@ΣΗΔΕ ΙΡΙΔΑ
686382a58a2c181a38c04fe9
ΑΠ:29796
Υπογραφή: 01/07/25 09:48
Διανομή: 01/07/25 10:45

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΝΟΜΟΣ ΧΙΟΥ
ΔΗΜΟΣ ΧΙΟΥ
Δ/ΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Μ Ε Λ Ε Τ Η

Ενίσχυση Υποδομών Ασφαλείας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΗΜΟΣ ΧΙΟΥ
Δ/ΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Μελέτη: Ενίσχυση Υποδομών Ασφαλείας

ΤΕΧΝΙΚΗ ΠΕΡΙΓΡΑΦΗ

Με την παρούσα μελέτη προβλέπεται να γίνουν όλες οι απαραίτητες ενέργειες προκειμένου να ενισχυθεί ο βαθμός ασφαλείας των πληροφοριακών συστημάτων του Δήμου Χίου σύμφωνα με την οδηγία NIS-2.

Συγκεκριμένα προβλέπεται να γίνει η προμήθεια μιας υποδομής offline backup και αδειών χρήσεων εξειδικευμένου λογισμικού του τείχους προστασίας που υπάρχει στο Δήμο.

Αναλυτικά η προτεινόμενη λύση περιλαμβάνει:

- **Μηχανισμός λήψης αντιγράφων ασφαλείας:**

- Tape library (autoloader) με σύνθεση ικανή να εξασφαλίσει την ζητούμενη λειτουργικότητα.
- Εξυπηρετητή Backup
- Data media για την διατήρηση δεδομένων
- Επέκταση του λογισμικού backup
- Υπηρεσίες εγκατάστασης

Μια δόκιμη και αποτελεσματική λύση για διαφύλαξη των δεδομένων είναι η τήρηση αντιγράφων ασφαλείας σε επανεγράψιμα φορητά μέσα αποθήκευσης όπως τα tape media. Τα media αυτά μετά την εγγραφή τους μπορούν να φυλάσσονται σε ασφαλείς τοποθεσίες (πχ θυρίδες ασφαλείας) και να εξασφαλίζουν την ανάσυρση των δεδομένων όποτε χρειάζεται. Η μέθοδος είναι συμβατή με όλες τις οδηγίες (Ευρωπαϊκές και Διεθνείς) που αφορούν στην ασφάλεια δεδομένων.

Υφιστάμενη Υποδομή

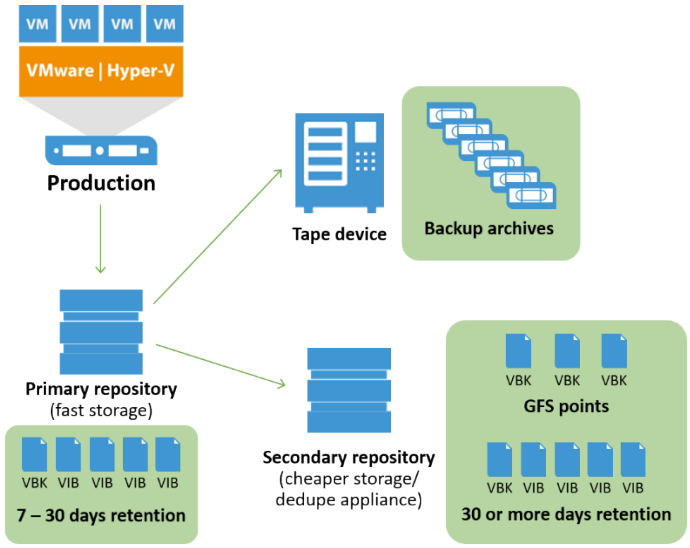
Η υφιστάμενη πληροφοριακή υποδομή του Δήμου Χίου απαρτίζεται από :

- Τρεις εξυπηρετητές DELL PE R740 που απαρτίζουν ένα VMware Cluster
- Ένα Storage system Compellent SCv 3020
- Η διασύνδεση της πληροφορικής υποδομής μέσω Ethernet γίνεται με δύο switch DELL S4048-ON.

Για την υποδομή αυτή έχει προβλεφθεί μηχανισμός λήψης αντιγράφων ασφαλείας, που στηρίζεται σε μια συσκευή αποθήκευσης σε δίσκους του τύπου DELL Data Domain 6300 και σε λογισμικό Veeam που καλύπτει το σύνολο των εξυπηρετητών και των δεδομένων.

D2D2T Bsckup

Μία από τις προσεγγίσεις που συνιστά η VEEAM είναι η διατήρηση της αρχικής αλυσίδας αντιγράφων ασφαλείας σε δίσκους, που επιτρέπει την ανάκτηση των δεδομένων στο συντομότερο χρονικό διάστημα. Η μακροπρόθεσμη και η ασφαλής διατήρηση προέρχεται από δευτερογενή αποθήκευση, η οποία συνήθως διατίθεται με πολύ χαμηλότερο κόστος αποθήκευσης, αλλά με αντιστάθμιση, το RTO αφού η αποκατάσταση από την αποθήκευση μπορεί να διαρκέσει περισσότερο χρόνο.
Μία από τις πιο δημοφιλείς επιλογές για τη δευτερογενή αποθήκευση είναι η ταινία. Είναι φτηνή, αξιόπιστη και προσφέρει προστασία από τους ιούς και τις επιθέσεις χάκερ. Επιπλέον, είναι εκτός σύνδεσης (offline) όταν δεν είναι σε Tape Library.
Με το Veeam, οι διαχειριστές μπορούν να χρησιμοποιήσουν ευέλικτες επιλογές για να δημιουργήσουν αντίγραφα των αντιγράφων ασφαλείας και να τα αποθηκεύσουν σε ταινίες, ακολουθώντας τον κανόνα 3-2-1 για την αποκατάσταση αντιγράφων ασφαλείας.



Συνοπτικά δημιουργείται ένα αντίγραφο ασφαλείας δίσκου προς δίσκο (στην παρούσα περίπτωση από το compellent στο datadomain) που επιτρέπει την γρήγορη πρόσβαση στα δεδομένα από ένα αντίγραφο δίσκου σε ταινία για τα ίδια ακριβώς δεδομένα. Τα αντίγραφα ασφαλείας που προκύπτουν στην ταινία μπορούν εύκολα να μεταφερθούν εκτός του κέντρου δεδομένων σε ασφαλές μέρος (λεγόμενο αντίγραφο ασφαλείας εκτός τόπου) και να παραμένουν εκεί μέχρι να χρειαστεί η ανάσυρση των δεδομένων.

Προς προμήθεια εξοπλισμός

1. **Tape Library IBM TS2900 ή ισοδύναμο**

Το βασικό συστατικό της λύσης είναι το IBM TS2900 Tape Autoloader εφοδιασμένο με ένα drive LTO9 HH SAS.
Το IBM TS2900 Tape Autoloader είναι μια συμπαγής μονάδα ταινίας 1U που προσφέρει την αξιοπιστία, την πυκνότητα και την απόδοση του Tape.
Με χωρητικότητα εννέα κασέτες, το TS2900 Tape AutoLoader είναι μια μονάδα που μπορεί να εγκατασταθεί σε rack και περιέχει μία μονάδα IBM LTO Ultrium 9 Half-High με διασύνδεση SAS
Η συσκευή συνοδεύεται από :

- (6171) Rack Mount Kit
- 1.5 m Mini-SAS HD/Mini-SAS HD 1X Cable
- (6171) Transparent LTO Encryption license

- Ultrium 9 Data Cartridges (5-pack) (τεμ. 3)
- Ultrium Cleaning Cartridge L1UCC (τεμ 1)

2. Backup Server PowerEdge R360 Server ή ισοδύναμος

Προτείνεται ένας DELL Server PowerEdge R360 στον οποίο θα μεταφερθεί το backup λογισμικό Veeam και πάνω στον οποίο θα συνδεθεί μέσω SAS Interface το Tape Autoloader.
Η σύνθεση του προτεινόμενου server θα έχει ως εξής:

Option Name	**Qty**
PowerEdge R360 Server	1
Trusted Platform Module 2.0 V5	1
2.5" Chassis with up to 8 Hot Plug Hard Drives, Front PERC 11	1
Intel® Xeon® 6 Performance 6353P 2.7G, 8C/16T, 24M Cache, Turbo, (65W) DDR5-4800	1
Heatsink	1
16GB UDIMM, 5600MT/s ECC	2
HBA355e Adapter FH & LP, DIB	1
C3, RAID 1 for 2 HDDs or SSDs (Matching Type/Speed/Capacity)	1
Front PERC H355 Front Load	1
480GB SSD SATA Mixed Use 6Gbps 512e 2.5in Hot-plug AG Drive, 3 DWPD	2
Power Saving BIOS Setting	1
UEFI BIOS Boot Mode with GPT Partition	1
Standard Fan	1
Dual, (1+1)Fully Redundant, H-P PSU, 700W MM HLAC (200-240V ONLY, not for 100-120V outlet) Titanium	1
Rack Power Cord 2M (C13/C14 10A)	2
Riser Config 2, Butterfly Gen4 Riser (x8/x8)	1
PowerEdge R360 Motherboard with with Broadcom 5720 Dual Port 1Gb On-Board LOM, MLK	1
Broadcom 57414 Dual Port 10/25GbE SFP28 Adapter, PCIe Low Profile, V2	1
PowerEdge 1U Standard Bezel	1
Dell Networking, Cable, SFP+ to SFP+, 10GbE, Copper Twinax Direct Attach Cable, 3 Meter	2
Windows Server 2025 Standard,16CORE,FI,No Med,No CAL, Multi Language	1
Windows Server 2025 Standard,16CORE,DF Recovery Image, Multi Lang, (Downgrade not included)	1
iDRAC9, Enterprise 16G	1
Dell Connectivity Client - Enabled	1
iDRAC,Factory Generated Password, No OMQR	1
ReadyRails™ Sliding Rails Without Cable Management Arm	1
PowerEdge R360 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew)	1
PowerEdge R350/R360 Shipping Material for 2.5" Chassis	1
PowerEdge R360 CE and CCC Marking, No BIS Marking	1
Titanium PSU configuration	1

Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM)	1
Basic Next Business Day 12 Months, 12 Month(s)	1
ProSupport and Next Business Day Onsite Service, 60 Month(s)	1
Asset Tag - ProSupport (Website, barcode, Onboard MacAddress)	1

Ο Server διατίθεται με λειτουργικό σύστημα Windows Server 2025 Standard

3. Λογισμικό Backup Veeam

Η προτεινόμενη λύση δεν απαιτεί νέες άδειες εγκατάστασης του λογισμικού backup παρά μόνο την επέκταση της άδειας χρήσης και της υποστήριξης των υφιστάμενων αδειών η οποία προτείνεται να είναι για τρία (3) έτη.
Συγκεκριμένα προτείνεται το:
Veeam Data Platform Essentials Universal Subscription License. Includes Enterprise Plus Edition features (5-instance). 3 Years Renewal Subscription Upfront Billing & Production(24/7) Support. Public Sector. (Τεμ. 6)

4. Υπηρεσίες Εγκατάστασης

Οι προσφερόμενες υπηρεσίες περιλαμβάνουν (όχι περιοριστικά):

- Την αρχικοποίηση του εξυπηρετητή
- Την εγκατάσταση του λειτουργικού και την ενημέρωση αυτού
- Την εγκατάσταση του λογισμικού
- Την παραμετροποίηση για την διασύνδεση με το tape library
- Την δοκιμή λειτουργίας
- Την σε συνεργασία σχεδίαση του backup policy
- Την εφαρμογή του backup policy και την παρακαλούθησή του για μια εβδομάδα.

- **Όσον αφορά την υποδομή τείχους προστασίας**

Προτείνονται οι εξής βελτιώσεις για την υποδομή της Fortinet που χρησιμοποιεί ο Δήμος:

1. **FortiAuthenticator VM**
   FAC-VM-BASE (VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms)

Προτείνεται ένα σύστημα αυθεντικοποίησης χρηστών FortiAuthenticator VM της Fortinet. Το σύστημα υποστηρίζει 100 χρήστες και υπάρχει η δυνατότητα για επέκταση των υποστηριζόμενων χρηστών με χρήση επιπλέον άδειας.

Στον παρακάτω πίνακα συνοψίζονται τα χαρακτηριστικά και οι επιδόσεις του προσφερόμενου FAC-VM:

FAC-VM	
Capacity	
Users (Local and Remote)	**100**
FortiTokens	**50**
NAS Devices	**33**
User Groups	**10**
CA Certificates	**5**
User Certificates	**500**
Virtual Machine	
HyperVisors Supported	**VMware ESXi/ ESX 6/ 7/ 8, Microsoft Hyper-V Server 2010, 2012 R2, 2016, and 2019, KVM, Xen, Microsoft Azure, AWS, Nutanix AHV (Acropolis Hypervisor), Oracle OCI, Alibaba Cloud**
Maximum vCPUs Supported	**64**
Virtual NICs Required (Minimum / Maximum)	**1 / 4**
Virtual Machine Storage (Minimum / Maximum)	**60 GB / 16 TB**
Virtual Machine Memory Required (Minimum / Maximum)	**2 GB / 1 TB**
High Availability Support	**Active-Passive HA and Config Sync HA**

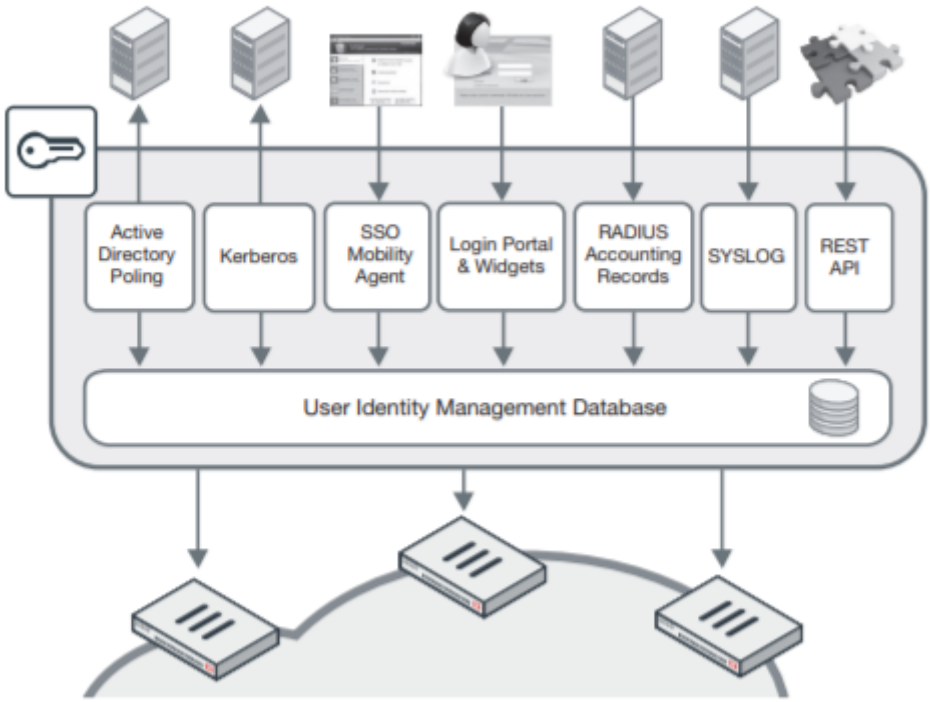
Πολλές από τις πιο επιζήμιες παραβιάσεις έχουν επιτευχθεί μέσω μη εξουσιοδοτημένων χρηστών που αποκτούν πρόσβαση σε ένα δίκτυο ή ακατάλληλων επιπέδων πρόσβασης που παραχωρούνται σε έγκυρους χρήστες. Το FortiAuthenticator παρέχει υπηρεσίες που είναι απαραίτητες για τη δημιουργία μιας αποτελεσματικής πολιτικής ασφάλειας διασφαλίζοντας ότι μόνο το κατάλληλο άτομο τη σωστή στιγμή μπορεί να έχει πρόσβαση στα ευαίσθητα δίκτυα και τα δεδομένα σας.

Το Σύστημα αυθεντικοποίησης FortiAuthenticator ενισχύει την ασφάλεια του φορέα απλοποιώντας τη διαχείριση και αποθήκευση πληροφοριών ταυτότητας χρήστη.

Πολιτική ταυτότητας εταιρικού δικτύου

Η πρόσβαση στο τοπικό δίκτυο και στο internet είναι το κλειδί για σχεδόν κάθε ρόλο εντός της επιχείρησης. Ωστόσο, αυτή η απαίτηση πρέπει να ισορροπεί με τον κίνδυνο που ενέχει. Ο βασικός στόχος είναι ο φορέας να παρέχει ασφαλή αλλά ελεγχόμενη πρόσβαση στο δίκτυο που επιτρέπει στο σωστό άτομο τη σωστή πρόσβαση τη σωστή στιγμή, χωρίς συμβιβασμούς στην ασφάλεια.

Το Fortinet Single Sign-On είναι η μέθοδος παροχής ασφαλούς ταυτότητας και πρόσβασης στο δίκτυο. Μέσω της ενοποίησης με τα υπάρχοντα συστήματα ελέγχου ταυτότητας Active Directory ή LDAP, χρησιμοποιεί ασφάλεια που βασίζεται στην ταυτότητα των εταιρικών χρηστών. Το FortiAuthenticator βασίζεται στα θεμέλια του Fortinet Single Sign-on, προσθέτοντας ένα μεγαλύτερο εύρος μεθόδων αναγνώρισης χρήστη και μεγαλύτερη επεκτασιμότητα. Το FortiAuthenticator είναι ο φύλακας της εξουσιοδότησης στο ασφαλές εταιρικό δίκτυο Fortinet που προσδιορίζει τους χρήστες, ζητά δικαιώματα πρόσβασης από συστήματα τρίτων και κοινοποιεί αυτές τις πληροφορίες σε συσκευές FortiGate για χρήση σε Πολιτικές βάσει ταυτότητας.

