# **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



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



- Monitor every session, device and user to identify potential threats efficiently.
- Al-powered analytics uncover suspicious behaviors, data exfiltration attempts and other malicious activity.
- Automate detection, prioritize alerts.
- 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.
- 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.
- Faster incident response: investigation and mitigation within a single console.
- Enhanced security efficiency: reduce manual workload and accelerate threat resolution.
- Maximum confidentiality and compliance. Purpose-built for highly secure and regulated environments.
- Full network visibility: maintain security without sacrificing insight into network traffic.

Agentless network visibility

Al-driven threat detection

Conduct threat hunting

, The second se

Enable orchestrated incident response



Perfect for air-gapped environments

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



# **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.

	Search	ore × 🕒 Alert Name × 🖗 Alert IP	× ¥ Flow ID >			25-06-02 22:09 🛗 🔻 UTC_ISO8601 D kStage × ¥MitrelD × ©Duration × €		- E Alert Name		
	@ View	UTC Time (UTC_ISOB(et))	ML Score (ML score)	Alert Name (AlertName)	© Alert IP (Nert_P)	He Flow ID (Now,IC)	80	PortScan Bruteforce		
<u>.</u>								DeviceAbnormatBehaviour		
		2025-06-02119:10:45.125959+00:00		DNSRequests	192.168.200.99	528F2271-4462-053F-C33E-A409DED172EC		LateralMovement		
								Heartbleed	5220	
	<b>e</b> \$\$	2025-06-02119:10:44.286265+00:00	50 📔	DNS not in WhiteList	192.168.200.135	055C6632-C764-961E-AA3C-2A078CAF0E61	MEC	CrypteMining		
	<b>e</b> \$	2025-06-02119:10:41,842973+00:00	» [	New External Device	au 109.191.139.4			Mysql activity TLS over non standard port		
				Detected				DNSTunnelingStatistically	678	
		2025-06-02119:10:37.025480+00:00	30 📒	New External Device Detected	nu 37.99.223.16			IOR IOCDomains	404	
								Volume alert	355	
								Communication over non standard port		
								Slow Network Scan		
ļ	Alert stat	istics – last	30 c	lays						



# 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.

T								* C superadmin 2
Search				01 22:09 📋 21	025-06-02 22:09 🗯 🔻 UTC_ISCI8601 D		Fig. /	Alert Name
OUTCTIME × C ML	icore 🛪 📴 Alert Name 🗴 🖗 Alert IP	× 44 Flow ID	× Bb Impact × Ga	Severity 🗴 🍣 Atta	tkStage × X MitrelD × @ Duration × 5	C Repea	Connections	294024
@ View	UTC Time	ML Score	Alert Name (AlertName)	Q Alert IP (Alert IP)	<sup>1</sup> 1 <sup>2</sup> Flow ID (Now ID)	8	New External Device Detected	
<b>0 </b>	2025-06-02719.1435.501826+00:00	30 🔋	New External Device Detected	NJ 92.248253.54			BruteForce	
							Device/lanormalBehaviour	
	2025-06-02119:14:34:352355+00:00	so 🥛	DNS not in WhiteList	192,168,200.99	E88F8C90-8280-9453-185F-3149E8FE2181		LateralMovement	
<b>Ø </b>	2025-06-02119.1434.329894+00:00	50 🥫	DNS not in WhiteList	192.168.200.121	A3EBF88A-D1F4-F2A4-8268-9A6C0EA3C417		Invalid\$53.	
			New External Device				Heartbleed	
•	2025-06-02119.14:06.834998+00:00	30 🕛	Detected					
							CryptoMining	
							Mysql activity	
							TLS over non standard port	
•	2025-06-02119.13:59.922869+00:00		DNSRequests	192,168,200.99	052723E7-1607-F062-07A1-A99929EB4284		DNSTunnelingStatistically	
							IOCDomains	
							Volume alert	
							Communication over non standard port	
Total Results: 122.M							Slow Network Scan	



