ΠΑΡΑΡΤΗΜΑ Ι

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

1.1 Αντικείμενο του Έργου

Το έργο που θα υλοποιηθεί, έχει ως αντικείμενο την ενίσχυση της ηλεκτρονικής και δικτυακής ασφάλειας του οργανισμού, στα πλαίσια των αναγκών και των αυξημένων απαιτήσεων της σύγχρονης εποχής και της ανακοινωθείσας εθνικής στρατηγικής για την κυβερνοασφάλεια 2021-2025.

Ειδικότερα, το Έργο αφορά την ολοκληρωμένη ανάπτυξη ενιαίου συστήματος κυβερνοασφάλειας, με όλες τις απαραίτητες άδειες χρήσης.

Το Έργο θα αναπτυχθεί στις υποδομές του Ε.Κ.Κ.Α. , προκειμένου να προσφέρει προστασία σε ολιστικό επίπεδο με αυτοματοποιημένους μηχανισμούς αναφοράς και αντιμετώπισης προκειμένουν να διασφαλιστεί η επιχειρησιακή συνέχεια και η ακεραιτότητα των συστημάτων και πληροφοριών του οργανισμού.

Τελικός στόχος είναι η θωράκιση της υπάρχουσας υποδομής των πληροφοριακών συστημάτων του οργανισμού καθώς και των υποστηριζόμενων ιστοσελίδων και υπηρεσιών που είναι διαθέσιμα στο κοινό, η εγκατάσταση και παραμετροποίηση δικτυακών και διαδικτυακών συστημάτων ελέγχου, καθώς και η προσθήκη νέων μέτρων ασφάλειας στο συνολικό δίκτυο των πληροφοριακών συστημάτων του οργανισμού.

Ακολούθως, βάσει των νέων μεθοδολογιών και αλγορίθμων ελέγχου της δικτυακής και διαδικτυακής επικοινωνίας των πληροφοριακών συστημάτων, θα προσδιοριστούν και θα θωρακισθούν έναντι κυβερνοεπιθέσεων όλα τα τρωτά σημεία στο σύνολο του δικτύου Η/Υ του οργανισμού που θα εντοπίσουν τα εγκατασταθησόμενα συστήματα. Τα ευρήματα και οι θωρακίσεις αυτών θα είναι συνεχώς διαθέσιμα σε αναλυτική αναφορά, όπου και θα αποτυπώνεται σε κάθε στιγμή και σε πραγματικό χρόνο, η τρέχουσα κατάσταση ασφάλειας του συνολικού δικτύου και υποδομών του οργανισμού και η διαδραστικότητα μεταξύ χρηστών, υποδομής και εν δυνάμει εισβολέων στην υποδομή.

Για την διασφάλιση της ασφαλούς επικοινωνίας των πληροφοριακών συστημάτων του Ε.Κ.Κ.Α. , καθώς και για την ασφαλή επεξεργασία των εγγράφων, αρχείων και πληροφοριών, η εγκατάσταση και παραμετροποίηση νέων συστημάτων ελέγχου και προστασίας του δικτύου Η/Υ του Ε.Κ.Κ.Α. κρίνεται απαράβατη.

Τα συστήματα ελέγχου που θα εγκατασταθούν από τον ανάδοχο, θα πρέπει να είναι ικανά να εκτελούν τις ακόλουθες διαδικασίες-διεργασίες:

• Με αυτοματοποιημένες διαδικασίες, να εντοπίζουν, να κατηγοριοποιούν και να απομονώνουν οποιαδήποτε ενέργεια ή προσπάθεια η οποία δεν συνάδει με την γνωστή συμπεριφορά των Η/Υ.

• Να αντιμετωπίζουν σε πραγματικό χρόνο, με βάση την παραμετροποίηση που έχει γίνει, τις απειλές που έχουν αναγνωριστεί, εκτελώντας τις κατάλληλες ενέργειες για την αντιμετώπισή τους.

• Να καταγράφουν όλα τα στοιχεία-δεδομένα (μη προσωπικού χαρακτήρα) του δικτύου Η/Υ με τα χαρακτηριστικά τους, όπως επίσης και τις αλλαγές που προκύπτουν στη ροή του χρόνου, παρέχοντας τη δυνατότητα αναγνώρισης "ξένων" οντοτήτων, απρόβλεπτων μεταβολών ή απωλειών.

• Να αναγνωρίζουν κακόβουλες ή επικίνδυνες ενέργειες, καθώς και να τις καταγράφουν για περαιτέρω διερεύνηση.

• Να αναγνωρίζουν σε κάθε σύστημα/υποσύστημα υπάρχοντα τρωτά σημεία που εντοπίζουν και αποτελούν είτε αιτία επίθεσης, είτε εν δυνάμει κίνδυνο, παρέχοντας παράλληλα και τον προτεινόμενο τρόπο αντιμετώπισης και διόρθωσης κάθε εκάστοτε περίπτωσης.

• Να παρακολουθούν και μελετούν την ευρύτερη συμπεριφορά χρηστών και υπολογιστών μέσα στο δίκτυο για την αναγνώριση περίεργων συμπεριφορών που δύνανται να συνιστούν περιπτώσεις εισβολής ή ρήγματος ασφαλείας.

• Να παρέχουν ασφάλεια με χρήση τεχνικών τεχνητής νοημοσύνης σε κάθε Device, Application και Network του Ε.Κ.Κ.Α.

• Να παρέχει πρόληψη απώλειας δεδομένων και να διασφαλίζει ότι οι κρίσιμες και ευαίσθητες πληροφορίες δεν αποστέλλονται εκτός του δικτύου του Ε.Κ.Κ.Α.

