SOCByte

All Bytes Secured

Solution Brief

AI-Powered Security Operations Platform

All-In-One Agentic SOC Platform

SOCByte consolidates your entire Security Operations Center into a single, cloud-native platform, enhanced by Dexter, your AI SOC analyst. Our next-generation solution transforms security operations with intelligent automation and proactive defenses.

60%	85%	24/7
Reduction in Alert Volume	Faster Investigation Time	Autonomous Monitoring

Security Challenges

Alert Fatigue

Security teams are overwhelmed with noisy alerts, making it difficult to identify and respond to genuine threats promptly.

Tool Sprawl

Organizations use multiple disconnected security tools, creating operational inefficiencies and potential security gaps.

Staff Shortage

Skilled cybersecurity professionals are scarce and expensive, limiting organizations' ability to maintain 24/7 security operations.

Slow Investigation Time

Manual investigation processes are time-consuming, leading to delayed responses and increased risk of security breaches.

The SOCByte Platform

SOCByte consolidates essential security operations into a single, unified platform. Our cloud-native solution integrates cutting-edge tools and real-time threat intelligence enhanced by Dexter, our AI SOC analyst, to help security teams identify and mitigate risks before they escalate.

SOCByte SIEM

Centralize logs, correlate events, and respond in real-time with our AI-driven SIEM solution. Built for hybrid SOCs with customizable dashboards and parser-friendly integration.

- MITRE-Aligned Detection
- Unified Log Collection
- Custom Log Parsers
- Offense Management

SOCByte SOAR

Automate incident response, orchestrate across tools, and manage cases with intelligence and speed. Designed for high-performing security teams.

- 200+ Native Integrations
- Case Management with Audit Trails
- Agentic AI Automation
- Flexible Reporting Options

SOCByte Phisher

Go beyond traditional phishing simulations with comprehensive employee cybersecurity awareness. Targeted, realistic simulations with built-in training.

- Customizable Campaigns
- Real-Time Alerts
- Training Content Integration
- Detailed Reporting & Analytics

SOCByte Threat Intel

Bring context-rich insights into one place, helping you detect faster, prioritize smarter, and understand who's targeting you before they strike.

- Advisories & CVEs
- IOCs & IOAs
- Threat Actor Profiling
- STIX/TAXII Support

Integration & Deployment

Flexible Deployment Options

- ✓ Cloud-native architecture with SaaS delivery
- ✓ On-premises deployment for sensitive environments
- ✓ Hybrid deployment supporting distributed teams
- ✓ Multi-tenant options for MSSPs

Seamless Integration

- ✓ 200+ pre-built integrations with security tools
- ✓ API-first design for custom integration
- ✓ Standard log format support (CEF, LEEF, etc.)
- ✓ Custom parser development assistance

Meet Dexter: Your AI SOC Analyst

Dexter is Pakistan's first autonomous SOC analyst, built to think, act, and learn like your best security hire — only faster, smarter, and always on. Dexter transforms security operations by automating alert investigation and response, reducing analyst workload, and accelerating incident resolution.

Autonomous Investigations

Dexter investigates every alert without human input, filtering noise and surfacing what matters.

Conversational Interface

Ask questions in natural language about alerts, logs, or security events.

Autonomous Response

From isolating hosts to escalating tickets, Dexter takes decisive actions when risks are confirmed.

Continuous Learning

Dexter learns from every decision, every alert, and every SOC analyst interaction.

Dexter in Action

Dexter
I've detected multiple failed login attempts from IP 203.0.113.42 targeting your admin portal.

Analyst
Show me more details about this IP.

Dexter
IP 203.0.113.42 is associated with a known threat actor group. It has attempted 23 logins in the past hour from Moscow, Russia.

Analyst
Block this IP and generate a report.

Dexter
IP successfully blocked. Incident report #4872 has been generated with all evidence and timeline attached.

How SOCByte Works

1. Data Collection

Unified log collection from all your security tools, endpoints, networks, and cloud services.

2. AI Analysis

Dexter analyzes data using machine learning to identify threats and correlate events.

3. Automated Response

Autonomous or guided responses to confirmed security incidents.

4. Unified Reporting

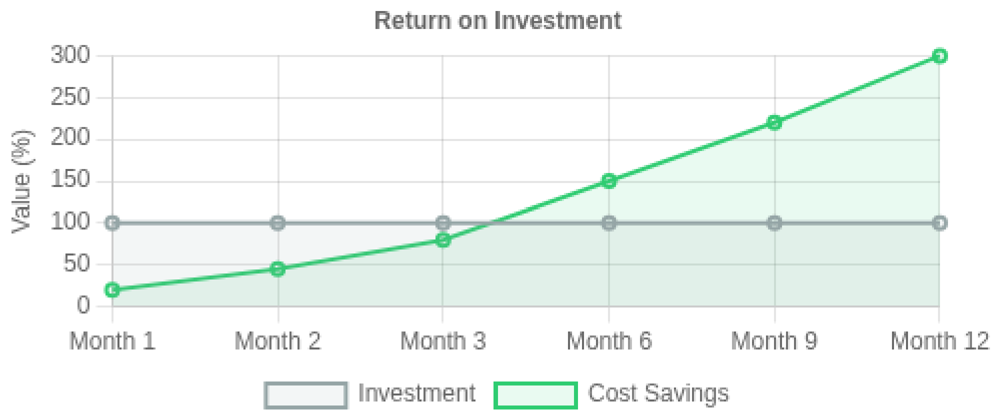
Comprehensive dashboards and reports for operational and executive visibility.

Key Performance Improvements

60% Reduction in Alerts

85% Faster Investigations

40% Cost Savings



Average SOCByte ROI over 12 months

Customer Success Story

> *"Before SOCByte, scaling our security operations meant hiring more analysts and drowning in false positives. Since switching, we've cut our alert volume by over 60%, automated our Tier-1 response, and onboarded 3 new clients WITHOUT adding headcount. It's the first platform that actually feels built for MSSPs."*
>
> ***— William TJ Sims***
>
> *CEO, Cythority*

Business Benefits

Operational Efficiency

- 60% reduction in alert volume
- 85% faster investigations
- Automated response to common threats
- Unified management console

Cost Optimization

- Reduced need for additional headcount
- Consolidation of security tools
- Decreased mean time to resolution
- Optimized analyst productivity

Enhanced Security

- 24/7 autonomous monitoring
- Consistent investigation methodology
- Proactive threat hunting
- Continuous security improvement

Next Steps

Transform Your Security Operations Today

Contact our team to schedule a personalized demonstration and see how SOCByte can help your organization enhance security operations while reducing costs.

Email
contact@socbyte.ai

Phone
+92 301 2730261

Web
www.socbyte.ai

Demo
www.socbyte.ai/demo

Request a Demo