nextgen

ONE CONNECTED TECHNOLOGY ECOSYSTEM.

CYBER DEFENSE CLUSTER

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.

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.

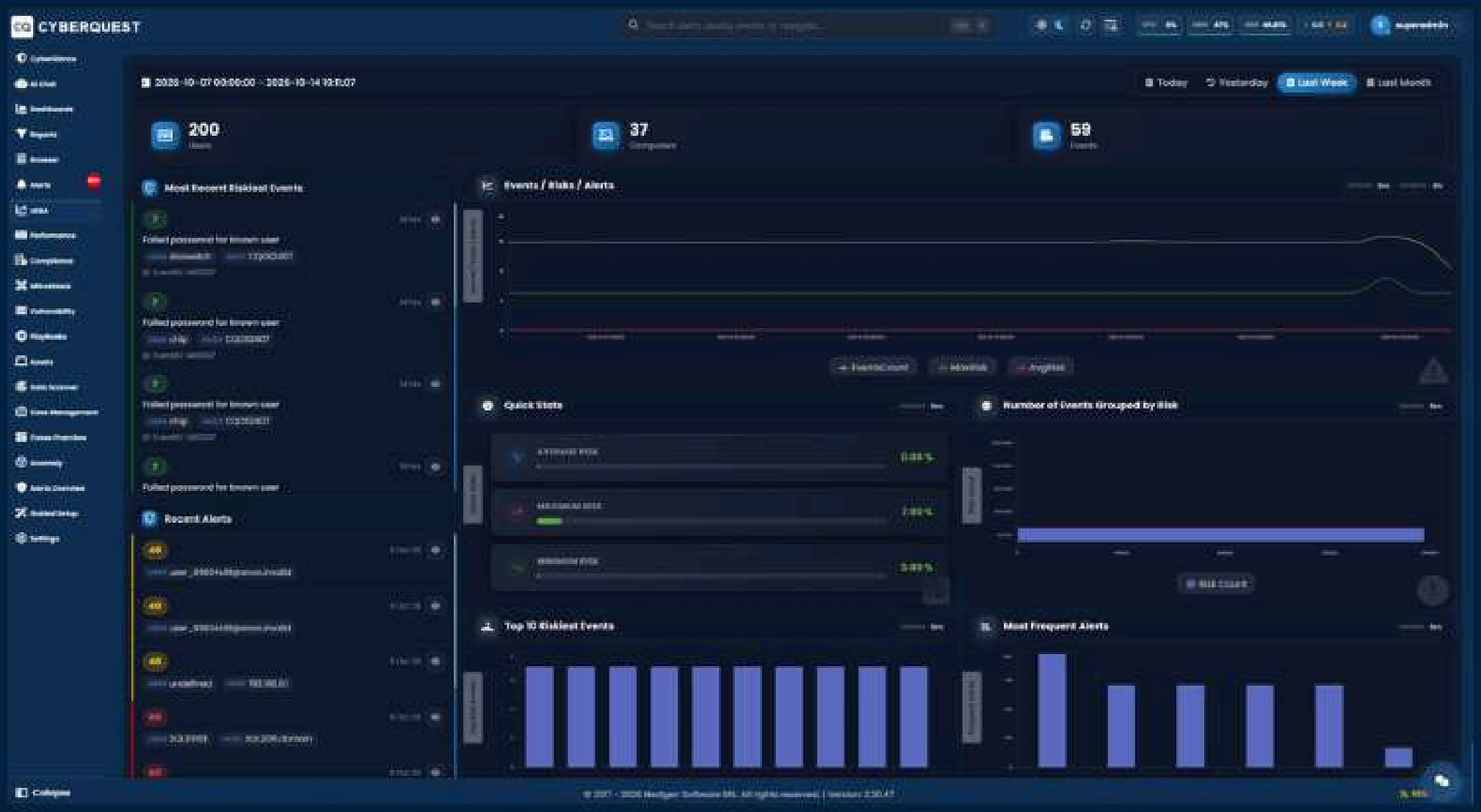
Cyberquest applies behavioral analytics to learn how users and systems typically behave and to flag abnormal activity in real time. This supports enriched alerts and risk context while the dedicated UEBA product provides specialized behavioral analytics.

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

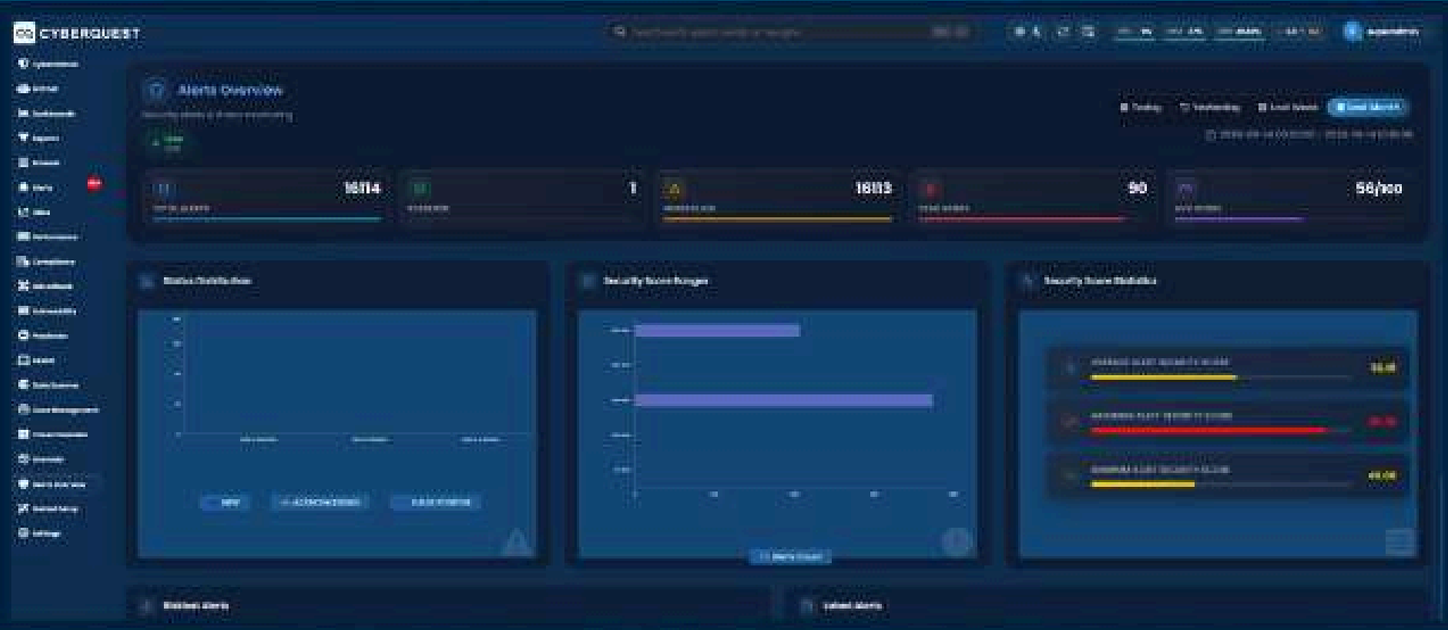
- Alert Name: Unique identifier for the alert.
- Alert Active: Enables or disables the alert.
- Sent as Alert: Supports backend correlation without user-facing notifications.

