CURATUM

Intelligent Cybersecurity Monitoring & Response Platform

Product Overview

Curatum is an intelligent cybersecurity monitoring and response platform designed to help organizations detect, analyze, and respond to security threats in real time. It combines automated threat detection, AI-assisted decision making, and a centralized security operations dashboard to give security teams full visibility and control over their environment.

Curatum is built to support modern enterprise infrastructures, enabling faster incident response, reduced operational overhead, and improved security posture without adding complexity.

> Curatum helps security teams detect and respond faster with AI-assisted analysis, centralized SOC visibility, and controlled automation.

Key Objectives

- Detect security threats in real time
- Reduce response time using AI-assisted actions
- Provide clear visibility to SOC teams and leadership
- Enable controlled automation with human oversight
- Support scalable deployment across enterprise environments

Core Capabilities

1. Real-Time Threat Detection

Curatum continuously monitors system logs, application activity, and security events to detect potential threats as they occur. The platform identifies common and advanced attack patterns without requiring manual intervention.

- Ransomware activity
- SQL Injection and NoSQL Injection attempts
- Brute-force authentication attacks
- Malware indicators
- Suspicious file and system behavior

2. AI-Assisted Threat Analysis

Each detected threat is analyzed by the AI engine, which assigns severity, confidence, and suggested response actions so SOC analysts can prioritize incidents effectively and focus on what matters most.

- Severity level: Low, Medium, High, Critical
- Confidence score based on observed behavior
- Suggested response actions

3. Automated and Manual Response Actions

Curatum supports both automated responses and manual overrides, ensuring automation never compromises control.

- Automatic threat resolution for low-risk and high-confidence events
- AI-driven remediation actions (where enabled)
- Manual intervention for critical or sensitive incidents
- Full audit trail of all actions taken

4. Risk Scoring & Visualization

The platform dynamically calculates organizational risk based on active threats and their severity. Risk is visualized using intuitive dashboards so teams instantly understand the current security posture.

- High / Medium / Low risk distribution
- Real-time updates as threats are resolved
- Risk automatically drops to zero when no active threats remain

5. Centralized SOC Dashboard

Curatum provides a single, unified dashboard for security operations.

- Latest detected threats
- Active alerts and system status
- Risk indicators and confidence metrics
- AI engine health and success rate
- Action history and resolution tracking

6. Alerting & Notifications

Curatum sends immediate notifications when threats are detected or resolved to ensure the right people are informed at the right time.

- Email alerts for security incidents
- Severity-based notification routing
- Custom recipient groups per threat type
- Clear, actionable alert content

7. Human-in-the-Loop Security

Critical actions can require approval before execution, supporting governance and compliance while still benefiting from automation.

- Approval workflows for sensitive actions
- Manual override capability
- Full traceability for audits and reviews

8. Secure and Scalable Architecture

Curatum is designed for enterprise deployment.

- Supports Windows Server and cloud environments
- Integrates with SQL Server for data persistence
- Secure API-based communication
- Scales with organizational growth

Operational Benefits

- Faster threat detection and response
- Reduced SOC workload through intelligent automation
- Improved visibility for security leadership
- Lower risk exposure and downtime
- Clear auditability and compliance support

Ideal Use Cases

- Security Operations Centers (SOC)
- Enterprise IT security teams
- Organizations seeking AI-assisted cybersecurity
- Environments requiring controlled automation with approvals

Deployment Model

- On-premise or cloud-hosted (e.g., AWS EC2)
- Backend API with centralized database
- Web-based frontend dashboard
- Role-based access for analysts and administrators

Summary

Curatum is not just a monitoring tool — it is a complete cybersecurity response platform that blends real-time detection, AI intelligence, and human control. It empowers organizations to stay ahead of threats while maintaining transparency, governance, and operational efficiency.