LEONARDO ELECTRONICS

ATM & Airport Cyber Security Management

Increased automation, connectivity, and reliance on digital information have raised concern over the risks inherent in the interconnected nature of the ATM system of systems. It is crucial that ATM systems ensure data security and continuous operational availability in a world of ever-changing cyber threats.

Future operational concepts, such as those developed by SESAR and NextGen, will increasingly rely on new technologies, connectivity methods, and architectures that will entail new vulnerabilities and threats.

Security represents an evolving, ever-changing and persistent challenge to the ATM world and, with the introduction of the Amendment 16th of ICAO ANNEX 17, also a duty for each ATM stakeholder. Since November 2018, each ATM Stakeholder will be obliged to develop and implement measures to protect ATM systems from unlawful interference in accordance with a relevant risk assessment.

LEONARDO SOLUTION

Leonardo IOC (Intelligence Operating Centre) provides intelligence based on real time analysis of open information sources: deep and dark web (obtained through data mining), machine learning algorithms, high performance computing. All those will be integrated with data feeds from select partners.

Leonardo cyber security and intelligence services grant efficient, perimetral and internal security with real-time monitoring of IT and OT infrastructures. Event correlation, and analysis of Customer infrastructures, and critical applications are granted as well such to ensure cyber threats to be proactively managed.

LEONARDO

PERFORMANCE OUTLINES

Leonardo offers turnkey solutions based on analysis of Customer needs including architecture and design specification, implementation, and integration. Leonardo solutions also include design of custom SOCs, secure collaboration solutions, information management. Focus is placed on document classification, protection, and secure web applications. Namely:

- Network and application design & protection
- Endpoint security
- Identity management, PKI, and digital signatures
- Cloud security and virtual environment protection
- Malware analysis
- Critical infrastructure access management and monitoring solutions
- Endpoint and data Integrity protection services

Among some of the most commonly adopted solutions are to be outlined:

- Access control management for applications, systems, and network devices
- User Privilege Management
- Malware Protection
- Secure configuration and Security hardening
- Boundary Protection (Firewall & IDS/IPS)
- Network Security Management
- Secure Data Transfer
- Alarm and Log collection, protection, and monitoring
- Service and Data availability (back-up, redundancy, disaster recovery)
- Vulnerability management (security source code analysis, penetration testing)

Leonardo also grants administrative services including:

- Security infrastructure assessment, design, and review
- Governance, risk, and compliance management
- Business continuity and disaster recovery planning
- Information security awareness and training
- Application security and secure coding

STATISTICAL FEATURES

Leonardo incident response services cover the entire spectrum, from initial incident and threat intelligence to forensic services and advanced malware analysis. The service is aimed to establish nature and origin of cyber attacks. This is achieved via:

- Incident response services identification of the most appropriate containments and reaction strategies
- Reduction of business impact and collateral damages
- Threat intelligence services information
- Forensic services collection, storage, and provision of all evidences

Following statistics are also available:

- Social network analysis
- Network analysis for intelligence and surveillance
- Security prevention & early warning
- Brand protection-reputation analysis
- Fraud & anti-phishing
- Transaction monitoring & alert management

CERTIFICATIONS AND STANDARDS

- UNI EN ISO 9001:2008 “Quality management systems requirements”
- EN 9100:2016 “QMS requirements for Aviation, Space & Defence Organizations”
- ISO/IEC 27001:2013 “Information technology — Security techniques — Information security management systems — Requirements”
- LSR18.6E certified infrastructure (Lampertz room)
- Leonardo LVS (Consorzio RES) accredited to OCSI (Organismo di Certificazione della Sicurezza Informatica)
- NIST Guidelines (sp800-171, sp500-299, Framework for Improving Critical Infrastructure Cyber Security)
- ISO/IEC 27000 family information security management systems

For more information:
infomarketing@leonardo.com
Electronics Division
Via Tiburtina
Km 12.400
00131 Rome - Italy
T +39 06 41501
F +39 06 4131133

leonardo.com

MM08630-03-24

LEONARDO