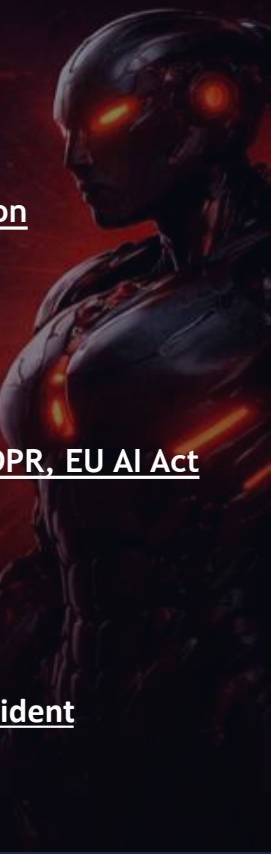

nextgen
Agentic Investigations
The future of Security Operations
How AI is transforming security investigations and redefining the SOC Analyst’s role

AGENDA



Why traditional SIEM is no longer enough

4,484
Enterprise security Alerts per day

40%
Uninvestigated alerts

80%
False positive rate

4.8M
Global shortage of security analysts

Core limitations

- EPS-based licensing → explosive cost growth as data volumes rise (+28% YoY)
- Static correlation rules → excessive noise, with 30% of time lost to false positives
- Weak support for cloud/hybrid environments and limited integration with modern tools
- Scaling becomes impossible without proportional hiring (4.8M unfilled roles globally)
- Burnout and churn exceed 25% annually in SOC teams (SANS 2025)

CYBERQUEST: Next Generation SIEM

CPU-core licensing

No EPS limits in the Ultimate edition. Performance depends on allocated resources, not on event volume.

Dual Storage

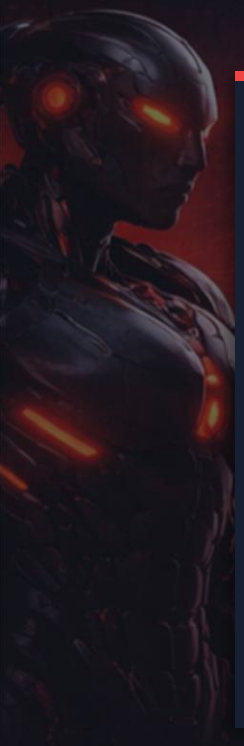
OpenSearch for sub-second queries, plus DataStorage with ~1:20 compression, AES-256 encryption, and PGP-signed files.

DTS Engine

Normalization via a JavaScript engine - custom parsing, enrichment, and anonymization. Turning noise into intelligence.

“Security-Driven Analytics Platform” - far beyond log management

AI: Accelerating both Attack and Defense



AI-Powered Attacks

- 82.6% of phishing emails now use AI
- AI-driven phishing attacks grew by 703% (2024–2025)
- Deepfakes surged from 500K to 8M (2023–2025)
- Over 70% of breaches involve polymorphic malware
- eCrime breakout time: 29 minutes on average / 27 seconds at fastest

AI-Powered Defense

- Alert fatigue reduced by 70–90%
- Investigation time cut to 3–4 minutes, from 15–20 minutes
- Breaches resolved 80 days faster
- Average breach cost without AI: $4.88M10x faster investigations with Cyberquest

CYBERQUEST AI: Capabilities

CQ AI Assistant

Conversational queries → precise commands with built-in explanations
Anomalous pattern detection & proactive AI-driven alerts
Error-free execution & guided onboarding
Natural language → automated investigations

NetAlert ML

5 models ML ensemble
IForest, KNN, LODA,
LOF, OCSVM
Confidence scoring

Anomaly Module + Smart Objects

Continuous monitoring with advanced analytics | 33 behavioral scenarios | 30-day / 1-year baselines | Automated deviation detection

Demo: Investigation workflow

1 Detection

Real-time DTS parsing with 500+ built-in alerting rules enabled

2 Triage

Alerts Module: New → Acknowledged → Investigated → Closed

3 MITRE

Automated ATT&CK mapping - real-time tactics and techniques

4 Investigation

Visual investigations: dynamic correlation across custom fields

5 Case

Case Management with SLAs, templates and evidence attachments

6 Response

Automated playbooks: block IP, disable user, kill process

Agentic Investigations: Concept

Traditional AI

Flags a suspicious login (pattern recognition)

Generative AI

Summarizes the alert for the analyst

Agentic AI

Investigates the login: queries identity logs, correlates endpoint data, cross-references threat intelligence, executes containment - in seconds

73% of organizations are using or developing agentic AI in cybersecurity (2026)
89% of CISOs are accelerating adoption

