nextgen

ONE CONNECTED TECHNOLOGY ECOSYSTEM.

CQ AUTOMATION

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.

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.

AUTOMATION
SOAR by Nextgen

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

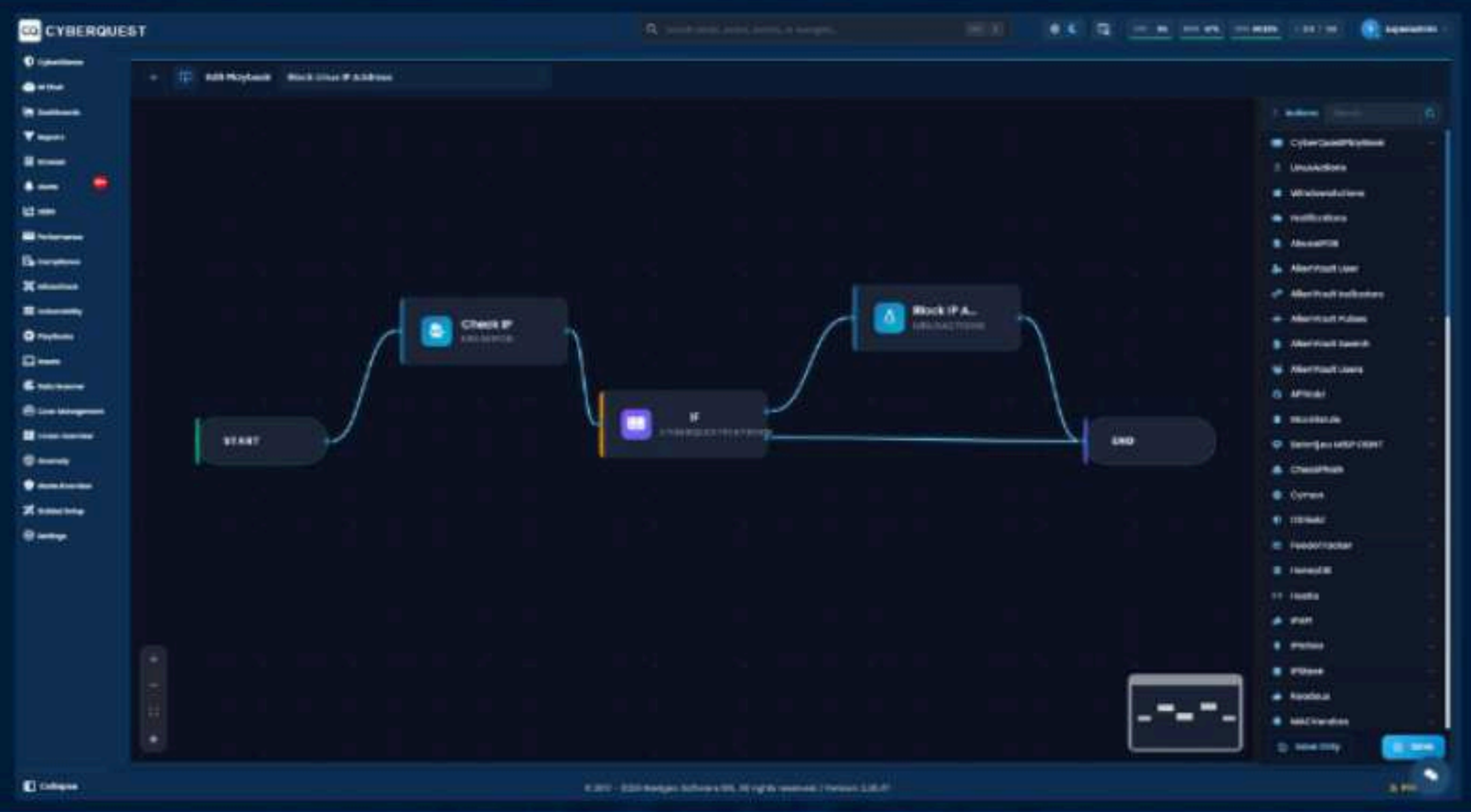
- Triggered by specific alerts.
- The alert instance becomes the global inputData for the playbook.
- Configured through the web graphical interface.

