Κυβερνοασφάλεια και Τεχνητή Νοημοσύνη: Ευκαιρίες και Προκλήσεις για τις Μικρομεσαίες Επιχειρήσεις

Δρ. Λέανδρος Μαγλαράς

Εφαρμογές της Τεχνητής Νοημοσύνης στις Μικρομεσαίες Επιχειρήσεις

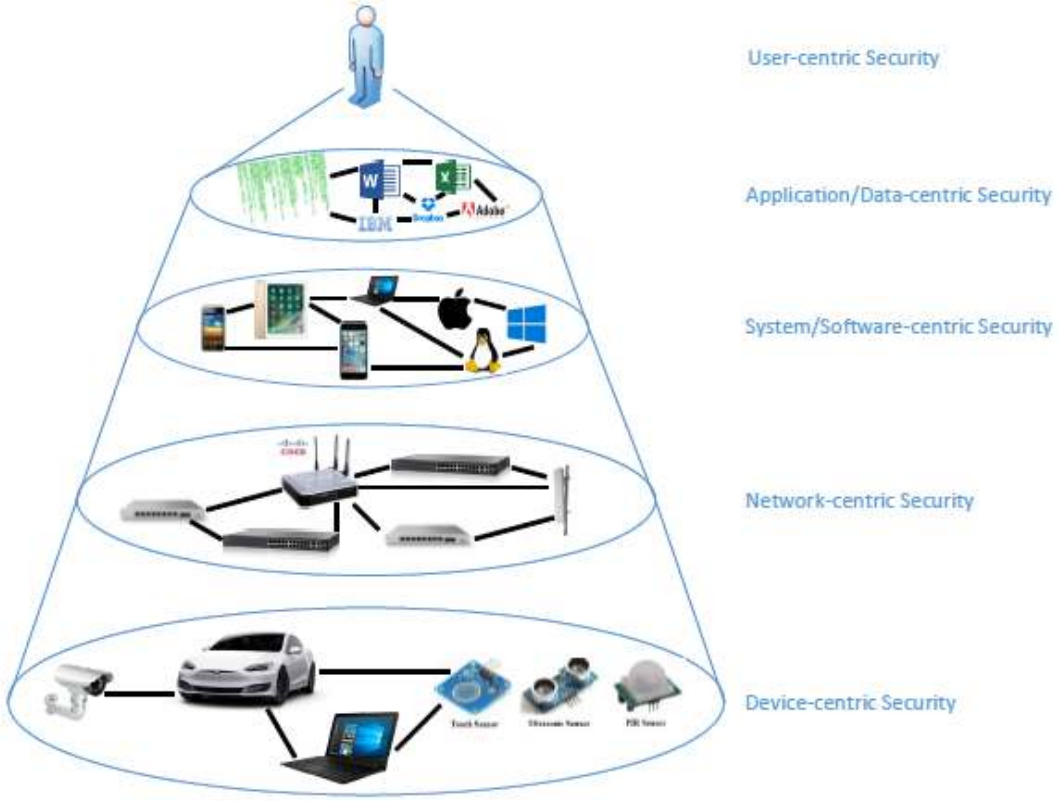
Επιμελητήριο Λάρισας – Τμήμα Ψηφιακών Συστημάτων Πανεπιστημίου Θεσσαλίας

Τρίτη 20 Μαΐου 2025

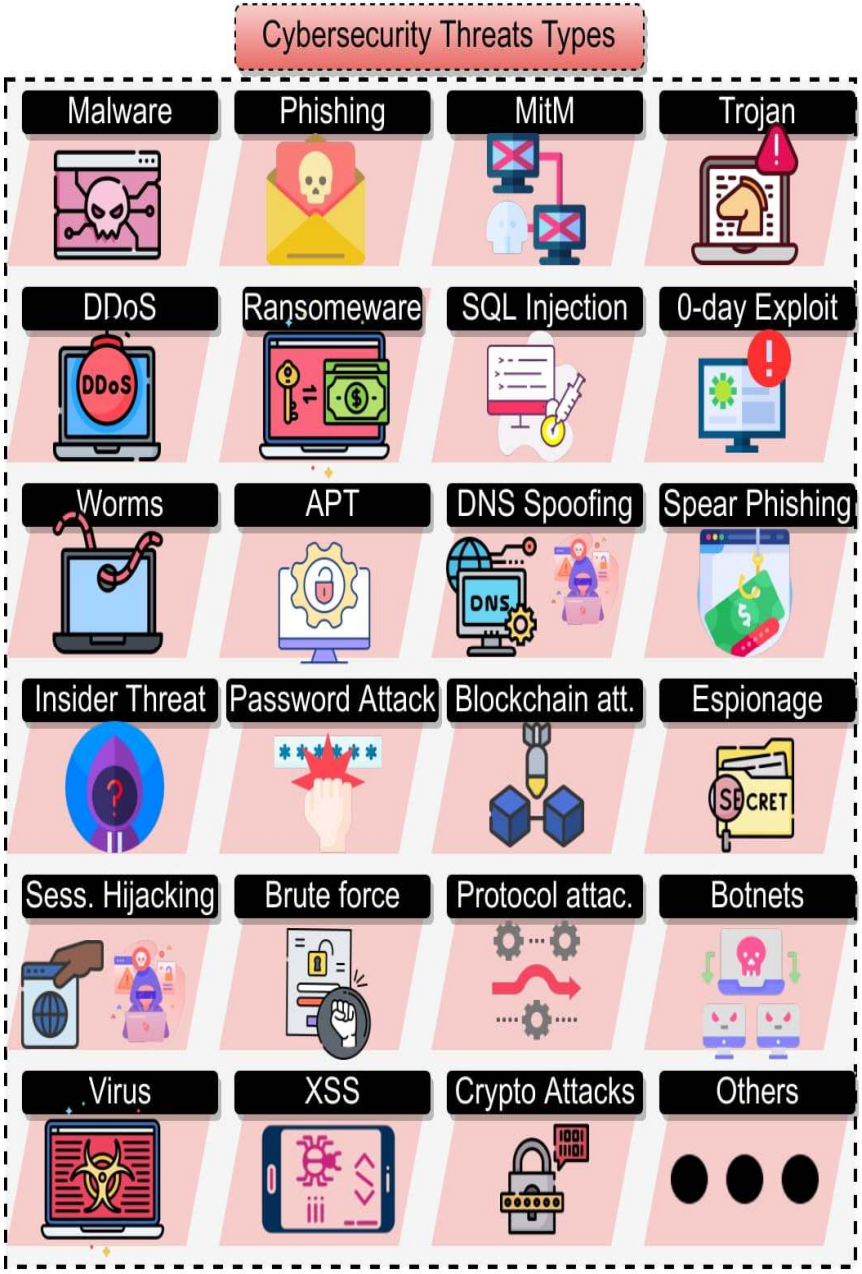
Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΕΠΙΠΕΔΑ

