METAMIND INNOVATIONS P.C.

# Minds

## Εργαλεία Τεχνητής Νοημοσύνης για Ανίχνευση Εισβολών, Αξιολόγηση Ευπαθειών, Honeypots και Κατανεμημένα Συστήματα Συνεργασίας

**Καθ. Παναγιώτης Σαρηγιαννίδης, Co-Founder, MetaMind Innovations P.C.**

psarigiannidis@metamind.gr

https://metamind.gr/

ΤΟ ΠΡΟΒΛΗΜΑ

# Σκιώδης χρήση ΤΝ. Φορετές/Περιφερειακές συσκευές σε κίνδυνο. Ανθρώπινος Παράγοντας.

Απειλή #1

## Shadow AI (Σκιώδης χρήση ΤΝ)


- **Διαρροή δεδομένων**
  Παραβίαση GDPR/NIS2 με σκιώδη χρήση ΤΝ
- **Μηδενική εποπτεία**
  Έλλειψη πολιτικών (Ασφαλείας & ΤΝ)

Απειλή #2

## Συνδεσιμότητα & Φορητές Συσκευές

- **Έλλειψη πρωτοκόλλων προστασίας**
  Εκτεθειμένα σε κυβερνοεπιθέσεις
- **Αδύναμη εποπτεία από πλατφόρμες SOC**
  Δεν εξασφαλίζεται η εποπτεία τους από εργαλεία SIEM/SOC – έλλειψη εφαρμογής πρακτικών security by design (ασφάλεια από τον σχεδιασμό)

Απειλή #3

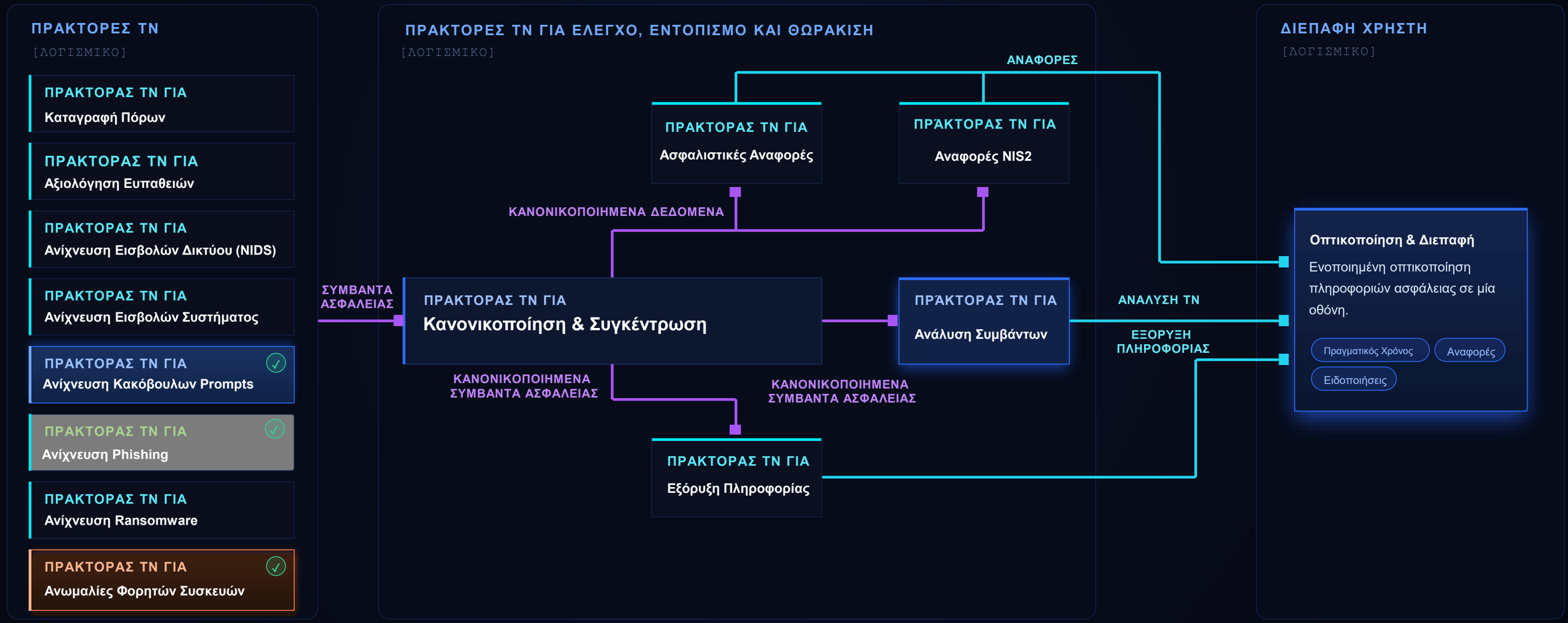
## Ανθρώπινος Παράγοντας


- **Ηλεκτρονικές Απάτες - Phishing**
  Κύρια πύλη εισόδου για ransomware.
- **Επιθέσεις Μηδενικής Ημέρας**
  Τα συμβατικά αντίμετρα αδυνατούν να τις αντιμετωπίσουν.

