INTRACOM TELECOM

Technology Shaping the Future

Cyber Threat Intelligence - CTI

What it is, How it can be used, What it offers!

Ioannis Vordos, MEng., MSCS, GSEC, GCFA, GPEN
Security Solutions Product Manager
iovor@intracom-telecom.com

Cyber Threat Intelligence

Threat Intelligence ή Cyber Threat Intelligence – CTI είναι η γνώση σχετικά με τις δυνατότητες, την υποδομή, τις προθέσεις, τους στόχους και τις πηγές των απειλών. Η χρήση/εφαρμογή αυτών των πληροφοριών βοηθά στην επιχειρησιακή και στρατηγική άμυνα των δυκτιοκεντρικών υποδομών.

http://cdn2.hubspot.net/hubfs/454298/ebook/Threat-Intel-Platform-ebook-ThreatConnect.pdf

Σε μία πιο αφαιρετική εκδοχή, το CTI είναι η διαδικασία μεταφοράς θεμάτων ασφαλείας από την περιοχή των «άγνωστων αγνώστων» στην περιοχή των «γνωστών αγνώστων» αποκαλύπτοντας την παρουσία απειλών και στη συνέχεια μεταφορά αυτών στην περιοχή των «γνωστών γνωστών», όπου οι απειλές έχουν γίνει κατανοητές και έχουν αντιμετωπιστεί.

https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf

Cyber Threat Intelligence - Αποστολή

Η κύρια αποστολή του CTI είναι να ερευνά και να αναλύει τις τάσεις και τα τεχνολογικά επιτεύγματα στις ακόλουθες περιοχές:

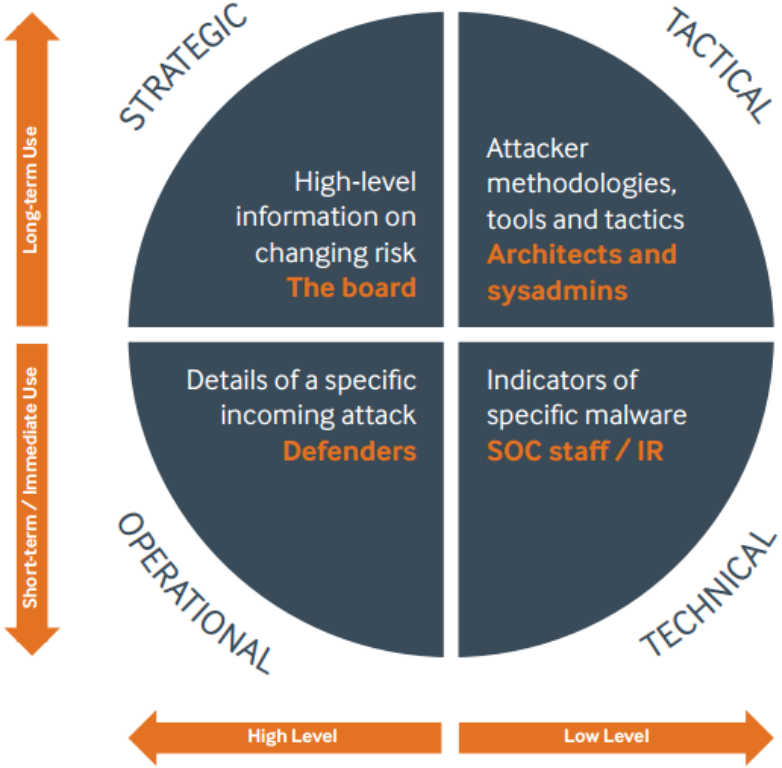
- Κυβερνο-έγκλημα (Cyber crime)
- Κυβερνο-ακτιβισμός (Cyber activism)
- Κυβερνο-κατασκοπεία (Cyber espionage) (Advanced Persistent Threat or APT)

https://www.ncsc.gov.uk/guidance/introduction-threat-intelligence

Τα δεδομένα που προκύπτουν από την έρευνα και ανάλυση, επιτρέπουν στις ενδιαφερόμενες πλευρές να λάβουν εκ των προτέρων μέτρα αντιμετώπισης.