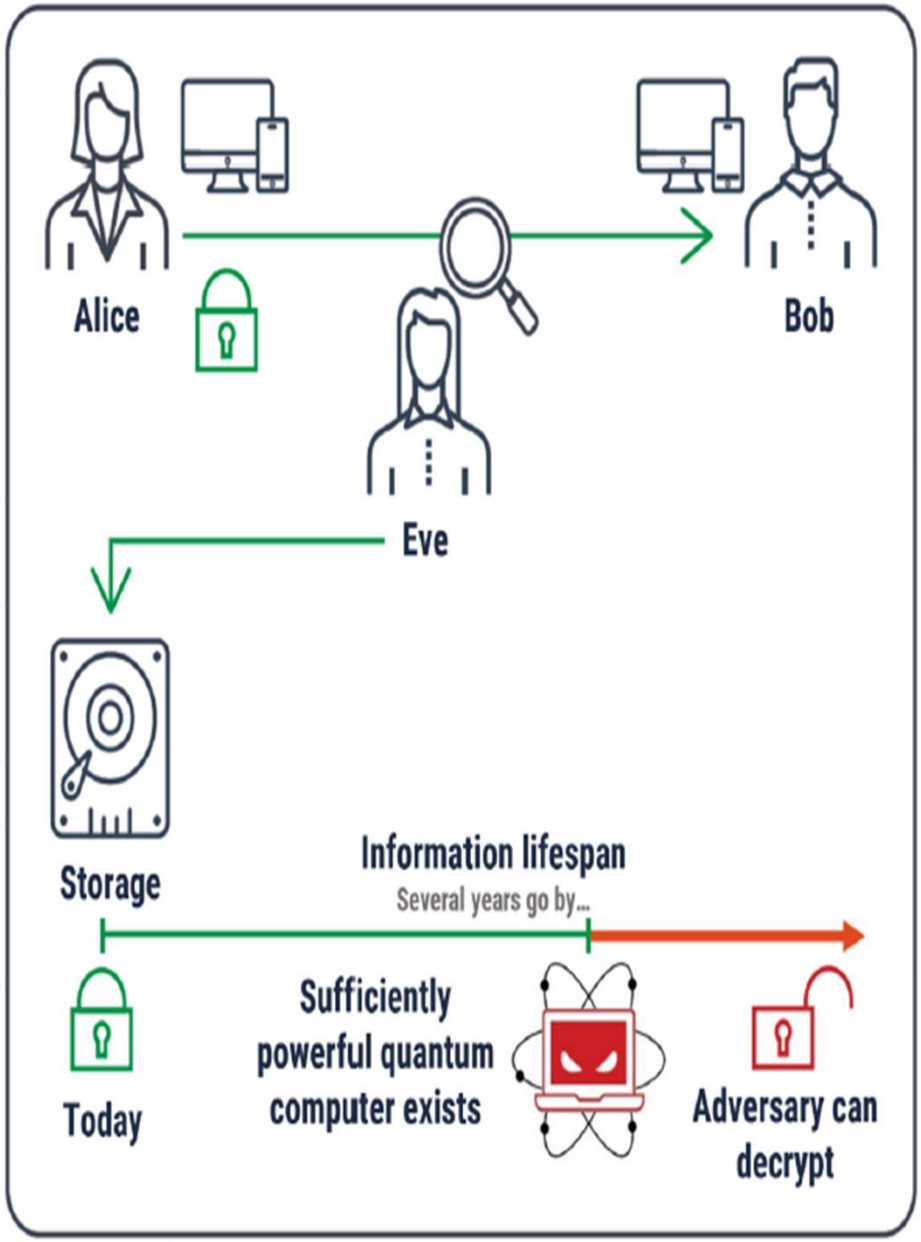
Το σύγχρονο τεχνολογικό περιβάλλον:

- πολύπλοκα αλληλοσυνδεόμενα συστήματα
- εξαιρετικά ετερογενή
- εξαιρετικά δυναμικά
- υψηλής κινητικότητας