# **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.

Search	Search									
SUTC Time ×	ML Score 🛛 🕞 Alert Name 🗡 🛇 Alert IP	E Alert Name								
@ View	UTC Time	ML Score	Alert Name (AlertName)	Alert IP     (Alert_IP)	Flow ID	85 (m	Quick Search			
Φ Φ	2025-05-27710:12:10.877080+00:00	50 🧧	DNS not in WhiteList	192.168.200.167	8A889561-8990-86E6-5D8D-C7CAD7C136EC	MED	8000-			
(b)	2025-05-2711012:08.875015+00:00	10	DNSRequests	192.168.200.153	687C798E-DE47-A208-CE88-02821E5EF666	ιc	4. 2. 60 64	Count		
						Field ONS not in WhiteList	Count 14318			
			DNSRequests	192.168.200.153	86864490-8876-7728-8460-384956631039		DNSRequests	12538		
		0 10 🎚				LC	New External Device Detected	9144		
Ф Ф	Q     Q     2025-05-27710:12:08.778216+00:00						DNSTunnelingStatistically	63		
						Slow Network Scan	5			
						Volume alert	4			
Total Results: 36.0	вк 🕞						BruteForce	3		
							PAN'T-ana Gan Pasalata			
			© 2017 - 202	25 Nextgen Software	SRL All rights reserved.   Version: 1.1					



# **Threat Detection Capabilities**

#### Malware Lateral Movement

- Mechanism: Detects SMB, RDP, or WMI-based lateral movement.
- Indicators: 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.



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).

NOT Destile="0.0.00" 🔞 🖞 🖡 🔍 2025-65 26 12:05 👹 2025-65-27 12:05 👹 💙 UTC_ISOB601 DESC										
O Local Time ×	UTC Time × 중 Source IP × 용		W Destination IP							
@ View	Local Time     (LocalTime)	UTC Time (UTC_JS08601)	Source IP	Destination IP     (DestIP)	Source Port C	Quick Search      600000 7	10 V 05			
	2025-05-27710:11:22+0000	2025-05-27710:11:22.221310+00:00	192.168.200.135	us 54.83.44.15		450000-				
	2025-05-27710:11:22+0000	2025-05-27710:11:22.210252+00:00	192.168.200.121	us 54.83.44.15		300000-				
	2025-05-27710:11:22+0000	2025-05-27710:11:22.209464+00:00	192.168.200.12	192.168.200.128		150000-				
	2025-05-27710:11:22+0000	2025-05-27710:11:22.201575+00:00	192.168.200.184	192.168.200.228		1,50000				
0 0 4	2025-05-27710:11:21+0000	2025-05-27110:11:21.780429+00:00	192.168.200.99	192.168.200.240	15817	A. 3. 30.				
000	> 2025-05-27710:11:21+0000	2025-05-27110:11:21.755510+00:00	192.168.200.110	192.168.200.255	137	1.45 6.43 6.45	राक्त 📷 राक्त राक्त राक्त राक्त Count			
0 0 0	2025-05-27710:11:21+0000	2025-05-27T10:11:21.536101+00:00	192.168.200.1	192.168.200.130		Field	Count			
	2025-05-27710:11:21+0000	2025-05-27110:11:21:311973+00:00	10.10.0.63	10.10.0.76		52.122.140.24	555556			
	2025-05-27710:11:21+0000	2025-05-27710:11:21:311973+00:00	10.10.0.63	10.10.0.1		192.168.200.240	177286			
0 0 0	2025-05-27710:11:21+0000	2025-05-27710:11:21:311973+00:00	10.10.0.63	10.10.0.76		79.118.198.200	152501			
0 0 0	2025-05-27710:11:21+0000	2025-05-27710:11:21:311973+00:00	10.10.0.63	10.10.0.1						
© ⊕ <	> 2025-05-27710:11:21+0000	2025-05-27710:11:21.290416+00:00	192.168.200.99	192.168.200.240	15817	192.168.200.239	106599			
	2025-05-27710:11:21+0000	2025-05-27T10:11:21.256660+00:00	fe80:8ac9:8d5e:505d:9e3f	ff02:fb	5353	192.168.200.10	64060			
	> 2025-05-27710:11:21+0000	2025-05-27110:11:21.255977+00:00	192.168.200.110	224.0.0.251	5353	192.168.200.21	56368			
Total Results: 2.2	м D•					192.168.200.108	52069			
						103.100.300.10	(1013			
		0	2017 - 2025 Nextgen Software	e SRL: All rights reserved.	Version: 1.1					



# **Traffic Monitoring & Analysis**

# **Connection Statistics**

- Metrics Collected:
  - Packet loss
  - Packet size distribution
  - Round-trip time (RTT)
  - $\circ$  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:
  - $\circ$  DNS
  - $\circ$  SMTP
  - $\circ$  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.



