nextgen

ONE CONNECTED TECHNOLOGY ECOSYSTEM.

CYBERQUEST SIEM

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.



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.

CYBERQUEST SIEM BY NEXTGEN

CYBERQUEST
SIEM by Nextgen

SIEM to elevate security operations.

Centralize and analyze security data in real time, detect what matters, investigate with context and respond before incidents escalate.

Unified SIEM | UEBA + Analytics | Flexible Deployment



3,500+ pre-built alerts & detections

1,500+ built-in reports

270+ integrations

DATA > INSIGHTS > ACTION > A SAFER TOMORROW

KEY CAPABILITIES

Log collection & normalization
Centralize, parse and normalize security data across sources and environments.

Real-time correlation
Detect complex threats using single- and multi-event correlation.

Case management
Investigate collaboratively with evidence, workflow and audit trails.

Dashboards & reporting
Operational dashboards plus reporting for audit, compliance and executive visibility.

UEBA & analytics
Behavioral context and risk analytics integrated into investigations.

AI-assisted investigation
Use AI support to accelerate triage, enrich context and suggest next steps.

CYBERQUEST
SIEM by Nextgen

Comprehensive visibility. Faster decisions. Flexible deployment.

Elevate your security operations with comprehensive observability across the organization, unmatched detection with 3500+ alerts and 1500+ reports, and actionable insights for faster, smarter decisions.

Analytics-powered experience for impactful decisions

- Actionable insights for faster, smarter decisions.
- Intuitive interface simplifies complex tasks.
- AI-assisted investigations streamline response.

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 and control.

Streamline threat detection, investigation & response

- Detection with 3500+ alerts & 1500+ reports.
- Endpoint forensic insights, threat intelligence.
- High-level overview for user devices incidents.

Behavior analytics context

- Behavior analytics is available as part of the SIEM investigation context, while the dedicated UEBA product extends this capability with specialized detection and analytics.

CYBERQUEST
SIEM by Nextgen

Collect, normalize and scale without losing visibility.

Cyberquest is designed to collect and process security data at high speed while supporting distributed, resilient deployments across on-premises and cloud environments.



Scalable and flexible log collection

- Collect, parse, normalize, index and store security logs at high speeds.
- Out-of-the-box support for multiple security systems and vendor APIs.
- Windows Agents provide scalable event collection.
- Modify and deploy parsers without downtime or event loss.
- Securely collect events for users and devices located anywhere.



Easy scale-out architecture

- Available as Virtual Machines on-premises and in public/private cloud.
- Scale across multiple servers to increase performance.
- Deploy multiple collectors and buffer events when connectivity is unavailable.
- Storage can use the Cyberquest NoSQL database or Elasticsearch.

CYBERQUEST
SIEM by Nextgen

Behavior context integrated into investigation.

