nextgen

Elevate your cyber security

Comprehensive protection ◆ User-centric design

Customized solutions ◆ Simplified compliance

CYBERQUEST SIEM ◆ CQ Automation ◆ NETALERT NDR

CQ Threat Intelligence ◆ CYBER MINDS

ONE PORTFOLIO
MULTIPLE LAYERS OF DEFENSE

CYBERQUEST

Automation

NETALERT NDR

CYBER MINDS

Unified architecture - SIEM, UEBA, SOAR and NDR in one integrated logic

Operational value from day one - 2500+ pre-built detection & correlation rules

Deployment flexibility - On-premises, air-gapped, cloud or hybrid.

Predictable economics - Full visibility without punitive data-volume pricing

European-native by design - Built in Europe for sovereignty and compliance

AI Actionable intelligence in real time

AI-powered automation

End-to-end visibility

Modular, scalable architecture

Real-time threat detection & response

CYBERQUEST SIEM

Elevate your security operations. Comprehensive visibility & observability across organization. Unmatched detection with UEBA and over 2500+ correlation rules. Actionable insights for faster, smarter decisions.

Advanced User and Entity Behavior Analytics - UEBA

- Anticipate threats before they happen.
- Scalable solutions for modern enterprises.
- Identify subtle behavioral patterns for risks.

Analytics-powered experience for impactful decisions

- Actionable insights for faster, smarter decisions.
- Intuitive Interface: Simplifies complex tasks for smooth navigation and efficiency.
- Efficient Workflow: AI-assisted investigations and responses that streamline processes.

Comprehensive observability & visibility

- Anticipate threats before they happen.
- Scalable solutions for modern enterprises.
- Identify subtle behavioral patterns for risks.

Flexible deployment options, ready to scale up

- Adapts to any IT policy.
- Reduces infrastructure constraints.
- Enhances operational agility. Ultimate control and flexibility.
- Scales with your business needs and can run on hundreds of big information screens, in large, real-time situations environments.

Streamline threat detection, investigation & response

- Detection with UEBA and 2500+ correlation rules.
- Endpoint forensic insights, threat intelligence.
- High level overview for user devices incidents.

Detect, anticipate and respond with the power of Cyberquest SIEM – request your demo NOW!

CYBERQUEST SIEM

Technical features

Scalable and Flexible Log Collection

- Collect, Parse, Normalize, Index and Store security logs at very high speeds
- Out-of-the-box support for a wide variety of security systems and vendor APIs, both on-premises and cloud
- Windows Agents provide highly scalable and rich event collection including standard or non-standard windows logs, file processing, database tables
- Modify parsers from within the GUI and redeploy on a running system without downtime and event loss
- Create new parsers via integrated parser development Web Interface and share among users via export/import function
- Securely & reliably collect events for users & devices located anywhere

Easy Scale Out Architecture

- Available as Virtual Machines for on-premises and public/ private cloud deployments on the following hypervisors — VMware ESX, Microsoft Hyper-V, KVM, Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP)
- Scale deploying on multiple servers to increase performance
- Scale data collection by deploying multiple Collectors
- Collectors can buffer events when connection to Cyberquest is not available
- Log storage can be either the Cyberquest proprietary NoSQL database, or Elasticsearch which provides the ultimate in scalability

CYBERQUEST SIEM

Technical features

Automation and Incident Management

- Ability to trigger a remediation script when a specified incident occurs
- API-based integration to external ticketing systems
- Built-in Case Management system
- Incident reports can be structured to provide the highest priority to critical business services and applications
- Trigger on complex event patterns in real time

Rich Customizable Dashboards

- Specialized layered dashboards for business services, virtualized infrastructure, event logging status dashboard, and specialized apps
- Out of the box dashgroups for all connected data sources.

External Technology Integrations

- Integration with any external web site for IP address lookup
- API-based integration for external threat feed intelligence sources
- API for easy integration with provisioning systems

External Threat Intelligence Integrations

- APIs for integrating external threat feed intelligence
- Malware domains, IPs, URLs, hashes, Tor nodes

CYBERQUEST SIEM

Advanced UEBA Module

Cyberquest's Advanced UEBA module brings intelligent threat detection to the next level. By applying machine learning, it learns how users and systems typically behave, so it can quickly spot when something's off.

Whether it's a user logging in at an unusual hour, accessing sensitive files they normally wouldn't, or a device acting out of character, UEBA flags abnormal activity in real time. This helps your security team catch threats early - before they escalate.

What makes Cyberquest UEBA stand out? You can go beyond standard detection by using custom detection patterns. Tailor alerts to your organization's specific needs - like monitoring for unusual admin actions, rare file transfers or policy violations.

Get a unified view of risk, enriched alerts and powerful dashboards - all designed to help you respond faster and smarter.

Alert definition parameters

- **Alert Name**: Unique identifier for the alert.
- **Alert Active**: Boolean flag to enable/disable the alert.
- **Sent as Alert**: Allows backend correlation without user-facing notifications.

