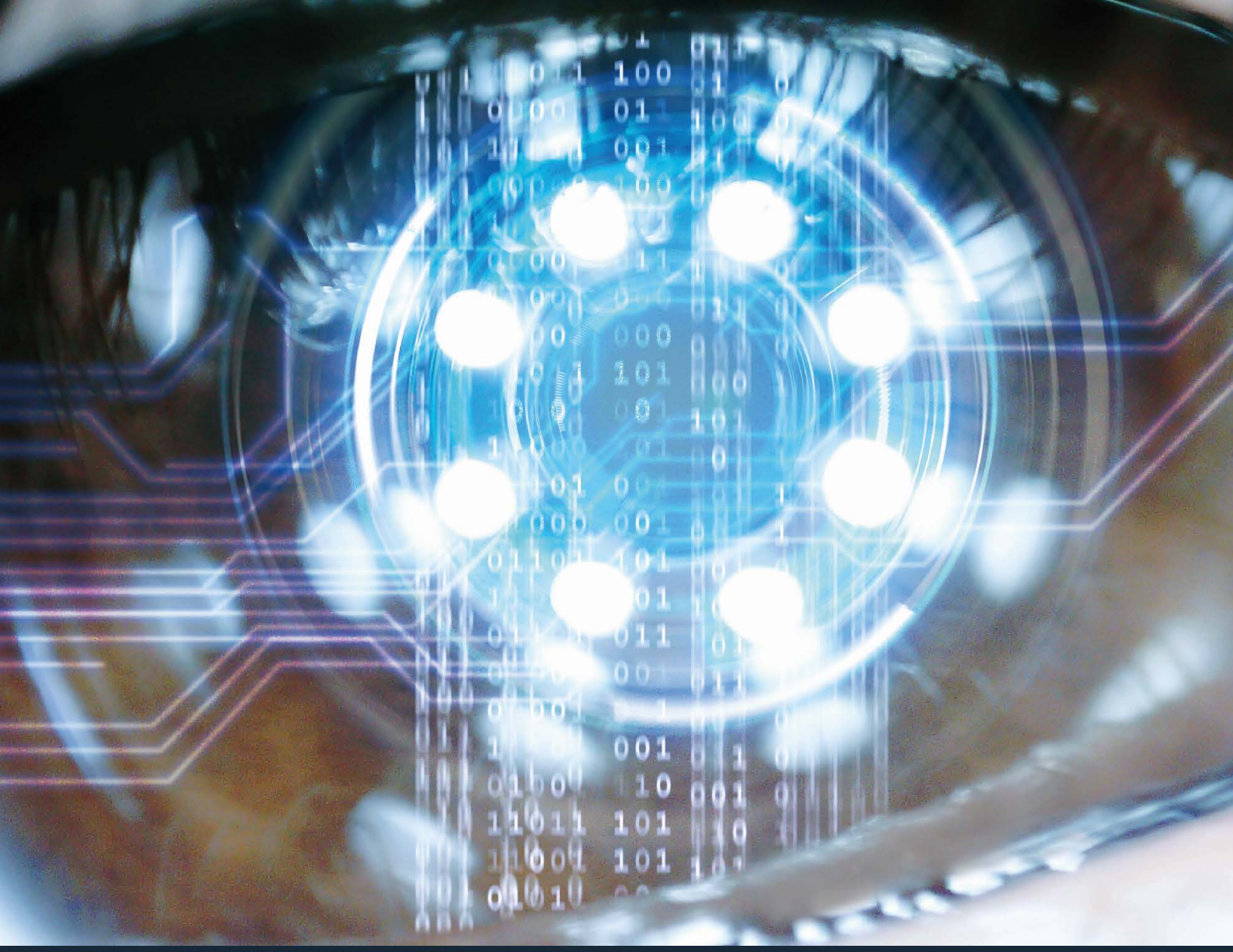


LEONARDO CYBER & SECURITY SOLUTIONS

CYBER SITUATIONAL AWARENESS SYSTEM

LEONARDO

In a digital economy in which institutions and companies are increasingly open to continuous outwards communications, traditional cyber security approaches are often inadequate to effectively respond to cyber threats with enough speed and coverage to minimise impact on the operational continuity of organisations.
These approaches are more technological than process-oriented, often detached from organizations' operational and business context, since they process information from heterogeneous systems separately.

Security teams dedicated to the protection of IT infrastructures are frequently forced to interact with multiple tools, and to perform analyses and correlations with data distributed across several applications. This makes it extremely complex to obtain an indication of the cyber risk to which an organisation is exposed to. This information is however essential to be able to respond promptly and effectively to an attack or an IT incident, prioritising, if needed, the reaction activities according to the impacts the malicious event may have on the organization's assets.

In this scenario, moreover, collecting the information needed to provide management with high-level views clearly and concisely representing the general security status of an infrastructure, can be difficult even for a highly qualified team. This may impact the correct allocation of cyber security investments and may force top management to make critical decisions in a short time based on fragmented information with potential significant consequences on organisation's operations and reputation.

