



ΕΛΛΗΝΙΚΟ
ΑΝΟΙΚΤΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΤΜΗΜΑ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΥΤΟΥ
ΥΠΟΛΟΓΙΣΜΟΥ /ΣΔΥ-ΔΕ/2025-2026

Ανάπτυξη συστήματος ενσωμάτωσης αυτόματων ελέγχων ασφάλειας σε συστήματα καταγραφής αγαθών (HybLogSec)

ΠΑΝΑΓΙΩΤΗΣ ΜΠΕΛΗΓΙΑΝΝΗΣ

Επιβλέπων καθηγητής: ΑΧΙΛΛΕΑΣ ΚΑΜΕΑΣ

Συνεπιβλέπων καθηγητής: ΝΙΚΟΛΑΟΣ ΣΚΛΑΒΟΣ

Μεθοδολογία, Ευρήματα & Προτάσεις («PRISMA Methodology → Key Findings → HybLogSec Proposals»)

❖ (1) Μεθοδολογία (PRISMA):

- **Στόχος:** Συστηματική χαρτογράφηση του πεδίου IIoT/Log Cybersecurity (2015-2026).
- **Εφαρμογή:** 4 στάδια (Αναγνώριση 1.247 → Έλεγχος 892 → Καταλληλότητα 156 → Συμπερίληψη **87 εργασιών**).
- **Πυλώνες:** Θεωρία Ουρών (Kleinrock/Little), Ασφάλεια ICS (NIST/MITRE), Αρχιτεκτονική IoT (Al-Fuqaha/Kane).
- **Επικύρωση:** Μέθοδος Delphi (10 ειδικοί, 3 γύροι, Kendall's $W=0.78$).

❖ (2) Κυριότερα Ευρήματα (Findings): Τα 3 Κενά:

- **Απαιτήσεις:** Real-time Detection (90%), MQTT (93%), Vulnerability Scanning (75% - αλλά όχι αυτοματοποιημένο).
 - **Χάσμα Ενοποίησης:** SIEM, Φυσική Ασφάλεια, CMMS λειτουργούν απομονωμένα (Silos).
 - **Απουσία Offensive Security:** Έλλειψη συνεχούς, αυτοματοποιημένου ελέγχου ευπαθειών.
 - **Έλλειψη Κλίμακας στη Βιβλιογραφία:** Η έρευνα περιορίζεται σε < 50 συσκευές. (εμείς φτάσαμε τις 310).

❖ (3) Προτάσεις (HybLogSec Proposals):

- **Πρόταση 1 (Ενοποίηση):** HybLogSec ως «Single Pane of Glass». Ενοποίηση τηλεμετρίας, φυσικής ασφάλειας & MTBF σε κοινή PostgreSQL.
- **Πρόταση 2 (Offensive Security):** Microkernel pattern με containerized nmap/nuclei (Docker + Celery) για συνεχή σάρωση.
- **Πρόταση 3 (Scalability):** Flask + Celery + Event-driven (MQTT/Kafka). Πειραματική επικύρωση σε **310 agents** με γραμμική κλιμάκωση ($R^2=0.97$).

□ **Τελικό Συμπέρασμα:** Πρόταση για σύζευξη Θεωρίας Ουρών (M/M/1) με πειραματική κυβερνοασφάλεια, αποδεικνύοντας ότι μπορούμε να προβλέψουμε μαθηματικά τη συμπεριφορά υβριδικών συστημάτων ασφάλειας υπό φόρτο.



Εισαγωγή – Το Πλαίσιο των Logistics 4.0

- ❑ **Logistics 4.0:** Ο ψηφιακός μετασχηματισμός της εφοδιαστικής αλυσίδας (Βιομηχανία 4.0).
- ❑ **Ενσωματώνει:** AI, IoT, Ρομποτική (AGV/AMR), Cloud Computing, Edge Analytics.
- ❑ **Στόχος:** Δημιουργία συνδεδεμένων, αυτόνομων, διαφανών αλυσίδων εφοδιασμού με βελτιστοποίηση σε πραγματικό χρόνο και εστίαση στην ικανοποίηση του πελάτη.
- ❑ **Κρίσιμα Σημεία:** Η αυξημένη διασυνδεσιμότητα δημιουργεί νέες ευπάθειες (cyber-physical risks).