Time-based control

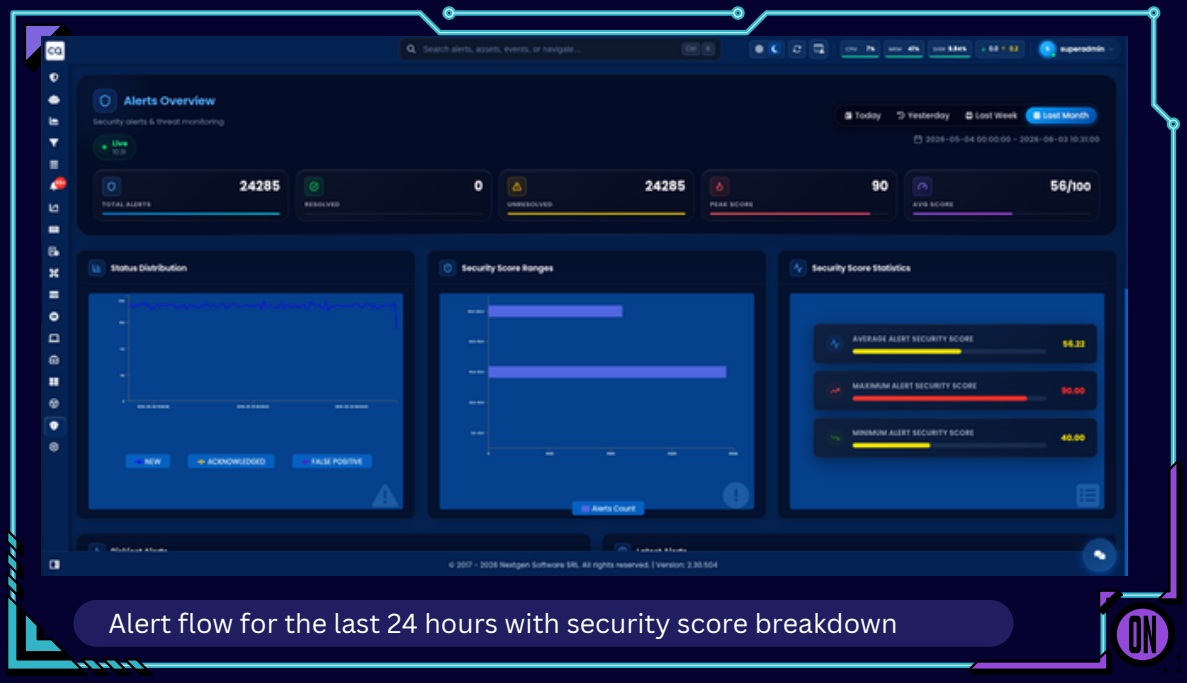
- Time Frame TTL (sec.): Defines how long the alert remains active after being triggered. This is crucial for time-sensitive correlation logic.

Security scoring system

- **Alert Security Score**: A dynamic score that starts from a baseline and adjusts based on rule matches and event frequency. Range: baseline to 100.
- **Alert Security Level**: Color-coded severity level that mirrors the score.

Notification system

- **Send via Email**: Enables email notifications to predefined recipients.
- **Notification Template**: Supports both built-in and custom templates for alert messages.



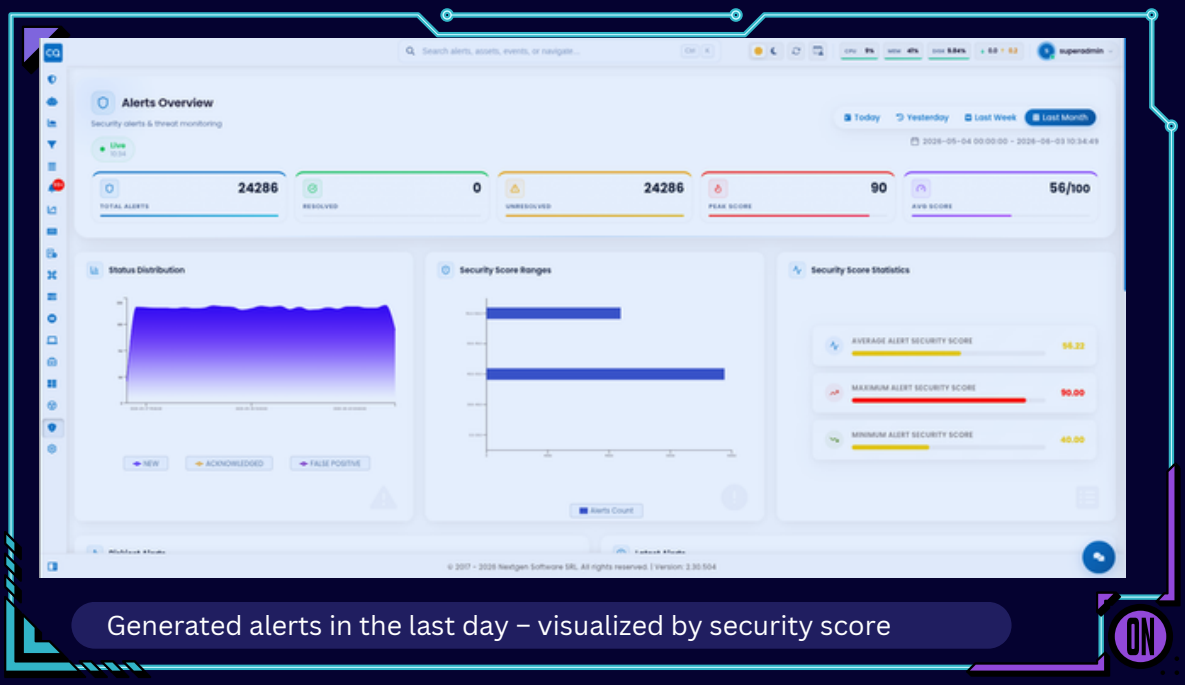
Alert flow for the last 24 hours with security score breakdown

Alert execution

- **Has Action**: Enables execution of a custom script when the alert is triggered.
- **Script Editor**: Embedded editor to define logic in a scripting language. This script overrides all other rule conditions.
- **Predefined Action Execution**: Facilitates the automatic triggering of configured actions or operational playbooks upon alert activation.

