# esra
Enhanced Security Risk Analytics
by aizoOn

Cognitive Risk Management Platform

Context

The digital transformation process has created **interconnected environments.**

Thanks to them **it is possible to supervise all the production processes, control the operative flows and program all the production's plants.** All departments benefit from this connectivity: administration, logistics, production, sales.

Operations become extremely rapid, downtimes are minimized and the **environment becomes a connected, sustainable and intelligent ecosystem.**
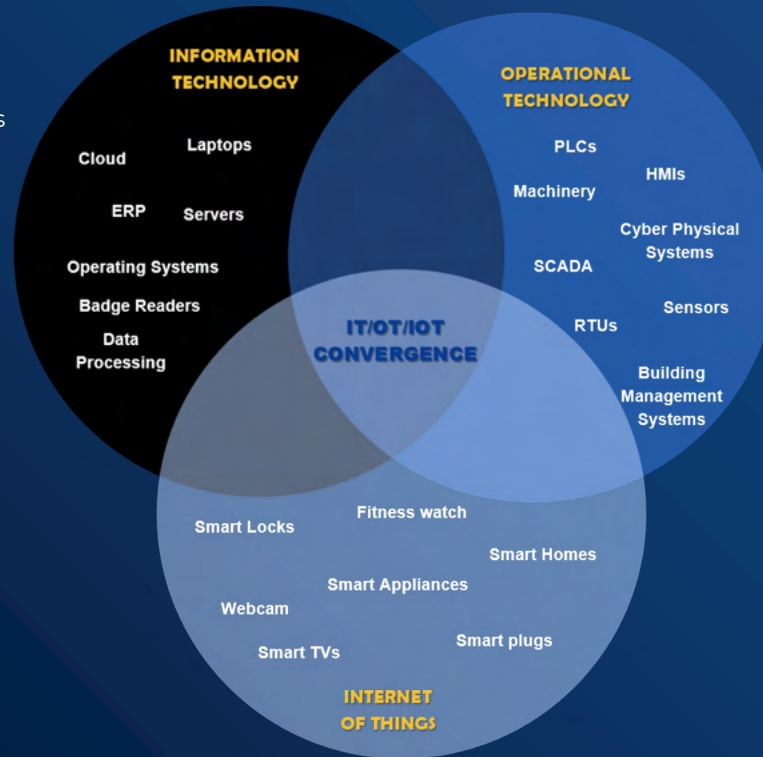
The **integration between IT, OT and IOT** determines a new hyper-connected vision but also pushes all to consider **new management issues that are by "nature" linked to Cyber Security.**

- The optimization of the security process is one of the milestones. The major vulnerability today comes from the extensive use of the Internet, **Wi-Fi** or the new **5G** network and we still do not know exactly the critical issues in terms of security.

Risk Evaluation

The IT risk assessment helps the company to determine which are the vulnerabilities in an infrastructure.

It is possible to understand the effectiveness of the existing countermeasures only after the identification of those risks.

This gives to the company the chance to think about new potential countermeasures and their potential effectiveness in relation to what they have after the risk assessment.

Furthermore, having the rate of each severity of the risks identified allows the company to decide and prioritize each countermeasure and have an idea of the costs of their implementation compared with the potential consequences.

An efficient evaluation of the risk will create a comprehensive overview of the strengths and weaknesses of the organization.
This overview can be used to improve the cyber security roadmap preventing a possible attack knowing exactly the risks and the weaknesses.
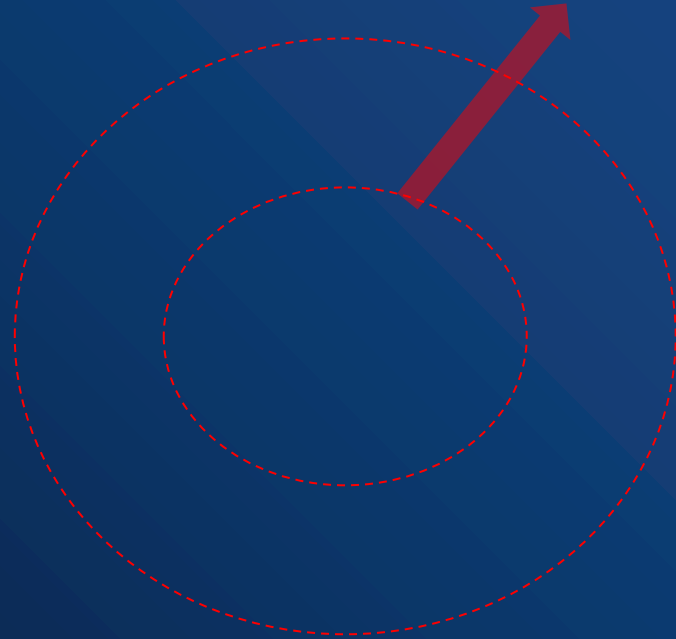
A collaborative tool

Why ESRA?
Because Enterprise Risk Management with **ESRA** is **pervasive** and **data-driven**, becoming an integral part of every decision and process.

