ΠΑΡΑΡΤΗΜΑ Ι

Αναλυτική Περιγραφή Φυσικού Αντικειμένου της Σύμβασης

Προμήθεια τριακοσίων (300) αδειών εξειδικευμένου λογισμικού μέσω του οποίου θα παρασχεθούν, για ένα (1) έτος, υπηρεσίες υποστήριξης, από ομάδα τεχνικών SOC (Security Operation Center), με σκοπό την ανίχνευση κακόβουλου λογισμικού, την αντιμετώπιση περιστατικών ασφαλείας, την έρευνα ψηφιακής εγκληματολογίας και την ανάλυση εσωτερικών απειλών .

CPV:	*(48732000-8)* *Πακέτα λογισμικού ασφαλείας δεδομένων*
ΕΚΤΙΜΩΜΕΝΗ ΑΞΙΑ ΣΥΜΒΑΣΗΣ:	*Συνολική εκτιμώμενη αξία της σύμβασης εξήντα χιλιάδες ευρώ (60.000,00 €) πλέον ΦΠΑ.*
ΑΡΙΘΜΟΣ ΠΡΩΤΟΚΟΛΛΟΥ	**12209/8359/02.11.2020 (ΑΔΑ : 02-06ΡΧ)**

ΑΘΗΝΑ, 04.11.2020

ΠΑΡΑΡΤΗΜΑ Ι

Προμήθεια τριακοσίων (300) αδειών εξειδικευμένου λογισμικού μέσω του οποίου θα παρασχεθούν, για ένα (1) έτος, υπηρεσίες υποστήριξης, από ομάδα τεχνικών SOC (Security Operation Center), με σκοπό την ανίχνευση κακόβουλου λογισμικού, την αντιμετώπιση περιστατικών ασφαλείας, την έρευνα ψηφιακής εγκληματολογίας και την ανάλυση εσωτερικών απειλών.

1. Αντικείμενο του έργου

Η Αναθέτουσα Αρχή διαθέτει μια υποδομή πληροφορικής η οποία εξυπηρετεί συνολικά τις ανάγκες της Βουλής των Ελλήνων (ΒτΕ). Για την αποτελεσματικότερη παροχή των ηλεκτρονικών υπηρεσιών, η ΒτΕ στοχεύει στην προμήθεια εξειδικευμένου λογισμικού μέσω του οποίου θα παρασχεθούν, για ένα (1) έτος, υπηρεσίες υποστήριξης, από ομάδα τεχνικών SOC (Security Operation Center), με σκοπό την ανίχνευση κακόβουλου λογισμικού, την αντιμετώπιση περιστατικών ασφαλείας, την έρευνα ψηφιακής εγκληματολογίας και την ανάλυση εσωτερικών απειλών.

2. Υφιστάμενες υποδομές

Η υφιστάμενη υποδομή της ΒτΕ περιλαμβάνει τερματικά λειτουργικών συστημάτων Windows Server 2012 R2, Windows 10, Windows 7 και σύστημα διαχείρισης περιστατικών ασφάλειας IBM QRadar. Το σύνολο των τερματικών της υποδομής της ΒτΕ ανέρχεται σε 1900 συμπεριλαμβανομένων σταθμών εργασίας και εξυπηρετητών και θα καλυφθούν αρχικά τα 300 εξ αυτών που αποτελούν και τα κρισιμότερα αναφορικά με τις παρεχόμενες υπηρεσίες και λειτουργίες.

3. Τεχνική Περιγραφή

Ανίχνευση κακόβουλου λογισμικού (Malware Detection) και Αντιμετώπιση περιστατικών ασφαλείας (Incident Response)

Το εργαλείο που θα επιλεγεί από την ΒτΕ θα πρέπει να έχει τη δυνατότητα να ανιχνεύει προσπάθειες εγκατάστασης κακόβουλου λογισμικού στην υποδομή και να παρέχει κατά περίπτωση αυτόματο αποκλεισμό του εν λόγω λογισμικού, ή να δίνει τη δυνατότητα στην ομάδα του Αναδόχου, ή του Κατασκευαστή και στην ομάδα ασφάλειας της ΒτΕ να αποκτήσουν πρόσβαση στο μολυσμένο σύστημα και να εκτελέσουν τις κατάλληλες ενέργειες αποτροπής. Το

εργαλείο θα συνοδεύουν υπηρεσίες υποστήριξης από ομάδα SOC (Security Operation Center) του Αναδόχου, ή του Κατασκευαστή. Η πρόσβαση της ομάδας του ανάδοχου θα πρέπει να γίνεται με ασφαλείς διαδικασίες και πρωτόκολλα. Το εργαλείο θα πρέπει να παρέχει τη δυνατότητα παραγωγής προσαρμοσμένων ενημερώσεων-συναγερμών και να παρέχει προσαρμοσμένη επεξεργασία των περιστατικών ασφαλείας.