Rule-based event correlation

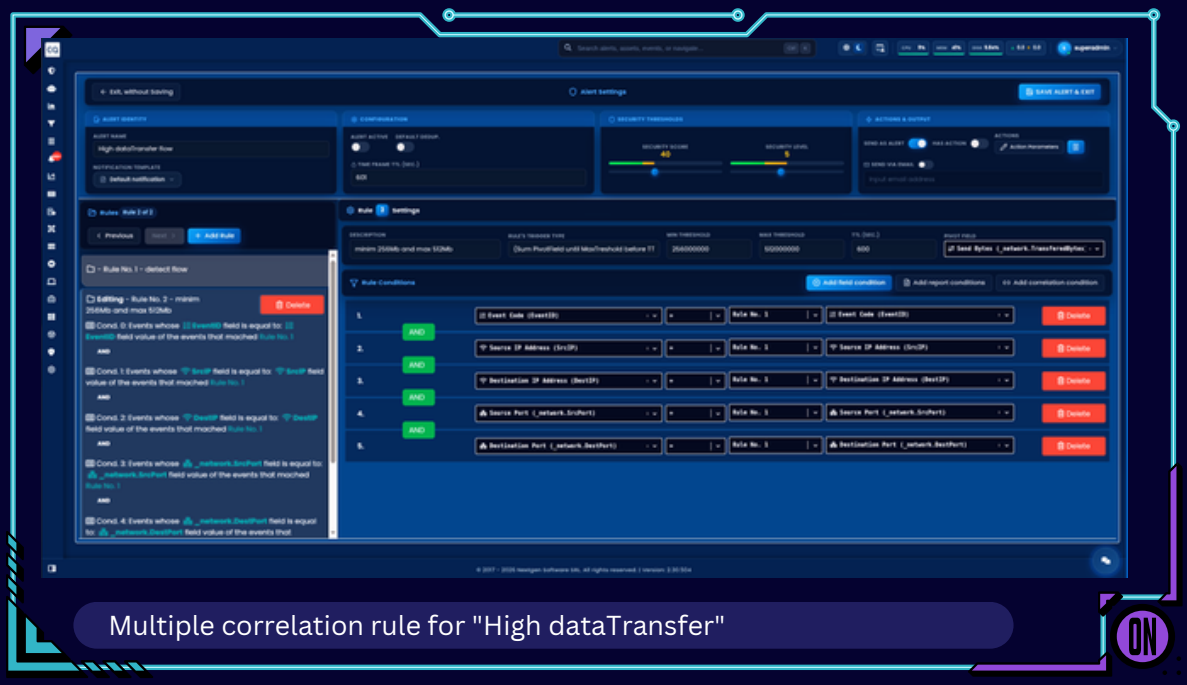
- **Rule Logic**: Supports complex logical conditions using:
  - AND, OR, NOT operators
  - Field-based filters (e.g., =, not =, is in list, not in list, starts with, ends with, contains, range, contains any of, contain all of, regex match)
  - Report-based triggers
  - Event correlation (e.g., sequence, absence, or timing of events)
- **Rule Settings Pane**: GUI for defining and managing rule logic.



Generated alerts in the last day – visualized by security score

Event correlation capabilities

- Single event triggers
- Multi-event correlation:
  - Event order
  - Missing events in a sequence
  - Logical succession of events
  - Multiple event sequence
  - Count, average or sum on specific field values
  - Multiple data sources correlations



Multiple correlation rule for "High dataTransfer"

CYBERQUEST SIEM

REPORTS

Report Types

- **Technological Reports**: Summarized and detailed reports for specific technologies (e.g., Windows, Linux).
- **Compliance Reports**: Mapped to standards like:
  - ISO 27001
  - GDPR
  - HIPAA
  - PCI DSS
  - SOX
  - COBIT
  - FISMA
  - NIS2.
  - **DORA Journey & reporting module.**
- **Best Practices**: Frequently used reports based on industry standards.
- **Custom Reports**: User-defined reports not included by default.
- **GDPR Reports**: Focused on data protection and privacy compliance.

CYBERQUEST Automation | SOAR

Automated incident response with intelligent orchestration. Simplify integration, enhance collaboration and maximize the efficiency of your security stack.

Automated playbooks

- Simplify complex processes, reduce manual effort and focus on what matters most: mitigating threats.
- Execute actions across your security and IT tools in seconds, not hours.
- Speed up incident response by automating workflows and decision-making, ensuring faster, more efficient threat management.

Comprehensive case management

- Supports custom templates and industry-standard frameworks.
- Efficient task segmentation, assignment and documentation for better organization.
- Collaborative process: Keeps teams aligned, ensuring thorough and detailed investigations.

Effortless application integrations

- Connect with 105+ tools effortlessly.
- 1,230 automated actions for workflows.
- Enhance collaboration & optimize security operations.