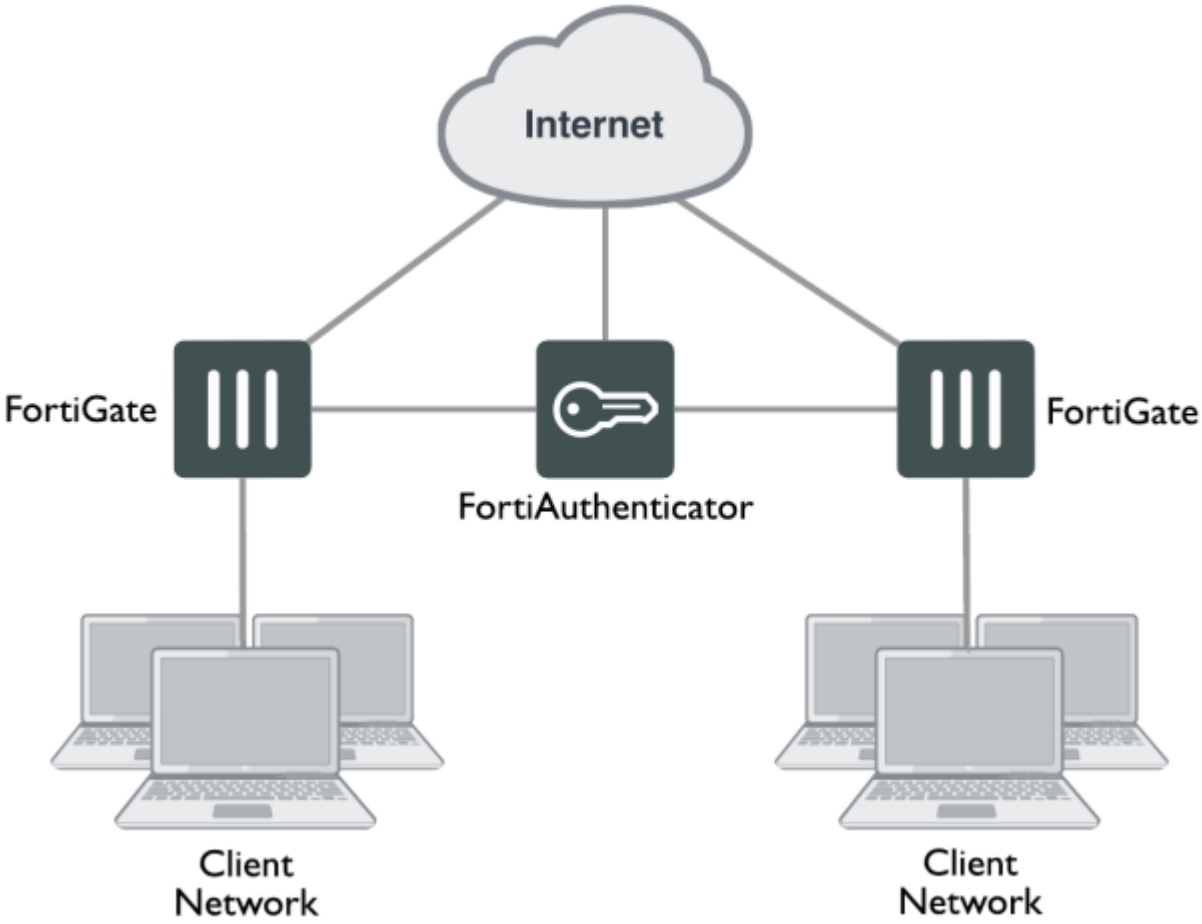


Χαρακτηριστικά

- Ενεργοποιεί πολιτικές ασφαλείας βάσει ταυτότητας και ρόλων στο ασφαλές εταιρικό δίκτυο Fortinet χωρίς την ανάγκη πρόσθετου ελέγχου ταυτότητας μέσω της ενσωμάτωσης με την υπηρεσία καταλόγου Active Directory
- Ενισχύει την ασφάλεια της επιχείρησης απλοποιώντας και συγκεντρώνοντας τη διαχείριση των στοιχείων ταυτότητας των χρηστών
- Ασφαλής έλεγχος ταυτότητας πολλαπλών παραγόντων/OTP με πλήρη υποστήριξη για το FortiToken
- Έλεγχος ταυτότητας RADIUS και LDAP
- Διαχείριση πιστοποιητικών για την ανάπτυξη εταιρικού VPN
- Υποστήριξη IEEE802.1X για ασφάλεια ενσύρματου και ασύρματου δικτύου
- SAML SP/IdP Web SSO
- OpenID Connect SSO
- Χαρακτηριστικά FIDO2 - Γνωστό και ως έλεγχος ταυτότητας χωρίς κωδικό πρόσβασης, το FIDO2 είναι ένας άλλος ισχυρός έλεγχος ταυτότητας που επιτρέπει τη χρήση ενός ισχυρού μόνο παράγοντα ταυτοποίησης (χωρίς κωδικό πρόσβασης), δύο παραγόντων και πολλαπλών παραγόντων έλεγχο ταυτότητας για πρόσθετη προστασία

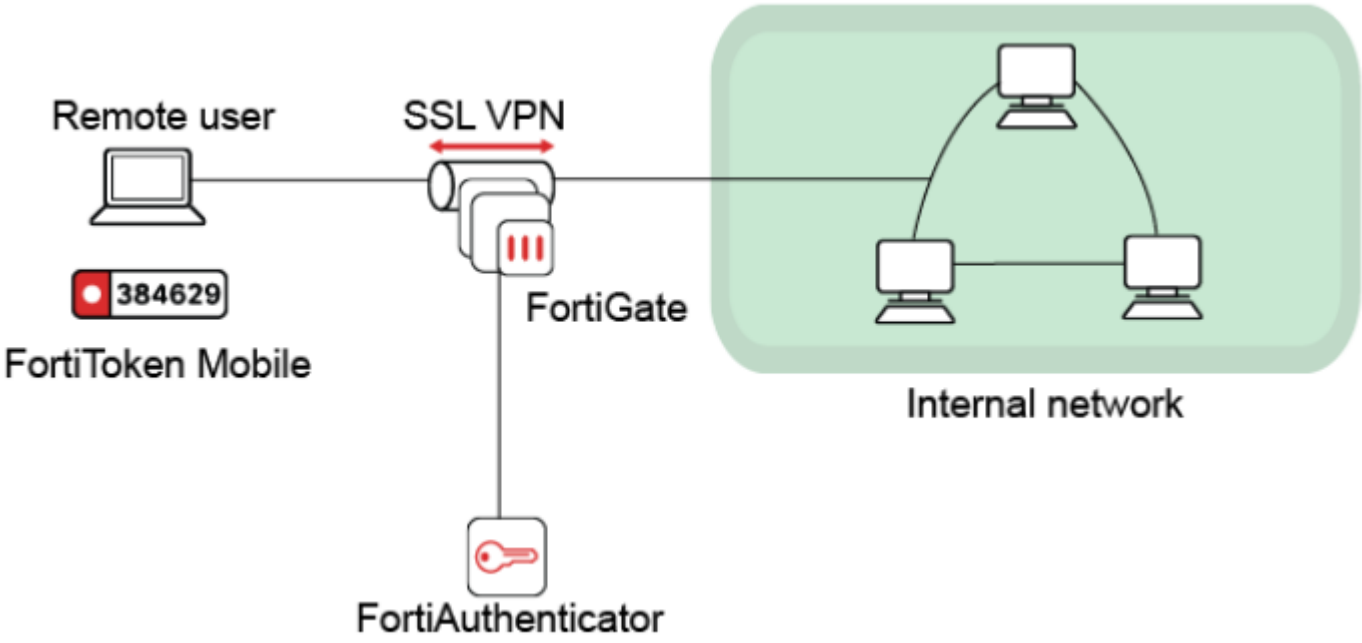
Πρόσθετη Λειτουργικότητα

Το FortiAuthenticator επεκτείνει τη δυνατότητα ελέγχου ταυτότητας πολλαπλών παραγόντων σε πολλές συσκευές FortiGate και σε λύσεις τρίτων κατασκευαστών που υποστηρίζουν έλεγχο ταυτότητας RADIUS ή LDAP. Τα στοιχεία ταυτότητας χρήστη από το FortiAuthenticator σε συνδυασμό με πληροφορίες ελέγχου ταυτότητας από το FortiToken ή/και την υπηρεσία ελέγχου ταυτότητας FIDO2 διασφαλίζουν ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση στις ευαίσθητες πληροφορίες του οργανισμού. Αυτό το πρόσθετο επίπεδο ασφάλειας μειώνει σημαντικά την πιθανότητα διαρροής δεδομένων, ενώ βοηθά τις εταιρείες να πληρούν τις απαιτήσεις ελέγχου που σχετίζονται με τους κυβερνητικούς και επιχειρηματικούς κανονισμούς περί απορρήτου.



Το FortiAuthenticator προσφέρει την ευρύτερη δυνατή γκάμα ελέγχου ταυτότητας πολλαπλών παραγόντων, συμπεριλαμβανομένης της υπηρεσίας ελέγχου ταυτότητας χωρίς κωδικό πρόσβασης FIDO2, για να ταιριάζει στις απαιτήσεις των χρηστών σας. Με τη φυσική συσκευή FortiToken 200, το FortiToken Mobile (για iOS, Android και Windows), το ηλεκτρονικό ταχυδρομείο/SMS OTP καθώς και το FIDO2, το FortiAuthenticator διαθέτει ισχυρές επιλογές ελέγχου ταυτότητας για όλους τους χρήστες και τα σενάρια.

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων μπορεί να χρησιμοποιηθεί για τον έλεγχο της πρόσβασης σε εφαρμογές όπως διαχείριση FortiGate, SSL και IPsec VPN, σύνδεση Wireless Captive Portal, εξοπλισμό δικτύου συμβατό με RADIUS και πάροχοι υπηρεσιών SAML. Το FortiAuthenticator προσφέρει επίσης ένα REST API που μπορεί να χρησιμοποιηθεί για την προσθήκη MFA σε οποιαδήποτε web εφαρμογή.