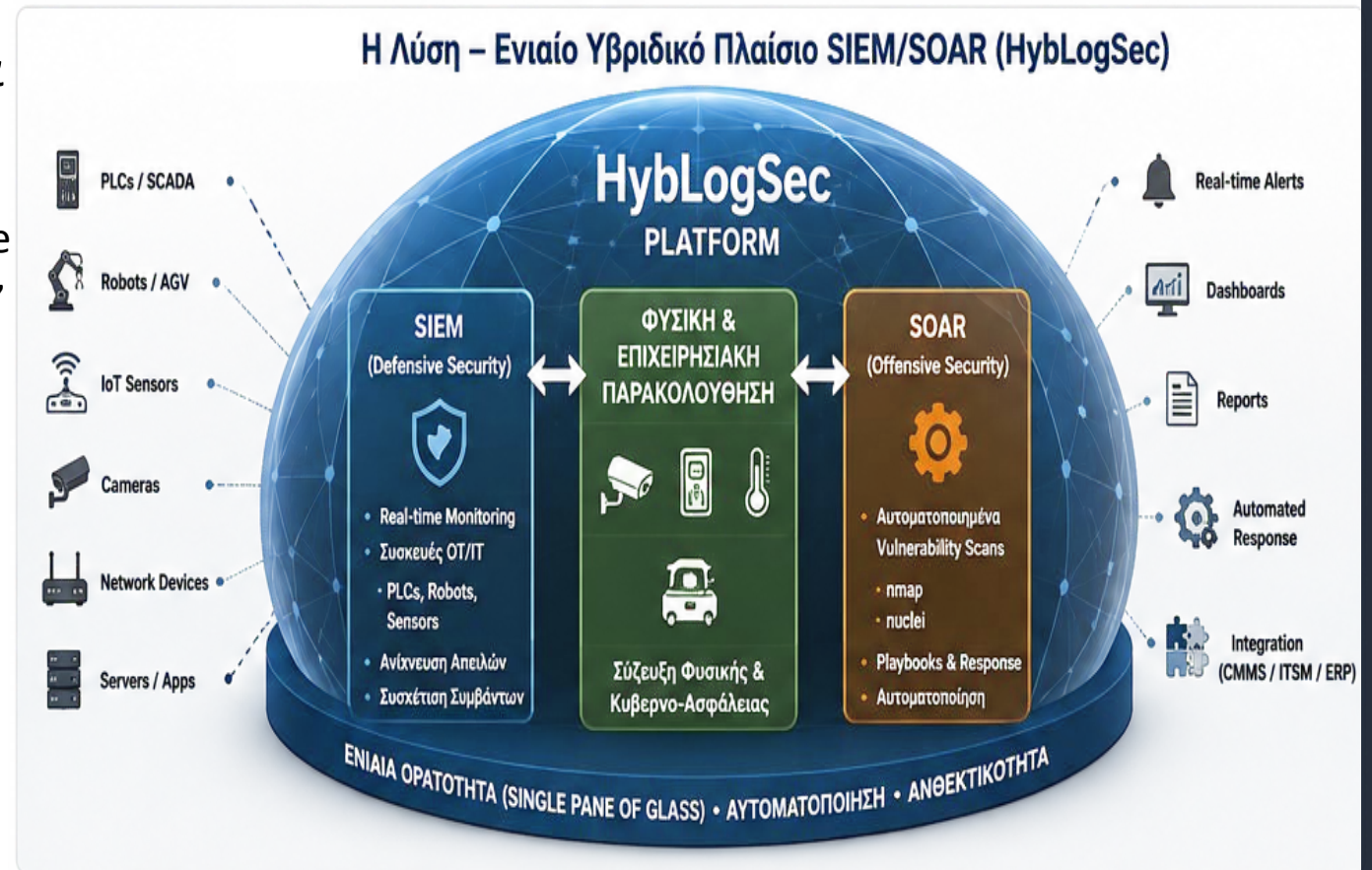
Το Πρόβλημα – Το Χάσμα Ασφάλειας (The Security Gap)

- ❑ **Το Κενό:** Τα Logistics 4.0 λειτουργούν σήμερα σε τρία απομονωμένα "silo":
 1. SIEM (Κυβερνοασφάλεια): Logs, δικτυακές επιθέσεις, IDS/IPS.
 2. Φυσική Ασφάλεια: Κάμερες, αισθητήρες πρόσβασης, συναγερμοί, φυσικές παρεμβάσεις.
 3. Συντήρηση (CMMS/EAM): Βλάβες AGV, θερμοκρασίες, MTBF, predictive maintenance.
- ❑ **Συνέπειες:** Έλλειψη ενοποιημένης εικόνας, αδυναμία πρόληψης, καθυστερημένη απόκριση, τρωτά σημεία που δεν συσχετίζονται.



