nextgen

ONE CONNECTED TECHNOLOGY ECOSYSTEM.

NETALERT

Technical Functionalities

Technology for a safer tomorrow.

www.nextgensoftware.eu

NEXTGEN CYBER DEFENSE

Six technologies.
One coordinated defense lifecycle.

Each capability works independentily – and becomes stronger when connected.

PEOPLE
TECHNOLOGY
INTELLIGENCE
STRONGER TOGETHER

1 IDENTIFY

Cyberquest SIEM

Collect, normalize and correlate security data.

Ingests data from across your environment – logs, endpoints, cloud, identity and more – normalizes it and correlates events to provide a unified view of risk.



CQ CYBERQUEST
SIEM by Nextgen

2 DETECT

NetAlert NDR

Continuous network visibility, protocal analytics and AI/ML-assisted detection.

Analyzes network traffic in real time to detect threats, anomalies and lateral movement using deep protocol analysis and machine learning.



NETALERT
NDR by Nextgen

3 CORRELATE & INVESTIGATE

Cyberquest + UEBA

Behavioral analytics, risk context and investigation workflows.

Combines SIEM data with user and entity behavior analytics to uncover hidden threats, prioritize risk and enable faster, deeper investigations with full context.



CQ CYBERQUEST SIEM by Nextgen + UEBA by Nextgen

4 AUTOMATE & RESPOND

CQ Automation

Playbooks, orchestration, tickets and controlled automated actions.

Transforms detections into action with automated playbooks, cross-platform orchestration, ticketing integrations and safe, controlled auto-response to contain threats faster.



CQ AUTOMATION
by Nextgen

5 PROTECT & MITIGATE

DeDDoS

Detect, validate, mitigate and keep services online.

Identifies DDoS attacks in real time, validates malicious traffic, applies intelligent mitigation and keeps your critical services available and performing.



DeDDoS
by Nextgen

6 RECOVER & IMPROVE

Tuning + lessons learned

Tuning, lessons learned, optimization and stronger defenses over time.

Continuously refines detections, playbooks and configurations using real-world experience, post-incident reviews and metrics – turning every event into a stronger, more resilient environment.



CQ THREAT INTELLIGENCE
by Nextgen

TRANSVERSAL INPUT

Threat intelligence enriches detection, investigation and response across the entire lifecycle.

Integrates global and local threat intelligence (IOCs, TTPs, reputations, campaigns) to improve correlation, detection accuracy and response decisions in every capability.

MORE CONTEXT
FASTER INSIGHTS
STRONGER DEFENSES

CYBERSECURITY LIFECYCLE

An integrated suite that works as one to identify, detect, investigate, respond, protect, recover and continuously improve.

ONE PLATFORM.
FULL LIFECYCLE.
CONTINUOUS PROTECTION.

AI-DRIVEN.
AUTOMATED.
RESILIENT.

1

CYBERQUEST
SIEM

IDENTIFY
Collect and unify data for complete visibility.

2

NETALERT
NDR

DETECT
Detect threats early with network intelligence.

3

CYBERQUEST
SIEM
UEBA

CORRELATE & INVESTIGATE
Uncover the full context with AI and behavioral analytics.

4

AUTOMATION
SOAR

AUTOMATE & RESPOND
Orchestrate and execute automated response.

5

DeDDoS

PROTECT & MITIGATE
Ensure service availability and continuous control.

6

RECOVER & IMPROVE
Tuning.
Lessons learned.
Stronger defenses over time.

CONTINUOUS PROTECTION

THREAT INTELLIGENCE
Enriches every stage with real-time threat context.

END-TO-END CYBER RESILIENCE

Detect threats early | Investigate with context | Respond automatically | Protect and keep online | Recover and improve continuously

Stronger together. Safer every day.

NETALERT
NDR by Nextgen

Own your network's safety. Outsmart threats. Eliminate blind spots.

Agentless network visibility with AI/ML-powered analysis for high-fidelity detection, threat hunting and investigative evidence.

AGENTLESS VISIBILITY | AI-DRIVEN DETECTION | THREAT HUNTING



32 KB
packet capture context
Richer evidence for faster, more accurate investigations.

200+
scenarios
built-in

AI/ML
detection stack
Signature, heuristic and ML-based detection.