Cyber Situational Awarness System

CYBER SITUATIONAL AWARENESS SYSTEM

To effectively respond to these needs, Leonardo has developed the Cyber Situational Awareness System (CSAS), a complete ecosystem for cyber monitoring and **achievement of high levels of cyber awareness**. The system is specifically designed to:

- keep the **security teams** and **executive profiles** of an organisation informed about what is happening in terms of Cyber security in its operational context through the continuous **collection and analysis of data**;
- support **security analysts investigation processes and company management decision-making** by providing an information centralizing platform that displays executive and technical-operational dashboards.

The platform supports two delivery models: on-premises, with installation of the system at the customer's site, and as a service, whereby the platform functions are delivered remotely.

PROPOSED APPROACH

Given a group of assets to be monitored, the Cyber Situational Awareness System is able to interact with a variety of information sources in order to collect data and information, analyse and correlate them. Through data warehousing functionalities, the CSAS provides centralised access to data through dedicated views for different types of users with the aim of facilitating the decision-making processes of technical and executive profiles.

The proposed approach consists in a **preliminary analysis phase** in which, according to Customer's needs and available technologies, the system configuration is defined, the data sources to be used (SIEM, Threat Intelligence, VA, Ticket, CMDB...) are identified, the desired dashboards are selected from a predefined dashboard catalogue or new dashboards are designed and created.

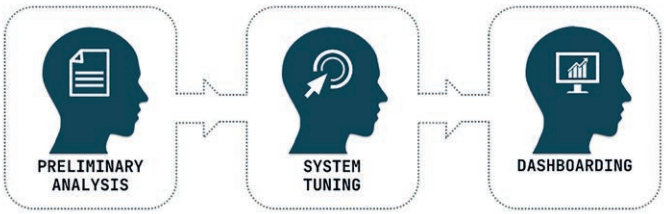
The **connector tuning phase** is preparatory for feeding the system with the heterogeneous data that will populate the technical-operational views and the executive dashboards.

Once the connectors are tuned, in the **dashboarding phase**, users can access user-friendly, interactive and filterable interfaces provided by the platform and populated in real time by the connected systems.

Dashboards contain aggregated information, statistics and performance metrics related to the overall security status of the monitored infrastructure, and can be exported via

reports in various formats. Reports can be executive or operational, depending on the profiles being addressed.
The **executive** dashboards are strategic in nature as they provide top managers with an overview of the organisation in relation to critical metrics and allow to monitor performance against established KPIs, identifying appropriate improvements and opportunities for expansion.

Operational dashboards are designed to monitor and manage processes and activities with a narrower time horizon, a more technical focus and a more granular, vertical view of issues of interest. In both cases, dashboards are a tool that provides periodic information reports to support decision-making processes.



MAIN FUNCTIONALITIES

Through the process described above, the Cyber Situational Awareness System performs the following functions:

- **Support of investigation and research processes** of security teams that have to interact with numerous tools on a daily basis, simplifying the task to make analysis and correlation with data distributed across numerous applications.
  Through interaction with heterogeneous sources and analysis and correlation functionalities, CSAS plays the role of data centralizer and exposes technical-operational overviews for the integrated visualisation of information, contributing to **improve the productivity of security teams and offering support in the investigation process**.

- **Cyber risk definition contribution:** data typically acquired in the context of cyber security do not provide a direct measure of cyber risk thus preventing the achievement of a complete and in-depth knowledge of the security status (cyber awareness). CSAS dashboards provide support in ensuring that the security controls adopted are appropriate to the specific risks faced by the organisation.
- Advanced dashboarding provision, responding to the need, often difficult to address even for qualified security teams, to collect information to generate high-level views capable to represent the organisation's overall security status to management profiles.
  Through the aggregation of data and Business Intelligence tools, CSAS displays dashboards, downloadable as reports, which present significant trends and metrics, providing immediate access to high value information without the need for manual queries and searches.

LOGICAL MODEL AND TECHNOLOGIES

CSAS is based on an advanced analytic engine that interacts with information sources and carries out data collection, normalisation, analysis and correlation operations, storing them in a data warehouse.
The system also includes a knowledge base containing threat intelligence information, fed by heterogeneous sources in this field.
Above these modules, the CSAS has application layers that expose both technical-operational dashboards and dashboards dedicated to executive profiles.
The CSAS relies on advanced technologies for the processing and visualisation of big data and takes advantage of advanced tools, skills and experience in the field of cyber defence developed by Leonardo in the most critical domains.

BENEFITS

- Greater integration of cyber security activities with business priorities, corporate strategies and key processes for the organisation's operation.
- Enhanced analytical and investigative capabilities of cyber-attacks.
- Overall view of the monitored perimeter, through the centralisation of heterogeneous data and information.
- Ability to represent information according to the specific users' needs through configurable executive and technical-operational dashboards.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

MM09136 09-23

leonardo.com

LEONARDO