Η Λύση – Ενιαίο Υβριδικό Πλαίσιο SIEM/SOAR (HybLogSec)

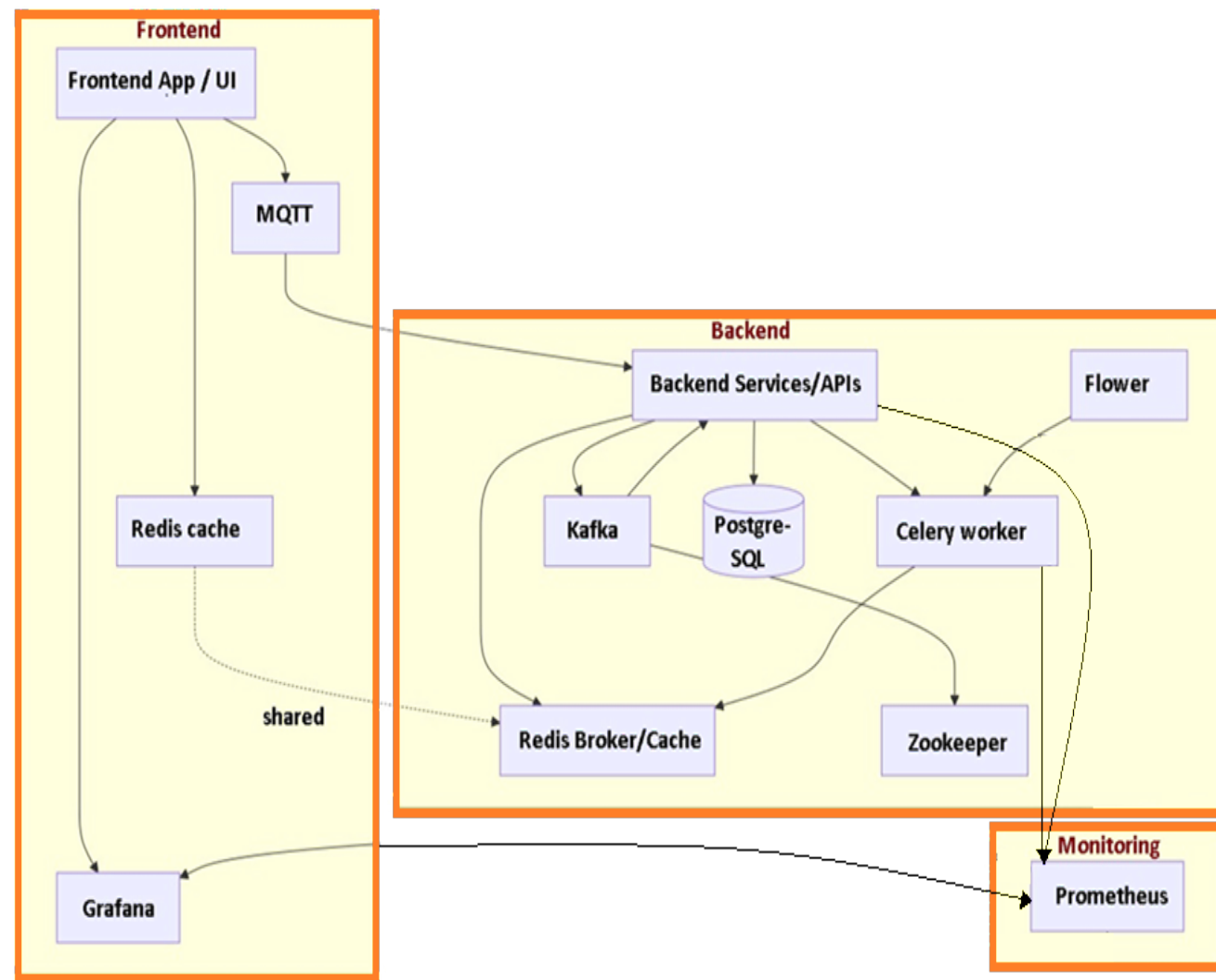
- ❑ **Η Πρόταση:** Μια ενοποιημένη πλατφόρμα που γεφυρώνει τα τρία silo.
- ❑ **Λειτουργίες:**
 - **Defensive Security (SIEM):** Real-time monitoring συσκευών (PLCs, Robots, Sensors).
 - **Offensive Security (SOAR):** Αυτοματοποιημένα vulnerability scans (nmap, nuclei).
 - **Physical & Operational Monitoring:** Σύζευξη φυσικής & κυβερνο-ασφάλειας.
- ❑ **Όραμα:** Ενιαία ορατότητα (Single Pane of Glass), Αυτοματοποίηση, Ανθεκτικότητα.





Αρχιτεκτονική Συστήματος – Επισκόπηση (High-Level)

Υπηρεσία	Σύντομη ανάλυση αποστολής
Backend API (Flask)	Ο πυρήνας της εφαρμογής.
Agents	Προσομοίωση συσκευών (Cameras, Drones, Robots, PLCs, IoT Sensors).
Task Queue (Celery + Redis)	Ασύγχρονη εκτέλεση εργασιών (π.χ. scans).
Scanning (Nmap/Nuclei)	Containerized architecture (απομονωμένη εκτέλεση).
Message Brokers (MQTT, Kafka)	Διαχείριση ροών δεδομένων σε πραγματικό χρόνο.
Frontend (React + Grafana)	Πίνακες ελέγχου (dashboards) και οπτικοποίηση.