Για την εφαρμογή των εν λόγω μέτρων ασφαλείας που θα εφαρμοστούν από τον εγκατασταθησόμενο εξοπλισμό και συστήματα, θα πρέπει να προσδιορισθούν όλα τα επίπεδα εκτέλεσης και εφαρμογής τους, καθώς και να διεξαχθούν ασκήσεις ετοιμότητας περιστατικών, για την διασφάλιση των πληροφοριακών συστημάτων, την τήρηση των μέτρων ασφαλείας κατά τη χρήση τους. Το προσωπικό του Ε.Κ.Κ.Α. θα πρέπει να εκπαιδευθεί στα νέα συστήματα ελέγχου που θα εγκατασταθούν.

Στα πλαίσια του παρόντος έργου ο Ανάδοχος αναλαμβάνει:

Α. Την Προμήθεια, εγκατάσταση, παραμετροποίηση και την θέση σε λειτουργία του του υπό προμήθεια εξοπλισμού, ο οποίος θα εγκατασταθεί στο data center της Αναθέτουσας Αρχής.

Β. Την προμήθεια, εγκατάσταση, παραμετροποίηση, ανάπτυξη ενιαίου συστήματος κυβερνοασφάλειας, με όλες τις απαραίτητες άδειες χρήσης και υποστήριξης, των δικτυακών και διαδικτυακών συστημάτων ελέγχου, καθώς και η προσθήκη νέων μέτρων ασφάλειας, στο συνολικό δίκτυο των πληροφοριακών συστημάτων του οργανισμού.

Γ. Την Δωρεάν συντήρηση του συστήματος, του εξοπλισμού, του έτοιμου λογισμικού, την τεχνική υποστήριξη και την υποστήριξη των χρηστών, την παροχή υπηρεσιών ασφαλείας για τα επόμενα τρία έτη από την Οριστική Παραλαβή του έργου

Στόχοι του Έργου

1. Θωράκιση του Ε.Κ.Κ.Α. από κυβερνοεπιθέσεις-κυβερνοαπειλές
2. Δημιουργία ενιαίου μηχανισμού αναφοράς περιστατικών.
3. Παραγωγή αναφορών σε πραγματικό χρόνο

4. Εφαρμογή μέτρων πρόληψης και προστασίας

1.2 Παραδοτέα

- ✓ Μελέτη Εφαρμογής
- ✓ Ηλεκτρονικός εξοπλισμός για την εγκατάσταση του συστήματος κυβερνοασφάλειας
- ✓ Λογισμικό συστήματος και εφαρμογών με άδειες χρήσης για 36 μήνες

✓ Εγκατάσταση και παραμετροποίηση και θέση του σε λειτουργεία του Εξοπλισμού, ΛογισμικούΣυστήματος και Εφαρμογών

✓ Εγχειρίδιο περιγραφής και λειτουργίας του πληροφορικού συστήματος

- ✓ Εκπαίδευση

1.3 Αρχιτεκτονική Συστήματος

Η προτεινόμενη αρχιτεκτονική πρέπει να εγγυάται την υψηλή ποιότητα και αποτελεσματική υποστήριξη για την συλλογή δεδομένων, την ανάλυση και επεξεργασία τους και την τελική αξιοποίηση τους από το σύστημα.

Η σχεδίαση της δικτυακής αρχιτεκτονικής του συστήματος θα γίνει με βάση τις λειτουργικές προδιαγραφές, οι οποίες θα προσδιοριστούν στην Μελέτη Εφαρμογής.

Για την ανάπτυξη της απαιτούμενης λειτουργικότητας, ο Ανάδοχος θα πρέπει να προτείνει: α) τη βέλτιστη προτεινόμενη αρχιτεκτονική, β) τις προτεινόμενες διαδικασίες συλλογής δεδομένων και γ) τρόπους αυτοματοποιημένων αποκρίσεων σε περιστατικά.

Οι χρήστες θα πρέπει να μπορούν να επικοινωνούν με το Πληροφορικό Σύστημα πλοηγούμενοι μέσα από διαδεδομένους WEB Browser (Internet Explorer, Mozilla, Chrome κτλ.). Ο χρήστης θα έχει τη δυνατότητα καταχώρισης ερωτημάτων αναζήτησης, στα οποία το σύστημα θα ανταποκρίνεται αντλώντας τη σχετική πληροφορία από τις αντίστοιχες βάσεις δεδομένων και παρουσιάζοντας τη στο λεγόμενο επίπεδο παρουσίασης (presentationlayer). Η ανακτώμενη πληροφορία θα διατίθεται και σε εκτυπώσιμη μορφή.

Συνοπτικά ο υποψήφιος ανάδοχος πρέπει να παρέχει μια ολοκληρωμένη λύση Πληροφοριακού Συστήματος, η οποία θα αποτελείται από:

- ✓ Τον εξοπλισμό, το λογισμικό λειτουργικών συστημάτων και τα λογισμικά ανάπτυξης του Πληροφοριακού Συστήματος
- ✓ Τη μελέτη και το σχεδιασμό του λογικού μοντέλου δεδομένων του Πληροφοριακού Συστήματος
- ✓ Την εκπαίδευση χρηστών

✓ Την υποστήριξη λειτουργίας του Πληροφοριακού Συστήματος (helpdesk γιαόλα τα επίπεδα των χρηστών)

- ✓ Την εγγύηση καλής λειτουργίας
- ✓ Την εγγύηση συντήρησης

Απαιτήσεις Αρχιτεκτονικής Συστήματος

Το Σύστημα πρέπει να είναι «ανοικτής» αρχιτεκτονικής (open architecture) και θα χρησιμοποιεί πρότυπα που θα διασφαλίζουν:

- ✓ Την ομαλή συνεργασία και λειτουργία μεταξύ των επιμέρους λειτουργικών εφαρμογών της ολοκληρωμένης λύσης.
- ✓ Τη δικτυακή συνεργασία μεταξύ εφαρμογών ή / και συστημάτων, τα οποία βρίσκονται σε διαφορετικά υπολογιστικά συστήματα (π.χ. firewalls, servers κτλ).
- ✓ Η αρχιτεκτονική του συστήματος θα πρέπει να υποστηρίζει την πλήρη διασυνδεσιμότητα με τρίτα συστήματα ανεξάρτητα των τεχνολογιών ανάπτυξής τους.

