nextgen elevates your cyber security

European technology. Local expertise.

Comprehensive protection ◆ User-centric design

Customized solutions ◆ Simplified compliance

CYBERQUEST SIEM ◆ CQ Automation ◆ NETALERT NDR

CQ Threat Intelligence ◆ CQ AI Assistant

NETALERT NDR

Advanced network defense. Agentless network visibility. AI-driven threat detection. Eliminate blind spots and take control. Single fabric integration with Cyberquest SIEM/ SOAR.

Agentless network visibility

- Monitor every session, device and user to identify potential threats efficiently.
- AI-powered analytics uncover suspicious behaviors, data exfiltration attempts and other malicious activity.
- Automate detection, prioritize alerts.

AI-driven threat detection

- Comprehensive traffic monitoring. Supports TAP, SPAN and ERSPAN for complete visibility.
- Advanced threat detection: utilizes both supervised and unsupervised AI/ML models.
- Continuous network insights: analyze network metadata and traffic in real time.

Conduct threat hunting

- Uncover hidden incidents: analyze historical network activity to identify past security events.
- Detect anomalies early: spot unusual behavior before it escalates into a threat.
- Strengthen your defense: identify and secure vulnerable assets to prevent future attacks.

Enable orchestrated incident response

- Faster incident response: investigation and mitigation within a single console.
- Enhanced security efficiency: reduce manual workload and accelerate threat resolution.

Perfect for air-gapped environments

- Maximum confidentiality and compliance. Purpose-built for highly secure and regulated environments.
- Full network visibility: maintain security without sacrificing insight into network traffic.

Eliminate blind spots and take control with Netalert NDR – deploy advanced network defense NOW!

NETALERT NDR

Threat Detection Capabilities

NetAlert NDR uses a combination of signature-based, heuristic and machine learning techniques to detect a wide range of threats. These include DDoS attacks, brute-force attempts, TOR traffic, lateral movement, crypto-mining and anomalies in DNS, SMTP and SSL traffic. It also integrates with threat intelligence feeds to detect known Indicators of Compromise (IOCs):

DDoS Detection

- **Mechanism**: Monitors for volumetric anomalies in traffic (e.g., SYN floods, UDP floods).
- **Techniques**: Rate-based thresholds, entropy analysis of source IPs and protocol-specific heuristics.
- **Indicators**: Sudden spikes in traffic, repeated requests to a single endpoint or protocol misuse.

TOR Endpoint Detection

- **Mechanism**: Matches outbound connections against known TOR exit node IPs.
- **Data Source**: Regularly updated threat intelligence feeds.
- **Use Case**: Identifies attempts to anonymize traffic, often used in exfiltration or C2 (Command & Control) channels.

Alert statistics – last 30 days

NETALERT NDR

Threat Detection Capabilities

Dynamic DNS (DDNS) Usage

- **Mechanism**: Flags DNS queries to known DDNS providers (e.g., No-IP, DynDNS).
- **Use Case**: Common in malware C2 infrastructure to maintain persistence.

Crypto-Mining Detection

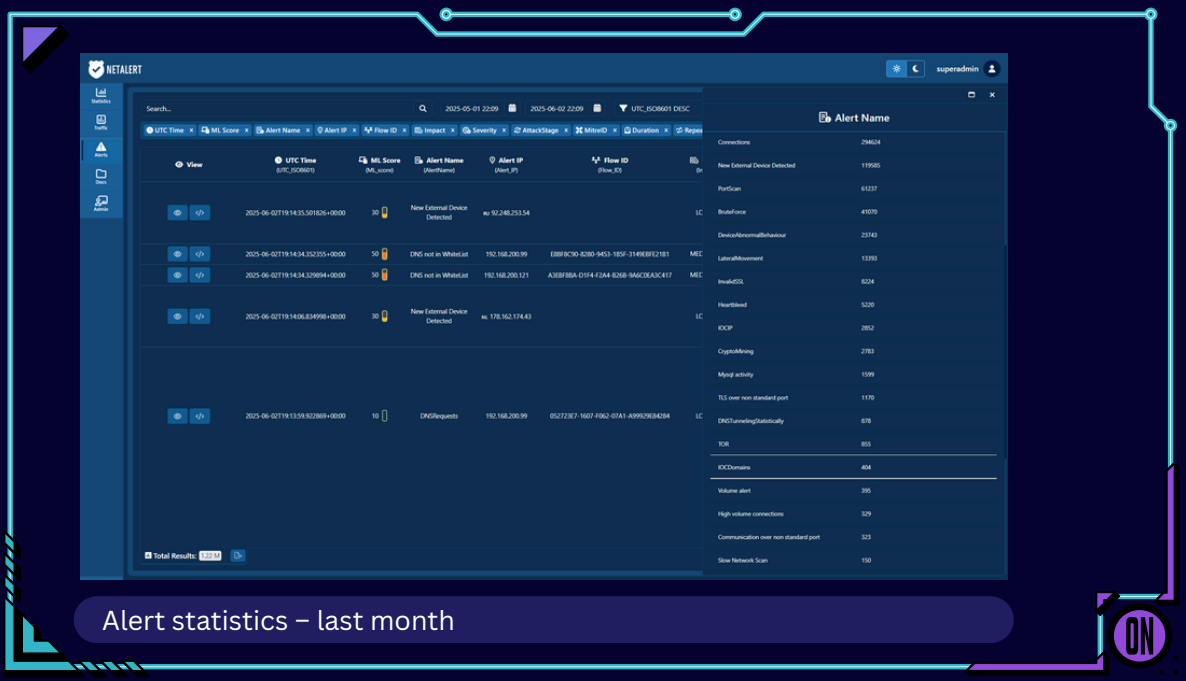
- **Mechanism**: Identifies mining pool traffic (e.g., Stratum protocol) and high CPU usage patterns.
- **Indicators**: Outbound connections to known mining pools, unusual traffic from non-user-facing devices.

