Η Αρχιτεκτονική SPEAR

Μία Καινοτόμα Προσέγγιση Προστασίας του Έξυπνου Ενεργειακού Δικτύου

Παναγιώτης Σαρηγιαννίδης, Γεώργιος Κακαμούκας, Δημήτριος Πλιάτσιος

Παναγιώτης Ράδογλου-Γραμματίκης και Άννα Τριανταφύλλου

Τμήμα Μηχανικών Πληροφορικής & Τηλεπικοινωνιών,
Πανεπιστήμιο Δυτικής Μακεδονίας,
Καραμανλή & Λυγερής, 501000, Κοζάνη, Ελλάδα

European Union's Horizon 2020
Framework Programme for
Research and Innovation

Σύνοψη

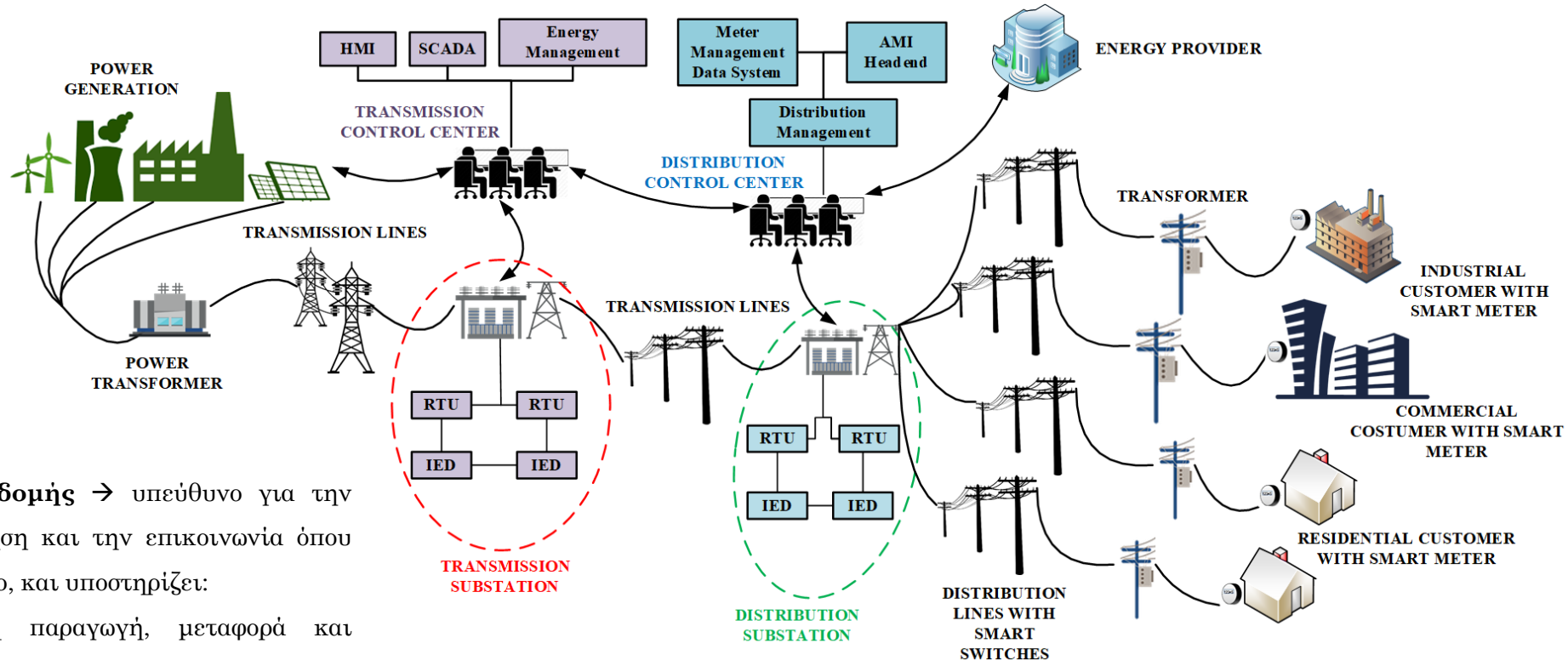
- Έξυπνο ενεργειακό δίκτυο (Electric Smart Grid)
- Προκλήσεις ασφαλείας στα ESGs
- Στόχοι του SPEARSecure and PrivatE smArt gRid (SPEAR)
- Αρχιτεκτονική SPEAR
  - System Information Event Management (SIEM)
  - SPEAR Forensic Readiness Framework (FRF)
  - Anonymous Incident Communication Channel (AICC)
- Εφαρμογές αρχιτεκτονικής SPEAR
- Καινοτομία και συνεισφορά

