nextgen

Elevate your cyber security

Comprehensive protection ◆ User-centric design

Customized solutions ◆ Simplified compliance

CYBERQUEST SIEM ◆ CQ Automation ◆ NETALERT NDR

CQ Threat Intelligence ◆ CYBER MINDS

ONE PORTFOLIO
MULTIPLE LAYERS OF DEFENSE

CYBERQUEST

Automation

NETALERT NDR

CYBER MINDS

Unified architecture - SIEM, UEBA, SOAR and NDR in one integrated logic

Operational value from day one - 2500+ pre-built detection & correlation rules

Deployment flexibility - On-premises, air-gapped, cloud or hybrid.

Predictable economics - Full visibility without punitive data-volume pricing

European-native by design - Built in Europe for sovereignty and compliance

AI Actionable intelligence in real time

AI-powered automation

End-to-end visibility

Modular, scalable architecture

Real-time threat detection & response

CYBERQUEST Automation | SOAR

Automated incident response with intelligent orchestration. Simplify integration, enhance collaboration and maximize the efficiency of your security stack.

Automated playbooks

- Simplify complex processes, reduce manual effort and focus on what matters most: mitigating threats.
- Execute actions across your security and IT tools in seconds, not hours.
- Speed up incident response by automating workflows and decision-making, ensuring faster, more efficient threat management.

Comprehensive case management

- Supports custom templates and industry-standard frameworks.
- Efficient task segmentation, assignment and documentation for better organization.
- Collaborative process: Keeps teams aligned, ensuring thorough and detailed investigations.

Effortless application integrations

- Connect with 105+ tools effortlessly.
- 1,230 automated actions for workflows.
- Enhance collaboration & optimize security operations.

Generative AI for faster, smarter decisions

- Automates tasks using natural language understanding.
- Enhances threat investigation, response and playbook creation.
- Boosts decision-making and streamlines complex workflows.

Tailored for enterprise or managed services needs

- Suited for enterprises with flexible solutions.
- Choose from on-prem or cloud hosting based on your needs.

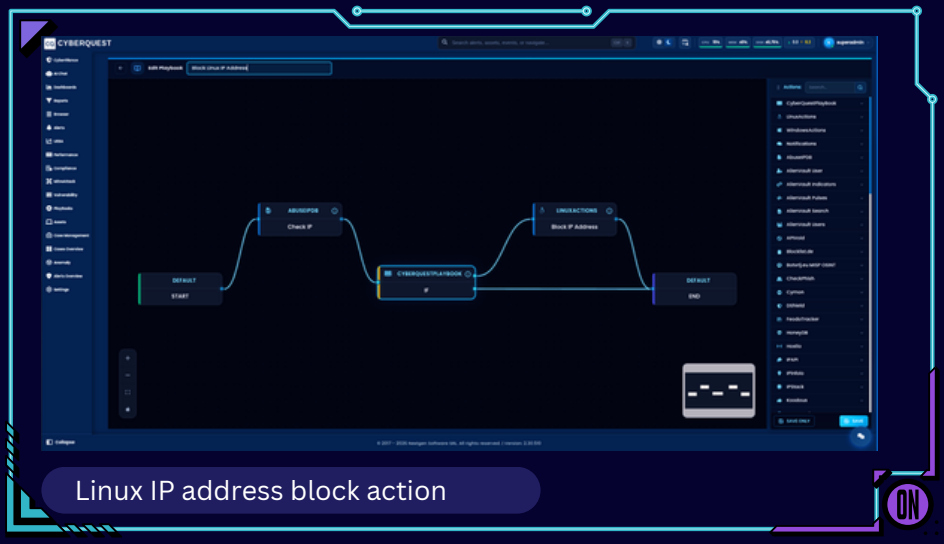
Automate, orchestrate and outpace threats with CQ Automation – see it in action TODAY!

CYBERQUEST Automation | SOAR

Playbook Automation Engine

Outlines how Cyberquest structures and executes automated response workflows (playbooks). It explains the graphical interface for building playbooks, the dynamic input system and the multiple triggering methods (automatic via alerts or manual via GUI).

- **Playbook Structure**:
  - A playbook is a sequence of actions grouped to perform a mitigation or response flow.
  - Actions are added/removed via a graphical interface.
  - Each action requires input parameters, which are dynamically evaluated at runtime.
- **Execution Modes**:
  - Automatic Triggering:
    - Triggered by specific alerts.
    - The alert instance becomes the global inputData for the playbook.
    - Configured via: web graphical interface.
  - **Manual Triggering:**
    - From the Event Browser: user clicks on a specific event.
    - From the Alert Browser: user clicks on a specific alert.
- **Execution History:**
  - Debugging tool to trace parameter values and action outcomes.
  - Helps identify failures or misconfigurations in playbook logic.