Θα πρέπει να υπάρχει η δυνατότητα εντοπισμού και ανάλυσης κακόβολου λογισμικού είτε αυτό είναι ήδη γνωστό στην κοινότητα είτε είναι νέο μηδενικού χρόνου (zero-day). Επίσης το εργαλείο θα πρέπει να είναι σε θέση να εντοπίζει και να αναλύει τις γνωστές διεργασίες που εκτελούνται στην υποδομή της ΒτΕ και να τις διαχωρίζει από τις άγνωστες, οι οποίες θα πρέπει να αντιμετωπίζονται επί της αρχής ως μη έμπιστες.

Το εργαλείο θα πρέπει να έχει τη δυνατότητα να ελέγχει παράλληλα και ταυτόχρονα όλα τα τερματικά της ΒτΕ και να εντοπίζει το κακόβουλο λογισμικό εντός λίγων δευτερολέπτων, ώστε να μειωθεί το ρίσκο απώλειας πληροφοριών. Ο έλεγχος, ο εντοπισμός και το fingerprinting θα πρέπει να γίνεται σε πραγματικό χρόνο, ελέγχοντας το 100% της ενεργής μνήμης RAM των τερματικών παράλληλα. Ο έλεγχος πρέπει να είναι αναλυτικός και σε πραγματικό χρόνο, δίνοντας τη δυνατότητα για απομακρυσμένη απόκριση.

Σε περίπτωση εντοπισμού, θα πρέπει να δίνεται η δυνατότητα μέσω κονσόλας στην ομάδα SOC του Αναδόχου, ή του Κατασκευαστή και στην ομάδα Ασφάλειας της ΒτΕ να απομονώνουν και να ξεκινούν τις διαδικασίες αποκατάστασης των απομακρυσμένων τερματικών εντός λίγων λεπτών κάνοντας χρήση ασφαλούς πρωτοκόλλου κρυπτογράφησης σε επίπεδο μεταφοράς.

Το λογισμικό θα εγκατασταθεί σε διαθέσιμη υποδομή της Βουλής και θα κάνει χρήση της τεχνολογίας cloud προκειμένου η ανάλυση των διεργασιών να γίνεται στην υποδομή του Κατασκευαστή. Δεν θα πρέπει όμως να αποστέλλονται εκτός της υποδομής της ΒτΕ εσωτερικές πληροφορίες, παρά μόνο μεταδεδομένα (meta-data).

Ο έλεγχος για κακόβουλο λογισμικό και η αντιμετώπιση των περιστατικών ασφαλείας θα πρέπει να γίνεται σε πραγματικό χρόνο και να περιλαμβάνει:

- Ανάλυση της μνήμης των τερματικών. Πρέπει να υποστηρίζεται απομακρυσμένος χειροκίνητος έλεγχος της μνήμης μεμονωμένων τερματικών και απομακρυσμένος αυτόματος έλεγχος της μνήμης όλων των τερματικών παράλληλα σε χρόνο μικρότερο των 10 λεπτών. Θα πρέπει ακόμα να δίνεται η δυνατότητα σε έναν χρήστη να προγραμματίζει αυτόματο έλεγχο και ανάλυση της μνήμης συγκεκριμένων μεμονωμένων τερματικών, μιας ομάδας τερματικών, ή ολόκληρης της υποδομής ταυτόχρονα.
- Απομακρυσμένη ανάλυση των σκληρών δίσκων των τερματικών, συμπεριλαμβανομένης πρόσβασης σε κατανεμημένες και μη κατανεμημένες περιοχές των σκληρών δίσκων.

Απομακρυσμένη καταγραφή ομοιώματος εγκληματολογίας (forensics imaging) της μνήμης, των μονάδων του τερματικού και όλων των διεργασιών.

- Απομακρυσμένη καταγραφή ομοιώματος εγκληματολογίας (forensics imaging) των σκληρών δίσκων.
- Δυνατότητα απομακρυσμένης απομόνωσης του τερματικού, εκτέλεσης ενεργειών αποκατάστασης και έρευνας περιστατικού.