Έξυπνο ενεργειακό δίκτυο (Electric Smart Grid - ESG)

- Το νέο τεχνολογικό άλμα στον τομέα της ηλεκτρικής ενέργειας, παρέχοντας καλύτερη διαχείριση ενέργειας, υψηλότερη απόδοση, μεγαλύτερη αξιοπιστία καθώς και δυνατότητες αυτοΐασης.
- Χαρακτηρίζεται από αμφίδρομη ροή ηλεκτρικής ενέργειας και πληροφοριών για τη δημιουργία ενός αυτοματοποιημένου, ευρέως κατανεμημένου δικτύου διανομής ενέργειας.
- Ενσωματώνει στο δίκτυο τα πλεονεκτήματα των κατανεμημένων υπολογιστικών συστημάτων και των επικοινωνιών, για τη μεταφορά σε πραγματικό χρόνο πληροφοριών με σκοπό την εξισορρόπηση της παροχής και της ζήτησης ρεύματος.

Έξυπνο ενεργειακό δίκτυο (Electric Smart Grid - ESG)

3. Έξυπνο σύστημα Προστασίας → αξιόπιστη χρήση του δικτύου, προστασία από πιθανές βλάβες, καθώς και άλλες υπηρεσίες ασφαλείας.



1. **Έξυπνο σύστημα υποδομής** → υπεύθυνο για την ενέργεια, την πληροφόρηση και την επικοινωνία όπου βασίζεται το έξυπνο δίκτυο, και υποστηρίζει:
    1. την ανεπτυγμένη παραγωγή, μεταφορά και κατανάλωση ενέργειας,
    2. την ανεπτυγμένη μέτρηση, παρακολούθηση και διαχείριση ενέργειας και
    3. τις ανεπτυγμένες τεχνολογίες επικοινωνίας.

2. Έξυπνο σύστημα Διαχείρισης → υπηρεσίες διαχείρισης και ελέγχου της ενέργειας, με στόχους την βελτίωση της ενεργειακής απόδοσης, των χαρακτηριστικών της ζήτησης, την μείωση του κόστους και τον έλεγχο των εκπομπών.