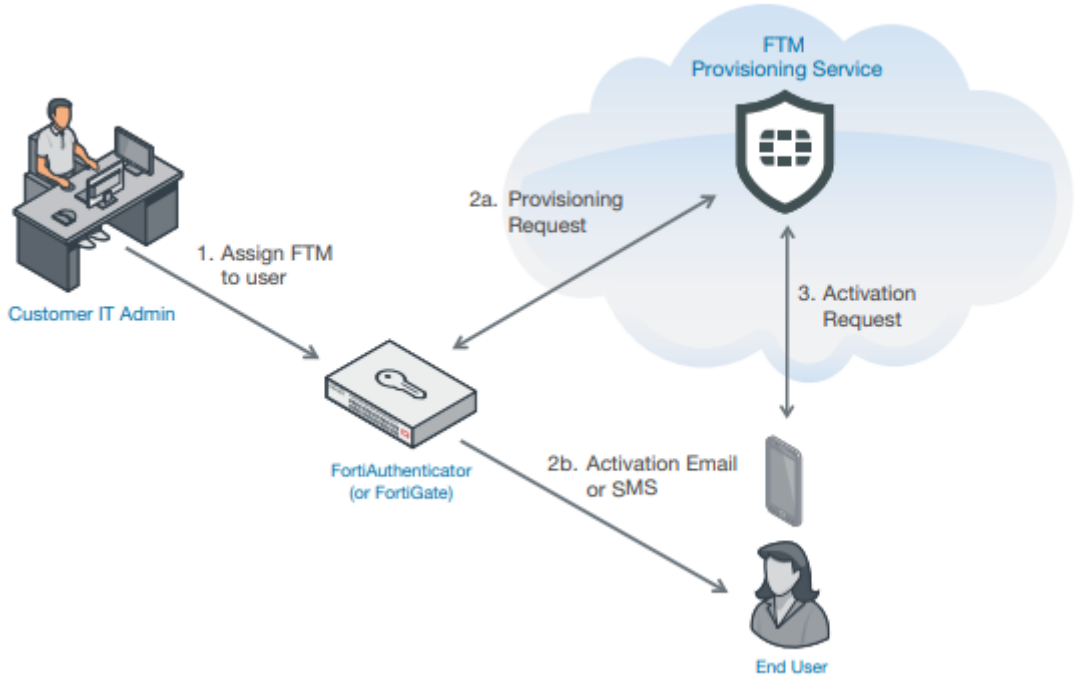
Για να βελτιστοποιήσει τη διαχείριση των τοπικών χρηστών, το FortiAuthenticator περιλαμβάνει λειτουργίες self-registration χρήστη και ανάκτησης κωδικού πρόσβασης.

2. **Υπηρεσία υποστήριξης FortiAuthenticator VM**
   FC2-10-0ACVM-248-02-36 (FortiCare Premium Support (1 - 1100 USERS)

3. **Λογισμικό Ασφαλούς Διάταξης Δημιουργίας Υπογραφής**
   FTM-ELIC-50 (Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. Electronic license certificate.)

Απαιτούνται 50 άδειες λογισμικού ασφαλούς διάταξης δημιουργίας υπογραφής για mobile συσκευές. Το συγκεκριμένο λογισμικό είναι το FortiToken Mobile της Fortinet.

Τα FortiTokens είναι tokens ασφαλείας που χρησιμοποιούνται ως μέρος ενός συστήματος ελέγχου ταυτότητας δύο παραγόντων στα FortiGate firewall. Το token παράγει ένα προσωρινό κωδικό ο οποίος χρησιμοποιείται για να αποδειχτεί ηλεκτρονικά η ταυτότητά του χρήστη.



Τα FortiToken Mobile παράγουν τους κωδικούς τους σε μια εφαρμογή συμβατή με Android ή σε iOS συσκευή. Το FortiToken Mobile χρησιμοποιεί τεχνολογία ώθησης – push notification - ώστε να λαμβάνονται ειδοποιήσεις σύνδεσης στο smartphone ή το tablet και να επαληθεύονται τα στοιχεία σύνδεσης με ένα μόνο πάτημα.

Συμμόρφωση NIS2 με τις λύσεις ασφάλειας της Fortinet

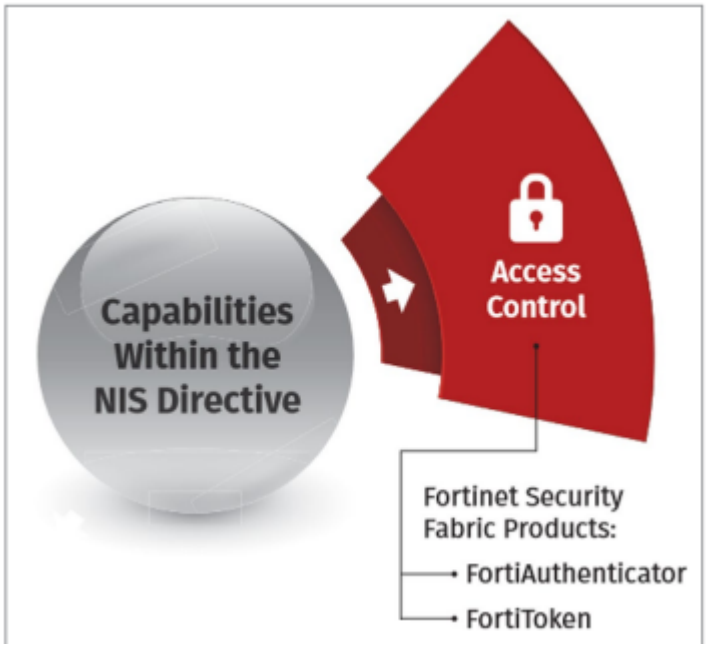
Το τοπίο της κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση υφίσταται σημαντικό μετασχηματισμό με την επικείμενη εφαρμογή της οδηγίας NIS2. Με στόχο την ενίσχυση της κυβερνοασφάλειας σε κρίσιμους τομείς, αυτή η οδηγία δίνει έντονη έμφαση στην ασφάλεια των συσκευών, οι οποίες είναι συχνά ευπαθείς και αποτελούν το σημείο εισόδου στα σύγχρονα δίκτυα.

Η Fortinet προσφέρει μια ολιστική σουίτα λύσεων ασφάλειας που έχουν σχεδιαστεί για να βοηθήσουν τους οργανισμούς να συμμορφωθούν με την οδηγία NIS2. Στον πυρήνα αυτών των λύσεων είναι ο έλεγχος πρόσβασης που αποτελεί ζωτικής σημασίας για τη διατήρηση ενός ασφαλούς IT περιβάλλοντος.

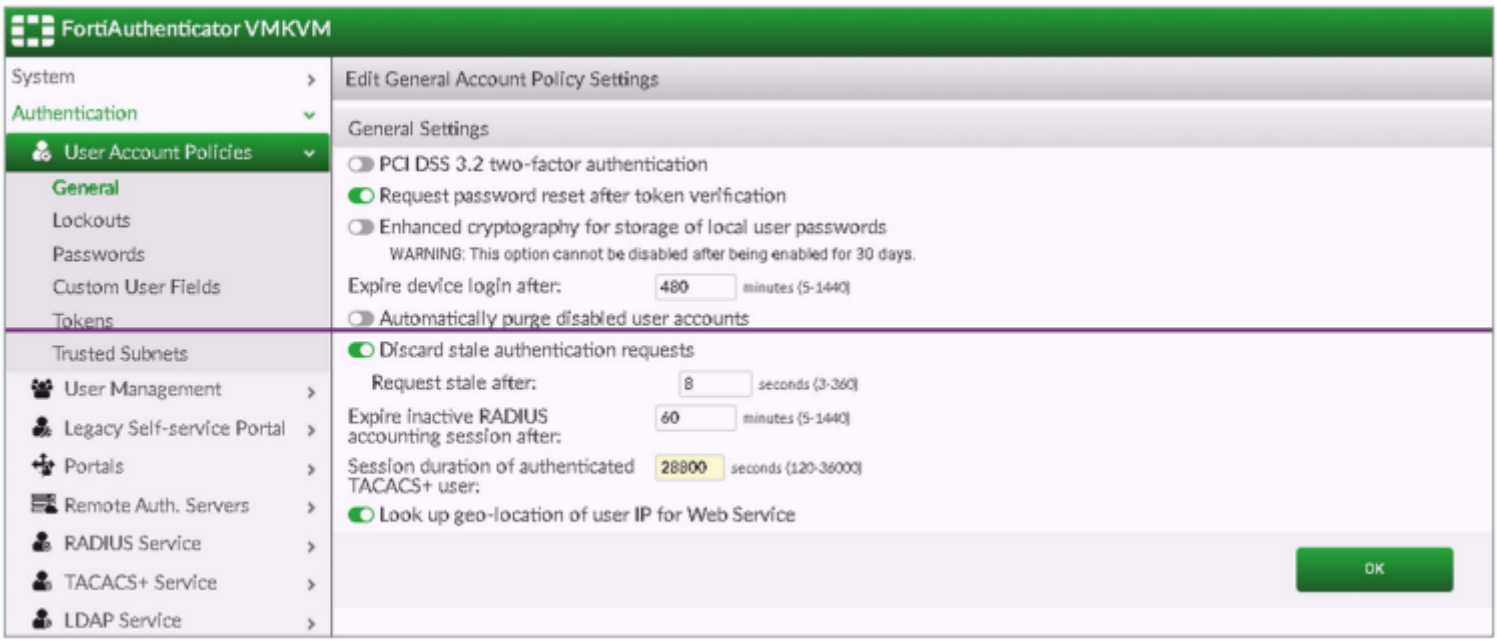
Σύντομη Περιγραφή προϊόντων Fortinet	
Προϊόν Fortinet	Περιγραφή
FortiAuthenticator	Το FortiAuthenticator προσφέρει ενιαία σύνδεση και εξουσιοδότηση χρήστη στο ασφαλές εταιρικό δίκτυο Fortinet. Προσδιορίζει τους χρήστες, ζητά δικαιώματα πρόσβασης από συστήματα τρίτων και προωθεί τα αιτήματα πρόσβασης στο FortiGate για την εφαρμογή πολιτικών ασφαλείας που βασίζονται σε ταυτότητα. Το FortiAuthenticator υποστηρίζει ένα ευρύ φάσμα μεθόδων και εργαλείων για έλεγχο ταυτότητας και εξουσιοδότηση, όπως Active Directory, RADIUS, LDAP, SAML SP/IdP, PKI και έλεγχο ταυτότητας πολλαπλών παραγόντων.
FortiToken	Το FortiToken επιτρέπει τον έλεγχο ταυτότητας δύο παραγόντων μέσω μιας εφαρμογής κωδικού πρόσβασης μίας χρήσης (OTP) με ειδοποιήσεις push ή ενός διακριτικού OTP βασισμένου σε χρόνο υλικού. Το FortiToken Mobile (FTM) και τα Hardware OTP Tokens είναι ασφαλισμένα από το FortiGuard και είναι διαθέσιμα για άμεση διαχείριση και χρήση στα προϊόντα ασφαλείας FortiGate και FortiAuthenticator. Η ολοκληρωμένη λύση FortiGate, FortiToken και FortiAuthenticator είναι εύκολη στην εφαρμογή, τη χρήση και τη διαχείριση για έλεγχο ταυτότητας πολλαπλών παραγόντων.