Artificial Intelligence and Machine Learning to help not only identify risks in the best way but also to make risk management widespread in all the organization's activities.

Enhanced Security Risk Analytics

ESRA is a data-driven Risk Management platform. It quantifies the risk based on the corporate organizational structure, starting from the real and live infrastructure.

- Provides a **data-oriented risk assessment** and compliance assessment;

- Automatically **detects the assets inventory** of the analyzed network perimeter (internal and external);

- Rebuilds **all network communications between assets** and creates a data-driven infrastructure model;

- It allows to produce a **risk mitigation roadmap** for achieving the expected risk and compliance objectives;

- **"Light" setup using a probe for traffic monitoring** and non-invasive agents for asset inventory;

- **Integrated reporting area** to have an extraction of specific views and export of raw data for internal use or c-level meetings.
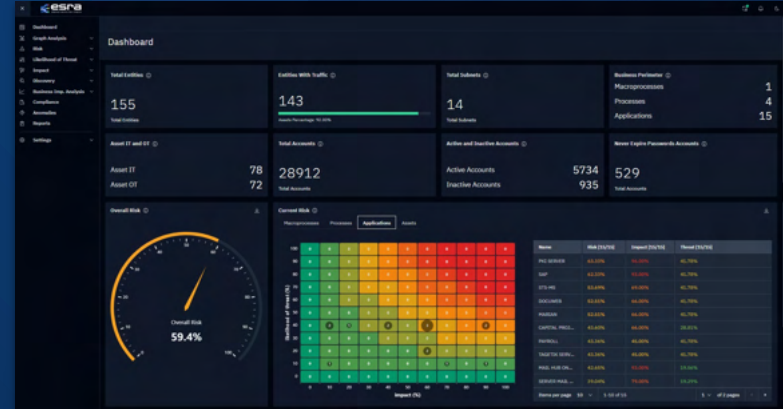
Data-driven Cyber Risk Assesment

Through a **digital-twin approach** of the corporate IT and OT infrastructure, ESRA is able to fully estimate the risk from each asset in the organization and map it on the organizational structure. Threats and impacts are extended to all assets involved by observing communications between them.

Risk and Traffic

Esra enables a capillary view of **internal and external network traffic**.

The representation of each communication between assets is totally interactive. The platform has a powerful capacity to filter information allowing the company to have a deep level of detail for each analysis scenario.

An intuitive and in-depth view of the data to evaluate the risk from cyber threats or possible business impacts.

Data-driven Cyber Risk Assesment

Risk at 360°

ESRA has a multi set of views, extractions and reporting designed to represent: **risks, threats, impacts**, in relation to each macro-processes, processes, applications and single assets.

It also provides single summary and detailed views of how every threat can be propagated and every potential impact across the entire infrastructure.

Indicators and What-if scenarios

ESRA provides a precise measurement of threat indicators detected on each individual asset.

Quantifying the possible threat allows the company to formalize a potential risk for single business processes related to the organizational structure with a different approach: starting from the assets involved.

Some threat indicators

Obsolescence, classification of CVEs, Configuration or misconfiguration, domain controllers and analysis of firewall rules show the company the classification of the possible IT risk based on the individual assets.
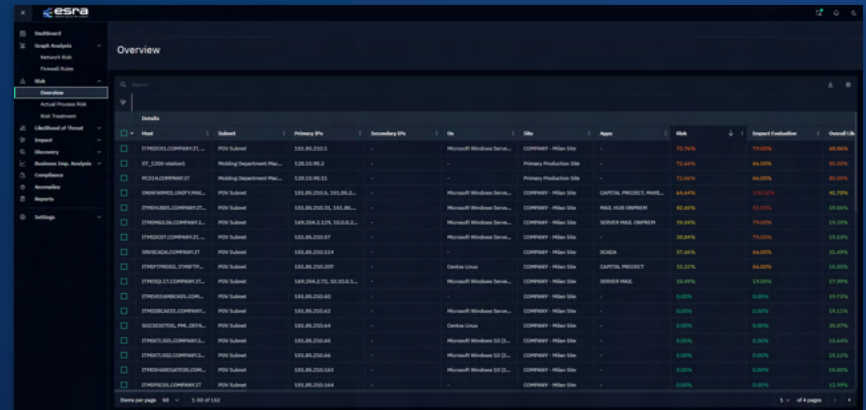
Indicators and What-if scenarios | Firewall

