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

CYBERQUEST SIEM

Elevate your security operations.
Comprehensive visibility & observability across organization.
Unmatched detection with UEBA and over 400 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 over 400 correlation rules.
- Endpoint forensic insights, real-time 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

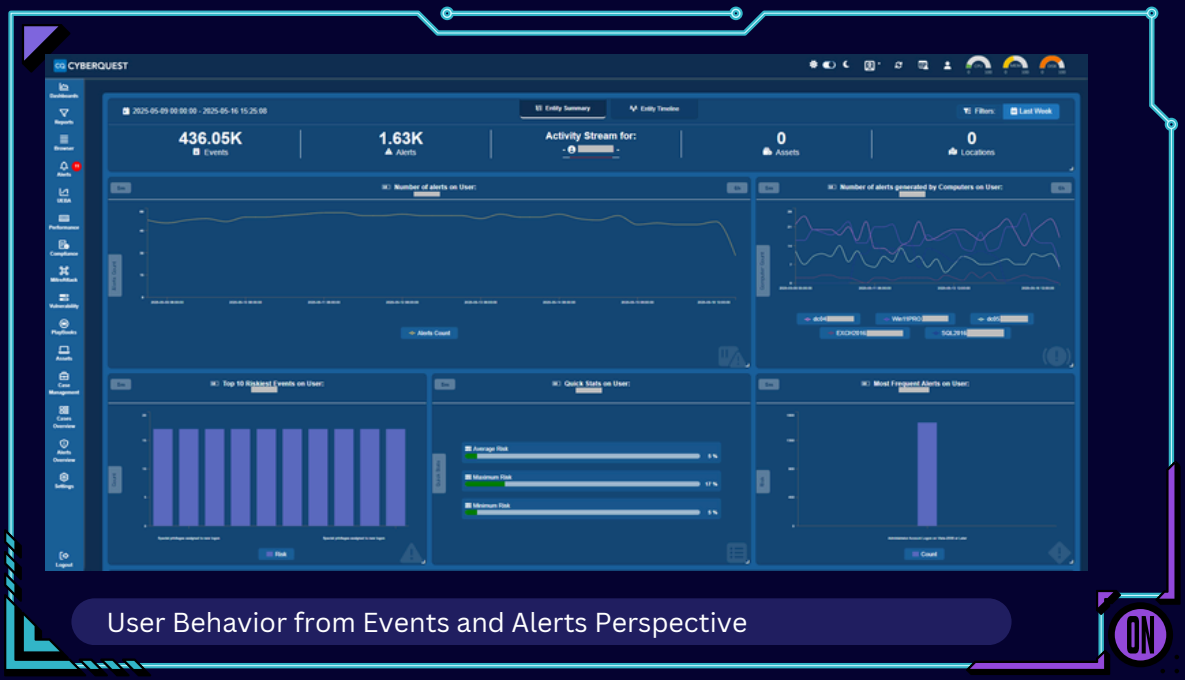
Advanced UEBA Module

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.



User Behavior from Events and Alerts Perspective

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.

