SOAR PLATFORM

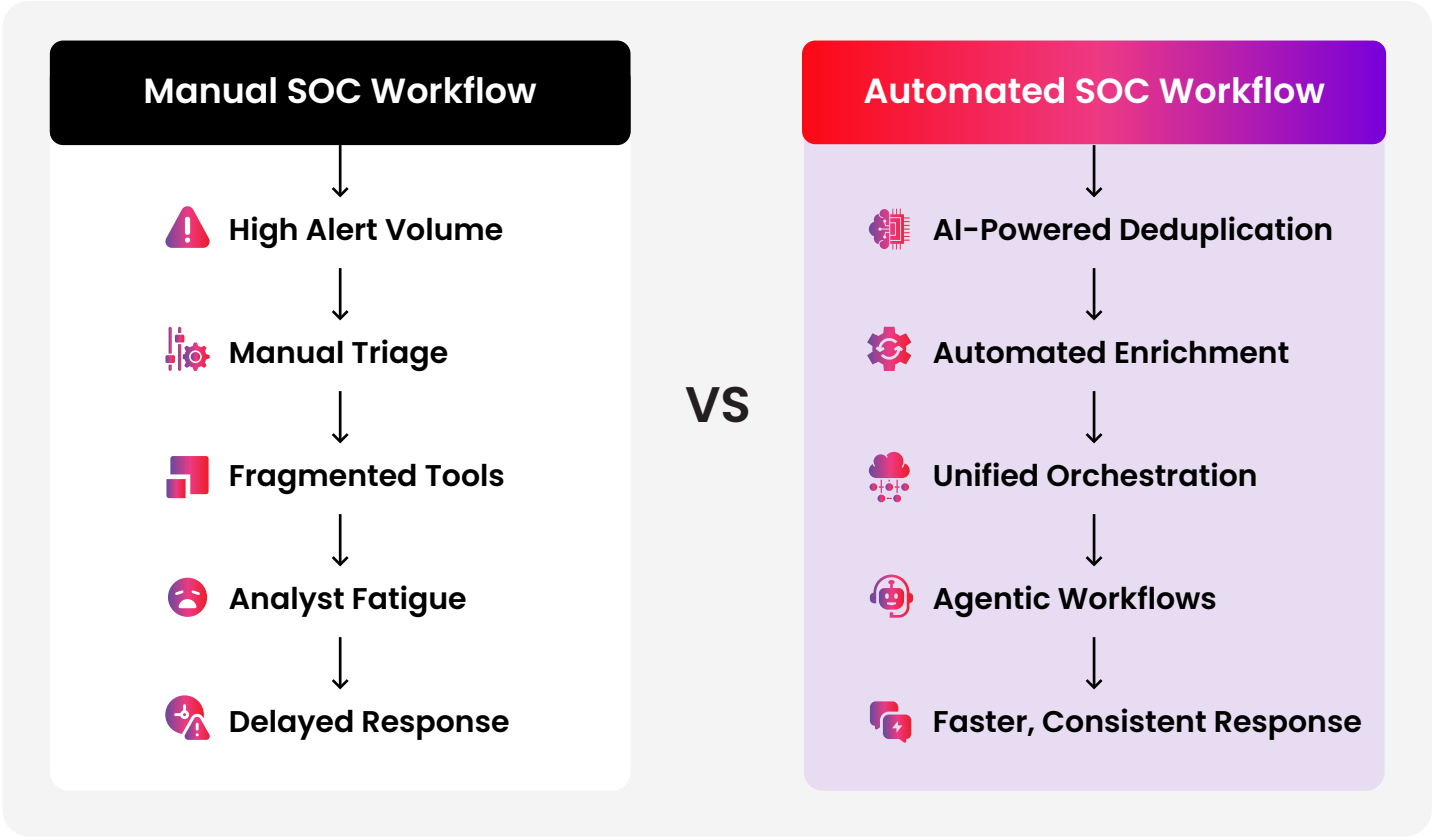
Transform Manual Security Operations into Intelligent Automated Defense

THE CHALLENGE

Security teams today struggle with overwhelming alert volumes, manual response processes, fragmented tool ecosystems, and analyst burnout. 85% of security alerts require manual investigation, overwhelming teams with routine tasks.

