RAPTAS
POWERING DIGITAL FUTURES

SHIELD SPHERE

Unified Security Operations & Compliance Platform

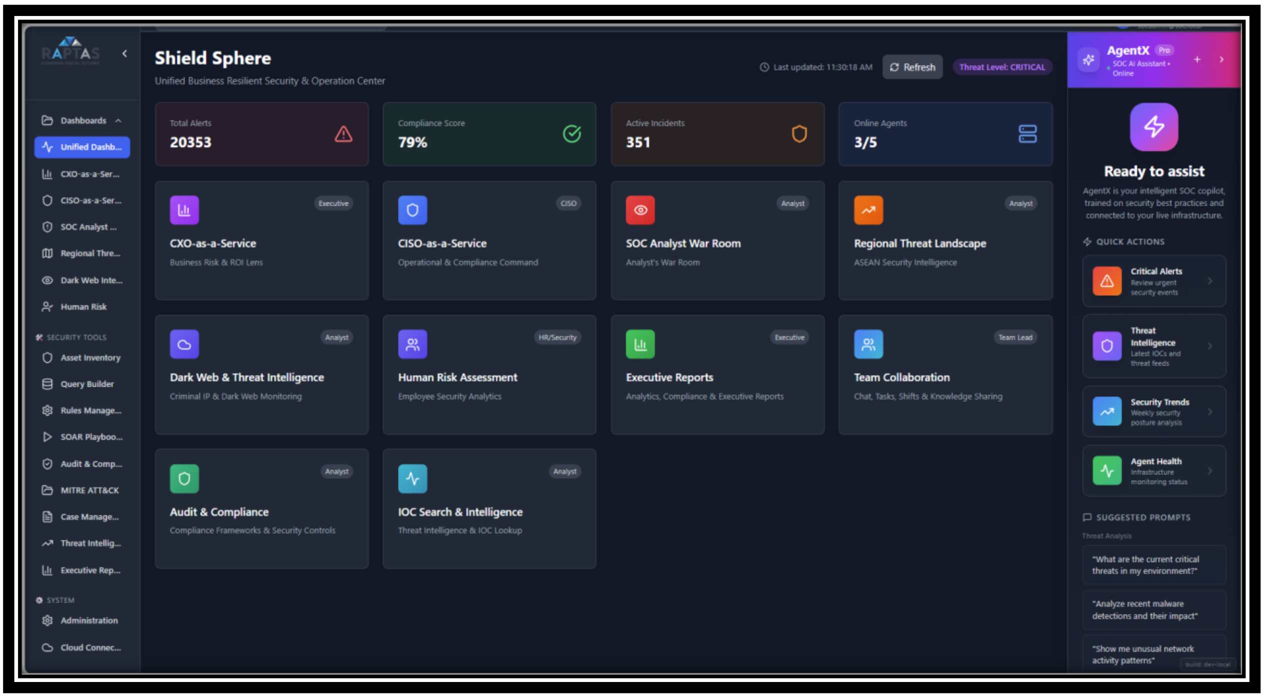
• SIEM • SOAR • IOC & Threat Intelligence • Compliance Automation • AI-Powered Query Builder & Analytics • Dark-Web Intelligence • AgentX

EXECUTIVE SUMMARY

Shield Sphere is an enterprise-grade unified Security Operations Center and Compliance platform that consolidates SIEM SOAR threat intelligence dark web monitoring compliance management and AI-powered analytics into a single intelligent solution. Shield Sphere delivers enterprise security capabilities at 50% lower cost than traditional multi-tool stacks with deployment measured in hours not months Available in flexible On-Premise and fully Managed Security Services (MSS) models to meet diverse organizational needs from small businesses to large enterprises

Platform Overview

Shield Sphere is a **next-generation security and compliance fabric** that unifies detection, response, intelligence, and audit readiness into a single platform. Designed for **CXOs, CISOs, SOC Analysts, and Regulators**, it translates technical risk into business clarity while automating resilience. Shield Sphere consolidates everything into one intelligent platform at half the cost deployable in just 4 hours.