Generative AI for faster, smarter decisions

- Automates tasks using natural language understanding.
- Enhances threat investigation, response and playbook creation.
- Boosts decision-making and streamlines complex workflows.

Tailored for enterprise or managed services needs

- Suited for enterprises with flexible solutions.
- Choose from on-prem or cloud hosting based on your needs.

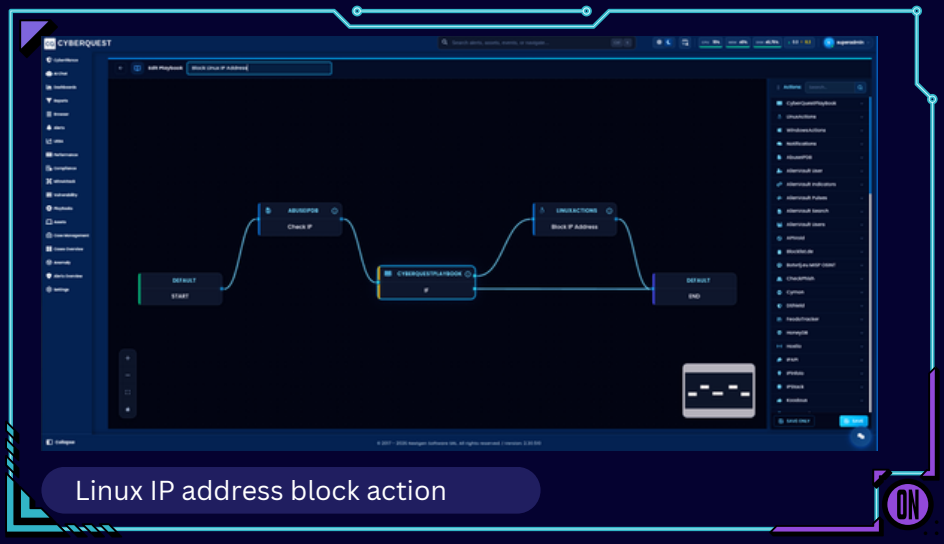
Automate, orchestrate and outpace threats with CQ Automation – see it in action TODAY!

CYBERQUEST Automation | SOAR

Playbook Automation Engine

Outlines how Cyberquest structures and executes automated response workflows (playbooks). It explains the graphical interface for building playbooks, the dynamic input system and the multiple triggering methods (automatic via alerts or manual via GUI).

- **Playbook Structure**:
  - A playbook is a sequence of actions grouped to perform a mitigation or response flow.
  - Actions are added/removed via a graphical interface.
  - Each action requires input parameters, which are dynamically evaluated at runtime.
- **Execution Modes**:
  - Automatic Triggering:
    - Triggered by specific alerts.
    - The alert instance becomes the global inputData for the playbook.
    - Configured via: web graphical interface.
  - **Manual Triggering:**
    - From the Event Browser: user clicks on a specific event.
    - From the Alert Browser: user clicks on a specific alert.
- **Execution History:**
  - Debugging tool to trace parameter values and action outcomes.
  - Helps identify failures or misconfigurations in playbook logic.