Το εργαλείο θα πρέπει να έχει τη δυνατότητα να ελέγχει σε πραγματικό χρόνο όλες τις δικτυακές συνδέσεις των τερματικών. Συγκεκριμένα:

- Έλεγχο όλων των δικτυακών συνδέσεων του τερματικού συμπεριλαμβανομένων των τοπικών και εξωτερικών συνδέσεων δικτύων LAN καθώς και της loopback.
- Διατήρηση της ακριβούς ώρας που πραγματοποιήθηκε η σύνδεση.
- Διατήρηση του ονόματος της διεργασίας και του καταλόγου (path) που σχετίζονται με την σύνδεση δικτύου.
- Διατήρηση του χρήστη που είναι υπεύθυνος για την εκτέλεση της διεργασίας που σχετίζεται με τη σύνδεση του δικτύου.
- Διατήρηση της τιμής κατακερματισμού (hash value) της διεργασίας.
- Διατήρηση της ταυτότητας και του ονόματος της τερματικής συσκευής από την οποία εκτελέστηκε η διασύνδεση του δικτύου.
- Διατήρηση της τοπικής διεύθυνσης IP και της πόρτας της σύνδεσης.
- Διατήρηση της απομακρυσμένης διεύθυνσης IP και της πόρτας της σύνδεσης.
- Διατήρηση της ποσότητας των δεδομένων που απεστάλησαν και ελήφθησαν μέσω της σύνδεσης.

Τα παραπάνω στοιχεία θα πρέπει να μπορούν να αποσταλούν σε σχεδόν πραγματικό χρόνο στο σύστημα IBM QRadar της ΒτΕ.

Έρευνα ψηφιακής εγκληματολογίας (Digital Forensic Investigation)

Το εργαλείο που θα επιλεγεί πρέπει να έχει τη δυνατότητα να παρέχει σε πραγματικό χρόνο απομακρυσμένη ορατότητα του σκληρού δίσκου των τερματικών και να διαφυλάσσει τα σχετικά πειστήρια. Συγκεκριμένα θα πρέπει κατ' ελάχιστον:

- Να κάνει προεπισκόπηση και να αντιγράφει το σύστημα αρχείων των απομακρυσμένων τερματικών, της δομής αρχείων και των μεταδεδομένων εντός ενός λεπτού από την επιλογή.
- Κατά τη διάρκεια της δημιουργίας του ομοιώματος (image) του σκληρού δίσκου θα πρέπει να προστατεύεται ο σκληρός δίσκος από αλλαγές, ή εγγραφές.
- Να υποστηρίζεται η δημιουργία των ομοιωμάτων (image) των σκληρών δίσκων σε λογική και φυσική μορφή (logical and physical imaging) σε μορφή DD.

- Να παρέχεται η δυνατότητα δημιουργίας κατακερματισμένων και κρυπτογραφημένων ομοιωμάτων σκληρών δίσκων (forensic image).
- Να υποστηρίζονται οι αλγόριθμοι MD5 και SHA1 για τη δημιουργία των αντιγράφων των σκληρών δίσκων.
- Να παρέχεται η δυνατότητα δημιουργίας ασφαλών χώρων αποθήκευσης (secure containers) για την αποθήκευση των αποδεικτικών δεδομένων εγκληματολογίας.
- Να υποστηρίζεται μια ασφαλής διαδικασία διαχείρισης και φύλαξης των δεδομένων εγκληματολογίας σε επίπεδο αρχείου, καταλόγου και σκληρού δίσκου.
- Να υπάρχει η δυνατότητα να προγραμματίζεται ή να ζητείται κατ' επίκληση η δημιουργία και λήψη ομοιώματος (image) του σκληρού δίσκου.
- Να έχει τη δυνατότητα να εξάγει αρχεία και καταλόγους που βρίσκονται στα απομακρυσμένα τερματικά στην αρχική τους μορφή και σε προορισμό που επιλέγει ο χρήστης.
- Να έχει τη δυνατότητα να κάνει προεπισκόπηση, να αναζητεί, να αναλύει και να διατηρεί εγκληματολογικά πειστήρια σε απομακρυσμένα τερματικά τα οποία έχουν ενεργοποιημένη την κρυπτογράφηση σε επίπεδο δίσκου.
- Να έχει τη δυνατότητα να αναλύει τους παρακάτω τύπους δεδομένων απευθείας και σε πραγματικό χρόνο:
    - Προεπισκόπηση αρχείων λειτουργικών συστημάτων Windows.
    - Ιστορικό περιήγησης διαδικτύου.
    - Δεδομένα εφαρμογών συνομιλίας (chat).
    - Αρχεία OLE.
    - EDB, OST Και PST email containers
    - Αρχεία ShimCache
- Τα ομοιώματα που θα δημιουργούνται πρέπει να είναι προσβάσιμα κατ΄ επίκληση, μέσω API αλλά και μέσω χρονοπρογραμματισμένης διαδικασίας.