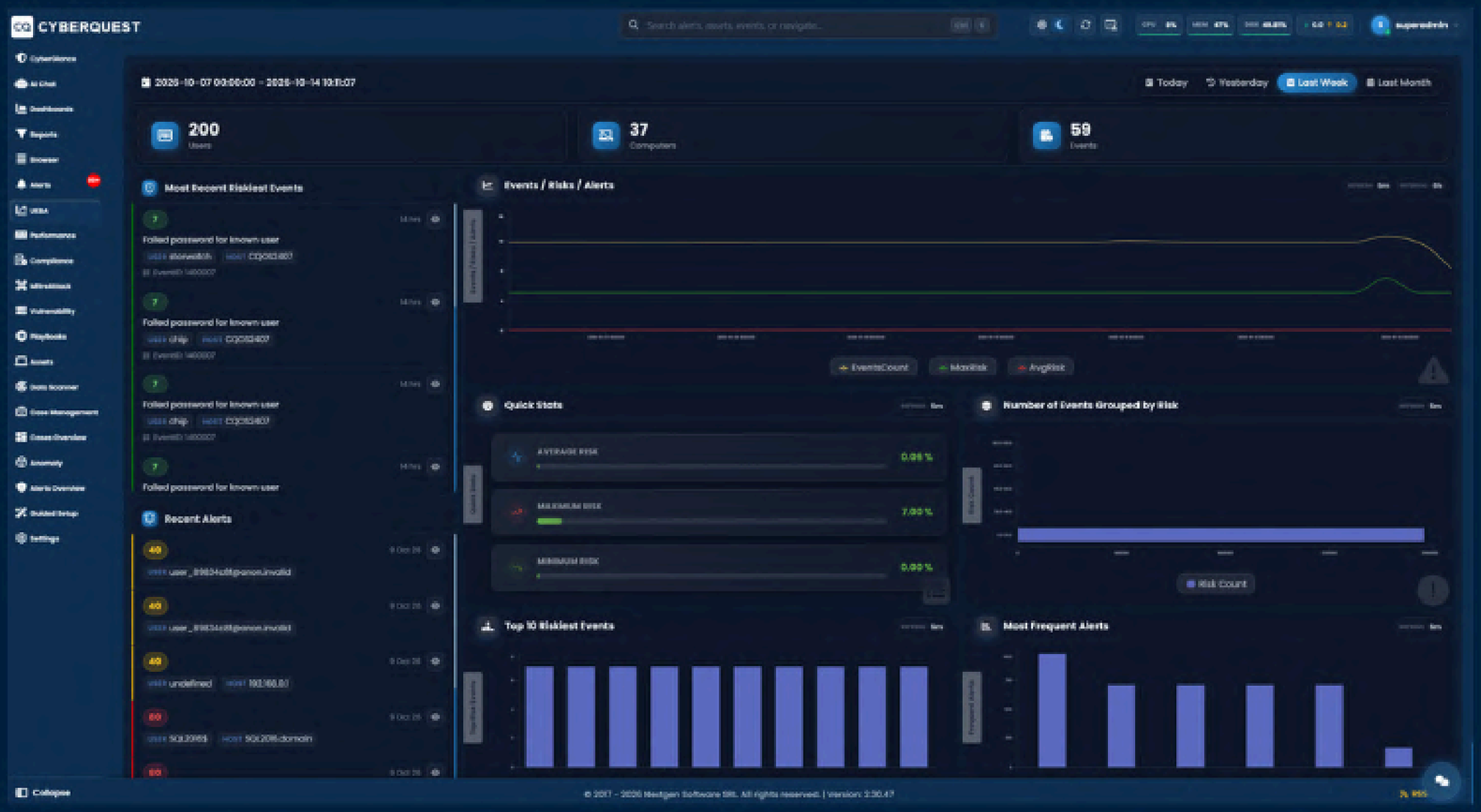
Cyberquest applies behavioral analytics to learn how users and systems typically behave and to flag abnormal activity in real time. This supports enriched alerts and risk context while the dedicated UEBA product provides specialized behavioral analytics.

Custom detection patterns

- Tailor alerts to organization-specific needs.
- Monitor unusual admin actions, rare file transfers or policy violations.

Unified risk context

- Surface abnormal activity in real time.
- Use dashboards and enriched alerts to support investigation.



User behavior from events and alerts perspective.

Define precise alert logic and control how incidents surface.