Shield Sphere
Unified Business Resilient Security & Operation Center

Last updated: 11:30:18 AM
Threat Level: CRITICAL

Total Alerts 20353
Compliance Score 79%
Active Incidents 351
Online Agents 3/5

CXO-as-a-Service – Business Risk & ROI Lens
CISO-as-a-Service – Operational & Compliance Command
SOC Analyst War Room – Analyst's War Room
Regional Threat Landscape – ASEAN Security Intelligence
Dark Web & Threat Intelligence – Criminal IP & Dark Web Monitoring
Human Risk Assessment – Employee Security Analytics
Executive Reports – Analytics, Compliance & Executive Reports
Team Collaboration – Chat, Tasks, Shifts & Knowledge Sharing
Audit & Compliance – Compliance Frameworks & Security Controls
IOC Search & Intelligence – Threat Intelligence & IOC Lookup

Ready to assist
AgentX is your intelligent SOC copilot, trained on security best practices and connected to your live infrastructure.

Critical Alerts – Review urgent security events
Threat Intelligence – Latest IOCs and threat feeds
Security Trends – Weekly security posture analysis
Agent Health – Infrastructure monitoring status

"What are the current critical threats in my environment?"
"Analyze recent malware detections and their impact"
"Show me unusual network activity patterns"

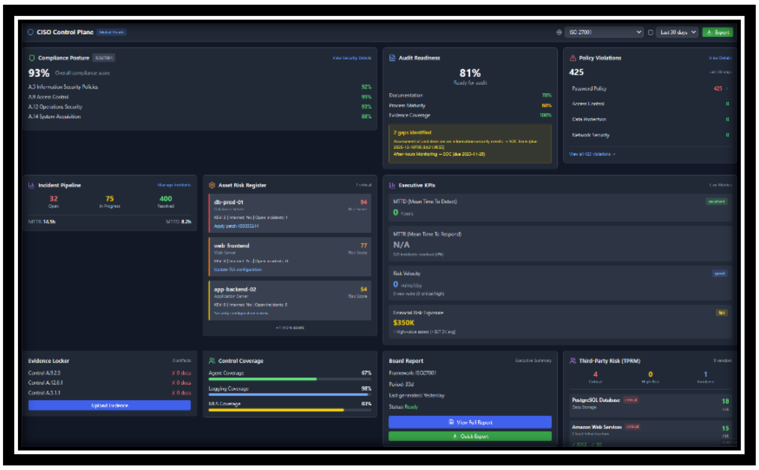
Key Platform Components:

Category	*Capability*	*Value Proposition*
Unified Visibility	Single-Pane Dashboard	Consolidates alerts, incidents, compliance scores, and threat levels in real time
Detection & Response	SIEM Core	Scalable log ingestion, correlation, and anomaly detection across enterprise systems
	SOAR Playbooks	Automated triage, enrichment, and remediation workflows
Threat Intelligence	Dark Web Monitoring	Continuous surveillance of underground forums, leaks, and exploits
	IOC & Threat Lookup	Real-time IOC search with adversary tactic mapping
Compliance & Audit	Compliance Frameworks	Built-in scorecards for PCI-DSS, ISO 27001, NIST, SWIFT
	Automated Evidence Collection	Streamlined audit readiness with control validation
AI & Automation	AI Query Builder	Natural language queries for logs and cases, reducing analyst learning curve
	AgentX SOC Assistant	Conversational AI for guided troubleshooting and contextual recommendations
Executive Lens	CXO-as-a-Service	ROI-focused dashboards translating risk into business impact
	CISO Command Center	Prioritized risk views, policy enforcement, and regulatory readiness
Analyst Experience	SOC War Room	Collaborative case management, shift handovers, and playbook execution
Regional Intelligence	Threat Landscape Insights	Benchmarking against global adversary activity
Human Risk	Insider & Behavior Analytics	Employee security behavior monitoring and awareness scoring
Operational Discipline	Secure System Administration	Role-based access, multi-tenancy, and agent health monitoring

CISO Control Plane

Compliance Posture & Operational Command Center

The CISO Control Plane provides executive-level visibility and control over the organizations entire security and compliance posture with real-time compliance scoring, audit readiness, tracking policy violation, monitoring and asset risk assessment. CISOs gain complete command and control over the organization security operations



Compliance Posture
93% Overall compliance score
A.5 Information Security Policies 92%
A.9 Access Control 95%
A.12 Operations Security 93%
A.14 System Acquisition 88%

Audit Readiness
81% Ready for audit
Documentation 78%
Process Maturity 68%
Evidence Coverage 100%
2 gaps identified
After-hours Monitoring — SOC (due 2025-11-28)

Policy Violations
425
Password Policy 425
Access Control 0
Data Protection 0
Network Security 0

