PostecH

Technical Specifications NCSM

NDR (Network Detection and Response) Solution

Product:	NCSM
Document version:	1.0.0
Document Type:	Technical Specifications
Date of preparation:	August 23, 2025
Author:	Postech

Network CyberSecurity
Monitoring

TECHNICAL SPECIFICATIONS

NDR (Network Detection and Response) Solution

Product:	NCSM Network Cyber Security Monitoring
Product version:	2.1
Document Type:	Technical Specifications
Date:	July 21, 2025
Classification:	Commercial
Contact:	sales@postech.us

Table of Content

1. General Product Information 3
   1.1 General Description 3
   1.2 Problem it Solves 3
   1.4 Value Proposition 4
      Covered Safety Pillars 4
      Main Benefits 4
2. Main Features 5
   2.1 Intrusion Detection (Suricata IDS) 5
   2.2 Traffic Analysis (NTOPNG) 5
   2.3 Types of Threats Detected 6
   2.4 Integration with SIEM 6
3. Technical Requirements and Architecture 6
   Appliance Profiles 6
      NCSM-COMPACT (Remote Offices) 6
      NCSM-STANDARD (Medium-sized Offices) 7
      NCSM-ENTERPRISE (Datacenters / HQ) 7
   3.2 Traffic Capture Methods 7
   3.3 Compatibility 8
      Supported Network Devices 8
4. Security and Compliance 8
   4.1 Certifications and Frameworks 8
   4.2 Platform Protection 8
      System Hardening 8
5. Support and Services 9
   5.1 Support Model 9
   5.2 Licensing Model 9
6. Use Cases 9
   6.1 C2 Communication Detection 9
   6.2 Data Exfiltration Detection 10
4. Specifications Summary 10

1. General Product Information

Solution Identification

Product Name	Network Cyber Security Monitor (NCSM)
Current Version	1.0
Manufacturer	Postech
Solution Type	Network Detection and Response (NDR) / Network IDS
Technological Base	pfSense + Suricata + NTOPNG
Website	www.postech.us

1.1 General Description

NCSM (Network Cyber Security Monitor) is a network detection and response (NDR) solution based on physical or virtual appliances that provides complete visibility into network traffic, threat detection using high-performance IDS/IPS, and network behavior analysis. The solution integrates pfSense as its base operating system, Suricata as its IDS engine with multiple threat intelligence sources, and NTOPNG for in-depth traffic analysis.

The platform integrates natively with centralized SIEM solutions such as Wazuh, CrowdStrike Falcon, Splunk, and IBM QRadar, enabling advanced event correlation and coordinated response to security incidents.

1.2 Problem it Solves

Limited Network Visibility:

It provides deep network traffic inspection (DPI) and flow analysis to identify threats that evade perimeter controls.

Advanced Threat Detection:

It uses multiple detection engines with commercial and open source rulesets to identify malware, C2, exfiltration, and lateral movement.

Blind Spots on the Net:

By capturing traffic (SPAN/TAP) from switches and firewalls, it eliminates blind spots in central and remote offices.

Integration with Existing SOC:

It sends standardized alerts to the centralized SIEM, enriching SOC visibility without requiring additional tools.

1.4 Value Proposition

Covered Safety Pillars

Pillar	Coverage	Mechanisms
Confidentiality	High	TLS encryption for management, HTTPS for alerts, network segmentation
Integrity	High	Rule checksums, immutable logs, configuration validation
Availability	High	Optional redundant architecture (CARP), health monitoring

Main Benefits

KEY BENEFITS

✓ Real-time threat detection with multiple analysis engines
✓ Full visibility of north-south and east-west traffic
✓ Native integration with market-leading SIEM platforms
✓ Low total cost of ownership (TCO) with open source components
✓ Flexible deployment: physical, virtual, or hybrid appliance
✓ Integrated commercial and open source threat intelligence
✓ Automatic mapping to MITRE ATT&CK frameworks

2. Main Features

2.1 Intrusion Detection (Suricata IDS)

NCSM uses Suricata as its primary intrusion detection engine, providing real-time traffic analysis with support for multiple commercial and open source rule sources .

Ruleset	Supplier	Coverage
ET Pro	Proofpoint	Malware, C2, Exploits, Policy
Snort VRT	Cisco Talos	Vulnerabilities, Malware
Feodo Tracker	abuse.ch	Banking Trojans, Botnets
SSL Blacklist	abuse.ch	Malicious SSL certificates
URLhaus	abuse.ch	Malware distribution URLs
CISA KEV	CISA	Exploited vulnerabilities

2.2 Traffic Analysis (NTOPNG)

NTOPNG provides in-depth analysis of network traffic through Deep Packet Inspection (DPI), Layer 7 application identification, and detection of behavioral anomalies.

Ability	Description
Deep Packet Inspection	Package content analysis using an nDPI engine
Flow Analysis	NetFlow v5/v9, sFlow, native IPFIX
App Identification	More than 300 identifiable applications and protocols
Anomaly Detection	Baseline of behavior and deviation alerts
Blacklist Correlation	Communication with known malicious IPs/domains

2.3 Types of Threats Detected

COVERED THREATS

✓ Malware and Ransomware (C2 communication, payload download)
✓ Exploitation of vulnerabilities (active CVEs)
✓ Lateral movement and privilege escalation
✓ Data exfiltration (DNS tunneling, ICMP tunneling)
✓ Communication with botnets and C2 servers
✓ Port scanning and network awareness
✓ Brute force attacks (SSH, RDP, SMB)
✓ Network policy violations

2.4 Integration with SIEM

NCSM sends alerts and events to centralized SIEM platforms using multiple industry-standard protocols and formats.