Το εργαλείο που θα επιλεγεί πρέπει να έχει τη δυνατότητα να διατηρεί ένα ομοίωμα (image) της μνήμης των τερματικών σε πραγματικό χρόνο και να διαφυλάσσει τα σχετικά πειστήρια. Συγκεκριμένα θα πρέπει:

- Να διατηρεί ένα ομοίωμα όλων των μονάδων της μνήμης σε πραγματικό χρόνο απομακρυσμένα, όπως βρίσκονται στην ενεργή μνήμη ή σε δυαδική μορφή.
- Να έχει τη δυνατότητα να δημιουργεί απομακρυσμένα ομοιώματα (image) και να διατηρεί όλες τις δραστηριότητες που εκτελούνται στην ενεργή μνήμη των τερματικών, σε πραγματικό χρόνο, είτε αυτές βρίσκονται στην ενεργή μνήμη είτε σε κάποια άλλη μονάδα μνήμης.
- Να έχει τη δυνατότητα να εξάγει τα δεδομένα σε μορφή RAW.

- Ο χρήστης θα πρέπει να μπορεί να αποθηκεύει τα παραπάνω αποτελέσματα και τα πειστήρια του εγκληματολογικού ελέγχου σε οποιαδήποτε τοποθεσία που έχει δικαιοδοσία, τοπικά ή σε δικτυακό προορισμό.
- Τα ομοιώματα (images) που θα δημιουργούνται πρέπει να είναι προσβάσιμα κατ΄ επίκληση, μέσω API αλλά και μέσω χρονοπρογραμματισμένης διαδικασίας.

Το εργαλείο που θα επιλεγεί πρέπει να παρέχει ορατότητα σε όλα τα τερματικά της υποδομής της ΒτΕ σε σχεδόν πραγματικό χρόνο μέσω τηλεμετρίας εγκληματολογίας (forensic telemetry), παράλληλα για όλα τα τερματικά. Ακόμα θα πρέπει να υπάρχει η δυνατότητα μεταφοράς των δεδομένων αυτών στο IBM QRadar της ΒτΕ. Τα δεδομένα τηλεμετρίας πρέπει να περιλαμβάνουν τα παρακάτω στοιχεία:

- Δραστηριότητα σύνδεσης και αποσύνδεσης χρήστη σε πραγματικό χρόνο.
    - Ώρα σύνδεσης
    - Ώρα αποσύνδεσης
    - Όνομα τερματικού
    - Όνομα χρήστη (domain\username)
    - Όνομα διεργασίας που εκκίνησε τη σύνδεση
    - Κατάλογος διεργασίας (process path)
    - ID διεργασίας
    - Hash της διεργασίας
    - ID σύνδεσης
    - Αυθεντικοποιημένο όνομα domain
    - Όνομα σύνδεσης
    - ID συνεδρίας
    - Τύπος συνεδρίας
    - Δείκτης απομακρυσμένης σύνδεσης (remote connection indicator)
    - Όνομα τερματικού από την οποία εκκίνησε η σύνδεση
- Αλληλεπίδραση δικτύου των τερματικών σε πραγματικό χρόνο.
    - Ημερομηνία και ώρα αρχικοποίησης της σύνδεσης
    - Ημερομηνία και ώρα τερματισμού της σύνδεσης
    - Ημερομηνία και ώρα ενημέρωσης της σύνδεσης
    - Την εφαρμογή από την οποία συλλέγηκαν οι πληροφορίες
    - Το όνομα χρήστη που εκκίνησε τη σύνδεση
    - Το όνομα της διεργασίας που εκκίνησε ή δέχτηκε τη σύνδεση
    - Τον κατάλογο της διεργασίας (process path)
    - ID διεργασίας
    - Το hash των διεργασιών που εκτελούνται στη μνήμη

- Την τοπική διεύθυνση IP της σύνδεσης
- Την τοπική πόρτα της σύνδεσης
- Την απομακρυσμένη διεύθυνση IP της σύνδεσης
- Την απομακρυσμένη πόρτα της σύνδεσης
- Το μέγεθος των δεδομένων σε bytes που έχουν σταλεί και ληφθεί από μια συγκεκριμένη διεργασία/σύνδεση.