Η ανοιχτή αρχιτεκτονική θα ακολουθηθεί, τόσο σε επίπεδο εξοπλισμού (εύκολη διασύνδεση, επέκταση, αντικατάσταση μερών, κ.λ.π.), όσο και σε επίπεδο λογισμικού εφαρμογών.

1.4 Τεχνολογίες και σχέδιο υλοποίησης Έργου

Ο υποψήφιος Ανάδοχος θα πρέπει να προτείνει μια ολοκληρωμένη λύση. Η προτεινόμενη πλατφόρμα θα πρέπει να αποτελεί μια ολοκληρωμένη λύση XDR (Extended Detection & Response) με χαρακτηριστικά και λειτουργίες Next Gen SOC, η οποία να εξασφαλίζει την κεντρική παρακολούθηση και διαχείριση, αποφεύγοντας τις παλαιού τύπου τεχνικές με την εγκατάσταση διαφορετικών ξεχωριστών απλών εργαλείων SIEM (Security Information & Events Management) και άλλων που εγκαθίσταται και διαχειρίζονται ξεχωριστά ή απαιτείται χειροκίνητη ξεχωριστή διαδικασία ενσωμάτωσής του.

Η πλατφόρμα πρέπει να έχει τη δυνατότητα συλλογής και επεξεργασίας από πολλαπλών τύπων πηγές δεδομένων και όχι μόνο αρχείων καταγραφής, κινούμενη στη φιλοσοφία του big data security analytics. Συνδυάζοντας πληροφορίες από δικτυακή κίνηση (network traffic), user data, cloud data, file data στόχος είναι η εξάλειψη πιθανών τυφλών σημείων και ο συσχετισμός όλων των δεδομένων για την παραγωγή καλύτερων αποτελεσμάτων. Μέσα από αυτοματοποιημένες διαδικασίες εμπλουτισμού και συσχετισμών, τα δεδομένα θα βελτιστοποιούνται για αξιοποίηση από μηχανισμούς έρευνας και εντοπισμού. Ειδικότερα δε με την εκμετάλλευση αυτοματοποιημένης επεξεργασίας και μηχανικής μάθησης, το σύστημα θα πρέπει να μπορεί να λειτουργεί αποτελεσματικά ως ένα ολοκληρωμένο κέντρο αναφοράς και αυτόματης πρότασης και λήψης αντιμέτρων. Το σύστημα θα πρέπει κατ'ελάχιστον να συνοδεύεται από τεχνολογίες SIEM, Sandbox, NTA, Threat Itelligence και IDS και να μην απαιτείται η ξεχωριστή προμήθεια λογισμικού.

Το προσφερόμενο σύστημα θα πρέπει να έχει τη δυνατότητα να υποστηρίζει και το μοντέλο MDR (Managed Detection & Response) και στο σύνολό του θα πρέπει να υποστηρίζει όλο τον κύκλο ζωής αναγνώρισης και αντιμετώπισης απειλών, που αναλύεται στα στάδια:

- Συλλογή (Collect)
- Εντοπισμός (Detect)
- Έρευνα (Investigate)
- Απόκριση (Respond)

Χαρακτηριστικά Next Gen Soc

1 Μοντέρνο περιβάλλον χρήσης (GUI) που ενσωματώνει όλες τις απαραίτητες λειτουργίες παρακολούθησης και διαχείρισης.

2 Πρόσβαση με χρήση ρόλων χρηστών (RBAC - Role Based Access) για την διαχείριση δικαιωμάτων (user privilege management)

3 Υποστήριξη πολλαπλών ενοίκων (multi-tenant) για την ξεχωριστή διαχείριση οντοτήτων, φυσικών δικτύων κτλ

4 Εφαρμογή ξεχωριστού μοντέλου μηχανικής μάθησης ανά tenant για τη βελτίωση της ακρίβειας των αποτελεσμάτων και τη μείωση των εσφαλμένων θετικών συμβάντων (false positives), εφαρμόζοντας ξεχωριστά συμπεριφορικά μοντέλα.

5 Εξελιγμένες δυνατότητες μηχανικής μάθησης που να συμπεριλαμβάνουν τόσο supervised όσο και unsupervised διαδικασίες, τεχνολογίες graph ML και να συνδυάζονται μεταξύ τους για την παραγωγή βέλτιστων αποτελεσμάτων

6 Δυνατότητες ενσωμάτωσης με εργαλεία και τεχνολογίες ασφαλείας όπως Firewalls, WAF, SWG, EDR, SOAR κτλ

7 Υποστήριξη API για ενσωμάτωση με άλλες τεχνολογίες όπως HoneyPots, εργαλεία OSINT κτλ.

8 Μία ενοποιημένη, υψηλής απόδοσης, αποθήκη δεδομένων (“Big Data” High Speed Lake)

9 Δυνατότητα εγκατάστασης τόσο σε φυσικό εξοπλισμό, όσο και σε εικονικό ή περιβάλλον cloud

10 Κατανεμημένη και επεκτάσιμη αρχιτεκτονική που να υποστηρίζει ωστόσο και “All In One” σενάρια.

11 Υψηλή διαθεσιμότητας με τη χρήση clusters και ευέλικτη τήρηση και αποθήκευση δεδομένων.