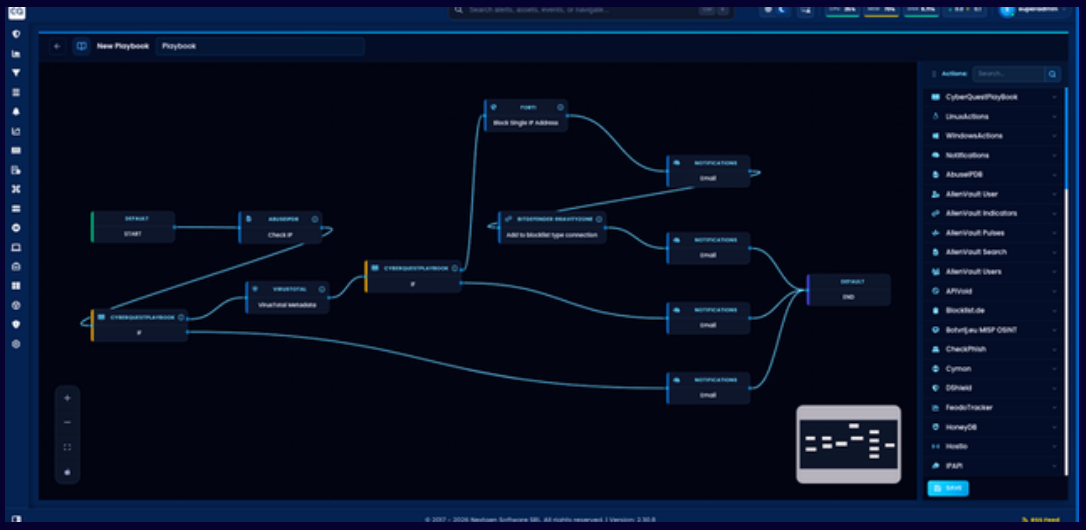


CYBERQUEST Automation | SOAR

Playbook Automation Engine

Disable domain account

ON



Block IP in various systems and notify for each action

ON

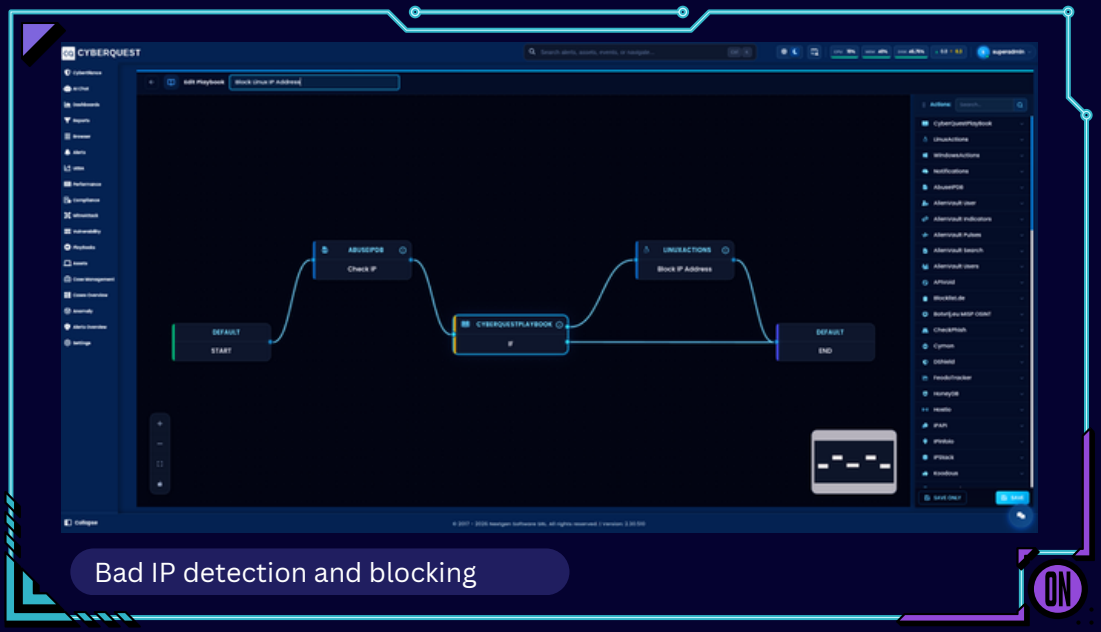
CYBERQUEST Automation | SOAR

Playbook Automation Engine

Details the two main categories of actions used in playbooks: vendor-specific (integrated with external security tools) and functional (logic-based actions like conditions, counters, and custom scripts). These actions form the building blocks of automated responses.

- **Vendor-Specific Actions:**
  - Integrated with a growing list of security vendors.
  - Uses vendor APIs for:
    - Blocking IPs
    - Isolating hosts
    - Updating firewall rules
    - Sending alerts or notifications
  - Updated automatically with new vendor integrations.

- **Functional Actions (under "CYBERQUEST Playbook"):**
  - **IF**: Conditional branching based on Boolean logic.
  - **Count**: Counts elements in an array-type variable.
  - **Code:** Executes a DTS object (custom logic written in JavaScript).



Bad IP detection and blocking

Smart Playbook Features

- Highlights advanced features that enhance flexibility and reusability in playbooks, such as dynamic parameter evaluation, modular logic blocks, and support for custom scripting using JavaScript (DTS objects).
- **Dynamic Parameter**s:
  - 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 and data manipulation.

Audit & Forensics

- Covers the logging and traceability features of CQ Automation/ SOAR. It explains how every action is recorded for compliance, debugging, and forensic analysis, ensuring transparency and accountability in automated responses.
- **Execution Logging**:
  - Every action is logged with:
    - Input parameters
    - Execution result
    - Timestamp and user ID (if manual)
- **Forensic Reports**: Generated from execution history for compliance and incident review.

nextgen

European cyber security for more resilient defense.

CYBERQUEST

Automation

NETALERT NDR

CYBER MINDS

www.nextgensoftware.eu no. 55 Clucerului Str, Bucharest office@nextgensoftware.eu