- Πληροφορίες Windows Registry
  - Ημερομηνία και ώρα που εκτελέστηκε ενέργεια στη registry
  - Τύπος ενέργειας (ερώτημα, τροποποίηση, δημιουργία)
  - ID διεργασίας
  - Όνομα χρήστη που σχετίζεται με την ενέργεια
  - Όνομα διεργασίας που σχετίζεται με την ενέργεια
  - Τον κατάλογο της διεργασίας (process path)
  - Το hash των διεργασιών που σχετίζονται με την ενέργεια
  - Όνομα κλειδιού πυρήνα
  - Τιμή κλειδιού
  - Τύπος τιμής
  - Δεδομένα τιμής
  - Τιμή binary
- Δεδομένα Αρχείων σε πραγματικό χρόνο.
  - Ημερομηνία και ώρα ενέργειας σε αρχείο
  - Τύπος ενέργειας (δημιουργία, αντιγραφή, διαγραφή, μεταφορά, τροποποίηση)
  - Παλιά και νέα τοποθεσία αρχείου (file path)
  - Παλιό και νέο σημείο προσάρτησης αρχείου (mount point)
  - Όνομα χρήστη
  - Όνομα διεργασίας
  - Περιγραφή ενέργειας
  - Hash της δραστηριότητας του αρχείου
- Στιγμιότυπα μνήμης προγραμματισμένα ή κατ' επίκληση σε πραγματικό χρόνο.
  - Πληροφορίες ενεργών δραστηριοτήτων
  - Πληροφορίες των οδηγών προγραμμάτων (drivers)
  - Πληροφορίες των υπηρεσιών που εκτελούνται
  - Πληροφορίες προστατευμένων χώρων αποθήκευσης
  - Πληροφορίες συνεδριών δικτύου

Ανάλυση εσωτερικών απειλών (Insider Threat analysis) και Αναζήτηση Απειλών (Threat Hunting)

Το εργαλείο που θα επιλεγεί πρέπει να έχει τη δυνατότητα να εκτελεί αναζητήσεις μεγάλης έκτασης σε όλη την υποδομή της ΒτΕ, οι οποίες πρέπει να ακολουθούν τις παρακάτω προδιαγραφές:

- Χρήση εντολών της μορφής regular expression GREP.
- Αναζήτηση δεικτών παραβίασης (IOCs) MD5 εντός 5 λεπτών και χωρίς να αποθηκεύει τα αποτελέσματα της αναζήτησης στο τερματικό.
- Δυνατότητα αναζήτησης ενός συγκεκριμένου ονόματος αρχείου εντός 5 λεπτών χωρίς να αποθηκεύει τα αποτελέσματα της αναζήτησης στο απομακρυσμένο τερματικό.
- Δυνατότητα αναζήτησης συγκεκριμένων λέξεων κλειδιών, οι οποίες μπορεί να περιέχονται στο κύριο σώμα ή στο περιεχόμενο ενός αρχείου που είναι αποθηκευμένο στις τερματικές συσκευές. Η αναζήτηση θα πρέπει να γίνεται ταυτόχρονα στα σχετικά τερματικά και τα αποτελέσματα πρέπει να επιστρέφονται σε πραγματικό χρόνο στην κονσόλα του εργαλείου.
- Οι αναζητήσεις μέσω λέξεων κλειδιών θα πρέπει να υποστηρίζουν λογικής Boolean εκφράσεις AND, OR, NOT και NEAR.
- Δυνατότητα αναζήτησης για νέα αρχεία που δημιουργήθηκαν, για την τελευταία πρόσβαση στα αρχεία, για τις ημερομηνίες τροποποίησης των αρχείων και δυνατότητα αναζήτησης αρχείων για ημερομηνίες μεταξύ ενός οριζόμενου χρονικού διαστήματος καθώς και πριν και μετά μια συγκεκριμένη ημερομηνία. Τα αποτελέσματα πρέπει να επιστρέφονται εντός 5 λεπτών χωρίς να γίνεται αποθήκευση των αποτελεσμάτων στο τερματικό.
- Δυνατότητα αναζήτησης ενός συγκεκριμένου τύπου αρχείων χωρίς να εξαρτάται η αναζήτηση αποκλειστικά στην προέκταση του αρχείου.
- Δυνατότητα αναζήτησης μεμονωμένων τερματικών, ομάδας τερματικών ή ολόκληρης της υποδομής.

Το εργαλείο θα πρέπει να είναι σε θέση να καταγράφει σε βίντεο την οθόνη των τερματικών συσκευών στις οποίες είναι εγκατεστημένο (Screen Capture Recording).

Βασική λειτουργικότητα

Το εργαλείο που θα επιλεγεί πρέπει να καλύπτει τις παρακάτω βασικές απαιτήσεις σε επίπεδο εγκατάστασης, ενσωμάτωσης και συντήρησης:

- Όλες οι αναβαθμίσεις του λογισμικού πρέπει να περιλαμβάνονται στην προσφορά.
- Διασύνδεση του εργαλείου με τις βάσεις Virus Total, OPSWAT, Joe Sandbox και με τουλάχιστον ένα cyber intelligence feed.