12 Μηχανισμοί Συλλογής που να μπορούν να εγκατασταθούν τόσο σε φυσικό όσο και σε εικονικό περιβάλλον

13 Το σύστημα θα πρέπει να ακολουθεί ανοιχτή αρχιτεκτονική που να επιτρέπει την εισαγωγή δεδομένων από οποιαδήποτε συσκευή με τη χρήση Integration APIS.

14 Κεντροποιημένη διαχείριση

15 Απλό ενοποιημένο μοντέλο αδειών χωρίς επιπλέον κόστη

Next-Generation SIEM

Η πλατφόρμα θα πρέπει να βασίζεται σε μια ενοποιημένη αποθήκη δεδομένων βασισμένη στην αρχιτεκτονική του big data lake. Τα δεδομένα θα πρέπει κατ’ ελάχιστον να μπορούν να εισαχθούν μέσω syslog. Όπου είναι εφικτό θα πρέπει να παρέχεται η

δυνατότητα χρήσης parsers για τις κυριότερες και δημοφιλέστερες λύσεις δικτύων και ασφαλείας ώστε οι πληροφορίες να κανονικοποιούνται και να συσχετίζονται με αυτοματοποιημένο τρόπο. Θα πρέπει να παρέχονται οι παρακάτω ελάχιστες λειτουργικότητες:

1 Απλός όσο και εξεζητημένος μηχανισμός αναζήτησης που να βασίζεται σε λογικούς τελεστές (Boolean modifiers)

2 Οι αναζητήσεις να μπορούν να εφαρμοστούν ως μόνιμα φίλτρα σε όλο το περιβάλλον για ταχύτερη διερεύνηση και ανάλυση περιστατικών.

3 Υψηλής απόδοσης και άμεσες ανταποκρίσεις στην αναζήτηση και το φιλτράρισμα στο big data

4 Πρόσβαση σε όλες τις πηγές δεδομένων και όχι μόνο σε syslog δεδομένα

5 Συλλογή δεδομένων από δικτυακή κίνηση (μέσω TAP ή Mirror Traffic). Τα πακέτα θα πρέπει να γίνονται reduce, να κανονικοποιούνται και να μετατρέπονται σε αξιοποιήσιμα μετα-δεδομένα για την ενσωμάτωση στο big data lake.

6 Συλλογή δεδομένων από user sources όπως το Microsoft AD μέσω API Connector

7 Συλλογή δεδομένων από πηγές νέφους (cloud) όπως Office365 μέσω Connectors

8 Τα δεδομένα από όλες τις πηγές πρέπει να κανονικοποιούνται, να εμπλουτίζονται και να συσχετίζονται αυτόματα από το σύστημα

9 Στις πηγές εμπλουτισμού πρέπει να περιλαμβάνονται γεωγραφικού προσδιορισμού (Geo-Awareness), IP Reputation, Threat Intelligence και DPI Application awareness.

10 Μοντέρνο περιβάλλον χρήστη με λειτουργίες SIEM που περιλαμβάνουν ερωτήματα και δημιουργίες κανόνων.

11 Πρόσθετο για παραδοσιακή απεικόνιση SIEM (π.χ. Kibana)

Εντοπισμός KillChain (KillChain Detections)

(συμπεριλαμβάνοντας IDS/Exploit, Malware και APT Sandboxing, Anti-Phishing κτλ.)

1. Το σύστημα πρέπει να έχει ενσωματωμένους μηχανισμούς εντοπισμών σε κάθε φάση του CyberSecurity KillChain, συμπεριλαμβάνοντας Reconnaissance, Delivery, Exploitation, Installation, Command & Control, and Actions & Exfiltrations

2. Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη βάση υπογραφών IDS, ενισχυμένη από ανάλυση μηχανικής μάθησης (ML-IDS)

3. Η πλατφόρμα πρέπει να υποστηρίζει πολλαπλά Threat Intelligence Feeds,

συμπεριλαμβάνοντας εμπορικές πηγές, open-source, anti-phising κ.α.

4. Η πλατφόρμα πρέπει να επιτρέπει ενσωμάτωση με 3rd party feeds μέσω STIX/TAXII και/η MISP

5. Η πλατφόρμα πρέπει να έχει ενσωματωμένες δυνατότητες APT Sandboxing για να αναγνωρίζει και να περιορίζει άγνωστα αρχεία, όπως επίσης και για εντοπισμό ransomware, spyware.

Ανάλυση Δικτύου (Network Traffic Analysis)

Με την επιθεώρηση της δικτυακής κίνησης σε πραγματικό χρόνο, η πλατφόρμα πρέπει να μπορεί να μοντελοποιήσει την κίνηση για αναγνώριση παράτυπων συμπεριφορών και ειδοποιήσεων.

1. Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα Deep Packet Inspection (DPI) για την αναγνώριση τουλάχιστον 4000 εφαρμογών και να δομεί σχετικά συμπεριφορικά μοντέλα.

2. Τα δεδομένα κίνησης δικτύου πρέπει να μετασχηματίζονται σε κατάλληλα μετα-δεδομένα που περιλαμβάνουν και το payload, για την αντίστοιχη προαιρετική μείωση της ανάγκης αποθηκευτικών χώρων.

3. Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα NTA Detections, συμπεριλαμβάνοντας Application Usage Anomalies, Long App Session Anomalies, και Unapproved Asset Activity

4. Το σύστημα θα πρέπει να εντοπίζει ανωμαλίες στη συμπεριφορά των Firewalls, όπως denial anomalies ή rule usage anomalies

User Behavior Analytics (UBA)

Σε συνδυασμό με την ανάλυση πακέτων, το σύστημα θα πρέπει να μπορεί να συνδεθεί με πηγές δεδομένων χρηστών, όπως το MS Active Directory

1. Το σύστημα πρέπει να πραγματοποιεί ανάλυση και εντοπισμό ανωμαλιών στη συμπεριφορά του χρήστη (user behavior)

2. Το σύστημα πρέπει να ενσωματώνει μοντέλα εντοπισμού ανωμαλιών όπως αδύνατου ταξιδιού (Impossible Travel Anomaly) ή ώρες αυθεντικοποίησης (Log In Time Anomaly)

3. Όπως και με τους εντοπισμούς NTA, έτσι κι εδώ όλα τα detections και τα σχετικά events στα logs και σε άλλες πηγές πρέπει να συσχετίζονται αυτόματα.