Έλεγχος πρόσβασης

Το Fortinet Security Fabric παρέχει ενσωματώσεις για πολλά προϊόντα Fortinet, συμπεριλαμβανομένου του FortiAuthenticator. Το FortiAuthenticator παρέχει αναλυτικά στοιχεία ελέγχου σε όλους τους χρήστες για πρόσβαση εντός του δικτύου ελέγχου, καθώς και καταγραφή και παρακολούθηση δραστηριότητας. Οι ίδιοι οι χρήστες μπορούν να βασίζονται σε πολιτικές που βασίζονται σε ταυτότητα και ρόλο, παρέχοντας δημιουργία προφίλ.

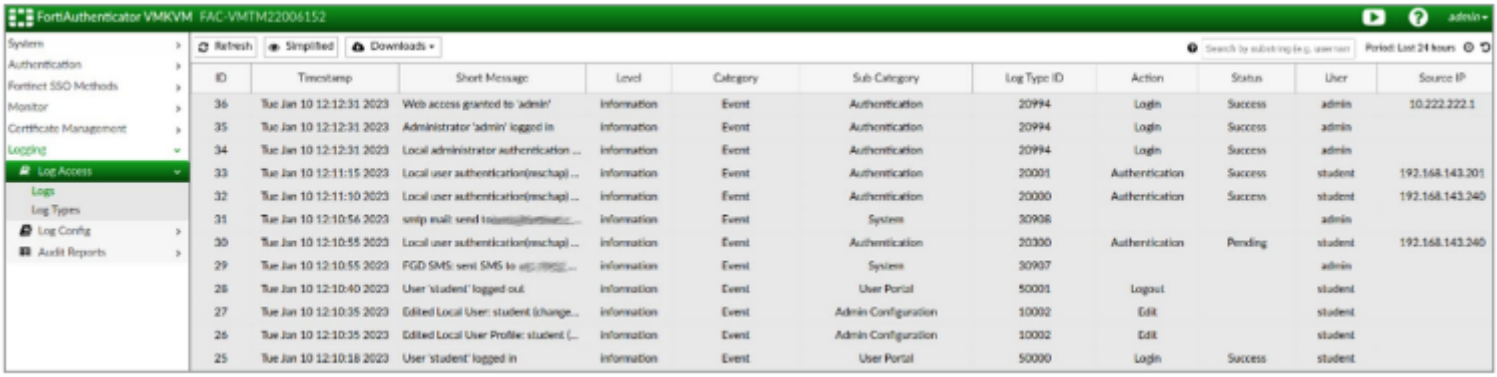


Το FortiAuthenticator έχει επίσης τη δυνατότητα διαχείρισης πιστοποιητικών, δημιουργώντας πρόσθετες επιλογές για τη διαχείριση της πρόσβασης σε πολλαπλές συσκευές δικτύου ελέγχου. Ορισμένα περιβάλλοντα θα ευνοήσουν τη διαχείριση πιστοποιητικών έναντι των μεμονωμένων διαπιστευτηρίων χρήστη και η ευελιξία διαχείρισης αυτών των πιστοποιητικών σε επίπεδο συστήματος μπορεί να παρέχει πρόσθετους ελέγχους ασφαλείας.



Το FortiAuthenticator παρέχει έλεγχο της πρόσβασης στα δίκτυα καθιερώνοντας ταυτοποίηση χρήστη (με δυνατότητα σύνδεσης με AD), έλεγχο ταυτότητας και εξουσιοδότηση (ακόμη και κλείνοντας προσωρινά, με αυτοποιημένο τρόπο τις συνδέσεις που έχουν λήξει). Το σύστημα συνδέει τους χρήστες με δίκτυα και επιτρέπει την προσθήκη ετικετών περιβάλλοντος στα δίκτυα για τον απαραίτητο συντονισμό με το IT. Μπορεί να παρέχεται ακόμη και διαχείριση επισκεπτών, κάτι που είναι επιθυμητό όταν οι επείγουσες καταστάσεις απαιτούν εξωτερική πρόσβαση για να διατηρούνται οι διαδικασίες διαφανείς και ανιχνεύσιμες χωρίς επιβράδυνση των λειτουργιών.

Το FortiToken μπορεί να προσθέσει έλεγχο ταυτότητας δύο παραγόντων στο FortiAuthenticator. Ενώ πολλά εταιρικά δίκτυα μπορούν να αναπτύξουν λύσεις που βασίζονται στο cloud για έλεγχο ταυτότητας δύο παραγόντων, υπάρχουν περιπτώσεις που το δίκτυο θα πρέπει να είναι απομονωμένο. Ο έλεγχος ταυτότητας δύο παραγόντων είναι ένας ισχυρός έλεγχος πρόσβασης ασφαλείας για λογαριασμούς υψηλού κινδύνου, όπως πρόσβαση διαχειριστή ή απομακρυσμένη πρόσβαση που παραχωρείται σε τρίτους για συντήρηση εντός του δικτύου. Τα αρχεία καταγραφής log είναι πολύτιμα για την απόκριση συμβάντων και μπορούν να χρησιμοποιηθούν για τη δημιουργία αναφορών χειρισμού συμβάντων. Το FortiToken βρίσκεται στο Fortinet Security Fabric και μπορεί να προσφέρει μια πιθανή on-premise λύση για αυτές τις περιπτώσεις.



