# **Πίνακες Συμμόρφωσης**

………………………………………………………………………………………………………………….…………………………

∆/νση: …………………………………………………………………….................................................................

Τηλ.: ………………………………………………………...................................................................................

ΑΦΜ:…………………………………………………………… ΔΟΥ……………………….……………………………………..

ΠΡΟΣ ΤΟ ΔΗΜΟ ΧΕΡΣΟΝΗΣΟΥ

ΓΙΑ ΤΗΝ ΥΠΗΡΕΣΙΑ ΜΕ ΤΙΤΛΟ:

«**ΑΝΑΝΕΩΣΗ, ΣΥΝΤΗΡΗΣΗ, ΑΝΑΒΑΘΜΙΣΗ ΣΥΣΤΗΜΑΤΟΣ ΚΥΒΕΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΕΠΙΤΗΡΗΣΗΣ/ΑΝΑΝΕΩΣΗΣ ΠΙΣΤΟΠΟΙΗΣΕΩΝ ΚΑΤΑ ISO 27001 ΚΑΙ ISO 27701 ΤΟΥ ΔΗΜΟΥ ΧΕΡΣΟΝΗΣΟΥ**»

(ΑΡΙΘ. ΜΕΛΕΤΗΣ ΔΔΥ03/2023)

ΑΡ. ΔΙΑΚ/ΞΗΣ ……./…-….-2023

**ΤΜΗΜΑ Α**

| **Α/Α** | **ΠΕΡΙΓΡΑΦΗ** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
| --- | --- | --- | --- | --- |
|  | Το σύστημα θα πρέπει να είναι ανοιχτού τύπου επιτρέποντας την διασύνδεση συστημάτων ασφαλείας ανεξαρτήτου προμηθευτή (Open XDR). | ΝΑΙ.  Να περιγραφεί ο προτεινόμενος μηχανισμός |  |  |
|  | Το σύστημα θα πρέπει να υποστηρίζει λειτουργία SIEM και θα μπορεί να αναπτυχθεί σε όλα τα περιβάλλοντα για να παρέχει διάχυτη ορατότητα. Η τεχνολογία θα πρέπει να συλλέγει και να συσχετίζει όλους άλλης τύπους δεδομένων, άλλης κυκλοφορία δικτύου (ΝΤΑ), αρχεία καταγραφής, εντολές διακομιστή, διεργασίες, εφαρμογές, πληροφορίες χρήστη, αρχεία κ.λπ. αυτοματοποιημένα έτσι ώστε το προσωπικό ασφαλείας να μπορεί να λειτουργεί πιο αποτελεσματικά. | ΝΑΙ |  |  |
|  | Το σύστημα να βασίζεται σε λογισμικό που μπορεί να εγκατασταθεί σε εικονικά και περιβάλλοντα νεφοϋπολογιστικής (cloud). | ΝΑΙ |  |  |
|  | Το σύστημα να πρέπει να παρέχει λειτουργικότητα πολλών μισθωτών (multi-tenant). | ΝΑΙ |  |  |
|  | Σε μια εγκατάσταση πολλαπλών tenants, το σύστημα να εκτελεί λειτουργία μηχανικής μάθησης και τεχνητής νοημοσύνης μόνο στα δεδομένα μεμονωμένων tenants. | ΝΑΙ |  |  |
|  | Προκειμένου να διασφαλιστεί η λεπτομερής ανάλυση των δειγμάτων, προσδιορίζοντας άγνωστες επιθέσεις 0-day (zero-day attacks), η μηχανή ανάλυσης πρέπει να είναι σε θέση να αναπαραγάγει την εκτέλεση κακόβουλου λογισμικού σε έναν εξομοιωτή μηχανής που αναπαράγει ένα εικονικό υλικό, συμπεριλαμβανομένης μιας προσομοιωμένης CPU (Sandboxing) . Η προσομοιωμένη CPU θα πρέπει να εκτελεί προσομοίωση κώδικα σε επίπεδο επεξεργαστή, δηλαδή θα πρέπει να εκτελεί απευθείας τον κακόβουλο κώδικα, ο οποίος, ως εκ τούτου, δεν θα πρέπει να εκτελείται στην φυσική CPU, δηλαδή την κεντρική CPU του προσομοιωμένου συστήματος. | ΝΑΙ |  |  |
|  | Το προστατευμένο περιβάλλον (sandbox) να βασίζεται στην πλήρη εξομοίωση του συστήματος και να ανιχνεύει επιθέσεις πολλαπλών σταδίων (multi-stage attack) όπου η εκμετάλλευση χωρίζεται σε πολλαπλά αντικείμενα | ΝΑΙ |  |  |
|  | Το σύστημα θα παρέχει προηγμένες δυνατότητες συσχέτισης για τον εντοπισμό περιστατικών ασφαλείας όπως: | ΝΑΙ |  |  |
|  | α. Επιθέσεις DDOS (SYN Flood | ΝΑΙ |  |  |
|  | β. Κρούσμα σκουληκιών (warms) | ΝΑΙ |  |  |
|  | γ. Σάρωση θύρας | ΝΑΙ |  |  |
|  | d. Έγχυση SQL | ΝΑΙ |  |  |
|  | e. Βίαιη επίθεση στην υποδομή (Brute Force) | ΝΑΙ |  |  |
|  | Το σύστημα θα προσφέρεται σε WEB GUI με πρωτόκολλο HTTPS | ΝΑΙ |  |  |