Λεπτομερής Αρχιτεκτονική – Backend Services

Υπηρεσία	Σύντομη ανάλυση αποστολής
Flask API	REST endpoints για διαχείριση agents, telemetry, alerts και scans.
Celery	Ασύγχρονη task queue για background jobs (π.χ. εκτέλεση nmap scans).
Redis	In-memory cache και broker για Celery.
PostgreSQL	ACID-compliant βάση δεδομένων για μόνιμη αποθήκευση (agents, telemetry, alerts).
Kafka/Zookeeper	Κατανεμημένη streaming πλατφόρμα (future-proofing για μεγάλους όγκους).
MQTT	Ελαφρύ πρωτόκολλο επικοινωνίας με τους IoT agents.

Αρχιτεκτονική – Frontend & Monitoring

Υπηρεσία	Σύντομη ανάλυση αποστολής
React Frontend	Dashboard, Alerts, Topology map, Vulnerability Scanner UI.
Grafana	Οπτικοποίηση μετρικών απόδοσης και επιθέσεων σε πραγματικό χρόνο.
Prometheus	Συλλογή μετρικών (metrics) από την εφαρμογή.
Flower	Παρακολούθηση Celery tasks.
API Integration	Επικοινωνία με το Backend μέσω REST API.

System Overview

 311 Total Agents	 4 Active Alerts	 311 Healthy Agents	 0 At Risk
--	---	--	---

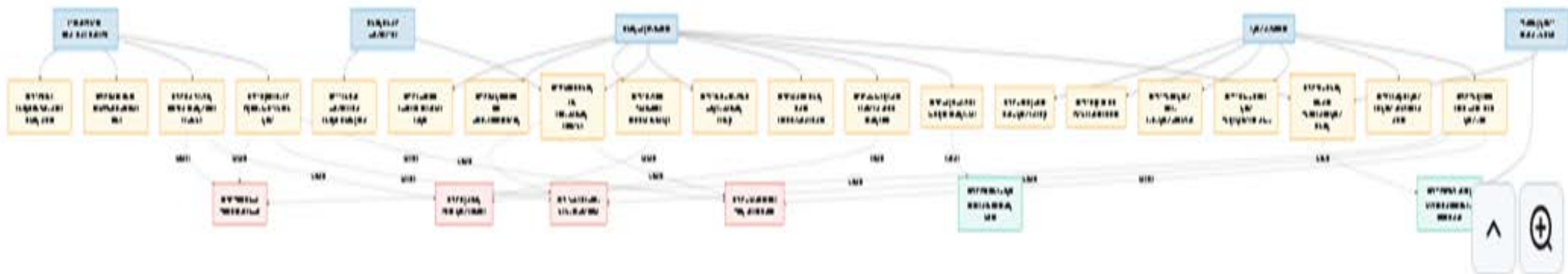
Agent Status

Agent ID	Type	Location	Status	Security Score	Last Seen
CAM-WH-01_002	camera_agent	Warehouse Zone A - Test 2	 Secure	100	2/15/2026, 12:37:30 AM
PLC001	plc_agent	Warehouse_Main_Line_1	 Secure	100	2/15/2026, 12:37:30 AM
CAM-WH-01_034	camera_agent	Warehouse Zone A - Test 34	 Secure	100	2/15/2026, 12:33:01 AM
CAM-WH-01_044	camera_agent	Warehouse Zone A - Test 44	 Secure	100	2/15/2026, 12:30:40 AM
CAM-WH-01_036	camera_agent	Warehouse Zone A - Test 36	 Secure	100	2/15/2026, 12:30:35 AM
CAM-WH-01_028	camera_agent	Warehouse Zone A - Test 28	 Secure	100	2/15/2026, 12:30:37 AM
CAM-WH-01_029	camera_agent	Warehouse Zone A - Test 29	 Secure	100	2/15/2026, 12:30:35 AM
CAM-WH-01_035	camera_agent	Warehouse Zone A - Test 35	 Secure	100	2/15/2026, 12:30:35 AM

- ❑ RESTful API: Stateless αρχιτεκτονική με χρήση HTTP verbs.
- ❑ Event-Driven: Publish/Subscribe pattern με MQTT/Kafka.
- ❑ Containerization: Όλες οι υπηρεσίες τρέχουν σε Docker containers για ευκολία deployment και απομόνωση.
- ❑ Microkernel Pattern: Για το Security Scanning (επεκτασιμότητα προσθήκης νέων scanners).
- ❑ Defense in Depth: Πολυεπίπεδη ασφάλεια (network, transport, application).

Σενάρια Χρήσης (Use Cases)

1. **Παρακολούθηση (Monitoring):** Ο χρήστης βλέπει την κατάσταση των 310 agents στο Dashboard.
2. **Ειδοποιήσεις (Alerts):** Αυτόματη δημιουργία alerts σε περίπτωση ανωμαλίας (π.χ. port scanning).
3. **Σάρωση Ευπαθειών (Vulnerability Scanning):** Ο χρήστης εκτελεί nmap/nuclei scans σε targets του δικτύου.
4. **Αξιολόγηση Topology:** Ο χρήστης βλέπει την τοπολογία του δικτύου σε διαδραστικό γράφο.