KEY CAPABILITIES

FROM NETWORK DATA TO ACTIONABLE INTELLIGENCE

Passive network visibility
Monitor network traffic through TAP, SPAN and ERSPAN without endpoint agents. See all assets, protocols and communications.

Protocol analytics
Analyze DNS, SMTP, HTTP and broader network traffic behavior to uncover anomalies, suspicious activity and hidden threats.

Detection stack
Combine signature-based, heuristic and ML-based detection methods to identify known and unknown threats with high fidelity.

Sigma rule support
Support for Sigma-style detection rules for portable, broader detection coverage.

Historical investigation
Investigate real-time and retained network activity with full context. Pivot across sessions, hosts, protocols and timelines.

Evidence capture
Retain packet context for deeper forensic analysis and response. Export PCAP, metadata and detection artifacts for casework.

NETALERT
NDR by Nextgen

Detect known threats, suspicious behavior and network anomalies.

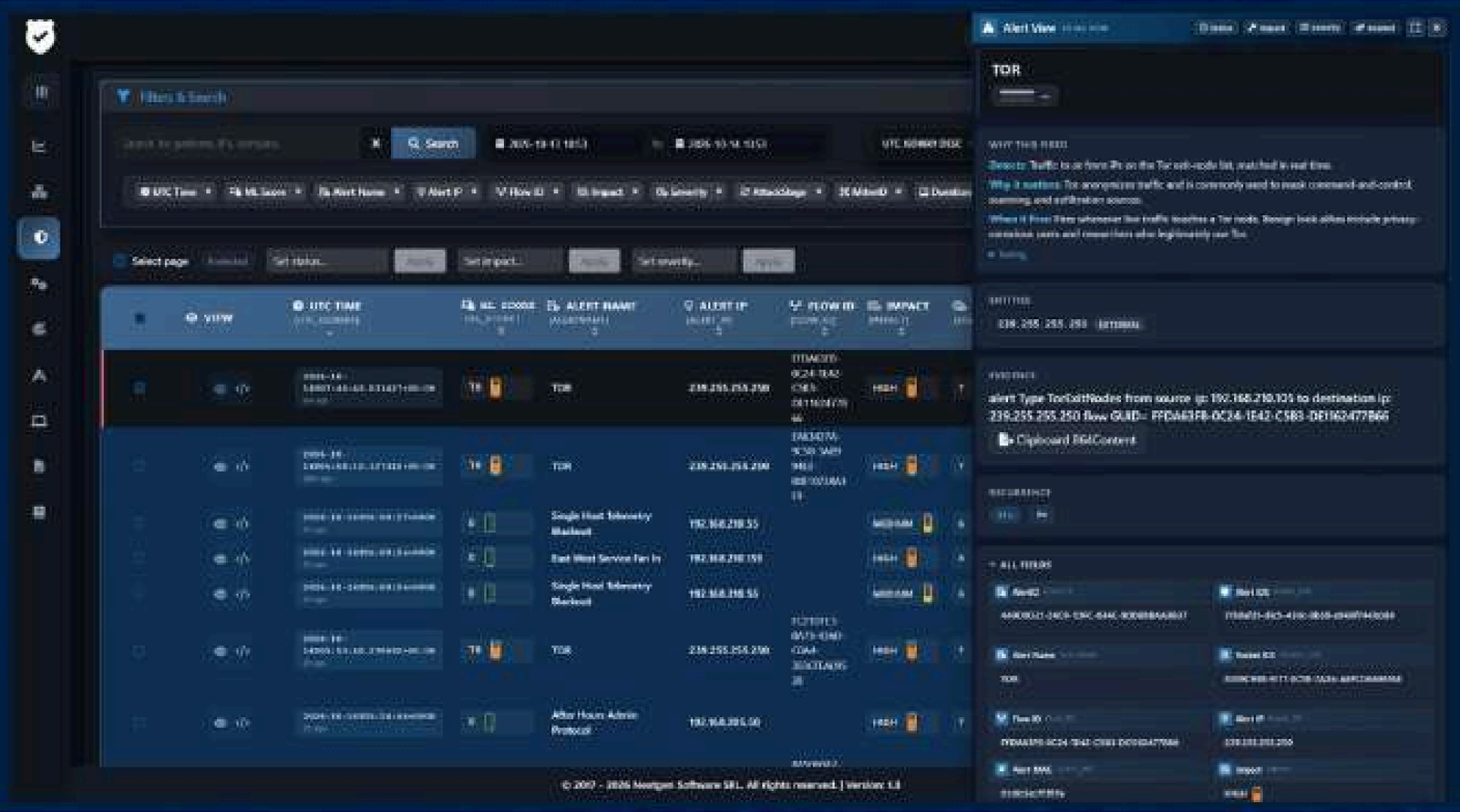
NetAlert NDR combines signature-based, heuristic and machine learning techniques and integrates threat intelligence feeds to detect known Indicators of Compromise.

