ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΕΛΛΗΝΙΚΗ ΣΤΑΤΙΣΤΙΚΗ ΑΡΧΗ

ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΔΙΟΙΚΗΣΗΣ & ΟΡΓΑΝΩΣΗΣ
ΔΙΕΥΘΥΝΣΗ ΟΙΚΟΝΟΜΙΚΩΝ ΥΠΗΡΕΣΙΩΝ
ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ & ΔΙΑΧΕΙΡΙΣΗΣ ΥΛΙΚΟΥ

Ταχ. Δ/νση: Πειραιώς 46 & Επονιτών
Ταχ. Κώδικας: 185 10 Πειραιάς
Πληροφορίες: Ε. Καραγιάννη
Τηλέφωνο: 213 135 3154
E-mail: el.karagianni@statistics.gr

ΑΔΑ:
ΑΔΑΜ: 23AWRD012721685

Πειραιάς, 17 Μαΐου 2023

Αριθ. πρωτ.: 3629/Α2-2178

ΘΕΜΑ: Έγκριση των αριθμ. 3/20.04.2023 και 4/11.05.2023 Πρακτικών και Κατακύρωση του υπ. αριθμ. 1217/Α2-761/10.02.2023 Ηλεκτρονικού Δημόσιου Ανοικτού Διαγωνισμού για την : « Α) Ετήσια παροχή υπηρεσιών ασφαλείας των πληροφοριακών συστημάτων της ΕΛΣΤΑΤ, Β) Ετήσια υπηρεσία AI-Adaptive Web Protection, Γ) Υπηρεσία Managed Detection and Response με προμήθεια τριάντα (30) αδειών, Δ) Υπηρεσία Managed Detection and Response για τους servers virtual-physical με προμήθεια τριανταπέντε (35) αδειών και Ε) Αναβάθμιση του συστήματος ODI (Oracle Data Integrator) και του λογισμικού εφαρμογών (BI, ETL, data warehouse) της ΕΛΣΤΑΤ», με αριθμό συστήματος ΕΣΗΔΗΣ 178918.

Α Π Ο Φ Α Σ Η

Έχοντας υπόψη:

1. Τις διατάξεις όπως αυτές ισχύουν:

α. του **Ν.3832/2010** (ΦΕΚ Α΄38) «Ελληνικό Στατιστικό Σύστημα (ΕΛ.Σ.Σ.), Σύσταση Ελληνικής Στατιστικής Αρχής (ΕΛ.ΣΤΑΤ.) ως Ανεξάρτητης Αρχής», όπως έχει τροποποιηθεί και ισχύει,

β. του **Π.Δ.73/2019** (ΦΕΚ Α΄114/4.7.2019), «Οργανισμός της Ελληνικής Στατιστικής Αρχής (ΕΛ.ΣΤΑΤ.)»,

γ. της υπ΄ αριθ. **ΓΠ-400/27-8-2012** (ΦΕΚ Β΄2390) απόφασης, με θέμα : «Έγκριση Κανονισμού Λειτουργίας και Διαχείρισης της ΕΛΣΤΑΤ,

δ. της υπ΄ αριθ. **22957 ΕΞ 2021/25.02.2021** απόφασης του Υπουργού Οικονομικών με θέμα: «Ανανέωση της θητείας του Προέδρου της Ελληνικής Στατιστικής Αρχής (ΕΛ.ΣΤΑΤ.)», ΦΕΚ Υ.Ο.Δ.Δ. 140/25.02.2021 και ΦΕΚ Υ.Ο.Δ.Δ. 149/26.02.2021**,**

ε. του **Ν.4412/2016** «Δημόσιες συμβάσεις έργων, προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)», όπως έχει τροποποιηθεί και ισχύει και ιδίως με τις διατάξεις του **ν.4782/2021** (ΦΕΚ Α΄36),

στ. του **Ν.4270/2014** (ΦΕΚ Α΄ 143) «Αρχές δημοσιονομικής διαχείρισης και εποπτείας (ενσωμάτωση της οδηγίας 2011/85/ΕΕ)-δημόσιο λογιστικό ή άλλες διατάξεις»,

ζ. του **ΝΔ. 496/1974** (ΦΕΚ Α΄ 204) «Περί Λογιστικού των Νομικών Προσώπων Δημοσίου Δικαίου»,

η. του **ν. 4622/19 (Α' 133)** «Επιτελικό Κράτος: οργάνωση, λειτουργία & διαφάνεια της Κυβέρνησης, των κυβερνητικών οργάνων & της κεντρικής δημόσιας διοίκησης» και ιδίως του άρθρου 37

θ. του ν. **4700/2020 (Α' 127)** «Ενιαίο κείμενο Δικονομίας για το Ελεγκτικό Συνέδριο, ολοκληρωμένο νομοθετικό πλαίσιο για τον προσυμβατικό έλεγχο, τροποποιήσεις στον Κώδικα

Νόμων για το Ελεγκτικό Συνέδριο, διατάξεις για την αποτελεσματική απονομή της δικαιοσύνης και άλλες διατάξεις» και ιδίως των άρθρων 324-337

ι. του **ν. 4601/2019 (Α' 44)** «*Εταιρικοί μετασχηματισμοί και εναρμόνιση του νομοθετικού πλαισίου με τις διατάξεις της Οδηγίας 2014/55/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Απριλίου 2014 για την έκδοση ηλεκτρονικών τιμολογίων στο πλαίσιο δημόσιων συμβάσεων και λοιπές διατάξεις*»

ια. του **Ν.4250/2014** (ΦΕΚ Α΄ 74/26.3.14) «Διοικητικές απλουστεύσεις-Καταργήσεις, Συγχωνεύσεις Νομικών προσώπων και Υπηρεσιών του Δημοσίου Τομέα-Τροποποίηση διατάξεων του π.δ. 318/1992 (Α' 161) και λοιπές ρυθμίσεις» και ειδικότερα τις διατάξεις του άρθρου 1.

ιβ. του **Ν.2859/2000** «Κύρωση Κώδικα Φόρου Προστιθέμενης Αξίας» (ΦΕΚ Α΄ 248), όπως έχει τροποποιηθεί και ισχύει,

ιγ. του άρθρου 64 **του Ν. 4172/2013** (ΦΕΚ Α΄ 167) «Φορολογία Εισοδήματος, επείγοντα μέτρα εφαρμογής του Ν.4046/2012, του Ν.4093/2012 και του Ν.4127/2013 και άλλες διατάξεις» περί παρακράτησης φόρου εισοδήματος, όπως έχει τροποποιηθεί και ισχύει.

ιδ. του **Ν.4738/2020** «Ρύθμιση οφειλών και παροχή δεύτερης ευκαιρίας και άλλες διατάξεις» (ΦΕΚ Α΄ 207),

ιε. του **Ν.4013/2011** (ΦΕΚ Α΄204) «Σύσταση Ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων και Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων …», όπως έχει τροποποιηθεί και ισχύει .

ιστ. του **Ν. 4912/22 (ΦΕΚ 59/17.03.2022 Α')** «Ενιαία Αρχή Δημοσίων Συμβάσεων και άλλες διατάξεις του Υπουργείου Δικαιοσύνης» και ειδικότερα του άρθρου 7 «Οικονομική αυτοτέλεια – Αντικατάσταση άρθρου 350 ν. 4412/2016» .

ιζ. του **Ν.3861/2010** (ΦΕΚ Α' 112) «Ενίσχυση της διαφάνειας με την υποχρεωτική ανάρτηση νόμων και πράξεων των κυβερνητικών, διοικητικών και αυτοδιοικητικών οργάνων στο διαδίκτυο «Πρόγραμμα Διαύγεια» και άλλες διατάξεις», όπως τροποποιήθηκε με το Ν. 4210/2013 (ΦΕΚ 254/Α΄).

ιη. Της παρ. Ζ του **Ν.4152/2013** (Α΄107) «Προσαρμογή της ελληνικής νομοθεσίας στην Οδηγία 2011/7 της 16.2.2011 για την καταπολέμηση των καθυστερήσεων πληρωμών στις εμπορικές συναλλαγές».

ιθ. Του **Ν.2690/1999** (ΦΕΚ 45/Α/9.3.1999) «Κύρωση του κώδικα διοικητικής διαδικασίας και άλλες διατάξεις» και ιδίως των άρθρων 1,2, 7, 11 και 13 έως 15,

κ. του **Ν.4155/2013** (ΦΕΚ 120/Α/29.5.2013) «Εθνικό Σύστημα Ηλεκτρονικών Δημοσίων Συμβάσεων και άλλες διατάξεις» όπως έχει τροποποιηθεί και ισχύει και ιδιαιτέρως των άρθρων 10,11 και 12.

κα. Του **Π.Δ. 80/2016** (Α΄145) «Ανάληψη υποχρεώσεων από τους Διατάκτες».

κβ.Του **Π.Δ. 28/2015** (Α΄34) «Κωδικοποίηση διατάξεων για την πρόσβαση σε δημόσια έγγραφα και στοιχεία».

κγ.Του **Π.Δ. 39/2017** (Α΄64) «Κανονισμός εξέτασης Προδικαστικών Προσφυγών ενώπιον της Αρχής Εξέτασης Προδικαστικών Προσφυγών».

κδ. **του ν. 4727/2020 (Α' 184)** «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972 και άλλες διατάξεις»,

κε. του **ν.3419/2005 (Α' 297)** «Γενικό Εμπορικό Μητρώο (Γ.Ε.ΜΗ.) και εκσυγχρονισμός της Επιμελητηριακής Νομοθεσίας»

κστ. του Γενικού Κανονισμού Προστασίας Δεδομένων, (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (GDPR)),

κζ.Του **Ν.4624/2019** (ΦΕΚ Α΄137/29.08.2019) «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία

της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις»,

κη.της με αρ. **57654 (Β' 1781/23.5.2017)** Απόφασης του Υπουργού Οικονομίας και Ανάπτυξης «*Ρύθμιση ειδικότερων θεμάτων λειτουργίας και διαχείρισης του Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ) του Υπουργείου Οικονομίας και Ανάπτυξης*»

κθ.της με αρ. **64233(Β'2453/09.06.2021)** Κοινής Απόφασης των Υπουργών Ανάπτυξης και Επενδύσεων και Ψηφιακής Διακυβέρνησης «Ρυθμίσεις τεχνικών ζητημάτων που αφορούν την ανάθεση και εκτέλεση των Δημοσίων Συμβάσεων Προμηθειών και Υπηρεσιών με χρήση των επιμέρους εργαλείων και διαδικασιών του Εθνικού Συστήματος Ηλεκτρονικών Δημοσίων Συμβάσεων (ΕΣΗΔΗΣ)».,

λ. της υπ΄ αριθμ. Κ.Υ.Α. οικ. 60967 ΕΞ 2020 (Β' 2425/18.06.2020) «Ηλεκτρονική Τιμολόγηση στο πλαίσιο των Δημόσιων Συμβάσεων δυνάμει του ν. 4601/2019» (Α΄44)

λα. της υπ΄ αριθμ. 63446/2021 Κ.Υ.Α. (Β' 2338/02.06.2020) «Καθορισμός Εθνικού Μορφότυπου ηλεκτρονικού τιμολογίου στο πλαίσιο των Δημοσίων Συμβάσεων».

λβ. Των σε εκτέλεση των ανωτέρω νόμων εκδοθεισών κανονιστικών πράξεων, των λοιπών διατάξεων που αναφέρονται ρητά ή απορρέουν από τα οριζόμενα στα συμβατικά τεύχη της παρούσας, καθώς και του συνόλου των διατάξεων του ασφαλιστικού, εργατικού, κοινωνικού, περιβαλλοντικού και φορολογικού δικαίου που διέπει την ανάθεση και εκτέλεση της παρούσας σύμβασης, έστω και αν δεν αναφέρονται ρητά παραπάνω.

2. Την υπ. αρ. **2024709/601/0026/8.4.1998** απόφαση του Υπουργού Οικονομικών με θέμα «Περί καθορισμού των δικαιολογητικών των δαπανών του Δημοσίου για προμήθειες και εργασίες».

3. Την υπ' αριθμ. **162/Α1-129/10.01.2023 (ΑΔΑ: ΨΕΖΝ6ΣΙ-Η5Θ)** απόφαση με θέμα: **«Ορισμός μελών Επιτροπών έτους 2023 και αντικατάσταση μελών ενεργών επιτροπών, λόγω συνταξιοδότησης τους»** του Τμήματος Διοικητικής Υποστήριξης, όπως τροποποιήθηκε με την υπ' αριθμ. **2002/Α1-1600/15.03.2023 (ΑΔΑ: 671Ζ6ΣΙ-Η0Σ)** απόφαση.

4. Το με αριθμ. πρωτ. **Α4-671/22.09.2022 (ΑΔΑΜ: 22REQ011288432**) Πρωτογενές αίτημα της Δ/νσης Πληροφορικής για την αναγκαιότητα της δαπάνης.

5. Το με αριθμ. πρωτ. **Α4-34/03.02.2023 (ΑΔΑΜ: 23REQ012075185)** Πρωτογενές αίτημα της Δ/νσης Πληροφορικής για την αναγκαιότητα της δαπάνης.

6. Την υπ΄ αριθμ. **236/Α2-130/12.01.2023 (ΑΔΑΜ: 23REQ012002806)** απόφαση δέσμευσης πίστωσης σε βάρος του **ΚΑΕ 0439** του προϋπολογισμού εξόδων της ΕΛΣΤΑΤ οικον. έτους 2023 η οποία αντικατέστησε την αριθμ. **6983/Α2-5265/27.09.2022 (ΑΔΑΜ: 22REQ011316572)** προέγκριση δέσμευσης πίστωσης σε βάρος του **ΚΑΕ 0439** του προϋπολογισμού εξόδων της ΕΛΣΤΑΤ οικον. έτους 2023.

7. Την υπ΄ αριθμ. **1085/Α2-721/08.02.2023 (ΑΔΑΜ: 23REQ01202332)** απόφαση δέσμευσης πίστωσης σε βάρος του **ΚΑΕ 0439** του προϋπολογισμού εξόδων της ΕΛΣΤΑΤ οικον. έτους 2023.

8. Την υπ΄ αριθμ. **1217/Α2-761/10.02.2023 (ΑΔΑΜ: 23PROC012122019)** Διακήρυξη Ηλεκτρονικού Δημόσιου Ανοικτού Διαγωνισμού για την : « Α) Ετήσια παροχή υπηρεσιών ασφαλείας των πληροφοριακών συστημάτων της ΕΛΣΤΑΤ, Β) Ετήσια υπηρεσία AI-Adaptive Web Protection, Γ) Υπηρεσία Managed Detection and Response με προμήθεια τριάντα (30) αδειών, Δ) Υπηρεσία Managed Detection and Response για τους servers virtual-physical με προμήθεια τριανταπέντε (35) αδειών και Ε) Αναβάθμιση του συστήματος ODI (Oracle Data Integrator) και του λογισμικού εφαρμογών (BI, ETL, data warehouse) της ΕΛΣΤΑΤ».

9. Την υπ΄ αριθμ. **2383/Α2-1575/30.03.2023** απόφαση έγκρισης των αριθμ. 1/10.03.2023 και 2/17.03.2023 Πρακτικών του υπ. αριθμ. 1217/Α2-761/10.02.2023 Ηλεκτρονικού Δημόσιου Ανοικτού Διαγωνισμού.

10. Τις ανάγκες της ΕΛΣΤΑΤ.

Α π ο φ α σ ί ζ ο υ μ ε

1.- Αποδεχόμαστε και εγκρίνουμε τα αριθμ. **3/20.04.2023 και 4/11.05.2023** Πρακτικά της Επιτροπής που συγκροτήθηκε με την ανωτέρω υπό στοιχ. 3 απόφαση του Προέδρου της ΕΛΣΤΑΤ και κατακυρώνουμε τα **ΤΜΗΜΑΤΑ (Α) , (Β) και (Γ)** του υπ' αριθ. 1217/Α2-761/10.02.2023 Ηλεκτρονικού Δημόσιου Ανοικτού Διαγωνισμού για την : «Α) Ετήσια παροχή υπηρεσιών ασφαλείας των πληροφοριακών συστημάτων της ΕΛΣΤΑΤ, Β) Ετήσια υπηρεσία AI-Adaptive Web Protection, Γ) Υπηρεσία Managed Detection and Response με προμήθεια τριάντα (30) αδειών, Δ) Υπηρεσία Managed Detection and Response για τους servers virtual-physical με προμήθεια τριανταπέντε (35) αδειών και Ε) Αναβάθμιση του συστήματος ODI (Oracle Data Integrator) και του λογισμικού εφαρμογών (BI, ETL, data warehouse) της ΕΛΣΤΑΤ», όπως αναλυτικά παρατίθενται στον παρακάτω πίνακα, στην εταιρεία **COSMOS BUSINESS SYSTEMS ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΑΝΩΝΥΜΗ ΕΜΠΟΡΙΚΗ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΗ ΕΤΑΙΡΕΙΑ»** με διακριτικό τίτλο «**COSMOS COMPUTERS A.E.B.E.»** (Π. Μπακογιάννη 44, Τ.Κ. 14452 – Μεταμόρφωση, **ΑΦΜ: 094223430**) στο συνολικό ποσό των **ογδόντα τεσσάρων χιλιάδων πεντακοσίων εξήντα οκτώ ευρώ (€ 84.568,00)** συμπεριλαμβανομένου ΦΠΑ (ήτοι καθαρό ποσό € 68.200,00 πλέον ΦΠΑ € 16.368,00) :

Α/Α	ΤΜΗΜΑ ΔΙΑΓΩΝΙΣΜΟΥ	ΚΑΘΑΡΟ ΠΟΣΟ (€)	ΦΠΑ 24% (€)	ΣΥΝΟΛΙΚΗ ΑΞΙΑ (€)
1	**ΤΜΗΜΑ (Α):** Ετήσια παροχή υπηρεσιών ασφαλείας των πληροφοριακών συστημάτων της ΕΛΣΤΑΤ	36.600,00	8.784,00	45.384,00€
2	**ΤΜΗΜΑ (Β):** Ετήσια υπηρεσία AI-Adaptive Web Protection	25.400,00	6.096,00	31.496,00
3	**ΤΜΗΜΑ (Γ):** Υπηρεσία Managed Detection and Response με προμήθεια τριάντα (30) αδειών για ένα (1) έτος (ενδεικτικά τύπου EDRAAS CISCO SECURE ENDPOINT ή ισοδύναμου)	6.200,00	1.488,00	7.688,00
	ΣΥΝΟΛΟ	**68.200,00**	**16.368,00**	**84.568,00**

Στην παρούσα Απόφαση ενσωματώνεται η αριθμ. **2383/Α2-1575/30.03.2023** Απόφαση έγκρισης πρακτικών 1 και 2 περί αξιολόγησης των δικαιολογητικών συμμετοχής, της τεχνικής και οικονομικής προσφοράς.

Οι παρεχόμενες από τον Ανάδοχο υπηρεσίες του έργου θα πρέπει να είναι σύμφωνες με τους όρους, τις απαιτήσεις και τις τεχνικές προδιαγραφές της αριθμ. **1217/Α2-761/10.02.2023** διακήρυξης, όπως παρατίθενται στα **ΠΑΡΑΡΤΗΜΑΤΑ Ι, ΙΙ και ΙΙΙ** της παρούσας, και αποτελούν αναπόσπαστο μέρος αυτής, καθώς και την τεχνική προσφορά του Αναδόχου που είναι δεσμευτική για αυτόν.

2.- Η παραπάνω δαπάνη βαρύνει την πίστωση του κωδικού αριθμού εξόδων **(ΚΑΕ) 0439** του προϋπολογισμού εξόδων της ΕΛΣΤΑΤ, οικον. έτους 2022 και υπόκειται σε κράτηση **(0,1%)** υπέρ της Ενιαίας Αρχής Δημοσίων Συμβάσεων (ΕΑΔΗΣΥ), μετά του αναλογούντος χαρτοσήμου και ΟΓΑ χαρτοσήμου, καθώς και οποιαδήποτε άλλη κράτηση τυχόν θεσμοθετηθεί κατά τη διάρκεια της υπογραφείσας σύμβασης με τον Ανάδοχο.

Με κάθε πληρωμή θα γίνεται η προβλεπόμενη από την κείμενη νομοθεσία παρακράτηση φόρου εισοδήματος αξίας εισοδήματος (%) επί του καθαρού ποσού βάσει του άρθρου 64 του Ν. 4172/2013 (ΦΕΚ Α΄ 167).

3.- Τη σχετική σύμβαση που θα ακολουθήσει της απόφασης αυτής, θα υπογράψουν ο Πρόεδρος της ΕΛΣΤΑΤ που με την ιδιότητά του αυτή την εκπροσωπεί και ο νόμιμος εκπρόσωπος της αναδόχου εταιρείας «**COSMOS COMPUTERS A.E.B.E.».**

4.- Για την υπογραφή της σύμβασης, η ανάδοχος εταιρεία υποχρεούται να προσκομίσει **εγγυητική επιστολή καλής εκτέλεσης** (εγγύηση για την τήρηση των όρων της σύμβασης), εκδοθείσα σύμφωνα με όσα ορίζονται στο **άρθ.72 του Ν.4412/2016**, αναγνωρισμένου πιστωτικού ιδρύματος, **ποσού δύο χιλιάδων επτακοσίων είκοσι οκτώ ευρώ (2.728,00 €)** που αντιστοιχεί στο (4%) της συνολικής προϋπολογισθείσας αξίας προ ΦΠΑ, με χρόνο ισχύος μεγαλύτερο κατά δύο (2) μήνες από το συνολικό συμβατικό χρόνο.

Η εγγυητική επιστολή καλής εκτέλεσης επιστρέφεται με τη λήξη της σύμβασης και μετά την εκπλήρωση όλων των συμβατικών υποχρεώσεων της αναδόχου εταιρείας.

Σε περίπτωση που η ανάδοχος εταιρεία, στην οποία έγινε η κατακύρωση του διαγωνισμού, δεν προσέλθει να υπογράψει τη σύμβαση εντός της προθεσμίας που του ορίστηκε ή αρνηθεί να καταθέσει προ της υπογραφής την εγγυητική επιστολή καλής εκτέλεσης, κηρύσσεται έκπτωτος και η αναθέτουσα αρχή επιβάλλει αθροιστικά ή διαζευκτικά τις προβλεπόμενες από τις κείμενες διατάξεις κυρώσεις.

5.- Οι παραπάνω υπηρεσίες θα παρασχεθούν σύμφωνα με τους όρους και τις επισυναπτόμενες τεχνικές προδιαγραφές της διακήρυξης καθώς και της τεχνικής προσφοράς του Αναδόχου, η οποία είναι δεσμευτική γι' αυτόν, επισυνάπτονται σαν ΠΑΡΑΡΤΗΜΑΤΑ Ι, ΙΙ και ΙΙΙ και αποτελούν αναπόσπαστο μέρος της παρούσας απόφασης.

Χρονική διάρκεια: Η διάρκεια της σύμβασης για τα τμήματα (Α)-(Γ) θα είναι από την υπογραφή της και μέχρι 31/12/2023.

Η παροχή των υπηρεσιών θα ξεκινήσει άμεσα με την υπογραφή της σύμβασης. Η πλήρης ανάπτυξη υπηρεσιών ασφαλείας θα πρέπει να έχει ολοκληρωθεί μέσα στον πρώτο μήνα. Θα πρέπει να διασφαλιστεί η συνεχής και αδιάληπτη παροχή των υπηρεσιών, χωρίς διακοπή κατά την περίοδο μετάβασης. Ο Ανάδοχος θα πρέπει επίσης να μεριμνήσει για την παροχή και εγκατάσταση όλων των αναβαθμίσεων και νεότερων εκδόσεων των εφαρμογών και λογισμικών που έχουν εκδοθεί στο διάστημα μέχρι την υπογραφή της σύμβασης.

Η εγκατάσταση των agents που προβλέπονται στο μέρος (Γ), θα γίνει άπαξ, εντός δέκα (10) ημερών από την υπογραφή της σύμβασης.

Αν ο Ανάδοχος παρέχει τις υπηρεσίες του πλημμελώς, θα κηρυχθεί έκπτωτος από την σύμβαση και από κάθε δικαίωμα που απορρέει απ' αυτή, ενώ θα επιβληθούν σε βάρος του οι νόμιμες κυρώσεις.

6.- Ο Ανάδοχος αναλαμβάνει ρητά κι ανεπιφύλακτα την υποχρέωση να τηρεί τις δεσμεύσεις που απορρέουν από την κείμενη ενωσιακή και ελληνική νομοθεσία περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τις σχετικές αποφάσεις, οδηγίες και κανονιστικές πράξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ο Ανάδοχος αναλαμβάνει επίσης ρητά κι ανεπιφύλακτα την υποχρέωση να εξασφαλίζει καταβάλλοντας την κατά νόμο επιμέλεια ότι, όποιοι υπάλληλοι\προστηθέντες του ή τρίτα πρόσωπα χρησιμοποιηθούν για την εκτέλεση της παρούσας σύμβασης, θα δεσμεύονται ότι θα τηρούν την ως άνω υποχρέωση που απορρέει από την προαναφερθείσα ενωσιακή κι ελληνική νομοθεσία.

Σε εφαρμογή του Γενικού Κανονισμού για την Προστασία Δεδομένων, (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (ΓΚΠΔ-GDPR)), καθώς και του ν. 4624/2019, ο Ανάδοχος αναλαμβάνει να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα που είναι αναγκαία για τη διασφάλιση του απαραίτητου επιπέδου ασφάλειας έναντι των κινδύνων, για τα δεδομένα προσωπικού χαρακτήρα, στα οποία ενδέχεται να αποκτήσει πρόσβαση

στο πλαίσιο της υλοποίησης της παρούσας, ώστε να πληρούνται οι απαιτήσεις του εν λόγω Κανονισμού.

Ο Ανάδοχος υπόσχεται κι αναλαμβάνει την υποχρέωση να μην ανακοινώνει, διαθέτει ή δημοσιοποιεί με οποιονδήποτε τρόπο σε τρίτους, οι οποίοι δεν σχετίζονται με τους σκοπούς της παρούσας και για τους οποίους δεν υπάρχει τέτοια υποχρέωση από το νόμο ή δικαστική απόφαση, πληροφορίες, που έχει λάβει και επεξεργάζεται, στο πλαίσιο της δραστηριότητάς του, όπως αυτή περιγράφεται κι απορρέει από τη παρούσα σύμβαση. Οι ως άνω παράγραφοι παραμένουν ισχυρές για απεριόριστο χρονικό διάστημα μετά την καθ' οιονδήποτε τρόπο λύση της παρούσας.

Ο Ανάδοχος αναλαμβάνει ρητά κι ανεπιφύλακτα την υποχρέωση όπως αμέσως μετά τη λήξη ή τη λύση της παρούσας σύμβασης, προβεί στη καταστροφή οποιουδήποτε ηλεκτρονικού, ή άλλου τυχόν αρχείου που περιήλθε στη κατοχή του κατά το ως άνω διάστημα και τη διακοπή της πρόσβασης σε αυτά. Ο Ανάδοχος αναλαμβάνει επίσης την υποχρέωση να εξασφαλίσει τη τήρηση των ανωτέρω υποχρεώσεων εκ μέρους των υπαλλήλων του/προστηθέντων του/ή τρίτων προσώπων που θα έχουν χρησιμοποιηθεί κατά την εκτέλεση της παρούσας σύμβασης.

Προς εφαρμογή των ανωτέρω ο Ανάδοχος θα υπογράψει σχετικά και Συμφωνία για την Επεξεργασία των Δεδομένων (Data Processing Agreement), η οποία θα αποτελεί αναπόσπαστο μέρος της σύμβασης που θα υπογραφεί.

Σε εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων, (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (GDPR)), καθώς και του ν. 4624/2019, η ΕΛΣΤΑΤ θα διατηρήσει αποθηκευμένο το σύνολο των προσωπικών δεδομένων που ο Ανάδοχος παραχώρησε σε αυτήν, όπως:

- τα στοιχεία επικοινωνίας του εκπροσώπου του Αναδόχου ή/και του προσωπικού που αυτός θα απασχολήσει στα πλαίσια αυτής της Σύμβασης,
- τα προσωπικά στοιχεία που ο Ανάδοχος έδωσε στην ΕΛΣΤΑΤ στο πλαίσιο της παρούσας Σύμβασης.

Η ΕΛΣΤΑΤ θα χρησιμοποιήσει το σύνολο των παρασχεθέντων στοιχείων κατά τα ανωτέρω μόνο για τους σκοπούς που απορρέουν από την παρούσα σύμβαση και σύμφωνα με τις επιταγές του νόμου. Πρόσβαση στα παρασχεθέντα δεδομένα έχει η ΕΛΣΤΑΤ. Τα δεδομένα ενδέχεται να διαβιβάζονται σε τρίτους, όπως είναι οι εθνικοί φορείς που είναι αρμόδιοι για θέματα που απορρέουν από την ισχύουσα νομοθεσία (Α.Α.Δ.Ε., Γενικό Λογιστήριο του Κράτους, Ε.Φ.Κ.Α., σύστημα Διαύγεια, Υπηρεσία Επιτρόπου του Ελεγκτικού Συνεδρίου, σύστημα taxis κ.α.), αποκλειστικά και μόνο όταν αυτό απαιτείται από το νόμο, τη σύμβαση ή άλλη βάση νόμιμης επεξεργασίας.

Η ΕΛΣΤΑΤ θα λάβει όλα τα προβλεπόμενα από τον άνω Κανονισμό και τη σχετική νομοθεσία μέτρα προστασίας, ώστε να προστατεύσει τα παρασχεθέντα δεδομένα από κάθε ανεξουσιοδότητη ή μη νόμιμη επεξεργασία.

Υπεύθυνος επεξεργασίας είναι ο εκ του νόμου οριζόμενος σε σχέση με τα ΝΠΔΔ και τις Ανεξάρτητες Αρχές. Τα δεδομένα θα τηρηθούν για όσο διάστημα απαιτείται εκ της σύμβασης και της σχετικής νομοθεσίας.

7.- Η πληρωμή του αναδόχου θα πραγματοποιηθεί σε 4 ισόποσες δόσεις για το (Α) και (Β) μέρος, ενώ το (Γ) μέρος θα αποπληρωθεί εφάπαξ με την υπογραφή της σύμβασης.

Απαιτούμενα δικαιολογητικά για την πληρωμή του Αναδόχου είναι:

α) Τιμολόγιο,

β) Αποδεικτικό φορολογικής ενημερότητας

γ) Πρακτικό καλής εκτέλεσης από την αρμόδια Επιτροπή.

δ) Βεβαίωση του ΕΦΚΑ για μη οφειλόμενες εισφορές (ασφαλιστική ενημερότητα)

ε) Εξοφλητική απόδειξη του αναδόχου εάν το τιμολόγιο δεν φέρει την ένδειξη «Εξοφλήθηκε»

στ) κάθε άλλο δικαιολογητικό που τυχόν ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή.

Η πληρωμή του συμβατικού τιμήματος θα γίνεται με την προσκόμιση των νομίμων παραστατικών και δικαιολογητικών που προβλέπονται από τις διατάξεις του άρθρου 200 παρ. 5 του ν. 4412/2016, ήτοι των σχετικών τιμολογίων και των σχετικών πρωτοκόλλων βεβαίωσης παραλαβής και καλής εκτέλεσης από την αρμόδια Επιτροπή Παραλαβής και Καλής Εκτέλεσης καθώς και κάθε άλλου δικαιολογητικού που τυχόν ήθελε ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή, με χρηματικά εντάλματα που θα εκδώσει η αναθέτουσα αρχή και θα εξοφληθούν από την Υπηρεσία Ταμειακής Διαχείρισης της αναθέτουσας αρχής.

8.- Πέραν του συμβατικού τιμήματος, οι ανάδοχες εταιρείες δεν θα έχουν καμία απαίτηση κατά της Αναθέτουσας Αρχής για δαπάνες, τις οποίες θα πραγματοποιήσουν κατά την εκτέλεση των έργων ή εξ αφορμής αυτού.
Η ανάδοχος εταιρεία θα αναλάβει την εκτέλεση της σύμβασης θεωρώντας το συμβατικό τίμημα επαρκές, νόμιμο και εύλογο για την εκτέλεση του αντικειμένου της σύμβασης μετά από συνολική έρευνα που θα έχει πραγματοποιήσει πριν την κατάθεση της προσφοράς του. Στο συμβατικό τίμημα περιλαμβάνονται όλες οι ενδεχόμενες αμοιβές τρίτων, καθώς και οι δαπάνες των αναδόχων για την εκτέλεση του έργου, χωρίς καμία περαιτέρω επιβάρυνση της Αναθέτουσας Αρχής.

9. Τα μέλη της Επιτροπής Παραλαβής έχουν επιλεγεί με τη διαδικασία που προβλέπεται στο άρθρο 26 του ν. 4024/2011 και συγκροτήθηκε με την ανωτέρω υπό στοιχ. 3 απόφαση του Προέδρου της ΕΛΣΤΑΤ και είναι τα παρακάτω :

ΤΑΚΤΙΚΑ ΜΕΛΗ

1. **Δήμας Σπυρίδων,** υπάλληλος με βαθμό Α΄
2. **Παπανικολάου Χρήστος,** υπάλληλος με βαθμό Α΄
3. **Δρακουλόγκωνας Παναγιώτης,** υπάλληλος με βαθμό Α΄

ΑΝΑΠΛΗΡΩΜΑΤΙΚΑ ΜΕΛΗ

1. **Καλυβάς Άγγελος,** υπάλληλος με βαθμό Α΄
2. **Καρκούλιας Αντώνιος,** υπάλληλος με βαθμό Α΄
3. **Μπαρδής Ιωάννης,** υπάλληλος με βαθμό Α΄

Συνημ.:
-Απόφαση έγκρισης πρακτικών 1 και 2
-Πρακτικά 3 και 4 (σελ. 3)

Ο Πρόεδρος
κ.α.α.
Ο Αναπληρωτής Προέδρου
Προϊστάμενος Γενικής Δ/νσης
Διοίκησης & Οργάνωσης

Ιωάννης Μοσχάκης

Ακριβές αντίγραφο
Η Προϊσταμένη του Τμήματος
Διοικητικής Υποστήριξης

Σοφία Μπακαλίδου

Εσωτερική Διανομή:
1.- Αυτοτελές Γραφείο Προέδρου
2.- Γεν. Δ/νση Στατιστικών
3.- Γεν. Δ/νση Διοίκησης & Οργάνωσης
4.- Δ/νση Οικον. Υπηρεσιών
Τμήμα Προμηθειών & Διαχείρισης Υλικού
5.- Δ/νση Πληροφορικής
6.- Μέλη Επιτροπής

Κοινοποίηση:
COSMOS COMPUTERS A.E.B.E.
Π. ΜΠΑΚΟΓΙΑΝΝΗ 44, ΤΚ 144 52, ΑΘΗΝΑ

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Ι – Αναλυτική Περιγραφή Φυσικού και Οικονομικού Αντικειμένου της Σύμβασης

ΜΕΡΟΣ Α - ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΒΑΣΗΣ

1. Γενικά

Το έργο αφορά στη συνέχιση της παροχής υπηρεσιών παρακολούθησης της ασφάλειας των πληροφοριακών συστημάτων και του δικτύου της ΕΛΣΤΑΤ για το έτος 2023, καθώς οι αιτούμενες υπηρεσίες ήδη παρέχονται κατά το έτος 2022.

Πιο συγκεκριμένα, στο πλαίσιο του έργου περιλαμβάνεται (α) η αποτίμηση ευπαθειών, (β) ο 24ωρος έλεγχος και η παρακολούθηση της ασφάλειας των συστημάτων της ΕΛΣΤΑΤ, (γ) ο έγκαιρος εντοπισμός συμβάντων και επιβεβαιωμένων περιστατικών ασφαλείας και (δ) η λήψη έγκαιρων αποφάσεων, από την ανάδοχο εταιρεία, και η υλοποίηση των κατάλληλων ενεργειών πρόληψης και αντιμετώπισης των εν λόγω περιστατικών, με χρήση υπηρεσιών τεχνητής νοημοσύνης και αυτοματισμού.

Λαμβάνοντας υπόψη ότι οι απειλές κυβερνοασφάλειας συνεχώς μεγαλώνουν και εντείνονται, γίνεται αναγκαία η προμήθεια υπηρεσιών παρακολούθησης και διαχείρισης περιστατικών κυβερνοασφαλείας, ειδικά εφόσον η ΕΛΣΤΑΤ δεν διαθέτει εξειδικευμένο προσωπικό ασφαλείας πληροφορικής. Η ανάγκη αυτή προκύπτει και από τη φύση και τον όγκο των δεδομένων τα οποία η ΕΛΣΤΑΤ συλλέγει και επεξεργάζεται, με πλήρη διασφάλισης της προστασίας και της ακεραιότητάς τους.

Επιπλέον, ζητείται η παροχή υπηρεσιών AI[1]-Adaptive Web Protection, ώστε να προστατεύεται ολιστικά ο ιστότοπος της ΕΣΤΑΤ από κυβερνοεπιθέσεις.

Τέλος, ζητείται η προμήθεια τριάντα (30) αδειών εξειδικευμένου λογισμικού για την υποστήριξη υπηρεσιών managed detection and response (ενδεικτικά τύπου EDRAAS CISCO SECURE ENDPOINT ή ισοδύναμου), ώστε να υπάρχει στοχευμένη παρακολούθηση ευπαθειών και επιθέσεων σε προσωπικούς υπολογιστές που περιέχουν κρίσιμες εφαρμογές της ΕΛΣΤΑΤ (κυρίως αυτούς των προγραμματιστών της ΕΛΣΤΑΤ).

Βάσει των παραπάνω, το έργο μπορεί να διακριθεί σε τρία (3) κύρια μέρη:

1) Παροχή υπηρεσιών ασφάλειας Πληροφοριακών Συστημάτων 24/7
2) Παροχή υπηρεσιών AI-Adaptive Web Protection
3) Προμήθεια τριάντα (30) αδειών εξειδικευμένου λογισμικού για την υποστήριξη υπηρεσιών managed detection and response (ενδεικτικά τύπου EDRAAS CISCO SECURE ENDPOINT ή ισοδύναμου)

Λόγω της ιδιομορφίας και της συνάφειας που παρουσιάζουν τα τρία αυτά μέρη, ζητείται η προμήθεια να γίνει από τον ίδιο προμηθευτή.