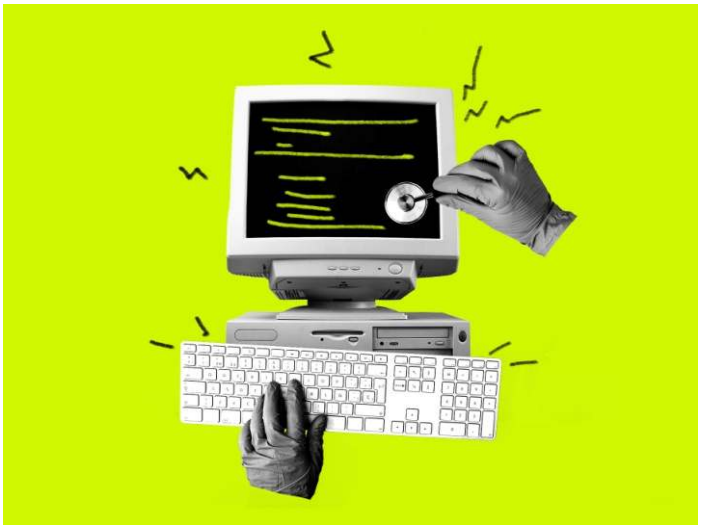
Τύποι κυβερνοεπιθέσεων



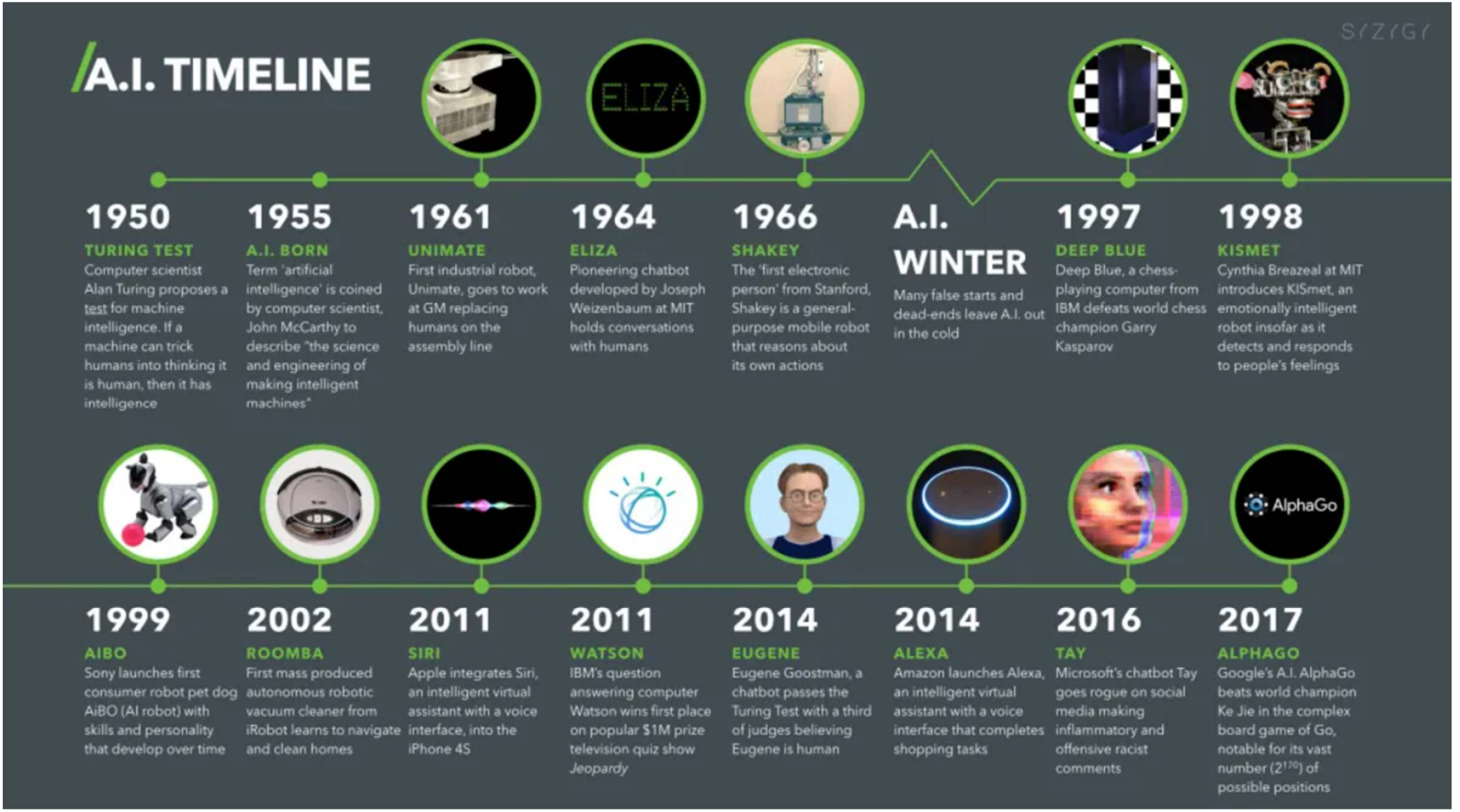


Κανάλια επίθεσης

- Οι επιθέσεις διαφέρουν ως προς τον τρόπο με τον οποίο αποκτούν πρόσβαση ή επεξεργάζονται ευαίσθητες πληροφορίες
- Οι επιθέσεις μπορούν να βασίζονται σε
  - Παρατηρήσιμα δεδομένα
  - Επανασχεδιασμένα δεδομένα
  - Δημόσια Δεδομένα
  - Διαρροή Δεδομένων



Τεχνητή νοημοσύνη στον χρόνο



Ένας νέος κόσμος γεννιέται

1940s-1950s	1960s-1970s	1980s-1990s	2000s-2010s	2020++
Introduction of AI	The first functioning GenAI (Eliza Chatbot)	Identification Patterns (TF-IDF, Deep Learning, CNN, LSTM, RNN)	Nearly flawless translation of the Natural Language + The first version of variational autoencoder + Creation of GENAIs + GPT by OpenAI	Launch of DALL-E + GPT-4 by Open AI + Google Gemini + Falcon AI

Παράκαμψη υπηρεσιών αυθεντικοποίησης χρηστών

Η τεχνολογία **deepfake** αξιοποιείται από απατεώνες για να προσποιούνται ότι είναι άλλοι χρήστες κατά τη διάρκεια ελέγχων ταυτοποίησης που βασίζονται σε εικόνες ή βίντεο.

Αυτή η μέθοδος καθιστά ευκολότερη τόσο τη δημιουργία ψεύτικων λογαριασμών όσο και την παράνομη πρόσβαση σε υπάρχοντες.

Παραβίαση επαγγελματικού ηλεκτρονικού ταχυδρομείου

Η τεχνητή νοημοσύνη ενισχύει τις **τεχνικές κοινωνικής μηχανικής**, επιτρέποντας στους απατεώνες να πείθουν υπαλλήλους να μεταφέρουν χρήματα σε δικούς τους λογαριασμούς.

Επιπλέον, χρησιμοποιούνται **deepfake ήχου και βίντεο** για την πειστική μίμηση ανώτατων στελεχών κατά τη διάρκεια τηλεφωνικών συνομιλιών ή εικονικών συναντήσεων.

Απάτες πλαστοπροσωπίας

Η χρήση μεγάλων γλωσσικών μοντέλων (LLMs) δίνει νέες δυνατότητες στους απατεώνες. Εκπαιδεύοντας τα μοντέλα σε δεδομένα που προέρχονται από παραβιασμένους ή δημόσια διαθέσιμους λογαριασμούς κοινωνικών δικτύων, οι δράστες μπορούν να μιμηθούν με ακρίβεια τα θύματά τους.

Έτσι, πραγματοποιούν απάτες όπως εικονικές απαγωγές, καταφέρνοντας να εξαπατήσουν φίλους ή συγγενείς και να αποσπάσουν χρήματα ή πληροφορίες.

Σπάσιμο κωδικών πρόσβασης

Η τεχνητή νοημοσύνη αναμένεται να αξιοποιηθεί για την ταχύτατη **αποκάλυψη διαπιστευτηρίων** χρηστών, επιταχύνοντας σημαντικά τη διαδικασία παραβίασης.

Αυτό διευκολύνει την **παράνομη πρόσβαση** σε εταιρικά δίκτυα, ευαίσθητα δεδομένα και λογαριασμούς πελατών.