DDoS Detection

- Monitors volumetric anomalies such as SYN floods and UDP floods.
- Uses rate-based thresholds, source-IP entropy analysis and protocol-specific heuristics.

TOR Endpoint Detection

- Matches outbound connections against known TOR exit-node IPs.
- Uses updated threat intelligence feeds.
- Identifies anonymized traffic that may be used for exfiltration or C2.



TOR alert investigation view.

NETALERT
NDR by Nextgen

Extend detection with DDNS, IOC and APT behavior analytics.

Dynamic DNS usage

- Flags DNS queries to known DDNS providers.
- Common in malware C2 infrastructure.

Crypto-mining detection

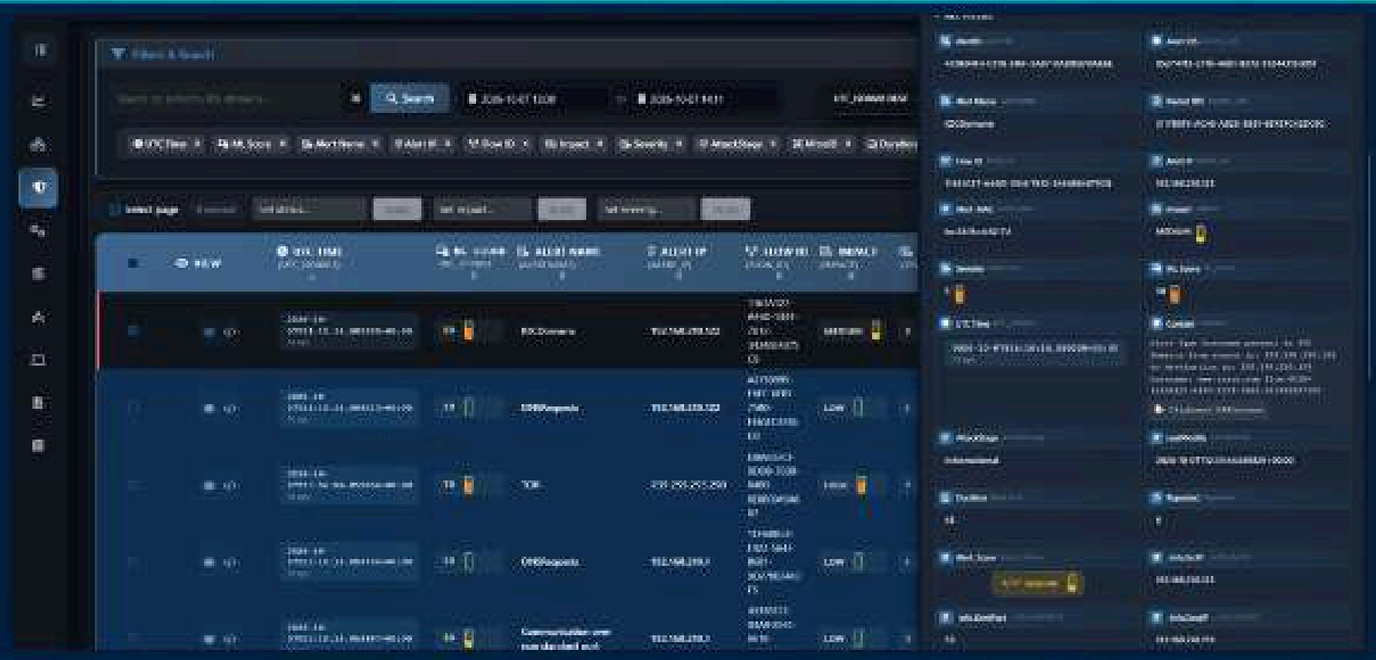
- Identifies mining-pool traffic and unusual patterns.

IOC-based detection

- Matches traffic against curated IPs, domains and hashes.

