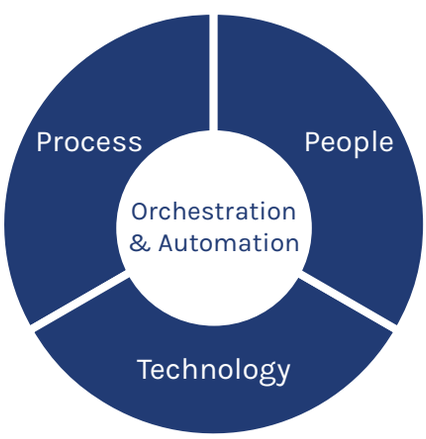
Aiuken Cybersecurity

VSOC
Virtual Security Operations Center

VSOC Basics

A SOC is a centralized unit that deals with security issues at an organizational and technical level. Its main components are processes, people, and technologies that interact to provide security services to an organization.



A modern SOC has the following basic functions:

- Threats and vulnerabilities management affecting organizations' assets
- Security monitoring and audit to prevent and detect internal or external threats
- Security devices maintenance and management to guarantee the functional operations of the SOC
- Cybersecurity Incidence Response management, to analyze, mitigate and respond to security incidents that happen to the organization
- Security compliance management in order to match the external regulations and constraints affecting the organization
- Security training to face new threats, incorporate new technologies and become more effective and efficient.

Concept

The VSOC, or Virtual SOC model, is a set of complementary, modular and scalable solutions designed to give customers the ability to: anticipate, detect and respond to advanced threats, along with the provision of robust solutions to mitigate risks and provide efficient management of their ICT customers' vulnerabilities.

Aiuken VSOC services allow the team responsible for the operation of customer security services the following: integration within the existing 3ng managed security domain in Aiuken, providing tools, solutions and predefined management processes including vulnerability assessment, forensics, ethical hacking, CSIRT, metrics and KPIs definition for reports, and an advanced risk management consulting team.

Security Cyber Intelligence capacities in Aiuken are based on its protection systems and managed cloud technologies, integrating the sophisticated intelligence embedded in each technology through our expertise and a VSOC centralized portal to provide access and visibility to the customer. The Protection system is integrated by three elements:

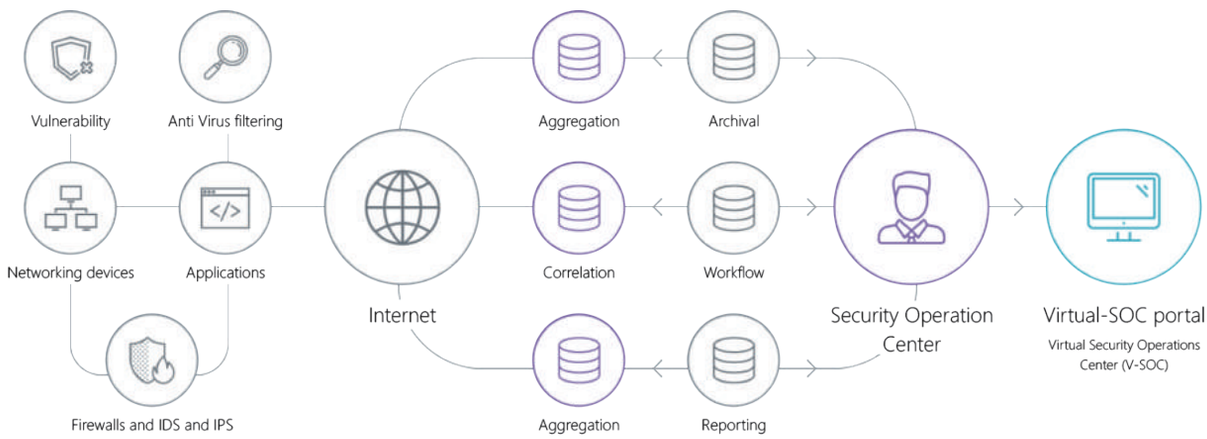
- Cloud-based SIEM: which receives the data (logs) coming from the different customer security devices, IT and communication systems. The collected events are correlated in real-time, enriching the events with external sources that provide context information regarding threats. In the process, alerts are generated and ranked for their analysis.
- CPE-based managed services provide the information required
- Global intelligence functionalities and tools are provided by customer and partner SOCs, vendors, and others, helping in the operation of the protection system

VSOC Architecture

The VSOC is integrated by a cloud-based set of technologies and products that, managed by a combination of local and remote teams, offer the service information and capabilities through integrated portals that may be deployed at customer's and partners' sites.

The information is collected through the Internet and aggregated in virtual technology platforms to be correlated.

The process is managed by an expert team, helped by workflow tools that implement tested procedures which guarantee the quality of the service.
The platform allows conducting all the operations required: aggregation, correlation, analysis, reporting.
Portals are customized to reflect customers' services and SLAs, providing real-time and historic information that facilitates security management, operation, and reporting.



VSOC Services

Such services are offered over multiple devices and technologies provided by several vendors to cover customer needs.
The initial proposed service categories are:

- SOC services
- Managed Security services
- Cloud Security Services
- Compliance/Analytics
- Professional & Consultancy services

Aiuken Cybersecurity

+34 912 90 98 05

www.aiuken.com

Location:
Avda. de la Hispanidad, nº6
Madrid, Spain