Προκλήσεις ασφαλείας στα ESGs

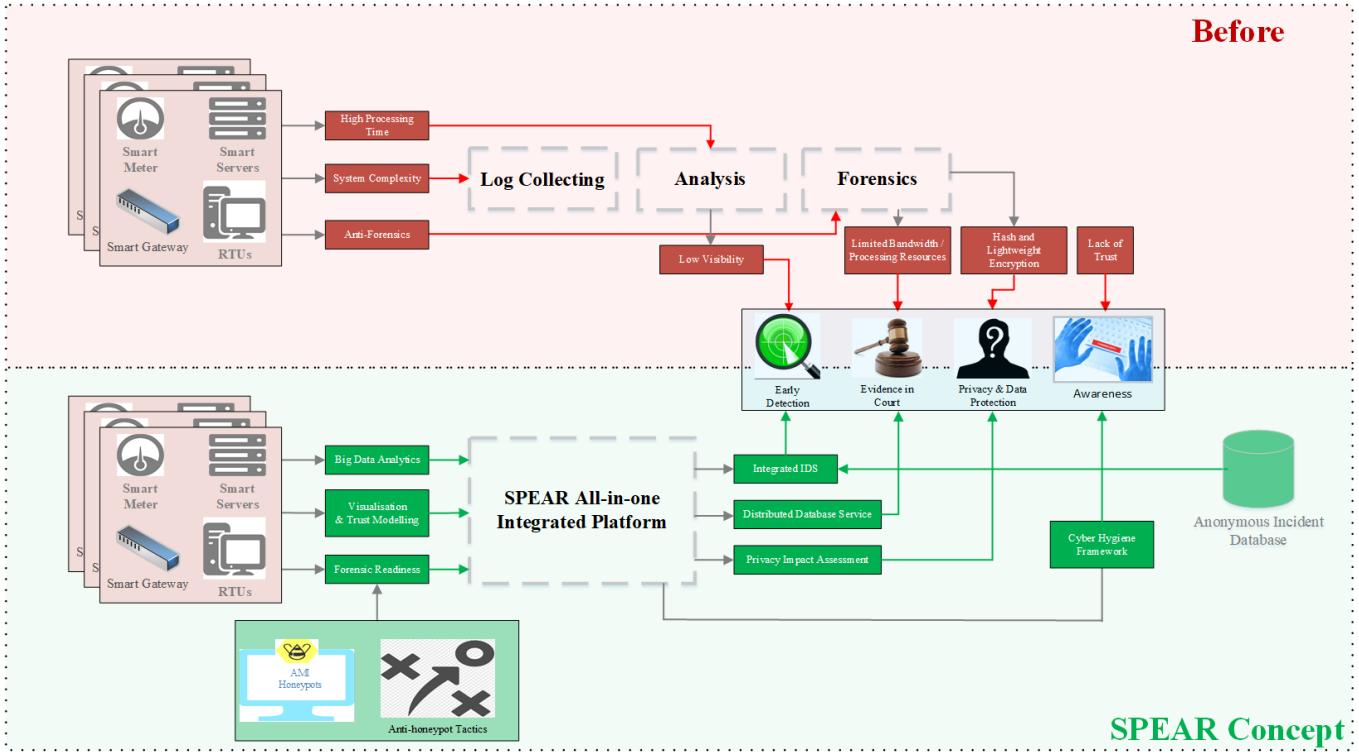
- Το έξυπνο ενεργειακό δίκτυο είναι μία από τις πιο ευάλωτες περιπτώσεις κρίσιμων υποδομών, καθώς πιθανές δυσλειτουργίες μπορούν να οδηγήσουν σε κρίσιμες καταστάσεις, όπως απώλειες ανθρώπινων ζωών, αδυναμία πρόσβασης και χειρισμού της ηλεκτρικής ενέργειας, καθώς και σοβαρές οικονομικές επιπτώσεις.
- **Τρωτά σημεία ασφαλείας των ESGs**:
  - Έξυπνες συσκευές διαχείρισης ως σημεία εισόδου επίθεσης στο δίκτυο.
  - Μη εξουσιοδοτημένη πρόσβαση στη προηγμένη υποδομή μέτρησης (Advanced Metering Infrastructure)
  - Απόκτηση πρόσβασης στο σύστημα εποπτικού ελέγχου και απόκτησης δεδομένων (Supervisory Control And Data Acquisition - SCADA)
  - Έλλειψη ασφαλείας στην ανταλλαγή μηνυμάτων των συστημάτων αυτοματισμού υποσταθμών (Substation Automation Systems)
  - Η χρήση διευθύνσεων IP στις έξυπνες συσκευές

Secure and PrivatE smArt gRid (SPEAR)

- Η ανίχνευση και η κατάλληλη έγκαιρη απόκριση σε κυβερνο-επιθέσεις, ειδικότερα από πηγές επιθέσεων με σημαντικά κίνητρα και υψηλή χρηματοδότηση, αποτελεί σημαντική πρόκληση.
- Το ερευνητικό πρόγραμμα H2020-DS-07-2016-2017 Secure and PrivatE smArt gRid (SPEAR), το οποίο συντονίζεται από το Πανεπιστήμιο Δυτικής Μακεδονίας (ΠΔΜ), στοχεύει στην υλοποίηση κατάλληλων λύσεων ασφάλειας στο έξυπνο ενεργειακό δίκτυο, εστιάζοντας σε καινοτόμες διαδικασίες ανίχνευσης και πρόληψης εισβολών.