APT behavior detection

- Correlates low-level indicators and uses behavioral analytics.



IOC domain alert investigation view.

NETALERT
NDR by Nextgen

Inspect DNS, TLS and scanning activity for signs of compromise.

Failed DNS requests

- Tracks query/response pairs and flags unresolved queries.

Heartbleed exploit detection

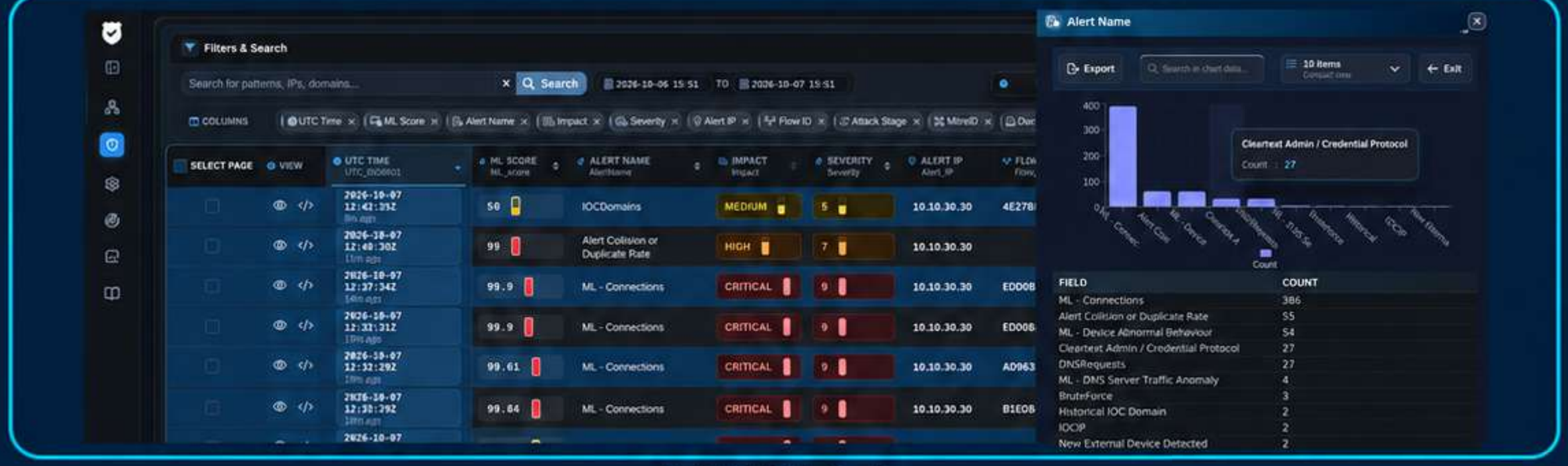
- Deep packet inspection of TLS heartbeat messages.

Invalid SSL certificate connections

- Validates certificate chains and certificate anomalies.

Port and address scanning

- Detects horizontal and vertical scans using flow patterns.



Alert detail distribution view.

NETALERT
NDR by Nextgen

Combine behavioral, protocol and rule-based detection.

Malware lateral movement

- Detects SMB, RDP or WMI-based lateral movement.

Abnormal network behavior

- Uses statistical baselining and ML to detect deviations.

DNS & SMTP anomalies

- Flags high-entropy domains, fast-flux DNS and suspicious mail patterns.

ML & rule-based alerts

- Unsupervised models generate confidence-scored anomalies.
- Rule engines provide portable detection coverage.

NETALERT
NDR by Nextgen

Passive visibility from packets to sessions and flows.