|  | Το σύστημα θα χρησιμοποιεί αλγόριθμους που βασίζονται στη μηχανική μάθηση. | ΝΑΙ  Να αναφερθούν άνω δύο περιπτώσεων χρήσης και αποδεικτικά στοιχεία ότι η εφαρμογή χρησιμοποιεί αλγόριθμους με βάση τη μηχανική μάθηση |  |  |
|  | Το σύστημα θα πρέπει να μπορεί να υποστηρίζει τουλάχιστον 850 χρήστες. | ΝΑΙ  Ο μεγαλύτερος αριθμός είναι επιθυμητός |  |  |
|  | Οι Sensors θα πρέπει να υποστηρίζουν ταχύτητα διασύνδεσης δικτύου 1Gbps, 10Gbps | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να υποστηρίζει ταυτόχρονα πολλαπλά locations. | ΝΑΙ |  |  |
|  | Το σύστημα να έχει τη δυνατότητα να αναγνωρίζει τα γεγονότα ως μέρος μιας ροής εργασίας (workflow). | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να διαθέτει προσαρμόσιμο widget στον πίνακα ελέγχου | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει ενσωματωμένο Intelligence Module για συστήματα βάσεων δεδομένων, άλλης MSSQL, MySQL, Azure EventHub | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να ενσωματώνεται με τουλάχιστον πέντε ανοιχτές πηγές πληροφοριών για απειλές (Open Source Threat Intelligence) | ΝΑΙ  Ο μεγαλύτερος αριθμός είναι επιθυμητός |  |  |
|  | Το σύστημα θα πρέπει να έχει μια κύρια κονσόλα διαχείρισης που αποτελείται από ευρετήριο και dashboard | ΝΑΙ |  |  |
|  | Λειτουργία υψηλής διαθεσιμότητας και ομαδοποίηση. | ΝΑΙ  Να αναφερθεί ο βαθμός διαθεσιμότητας |  |  |
|  | Το σύστημα θα πρέπει να παρέχει απόλυτη προστασία από επιθέσεις APT μέσω δικτύου και web. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να υποστηρίζει ειδοποιήσεις συμβάντος (event notification) σε μορφή JSON. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να είναι ικανό να κατηγοριοποιεί την σοβαρότητα συμβάντων (Incident Severity) που συνδέεται με Ειδοποιήσεις. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να έχει τη δυνατότητα να αναφέρει πότε εμφανίζεται DATA THEFT περιστατικό. | ΝΑΙ |  |  |
|  | θα πρέπει να είναι δυνατή η εγκατάσταση όλων των στοιχείων άλλης αρχιτεκτονικής σε τυπικούς διακομιστές και όχι σε ειδικές συσκευές. | ΝΑΙ  Να αναφερθούν οι συμβατοί τύποι διακομιστών |  |  |
|  | Το σύστημα πρέπει θα είναι σε θέση να εφαρμόζει τόσο Εποπτευόμενη όσο και Μη Εποπτευόμενη Μηχανική Μάθηση και Προσαρμοσμένη Μηχανική Μάθηση σε αρχεία καταγραφής ή επισκεψιμότητα που λαμβάνει δεδομένα από τα ακόλουθα στοιχεια του δικτύου:  IDS  Τείχος προστασίας  Traffic δικτύου (Network Traffic)  Συστήματα Windows ή Linux  AWS Cloudtrail, Office 365, G-Suite, SNMP,  Vulnerability Scanners όπως Nessus, Rapid7, Tenable  Syslogs, CEF, LEEF, Netflow, JSON | ΝΑΙ  Να αναφερθούν τα χαρακτηριστικά των χρησιμοποιούμενων μεθόδων Μηχανικής Μάθησης |  |  |
|  | Το σύστημα θα έχει τη δυνατότητα εφαρμογής Μηχανικής Εκμάθησης στο Τείχος προστασίας και τα IDS (ML-IDS) | ΝΑΙ |  |  |
|  | Το σύστημα να υποστηρίζει πολλαπλούς μηχανισμούς συλλογής δεδομένων, συμπεριλαμβανομένων αισθητήρων ασφάλειας δικτύου (Network Security Sensors) και Agent Sensors. | ΝΑΙ  Να αναφερθούν τα χαρακτηριστικά των αισθητήρων |  |  |
|  | Το σύστημα να παρέχει στον διαχειριστή υπηρεσίες για την εφαρμογή συνεχούς απεριόριστης ενημέρωσης σε dashboard | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να εξαγάγει αναγνώσιμα μεταδεδομένα (layers 2-7) | ΝΑΙ |  |  |