IOC-Based Detection

- **Mechanism**: Matches traffic against curated lists of IPs, domains, and file hashes.
- **Sources**: Threat intelligence feeds (STIX/TAXII, MISP, etc.).

APT Behavior Detection

- **Mechanism**: Correlates multiple low-level indicators (e.g., lateral movement, privilege escalation).
- **Techniques**: Behavioral analytics and ML-based anomaly scoring.



Alert statistics – last month

NETALERT NDR

Threat Detection Capabilities

Failed DNS Requests

- **Mechanism**: Tracks DNS query/response pairs and flags unresolved queries.
- **Indicators**: High volume of NXDOMAIN responses, which may indicate domain generation algorithm (DGA) activity.

Heartbleed Exploit Detection

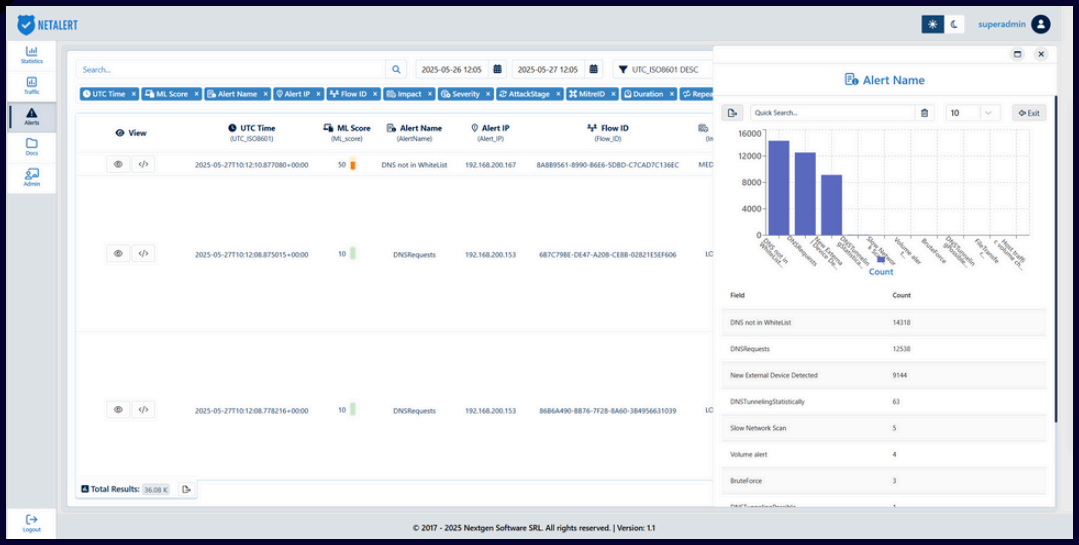
- **Mechanism**: Deep packet inspection (DPI) of TLS heartbeat messages.
- **Signature-Based**: Looks for malformed heartbeat requests that attempt to read memory beyond buffer limits.

Invalid SSL Certificate Connections

- **Mechanism**: Parses SSL/TLS handshakes to validate certificate chains.
- **Checks**: Expired certs, self-signed certs, mismatched CN/SAN fields, or untrusted CAs.

Port and Address Scanning

- **Mechanism**: Detects horizontal (same port, many IPs) and vertical (many ports, same IP) scans.
- **Techniques**: Flow analysis and connection attempt patterns.