Η τεχνητή νοημοσύνη ενισχύει τις **τεχνικές κοινωνικής μηχανικής.**

Παραδείγματα

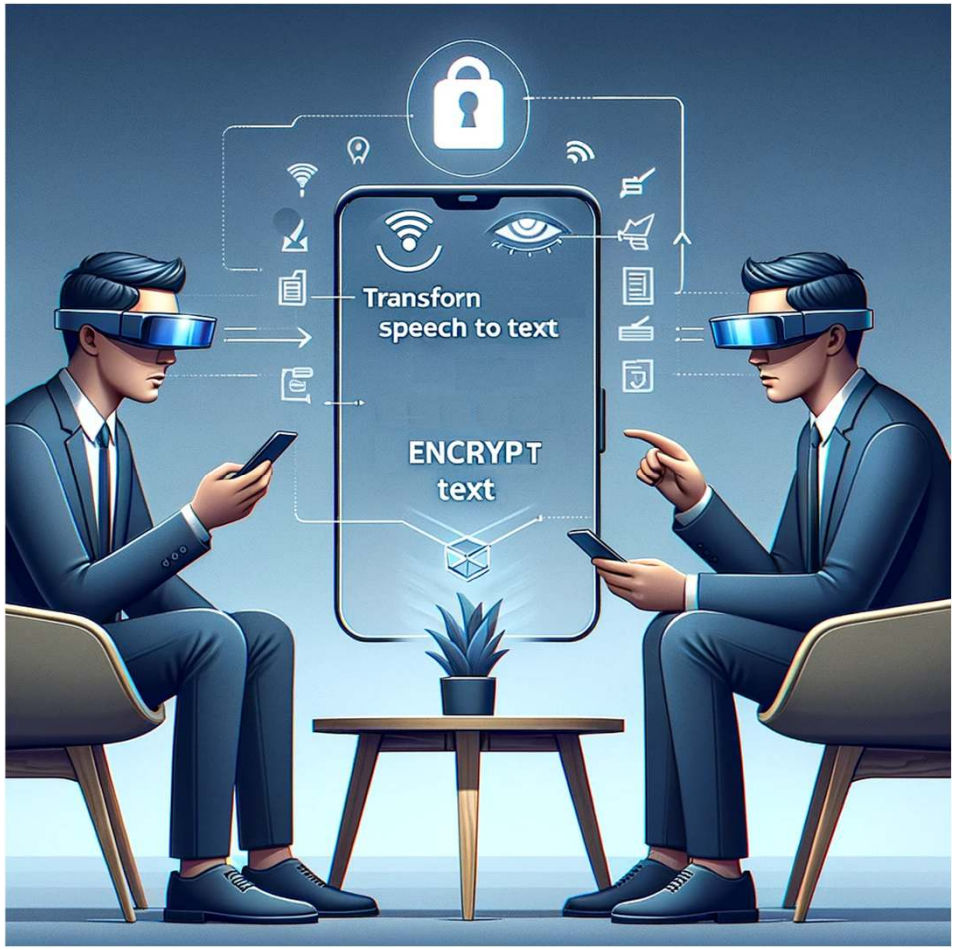
1. 2020 – Απάτη με ψεύτικη φωνή CEO στο Ηνωμένο Βασίλειο

Μια εταιρεία ενέργειας στο Ηνωμένο Βασίλειο εξαπατήθηκε και μετέφερε **220.000 ευρώ** σε λογαριασμό απατεώνων. Οι επιτήδειοι χρησιμοποίησαν τεχνητή νοημοσύνη για να **μιμηθούν τη φωνή του διευθύνοντος συμβούλου** της μητρικής εταιρείας. Η φωνή ήταν τόσο πειστική που ο υπάλληλος πίστεψε ότι η εντολή ήταν αληθινή.

2. 2023 – Συνεντεύξεις εργασίας με deepfake στις ΗΠΑ

Αναφέρθηκαν περιστατικά στις Ηνωμένες Πολιτείες όπου **υποψήφιοι για εργασία** σε τεχνολογικές εταιρείες χρησιμοποίησαν deepfake βίντεο κατά τη διάρκεια **τηλεσυνεντεύξεων**, προσπαθώντας να παραστήσουν άλλους. Σε ορισμένες περιπτώσεις, τα χείλη τους δεν συγχρονίζονταν με τη φωνή, ή η φωνή δεν ταίριαζε με την εικόνα της ταυτότητας.

Το AI στην υπηρεσία του ανθρώπου



Ανίχνευση ανωμαλιών στο σύστημα

Το **AI** μαθαίνει τι είναι "φυσιολογική" δραστηριότητα σε ένα δίκτυο και μπορεί να εντοπίσει ασυνήθιστη συμπεριφορά, όπως:

- Ξαφνικές μεταφορές μεγάλου όγκου δεδομένων
- Παράξενη δραστηριότητα χρηστών εκτός ωραρίου
- Απόπειρες πρόσβασης από ασυνήθιστες τοποθεσίες

Τεχνολογίες: Machine learning (ML), unsupervised learning, LLMs, Deep Learning

Ανάλυση κακόβουλου λογισμικού

Το I μπορεί να αναγνωρίσει καινούριους ιούς και κακόβουλο λογισμικό με βάση:

- Τη συμπεριφορά τους
- Την κατανομή των εντολών τους
- Την αλληλεπίδρασή τους με το σύστημα

Αυτόματη ανταπόκριση σε επιθέσεις

I-powered συστήματα μπορούν να:

- Απομονώσουν ένα ύποπτο endpoint από το δίκτυο
- Τερματίσουν ύποπτες διεργασίες
- Ξεκινούν αυτόματη έρευνα και ειδοποιούν το SOC (Security Operations Center) εφόσον υπάρχει

Ανίχνευση phishing & s□cial engineering

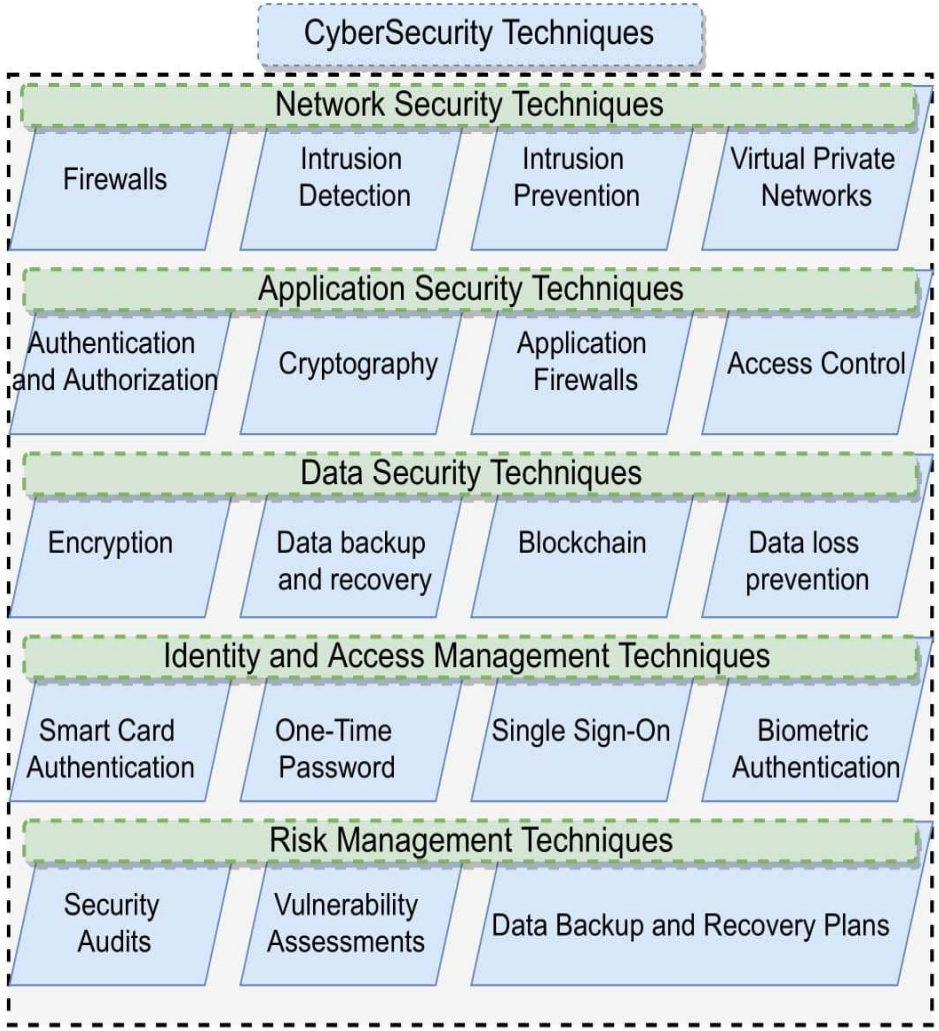
Το □I μπορεί να αναλύσει μηνύματα email και ιστοσελίδες για να εντοπίσει:

- Ψεύτικα domains
- Παραποιημένες διευθύνσεις
- Κείμενα με χαρακτηριστικά απάτης

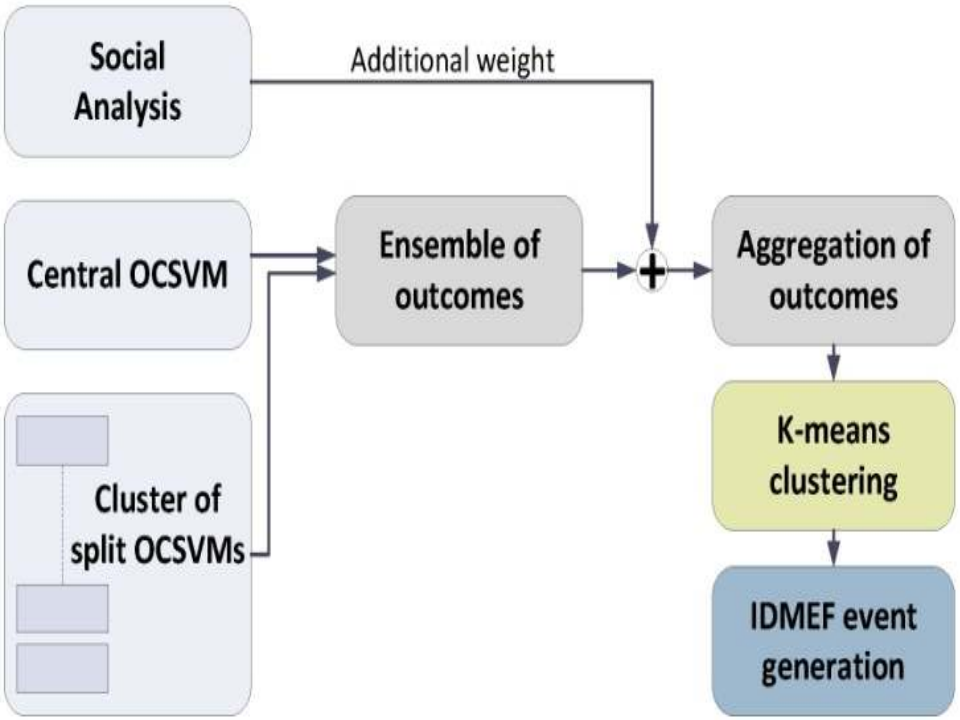
Μέθοδοι αντιμετώπισης

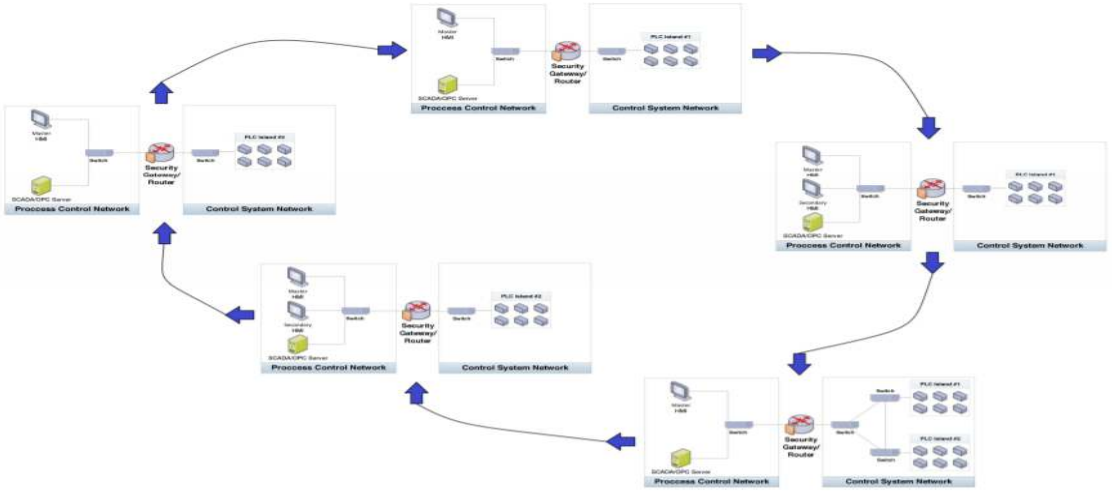
Αναλύουμε όλες τις πτυχές

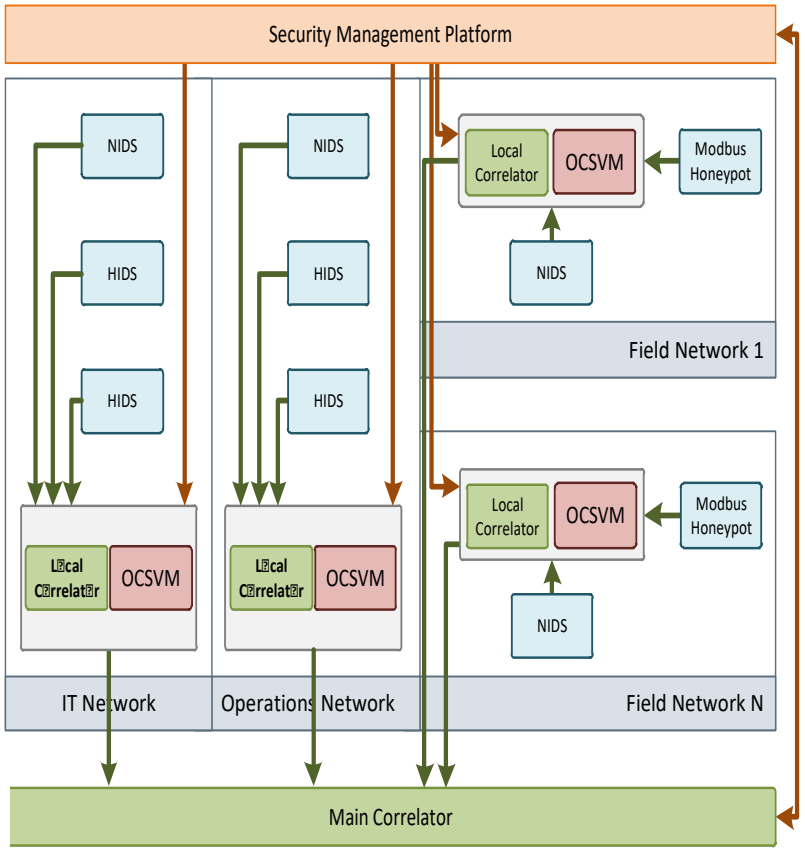
- Επιτιθέμενοι
- Κανάλια επίθεσης
- Τύποι απορρήτου
- Τεχνολογίες



SCADA & Smart Grid (IT-OCSVM)



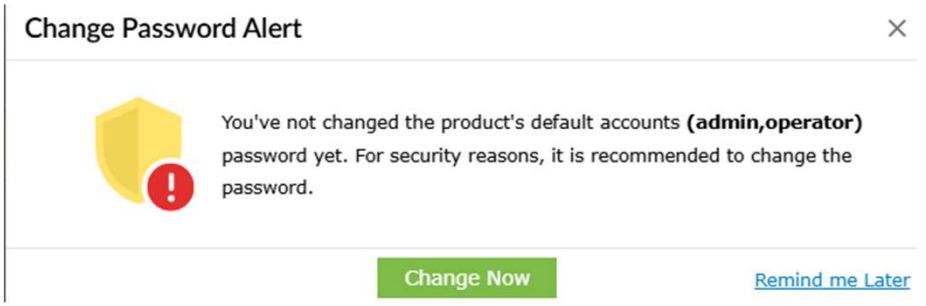




Αυθεντικοποίηση

Πρακτικές λύσεις:

- **Multi-Fact□r Authenticati□n (MFA):** Ενεργοποίηση παντού (email, VPN, cloud apps, □RP, CRM).
- **□assw□rd Managers:** Υιοθέτηση διαχειριστών κωδικών (π.χ. 1Password, □itwarden, LastPass).
- **Πολιτική Λήξης Κωδικών:** Ανανέωση κάθε 90 μέρες
- **Αποφυγή Κοινών Κωδικών:** Εντοπισμός με εργαλεία όπως το Have I □een Pwned □PI.



Ασφάλεια Δικτύων

Πρακτικές λύσεις:

- **Firewall και IDS/I□S:** Π.χ. pfSense, Fortinet, Cisco Firepower.
- **Διαχωρισμός Δικτύων (Netw□rk Segmentati□n):** Ξεχωριστό VL□N για επισκέπτες, IoT, servers.
- **V□N για απομακρυσμένη πρόσβαση:** OpenVPN, WireGuard, ή εμπορικές λύσεις.
- **Netw□rk M□nit□ring:** Λύσεις όπως Zabbix, Nagios, ή commercial (□lienVault, Datadog).