Endpoint Behavior Analytics (EBA)

Όπως με τα αναλυτικά δεδομένα δικτύου και χρηστών, το σύστημα πρέπει να μπορεί να συλλέγει δεδομένα από assets/endpoints στο περιβάλλον, να εκτελεί analytics και να εντοπίζει συμπεριφορικές ανωμαλίες.

1. Το σύστημα θα πρέπει να μπορεί να εισάγει δεδομένα από τρίτα συστήματα εντοπισμού ευπαθειών (vulnerability scanners) όπως Nessus, Tenable, Rapid7 και να συσχετίζει τα ευρήματα με σχετικά γεγονότα ασφαλείας.

2. Το σύστημα θα πρέπει να μπορεί να ανακαλύψει όλα τα assets σε ένα περιβάλλον και να τα κατηγοριοποιεί με βάση τη διεύθυνση MAC και IP.

3. Η λίστα των ανακαλυφθέντων/εντοπισθέντων assets θα πρέπει να μπορεί να επαυξάνεται και να παραμετροποιείται με τη χρήση αρχείων csv με λίστες assets και περιγραφές.

4. Το σύστημα πρέπει να μπορεί να καταγράφει όλους τους συσχετισμούς με ένα asset με IP διευθύνσεις, ιστορικά στοιχεία για τη χρήση εφαρμογών κτλ.

Ορατότητα Δικτύου και Υπηρεσιών (Network & Service Visibility)

Το σύστημα θα πρέπει να περιλαμβάνει δυνατά εργαλεία απεικόνισης δικτύων και υπηρεσιών, μαζί με analytics, με στόχο να προσφέρει ορατότητα στις επιδόσεις δικτύου (network performance), application usage κτλ.

Κυνήγι Απειλών και Διερεύνηση (Threat Hunting & Investigation)

Με όλες τις πηγές δεδομένων στο unifed data lake, τα κανονικοποιημένα και συσχετισμένα δεδομένα πρέπει να είναι διαθέσιμα για διερεύνηση και threat hunting οποιαδήποτε στιγμή.

1. Το σύστημα πρέπει να έχει ενσωματωμένα σχετικά εργαλεία, προκαθορισμένες αναζητήσεις και ερωτήματα, όπως επίσης και οπτικοποιήσεις (visualizations).

2. Τα visualizations πρέπει να είναι παραμετροποιήσιμα

3. Το σύστημα πρέπει να προσφέρει εξελιγμένες δυνατότητες όπως συσχετισμένες αναζητήσεις, που επιτρέπουν στους αναλυτές να συνδέσουν πολλαπλά ανεξάρτητα ερωτήματα με κοινά κριτήρια προκειμένου να δομήσουν πληροφορίες από attack sequences ή να απομονώσουν κοινές πληροφορίες.

4. Όλα τα ερωτήματα θα πρέπει να μπορούν να αποθηκευθούν, επεξεργαστούν, κλωνοποιηθούν κτλ από τους χρήστες.

5. Τα visualizations πρέπει να μπορούν να αποθηκευθούν σαν custom dashboards.

6. Τα ερωτήματα θα πρέπει να μπορούν να συνδυαστούν με ενέργειες/αποκρίσεις για PlayBooks

Playbooks / Integrated Orchestration & Response (SOAR)

1. Το σύστημα πρέπει να συμπεριλαμβάνει μια βιβλιοθήκη με έτοιμα ενσωματωμένα playbooks, που είναι αυτό-εκτελέσιμα ερωτήματα με ενσωματωμένες ενέργειες.
2. Οι ενσωματωμένες ενέργειες/αποκρίσεις θα πρέπει να συμπεριλαμβάνουν
    - Alerts - Αποστολή e-mail/slack message κτλ
    - Actions – Άνοιγμα ενός case, εκτέλεση μια εντολής API, δημιουργία ενός security event κτλ
    - Responses – Μπλοκάρισμα μιας IP στο

Firewall, απενεργοποίηση ενός χρήστη στο AD, εκτέλεση δέσμης ενεργειών κτλ

3. Παράλληλα με τις αυτοματοποιημένες ενέργειες, πολλές από τις εξωτερικές ενέργειες όπως το μπλοκάρισμα μια IP ή ενός χρήστη θα πρέπει να είναι διαθέσιμες στο χρήστη μέσω του UI ώστε να μπορούν παράλληλα να υλοποιηθούν ως μέρος διερεύνησης/αντιμετώπισης ή ανάλυσης.
4. Δυνατότητα ενσωμάτωσης με ήδη έτοιμα εμπορικά εργαλεία SOAR

Επιπλέον Δυνατότητες

Ειδοποιήσεις (Alarming)

1. Το σύστημα θα πρέπει να προσφέρει έναν έξυπνο, μοντέρνο και παραμετροποιήσιμο μηχανισμό ειδοποιήσεων που να δύναται να οριστεί με βάση παραλήπτες και άλλα κριτήρια (score severity, killchain category, etc.)
2. Οι ειδοποιήσεις πρέπει να μπορούν να αποσταλούν με email ή slack μηνύματα και τα μηνύματα πρέπει να είναι παραμετροποιήσιμα ως προς το περιεχόμενο και τα σχετικά δεδομένα.