Alert definition parameters

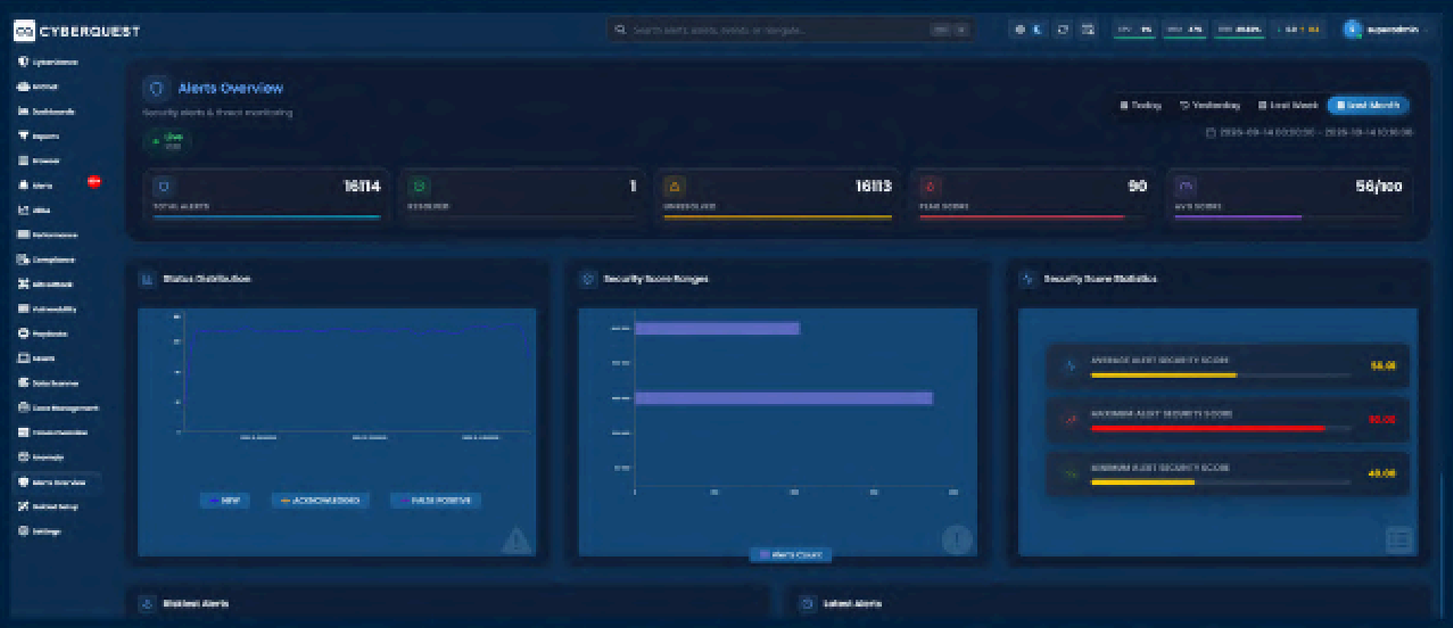
- Alert Name: Unique identifier for the alert.
- Alert Active: Enables or disables the alert.
- Sent as Alert: Supports backend correlation without user-facing notifications.

Security scoring system

- Alert Security Score: Dynamic score adjusted by rule matches and event frequency.
- Alert Security Level: Color-coded severity that mirrors the score.

Notification system

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



Alert overview and security score breakdown.