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

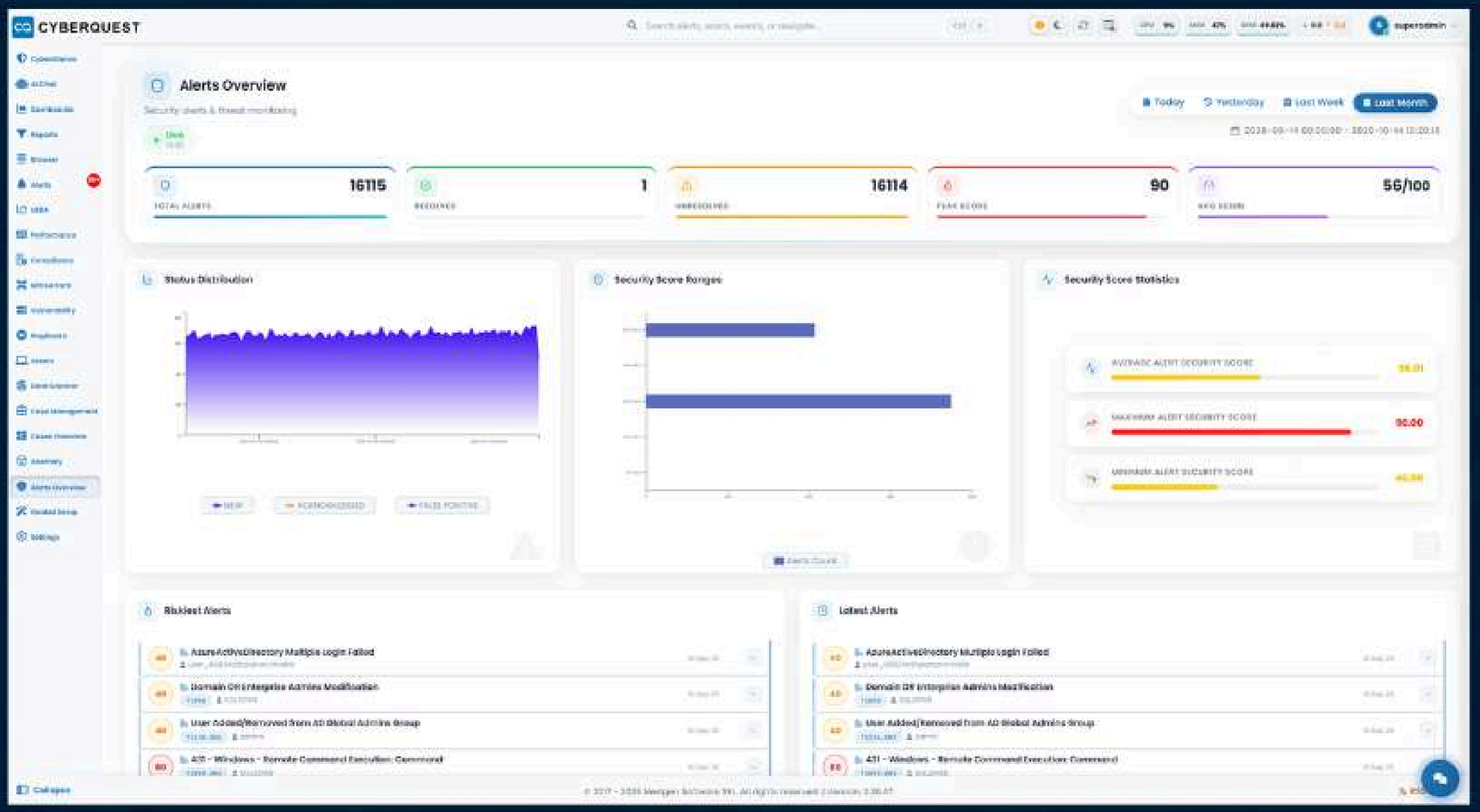
Move from detection logic to controlled action.

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

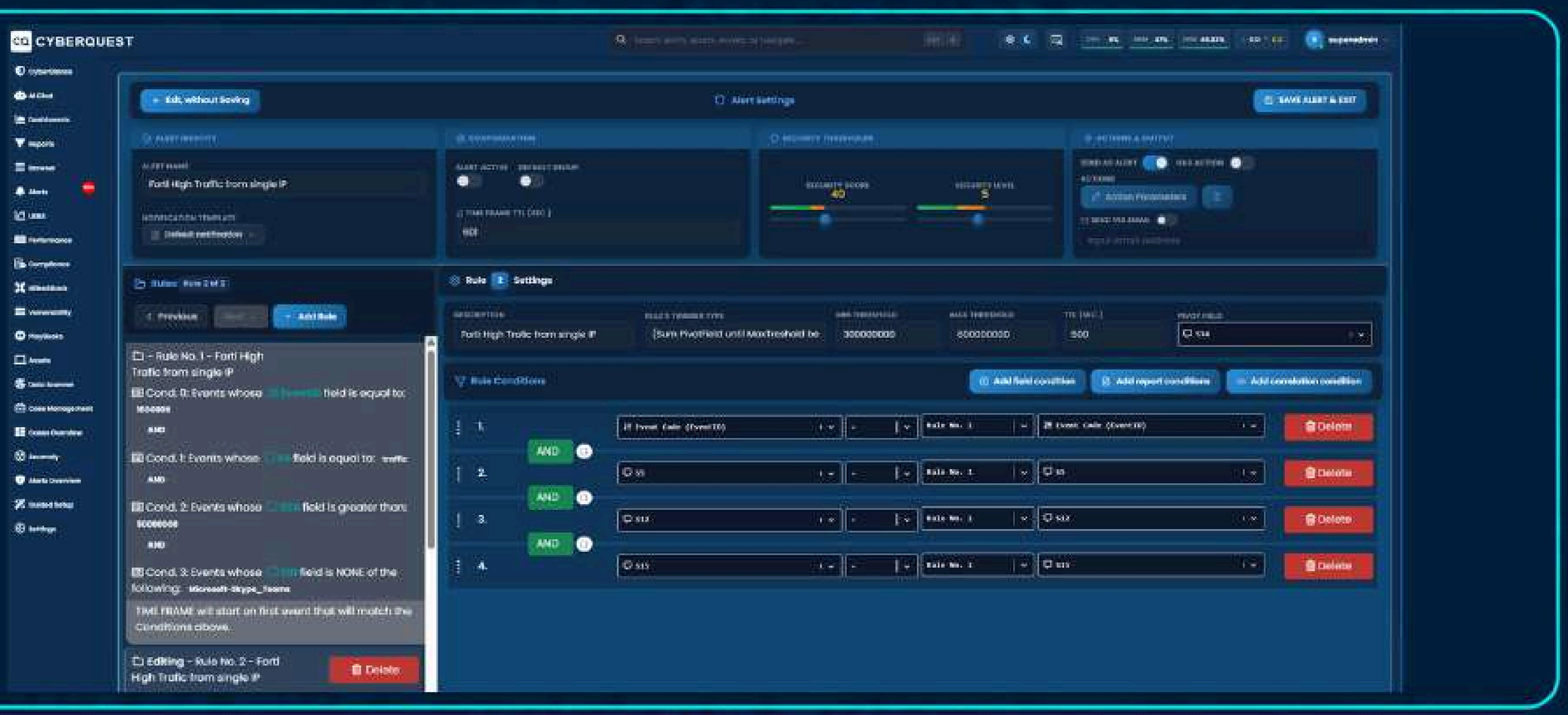
- Single event triggers and ordered sequences.
- Detect missing events and logical succession.

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.

CQ AUTOMATION

SOAR by Nextgen

Automate response. Orchestrate every action.

Turn complex incident workflows into fast, controlled and repeatable responses across the security stack.



AUTOMATED PLAYBOOKS | CASE MANAGEMENT | 270+ INTEGRATIONS

1,230+
automated actions

75%
fewer incidents requiring manual interaction

300+
playbooks

KEY CAPABILITIES

Graphical playbooks
Build reusable response workflows through a visual orchestration interface.