2. Περιγραφή λειτουργικών και τεχνικών απαιτήσεων

2.1 ΜΕΡΟΣ Α: Παροχή υπηρεσιών ασφάλειας πληροφοριακών συστημάτων 24/7

2.1.1 Στόχος

Στόχος είναι να καταστεί εφικτός ο έγκαιρος εντοπισμός συμβάντων ασφαλείας και δυνητικών κινδύνων, με τρόπο που θα δίνει τη δυνατότητα έγκαιρης προειδοποίησης και απόκρισης έναντι ποικίλων απειλών προς τα πληροφοριακά συστήματα, αξιοποιώντας υπηρεσία SIEM as a Service αλλά και την τεχνογνωσία της Αναδόχου, ώστε να διασφαλιστεί πως οι επιχειρησιακές λειτουργίες της ΕΛΣΤΑΤ είναι ασφαλείς μέσω της προληπτικής παρακολούθησης έναντι των απειλών.

[1] AI: Artificial Intelligence

2.1.2 Τεχνικές απαιτήσεις υπηρεσιών ασφαλείας

Η ΕΛΣΤΑΤ επιθυμεί τη συνέχιση της παροχής υπηρεσιών ασφαλείας και για το έτος 2023. Οι εν λόγω υπηρεσίες περιλαμβάνουν τη συνεχή παρακολούθηση της υποδομής της σε σχέση με το επίπεδο ασφάλειας και την ενημέρωση για πιθανά συμβάντα ασφάλειας που σχετίζονται με αυτήν σε 24ωρη βάση. Για το λόγο αυτό ο Ανάδοχος θα πρέπει να παρέχει υπηρεσία αποτίμησης ευπαθειών και παρακολούθησης και διαχείρισης περιστατικών ασφαλείας μέσω λογισμικού SIEM as a Service. Οποιαδήποτε επεξεργασία δεδομένων, τα οποία αποστέλλονται από εξοπλισμό ή και στελέχη της ΕΛΣΤΑΤ στο πλαίσιο του παρόντος έργου και της λειτουργίας των υπηρεσιών που περιγράφονται σε αυτό πρέπει να λαμβάνει χώρα αποκλειστικά σε ιδιόκτητες μηχανογραφικές υποδομές της αναδόχου, οι οποίες θα βρίσκονται σε χώρους στην Ελλάδα που τελούν υπό τον απόλυτο και αποκλειστικό έλεγχο της αναδόχου.

Η ΕΛΣΤΑΤ θα πρέπει να ενημερώνεται άμεσα για πιθανά περιστατικά ασφάλειας σε 24ωρη βάση μέσω e-mail, sms ή τηλεφωνικής κλήσης ανάλογα με την κρισιμότητά τους. Επιπρόσθετα θα πρέπει να μπορεί να παρακολουθεί τα εν λόγω περιστατικά μέσω Web Portal.

Ο Ανάδοχος οφείλει να εκπαιδεύσει το εντεταλμένο προσωπικό της ΕΛΣΤΑΤ στη χρήση του portal με πρόγραμμα εκπαίδευσης, αναλυτική περιγραφή του οποίου θα υποβάλλει στην προσφορά του. Ειδικότερα για περιστατικά ασφάλειας τα οποία χαρακτηρίζονται σαν ύψιστης κρισιμότητας και μπορεί να επιφέρουν ιδιαίτερα σημαντικές επιπτώσεις στις υποδομές της ΕΛΣΤΑΤ, απαιτείται τηλεφωνική ενημέρωση εντός 15 λεπτών από τη στιγμή εκδήλωσης του περιστατικού. Σε κάθε περίπτωση, κατά την ενημέρωση για ένα περιστατικό ασφάλειας θα πρέπει να περιγράφεται το περιστατικό, να υλοποιούνται άμεσα παρεμβάσεις για την αντιμετώπιση και τον περιορισμό του, καθώς επίσης να παρέχονται συμβουλές για την περαιτέρω αντιμετώπισή του και την αποφυγή επανάληψής του στο μέλλον.

Ο Ανάδοχος, πλην της επιτόπιας επέμβασης και ενημέρωσης για τυχόν περιστατικά ασφαλείας, οφείλει να παραδίδει την κατάλληλη αναφορά σε μηνιαία βάση. Η αναφορά θα περιγράφει τα περιστατικά που έλαβαν χώρα ομαδοποιημένα βάσει τις κρισιμότητάς τους, τα μέτρα που ελήφθησαν για την αντιμετώπισή τους, τις πιθανές επιπτώσεις τους σε βραχυχρόνια και μακροχρόνια βάση, τυχόν προτεινόμενες βελτιστοποιήσεις, και ότι άλλο κρίνει χρήσιμο.

Ο Ανάδοχος οφείλει να περιγράψει και να υποβάλλει στην ΕΛΣΤΑΤ τη μεθοδολογία διαβάθμισης των περιστατικών ασφάλειας και ενημέρωσης της ΕΛΣΤΑΤ ανάλογα με την κρισιμότητά τους. Για παράδειγμα, ένα πιθανό περιστατικό ασφαλείας είναι η αδυναμία δικτυακής πρόσβασης λόγω συγκεκριμένης επίθεσης. Το περιστατικό αυτό μπορεί να διαβαθμιστεί ως προς τη σοβαρότητά του ανάλογα του πιθανού χρόνου απουσίας πρόσβασης και της ιδιαιτερότητας της υποδομής. Στη συνέχεια θα πρέπει να καταγράφονται όλες οι απαραίτητες ενέργειες για την αντιμετώπιση του περιστατικού στοχεύοντας στην αδιάλειπτη λειτουργία των υποδομών, καθώς και των μέτρων που έλαβε ο Ανάδοχος σε πρώτο βαθμό για τον περιορισμό του περιστατικού.

Κατά τη φάση της αποτίμησης των πιθανών ευπαθειών ο Ανάδοχος οφείλει να πραγματοποιήσει μεταξύ άλλων και penetration tests, με στόχο των καθορισμό του αρχικού επιπέδου ασφαλείας των συστημάτων της ΕΛΣΤΑΤ και τον προσδιορισμό τυχόν άμεσων παρεμβάσεων από πλευράς ΕΛΣΤΑΤ. Επιπρόσθετα, ο Ανάδοχος θα πρέπει να εκπονήσει σε συνεργασία με την ΕΛΣΤΑΤ, την διαδικασία απόκρισης σε περιστατικά ασφαλείας και να αναπτύξει σχέδιο Πολιτικής για τη Διαχείριση Συμβάντων Ασφαλείας της ΕΛΣΤΑΤ. Παράλληλα, θα πρέπει να προτείνει μέτρα και δράσεις βελτίωσης του συνολικού επιπέδου ασφαλείας των υποδομών πληροφορικής της ΕΛΣΤΑΤ, τα οποία θα καταγράφονται σε αναλυτική αναφορά που θα παραδοθεί στην ΕΛΣΤΑΤ.

2.2 ΜΕΡΟΣ Β: Παροχή υπηρεσιών AI-Adaptive Web Protection

2.2.1 Στόχος

Μέσα από τις συγκεκριμένες υπηρεσίες ασφάλειας διαδικτύου και εφαρμογών τίθεται ως στόχος η ολιστική προστασία του ιστότοπου της ΕΛΣΤΑΤ από κυβερνοεπιθέσεις και άλλες κακόβουλες ενέργειες. Για την επίτευξη του στόχου αυτού, η ΕΛΣΤΑΤ στρέφεται στην εφαρμογή λύσεων AI-Adaptive Web Protection, οι οποίες αξιοποιούν τεχνικές τεχνητής νοημοσύνης για τον εντοπισμό και την αντιμετώπισης κυβερνοεπιθέσεων που προέρχονται από ανθρώπινη δραστηριότητα (κυρίως hackers). Οι μέθοδοι αυτοί

συλλέγουν δεδομένα, τα οποία αναλύουν ώστε να εντοπίζουν πιθανούς κινδύνους, να εκτιμούν τον βαθμό επικινδυνότητας αυτών και εν τέλει να λαμβάνουν και εφαρμόζουν τα κατάλληλα αποτρεπτικά μέτρα.

2.2.2 Τεχνικές απαιτήσεις

Στις κυβερνοεπιθέσεις, ιδίως αυτές που πραγματοποιούνται από άνθρωπο, οι παράγοντες απειλών χρησιμοποιούν προβλέψιμες μεθόδους για να εισέλθουν σε μια συσκευή, αλλά τελικά βασίζονται στις ανθρώπινες δραστηριότητες μέσω πληκτρολογίου για να εγκατασταθούν και μετακινηθούν μέσα σε ένα δίκτυο. Για να ενισχυθεί η προστασία των εφαρμογών που είναι εκτεθειμένες στο διαδίκτυο έχουν αναπτυχθεί συστήματα machine learning, τα οποία προβλέπουν και εκτιμούν εάν κινδυνεύει η συσκευή / εφαρμογή και εν συνεχεία εκτελούν αυτόματα διαδικασίες αποκλεισμού και προστασίας της συσκευής, εμποδίζοντας τα επόμενα βήματα ενός εισβολέα. Οι αποφάσεις βασίζονται σε δεδομένα που λαμβάνει το σύστημα και έχουν προκύψει από εκτενή έρευνα και πειραματισμό για τη μεγιστοποίηση της αποτελεσματικότητας αποκλεισμού χωρίς να επηρεάζεται η εμπειρία των χρηστών. Δεδομένου ότι η adaptive προστασία βασίζεται σε μεθόδους τεχνητής νοημοσύνης, ο βαθμός (αξιολόγηση) κινδύνου που δίνεται σε μια συσκευή δεν εξαρτάται μόνο από μεμονωμένους δείκτες αλλά από ένα ευρύ φάσμα μοτίβων και χαρακτηριστικών που χρησιμοποιεί το σύστημα για να καθορίσει εάν μια επίθεση είναι επικείμενη ή σε εξέλιξη. Αυτή η δυνατότητα είναι κατάλληλη για την καταπολέμηση π.χ. ransomware επιθέσεων που εκτελούνται από hackers, επειδή ακόμα κι αν οι εισβολείς χρησιμοποιούν ακόμα και γνωστό ή νόμιμο αρχείο ή διαδικασία, το σύστημα μπορεί να βοηθήσει στην αποτροπή εκκίνησης του αρχείου ή της διαδικασίας.

Συνοψίζοντας, η γνωστική υπολογιστική είναι ένας προηγμένος τύπος τεχνητής νοημοσύνης, ο οποίος αξιοποιεί διάφορες μορφές AI, συμπεριλαμβανομένων αλγορίθμων μηχανικής εκμάθησης και δικτύων βαθιάς εκμάθησης, που ενισχύονται και γίνονται πιο έξυπνα με την πάροδο του χρόνου. Κάθε κακόβουλη δραστηριότητα αναλύεται και μοντελοποιείται μέσα από μια μοναδική προσέγγιση που συνδυάζει την μεθοδολογία και τα στάδια μίας επίθεσης στις υποδομές με:

- το πλαίσιο (framework) MITER ATT&CK,[2]
- την συμπεριφορά χρηστών/τελικών σημείων/δικτύου και
- πληροφορίες από security big data,

προσδιορίζοντας τον βαθμό επικινδυνότητας, τα χαρακτηριστικά της επίθεσης, και το σύνολο της κακόβουλης δραστηριότητας.

Σε πραγματικές συνθήκες λειτουργίας, μέσα από την εξέταση δεικτών που διαφορετικά θα θεωρούνταν χαμηλής προτεραιότητας ή κινδύνου, οι λύσεις adaptive protection μπορούν να σταματούν τη διαδικασία σε πρώιμο στάδιο, με αποτέλεσμα ο συνολικός αντίκτυπος της επίθεσης να μειώνεται σημαντικά.

Οι υπηρεσίες web adaptive protection συνήθως αποτελούνται από τα ακόλουθα δομικά στοιχεία:

- WAF as a service
- Υπηρεσία Threat Intelligence
- Real Time Threat Management 24x7

2.2.2.1 WAF as a service

Η υπηρεσία WAF as a Service ζητείται ώστε να ανιχνεύει και εμποδίζει οποιαδήποτε κακόβουλη επίθεση προς τον ιστότοπο (portal) της ΕΛΣΤΑΤ, συμπεριλαμβανομένων των προηγμένων επιθέσεων από bot, web defacement, sql injection, cross site scripting, command injection κ.λπ.

Οι υπηρεσίες αυτές δημιουργούν ένα δυναμικό προφίλ του φορέα και ειδικότερα του ιστότοπου, το οποίο εφόσον ενσωματωθεί στην υπηρεσία εντοπίζει με ακρίβεια τις επιθέσεις και ελαχιστοποιεί τα false positives έτσι ώστε να εξασφαλίσει την, χωρίς πρόβλημα, πρόσβαση των νόμιμων χρηστών ενώ ταυτόχρονα να εμποδίσει την μη εξουσιοδοτημένη κίνηση από τους hackers.

[2] https://attack.mitre.org/

2.2.2.2 Υπηρεσία Threat Intelligence

Η υπηρεσία Threat Intelligence δημιουργήθηκε για να ενισχύσει τις δυνατότητες των μηχανισμών ανίχνευσης απειλών των web sites ώστε να μπορούν οι αναλυτές, να εντοπίσουν πιο αποτελεσματικά γνωστές προηγμένες επιθέσεις. Οι υπηρεσίες Threat Intelligence ή αλλιώς Threat Feeds, όπως είναι ευρέως γνωστές, ενισχύουν την αμυντική γραμμή ενός οργανισμού ως ένα επιπλέον εργαλείο άμεσου εντοπισμού των "known-knowns". Ενσωματώνοντας τα Threat Feeds στην υπηρεσία δημιουργείται μία βασική γραμμή άμυνας για συστήματα με αυξημένη επικινδυνότητα για άμεση εξωτερική επίθεση. Με τον τρόπο αυτό, ενσωματώνονται μια σειρά από Threat Intelligence Feeds ώστε να συμπεριληφθούν και γεωγραφικά περιεχόμενα και ο βαθμός φήμης (reputation score) σε όλα τα επίπεδα λειτουργίας της υπηρεσίας.

2.2.2.3 Real Time Threat Management 24x7

Το τεχνικό προσωπικό του αναδόχου οφείλει να παρακολουθεί σε πραγματικό χρόνο 24x7 όλες τις επιθέσεις προς τον ιστότοπο της ΕΛΣΤΑΤ, με χρήση της κατάλληλης πλατφόρμας και ανάλογα με τον τύπο του περιστατικού θα προβαίνουν στις απαραίτητες ενέργειες αντιμετώπισης του.

Οι ενέργειες αυτές συμπεριλαμβάνουν, μεταξύ άλλων, τις ενέργειες ενημέρωσης, επικύρωσης, προτεραιοποίησης, αντιμετώπισης και διερεύνησης του εκάστοτε ύποπτου ή/και επιβεβαιωμένου περιστατικού ασφαλείας, με χρήση μηχανισμών AI.

Σε περίπτωση που ανιχνευθεί ένα περιστατικό ασφαλείας, οι αναλυτές οφείλουν να ενημερώνουν άμεσα το κατάλληλο προσωπικό της ΕΛΣΤΑΤ, μέσω e-mail, τηλεφώνου, sms σύμφωνα με το SLA και θα προβαίνουν στις ενέργειες αντιμετώπισης του σύμφωνα με το σχέδιο που θα έχει καταρτιστεί και συμφωνηθεί.

2.3 ΜΕΡΟΣ Γ: Προμήθεια τριάντα (30) αδειών εξειδικευμένου λογισμικού για την υποστήριξη υπηρεσιών managed detection and response (ενδεικτικά τύπου EDRAAS CISCO SECURE ENDPOINT ή ισοδύναμου)

Ως EDR (Endpoint Detection and Response), ορίζονται οι λύσεις ασφάλειας και παρακολούθησης ασφαλείας που ελέγχουν τις τελικές συσκευές χρηστών (π.χ. προσωπικούς υπολογιστές) σε συνεχή βάση έναντι απειλών ασφαλείας όπως είναι οι επιθέσεις τύπου ransomware και malware.

Η ΕΛΣΤΑΤ επιθυμεί την χρήση τέτοιου τύπου agents με τη μορφή υπηρεσίας για τριάντα (30) προσωπικούς υπολογιστές υψηλής κρισιμότητας. Πρόκειται για υπολογιστές που χρησιμοποιεί το προσωπικό της Διεύθυνσης Πληροφορικής και κυρίως οι προγραμματιστές και το προσωπικό ασφάλειας υποδομών πληροφορικής.

3. Παραδοτέα

1. Υπηρεσία Ελέγχου Ευπαθειών
2. Υπηρεσία Παρακολούθησης - Διαχείρισης Περιστατικών Ασφάλειας
3. Υπηρεσία Διερεύνησης με χρήση Τεχνητής Νοημοσύνης (AI)
4. Υπηρεσία Ενορχήστρωσης, αυτοματισμού και απόκρισης ασφάλειας (Security Orchestrator, Automation and Response - SOAR)
5. Λογισμικό Διαχείρισης Περιστατικών Ασφαλείας ως Υπηρεσία (Security Information Event Management as a Service)

Τα ανωτέρω παραδοτέα αφορούν τα μέρη (Α) και (Β).

ΠΑΡΑΡΤΗΜΑ ΙΙ – Ειδική Συγγραφή Υποχρεώσεων

ΓΕΝΙΚΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΑΝΑΔΟΧΟΥ

Ο Ανάδοχος πρέπει, επί ποινή κυρώσεων που προβλέπονται στο άρθ. **203 του Ν.4412/2016**, να τηρεί τα παρακάτω:

- Κατά τη διάρκεια εκτέλεσης της σύμβασης, ο ανάδοχος θα πρέπει **να συνεργάζεται στενά με την Αναθέτουσα Αρχή**, υποχρεούται δε να λαμβάνει υπόψη του οποιεσδήποτε παρατηρήσεις της σχετικά με την εκτέλεση των υπηρεσιών που προβλέπονται στη σχετική σύμβαση που θα υπογραφεί.

- Η εκτέλεση του έργου θα γίνει από **προσωπικό του Αναδόχου, κατάλληλα εκπαιδευμένο και έμπειρο**. Ο Ανάδοχος είναι αποκλειστικά **υπεύθυνος για την ποιότητα και απόδοση του, σύμφωνα με τη διακήρυξη** και την παρούσα σύμβαση της εργασίας του προσωπικού του.

- Ο Ανάδοχος **εγγυάται για τη διάθεση του αναφερομένου στην προσφορά του προσωπικού για την υλοποίηση του Έργου**, καθώς επίσης και συνεργατών, που θα διαθέτουν την απαιτούμενη εμπειρία, τεχνογνωσία και ικανότητα, ώστε να ανταποκριθούν πλήρως στις απαιτήσεις της Σύμβασης, υπόσχεται δε και βεβαιώνει ότι θα επιδεικνύουν πνεύμα συνεργασίας κατά τις επαφές τους με τις αρμόδιες Υπηρεσίες και τα στελέχη της Αναθέτουσας Αρχής ή των εκάστοτε υποδεικνυομένων από αυτό προσώπων. Σε αντίθετη περίπτωση, **η Αναθέτουσα Αρχή δύναται να ζητήσει την αντικατάσταση μέλους του προσωπικού του Αναδόχου**, οπότε ο Ανάδοχος οφείλει να προβεί σε αντικατάσταση με άλλο πρόσωπο, ανάλογης εμπειρίας και προσόντων. Αντικατάσταση μέλους του προσωπικού του Αναδόχου, κατόπιν αιτήματός του, κατά τη διάρκεια της εκτέλεσης του Έργου, δύναται να γίνει μετά από έγκριση της Αναθέτουσας Αρχής και μόνο με άλλο πρόσωπο αντιστοίχων προσόντων ή εμπειρίας. Ο Ανάδοχος υποχρεούται να ειδοποιήσει την Αναθέτουσα Αρχή εγγράφως, τουλάχιστον τριάντα (30) ημερολογιακές ημέρες πριν από την αντικατάσταση.

- Ο ανάδοχος οφείλει **να ενεργεί με επιμέλεια και φροντίδα**, ώστε να εμποδίζει πράξεις ή παραλείψεις, που θα μπορούσαν να έχουν αποτέλεσμα αντίθετο με το συμφέρον της Αναθέτουσας Αρχής.

- Ο Ανάδοχος θα είναι **πλήρως και αποκλειστικά υπεύθυνος για την τήρηση της ισχύουσας νομοθεσίας ως προς το απασχολούμενο από αυτόν προσωπικό για την εκτέλεση των υποχρεώσεων της Σύμβασης, συμπεριλαμβανομένης της εργατικής και ασφαλιστικής νομοθεσίας**. Σε περίπτωση δε αλλοδαπών υπαλλήλων, ο Ανάδοχος είναι υπεύθυνος για την ύπαρξη άδειας παραμονής και εργασίας. Σε περίπτωση οποιασδήποτε παράβασης ή ζημίας που προκληθεί στην Αναθέτουσα Αρχή ή σε τρίτους από την μη τήρηση της νομοθεσίας αυτής, υποχρεούται μόνος ο Ανάδοχος προς την αποκατάστασή της.

- Σε περίπτωση κατά την οποία εγερθεί αγωγή κατά της Αναθέτουσας Αρχής από οποιοδήποτε τρίτο που απαιτεί αποζημίωση και που έχει σχέση άμεση ή έμμεση με το αντικείμενο που εκτέλεσε ο Ανάδοχος, αυτός έχει την υποχρέωση να παρέμβει στη δίκη υπέρ της Αναθέτουσας Αρχής, με δικά του έξοδα (δηλ. του Αναδόχου), αναλαμβάνει ρητά και ανεπιφύλακτα την υποχρέωση να καταβάλλει στην Αναθέτουσα Αρχή κάθε ποσό που τυχόν επιδικασθεί ακόμη και με προσωρινή διαταγή ή ως ασφαλιστικό ή συντηρητικό μέτρο υπέρ τρίτων και κατά της Αναθέτουσας Αρχής για κεφάλαιο, τόκους και δικαστική δαπάνη και να αποζημιώσει πλήρως τον τρίτο, απαλλάσσοντας από κάθε ευθύνη την Αναθέτουσα Αρχή.

- Ο Ανάδοχος σε περίπτωση παράβασης οποιουδήποτε όρου της σύμβασης ή της διακήρυξης ή της προσφοράς του, έχει πέραν των προβλεπόμενων νομικών σε βάρος του κυρώσεων και την υποχρέωση να αποζημιώσει την Αναθέτουσα Αρχή για κάθε θετική και αποθετική ζημία που προκάλεσε με αυτήν την παράβαση εξ οιασδήποτε αιτίας και αν προέρχεται.

- Σε περίπτωση που ο ανάδοχος είναι Ένωση/Κοινοπραξία, τα μέλη που αποτελούν την Ένωση/ Κοινοπραξία, θα είναι από κοινού και εις ολόκληρον υπεύθυνα έναντι της Αναθέτουσας Αρχής για την εκπλήρωση όλων των απορρεουσών από τη διακήρυξη και τη σύμβαση υποχρεώσεών τους, του τρόπου πληρωμής και του προσώπου (φυσικού ή νομικού) που προσφέρει τις υπηρεσίες ή ενεργεί γενικότερα για την εκπλήρωση των υποχρεώσεων της Ένωσης. Τυχόν υφιστάμενες μεταξύ τους συμφωνίες περί κατανομής των ευθυνών τους έχουν ισχύ μόνον στις εσωτερικές τους σχέσεις και σε καμία περίπτωση δεν δύνανται να προβληθούν έναντι της Αναθέτουσας Αρχής, ως λόγος απαλλαγής του ενός Μέλους από τις ευθύνες και τις υποχρεώσεις του άλλου ή των άλλων Μελών για την ολοκλήρωση του Έργου. Εάν κατά τη διάρκεια της εκτέλεσης της σύμβασης, οποιαδήποτε από τα μέλη της ένωσης/κοινοπραξίας, εξαιτίας ανικανότητας για οποιοδήποτε λόγο ή λόγω ανωτέρας βίας, δεν μπορεί να ανταποκριθεί στις υποχρεώσεις του, τα υπόλοιπα μέλη συνεχίζουν να έχουν την ευθύνη ολοκλήρωσης της σύμβασης με τους ίδιους όρους και την ίδια τιμή.

- Κατά τη διάρκεια της σύμβασης αλλά και μετά τη λήξη ή λύση αυτής, ο Ανάδοχος θα αναλάβει την υποχρέωση να τηρήσει – τόσο ο ίδιος όσο και ο τυχόν υπεργολάβος του – εμπιστευτικές και να μη γνωστοποιήσει σε οποιοδήποτε τρίτο, οποιαδήποτε έγγραφα ή πληροφορίες που θα περιέλθουν σε γνώση τους κατά την εκτέλεση των υπηρεσιών και την εκπλήρωση των υποχρεώσεων τους.

- Σε περίπτωση λύσης ή πτώχευσης του Αναδόχου ή θέσης της περιουσίας αυτού σε αναγκαστική διαχείριση, τότε η σύμβαση λύεται αυτοδίκαια από την ημέρα επέλευσης των ανωτέρω γεγονότων. Σε τέτοια περίπτωση, καταπίπτει υπέρ της Αναθέτουσας Αρχής η Εγγυητική Επιστολή Καλής Εκτέλεσης, που προβλέπεται στη σύμβαση.

ΓΕΝΙΚΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗΣ

Η Αναθέτουσα Αρχή θα εξασφαλίσει την απαραίτητη συνεργασία όλων των εμπλεκόμενων Διευθύνσεων και Τμημάτων της, ώστε να αποφευχθούν τυχόν προβλήματα στην τήρηση των συμβατικών υποχρεώσεων του Αναδόχου.

Η Αναθέτουσα Αρχή δε φέρει καμία ευθύνη και υποχρέωση από τυχόν ατύχημα στο προσωπικό του Αναδόχου ή τρίτων που οφείλεται σε ανωτέρα βία ή τυχαίο γεγονός ή αμέλειά του κατά την εκτέλεση του Έργου.

Η Αναθέτουσα Αρχή απαλλάσσεται από κάθε ευθύνη και υποχρέωση από τυχόν οποιασδήποτε φύσης και νομικού χαρακτηρισμού ατύχημα ή από κάθε άλλη αιτία, κατά την εκτέλεση της Σύμβασης, του προσωπικού και εργαζόμενων του αναδόχου.

Η Αναθέτουσα Αρχή δεν έχει υποχρέωση καταβολής αποζημίωσης για υπερωριακή απασχόληση ή οποιαδήποτε άλλη αιτία στο προσωπικό του Αναδόχου ή τρίτων.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ – ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ «COSMOS COMPUTERS Α.Ε.Β.Ε.»

COSMOS BUSINESS SYSTEMS AEBE

TURN Key SOLUTIONS

30 YEARS Your IT Business Partner

Τεχνική Προσφορά

Cosmos Business Systems
44 P. Bakogianni Str.,
14452 Metamorfosi Attikis, Athens Greece
Tel. +30 210 6492800, Fax +30 210 6464069
email: cosmos@cbs.gr, www.cbs.gr

Thessaloniki
Thermokoitida, Thermi 1,
9th km Thessaloniki-Thermi, 57001 Thessaloniki
Tel. +30 2310 477670, Fax +30 2310 477672
email: cosmos.thess@cbs.gr

Μεταμόρφωση, 06/03/2023

Προς: ΕΛΛΗΝΙΚΗ ΣΤΑΤΙΣΤΙΚΗ ΑΡΧΗ (ΕΛΣΤΑΤ)
Τηλ.: 2131353143
Πειραιώς 46 & Επονιτών, 18510, Πειραιάς

Θέμα: Προσφορά για τον «Ηλεκτρονικό Δημόσιο Ανοικτό Διαγωνισμό για την: Α) Ετήσια παροχή υπηρεσιών ασφαλείας πληροφοριακών συστημάτων ΕΛΣΤΑΤ, Β) Ετήσια υπηρεσία AI-Adaptive Web Protection, Γ) Υπηρεσία Managed Detection and Response με προμήθεια τριάντα (30) αδειών, Δ) Υπηρεσία Managed Detection and Response για τους servers Virtual – Physical με προμήθεια τριάντα πέντε (35) αδειών και Ε) Αναβάθμιση του Συστήματος ODI και του λογισμικού εφαρμογών BI της ΕΛΣΤΑΤ.»
με Αρ. Πρωτ. Διακήρυξης: 1217/Α2-761 και Α/Α ΕΣΗΔΗΣ 178918

Ημερομηνία κατάθεσης διαγωνισμού: 06/03/2022

Κύριοι,

Η εταιρεία **Cosmos Computers A.E.B.E.** βρίσκεται στην ευχάριστη θέση να σας υποβάλλει πλήρη φάκελο τεχνικής προσφοράς για τα **Τμήματα Α, Β και Γ** της Διακήρυξης, στα πλαίσια της διενέργειας του συνοπτικό διαγωνισμού για την ανωτέρω προμήθεια. Η παρούσα προσφορά έχει συνταχθεί σύμφωνα με τους όρους και τις απαιτήσεις της διακήρυξης, της οποίας λάβαμε γνώση και αποδεχόμαστε πλήρως και ανεπιφύλακτα.

Η προσφορά ισχύει και δεσμεύει την εταιρεία **Cosmos Computers A.E.B.E** για εκατόν ογδόντα (180) ημερολογιακές ημέρες, προσμετρούμενες από την επομένη της διενέργειας του διαγωνισμού.

Η εταιρεία **Cosmos Computers A.E.B.E.** συγκαταλέγεται στις πλέον πρωτοπόρες και τεχνολογικά προηγμένες εταιρείες στον χώρο της πληροφορικής. Έχει αποδεδειγμένα και επανειλημμένα σχεδιάσει, αναλάβει και υλοποιήσει έργα υψηλών απαιτήσεων και προδιαγραφών. Επίσης διαθέτει οικονομική επάρκεια, επιχειρηματική ικανότητα, άριστα τεχνικές υποδομές και εξειδικευμένο προσωπικό.

Η εταιρεία **Cosmos Computers A.E.B.E.** συγκεντρώνει την τεχνογνωσία, εμπειρία, ικανότητα και τεχνολογική πρωτοπορία με σκοπό την επιτυχή υλοποίηση του Έργου.

Παραμένουμε στη διάθεσή σας για οποιαδήποτε πληροφορία ή / και διευκρίνιση.

Με τιμή,
Για την **Cosmos Computers A.E.B.E**

Digitally signed by DIMITRIOS DAFNIS
Date: 2023.03.06 14:56:59 EET

Δημήτρης Δάφνης
Πρόεδρος & Διευθύνων Σύμβουλος

Περιεχόμενα

1 ΠΡΟΣΕΓΓΙΣΗ ΤΗΣ COSMOS COMPUTERS A.E.B.E. ΓΙΑ ΤΟ ΈΡΓΟ

1.1 Εισαγωγή

Η εταιρεία **Cosmos Computers A.E.B.E.** βρίσκεται στην ευχάριστη θέση να σας υποβάλλει προσφορά, για τον «Ηλεκτρονικό Δημόσιο Ανοικτό Διαγωνισμό για την ετήσια ανανέωση έξι (6) λογισμικών της ΕΛΣΤΑΤ, την ετήσια παροχή υπηρεσιών ασφαλείας πληροφοριακών συστημάτων, την παροχή υπηρεσιών υποστήριξης για την ολοκλήρωση της επεξεργασίας των δεδομένων των γενικών απογραφών 2021 και την συντήρηση-υποστήριξη του κεντρικού συστήματος λήψης αντιγράφων ασφαλείας» με Αρ. Πρωτ. Διακήρυξης: 8268/Α2-6157 και Α/Α ΕΣΗΔΗΣ 146090, για την κάλυψη αναγκών της ΕΛΣΤΑΤ. Με την 30ετή παρουσία της στην Ελληνική αγορά της πληροφορικής και τα δεκάδες υλοποιημένα έργα, η **Cosmos Computers A.E.B.E.** είναι σε θέση να καλύψει με τον καλύτερο τρόπο όλο τον κύκλο ζωής των πληροφοριακών συστημάτων.

Σαν πρωτοπόρα εταιρεία στην υλοποίηση και συντήρηση πληροφοριακών συστημάτων που περιλαμβάνουν τόσο εξοπλισμό (hardware), όσο και λογισμικό (software) προσφέρει:

- Αναλυτική προσέγγιση στις ανάγκες και της απαιτήσεις του κάθε πελάτη της.
- Την οικονομική στιβαρότητα που απαιτείται στην ανάληψη της συνολικής ευθύνης και των κινδύνων μεγάλων έργων πληροφορικής.
- Αναλυτικές διαδικασίες στην διαχείριση του έργου.
- Σχέσεις συνεργασίας και παροχής υπηρεσιών με όλους τους σημαντικούς κατασκευαστές υλικού και λογισμικού.
- Αποδεδειγμένη εμπειρία στις εμπορικές αγορές αλλά και στον δημόσιο τομέα.
- Υποστήριξη με συνέπεια και συνέχεια για όσο χρόνο χρειαστεί.
- Την Διάθεση εξειδικευμένου προσωπικού για την λειτουργία και την παραγωγική αξιοποίηση του συστήματος σας.

1.2 Συνοπτική Εταιρική παρουσίαση Cosmos Computers AEBE

Η COSMOS BUSINESS SYSTEMS A.E.B.E. (δ.τ. COSMOS COMPUTERS) είναι μια από τις μεγαλύτερες εταιρίες Υψηλής Τεχνολογίας, στην Ελλάδα και την Κύπρο, ειδικευόμενη στην Πληροφορική και τις Τηλεπικοινωνίες, η οποία στοχεύει να καλύψει τις ανάγκες ιδιωτικών και δημοσίων επιχειρήσεων στους παραπάνω τομείς, παρέχοντας υψηλής ποιότητας ολοκληρωμένες λύσεις με το «κλειδί στο χέρι» -Turn Key Solutions.

Η στρατηγική της εταιρίας είναι καθαρά πελατοκεντρική, προσφέροντας εκείνες τις λύσεις (Εξοπλισμός, Λογισμικό, Υπηρεσίες) στους πελάτες της που μέσω αυτών, θα μεγιστοποιήσουν την ανταγωνιστικότητα και την αποδοτικότητα της επιχείρησης τους.

Στόχος της Cosmos είναι να προσφέρει στους πελάτες της, υψηλού επιπέδου προϊόντα και υπηρεσίες τεχνολογίας, ώστε μέσω αυτών να μεγιστοποιήσουν την ανταγωνιστικότητα και αποδοτικότητα της επιχείρησής τους.

ΙΣΤΟΡΙΚΑ ΣΤΟΙΧΕΙΑ

Η εταιρεία **Cosmos Computers A.E.B.E.** ιδρύθηκε το 1988 και δραστηριοποιήθηκε με επιτυχία στον χώρο των πωλήσεων προϊόντων πληροφορικής.

Μετά την εξαγορά της το 2000 από στελέχη της αγοράς πληροφορικής, με μεγάλη επιχειρηματική εμπειρία η μορφή και η κατεύθυνση της εταιρείας άλλαξαν. Την ίδια περίοδο, τα ίδια κεφάλαια της εταιρείας αυξήθηκαν στα 3,3 εκ. € ενώ το 2007 τα κεφάλαια της εταιρείας αυξήθηκαν στα 4,3 εκ €.

Πρόεδρος της εταιρείας είναι ο κος Δημ. Δάφνης

Η Cosmos ΑΕΒΕ, έχει ως στόχο της επιχειρηματικής δραστηριότητας της εταιρείας την παροχή ολοκληρωμένων μηχανογραφικών λύσεων πληροφορικής, δικτύων, office automation, τηλεπικοινωνιών (turn-key solutions) και υπηρεσιών, απευθυνόμενη στην Ελληνική Αγορά των επιχειρήσεων και των επαγγελματιών – με έμφαση σ' αυτήν των μεσαίων και μεγάλων επιχειρήσεων του Ιδιωτικού και Δημόσιου τομέα, των Τραπεζών και των Τηλεπικοινωνιών.

Η ηλεκτρονική διεύθυνση της εταιρείας είναι www.cbs.gr

ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ

Καθοριστικό ρόλο στην επιτυχημένη πορεία της Cosmos Computers Α.Ε.Β.Ε. διαδραματίζει το ανθρώπινο δυναμικό της, το οποίο στελεχώνει όλα τα επιμέρους τμήματα και ιδιαίτερα της Τεχνικής Διεύθυνσης, τα οποία εκπαιδεύονται διαρκώς ώστε να ανταποκρίνονται με επιτυχία στις ανάγκες των πελατών και τις εξελίξεις της τεχνολογίας.

Αναλυτικότερα η Cosmos απασχολεί σήμερα 170 περίπου άτομα προσωπικό εκ των οποίων 65 απασχολούνται στην τεχνική διεύθυνση.

Για τον σχεδιασμό και την υλοποίηση των προσφερομένων λύσεων η Cosmos απασχολεί τεχνικό προσωπικό με εξειδίκευση σε ένα ευρύ φάσμα τεχνολογιών όπως ο τομέας των επικοινωνιών, ο τομέας του systems software και ο τομέας των ERP συστημάτων και των εξειδικευμένων λύσεων λογισμικού όπως Security, CTI, Unified Messaging, Workflow και Document Management.

Προσφερόμενες Υπηρεσίες

Πιο συγκεκριμένα οι τεχνικές υπηρεσίες καλύπτουν τους παρακάτω τομείς :

- Μελέτες και προτάσεις : Για την βελτιστοποίηση της εγκατάστασης και της λειτουργίας του κάθε δικτύου (LAN, WAN, INTERNET), για την μεταφορά φωνής, δεδομένων ή video (εικόνας), η Cosmos αναλαμβάνει την σύνταξη της οικονομοτεχνικής μελέτης που απαιτείται, ώστε να επιτευχθεί η μέγιστη δυνατή απόδοση της επένδυσης.
- Δίκτυα & Τηλεπικοινωνίες : Ενεργός εξοπλισμός (active components) για τις ανάγκες δικτύων WAN / LAN / INTRANETS, για τη μεταφορά φωνής, εικόνας και δεδομένων. Ασύρματα δίκτυα. Εγκαταστάσεις λύσεων VoiP (Avaya, Cisco). Network management και Security.
- Καλωδιακές και Ηλεκτρολογικές εγκαταστάσεις, Κλιματισμός : μελέτη και εγκατάσταση καλωδιακών συστημάτων για ασθενή και ισχυρά ρεύματα , και εγκαταστάσεις δομημένης καλωδίωσης σε category 5 και 6 ή σε οπτικές ίνες (fiber optics). Ηλεκτρολογικές εγκαταστάσεις όπου απαιτείται, κλιματισμός, ψευδοδάπεδα κλπ.
- Data Centers-Server rooms : Τα server rooms , οι χώροι οι οποίοι χρησιμοποιούνται για την "αποθήκευση " της καρδιάς κάθε δικτύου ή τηλεφωνικού κέντρου, απαιτεί ειδική κατασκευή και μελέτη (π.χ. συνθήκες κλιματισμού, αδιάλειπτης παροχής ρεύματος κλπ), την μελέτη και υλοποίηση της οποίας αναλαμβάνει η Cosmos.
- Τηλεφωνικά κέντρα, VoiP & Office Automation : Τα τηλεφωνικά κέντρα, τα fax's και τα φωτοτυπικά μηχανήματα (MFP), προσαρμοσμένα στις ανάγκες της μεγάλης ή μικρής επιχείρησης και γραφείου, προσφέρονται αλλά και υποστηρίζονται με αντίστοιχες συμβάσεις ή με την διαδικασία της on call κλήσης

του τεχνικού. Εξειδικευμένες λύσεις διαχείρισης εγγράφων (document management), Ροής εργασιών (Workflow), διαχείρισης Fax (Captaris Right Fax), Unified Messaging (Cycos, Cisco, Microsoft, Avaya),

- Help desk και call center: Η Cosmos διαθέτει κατάλληλα οργανωμένο call center το οποίο παρέχει υπηρεσίες τηλεφωνικής υποστήριξης για θέματα hardware ή software. Η υπηρεσία αυτή παρέχεται κατόπιν συμβάσεως και το αντικείμενό της μπορεί να προσαρμοστεί στις ανάγκες του πελάτη.
    - Αποδεδειγμένη εμπειρία στις εμπορικές αγορές αλλά και στον δημόσιο τομέα.
    - Υποστήριξη με συνέπεια και συνέχεια για όσο χρόνο χρειαστεί.
    - Την Διάθεση εξειδικευμένου προσωπικού για την λειτουργία και την παραγωγική αξιοποίηση του συστήματος σας.

