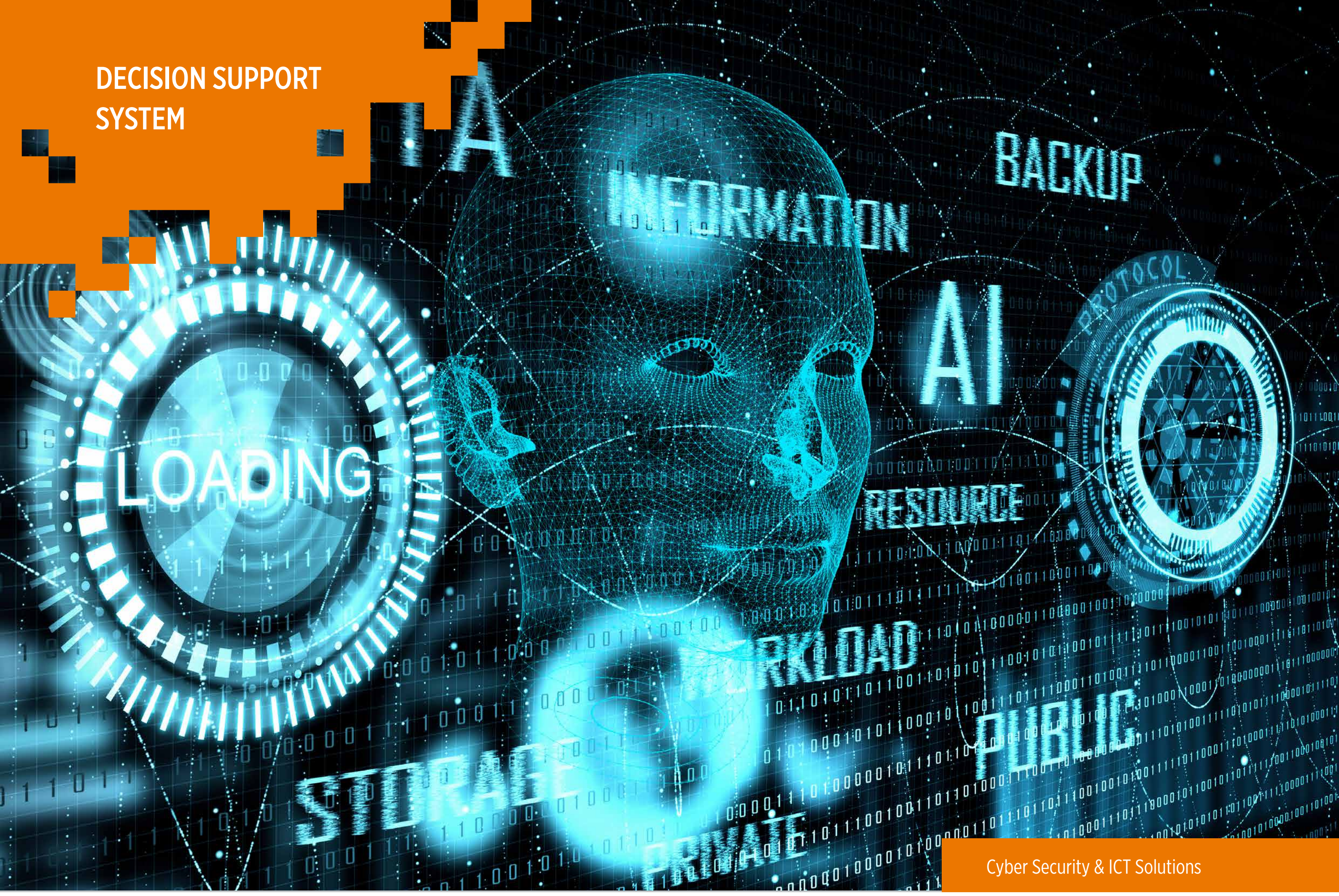


DECISION SUPPORT SYSTEM

Cyber Security & ICT Solutions

ARTIFICIAL INTELLIGENCE DECISION SUPPORT SYSTEM

In a digital economy where defence infrastructures, critical infrastructures and enterprises are progressively opening up to continuous outwards communication, traditional approaches to cyber security are insufficient to respond quickly and adequately to cyber threats in order to minimise the impact on business continuity. These approaches are more technological rather than process oriented, often disconnected from the company business and operational context since they process separately information coming from Threat Intelligence, Business Impact Analysis, and Security Information Event Management systems.

