Business Partner IBM
Authorized Software Value Plus
B2B Integration
Security

INNOVERY
INNOVATION DISCOVERY

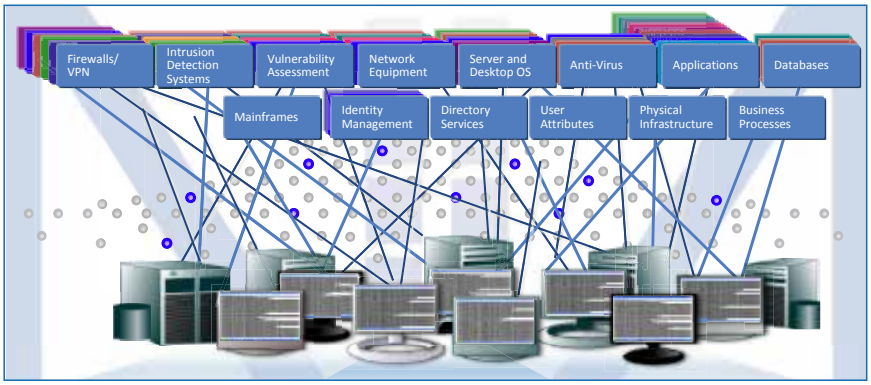
INNOVERY PROACTIVE DECISION SUPPORT SOLUTION

Inside every Company there are millions of electronic events that they must be handled in order to manage potential risks and threats.

Every internal and external company resource (a person, an hardware device, a software application) can represent a source of risk or criticality;

The activity of those resources generates, on different systems, information that must be managed, stored and correlated with the objective of "create knowledge", that it must be used as support for making decisions in case of specific events occur.

SIEM platform aren't able to discover new statistical relationship between critical events.



CRITICALITIES

- **Correlate events and identify complex events**
  Identify those cases that analyzed "one by one", they have a low risk possibility, but if they occur contextually, they could represent high risk situations.
- **Define priorities**
  The rules for managing criticalities may change depending on the alert conditions, by the definition of new policies, etc. That's why the level of attention with respect to some events may change along the time.
- **Criticality Management**
  The right management of criticality depends in a very strict way on the experience of the operator.
- **Identify the best practices**
  Analyze the effectiveness of the developed actions, learning from the past and share the best practices with the rest of the Organization.

The principle: a structured methodological approach

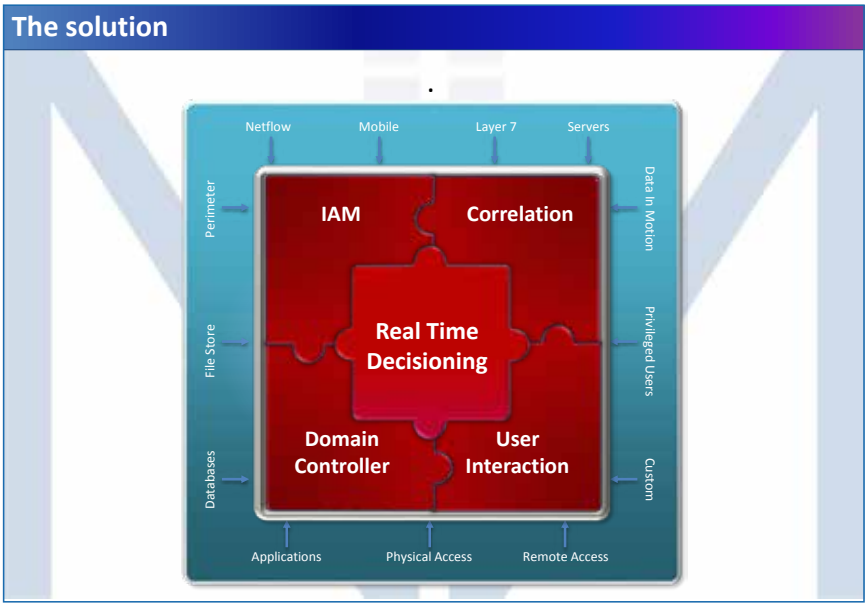
A DECISION SUPPORT SYSTEM IS NEEDED

- **Real time**
- **Integrate**
- **Dynamic**
- **Modular**
- **Complete**
- **Based on COTS**