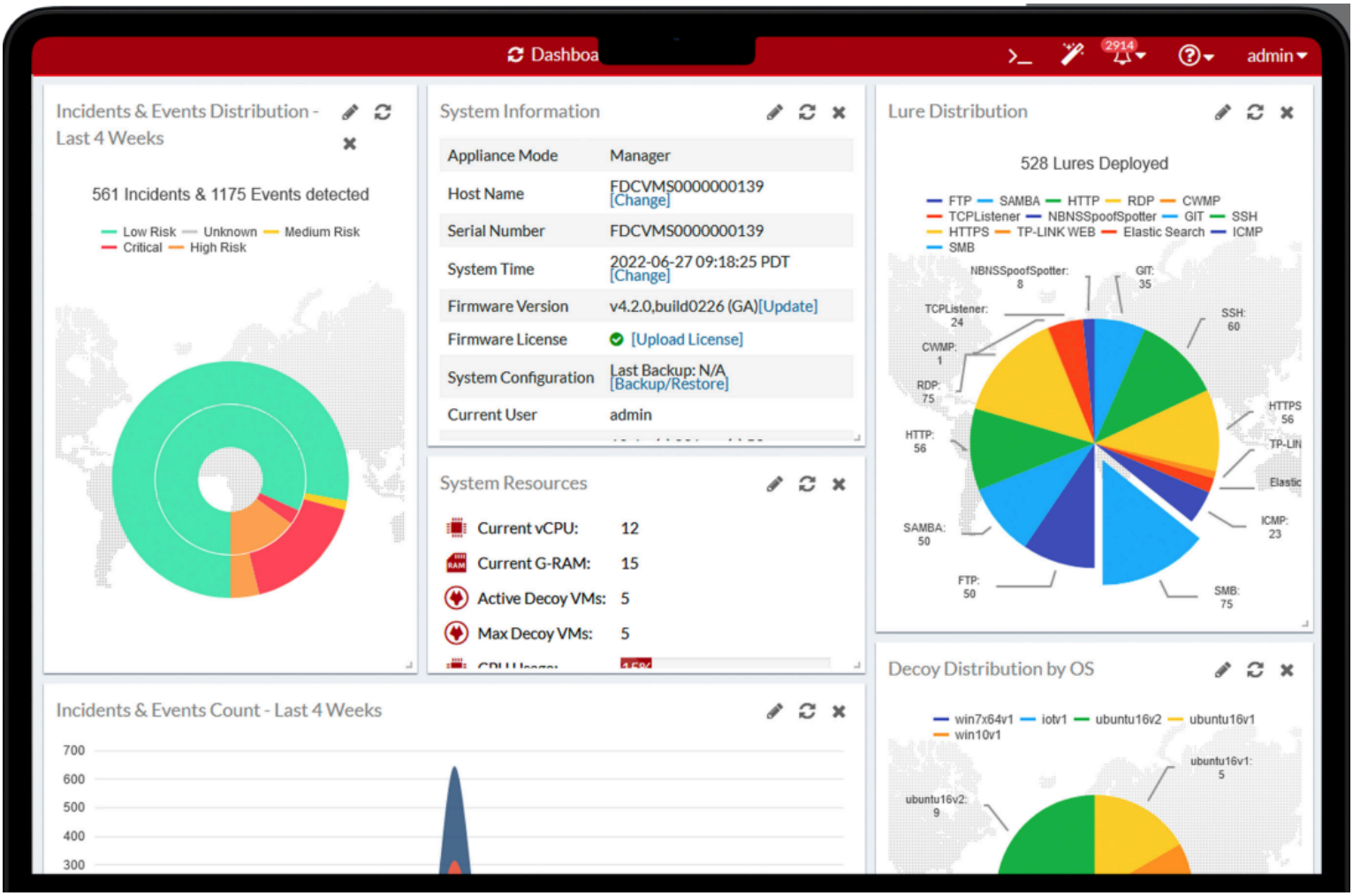
Περίληψη: Χρήση συμμόρφωσης για τη βελτίωση της ασφάλειας IT

Το NIS2 αποτελεί μια βελτίωση της αρχικής οδηγία NIS, όσον αφορά τόσο το πεδίο εφαρμογής όσο και τον οργανωτικό αντίκτυπο. Εστιάζοντας σε συγκεκριμένους τομείς καθώς και σε μεσαίες και μεγάλες οντότητες, το NIS2 μετατοπίζει τη συζήτηση προς τους οργανισμούς που έχουν ουσιαστικό κοινωνικό αντίκτυπο εάν δεν είναι διαθέσιμοι λόγω κυβερνοεπίθεσης. Αυτοί οι οργανισμοί βασίζονται σε περιβάλλοντα ICS και OT,

καθιστώντας το επίκεντρο των λειτουργιών, της φυσικής και της μηχανικής κρίσιμης σημασίας για την ασφάλεια αυτών των δικτύων.
Η συμμόρφωση απαιτεί κάτι περισσότερο από τεχνολογία. Ένα πρόγραμμα που βασίζεται σε NIS2 απαιτεί επαρκή προϋπολογισμό, εκπαιδευμένο προσωπικό και βιώσιμες διαδικασίες. Η σωστή τεχνολογία, ωστόσο, θα πρέπει να επιτρέπει την ισχυρή διαχείριση της συμμόρφωσης. Χρησιμοποιώντας τα πρόσθετα χαρακτηριστικά του Fortinet Security Fabric, που υποστηρίζονται από έμπειρες ομάδες μηχανικών ασφαλείας, ο φορέας θα είναι σε θέση να βελτιώσει τόσο τη διαχείριση του κινδύνου στον κυβερνοχώρο όσο και τις δυνατότητες αντιμετώπισης συμβάντων.
Με την προτεινόμενη λύση του FortiAuthenticator ο Δήμος Χίου καλύπτει το άρθρο 21 του NIS2.
NIS 2 Article 21: Cybersecurity risk-management measures (advisera.com) (Article 21 – G, Article 21 – I, Article 21 – J)

4. **Λογισμικό Cyber Deception As-A-Service**
   FC1-10-DCDAS-496-02-36 (FortiDeceptor-as-a-Service, FortiCare Premium Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs.)

Οι κυβερνητικοί οργανισμοί γίνονται ολοένα και πιο εξαρτημένοι από **συνδεδεμένα συστήματα (OT & IT), IoT αισθητήρες και ασύρματες επικοινωνίες**, καθιστώντας τους στόχο για κυβερνοεπιθέσεις. Το **FortiDeceptor** της Fortinet είναι μια **πλατφόρμα deception** που δημιουργεί **ψηφιακές παγίδες (honeypots & decoys)** για την ανίχνευση και την εξουδετέρωση απειλών προτού αυτές επηρεάσουν πραγματικά τις υποδομές πληροφορικής.



Για το σκοπό αυτό προτείνεται η υπηρεσία **FortiDeceptor-as-a-Service**. **Το FortiDeceptor-as-a-Service** είναι μια **SaaS-based deception λύση**, φιλοξενούμενη στο **ιδιωτικό cloud της Fortinet**, που ανιχνεύει και ανταποκρίνεται σε επιθέσεις εντός του δικτύου, όπως:

- Χρήση **κλεμμένων διαπιστευτηρίων**
- **Lateral movement** (πλευρική κίνηση επιτιθέμενων)
- **Man-in-the-Middle** (MITM) επιθέσεις
- **Ransomware**

Η ανάπτυξη του **FortiDeceptor-as-a-Service** μετατρέπει ολόκληρο το δίκτυο του οργανισμού σε έναν λαβύρινθο, γεμάτο με αυθεντικοφανή ψεύτικα assets μέσα σε λίγα λεπτά. Μόλις εντοπιστεί μια επίθεση, το σύστημα παράγει ειδοποιήσεις υψηλής αξιοπιστίας (zero-false-positive alerts) σε πραγματικό χρόνο. Αυτή η δυνατότητα επιτρέπει στην ομάδα ασφαλείας να ανιχνεύει ανθρώπινες και αυτοματοποιημένες επιθέσεις νωρίτερα στην αλυσίδα επίθεσης (kill chain) και να μεταφέρει τους επιτιθέμενους στο **FortiDeceptor-as-a-Service cloud**, αποτρέποντας ζημιές στο πραγματικό περιβάλλον.

Το **FortiDeceptor-as-a-Service** περιλαμβάνει επίσης μια **ελαφριά συσκευή**, το **FortiDeceptor 100G Edge**, διαθέσιμη ως **εικονική συσκευή (virtual appliance)**.

Όταν αναπτύσσεται στο δίκτυο, το **FortiDeceptor 100G Edge** χρησιμοποιεί **ασφαλή Layer 2 τούνελ** για να **συνδέει τα decoys που φιλοξενούνται στο ιδιωτικό cloud της Fortinet** με τα αντίστοιχα VLANs του φορέα.

Το **ιδιωτικό Layer 2 τούνελ του FortiDeceptor** ενσωματώνει:

- **Μηχανισμούς ταυτοποίησης και κρυπτογράφησης**
- **Heartbeat checks** για συνεχή παρακολούθηση της ασφάλειας
- **Κρυπτογράφηση SSL/TLS** για προστασία των δεδομένων

Αυτό διασφαλίζει ότι η επικοινωνία μεταξύ των **decoys και του εσωτερικού δικτύου** είναι **απόλυτα ασφαλής και αδιάλειπτη**, χωρίς να επηρεάζει τις πραγματικές λειτουργίες του φορέα.

Το **FortiDeceptor** λειτουργεί ως πολλαπλασιαστής ισχύος για τις υπάρχουσες άμυνες κυβερνοασφάλειας, συνδυάζοντας την έννοια του **honeypot** με δυνατότητες για ανάλυση δεδομένων και αντιμετώπιση απειλών. Αυτό επιτυγχάνεται μέσω ενός επιπέδου παραπλανητικών στοιχείων (deception assets) στο δίκτυο—όπως δόλωμα-συστήματα (decoys) και tokens, συμπεριλαμβανομένων ψεύτικων κλειδιών και αρχείων σε endpoints και servers. Δημιουργείται έτσι ένα σύστημα παγίδων που μοιάζουν και λειτουργούν όπως τα πραγματικά στοιχεία (assets) των IT, OT και IoT δικτύων, με σκοπό να παραπλανήσουν, ανιχνεύσουν και απομονώσουν γνωστές και άγνωστες ανθρώπινες και αυτοματοποιημένες επιθέσεις.

Με το **FortiDeceptor**, αντί να περιμένουμε τον εισβολέα να κάνει ένα λάθος για να ανιχνευτεί η παρουσία του, **μπορούμε να υιοθετήσουμε μια ενεργή αμυντική προσέγγιση**, όπου κάθε κίνηση του επιτιθέμενου - είτε προσπαθεί να κλιμακώσει τα προνόμιά του είτε να εκτελέσει κακόβουλο λογισμικό - **γίνεται μια ευκαιρία για την ανίχνευσή του**.