THE DECISION SUPPORT SYSTEM

Leonardo's Decision Support System is based on edge technologies such as Artificial Intelligence and Big Data, Analytics & IoT and takes advantage of the interconnections between heterogeneous cyber sources to actively measure the impact of cyber risks. The system supports organisations to decide on the proper actions to be taken to ensure business continuity and to minimise the consequences of dangerous, damaging cyber incidents.
The system is also based on sophisticated, state-of-the-art tools, skills and investigation experiences acquired in specific cyber defence domains.
Through the correlation of data and information sources traditionally processed separately (threat intelligence, SIEM, Risk assessment, asset management, and SCADA cyber protection), the system measures the impact of threats or cyber attacks at operational and business level and suggests remediation actions in real time, leveraging and learning from previous experiences.

Finally integrated, the reaction process to cyber incidents covers both business and technological aspects. Moreover, Leonardo's teams of certified cyber security and intelligence analysts and consultants are willing to help with their expertise in preliminary and in-depth analysis of suspicious events.

ARTIFICIAL INTELLIGENCE DECISION SUPPORT SYSTEM

LEONARDO APPROACH AND SKILLS

Based on a technological and organisational approach along all steps, Leonardo's Artificial Intelligence Decision Support System operates on decision making and remediation processes relevant to cyber threats that could potentially damage critical infrastructures.

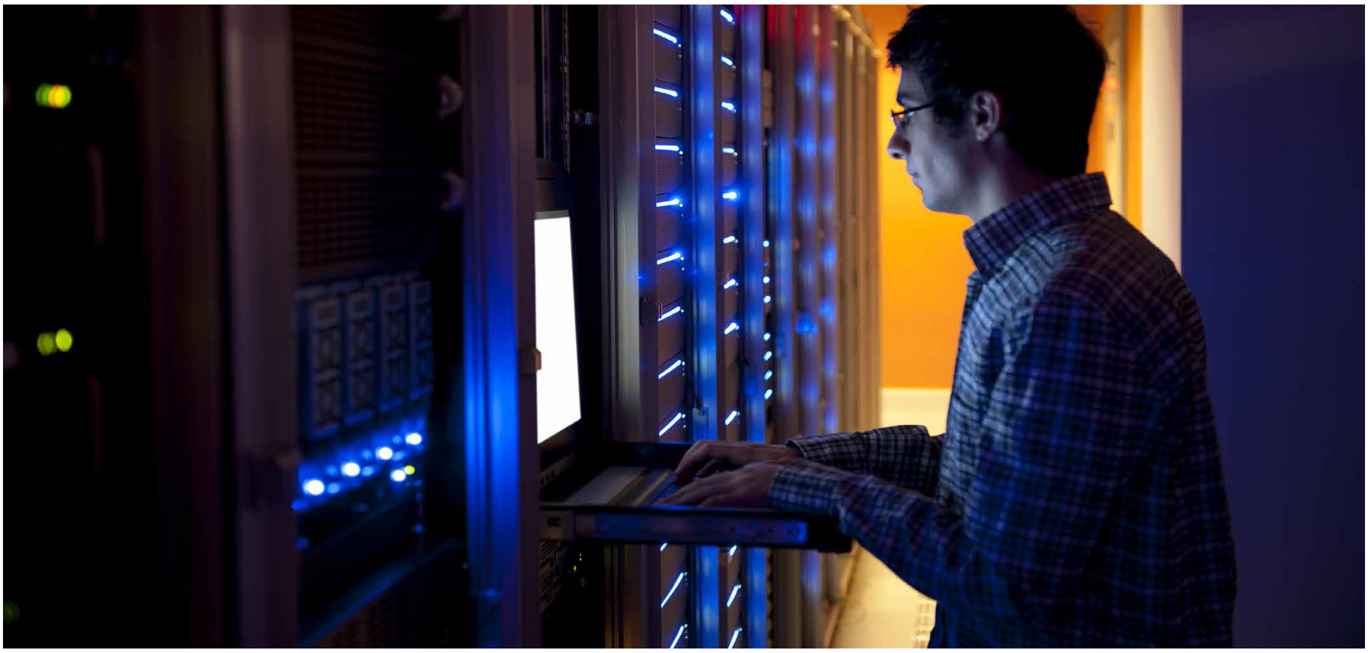
Preliminary analysis: Leonardo's cyber security consultants define, together with the customer, the impact of risks on the organisation's operations, designing both the architecture and the configuration of the AI Decision Support System. The support of Data Scientists helps to produce the necessary data and predictive models for the dynamic assessment of related risks.
Continuos monitoring & event prioritization: SOC operators continuously monitor the security of organisation's IT and OT infrastructures while the DSS system, through dedicated operators, detects and identifies high risk threats of possible cyber attacks.
Cyber threat escalation: DSS operators focus on and take charge of high risk threats. Potentially damaging cyber security events are evaluated both by Threat Intelligence analysts, using open sources information, and by company management, regarding the involved area and its impact on business and operating continuity. At the same time, cyber security operators, supported by artificial intelligence tools, analyse the suggestions generated by the system.

