Ficha Técnica
NCSM

Solución NDR (Network Detection and Response)

Producto:	NCSM
Versión de documento:	1.0.0
Tipo de Documento:	Ficha Técnica
Fecha de elaboración:	23 de agosto de 2025
Autor:	Postech

Network CyberSecurity
Monitoring

FICHA TÉCNICA

Solución NDR (Network Detection and Response)

Producto:	NCSM Network Cyber Security Monitoring
Versión de producto:	2.1
Tipo de Documento:	Ficha Técnica
Fecha:	21 de julio de 2025
Clasificación:	Comercial
Contacto:	ventas@postech.us

Tabla de Contenido

1. Información General del Producto

Identificación de la Solución

Nombre del Producto	Network Cyber Security Monitor (NCSM)
Versión Actual	1.0
Fabricante	Postech
Tipo de Solución	Network Detection and Response (NDR) / IDS de Red
Base Tecnológica	pfSense + Suricata + NTOPNG
Sitio Web	www.postech.us

1.1 Descripción General

NCSM (Network Cyber Security Monitor) es una solución de detección y respuesta de red (NDR) basada en appliances físicos o virtuales que proporciona visibilidad completa del tráfico de red, detección de amenazas mediante IDS/IPS de alto rendimiento, y análisis de comportamiento de red. La solución integra pfSense como sistema operativo base, Suricata como motor IDS con múltiples fuentes de inteligencia de amenazas, y NTOPNG para análisis profundo de tráfico.

La plataforma se integra nativamente con soluciones SIEM centralizadas como Wazuh, CrowdStrike Falcon, Splunk y IBM QRadar, permitiendo correlación avanzada de eventos y respuesta coordinada a incidentes de seguridad.

1.2 Problema que Resuelve

Visibilidad de Red Limitada:

Proporciona inspección profunda del tráfico de red (DPI) y análisis de flujos para identificar amenazas que evaden controles perimetrales.

Detección de Amenazas Avanzadas:

Utiliza múltiples motores de detección con rulesets comerciales y open source para identificar malware, C2, exfiltración y movimiento lateral.

Puntos Ciegos en la Red:

Mediante captura de tráfico (SPAN/TAP) desde switches y firewalls, elimina los puntos ciegos en oficinas centrales y remotas.

Integración con SOC Existente:

Envía alertas normalizadas al SIEM centralizado, enriqueciendo la visibilidad del SOC sin requerir herramientas adicionales.

1.4 Propuesta de Valor

Pilares de Seguridad Cubiertos

Pilar	Cobertura	Mecanismos
Confidencialidad	Alta	Cifrado TLS para gestión, HTTPS para alertas, segmentación de red
Integridad	Alta	Checksums de reglas, logs inmutables, validación de configuración
Disponibilidad	Alta	Arquitectura redundante opcional (CARP), monitoreo de salud

Beneficios Principales

BENEFICIOS CLAVE

✓ Detección de amenazas en tiempo real con múltiples motores de análisis
✓ Visibilidad completa del tráfico norte-sur y este-oeste
✓ Integración nativa con plataformas SIEM líderes del mercado
✓ Bajo costo total de propiedad (TCO) con componentes open source
✓ Despliegue flexible: appliance físico, virtual o híbrido
✓ Threat Intelligence comercial y open source integrada
✓ Mapeo automático a frameworks MITRE ATT&CK

2. 2. Funcionalidades Principales

2.1 Detección de Intrusiones (Suricata IDS)

NCSM utiliza Suricata como motor principal de detección de intrusiones, proporcionando análisis de tráfico en tiempo real con soporte para múltiples fuentes de reglas comerciales y open source.

Ruleset	Proveedor	Cobertura
ET Pro	Proofpoint	Malware, C2, Exploits, Policy
Snort VRT	Cisco Talos	Vulnerabilidades, Malware
Feodo Tracker	abuse.ch	Banking Trojans, Botnets
SSL Blacklist	abuse.ch	Certificados SSL maliciosos
URLhaus	abuse.ch	URLs de distribución de malware
CISA KEV	CISA	Vulnerabilidades explotadas

2.2 Análisis de Tráfico (NTOPNG)

NTOPNG proporciona análisis profundo del tráfico de red mediante Deep Packet Inspection (DPI), identificación de aplicaciones Layer 7, y detección de anomalías de comportamiento.