|  | Οι αισθητήρες του συστήματος να καταγράφουν δεδομένα του δικτύου και να αποστέλνουν μόνο σχετικά δεδομένα στον επεξεργαστή για ανάλυση. | ΝΑΙ |  |  |
|  | Το σύστημα θα παρέχει ολοκληρωμένη ανάλυση κίνησης δικτύου (NTA). | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει τεχνολογία εξαπάτησης / honeypot με υποστήριξη τουλάχιστον 2 κοινών πρωτοκόλλων (π.χ. HTTP/FTP) | ΝΑΙ  Να αναφερθεί η διαδικασία άλλης εξαπάτησης |  |  |
|  | Το προτεινόμενο σύστημα να είναι ικανό να υποστηρίζει τη συλλογή πληροφοριών και δεδομένων τόσο με τη χρήση agents όσο και χωρίς. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να είναι ικανό να εκτελεί παρακολούθηση άλλης υποδομής διακομιστή και Δικτύου out of the box. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να είναι ικανό να εκτελεί την Παρακολούθηση Εφαρμογών out of the box. | ΝΑΙ |  |  |
|  | Το σύστημα να υποστηρίζει αναζήτηση γεωγραφικής τοποθεσίας IP (Geo Location Public IP look up) | ΝΑΙ |  |  |
|  | Το σύστημα να υποστηρίζει προσαρμοσμένα και εσωτερικά αρχεία καταγραφής ασφαλείας και on-the-fly δημιουργία συσχέτισης για τα αρχεία καταγραφής | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να συλλέγει πληροφορίες στοιχείων (network assets) και πληροφορίες ροής δικτύου (network flows) με παθητικό τρόπο (passive) | ΝΑΙ |  |  |
|  | To σύστημα να είναι σε θέση να απορροφήσει όλα τα δεδομένα (χρήστες, εφαρμογές) και να τα καταστήσει διαθέσιμα για χρήση — παρακολούθηση, ειδοποίηση, έρευνα και ad hoc αναζήτηση | ΝΑΙ |  |  |
|  | Το σύστημα θα παρέχει ευελιξία για ενσωμάτωση με εργαλεία και πύλες αναφοράς τρίτων | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει δυνατότητα προβολής για αποθηκευμένα ακατέργαστα δεδομένα (raw data view) | ΝΑΙ |  |  |
|  | Το σύστημα να κατατάσσει ειδοποιήσεις ασφαλείας με βάση το CyberSecurity KillChain. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να παρέχει περιγραφή του κακόβουλου λογισμικού που εντοπίστηκε. | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει ένα ολοκληρωμένο σύστημα ανίχνευση εισβολής (IDS). | ΝΑΙ |  |  |
|  | Το σύστημα να αποστέλλει ειδοποίηση στο αντίστοιχο προσωπικό σχετικά με το ζήτημα ασφάλειας βάσει συσχετισμένου συμβάντος. | ΝΑΙ |  |  |
|  | Το σύστημα να παρακολουθεί κάθε αλλαγή και να προστατεύει το περιβάλλον παρακολουθώντας ύποπτη δραστηριότητα, αλλαγές ρόλου χρήστη, μη εξουσιοδοτημένη πρόσβαση και άλλα. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να είναι σε θέση να εντοπίσει παραβιασμένους κεντρικούς υπολογιστές που σχετίζονται με προηγμένες απειλές και μολύνσεις από κακόβουλα προγράμματα | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να παρέχει δυνατότητα παρακολούθησης συμβάντων ασφαλείας εκτός δεδομένων υπολογιστή (π.