Για το λόγο αυτό το CTI έχει αναδειχθεί ως μία αξιόπιστη λύση για την υποστήριξη της κυβερνο-ασφάλειας σε διεθνές επίπεδο.

Τύποι CTI



Σύμφωνα με το Βρετανικό Κέντρο Προστασίας Εθνικών Υποδομών (UK's Centre for the Protection of National Infrastructure (CPNI)), υπάρχουν **4 τύποι threat intelligence**:

- **Τακτικό (Tactical)**
- **Τεχνικό (Technical)**
- **Επιχειρησιακό (Operational)**
- **Στρατηγικό (Strategic)**

https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf

Πηγές Τροφοδότησης CTI

- **Ανοιχτές Πηγές - Open Source Intelligence (OSINT):** Αφορά Intelligence που διατίθεται φανερά από δημόσιες πηγές.
  - Γενική on-line έρευνα, σχετικά με το brand μίας εταιρείας, ή αναζήτηση προσωπικών πληροφοριών.
  - Αυτοματοποιημένα συστήματα που συλλέγουν δεδομένα σχετικά με επιθέσεις.
  - Παραγόμενα Logs από συστήματα ασφαλείας, όπως επίσης και δεδομένα από αναλύσεις forensic.
  - Δωρεάν (open) δημόσιες πηγές τροφοδότησης threat intelligence από εξειδικευμένους οργανισμούς ασφαλείας.
  - Κυβερνητικά σχήματα ανταλλαγής intelligence (π.χ. ΕΑΠΔΠΧ, ΕΥΠ, επιμέρους CERT)
  - Βιομηχανικό intelligence από συνεργάτες και επίσημους φορείς διανομής intelligence (πχ ENISA)
  - Εμπορικοί πάροχοι με μισθωμένες υπηρεσίες παροχής threat intelligence.

- **Καλυμμένες Πηγές - Covert Human Intelligence Sources (CHIS)**: Το intelligence συλλέγεται από διαπροσωπικές επαφές. Κατά βάση περιλαμβάνει intelligence που συλλέγεται από πηγές στο Deep Web.

- Μερικοί θεωρούν ότι αυτές οι πηγές από μόνες τους αποτελούν το CTI. Ωστόσο **σημαντικό έργο ανάλυσης είναι απαραίτητο** ώστε να παραχθεί **πραγματικό** threat intelligence.