ΑΡΧΙΤΕΚΤΟΝΙΚΗ

# Πολλαπλοί Πράκτορες ΤΝ. Ενιαίο Σύστημα Θωράκισης.

Minds
https://metamind.gr/

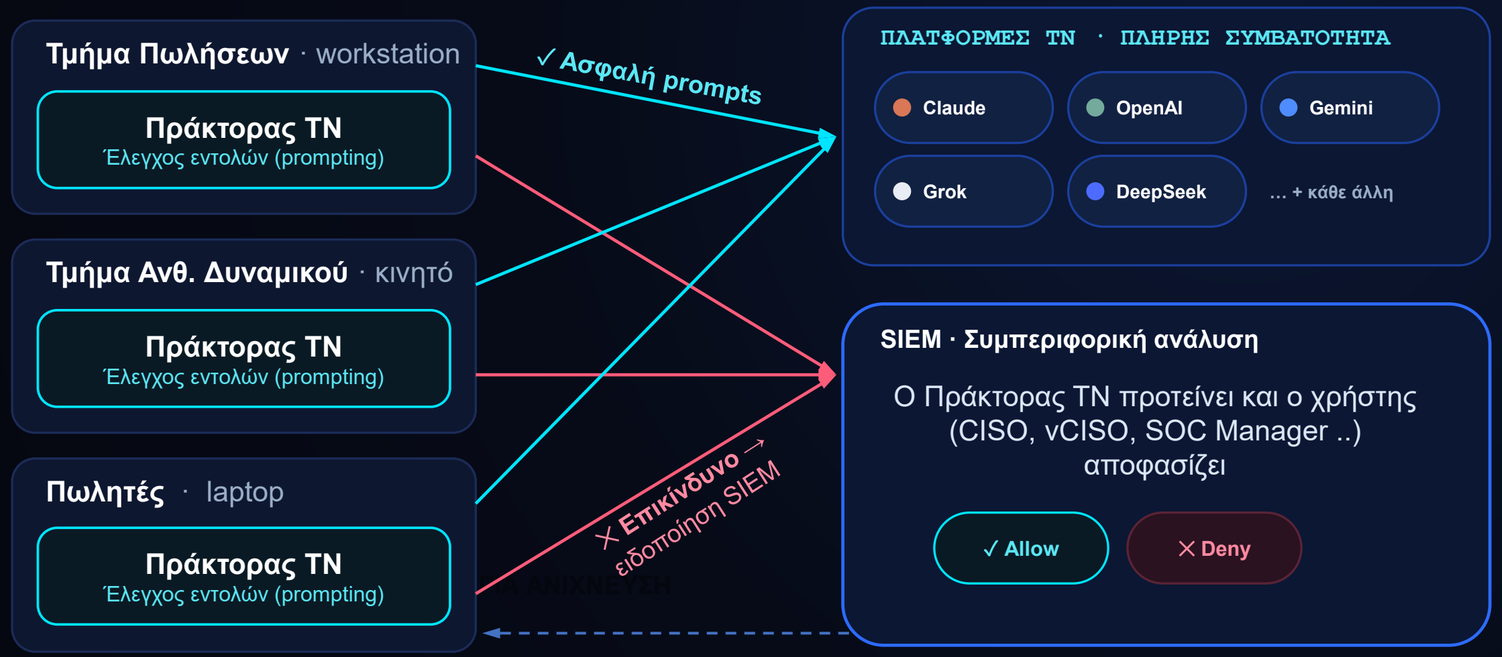


Σκιώδης χρήση ΤΝ

# Πράκτορας ΤΝ για την αντιμετώπιση σκιώδους χρήσης ΤΝ

Minds
https://metamind.gr/

Θωρακίζει έναντι Prompt Injection (εισαγωγή κακόβουλων εντολών), Jailbreaks (παράκαμψη περιορισμών) και ακούσιες διαρροές δεδομένων.