Capacidad	Descripción
Deep Packet Inspection	Análisis de contenido de paquetes con motor nDPI
Análisis de Flujos	NetFlow v5/v9, sFlow, IPFIX nativo
Identificación de Apps	Más de 300 aplicaciones y protocolos identificables
Detección de Anomalías	Baseline de comportamiento y alertas de desviación
Blacklist Correlation	Comunicación con IPs/dominios maliciosos conocidos

2.3 Tipos de Amenazas Detectadas

AMENAZAS CUBIERTAS

✓ Malware y Ransomware (comunicación C2, descarga de payloads)
✓ Explotación de vulnerabilidades (CVEs activos)
✓ Movimiento lateral y escalación de privilegios
✓ Exfiltración de datos (DNS tunneling, ICMP tunneling)
✓ Comunicación con botnets y C2 servers
✓ Escaneo de puertos y reconocimiento de red
✓ Ataques de fuerza bruta (SSH, RDP, SMB)
✓ Violaciones de política de red

2.4 Integración con SIEM

NCSM envía alertas y eventos a plataformas SIEM centralizadas utilizando múltiples protocolos y formatos estándar de la industria.

SIEM	Método	Formato	Puerto
Wazuh	Wazuh Agent	JSON (EVE)	1514/TCP
CrowdStrike	HTTP Collector	JSON	443/HTTPS
Splunk	Syslog + HEC	CEF/JSON	8088/HTTPS
IBM QRadar	Syslog	LEEF/CEF	514/UDP
Elastic Security	Filebeat	JSON (ECS)	5044/TCP

3. Requisitos Técnicos y Arquitectura

3.1 Perfiles de Appliance

NCSM-COMPACT (Oficinas Remotas)

Componente	Especificación
Throughput	Hasta 500 Mbps
CPU	Intel Core i5 / AMD Ryzen 5 (4 cores)
RAM	16 GB DDR4
Almacenamiento	256 GB NVMe SSD
Red	2x 1GbE (Management + SPAN)
Usuarios Soportados	50-200 usuarios

NCSM-STANDARD (Oficinas Medianas)

Componente	Especificación
Throughput	Hasta 2 Gbps
CPU	Intel Xeon E-2300 / AMD EPYC (8 cores)
RAM	32 GB DDR4 ECC
Almacenamiento	512 GB NVMe SSD + 2TB HDD
Red	4x 1GbE + 2x 10GbE SFP+
Usuarios Soportados	200-1,000 usuarios

NCSM-ENTERPRISE (Datacenters / HQ)

Componente	Especificación
Throughput	Hasta 10 Gbps
CPU	2x Intel Xeon Gold / AMD EPYC (32+ cores)
RAM	128 GB DDR4 ECC
Almacenamiento	1TB NVMe (OS) + 4TB NVMe (logs)
Red	2x 1GbE (Mgmt) + 4x 10GbE / 2x 25GbE
Usuarios Soportados	1,000-10,000 usuarios

3.2 Métodos de Captura de Tráfico

Método	Descripción	Uso Recomendado
SPAN Port	Puerto espejo en switch	Oficinas remotas, <1Gbps
Network TAP	Dispositivo físico de captura	Datacenters, enlaces críticos
Port Mirror	Similar a SPAN (terminología vendor)	General, switches enterprise
Inline TAP	TAP con bypass para IPS activo	Cuando se requiere bloqueo

3.3 Compatibilidad

Dispositivos de Red Soportados

Categoría	Fabricantes/Productos
Firewalls	Palo Alto, Fortinet, Check Point, Cisco ASA/Firepower, pfSense
Switches	Cisco Catalyst/Nexus, Juniper, Arista, HP/Aruba, Dell
Routers	Cisco ISR/ASR, Juniper MX, Mikrotik
Cloud	AWS VPC Mirroring, Azure vTAP, GCP Packet Mirroring