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.

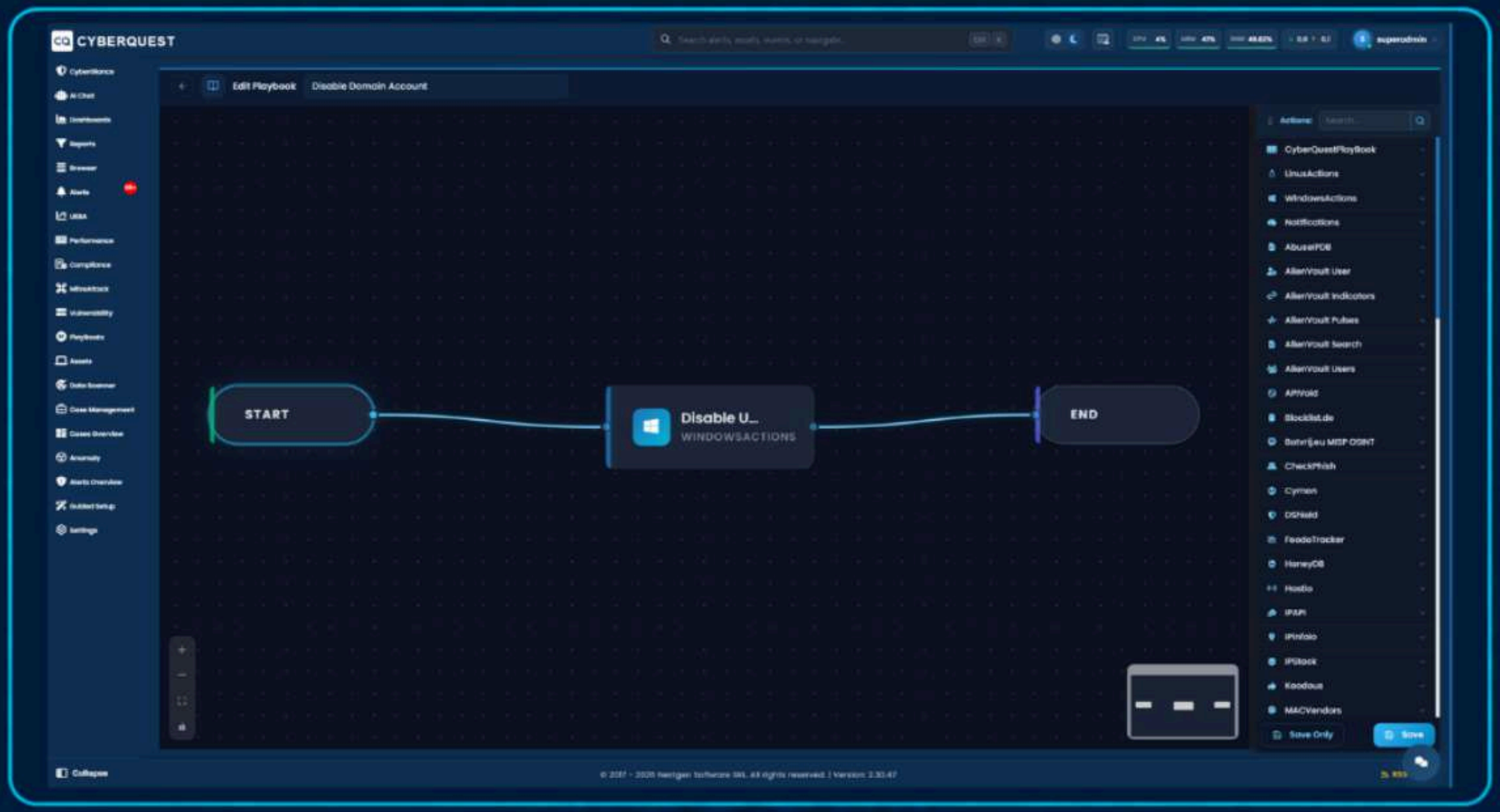
From focused actions to multi-system response flows.

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.