Alerts – last 24 hours

NETALERT NDR

Threat Detection Capabilities

Malware Lateral Movement

- **Mechanism**: Detects SMB, RDP, or WMI-based lateral movement.
- I**ndicators**: Unusual peer-to-peer connections, credential reuse, or privilege escalation attempts.

Abnormal Network Behavior

- **Mechanism**: Uses statistical baselining and ML to detect deviations in traffic volume, protocol usage, or peer communication.
- **Models**: Time-series anomaly detection, clustering, and outlier detection.

DNS Anomalies

- **Mechanism**: Flags suspicious DNS patterns like:
  - High entropy domains (DGA)
  - Fast-flux DNS
  - Unusual TTL values

SMTP Traffic Monitoring

- **Mechanism**: Parses SMTP headers and payloads.
- **Use Case**: Detects spam, phishing attempts, and data exfiltration via email.

ML-Based Anomaly Detection

- **Mechanism**: Ensemble of unsupervised models (e.g., Isolation Forest, Autoencoders).
- **Output**: Alerts with confidence scores and contributing features.

IDS Rule-Based Alerts

- **Mechanism**: Integrates with Suricata/Snort rule engines.
- **Use Case**: Signature-based detection of known exploits, malware, and protocol violations.

NETALERT NDR

Traffic Monitoring & Analysis

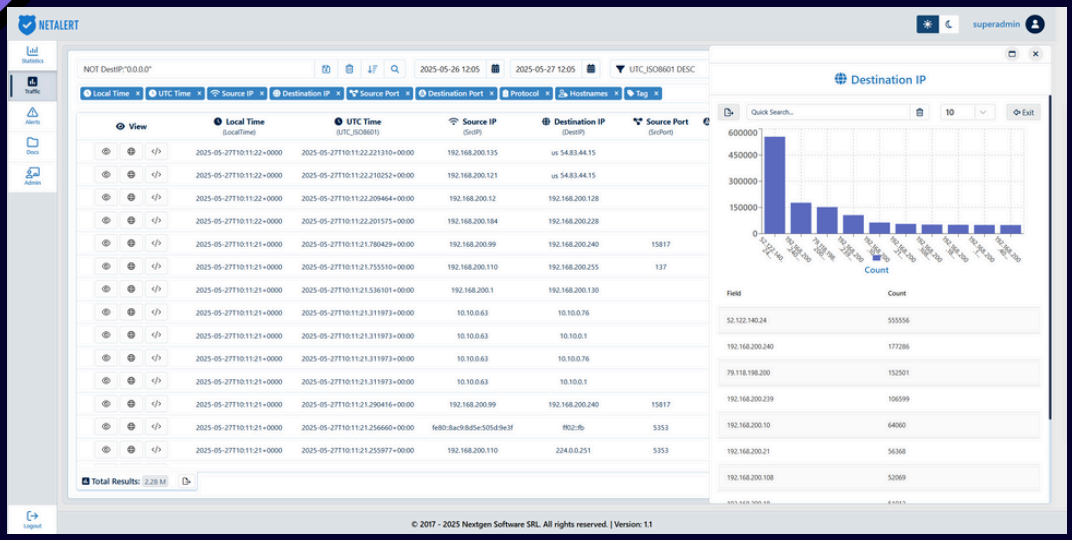
The system passively captures traffic via TAP/ SPAN ports, aggregates TCP sessions and collects flow data across VLANs. It decodes binary protocols like DNS, SMTP and HTTP, and supports PCAP recording for forensic analysis. This enables deep visibility into network behavior and supports both real-time and historical analysis.

Passive Traffic Capture

- **Method**: Uses TAP (Test Access Point) or SPAN (Switched Port Analyzer) ports.
- **Deployment**: Works in both VMware virtual environments and physical network setups.
- **Purpose**: Enables full visibility into network traffic without interfering with it (non-intrusive).

Connection Grouping for TCP

- **Function**: Aggregates individual TCP packets into logical connections or flows.
- **Benefits**:
  - Simplifies analysis by treating a session as a unit.
  - Enables detection of session-level anomalies (e.g., long-lived connections, retransmissions).



Analyzed traffic – top destinations (last day)

Connection Statistics

- **Metrics Collected**:
  - Packet loss
  - Packet size distribution
  - Round-trip time (RTT)
  - Flow duration
- **Use Case**: Helps in performance monitoring and anomaly detection (e.g., degraded service quality).