- Να παρέχει διαχείριση χρηστών, αυθεντικοποίηση χρηστών, ορισμό ρόλων και προσβάσεων σε επίπεδο τερματικών, ομάδας τερματικών και σε λειτουργικότητες της κονσόλας. Σε επίπεδο τερματικών θα πρέπει να παρέχεται η δυνατότητα δημιουργίας, διαχείρισης και διαγραφής χρηστών και ορισμού προσβάσεων βάση δικαιωμάτων.
- Δυνατότητα δημιουργίας και διατήρησης αρχείων καταγραφής (audit logs) για όλες τις ενέργειες των χρηστών του εργαλείου.
- Η εγκατάσταση των ειδικών προγραμμάτων στα τερματικά (agents) θα πρέπει να υποστηρίζεται απομακρυσμένα με χρήση GPO, SCCM ή άλλων εργαλείων διαχείρισης λογισμικών.

Θα πρέπει να παρέχεται η δυνατότητα χρήσης και διασύνδεσης μέσω έτοιμων API με εργαλεία τρίτων κατασκευαστών και ειδικά με το εργαλεία IBM Qradar. Η διασύνδεση μέσω API πρέπει να είναι ασφαλής με χρήση πιστοποιητικών.

Απόδοση και συμβατότητα

Το εργαλείο που θα επιλεγεί από την ΒτΕ πρέπει να έχει τη δυνατότητα να εκτελεί τις ενέργειες εντοπισμού εντός λίγων δευτερολέπτων και αποκατάστασης εντός λίγων λεπτών, στο σύνολο της υποδομής και διενεργώντας παράλληλες ενέργειες.

Ο τρόπος λειτουργίας του εργαλείου θα πρέπει να μην επηρεάζει τη λειτουργία των τερματικών και δεν θα πρέπει να γίνεται αντιληπτή από τον χρήστη.

Όλες οι προδιαγραφές που αναφέρθηκαν θα πρέπει να καλύπτονται με την εγκατάσταση ενός και μόνο ειδικού προγράμματος (agent) στα τερματικά. Η εγκατάσταση θα πρέπει να είναι εύκολη και δεν θα πρέπει να χρήζει επανεκκίνησης του τερματικού. Μετά την εγκατάσταση θα πρέπει να δίνεται η πλήρης λειτουργικότητα άμεσα.

Θα πρέπει να διασφαλιστεί διαλειτουργικότητα με τα λειτουργικά συστήματα της ΒτΕ Windows Server 2012 R2, Windows 10, Windows 7 καθώς και με το σύστημα διαχείρισης περιστατικών ασφάλειας IBM QRadar.

Επιλέξιμες υπηρεσίες

Ο ανάδοχος ή ο κατασκευαστής θα πρέπει να έχει την δυνατότητα να αναλάβει -έναντι πρόσθετης αμοιβής που θα προσδιορίζει στην προσφορά του- την εκτέλεση των ενεργειών που πρέπει να γίνουν για την περαιτέρω διερεύνηση για τον περιορισμό ή για την αποκατάσταση του συμβάντος.

4. Πίνακες Συμμόρφωσης

Ανίχνευση κακόβουλου λογισμικού (Malware Detection) και Αντιμετώπιση περιστατικών ασφαλείας (Incident Response)

Α.Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Εντοπισμός κακόβολου λογισμικού (zero-day) και αυτόματος ή χειροκίνητος αποκλεισμός της απειλής.	ΝΑΙ		
2.	Πρέπει να παρέχονται υπηρεσίες SOC 24x7x365 με δυνατότητα απόκρισης σε περιστατικό ασφάλειας μέσω του εργαλείου.	ΝΑΙ		
3.	Η διάρκεια παρεχόμενων υπηρεσιών θα είναι ένα (1) έτος από την ημερομηνία ενεργοποίησης των αδειών	ΝΑΙ		
4.	Σύνδεση της ομάδας SOC με ασφαλείς διαδικασίες και πρωτόκολλα.	ΝΑΙ		
5.	Παραγωγή προσαρμοσμένων ενημερώσεων-συναγερμών και προσαρμοσμένη επεξεργασία των περιστατικών.	ΝΑΙ		
6.	Ανάλυση διεργασιών των τερματικών για διαχωρισμό των γνωστών και άγνωστων-πιθανών περιστατικών.	ΝΑΙ		
7.	Δυνατότητα να ελέγχει παράλληλα και ταυτόχρονα όλα τα τερματικά και να εντοπίζει το ο λογισμικό εντός λίγων δευτερολέπτων.	ΝΑΙ		
8.	Ο έλεγχος, ο εντοπισμός και το fingerprinting θα πρέπει να γίνεται σε πραγματικό χρόνο, ελέγχοντας το 100% της ενεργής μνήμης RAM.	ΝΑΙ		
9.	Θα πρέπει να υπάρχει η δυνατότητα πρόσβασης μέσω κονσόλας στα τερματικά για ενέργειες απομόνωσης και αποκατάστασης τους εντός λίγων λεπτών με χρήση ασφαλών πρωτοκόλλων.	ΝΑΙ		
10.	Το λογισμικό θα πρέπει να κάνει χρήση της τεχνολογίας cloud αλλά μόνο μεταδεδομένα μπορούν να αποστέλλονται στην υποδομή του Κατασκευαστή.	ΝΑΙ		