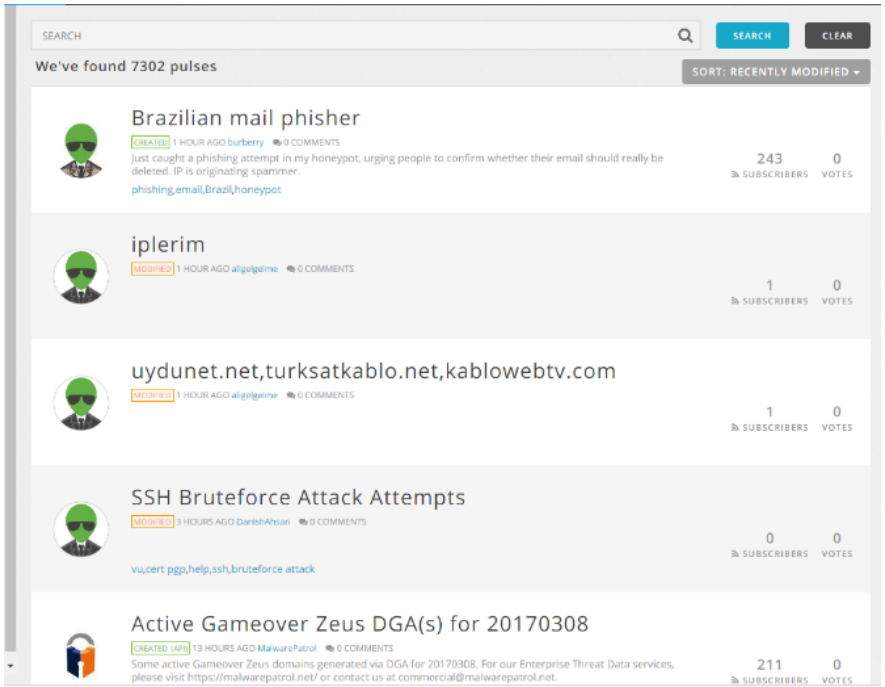
Πρότυπα Ανταλλαγής CTI

Οι πλέον χρησιμοποιούμενοι τρόποι ανταλλαγής Threat Intelligence (κυρίως IOCs) ακολουθούν τα ακόλουθα πρότυπα:

APEC	The Common Attack Pattern Enumeration and Classification (CAPEC) is a comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses.
CybOX	The Cyber Observable eXpression (CybOX) language provides a common structure for representing cyber observables across and among the operational areas of enterprise cyber security that improves the consistency, efficiency, and interoperability of deployed tools and processes, as well as increases overall situational awareness by enabling the potential for detailed automatable sharing, mapping, detection, and analysis heuristics.
IODEF (RFC5070)	The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents.
IDMEF (RFC4765)	*Experimental* - The purpose of the Intrusion Detection Message Exchange Format (IDMEF) is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them.
MAEC	The Malware Attribute Enumeration and Characterization (MAEC) projects is aimed at creating and providing a standardized language for sharing structured information about malware based upon attributes such as behaviors, artifacts, and attack patterns.
STIX	The Structured Threat Information eXpression (STIX) language is a standardized construct to represent cyber threat information. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, and automatable. STIX does not only allow tool-agnostic fields, but also provides so-called *test mechanisms* that provide means for embedding tool-specific elements, including OpenIOC, Yara and Snort.
TAXII	The Trusted Automated eXchange of Indicator Information (TAXII) standard defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII defines concepts, protocols, and message exchanges to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats.
VERIS	The Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS is a response to one of the most critical and persistent challenges in the security industry - a lack of quality information. In addition to providing a structuref format, VERIS also collects data from the community to report on breaches in the Verizon Data Breach Investigations Report (DBIR) and publishes this database online at VCDB.org.

CTI – Προσφερόμενες Λύσεις

- Τροφοδοσία Threat Intelligence
- Ενσωμάτωση σε υφιστάμενο ή προς απόκτηση εξοπλισμό ασφάλειας
- Πλατφόρμες Threat Intelligence (Threat Intelligence Platforms – TIP)
- Threat Intelligence Platform as a Service



https://otx.alienvault.com/browse/pulses/?sort=-modified

Threat Intelligence Platform (TIP) - Δυνατότητες

Οι πλατφόρμες Threat Intelligence (TIP) είναι μία σχετικά νέα τεχνολογία που βοηθά τους οργανισμούς να συγκεντρώνουν, συσχετίζουν και αναλύουν δεδομένα σχετικά με τις απειλές από πολλαπλές πηγές σε πραγματικό χρόνο, για την υποστήριξη των αμυντικών ενεργειών. Οι λειτουργίες που παρέχουν είναι:

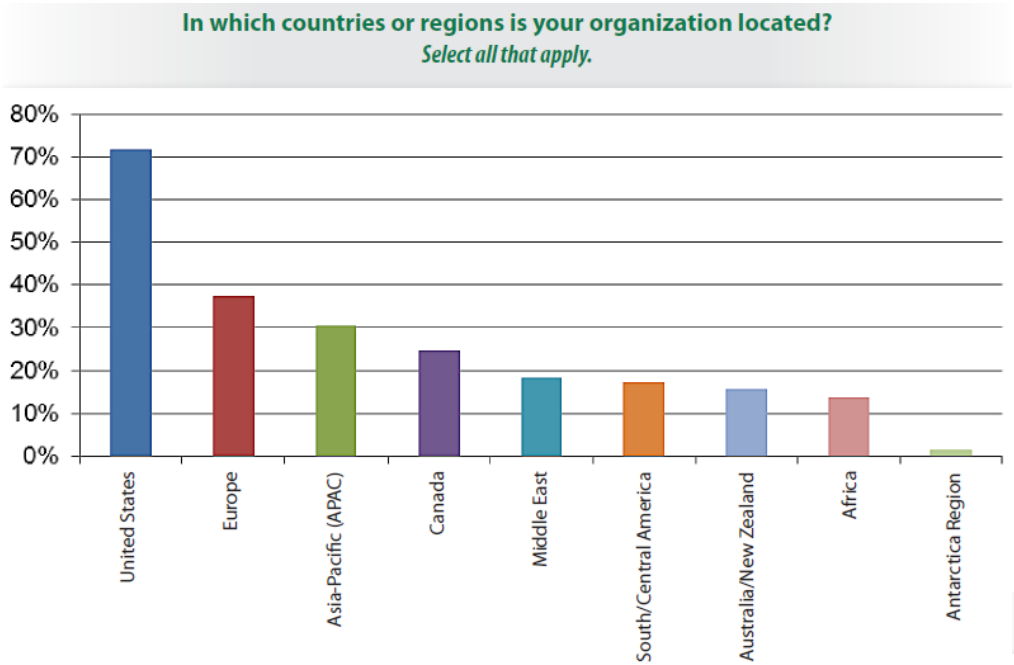
- **Συλλογή (Collect)**
- **Συσχέτιση (Correlate)**
- **Εμπλουτισμός και Οριοθέτηση (Enrichment and Contextualization)**
- **Ανάλυση (Analyze)**
- **Ενσωμάτωση (Integrate)**
- **Δράση (Act)**