χ. παρακολούθηση συμβάντων / απειλών ασφαλείας που έχουν αναρτηθεί στο Διαδίκτυο) | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να είναι σε θέση να βρει δραστηριότητες και συμβάντα που σχετίζονται με επιτυχείς επιθέσεις και μολύνσεις από κακόβουλα προγράμματα | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να παράγει ειδοποίηση κατά τον εντοπισμό εξωτερικής IP που ανήκει σε μαύρη λίστα (blacklist) | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να περιλαμβάνει ενσωματωμένη διαχείριση ειδοποιήσεων για νέα κακόβουλα συμβάντα | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει ορατότητα δικτύου (network visibility) από wire data που περιέχουν κρίσιμες πληροφορίες για payload, πληροφορίες συνεδρίας (session information), σφάλματα, DNS κ.λπ. | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει δυνατότητες ανίχνευσης χωρίς χρήση υπογραφών (Signatureless Detection Capability). | ΝΑΙ |  |  |
|  | Το σύστημα να έχει δυνατότητες ανάλυσης συμπεριφοράς χρήστη (User Behavior Analytics) | ΝΑΙ |  |  |
|  | Το σύστημα να έχει δυνατότητες ανάλυσης συμπεριφοράς τερματικών (EndPoint Behavior Analytics) | ΝΑΙ |  |  |
|  | Το σύστημα να έχει προ-εγκατεστημένους κανόνες ανίχνευσης που βασίζονται στο CyberSecurity KillChain | ΝΑΙ |  |  |
|  | Nα υποστηρίζει αναζήτηση βάσει ανάλυσης καταγραφής και να εκδίδεται αναφορά. | ΝΑΙ |  |  |
|  | Να πραγματοποιείται ανάλυση και συσχέτιση συμβάντων ασφαλείας. | ΝΑΙ |  |  |
|  | Το σύστημα έρευνας να προσφέρει διαχείριση ολοκληρωμένων απειλών, συμβάντων και συμμόρφωσης | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να καλύψει ιδιωτικά δεδομένα (π.χ. κωδικό πρόσβασης, αριθμό πιστωτικής κάρτας) πριν τα αποθηκεύσει. | ΝΑΙ |  |  |
|  | Το σύστημα να παρακολουθεί αυτόματα τα γνωστά κακόβουλα γεγονότα και να χρησιμοποιεί εξελιγμένη συσχέτιση μέσω αναζήτησης, για να εντοπίσει γνωστά μοτίβα κινδύνου άλλης επιθέσεις brute force, διαρροή δεδομένων και ακόμη και απάτη σε επίπεδο εφαρμογής (application-level fraud). | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να βοηθήσει αναλυτές ασφαλείας να διενεργήσουν αξιολόγηση παραβίασης και ρηγμάτων (compromise and breach assessments). | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να συσχετίζει πληροφορίες στοιχείων (asset info) με δεδομένα απειλών (threat) και ευπαθειών(vulnerability) | ΝΑΙ |  |  |
|  | Το σύστημα να είναι πλήρως προσαρμόσιμο στη δημιουργία προειδοποιήσεων ή συναγερμών για συμβάντα υψηλού κινδύνου | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να παρέχει λειτουργία αναζήτησης που θα υποστηρίζει απλή αναζήτηση μοτίβων τύπου Boolean καθώς και σύνθετες κανονικές εκφράσεις (Boolean-style patterns search as well as complex regular expressions). | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να επιτρέπει στον αναλυτή να δημιουργεί ερωτήματα χρησιμοποιώντας συνδυασμένη μέθοδο αναζήτησης. Ένα μεμονωμένο ερώτημα μπορεί να περιέχει λέξεις-κλειδιά, συνθήκες βάσει πεδίου και κανονικές εκφράσεις  (keywords, field based conditions and regular expression). | ΝΑΙ |  |  |
|  | Το σύστημα να υποστηρίζει τη δυνατότητα σύνδεσης με Threat Intelligence για έκτακτο συμβάν ή και ειδοποίηση. | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να ανιχνεύει απειλές που στοχεύουν διάφορα λειτουργικά συστήματα. | ΝΑΙ |  |  |
|  | Το σύστημα να προσφέρει δυνατότητα εγκατάστασης αισθητήρα/agent σε εικονικό περιβάλλον (virtualization) | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να παρέχει συσχέτιση συμβάντων από πολλούς τύπους συσκευών. | ΝΑΙ |  |  |