Στόχοι του SPEAR

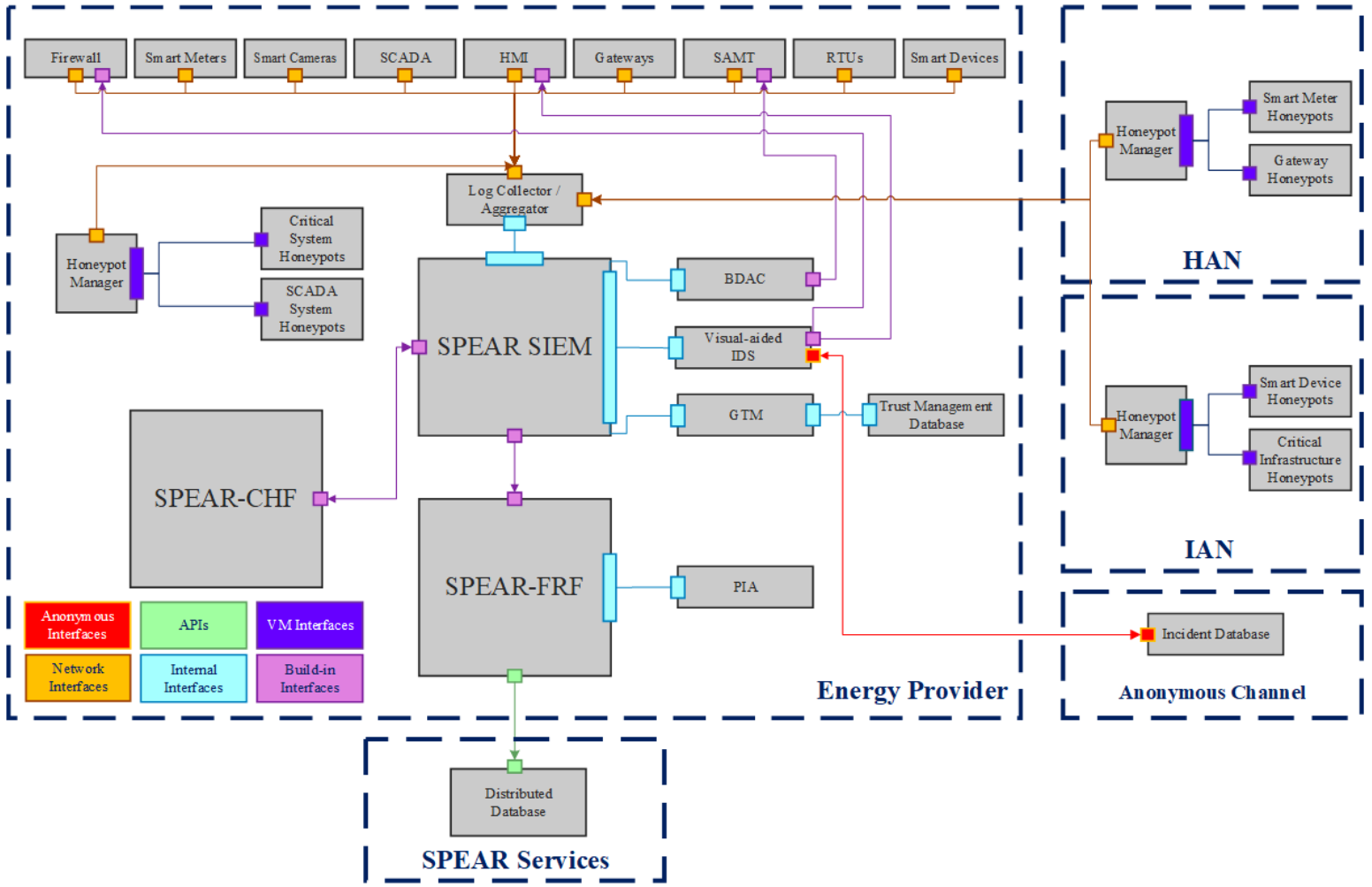
1. Η **έγκαιρη ανίχνευση εξελισσόμενων επιθέσεων ασφάλειας** → Ανάλυση δεδομένων, προηγμένη ανίχνευση ανωμαλιών με οπτικές δυνατότητες και ενσωματωμένη διαχείριση εμπιστοσύνη έξυπνων κόμβων
2. **Ανάπτυξη ενός προηγμένου πλαισίου εγκληματολογικής ετοιμότητας** → Honeypots → ίχνη επίθεσης → απαραίτητα νομικά στοιχεία στο δικαστήριο, διατηρώντας ταυτόχρονα τις προσωπικές πληροφορίες του χρήστη.
3. **Εφαρμογή ενός ανώνυμου καναλιού έξυπνου δικτύου** για τον μετριασμό της έλλειψης εμπιστοσύνης στην ανταλλαγή ευαίσθητων πληροφοριών σχετικά με περιστατικά επιθέσεων στο κυβερνοχώρο.
4. **Ενδυνάμωση της συνεργασίας** με ευρωπαϊκούς και παγκόσμιους οργανισμούς ασφάλειας, φορείς τυποποίησης, βιομηχανικές ομάδες και φορείς εκμετάλλευσης έξυπνων δικτύων.



