nextgen

ONE CONNECTED TECHNOLOGY ECOSYSTEM.

UEBA

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

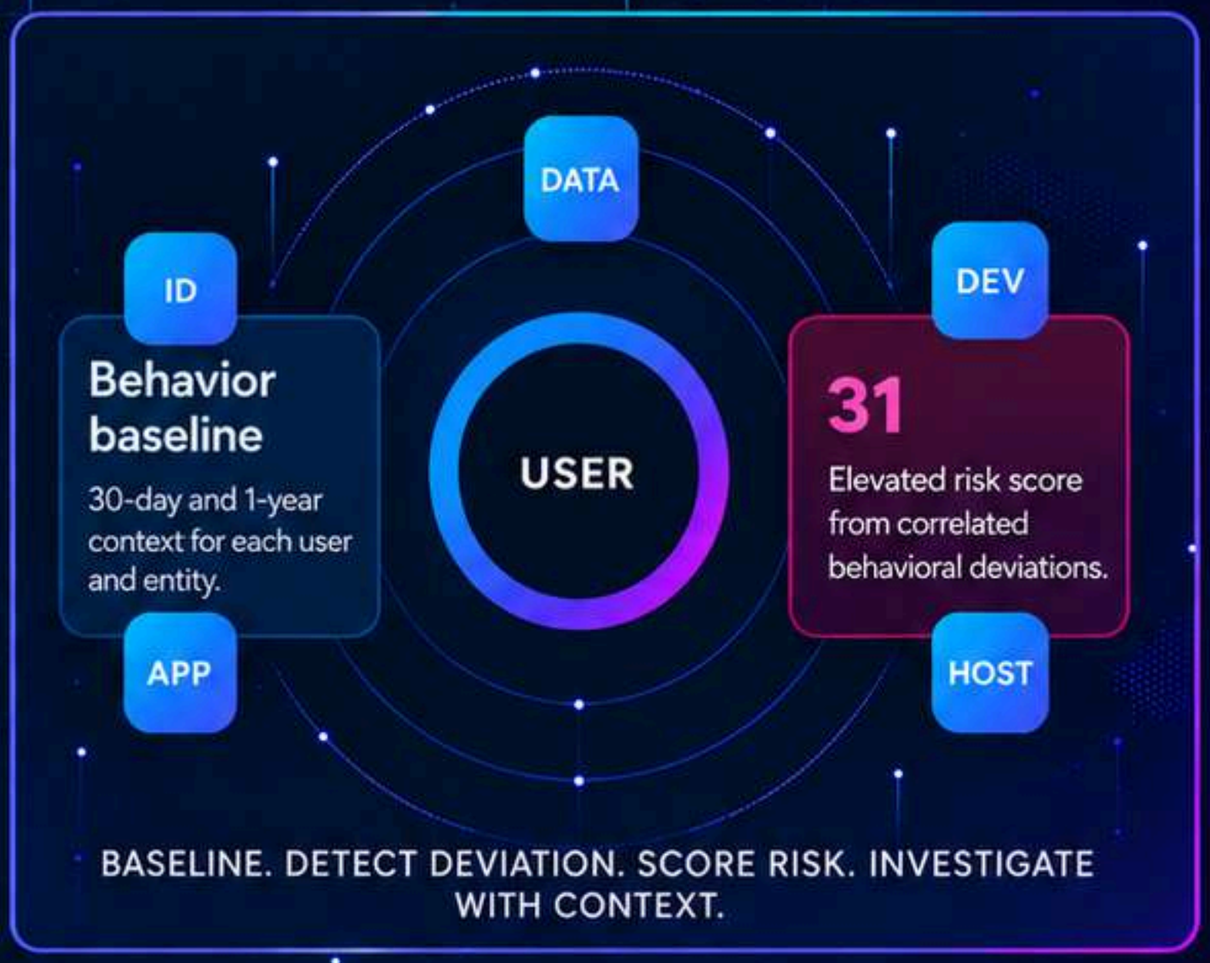
Stronger together. Safer every day.

UEBA
by Nextgen

Detect behavior that rules alone miss.

Establish baselines, spot anomalous activity and surface user and entity risk before it becomes incident impact.

BEHAVIORAL ANALYTICS · RISK SCORING · ENTITY BASELINES



33
detection scenarios
Covering users, devices, applications and other entities

30-day
baseline learning
Build behavioral baselines from real activity

1-year
historical context
Long-term analysis for stronger risk insight

KEY CAPABILITIES

Behavior baselining
Learn normal patterns per user and entity.

Risk scoring
Prioritize suspicious users and assets.

Anomaly detection
Detect deviations in accounts, systems and activity.

Insider risk visibility
Highlight misuse, policy drift and abnormal actions.

Peer group analytics
Compare users against relevant behavioral groups.

SIEM-linked investigation context
Feed UEBA findings into investigations and response.

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