Εμπειρία & Τεχνική Επάρκεια

Με την 30ετή παρουσία της στην Ελληνική αγορά της πληροφορικής και τα δεκάδες υλοποιημένα έργα, η COSMOS είναι σε θέση να καλύψει με τον καλύτερο τρόπο όλο τον κύκλο ζωής των πληροφοριακών συστημάτων.

Σαν πρωτοπόρα εταιρεία στην υλοποίηση και συντήρηση πληροφοριακών συστημάτων που περιλαμβάνουν τόσο εξοπλισμό (hardware), όσο και λογισμικό (software) προσφέρει:

- Αναλυτική προσέγγιση στις ανάγκες και της απαιτήσεις του κάθε πελάτη της.
- Την οικονομική στιβαρότητα που απαιτείται στην ανάληψη της συνολικής ευθύνης και των κινδύνων μεγάλων έργων πληροφορικής.
- Αναλυτικές διαδικασίες στην διαχείριση του έργου.
- Σχέσεις συνεργασίας και παροχής υπηρεσιών με όλους τους σημαντικούς κατασκευαστές υλικού και λογισμικού.

Η **Cosmos Computers A.E.B.E.** συνεργάζεται με τους μεγαλύτερους κατασκευαστικούς οίκους παγκοσμίως και επενδύει διαρκώς στην εκπαίδευση και την τεχνογνωσία του προσωπικού της στις τεχνολογίες των οίκων αυτών.

Η COSMOS COMPUTERS A.E.B.E. είναι Πιστοποιημένη από την TUV HELLAS (TUV NORD) A.E. κατά τα πρότυπα **ISO 9001:2015** στην Παροχή Ολοκληρωμένων Λύσεων Πληροφορικής, συμπεριλαμβανόμενης της Σχεδίασης & Ανάπτυξης Λογισμικού, την Διαχείριση Έργων Τηλεπικοινωνιακών Δικτύων και στον Σχεδιασμό, Ανάπτυξη και Συντήρηση Τηλεπικοινωνιακών Δικτύων και **ISO/IEC 27001:2013** στον τομέα της Παροχής Ολοκληρωμένων Λύσεων Πληροφορικής. Επιπρόσθετα διαθέτει από τον ίδιο φορέα τις πιστοποιήσεις **ISO 14001:2015** στο σύστημα περιβαλλοντικής διαχείρισης και **OHSAS 18001:2007** στο σύστημα διαχείρισης υγείας και ασφάλειας στην εργασία, στον τομέα της Παροχής Ολοκληρωμένων Λύσεων Πληροφορικής. Τέλος, είναι πιστοποιημένη από την TUV HELLAS κατά το πρότυπο ISO/IEC 20000-1:2011 για την παροχή Υπηρεσιών Υποστήριξης Συστημάτων Πληροφορικής & Επικοινωνιών σε Εξωτερικούς Πελάτες, σύμφωνα με τον κατάλογο υπηρεσιών.

Συνεργασίες της Cosmos Computers A.E.B.E.

2 ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΒΑΣΗΣ

Η εταιρεία COSMOS Computers A.E.B.E. καταθέτει φάκελο προσφοράς για τα Τμήματα: Α, Β και Γ. Η παροχή των υπηρεσιών θα υλοποιηθεί σε συνεργασία με την εταιρεία «ΑΝΤΑΚΟΜ Α.Ε.» ως υπεργολάβο. Η εταιρεία COSMOS Computers A.E.B.E. θα προβεί στην παροχή όλων των υπηρεσιών καθώς και στην εγκατάσταση όλων των λογισμικών και των αναβαθμίσεων που έχουν γίνει διαθέσιμες μέχρι την έναρξη ισχύος της σύμβασης και θα παρέχει όλες τις νέες αναβαθμίσεις μέχρι τις 31/12/2023.

Συνοπτικά το αντικείμενο των προσφερόμενων αναλύεται στον παρακάτω πίνακα:

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΠΟΣΟΤΗΤΑ
1	Ετήσια παροχή υπηρεσιών ασφαλείας των πληροφοριακών συστημάτων της ΕΛΣΤΑΤ	1
2	Ετήσια υπηρεσία AI-Adaptive Web Protection	1
3	Υπηρεσία Managed Detection and Response με προμήθεια τριάντα (30) αδειών (ενδεικτικά τύπου EDRAAS CISCO SECURE ENDPOINT ή ισοδύναμου)	30

Ακολουθεί μία πιο αναλυτική περιγραφή του έργου και των υπηρεσιών που προσφέρει η COSMOS Computers A.E.B.E. μαζί με την υπεργολάβο εταιρεία ΑΝΤΑΚΟΜ Α.Ε.:

2.1 Γενικά

Το έργο αφορά στη συνέχιση της παροχής υπηρεσιών παρακολούθησης της ασφάλειας των πληροφοριακών συστημάτων και του δικτύου της ΕΛΣΤΑΤ για το έτος 2023, καθώς οι αιτούμενες υπηρεσίες ήδη παρέχονται κατά το έτος 2022.

Πιο συγκεκριμένα, στο πλαίσιο του έργου περιλαμβάνεται (α) η αποτίμηση ευπαθειών, (β) ο 24ωρος έλεγχος και η παρακολούθηση της ασφάλειας των συστημάτων της ΕΛΣΤΑΤ, (γ) ο έγκαιρος εντοπισμός συμβάντων και επιβεβαιωμένων περιστατικών ασφαλείας και (δ) η λήψη έγκαιρων αποφάσεων, από την ανάδοχο εταιρεία, και η υλοποίηση των κατάλληλων ενεργειών πρόληψης και αντιμετώπισης των εν λόγω περιστατικών, με χρήση υπηρεσιών τεχνητής νοημοσύνης και αυτοματισμού.

Λαμβάνοντας υπόψη ότι οι απειλές κυβερνοασφάλειας συνεχώς μεγαλώνουν και εντείνονται, γίνεται αναγκαία η προμήθεια υπηρεσιών παρακολούθησης και διαχείρισης περιστατικών κυβερνοασφαλείας, ειδικά εφόσον η ΕΛΣΤΑΤ δεν διαθέτει εξειδικευμένο προσωπικό ασφαλείας πληροφορικής. Η ανάγκη αυτή προκύπτει και από τη φύση και τον όγκο των δεδομένων τα οποία η ΕΛΣΤΑΤ συλλέγει και επεξεργάζεται, με πλήρη διασφάλισης της προστασίας και της ακεραιότητάς τους.

Επιπλέον, απαιτείται η παροχή υπηρεσιών AI1-Adaptive Web Protection, ώστε να προστατεύεται ολιστικά ο ιστότοπος της ΕΣΤΑΤ από κυβερνοεπιθέσεις.

Τέλος, ζητείται η προμήθεια τριάντα (30) αδειών εξειδικευμένου λογισμικού για την υποστήριξη υπηρεσιών managed detection and response (EDRAAS CISCO SECURE ENDPOINT), ώστε να υπάρχει στοχευμένη παρακολούθηση ευπαθειών και επιθέσεων σε προσωπικούς υπολογιστές που περιέχουν κρίσιμες εφαρμογές της ΕΛΣΤΑΤ (κυρίως αυτούς των προγραμματιστών της ΕΛΣΤΑΤ).

Βάσει των παραπάνω, το έργο μπορεί να διακριθεί σε τρία (3) κύρια μέρη:

1) Παροχή υπηρεσιών ασφάλειας Πληροφοριακών Συστημάτων 24/7
2) Παροχή υπηρεσιών AI-Adaptive Web Protection

3) Προμήθεια τριάντα (30) αδειών εξειδικευμένου λογισμικού για την υποστήριξη υπηρεσιών managed detection and response (ενδεικτικά τύπου EDRAAS CISCO SECURE ENDPOINT ή ισοδύναμου)

Λόγω της ιδιομορφίας και της συνάφειας που παρουσιάζουν τα τρία αυτά μέρη, η προμήθεια πρέπει να γίνει από τον ίδιο προμηθευτή.

2.2 ΜΕΡΟΣ Α: Παροχή υπηρεσιών ασφάλειας πληροφοριακών συστημάτων 24/7

2.2.1 Στόχος

Στόχος είναι να καταστεί εφικτός ο έγκαιρος εντοπισμός συμβάντων ασφαλείας και δυνητικών κινδύνων, με τρόπο που θα δίνει τη δυνατότητα έγκαιρης προειδοποίησης και απόκρισης έναντι ποικίλων απειλών προς τα πληροφοριακά συστήματα, αξιοποιώντας υπηρεσία SIEM as a Service αλλά και την τεχνογνωσία της Αναδόχου, ώστε να διασφαλιστεί πως οι επιχειρησιακές λειτουργίες της ΕΛΣΤΑΤ είναι ασφαλείς μέσω της προληπτικής παρακολούθησης έναντι των απειλών.

2.2.2 Τεχνικές απαιτήσεις υπηρεσιών ασφαλείας

Η ΕΛΣΤΑΤ επιθυμεί τη συνέχιση της παροχής υπηρεσιών ασφαλείας και για το έτος 2023. Οι εν λόγω υπηρεσίες περιλαμβάνουν τη συνεχή παρακολούθηση της υποδομής της σε σχέση με το επίπεδο ασφάλειας και την ενημέρωση για πιθανά συμβάντα ασφάλειας που σχετίζονται με αυτήν σε 24ωρη βάση. Για το λόγο η COSMOS Computers A.E.B.E. θα παρέχει υπηρεσία αποτίμησης ευπαθειών και παρακολούθησης και διαχείρισης περιστατικών ασφαλείας μέσω λογισμικού SIEM as a Service. Οποιαδήποτε επεξεργασία δεδομένων, τα οποία αποστέλλονται από εξοπλισμό ή και στελέχη της ΕΛΣΤΑΤ στο πλαίσιο του παρόντος έργου και της λειτουργίας των υπηρεσιών που περιγράφονται σε αυτό θα λαμβάνει χώρα αποκλειστικά σε ιδιόκτητες μηχανογραφικές υποδομές της αναδόχου, οι οποίες θα βρίσκονται σε χώρους στην Ελλάδα που τελούν υπό τον απόλυτο και αποκλειστικό έλεγχο της αναδόχου.

Η ΕΛΣΤΑΤ θα ενημερώνεται άμεσα για πιθανά περιστατικά ασφάλειας σε 24ωρη βάση μέσω e-mail, sms ή τηλεφωνικής κλήσης ανάλογα με την κρισιμότητά τους. Επιπρόσθετα θα μπορεί να παρακολουθεί τα εν λόγω περιστατικά μέσω Web Portal.

Η COSMOS Computers A.E.B.E. θα εκπαιδεύσει το εντεταλμένο προσωπικό της ΕΛΣΤΑΤ στη χρήση του portal με πρόγραμμα εκπαίδευσης, αναλυτική περιγραφή του οποίου ακολουθεί παρακάτω στο Κεφάλαιο 3. Ειδικότερα για περιστατικά ασφάλειας τα οποία χαρακτηρίζονται σαν ύψιστης κρισιμότητας και μπορεί να επιφέρουν ιδιαίτερα σημαντικές επιπτώσεις στις υποδομές της ΕΛΣΤΑΤ, υπάρχει δέσμευση για τηλεφωνική ενημέρωση εντός 15 λεπτών από τη στιγμή εκδήλωσης του περιστατικού. Σε κάθε περίπτωση, κατά την ενημέρωση για ένα περιστατικό ασφάλειας θα περιγράφεται το περιστατικό, θα υλοποιούνται άμεσα παρεμβάσεις για την αντιμετώπιση και τον περιορισμό του, καθώς επίσης θα παρέχονται συμβουλές για την περαιτέρω αντιμετώπισή του και την αποφυγή επανάληψής του στο μέλλον.

Η COSMOS Computers A.E.B.E., πλην της επιτόπιας επέμβασης και ενημέρωσης για τυχόν περιστατικά ασφαλείας, θα παραδίδει την κατάλληλη αναφορά σε μηνιαία βάση. Η αναφορά θα περιγράφει τα περιστατικά που έλαβαν χώρα ομαδοποιημένα βάσει τις κρισιμότητάς τους, τα μέτρα που ελήφθησαν για την αντιμετώπισή τους, τις πιθανές επιπτώσεις τους σε βραχυχρόνια και μακροχρόνια βάση, τυχόν προτεινόμενες βελτιστοποιήσεις, και ότι άλλο κρίνει χρήσιμο.

Η COSMOS Computers A.E.B.E. θα περιγράψει και θα υποβάλλει στην ΕΛΣΤΑΤ τη μεθοδολογία διαβάθμισης των περιστατικών ασφάλειας και ενημέρωσης της ΕΛΣΤΑΤ ανάλογα με την κρισιμότητά τους. Για παράδειγμα, ένα πιθανό περιστατικό ασφαλείας είναι η αδυναμία δικτυακής πρόσβασης λόγω συγκεκριμένης επίθεσης. Το περιστατικό αυτό μπορεί να διαβαθμιστεί ως προς τη σοβαρότητά του ανάλογα του πιθανού χρόνου απουσίας πρόσβασης και της ιδιαιτερότητας της υποδομής. Στη συνέχεια θα καταγράφονται όλες οι απαραίτητες ενέργειες για την αντιμετώπιση του περιστατικού στοχεύοντας στην αδιάλειπτη λειτουργία των υποδομών, καθώς και των μέτρων που έλαβε η COSMOS Computers A.E.B.E. σε πρώτο βαθμό για τον περιορισμό του περιστατικού.

Κατά τη φάση της αποτίμησης των πιθανών ευπαθειών η COSMOS Computers Α.Ε.Β.Ε. θα πραγματοποιήσει μεταξύ άλλων και penetration tests, με στόχο των καθορισμό του αρχικού επιπέδου ασφαλείας των συστημάτων της ΕΛΣΤΑΤ και τον προσδιορισμό τυχόν άμεσων παρεμβάσεων από πλευράς ΕΛΣΤΑΤ. Επιπρόσθετα, η COSMOS Computers Α.Ε.Β.Ε. θα εκπονήσει σε συνεργασία με την ΕΛΣΤΑΤ, την διαδικασία απόκρισης σε περιστατικά ασφαλείας και θα αναπτύξει σχέδιο Πολιτικής για τη Διαχείριση Συμβάντων Ασφαλείας της ΕΛΣΤΑΤ. Παράλληλα, θα προτείνει μέτρα και δράσεις βελτίωσης του συνολικού επιπέδου ασφαλείας των υποδομών πληροφορικής της ΕΛΣΤΑΤ, τα οποία θα καταγράφονται σε αναλυτική αναφορά που θα παραδοθεί στην ΕΛΣΤΑΤ.

2.3 ΜΕΡΟΣ Β: Παροχή υπηρεσιών AI-Adaptive Web Protection

2.3.1 Στόχος

Μέσα από τις συγκεκριμένες υπηρεσίες ασφάλειας διαδικτύου και εφαρμογών τίθεται ως στόχος η ολιστική προστασία του ιστότοπου της ΕΛΣΤΑΤ από κυβερνοεπιθέσεις και άλλες κακόβουλες ενέργειες. Για την επίτευξη του στόχου αυτού, η ΕΛΣΤΑΤ στρέφεται στην εφαρμογή λύσεων AI-Adaptive Web Protection, οι οποίες αξιοποιούν τεχνικές τεχνητής νοημοσύνης για τον εντοπισμό και την αντιμετώπισης κυβερνοεπιθέσεων που προέρχονται από ανθρώπινη δραστηριότητα (κυρίως hackers). Οι μέθοδοι αυτοί συλλέγουν δεδομένα, τα οποία αναλύουν ώστε να εντοπίζουν πιθανούς κινδύνους, να εκτιμούν τον βαθμό επικινδυνότητας αυτών και εν τέλει να λαμβάνουν και εφαρμόζουν τα κατάλληλα αποτρεπτικά μέτρα.

2.3.2 Τεχνικές απαιτήσεις

Στις κυβερνοεπιθέσεις, ιδίως αυτές που πραγματοποιούνται από άνθρωπο, οι παράγοντες απειλών χρησιμοποιούν προβλέψιμες μεθόδους για να εισέλθουν σε μια συσκευή, αλλά τελικά βασίζονται στις ανθρώπινες δραστηριότητες μέσω πληκτρολογίου για να εγκατασταθούν και να μετακινηθούν μέσα σε ένα δίκτυο. Για να ενισχυθεί η προστασία των εφαρμογών που είναι εκτεθειμένες στο διαδίκτυο έχουν αναπτυχθεί συστήματα machine learning, τα οποία προβλέπουν και εκτιμούν εάν κινδυνεύει η συσκευή / εφαρμογή και εν συνεχεία εκτελούν αυτόματα διαδικασίες αποκλεισμού και προστασίας της συσκευής, εμποδίζοντας τα επόμενα βήματα ενός εισβολέα. Οι αποφάσεις βασίζονται σε δεδομένα που λαμβάνει το σύστημα και έχουν προκύψει από εκτενή έρευνα και πειραματισμό για τη μεγιστοποίηση της αποτελεσματικότητας αποκλεισμού χωρίς να επηρεάζεται η εμπειρία των χρηστών. Δεδομένου ότι η adaptive προστασία βασίζεται σε μεθόδους τεχνητής νοημοσύνης, ο βαθμός (αξιολόγηση) κινδύνου που δίνεται σε μια συσκευή δεν εξαρτάται μόνο από μεμονωμένους δείκτες αλλά από ένα ευρύ φάσμα μοτίβων και χαρακτηριστικών που χρησιμοποιεί το σύστημα για να καθορίσει εάν μια επίθεση είναι επικείμενη ή σε εξέλιξη. Αυτή η δυνατότητα είναι κατάλληλη για την καταπολέμηση π.χ. ransomware επιθέσεων που εκτελούνται από hackers, επειδή ακόμα κι αν οι εισβολείς χρησιμοποιούν ακόμα και γνωστό ή νόμιμο αρχείο ή διαδικασία, το σύστημα μπορεί να βοηθήσει στην αποτροπή εκκίνησης του αρχείου ή της διαδικασίας.

Συνοψίζοντας, η γνωστική υπολογιστική είναι ένας προηγμένος τύπος τεχνητής νοημοσύνης, ο οποίος αξιοποιεί διάφορες μορφές AI, συμπεριλαμβανομένων αλγορίθμων μηχανικής εκμάθησης και δικτύων βαθιάς εκμάθησης, που ενισχύονται και γίνονται πιο έξυπνα με την πάροδο του χρόνου. Κάθε κακόβουλη δραστηριότητα αναλύεται και μοντελοποιείται μέσα από μια μοναδική προσέγγιση που συνδυάζει την μεθοδολογία και τα στάδια μίας επίθεσης στις υποδομές με:

- το πλαίσιο (framework) MITER ATT&CK,2
- την συμπεριφορά χρηστών/τελικών σημείων/δικτύου και
- πληροφορίες από security big data,

προσδιορίζοντας τον βαθμό επικινδυνότητας, τα χαρακτηριστικά της επίθεσης, και το σύνολο της κακόβουλης δραστηριότητας.

Σε πραγματικές συνθήκες λειτουργίας, μέσα από την εξέταση δεικτών που διαφορετικά θα θεωρούνταν χαμηλής προτεραιότητας ή κινδύνου, οι λύσεις adaptive protection μπορούν να σταματούν τη διαδικασία σε πρώιμο στάδιο, με αποτέλεσμα ο συνολικός αντίκτυπος της επίθεσης να μειώνεται σημαντικά.

Οι υπηρεσίες web adaptive protection συνήθως αποτελούνται από τα ακόλουθα δομικά στοιχεία:

- WAF as a service
- Υπηρεσία Threat Intelligence
- Real Time Threat Management 24x7

- 2.3.2.1 WAF as a service

Η υπηρεσία WAF as a Service προσφέρεται ώστε να ανιχνεύει και να εμποδίζει οποιαδήποτε κακόβουλη επίθεση προς τον ιστότοπο (portal) της ΕΛΣΤΑΤ, συμπεριλαμβανομένων των προηγμένων επιθέσεων από bot, web defacement, sql injection, cross site scripting, command injection κ.λπ.

Οι υπηρεσίες αυτές δημιουργούν ένα δυναμικό προφίλ του φορέα και ειδικότερα του ιστότοπου, το οποίο εφόσον ενσωματωθεί στην υπηρεσία εντοπίζει με ακρίβεια τις επιθέσεις και ελαχιστοποιεί τα false positives έτσι ώστε να εξασφαλίσει την, χωρίς πρόβλημα, πρόσβαση των νόμιμων χρηστών ενώ ταυτόχρονα να εμποδίσει την μη εξουσιοδοτημένη κίνηση από τους hackers.

- 2.3.2.2 Υπηρεσία Threat Intelligence

Η υπηρεσία Threat Intelligence δημιουργήθηκε για να ενισχύσει τις δυνατότητες των μηχανισμών ανίχνευσης απειλών των web sites ώστε να μπορούν οι αναλυτές, να εντοπίσουν πιο αποτελεσματικά γνωστές προηγμένες επιθέσεις. Οι υπηρεσίες Threat Intelligence ή αλλιώς Threat Feeds, όπως είναι ευρέως γνωστές, ενισχύουν την αμυντική γραμμή ενός οργανισμού ως ένα επιπλέον εργαλείο άμεσου εντοπισμού των “known-knowns”. Ενσωματώνοντας τα Threat Feeds στην υπηρεσία δημιουργείται μία βασική γραμμή άμυνας για συστήματα με αυξημένη επικινδυνότητα για άμεση εξωτερική επίθεση. Με τον τρόπο αυτό, ενσωματώνονται μια σειρά από Threat Intelligence Feeds ώστε να συμπεριληφθούν και γεωγραφικά περιεχόμενα και ο βαθμός φήμης (reputation score) σε όλα τα επίπεδα λειτουργίας της υπηρεσίας.

- 2.3.2.3 Real Time Threat Management 24x7

Το τεχνικό προσωπικό της COSMOS Computers A.E.B.E. θα παρακολουθεί σε πραγματικό χρόνο 24x7 όλες τις επιθέσεις προς τον ιστότοπο της ΕΛΣΤΑΤ, με χρήση της κατάλληλης πλατφόρμας και ανάλογα με τον τύπο του περιστατικού θα προβαίνει στις απαραίτητες ενέργειες αντιμετώπισης του.
Οι ενέργειες αυτές συμπεριλαμβάνουν, μεταξύ άλλων, τις ενέργειες ενημέρωσης, επικύρωσης, προτεραιοποίησης, αντιμετώπισης και διερεύνησης του εκάστοτε ύποπτου ή/και επιβεβαιωμένου περιστατικού ασφαλείας, με χρήση μηχανισμών AI.
Σε περίπτωση που ανιχνευθεί ένα περιστατικό ασφαλείας, οι αναλυτές θα ενημερώνουν άμεσα το κατάλληλο προσωπικό της ΕΛΣΤΑΤ, μέσω e-mail, τηλεφώνου, sms σύμφωνα με το SLA και θα προβαίνουν στις ενέργειες αντιμετώπισης του σύμφωνα με το σχέδιο που θα έχει καταρτιστεί και συμφωνηθεί.

2.4 ΜΕΡΟΣ Γ: Προμήθεια τριάντα (30) αδειών εξειδικευμένου λογισμικού για την υποστήριξη υπηρεσιών managed detection and response (EDRAAS CISCO SECURE ENDPOINT)

Ως EDR (Endpoint Detection and Response), ορίζονται οι λύσεις ασφάλειας και παρακολούθησης ασφαλείας που ελέγχουν τις τελικές συσκευές χρηστών (π.χ. προσωπικούς υπολογιστές) σε συνεχή βάση έναντι απειλών ασφαλείας όπως είναι οι επιθέσεις τύπου ransomware και malware.
Η ΕΛΣΤΑΤ επιθυμεί την χρήση τέτοιου τύπου agents με τη μορφή υπηρεσίας για τριάντα (30) προσωπικούς υπολογιστές υψηλής κρισιμότητας. Πρόκειται για υπολογιστές που χρησιμοποιεί το προσωπικό της Διεύθυνσης Πληροφορικής και κυρίως οι προγραμματιστές και το προσωπικό ασφάλειας υποδομών πληροφορικής.

2.5 ΠΑΡΑΔΟΤΕΑ

1. Υπηρεσία Ελέγχου Ευπαθειών
2. Υπηρεσία Παρακολούθησης - Διαχείρισης Περιστατικών Ασφάλειας
3. Υπηρεσία Διερεύνησης με χρήση Τεχνητής Νοημοσύνης (AI)
4. Υπηρεσία Ενορχήστρωσης, αυτοματισμού και απόκρισης ασφάλειας (Security Orchestrator,Automation and Response - SOAR)
5. Λογισμικό Διαχείρισης Περιστατικών Ασφαλείας ως Υπηρεσία (Security Information Event Managementas a Service)
6. Τριάντα (30) άδειες εξειδικευμένου λογισμικού για την υποστήριξη υπηρεσιών managed detection and response (EDRAAS CISCO SECURE ENDPOINT)

3 ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΠΡΟΤΕΙΝΟΜΕΝΗΣ ΛΥΣΗΣ

Στο κεφάλαιο αυτό παρουσιάζεται τεχνικά η προσφερόμενη λύση σύμφωνα με τις ανάγκες της ΕΛΣΤΑΤ.

Όλες οι τεχνικές πληροφορίες σε σχέση με τις τεχνικές απαιτήσεις, που πρέπει να παρέχει η ΕΛΣΤΑΤ για την επιτυχή υλοποίηση της προσφερόμενης λύσης θα δοθούν μετά την αποδοχή της προσφοράς και θα αναλυθούν και οριστικοποιηθούν στις σχετικές συναντήσεις.

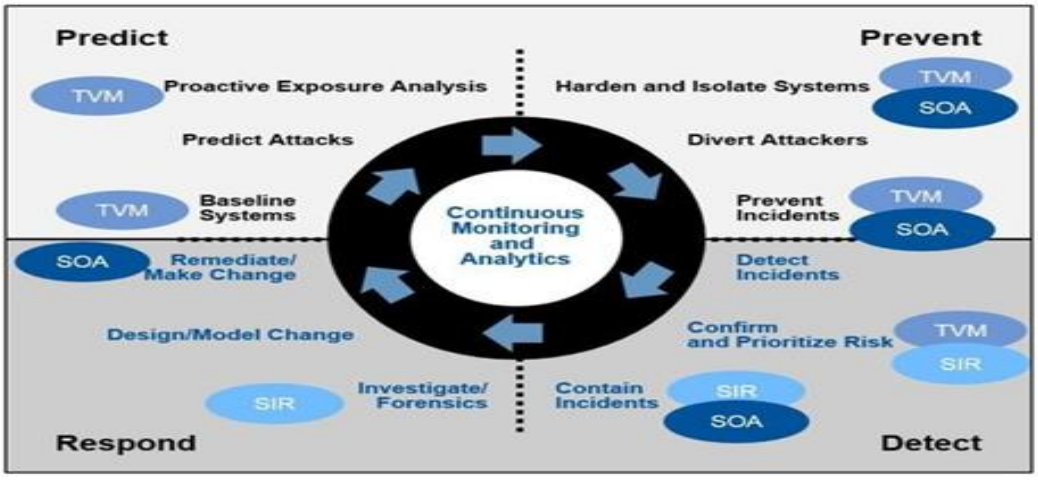
Το έργο αφορά την ετήσια παροχή υπηρεσιών αποτίμησης ευπαθειών, 24ωρου ελέγχου ασφαλείας των συστημάτων της ΕΛΣΤΑΤ, έγκαιρου εντοπισμού επιβεβαιωμένων περιστατικών ασφαλείας και λήψη από την ανάδοχο εταιρεία κατάλληλων ενεργειών πρόληψης και αντιμετώπισης των εν λόγω περιστατικών με χρήση υπηρεσιών τεχνητής νοημοσύνης και αυτοματισμού σύμφωνα με την επισυναπτόμενη τεχνική περιγραφή.

Η παροχή των ανωτέρω υπηρεσιών καθίσταται αναγκαία καθώς η ΕΛΣΤΑΤ δεν διαθέτει εξειδικευμένο προσωπικό ασφαλείας πληροφορικής, ενώ απαιτείται η προστασία των πληροφοριών που συλλέγει και επεξεργάζεται. Δεδομένου ότι οι απειλές κυβερνοασφάλειας συνεχώς μεγαλώνουν γίνεται αναγκαία η προμήθεια υπηρεσιών παρακολούθησης και διαχείρισης περιστατικών κυβερνοασφαλείας.

Στόχος είναι η δυνατότητα έγκαιρης προειδοποίησης και απόκρισης έναντι απειλών προς τα πληροφοριακά συστήματα, αξιοποιώντας υπηρεσία SIEM as a Service αλλά και την τεχνογνωσία της εταιρείας μας ώστε να διασφαλιστεί πως οι επιχειρησιακές λειτουργίες της ΕΛΣΤΑΤ είναι ασφαλείς μέσω της προληπτικής παρακολούθησης έναντι των απειλών.

3.1 Εισαγωγή

Το περιβάλλον των απειλών έχει μεταβληθεί πολύ τα τελευταία πέντε χρόνια, και χαρακτηρίζεται από την αύξηση των επιθέσεων, την πολυπλοκότητα τους και τέλος στις σημαντικές επιπτώσεις που επιφέρουν στους οργανισμούς. Για να αντιμετωπίσουμε τις απειλές αυτές αναπτύξαμε μία στρατηγική η οποία χαρακτηρίζεται από την αρχή ότι τελικά η πληροφοριακή υποδομή ενός οργανισμού έχει τεθεί σε κίνδυνο και βασίζεται σε πιθανά σενάρια επίθεσης. Η στρατηγική αυτή μας οδήγησε στην εξέλιξη των υπηρεσιών που παρέχουμε μέσω του Security Operation Center (SOC), σε Intelligence-Driven Managed Security Services στους τομείς της Πρόβλεψης, της Αποτροπής, της Ανίχνευσης, και της Αντιμετώπισης (Εικόνα 1), με χρήση τεχνολογιών τεχνητής νοημοσύνης (Artificial Intelligence) και μηχανικής εκμάθησης.



Εικόνα 1: Intelligence Driven Managed Security Services

3.2 Παρεχόμενες Υπηρεσίες

3.2.1 Μέρος Α

Η εταιρεία μας θα παρέχει υπηρεσίες παρακολούθησης, ανάλυσης και αξιολόγησης των περιστατικών ασφαλείας σε πραγματικό χρόνο 24x7, συμπεριλαμβανομένων των υπηρεσιών της αντιμετώπισης, της διερεύνησης, της ψηφιακής εγκληματολογίας και της ανάλυσης κακόβουλου λογισμικού. Περιλαμβάνει επίσης ενημέρωση σχετικά με νέες απειλές, έγκαιρων προειδοποιήσεων / αντιμέτρων και συστάσεων. Οι παρεχόμενες υπηρεσίες, στον τομέα της διαχείρισης περιστατικών ασφαλείας διακρίνονται στους ακόλουθους τομείς:

- Πρόβλεψη
- Ανίχνευση
- Απόκριση

3.2.1.1 Πρόβλεψη

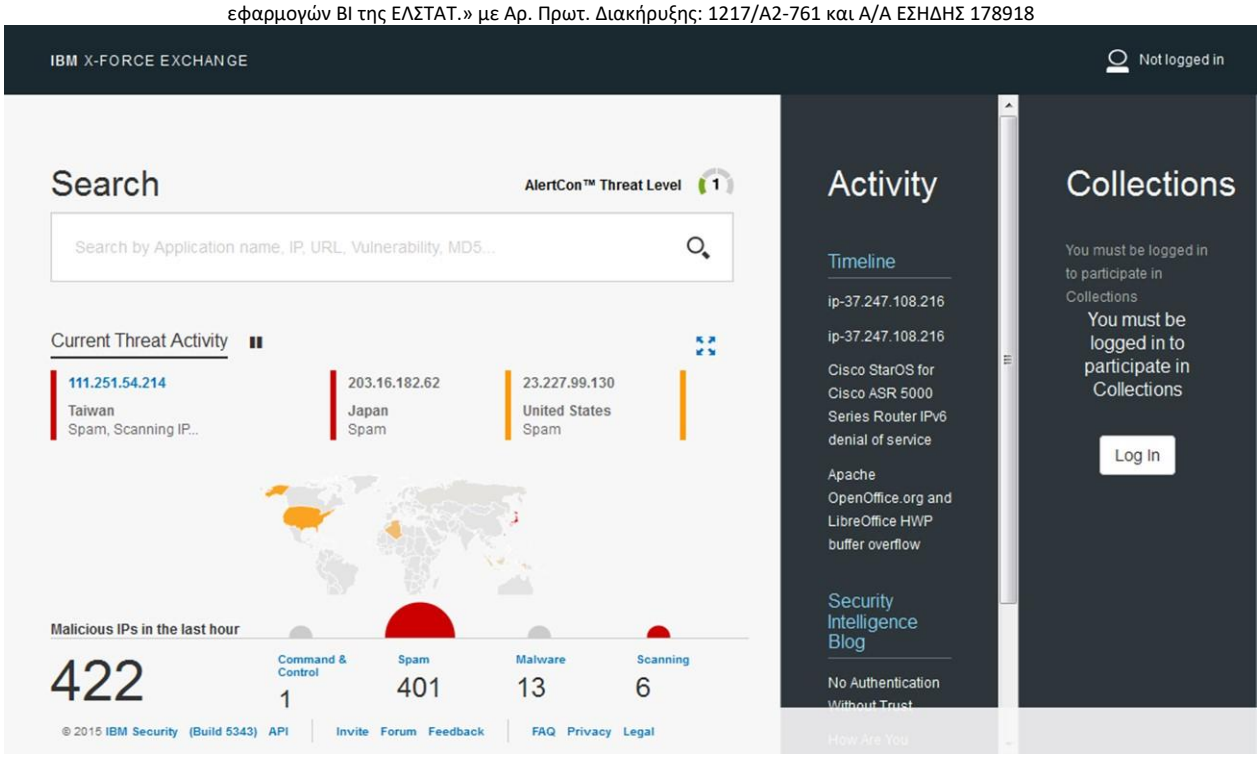
Οι υπηρεσίες πρόβλεψης που παρέχονται χωρίζονται στις ακόλουθες κατηγορίες:

- Υπηρεσία παρακολούθησης του παγκόσμιου δείκτη απειλών
- Υπηρεσία αποτίμησης ευπαθειών (Vulnerability Assessment)
- Υπηρεσία ευφυούς ανάλυσης απειλών (Threat Intelligence)
- Υπηρεσία προληπτικού Κυνηγιού Απειλών (Proactive Threat Hunting)

3.2.1.2 Υπηρεσία Παρακολούθησης του παγκόσμιου δείκτη απειλών

Μέσω της υπηρεσίας Παγκόσμιας Παρακολούθησης Απειλών, η εταιρεία μας παρακολουθεί τα γεγονότα ασφαλείας σε παγκόσμιο επίπεδο, παρέχοντας:

- Έγκαιρη προειδοποίηση για νέες ευπάθειες και ενεργές επιθέσεις
- Virtual Patches στην περίπτωση νέων ευπαθειών λογισμικού του οποίου ο κατασκευαστικός οίκος δεν έχει εκδώσει security patch μέσω της υλοποίησης custom IPS rule, firewall rule, endpoint detection rule κλπ.
- Δημιουργία Indicators of Compromise (IoC) για τον εντοπισμό επιβεβαιωμένων περιστατικών ασφάλειας μέσω της υπηρεσίας proactive threat hunting



Εικόνα 2: Global Threat Level Monitor Service

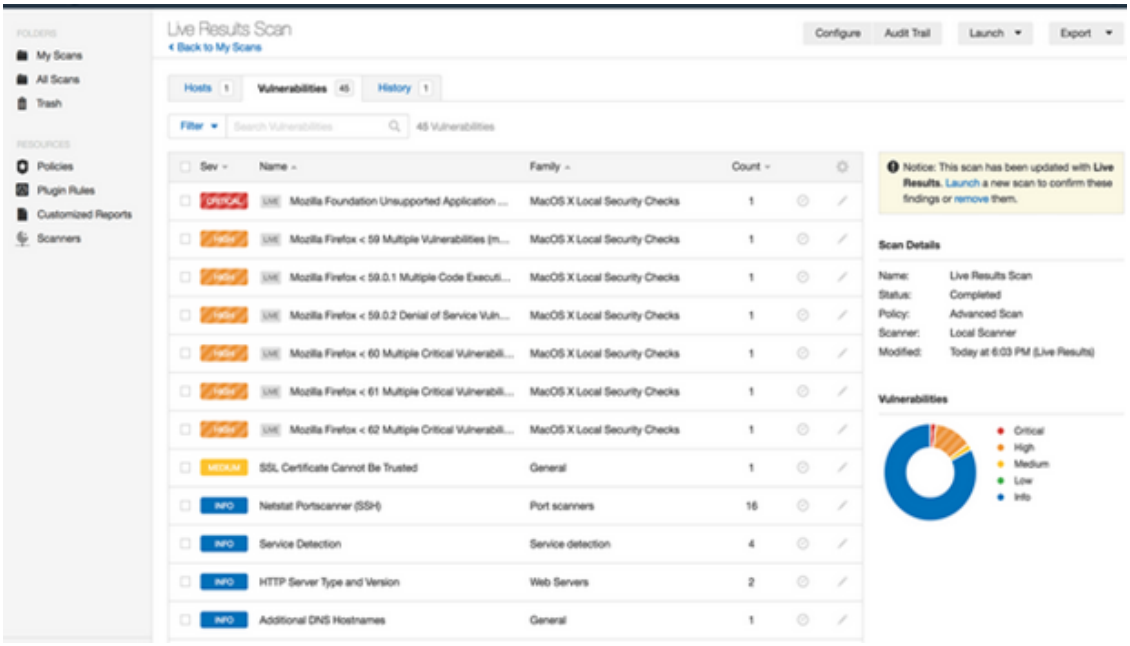
Στον πίνακα που ακολουθεί αναφέρονται τα IoC που δημιουργήσαμε στην πλατφόρμα του IBM Qradar μέσω του εργαλείου IBM Qradar IoC Manager και στην λύση Cisco Secure Endpoint για τα IoC της επίθεσης της ομάδας HAFNIUM στους Exchange Servers με 0-day exploits.