Κινητές Συσκευές

Πρακτικές λύσεις:

- **M□bile Device Management (MDM):** Microsoft Intune, Jamf
- **BYOD □□licies:** Όρια χρήσης προσωπικών συσκευών.
- **Κρυπτογράφηση & Rem□te Wipe:** Σε περίπτωση απώλειας.
- **M□bile □hreat Defense:** Lookout, Zimperium

Endp□int Security (□Cs, Lapt□ps, Servers)

Πρακτικές λύσεις:

- **EDR/XDR Λογισμικό:** Crowdstrike, SentinelOne, Microsoft Defender for □ndpoint.
- (Ο εντοπισμός και απόκριση τελικού σημείου (□DR) και ο εκτεταμένος εντοπισμός και απόκριση (XDR))
- **Περιορισμένα Δικαιώματα Χρηστών:** Οι χρήστες να μην έχουν δικαιώματα administrators.
- **Applicati□n Whitelisting:** Να εκτελούνται μόνο εγκεκριμένα προγράμματα.
- **Aut□ Updates / □atch Management:** WSUS, PDQ Deploy, ή μέσω RMM λογισμικών.

Εκπαίδευση Προσωπικού

Πρακτικές λύσεις:

- **Τακτικά W□rksh□ps & Simulati□ns:** Phishing tests, awareness training.
- **Κανονισμοί Ασφαλείας:** Ορατοί, εύληπτοι, υπογεγραμμένοι από τους εργαζομένους.
- **Ενημέρωση για Scams:** Εβδομαδιαία/μηνιαία email με πρόσφατα παραδείγματα επιθέσεων.

Διαχείριση Συμβάντων

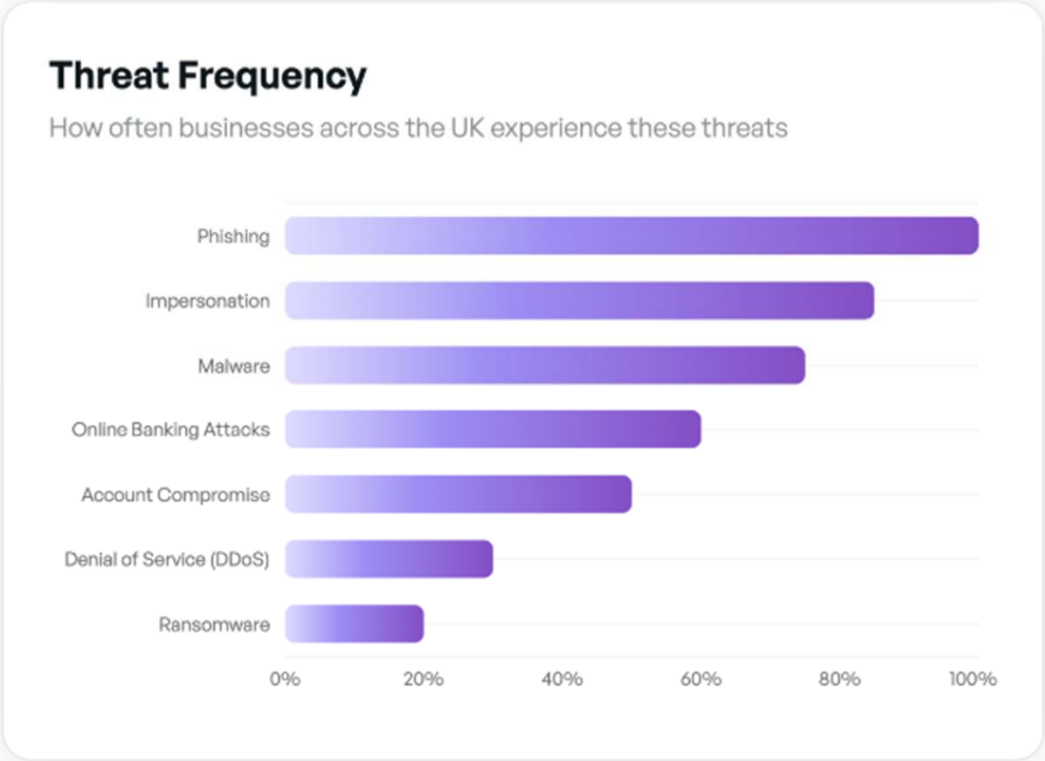
Πρακτικές λύσεις:

- **Incident Resp□nse □lan (IR□):** Σαφές πλάνο με ρόλους, επικοινωνίες, ενέργειες.
- **□ablet□p Exercises:** Προσομοίωση επιθέσεων για εξάσκηση ομάδων IT/HR/νομικών.
- **Backups – με στρατηγική 3-2-1:** 3 αντίγραφα, 2 μέσα, 1 offsite/offline.
- **SIEM/L□g M□nit□ring:** Graylog, □LK Stack, Splunk, Microsoft Sentinel.

Νεες προσφερόμενες λύσεις
από εταιρείες στην Ελλάδα & U

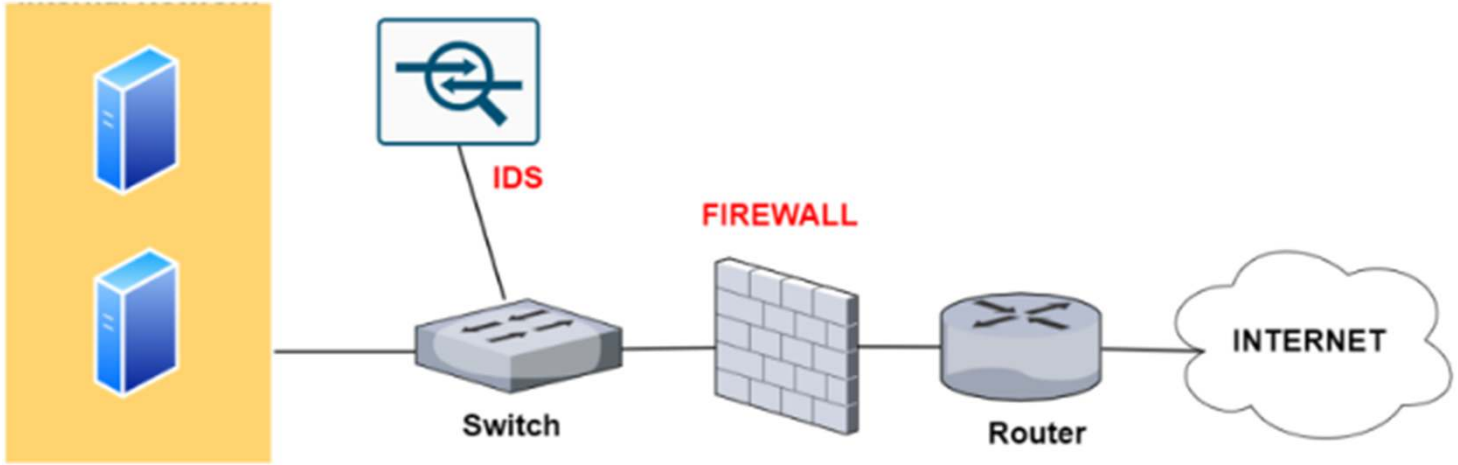
- NIS2, GDPR **cmpliance**
- **LastingAsset** → πλαστοπροσωπία μέσω τηλεφώνου
- **Παροχή υπηρεσιών** Honeypot as a Service
- **Παροχή υπηρεσιών SOC as a service**
- SOC with LLM → Πρόγραμμα ΗΕ **iSOCaas**
- **Cyber Risk Radar** → **https://cyberiskradar.cm/**