5. **Δημιουργία ανταγωνιστικών επιχειρηματικών μοντέλων** για τη χρήση των εφαρμοσμένων εργαλείων ασφάλειας σε φορείς εκμετάλλευσης έξυπνων δικτύων και συντελεστών σε ολόκληρη την Ευρώπη.

Αρχιτεκτονική SPEAR

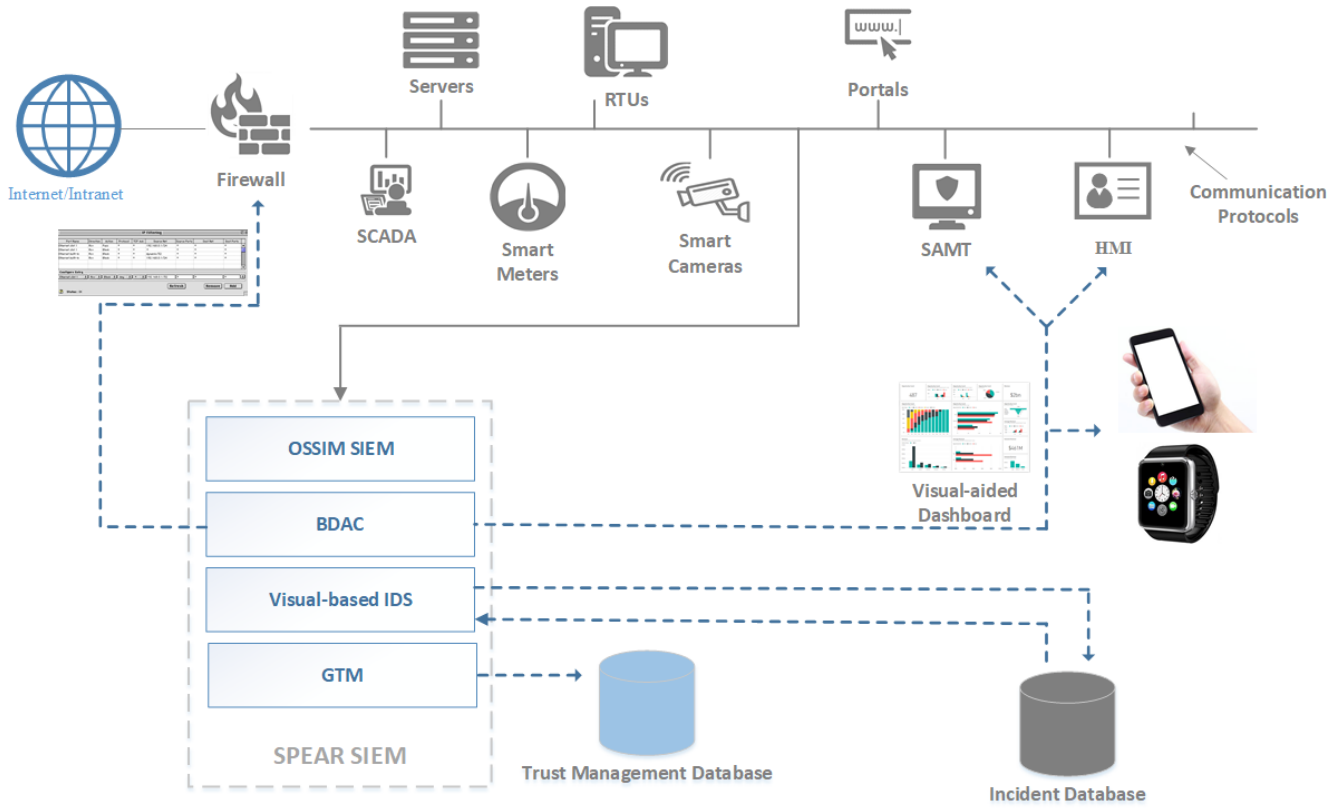
- Το πρόγραμμα SPEAR εισάγει μία αρχιτεκτονική καινοτομία τριών επιπέδων, διασφαλίζοντας τις ανάγκες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των υπηρεσιών.