Case management
Coordinate investigation tasks, evidence and response in one workflow.

Security / IT integrations
Connect playbooks with third-party security and IT systems.

Execution traceability
Log actions, parameters and outcomes for audit and forensics.

Automated actions
Trigger controlled response actions directly from alerts and cases.

AI-assisted support
Accelerate playbook creation and repetitive response workflows.

Build automated response workflows visually and execute them with context.

A playbook is a sequence of actions grouped to perform a mitigation or response flow. Actions are added and removed through a graphical interface, while input parameters are evaluated dynamically at runtime.

Automatic triggering

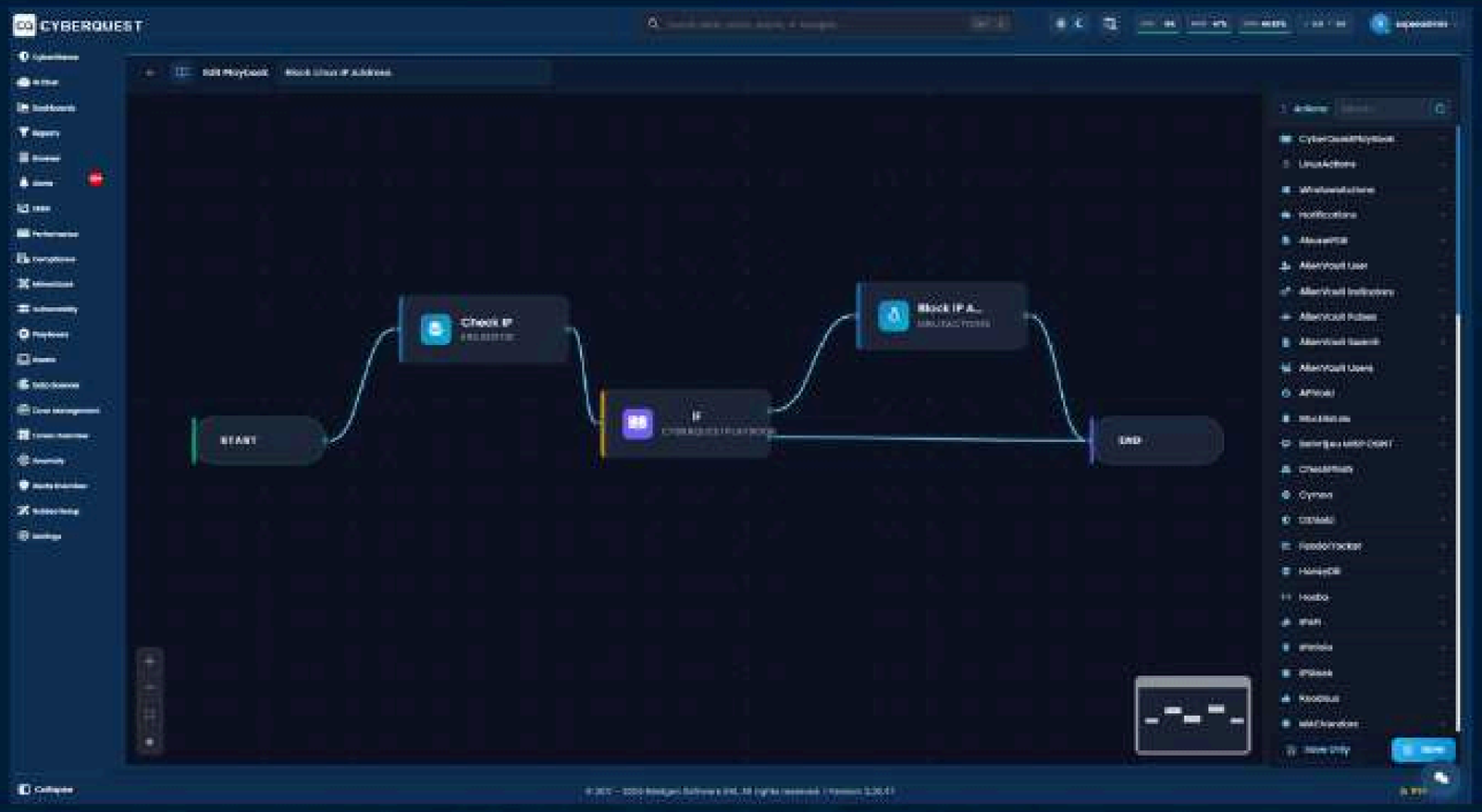
- Triggered by specific alerts.
- The alert instance becomes the global inputData for the playbook.
- Configured through the web graphical interface.

Manual triggering

- Launch from the Event Browser for a selected event.
- Launch from the Alert Browser for a selected alert.

Execution history

- Trace parameter values and action outcomes.
- Identify failures or misconfigurations in playbook logic.



Example of a multi-step playbook workflow.

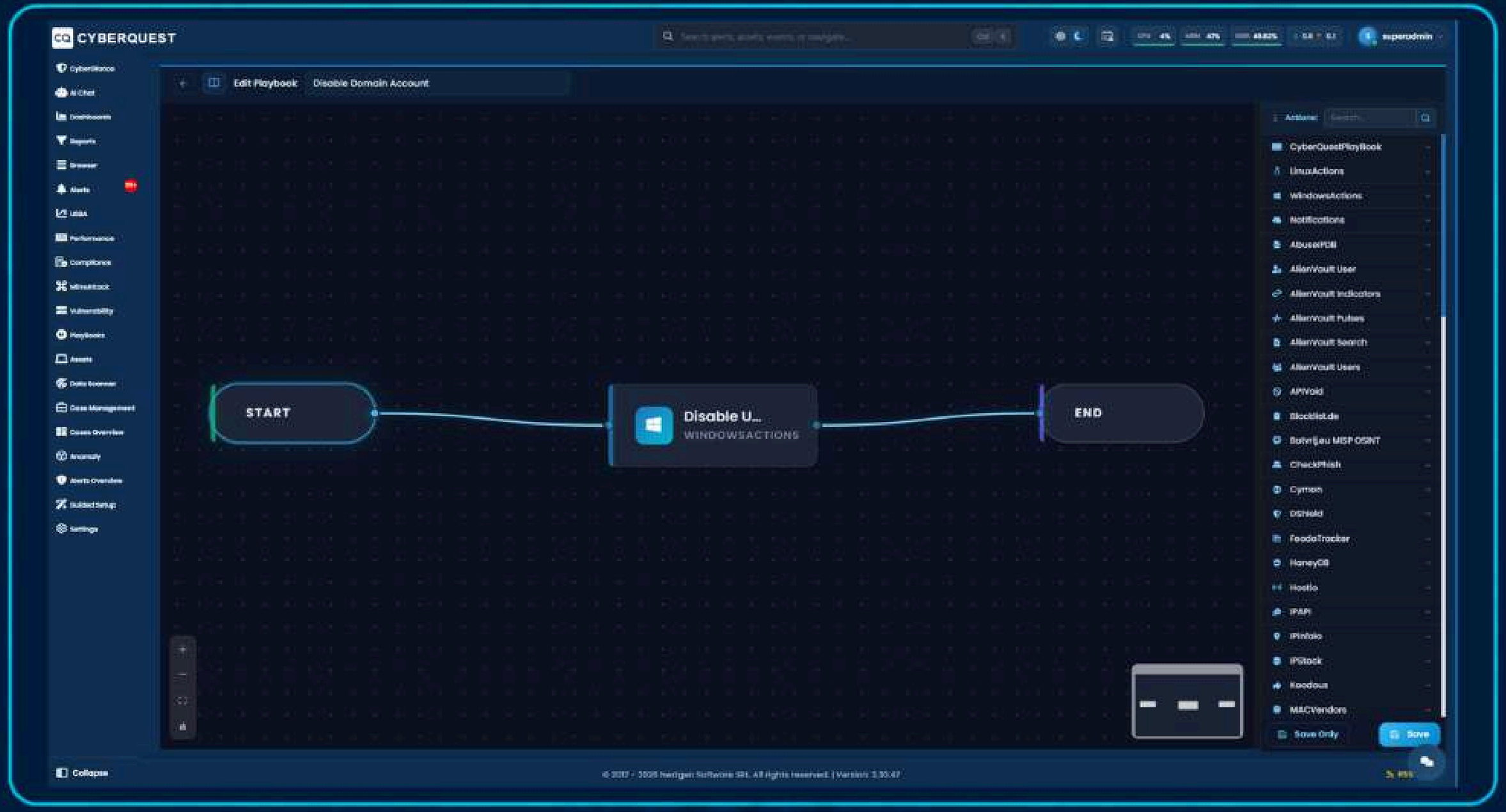
From focused actions to multi-system response flows.

