NETWORK CYBER SECURITY MONITORING

FOLLETO

www.tssc.mx

Network CyberSecurity
Monitoring

Introducción

NCSM (Network Cyber Security Monitoring) es una solución **NDR** que combina **IDS de alto rendimiento**, **análisis profundo de tráfico** y **correlación de inteligencia de amenazas** para ofrecer **visibilidad integral de la red.**

Está orientada al **monitoreo continuo**, la **detección de amenazas avanzadas** que evaden controles perimetrales y la **integración con plataformas SIEM**. Su arquitectura **flexible (física o virtual)** permite adaptarse a organizaciones de cualquier tamaño, desde oficinas remotas hasta grandes datacenters.

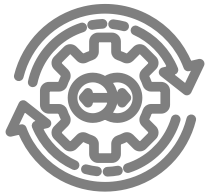
Propuesta de Valor

Detección Multi-Motor

Utiliza Suricata como motor IDS con soporte para múltiples fuentes de reglas comerciales (ET Pro, Snort VRT) y open source (abuse.ch, CISA KEV) para identificar amenazas conocidas y emergentes.

Análisis Profundo de Tráfico

NTOPNG proporciona Deep Packet Inspection (DPI), análisis de flujos y detección de anomalías de comportamiento para identificar actividad sospechosa que evade firmas tradicionales.

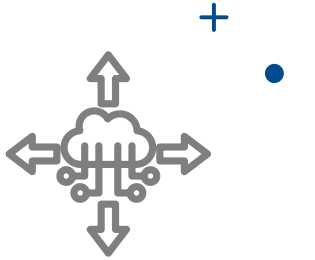


Integración SIEM Nativa

Envío de alertas normalizadas a plataformas SIEM líderes como Wazuh, CrowdStrike, Splunk y QRadar, enriqueciendo la visibilidad del SOC sin herramientas adicionales.

Bajo Costo de Propiedad

Basado en pfSense (FreeBSD) y componentes open source, eliminando costos de licenciamiento de sistema operativo y maximizando el ROI.



Despliegue Flexible

Appliances físicos o virtuales desplegables en oficinas centrales y remotas mediante captura de tráfico SPAN/TAP desde switches y firewalls.

Integraciones

NCSM está diseñado como sensor que se integra con el ecosistema de seguridad existente, enviando alertas a plataformas SIEM para correlación y respuesta.

wazuh.

splunk>

CROWDSTRIKE

IBM QRadar

Fuentes de Threat Intelligence

NETWORK CYBER SECURITY MONITORING

Caso de Uso

Detección de Comunicación C2 (Command & Control)

Escenario

Un endpoint comprometido por malware establece comunicación con un servidor de Command & Control para recibir instrucciones y enviar datos robados.

Detección NCSM

Indicador	Motor de Detección	Severidad
Conexión a IP en blacklist Feodo	Suricata + Threat Intel	CRITICAL
Dominio generado algorítmicamente (DGA)	Suricata ML Rules	HIGH
Patrón de beaconing periódico	NTOPNG Anomaly Detection	HIGH
Tráfico TLS con JA3 conocido como malware	Suricata JA3	HIGH

Resultado

Alertas enviadas al SIEM en tiempo real. El equipo SOC identifica el endpoint comprometido mediante correlación con logs de EDR y ejecuta contención en menos de 15 minutos.

NETWORK CYBER SECURITY MONITORING

GRACIAS

ventas@tssc.mx