Τύπος IoC	**Τιμή**
Web Shell hashes	• b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0 • 097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e • 2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1 • 65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5 • 511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1 • 4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea • 811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d • 1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e7294
Web shell paths	• *C:|inetpub|wwwroot|aspnet_client|* • *C:|inetpub|wwwroot|aspnet_client|system_web|* • %PROGRAMFILES%\Microsoft\ExchangeServer\V15\FrontEnd\ HttpProxy\owa\auth\ • C:\Exchange\FrontEnd\HttpProxy\owa\auth\
Web shell file names	• *web.aspx* • *help.aspx* • *document.aspx* • *errorEE.aspx*

	• *errorEEE.aspx* • *errorEW.aspx* • *errorFF.aspx* • *healthcheck.aspx* • *aspnet_www.aspx* • *aspnet_client.aspx* • *xx.aspx* • *shell.aspx* • *aspnet_iisstart.aspx* • *one.aspx* .zip, .rar, and .7z files στο path n *C:|ProgramData|*, LSASS dumps: • *C:|windows|temp|* • *C:|root|*

3.2.1.3 Υπηρεσία Αποτίμησης Ευπαθειών (Vulnerability Assessment Service)

Η εταιρεία μας θα παρέχει την υπηρεσία αποτίμησης των ευπαθειών με χρήση του λογισμικού Nessus έτσι ώστε (α) σε κάθε περιστατικό να συσχετίζονται και οι ευπάθειες ενός συστήματος με τα συμβάντα ασφαλείας και (β) να προσδιορισθούν οι ευπάθειες ώστε ο πελάτης να προβεί στην επιδιόρθωση τους. Λόγω της γρήγορης μεταβαλλόμενης φύσης των ευπαθειών οι έλεγχοι αυτοί πραγματοποιούνται σε τετραμηνίαια βάση (τρείς (3) φορές το έτος) ή ad-hoc όταν παρουσιαστεί ανάγκη όπως εγκατάσταση νέου εξυπηρετητή, παροχή νέας υπηρεσίας κ.λπ.



Εικόνα 3: Υπηρεσία Ελέγχου Ευπαθειών

Η υπηρεσία καλύπτει ένα ευρύ φάσμα των τρωτών σημείων, πρωτοκόλλων, εφαρμογών, λειτουργικών συστημάτων, Web Εφαρμογών, Cloud συστημάτων και υπηρεσιών ώστε να εντοπισθούν όλα τα γνωστά τρωτά σημεία, παρέχοντας ακριβή αποτελέσματα και αποκλείοντας έτσι ψευδώς θετικά και ψευδώς αρνητικά ευρήματα.

Ουσιαστικά οι ευπάθειες που εντοπίζονται από την υπηρεσία μας αποτελούν μέρος της ευφυούς πληροφορίας των συστημάτων που έχουν εισαχθεί ή έχουν εντοπιστεί από την υπηρεσία όπως οι υπηρεσίες, οι θύρες κ.λπ. Χρησιμοποιώντας αυτές τις πληροφορίες μπορούμε να ολοκληρώσουμε και να συνδέσουμε τα περιστατικά ασφαλείας με τα επικοινωνιακά και υπολογιστικά συστήματα ως μέρος της διερεύνησης. Μέσω της υπηρεσίας αποτίμησης ευπαθειών συσχετίζονται συμβάντα ασφαλείας, δραστηριότητα δικτύου και συμπεριφορικές αλλαγές με τις ευπάθειες για τον προσδιορισμό του επιπέδου απειλής των συστημάτων .

Τα τεχνικά χαρακτηριστικά της υπηρεσίας είναι:

- Απεριόριστος υποστηριζόμενος αριθμός ελεγχόμενων συσκευών και συστημάτων
- Ανίχνευση αδυναμιών σε επίπεδο λειτουργικών συστημάτων, υπηρεσιών, δικτύου, τερματικών και Web Εφαρμογών.
- Διεξαγωγή των ελέγχων σε προγραμματισμένα χρονικά διαστήματα ή μετά από αίτημα της ΕΛΣΤΑΤ, χωρίς περιορισμό στο συνολικό αριθμό ελέγχων.
- Αυτόματη ανανέωση της βάσης επιθέσεων/αδυναμιών μέσα από τη λήψη τακτικών ενημερώσεων.
- Υποστήριξη διαφορετικών πολιτικών ελέγχου ανάλογα με το είδος των συστημάτων, το επιθυμητό βάθος του ελέγχου και τα αντίστοιχα πρότυπα κανονιστικής συμμόρφωσης.
- Εκτέλεση των ελέγχων ασφάλειας στα συστήματα της υποδομής χωρίς να απαιτείται η εγκατάσταση ειδικού λογισμικού (agent) σε αυτά (agent-less).
- Παραγωγή διαφορετικών τύπων αναφορών για διαφορετικού τύπου παραλήπτες όπως λεπτομερείς τεχνικές αναφορές αποκατάστασης αδυναμιών (technical remediation reports) προς τους διαχειριστές της υποδομής, καθώς και συνοπτικές αναφορές υψηλού επιπέδου προς τη διοίκηση (high level executive reports).
- Ολοκλήρωση με την υπηρεσία παρακολούθησης και ενημέρωσης για περιστατικά ασφάλειας.

3.2.1.4 Ανίχνευση

Με τον εντοπισμό ενός συμβάντος, δημιουργείτε αυτόματα από την SOAR υποδομή μας ένα περιστατικό, το οποίο ανατείθεται σε αναλυτή επιπέδου 1. Οι αναλυτές επιπέδου 1, υπεύθυνοι για τη συνεχή παρακολούθηση των περιστατικών ασφαλείας, θα αναλύσουν αρχικά κάθε περιστατικό και με την χρήση της υπηρεσίας τεχνητής νοημοσύνης IBM QRadar Advisor with Watson θα καθορίσουν τις πληροφορίες επίθεσης, την εγκυρότητα του κ.λπ.

Το επίπεδο και η απόκριση στο περιστατικό ασφαλείας διέπετε από υψηλή αυστηρότητα. Τα επίπεδα σοβαρότητας θα έχουν προ-συμφωνηθεί με τον πελάτη ανάλογα με τον αντίκτυπο στις λειτουργίες και την κρισιμότητα της υποδομής.

Αν κατά την αρχική ανάλυση προκύψει ότι το περιστατικό ασφάλειας, είναι «ψευδώς θετικό», τότε θα το αγνοήσουν και θα το κλείσουν. Εάν όχι, τότε θεωρείτε αποδεδειγμένο περιστατικό ασφαλείας, θα δημιουργήσουν εισιτήριο ώστε να καταγράψουν τις σχετικές πληροφορίες και θα το κλιμακώσουν στους αναλυτές επιπέδου 2 (εάν απαιτηθεί από

τον τύπο του περιστατικού). Σε διαφορετική περίπτωση θα ενημερώσουν τον πελάτη μέσω e-mail, sms, web portal, Microsoft Teams ή τηλεφωνικά.

Για κάθε περιστατικό θα αναφέρονται:

- Ημερομηνία και ώρα
- Τύπος
- Περιγραφή
- Κρισιμότητα
- Προτεραιότητα
- Ενέργειες Εξάλειψής
- Υπεύθυνος Αναλυτής
- Κατάσταση

Στη συνέχεια, οι αναλυτές επιπέδου 2, υπεύθυνοι για την διαχείριση των περιστατικών ασφαλείας, θα αναλύσουν το περιστατικό ασφαλείας σύμφωνα την μεθοδολογία διερεύνησης περιστατικών ασφαλείας του SOC ώστε να συλλέξουν όλες τις απαραίτητες πληροφορίες για το εύρος, τον εισβολέα, την μεθοδολογία, τις τεχνικές και τον στόχο της επίθεσης.

Ο αναλυτής επιπέδου 2 υποστηρίζεται από μία ολοκληρωμένη γνωσιακή βάση, η οποία διαθέτει τις απαραίτητες ροές και τα πλάνα απόκρισης για κάθε τύπο περιστατικού εμπλουτισμένα με τις απαραίτητες ευφυής πληροφορίες ανάλυσης απειλών. Στη συνέχεια θα καθορίσει τις επιπτώσεις από το περιστατικό και τις δράσεις που απαιτούνται για την άμεση αποκατάσταση του.

Ανάλογα με την πολυπλοκότητα του περιστατικού, μπορεί να χρειαστεί να κλιμακώσουν ένα περιστατικό σε αναλυτή επιπέδου 3, οι οποίοι είναι υπεύθυνοι για την διαχείριση άγνωστου τύπου περιστατικών ασφαλείας όπως κακόβουλο λογισμικό μηδενικού χρόνου, κ.λπ. που απαιτεί περαιτέρω έρευνα για την αξιολόγηση της φύσης της απειλής. Αυτή η έρευνα θα βασισθεί στις πληροφορίες που είναι άμεσα προσβάσιμες στο SOC εντός του πεδίου εφαρμογής των υπηρεσιών του.

Μετά την ολοκλήρωση της ανάλυσης, θα δοθούν οι κατάλληλες συστάσεις στον πελάτη. Οι συστάσεις μπορεί να περιλαμβάνουν άμεσες ενέργειες τερματισμού, αποκατάστασης, εγκληματολογική ανάλυση κ.λπ.

Επιπροσθέτως η Adacom μπορεί να παρέχει συμβουλευτικές υπηρεσίες για την προετοιμασία του πλάνου και της στρατηγικής αντιμετώπισης των περιστατικών ασφαλείας, των απαραίτητων διαδικασιών απόκρισης και αποκατάστασης, των playbooks για την αντιμετώπιση συγκεκριμένων κυβερνοεπιθέσεων, καθώς και υπηρεσίες εκπαίδευσης και εξομοίωσης επιθέσεων με εξειδικευμένα σενάρια βασισμένα σε διεθνής μεθοδολογίες και πλαίσια. Αυτές οι υπηρεσίες μπορούν να βοηθήσουν τον πελάτη να κατανοήσει καλύτερα τη φύση και το εύρος των εξειδικευμένων περιστατικών ασφαλείας, τον επιδιωκόμενο σκοπό τους, κ.λπ. καθώς να εμπλουτίσει τις δράσεις για μια επιτυχημένη αποκατάσταση.

3.2.1.4.1 Ανάλυση συμπεριφοράς χρηστών

Με την υπηρεσία UBA, οι αναλυτές μας θα αναλύουν την δραστηριότητα των χρηστών για την ανίχνευση κακόβουλης δραστηριότητας και θα εντοπίζουν οποιαδήποτε εσωτερική απειλή. Επίσης, θα μπορούν εύκολα να εντοπίσουν τους υψηλής επικινδυνότητας χρήστες, τις ανώμαλες δραστηριότητές τους και να ελέγξουν τα συμβάντα ασφαλείας και τις δικτυακές ροές που συνέβαλαν στη βαθμολογία της επικινδυνότητας ενός χρήστη.

Ως ενσωματωμένη υπηρεσία της πλατφόρμας μας, η υπηρεσία UBA αξιοποιεί τα μοντέλα συμπεριφοράς και της μηχανικής μάθησης (ML) για να προσθέσει το περιβάλλον των χρηστών στις δικτυακές ροές, στα συμβάντα ασφαλείας, στις ευπάθειες και στις απειλές για την ταχύτερη και ακριβέστερη ανίχνευση επιθέσεων.

Η υπηρεσία UBA προσθέτει δύο βασικές λειτουργίες:

- τη δημιουργία προφίλ κινδύνου και
- την ενοποίηση των ταυτοτήτων των χρηστών

Ο προσδιορισμός μίας απειλής πραγματοποιείται με την βαθμολόγηση της επικινδυνότητας σε διάφορα συμβάντα με την χρήση είτε στατικών κανόνων ασφαλείας οι οποίο περιλαμβάνουν στοιχεία όπως κακόβουλοι ιστότοποι, IPs, κ.λπ. είτε προηγμένων μαθηματικών μοντέλων που χρησιμοποιούν μηχανική μάθηση. Σε κάθε συμβάν καθορίζεται ο κίνδυνος, ανάλογα με τη σοβαρότητα και την κρισιμότητα του συμβάντος που εντοπίστηκε.

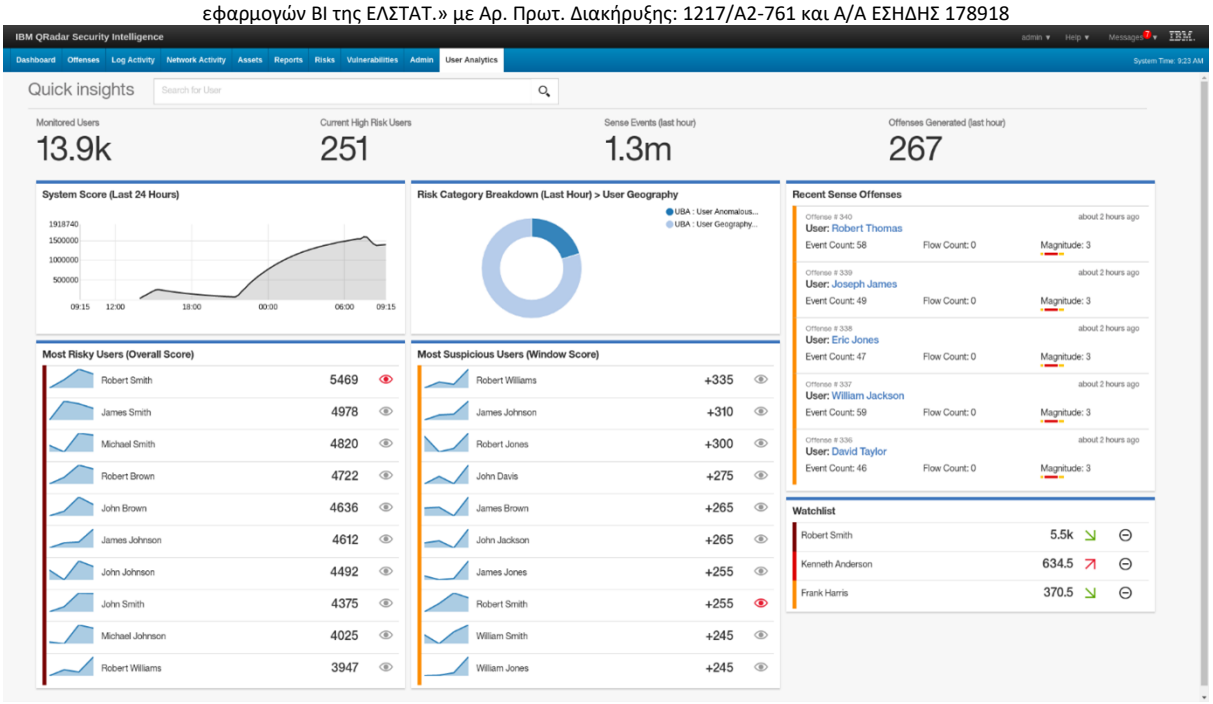
Η υπηρεσία UBA βασίζει τα αποτελέσματα της σε τρεις βασικές κατηγορίες συμβάντων και ροών:

1. Στην δικτυακή κίνηση σχετικά με την πρόσβαση, τον έλεγχο της ταυτότητας και τις αλλαγές λογαριασμών.
2. Στην συμπεριφορά των χρηστών στο δίκτυο, από συσκευές όπως: proxies, firewalls, IPS και VPN.
3. Στα συμβάντα από τα τελικά σημεία και εφαρμογές, όπως από Windows ή το Linux, και τις εφαρμογές SaaS.

Η ενοποίηση των ταυτοτήτων των χρηστών επιτυγχάνεται συνδυάζοντας διαφορετικούς λογαριασμούς για ένα χρήστη. Με την εισαγωγή των λογαριασμών από έναν κατάλογο Active Directory, LDAP, πίνακα αναφοράς ή CSV, η υπηρεσία μπορεί να μάθε ποιοι λογαριασμοί ανήκουν έναν χρήστη. Το ως άνω χαρακτηριστικό επιτρέπει τον υπολογισμό της επικινδυνότητας για έναν χρήστη ακόμα και αν έχει πολλαπλούς λογαριασμούς.

Η Μηχανική Μάθηση (ML) είναι ένα πρόσθετο εργαλείο που ενισχύει την υπηρεσία UBA και παρέχει ακριβή και εις βάθος υπολογισμών για τον εντοπισμό μίας απειλής ακόμα και μηδενικού χρόνου.

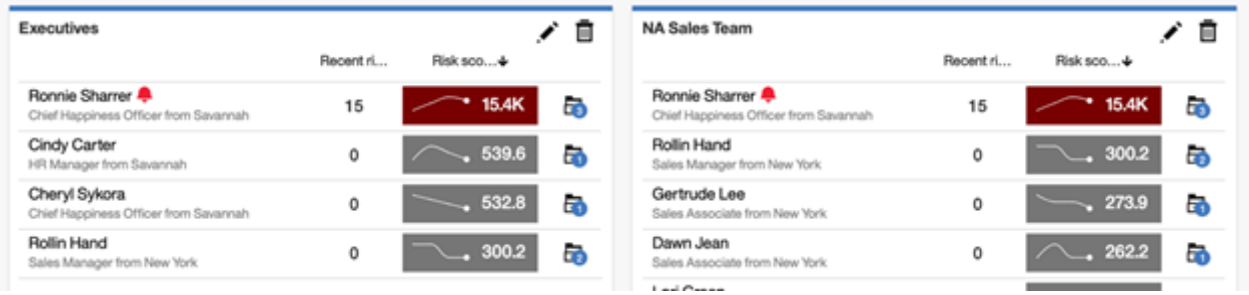
Η υπηρεσία παρέχει ένα dashboard που εμφανίζονται οι επικίνδυνοι χρήστες σύμφωνα με το λογαριασμό τους και την δραστηριότητα τους.



Εικόνα 4: Ανάλυση Συμπεριφοράς των χρηστών

Επίσης μπορούμε να επιλέξουμε οποιονδήποτε χρήστη και να ελέγξουμε την δραστηριότητα τους (π.χ. αυξήσεις δικαιωμάτων, εντολές που εκτελούνται σε όλες τις συσκευές, geolocation)

Με ένα μόνο κλικ του ποντικιού προσθέτουμε έναν λογαριασμό σε μία λίστα παρακολούθησης π.χ. έναν λογαριασμό με αυξημένα προνόμια, όπου παρέχονται τα γεγονότα ασφαλείας και οι δικτυακές ροές.

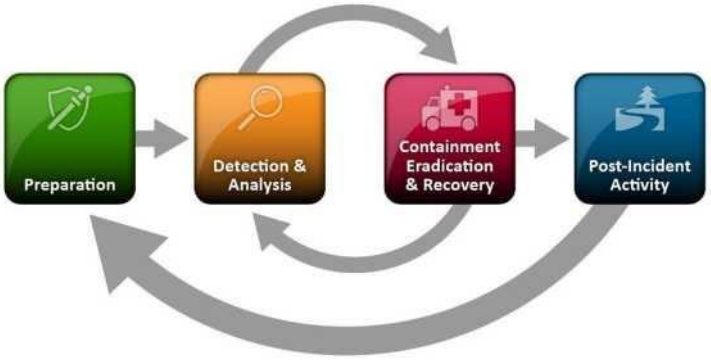


Εικόνα 7: WatchList

Επιπλέον, οι αναλυτές μπορούν να κλιμακώσουν τον βαθμό επικινδυνότητας όλων των χρηστών σε μια λίστα παρακολούθησης καθορίζοντας τον συντελεστή κλιμάκωσης.

3.2.1.5 Απόκριση

Η μεθοδολογία που έχει υιοθετηθεί από την εταιρεία μας για την απόκριση σε πραγματικά περιστατικά ασφαλείας διακρίνεται σε τέσσερεις φάσεις:



Εικόνα 6: Μεθοδολογία απόκρισης

3.2.1.5.1 Προετοιμασία

Στην φάση της προετοιμασίας, καθορίζονται οι ομάδες απόκρισης, η απαιτούμενη υποδομή, οι απαραίτητες διαδικασίες και πολιτικές καθώς και τα προτεινόμενα έντυπα. Συγκεκριμένα σε αυτή τη φάση:

- Καθορίζονται οι ομάδες αντιμετώπισης
- Καθορίζονται οι απαραίτητες πολιτικές και διαδικασίες λαμβάνοντας υπόψη τις προσφερόμενες υπηρεσίες SOC
- Διαμορφώνεται το σχέδιο επικοινωνίας με τους υπεύθυνους του οργανισμού
- Θεσπίζονται κριτήρια για την λήψη αποφάσεων για το περιστατικό
- Καθορίζεται μια ασφαλή τοποθεσία ως τόπος εφαρμογής του σχεδίου αντιμετώπισης
- Διασφαλίζεται η διαθεσιμότητα του απαραίτητου εξοπλισμού
- Καθορίζονται τα απαραίτητα playbooks ανά τύπου περιστατικού. Ενδεικτικά αναφέρονται:
    - Ransomware playbook
    - Phishing playbook
    - DoS/DDoS playbook
    - Unauthorized Access playbook
    - Data Leakage playbook κ.λπ.

3.2.1.5.2 Ανάλυση

Σε αυτό το σημείο η αξιολόγηση του περιστατικού, ο εντοπισμός των αιτιών και το άμεσο σχέδιο αντιμετώπισης του είναι πολύ σημαντικά για την αποφυγή σοβαρού προβλήματος στον οργανισμό. Σε αυτή τη φάση λαμβάνουν χώρα τα εξής βήματα:

- Αξιολόγηση του περιστατικού
- Κλιμάκωση σε αναλυτή L2 εάν απαιτείται
- Καθορισμός κρισιμότητας
- Καθορισμός στρατηγικής και σχεδίου αντιμετώπισης του περιστατικού ασφαλείας

3.2.1.5.3 Αναχαίτιση - Εξάλειψη - Ανάκαμψη

Μετά την ανάλυση του περιστατικού, ακολουθεί το στάδιο της αναχαίτισης. Η ομάδα διαχείρισης των περιστατικών αναλαμβάνει δράση για να περιορίσει την έκθεση του οργανισμού και των ζημιών. Ανάλογα με το είδος της παραβίασης θα εκτελέσει τις κατάλληλες ενέργειες. Ενδεικτικά σε αυτό το στάδιο εκτελούνται οι ακόλουθες :

- Ενεργοποιείται η ομάδα αντιμετώπισης περιστατικών
- Γίνεται κλίμακωση του περιστατικού
- Γίνεται ανάλυση (forensics) για τον εντοπισμό της προέλευσης των απειλών, τον μετριασμό τους, την έναρξη μέτρων για την πρόληψη της επανεμφάνισης.
- Παροχή υπηρεσίας Managed Detection and Response
- Υλοποιούνται οι δράσεις αναχαίτισης είτε τοπικά είτε απομακρυσμένα
- Συλλέγονται και φυλάσσονται στοιχεία σχετικά με το περιστατικό
- Τεκμηριώνεται κάθε ενέργεια και λαμβάνονται αντίγραφα ασφαλείας

Το επόμενο στάδιο της αντιμετώπισης περιστατικών ασφάλειας είναι το στάδιο της εξάλειψης. Μετά την ολοκλήρωση της φάσης αναχαίτισης, είναι απαραίτητος ο εντοπισμός των αιτιών που προκάλεσαν το περιστατικό. Οι αιτίες μπορεί να εξαλειφθούν με την αποκατάσταση των συστημάτων μέσω αντιγράφων ασφαλείας, μέσω της απομάκρυνσης τους, μέσω της βελτίωσης της άμυνας ή μέσω της διεξαγωγής ανάλυσης των ευπαθειών του συστήματος. Συνοπτικά, στο στάδιο της εξάλειψης:

- Καθορίζονται οι ενδείξεις και τα αίτια του περιστατικού
- Εντοπίζονται τα αντίγραφα ασφαλείας
- Απομακρύνονται τα αίτια του περιστατικού
- Βελτιώνεται η άμυνα με την υλοποίηση μέτρων προστασίας
- Διεξάγονται αναλύσεις ευπαθειών

Αμέσως μετά ακολουθεί το στάδιο της Ανάκαμψης, στο οποίο πρέπει ο οργανισμός να επανέλθει στα φυσιολογικά του πλαίσια και στην κανονική του λειτουργία. Συγκεκριμένα στο στάδιο αυτό:

- Επαναφέρονται όλες οι λειτουργίες στην κανονική τους κατάσταση
- Επικυρώνεται η επιτυχία των ενεργειών αποκατάστασης
- Ελέγχεται η σωστή λειτουργία των συστημάτων
- Εξασφαλίζεται η κατάσταση κανονικής λειτουργίας των συστημάτων

3.2.1.5.4 Ανασκόπηση

Το τελευταίο στάδιο είναι αυτό της ανασκόπησης, η οποία είναι αρκετά σημαντική καθώς χρειάζεται να γίνει μια συνολική εκτίμηση του περιστατικού. Δημιουργείται μια έκθεση μέσω της οποίας ο οργανισμός ενημερώνεται για το περιστατικό, τι ακριβώς συνέβη, ποια μέτρα πάρθηκαν και ποια ήταν τα αποτελέσματα. Γενικά λοιπόν, σε αυτή τη φάση γίνονται τα εξής βήματα:

- Γίνεται ανασκόπηση του περιστατικού με σκοπό να βγάλουμε χρήσιμα συμπεράσματα για τον τρόπο

ανίχνευσης και αντιμετώπισης του εν λόγω περιστατικού

- Συντάσσεται μια έκθεση για το περιστατικό
- Αναλύονται τα θέματα που προέκυψαν κατά την αντιμετώπιση του
- Παρέχονται συμβουλευτικές υηηρεσίες για την βελτίωση των οργανωτικών και τεχνολογικών μηχανισμών προστασίας

Επιπροσθέτως στην άμεση και αποτελεσματική απόκριση σε ένα περιστατικό, συμβάλλει η υπηρεσία Managed detection and response.

Τεχνικά και λειτουργικά χαρακτηριστικά

Τα τεχνικά και λειτουργικών της υπηρεσίας είναι:

- Διερεύνηση περιστατικών ασφαλείας με χρήση τεχνητής νοημοσύνης
- Συμφωνημένο Επίπεδο Υπηρεσιών
- Περιπτώσεις Χρήσης (use cases)
- Αναφορές
- Σύγχρονο Κέντρο Επιχειρήσεων της Ασφάλειας Πληροφοριών
- Web Portal ανά πελάτη
- Δυνατότητα συνεχούς βελτιστοποίησης της παρεχόμενης υπηρεσίας
- Ασφαλή Διασύνδεση
- Πλατφόρμα SIEM IBM QRadar

3.2.1.6 Συμφωνημένο Επίπεδο Υπηρεσιών

Το SLA θα είναι μέρος της σύμβασης και θα παρακολουθείται. Ενδεικτικά αναφέρονται οι ακόλουθοι χρόνοι MTTR (Mea Time to Respond) και KPI της προσφερόμενης υπηρεσίας.

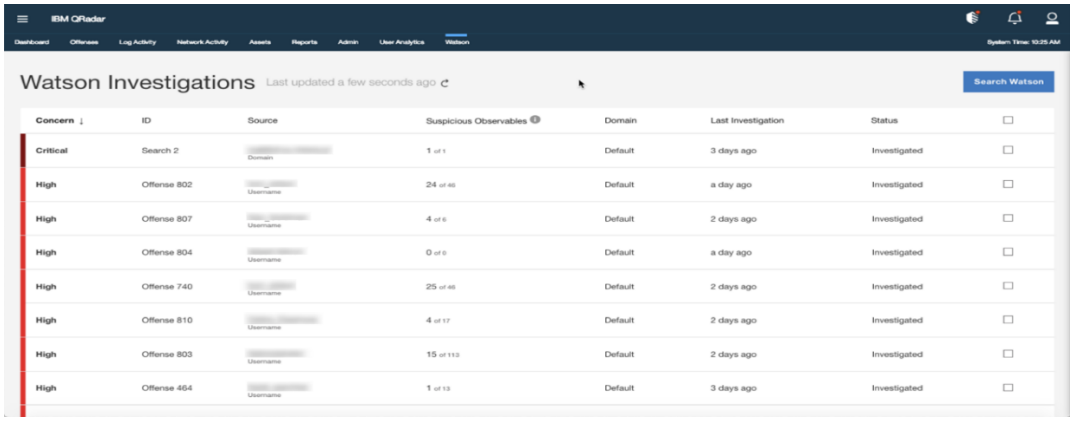
Επίπεδο Σοβαρότητας	Χρόνος Απόκρισης	Ενέργειες
Σοβαρότητα 4	15 λεπτά	Αρχική Ανάλυση - Επιβεβαίωση Περιγραφή του περιστατικού Προτεινόμενες ενέργειες μετριασμού Ενημέρωση
Σοβαρότητα 3	60 λεπτά	Αρχική Ανάλυση - Επιβεβαίωση Περιγραφή του περιστατικού Προτεινόμενες ενέργειες μετριασμού Ενημέρωση
Σοβαρότητα 2	8 ώρες	Αρχική Ανάλυση - Επιβεβαίωση Περιγραφή του περιστατικού Ενημέρωση
Σοβαρότητα 1	Καμία κλιμάκωση	-

Πίνακας 1: Mean Time to respond (MTTR)

3.2.2 Μέρος Β

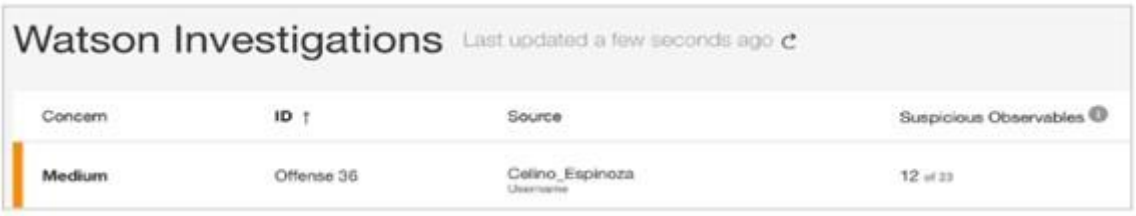
3.2.2.1 Διερεύνηση περιστατικών ασφαλείας με χρήση τεχνητής νοημοσύνης

Η εταιρεία μας, πρωτοπόρος στην ασφάλεια των πληροφοριών, ενσωμάτωσε τεχνολογίες τεχνητής νοημοσύνης στο SOC της, διαθέτοντας πια ένα state-of-the-art Security Intelligence Center (SIC). Πέρα από τους παραδοσιακούς μηχανισμούς ανίχνευσης απειλών μπορούμε να εντοπίσουμε και να αντιμετωπίσουμε οποιαδήποτε απειλή με ακρίβεια και αποτελεσματικότητα μέσω της υπηρεσίας τεχνητής νοημοσύνης, IBM Qradar Advisor with Watson. Η λύση αυτή έχει σχεδιαστεί με την λογική της άμεσης ανίχνευσης του πρώιμου σταδίου μίας επίθεσης, κατανοώντας την λογική της επίθεσης και την μεθοδολογία ενός εξειδικευμένου hacker. Αυτό επιτυγχάνεται μέσω των Big Data Security Analysis, και την τεχνολογία γνωστικής υπολογιστικής.



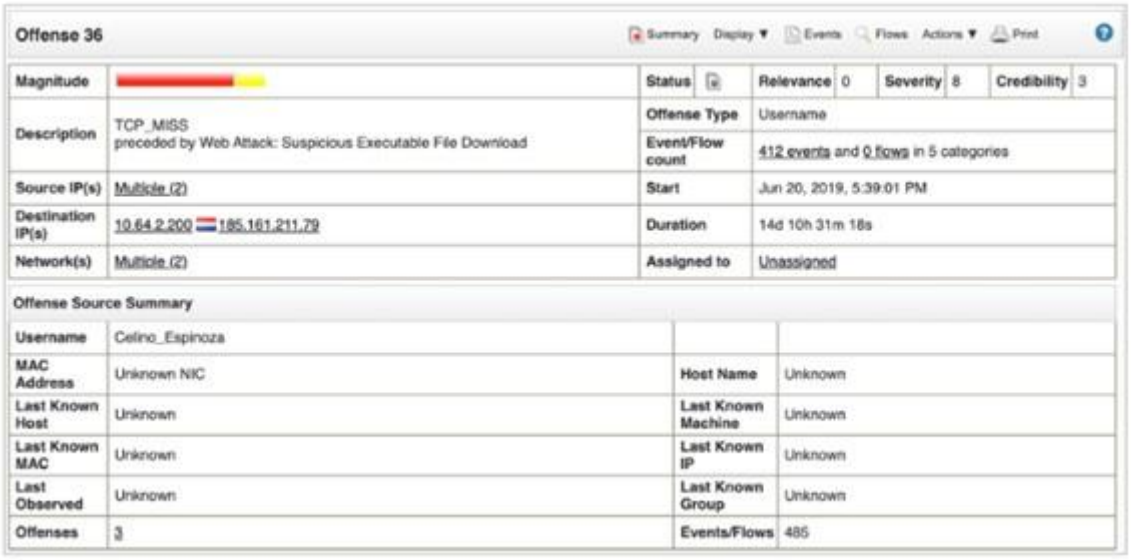
Εικόνα 7: IBM Watson

Μία από τις σημαντικές δυνατότητες της υπηρεσίας IBM QRadar advisor with Watson (QRAW) είναι ο αυτοματισμός της εξόρυξης των IOC (IOC mining) και ο εντοπισμός εκείνων των πληροφοριών που θεωρούνται σημαντικές. Όπως φαίνεται στην εικόνα 10, η υπηρεσία Watson ξεκινά κατηγοριοποιώντας μία διερεύνηση.



Εικόνα 8: IBM Watson

Ουσιαστικά η υπηρεσία δεν παρέχει ένα πρότυπο στο οποίο ένας αναλυτής προσθέτει τα αποτελέσματα από μία διερεύνηση που υλοποιεί αλλά αντίθετα παρέχει ένα σύνολο μεταδομένων που το έχει συσχετίσει με την διερεύνηση. Μία διερεύνηση συσχετίζεται ένα περιστατικό, όπως φαίνεται στην εικόνα 11, το οποίο παρέχει πληροφορίες για ύποπτη δραστηριότητα και με ανωμαλίες στο περιβάλλον.



Εικόνα 9

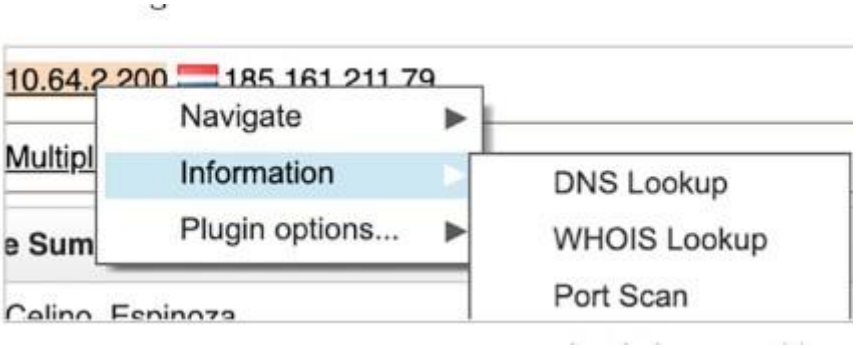
Ένα από τα σημαντικά μεταδεδομένα είναι η σημαντικότητα (magnitude) ενός συγκεκριμένου περιστατικού. Αυτή η οπτική απεικόνιση βοηθά τους αναλυτές να προσδιορίσουν άμεσα τα πιο σημαντικά περιστατικά, ώστε να μπορούν να εστιάσουν το χρόνο τους ανάλογα. Επιπροσθέτως η προσφερόμενη υπηρεσία παρέχει προτεραιότητες στα περιστατικά με βάση τους Indicators Of Compromise (IOC), τους πόρους και τους κανόνες. Αυτή η ανάλυση μπορεί να εκπαιδευτεί από τον χρήστη επικυρώνοντας εάν συμφωνεί ή όχι με αυτή.

Η υπηρεσία διαθέτει διεπαφές και δυνατότητας για αυτοματοποιημένη δράση και οτιδήποτε υπογραμμίζεται στην καρτέλα Επίθεση είναι διαδραστικό για τον αναλυτή. Για παράδειγμα, στο περιστατικό της εικόνας 2, υπάρχουν δύο διευθύνσεις IP: μία εσωτερική και μία εξωτερική.

Η υπηρεσία QRadar Advisor αναγνωρίζει αυτούς τους τύπους δεδομένων και παρέχει χρήσιμες ενέργειες απευθείας από αυτήν την οθόνη. Για παράδειγμα, απλά τοποθετώντας το δείκτη του ποντικιού πάνω από την εξωτερική διεύθυνση IP, όπως φαίνεται στην εικόνα 10, εμφανίζεται αυτόματα η γεωγραφική τοποθεσία.

