redShift

RED·SOC

Monitoring, detection and response to *security incidents*

Managing is making decisions!
Decisions are based on information, which has to be available when and where it is needed!

Information *security*

Organizations are increasingly exposed to digital risk, not being able to cope with the resources (technological and/or human) to face the threats that proliferate every day.
RedShift, in order to respond to the current needs of its customers/partners, has designed a service that intends to guarantee solutions tailored to the requirements of each business reality.

RedSOC

Through the establishment of a set of monitoring (NOC) and security (SOC) capabilities, RedShift provides personalized support services to partners from its operations center (redSOC).
From redSOC, information systems, services and critical assets are monitored, assessed and protected against cyber threats that may jeopardize their integrity, confidentiality and availability.

Areas of *operation*

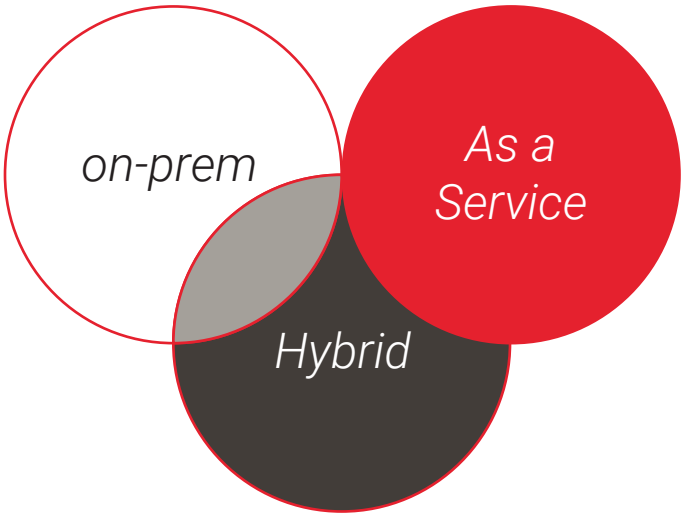
The plan of implementation of redSOC consists of the following phases:

Identification and configuration of use cases;
Incident management plan definition;
Incident monitoring, detection, and response;
Two levels of response.

Operating

Operating Models

The SOC service can be operationalized using one of three different models:



On-prem
Internally in the Organization.

As a Service
Provided from an external Operations Center, responsible for the operation and management of the Organization's SOC.

Hybrid
Balancing services between internal and external capabilities.

Operating profiles

SOC Manager - Responsible for the redSOC operation.
Service Delivery Manager - focal point for client and internal teams, managing the contracted service level.
1st Line Analyst - Incident monitoring, triage and treatment.
2nd Line Analyst - Detailed analysis of more complex incidents, supporting corrective actions.

After going into production, the redSOC service guarantees:

Monitoring of use cases according to the recommended incident life cycle and established SLA's;
Situational dashboards;
Periodic activity reports.

Contacts
+351 217 230 635 . redshift.global . sales@redshift.pt