PostecH

NETWORK CYBER SECURITY MONITORING

BROCHURE

postech.us

Network CyberSecurity
Monitoring

Introduction

NCSM (Network Cyber Security Monitoring) is an NDR solution that combines **high-performance IDS** , **deep traffic analysis** , and **threat intelligence correlation** to provide **comprehensive network visibility.**

It is geared towards **continuous monitoring**, **detection of advanced threats** that evade perimeter controls, and **integration with SIEM platforms**. Its **flexible architecture (physical or virtual)** allows it to adapt to organizations of any size, from remote offices to large data centers .

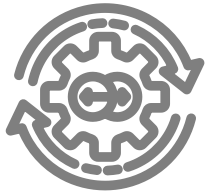
Value Proposition

Multi-Motor Detection

It uses Suricata as an IDS engine with support for multiple commercial rule sources (ET Pro, Snort VRT) and open source (abuse.ch, CISA KEV) to identify known and emerging threats.

In-depth Traffic Analysis

NTOPNG provides Deep Packet Inspection (DPI), flow analysis and detection of behavioral anomalies to identify suspicious activity that evades traditional signatures.

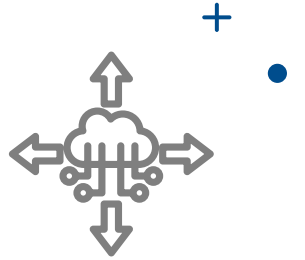


Native SIEM Integration

Sending standardized alerts to leading SIEM platforms such as Wazuh, CrowdStrike, Splunk, and QRadar, enriching SOC visibility without additional tools.

Low Cost of Ownership

Based on pfSense (FreeBSD) and open source components, eliminating operating system licensing costs and maximizing ROI.



Flexible Deployment

Appliances deployable in central and remote offices by capturing SPAN/TAP traffic from switches and firewalls.

Integrations

NCSM is designed as a sensor that integrates with the existing security ecosystem, sending alerts to SIEM platforms for correlation and response.

wazuh.

splunk>

CROWDSTRIKE

IBM QRadar

Sources of Threat Intelligence

NETWORK CYBER SECURITY MONITORING

Use Case

C2 Communication Detection (Command & Control)

Scenery

An endpoint compromised by malware establishes communication with a Command & Control server to receive instructions and send stolen data.

NCSM Detection

Indicator	Detection Motor	Severity
Connection to IP in Feodo blacklist	Suricata + Threat Intel	CRITICAL
Algorithmically generated domain (AGD)	Suricata ML Rules	HIGH
Periodic beaconing pattern	NTOPNG Anomaly Detection	HIGH
TLS traffic with JA3 known as malware	Suricata JA3	HIGH

Result

Alerts are sent to the SIEM in real time. The SOC team identifies the compromised endpoint by correlating it with EDR logs and implements containment measures in less than 15 minutes.

NETWORK CYBER SECURITY MONITORING

THANK YOU

sales@postech.us