Αναφορές (Reporting)

1. Το σύστημα πρέπει να περιέχει ένα σύγχρονο εξελιγμένο μηχανισμό αναφορών που θα επιτρέπει παράλληλα εύκολη δημιουργία νέων αναφορών με drag and drop και αποθήκευσή τους για χρήση σε οποιοδήποτε σημείο.
2. Οι αναφορές θα πρέπει επίσης να παράγονται με χρονοπρογραμματισμό και να αποστέλλονται σε διαφορετικούς χρήστες.
3. Οι αναφορές πρέπει να είναι δυνατόν να αποστέλλονται με email σαν pdf ή csv ή να γράφονται σε αρχείο.
4. Το σύστημα θα πρέπει να περιλαμβάνει πληθώρα έτοιμων αναφορών και templates.

Portal

1. Πρόσβαση των χρηστών βάση ρόλου (User RBAC access) στο Portal με συνολική ή περιορισμένη πρόσβαση στις πληροφορίες.
2. Custom Dashboards ανά ρόλο χρήστη.
3. Χρονοπρογραμματισμένες αναφορές για κάθε tenant, tenant group και RBAC users.
4. Η πρόσβαση των χρηστών πρέπει να μπορεί να περιορίζεται σε Read-Only, limited view, μέχρι full visibility and access.

1.6 Χρονοδιάγραμμα και Φάσεις Έργου

Α/Α	***Τίτλος Φάσης***	***1ος Μήνας***	***2ος Μήνας***	***3ος Μήνας***	***4ος Μήνας***

1	***Μελέτη Εφαρμογής***				
2	***Προμήθεια, εγκατάσταση και παραμετροποίηση εξοπλισμού και λογισμικού συστήματος κυβερνοασφάλειας***				
3	***Εκπαίδευση***				
4	***Πιλοτική λειτουργία***				
5	***Παραγωγική λειτουργία***				

Φάσεις Έργου

Φάση Νο	**1**	**Τίτλος**	Μελέτη Εφαρμογής
Μήνας Έναρξης	**1**	**Μήνας Λήξης**	**1**
1 Μήνας			
Στόχοι Η μελέτη εφαρμογής αφορά στην αποτύπωση και οριστικοποίηση των προδιαγραφών υλοποίησης του συστήματος κυβερνοασφάλειας			
Περιγραφή Υλοποίησης Η μελέτη εφαρμογής θα περιλαμβάνει κατ' ελάχιστον τα παρακάτω: τις παρακάτω απαιτήσεις / ενέργειες: Σχέδιο Διαχείρισης και Ποιότητας Έργου (ΣΔΠΕ) Τον πλήρη και λεπτομερή σχεδιασμό του συνολικού συστήματος (μοντέλο υλοποίησης και αρχιτεκτονικής δικτύου, διαγράμματα μεταφοράς δεδομένων, ρόλοι χρηστών διασυνδεσιμότητα εφαρμογών,κτλ.). Πλήρη και αναλυτική περιγραφή όλου του λογισμικού που θα αναπτυχθεί (ρόλος, σκοπός, χρησιμοποιούμενη τεχνολογία κλπ) Πλήρη περιγραφή όλου του έτοιμου λογισμικού που θα χρησιμοποιηθεί. Αναλυτικό χρονοδιάγραμμα υλοποίησης με πρόβλεψη για όλα τα παραδοτέα και τον απαιτούμενο χρόνο ελέγχου/αποδοχής τους. Τον προσδιορισμό της μεθοδολογίας και των αρχικών σεναρίων ελέγχου αποδοχής καθώς και τον καθορισμό της μεθόδου καταγραφής δεικτών απόδοσης των συστημάτων και εφαρμογών. Τον προγραμματισμό τεκμηρίωσης (Documentation Plan) για το συνολικό σύστημα. Περιγραφή ρόλων χρηστών (job descriptions) Πηγή αναλυτικών δεδομένων εισόδου(inputs). Μελέτη διαλειτουργικότητας και διασυνδεσιμότητας με τρίτες εφαρμογές Καθορισμό των απαιτήσεων εκπαίδευσης ανά ομάδα εκπαιδευομένων για την λειτουργία του συστήματος και των υποσυστημάτων του έργου			
Παραδοτέα Π.1: Μελέτη εξειδίκευσης τεχνικών προδιαγραφών υποδομής έργου			

Φάση Νο	**2**	**Τίτλος**	Προμήθεια, εγκατάσταση και παραμετροποίηση εξοπλισμού και λογισμικού κυβερνοασφάλειας
Μήνας Έναρξης	**1**	**Μήνας Λήξης**	**2**
2 Μήνες			
Στόχοι Προμήθεια εξοπλισμού και λογισμικού συστήματος κυβερνοασφάλειας. Εγκατάσταση εξοπλισμού και λογισμικού συστήματος κυβερνοασφάλειας. Παραμετροποίηση πληροφοριακών συστημάτων και λογισμικού συστήματος Διενέργεια δοκιμών κυβερνοασφάλειας			
Περιγραφή Υλοποίησης Περιλαμβάνει το σύνολο του απαιτούμενου εξοπλισμού για την υλοποίηση του έργου την εγκατάσταση του και παραμετροποίηση του. Εγκατάστασή λογισμικού συστήματος και θέση του σε λειτουργία			
Παραδοτέα Π.2: Προμήθεια εξοπλισμού και λογισμικού συστήματος Π.2.1:Εγκατάσταση εξοπλισμού και λογισμικού συστήματος κυβερνοασφάλειας, παραμετροποίηση και θέση του σε λειτουργία. Π.2.2 : Διενέργεια σεναρίων ελέγχου Π.2.3 : Αποτελέσματα διενέργειας σεναρίων ελέγχου Π.2.4 :Εκσφαλμάτωση			