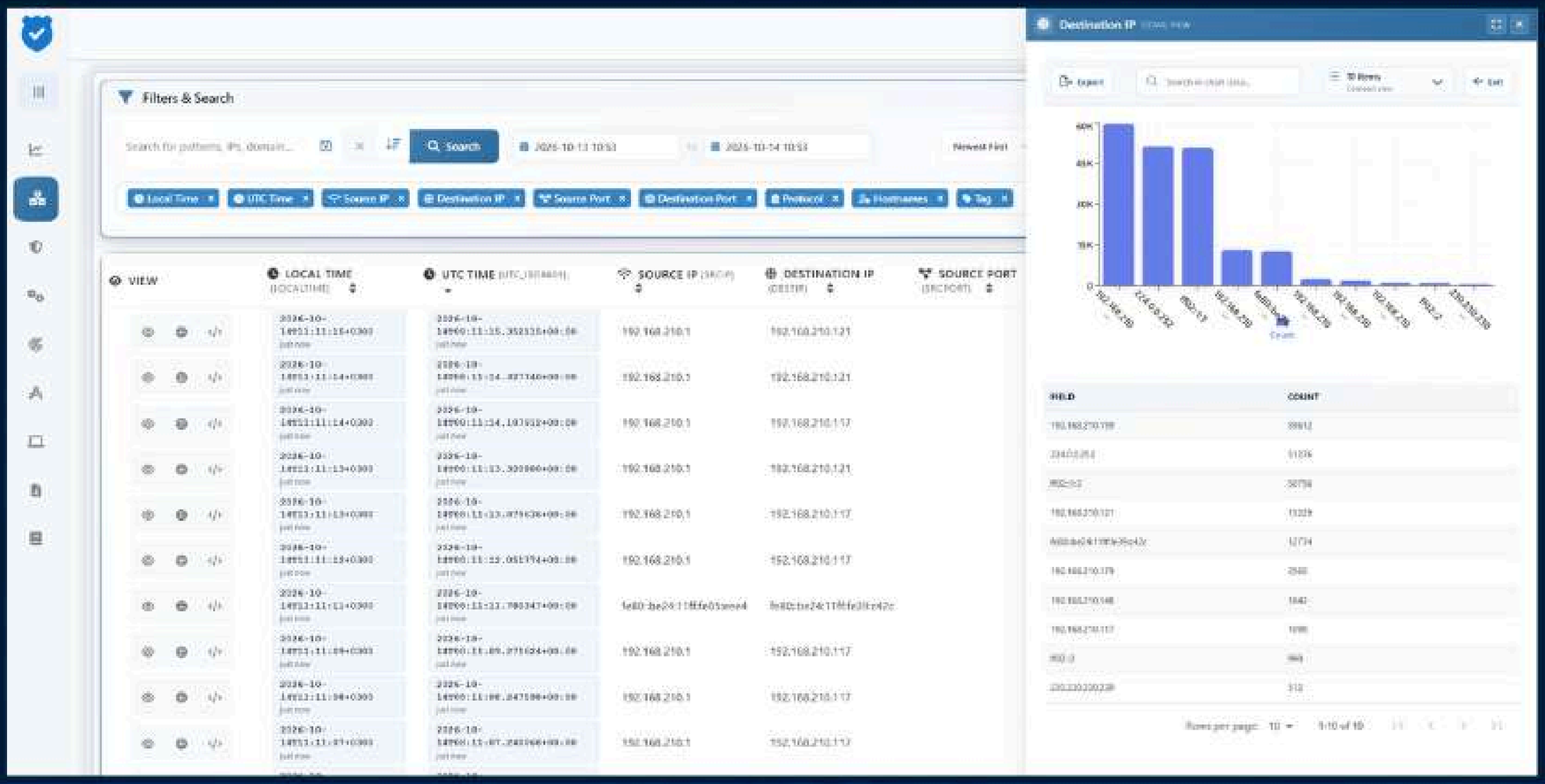
The system passively captures traffic via TAP/SPAN ports, aggregates TCP sessions and collects flow data across VLANs. It decodes DNS, SMTP and HTTP and supports PCAP recording for forensic analysis.

Passive traffic capture

- Uses TAP or SPAN ports.
- Works in virtual and physical network environments.
- Provides visibility without interfering with traffic.

Connection grouping for TCP

- Aggregates individual TCP packets into logical connections or flows.
- Supports session-level anomaly analysis.



Analyzed traffic - top destinations.

Measure performance, inspect protocols and retain packet evidence.



Connection statistics

- Packet loss, packet size distribution, RTT and flow duration.



Flow collection across VLANs

- Can ingest NetFlow/IPFIX/sFlow from third-party devices.



Binary protocol decoding

- Supported protocols include DNS, SMTP and HTTP.



PCAP recording

- Up to 32 KB per session for forensic analysis.