System Information Event Management (SIEM)

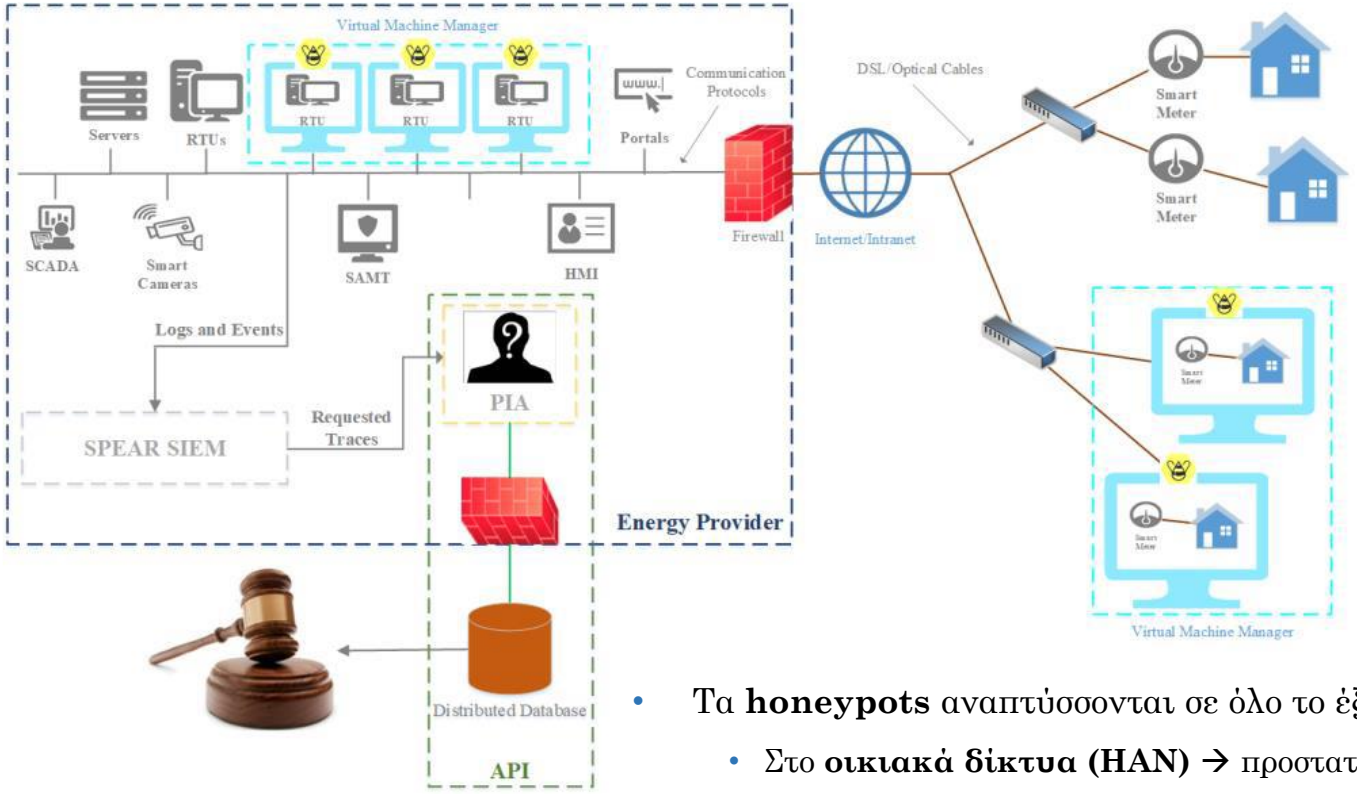
- **Σκοπός** του **πρώτου επιπέδου** της αρχιτεκτονικής → Σύστημα Διαχείρισης Πληροφοριών και Δεδομένων (System Information Event Management) - SPEAR-SIEM.
- Στοχεύει **στην ανάλυση και στη βέλτιστη διαχείριση πολλαπλών πληροφοριών**, ανιχνεύοντας πιθανά πρότυπα απειλών και ενεργοποιώντας τα κατάλληλα αντίμετρα.
- Συνεργάζεται με έναν **συλλέκτη καταγραφής ανοιχτού κώδικα** και τον **μηχανισμό OSSIM** του AlienVault → **ίχνη του συστήματος και του δικτύου** από όλα τα στοιχεία (π.χ. SCADA συστήματα, πύλες, εσωτερικοί έξυπνοι μετρητές, συσκευές και αισθητήρες και RTUs)