Φάση Νο	**3**	**Τίτλος**	Εκπαίδευση
Μήνας Έναρξης	**3**	**Μήνας Λήξης**	**3**
1 Μήνας			
Στόχοι Εκπαίδευση χρηστών / διαχειριστών του συστήματος			
Περιγραφή Υλοποίησης Οι δράσεις εκπαίδευσης, χρηστών περιλαμβάνουν: Την εκπαίδευση διαχειριστών του συστήματος.			
Παραδοτέα Π.3. : Εκπαίδευση Π.3.1: Πρόγραμμα εκπαίδευσης Π.3.2: Εκπαιδευτικό υλικό Π.3.3: Έκθεση ολοκλήρωσης			

Φάση Νο	**4**	**Τίτλος**	Πιλοτική λειτουργία.
Μήνας Έναρξης	**3**	**Μήνας Λήξης**	**3**
1 Μήνας			

Στόχοι Πιλοτικής λειτουργίας

Περιλαμβάνει όλες τις απαραίτητες ενέργειες για την εξασφάλιση της ομαλής μετάβασης στην κανονική λειτουργία του έργου με την υποστήριξη από τον ανάδοχο.

Εκπαίδευση (on the job training) χρηστών / διαχειριστών του συστήματος

Στην φάση αυτή θα ελέγχει την ορθή λειτουργία του έργου, θα πραγματοποιηθούν οι απαραίτητες αλλαγές και προσαρμογές, και θα πραγματοποιηθούν οι δοκιμές ασφάλειας

Περιγραφή Υλοποίησης

Περιλαμβάνει όλες τις απαραίτητες ενέργειες και την εξασφάλισης της πιλοτικής καλής λειτουργίας όλου του πληροφοριακού συστήματος.

1.Τεκμηρίωση Συστήματος (Τ.Σ.).

Περιλαμβάνει την πλήρη και αναλυτική τεκμηρίωση του συστήματος που απαιτείται για την υποστήριξη της λειτουργίας του υλικού και του λογισμικού συστήματος και εφαρμογών.

1. 2. Υποστήριξη λειτουργίας – Συντήρησης

Περιλαμβάνει όλες τις απαραίτητες ενέργειες και την εξασφάλισης της πιλοτικής λειτουργίας όλου του συστήματος.

Περιλαμβάνει κατ' ελάχιστον τα ακόλουθα:

- - Προληπτική και διορθωτική συντήρηση εξοπλισμού
- - Υποστήριξη λειτουργίας υλικού και λογισμικού
- - Τηλεφωνική υποστήριξη – Helpdesk
- - Παρακολούθηση και Αντιμετώπιση περιστατικών ασφαλείας
- - On the Job training.
- - Τελική Παραμετροποίηση πληροφοριακού συστήματος

Ότι αντίστοιχο προβλέπεται στις παραπάνω διακριτές ενότητες και τα παρακάτω επιμέρους υποσυστήματα

Αποσφαλμάτωση πληροφοριακού συστήματος

Τελική Παραμετροποίηση πληροφοριακού συστήματος

Παραδοτέα

Π.4 : Πιλοτική Λειτουργία

Π.4.1: Έντυπο και ηλεκτρονικό υλικό τεκμηρίωσης
Π.4.2: Υποστήριξη πιλοτικής λειτουργίας πληροφοριακού συστήματος
Π.4.3: On the Job training
Π.4.4: Εκσφαλμάτωση πληροφοριακού συστήματος.
Π.4.5: Τελική Παραμετροποίηση πληροφοριακού συστήματος

Φάση Νο	**5**	**Τίτλος**	Παραγωγική λειτουργία.
Μήνας Έναρξης	**4**	**Μήνας Λήξης**	**4**
1 Μήνας			

Στόχοι

Παραγωγικής λειτουργίας

Περιλαμβάνει όλες τις απαραίτητες ενέργειες για την εξασφάλισης της κανονικής λειτουργίας όλου του πληροφοριακού συστήματος με την υποστήριξη από τον ανάδοχο.

Εκπαίδευση (on the job training) χρηστών / διαχειριστών του συστήματος

Έλεγχος της ορθής λειτουργία του συστήματος.

Περιγραφή Υλοποίησης

Τεκμηρίωση Συστήματος (Τ.Σ.).

Περιλαμβάνει την πλήρη και αναλυτική τεκμηρίωση του συστήματος που απαιτείται για την υποστήριξη της λειτουργίας του υλικού και του λογισμικού συστήματος και εφαρμογών.

Υποστήριξη λειτουργίας – Συντήρησης

Περιλαμβάνει όλες τις απαραίτητες ενέργειες και την εξασφάλισης της κανονικής λειτουργίας όλου του συστήματος.

Περιλαμβάνει κατ' ελάχιστον τα ακόλουθα:

- - Υποστήριξη λειτουργίας υλικού και λογισμικού
- - Τηλεφωνική υποστήριξη – Helpdesk
- - Παρακολούθηση κατάσταση ασφαλείας
- - Αντιμετώπιση περιστατικών ασφαλείας
- - On the Job training.
- - Αποσφαλμάτωση πληροφοριακού συστήματος
- - Τελική Παραμετροποίηση πληροφοριακού συστήματος

Παραδοτέα

Π.5. : Παραγωγική λειτουργία

Π.5.1: Έντυπο και ηλεκτρονικό υλικό τεκμηρίωσης
Π.5.2: Υποστήριξη παραγωγικής λειτουργίας πληροφοριακού συστήματος
Π.5.3: On the Job training
Π.5.4: Παράδοση επικαιροποιημένου Εκπαιδευτικού υλικού
Π.5.5: Παράδοση Λογισμικού συστήματος και εφαρμογών με άδειες χρήσης για 36 μήνες

1.7 . Πίνακας Παραδοτέων

Στον παρακάτω πίνακα αναφέρονται τα ελάχιστα αποδεκτά παραδοτέα. Ο ανάδοχος έχει τη δυνατότητα να προτείνει επιπλέον παραδοτέα κατά τη κρίση του που συνεισφέρουν στην αρτιότητα και την έγκαιρη υλοποίηση του έργου.