5 key characteristics of Agentic AI in the SOC

Goal-Oriented	Goal-oriented behavior, not just reactions to patterns
Context Awareness	Complete contextual understanding: identity, asset, timeline
Multi-Step Reasoning	Multi-step reasoning - correlates signals across systems
Action-Driven	Autonomous containment execution based on confidence thresholds
Self-Improvement	Continuous learning from feedback and previous outcomes

UEBA: Eliminating Blind Spots

33 behavioral scenarios | 30-day + 1-year baseline | Alerts on deviations from normal

Windows Logon (14)

7 success + 7 failure scenarios
Interactive, Network, Batch, Service, Remote, Cached

Service Activity (6)

New services, user-service combinations, service-PC combinations1-year history

Linux/SSH (5)

SSH, SUDO, SU monitoring
Per computer and source IP

VPN Behavior (2)

Logins from new countries
New client Ips
Impossible travel

File Monitoring (6)

Move, delete, create, modify, rename, access events
Exfiltration data

Unified Visibility: the foundation for AI

270+

Native connectors

Endpoint

Windows WMI, Linux syslog, OSSEC HIDS, Bitdefender

Network

CheckPoint, FortiGate, NetFlow v5/v9/v10, IPFIX, sFlow

Cloud & Apps

AWS CloudTrail, O365, Apache, NGINX, IIS

DTS (Data Transformation System):Normalization → Enrichment (GeoIP, TI, AD) → Anonymization → Feed for AI, correlation and UEBA

Correlation across full attack chains

Recon	Initial Access	Persist.	Lateral Mov.	C2	Exfil.
SSH, RDP, SMB scans DNS/DB recon	Brute force Impossible travel	Group changes GPO modified	Multi-IP logon Multi-host logon	DNS malicious Blacklist IP	DNS exfil, FTP P2P, IM transfers

500+ pre-built correlation rules

5 types: Real-time, Summary, Correlated (multi-step), DTS (JavaScript), Anomaly (baseline deviation) | Real-time MITRE ATT&CK mapping

MITRE ATT&CK: real-time visualization

MITRE ATT&CK module in CYBERQUEST:

- Extends the Alerts module with automatic mapping to the ATT&CK framework
- Alerts are generated and mapped in real time to tactics and techniques
- Detailed analysis of the tactics and techniques used by attackers
- Correlates alerts across tactics to visualize full attack chains
- Context: one threat actor used AI across 12 of 14 ATT&CK tactics

14 correlated ATT&CK tactics

Case Management assisted by AI

Create → Open → Solved → Closed → Archived

Evidences

Events, alerts, and notes attached as evidence to each case

Templates

Reusable templates for standardized investigations

SLA

Defined confirmation and response times by case type

AI Investigation

CQ AI Assistant: natural language queries directly on data

Automated audit trail: every case generates digitally signed, framework-mapped compliance artifacts

Incident Response Automation

1,230
Automated actions

95+
3rd party integrations

SOAR
Native capability

Playbook Building Blocks

- IF/THEN conditional branching
- RunPlayBook (nested execution)
- ForEachRunPlayBook (loop iteration)
- Code (custom JavaScript via DTS)
- Analyst Input (human-in-the-loop)
- Global state management (Key/Value)

Response Actions

- Network: Block/Unblock IP, Domain, Subnet
- Identity: Disable User (AD/Linux), Reset PW
- Endpoint: Kill Process, Stop/Restart Service
- Comms: Teams, Slack, Email, SMS, Twilio
- TI: VirusTotal, AbuseIPDB, OTX, MISP, 30+
- ITSM: ServiceNow, Jira, Zendesk, Opsgenie

Compliance in AI era: NIS2, DORA, GDPR, EU AI Act

NIS2 (Law 124/2025 RO)

Real-time alerting + SOAR → 24-hour notification

270+ connectors → supply chain monitoring

Audit-ready documentation for the board

Agentless OT module for industrial environments

DORA

Automated DORA reporting

Digitally signed, timestamped logs

Investigation timelines = audit trail

Planned integration with BNR + DNSC

GDPR + EU AI Act

Data anonymization in DTS (Art. 25)

RBAC, configurable retention, AES-256

Analyst input = human oversight (AI Act)

Digital evidence for auditors

Compliance as a natural outcome of operations - not as an added effort

The SOC of 2026

Only 7% of organizations are equipped with AI to counter AI-driven attacks - a massive opportunity

Autonomous triage at scale

AI triazează 100% din alerte (vs 40-60% manual)
3-10 min vs 60-90 min

Threat Stories

Narațiuni corelate: identitate + comportament + asset + timeline

Natural Language SOC

Analiștii lucrează în limbaj natural, nu în query-uri complexe

Phased autonomy

High-confidence → automat
Low-confidence → human-on-the-loop

"From AI Assistants to AI Agents — systems that actively execute detection, investigation and response"