ESRA acquires corporate firewall rules and makes them an important path for risk analysis. The identification – and a clear visualisation - of deny/allow or superfluous firewall rules, compared with the actual real-time traffic between the assets, gives the company the right cyber security approach for better correlation rules, reviewing them for a significant reduction in risk.

**Firewall rules**

Segregation Index

Indicators and What-if Scenarios

What-if based Mitigation Planning

Through a What-if approach scenario it is possible to build mitigation plans, based on predefined risk objectives.

ESRA shows:

- the **selection of interventions by priorities** and single needs;

- the composition of a **risk management plan** associated with regulatory elements;

- the projection of the **residual risk** compared to the current one.
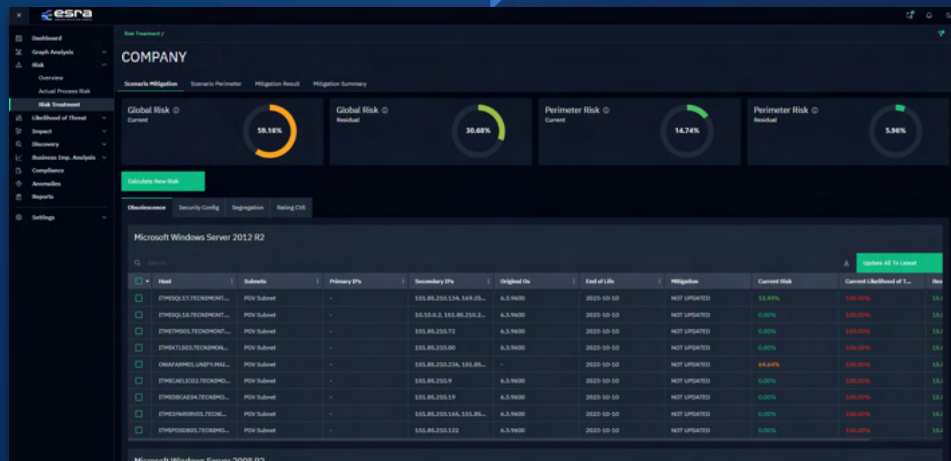
Impact

ESRA allows the view of the inventory of the applications impacts in relation of each business unit and a shareable **Business Impact Analysis** with an immediate view on the propagation of Impacts.

ESRA allows to have knowledge of the **applications most stressed** by operational or highly specialized processes, with an immediate view on the **propagation** of Impacts.

Business Impact Analysis
Centralized management for an impact assessment up to the maximum level of detail for each business process:

- **Evaluation of Loss of data and Unavailability by application**, on a predefined and customizable impact matrix;
- Evaluation by dimension: financial, reputational, operational, and so on

Through ESRA it is possible to have a centralized vision of the impact and understand how this propagates on the business:

- **Complete view of the combined and cascading impact on the organizational structure;**
- Understanding of **impact propagation;**
- View **application dependencies.**
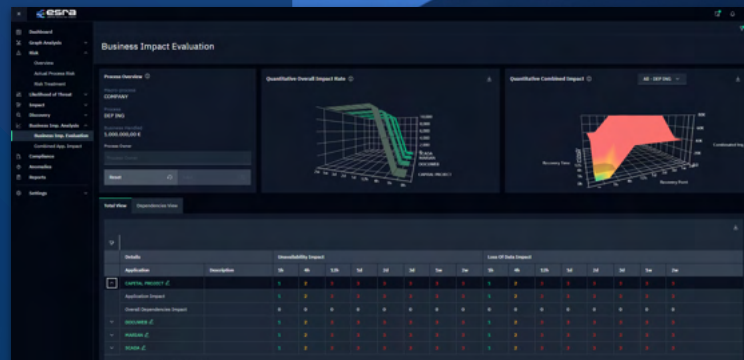
Compliance

The adoption of ESRA **natively solves a wide area of obligations required by regulations and standards.** It carries a large set of technical and organizational indicators integrated with international reference standards, performing integrated assessment activities without requiring widespread campaigns to detect the status of controls.