|  | Το σύστημα να υποστηρίζει κοινή χρήση πληροφοριών όπου απαιτείται (community based intel sharing). | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει ανάλυση κατ ‘απαίτηση για IP και Domains. | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί ενσωματωθεί με σύστημα ασφάλειας SIEM μέσω προσαρμογέα πληροφοριών ασφαλείας και άλλης εφαρμογής. | ΝΑΙ |  |  |
|  | Το σύστημα να έχει δυνατότητα αξιοποίησης, ανάλυσης και οπτικοποίησης των δεδομένων στον ανοικτού κώδικα Kibana με ενεργοποίηση Plugin. | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει δυνατότητες ενορχήστρωσης άλλης αυτοματοποίησης απόκρισης ασφάλειας (SOAR) σε email, διαχείριση υποθέσεων (case management), τείχους προστασίας (firewall) και Active Directory | ΝΑΙ |  |  |
|  | Η λειτουργία SIEM να μεταδίδει άλλης ροές συμβάντων και άλλης ανιχνεύσεις SOAR για την αυτόματη ενεργοποίηση πληροφοριών που βρίσκονται σε προϊόντα ενορχήστρωσης SOAR, για την εκτέλεση σειράς οδηγιών που θα μπορούσαν να περιλαμβάνουν την εκτέλεση σεναρίων(playbooks) ή την ενσωμάτωση με άλλα εργαλεία στο ίδιο περιβάλλον. | ΝΑΙ |  |  |
|  | Το σύστημα να έχει τη δυνατότητα να εντοπίζει και να αυτοματοποιεί την παρακολούθηση απειλής (Threat Hunting) και να εφαρμόζεται στο SOAR | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει ενσωματωμένη διαχείριση υποθέσεων (case management) ή να μπορεί να συνδεθεί με διαχείριση συμβάντων (case management) άλλων συστημάτων | ΝΑΙ |  |  |
|  | Το σύστημα να έχει ήδη προκαθορισμένα πρότυπα για γενικές αναφορές και αναφορές συμμόρφωσης (general and compliance reporting) | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να είναι σε θέση να συλλέγει ποσότητες δεδομένων χωρίς να περιορίζει τον αριθμό των συσκευών από άλλης οποίες θα πρέπει να συλλέγονται. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να παρέχει απεριόριστο όριο στον αριθμό των χρηστών στο σύστημα, αναζητήσεις, ειδοποιήσεις, συσχετίσεις, αναφορές, πίνακες ελέγχου. | ΝΑΙ |  |  |
|  | Συλλέγει όλους άλλης τύπους αρχείων καταγραφής και δεδομένων από διάφορες πηγές, π.χ. syslog, προσαρμοσμένες / εσωτερικές εφαρμογές και αρχεία καταγραφής βάσεων δεδομένων | ΝΑΙ |  |  |
|  | Ενοποιεί όλα τα συλλεγόμενα αρχείων καταγραφής σε ένα κεντρικό αποθετήριο. | ΝΑΙ |  |  |
|  | Εκτελεί συγκέντρωση και ομαλοποίηση αρχείων καταγραφής. | ΝΑΙ |  |  |
|  | Αναλύει και να συσχετίζει τα συμβάντα ασφαλείας. | ΝΑΙ |  |  |
|  | Στέλνει ειδοποίηση στο αντίστοιχο προσωπικό σχετικά με το ζήτημα ασφάλειας βάσει συσχετισμένου συμβάντος. | ΝΑΙ |  |  |
|  | Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη διαχείριση απειλών, συμβάντων και συμμόρφωσης. | ΝΑΙ |  |  |
|  | Το σύστημα πρέπει να είναι μια λύση βάσει λογισμικού που να μπορεί να εγκατασταθεί σε εικονικά περιβάλλοντα (virtualized environments). | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να περιλαμβάνει αισθητήρα συλλογής δεδομένων | ΝΑΙ |  |  |