CYBERQUEST ecosystem

CYBERQUEST SIEM

Core: collection, correlation, detection, visualization, UEBA, compliance

CQ Automation

SOAR: playbooks, 1,230 automated actions, 95+ integrations

Cyber Minds

Gen AI: natural language queries, guided investigation, onboarding

CQ Threat Intelligence

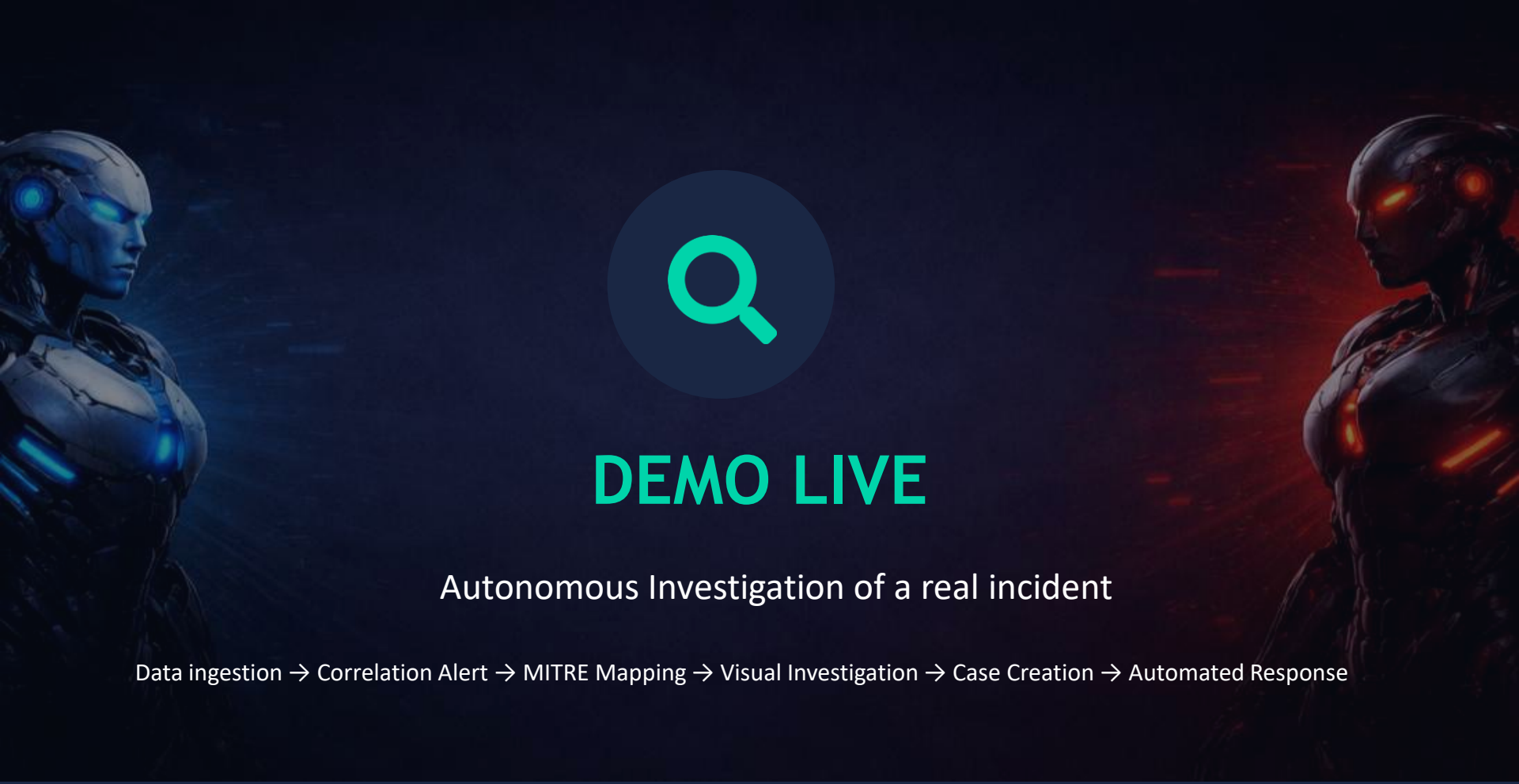
TI aggregation: 30+ providers, real-time correlation, IOC management

NetAlert NDR

Network detection: ML-based anomaly detection, DPI, flow analysis

Smart Objects + DTS

Behavioral baselines (33 scenarios) + parsing, enrichment, normalization



DEMO LIVE

Autonomous Investigation of a real incident

Data ingestion → Correlation Alert → MITRE Mapping → Visual Investigation → Case Creation → Automated Response


CYBERQUEST
Agentic Investigations - Faster investigations. Better decisions.
www.nextgensoftware.eu| office@nextgensoftware.eu
Questions?