Α/Α Παραδοτέου	Τίτλος Παραδοτέου	Τύπος Παραδοτέου[1]	Μήνας Παράδοσης[2]

1	Π.1: Μελέτη εξειδίκευσης τεχνικών προδιαγραφών υποδομής έργου	Μ	1
2	Π.2: Προμήθεια εξοπλισμού και λογισμικού συστήματος	ΥΛ	2
3	Π.2.1: Εγκατάσταση εξοπλισμού και λογισμικού συστήματος κυβερνοασφάλειας, παραμετροποίηση και θέση του σε λειτουργία	ΥΛ	2
4	Π.2.2 : Διενέργεια σεναρίων ελέγχου	ΑΛ	2
5	Π.2.3 : Αποτελέσματα διενέργειας σεναρίων ελέγχου	ΑΛ	2
6	Π.2.4 : Εκσφαλμάτωση	ΑΛ	2
7	Π.3 : Εκπαίδευση	Υ	3
8	Π.3.1: Πρόγραμμα εκπαίδευσης	ΑΛ	3
9	Π.3.2: Εκπαιδευτικό υλικό	ΑΛ	3
10	Π.3.3: Έκθεση ολοκλήρωσης	ΑΛ	3
11	Π.4 : Πιλοτική Λειτουργία	ΑΛ	3
12	Π.4.1: Έντυπο και ηλεκτρονικό υλικό τεκμηρίωσης	ΑΛ	3
14	Π.4.2: Υποστήριξη πιλοτικής λειτουργίας πληροφοριακού συστήματος	Υ	3
15	Π.4.3: On the Job training	Υ	3
16	Π.4.5: Τελική Παραμετροποίηση πληροφοριακού συστήματος	ΑΛ	3
17	Π.5. : Παραγωγική Λειτουργία	ΑΛ	4
18	Π.5.1: Έντυπο και ηλεκτρονικό υλικό τεκμηρίωσης	ΑΛ	4
19	Π.5.2: Υποστήριξη παραγωγικής λειτουργίας πληροφοριακού συστήματος	Υ	4
20	Π.5.3: On the Job training πληροφοριακού συστήματος	Υ	4

21	Π.5.4: Παράδοση επικαιροποιημένου Εκπαιδευτικού υλικού	ΑΛ	4
22	Π.5.5: Παράδοση Λογισμικού συστήματος και εφαρμογών με άδειες χρήσης για 36 μήνες	ΑΛ	4

[1] Τύπος Παραδοτέου: Μ (Μελέτη), ΑΝ (Αναφορά), Λ (Λογισμικό), Υ (Υλικό/Εξοπλισμός), Υ (Υπηρεσία), Σ (Σύστημα), ΑΛ (Άλλο)

[2] Μήνας Παράδοσης Παραδοτέου(π.χ.Μ1,Μ2,...ΜΝ)όπου Μ1 είναι ο πρώτος μήνας (δηλ. μήνας έναρξης) του Έργου

Όλα τα παραδοτέα πρέπει να υποβάλλονται και σε ηλεκτρονική μορφή (με ανοιχτή τη δυνατότητα επεξεργασίας). Όλα τα παραδοτέα πρέπει να παραχθούν και να γίνουν αποδεκτά από την Αναθέτουσα Αρχή εντός του συμβατικού χρόνου υλοποίησης του έργου.

Όλα τα ανωτέρω παραδοτέα είναι υποχρεωτικά.

Σημαντικά Ορόσημα υλοποίησης Έργου

Α/Α	**Τίτλος Οροσήμου**	**Μήνας Επίτευξης**	**Μέθοδος μέτρησης της επίτευξης**	**% επί του συνολικού κόστους/αμοιβής**
1.	Ολοκλήρωση της Εξειδίκευσης Τεχνικών Προδιαγραφών	**1**	Παραλαβή παραδοτέων φάσης 1	40%
2.	Ολοκλήρωση της Προμήθειας, εγκατάστασης και παραμετροποίησης εξοπλισμού και έτοιμου λογισμικού Εκπαίδευση χρηστών	**2**	Παραλαβή παραδοτέων φάσεων 2 και3	
3.	Ολοκλήρωση της παραμετροποίησης λογισμικού, της εγκατάστασης και θέσης σε λειτουργία συστημάτων και υλοποίησης της Πιλοτικής και Παραγωγικής λειτουργίας και παράδοση Λογισμικού συστήματος και εφαρμογών με άδειες χρήσης για 36 μήνες	**4**	Παραλαβή παραδοτέων φάσεων 4 και 5	60%

1.8 Περίοδος Εγγύησης και Συντήρησης (ΠΕΣ)

Ως ΠΕΣ ορίζεται η συνολική Περίοδος Εγγύησης και Συντήρησης, με έναρξη την Οριστική Παραλαβή του Έργου και με χρονική διάρκεια τρία (3) έτη.

Η ζητούμενη Περίοδος Εγγύησης και Συντήρησης είναι τρία (3) έτη από την Οριστική Παραλαβή του Έργου και **οι υπηρεσίες της** (συντήρηση του συστήματος, του εξοπλισμού, του έτοιμου λογισμικού, την τεχνική υποστήριξη και την υποστήριξη των χρηστών, την παροχή υπηρεσιών ασφαλείας) **παρέχονται δωρεάν**.

Ο Ανάδοχος, μετά την Οριστική Παραλαβή του Έργου, **είναι υποχρεωμένος να υπογράψει** με

την Αναθέτουσα Αρχή Σύμβαση Εγγύησης και Συντήρησης για τρία έτη.