INTRACOM TELECOM

Technology Shaping the Future

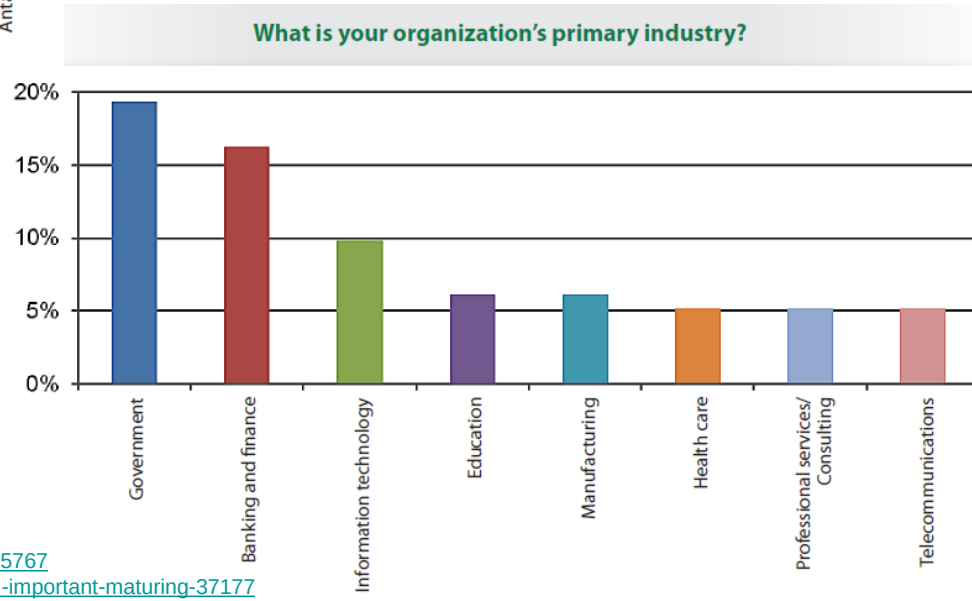
Διείσδυση CTI - Αποτελέσματα

Διείσδυση Threat Intelligence



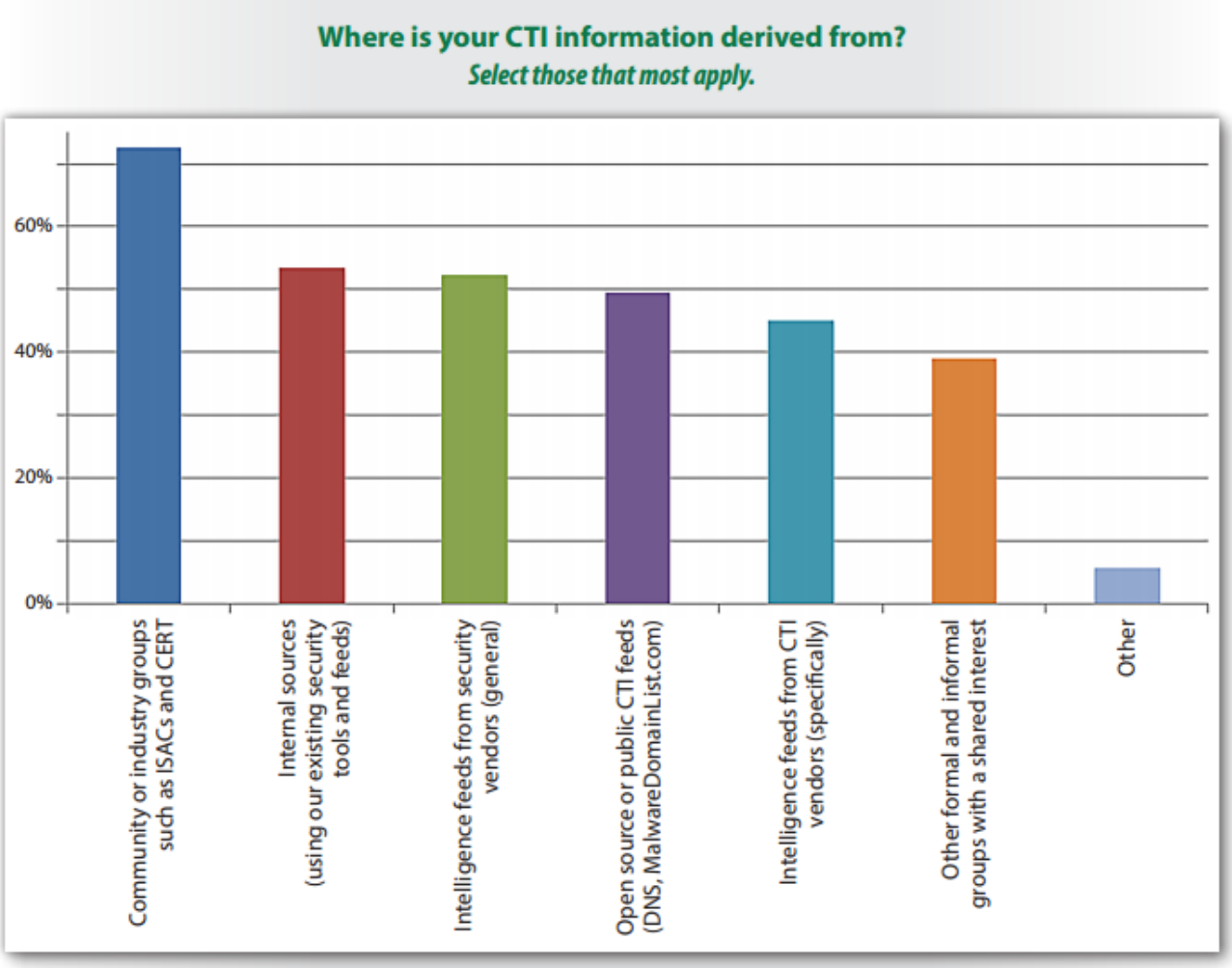
Ο εκπαιδευτικός οργανισμός SANS εκτελεί σε τακτά χρονικά διαστήματα έρευνες για τη διείσδυση του Cyber Threat Intelligence.

- Περισσότεροι από 600 (2017) συμμετέχοντες,
- 60% (2017) ανέφεραν ότι υλοποιούν CTI σε κάποιο βαθμό, 25% ότι σχεδιάζουν να υλοποιήσουν και 15% ότι δεν έχουν ανάλογο σχεδιασμό.