CYBERQUEST
SIEM by Nextgen

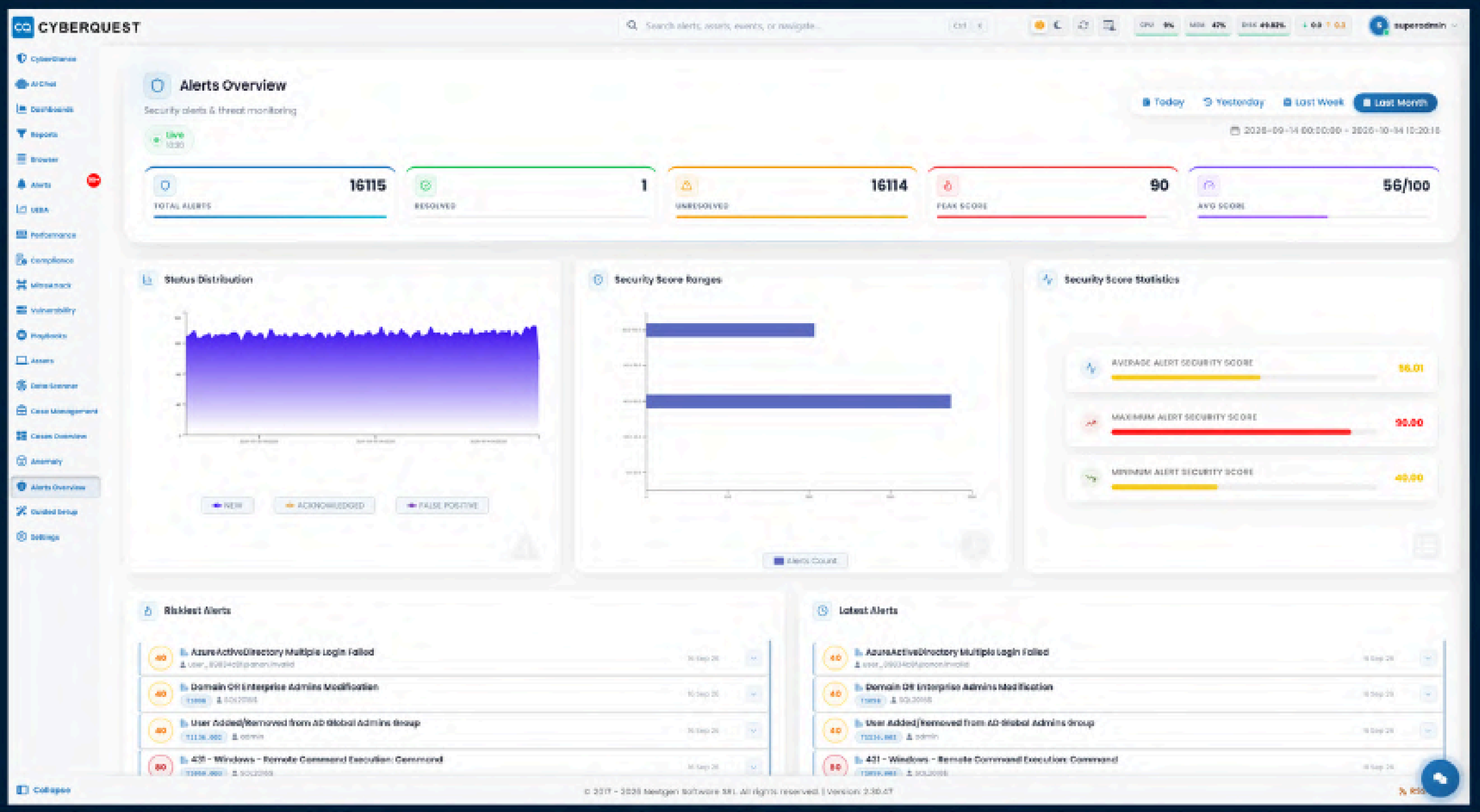
Move from detection logic to controlled action.

Alert execution

- Has Action: Enables execution of a custom script when the alert is triggered.
- Script Editor: Embedded scripting for custom logic.
- Predefined Action Execution: Triggers configured actions or operational playbooks.

Rule-based event correlation

- Rule logic supports AND, OR and NOT operators.
- Field-based filters and report-based triggers.
- Event correlation for sequence, absence or timing of events.



CYBERQUEST
SIEM by Nextgen

Correlate events across sequences, sources and conditions.

