



MIDDLEBOX STANDARDISATION?



ASSUMPTIONS AND SOURCES



- WE ASSUME AUDIENCE FAMILIAR WITH MIDDLEBOXES AND INTERCEPTION
- SOURCES FOR THIS PRESENTATION
 - ETSI
 - CYBERSECURITY ECOSYSTEM
 - TC CYBER / MIDDLEBOXES
 - TUTORIAL TO FORTHCOMING ITU-T SG17 MEETING (20th to 29th of MARCH)
 - TONY RUTKOWSKI (YANNA), ARNAUD TADDEI (SYMANTEC)
 - IEEE/ICSG/ETI
 - ITU-T SG17
 - IETF SEC (TLS, I2NSF, etc.) TRANSPORT (QUIC)

METRICS OF IMPORTANCE TODAY



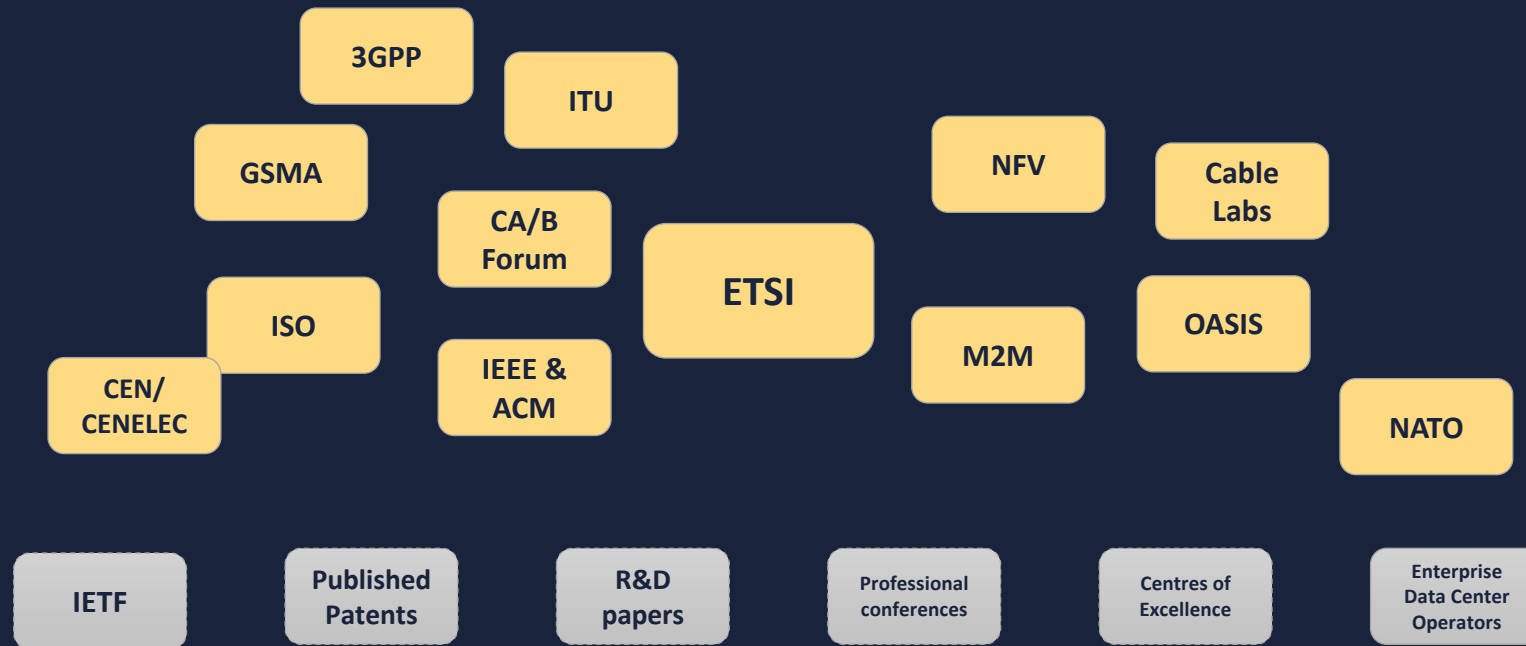
MORE AND MORE EVERYDAY

- MIDDLEBOXES AND INTERCEPTION ONE OF THE MOST ACTIVE/INNOVATIVE SECTORS
- HUGE INCREASE IN MIDDLEBOXES PATENTS FILED WORLDWIDE
- LARGE INCREASE IN FUNDED R&D INITIATIVES, ENGINEERING COURSES AND CONF.
- MORE THAN 10,000 PUBLISHED ACADEMIC PAPERS ON MIDDLEBOXES LAST DECADE
 - HUNDRED OF NEW ONES APPEARING EVERY MONTH
- MIDDLEBOX TOPICS RECEIVING INCREASED ATTENTION
 - PERVASIVENESS IN NETWORK INFRASTRUCTURES, PARTICULARLY MOBILE NETWORKS
 - DISCOVERY AND MANAGEMENT
 - SDN/NFV INSTANTIATIONS
 - CRYPTOGRAPHIC PROTOCOLS
- FUNDAMENTAL COMPONENT OF SHIFT TO 'INTELLIGENCE IN THE NETWORK'