SIEM	Method	Format	Port
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. Technical Requirements and Architecture

Appliance Profiles

NCSM-COMPACT (Remote Offices)

Component	Specification
Throughput	Up to 500 Mbps
CPU	Intel Core i5 / AMD Ryzen 5 (4 cores)
RAM	16 GB DDR4
Storage	256 GB NVMe SSD
Grid	2x 1GbE (Management + SPAN)
Supported Users	50-200 users

NCSM-STANDARD (Medium-sized Offices)

Component	Specification
Throughput	Up to 2 Gbps
CPU	Intel Xeon E-2300 / AMD EPYC (8 cores)
RAM	32 GB DDR4 ECC
Storage	512 GB NVMe SSD + 2TB HDD
Grid	4x 1GbE + 2x 10GbE SFP+
Supported Users	200-1,000 users

NCSM-ENTERPRISE (Datacenters / HQ)

Component	Specification
Throughput	Up to 10 Gbps
CPU	2x Intel Xeon Gold / AMD EPYC (32+ cores)
RAM	128 GB DDR4 ECC
Storage	1TB NVMe (OS) + 4TB NVMe (logs)
Grid	2x 1GbE (Mgmt) + 4x 10GbE / 2x 25GbE
Supported Users	1,000-10,000 users

3.2 Traffic Capture Methods

Method	Description	Recommended Use
SPAN Port	Mirror port on switch	Remote offices, <1Gbps
Network TAP	Physical capture device	Datacenters, critical links
Port Mirror	Similar to SPAN (vendor terminology)	General, enterprise switches
Inline Tap	TAP with bypass for active IPS	When lockout is required

3.3 Compatibility

Supported Network Devices

Category	Manufacturers/Products
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. Security and Compliance

4.1 Certifications and Frameworks

Framework	State	Coverage
ISO 27001	Compatible	Information security controls
NIST CSF	Compatible	Functions: Identify, Protect, Detect, Respond
MITRE ATT&CK	Integrated	TTP mapping in detections
PCI-DSS	Compatible	Network monitoring requirements
CIS Controls	Compatible	Critical security controls

4.2 Platform Protection

System Hardening

SECURITY CONTROLS

✓ FreeBSD hardening according to CIS Benchmarks
✓ Host firewall with restrictive rules (deny by default)
✓ Automated security updates
✓ Administrative access only via HTTPS/SSH
✓ Immutable audit logs
✓ Support for RADIUS/LDAP authentication

5. Support and Services

5.1 Support Model

Level	Availability	Response Time	Channels
Critical (P1)	24/7/365	15 minutes	Phone, Email, WhatsApp
High (P2)	24/7/365	1 hour	Phone, Email, WhatsApp
Medium (P3)	Mon-Fri 8am-8pm	4 hours	Email, Portal
Low (P4)	Mon-Fri 9am-6pm	24 hours	Email, Portal

5.2 Licensing Model

Model	Calculation Basis	Includes
By Appliance	Number of deployed appliances	Hardware, Software, Support
By Throughput	Gbps of monitored traffic	Flexible scalability
Enterprise	Unlimited all-inclusive package	All-inclusive + Premium

6. Use Cases

6.1 C2 Communication Detection

Scenery:
A compromised endpoint establishes communication with a Command & Control server to receive instructions and exfiltrate data.

NCSM Detection:

Indicator	Engine	Action
Connection to IP in Feodo blacklist	Suricata + TI	CRITICAL Alert
DGA domain detected	Suricata ML	HIGH Alert
beaconing pattern	NTOPNG Anomaly	SIEM Correlation

Result:
Alerts are sent to the SIEM in real time. The SOC team identifies the compromised endpoint and implements containment measures in less than 15 minutes.

6.2 Data Exfiltration Detection

Scenery:

An attacker uses DNS tunneling to exfiltrate sensitive data by bypassing traditional firewall controls.

NCSM Detection:

Suricata detects DNS queries with anomalous patterns (excessive length, high frequency). NTOPNG identifies unusual DNS traffic volume from a specific endpoint. Correlation in SIEM triggers an exfiltration alert.

Result:
Exfiltration stopped before significant data loss. Full forensic investigation with traffic capture.

4. Specifications Summary

Category	Specification
Product	Network Cyber Security Monitor (NCSM) v1.0
Guy	Network Detection and Response (NDR) / IDS
Manufacturer	Postech
Technological Base	pfSense + Suricata + NTOPNG
Deployment	Physical Appliance, Virtual (VMware, Proxmox, KVM)
Maximum Throughput	Up to 10 Gbps (Enterprise profile)
Supported Rulesets	ET Pro, Snort VRT, Feodo, URLhaus, SSL Blacklist, CISA KEV
SIEM Integrations	Wazuh, CrowdStrike, Splunk, QRadar, Elastic, Sentinel
Traffic Capture	SPAN Port, Network TAP, Port Mirror
Frameworks	ISO 27001, NIST CSF, MITER ATT&CK, PCI-DSS, CIS
Medium	24/7 (P1/P2), Email, Phone, WhatsApp