Βασικά Χαρακτηριστικά & Πλεονεκτήματα

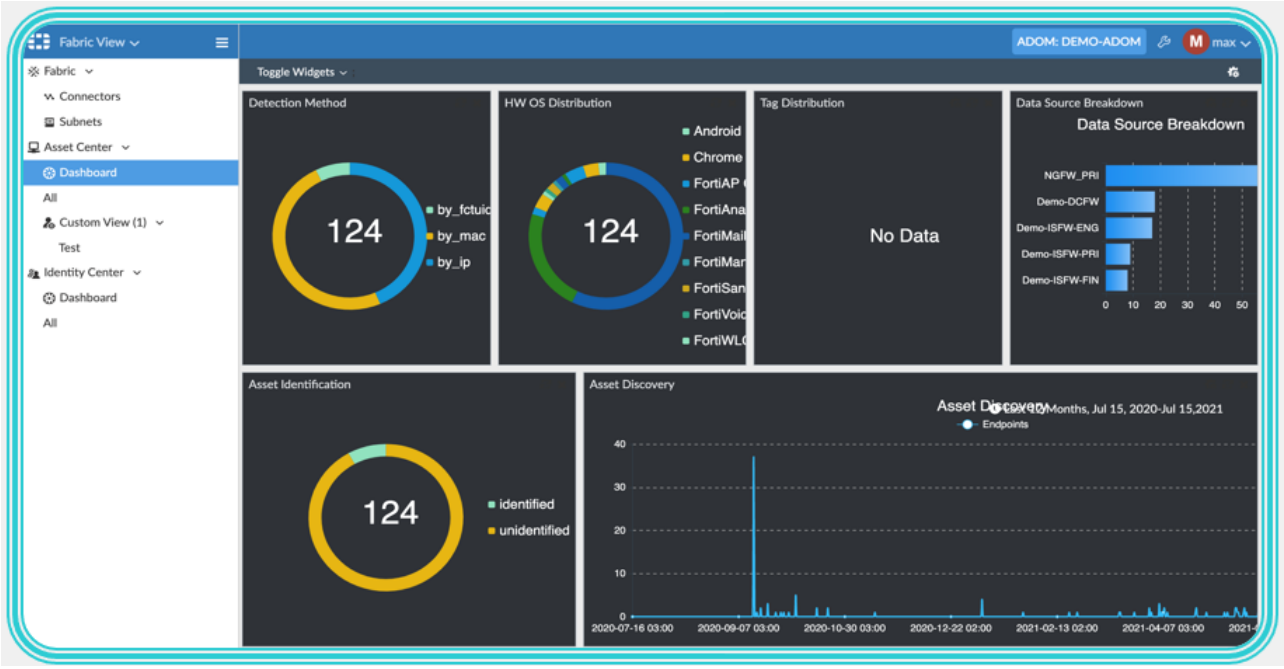
- **Early Threat Detection**: Εντοπίζει APTs (Advanced Persistent Threats) και στοχευμένες επιθέσεις σε υποδομές.
- **Zero Trust Protection**: Αποτρέπει lateral movement από κακόβουλους χρήστες.
- **OT & IT Security**: Δημιουργεί deception assets για βιομηχανικά και εταιρικά δίκτυα.
- **Low-Impact Deployment**: Δεν επηρεάζει τις κανονικές λειτουργίες του οργανισμού.
- **Αυτοματοποιημένη Απόκριση**: Συνδυάζεται με **FortiGate, FortiSIEM, FortiSOAR, FortiAnalyzer** για ταχύτερη απομόνωση απειλών.

5. **Υπηρεσία υποστήριξης του FortiDeceptor VM**
   FC-10-DCVME-248-02-36 (FortiCare premium support Contract for FortiDeceptor-Edge virtual appliance supports on-premise FortiDeceptor Central Management and FortiDeceptor-as-a-Service and can extend up to 128 VLANs)

6. **Κεντρικό σύστημα συλλογής και επεξεργασίας αρχείων καταγραφής**
   FAZ-VM-GB5 (Upgrade license for adding 5 GB/Day of Logs)

Προτείνεται για το υπάρχων σύστημα συλλογής δεδομένων καταγραφής συσκευών ασφαλείας FortiAnalyzer της Fortinet μια επιπλέον άδεια για 5GB log ανά ημέρα.

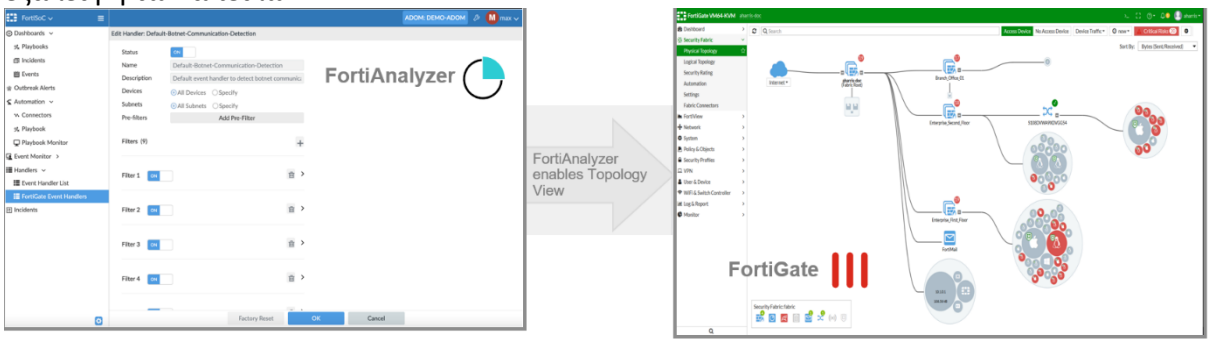
Ο FortiAnalyzer παρέχει πληροφορίες για προηγμένες απειλές μέσω της ενορχήστρωσης, του αυτοματισμού και της απόκρισης βελτιώνοντάς συνολικά την ασφάλεια του οργανισμού.



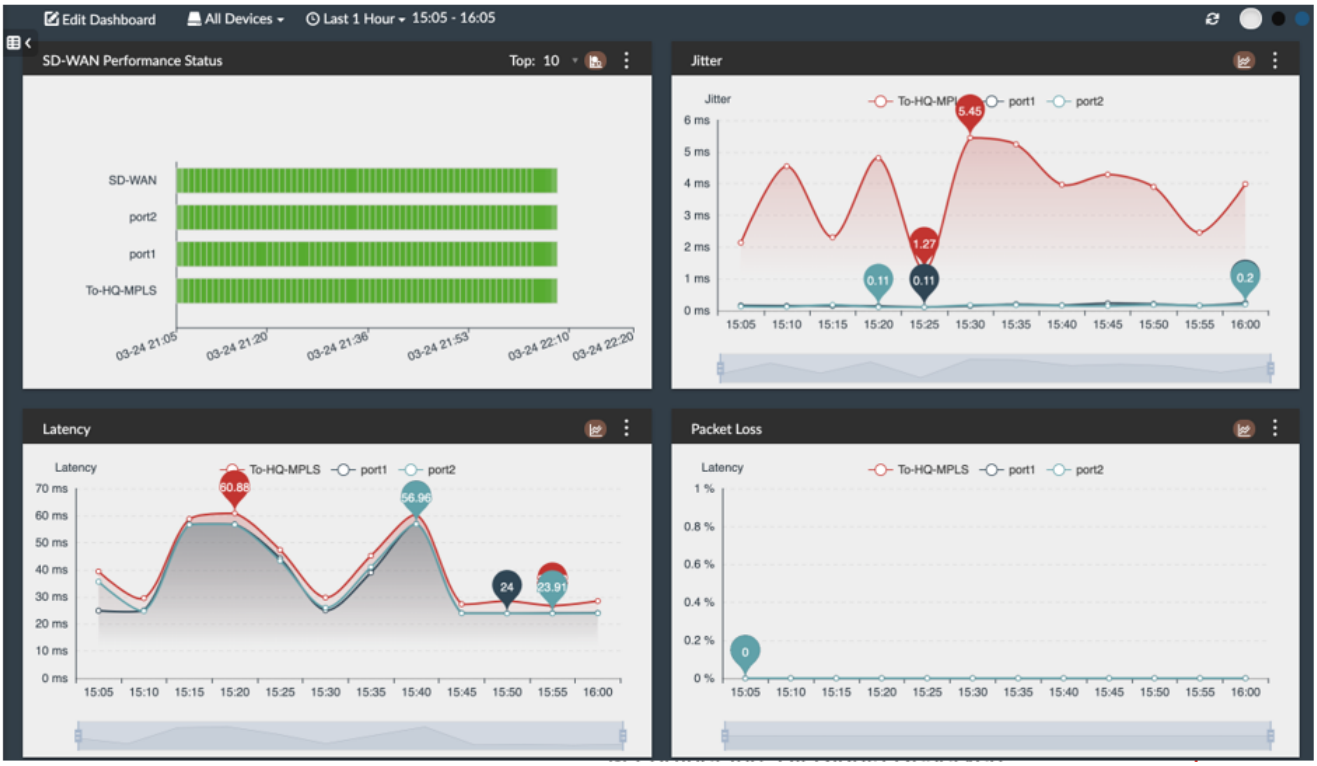
Ο FortiAnalyzer αποτελεί κεντρικό σύστημα συλλογής και επεξεργασίας αρχείων καταγραφής, ενσωματώνοντας τις λειτουργίες:

- Log management
- Event management
- Report management
- NOC services
- FortiView

Καθώς ενσωματώνεται με το security fabric της Fortinet, ο FortiAnalyzer απλοποιεί την πολυπλοκότητα της ανάλυσης και της παρακολούθησης νέων και αναδυόμενων απειλών και παρέχει ορατότητα από άκρο σε άκρο, βοηθώντας στον εντοπισμό και την εξάλειψη των απειλών.