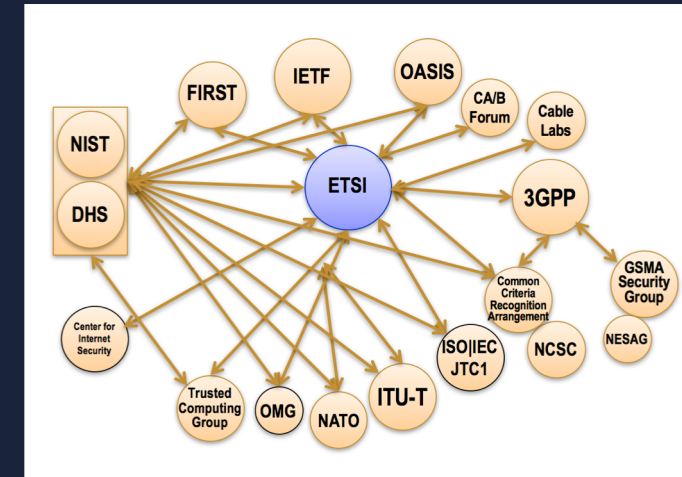
WHAT IS THE ECOSYSTEM OF RELATED ACTIVITIES



THE SHORT VERSION IN AN EVEN BIGGER CYBERSECURITY ECOSYSTEM



AS A REMINDER



GLOBAL STANDARD DEFINING ORGANIZATIONS DEALING WITH CYBERSECURITY

WHAT IS THE PROBLEM BEHIND THE SCENE

PRIVACY vs SECURITY instead of PRIVACY with SECURITY

- DISAGREEMENT ON THE SECURITY MODEL: WHERE TO PLACE SECURITY?
- 'PERVASIVE ENCRYPTION' MOVEMENT
 - AIMS TO CREATE HIGHLY ENCRYPTED TRANSPORT PATHS DIRECTLY BETWEEN END POINTS
 - ALSO TO CREATE MULTIPLE HIGHLY ENCRYPTED STREAMS
 - 2 WAY MODEL → TLS, QUIC, APPLICATION LAYER ENCRYPTION
 - SECURITY ON ENDPOINT AND PLATFORM ONLY
- THE ALTERNATIVE
 - RECOGNIZES THE MANY LIMITS
 - WANTS TO OFFER AN N WAY MODEL IN AN END TO END FORM
 - SECURITY ON ENDPOINT WHEN POSSIBLE, IN THE NETWORK AND ON PLATFORM
- BOTH SIDES HAVE THEIR ARGUMENTS
 - YET WE OBSERVE THE DIFFICULTY TO SPEAK RESPECTFULLY WITH EACH OTHER

EXAMPLES OF RELATED WORK ITEMS

A VERY SMALL EXTRACT FROM AN ABYSSAL AMOUNT OF CONTRIBUTIONS

SDO	« WORKING GROUP »	WHAT	COMMENTS
ETSI	TC CYBER/MIDDLEBOX	5 WORK ITEMS	INCLUDING mcTLS, mbTLS + A HACKATON IN JUNE (ETSI SECURITY WEEK) WE NOTE THE CLASH WITH IETF ON THE USE OF TLS WORD
IEEE	CISG/ETI	REQUIREMENTS FOR PROPER ENCRYPTION TRAFFIC INSPECTION	WE NOTE THE CLASH WITH IETF IN 2016
ITU	SG17/WP3/Q7	TECHNICAL FRAMEWORK FOR SECURITY AS A SERVICE BY OPERATORS	NEW AT ITU
3GPP	SA2 and SA3	ENTRADE	NEW
IETF	SEC I2NSF	CAPABILITY MODELS	I2NSF IS STANDARDISING MIDDLEBOXES AS VNF IN AN SDN/NFV ENVIRONMENT



Thank You!

ARNAUD TADDEI
DIRECTOR, STANDARDS AND ARCHITECTURES
OFFICE OF THE CTO