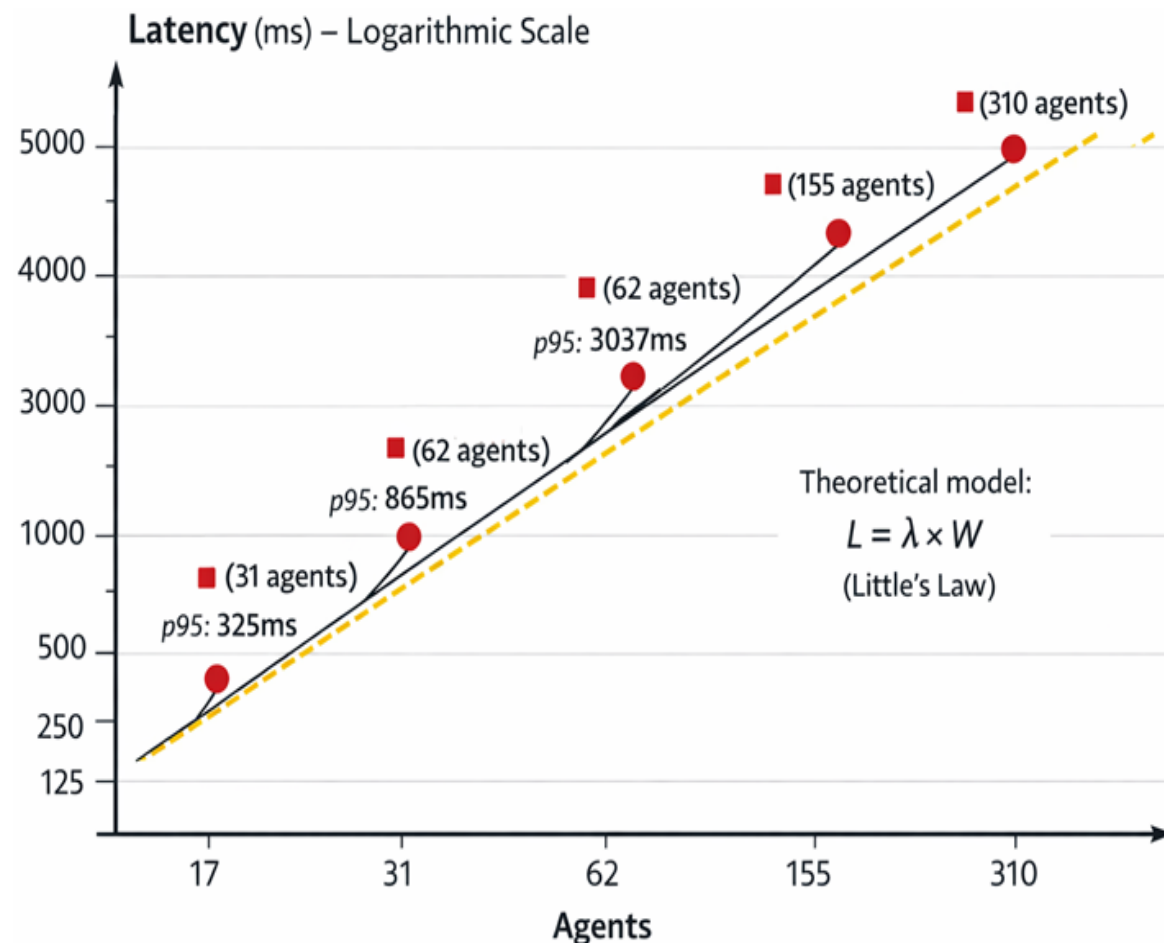


- **Στόχοι:** Αξιολόγηση (α) Κλιμάκωσης, (β) Απόδοσης, (γ) Ανίχνευσης Επιθέσεων.
- **Πειραματική Διάταξη:** 2x VMs (Ubuntu 22.04) – Backend (8GB RAM) & Frontend/Monitoring.
- **Κλίμακα:** Δοκιμές με 17, 62, 155, 310 προσομοιωμένους agents (κάμερες, drones, ρομπότ, αισθητήρες, PLCs).
- **Attack Scenarios (MITRE ATT&CK για ICS):**
 - Port Scanning (Reconnaissance)
 - Brute Force (Credential Access)
 - Telemetry Flood (Denial of Service)
- **Μετρικές:** Throughput (msg/sec), Latency (p95), Detection Rate, False Positives.