Disable domain account

- Focused playbook for disabling a domain account as part of response.

Block IP in various systems

- Coordinate blocking across multiple systems and notify for each action.



Playbook example: disable domain account.

Combine vendor integrations with reusable functional logic.

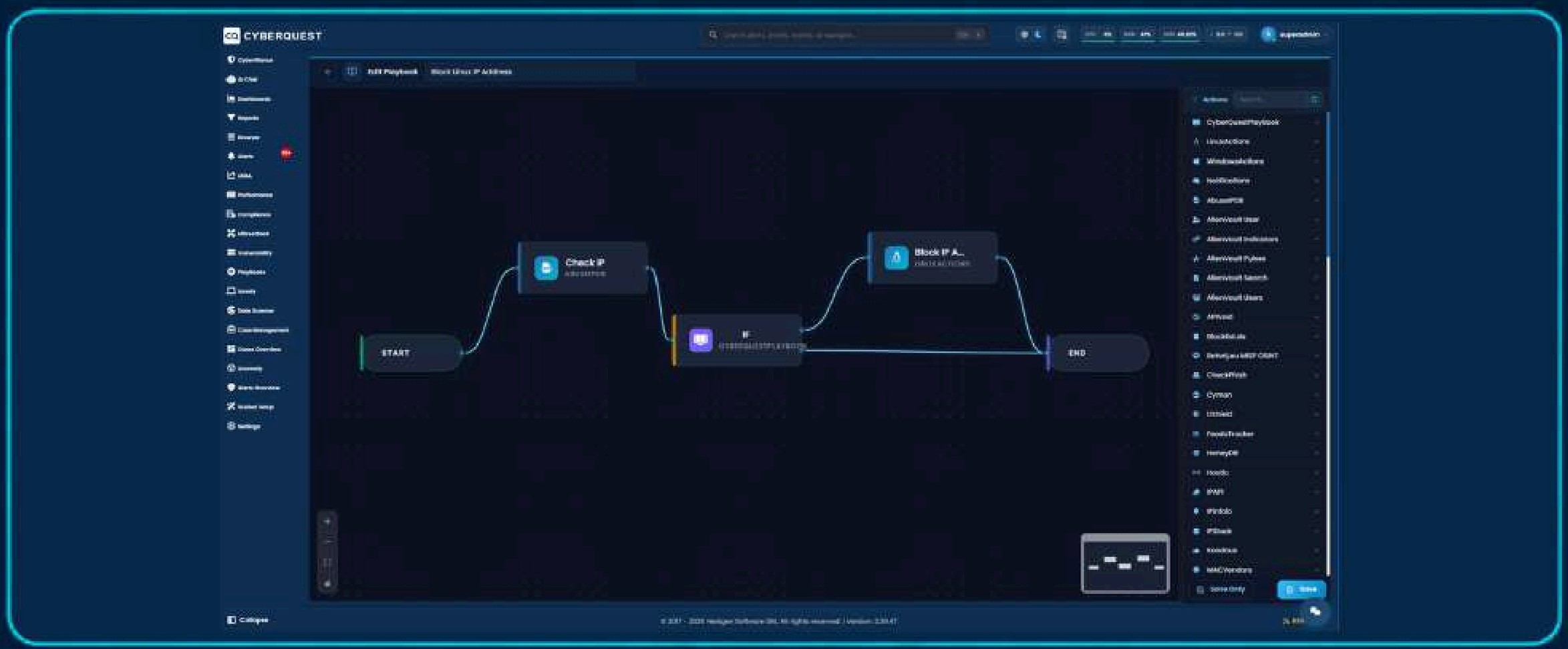
Actions form the building blocks of automated responses. They connect to external security tools or implement internal logic such as conditions, counters and custom scripts.

Vendor-specific actions

- Integrated with a growing list of security vendors.
- Use vendor APIs for blocking IPs, isolating hosts, updating firewall rules and sending notifications.

Functional actions

- IF: Conditional branching based on Boolean logic.
- Count: Counts elements in an array-type variable.
- Code: Executes a DTS object with custom JavaScript logic.



Bad IP detection and blocking.

Reusable automation with traceability built in.



Smart Playbook Features

- Dynamic Parameters: 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.



Audit & Forensics

- Every action is recorded for compliance, debugging and forensic analysis.
- Execution logging includes input parameters, result, timestamp and user ID if manual.
- Forensic reports are generated from execution history.

NETALERT NDR BY NEXTGEN

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.

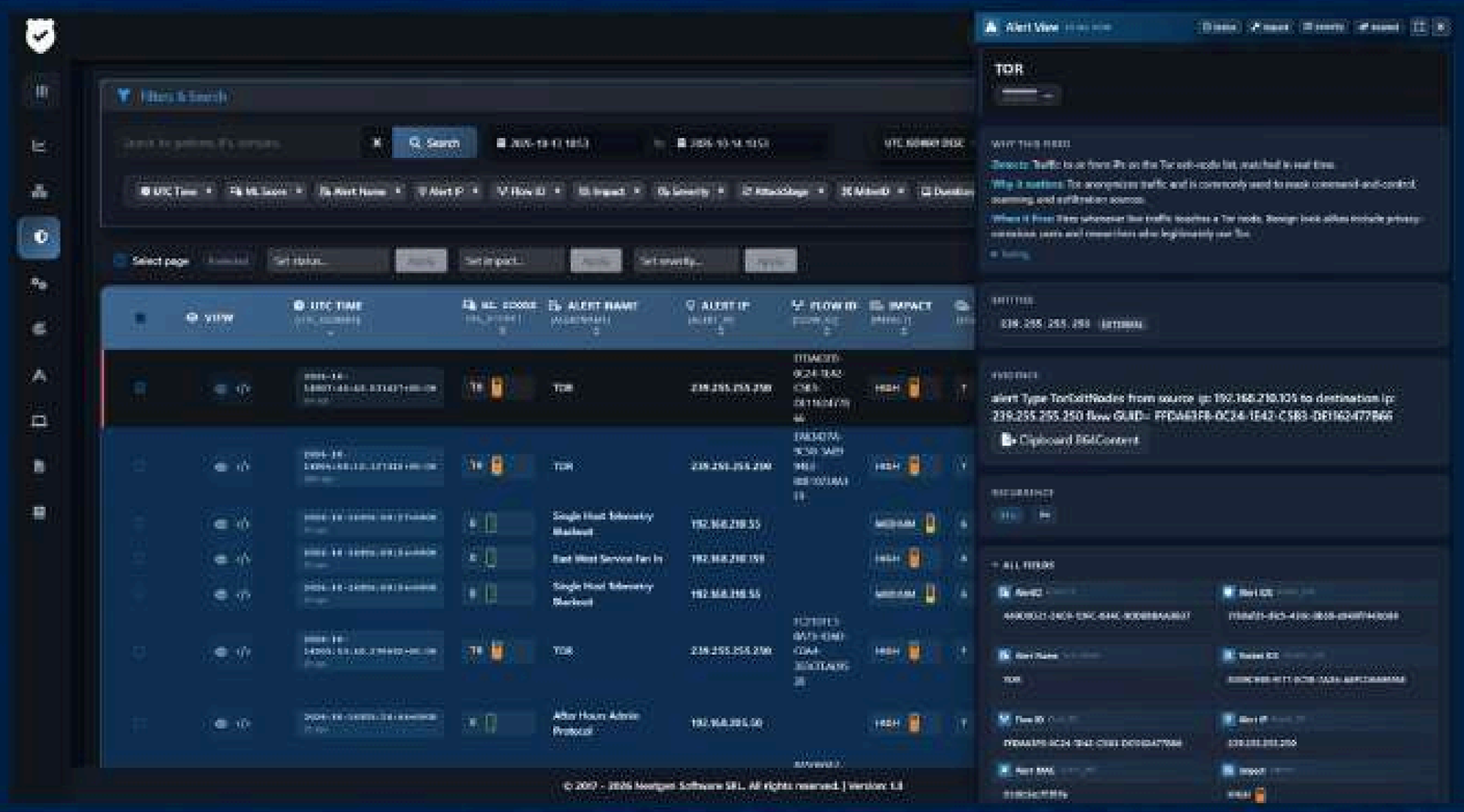
NetAlert NDR combines signature-based, heuristic and machine learning techniques and integrates threat intelligence feeds to detect known Indicators of Compromise.