Action & resolution: Through the usage of the operational suggestions provided by the system, intervention decisions are turned into detailed business and technological steps and remediation actions, and are carried out ensuring operational continuity of the organisation under attack.

FUNCTIONALITIES AND TECHNOLOGIES

Leonardo's DSS system uses Artificial Intelligence algorithms and a Big Data Analytics & IoT engine to determine the necessary protection and action steps to be taken in order to neutralise cyber attacks, and interacts continuously with cyber sources that process critical information:

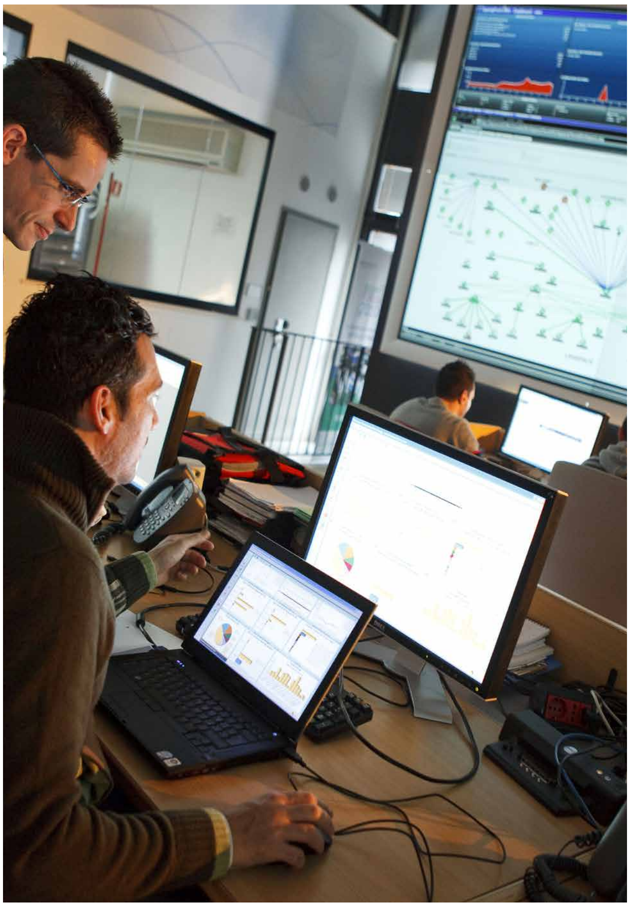
- **Scorecard calculation & prioritization:** automatic and dynamic calculation of a «scorecard» quantifying the effect of threats on IT/OT infrastructure entities at risk and production of an event ranking based on the severity level of the involved risk.
  Business risk calculation: calculation of the actual and potential risk of business and financial loss as a result of cyberattacks that could compromise the organisation's operations.
- **Entities' behavioral & relationships analysis:** complex analysis in a time frame of the behaviour of users linked to individual entities of the IT/OT infrastructure at risk and of the relationships with entities outside the organisation.



- **AI operational suggestions:** automatic generation of operational suggestions for each scorecard with proposed remediation actions to be taken, leveraging the use of artificial intelligence technologies.

The **Big Data & Analytics & IoT** engine, included in the system, enables real-time integration of organisation, assets and Security Governance information with possible threats reported by intelligence systems and anomalies detected by security systems.