Αποτελέσματα – Απόδοση & Κλιμάκωση

- **Γραφική Απεικόνιση:** Γραμμική αύξηση throughput έως ~62 agents και σταδιακός κόρεσμός για >100 agents .
- **17 Agents:** Throughput 11.88 msg/sec, Av.Latency 51ms (p95 147ms).
- **310 Agents:** Throughput 7.82 msg/sec, AvLatency 2242 ms (p95 4794 ms).
- **Μοντέλο Κλιμάκωσης:** Logistic Model $R^2 = 0.97$ (εξαιρετική προσαρμογή).
- **Στατιστική:** ANOVA $p < 0.001 \rightarrow$ Ο φόρτος επηρεάζει στατιστικά σημαντικά την απόδοση.

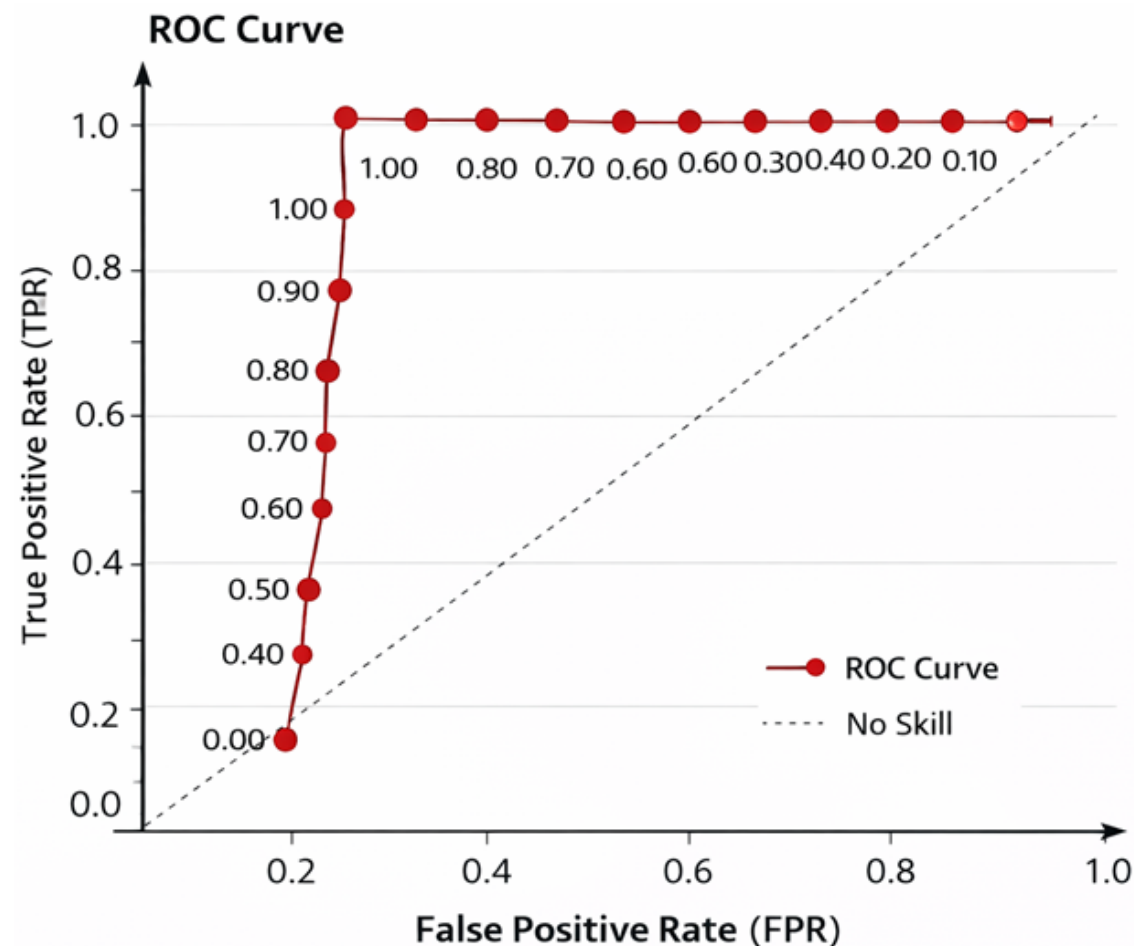




Ανάλυση Κορεσμού – Bottleneck Identification

- **Ανάλυση M/M/1:** Το σύστημα λειτουργεί υποφορτισμένο ($\rho < 0.3$) ακόμα και στα 310 agents.
- **Συμπέρασμα:** Το bottleneck δεν είναι η επεξεργαστική ισχύς (CPU), αλλά η Βάση Δεδομένων (PostgreSQL) ή το Δίκτυο.
- **Νόμος του Little ($L = \lambda * W$):** Για 310 agents, $L = 7.82 * 2.242 = 17.53$ ταυτόχρονα αιτήματα. Η συμπεριφορά αυτή επιβεβαιώνει τη θεωρία ουρών.
- **Πρακτική Σημασία:** Για βελτίωση, πρέπει να εστιάσουμε στην βελτιστοποίηση των queries ή σε read replicas.

