V1.1

AI Ecosystem and Critical Security Controls

ETSI AI Security Technical Committee (SAI) Work Items 001 and 002

Tony Rutkowski, tony.rutkowski@cisecurity.org
Rapporteur

AI Ecosystem

ETSI AI Security Technical Committee (SAI), Work Item DTRSAI-001

- **Discovery and organization of the ecosystem forums and activities with hyperlinks to current work**
  - Fora that develop AI techniques, technical standards and operational practices (40++)
  - Major developer forums affecting AI security (22++)
  - Activities for continuous information exchange
  - Centres of excellence
  - Reference libraries, continuing conferences, and publications
  - Heritage sites and historical collections
  - Additional exchange sources and methods
  - National AI security ecosystems

AI Ecosystem

Challenges

- **AI is now Everything, Everywhere, All at Once**
- **AI running code, processes, facilitating computational devices are ubiquitous and exponentially expanding**
- **More than 100,000 AI patents (standards dark matter)**
- **Alleged 100 million AI coders**
- **Almost every company, institution, and standards body are engaged in AI work**
- **AI development, innovation, and deployment is driven overwhelmingly by private sector and marketplace**
- **AI has enormous business, societal, economic, and national security significance**
- **AI is politically popular**
  - Regulation and limits of cybersecurity conformance testing shown in 1967
- **Use of AI gives rise to multiple legal issues, especially tort, IPR, anticompetition, human rights, discovery and conflict of law**
  - COE AI treaty draft released 8 Feb
- **Understand AI vulnerabilities, threats, and attacks, and how they may be different**
- **Trend is toward security standards centricity**
  - Principal emerging AI security framework is Bletchley Agreement and the NCSC+21 guidelines

AI Security Controls

ETSI AI Security Technical Committee (SAI), Work Item DTRSAI-002

01 Inventory and Control of Enterprise Assets
02 Inventory and Control of Software Assets
03 Data Protection
04 Secure Configuration of Enterprise Assets and Software
05 Account Management
06 Access Management Control
07 Continuous Vulnerability Management
08 Audit Log Management
09 Email and Web Browser Protections
10 Malware Defences
11 Data Recovery
12 Network Infrastructure Management
13 Network Monitoring and Defense
14 Security Awareness and Skills Training
15 Service Provider Management
16 Application Software Security
17 Incident Response Management
18 Penetration Testing

- **AI control Safeguards likely similar to those for cloud – See ETSI TR 103 959**
- **Significantly more important that ex-anti certification schemes**
- **Referenced in the NCSC+21 AI security guidelines**
- **CSA is also developing a set of control safeguards for AI**
  - ETSI is collaborating with CSA
- **Initial task is to differentiate AI Implementation Groups and Service Models**