Maturity Levels

Maturity VS Target
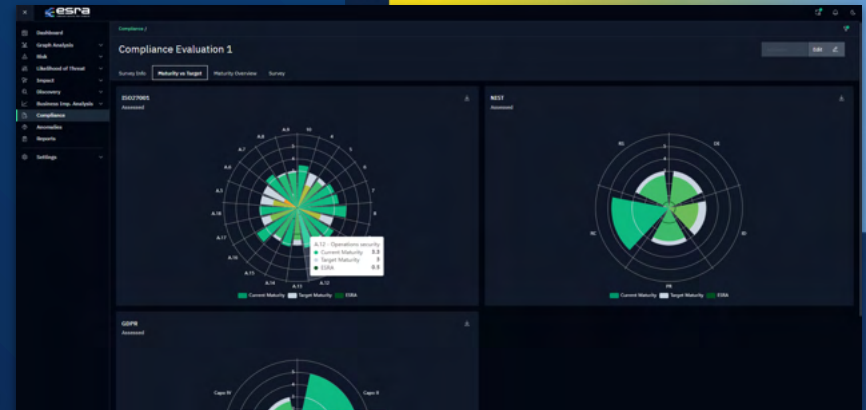
Risk Management

IN SHORT

Understand the risk status of your infrastructure and how any mitigations impact the overall scenario;

Understand **possible threats**, distribution and propagation of impacts;

Fully **understand the intrinsic and hidden dynamics** of your architecture;

Analyze network traffic and define firewall rules, in a simple and intuitive way;

Create risk mitigation scenarios to be reported in operational plans.

Pdf and Word reporting system starting from the contents of the various pages;

Management of multiple risk assessments;

Allows to **download all the contents**, both graphic and tabular.

esra

Enhanced Security Risk Analytics
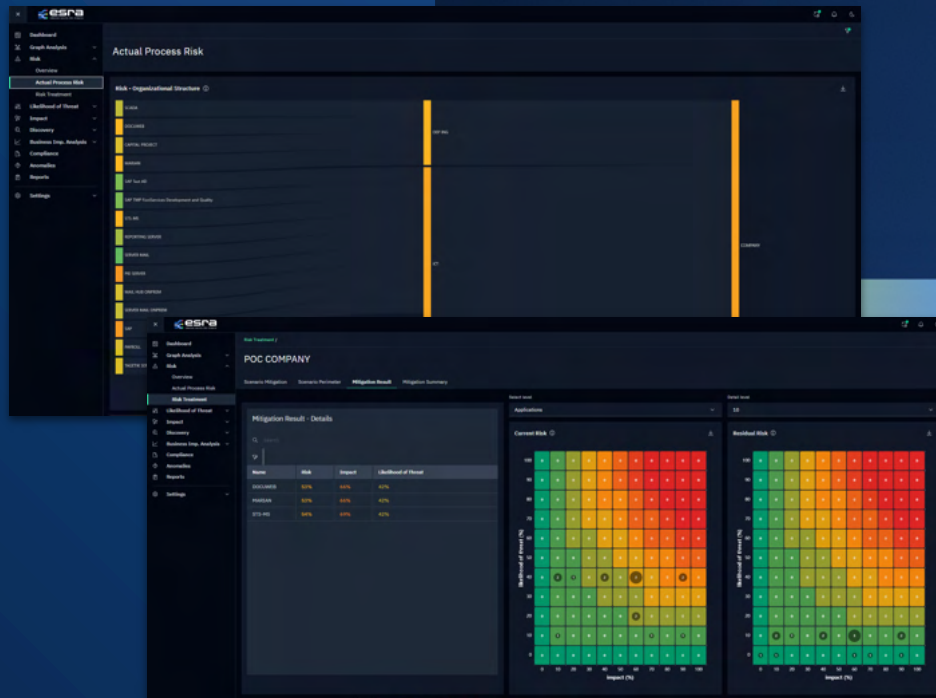
aizoongroup.com

AUSTRALIA
Sydney NSW | Adelaide SA

EUROPE
Aosta ITA | Bari ITA | Bologna ITA
Catania ITA | Cuneo ITA | Genova ITA
Milano ITA | Roma ITA | Terni ITA | Torino ITA
Sheffield UK | Zurigo CH

USA
New York NY | Cambridge MA

AIZOON
TECHNOLOGY & CONSULTING

AUSTRALIA
EUROPE
USA