THE EVENTUS SOLUTION

The Eventus SOAR Platform transforms traditional SOCs into intelligent defense centers through AI-driven agentic workflows, intelligent case management, and seamless orchestration—enabling faster response, consistent processes, and reduced analyst workload.



CORE CAPABILITIES

Intelligent Automation

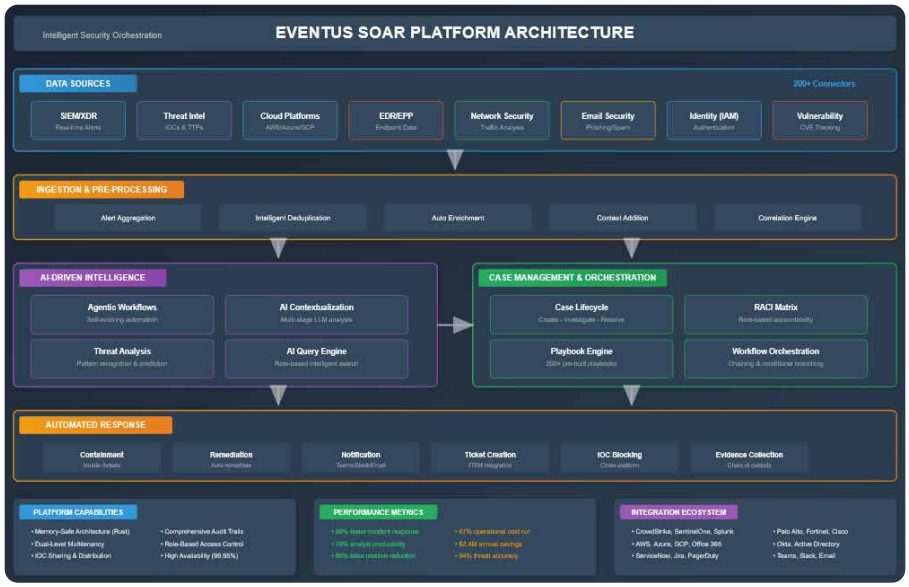
1. **Autonomous Agentic Workflows:** Self-evolving AI agents that triage, investigate, and respond while learning from outcomes.
2. **Intelligent Deduplication:** Advanced correlation reduces alert fatigue while preserving critical context.
3. **Playbook Chaining:** Sophisticated multi-stage workflows with dynamic conditional branching.
4. **Auto Enrichment:** Automatic enhancement with threat intelligence, asset context, and historical patterns.

Advanced Features

1. **AI-Aided Query Engine:** Role-based intelligent query processing for faster investigations.
2. **RACI Matrix Integration:** Clear accountability and streamlined incident communication
3. **Email Communication:** Native ticketing functionality for seamless stakeholder engagement.
4. **IOC Sharing & Multitenancy:** Secure cross-tenant intelligence sharing with strict isolation.
5. **200+ Pre-Built Connectors:** Zero-downtime orchestration across security infrastructure.

WHY EVENTUS SOAR IS DIFFERENT

1. **Agentic AI Workflows:** Self-improving automation, not static playbooks
2. **Memory-Safe Architecture:** Rust-based for zero vulnerabilities and concurrent operations
3. **Intelligent Deduplication:** Advanced correlation preserving investigation context
4. **Dual-Level Multitenancy:** Built for MSSPs and enterprise partner collaboration