Single & multi-event correlation

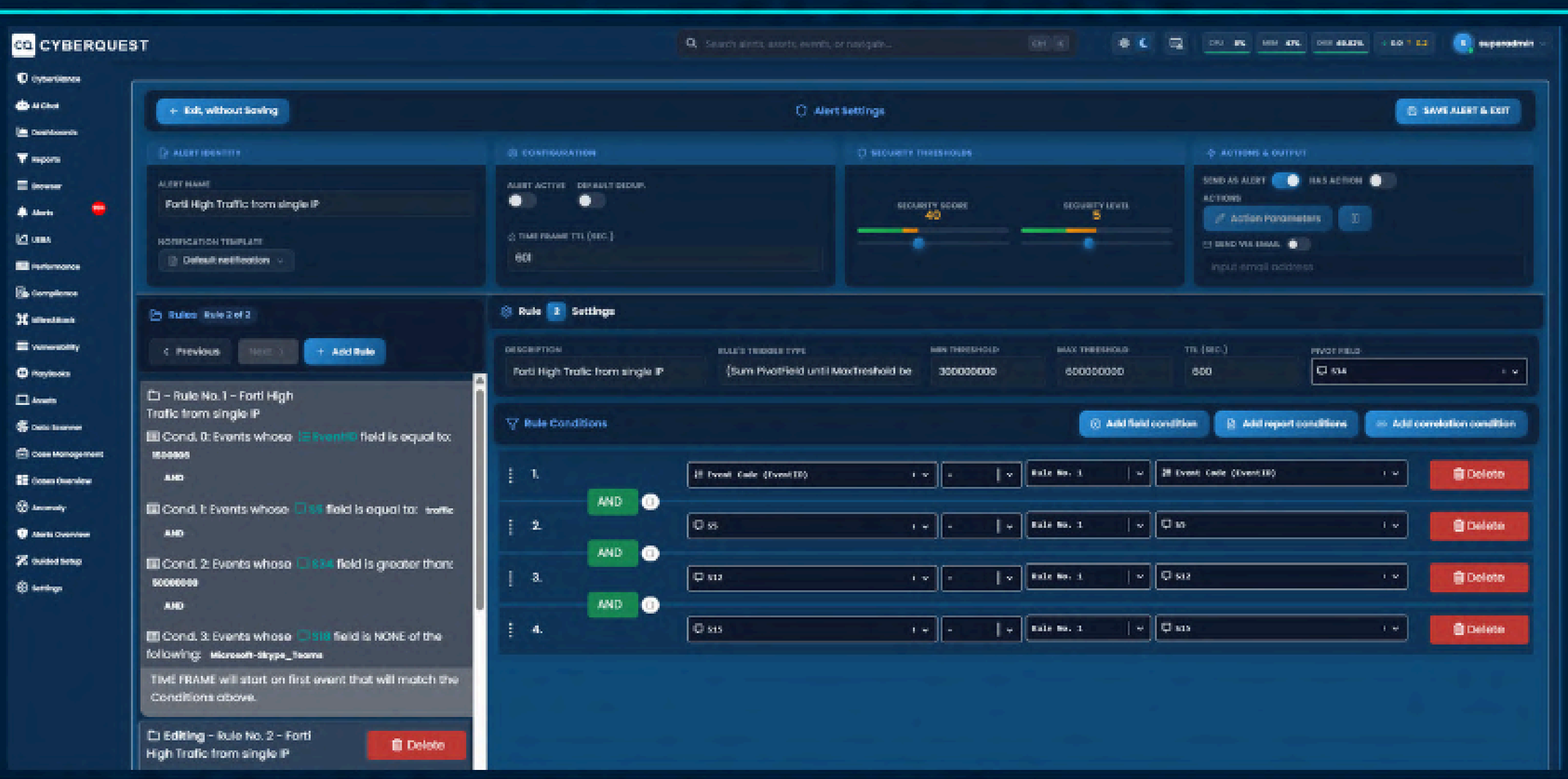
- Single event triggers and ordered sequences.
- Detect missing events and logical succession.

Aggregation & cross-source logic

- Count, average or sum on selected field values.
- Correlate multiple data sources.

Pivoting

- Pivot on selected fields to follow related activity.
- Useful in transaction-oriented investigations where a common identifier links records.



Correlation rule builder and multi-condition logic.

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