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

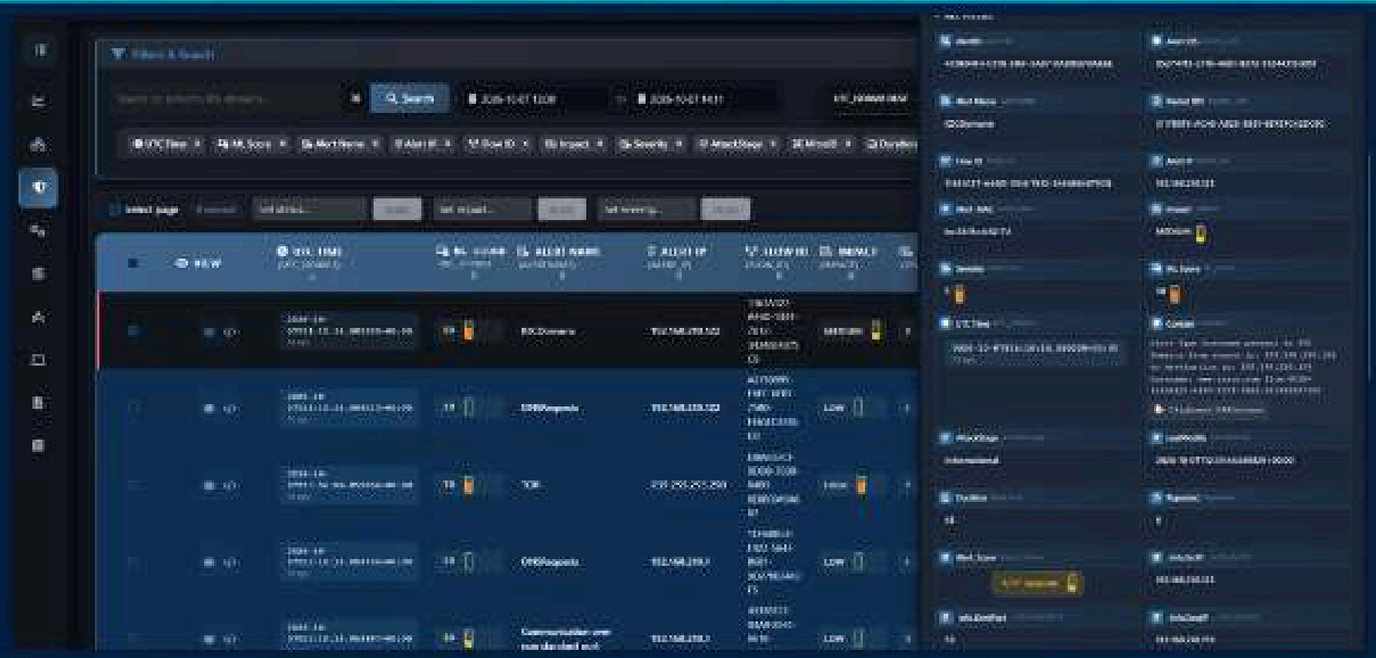
- Identifies mining-pool traffic and unusual patterns.

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

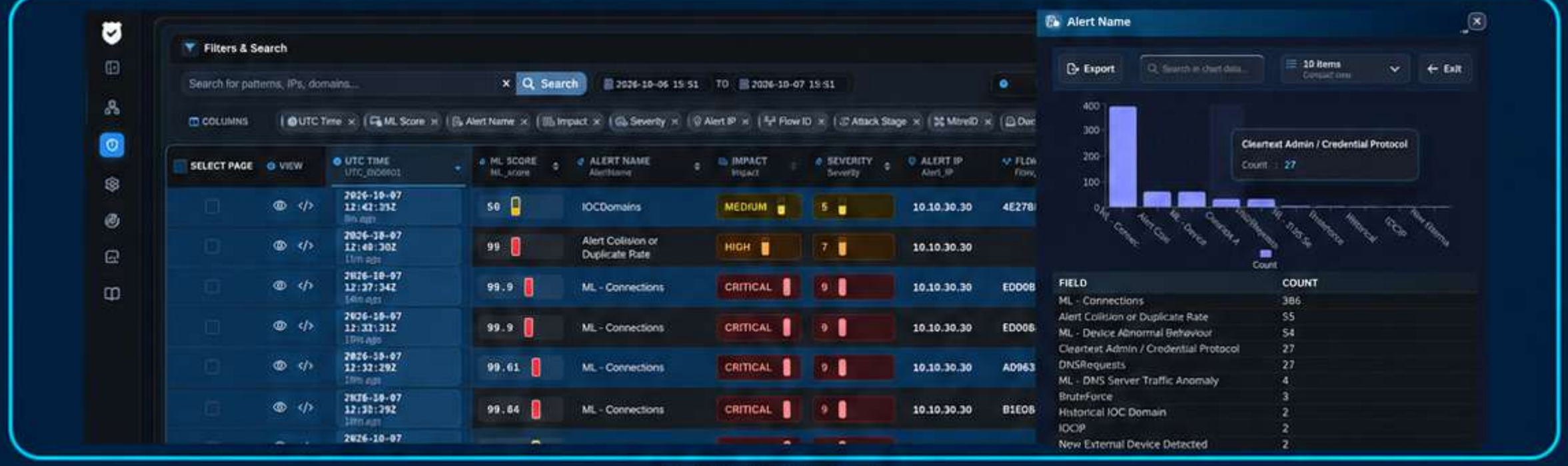
- Deep packet inspection of TLS heartbeat messages.

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.