|  | Το σύστημα να υποστηρίζει τη συλλογή δεδομένων με χρήση ή και χωρίς agent (agent & agentless) | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να είναι ικανό να εκτελεί Παρακολούθηση Εφαρμογών out of the box. | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει παρακολούθηση αλλαγών και προστασία του περιβάλλοντος του Οργανισμού , παρακολουθώντας ύποπτη δραστηριότητα, αλλαγές ρόλου χρήστη, μη εξουσιοδοτημένη πρόσβαση και άλλα. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να παρακολουθεί αυτόματα την υποδομή για γνωστά κακόβουλα συμβάντα και θα χρησιμοποιεί εξελιγμένη συσχέτιση μέσω αναζήτησης, για να εντοπίσει γνωστά μοτίβα κινδύνου άλλης επιθέσεις με ωμή βία (brute-force attack), διαρροή δεδομένων (data leakage) και ακόμη και απάτη σε επίπεδο εφαρμογής (application level fraud). | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να εντοπίσει παραβιασμένους κεντρικούς υπολογιστές που σχετίζονται με προηγμένες απειλές και μολύνσεις από κακόβουλα προγράμματα | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να εντοπίζει δραστηριότητες και συμβάντα που σχετίζονται με επιτυχείς επιθέσεις και μολύνσεις από κακόβουλα προγράμματα | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να βοηθήσει άλλης αναλυτές ασφαλείας να διενεργήσουν διερεύνηση εισβολών και ρηγμάτων (compromise and breach assessment). | ΝΑΙ |  |  |
|  | Nα παρέχει τη δυνατότητα παρακολούθησης συμβάντων ασφαλείας εκτός δεδομένων υπολογιστή (π.χ. παρακολούθηση συμβάντων / απειλών ασφαλείας που έχουν αναρτηθεί στο Διαδίκτυο) | ΝΑΙ |  |  |
|  | Nα υποστηρίζει προσαρμοσμένα και εσωτερικά αρχείων καταγραφής ασφαλείας και την on-the-fly συσχετισμό άλλης. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να υποστηρίζει ενσωμάτωση με μηχανισμούς αναγνώρισης ευπαθειών (vulnerability scanners) | ΝΑΙ |  |  |
|  | Το σύστημα θα είναι σε θέση να συσχετίζει πληροφορίες στοιχείων (assets) με δεδομένα απειλής και ευπάθειας | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να συλλέγει παθητικά (passively) πληροφορίες στοιχείων (assets) και πληροφορίες ροής δικτύου (network flow) | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να υποστηρίζει προβολή για αποθηκευμένα ακατέργαστα δεδομένα | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να εκδίδει ειδοποίηση κατά τον εντοπισμό εξωτερικής IP μαύρης λίστας | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να ενοποιήσει άλλης απειλές με την ομαλοποίηση (normalization) , τη φήμη (reputation), τη γνώση (knowledge) και payload του γεγονότος ενεργοποίησης | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει λειτουργία network packet analysis για διαγνωστικό έλεγχο. | ΝΑΙ |  |  |
|  | Το σύστημα να είναι πλήρως παραμετροποιήσιμο κατά τη δημιουργία προειδοποιήσεων (warnings) ή συναγερμών (alarms) για συμβάντα υψηλού κινδύνου | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει ορατότητα δικτύου (network visibility) από wire data που περιέχουν κρίσιμες πληροφορίες για payload, πληροφορίες περιόδου λειτουργίας (session information), σφάλματα, DNS κ.