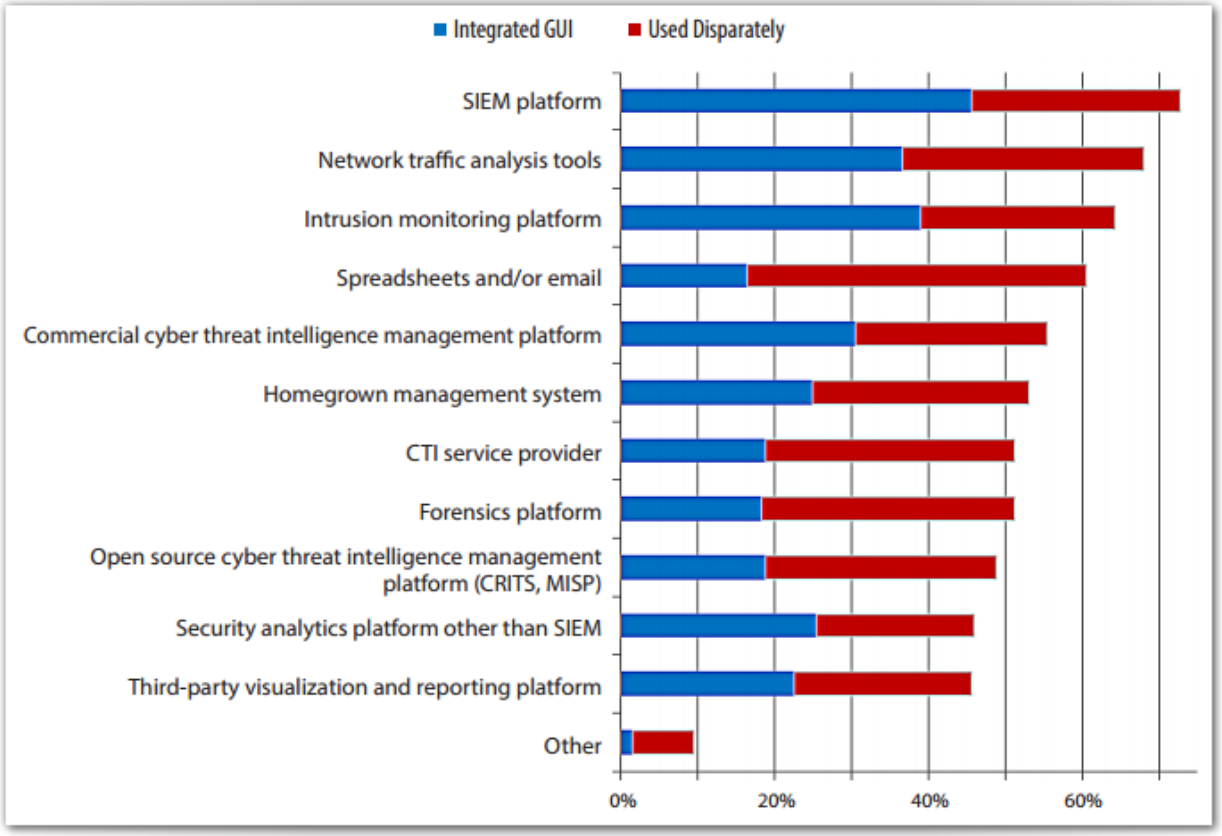
https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767
https://www.sans.org/reading-room/whitepapers/bestprac/state-cyber-threat-intelligence-survey-cti-important-maturing-37177
https://www.sans.org/reading-room/whitepapers/threats/cyber-threat-intelligence-uses-successes-failures-2017-cti-survey-37677