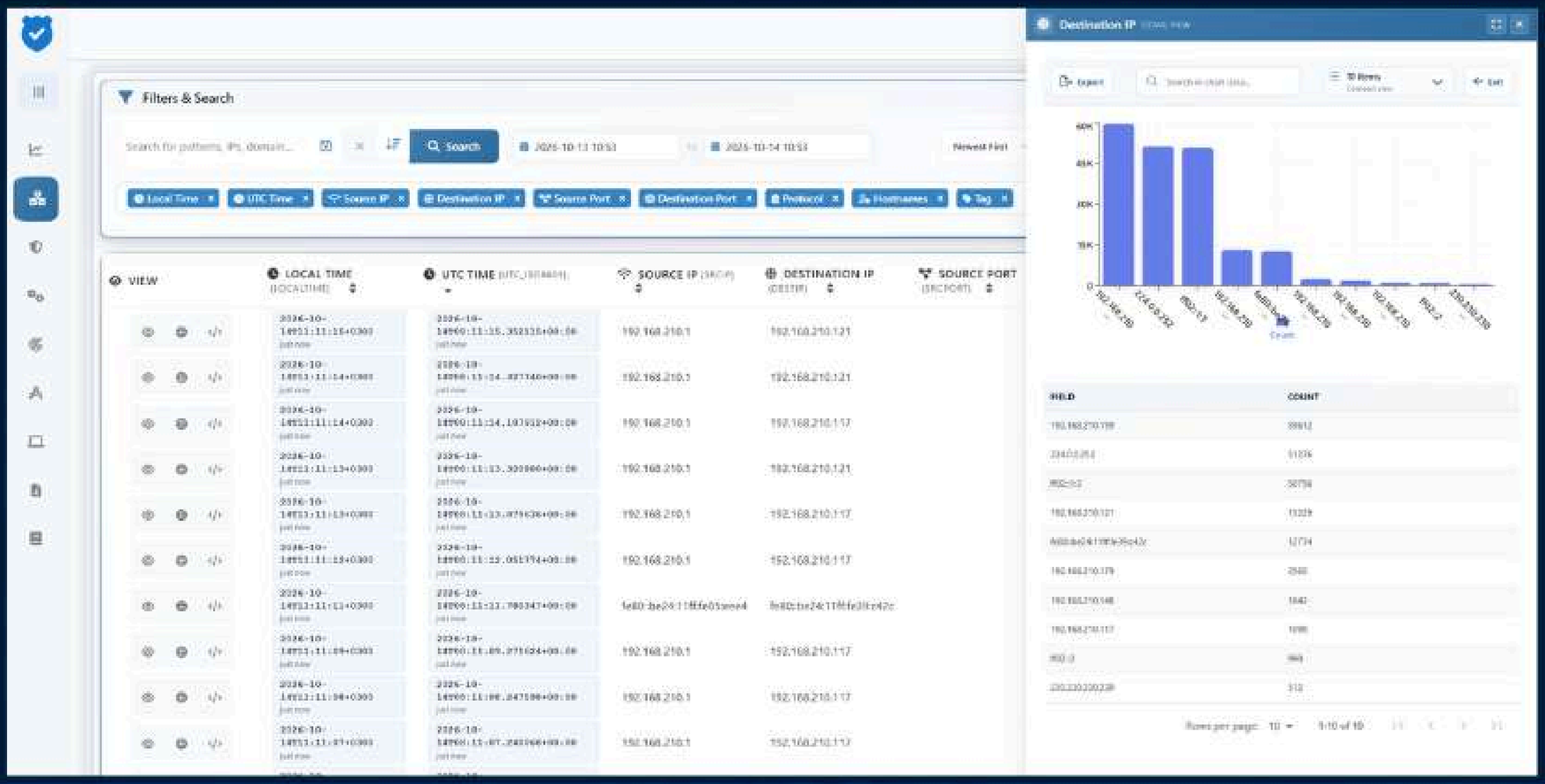
The system passively captures traffic via TAP/SPAN ports, aggregates TCP sessions and collects flow data across VLANs. It decodes DNS, SMTP and HTTP and supports PCAP recording for forensic analysis.

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.

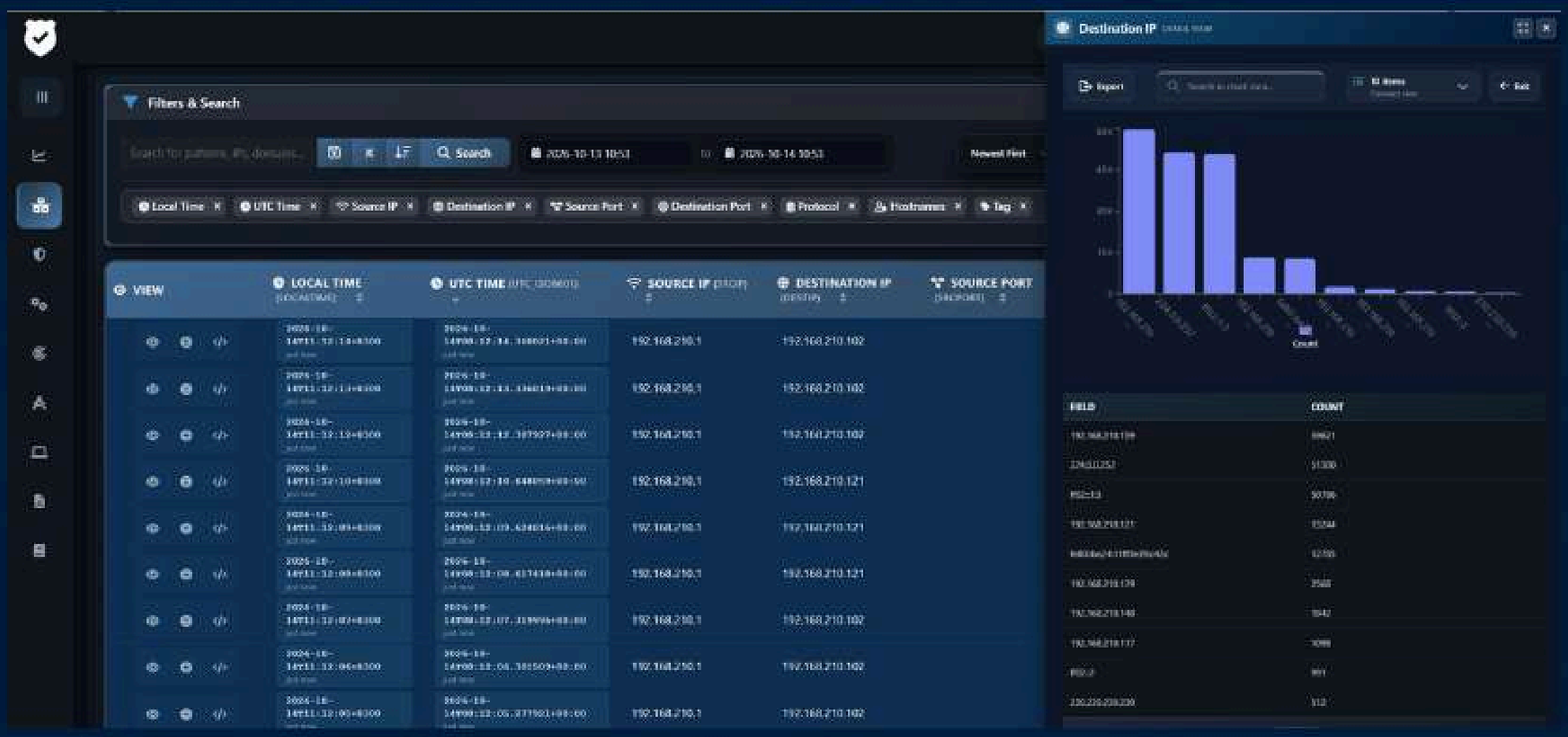
NETALERT
NDR by Nextgen

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.