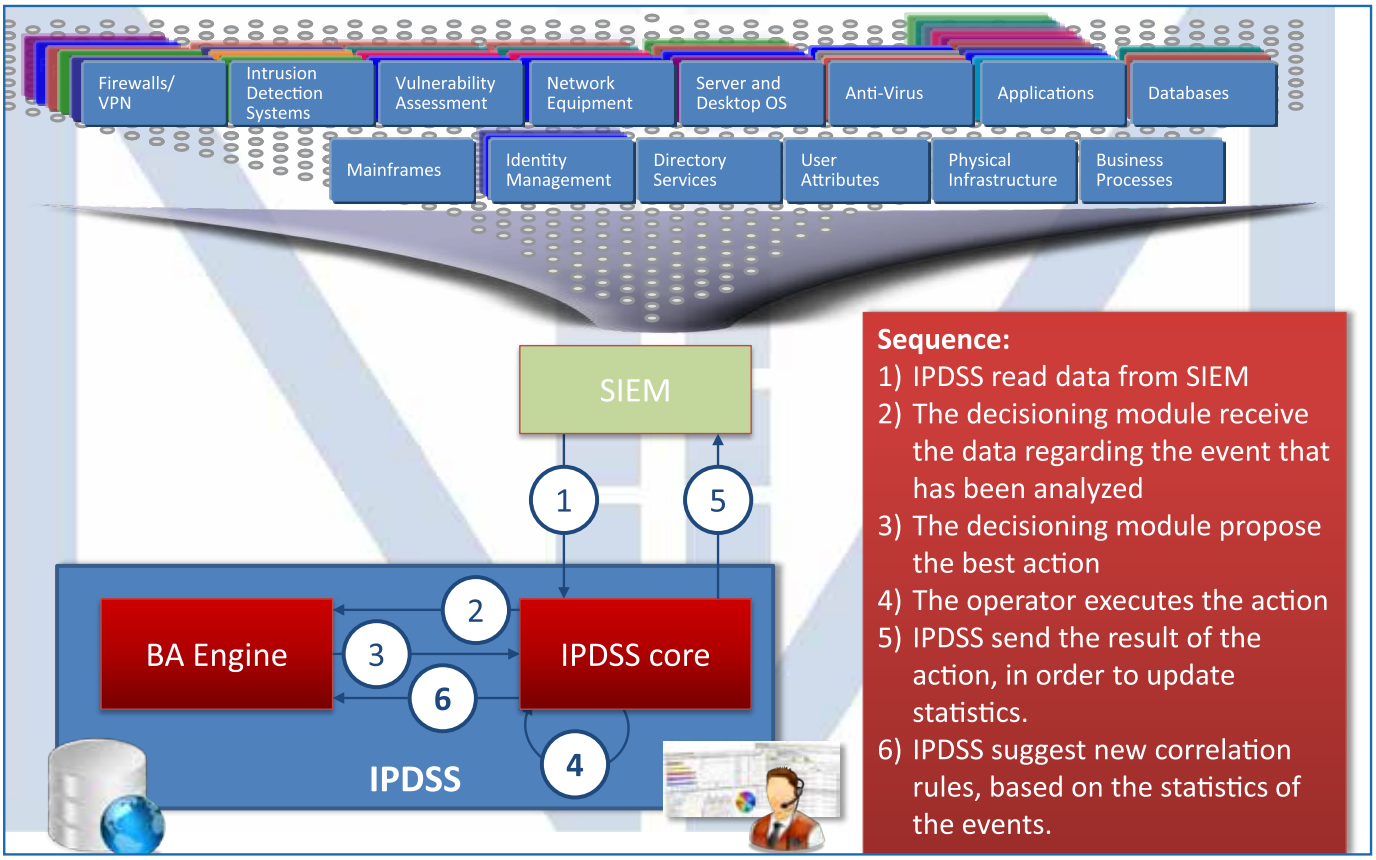
THE BENEFITS

- **Qualitative**
  - Homogenization of the effectiveness of the decisions
  - Flexibility
  - Best practice as a company patrimony
  - Better visibility and efficiency for SIEM solutions
- **Quantitative**
  - Reduction of the time/costs management
  - Resources optimization

The solution



How it works: the sequence



Sequence:

1) IPDSS read data from SIEM
2) The decisioning module receive the data regarding the event that has been analyzed
3) The decisioning module propose the best action
4) The operator executes the action
5) IPDSS send the result of the action, in order to update statistics.
6) IPDSS suggest new correlation rules, based on the statistics of the events.

Why it is important…

The most important characteristics of this solution are:

1. It is very important to manage in a unified and homogeneous way the different systems (hardware and software) that they could generate alerts/critical events within the company.

   This allows to manage procedures/mechanisms that are not only based on specifics alerts depending on the system to monitor.

2. The "knowledge" needed to answer to the different alerts/critical events is moved to an "expert system", that it would be able to learn by the feedbacks received on the executed actions.

   This allows to provide a very qualified service, also when the operators do not own high level of competencies.

3. SIEM solutions aren't able to automatically generate new correlation rules.

   This solutions allow analysts to discover new statistical relationships between correlated events.

To whom it is important…

The proposed solution is specifically important for those companies where:

- they need to control very strictly the "health" of their (many)
- hardware/software systems;
- they don't want to use necessary high qualified resources in order to answer to every alert/critical event generated by the different systems;
- it is extremely difficult to describe through simple procedures, managed by resources not highly qualified, the necessary troubleshoot in order to answer to the alert/critical event messages;
- the definition of the "best actions", that are consulted when an alert/critical event occurs, evolves along the time depending on different matters.

What really makes it different from the others…

Normally the other solutions are based on "Decision Tree", whose schema related to resolution/management remains static along the time.

The IPDSS application, taking advantage on a Real Time Decisioning component:

- associates to an "expert system" an easy-to-use web-based graphical user interface, that do not require specific knowledge for the operators, neither competences in troubleshooting;
- uses self-learning mechanisms in order to enforce and extend own "knowledge data base";
- takes advantage on the Internet powerfulness for communicating and monitoring the "health status" of the under control systems;
- improve efficiency and visibility of SIEM platforms suggesting new correlation rules.

Brescia (Sede Legale)
Via Creta, 78
25124 Brescia
Phone: +39 030 8373600
Fax: +39 030 8373630

Milano
Via Borsieri, 22
20159 Milano
Phone: +39 02 6685549
Fax: +39 02 700596750

Roma
Via Antonio Giunio Resti, 63
00143 Roma
Phone: +39 0651963439
Fax: +39 030 8373630

Madrid
C/María Tubau, 3 planta 5
28050 Madrid
Phone: +34 91 3587229
Fax: +34 91 3589890

Mexico City
Av. Paseo de la Reforma, 404
Juarez Cuauhtemoc
Distrito Federal 06600
Phone: +52 55 91711904

www.innovery.net • info@innovery.net