Πηγές CTI



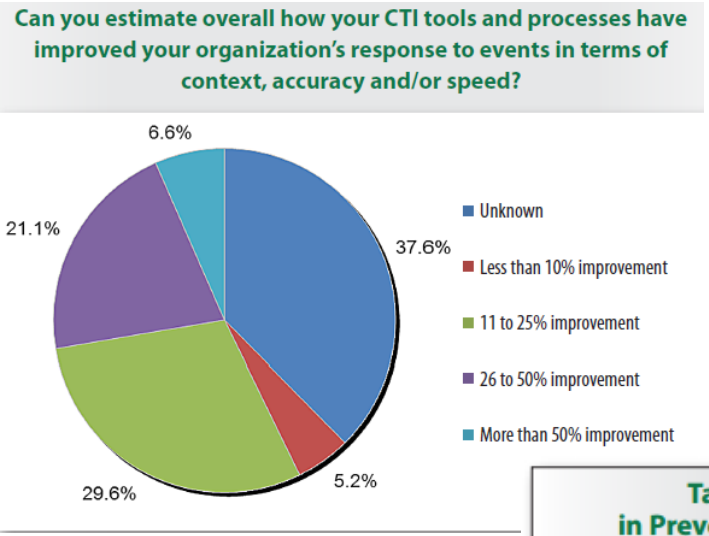
Οι πλέον ώριμοι από πλευράς CTI οργανισμοί (που διαθέτουν και αντίστοιχες εσωτερικές ομάδες CTI) χρησιμοποιούν ανοιχτές ή εσωτερικές πηγές τροφοδοσίας CTI. Ωστόσο οι «κλειστές» πηγές τροφοδοσίας διαθέτουν ένα εξίσου σημαντικό μερίδιο (3η και 5η θέση).

Συσκευές που χρησιμοποιούνται για CTI



69% χρησιμοποιούν το SIEM για τη συλλογή και διαχείριση του (15% αύξηση από το 2015),
68% χρησιμοποιούν συστήματα ανάλυσης δικτυακής κίνησης (FW, UTM) και 65% IDS/IPS (10% αύξηση από το 2015),
55% χρησιμοποιούν εμπορικές πλατφόρμες διαχείρισης CTI εμφανίζοντας αύξηση πάνω από 40% από το 2015.

Βελτιώσεις στην Ασφάλεια από το CTI

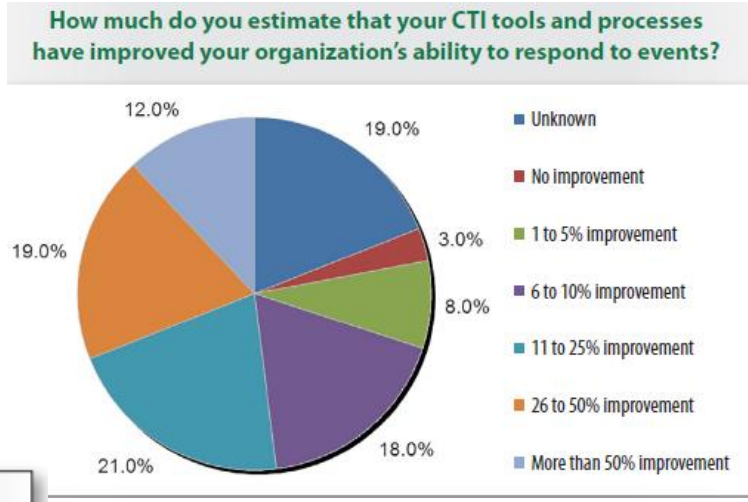


2015

2017

Table 2. Improvement Rates in Prevention/Detection and Response

Percentage Improvement	Security (Prevention and Detection)	Response
Unknown	29.0%	31.0%
No improvement	0.0%	0.5%
1–5%	3.0%	3.5%
6–10%	7.0%	8.5%
11–25%	17.5%	18.0%
26–50%	17.5%	18.0%
51–75%	19.0%	10.5%
76–100%	7.0%	10.0%