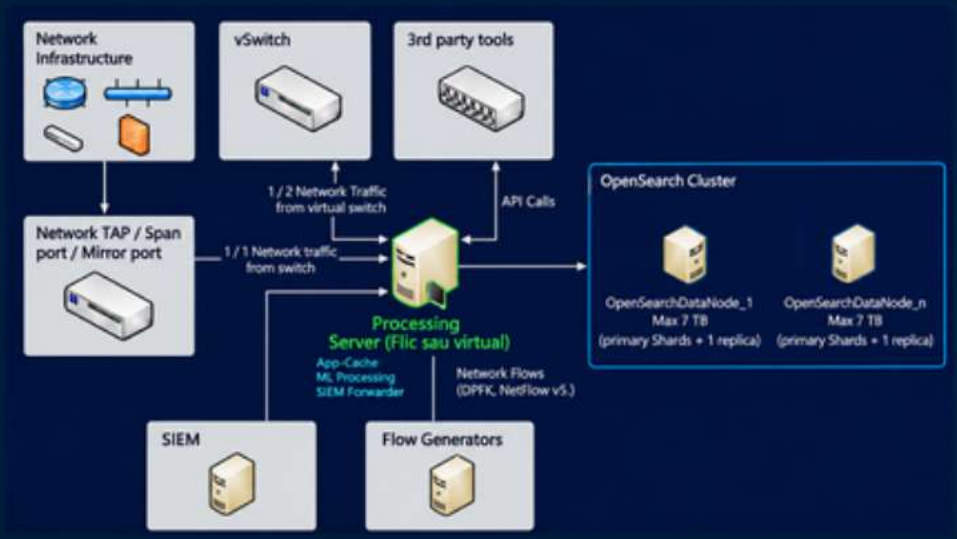
NetAlert is built on a modular Docker Compose architecture supporting single-node and distributed deployments. It provides real-time alerting, integrates with SIEM platforms and scales with available hardware resources.

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.

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

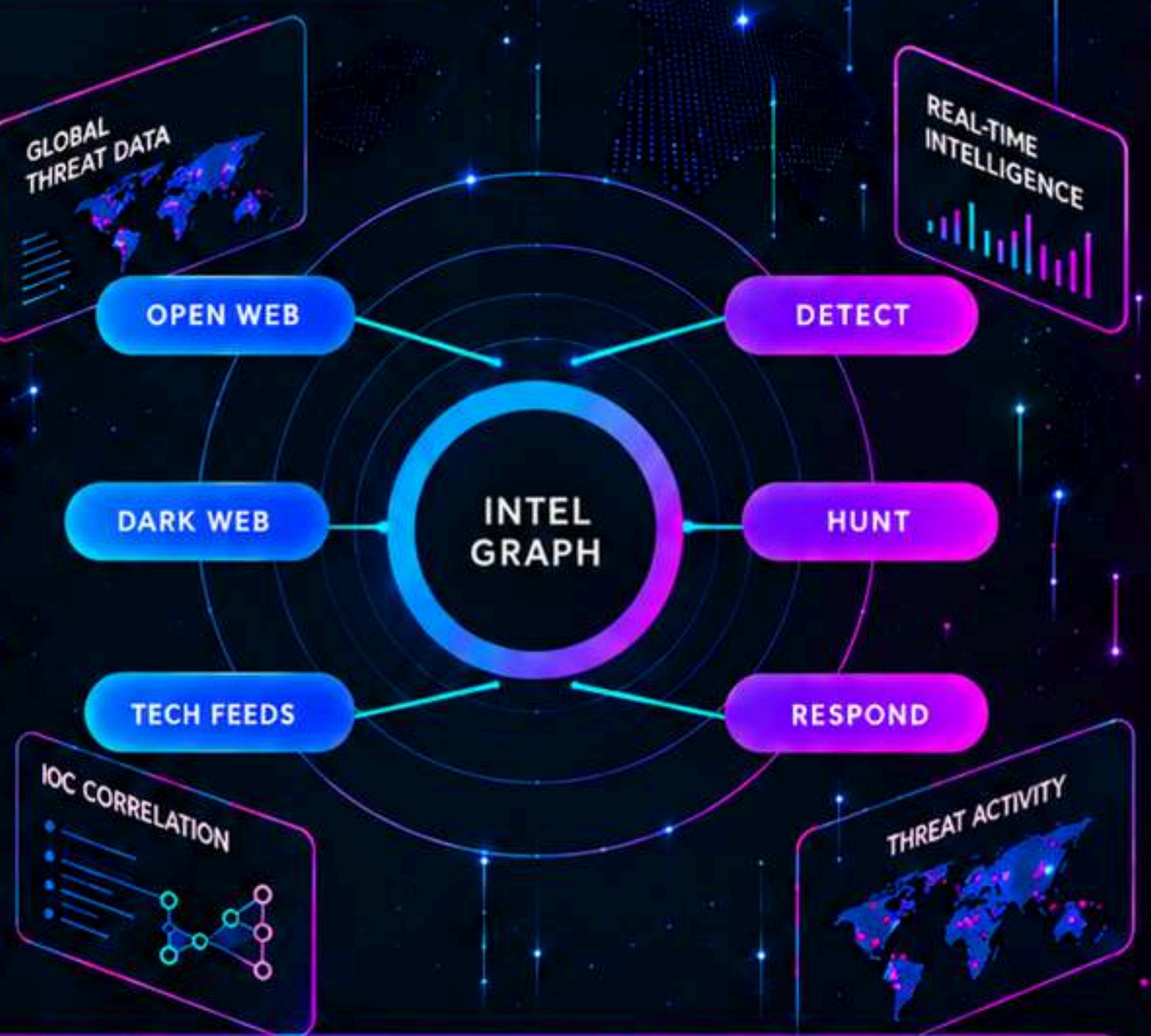
- No hardcoded limits on device count or EPS.
- Performance is hardware-dependent.
- Distributed deployment supports large-scale environments.

THREAT INTELLIGENCE
by Nextgen

Turn scattered signals into actionable intelligence.

Aggregate, enrich and correlate threat data from across open, deep and dark web sources to strengthen detection, investigation and response.

THREAT FEEDS · IOC CONTEXT · TRANSVERSAL INPUT



80+
providers
Including commercial, open and community sources

Public application
threats.cyberquest.cloud

8
context areas
Bridge the gap from threat data to real-world impact

KEY CAPABILITIES

IOC ingestion
Ingest IOCs from multiple sources.

Enrichment
Add context from internal and external sources.

Data exploration
Search, connect and explore indicators, entities and relationships.

Correlation context
Link threats across alerts, assets and actors.

Reputation & investigation
Assess risk and guide analyst decisions.