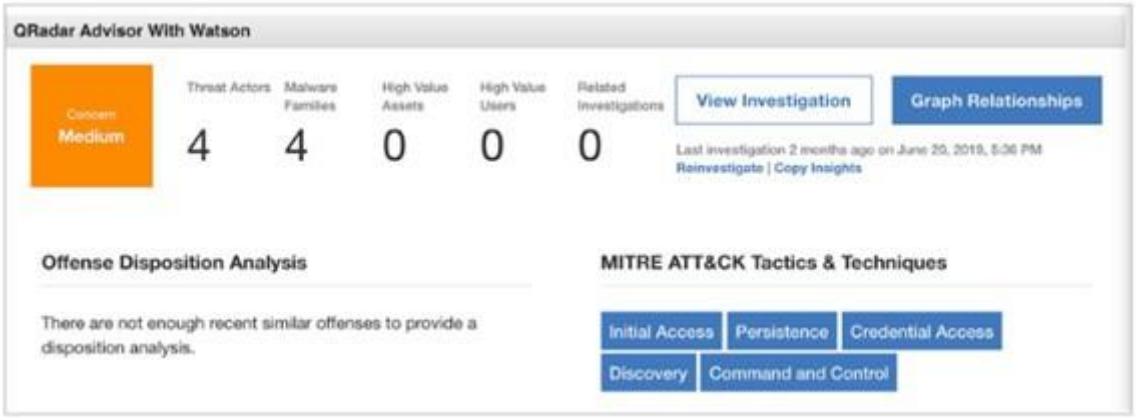
Εικόνα 10

Επιπλέον, ένας αναλυτής μπορεί επίσης να εκπονήσει μία σειρά από ενέργειες σε οποιασδήποτε από τις δύο διευθύνσεις IP. Όπως φαίνεται στην εικόνα 11, κάνοντας δεξί κλικ σε οποιαδήποτε διεύθυνση IP επιτρέπει σε έναν αναλυτή να εκτελεί αναζητήσεις DNS και WHOIS, σάρωση θύρας ή προβολή δικτύου.



Εικόνα 11

Μετά από διερεύνηση ενός περιστατικού με την υπηρεσία QRadar Watson, τα βασικά μεταδεδομένα σχετικά με την έρευνα θα υπάρχουν και στην καρτέλα "Offence" (εικόνα 12).



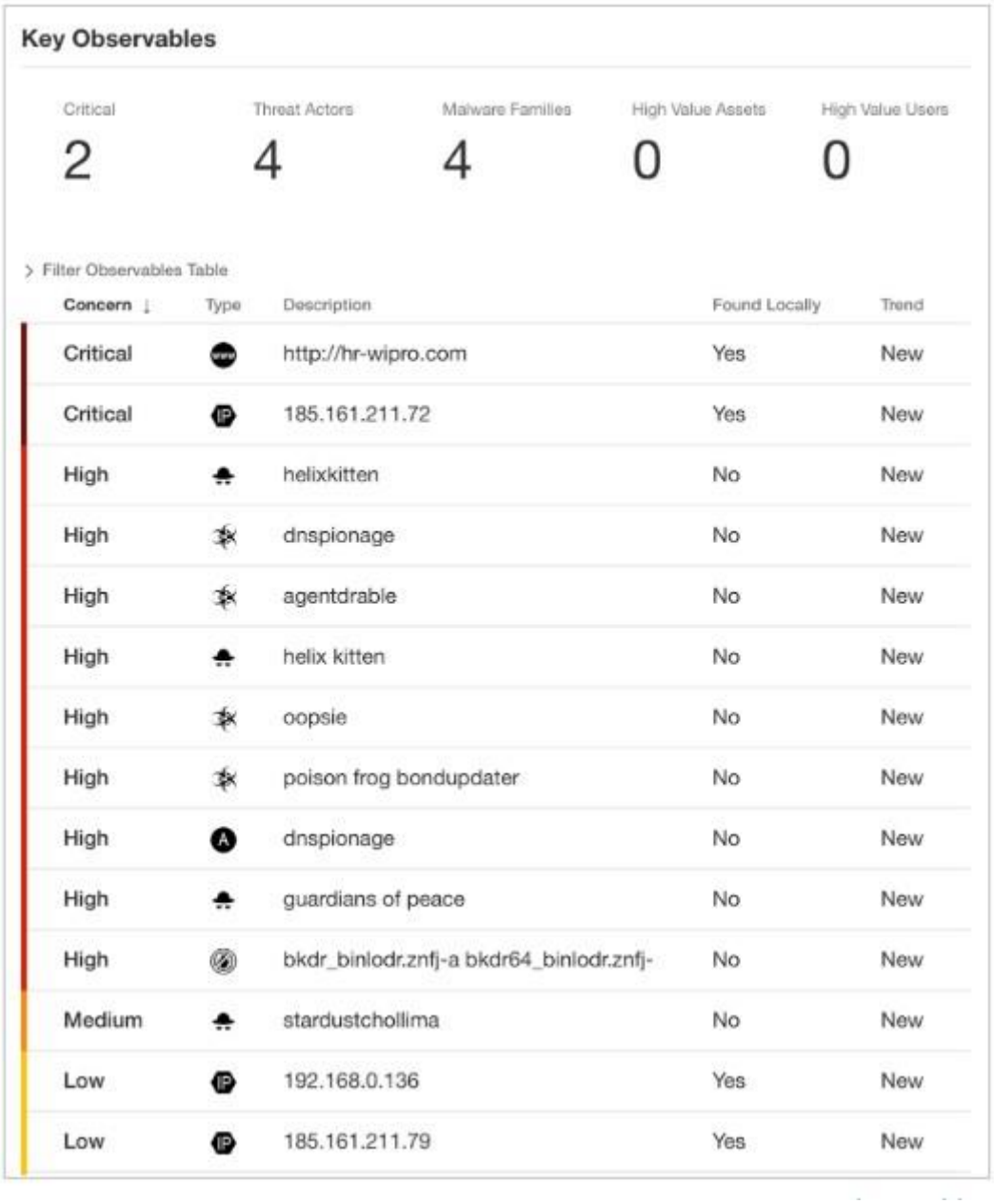
Εικόνα 12: Offence

Με την υπηρεσία IBM Watson, ο αναλυτής διαθέτει ένα βασικό πλαίσιο πληροφοριών για το περιστατικό που θα τον βοηθήσει στην περαιτέρω αξιολόγηση της κρισιμότητας ενός περιστατικού. Τα βασικά μεταδεδομένα που υπάρχουν στο συγκεκριμένο πλαίσιο είναι:

- Ο αριθμός των συσχετιζόμενων παραγόντων απειλών και των οικογενειών κακόβουλου λογισμικού
- Ο εντοπισμός και η σύγκριση παρόμοιων ή/και προηγούμενων περιστατικών ασφαλείας που συσχετίζονται με το εν λόγω περιστατικό,
- Οι τακτικές και οι τεχνικές σύμφωνα με το πλαίσιο Mitre's ATT & CK
- Η αξία των περιουσιακών στοιχείων και των χρηστών που εμπλέκονται με ένα περιστατικό. υπηρεσία εντοπίζει αμέσως τις κρίσιμες πληροφορίες που μπορεί θα βοηθήσουν σημαντικά στην διερεύνηση.
- Τα IOCs που συσχετίζονται με ένα περιστατικό

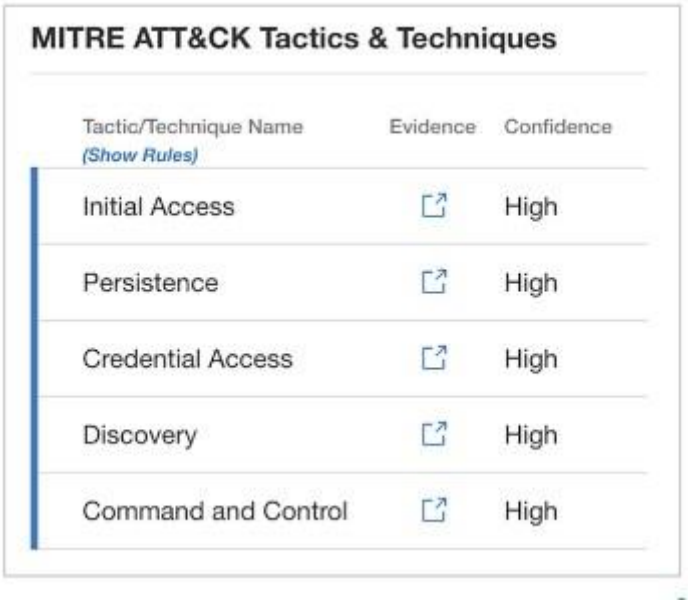
Επίσης επιτρέπει την εξαγωγή των IOC σε σύνολα αναφοράς, CSV αρχεία ή Structured Threat Information eXpression (STIX) υπηρεσίες.

Η υπηρεσία IBM Watson ουσιαστικά ξεκινά από την στιγμή που θα κάνουμε ένα κλικ σε μία διερεύνηση. Ουσιαστικά αυτό το κλικ επιτρέπει στην υπηρεσία να εμπλουτίσει τα μεταδομένα μίας επίθεσης. Η εικόνα 15 δείχνει, για παράδειγμα, ότι τα μεταδεδομένα για αυτό το περιστατικό έχει εμπλουτιστεί με δύο κρίσιμα alerts που είναι και τα δύο στοιχεία δικτύου.



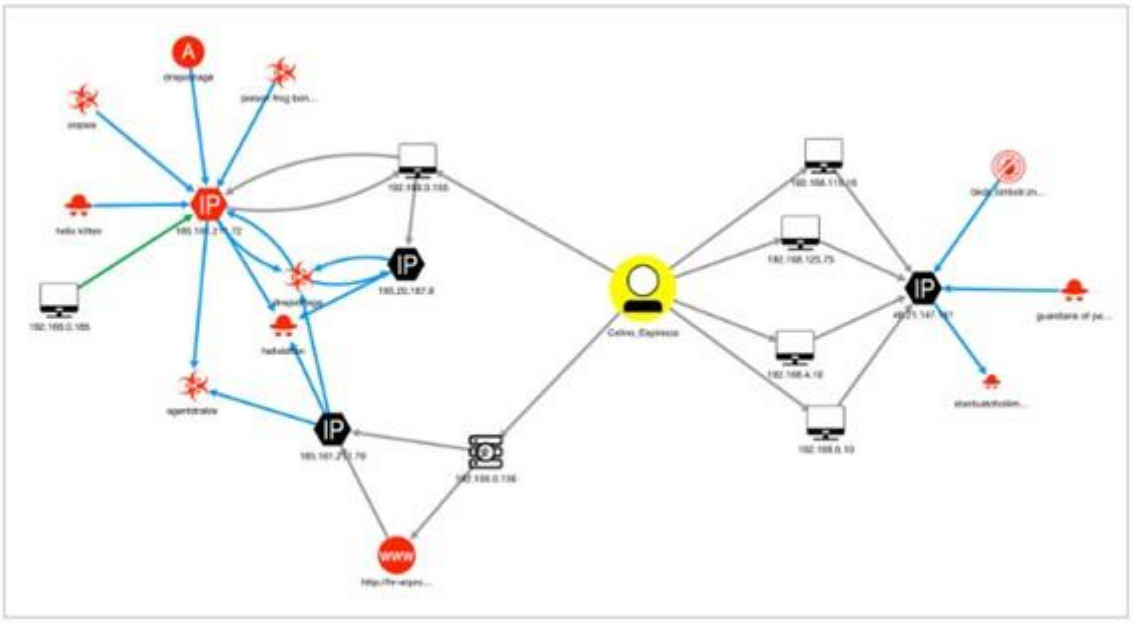
Εικόνα 13

Επιπλέον, μπορούμε να δούμε τους σχετικούς παράγοντες απειλής και τις οικογένειες κακόβουλου λογισμικού που συσχετίζονται με αυτό το περιστατικό. Επίσης μας αναφέρει εάν τα συγκεκριμένα στοιχεία έχουν ανιχνευθεί τοπικά στην υποδομή μας. Επίσης παρέχεται η αυτόματη χαρτογράφηση των μεταδεδομένων σε γνωστές τακτικές και τεχνικές σύμφωνα με το πλαίσιο MITRE ATT & CK (εικόνα 14).



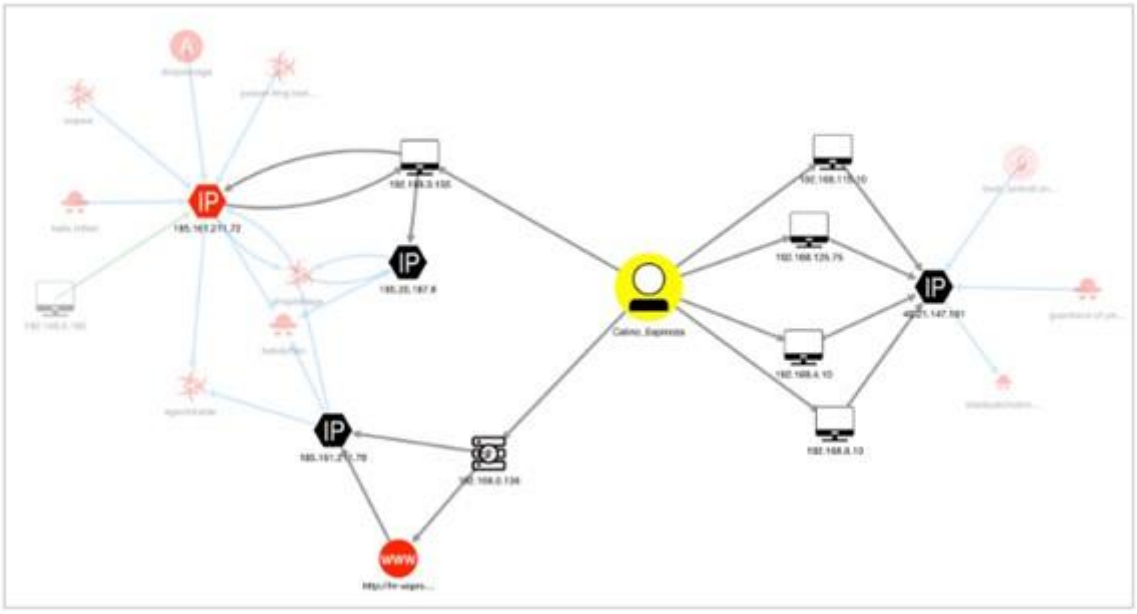
Εικόνα 14

Επίσης η υπηρεσία για κάθε διερεύνηση δημιουργεί ένα γράφημα όπου απεικονίζονται τα μεταδομένα και οι συνδέσεις μεταξύ τους (Εικόνα 15).



Εικόνα 15

Από το γράφημα η υπηρεσία μας επιτρέπει να προσαρμόσουμε το γράφημα στις ανάγκες μας και να αφαιρέσουμε τα μεταδεδομένα που ενδέχεται να μην σχετίζονται με την εν λόγω διερεύνηση. Η εικόνα 18 παρουσιάζει μία οθόνη του ίδιου ακριβώς γραφήματος του οποίου έχουν γκριζαριστεί όλα τα μεταδεδομένα που δεν έχουν βρεθεί τοπικά στην υποδομή του QRadar. Αυτό το χαρακτηριστικό επιτρέπει σε έναν αναλυτή να εντοπίσει ποια δεδομένα έχουν εντοπιστεί από την υπηρεσία τοπικά και ποια έχουν εμπλουτιστεί από την υπηρεσία, μέσω του νέφους.



Εικόνα 16

Οι συσχετισμοί που αναφέρονται σε ένα γράφημα επιτρέπει σε έναν αναλυτή να συγκεντρωθεί σε συγκεκριμένα μεταδεδομένα και συσχετισμούς (εικόνα 17):

- Local: Εμφανίζει τα δεδομένα που εντοπίσθηκαν στην τοπική υποδομή IBM QRadar
- QRAW Enriched: Εμφανίζει τα μεταδεδομένα που εντοπίστηκαν κατά τον εμπλουτισμό μέσω των αυτόματων ευφυών αναζητήσεων που εκτελεί η υπηρεσία.
- New Local Context: Επιπρόσθετα μεταδεδομένα ή τεχνικές που εντοπίσθηκαν στην τοπική υποδομή του QRadar μέσω των εμπλουτισμένων μεταδεδομένων

Εικόνα 17

Η επιλογή New Local Context παρέχει σε έναν αναλυτή να εντοπίσει νέα κακόβουλη δραστηριότητα που ενδέχεται να μην είχε εντοπιστεί στο παρελθόν. Θα πρέπει να επισημάνουμε ότι συνήθως ένας εισβολέας σπάνια επιτίθεται σε ένα μόνο σύστημα και η επίθεση να διαρκέσει μία ημέρα. Για να εντοπίσουμε έναν περιστατικό ασφαλείας πρέπει να αναλύσουμε τα συμβάντα ασφαλείας σε βάθος ώστε να βρεθεί η έκταση και το εύρος του.

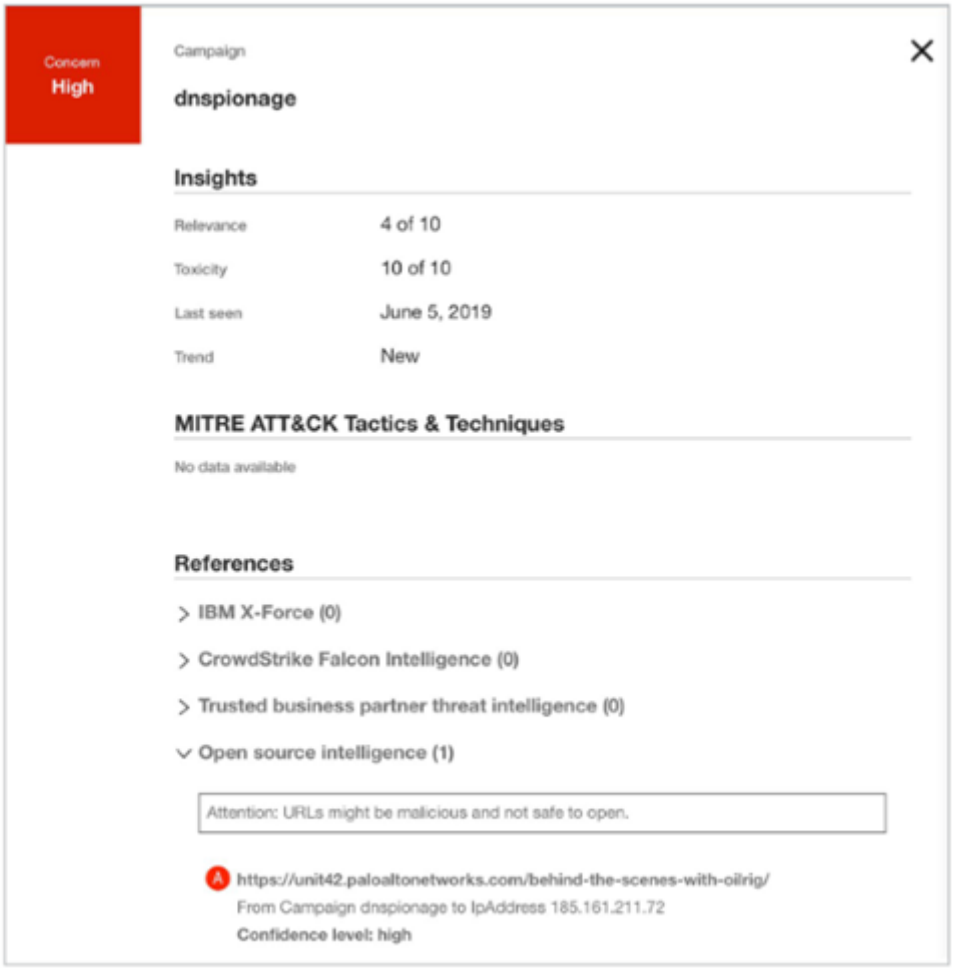
Η εν λόγω υπηρεσία αντιστοιχεί σε κάθε περιστατικό μία διερεύνηση και συλλέγει τις απαραίτητες πληροφορίες του περιστατικού από την τοπική υποδομή QRadar. Στη συνέχεια εμπλουτίζει τα τις πληροφορίες ενός περιστατικού με

νέες που εντοπίζει μέσω ευφυών αναζητήσεων σε νέφη υπηρεσιών ασφαλείας και τέλος εκτελεί επιπλέον αναζητήσεις, για κακόβουλη δραστηριότητα στην τοπική υποδομή χωρίς να αλλάξουμε οθόνη.

Η ανάλυση και η γραφική παράσταση συνδέσμων της υπηρεσίας επιτρέπει επίσης στους αναλυτές να αναλύουν τα χαρακτηριστικά της επίθεσης και εντοπίζουν συγκεκριμένες τακτικές και τεχνικές σύμφωνα με το MITRE ATT &CK (Εικόνα 18).

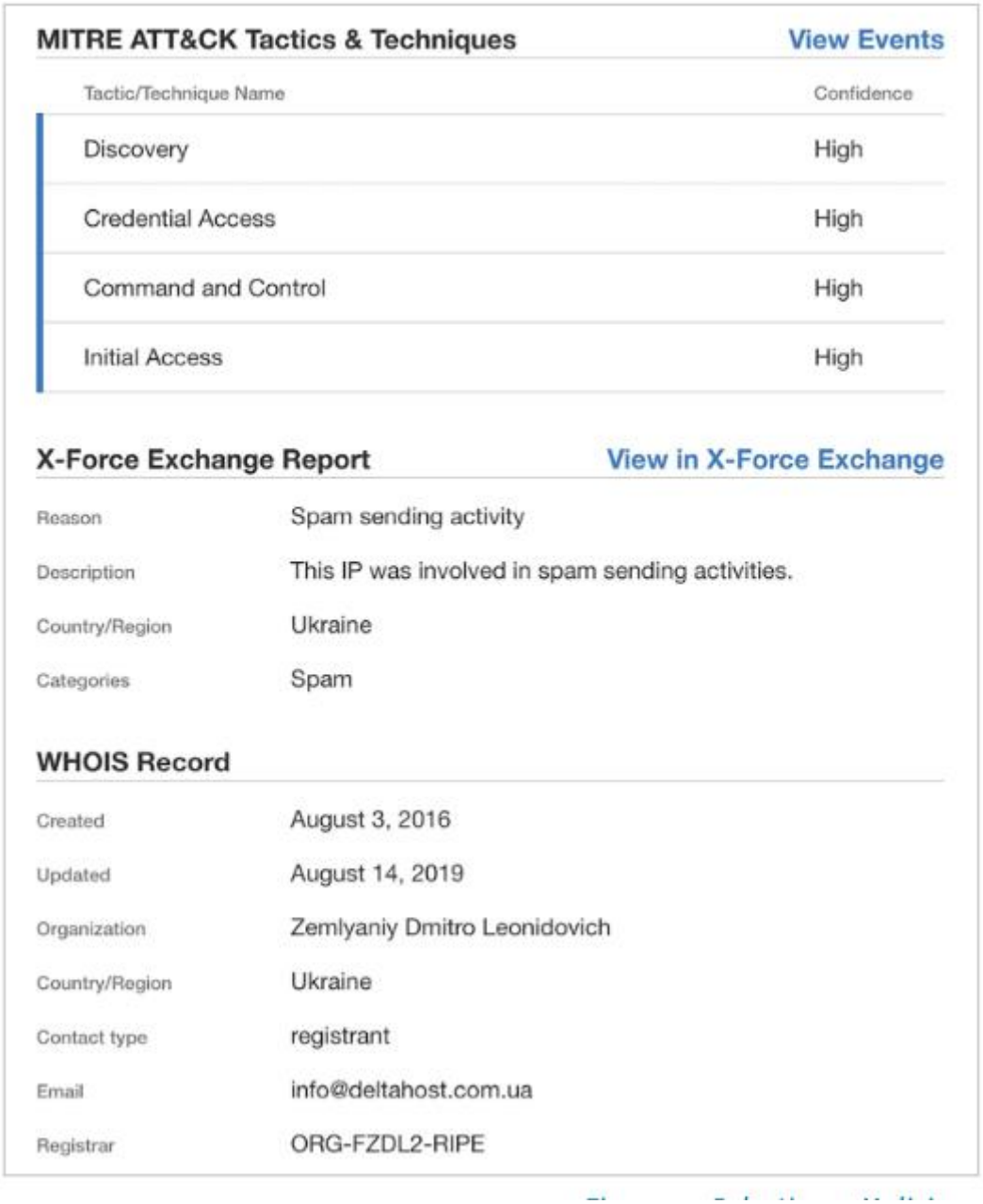
Εικόνα 18

Το γράφημα είναι διαδραστικό, και παρέχει άμεσες πληροφορίες για ένα περιστατικό. Παραδείγματος χάρη, η επιλογή του κόμβου "dnspionage", παρέχει τα μεταδεδομένα που συσχετίζονται με τον εν λόγω κόμβο (Εικόνα 19).



Εικόνα 19

Επιλέγοντας επίσης μία από τις κακόβουλες διευθύνσεις IP, όπως φαίνεται στην εικόνα 20, μας παρέχει ακόμα περισσότερες πληροφορίες για την εν λόγω IP που ένας αναλυτής θα έπρεπε να καταναλώσει επιπρόσθετο χρόνο και κόπο για τις εντοπίσει.



Εικόνα 20

Τέλος, η εν λόγω υπηρεσία, ανάλογα με τον τύπο του περιστατικού, μας παρέχει συμβουλές αποκατάστασης και απόκρισης.

3.2.2.2 Real Time Threat Management 24x7

Το τεχνικό προσωπικό της εταιρείας θα παρακολουθεί σε πραγματικό χρόνο 24x7 όλες τις επιθέσεις προς τον ιστότοπο της ΕΛΣΤΑΤ, με χρήση της κατάλληλης πλατφόρμας και ανάλογα με τον τύπο του περιστατικού θα προβαίνει στις απαραίτητες ενέργειες αντιμετώπισης του.

Οι ενέργειες αυτές συμπεριλαμβάνουν, μεταξύ άλλων, τις ενέργειες ενημέρωσης, επικύρωσης, προτεραιοποίησης, αντιμετώπισης και διερεύνησης του εκάστοτε ύποπτου ή/και επιβεβαιωμένου περιστατικού ασφαλείας, με χρήση μηχανισμών AI.

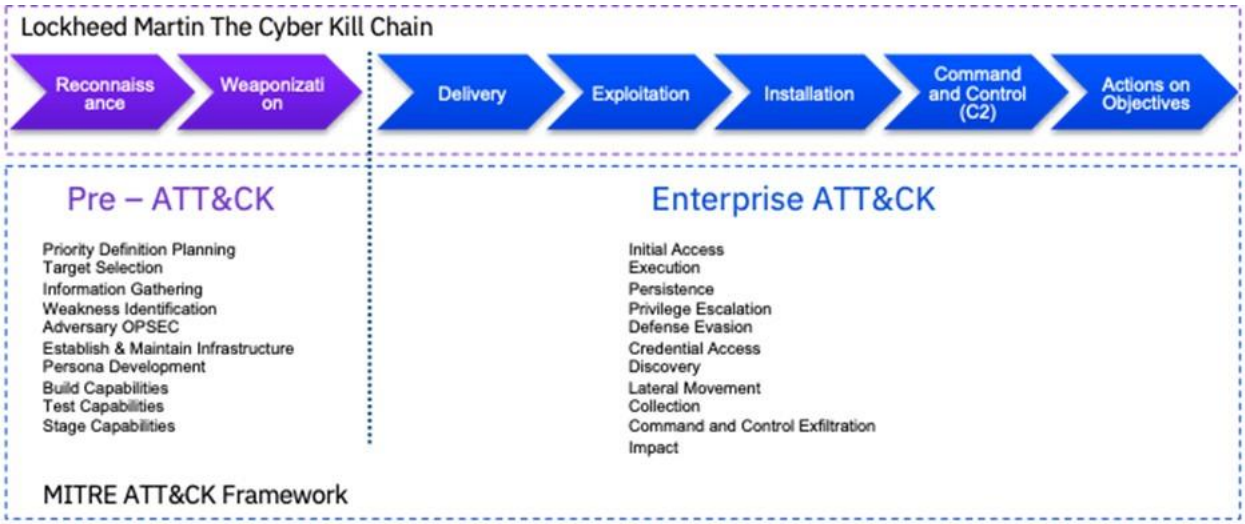
Σε περίπτωση που ανιχνευθεί ένα περιστατικό ασφαλείας, οι αναλυτές θα ενημερώνουν άμεσα το κατάλληλο προσωπικό της ΕΛΣΤΑΤ, μέσω e-mail, τηλεφώνου, sms σύμφωνα με το SLA και θα προβαίνουν στις ενέργειες αντιμετώπισης του σύμφωνα με το σχέδιο που θα έχει καταρτιστεί και συμφωνηθεί.

3.2.2.3 Περιπτώσεις Χρήσης (use cases)

Οι υπηρεσίες μας έχουν δομηθεί στις περιπτώσεις χρήσης (use cases) και στην δημιουργία εξατομικευμένων κανόνων συσχετισμού σύμφωνα με τις απαιτήσεις και τις ιδιαιτερότητες των πληροφοριακών συστημάτων ενός Φορέα. Οι περιπτώσεις χρήσης σχεδιάζονται ανά πελάτη και βασίζονται:

- Στις IT υποδομές
- Στις απαιτήσεις ασφαλείας
- Στους επιχειρησιακούς κανόνες και τέλος
- Στα κανονιστικά πλαίσια συμμόρφωσης

Για την δημιουργία σεναρίων επίθεσης η εταιρεία μας χρησιμοποιεί τα framework MITRE ATT & CK και το Cyber Kill Chain (Lockheed Martin). Και τα δύο πλαίσια χωρίζονται σε δύο ενότητες: πριν και μετά την επίθεση. Η ενότητα πριν-την-επίθεση περιλαμβάνει όλα τα σενάρια επίθεσης και τους κανόνες που σχετίζονται με την επιλογή στόχου και την εύρεση τρωτών σημείων. Η ενότητα μετά-την-επίθεση περιλαμβάνει όλα τα σενάρια επίθεσης και τους κανόνες που σχετίζονται με την παράδοση, την εκτέλεση, τη σύνδεση και την εξαγωγή.



Έχουμε σχεδιάσει και υλοποιήσει πάνω από 800 use cases τα οποία σχετίζονται με την αναγνώριση πλήθους περιστατικών ασφαλείας όπως Common Security Threats, Advanced Security Threats, Perimeter Threats, Insider Threats. Ενδεικτικά αναφέρονται οι ακόλουθες περιπτώσεις χρήσης.

Κατηγορίες Use Cases / Πηγές Δεδομένων	Advanced Persistent Threat	Insider Threat	Securing the Cloud	Critical Data Protection	Incident Response	Compliance	Risk and Vulnerability Management	Perimeter Threats	Common Security Threats
Firewall/Router	✓		✓	✓	✓	✓	✓	✓	✓
IDS/IPS (Intrusion Detection System/Intrusion Protection System)	✓			✓	✓		✓	✓	✓
VPN	✓							✓	✓
DNS	✓	✓					✓	✓	✓
Mail Logs	✓	✓		✓				✓	✓
DLP (Data Loss Prevention)	✓	✓		✓		✓			
Endpoint	✓	✓		✓		✓	✓		✓
Identity/Authentication(LDAP/AD/Radius)	✓	✓	✓		✓				✓
Endpoint Security	✓			✓	✓	✓	✓	✓	✓
Database Logs/Guardium	✓	✓	✓	✓	✓	✓			✓
EDR	✓				✓		✓	✓	
Cloud Infrastructure /Audit (Azure Event Hubs)	✓	✓	✓	✓		✓			✓
Office 365			✓		✓	✓			✓

3.2.2.4 Αναφορές

Μια φορά το μήνα η εταιρεία μας, θα υποβάλλει έκθεση στην οποία θα συνοψίζονται τα περιστατικά ασφάλειας και η συνολική κατάσταση του περιβάλλοντος του Οργανισμού κατά την περίοδο αναφοράς. Η αναφορά θα συντάσσεται σε επιχειρηματική γλώσσα που μπορεί να γίνει κατανοητή από μη τεχνικό κοινό.

Μέσω των προσφερόμενων υπηρεσιών SOC μπορούμε να δημιουργήσουμε προσαρμοσμένες αναφορές ή να χρησιμοποιήσετε τις ήδη προεπιλεγμένες αναφορές. Η υπηρεσία μας παρέχει προεπιλεγμένα πρότυπα αναφοράς που μπορούμε να προσαρμόσουμε, να μετονομάσουμε και να αποστείλουμε μέσω e-mail. Τα πρότυπα αναφοράς ομαδοποιούνται σε τύπους αναφορών, όπως αναφορές συμμόρφωσης, συστημάτων, επιτελικής σύνοψης και δικτύου. Η υπηρεσία αναφορών παρέχει τα ακόλουθα:

- Δημιουργία, διανομή και διαχείριση αναφορών
- Δημιουργία προσαρμοσμένων αναφορών
- Συνδυασμός πληροφοριών ασφάλειας και δικτύου σε μια ενιαία αναφορά.
- Χρήση και επεξεργασία πρότυπων αναφοράς.
- Εισαγωγή του λογότυπου της εταιρεία σας στις αναφορές.
- Χρονοπρογραμματισμός για τη δημιουργία των προσαρμοσμένων και προεπιλεγμένων αναφορών.
- Υποστήριξη αναφορών σε διάφορα μορφότυπα αναφορών σε διάφορες μορφές όπως .pdf,html, xml κ.λπ.

3.2.2.5 Σύγχρονο Κέντρο Επιχειρήσεων της Ασφάλειας Πληροφοριών

Οι υπηρεσίες παρέχονται από το SOC, το οποίο έχει σχεδιαστεί με στόχο να βοηθήσει τους οργανισμούς να εντοπίζουν έγκαιρα τις απειλές, πριν αυτές καταφέρουν να παραβιάσουν τους μηχανισμούς προστασίας.

Καινοτομία και τεχνολογίες IT, όπως για παράδειγμα το cloud, τα social media, τα Big Data και το mobile computing, βοηθούν τους οργανισμούς να κινηθούν προς το μέλλον, ταυτόχρονα όμως, δημιουργούν περισσότερες ευκαιρίες για όσους κακόβουλους βάζουν στόχο να παρακάμψουν τα συστήματα προστασίας, παλιά ή σύγχρονα. Συνδυάζοντας πληροφορίες ασφαλείας, διαχείριση events, και δυνατότητες εντοπισμού απειλών σε οποιοδήποτε σημείο (endpoint) του δικτύου και εξειδικευμένο προσωπικό, το Κέντρο σχεδιάστηκε με στόχο να βοηθήσει τους υπεύθυνους ασφαλείας να εντοπίζουν γρήγορα επιθέσεις οι οποίες συχνά δεν μπορούν να ανιχνευθούν και να διαχειριστούν από την IT ομάδα ενός Οργανισμού.

Ενσωματώνοντας τεχνολογίες από IBM Cisco, RSA κ.λπ. το adacom SOC ικανοποιεί τις απαιτήσεις συμμόρφωσης και ασφαλείας IT, δίνοντας έτσι τη δυνατότητα στους Οργανισμούς να εντοπίζουν και να αντιμετωπίζουν πιο αποτελεσματικά τις πλέον προηγμένες απειλές, πριν αυτές προκαλέσουν αρνητικές επιπτώσεις στη δραστηριότητα της επιχείρησης.

3.2.2.5.1 Εξειδικευμένο Προσωπικό

Όλοι οι αναλυτές έχουν πολυετή εμπειρία σε θέματα δικτυακής ασφάλειας σε πραγματικά περιβάλλοντα εργασίας όπου διερευνούν και αναλύουν την δραστηριότητα ασφαλείας. Οι υπηρεσίες ασφαλείας που προσφέρουμε στους

πελάτες περιλαμβάνουν την υποστήριξη και τις συμβουλευτικές υπηρεσίες από την ομάδα ασφάλειας. Όταν ανιχνεύεται ένα περιστατικό η ομάδα παίρνει τα κατάλληλα μέτρα για να αντιμετωπίσει την απειλή πριν προκαλέσει οποιαδήποτε επίπτωση στον οργανισμό.

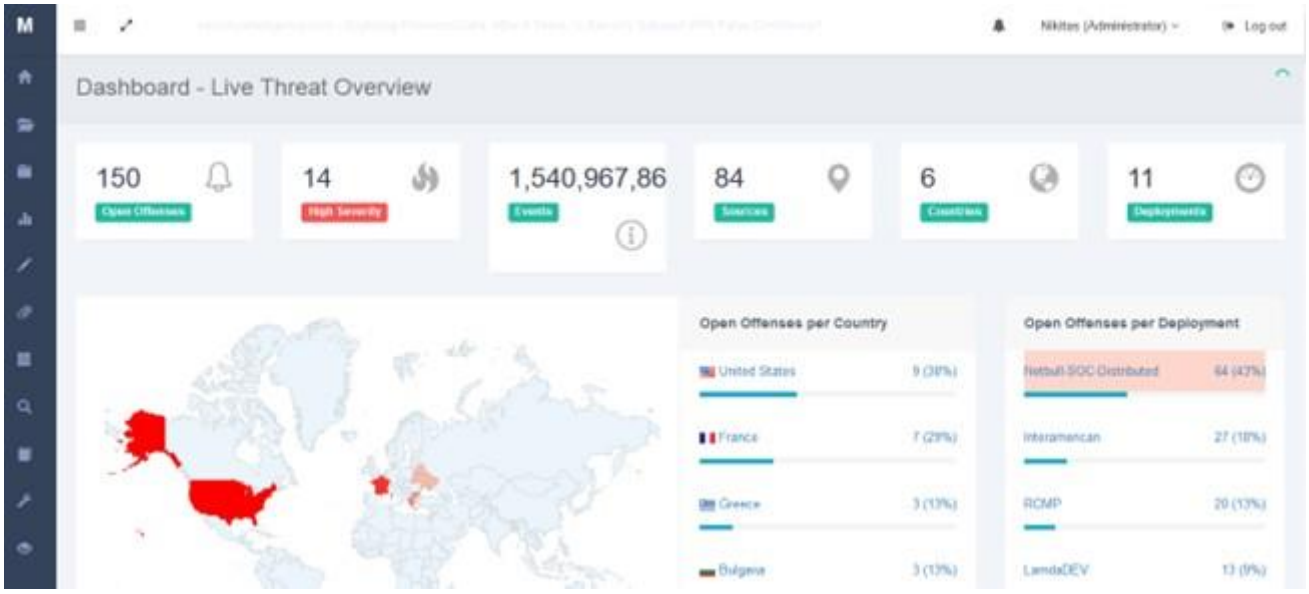
Οι αναλυτές εργάζονται σε ένα ομαδικό περιβάλλον κάνοντας άμεσο και ακριβή, τον εντοπισμό και την απόκριση στα περιστατικά ασφαλείας.

