

Νέο εκπαιδευτικό υλικό από τον ENISA σχετικά με την Αντιμετώπιση Περιστατικών Απειλών μέσω Κινητών και ανάλυση Τεχνικών Σφαλμάτων

Ο ENISA παρουσιάζει δημόσια μια συνέχεια στο πιο διαδεδομένο και αξιόλογο τεχνικό εκπαιδευτικό υλικό του, σχετικά με την Αντιμετώπιση Περιστατικών Απειλών μέσω Κινητών και ανάλυση Τεχνικών Σφαλμάτων.

Το υλικό που παρουσιάζεται αποτελείται από δυο μέρη:

- Το νέο περιεχόμενο εξοικειώνει εκπαιδευόμενους με τις έννοιες, τα εργαλεία και τις τεχνικές που χρησιμοποιούνται για την **αντιμετώπιση περιστατικών σε κινητές συσκευές**, ενώ προσφέρει ταυτόχρονα μεθοδολογία για την - ορθή και έγκαιρη - αντίδραση όταν προκύψει ανάγκη.
- Το νέο εκπαιδευτικό υλικό **ανάλυσης τεχνικών σφαλμάτων** βοηθά τους αναλυτές ασφάλειας των πληροφοριών να αναλύσουν ορθά κακόβουλο λογισμικό, καθώς επίσης να κατανοήσουν τη δυνητική λειτουργικότητά του, επιτρέποντας στον οργανισμό να δημιουργήσει κατάλληλα αντίμετρα και σχέδια μετριασμού.

Η ικανότητα διαχείρισης και επίλυσης περιστατικών ασφάλειας των πληροφοριών έχει καταστεί κύρια προτεραιότητα για επιχειρήσεις, κυβερνητικά όργανα, πανεπιστήμια και άλλους οργανισμούς με πρωτοβουλίες που λαμβάνουν χώρα σε όλα τα κράτη μέλη της ΕΕ.

Το υλικό έχει κατηγοριοποιηθεί σε τέσσερις κύριες θεματικές ενότητες:

- Τεχνικό
- Λειτουργικό
- Δημιουργία CSIRT
- Νομικά και συνεργασία

Παρέχονται επίσης διάφορα εργαλεία για πρακτική εκπαίδευση, όπως το Virtual Machines. Για πρόσβαση στο νέο υλικό:

- **Mobile Threats Incident Handling Part II** (Αντιμετώπιση Περιστατικών Απειλών μέσω Κινητών Μέρος II)
- **Advanced artefact analysis training material** (Εκπαιδευτικό υλικό ανάλυσης τεχνικών σφαλμάτων για προχωρημένους)

Για επισκόπηση των εκπαιδευτικών προγραμμάτων του ENISA και το **‘πρόγραμμα εκπαίδευσης του εκπαιδευτή’** παρακολουθήστε το ακόλουθο **βίντεο**.

Για πρόσβαση σε όλους τους διαθέσιμους εκπαιδευτικούς πόρους, επισκεφθείτε το **σύνδεσμο**.

Για περισσότερες πληροφορίες επί του θέματος καθώς και ερωτήματα από τον Τύπο, επικοινωνήστε με τα press@enisa.europa.eu, Τηλ. +30 2814 409576