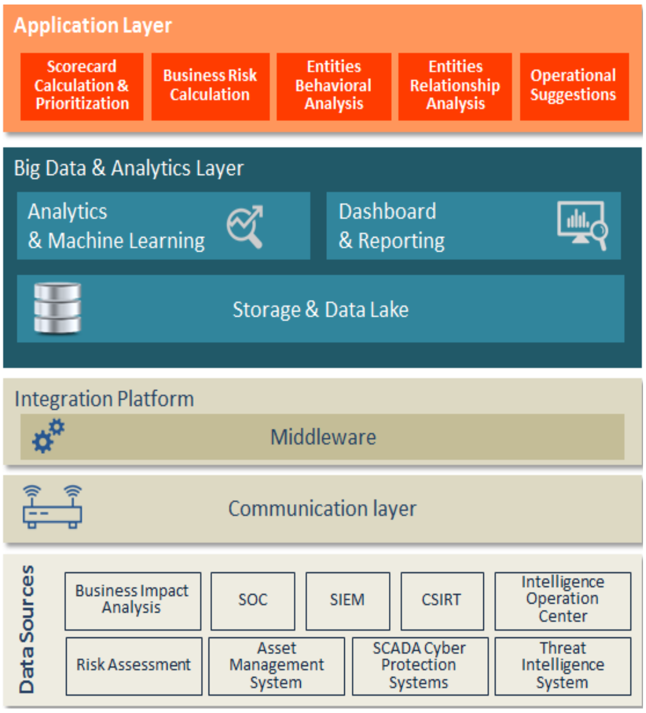
The Artificial Intelligence used by Leonardo's AI Decision Support System generates operational suggestions appropriate for the current situation, especially when the decision making process is not linear and is complex even for the human brain. Leonardo's approach involves the use of semantic reasoning to deduce logical consequences, called inferences, starting from a knowledge base characterised by a unique language which integrates different ontologies coming from heterogeneous contents in terms of source, formats and dimensions.



ARCHITECTURE

The platform architecture includes the following layers:

- **Data sources:** cyber sources that feed operational decisions in order to react to cyber threats and attacks, information related to risk assessment, intelligence and events detected by SIEM systems to protect IT and OT systems.
- **Integration & Communication:** it enables the connection of heterogeneous cyber sources with the processing, correlation and analysis infrastructure of information and events.
- **Big data analytics:** it represents the Big Data & Analytics engine where the data collection, normalisation, analysis and visualization tasks are carried out to support risk scorecard calculation and behavioural analysis.
- **Application:** it includes applications implementing Decision Support functionalities.



Application Layer
Scorecard Calculation & Prioritization
Business Risk Calculation
Entities Behavioral Analysis
Entities Relationship Analysis
Operational Suggestions
Big Data & Analytics Layer
Analytics & Machine Learning
Dashboard & Reporting
Storage & Data Lake
Integration Platform
Middleware
Communication layer
Data Sources
Business Impact Analysis
SOC
SIEM
CSIRT
Intelligence Operation Center
Risk Assessment
Asset Management System
SCADA Cyber Protection Systems
Threat Intelligence System

ARTIFICIAL INTELLIGENCE DECISION SUPPORT SYSTEM

BENEFITS

- Capability to align cyber security management with business priorities, business strategies and core processes essential to company operations.
- Improved analytical and detection capabilities related to threats and potential cyber attacks.
- Quick understanding of potential damages generated by an incident.
- Fast, efficient and synergistic responses in terms of business and technology.
- A team of operators that covers the entire internal and external cyber security life cycle (from threat intelligence analysts, SOC and DSS operators up to the management of the company at risk of attack) integrated, informed and focused on the organisation processes and cohesive in the response phase.
- Protection and fast recovery of the company operating functions.

LEONARDO'S OFFER PORTFOLIO

Leonardo protects Governments, National Critical Infrastructures and National Strategic Industries against cyber threats and attacks using its technology and experience in cutting-edge cyber security and critical IT systems, all crucial for the operation and service continuity for citizens and countries.

Organized into two different lines **Business-driven Cyber Security and Critical Information Systems**, Leonardo's Portfolio leverages the main emerging technologies and the most up to date technological paradigms to offer solutions, platforms and services able to support customers' secure digital transformation.

The Artificial Intelligence Decision Support Systems is part of the Business-driven Cyber Security offer, including:

- **Cyber Protection & Resilience** for governments and critical infrastructures through services, tools and methodologies for the management of the entire threat life cycle and for the resilience of systems and services against cyber-attacks.
- **Intelligence & Investigation** in order to support Law Enforcement Agencies, Blue Lights and Defence in the research, the collection and the analysis of relevant information for investigation activities, strategic intelligence and preventing crime.
- **Cyber Training**: for the creation and simulation of complex cyber-warfare scenarios aiming at training operators in charge of IT/OT system security, both in the civil and military sector.

LEONARDO
SISTEMI PER LA SICUREZZA E LE INFORMAZIONI

For more information please email: ICT-Cyber@leonardocompany.com
Leonardo S.p.a.
Via Laurentina, 760 - 00143 Roma - Italy - Tel: +39 06 50275738 - Tel +39 06 50275685

This publication is issued to provide outline information only and is supplied without liability for errors or omissions. No part of it may be reproduced or used unless authorised in writing. We reserve the right to modify or revise all or part of this document without notice