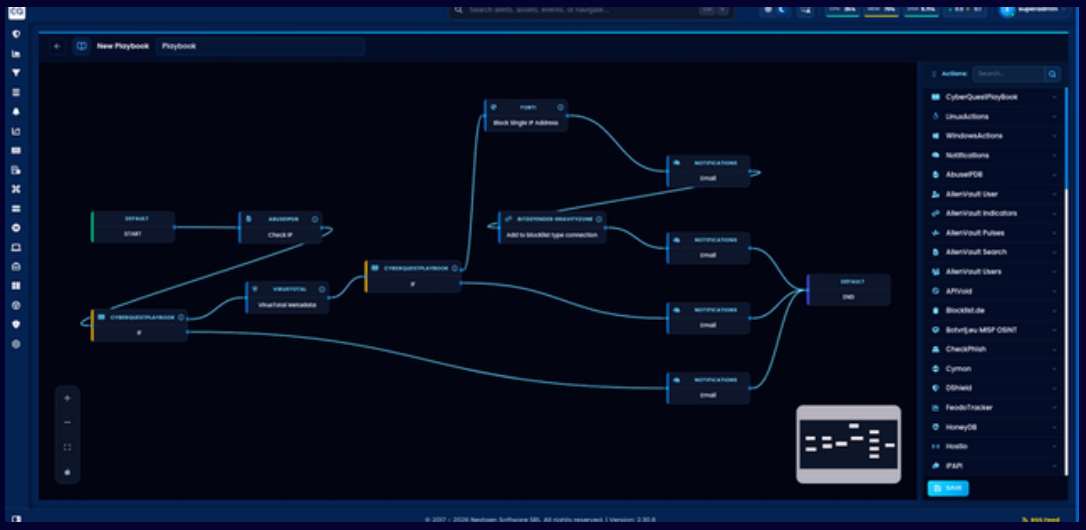


CYBERQUEST Automation | SOAR

Playbook Automation Engine

Disable domain account

ON



Block IP in various systems and notify for each action

ON

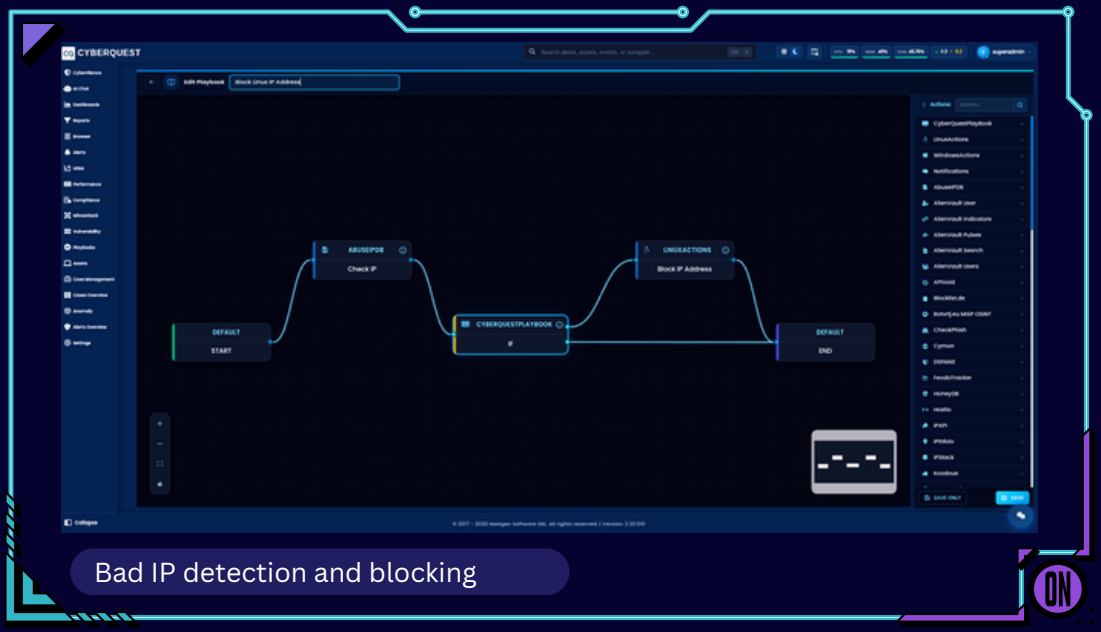
CYBERQUEST Automation | SOAR

Playbook Automation Engine

Details the two main categories of actions used in playbooks: vendor-specific (integrated with external security tools) and functional (logic-based actions like conditions, counters, and custom scripts). These actions form the building blocks of automated responses.

- **Vendor-Specific Actions:**
  - Integrated with a growing list of security vendors.
  - Uses vendor APIs for:
    - Blocking IPs
    - Isolating hosts
    - Updating firewall rules
    - Sending alerts or notifications
  - Updated automatically with new vendor integrations.

- **Functional Actions (under "CYBERQUEST Playbook"):**
  - **IF**: Conditional branching based on Boolean logic.
  - **Count**: Counts elements in an array-type variable.
  - **Code:** Executes a DTS object (custom logic written in JavaScript).



Bad IP detection and blocking

Smart Playbook Features

- Highlights advanced features that enhance flexibility and reusability in playbooks, such as dynamic parameter evaluation, modular logic blocks, and support for custom scripting using JavaScript (DTS objects).
- **Dynamic Parameter**s:
  - Input values are computed at runtime using placeholders and context variables.
- **Reusable Logic**:
  - Actions and logic blocks can be reused across multiple playbooks.
- **Custom Scripting**:
  - Supports JavaScript via DTS objects for advanced logic and data manipulation.

Audit & Forensics

- Covers the logging and traceability features of CQ Automation/ SOAR. It explains how every action is recorded for compliance, debugging, and forensic analysis, ensuring transparency and accountability in automated responses.
- **Execution Logging**:
  - Every action is logged with:
    - Input parameters
    - Execution result
    - Timestamp and user ID (if manual)
- **Forensic Reports**: Generated from execution history for compliance and incident review.

NETALERT NDR

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

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

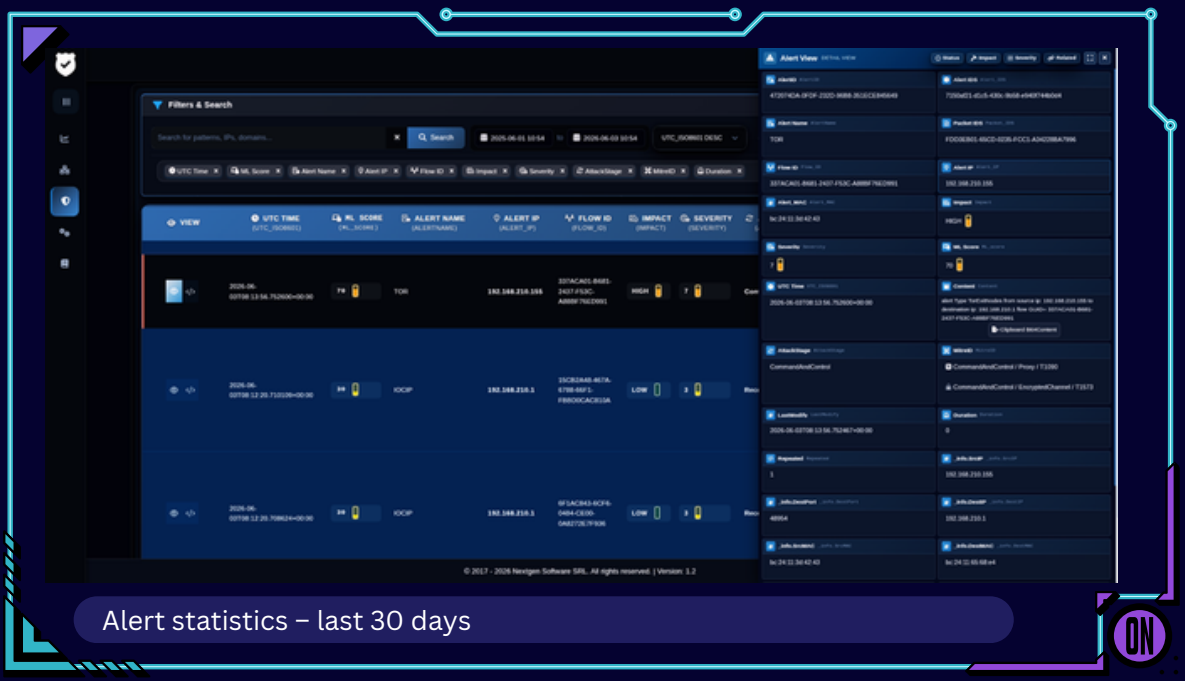
NetAlert NDR uses a combination of signature-based, heuristic and machine learning techniques to detect a wide range of threats. These include DDoS attacks, brute-force attempts, TOR traffic, lateral movement, crypto-mining and anomalies in DNS, SMTP and SSL traffic. It also integrates with threat intelligence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