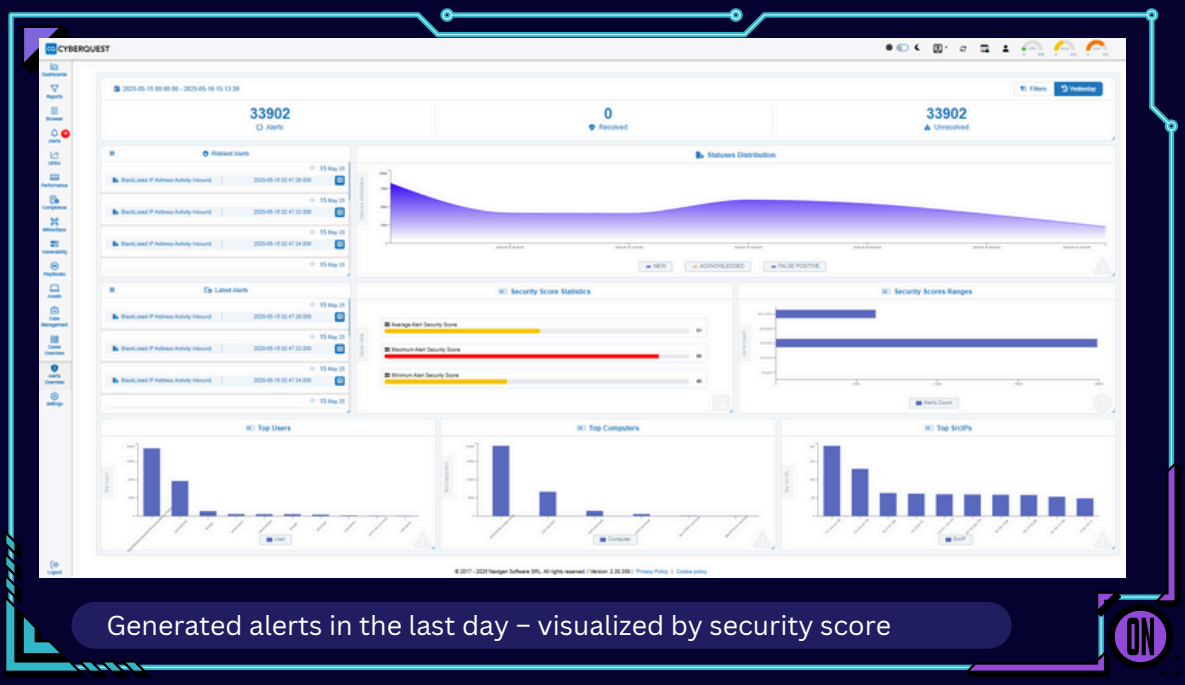
Alert flow for the last 24 hours with security score breakdown

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

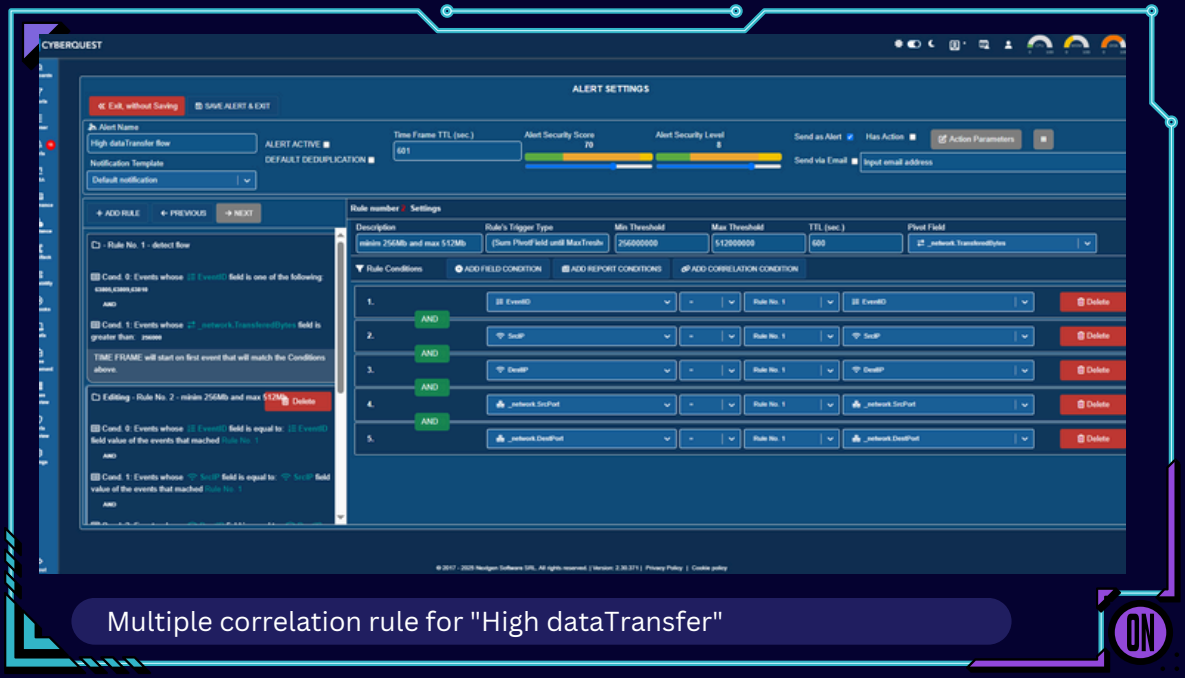
- **Rule Logic**: Supports complex logical conditions using:
  - AND, OR, NOT operators
  - Field-based filters (e.g., =, not =, is in list, not in list, starts with, ends with, contains, range, contains any of, contain all of, regex match)
  - Report-based triggers
  - Event correlation (e.g., sequence, 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



