¿Quienes somos?

CiN Consejo Interuniversitario Nacional

SUBCOMISIÓN DE CIBERSEGURIDAD

COMISIÓN DE CONECTIVIDAD Y SISTEMAS DE INFORMACIÓN

¿Qué es un SOC?

Un centro de operaciones de seguridad (SOC), a veces denominado centro de operaciones de seguridad de la información o ISOC, es un equipo interno o externo de profesionales de seguridad de TI que supervisa toda la infraestructura tecnológica de una organización

¿Por qué implementar un SOC?

El principal beneficio de operar un SOC es que unifica y coordina las herramientas, las prácticas y la respuesta a incidentes de seguridad. Esto generalmente da como resultado mejores medidas preventivas, una detección de amenazas más rápida y una respuesta más rápida, más efectiva y más rentable a las amenazas de seguridad.

Otro beneficio es que generalmente viene acompañado de políticas de seguridad

Herramientas comunes en el área de comunicaciones

Herramientas de monitoreos: Nagios® ZABBIX Xymon System Monitoring Grafana SHADOWSERVER

Herramientas de logs: logstash {GRAYLOG2

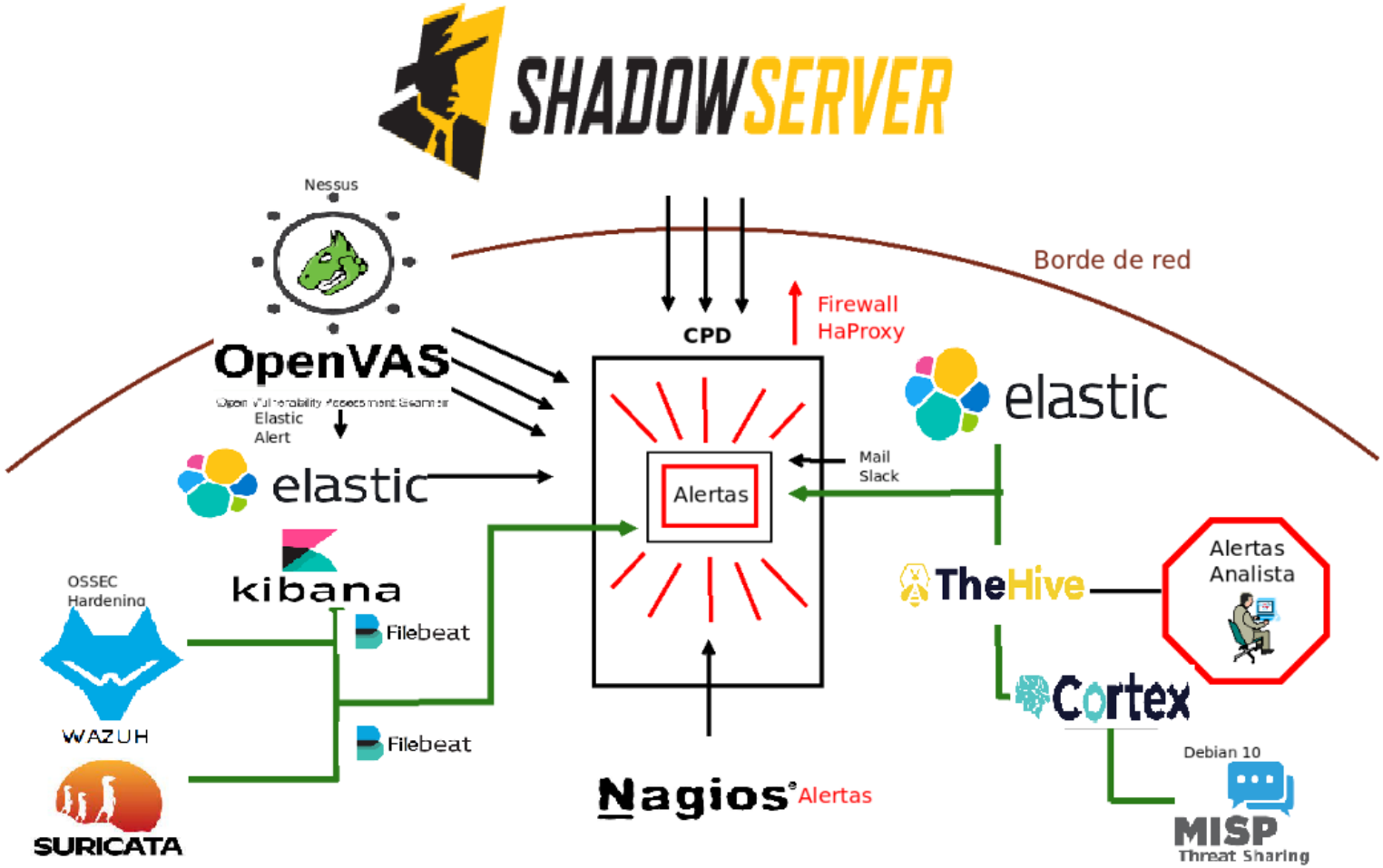
Herramienta de tickets: GLPI itop easy service management osTicket Support Ticket System OTRS

Lineamientos implementación del SOC

Utilizar herramientas open source
Reducir la cantidad de vistas
Incorporar:

Herramienta de gestión de riesgos
Herramienta de gestión de incidentes
Herramienta de análisis de vulnerabilidades
Herramienta de recoleccion y distribucion de informacion

CiN


SHADOWSERVER
Nessus
Borde de red
CPD
Firewall
HaProxy
OpenVAS
Elastic
Alert
elastic
elastic
Mail
Slack
Alertas
kibana
OSSEC
Hardening
Filebeat
Filebeat
WAZUH
SURICATA
TheHive
Alertas
Analista
Cortex
Debian 10
MISP
Threat Sharing
Nagios
Alertas

MUCHAS GRACIAS

Preguntas?

Pueden encontrarnos en:

- subcociberseg@campus.ungs.edu.ar
- https://www.cin.edu.ar