λπ. | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να παρέχει λειτουργία αναζήτησης που θα υποστηρίζει απλή αναζήτηση μοτίβων τύπου Boolean καθώς και σύνθετες κανονικές εκφράσεις (Boolean-style patterns search και complex regular expressions). | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να επιτρέπει στον αναλυτή να δημιουργεί ερωτήματα (queries) χρησιμοποιώντας συνδυασμένη μέθοδο αναζήτησης. Ένα μεμονωμένο ερώτημα μπορεί να περιέχει λέξεις-κλειδιά, συνθήκες βάσει πεδίου και κανονικές εκφράσεις  (keywords, field based conditions and regular expression). | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να εκτελεί υπο-αναζήτηση όσον αφορά την ασφάλεια στα αποτελέσματα τρέχουσας αναζήτησης | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να παρακολουθεί άγνωστες απειλές | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει οπτικές αναφορές που μπορούν να μεταφράσουν τα ζητήματα ασφαλείας σε επιχειρηματικό κίνδυνο / απώλεια και αντίκτυπο (risk/loss and impact). | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να απορροφήσει όλα τα δεδομένα (χρήστες, εφαρμογές) και να τα καταστήσει διαθέσιμα για χρήση — παρακολούθηση, ειδοποίηση, έρευνα, ad hoc αναζήτηση | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει είναι ένα διαδικτυακό WEB GUI με πρωτόκολλο HTTPS | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει ευελιξία για ενσωμάτωση με εργαλεία και πύλες αναφοράς τρίτων | ΝΑΙ |  |  |
|  | Το σύστημα θα χρησιμοποιεί αλγόριθμους που βασίζονται στη μηχανική μάθηση. Καταχωρίστε ορισμένες περιπτώσεις χρήσης και αποδεικτικά στοιχεία ότι η εφαρμογή χρησιμοποιεί αλγόριθμους με βάση τη μηχανική μάθηση | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει ενσωμάτωση με advanced security advisory | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει υποστήριξη για ενοποίηση δεδομένων υποστήριξης για την ανάλυση του κινδύνου (Risk Analytic data integration) | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει υποστήριξη για ενημερώσεις κινδύνου και απειλών στον κυβερνοχώρο (Risk and Cyber Threat Advisory Alert) | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει παρέχει στον διαχειριστή την δυνατότητα συνεχούς, απεριόριστης ενημέρωσης του πίνακα ελέγχου (dashboard) και των ερωτημάτων συσχέτισης | ΝΑΙ |  |  |
|  | Το σύστημα θα παρέχει προεγκατεστημένο Intelligence Module, πλαίσιο λειτουργίας (dashboard) και αναφορών για τα Windows | ΝΑΙ |  |  |
|  | Να διαθέτει αισθητήρα/λειτουργία υψηλής διαθεσιμότητας | ΝΑΙ |  |  |
|  | Το σύστημα να διαθέτει ενότητα ανάλυσης επιχειρησιακής ευφυίας (Intelligent business analysis module) | ΝΑΙ |  |  |
|  | Το σύστημα να διαθέτει συμβουλευτική ενότητα αξιολόγησης ρίσκου και συμμόρφωσης (risk and compliance advisory module) | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει προστασία από επιθέσεις APT μέσω δικτύου ή Web | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει άλλης δυνατότητες ανίχνευσης χωρίς σήμανση (Signatureless Detection). | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να υποστηρίζει SNMP. | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να αντιμετωπίσει όλους άλλης τύπους ειδοποιήσεων που συνδέονται με άλλης φάσεις του κύκλου ζωής άλλης μόλυνσης (Infection Life Cycle). | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να είναι ικανό να κατηγοριοποιήσει άλλης ειδοποιήσεις με βάση τη σοβαρότητα (Incident Severity). | ΝΑΙ |  |  |