Οι ρόλοι και οι αρμοδιότητες του προσωπικού του SOC είναι:

- SOC Manager: Υπεύθυνος διαχείρισης του SOC
- L1 Security Analyst: Παρακολούθηση των περιστατικών ασφαλείας
- L2 Security Analyst: Διαχείριση των περιστατικών Ασφαλείας και επικοινωνία με τον πελάτη
- L3 Security Analyst: Ανάλυση (forensics) των περιστατικών ασφαλείας όπως malware analysis, packet capturing, use cases κ.λπ.
- SIEM Engineer: Εγκατάσταση και βελτιστοποίηση της πλατφόρμας SIEM

3.2.2.5.2 Web Portal

Κάθε πελάτης διαθέτει την δική του πύλη στις υπηρεσίες SOC, μέσω της οποίας έχει πρόσβαση στις πληροφορίες ασφαλείας όπως ανοιχτά περιστατικά ασφαλείας σε πραγματικό χρόνο, τρωτά σημεία, συμμόρφωση με κανονιστικά πρότυπα κ.λπ. όποτε το θελήσει. Η πύλη είναι προσβάσιμη μέσω ισχυρών μηχανισμών πιστοποίησης και κρυπτογράφησης μέσω του πρωτοκόλλου TLS. Επιπροσθέτως μέσω της πύλης είναι δυνατή η πρόσβαση στην κονσόλα για εξειδικευμένες λειτουργίες.



Εικόνα 21: Web Portal

3.2.2.5.3 Δυνατότητα συνεχούς βελτιστοποίησης της παρεχόμενης υπηρεσίας

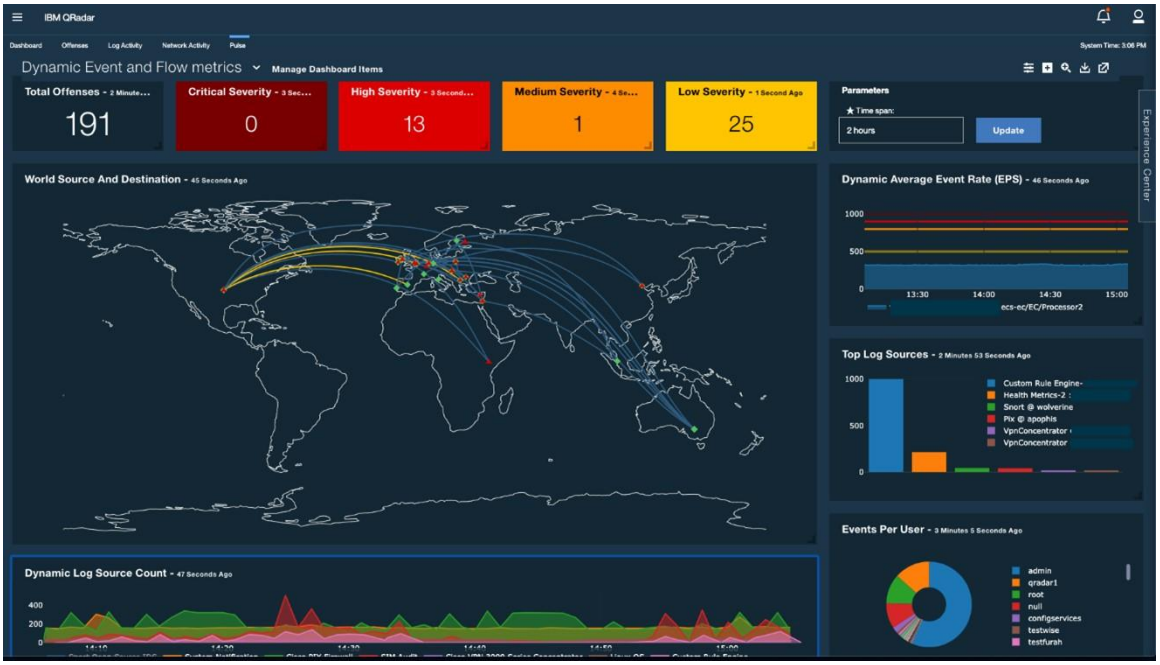
Η εταιρεία μας θα παρέχει την υπηρεσία συνεχούς βελτιστοποίησης της υπηρεσίας μέσω των κάτωθι περιπτώσεων:

- Έλεγχος ορθής λειτουργίας
- Τροποποίηση των κανόνων και των πιθανών σεναρίων (use cases) και δημιουργία νέων όποτε κριθεί αυτό απαραίτητο
- Μείωση των False posotives/False negatives
- Διαχείριση της απόδοσης
- Ακριβή προσαρμογή των logs, των πολιτικών και της υποδομής που περιλαμβάνεται
- Ενσωμάτων νέων συστημάτων /log sources
- Προληπτικός προσδιορισμός του τοπίου απειλών
- Προτάσεις για την συνεχή βελτίωση της υπηρεσίας

Η εταιρεία μας θα εκπαιδεύσει το εντεταλμένο προσωπικό της ΕΛΣΤΑΤ στη χρήση του portal με πρόγραμμα εκπαίδευσης

3.2.2.6 Πλατφόρμα SIEM IBM QRadar

Η καρδιά της υπηρεσίας αυτής είναι η λύση IBM QRadar η οποία παρέχεται ως υπηρεσία από την εταιρεία μας. Η εν λόγω λύση είναι μια ολοκληρωμένη λύση SIEM είναι στους Leaders της Gartner και ενοποιεί γεγονότα ασφαλείας από χιλιάδες πηγές καταγραφής, αποθηκεύει κάθε γεγονός σε πρωτογενή μορφή και τέλος συσχετίζει όλα τα γεγονότα μεταξύ τους ώστε να διακρίνει τις πραγματικές απειλές από τις ψευδείς.



Εικόνα 22: IBM QRadar

Η υλοποίηση της λύσης θα ακολουθεί τις ακόλουθες βασικές αρχές:

- Συλλογή περιστατικών ασφαλείας ή σχετικών με την ασφάλεια από το σύνολο της πληροφορική υποδομή της εταιρείας όπως: τα λειτουργικά συστήματα (Windows, Unix, Linux, …), τους μηχανισμούς-συστήματα ασφάλειας, τις βάσεις δεδομένων, τις εφαρμογές, και τον δικτυακό εξοπλισμό.

- Αυτοματοποιημένη Συλλογή και Ασφαλής Αποθήκευση των δεδομένων καταγραφής (logs) από τα διάφορα συστήματα και εφαρμογές του ευρύτερου εταιρικού δικτύου σε κεντρικό. Η προτεινόμενη λύση ασφάλειας ως υπηρεσία θα αποθηκεύει τα δεδομένα καταγραφής από ολόκληρη την πληροφορική υποδομή του οργανισμού σε συμπιεσμένη μορφή για περαιτέρω ανάλυση και επεξεργασία.

Πιο συγκεκριμένα η εν λόγω υπηρεσία θα παρέχει τις ακόλουθες λειτουργίες και χαρακτηριστικά:

- Ομοιόμορφη διαμόρφωση (κανονικοποίησης) των δεδομένων καταγραφής ανεξαρτήτως του συστήματος προέλευσης και αποθήκευσης αυτών με την ίδια δομή με σκοπό την επιτάχυνση των μηχανισμών επεξεργασία, αναζήτησης και παραγωγής αναφορών (normalization).
- Παράλληλη συλλογή και αποθήκευση δεδομένων καταγραφής τόσο σε πρωτογενή μορφή (raw data) όσο και σε κανονικοποιημένη μορφή (normalized).
- Ομαδοποίηση των πηγών των logs ανά είδος πηγής (π.χ. web server, router) και ανά διαχειριστικό τομέα (π.χ. δίκτυο IP, δίκτυο IP core, NMS admins). Να τεκμηριωθεί αναλυτικά.
- Άντληση δεδομένων καταγραφής από κάθε πληροφορικό σύστημα ή εφαρμογή της υποδομής, ανεξαρτήτως κατασκευαστή, όπως:Συστήματα ασφάλειας (Firewalls, IDS/IPS, Content Security systems, VPNs, Vulnerability scanners, Antivirus servers, AAA servers, NAC κ.α.), Συσκευές Δικτύου(Routers, Switches, Λειτουργικά Συστήματα, Βάσεις Δεδομένων, Directory Services, Web Servers, Applications
- συλλογή δεδομένων καταγραφής από οποιαδήποτε πηγή δεδομένων καταγραφής (σύστημα ή εφαρμογή) στο δίκτυο.
- ασφαλής συλλογή και αποθήκευση των δεδομένων στο σύστημα η οποία περιλαμβάνει:
- έλεγχο ακεραιότητας αποθηκευμένων δεδομένων
- έλεγχος πρόσβασης στα αποθηκευμένα δεδομένα
- αυτοματοποιημένες πολιτικές διατήρησης των δεδομένων στο σύστημα (log retention policies)
- εξελιγμένη αναζήτηση ανάμεσα στα αποθηκευμένα δεδομένα και παραγωγή σχετικών αναφορών.
- Απόδοση >= 2.500 EPS (Events- per-second).
- Δυνατότητες συμπίεσης δεδομένων.
- Εύχρηστο περιβάλλον διαχείρισης
- Συσχετισμό (correlation) των περιστατικών τα οποία έχουν συλλεχθεί από τις διάφορες πηγές, με σκοπό την ελαχιστοποίηση των λάθος συναγερμών (false alarms) και την ανάδειξη των πραγματικά κρίσιμων περιστατικών ασφάλειας.
- Η λειτουργία του μηχανισμού συσχέτισης θα βασίζεται σε μια σειρά προκαθορισμένων πολιτικών και κανόνων συσχέτισης οι οποίοι εφαρμόζονται σε πραγματικό χρόνο σε όλα τα περιστατικά τα οποία συλλέγονται από τους διάφορους πληροφοριακούς πόρους του δικτύου. Σκοπός του μηχανισμού θα είναι η ανάδειξη των πραγματικών απειλών και η υποβάθμιση των μη σχετικών με την ασφάλεια ή χαμηλής επικινδυνότητας περιστατικών. Παραδείγματα τέτοιων κανόνων συσχέτισης είναι:
    - Τύπος επίθεσης (τον οποίο έχει ανιχνεύσει το σύστημα) με Τύπο συστήματος (έκδοση λειτουργικού)

- Τύπος επίθεσης (τον οποίο έχει ανιχνεύσει το σύστημα) με Εγκατεστημένες ενημερώσεις (Patch level) στο σύστημα
- Περιστατικό Ασφαλείας με Ώρα της ημέρας
- Περιστατικό Ασφαλείας με Χρήστη
- Περιστατικά σε επίπεδο Web server με περιστατικά σε επίπεδο DB server κ.α.

- Αρχιτεκτονική η οποία παρέχει ενσωμάτωση επιπρόσθετων πληροφοριακών πόρων (συστημάτων, εφαρμογών) και περαιτέρω επέκτασης της υποδομής στο μέλλον.
- Εύκολη και γρήγορη αναζήτηση ανάμεσα στα αποθηκευμένα δεδομένα καταγραφής και παραγωγή σχετικών αναφορών με εφαρμογή ειδικών φίλτρων.
- Εφαρμογή κανόνων συσχέτισης (correlation rules) σε πραγματικό χρόνο και καθώς τα δεδομένα καταγραφής εισέρχονται στο κεντρικό σύστημα επεξεργασίας.
- Παροχή έτοιμων κανόνων συσχέτισης για την άμεση ανάδειξη σημαντικών θεμάτων ασφάλειας της υποδομής.
- Γρήγορη και εύκολη δημιουργία κανόνων συσχέτισης χρησιμοποιώντας ως βάση τους έτοιμους κανόνες που παρέχει η λύση.
- Λεπτομερής εξέταση των γεγονότων καταγραφής που προκαλούν την ενεργοποίηση ενός κανόνα, με επιλογή γραφικής αναπαράστασης της σειράς των γεγονότων.
- Εφαρμογή κανόνων συσχέτισης δεδομένων καταγραφής από διαφορετικές πηγές (συστήματα και εφαρμογές).
- Δημιουργία και αποστολή ειδοποιήσεων (alerts) σε καθορισμένους χρήστες, σε μορφή email.
- Παραγωγή alerts με βάση τη συχνότητα και τον χρόνο εμφάνισης κάποιου γεγονότος, καθώς επίσης και όταν κάποιος κανόνας πληρείται
- Δυνατότητα ιεράρχησης της υπό παρακολούθηση υποδομής βάσει των ιδιαίτερων χαρακτηριστικών των συστημάτων και εφαρμογών καθώς και της χρησιμοποίησης αυτών στην δημιουργία κανόνων συσχέτισης.Τα χαρακτηριστικά αυτά θα μπορούν να καθορίζουν την κρισιμότητα και κατηγοριοποίηση των παραγόμενων ειδοποιήσεων (alerts).
- Παραγωγή ειδοποίησης (alert) όταν κάποια πηγή logs σταματήσει να στέλνει logs για ορισμένο χρονικό διάστημα.
- Δημιουργία αναφορών προσαρμοσμένων στις απαιτήσεις και ανάγκες του χρήστη (custom reports) χρησιμοποιώντας ως παράμετρο κάθε είδους πληροφορία η οποία περιέχεται στα δεδομένα καταγραφής

- Υποστήριξη εξαγωγής δεδομένων (επεξεργασμένων και μη) σε xls, pdf, rtf, html και xml
- Υποστήριξη User Behavior Analysis τεχνολογίας
- Υποστήριξη Machine-Learning τεχνολογίας
- Υποστήριξη Anomaly Detection τεχνολογίας

3.2.2.6.1 Περιγραφή της λύσης

Η προτεινόμενη υπηρεσία βασίζεται στο λογισμικό IBM QRadar που υποστηρίζει την ταυτόχρονη και σε πραγματικό χρόνο (real time) παρακολούθηση, ανάλυση και καταγραφή συμβάντων από ετερογενείς υποδομές.

Απειλές και απάτες που προέρχονται από το Internet, αλλά και από εσωτερικούς κινδύνους, συνεχίζουν να πολλαπλασιάζονται με ταχύς ρυθμούς σε περιβάλλονται που χαρακτηρίζονται από ολοένα αυξανόμενη πολυπλοκότητα. Αυτό το πρόβλημα εντείνεται περισσότερο, καθώς όλο και πιο συχνά παρατηρείται η υποκλοπή εμπιστευτικών πληροφοριών που είναι σημαντικές.

Η προτεινόμενη υπηρεσία IBM QRadar ενοποιεί αποσπασματικές πληροφορίες, προερχόμενες από διαφορετικές μεταξύ τους πηγές, με σκοπό να ανιχνεύσει και να διαχειρισθεί πιο αποτελεσματικά πολύπλοκες απειλές. Οι πληροφορίες που συλλέγονται συσχετίζονται σε πραγματικό χρόνο, με αποτέλεσμα να είναι εφικτή η δυνατότητα απόκρισης σε σύνθετες απειλές, που συνήθως είναι απαρατήρητες από άλλα συστήματα ασφαλείας με περιορισμένη ορατότητα στο δίκτυο ενός Οργανισμού.

Η προτεινόμενη υπηρεσία θα βοηθήσει να:

- Ανιχνεύσει και να αποκαταστήσει απειλές όπως ακατάλληλη χρήση εφαρμογών, κλοπή εμπιστευτικών πληροφοριών, επικίνδυνες αλλαγές σε παραμέτρους των συστημάτων
- Πιστοποιηθεί με βάση κανονιστικές αρχές, όπως το ISO27000, για την παρακολούθηση των γεγονότων στις υποδομές

Υποστηρίζονται πλήρως οι ακόλουθες υποδομές:

- Security Events - Συμβάντα που προέρχονται από Firewalls, VPNs, IDS/IPS, switches κλπ
- Network Activity Context – Παρακολούθηση κίνησης εφαρμογών από φυσικά και εικονικά δίκτυα σε διάφορα επίπεδα (έως και Layer 7)
- User / Asset Context – Contextual data από Identity Access Management συστήματα και Vulnerability Scanners
- Network events - Συμβάντα από switch, routers, servers, hosts, κα
- Application Logs - ERP, Custom Applications, workflows, Βάσεις Δεδομένων, Πλατφόρμες Διαχείρισης, Εξυπηρετητές Εφαρμογών (Oracle, WebSphere, Tomcat, JBoss, κα)

Η προτεινόμενη υπηρεσία συλλέγει, αποθηκεύει και παρέχει σε πραγματικό χρόνο συσχετίσεις μεταξύ συμβάντων με σκοπό την ανίχνευση απειλών αλλά και τη συμμόρφωση με κανονισμούς για reporting και auditing.

Εκατομμύρια συμβάντα και ροές ασφάλειας μπορούν να κατηγοριοποιηθούν και να ταξινομηθούν σύμφωνα με την επίδραση και τον αντίκτυπο που έχουν στην λειτουργία της επιχείρησης και αντιστοίχως να αντιμετωπισθούν με κατάλληλες ενέργειες.

Παρέχει μακροπρόθεσμη συλλογή, αρχειοθέτηση, αναζήτηση και καταγραφή των γεγονότων και των δεδομένων των εφαρμογών καθιστώντας ευκολότερο τον έλεγχο και την αναζήτηση για σύνθετες επίμονες απειλές (persistent attacks) που συνήθως πραγματοποιούνται σε βάθος χρόνου.

Η εν λόγω υπηρεσία έχει μια ολοκληρωμένη μηχανή συσχέτισης συμβάντων ασφαλείας, η οποία ενεργεί σε πραγματικό χρόνο σε κάθε Event processor και/ή Flow processor. Ο σκοπός είναι να γίνεται γρήγορα η

κανονικοποίηση και η συσχέτιση των δεδομένων που λαμβάνονται από τα επιμέρους log sources. Η κανονικοποίηση, η συσχέτιση και η ειδοποίηση γίνεται σε κάθε Event processor appliance. Η λύση IBM Qradar συλλέγει, επεξεργάζεται, συγκεντρώνει και αποθηκεύει δεδομένα δικτύου σε πραγματικό χρόνο. Το Qradar χρησιμοποιεί τα δεδομένα αυτά για τη διαχείριση της ασφάλειας του δικτύου παρέχοντας πληροφορίες και παρακολούθηση σε πραγματικό χρόνο, ειδοποιήσεις, offenses και απαντήσεις σε απειλές δικτύου.

3.2.2.6.2 IBM Qradar Δομικά Στοιχεία

Η λειτουργία της υπηρεσίας αποτελείται από τρία στρώματα τα οποία εφαρμόζονται σε οποιαδήποτε IT υποδομή, ανεξάρτητα από το μέγεθος και την πολυπλοκότητά. Πιο αναλυτικά:

Data Collection Layer – Η συλλογή δεδομένων είναι το πρώτο στρώμα, όπου συλλέγονται δεδομένα όπως γεγονότα ή ροές από το δίκτυο. Υπάρχουν διάφοροι τρόποι με τους οποίους οι πληροφορίες μπορούν να συλλεχθούν για να σταλούν στο κεντρικό στρώμα επεξεργασίας. Όταν έχουμε λίγα παραγόμενα από την πηγή γεγονότα, είναι δυνατή η αποστολή των αρχείων καταγραφής (logs) ή ροών (flows) απευθείας στον επεξεργαστή συμβάντων QRadar (Event processor). Ένας άλλος τρόπος για μεγαλύτερους όγκους συλλογής είναι να συλλέγονται τα αρχεία καταγραφής συλλέκτες όπως οι QRadar Event Collectors ή QRadar flow collectors για τη συλλογή δεδομένων συμβάντων ή ροών αντίστοιχα. Τα δεδομένα αναλύονται και κανονικοποιούνται πριν μεταφερθούν στο στρώμα επεξεργασίας.

Data Processing Layer – Μετά τη συλλογή δεδομένων, το δεύτερο επίπεδο είναι αυτό της επεξεργασίας δεδομένων. Εδώ τα δεδομένα συμβάντων και τα δεδομένα ροής εισάγονται στο Custom Rules Engine (CRE), το οποίο παράγει offenses και ειδοποιήσεις και στη συνέχεια τα δεδομένα αποθηκεύονται. Τα events και τα flows μπορούν να υποβληθούν σε επεξεργασία στο στρώμα επεξεργασίας συμβάντων. Ένα από τα κύρια χαρακτηριστικά της συγκεκριμένης πλατφόρμας είναι η ευελιξία στην υλοποίηση αλλά και στην αλλαγή καθώς μπορεί να αλλάξει ανάλογα με το πως μετατρέπονται και οι ανάγκες του οργανισμού στη διάρκεια του χρόνου. Συνεπώς είναι ιδιαιτέρως εύκολο να προστεθούνε επιπλέον επεξεργαστές συμβάντων ή οι επεξεργαστές ροής, ανάλογα με το πως αυξάνονται οι ανάγκες ενός οργανισμού. Έτσι, έχουμε περιπτώσεις υλοποιήσεων οι οποίες ξεκίνησαν από μια συσκευή, ένα All-in-One όπως ονομάζεται, χωρίς να χρειάζεται να προσθέσετε επεξεργαστές συμβάντων ή επεξεργαστές ροής και σε αργότερη φάση προστέθηκαν επιπλέον event processors και collectors ανάλογα με τα δεδομένα που είχαμε να διαχειριστούμε. Η λύση είναι πολύ ευέλικτη και υπάρχουν διάφοροι τρόποι υλοποίησης και εφαρμογής του Qradar σε μια ανάπτυξη. Ο βασικός μας στόχος είναι να χειρίζονται από τις πιο απλές έως τις πιο πολύπλοκες απαιτήσεις που μπορεί να θέσει ένας οργανισμός που αναζητά διαχειριζόμενες υπηρεσίες ασφαλείας.

Data Search Layer – Στο τρίτο και ανώτερο επίπεδο, τα δεδομένα που συλλέγονται και επεξεργάζονται από το QRadar. Από εδώ και πέρα είναι διαθέσιμα στους χρήστες για αναζητήσεις, αναλύσεις, αναφορές και ειδοποιήσεις ή έρευνα παράβασης. Οι χρήστες μπορούν να αναζητήσουν και να διαχειριστούν τις εργασίες τους από τη διεπαφή χρήστη στην κονσόλα QRadar. Η οπτική αναπαράσταση λειτουργικών δεδομένων, όπως η χρήση της CPU, η δραστηριότητα δικτύου και δίσκου, η χρήση της μνήμης και τα ποσοστά συμβάντων και ροών, καθιστά εύκολη την παρακολούθηση της υγείας της υλοποίησης. Η κεντρική κονσόλα διαχείρισης δείχνει τα offenses με βάση την

εσωτερική διαβάθμιση του συμβάντος όπως το κάνει το QRadar. Αυτό γίνεται με βάση το magnitude το οποίο υπολογίζει το εργαλείο με βάση τους εσωτερικούς μηχανισμούς του.

3.2.2.7 Υπηρεσία SOAR IBM Resilient

Η εταιρεία μας έχει ενσωματώσει μηχανισμούς ενορχήστρωσης, αυτοματισμού και απόκρισης στις υπηρεσίες MSS μέσω της πλατφόρμας SOAR IBM Resilient. Η εν πλατφόρμα, έχει συμβάλλει αποτελεσματικά στην βέλτιστη λειτουργία του SOC της εταιρεία μας, διότι έχοντας δημιουργήσει πολλαπλά playbooks και ροές εργασίας έχουμε αυτοματοποιήσει τις ενέργειες απόκρισης. Η προσφερόμενη υπηρεσία θα επιτρέπει στους εντεταλμένους υπαλλήλους της ΕΛΣΤΑΤ να δοκιμάζουν διαδικασίες απόκρισης σε περιστατικά ασφαλείας, επιτρέποντάς τους να εντοπίζουν τα όποια σχεδιαστικά κενά και να βελτιώνουν τις διαδικασίες τους πριν συμβεί ένα πραγματικό συμβάν. Η υπηρεσία που παρέχεται είναι μια κορυφαία υπρεσία ενορχήστρωσης και αυτοματοποίησης των διαδικασιών απόκρισης περιστατικών με μοναδικές δυνατότητες αυτοματοποίησης, αναφοράς και απορρήτου στο οποίο έχουμε ενσωματώσει ένας πλήθος υπηρεσιών του SOC όπως υπηρεσία Ticketing, alerting, web portal κ.λπ.
Τα κύρια χαρακτηριστικά της υπηρεσίας SOAR που παρέχουμε σε κάθε πελάτη είναι:

3.2.2.7.1 Δυναμικά Playbooks

Για να μετριάσουμε τον κίνδυνο και να ανταποκριθούμε καλύτερα στις κυβερνοεπιθέσεις έχουμε αναπτύξει τις απαραίτητες οδηγίες και ενέργειες για το πως θα αποκριθούν οι αναλυτές του SOC μας στους διάφορους τύπους περισταικών. Οι ροές και οι οδηγίες αυτές έχουν εισαχθεί στην πλατφόρμα IBM Resilient, με αποτέλεσμα την δημιουργία πολλαπλών δυναμικών playbooks, που αποτελούνται από μεμονωμένες ή πολλαπλές διακριτές ροές εργασιών (workflows), και παρέχουν στους αναλυτές μας καθοδηγούμενη απάντηση ανάλογα με τον Workflow and Collaboration
Η ανάγκη για συνεχής και επαναλαμβανόμενες διαδικασίες και συνεργασία των ομάδων είναι πιο επίκαιρη από ποτέ. Η ανάγκη για προστασία συνεχίζει να επεκτείνεται με περισσότερες συσκευές και οργανισμοί μετακινούν τις ροές εργασίας τους στο cloud και ενώ ομάδες ασφαλείας γίνονται και υποστηρίζουν απομακρυσμένο εργατικό δυναμικό.

3.2.2.7.2 Dynamic Workflows

Για να μετριάσουμε τον κίνδυνο και να ανταποκριθούμε καλύτερα στα cyberattacks, η εταιρεία μας έχει θεσπίσει και τεκμηριώσει διαδικασίες αντιμετώπισης συμβάντων για να παρέχει οδηγίες στους αναλυτές μας σχετικά με τον τρόπο απάντησης σε περιστατικά. Η υπηρεσία καταγράφει αυτές τις διαδικασίες σε workflows διαθέσιμες μέσω μιας drag-and-drop μηχανή ροής εργασιών διαχείρισης επιχειρησιακών διαδικασιών . Αυτό δίνει τη δυνατότητα στην εταιρεία μας να δημιουργήσει δυναμικά playbooks, που αποτελούνται από μεμονωμένες ή πολλαπλές διακριτές ροές εργασιών (workflows), που παρέχουν στους αναλυτές μας καθοδηγούμενη απόκριση βήμα προς βήμα, ενώ μέσω API επιτρέπει τον αποκλεισμό ενός εισβολέα.

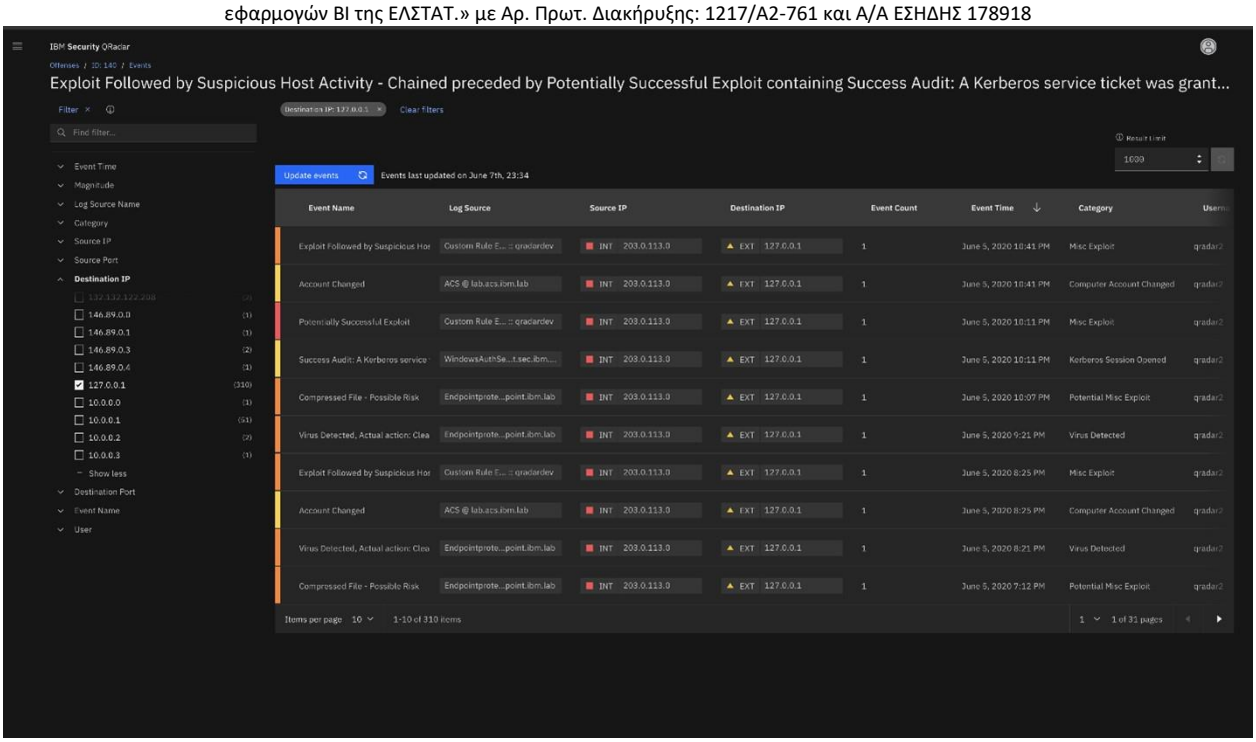
Προσφέρει μια ποικιλία από playbooks αντιμετώπισης περιστατικών έτοιμα για άμεση χρήση. Αυτό περιλαμβάνει προκαθορισμένες λίστες εργασιών που βασίζονται στο US National Institute of Standards and Technologies (NIST) και στις βέλτιστες πρακτικές του Ινστιτούτου SANS. Αυτά τα playbooks είναι μοναδικά στο ότι είναι δυναμικά και πρόσθετα. Προσαρμόζονται και αλλάζουν καθώς τα γνωστά γεγονότα εξελίσσονται κατά τη διάρκεια μιας έρευνας περιστατικού. Αυτός ο δυναμισμός είναι κρίσιμος για τους αναλυτές μας. Επιτρέπει να ακολουθήσουν μια προτεινόμενη πορεία δράσης και να περιστρέφεται όπως απαιτείται από την αλλαγή συμβάντων.

Οι κανόνες που επιτρέπουν τη δυναμική ικανότητα των playbooks βασίζονται σε συνθήκες που έχουν οριστεί από τον διαχειριστή. Μετά από οποιαδήποτε αλλαγή ή/και προσθήκη στις πληροφορίες περίπτωσης, αυτοί οι κανόνες επανεκτιμώνται και επιτρέπουν τον προγραμματισμό της απάντησης. Ως αποτέλεσμα, ο αρχιτέκτονας ασφαλείας σας μπορεί να δημιουργήσει απλά σχέδια που βασίζονται σε σενάρια αντί για υπερβολικά πολύπλοκες ροές εργασιών που πρέπει να ταιριάζουν σε όλες τις μεταβλητές. Η επεξεργασία κανόνων μπορεί να καλέσει μεμονωμένες εργασίες, να εκτελέσει ένα σύνολο ενεργειών και να ορίσει τιμές πεδίου, κάτι που είναι χρήσιμο για σενάρια κλιμάκωσης

Η προτεινόμενη λύση αυξάνει την ωριμότητα της ομάδας σας και γίνεται πολλαπλασιαστής δυνάμεων, αποτυπώνοντας αυτήν την καθιερωμένη και επαναλαμβανόμενη διαδικασία. Επιτρέπει στους αναλυτές ασφάλειας να μοιράζονται τις γνώσεις τους με την υπόλοιπη ομάδα, να αναπτύσσουν γρηγορότερα τις δεξιότητές τους και να ενισχύουν τη συνολική τους ικανότητα να ανταποκρίνονται σε περιστατικά, μειώνοντας συνεπώς το μέσο χρόνο ανταπόκρισης για τον οργανισμό.

3.2.2.7.3 Ticket and Case Management

Η εν λόγω υπηρεσία IBM Security SOAR παρέχει στους αναλυτές μας μια λύση ticketing systems μέσω ισχυρής διαχείρισης υποθέσεων. Ο κάθε οργανισμός μπορεί να δημιουργήσει, να κλιμακώσει και να διαχειριστεί περιστατικά μέσα από τη λύση. Οι αναλυτές μπορούν να ανατεθούν σε εργασίες με ημερομηνίες λήξης (αυτόματα ή χειροκίνητα). Έχουν ορατότητα για το πώς προχωρούν τα περιστατικά και πότε ολοκληρώνονται οι εργασίες. Μπορούν επίσης να διαχειριστούν πολλά περιστατικά μέσα από τη λύση και να τα εντοπίσουν εύκολα χρησιμοποιώντας έναν ισχυρό και ευέλικτο κινητήρα φίλτρων.



Εικόνα 23 Case Management

Μπορείτε να διαμορφώσετε ενέργειες για διάφορες ομάδες μέσω ενός λεπτομερούς ελέγχου πρόσβασης βάσει ρόλων. Αυτό είναι ιδιαίτερα χρήσιμο για εκείνα τα περιστατικά που απαιτούν περιορισμένη ορατότητα λόγω εμπορικής ευαισθησίας ή εμπιστευτικότητας των εργαζομένων. Όλη η δραστηριότητα του συστήματος είναι χρονικά σφραγισμένη, αποθηκευμένη και διαθέσιμη για σκοπούς ελέγχου. Για πιο περίπλοκα περιστατικά ασφάλειας, μπορείτε να αναπτύξετε την ομάδα σας όπως απαιτείται και να παρακολουθείτε

Το case management της λύσης έχει έναν flexible rule μηχανισμό . Σας επιτρέπει να ορίσετε κανόνες με εκτεταμένες επιλογές φίλτρου (π.χ. δημιουργία, αλλαγή, ίσο, όχι ίσο) σε τυχόν προεπιλεγμένα ή προσαρμοσμένα πεδία δεδομένων, πίνακες δεδομένων, περιστατικά, εργασίες, σημειώσεις, artifacts, συνημμένα κ.λπ., και για να ενεργοποιήσετε στη συνέχεια ενέργειες όπως, αλλά χωρίς περιορισμό:

- Προσθήκη πρόσθετων εργασιών συμβάντος
- Εκτέλεση σε δέσμες ενεργειών (ισχυρά σενάρια Python για άμεσο χειρισμό του τρόπου λειτουργίας της λύσης)
- Ρύθμιση πεδίου (αλλαγή πεδίων δεδομένων)
- Έναρξη ροών εργασίας εξωτερικού αυτοματισμού (ενσωματώσεις σε συστήματα τρίτων)

- Αυτό το ισχυρό Rule Engine επιτρέπει στους αναλυτές ασφάλειας να εστιάζουν σε εργασίες υψηλότερης αξίας, ενώ άλλες διαδικασίες ξεκινούν αυτόματα, όπως:
  - Οργανωτικές διαδικασίες για την ενημέρωση του C-Level ή άλλων τμημάτων (π.χ. HR, IT, νομικά κ.λπ.)
  - Έναρξη διαδικασιών εμπλουτισμού συμβάντων (προσθήκη IOC / τεχνουργήματα από ροές απειλών τρίτων)

- Έλεγχος διαχείρισης περιπτώσεων (π.χ., προσθήκη ή κατάργηση πρόσθετων εργασιών όταν προστίθενται τύποι συμβάντων)

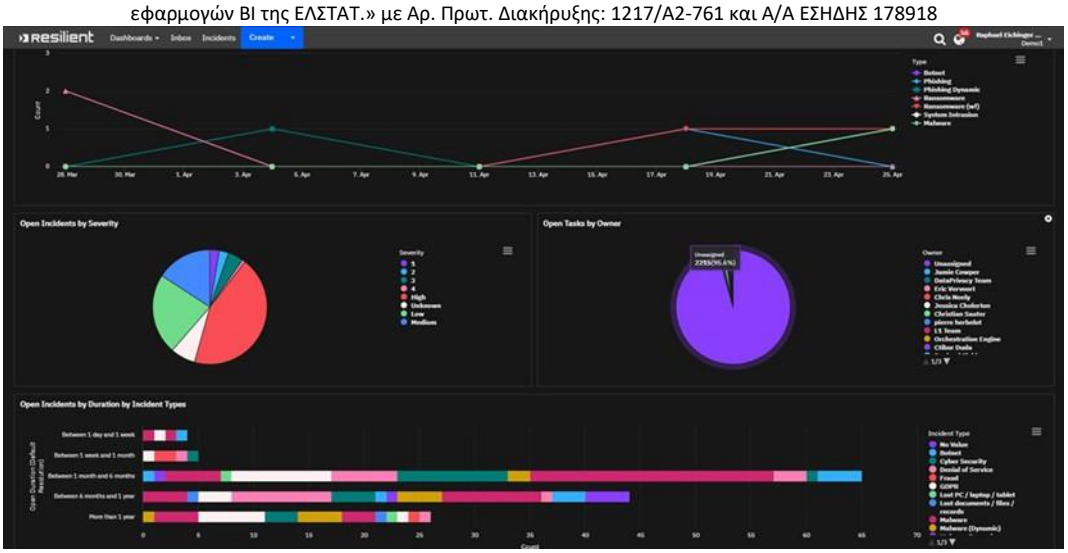
Οι δυνατότητες διαχείρισης περιπτώσεων IBM Security SOAR προσφέρουν έναν βήμα προς βήμα οδηγό με λεπτομερείς περιγραφές εργασιών που επιτρέπουν στους αναλυτές ασφάλειας να εργάζονται μέσω μιας έρευνας περιστατικών. Αυτή η διαχείριση υποθέσεων που βασίζεται σε εργασίες διασφαλίζει ότι δεν έχει παραληφθεί κανένα κρίσιμο βήμα. Επειδή τεκμηριώνει λεπτομερείς σημειώσεις του κάθε αναλυτή και βήματα που έγιναν κατά τη διάρκεια του κύκλου ζωής του συμβάντος, οι ομάδες παγκοσμίως μπορούν να συνεργαστούν γρήγορα και με ασφάλεια και να παραδώσουν περιστατικά ασφαλείας.

Η προτεινόμενη λύση έχει επίσης τη μοναδική δυνατότητα επέκτασης της διαχείρισης περιπτώσεων με την προσθήκη προσαρμοσμένων καθορισμένων πεδίων δεδομένων και πινάκων δεδομένων. Αυτά συμπληρώνονται αυτόματα με δεδομένα από οποιοδήποτε σύστημα τρίτων (Security Information and Event Management [SIEM], Endpoint Detection and Response [EDR], IT Service Management [ITSM], antivirus [AV], vulnerability scanner κ.λπ.). Ο αναλυτής μπορεί στη συνέχεια να αποκτήσει πρόσβαση στα δεδομένα που έχουν ληφθεί χρησιμοποιώντας προσαρμόσιμες views εντός του συμβάντος. Αυτό εξοικονομεί χρόνο στον αναλυτή εμπλουτίζοντας αυτόματα το περιστατικό χωρίς εναλλαγή μεταξύ διεπαφών άλλων εργαλείων ασφαλείας για τη συλλογή των πληροφοριών έρευνας.