11.	Ο έλεγχος για ο λογισμικό και η αντιμετώπιση των περιστατικών ασφαλείας θα πρέπει να γίνεται με ανάλυση σε πραγματικό χρόνο και να περιλαμβάνει: • Ανάλυση της μνήμης όλων τερματικών παράλληλα σε χρόνο μικρότερο των 10λεπτών. • Ανάλυση των σκληρών δίσκων. • Απομακρυσμένη διατήρηση αντιγράφου της μνήμης, των μονάδων του τερματικού και όλων των διεργασιών. • Απομακρυσμένη διατήρηση αντιγράφου των σκληρών δίσκων.	ΝΑΙ		
	Δυνατότητα να ελέγχει σε πραγματικό χρόνο όλες τις δικτυακές συνδέσεις: • Έλεγχος των τοπικών και εξωτερικών συνδέσεων δικτύων LAN και της loopback. • Διατήρηση της ακριβής ώρας που πραγματοποιήθηκε η σύνδεση. • Διατήρηση του ονόματος της διεργασίας και του καταλόγου (path) • Διατήρηση του χρήστη • Διατήρηση της τιμής κατακερματισμού (hash value) • Διατήρηση της ταυτότητας και του ονόματος της τερματικής συσκευής • Διατήρηση της τοπικής και απομακρυσμένης διεύθυνσης IP και της πόρτας της σύνδεσης. • Διατήρηση της ποσότητας των δεδομένων που απεστάλησαν και ελήφθησαν • Αποστολή των δεδομένων στο IBM QRadar.	ΝΑΙ		

Έρευνα ψηφιακής εγκληματολογίας (Digital Forensic Investigation)

Α.Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Δυνατότητα διατήρησης ομοιώματος (image) του σκληρού δίσκου των τερματικών και	ΝΑΙ		

	διαφύλαξη των σχετικών πειστηρίων.			
2.	Δυνατότητα διατήρησης ομοιώματος (image) της μνήμης των τερματικών σε πραγματικό χρόνο και διαφύλαξη των σχετικών πειστηρίων.	ΝΑΙ		
3.	Το εργαλείο που θα επιλεγεί πρέπει να παρέχει ορατότητα σε όλα τα τερματικά σε σχεδόν πραγματικό χρόνο μέσω τηλεμετρίας εγκληματολογίας (forensic telemetry), παράλληλα για όλα τα τερματικά.	ΝΑΙ		
4.	Δυνατότητα μεταφοράς των δεδομένων Digital Forensic στο IBM QRadar.	ΝΑΙ		
5.	Τα δεδομένα Digital Forensics πρέπει να περιλαμβάνουν (σε πραγματικό χρόνο): Δραστηριότητα σύνδεσης και αποσύνδεσης χρήστη Αλληλεπίδραση δικτύου των τερματικών Πληροφορίες Windows Registry Δεδομένα Αρχείων Στιγμιότυπα μνήμης προγραμματισμένα ή κατ' επίκληση	ΝΑΙ		

Ανάλυση εσωτερικών απειλών (Insider Threat analysis) και Αναζήτηση Απειλών (Threat Hunting)

Α.Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Δυνατότητα εκτέλεσης αναζητήσεων μεγάλης έκτασης σε όλη την υποδομή μέσω: Regular expression GREP Αναζήτησης δεικτών παραβίασης (IOCs) MD5 εντός 5 λεπτών Αναζήτησης ενός συγκεκριμένου ονόματος αρχείου εντός 5 λεπτών Αναζήτησης συγκεκριμένων λέξεων κλειδιών Αναζήτησης για νέα αρχεία που δημιουργήθηκαν, για την τελευταία πρόσβαση στα αρχεία, για της ημερομηνίες τροποποίησης των αρχείων	ΝΑΙ		

	Αναζήτησης ενός συγκεκριμένου τύπου αρχείων Δεν θα πρέπει να αποθηκεύει τα αποτελέσματα της αναζήτησης στο τερματικό. Δυνατότητα αναζήτησης μεμονωμένων τερματικών, ομάδας τερματικών ή ολόκληρης της υποδομής.			
2.	Δυνατότητα καταγραφής οθόνης σε βίντεο (Screen Capture Recording).	ΝΑΙ		