2016

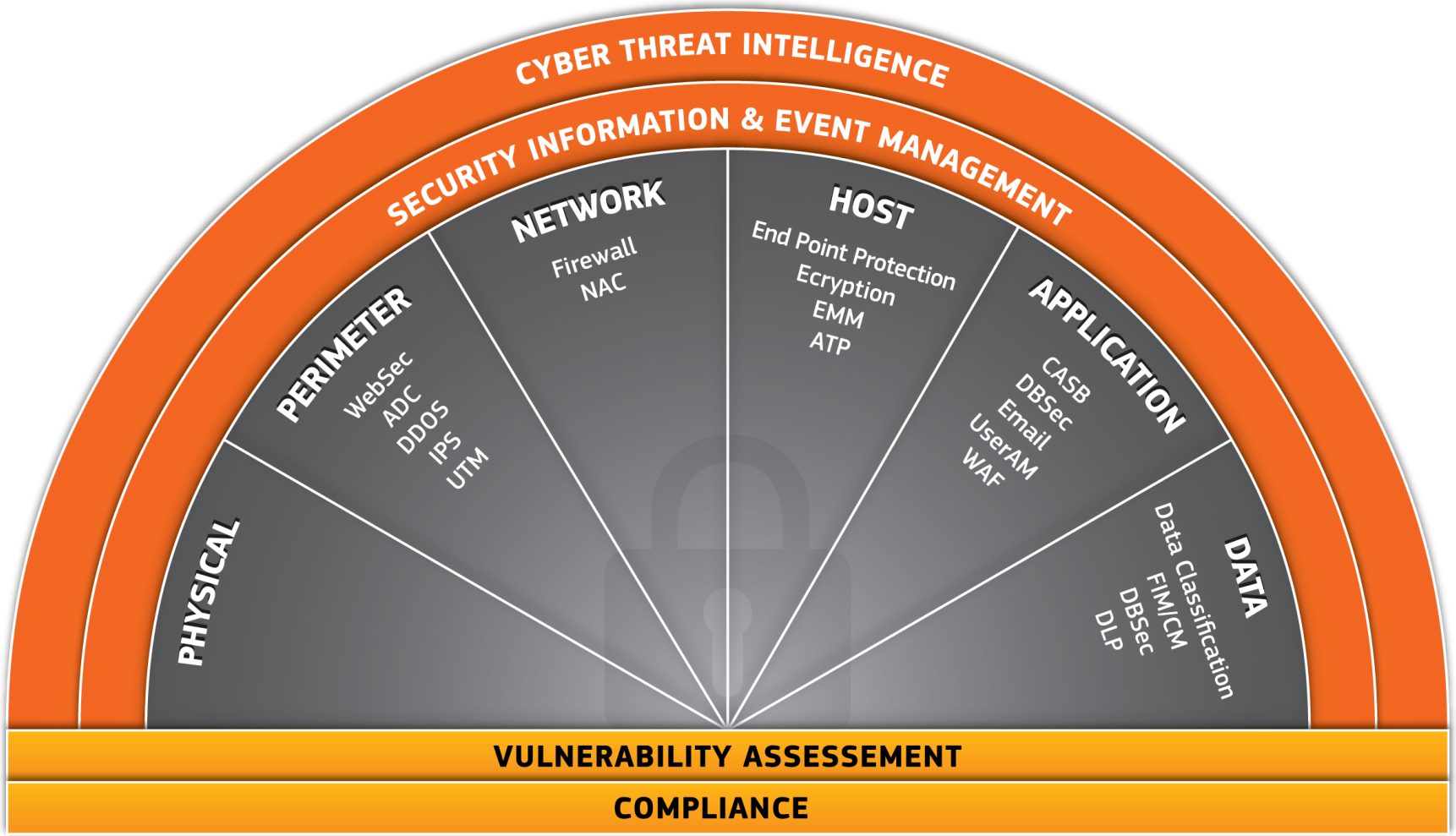
<u>Σταθερά αυξανόμενη θετική άποψη</u> για τη βελτίωση των δυνατοτήτων του οργανισμού να εντοπίζει, αποτρέπει και διερευνά συμβάντα ασφαλείας με τη συμβολή των CTI tools. Περισσότερο από 70% θετική άποψη το 2017.

INTRACOM TELECOM

Technology Shaping the Future

Intracom Telecom

Intracom Telecom's Security Portfolio



thank you

For more information, visit

www.intracom-telecom.com

INTRACOM TELECOM

Follow | Link | Watch