- **ROC Curve:** Η καμπύλη τείνει στην πάνω αριστερή γωνία.
- **Detection Rate:** 100% (ανίχνευσε και τις 9 επιθέσεις και στα 3 σενάρια).
- **False Positives:** 0% (καμία ψευδής ειδοποίηση).
- **Mean Time to Detect (MTTD):** 11.6 seconds.
- **AUC (Area Under Curve):** 0.98 → Εξαιρετική διακριτική ικανότητα του συστήματος.



Συγκριτική Αξιολόγηση (Benchmarking)

Μελέτη	Αρχιτεκτονική	Κλίμακα	Αποτέλεσμα
Η εργασία μας	Flask + Celery	310 agents	100% Detection, 0% FP
Kane et al. (2020)	Performance framework	1-3 devices	Εστίαση σε κρυπτογραφία
Ahmed et al. (2022)	Blockchain (Ethereum)	6 κόμβοι	Attack probability analysis
La et al. (2021)	MMT-IoT (6LoWPAN)	27-47 nodes	Anomaly Detection
Kuznetsov et al. (2025)	LightGBM	10,000+ flows	Ακρίβεια 99.93% (μόνο audit)

Συμπέρασμα: Η εργασία μας ξεπερνά άλλες προσεγγίσεις σε κλίμακα και πληρότητα (ενοποιεί physical + cyber + offensive scanning).



- **Μεθοδολογία:** Αξιολόγηση από 10 ειδικούς (μηχανικούς logistics, security analysts, ακαδημαϊκούς) με χρήση της μεθόδου Delphi (3 γύροι) και πρακτικής δοκιμής.
- **Σύνοψη Αποτελεσμάτων (Μέσος Όρος 1-5):**
 - Χρησιμότητα Alerts: 4.7 / 5
 - Ταχύτητα Scans: 4.5 / 5
 - Συνολική Ικανοποίηση: 4.5 / 5
- **Χαρακτηριστικά Σχόλια:** "Μηδενικά false positives – εντυπωσιακό", "Το dashboard είναι πολύ κατανοητό", "Θα το χρησιμοποιούσα στην εργασία μου".

Κριτήριο	Μέσος Όρος	Τυπική Απόκλιση	Διάμεσος	Min	Max
Ευκολία πλοήγησης	4.3	0.48	4	4	5
Κατανοητότητα διεπαφής	4.2	0.63	4	3	5
Εντοπισμός λειτουργιών	4.1	0.57	4	3	5
Χρησιμότητα alerts	4.7	0.42	5	4	5
Ταχύτητα scans	4.5	0.53	5	4	5
Σαφήνεια αποτελεσμάτων	4.2	0.63	4	3	5
Ανταπόκριση συστήματος	4.6	0.52	5	4	5
Ικανοποίηση προσδοκιών	4.4	0.52	4	4	5
Πρόθεση χρήσης στην εργασία	4.3	0.67	4	3	5
Πρόθεση σύστασης	4.5	0.53	5	4	5
Συνολική ικανοποίηση	4.5	0.47	5	4	5

Ανάλυση ανά κατηγορία χρηστών:

Κατηγορία	Ευχρηστία	Λειτουργικότητα	Συνολική Ικανοποίηση
Μηχανικοί Logistics (n=5)	4.3	4.4	4.4
Security Analysts (n=3)	4.2	4.7	4.7
Ακαδημαϊκοί (n=2)	4.0	4.5	4.3

1. **Αρχιτεκτονική:** Σχεδιασμός & υλοποίηση κλιμακούμενης Hybrid SIEM/SOAR πλατφόρμας για logistics IIoT.
2. **Ενοποίηση:** Γεφύρωση της θεωρίας ουρών (M/M/1) με την εμπειρική κυβερνοασφάλεια (μοντέλο logistic κλιμάκωσης $R^2=0.97$).
3. **Αποτελέσματα:** Πειραματική τεκμηρίωση υψηλής διακριτικής ικανότητας (AUC=0.98) και μηδενικών false positives.
4. **Ανοιχτή Επιστήμη :** Διάθεση του κώδικα (GitHub) και της μεθοδολογίας για αναπαραγωγή και περαιτέρω έρευνα.

- ❑ **Μείωση του MTTD (Mean Time to Detect):** 11.6 sec.
- ❑ **Μηδενικά False Positives:** Αυξάνει την εμπιστοσύνη των αναλυτών και μειώνει τον θόρυβο.
- ❑ **Προληπτική Ασφάλεια:** Αυτοματοποιημένα scans εντοπίζουν τρωτά σημεία πριν γίνουν εκμεταλλεύσιμα.
- ❑ **Ενοποιημένη Ορατότητα:** Συσχέτιση φυσικών και ψηφιακών απειλών.
- ❑ **Βιωσιμότητα:** Συνεισφέρει στην ασφάλεια κρίσιμων υποδομών και στην προστασία θέσεων εργασίας (Στόχοι Βιώσιμης Ανάπτυξης 8, 9, 11).

