Cymerius is a security incident response tool used by teams in the Security Operations Centre (SOC). It allows you to collect security alerts from different detectors in a unified interface, to perform sorting and analysing by combining the work of computers and humans to manage the response to the security incident. Whilst respecting the standards and procedures defined by the organisation by orchestrating the security tools.

We help your SOC teams to prioritise, analyse and respond effectively to security incidents that your organisation is facing.

- Situational knowledge with a state in real time of the supervised system and a capacity of prioritisation of incident processing based on their impact on critical services or resources necessary for the successful completion of an operational mission. Cymerius also offers a shared vision of the security status of the hypervised system(s). The supervised system is represented in topological and cartographic form.

- The coordination of multidisciplinary security teams during the life cycle of the incident (CSIRT, SOC, NOC, analysts, managers, experts, level 1 operators non-experts) by the implementation of a workflow, analysis interfaces, as well as manual procedures or automatic response.

- The automation of responses with “tailored” reaction plans automatically operable or by the operator's hand. The association of a specific plan to an incident typology favours the application of procedures for processing the organisation’s incidents by security teams. Automation is particularly suitable for repetitive, time-consuming and recurring tasks identified at SOC level.

- The orchestration or unified management of a large number of security tools in a single interface (SIEM, NIDS, sandboxes, vulnerability scanner, CMDB, ticketing tools). This makes navigation and the analysis work of the operators easier and allows a capitalisation of all available information in connection with an incident at Cymerius level.
Positioning and role of **Cymerius**

**Cymerius**

(orchestrate)

(feed)  (enrich)

Log Management (SIEM, IDS, etc...)

Database

Security tools

Information System

---

### Your benefits

**Reduce the required time needed to process a security incident**
The combination of orchestration and automation capacities of Cymerius allows operators to:
- **Identify the incidents** to be treated as a priority depending on the impacts on operations and in accordance with the security policy.
- **To operate** the various security tools in the resolution framework.
- **To work collaboratively** on the analysis of the incident.

**Control the risk of human error in processing of alerts**
Cymerius allows you to associate to each alert one or several reflex cards validated at organisation level.
- **Access to knowledge bases and guided procedures** (which can be activated manually or automatically).
- **Reducing the risk** of unilateral decisions.

**Full reporting & dashboarding**
Cymerius centralises all information related to the security status of the system and the teams in charge of hypervision.
- **Users benefit from visual views** that allow them to measure the activity managed at SOC level.
- The information recorded - for example the detailed history of the management of an incident - can be used for **audit procedures** by the investigation teams.

**Preservation of investments**
Cymerius can interface with any security tool:
- **Flexibility of integration** at SOC or platform level.
- **Guarantee** not to question the IT investments of past or planned security.