Βασική λειτουργικότητα

Α.Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Όλες οι αναβαθμίσεις του λογισμικού πρέπει να περιλαμβάνονται στην προσφορά.	ΝΑΙ		
2.	Πρέπει να υπάρχει διασύνδεση του εργαλείου με τις βάσεις Virus Total, OPSWAT, Joe Sandbox και με τουλάχιστον ένα cyber intelligence feed.	ΝΑΙ		
3.	Θα πρέπει να παρέχει διαχείριση χρηστών, αυθεντικοποίηση χρηστών, ορισμό ρόλων και προσβάσεων σε επίπεδο τερματικών, ομάδας τερματικών και σε λειτουργικότητες της κονσόλας.	ΝΑΙ		
4.	Σε επίπεδο τερματικών θα πρέπει να παρέχεται η δυνατότητα δημιουργίας, διαχείρισης και διαγραφής χρηστών και ορισμού προσβάσεων βάση δικαιωμάτων.	ΝΑΙ		
5.	Δυνατότητα δημιουργίας και διατήρησης αρχείων καταγραφής για όλες τις ενέργειες των χρηστών του εργαλείου.	ΝΑΙ		
6.	Η εγκατάσταση θα πρέπει να υποστηρίζεται απομακρυσμένα με χρήση GPO, SCCM ή άλλων εργαλείων διαχείρισης λογισμικών.	ΝΑΙ		
7.	Δυνατότητα χρήσης και διασύνδεσης μέσω έτοιμων API με εργαλεία τρίτων κατασκευαστών και ειδικά με το εργαλεία IBM	ΝΑΙ		

	Qradar. Η διασύνδεση μέσω API πρέπει να είναι ασφαλής με χρήση πιστοποιητικών.			

Απόδοση και συμβατότητα

Α.Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Δυνατότητα να εκτελεί τις ενέργειες εντοπισμού εντός λίγων δευτερολέπτων.	ΝΑΙ		
2.	Το εργαλείο θα πρέπει να έχει τη δυνατότητες αποκατάστασης περιστατικού εντός λίγων λεπτών.	ΝΑΙ		
3.	Το τρόπος λειτουργίας του εργαλείου θα πρέπει να μην επηρεάζει τη λειτουργία των τερματικών και δεν θα πρέπει να γίνεται αντιληπτή από τον χρήστη.	ΝΑΙ		
4.	Όλες οι προδιαγραφές που αναφέρθηκαν θα πρέπει να καλύπτονται με την εγκατάσταση ενός και μόνο ειδικού προγράμματος (agent) στα τερματικά.	ΝΑΙ		
5.	Η εγκατάσταση θα πρέπει να είναι εύκολη και δεν θα πρέπει να χρήζει επανεκκίνησης του τερματικού.	ΝΑΙ		
6.	Μετά την εγκατάσταση θα πρέπει να δίνεται η πλήρης λειτουργικότητα άμεσα.	ΝΑΙ		
7.	Θα πρέπει να υπάρχει υποστήριξη των λειτουργικών συστημάτων Windows Server 2012 R2, Windows 10, Windows 7 καθώς και με το σύστημα διαχείρισης περιστατικών ασφάλειας IBM QRadar.	ΝΑΙ		

Παρεχόμενες Υπηρεσίες

Α.Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Ο ανάδοχος θα πρέπει να παράσχει εκπαίδευση μιας εβδομάδος σε τουλάχιστον τρία άτομα της Δνσης Πληροφορικής και Επικοινωνιών για την παραγωγική και επιχειρησιακή αξιοποίηση του λογισμικού	ΝΑΙ		

Α.Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.	Το λογισμικό θα συνοδεύεται από δικαίωμα χρήσης ενός έτους (subscription based licensing), κατά την διάρκεια του οποίου θα παρέχονται από τον κατασκευαστή δωρεάν ενημερώσεις και επιδιορθώσεις προβλημάτων καλής λειτουργίας	ΝΑΙ		
3.	Ο ανάδοχος θα πρέπει να παράσχει υπηρεσίες SOC 24x7x365	ΝΑΙ		
4	Ο ανάδοχος θα πρέπει να διαθέτει Help desk και να περιγράψει τη διαδικασία επικοινωνίας με τον οργανισμό για την αναφορά προβλημάτων και περιστατικών ασφαλείας	ΝΑΙ		
5	Το SOC της κατασκευάστριας εταιρείας ή του αναδόχου θα ενημερώνει την ΒτΕ εντός 10', μέσω τρόπου που θα αποφασιστεί από κοινού (τηλέφωνο, mail, ticket, κλπ) για το συμβάν που παρατήρησε και για τις πρώτες ενέργειες που πρέπει να γίνουν για τον περιορισμό ή για την αποκατάσταση του.	ΝΑΙ		