Spidernext - SOAR

Spidernext SOAR is an advanced Security Orchestration, Automation and Response (SOAR) solution.

It allows the capture and analysis of events and security IOCs, as well as establishing the automation of the response, interconnecting if necessary with other solutions and tools, with which you can exchange information or request the execution of actions to deal with events or incidents of security.

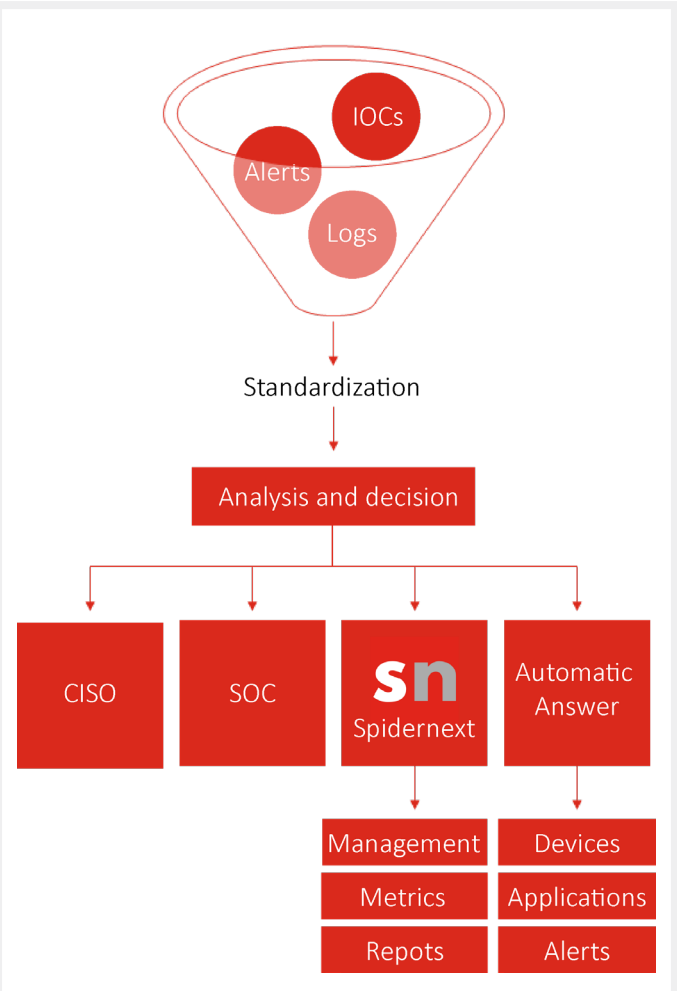
Capabilities

Response to security incidents: Immediate and automated response to security events and incidents, limiting their possible impact on the organization.

Automation of security operations: Through the definition of workflows, it allows the automation of security operations, such as analysis, audits, verifications and other recurring processes, which will influence an improvement in protection.

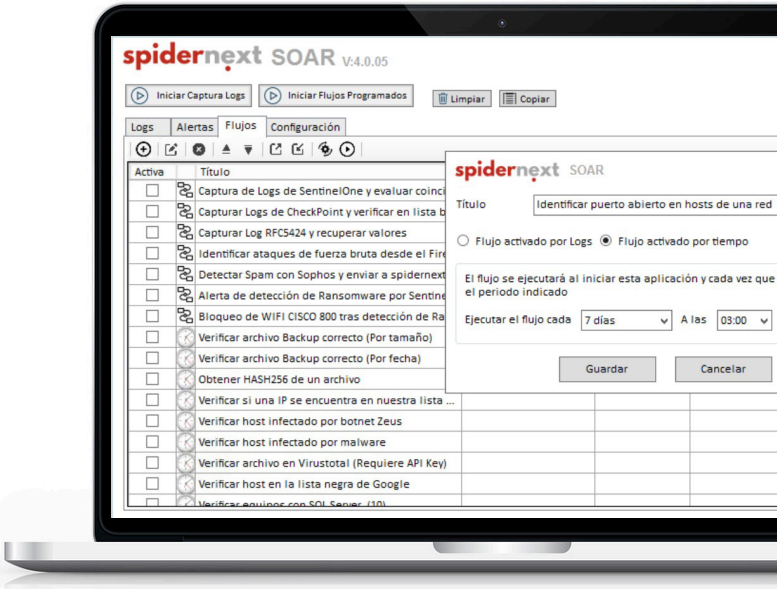
Identification and management of threats and vulnerabilities: The centralization and correlation of capabilities, allow the simple identification of vulnerabilities and events.

Higher performance and productivity: Process automation frees up resources and makes IT, SOC and SecOps teams work more efficiently.



Work smarter, speed up audits and incident response with process automation.

Organize security workflows and automate tasks in seconds to streamline and empower your SOC.



Features and functionalities

Obtaining information and IOCs

- UDP Logs (RFC 5424, RFC 3164, DSF and others).
- Network infrastructure information.
- Information on Operating Systems and users.
- Information of the implemented applications.
- Information and events of other solutions.

Operations

- Carrying out operations with securities received.
- Assignment, grouping, classification and evaluation of data and information.
- Operations with network equipment management information.
- Sending alerts to the centralized platform.
- Sending notifications by email.
- Show messages and alerts.

Normalization

- Normalization of the data received by the information sources.
- Normalization of the format of the Logs.

Interconnections

- Query and send instructions to network electronics (SSH, SNMP and others).
- Direct interconnection with the NMAP tool and use of its more than 600 NSE scripts.
- Bidirectional integration with EMMA of the CCN-CERT.
- Interconnection with security solutions (SIEMs, PAMs, DLPs and others).
- Interconnection with third-party applications.
- Consumption of services and APIs of third parties.

Verifications

- Comparison of data and values obtained.
- Pattern checking and regular expressions.
- Verification according to file information.
- Check availability of assets.
- IOC verification.

Export

- Sending data and information to other solutions, APIs or files.