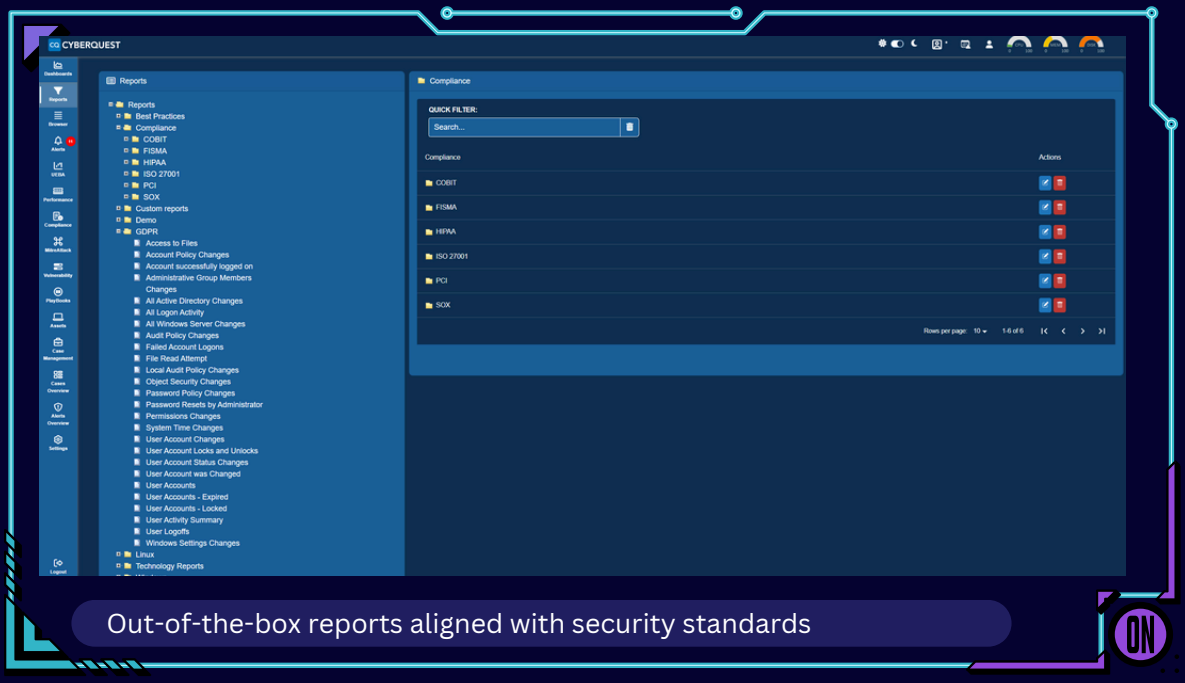
Multiple correlation rule for "High dataTransfer"

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
  - DORA, NIS2 ???
- **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.



The cybersecurity edge you need. Now.

nextgen

CYBERQUEST

NETALERT

www.nextgensoftware.eu

no. 55 Clucerului Str., Bucharest

office@nextgensoftware.eu