Ο FortiAnalyzer παρέχει προσαρμοσμένες αναφορές (report) και προηγμένους χειρισμούς ροής εργασίας επιταχύνοντας την ροή των εργασιών και βοηθώντας σε ελέγχους κανονισμών και συμμόρφωσης.



Ο FortiAnalyzer παρέχει περισσότερα από 70 πρότυπα αναφορών (report template), 950 datasets, 900 διαγράμματα (charts) και 160 macros που είναι έτοιμα για χρήση, τα οποία βοηθούν τον Φορέα να επιλέξει για την σύνθεση των δικών του προσαρμοσμένων σύνθετων αναφορών, σύμφωνα με τις ανάγκες του.

Η δαπάνη της υπηρεσίας ανέρχεται στο ποσό των 49.993,90€ περιλαμβανομένου του ΦΠΑ και υπάρχει εγγεγραμμένη πίστωση στον προϋπολογισμό του έτους 2025 συνολικού ποσού 50.000,00€ στον ΚΑ 91-6266.001 με τίτλο «Αναβάθμιση backup υποδομής Δ. Χιου».

Η προμήθεια προβλέπεται να εκτελεσθεί σύμφωνα με τις διατάξεις του Ν. 4412/16.

Ο συντάξας

Μιχαήλ Φραγκούλης
ΠΕ Πληροφορικής

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΗΜΟΣ ΧΙΟΥ
Δ/ΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Μελέτη: Ενίσχυση Υποδομών Ασφαλείας

ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

Α/Α	ΠΕΡΙΓΡΑΦΗ	Ειδος Μοναδας	Ποσότητα	Τιμή Μονάδας σε Ευρώ	Σύνολο
	ΜΕΡΟΣ Α1 ΠΡΟΜΗΘΕΙΕΣ ΥΛΙΚΩΝ				
1	Tape Library IBM TS2900 ή ισοδύναμο	τεμ	1	12.750,00	12.750,00
2	Backup Server PowerEdge R360 Server ή ισοδύναμος	τεμ	1	6.600,00	6.600,00
				Μερικό Σύνολο Μέρος Α1	**19.350,00**
	ΜΕΡΟΣ Α2 ΠΡΟΜΗΘΕΙΕΣ ΛΟΓΙΣΜΙΚΩΝ-ΥΠΗΡΕΣΙΕΣ				
3	Λογισμικό Backup Veeam	τεμ	6	1.320,00	7.920,00
4	Υπηρεσίες Εγκατάστασης	τεμ	1	2.100,00	2.100,00
				Μερικό Σύνολο Μέρος Α2	**10.020,00**
	ΜΕΡΟΣ Β΄ ΠΡΟΜΗΘΕΙΑ ΛΟΓΙΣΜΙΚΩΝ FORTINET				
5	FortiAuthenticator VM	τεμ	1	1.250,00	1.250,00
6	Υπηρεσία υποστήριξης FortiAuthenticator VM	τεμ	1	1.380,00	1.380,00
7	Λογισμικό Ασφαλούς Διάταξης Δημιουργίας Υπογραφής	τεμ	1	2.440,00	2.440,00
8	Λογισμικό Cyber Deception As-A-Service	τεμ	2	2.600,00	5.200,00
9	Υπηρεσία υποστήριξης FortiDeceptor VM	τεμ	1	440,00	440,00
10	Κεντρικό σύστημα συλλογής και επεξεργασίας αρχείων καταγραφής	τεμ	1	1.330,00	1.330,00
				Μερικό Σύνολο Μέρος Β΄	**12.040,00**
				Πίστωση για ΦΠΑ 17% (ΜΕΡΟΣ Α1)	**3.289,50**
				Πίστωση για ΦΠΑ 24% (ΜΕΡΟΣ Α2)	**2.404,80**
				Ιερικό Σύνολο με ΦΠΑ ΜΕΡΟΥΣ Α1+Α2	**35.064,30**
				Πίστωση για ΦΠΑ 24% (ΜΕΡΟΣ Β΄)	**2.889,60**
				Μερικό Σύνολο με ΦΠΑ ΜΕΡΟΥΣ Β΄	**14.929,60**
				ΓΕΝΙΚΟ ΣΥΝΟΛΟ (ΜΕΡΟΣ Α΄+Β΄)	**49.993,90**

Ο Συντάξας	Ο Προϊστάμενος του τμήματος ΤΠΕ	Θεωρήθηκε Ο Προϊστάμενος της Δ/νσης Προγραμματισμού Οργάνωσης και Πληροφορικής
Μιχαήλ Φραγκούλης ΠΕ Πληροφορικής	Ιωάννης Δεληγιάννης ΤΕ 4 Μηχανολόγων Μηχ/κων	Νικόλαος Τσιπουρλής ΠΕ Αρχιτεκτόνων-Μηχανικών

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΗΜΟΣ ΧΙΟΥ
Δ/ΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Μελέτη: Ενίσχυση Υποδομών Ασφαλείας

Τιμολόγιο

ΜΕΡΟΣ Α΄

Άρθρο 1ο
Για την προμήθεια ενός Tape Library IBM TS2900 ή ισοδύναμο με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Δώδεκα χιλιάδες Επτακόσια Πενήντα Ευρώ (12.750,00)

Άρθρο 2ο
Για την προμήθεια ενός Backup Server PowerEdge R360 Server ή ισοδύναμου με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Έξι χιλιάδες Εξακόσια Ευρώ (6.600,00)

Άρθρο 3ο
Για την προμήθεια ενός πακέτου Λογισμικού Backup Veeam με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Χίλια Τριακόσια Είκοσι Ευρώ (1.320,00)

Άρθρο 4ο
Για την παροχή υπηρεσίας εγκατάστασης και παραμετροποίησης του μηχανισμού λήψης αντιγράφων ασφαλείας με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Δύο Χιλιάδες Εκατό Ευρώ (2.100,00)

ΜΕΡΟΣ Β΄

Άρθρο 1ο
Για την προμήθεια ενός πακέτου λογισμικού FortiAuthenticator VM με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Χίλια Διακόσια Πενήντα Ευρώ (1.250,00)

Άρθρο 2ο
Για την προμήθεια ενός πακέτου λογισμικού υπηρεσίας υποστήριξης FortiAuthenticator με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Χίλια Τριακόσια Ογδόντα Ευρώ (1.380,00)

Άρθρο 3ο
Για την προμήθεια ενός πακέτου λογισμικού Ασφαλούς Διάταξης Δημιουργίας Υπογραφής με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Δύο χιλιάδες Τετρακόσια Σαράντα Ευρώ (2.440,00)

Άρθρο 4ο

Για την προμήθεια ενός πακέτου λογισμικού Cyber Deception AAS με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Δύο χιλιάδες Εξακόσια Ευρώ (2.600,00)

Άρθρο 5ο
Για την προμήθεια ενός πακέτου λογισμικού FortiDeceptor VM με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Τετρακόσια Σαράντα Ευρώ (440,00)

Άρθρο 6ο
Για την προμήθεια ενός πακέτου λογισμικού αναβάθμισης του κεντρικού συστήματος συλλογής και επεξεργασίας των αρχείων καταγραφής με προδιαγραφές σύμφωνα με τη συνημμένη στη μελέτη Τεχνική Περιγραφή.
Τιμή: Χίλια Τριακόσια Τριάντα Ευρώ (1.330,00)

Ο Συντάξας	Ο Προϊστάμενος του τμήματος ΤΠΕ	Θεωρήθηκε Ο Προϊστάμενος της Δ/νσης Προγραμματισμού Οργάνωσης και Πληροφορικής
Μιχαήλ Φραγκούλης ΠΕ Πληροφορικής	Ιωάννης Δεληγιάννης ΤΕ 4 Μηχανολόγων Μηχ/κων	Νικόλαος Τσιπουρλής ΠΕ Αρχιτεκτόνων-Μηχανικών

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΗΜΟΣ ΧΙΟΥ **Μελέτη: «Ενίσχυση Υποδομών Ασφαλείας»**
Δ/ΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Π Ρ Ο Μ Ε Τ Ρ Η Σ Η

Α/Α	ΠΕΡΙΓΡΑΦΗ	Είδος Μονάδας	Ποσότητα προϋπολογισθείσα
1	Tape Library IBM TS2900 ή ισοδύναμο	τεμ.	1
2	Backup Server PowerEdge R360 Server ή ισοδύναμος	τεμ.	1
3	Λογισμικό Backup Veeam	τεμ.	6
4	Υπηρεσίες Εγκατάστασης	τεμ.	1
5	FortiAuthenticator VM	τεμ.	1
6	Υπηρεσία υποστήριξης FortiAuthenticator VM	τεμ.	1
7	Λογισμικό Ασφαλούς Διάταξης Δημιουργίας Υπογραφής	τεμ.	1
8	Λογισμικό Cyber Deception As-A-Service	τεμ.	2
9	Υπηρεσία υποστήριξης FortiDeceptor VM	τεμ.	1
10	Κεντρικό σύστημα συλλογής και επεξεργασίας αρχείων καταγραφής	τεμ.	1

Ο συντάξας

Μιχαήλ Φραγκούλης