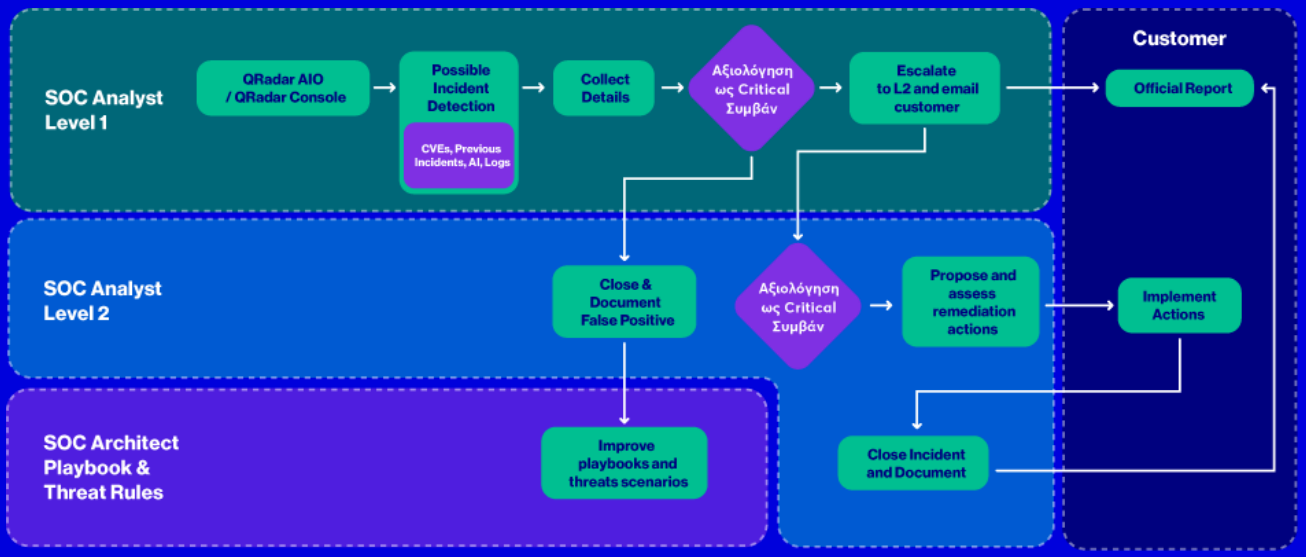
Η παραπάνω συνοπτική λίστα απεικονίζεται λεπτομερέστερα στο action workflow που βρίσκεται στα δεξιά της σελίδας.

Η αλληλουχία δράσεων για την on premise διαχείριση περιστατικών αρχίζει με την ανάλυση των χαρακτηριστικών τους και συνεχίζεται με την χρήση κατάλληλων εργαλείων για την καταγραφή της κακόβουλης δραστηριότητας. Αφού επιβεβαιωθεί η αιτία του περιστατικού γίνεται ανάλυση και εκτίμηση της έκτασης του και των πιθανών επιπτώσεων.

Μετά τη λήξη των σχετικών δράσεων δημιουργείται λεπτομερής ανάλυση με όλα τα ευρήματα και τις ενέργειες για την αντιμετώπιση του συμβάντος. Στην σχετική αναφορά θα υπάρχουν κ προτάσεις για την αφαίρεση των λόγων που οδήγησαν στο συμβάν.



Ακολουθεί συνοπτική απεικόνιση της διαχείρισης συμβάντος:



Οι SOC Analysts (Level 1) παρακολουθούν σε 24ωρη βάση την SOC πλατφόρμα για εντοπισμό συμβάντων κ επιθέσεων σε πραγματικό χρόνο. Όταν εμφανιστεί νέο περιστατικό ξεκινά η διαδικασία διαχείρισης. Ο SOC Analyst ενημερώνεται από όλες τις διαθέσιμες πηγές για τα τεχνικά στοιχεία της απειλής και το επιβεβαιώνει με τη σχετική διερεύνηση συνδυάζοντας όλες τις πηγές.

Αν ο SOC Analyst είναι σίγουρος για την πιθανή απειλή ακολουθεί τα επόμενα βήματα ή διαφορετικά προωθεί το περιστατικό στους Level 2 και παράλληλα ενημερώνει τον πελάτη μέσω email ή τηλεφωνικά. Για χαμηλότερης σπουδαιότητας συμβάντα προχωρά στην διαδικασία ανάλυσης και της σχετικής τεκμηρίωσης. Η τελική μελέτη αξιολογείται και κλείνει το περιστατικό.

Αν πρόκειται για “False Positive” τότε καταγράφονται οι λεπτομέρειες και το συμβάν κλείνει. Ακολούθως ανατίθεται εργασία στους SOC Engineers για προσαρμογή των Playbooks ώστε να αποφευχθούν παρόμοια “False Positives”.

Αν κριθεί απαραίτητο ο L2 SOC Analyst παρέχει εξ’ αποστάσεως δράσεις (μέσω IPSec VPN) για την αντιμετώπιση του συμβάντος, σε κάποιο από τα ειδικά τερματικά που θα στηθούν στην υποδομή του πελάτη για τον σκοπό αυτό και με την επιτυχή αντιμετώπιση του περιστατικού ενημερώνεται το SOC. Αν απαιτηθεί μεταβαίνει στην υποδομή του πελάτη για επιτόπια δράση. Διαφορετικά ο πελάτης δρα μόνος του και στο τέλος ενημερώνει το SOC.

6. Customer Reporting

Θα δημιουργείται αναφορά και θα αποστέλλεται στον πελάτη, είτε ημερήσια (θα απευθύνονται στον IT engineer) είτε εβδομαδιαία (θα απευθύνονται στον IT Director). ΑΝ απαιτηθεί θα δίνονται και μηνιαίες αναφορές (θα απευθύνονται σε διευθυντικά στελέχη που θα υποδείξει ο πελάτης).

info@cbslan.com +30 211 444 1000

www.cbslan.com