Flow Collection Across VLANs

- **Integration**: Can ingest NetFlow/IPFIX/sFlow data from third-party devices.
- **Cross-VLAN Visibility**: Enables monitoring of traffic that spans multiple VLANs, which is crucial in segmented networks.

Binary Protocol Decoding

- **Supported Protocols**:
  - DNS
  - SMTP
  - HTTP
- **Function**: Parses and extracts structured data from protocol payloads.
- **Use Case**: Enables deep inspection for threat detection (e.g., DNS tunneling, phishing emails, malicious HTTP headers).

PCAP Recording

- **Limit**: Up to 32 KB per session.
- **Purpose**: Stores raw packet captures for forensic analysis.
- **Trigger**: Typically initiated upon detection of suspicious activity or policy-defined events.

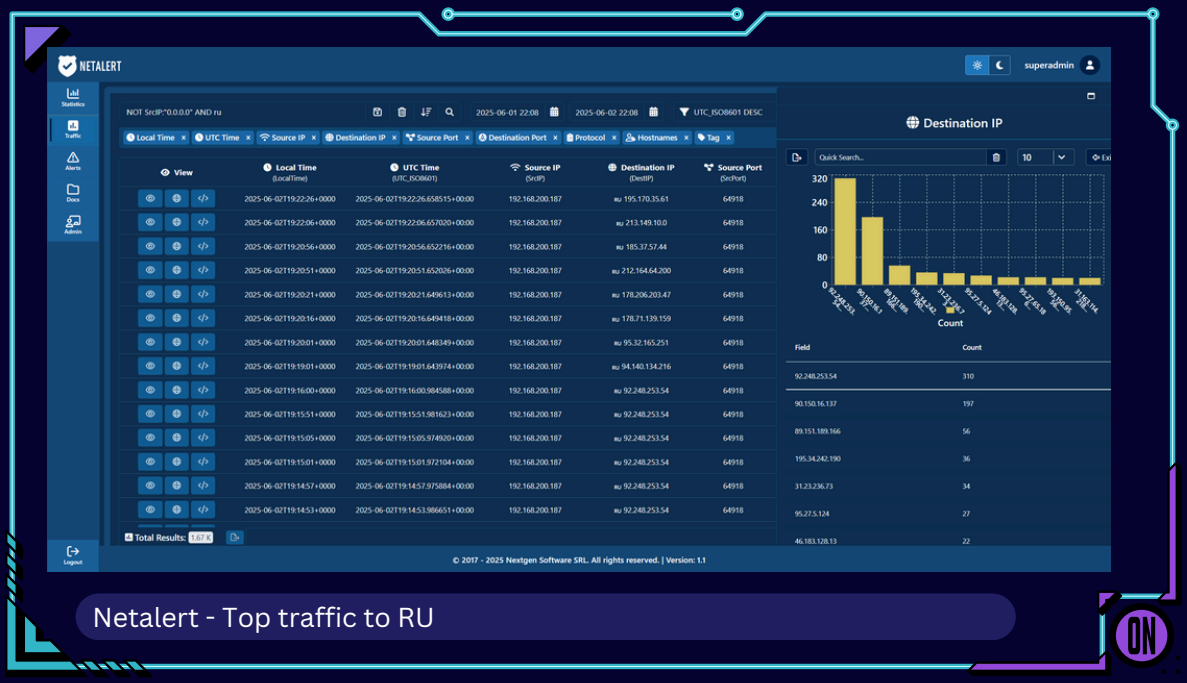
NETALERT NDR

Machine Learning Integration

NetAlert supports a modular ML framework using models from PyOD, Graphomaly and Prophet. Users can configure detection behavior via JSON files, adjust contamination levels and apply ensemble voting strategies. It supports multiple anomaly detection tasks (e.g., Kerberos, TCP, DNS) and allows fine-tuning for accuracy and false positive reduction.

Contamination Level

- **Definition**: A key hyperparameter in unsupervised anomaly detection.
- **Purpose**: Specifies the expected proportion of anomalies in the dataset.
- **Impact**: Affects the sensitivity of models like Isolation Forest, LOF, and others.
- **Configuration**: Set independently from other parameters due to its critical role.



Netalert - Top traffic to RU

NETALERT NDR

Machine Learning Integration

JSON-Based Configuration Files

- **Purpose**: Allow detailed customization of ML models for different traffic types.
- **Structure**: Each file defines:
  - Model type
  - Parameters (e.g., thresholds, contamination)
  - Voting schemes
  - Feature selection
- **Upload/ Edit**: Users can upload or modify these files via the UI.