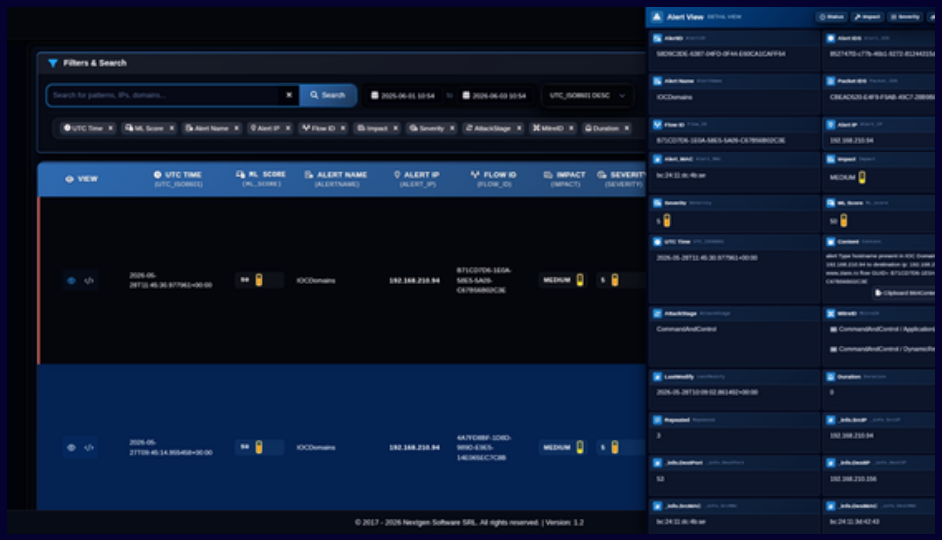
- **Mechanism**: Identifies mining pool traffic (e.g., Stratum protocol) and high CPU usage patterns.
- **Indicators**: Outbound connections to known mining pools, unusual traffic from non-user-facing devices.

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

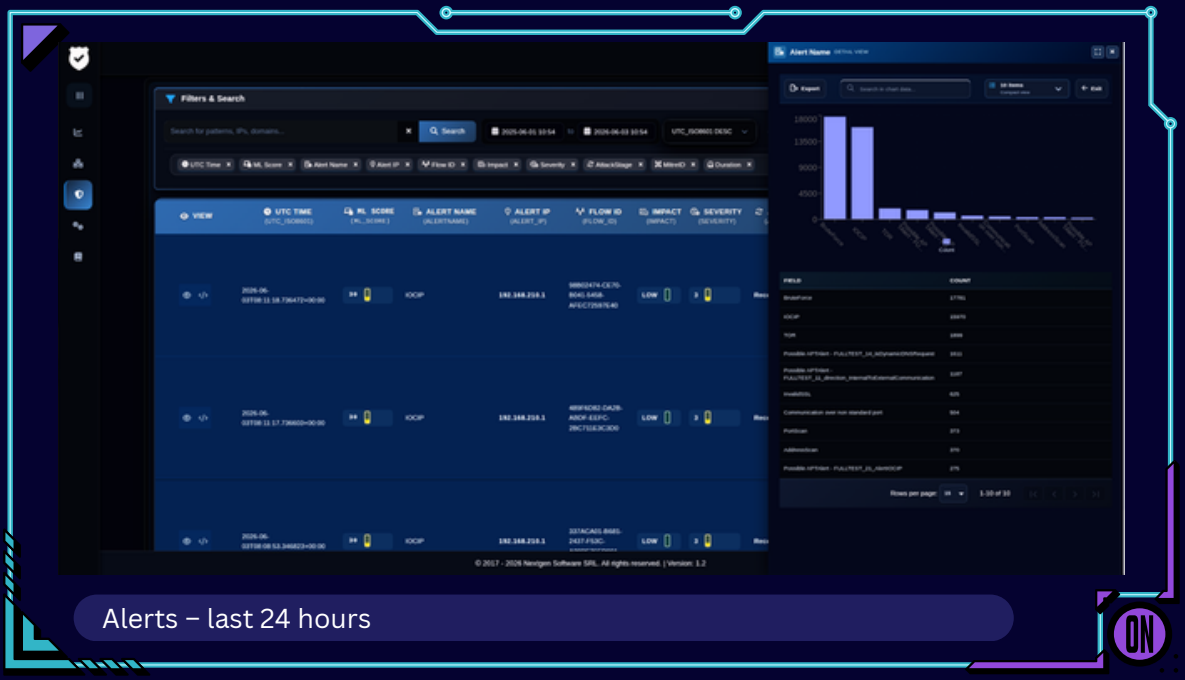
- **Mechanism**: Deep packet inspection (DPI) of TLS heartbeat messages.
- **Signature-Based**: Looks for malformed heartbeat requests that attempt to read memory beyond buffer limits.