Ανάλυση απειλών και ρίσκων



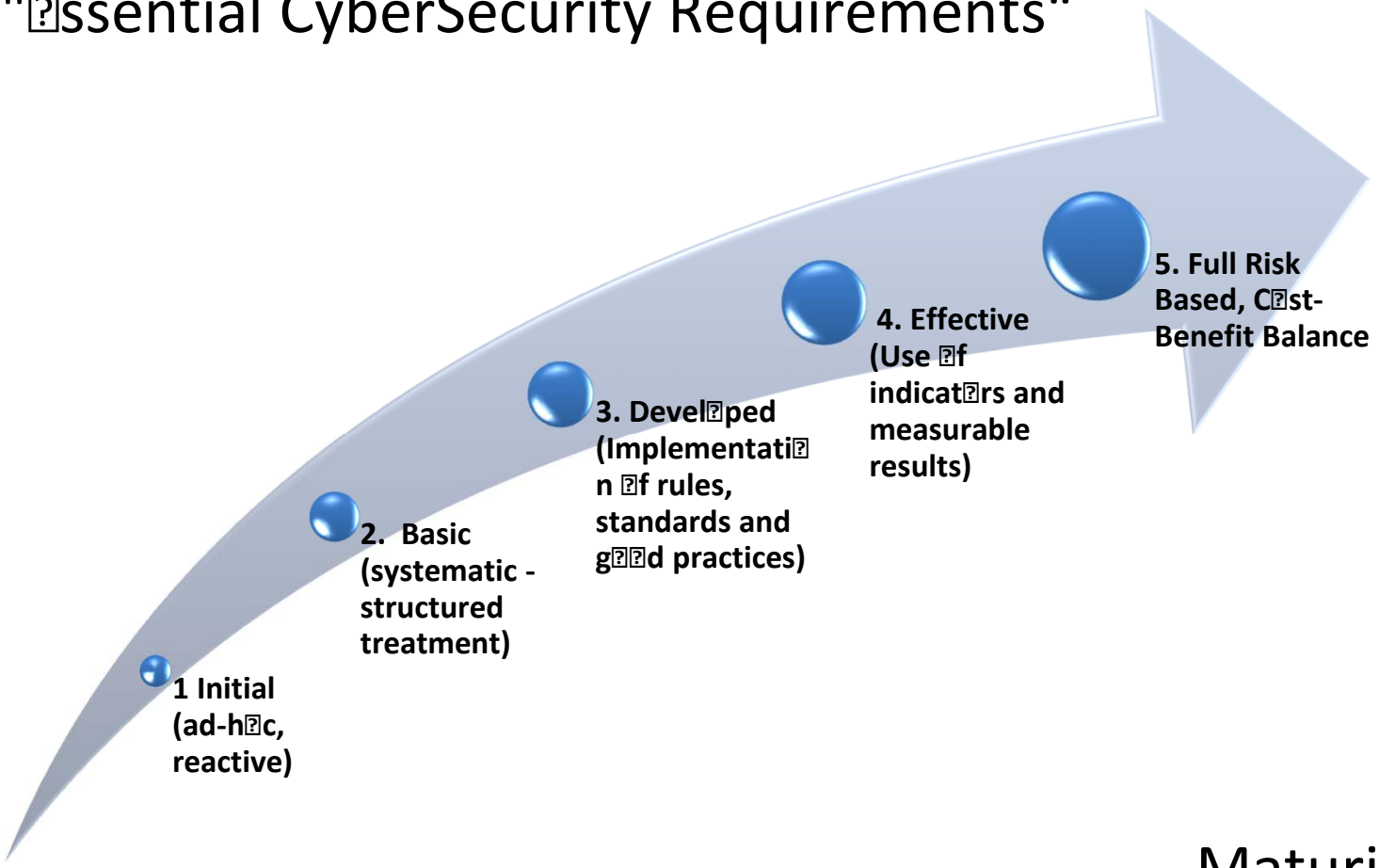
Εργαλεία

- Snort
- Suricata
- SecML
- PhishTank + □I
- Rspamd
- MailScanner



Πλαίσιο Αξιολόγησης Ωριμότητας

"□ssential CyberSecurity Requirements“



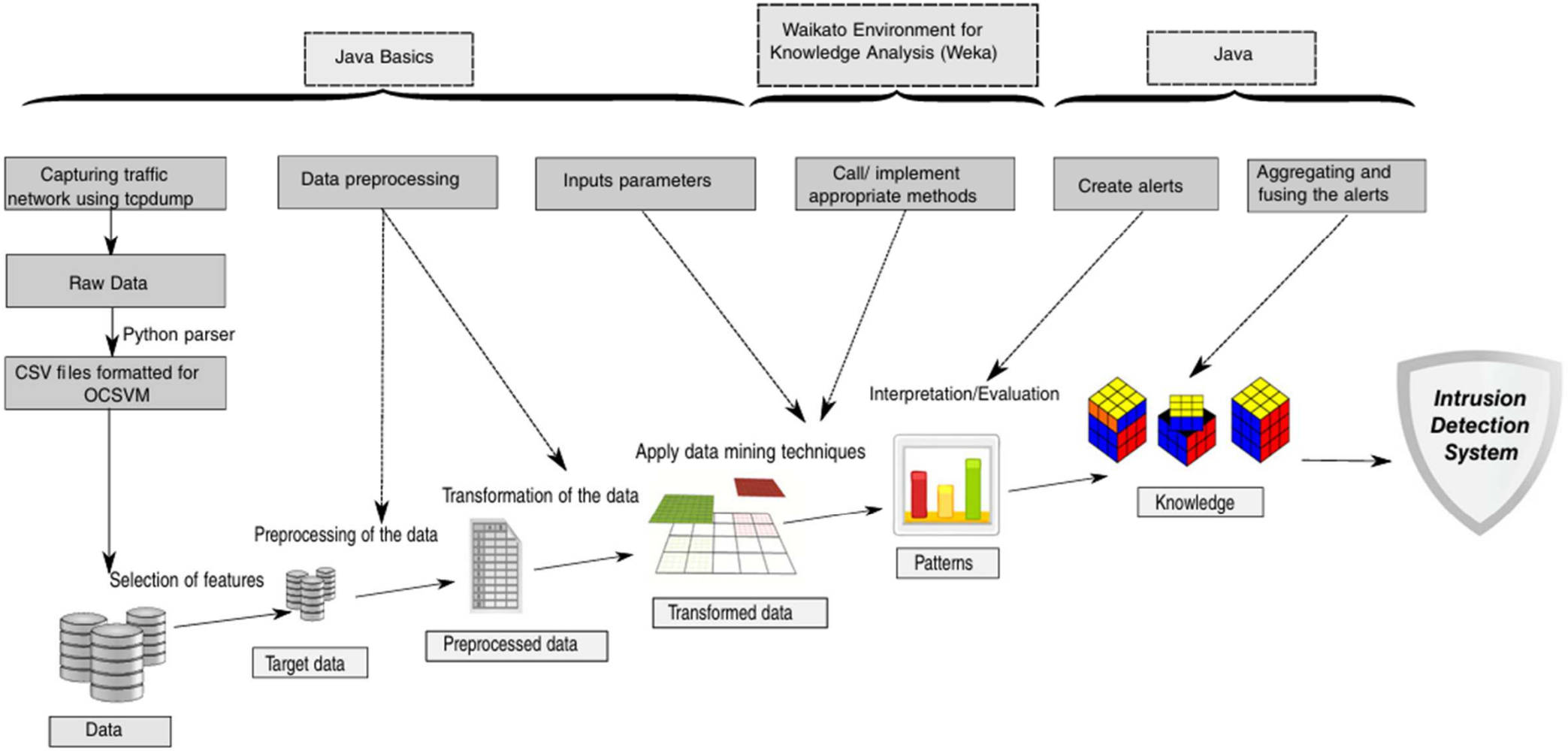
Maturity

Levels (0-5)

Κύκλος Κυβερνοασφάλειας

1. Σχεδιασμός
2. Υλοποιήση
3. Αξιόλογηση
   - Εσωτερική (Self-□ssessment)
   - Εξωτερική (Outsourcing)
4. Διόρθωση / Επαναπροσδιορισμός

Σύστημα ανίχνευσης εισβολών με AI



Συμπεράσματα

- Η τεχνητή νοημοσύνη φέρνει ριζικές αλλαγές στον τρόπο που αλληλοεπιδρούμε με την τεχνολογία, με θετικές αλλά και αρνητικές συνέπειες
- Οι εταιρείες πρέπει να είναι προετοιμασμένες για να αντιμετωπίσουν κυβερνοεπιθέσεις
- Προτείνεται να δημιουργηθεί ένας τοπικός φορέας παροχής υπηρεσιών ασφάλειας σε σύμπραξη του πανεπιστήμιου Θεσσαλίας και τοπικών φορέων και εταιρειών (**Cybersecurity One st□p sh□p f□r □hessaly**)

Ερωτήσεις


ca technologies
CA.COM/CLOUD-MONITORING
ALL I KNOW IS THE BOSS SAID WE HAD TO MONITOR THE CLOUD.
© D.Fletcher for CloudTweaks.com