BUSINESS OUTCOMES

Operational Excellence

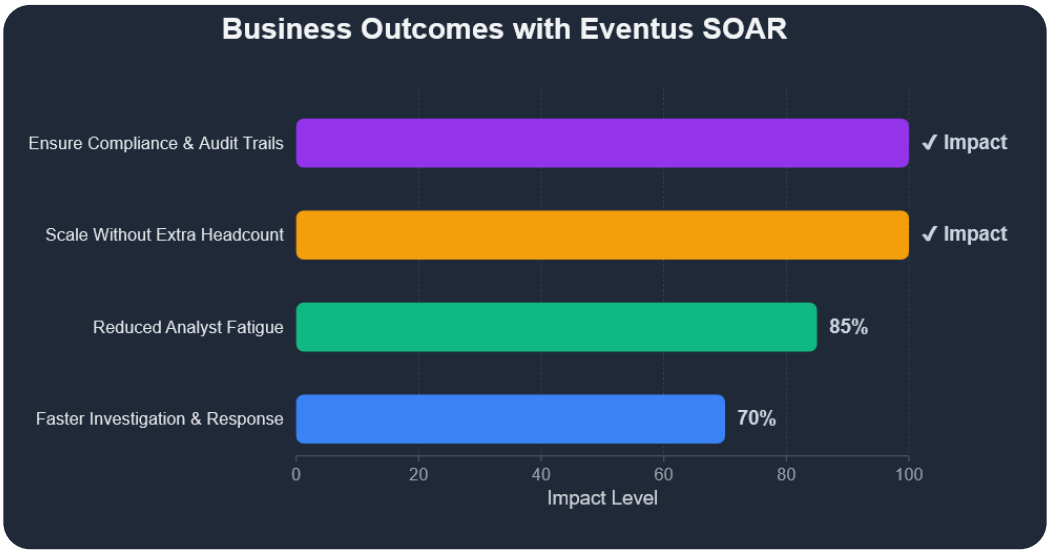
1. Reduce response time through intelligent automation
2. Eliminate analyst fatigue via case consolidation
3. Scale operations without proportional headcount

Cost Optimization

1. Substantial operational cost reduction
2. Minimize false positive investigations
3. Ensure compliance with audit trails

KEY BENEFITS

- **Proactive Security -** Transform reactive response into proactive automated defense
- **Operational Efficiency -** Substantial manual effort reduction with comprehensive coverage
- **Enhanced Reliability -** Memory-safe architecture ensures continuous operations
- **Scalable Integration -** Seamless orchestration with 200+ connectors
- **Cost Effectiveness -** Significant overhead reduction through intelligent automation



IMPLEMENTATION METHODOLOGY

1. **Assessment -** Evaluate existing ecosystem and identify automation opportunities.
2. **Workflow Design -** Develop custom playbooks and configure RACI controls.
3. **Integration -** Deploy 200+ connectors across security infrastructure.
4. **AI Optimization -** Initialize agentic workflows with continuous learning.
5. **Monitoring -** Track effectiveness metrics with ongoing support.

USE CASES

SOC Automation | Incident Response | Threat Hunting | MSSP Operations | Compliance Management

Streamline alert triage, coordinate multi-team response, enable cross-platform investigation, deliver managed services with tenant isolation, and maintain comprehensive audit trails.

ORCHESTRATION AND AUTOMATION
Unified Security Operations Hub

SOC Automation

- Automated alert triage
- AI-driven workflows
- 89% faster response
- Intelligent orchestration
- Reduced false positives
- Agentic AI automation

Incident Response

- Multi-team coordination
- 200+ pre-built playbooks
- Automated communications
- Real-time status tracking
- RACI matrix integration
- Case management

Threat Hunting

- Cross-platform investigation
- 6-vector correlation
- AI-enhanced intelligence
- Advanced hunting queries
- IOC retrospective scanning
- Vulnerability correlation

MSSP Operations

- Secure tenant isolation
- Persona-based dashboards
- Multi-customer delivery
- Scalable operations
- Role-specific views
- Client data segregation

Compliance Management

- Comprehensive audit trails
- Automated reporting
- SOC 2, GDPR, HIPAA
- Real-time monitoring
- Regulatory compliance
- Evidence management

TRANSFORM YOUR SECURITY OPERATIONS

Eventus SOAR empowers teams to move from reactive firefighting to proactive resilience with intelligent automation that continuously improves.

eventus™

Built to Scale. Powered by AI. Ready for Enterprise.

Request a Demo Today

hello@eventussecurity.com
www.eventussecurity.com
India | SEA | Middle East | USA