System Information Event Management (SIEM)



- Περιλαμβάνει:
  1. **Big Data Analytics (BDAC) →** ανίχνευση ανωμαλιών με την εφαρμογή αποφάσεων συσχετισμού και μηχανικής μάθησης στα αρχεία καταγραφής
  2. **Visual IDS**
  3. **Grid Trusted Module (GTM) →** εξοπλισμένο με αλγόριθμους διαχείρισης εμπιστοσύνης κατά την εφαρμογή φιλτραρίσματος που βασίζεται στη φήμη σε όλους τους κόμβους (συσκευές, μετρητές, διεπαφές και πύλες) που συνδέονται με το έξυπνο δίκτυο

Forensic Readiness Framework (FRF)



- Το **δεύτερο επίπεδο** → SPEAR Forensic Readiness Framework (SPEAR-FRF)
  - **Πλαίσιο επεξεργασίας δεδομένων και θέσπισης ενεργειών** για χρήση σε δικαστικές διαδικασίες
  - Καινοτόμες **διαδικασίες προσέλκυσης επιτιθέμενων**
  - Χρήση της **μεθοδολογίας OSCAR** για τη διασφάλιση της ορθής συλλογής των αναγκαίων εγκληματολογικών πληροφοριών.

- Τα **honeypots** αναπτύσσονται σε όλο το έξυπνο ενεργειακό δίκτυο προσομοιώνοντας διεπαφές.
  - Στο **οικιακά δίκτυα (HAN)** → προστατεύουν το έξυπνο δίκτυο από κλοπή ενέργειας.
  - Σε **βιομηχανικά δίκτυα (IAN)** → μιμούνται έξυπνες συσκευές όπως (έξυπνες) τουρμπίνες στον τομέα παραγωγής ενέργειας
  - Στο **κέντρο ελέγχου του φορέα παροχής ενέργειας** → για επιτιθέμενους του κυβερνοχώρου που πέτυχαν να «περάσουν» το τείχος προστασίας ή ακόμη και κακόβουλους υπαλλήλους που σκοπεύουν να βλάψουν τα έξυπνα δίκτυα από το εσωτερικό.