# **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.

NOT SrcIP:"0.0.0.0" AND ru		12 💼 ↓₹ Q 20	25-06-01 22:08 🗰 20	025-06-02 22:08 🗰 🔻	UTC_ISO8601 DESC	Destination IP				
O Local Time × O UTC Ti	ime 🗴 🗢 Source IP 🗴 🕘 De	estination IP 🗴 🐨 Source Port 🗴 🔕	♦ Tag X	````						
Ø View	Local Time (Local Time)	UTC Time (UTC_ISO8601)	Source IP	Destination IP (DestIP)	Source Port (SrcPort)	Cuick Search	<b>1</b> 0 ▼ ◆			
	2025-06-02119:22:26+0000	2025-06-02T19:22:26.658515+00:00	192.168.200.187		64918	240				
	2025-06-02119:22:06+0000	2025-06-02119:22:06.657020+00:00	192.168.200.187	mu 213.149.10.0	64918	160				
	2025-06-02119:20:56+0000	2025-06-02T19:20:56.652216+00:00	192.168.200.187		64918	80				
	2025-06-02119:20:51+0000	2025-06-02T19:20:51.652026+00:00	192.168.200.187	mu 212.164.64.200	64918		▅▅▅ዹዹዹ			
	2025-06-02T19:20:21+0000	2025-06-02T19:20:21.649613+00:00	192.168.200.187	mu 178.206.203.47	64918	0	at the art the art are the			
	2025-06-02T19:20:16+0000	2025-06-02T19:20:16.649418+00:00	192.168.200.187		64918	100 100 100	र के 📷 रहे के कि रहे रहे Count			
© <b>0</b> \$	2025-06-02T19:20:01+0000	2025-06-02T19:20:01.648349+00:00	192.168.200.187		64918	Field	Count			
• •	2025-06-02119:19:01+0000	2025-06-02T19:19:01.643974+00:00	192.168.200.187	mu 94.140.134.216	64918	92,248,253,54				
@ <b>(</b> ) \$	2025-06-02T19:16:00+0000	2025-06-02T19:16:00.984588+00:00	192.168.200.187	mu 92.248.253.54	64918	90.150.16.137				
@ <b>(</b> ) 4	2025-06-02119:15:51+0000	2025-06-02T19:15:51.981623+00:00	192.168.200.187	mu 92.248.253.54	64918	89,151,189,166	56			
	2025-06-02T19:15:05+0000	2025-06-02T19:15:05:974920+00:00	192.168.200.187	mJ 92.248.253.54	64918					
	2025-06-02T19:15:01+0000	2025-06-02T19:15:01.972104+00:00	192.168.200.187	RJ 92.248.253.54	64918	195.34.242.190				
	2025-06-02119:14:57+0000	2025-06-02T19:14:57.975884+00:00	192.168.200.187	nu 92.248.253.54	64918					
	2025-06-02119:14:53+0000	2025-06-02T19:14:53.986651+00:00	192.168.200.187	nu 92.248.253.54	64918					
Total Results: 1.67 K										
		© 2017 -	2025 Nextgen Software SR	L. All rights reserved.   Versio	n: 1.1					



# **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

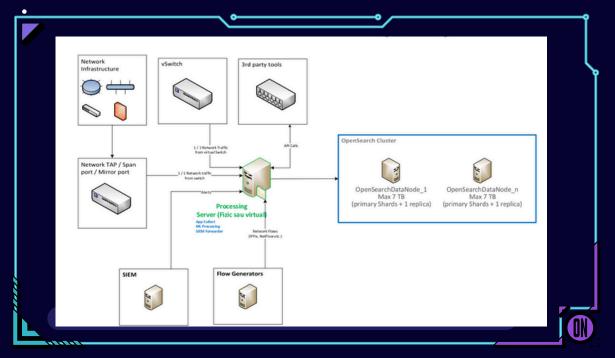


# Architecture & Integration

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.
  - $\circ~$  Isolation of components (e.g., ML engine, database, frontend).





# **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.