Supported ML Algorithms

NetAlert integrates multiple ML methods from PyOD, Graphomaly and Prophet:

From PyOD:

- **kNN**: Distance-based anomaly detection
- **Isolation Forest (IForest)**: Tree-based isolation of outliers
- **COPOD**: Copula-based probabilistic outlier detection
- **LODA**: Lightweight online anomaly detection
- **MCD**: Minimum Covariance Determinant for robust multivariate outlier detection
- **LOF**: Local density-based anomaly detection
- **HBOS**: Histogram-based outlier scoring.

From Graphomaly:

- **Autoencoder (AE)**: Neural network for reconstructing normal behavior
- **Variational Autoencoder (VAE)**: Probabilistic version of AE for uncertainty modeling.

From Prophet:

- **Time-Series Forecasting**: Uses uncertainty intervals to detect deviations in DNS/SMTP traffic patterns

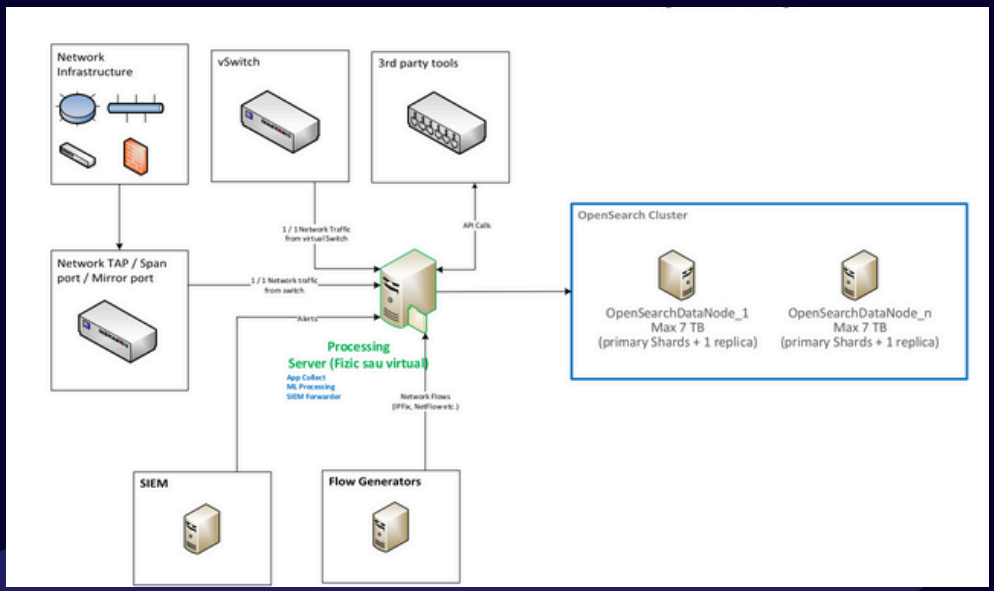
NETALERT NDR

Architecture & Integration

NetAlert is built on a modular Docker Compose architecture, supporting both single-node and distributed deployments. It provides real-time alerting, integrates with SIEM platforms, and is designed to scale based on available hardware resources, with no hardcoded limits on throughput or device count.

Modular Architecture with Docker Compose

- **Deployment Modes**:
  - **Single-node:** All services run on one host.
  - **Distributed**: Services (e.g., capture, ML, UI) can be deployed across multiple nodes.
- **Technology:** Uses Docker Compose to orchestrate containers.
- **Benefits**:
  - Easy to scale horizontally.
  - Simplified updates and maintenance.
  - Isolation of components (e.g., ML engine, database, frontend).



NETALERT NDR

Architecture & Integration

Real-Time Alerting

- **Mechanism**: Alerts are generated and pushed as soon as anomalies or threats are detected.
- **Sources**:
  - Signature-based (e.g., Suricata rules)
  - ML-based anomaly detection
  - Behavioral heuristics
- **Delivery**: Alerts can be visualized in the UI or forwarded to external systems.

SIEM Integration

- **Purpose**: Centralizes alert management and correlation with other security data.
- **Supported Formats**:
  - Syslog
  - JSON over HTTP(S)
  - Kafka or other message brokers (depending on configuration)
- **Use Case**: Enables integration with platforms like Splunk, ELK Stack, IBM QRadar, etc.

Performance Scaling

- **Design Principle**: No hardcoded limits on:
  - Number of monitored devices
  - Events per second (EPS)
- **Scalability**: Performance is hardware-dependent:
  - More CPU/RAM allows higher throughput.
  - Distributed deployment can handle large-scale environments.

The cybersecurity edge you need. Now.

nextgen

CYBERQUEST

NETALERT

www.nextgensoftware.eu

no. 55 Clucerului Str., Bucharest

office@nextgensoftware.eu