AUTOMATION
SOAR by Nextgen

Combine vendor integrations with reusable functional logic.

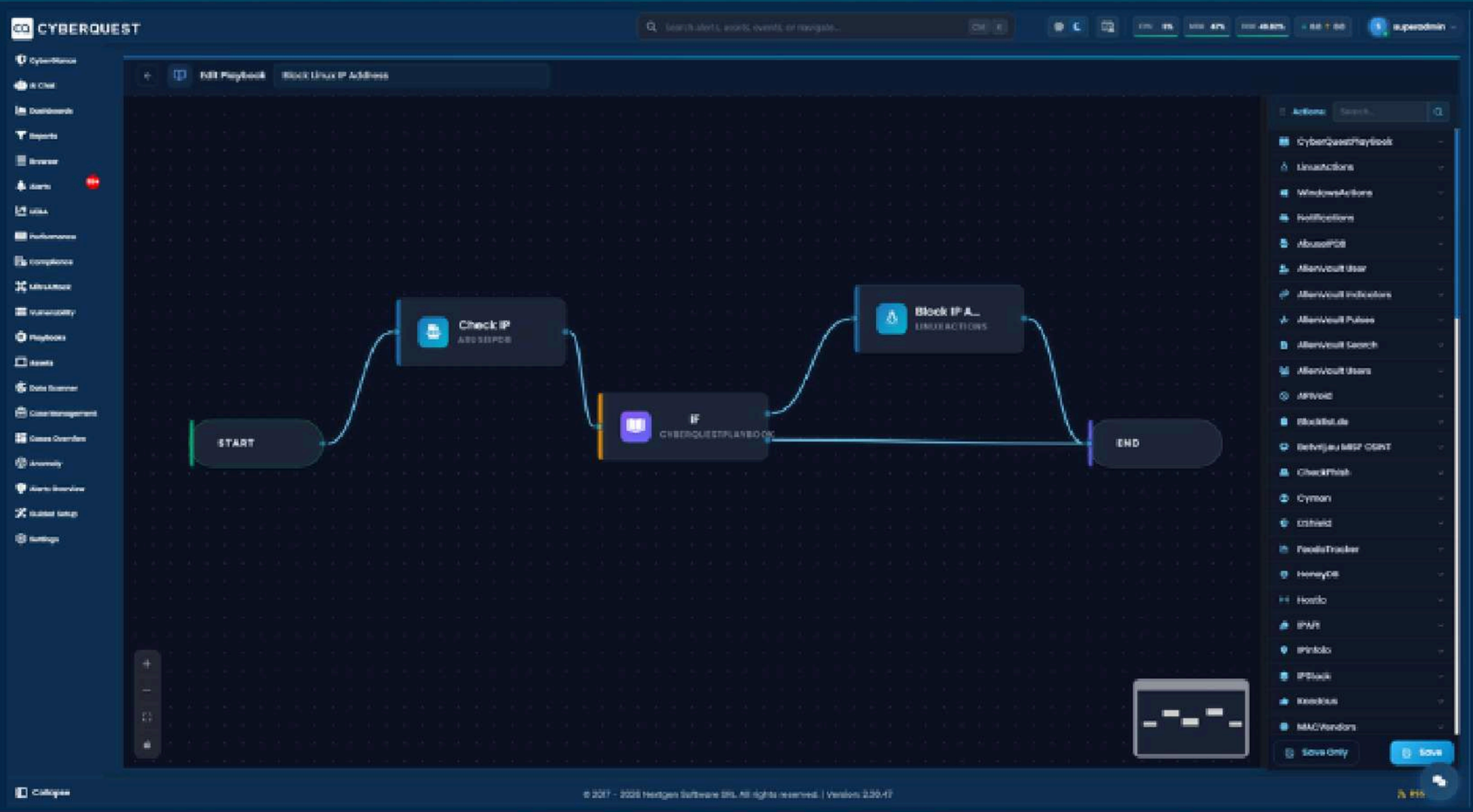
Actions form the building blocks of automated responses. They connect to external security tools or implement internal logic such as conditions, counters and custom scripts.

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.

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