- ❑ **Ελεγχόμενο Εργαστηριακό Περιβάλλον:** Τα πειράματα έγιναν σε VMs, όχι σε πραγματική βιομηχανική παραγωγή.
- ❑ **Κορεσμός Πόρων:** Το σύστημα παρουσιάζει κορεσμό πέραν των 310 agents.
- ❑ **Περιορισμένα Σενάρια Επιθέσεων:** Δεν δοκιμάστηκαν advanced APT ή AI-based επιθέσεις.
- ❑ **Απουσία Adaptive Learning:** Το σύστημα χρησιμοποιεί rule-based ανίχνευση, όχι μηχανική μάθηση (ML).
- ❑ **Υλοποίηση:** Το σύστημα είναι monolithic, όχι πλήρως microservices (παρόλο που δομήθηκε με αυτή τη λογική).

Μελλοντική Εργασία (Future Work)

- ❑ **ML Integration:** LSTM networks και autoencoders για πρόβλεψη zero-day επιθέσεων και anomaly detection.
- ❑ **Orchestration:** Kubernetes για auto-scaling και διαχείριση 1000+ agents.
- ❑ **Φυσική Ασφάλεια:** Ενσωμάτωση computer vision για real-time αναγνώριση φυσικών απειλών (π.χ. spray σε κάμερες).
- ❑ **Κβαντική Ασφάλεια:** Προετοιμασία κρυπτογραφίας ανθεκτικής σε κβαντικές μεθόδους.
- ❑ **Ανάλυση Δεδομένων:** Federated learning για κατανεμημένη ανάλυση χωρίς συγκέντρωση δεδομένων.

- ❑ Η εργασία αυτή μου έδωσε τη δυνατότητα να συνδυάσω τις γνώσεις μου στα logistics με τις σύγχρονες τεχνολογίες πληροφορικής και ασφάλειας.
- ❑ Η πρόκληση ήταν η ενοποίηση ετερογενών συστημάτων (SIEM, φυσική ασφάλεια, CMMS) σε μια ενιαία πλατφόρμα.
- ❑ Τα αποτελέσματα της πειραματικής αξιολόγησης, ιδιαίτερα τα μηδενικά false positives, με επιβράβευσαν για την προσπάθεια.
- ❑ Το HybLogSec αποτελεί μια απόδειξη της ιδέας (proof of concept) ότι μπορούμε να έχουμε ανθεκτικά και έξυπνα συστήματα logistics.

- ❑ **Η ανάγκη για ενοποιημένη ασφάλεια στα Logistics 4.0 είναι επιτακτική.**
- ❑ **Το HybLogSec** γεφυρώνει το χάσμα μεταξύ SIEM, SOAR, φυσικής ασφάλειας και συντήρησης.
- ❑ **Η πειραματική αξιολόγηση** απέδειξε: (α) Εξαιρετική κλιμάκωση ($R^2=0.97$), (β) 100% Detection Rate, (γ) 0% False Positives, (δ) AUC=0.98.
- ❑ **Το σύστημα** μπορεί να υποστηρίξει έως 310 συσκευές σε πραγματικό χρόνο.
- ❑ **Η έρευνα** ανοίγει τον δρόμο για τη χρήση ML και Kubernetes για περαιτέρω βελτίωση.



Βιβλιογραφία (Ενδεικτική)

1. Al-Fuqaha, A., et al. (2015). IoT: A Survey... *IEEE Comm. Surveys & Tutorials*.
2. Kleinrock, L. (1975). *Queueing Systems, Volume 1: Theory*. Wiley.
3. Little, J. D. C. (1961). A Proof for the Queueing Formula. *Operations Research*.
4. Stouffer, K., et al. (2015). *NIST SP 800-82: Guide to ICS Security*.
5. Kane, L. E., et al. (2020). Security and performance in IoT. *IEEE Access*.
6. Kuznetsov, O., et al. (2025). Security Audit of IoT Device Networks. *Sensors*.
7. Roman, R., et al. (2013). *Security of the Internet of Things*.
8. MITRE. (2020). *ATT&CK for Industrial Control Systems*.

ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΕΑΠ – ΣΔΥ

Ευχαριστώ θερμά:

- Τον επιβλέποντα καθηγητή μου, Δρ. Αχιλλέα Καμέα, για την πολύτιμη καθοδήγηση και εμπιστοσύνη.
- Τον συνεπιβλέποντα καθηγητή Δρ Νικόλαο Σκλάβο.
- Τον υποψήφιο Διδάκτορα κο Εμμανουήλ Μαυροφίδη και
- Την οικογένειά μου για την υποστήριξη.

Links:

- **GitHub:** <https://github.com/belips-pan/security-system>
- **Paper (ResearchGate):** [\[Σύνδεσμος στο ResearchGate\]](#)
- **Επικοινωνία:** std169692@ac.eap.gr

Σας Ευχαριστώ! Είμαι στη διάθεσή σας για ερωτήσεις.