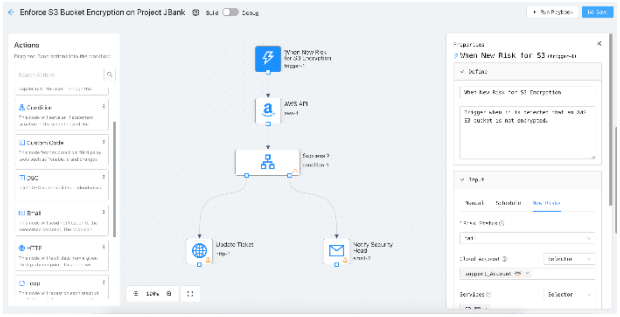
CLOUDNOSYS
Security • Compliance

Playbooks

Security Orchestration, Automation and Response (SOAR)

Centralize all security findings, prioritize and enrich alerts, and remediate threats faster via automation:



OPTIMIZE SOC SECURITY OPERATIONS

- Dynamic risk assessments, remediation, and analysis
- Collaborations with SOC team members
- Prevent issues and resolve challenges faster

INCIDENT MANAGEMENT

- Ensure proactive protection of your data and application by continuous analysis of your alerts and remediations

SECURITY TOOLS INTEGRATIONS

- Playbooks can ingest complex set of findings from other security tools
- All integrations plugin is dynamically update to get access to latest tools.
- Solutions that work and align to your IT business priorities

Today's SOC Operation Challenges

SOC Analysts and Cloud Operations teams continue to suffer from endless false positive alert analysis, and manual triage data from multiple security tools manually. Insufficient security tools integrations, triage, and talent retention is increasing security risk and leaving Enterprise system exposed to high number of Vulnerabilities. Sr SOC Analysts or Tier-3 level suffer from gathering contextual information from sea of data. They sift through multiple security tools to build this context which is risky, expensive and time consuming.

The Solution – ROI of Playbooks

Save 75% of labor hours that require triage from multiple system. Reduce staff turnover due to high pressure of resolving alert count. With open and extensible platform and pre-built plugins with data enrichments processes, the threat feeds, SIEM tools integrations of your choice drives automated triage and alert prioritization.

- Playbooks workflow driven response actions and investigations
- Auto documentation and process action logs that speeds up the compliance audits
- Build your security solutions best practices specific to your needs
- Assists with crisis and incident management related with Cloud
- Work closely with auditors to prove compliance with evidence data within Cloudnosys Platform
- Available as SaaS or hosted in your cloud solution for maximum security and privacy
- Collaborate with Security Operations Center (SOC) and CloudOps teams to build remediation plans.

Cloudnosys Cloud Security, Risk Management and SOAR in one integrated solution:

We provide combination of fully integrated Cloud Infrastructure protection, governance, and risk management with automated Playbooks. Open API interface and ETL data ingestion playbooks leverages your current security tool investments and helps you consolidate risks and findings in one location to drive governance, and self-healing cloud through live remediation playbooks that are triggered via manual, automated, scheduled or set of conditions that may occur. All this flexibility is provided to meet Enterprise needs. We provide an API first architecture to quickly tie into your current process to help triage information and drive context for an alert or incident at scale. This provides faster Mean-Time-to-Resolution (MTTR) Dashboards and reports meet SOC, CISO and Auditors requirements.

CLOUDNOSYS
Security • Compliance

Everything Consolidated SOC Operations Visibility with Context

Cloudnosys Playbooks provides security orchestration, automation and response (SOAR) as solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. Our Playbooks self-documents and implements; support security incident management; security tools integrations, and apply machine-based assistance to human security analysts and operators. Playbook workflows can be orchestrated via integrations with other security technologies, and automated to achieve desired outcomes, such as:

- Remediation for an incident.
- Incident triage – Security Tools Integrations
- Incident response
- TI curation and management
- Compliance monitoring and management

Alerting and notifications to end users when a potential threat has been detected is no longer sufficient, given the speed at which attacks can progress in a cloud environment one needs contextual understanding and risk prioritization. The additional contextual information which exists in other security tools that are running in your environment can be brought together to surface patterns of attack. Cloudnosys Playbooks has the power of integration built in by importing dynamically via prebuilt APIs that brings security findings and associated policies to triage and provide a holistic view of an alert.

If you are struggling with endless alerts, or time-consum by security or cloud team, then you will benefit from play Centralize, consolidate and document all your custom c revisions, logs and reduce rework by your SOC teams. D your Cloud operations team and optimize your human c

Core use cases Playbooks focuses on are as follows

- SOC optimization
- Threat monitoring, investigation and response
- Threat management

The above areas are defined further as follows:

- Alert Triage and Prioritization: Playbooks can ir sources and apply a process of contextual data prioritizes incidents which will have a negative i goal is to focus on most critical and well deserv security analyst.
- Orchestration and Automation: The complexity the coordination of workflows with manual and security tools and affecting information systems operating level.
- **Dashboard and Reporting:** Dashboard and re aggregate contextual data. This SOC data is fo various audiences, such as Auditors, SOC mar

Its time your enterprise optimizes your SOC and C focusing on automating repeated events, out of po fatigue. Cloudnosys Playbooks deliver the automat documented process in one solution.

TECHNICAL SUPPORT

Experienced Solutions Specialist for guidance on all matters Implement best practices, recommendations for optimal performance Insight and planning

ZERO DOWNTIME

Immediate proactive access to the right resources and at the right time.

TURNKEY SOLUTIONS

Cloudnosys makes your Cloud Security journey safe and secure quickly with minimal risks.

FOR MORE INFORMATION

Please visit us on the Web at: www.cloudnosys.com or email info@cloudnosys.com

CLOUDNOSYS
Security • Compliance

205 Market Pl, Roswell, GA
30075 USA
Phone 404-692-5787
Email: Info@cloudnosys.com