Anonymous Incident Communication Channel (AICC)

- Το τρίτο επίπεδο περιλαμβάνει **ένα ανώνυμο κανάλι επικοινωνίας μεταξύ παρόχων και διανομής ενέργειας στην Ευρώπη**, με στόχο την ανταλλαγή πληροφοριών για ζητήματα ασφάλειας στον κυβερνοχώρο.
- Δημιουργία και διατήρηση ενός χώρου αποθήκευσης συμβάντων ασφαλείας έξυπνων ενεργειακών δικτύων – **Repository of Incidents - SPEAR-RI**
- Μετάδοση ευαίσθητων πληροφορίων **με ανώνυμο τρόπο** χωρίς να εκτίθεται η φήμη του κάθε οργανισμού.
- Οι **τεχνικές λεπτομέρειες της επίθεσης θα είναι διαθέσιμες για όλους** να λάβουν έγκαιρα αντίμετρα.
- Ανταλλαγή δεδομένων ασφαλείας και ανάλυσης σε πραγματικό χρόνο
- Κυκλοφορία των βέλτιστων πρακτικών αντιμέτρων
- Σύγκριση διαφόρων λύσεων ασφάλειας τόσο από τεχνική όσο και επιχειρησιακή άποψη

Εφαρμογές αρχιτεκτονικής SPEAR

1. **Εφαρμογή σε μονάδα υδροηλεκτρικής ενέργειας (Hydro Power Plant)** → Ανίχνευση εξωτερικής επίθεσης στο τμήμα παραγωγής ηλεκτρικής ενέργειας.
2. **Εφαρμογή σε υποσταθμό του έξυπνου δικτύου (Substation)** → Αντιμετώπιση επιθέσεων κατά των RTUs.
3. **Εφαρμογή σε οικιακά και βιομηχανικά δίκτυα (IAN - HAN)** → Αντιμετώπιση και ανίχνευση επιθέσεων σε οικιακά και βιομηχανικά δίκτυα μέσω των εγκαταστάσεων της ΔΕΗ.
4. **Εφαρμογή σε έξυπνο σπίτι (Smart Home)** → Ανίχνευση επιθέσεων στο Έξυπνο Σπίτι του ΕΚΕΤΑ με βάση έξυπνες συσκευές του Διαδικτύου των Πραγμάτων (IoT).

Καινοτομία και συνεισφορά

- Ανάπτυξη **μιας νέας αρχιτεκτονικής τριών επιπέδων** για την προστασία των κρίσιμων υποδομών, που θα επιτρέπει την εξέλιξη των έξυπνων ενεργειακών δικτύων για την αντιμετώπιση του συνεχώς αυξανόμενου αριθμού απειλών στον κυβερνοχώρο.
- **Περιορισμός των φυσικών πόρων** και καλύτερη ισορροπία φορτίου στο δίκτυο.
- **Εξοικονόμηση** υψηλού κόστους απόκρισης, επισκευής και καθαρών ενεργειών.
- Υλοποίηση ενός **συνεργατικού πλαισίου** από εταιρίες παροχής και διανομής ηλεκτρικής ενέργειας, κατασκευαστικές επιχειρήσεις, πανεπιστήμια, ερευνητικά κέντρα και μικρομεσαίες επιχειρήσεις, **δημιουργώντας και επικυρώνοντας** παράλληλα νέες δυνατότητες στον τομέα της ασφάλειας του έξυπνου ενεργειακού δικτύου διάμεσου τεσσάρων πιλοτικών εφαρμογών.

- **Ενίσχυση εμπιστοσύνης των πολιτών** έναντι των κρίσιμων υποδομών.
- Η **ευρωπαϊκή βιομηχανία να παραμείνει ανταγωνιστική** στα συστήματα κρίσιμων υποδομών και στον χώρο της τεχνολογίας.

Σας ευχαριστώ

- Ερωτήσεις?