4. Seguridad y Cumplimiento

4.1 Certificaciones y Frameworks

Framework	Estado	Cobertura
ISO 27001	Compatible	Controles de seguridad de la información
NIST CSF	Compatible	Funciones: Identify, Protect, Detect, Respond
MITRE ATT&CK	Integrado	Mapeo de TTPs en detecciones
PCI-DSS	Compatible	Requisitos de monitoreo de red
CIS Controls	Compatible	Controles críticos de seguridad

4.2 Protección de la Plataforma

Hardening del Sistema

CONTROLES DE SEGURIDAD

✓ Hardening de FreeBSD según CIS Benchmarks
✓ Firewall de host con reglas restrictivas (deny by default)
✓ Actualizaciones de seguridad automatizadas
✓ Acceso administrativo solo por HTTPS/SSH
✓ Logs de auditoría inmutables
✓ Soporte para autenticación RADIUS/LDAP

5. Soporte y Servicios

5.1 Modelo de Soporte

Nivel	Disponibilidad	Tiempo Respuesta	Canales
Crítico (P1)	24/7/365	15 minutos	Tel, Email, WhatsApp
Alto (P2)	24/7/365	1 hora	Tel, Email, WhatsApp
Medio (P3)	Lun-Vie 8-20h	4 horas	Email, Portal
Bajo (P4)	Lun-Vie 9-18h	24 horas	Email, Portal

5.2 Modelo de Licenciamiento

Modelo	Base de Cálculo	Incluye
Por Appliance	Número de appliances desplegados	Hardware, Software, Soporte
Por Throughput	Gbps de tráfico monitoreado	Escalabilidad flexible
Enterprise	Paquete integral ilimitado	Todo incluido + Premium

6. Casos de Uso

6.1 Detección de Comunicación C2

Escenario:
Un endpoint comprometido establece comunicación con un servidor de Command & Control para recibir instrucciones y exfiltrar datos.

Detección NCSM:

Indicador	Motor	Acción
Conexión a IP en blacklist Feodo	Suricata + TI	Alerta CRITICAL
Dominio DGA detectado	Suricata ML	Alerta HIGH
Patrón de beaconing	NTOPNG Anomaly	Correlación SIEM

Resultado:
Alertas enviadas al SIEM en tiempo real. El equipo SOC identifica el endpoint comprometido y ejecuta contención en menos de 15 minutos.

6.2 Detección de Exfiltración de Datos

Escenario:

Un atacante utiliza DNS tunneling para exfiltrar datos sensibles evadiendo controles de firewall tradicionales.

Detección NCSM:

Suricata detecta consultas DNS con patrones anómalos (longitud excesiva, alta frecuencia). NTOPNG identifica volumen de tráfico DNS inusual desde un endpoint específico. Correlación en SIEM dispara alerta de exfiltración.

Resultado:
Exfiltración detenida antes de pérdida significativa de datos. Investigación forense completa con captura de tráfico.

4. Resumen de Especificaciones

Categoría	Especificación
Producto	Network Cyber Security Monitor (NCSM) v1.0
Tipo	Network Detection and Response (NDR) / IDS
Fabricante	Postech
Base Tecnológica	pfSense + Suricata + NTOPNG
Despliegue	Appliance Físico, Virtual (VMware, Proxmox, KVM)
Throughput Máximo	Hasta 10 Gbps (perfil Enterprise)
Rulesets Soportados	ET Pro, Snort VRT, Feodo, URLhaus, SSL Blacklist, CISA KEV
Integraciones SIEM	Wazuh, CrowdStrike, Splunk, QRadar, Elastic, Sentinel
Captura de Tráfico	SPAN Port, Network TAP, Port Mirror
Frameworks	ISO 27001, NIST CSF, MITRE ATT&CK, PCI-DSS, CIS
Soporte	24/7 (P1/P2), Email, Teléfono, WhatsApp

Para más información: **www.postech.us** | support@ncsm.mx |