3.2.2.7.4 Ορατότητα μέσω Dashboards και Reporting

Ο κάθε πελάτης μας έχει πρόσβαση σε πολύπλοκα dashboards και έτοιμα πρότυπα αναφοράς. Μπορείτε να παρακολουθεί μετρήσεις και KPI, συμπεριλαμβανομένου του ενδιάμεσου εντοπισμού (MTTD) και του χρόνου ανταπόκρισης (MTTR).

Η προσφερόμενη υπηρεσία επιτυγχάνει αυτό το επίπεδο λεπτομερειών μέσω χρονομέτρων πεδίου για την παρακολούθηση και καταγραφή του χρόνου που πραγματοποιείται οποιαδήποτε αλλαγή στο σύστημα καθ 'όλη τη διάρκεια ζωής ενός συμβάντος. Με βάση τα ευρήματά σας, μπορείτε να επιλέξετε να εκτελέσετε προσομοιώσεις για να εκπαιδεύσετε νέα μέλη της ομάδας, να δοκιμάσετε νέες ροές εργασίας και σχέδια απόκρισης ή να ασκήσετε ασυνήθιστα σενάρια. Μπορείτε να εξάγετε πίνακες εργαλείων και αναφορές σε τυπικά βιομηχανικά εργαλεία αναφοράς, όπως το Tableau ή να κάνετε λήψη σε διάφορες μορφές, όπως CSV, PDF, JPG, SVG κ.λπ.



Εικόνα 24: CISO Dashboard με εξαγώγιμα στατιστικά στοιχεία σε πραγματικό χρόνο

Συμπληρώνει το υπάρχον ticketing system για να προσφέρει το καλύτερο και των δύο κόσμων, διατηρώντας παράλληλα την ασφάλεια και το IT ξεχωριστά. Η αμφίδρομη ενσωμάτωση εργαλείων επιτρέπει στην ομάδα ασφαλείας σας να διορθώσει ένα περιστατικό δημιουργώντας ένα ticket από το IBM Security SOAR και αναθέτοντας εργασίες απόκρισης σε μη χρήστες. Εργασίες όπως η επιδιόρθωση κώδικα διακομιστών ή η επανεκτίμηση τελικών σημείων γίνονται χωρίς οι αναλυτές σας να μάθουν ή να συνδεθούν σε άλλο εργαλείο.

Αυτή η αμφίδρομη ολοκλήρωση διατηρεί διαδικασίες ελέγχου οργανωτικής αλλαγής σε διαφορετικά μέρη του οργανισμού σας. Οι ομάδες ασφαλείας μπορούν να αξιοποιήσουν τα προϋπάρχοντα workflows, ενώ παρακολουθούν και διαχειρίζονται τον συνολικό κύκλο ζωής του συμβάντος στη λύση SOAR.

Η ενσωμάτωση με δημοφιλή συστήματα έκδοσης εισιτηρίων όπως το ServiceNow και το Jira είναι άμεσα διαθέσιμη.

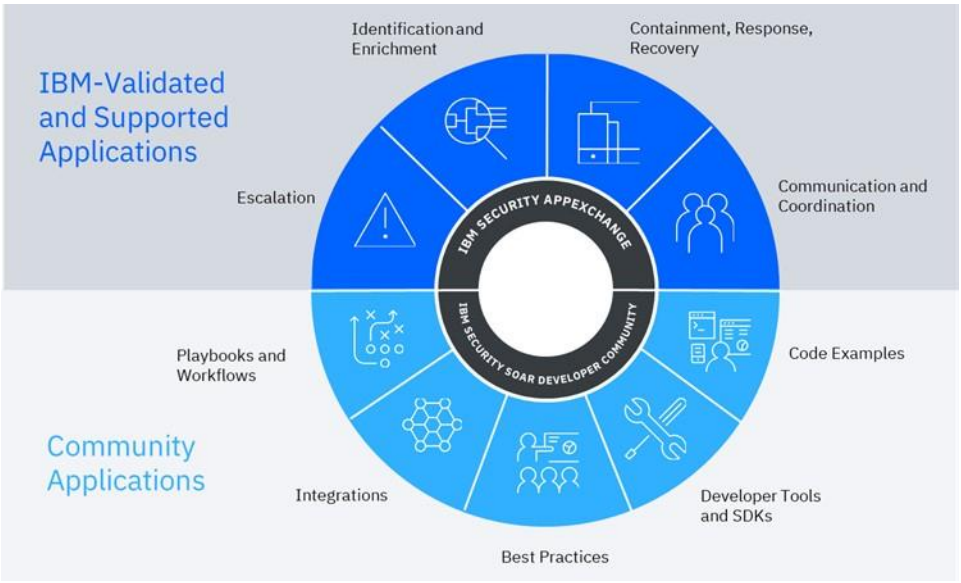
3.2.2.7.5 Ενορχήστρωση και αυτοματισμός (Orchestration and Automation)

Η προσφερόμενη υπηρεσία ενσωματώνει διαφορετικά εργαλεία ασφαλείας στο SOC μας, μέσω καθορισμένων συνδέσεων και API, τα οποία επιτρέπουν την ενορχήστρωση αυτών των τεχνολογιών και επεκτείνουν τη λύση SOAR.

Διαθέτει το καλύτερο οικοσύστημα αυτοματισμού και ενορχήστρωσης στον κλάδο, αποτελούμενο από περισσότερες από 180 επικυρωμένες IBM και community εφαρμογές διαθέσιμες μέσω του IBM Security AppExchange. Οι επικυρωμένες εφαρμογές δίνουν στους χρήστες δυνατότητες γρήγορης ενσωμάτωσης αξιοποιώντας τις συνεργασίες της IBM Security με τρίτους προμηθευτές τεχνολογίας. Οι επικυρωμένες εφαρμογές υποστηρίζονται πλήρως από την IBM ή από αξιόπιστους συνεργάτες.

Ο κάθε πελάτης μας μπορεί να αυξήσει τα tickets υποστήριξης μέσω των κανονικών καναλιών σε περίπτωση οποιουδήποτε προβλήματος. Οι community εφαρμογές αναπτύσσονται είτε από πελάτες, συνεργάτες είτε από οργανισμούς υπηρεσιών της IBM. Αυτές οι εφαρμογές υποβάλλονται σε δοκιμές λειτουργίας και ασφάλειας πριν από

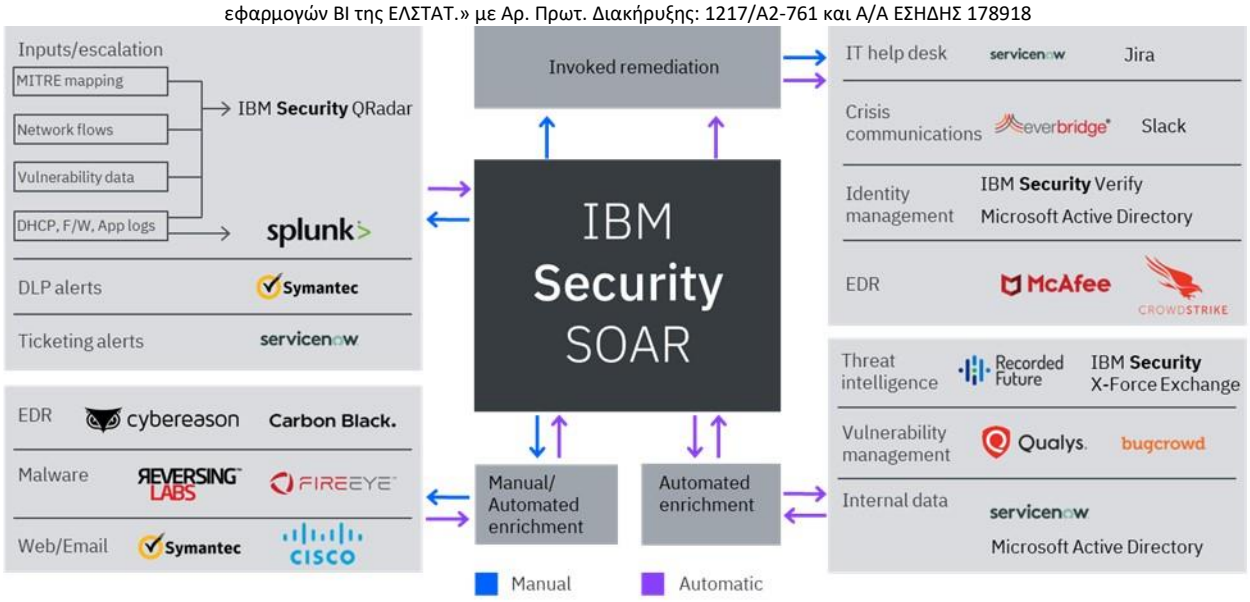
τη δημοσίευσή τους. Η υποστήριξη είναι διαθέσιμη μέσω της IBM Security SOAR Community, μιας ανοιχτής διαδικτυακής κοινότητας που περιλαμβάνει blogs και φόρουμ για συζήτηση και συνεργασία καθώς και πρόσβαση στα τελευταία white papers, εκπομπές, παρουσιάσεις και έρευνες.



Εικόνα 25: IBM Security AppExchange

Με τον ενσωμάτωσης IBM Security SOAR AppHost integration server, μπορείτε να εγκαταστήσετε και να αναπτύξετε εφαρμογές μέσα σε λίγα λεπτά. Όταν κάνετε λήψη μιας εφαρμογής από το IBM Security AppExchange, μπορείτε στη συνέχεια να την εγκαταστήσετε από το UI μέσω μιας απλής διαδικασίας εγκατάστασης βήμα προς βήμα. Αυτή η καθοδηγούμενη διαδικασία επιτρέπει τη διαμόρφωση κάθε εφαρμογής μέσω αυτόματης δημιουργίας και επεξεργάσιμων ρυθμίσεων. Οι εφαρμογές αναπτύσσονται σε διαφορετικά containers, ενισχύοντας την ασφάλεια και τη διαχείριση εφαρμογών.

Αυτές οι εφαρμογές επιτρέπουν ενσωματώσεις. Αυτές οι ενσωματώσεις εκτείνονται σε εγγενείς, προσανατολισμένες στην ασφάλεια ενσωματώσεις και ευρύτερες ενσωματώσεις IT/DevOps, για παράδειγμα, ενσωμάτωση με το Red Hat Ansible και άλλα κορυφαία εργαλεία και τεχνολογίες ασφάλειας στον κλάδο. Οι εφαρμογές συνήθως περιέχουν πολλαπλές λειτουργίες και workflows για την κάλυψη συγκεκριμένων περιπτώσεων χρήσης. Μπορείτε να προσθέσετε γρήγορα και εύκολα αυτές τις περιπτώσεις χρήσης σε υπάρχοντα βιβλία αναπαραγωγής χρησιμοποιώντας το Visual Workflow Editor. Η IBM Security παρέχει πλήρες documentation, βίντεο και αποσπάσματα κώδικα για αναλυτές ασφάλειας και προγραμματιστές που θέλουν να επεκτείνουν υπάρχουσες εφαρμογές ή να αναπτύξουν δικές τους περιπτώσεις χρήσης.



Εικόνα 26: Ένα κεντρικό hub για την επίλυση περιστατικών ασφαλείας

3.2.2.7.6 Στρατηγική αυτοματοποίηση

Ο κάθε οργανισμός μπορεί να χρησιμοποιήσει τον αυτοματισμό για να βελτιστοποιήσει τις λειτουργίες ασφαλείας και να δώσει αξία στην απόκριση συμβάντων, εξαλείφοντας περιττές εργασίες. Με αυτόν τον τρόπο, οι αναλυτές μπορούν να επικεντρωθούν σε αυτό που έχει σημασία. Μπορείτε να χρησιμοποιήσετε περισσότερο ή λιγότερο αυτοματοποίηση ανάλογα με τον τύπο του συμβάντος, τη διαδικασία και το επιθυμητό αποτέλεσμα και εάν αυτή η διαδικασία έχει δοκιμαστεί.

Μπορείτε να ισορροπήσετε τις διαδικασίες, την ανθρώπινη νοημοσύνη και την ευελιξία μέσω των δυναμικών playbooks της λύσης, τα οποία εξελίσσονται με ένα περιστατικό που προσθέτει τις ροές εργασίας που απαιτούνται για να καθοδηγήσει την απάντηση της ομάδας σας. Μπορείτε να χρησιμοποιήσετε στρατηγικά τον αυτοματισμό με τον workflow επεξεργαστή . Αυτό δίνει τη δυνατότητα στην ομάδα ασφαλείας σας να σχεδιάσει και να ενορχηστρώσει διαδικασίες απόκρισης συμβάντων με οπτικά κατασκευασμένες, πολύπλοκες ροές εργασίας που βασίζονται σε εργασίες για αναλυτές, εργασίες αυτοματοποίησης και τεχνικές ενοποιήσεις. Οι εργασίες και τα σενάρια επιτρέπουν την αυτοματοποίηση στη λύση προσθέτοντας λειτουργίες δέσμης ενεργειών. Μπορείτε να δημιουργήσετε τεχνητές ροές εργασίας για να ενεργοποιήσετε ροές εργασιών αυτοματοποίησης εργαλείων-εργαλείων, επιτρέποντας παράλληλα εργασίες και έγκριση με επίκεντρο τον άνθρωπο. Για να ενεργοποιήσετε μια έγκαιρη απόκριση και να συμμορφωθείτε με τις οργανωτικές SLA, μπορείτε να προσθέσετε χρονοδιακόπτες στις ροές εργασίας σας επιτρέποντας κανόνες βάσει χρόνου.

3.2.2.8 Threat Intelligence

Η προσφερόμενη υπηρεσία ενσωματώνεται με ροές πληροφοριών απειλών για να μειώσει τους χρόνους έρευνας εμπλουτίζοντας περιστατικά και προσδιορίζοντας σχέσεις με άλλα ανοιχτά ή κλειστά περιστατικά στη λύση. Με προκαθορισμένες ροές απειλών, όπως το IBM X Force Exchange, οι αναλυτές μπορούν να εμπλουτίσουν αυτόματα

περιστατικά που προέρχονται από ολοκληρωμένα εργαλεία όπως το SIEM, το EDR και άλλα. Πολλές πρόσθετες πηγές πληροφοριών απειλής και υποστήριξη για μεγάλες πλατφόρμες πληροφοριών απειλής (TIP) διατίθενται μέσω του IBM Security AppExchange και οι προσαρμοσμένες ροές απειλών μπορούν εύκολα να ενσωματωθούν μέσω βιομηχανικών προτύπων όπως το STIX/TAXII.

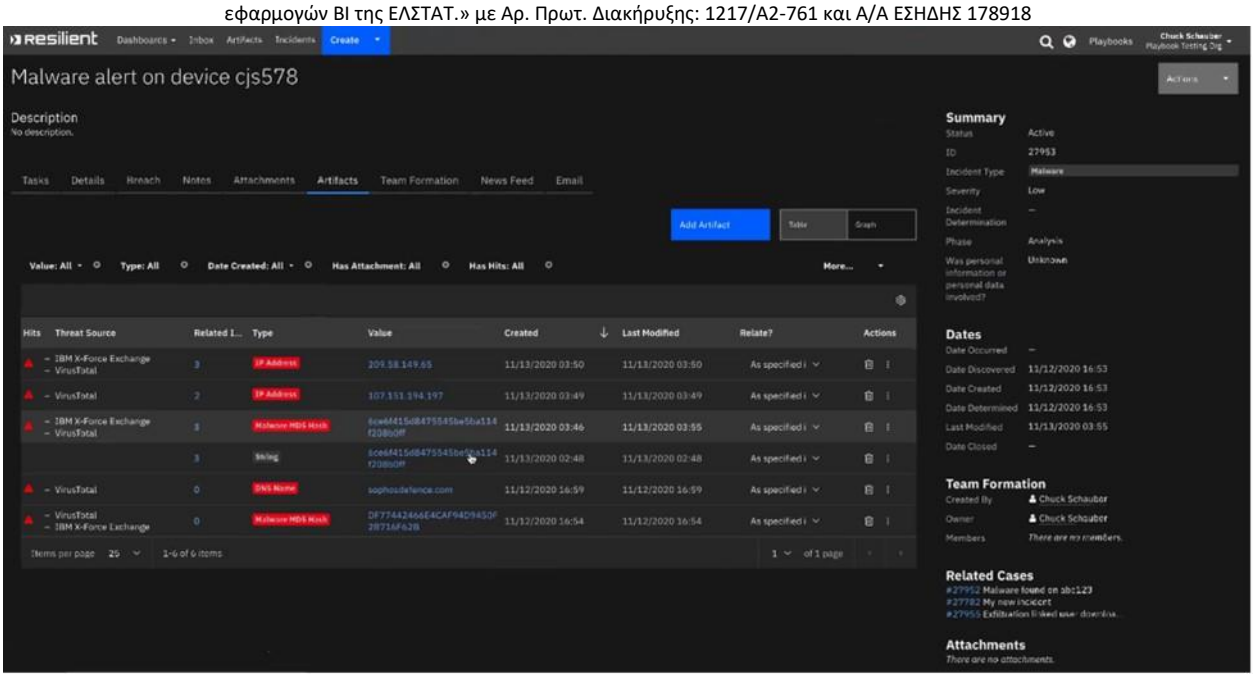
Μόλις ενεργοποιηθούν οι ροές πληροφοριών απειλής, η λύση μπορεί να συσχετίσει αυτόματα δείκτες συμβιβασμού (IOCs), αποθηκευμένους ως artifacts, με πηγές πληροφοριών απειλής όπως geolocation, botnets, κακόβουλα δίκτυα κ.λπ. Μπορείτε να διαμορφώσετε τη λύση να εκτελείται αυτόματα σάρωση συνεχώς προκειμένου να εντοπίζονται αλλαγές στις IOC, με αυτόν τον τρόπο εάν μια ΔΟΕ που θεωρήθηκε αρχικά καλοήθης γίνει απειλή, οι αναλυτές μπορούν να ειδοποιηθούν αμέσως.

Η υπηρεσία Threat Intelligence θα ενισχύσει τις δυνατότητες των μηχανισμών ανίχνευσης απειλών των web sites ώστε να μπορούν οι αναλυτές, να εντοπίσουν πιο αποτελεσματικά γνωστές προηγμένες επιθέσεις. Οι υπηρεσίες Threat Intelligence ή αλλιώς Threat Feeds, όπως είναι ευρέως γνωστές, ενισχύουν την αμυντική γραμμή ενός οργανισμού ως ένα επιπλέον εργαλείο άμεσου εντοπισμού των “known-knowns”. Ενσωματώνοντας τα Threat Feeds στην υπηρεσία δημιουργείται μία βασική γραμμή άμυνας για συστήματα με αυξημένη επικινδυνότητα για άμεση εξωτερική επίθεση. Με τον τρόπο αυτό, ενσωματώνονται μια σειρά από Threat Intelligence Feeds ώστε να συμπεριληφθούν και γεωγραφικά περιεχόμενα και ο βαθμός φήμης (reputation score) σε όλα τα επίπεδα λειτουργίας της υπηρεσίας.

3.2.2.9 Artifacts Management

Η Artifacts Management είναι η κεντρική άποψη της λύσης που επιτρέπει στις ομάδες ασφαλείας να δοκιμάζουν, να διερευνούν και να αποκαθιστούν ταχύτερα περιστατικά. Αυτή η συγκεντρωτική προβολή παρέχει στις ομάδες έναν αποτελεσματικό τρόπο για την παρακολούθηση artifact στον οργανισμό σας, την ανταλλαγή ιστορικών γνώσεων και τη μεγιστοποίηση των υφιστάμενων ενοποιήσεών σας με ροές πληροφοριών απειλής

Η καρτέλα Artifacts παρέχει αυτόματα στους αναλυτές την σχέση μεταξύ περιστατικών και τεκμηρίων, ακόμα και για διαφορετικών περιστατικών, για γρήγορη λήψη αποφάσεων. Οι αναλυτές μπορούν να διαπιστώσουν εάν υπάρχουν χτυπήματα σε πηγές πληροφοριών απειλής που σχετίζονται με ένα artifact, τον τύπο της πηγής απειλής και τον αριθμό των περιπτώσεων που σχετίζονται με το αντικείμενο που διερευνάται. Αυτές οι πληροφορίες είναι δυναμικές, ενημερώνονται περιοδικά, και μπορούν να βοηθήσουν τους αναλυτές μας στον προσδιορισμό της κλίμακας και την πιθανή σοβαρότητα της επίθεσης.



Artifacts Management provides security analysts with a comprehensive view to investigate further.

Οι αναλυτές ασφαλείας μπορούν να δοκιμάσουν και να επανορθώσουν τις περιπτώσεις ταχύτερα, αναφερόμενοι στις σημειώσεις αναλυτών που αντιμετώπισαν ή έλαβαν μέτρα για το συγκεκριμένο artifact που ερευνάται. Θα μπορούσε να είναι ότι ένα artifact που σχετίζεται με άλλες περιπτώσεις στον οργανισμό, οπότε το IBM Security SOAR συγκεντρώνει όλες τις ιστορικές πληροφορίες σε ένα μέρος για να δώσει στον αναλυτή ένα σημείο εκκίνησης για να επιθεωρήσει τις σχετικές περιπτώσεις, εάν είναι απαραίτητο. Η συγκεντρωτική άποψη των artifacts σε ολόκληρο τον οργανισμό επιτρέπει στους αναλυτές ασφάλειας να αναλύουν προσεκτικά τα τεχνουργήματα και τις σχετικές πληροφορίες σχετικά με τα συμφραζόμενα για να προσδιορίσουν τον κίνδυνο που ενέχουν στον οργανισμό σας και να αναλάβουν δράση.

3.2.2.10 Breach Response

Με τις συνεχώς αυξανόμενες προκλήσεις για την αντιμετώπιση σύνθετων απαιτήσεων αναφοράς παραβίασης απορρήτου και την τήρηση των προτύπων συμμόρφωσης, η προσφερόμενη υπηρεσία είναι η μόνη λύση SOAR που ενσωματώνει την αναφορά παραβίασης απορρήτου στην ίδια διαδικασία διαχείρισης περιπτώσεων με τη διαχείριση περιστατικών ασφαλείας. Η IBM Security SOAR Breach Response παρέχει μια παγκόσμια βιβλιοθήκη με περισσότερους από 180 παγκόσμιους κανονισμούς, συμπεριλαμβανομένου του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), της Προστασίας Προσωπικών Πληροφοριών και του Νόμου για τα Ηλεκτρονικά Έγγραφα (Καναδάς) (PIPEDA), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA) και οι κανόνες ειδοποίησης παραβίασης και των 50 κρατών.

Σε περίπτωση παραβίασης δεδομένων απορρήτου, το Breach Response μπορεί να προσθέσει τις σχετικές ρυθμιστικές εργασίες για τη χώρα ή/και τον κλάδο στο σχέδιο απόκρισης, συμπεριλαμβανομένων πληροφοριών όπως:

- Η συγκεκριμένη διαδικασία ειδοποίησης
- Τα στοιχεία επικοινωνίας για ειδοποίηση
- Χρονικά πλαίσια
- Πρότυπα για ειδοποίηση

Μπορείτε να αναθέσετε αυτές τις εργασίες στους απαιτούμενους χρήστες στο SOC και σε άλλα τμήματα, όπως ανθρώπινο δυναμικό, νομικό τμήμα και επικοινωνίες. Αυτοί οι χρήστες μπορούν να ολοκληρώσουν εργασίες στη λύση, μέσω email ή μέσω ticketing συστήματος . Στη συνέχεια, μπορούν να δημιουργηθούν αναφορές από το περιστατικό με συγκεκριμένες πληροφορίες για τον κανονισμό. Η λύση περιλαμβάνει επίσης ένα εργαλείο εκτίμησης κινδύνου παραβίασης για να βοηθήσει την ομάδα απορρήτου στη δημιουργία αναφορών ρυθμιστικών αρχών, όπως απαιτείται. Αυτό ισχύει ιδιαίτερα για τον GDPR, τον HIPAA και τον PIPEDA.

Το Breach Response επιτρέπει στον κάθε οργανισμό να εκτελέσει πλήρεις ασκήσεις προσομοίωσης και table-top ασκήσεις για να εκπαιδεύσει τις ομάδες ασφάλειας και απορρήτου. Αυτό παρέχει συνεπείς και επαναλαμβανόμενες διαδικασίες για την αντιμετώπιση σύνθετων παραβιάσεων απορρήτου δεδομένων και αιτημάτων πρόσβασης υποκειμένου δεδομένων. Οι πίνακες ελέγχου αναφοράς απορρήτου παρέχουν πληροφορίες στους ηγέτες ασφάλειας και απορρήτου σχετικά με τον κίνδυνο παραβίασης δεδομένων εντός του οργανισμού.

3.2.2.11 Υπηρεσία WAF as a Service

Για την προστασία της υπηρεσίας του ιστοτόπου της ΕΛΣΤΑΤ προτείνεται η λύση WAF as a service. Η συγκεκριμένη λύση ασφάλειας πρόκειται να καλύψει την ανάγκη προστασίας του συνόλου των ιστοσελίδων της Εταιρείας από επιθέσεις και απειλές τόσο στο περιεχόμενο τους.

Ο ρόλος της εν λόγω λύσης ασφαλείας στην υποδομή της εταιρίας θα καλύπτει τουλάχιστον τα ακόλουθα:

- Ανάλυση και έλεγχο της δικτυακής κίνησης που δρομολογείται προς τις κρίσιμες ιστοσελίδες και το portal.
- Διαχείριση μέσω κεντρικής κονσόλας διαχείρισης (GUI)
- Έγκαιρος εντοπισμός και καταστολή επιθέσεων – απειλών σε επίπεδο portal συμπεριλαμβανομένων των ακόλουθων SQL injection, Cross Site Scripting (XSS), Session Hijacking, Buffer Overflow, Cookie Poisoning, Denial of Service, Parameter Manipulation, Brute Force Login, Malicious Encoding, Identity Theft, Phishing, Data Destruction, Scanning, Worms Infection, “Zero Day” Worms, OWASP Top10 κλπ.
- Η συσκευή ασφάλειας θα μπορεί μέσω ανάλυσης της δικτυακής κίνησης και εντός ευλόγου χρονικού διαστήματος να «μαθαίνει» την κανονική και νόμιμη λειτουργία του portal & να δημιουργεί αυτόματα το «προφίλ» νόμιμης και ασφαλούς λειτουργίας αυτής.
- Εντοπισμός και αποτροπή κάθε είδους δικτυακής κίνησης – πρόσβασης προς το portal η οποία αντιτίθεται στο “προφίλ” ασφαλούς λειτουργίας του.

- Αποτροπή της επιστροφής ευαίσθητων πληροφοριών προς τον client ως αποτέλεσμα κάποιου μη εξουσιοδοτημένου http request προστατεύοντας τα ευαίσθητα δεδομένα από διαρροή
- Εντοπισμός και αποτροπή επιθέσεων σε επίπεδο πρωτοκόλλου HTTP (protocol anomalies π.χ. malformed URLs)
- Ολοκληρωμένη προστασία σε επίπεδο Web υπηρεσιών επιτρέποντας τον εντοπισμό και αποτροπή επιθέσεων ενάντια σε εφαρμογές τύπου XML, SOAP & WSDL.
- Ο μηχανισμός προστασίας web εφαρμογών που ενσωματώνει η συσκευή ασφάλειας θα μπορεί να θέτει περιορισμούς σε παραμέτρους των εφαρμογών όπως:
    - Αποδεκτό “μήκος” μεταβλητών
    - Αποδεκτός τύπος χαρακτήρων
    - “Read only”, δηλαδή ότι ο χρήστης δεν προβλέπεται να την αλλάξει κ.α.
- Ο μηχανισμός προστασίας web εφαρμογών που ενσωματώνει η συσκευή ασφάλειας θα επιτρέπει την αναλυτική καταγραφή των προσβάσεων στην Web εφαρμογή παρέχοντας πληροφορίες όπως:
    - Date/Time
    - Client IP Address
    - Client Hostname
    - Client application
    - Number of Events
    - Event Type
    - HTTP Query

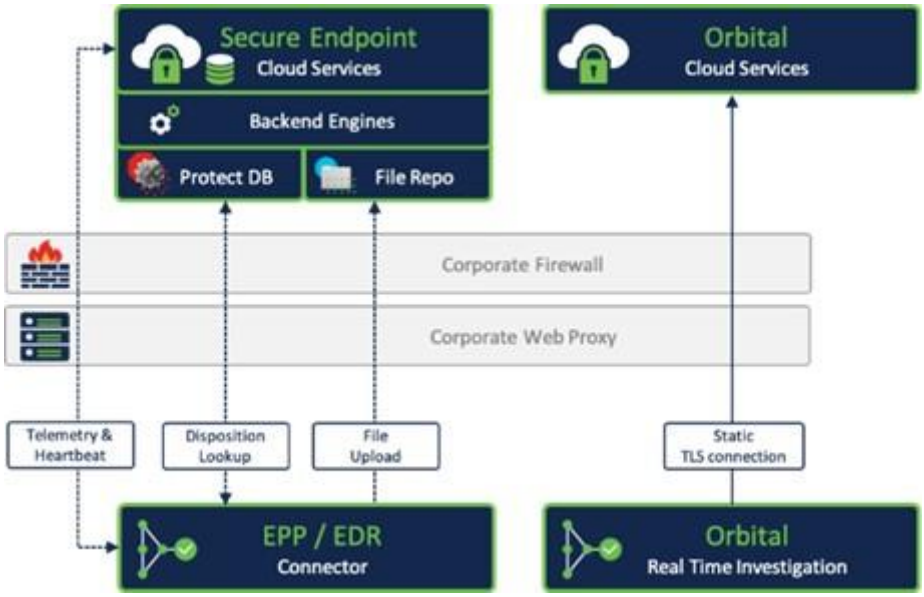
Οι υπηρεσίες αυτές θα δημιουργήσουν ένα δυναμικό προφίλ του φορέα και ειδικότερα του ιστότοπου, το οποίο εφόσον ενσωματωθεί στην υπηρεσία εντοπίζει με ακρίβεια τις επιθέσεις και ελαχιστοποιεί τα false positives έτσι ώστε να εξασφαλίσει την, χωρίς πρόβλημα, πρόσβαση των νόμιμων χρηστών ενώ ταυτόχρονα να εμποδίσει την μη εξουσιοδοτημένη κίνηση από τους hackers.

3.2.1 Μέρος Γ

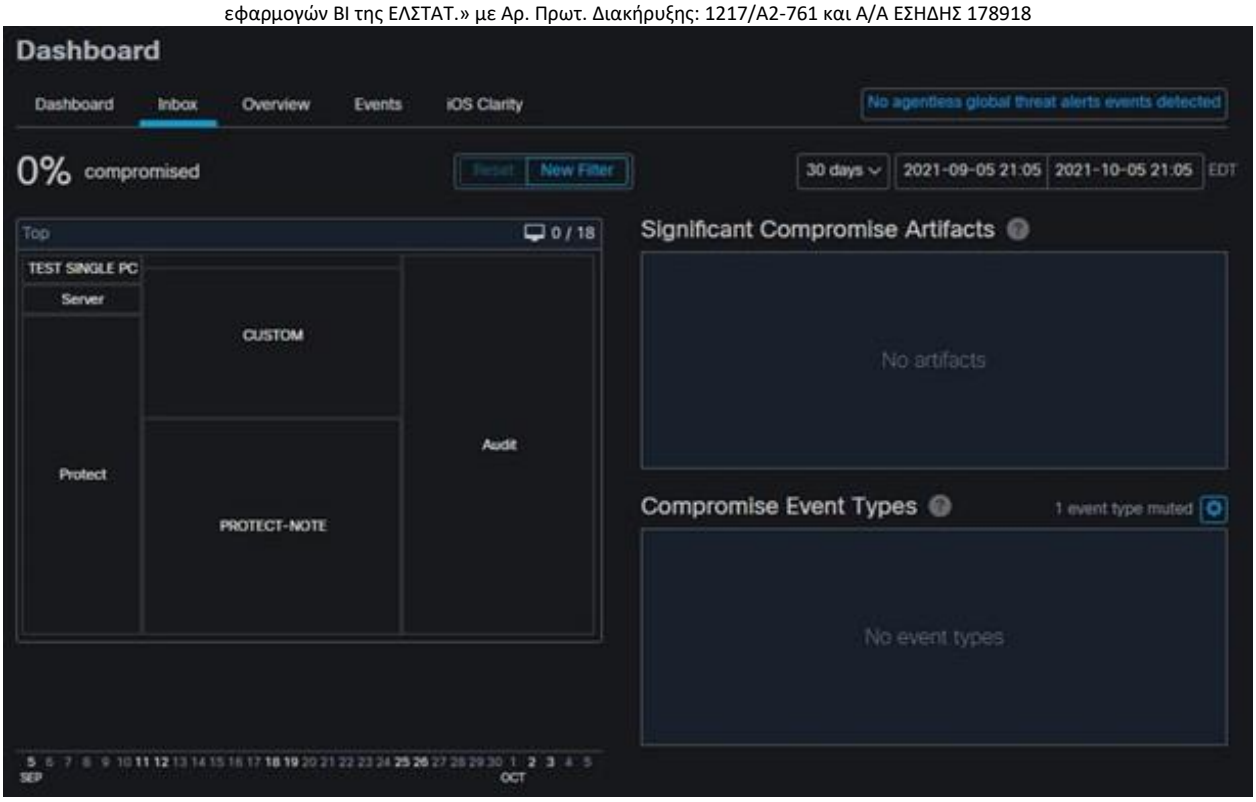
Προσφέρονται τριάντα (30) άδειες εξειδικευμένου λογισμικού (EDR) ως υπηρεσία για την υποστήριξη προσωπικών υπολογιστών υψηλής κρισιμότητας. Πρόκειται για υπολογιστές που χρησιμοποιεί το προσωπικό της Διεύθυνσης Πληροφορικής του οργανισμού και κυρίως οι προγραμματιστές και το προσωπικό ασφάλειας υποδομών πληροφορικής. Προτείνουμε τη χρήση του λογισμικού Cisco Secure Endpoint.

Το Cisco Secure Endpoint ενσωματώνει τις δυνατότητες πρόληψης, ανίχνευσης, κυνηγιού απειλών και απόκρισης σε μια ενοποιημένη λύση που αξιοποιεί τη δύναμη των αναλύσεων που βασίζονται σε σύννεφο. Το Secure Endpoint θα προστατεύει τις συσκευές σας Windows, Mac, Linux, Android και iOS μέσω μιας δημόσιας ή ιδιωτικής ανάπτυξης cloud.

Το Cisco Secure Endpoint είναι μια λύση ενός παράγοντα που παρέχει ολοκληρωμένη προστασία, ανίχνευση, απόκριση και κάλυψη πρόσβασης χρήστη για προστασία από απειλές στα τελικά σημεία σας. Η πλατφόρμα SecureX™ είναι ενσωματωμένη στο Secure Endpoint, καθώς και στις δυνατότητες Extended Detection and Response (XDR). Το νεοεισαχθέν Cisco Secure MDR for Endpoint συνδυάζει τις ανώτερες δυνατότητες του Secure Endpoint με την τεχνογνωσία σε λειτουργίες ασφαλείας για να μειώσει δραματικά τον μέσο χρόνο εντοπισμού και απόκρισης σε απειλές.



Στον ταχέως εξελισσόμενο κόσμο του κακόβουλου λογισμικού, οι απειλές γίνονται όλο και πιο δύσκολο να εντοπιστούν. Το πιο προηγμένο 1% αυτών των απειλών, αυτές που τελικά θα εισέλθουν και θα προκαλέσουν τον όλεθρο στο δίκτυό σας, θα μπορούσαν ενδεχομένως να μην εντοπιστούν. Ωστόσο, το Secure Endpoint παρέχει ολοκληρωμένη προστασία έναντι αυτού του 1%. Το Secure Endpoint αποτρέπει τις παραβιάσεις, μπλοκάρει το κακόβουλο λογισμικό στο σημείο εισόδου και παρακολουθεί και αναλύει συνεχώς τη δραστηριότητα αρχείων και διεργασιών για τον γρήγορο εντοπισμό, τον περιορισμό και την αποκατάσταση απειλών που μπορούν να αποφύγουν τις άμυνες πρώτης γραμμής.



Με τις παραπάνω EDR άδειες ,οι οποίες και παρέχονται με την μορφή υπηρεσίας για να προστατευτούν οι τριάντα (30) προσωπικοί υπολογιστές υψηλής κρισιμότητας του οργανισμού.

4 ΓΕΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

4.1 Εισαγωγή

Η **Cosmos Computers A.E.B.E.** δίνει ιδιαίτερη έμφαση στην ομαλή και απρόσκοπτη λειτουργία των πληροφοριακών και επικοινωνιακών συστημάτων που υποστηρίζει για λογαριασμό των πελατών της, γνωρίζοντας την ουσιαστική σημασία που κατέχει η συντήρηση και η υποστήριξη των συστημάτων αυτών ιδιαίτερα σε απαιτητικά περιβάλλοντα συνεχούς λειτουργίας. Επιπλέον διαθέτει την κατάλληλη εσωτερική υποδομή τόσο σε ανθρώπινο δυναμικό όσο και σε τεχνικό εξοπλισμό ώστε να μπορεί να προσφέρει αξιόπιστες υπηρεσίες συντήρησης και υποστήριξης όσο εξειδικευμένες και αν είναι αυτές, σύμφωνα πάντα με τις ανάγκες των πελατών της και την μορφή του ολοκληρωμένου έργου με το οποίο σχετίζονται.

Η σημαντικότερη φάση στον κύκλο ζωής κάθε πληροφοριακού συστήματος είναι αναμφισβήτητα η περίοδος λειτουργίας του. Σε αυτή την φάση το πληροφοριακό σύστημα καλείται να υλοποιήσει την αποστολή του και να προσφέρει στην επιχείρηση ή τον οργανισμό την υποστήριξη στην παραγωγική διαδικασία. Η συνεχή λειτουργία του μηχανογραφικού εξοπλισμού, ο οποίος αποτελεί τον πυρήνα κάθε πληροφοριακού συστήματος, απειλείται αφενός από την επίδραση της φυσιολογικής φθοράς λόγω χρόνου και χρήσης και αφετέρου από διάφορους εσωτερικούς ή εξωτερικούς παράγοντες (π.χ. κατασκευαστική αστοχία, σφάλμα στον χειρισμό κτλ.) που επιδρούν στην ομαλή απρόσκοπτη λειτουργία του.

Η εταιρία μας εγγυάται προς την ΕΛΣΤΑΤ ότι το έργο θα εκτελεσθεί σύμφωνα με τους τεχνικούς κανόνες και τα διεθνώς αναγνωρισμένα πρότυπα που ισχύουν στη σύγχρονη ψηφιακή και ηλεκτρονική τεχνολογία και θα πληροί όλες τις ιδιότητες και χαρακτηριστικά που θα προβλέπονται στην σχετική σύμβαση που θα υπογραφεί.