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.



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

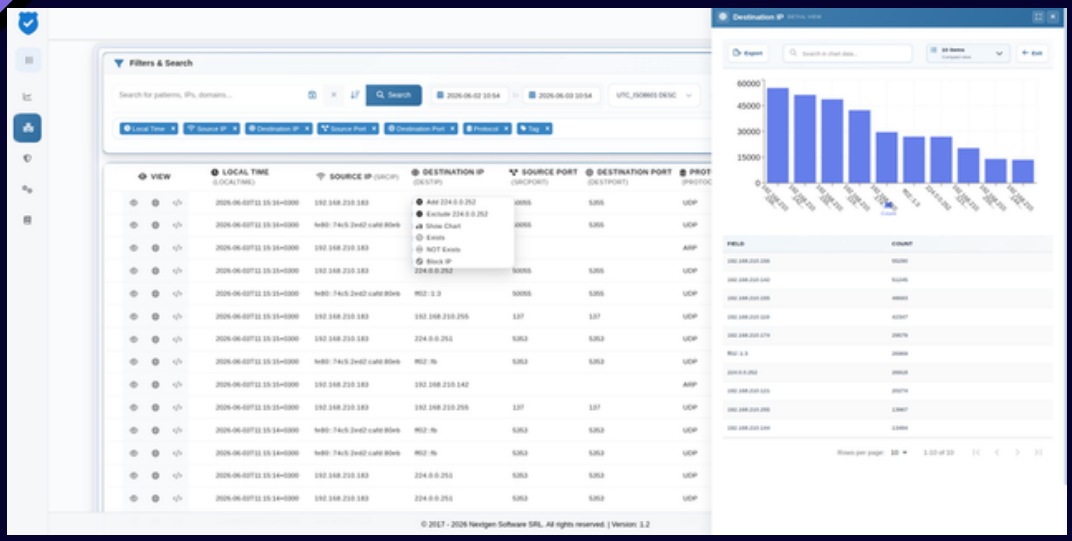
The system passively captures traffic via TAP/ SPAN ports, aggregates TCP sessions and collects flow data across VLANs. It decodes binary protocols like DNS, SMTP and HTTP, and supports PCAP recording for forensic analysis. This enables deep visibility into network behavior and supports both real-time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

Traffic Monitoring & Analysis

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.