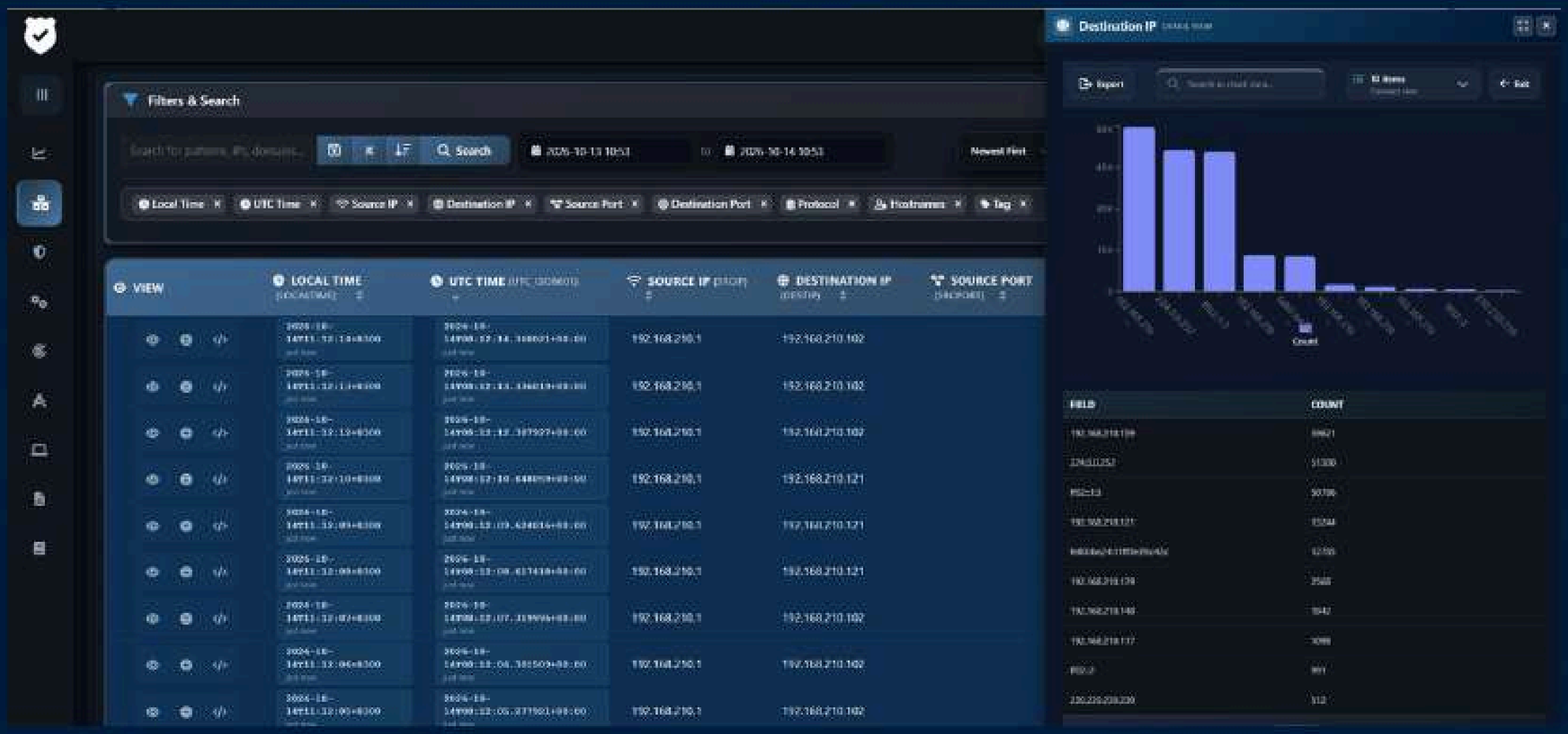
NETALERT
NDR by Nextgen

A modular ML framework tuned for network anomaly detection.

NetAlert uses models from PyOD, Graphomaly and Prophet. Users can configure detection behavior through JSON files, adjust contamination levels and apply ensemble voting strategies across multiple anomaly-detection tasks.

Contamination level

- A key hyperparameter in unsupervised anomaly detection.
- Specifies the expected proportion of anomalies in the dataset.
- Affects sensitivity of models such as Isolation Forest and LOF.



Destination IP analysis.

DETECTION ENGINES

Four detection engines, one unified risk score.

Every alert, whichever engine raised it, carries the same metadata and a single 0-10 risk score for consistent triage.



Scenario Engine

- Correlates individual detections into multi-stage APT campaign scenarios.
- Surfaces the attack chain, not just isolated events.