**Παρακολουθεί σε πραγματικό χρόνο**

- Επικοινωνία από & προς εργαλεία ΤΝ

**ΠΑΡΑΓΕΙ**

- Συμβάντα ασφάλειας
- Τεχνικές MITRE ATLAS
- Ενέργειες απόκρισης
- Προτεινόμενο πλάνο
- Σοβαρότητα & βεβαιότητα

Φορετές συσκευές και περιμετρικό δίκτυο

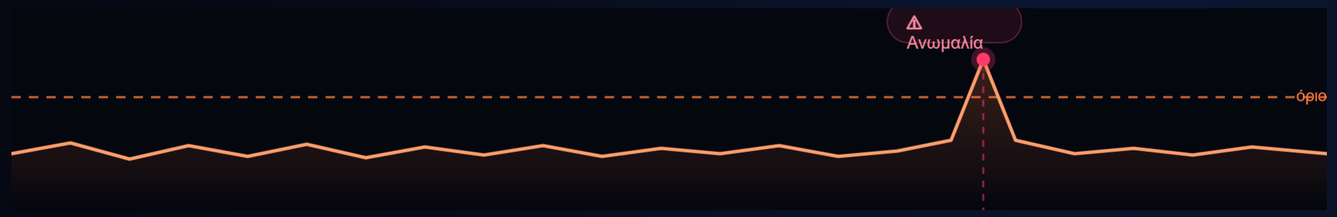
# Πράκτορας ΤΝ για Φορετές & Περιφερειακές Συσκευές

Minds
https://metamind.gr/

Εποπτεία φορετών συσκευών & περιφερειακού δικτύου σε πραγματικό χρόνο.

Υλοποίηση του security by design με ενσωμάτωση του Πράκτορα ΤΝ στο firmware

Ροή Επεξεργασίας




ΕΛΕΓΧΟΣ & ΕΝΤΟΠΙΣΜΟΣ

ΑΠΟΜΟΝΩΣΗ & ΑΠΟΚΑΤΑΣΤΑΣΗ

ΕΝΗΜΕΡΩΣΗ & ΑΞΙΟΛΟΓΗΣΗ

ΠΡΑΚΤΟΡΕΣ ΤΝ ΓΙΑ ΑΝΙΧΝΕΥΣΗ

**ΛΑΜΒΑΝΕΙ**

- Τηλεμετρία φορητών συσκευών

**ΠΑΡΑΓΕΙ**

- Συμβάντα ασφάλειας
- Προφίλ συμπεριφοράς
- Τεχνικές MITRE ATT&CK

# Πράκτορας ΤΝ Για Phishing & Ransomware

Minds
https://metamind.gr/

Εποπτεία εταιρικών email σε πραγματικό χρόνο. Εντοπισμός απειλών Ransomware. Μείωση των False Alarms (άσκοποι συναγερμοί) με την χρήση ψηφιακών παγίδων ασφαλείας (VM honeynets)


**ΛΑΜΒΑΝΕΙ**

- Εισερχόμενα ανώνυμα στοιχεία emails: μοτίβα, υπογραφές και αποτύπωμα

**ΠΑΡΑΓΕΙ**

- Συμβάντα ασφάλειας
- Τεχνικές MITRE ATT&CK
- Ενέργειες απόκρισης (διαγραφή / καραντίνα)

ΑΝΤΙΚΤΥΠΟ & ΟΦΕΛΗ

# Αντίκτυπο & Οφέλη

Minds
https://metamind.gr/

**-30%**

**False alarms (άσκοποι συναγερμοί)**

με χρήση παγίδων εισβολών

**100%**

**Υποστήριξη στα ελληνικά**

και σε κάθε άλλη γλώσσα προτίμησης

**NIS2 · DORA · Insurance**

**Αυτοματοποιημένες αναφορές**

100% συμμόρφωση με εταιρικές πολιτικές

## Οφέλη

- **Προστασία από κακόβουλη χρήση εργαλείων ΤΝ**
- **Ανάπτυξη πολιτικών ασφάλειας για εταιρείες και οργανισμούς**
- **Ευθυγράμμιση με πολιτικές NIS2 και ΤΝ**
- **Ευθυγράμμιση με κανόνες SIEM/SOC και τις επιχειρησιακές απαιτήσεις**

Minds

## ΕΥΧΑΡΙΣΤΟΥΜΕ

METAMIND INNOVATIONS P.C.

Καθ. Παναγιώτης Σαρηγιαννίδης, Co-Founder MetaMind Innovations P.C.

psarigiannidis@metamind.gr

https://metamind.gr/