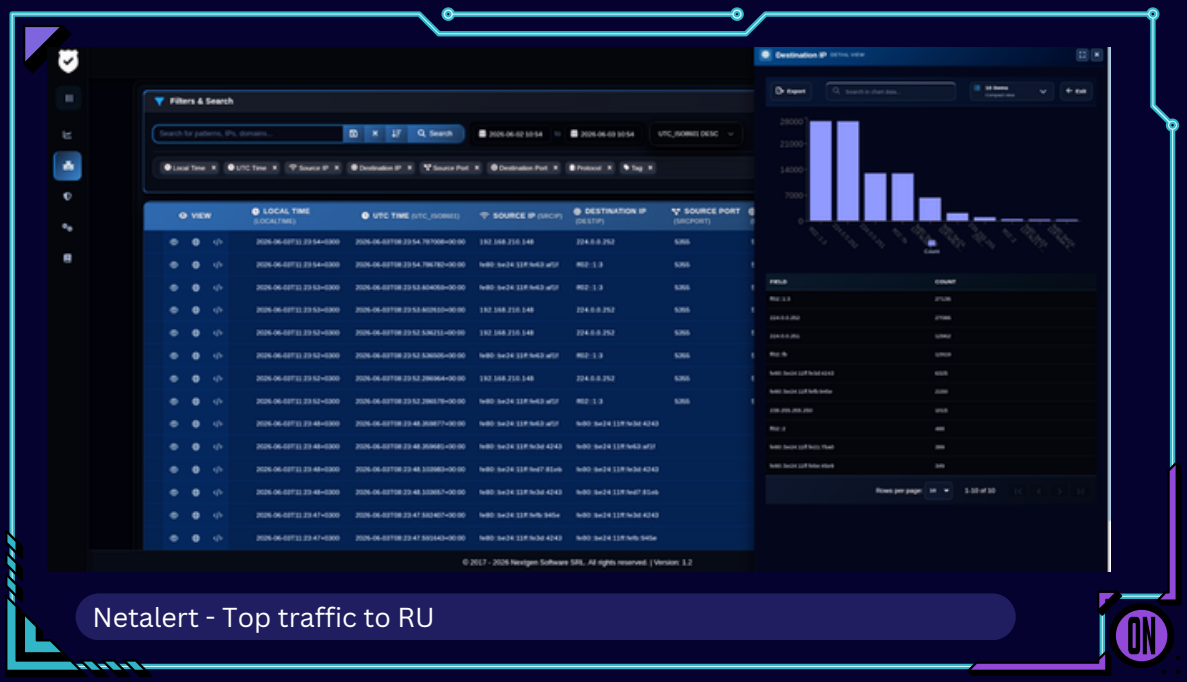
NETALERT NDR

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

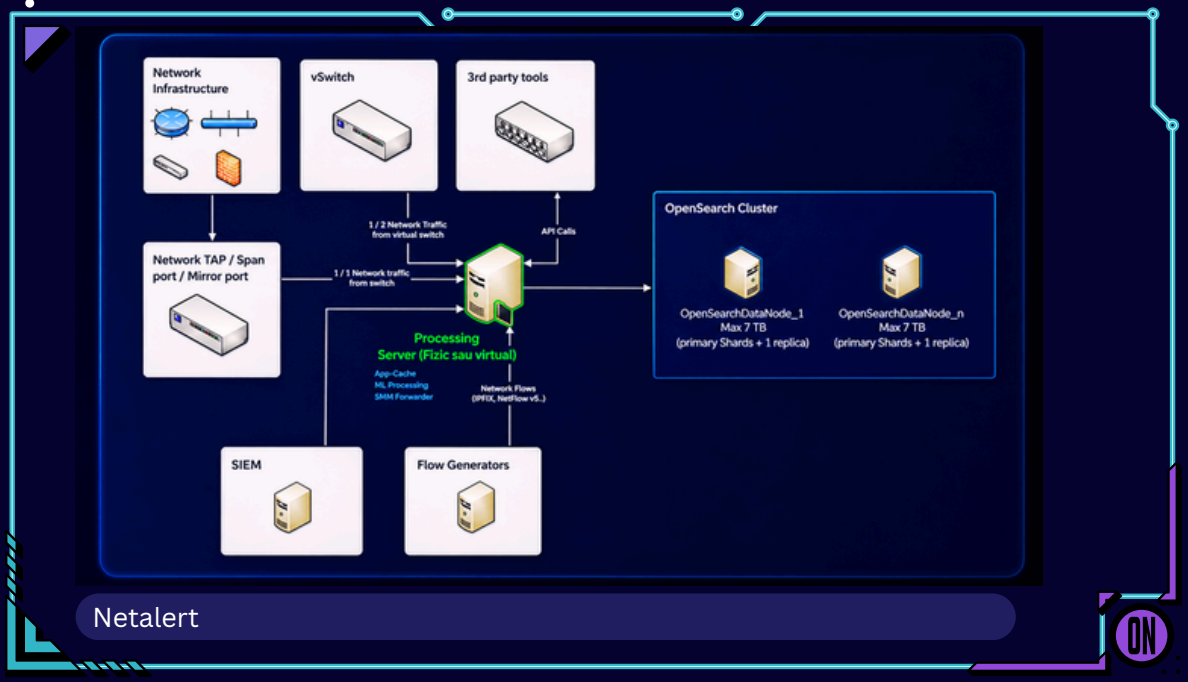
NETALERT NDR

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.

CYBERQUEST Threat Intelligence

Outsmart every threat proactively.
Stay ahead of cyber threats with high-value, relevant and actionable intelligence.

High-quality, unique data.

- Less clutter, more accuracy – reduce noise with unique, curated threat data.
- Always receive fresh, actionable intelligence.
- Better decision-making – trust in verified, high-quality threat insights.

Industry & geographical relevance

- Precision targeting – eliminate irrelevant threat data and focus only on real risks.
- Resource optimization – reduce processing power wasted on unnecessary IOCs.
- Faster threat response – respond quicker with intelligence tailored to your threat landscape.

Measurable, actionable outcomes

- Track how intelligence strengthens security.
- Actionable Insights, not just data. Intelligence designed for real-world response.
- Make informed decisions based on measurable outcomes.

Real-time & continuous updates

- Immediate threat awareness – be the first to know about new cyber threats.
- Proactive defense – stop threats before they reach your network.
- Minimized risk exposure – continuous updates mean no outdated security gaps.

Technology - specific insights

- Customized security: get intelligence that
- fits your exact IT environment.
- Graph to visualize relationships between users, devices and incidents.

Outsmart every threat - act on real, high-value intelligence tailored to your risk landscape, in real time.

CYBER MINDS

Which one are you? Discover your AI persona
on nextgesoftware.eu/cyberminds

The Mentor

- Helping analysts understand alerts and why they matter
- Guiding step-by-step investigation workflows
- Explaining detection logic and how-to document findings
- Provides guidance.

The Forensic Investigator

- Reconstructing complete attack timelines
- Identifying initial access and lateral movement paths
- Offering help in extracting & classifying IOCs for threat intelligence.

The Risk Advisor

- Evaluating business risk for vulnerabilities or threats
- Prioritizing findings based on operational impact
- Generating concise executive-level risk summaries.

The SOC Analyst

- Rapid alert analysis with contextual insights
- Investigating suspicious activity across logs and telemetry
- Producing clear, actionable incident reports.

nextgen

European cyber security for more resilient defense.

CYBERQUEST

Automation

NETALERT NDR

CYBER MINDS

www.nextgensoftware.eu no. 55 Clucerului Str, Bucharest office@nextgensoftware.eu