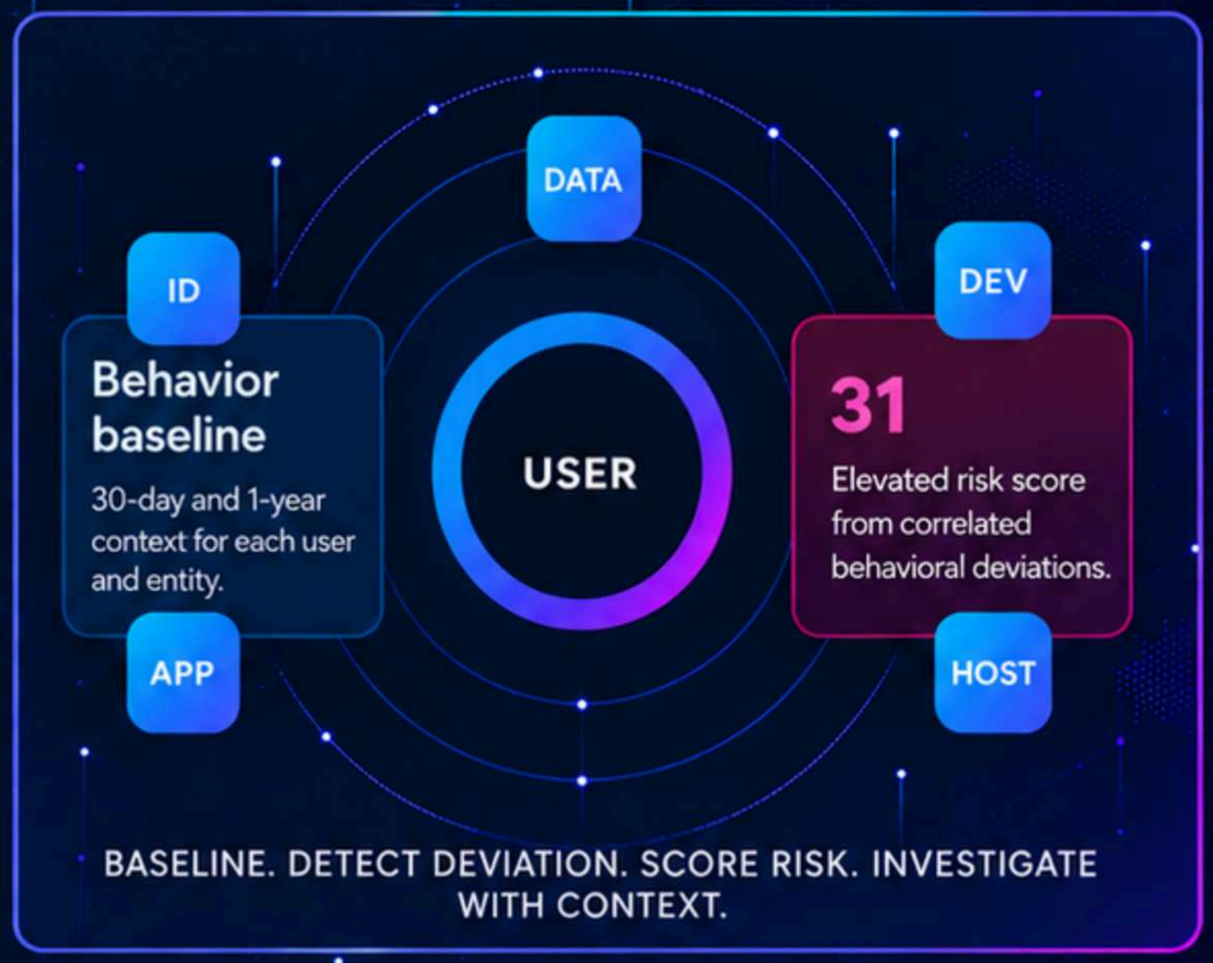
Integration with SIEM
Enrich detections and investigations automatically.

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.

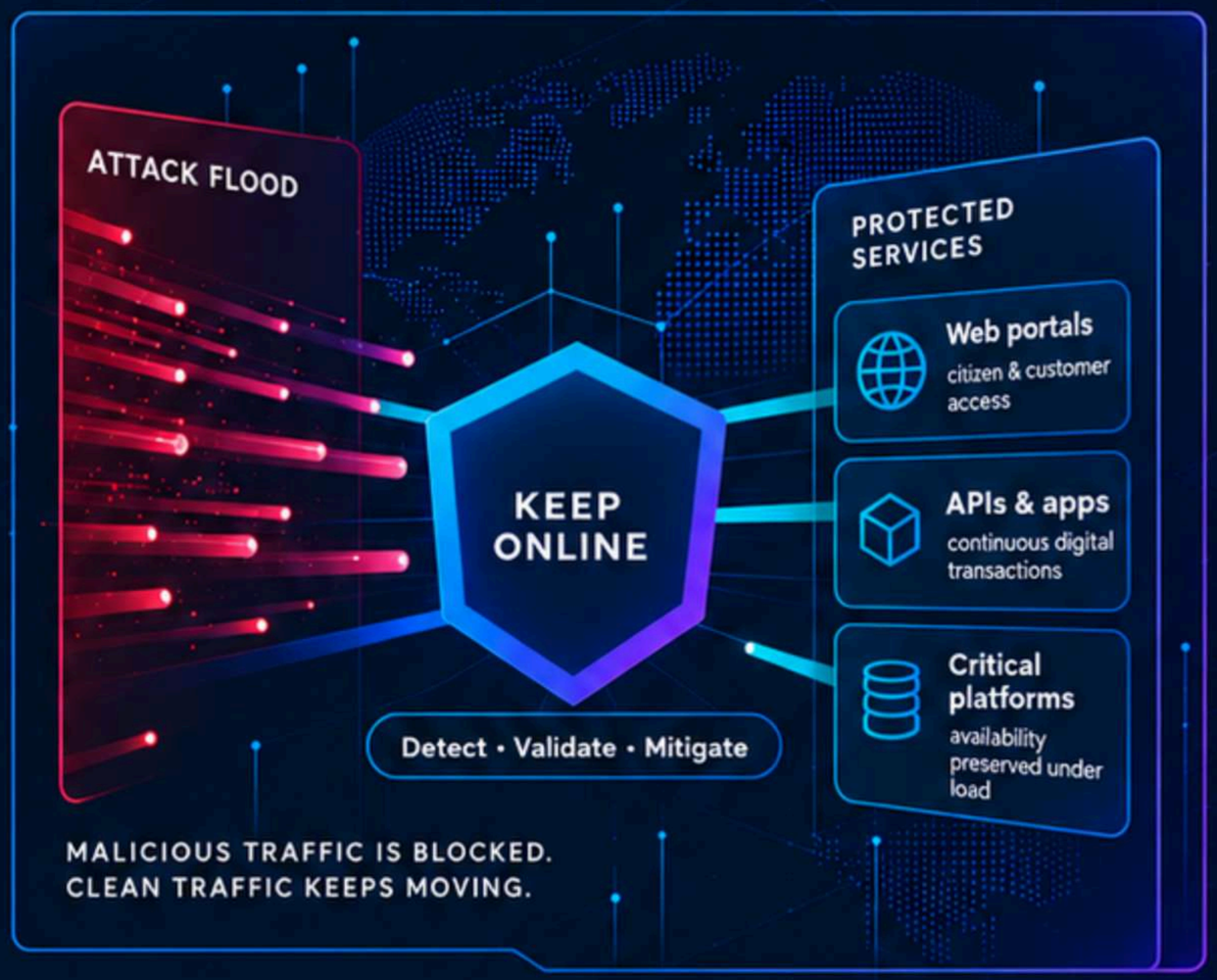
SIEM-linked investigation context
Feed UEBA findings into investigations and response.

DeDDoS by Nextgen

Keep critical services online under pressure.

Protect availability with continuous DDoS detection, validation and mitigation control for critical online services.

- CONTINUOUS CONTROL
- SERVICE AVAILABILITY
- AUTOMATED MITIGATION



10 Gbps
mitigation target
Designed to mitigate high-volume attacks.

30 min
TTL
Keep services available with rapid response.

Closed-loop protection
Detect, validate, mitigate and adapt continuously.

KEY CAPABILITIES

Attack detection
Identify volumetric and protocol-based DDoS activity.

Traffic validation
Distinguish malicious traffic from legitimate usage.

Mitigation policies
Trigger controlled response and filtering actions.

Service continuity
Protect critical services while maintaining availability.

Automated control loop
Support fast response without manual delay.

Monitoring & reporting
Track events, actions and service posture.

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