4.2 Υπηρεσίες στα πλαίσια του παρόντος έργου

Η Cosmos Computers A.E.B.E. σε συνεννόηση με την ΕΛΣΤΑΤ, θα συντονίζει τις εργασίες ενεργοποίησης των αδειών , συντήρησης, παροχής υπηρεσιών κλπ, σύμφωνα με τους όρους της συμβάσης που θα υπογραφεί.

Οι υπηρεσίες στα πλαίσια του παρόντος έργου περιλαμβάνουν:

- Την υλοποίηση της προμήθειας.
- Την ενεργοποίηση των ζητούμενων
- Την πλήρη υποστήριξη των λογισμικών και την παροχή υπηρεσιών σύμφωνα με τα όσα ορίζει η διακήρυξη, με αρχή την ημερομηνία οριστικής παραλαβής.

4.2.1 Υπηρεσίες Υλοποίησης της Προμήθειας

Η Υλοποίηση της προμήθειας, θα ολοκληρωθεί στις παρακάτω φάσεις:

- **Πλάνο Εγκατάστασης:** Οι μηχανικοί της Cosmos Computers A.E.B.E. σε συνεργασία με το αρμόδιο προσωπικό της Αναθέτουσας Αρχής καθορίζουν το ακριβές χρονοδιάγραμμα της υλοποίησης και τις παραμέτρους λειτουργίας του εξοπλισμού.
- **Παραλαβή Εξοπλισμού:** Η Cosmos Computers A.E.B.E. παραλαμβάνει τον εξοπλισμό και γίνεται η εισαγωγή στις αποθήκες της σύμφωνα με διαδικασίες διασφάλισης ποιότητας κατά ISO 9001.

4.2.2 Υπηρεσίες Παράδοσης

Τα λογισμικά θα ενεργοποιηθούν στον λογαριασμό της ΕΛΣΤΑΤ. Η παροχή των ζητούμενων υπηρεσιών θα πραγματοποιηθεί σύμφωνα με τις υποδείξεις της αναθέτουσας αρχής.

4.2.3 Αναλυτικό Σχέδιο Εγγύησης – Συντήρησης

Για την οργανωμένη αντιμετώπιση των αναγκών υποστήριξης του εξοπλισμού και την αντιμετώπιση πιθανών βλαβών και προβλημάτων, η **Cosmos Computers A.E.B.E.** προτείνει και ακολουθεί σχέδιο κλήσης/επέμβασης/παρακολούθησης αναγκών και επιδιόρθωσης βλαβών που παρουσιάζεται στη συνέχεια:

- Λήψη κλήσης - αναφοράς βλάβης που δίνει ο πελάτης
- Καταχώρηση της κλήσης στο Αυτοματοποιημένο Σύστημα Διαχείρισης Κλήσεων
- Μελέτη της κλήσης από εξειδικευμένο επιστημονικό προσωπικό στο Help-Desk Office
- Διάγνωση προβλήματος
- Ενέργειες αποκατάστασης προβλήματος (Τηλεφωνικά ή με επιτόπου επέμβαση)

Κάθε υπόθεση θα χαρακτηρίζεται από μοναδικό αριθμό αναφοράς ο οποίος θα χρησιμοποιείται σε κάθε επικοινωνία με τον Οργανισμό. Η παρεχόμενη συντήρηση θα αποδεικνύεται με δελτίο επίσκεψης το οποίο θα προσυπογράφεται εκ μέρους μεν της **Cosmos Computers A.E.B.E.** από τον τεχνικό του που θα προβεί στη συντήρηση, εκ μέρους δε του Φορέα από τον αρμόδιο υπεύθυνο. Μετά το πέρας της συντήρησης ένα αντίγραφο του συγκεκριμένου δελτίου επίσκεψης θα παραμένει στον πελάτη και ένα αντίγραφο θα παραμένει στον τεχνικό. Στο δελτίο επίσκεψης θα περιλαμβάνονται τα παρακάτω στοιχεία:

- Αριθμός αναφοράς της υπόθεσης
- Στοιχεία του πελάτη
- Στοιχεία του τεχνικού
- Ώρα έναρξης και αποπεράτωσης της συντήρησης
- Ενέργειες αποκατάστασης του προβλήματος και στοιχεία ανταλλακτικών που τυχόν χρησιμοποιήθηκαν
- Παρατηρήσεις ποιοτικού ελέγχου (οριστική ή προσωρινή αποκατάσταση, αν πρόκειται να επαναληφθεί η επίσκεψη κτλ.)

Επιπρόσθετα με μέριμνα της εταιρίας μας θα τηρείται **ημερολόγιο συντηρήσεως** το οποίο θα περιλαμβάνει οπωσδήποτε τα παρακάτω στοιχεία:

- Έδρα κλιμακίου συντηρήσεως της εταιρίας μας.
- Ημερομηνία και ώρα ειδοποιήσεως-αναφοράς δυσλειτουργίας ή αιτήσεως συντηρήσεως εκ μέρους του φορέα.
- Ημερομηνία και ώρα ενάρξεως της συντηρήσεως από το προσωπικό της εταιρίας μας.
- Είδος δυσλειτουργίας ή βλάβης ή συντηρήσεως που έγινε.
- Χρησιμοποιηθέντα μέσα και ανταλλακτικά (αναλυτική καταχώρηση στοιχείων αναγνωρίσεως ανταλλακτικών ή υλικών που χρησιμοποιήθηκαν για την επισκευή).
- Ημερομηνία και ώρα επαναλειτουργίας του είδους που συντηρήθηκε ή επισκευάσθηκε.
- Τμήματα του εξοπλισμού που αντικαταστάθηκαν προσωρινά και παραλήφθηκαν από την εταιρία μας για την επισκευή ή συντήρησή τους στις εγκαταστάσεις μας.
- Παρατηρήσεις σχετικά με την παρασχεθείσα υπηρεσία συντήρησης, την καλή επαναλειτουργία του εξοπλισμού, κλπ.

Σε τακτά χρονικά διαστήματα (εβδομαδιαία ή μηνιαία), εφόσον το επιθυμεί ο Οργανισμός, θα παρέχεται αναφορά (report) για το σύνολο των κλήσεων και την εξέλιξη κάθε υπόθεσης.

COSMOS BUSINESS SYSTEMS AEBE — Turn key SOLUTIONS COMPANY

ΣΕΙΡΑ: No:

ΒΡΙΛΗΣΣΟΥ 73, 114 76 ΠΟΛΥΓΩΝΟ, Τηλ.: 210 6492 800, fax: 210 6464 069

ΔΕΛΤΙΟ ΕΠΙΣΚΕΨΗΣ ΤΕΧΝΙΚΟΥ

ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ ΕΝΤΟΛΗ ΜΕ Α/Α:.....

ΣΤΟΙΧΕΙΑ ΠΕΛΑΤΗ		ΣΤΟΙΧΕΙΑ ΤΕΧΝΙΚΟΥ	
ΕΠΩΝΥΜΙΑ		ΕΠΩΝΥΜΟ	
ΕΠΑΓΓΕΛΜΑ		ΗΜΕΡΟΜΗΝΙΑ ΕΠΙΣΚΕΨΗΣ	
ΔΙΕΥΘΥΝΣΗ		ΩΡΑ ΕΝΑΡΞΗΣ ΕΠΙΣΚΕΥΗΣ	
ΑΦΜ		ΩΡΑ ΠΕΡΑΤΩΣΗΣ	
Δ.Ο.Υ.		ΣΥΝΟΛΟ ΩΡΩΝ	
ΤΗΛΕΦΩΝΟ		ΧΑΜ/ΚΟΣΤΟΣ ΜΕΤΑΦΟΡΑΣ	

ΕΝΕΡΓΕΙΕΣ: _____

ΚΑΤΟΠΙΝ ΠΡΩΤΟΒΟΥΛΙΑΣ ΤΕΧΝΙΚΟΥ / ΜΗΧΑΝΙΚΟΥ ☐
ΚΑΤΟΠΙΝ ΑΠΟΦΑΣΗΣ ΠΡΟΪΣΤΑΜΕΝΟΥ ΤΜΗΜΑΤΟΣ ☐
ΚΑΤΟΠΙΝ ΑΠΟΦΑΣΗΣ ΤΕΧΝΙΚΟΥ ΤΜΗΜΑΤΟΣ ☐

ΑΝΤΑΛΛΑΚΤΙΚΑ ΝΑΙ ☐ ΟΧΙ ☐

Α/Α	ΚΩΔΙΚΟΣ	ΠΕΡΙΓΡΑΦΗ ΕΙΔΟΥΣ	ΠΟΣΟΤΗΤΑ	ΤΙΜΗ ΜΟΝΑΔ.	ΑΞΙΑ
				ΕΡΓΑΣΙΑ	
				Φ.Π.Α.	
				ΓΕΝΙΚΟ ΣΥΝΟΛΟ	

ΕΞΩΦΛΗΘΗ ΝΑΙ ☐ ΟΧΙ ☐

Ο ΤΕΧΝΙΚΟΣ Ο ΠΕΛΑΤΗΣ

ΠΑΡΑΤΗΡΗΣΕΙΣ ΠΟΙΟΤΙΚΟΥ ΕΛΕΓΧΟΥ: Η ΛΥΣΗ ΠΟΥ ΔΟΘΗΚΕ ΕΙΝΑΙ: ΣΩΣΤΗ ☐
ΑΜΦΙΒΟΛΟΥ ΑΠΟΤΕΛΕΣΜΑΤΟΣ ☐ ΤΗΛΕΦ. ΣΕ ΠΕΛΑΤΗ ☐
ΛΑΘΟΣ ☐ ΝΕΑ ΕΠΙΣΚΕΨΗ ΤΕΧΝΙΚΟΥ ☐

Ο ΕΛΕΓΚΤΗΣ

CBS Συμβόλαια -Εντολές Τ/Υ - Εργασίες - Σχόλια

ΤΥΠΑ025680 ΑΘΗΝΑ

		Τύπος	Κωδικός	Ποσότητα	Ημ/νία Επίσκεψης	Ώρα Επίσκεψης	Κωδ. Χρόνου	Αφ. Χρόνου
ΤΥΠΑ025680		Πόρος	ΠΟΡ030	1 ΩΡΑ	11/02/10	2:40:00 μμ	TIME00278	Ναι
Βλάβη	*11/02/10*	*ΜΠΛΟΚΑΡΕΙ ΧΑΡΤΙ ΑΠΟ ΤΟ ΕΞΩΤΕΡΙΚΟ TRAY*						
Βλάβη		*SCANNER hp 7650 - s/n : CN731T70TJ*						
Τρόπος Επίλυσης	*11/02/10*	*ΕΠΑΝΑΤΟΠΟΘΕΤΗΣΗ ΕΞΑΡΤΗΜΑΤΟΣ, ΕΛΕΓΧΟΣ ΡΥΘΜΙΣΗ SCANNER TEST OK.*						
Τρόπος Επίλυσης	*11/02/10*	*ΣΑΜΑΡΑΣ:ΕΛΕΓΧΟΣ ΡΥΘΜΙΣΗ FEEDER FOR SCANNER HP7650 S/N:CN731T707J OK.*						

ΤΥΠΑ025749 ΡΟΔΟΣ

8. Μαρ 2010
Σελίδα 3
koutsothog

CBS Συμβόλαια -Εντολές Τ/Υ - Εργασίες - Σχόλια
CBS

Πελάτης

		Τύπος	Κωδικός	Ποσότητα	Ημ/νία Επίσκεψης	Ώρα Επίσκεψης	Κωδ. Χρόνου	Αφ. Χρόνου
ΤΥΠΑ025749		Πόρος	ΠΟΡ018	1 ΩΡΑ	19/02/10	9:56:56 πμ	TIME00278	Ναι
Τρόπος Επίλυσης	*22/02/10*	*ΚΑΘΑΡΙΣΜΟΣ TAPE - TEST OK*						

ΤΥΠΑ025776 ΚΑΒΑΛΑ

		Τύπος	Κωδικός	Ποσότητα	Ημ/νία Επίσκεψης	Ώρα Επίσκεψης	Κωδ. Χρόνου	Αφ. Χρόνου
ΤΥΠΑ025776		Πόρος	ΠΟΡ030	1 ΩΡΑ	18/02/10	10:13:51 πμ	TIME00278	Ναι
Τρόπος Επίλυσης	*19/02/10*	*ΑΝΤΙΚΑΤΑΣΤΑΣΗ ΤΡΟΦΟΔΟΤΙΚΟΥ - TEST OK*						

ΤΥΠΑ025891 ΜΑΡΟΥΣΙ

		Τύπος	Κωδικός	Ποσότητα	Ημ/νία Επίσκεψης	Ώρα Επίσκεψης	Κωδ. Χρόνου	Αφ. Χρόνου
ΤΥΠΑ025891		Πόρος	ΠΟΡ030	1 ΩΡΑ	25/02/10	10:45:00 πμ	TIME00278	Ναι
Βλάβη	*25/02/10*	*ΔΕΝ ΕΚΤΥΠΩΝΕΙ ΣΩΣΤΑ ΣΤΗΝ ΑΡΙΣΤΕΡΗ ΠΛΕΥΡΑ ΤΟΥ ΧΑΡΤΙΟΥ*						
Βλάβη		*PRINTER HP LASERJET 4200n s/n : CNHX154310*						
Τρόπος Επίλυσης	*25/02/10*	*ΑΝΤΙΚΑΤΑΣΤΑΣΗ FUSER ΕΝΤΟΣ ΕΓΓΥΗΣΗΣ ΑΠΟ ΠΡΟΗΓΟΥΜΕΝΗ*						
Τρόπος Επίλυσης		*ΕΠΙΣΚΕΥΗ ΤΟΝ ΙΑΝΟΥΑΡΙΟ 2010 ΤΥΠΑ25083*						
Τρόπος Επίλυσης	*25/02/10*	*ΣΑΜΑΡΑΣ:ΕΛΕΓΧΟΣ LASERJET 4200 S/N:CNHX154310*						
Τρόπος Επίλυσης		*ΑΝΤ/ΣΗ FUSER.*						

file://C:\Documents and Settings\koutsothog\Local Settings\Temporary Internet Files\Co... 9/3/2010

4.2.4 Εξασφάλιση Ανταλλακτικών

Η **Cosmos Computers A.E.B.E.** αναλαμβάνει την δέσμευση της κάλυψης με επαρκές απόθεμα ανταλλακτικών των προσφερόμενων ειδών για το σύνολο της περιόδου παροχής των υπηρεσιών.

4.2.5 Βλαβοληπτικό Κέντρο – Helpdesk

Για την αντιμετώπιση των αναγκών υποστήριξης η εταιρία COSMOS COMPUTERS A.E.B.E. διατηρεί πλήρως οργανωμένο **Κέντρο Επικοινωνίας (Helpdesk)** το οποίο λειτουργεί τόσο σαν **Βλαβοληπτικό Κέντρο** όσο και σαν **Κέντρο Παρακολούθησης** και βρίσκεται στο Datacenter της Εταιρίας, στις κεντρικές της εγκαταστάσεις, στην Μεταμόρφωση Αττικής. Το Helpdesk της COSMOS COMPUTERS A.E.B.E. παρέχει μεταξύ άλλων υπηρεσίες **τηλεφωνικής υποστήριξης**, **διαχείρισης αιτημάτων**, **παρακολούθησης** και **αναφορών**.

Α. Υπηρεσίες Υποστήριξης

Ακολουθεί αναλυτική περιγραφή των παρεχόμενων υπηρεσιών (Service Catalog) του Helpdesk της COSMOS COMPUTERS A.E.B.E. Το σύνολο των διαδικασιών ακολουθεί το πρότυπο **ITIL**, ενώ τα εμπλεκόμενα στελέχη του Helpdesk είναι πιστοποιημένα σύμφωνα με το συγκεκριμένο πρότυπο.

- Αιτήματα παροχής λύσεων
  Αφορά κυρίως συμβουλές του τύπου *«Request for info»*, είναι δηλαδή συμβουλές επικεντρωμένες στη λειτουργικότητα των προϊόντων, την ρύθμιση - παραμετροποίηση τους και τις τεκμηριωμένες δυνατότητες τους.

- Βοήθεια στην εγκατάσταση – Διαχείριση αιτημάτων αλλαγών
  Αφορά κυρίως εργασίες του τύπου *«Request for action»*, είναι δηλαδή εργασίες για την υποστήριξη στην εγκατάσταση των προϊόντων και τη ρύθμιση του λογισμικού τους ή αλλαγές σε υφιστάμενες υποδομές (change management).

- Απομόνωση λαθών - Επίλυση δυσλειτουργιών
  Αφορά κυρίως εργασίες του τύπου *«Incident Management»*, είναι δηλαδή εργασίες για την ανεύρεση και απομόνωση της πηγής των προβλημάτων. Οι προβλεπόμενες ενέργειες περιλαμβάνουν την ανίχνευση και την αντιμετώπιση του προβλήματος (1st level trouble shooting). Εφόσον η επίλυσή του δεν είναι άμεσα εφικτή, γίνονται οι απαραίτητες ενέργειες ώστε να δοθεί μια ενδιάμεση λύση (workarounds).

- Κλιμάκωση ενεργειών (escalation)
  Αφορά εργασίες συντονισμού και επικοινωνίας μεταξύ ατόμων, όταν η επίλυση ενός προβλήματος απαιτεί την ανάμιξη και άλλων πόρων (δυναμικού) όπως, για παράδειγμα, υποστήριξη από ειδικό προσωπικό του κατασκευαστή. Σε μια τέτοια περίπτωση, οι μηχανικοί μεταβιβάζουν την κλήση κατάλληλα.

Α.1. Οργάνωση και Λειτουργία

Το Helpdesk της COSMOS COMPUTERS A.E.B.E. αποτελείται από δύο βασικούς πυλώνες: Το τηλεφωνικό κέντρο **(Call-Center)** και τους μηχανικούς υποστήριξης **(Help-Desk Office)** και είναι η κεντρική υπηρεσία καταγραφής και υποστήριξης αιτημάτων, επανδρωμένη με στελέχη έμπειρους τεχνικούς.

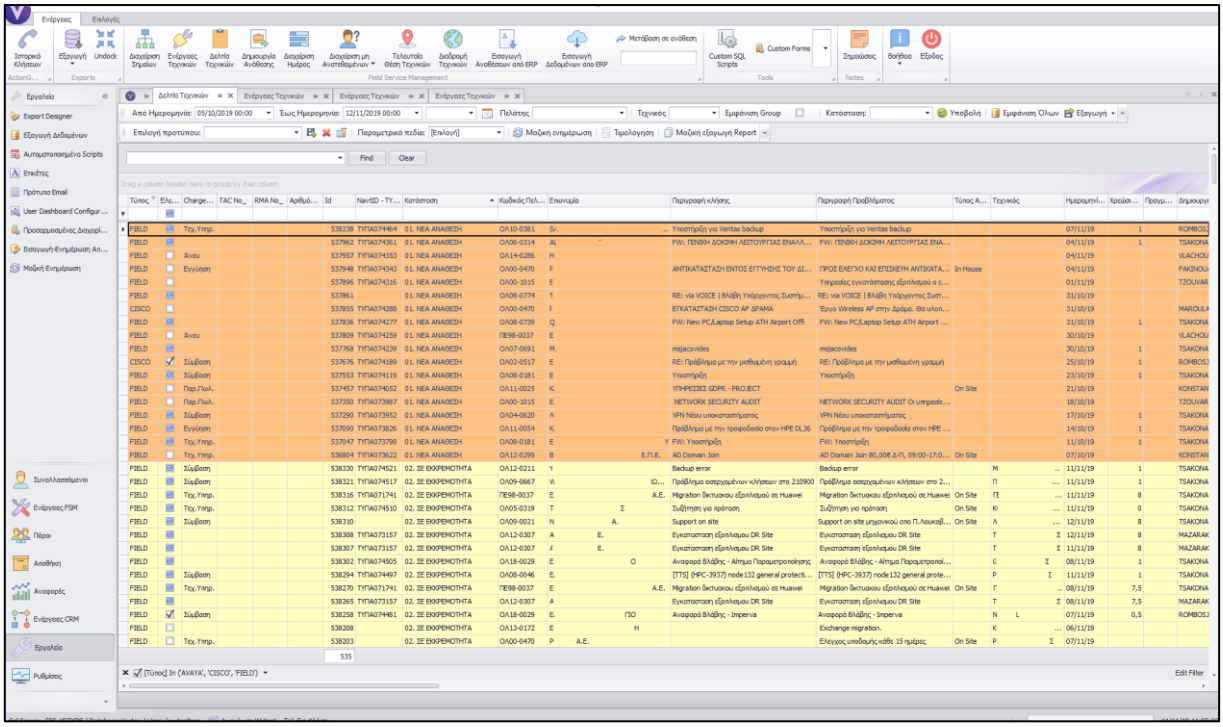
Για την διαχείριση των κλήσεων του Helpdesk χρησιμοποιείται το Αυτοματοποιημένο Σύστημα Κλήσεων **(Service Desk)** το οποίο υλοποιείται με την χρήση της πλατφόρμας Vortex, ενώ υποστηρικτικά χρησιμοποιείται η πλατφόρμα Dynamics NAV της Microsoft μέσω της οποίας λαμβάνονται χρήσιμες πληροφορίες όπως στοιχεία τιμολόγησης, διαδικαστικά έξοδα, διαχείριση υλικών, αναφορές κτλ. Επιπλέον, οι μηχανικοί του Help-Desk Office διαθέτουν όλα τα διαθέσιμα ειδικά εργαλεία λογισμικού με τα οποία μπορούν να εντοπισθούν τα προβλήματα ενώ συντηρείται απευθείας επικοινωνία με τα αντίστοιχα τμήματα όλων των κατασκευαστικών οίκων με τους οποίους συνεργάζεται η COSMOS COMPUTERS A.E.B.E. για την λήψη εξειδικευμένης τεχνικής υποστήριξης όποτε αυτό απαιτηθεί

Η τυπική διαδικασία που ακολουθείται κατά τη λήψη μιας κλήσης και οι ενέργειες οι οποίες εκτελούνται είναι οι ακόλουθες:

- **Λήψη Κλήσης:**

Ο πελάτης της COSMOS COMPUTERS A.E.B.E. έχει τη δυνατότητα να ενημερώνει το βλαβοληπτικό κέντρο με τους ακόλουθους τρόπους:

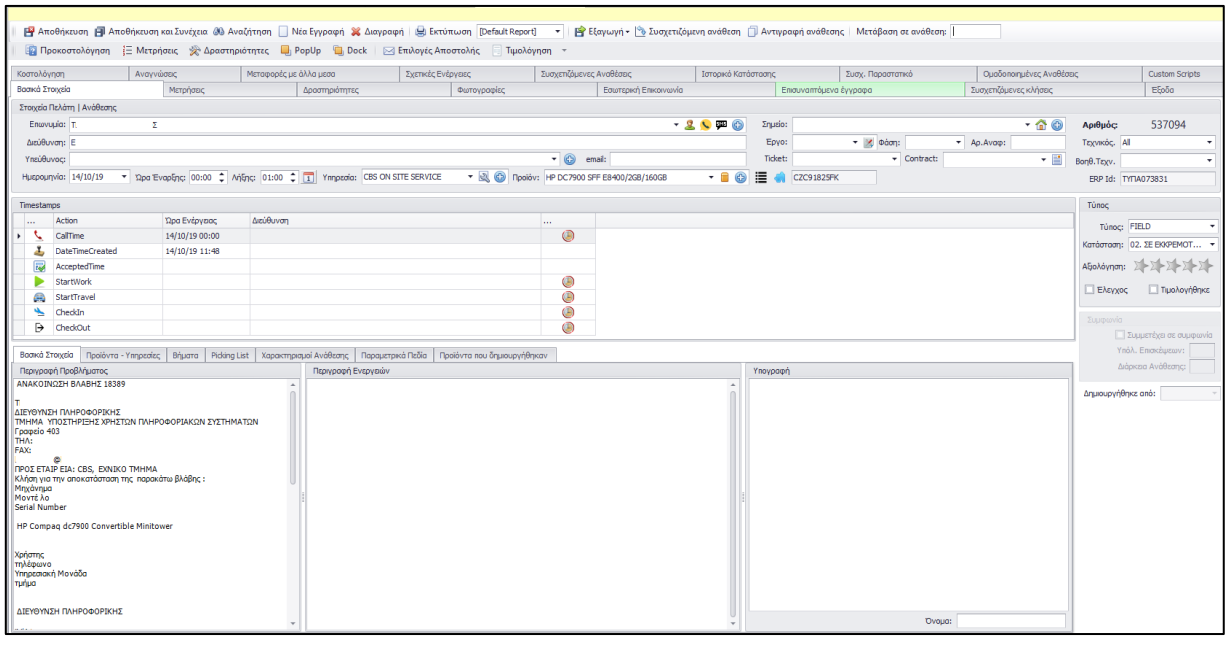
- **Τηλεφωνική επικοινωνία**: Με απευθείας κλήση στον αριθμό **210-6492800**
- **Ηλεκτρονικό ταχυδρομείο**: Με αποστολή mail στον λογαριασμό **servicedesk@cbs.gr** (κατόπιν αιτήματος του πελάτη και εφόσον τούτο προβλέπεται από το συμβόλαιο συντήρησης υπάρχει η δυνατότητα παροχής εξατομικευμένης διεύθυνσης ηλεκτρονικού ταχυδρομείου για αποκλειστική χρήση)
- **Τηλεομοιοτυπία**: Με αποστολή στον αριθμό **210-6464069**
- **Αυτοματοποιημένα, μέσω λογισμικού παρακολούθησης (NMS)** (στις περιπτώσεις όπου παρέχεται η δυνατότητα εκ μέρους του πελάτη και εφόσον τούτο προβλέπεται από το συμβόλαιο συντήρησης)



Εικόνα 1.Λίστα αιτημάτων τεχνικής υποστήριξης ρυθμισμένη ανά κατάσταση για πιο εύκολη διαχείριση

- **Καταγραφή κλήσης:**

Το στέλεχος του Call Center που δέχεται την κλήση, συμπληρώνει μια φόρμα στην οποία καταγράφει τις πληροφορίες που δίνει ο πελάτης και οι οποίες σχετίζονται με το αίτιο της κλήσης (βλάβη κτλ). Στη συνέχεια το περιεχόμενο της φόρμας καταχωρείται στο Αυτοματοποιημένο Σύστημα Κλήσεων σαν νέο συμβάν (Ticket):



Εικόνα 2.Εντολή τεχνικής υποστήριξης με την αρχική οθόνη

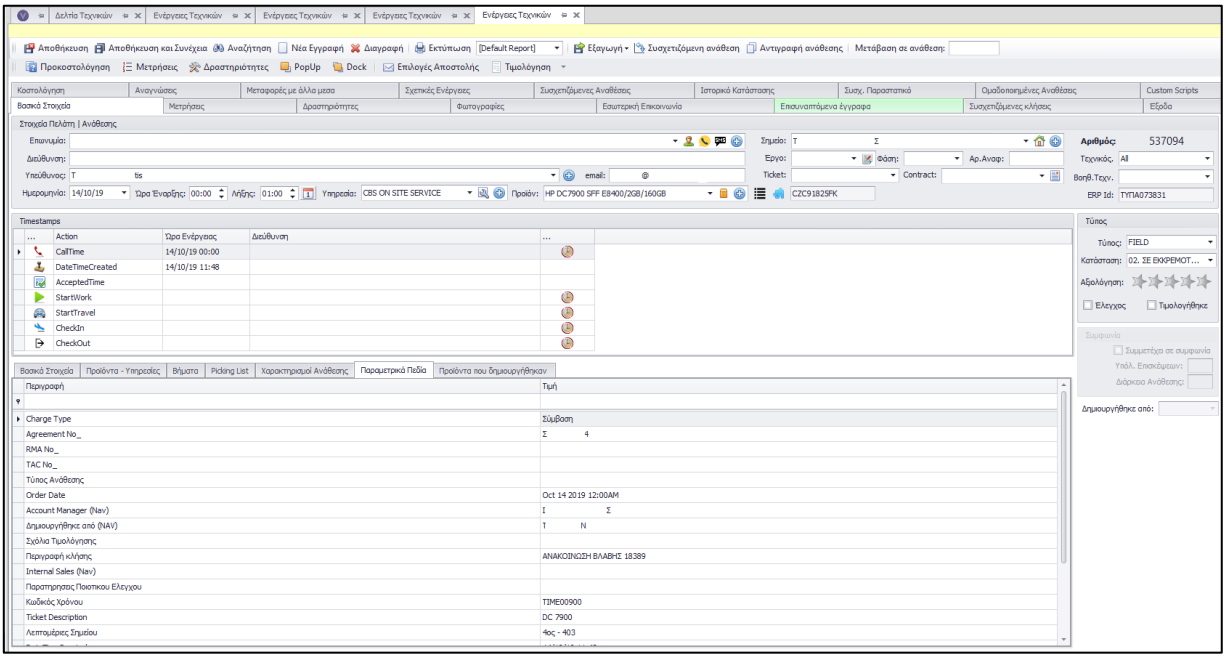
Ενδεικτικά, στην περίπτωση δυσλειτουργίας ή αιτήσεως συντήρησης, ένα ticket στο ιστορικό του περιλαμβάνει τις παρακάτω πληροφορίες:

- Ημερομηνία και ώρα ειδοποιήσεως-αναφοράς
- Ημερομηνία και ώρα ενάρξεως της συντήρησης

- Είδος δυσλειτουργίας που διορθώθηκε ή συντήρησης που πραγματοποιήθηκε
- Κατηγορία παρασχεθείσας υπηρεσίας συντήρησης
- Ημερομηνία και ώρα επαναλειτουργίας του συστήματος

Με την καταγραφή και καταχώρηση των πληροφοριών αυτών είναι εφικτή η:

- Διαχείριση των εισερχόμενων κλήσεων, ανάθεση καθηκόντων και δραστηριοτήτων, χρονοπρογραμματισμός και παρακολούθηση εργασιών
- Διαχείριση της εγκατεστημένης βάσης της υποδομής του πελάτη, με πλήρη καταγραφή του τύπου του εξοπλισμού, της συνολικής διάρθρωσης, των επιμέρους δομικών συστατικών του, καθώς επίσης και των σειριακών αριθμών.
- Διαχείριση Εγγυήσεων και Συμβολαίων Τεχνικής Υποστήριξης (SLAs) και των σχετιζόμενων με αυτά υποχρεώσεων ανταπόκρισης τεχνικής υποστήριξης και αποκατάστασης βλαβών
- Τήρηση αρχείου βλαβών
- Παραγωγή αναλυτικών και πλήρως προσαρμόσιμων αναφορών (reports)



Εικόνα 3.Συμπληρωματικά στοιχεία και πληροφορίες της κλήσης

➢ **Επικοινωνία με τον πελάτη και επίλυση του προβλήματος:**

Ο υπεύθυνος του Help Desk αναθέτει το συμβάν (ticket) στον αρμόδιο μηχανικό ο οποίος με την σειρά του επικοινωνεί με τον πελάτη το συντομότερο δυνατόν (και πάντα εντός του σχετικού χρόνου απόκρισης που ορίζεται από την σύμβαση συντήρησης SLA) για τη συγκέντρωση των απαραίτητων πληροφοριών που αφορούν την μορφή της βλάβης. Μόλις ολοκληρωθεί η μελέτη του προβλήματος, υπάρχουν οι παρακάτω επιλογές:

- Παροχής των κατάλληλων οδηγιών μέσω τηλεφώνου για την επίλυση του προβλήματος.
- Τηλε-διάγνωσης και τηλε-υποστήριξης μέσω απομακρυσμένης πρόσβασης στην υποδομή του πελάτη για επίλυση του προβλήματος (εφόσον παρέχεται η έγκριση εκ μέρους του πελάτη), με την τήρηση, πάντα, των σχετικών μέτρων ασφάλειας.

Εάν δεν δοθεί λύση με τους παραπάνω τρόπους, τότε αποστέλλεται τεχνικός στον χώρο του πελάτη για την αποκατάσταση της βλάβης. Εάν κάτι τέτοιο προβλέπεται από την σύμβαση συντήρησης, κατά τις μη εργάσιμες ημέρες και ώρες υπάρχει προσωπικό βάρδιας διαθέσιμο για την αντιμετώπιση των βλαβών (24x7x365). Στην περίπτωση που η εγκατεστημένη βάση του πελάτη βρίσκεται εκτός Αθηνών ή Θεσσαλονίκης το Help-Desk Office δρομολογεί την κλήση στα Τοπικά Κέντρα Υποστήριξης που ανήκουν στο **Πανελλαδικό Δίκτυο Συνεργατών** της.

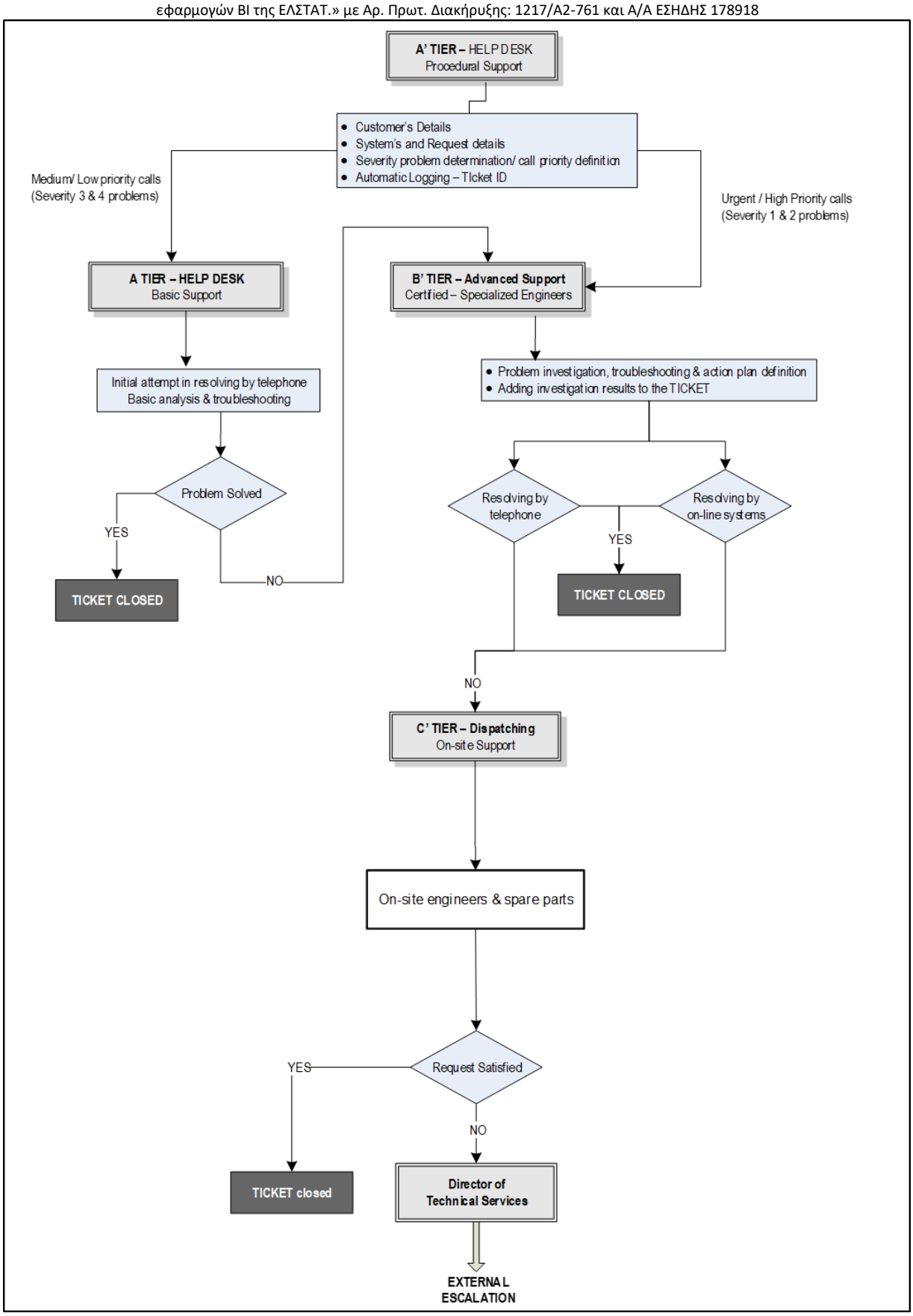
Στην περίπτωση που οι χρόνοι ανταπόκρισης και επίλυσης που προβλέπονται από το συμβόλαιο συντήρησης (SLA) κινδυνεύουν να μην δεν ικανοποιηθούν, το σύστημα ενημερώνει αυτόματα τους εμπλεκόμενους χειριστές σε συγκεκριμένα χρονικά διαστήματα για τις απαραίτητες ενέργειες (ανάθεση σε μηχανικό υποστήριξης 2^{ου} επιπέδου, επικοινωνία με τον κατασκευαστή κτλ.)

Τέλος, στην περίπτωση που απαιτηθεί η επισκευή κάποιου προϊόντος, παρέχεται η δυνατότητα επισκευής υλικού στις εγκαταστάσεις της COSMOS COMPUTERS A.E.B.E. η οποία, μεταξύ άλλων, αποτελεί **πιστοποιημένο επισκευαστικό κέντρο** (Authorized Service Provider) των κατασκευαστών **IBM**, **Lenovo**, **HP Inc**, **Hewlett Packard Enterprise**, **Avaya**, **Cisco** κ.α.

- **Παροχή αναφορών (Reports)**

Μέσω της υποδομής Service Desk υποστηρίζεται η δημιουργία αναφορών (reports), που περιλαμβάνουν τα στατιστικά των συμβάντων, ενδεικτικά: Ανοιχτά & κλειστά tickets ανα κατηγορία, χρόνους απόκρισης, αριθμό βλαβών ανα κατηγορία ή τοποθεσία κτλ. Γενικότερα για το σύνολο των αναφορών, εξασφαλίζεται η έκδοση περιοδικών, συγκεντρωτικών αναφορών ώστε να διευκολύνεται η παρακολούθηση και ο έλεγχος τήρησης των όρων της σύμβασης. Εφόσον το επιθυμεί ο πελάτης, οι αναφορές μπορούν να αποστέλλονται σε αυτόν σε εβδομαδιαία ή μηνιαία βάση.

Στο διάγραμμα ροής που ακολουθεί, παρουσιάζεται η διαδικασία παροχής τεχνικής υποστήριξης μέσω του Help Desk της COSMOS COMPUTERS A.E.B.E.:



Εικόνα 4.Διάγραμμα Helpdesk