|  | θα πρέπει να είναι δυνατή η εγκατάσταση όλων των στοιχείων άλλης αρχιτεκτονικής σε τυπικούς διακομιστές του εμπορίου και όχι σε ειδικές συσκευές. | ΝΑΙ |  |  |
|  | Το σύστημα θα υποστηρίζει τη δυνατότητα σύνδεσης ειδοποιήσεων/συμβάντων με Threat Intelligence. | ΝΑΙ |  |  |
|  | Το σύστημα να μπορεί να ανιχνεύει απειλές που στοχεύουν διάφορα λειτουργικά συστήματα. | ΝΑΙ |  |  |
|  | Το σύστημα να υποστηρίζει Διαμόρφωση Υψηλής Διαθεσιμότητας (HA). Να αναφερθεί | ΝΑΙ |  |  |
|  | Το σύστημα να είναι σε θέση να παρέχει συσχέτιση συμβάντων από πολλούς τύπους συσκευών. | ΝΑΙ |  |  |
|  | Το σύστημα θα περιλαμβάνει ενοποιημένες λήψεις περιεχομένου ασφαλείας για άλλης διαχειριζόμενες συσκευές. | ΝΑΙ |  |  |
|  | Το σύστημα να υποστηρίζει κοινή χρήση πληροφοριών. | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει δημιουργία ειδοποιήσεων για γνωστούς παράγοντες απειλής (attribution of alerts to known threat actors). | ΝΑΙ |  |  |
|  | Το σύστημα να παρέχει περιγραφή άλλης οικογένειας των κακόβουλων προγραμμάτων. | ΝΑΙ |  |  |
|  | Το σύστημα nα παρέχει ανάλυση κατ ‘απαίτηση για IP και Domains. | ΝΑΙ |  |  |
|  | Το σύστημα θα πρέπει να ενσωματωθεί με το σύστημα ασφάλειας SIEM. | ΝΑΙ |  |  |
|  | Nα είναι δυνατή η εγκατάσταση του αισθητήρα/agent σε εικονικό περιβάλλον | ΝΑΙ |  |  |
|  | Να είναι δυνατή η εγκατάσταση όλων των στοιχείων άλλης αρχιτεκτονικής σε τυπικούς διακομιστές | ΝΑΙ |  |  |
|  | Το IDS θα πρέπει να συνδυάζει την τεχνητή νοημοσύνη και υπογραφές για την μείωση των περιττών ειδοποιήσεων/συμβάντων και τον εντοπισμό ανωμαλιών υψηλής πιστότητας | ΝΑΙ |  |  |
|  | Η αρχιτεκτονική θα πρέπει να παρέχει εκτεταμένη ανάλυση κίνησης δικτύου χρησιμοποιώντας τόσο εποπτευόμενη όσο και μη εποπτευόμενη μάθηση | ΝΑΙ |  |  |
|  | Θα πρέπει να παρέχει παρακολούθηση άλλης αλληλεπίδρασης μεταξύ συσκευών, υπηρεσιών, εφαρμογών που εκτελούνται στο δίκτυό σε πραγματικό χρόνο όσο και ιστορικά. | ΝΑΙ |  |  |
|  | Στατιστικά στοιχεία απόδοσης δικτύου (Network Statistics) | ΝΑΙ |  |  |
|  | Απόδοση διακομιστών (Server Performance) | ΝΑΙ |  |  |
|  | Ανίχνευση εφαρμογών και παρακολούθηση απόδοσης (Application detection and performance monitoring) | ΝΑΙ |  |  |
|  | Κορυφαίες πηγές και κορυφαίοι προορισμοί (Top sources & Top destinations) | ΝΑΙ |  |  |
|  | Asset throughput | ΝΑΙ |  |  |
|  | Asset application performance | ΝΑΙ |  |  |
|  | Application processing time | ΝΑΙ |  |  |
|  | Network interactions with asset | ΝΑΙ |  |  |
|  | Στατιστικά HTTP | ΝΑΙ |  |  |
|  | Στατιστικά DNS | ΝΑΙ |  |  |
|  | διεύθυνση IP | ΝΑΙ |  |  |
|  | Υπηρεσίες Εφαρμογών (Application Services)  Πρώτη και τελευταία εμφάνιση  Ετικέτες και περιγραφή στοιχείων  Server certificate visibility. | ΝΑΙ |  |  |
|  | Θα πρέπει να παρέχει εξομοιώσεις (emulations) και δολώματα (decoys) που εκτελούνται στον Deception Server:  Διακομιστή HTTP Apache  Διακομιστή FTP  Διακομιστή SSH  Διακομιστή αστερίσκου (VOIP)  Διακομιστή Tomcat  Πρόσθετο Strut2  Διακομιστή SQL | ΝΑΙ |  |  |
|  | Επανεξέταση ελέγχου συστήματος (System auditing) | ΝΑΙ |  |  |

ΗΜΕΡΟΜΗΝΙΑ:

ΥΠΟΓΡΑΦΗ

ΣΦΡΑΓΙΔΑ