Enhancement Engine

- 90+ targeted network detectors mapped to MITRE ATT&CK.
- Covers Active Directory abuse (Kerberoasting, AS-REP Roasting, shadow credentials, DCSync), PrintNightmare, SMBv1/EternalBlue and 30 known CVE exploits (2017-2026).



Sigma Engine

- Runs SigmaHQ community rules directly against captured network traffic.
- Imported rules are evaluated alongside native detectors, with MITRE tactic classification.



ML Anomaly Engine

- Unsupervised models (PyOD, Graphomaly, Prophet) baseline each host and flag deviations.
- ATT&CK mapping applied only where model output supports a specific technique: DGA/DNS tunnelling, scanning, lateral movement.

NETALERT
NDR by Nextgen

Scale capture, ML and UI services independently.

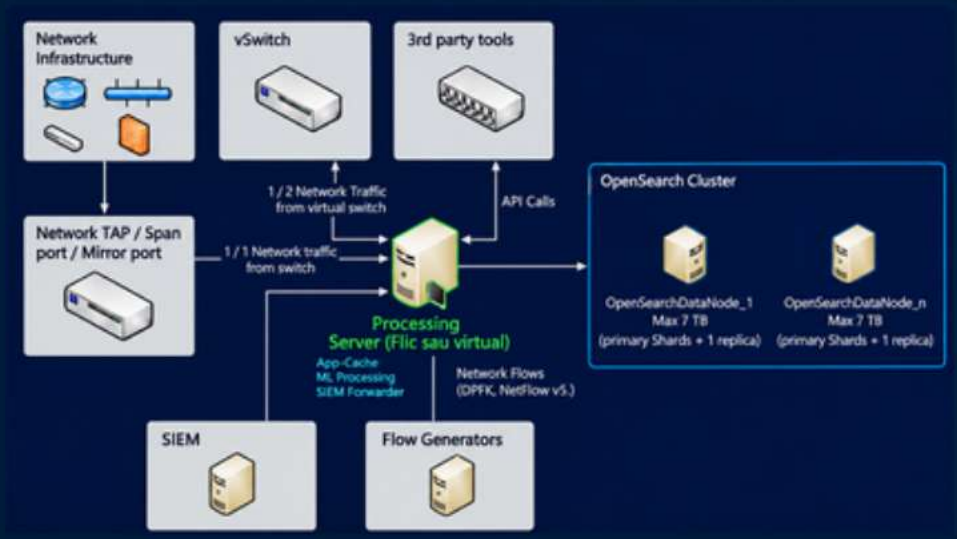
NetAlert is built on a modular Docker Compose architecture supporting single-node and distributed deployments. It provides real-time alerting, integrates with SIEM platforms and scales with available hardware resources.

Deployment modes

- Single-node: all services run on one host.
- Distributed: capture, ML, UI and other services can be deployed across multiple nodes.

Operational benefits

- Easy horizontal scaling.
- Simplified updates and maintenance.
- Isolation of components such as ML engine, database and frontend.



NetAlert architecture.

NETALERT
NDR by Nextgen

Real-time alerting, SIEM integration and hardware-based scaling.



Real-Time Alerting

- Alerts are generated and pushed as soon as anomalies or threats are detected.
- Sources include rule-based, ML-based and behavioral detection.



SIEM Integration

- Centralizes alert management and correlation with other security data.
- Supports Syslog, JSON over HTTP(S), Kafka and other brokers.



Performance Scaling

- No hardcoded limits on device count or EPS.
- Performance is hardware-dependent.
- Distributed deployment supports large-scale environments.

nextgen

TECHNOLOGY FOR A SAFER TOMORROW

Explore the full Nextgen portfolio online.

Discover products, technical capabilities, use cases, architecture insights and ways to connect with our team.

Product Pages

Browse Cyber Defense, AI Agents and Intelligence solutions.

Technical Details

Review capabilities, deployment models and operational benefits.

Use Cases

See real-world scenarios and practical outcomes.

Talk to Us

Start discussions, demos and solution planning.

VISIT OUR WEBSITE

nextgensoftware.eu

Products • Technical discussions • Demos • Architecture • Portfolio information

SCAN TO EXPLORE NEXTGEN

CYBER DEFENSE • AI AGENTS • INTELLIGENCE