Incident Pipeline
32 Open
75 In Progress
400 Resolved
MTTR: 14.5h
MTTD: 8.2h

Asset Risk Register
db-prod-01 94 Risk Score
web frontend 77 Risk Score
Web Server
Update TLS configuration
app-backend-02 54 Risk Score
Application Server
KEV: 0 | Internet: No | Open Incidents: 0

Executive KPIs
MTTD (Mean Time To Detect) 0 hours
MTTR (Mean Time To Respond) N/A
Risk Velocity 0 vulns/day
0 new vulns (0 critical/high)
Financial Risk Exposure $350K

Evidence Locker
Control A.9.2.3 ✗ 0 docs
Control A.12.6.1 ✗ 0 docs
Control A.5.1.1 ✗ 0 docs

Control Coverage
Agent Coverage 67%
Logging Coverage 98%
MFA Coverage 83%

Board Report
Framework: ISO27001
Period: 30d
Last generated: Yesterday
Status: Ready

Third-Party Risk (TPRM)
4 Critical
0 High Risk
1 Incidents
PostgreSQL Database 18 risk
Data Storage
Amazon Web Services 15 risk

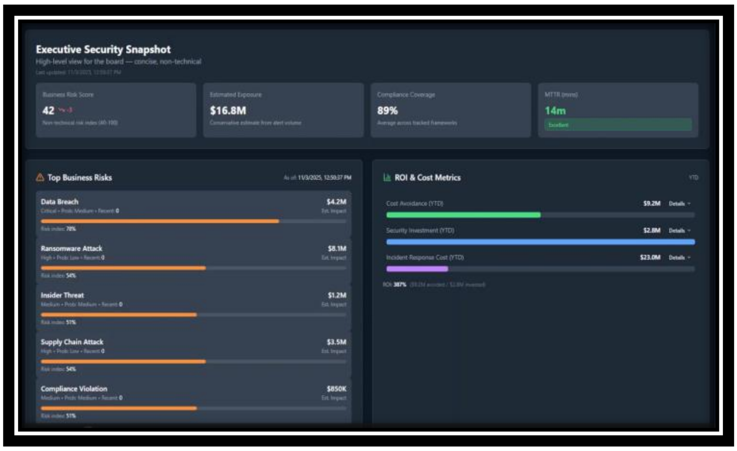
Key Capabilities:

- **Compliance Oversight** – ISO27001, SWIFT, NIST, SOC 2 etc framework are aligned with clear visibility into controls and audit readiness.
- **Security Posture Monitoring** – Real-time tracking of compliance scores, violations, and gaps.
- **Policy & Access Governance** – Centralized management of password hygiene and access controls.
- **Incident Management** – Streamlined detection, triage, and resolution with transparent response metrics.
- **Asset Risk Intelligence** – Prioritized view of critical systems, vulnerabilities, and remediation needs.
- **Remediation Tracker** – Clear visibility into tasks, progress, and blockers across IT and SecOps.
- **Industry News Integration** – Automated feed of global cyber developments for proactive decision-making.
- **Benchmarking & Reporting** – Peer comparison and board-ready KPIs that translate posture into business impact.

Executive Security Snapshot

Board-Level Risk & ROI Visibility

The Executive Security Snapshot provides board-ready high-level security metrics in non-technical language Perfect for board meetings investor relations and executive briefings this dashboard translates complex security data into business risk and financial impact



Executive Security Snapshot
High-level view for the board — concise, non-technical
Last updated: 11/3/2025, 12:59:37 PM

Business Risk Score
42
Non-technical risk index (40-100)

Estimated Exposure
$16.8M
Conservative estimate from alert volume

Compliance Coverage
89%
Average across tracked frameworks

MTTR (mins)
14m
Excellent

Top Business Risks — As of: 11/3/2025, 12:50:37 PM

Data Breach — $4.2M Est. impact
Critical • Prob: Medium • Recent: 0
Risk index: 78%

Ransomware Attack — $8.1M Est. impact
High • Prob: Low • Recent: 0
Risk index: 54%

Insider Threat — $1.2M Est. impact
Medium • Prob: Medium • Recent: 0
Risk index: 51%

Supply Chain Attack — $3.5M Est. impact
High • Prob: Low • Recent: 0
Risk index: 54%

Compliance Violation — $850K Est. impact
Medium • Prob: Medium • Recent: 0
Risk index: 51%

ROI & Cost Metrics — YTD

Cost Avoidance (YTD) — $9.2M Details
Security Investment (YTD) — $2.8M Details
Incident Response Cost (YTD) — $23.0M Details

ROI: 387% ($9.2M avoided / $2.8M invested)

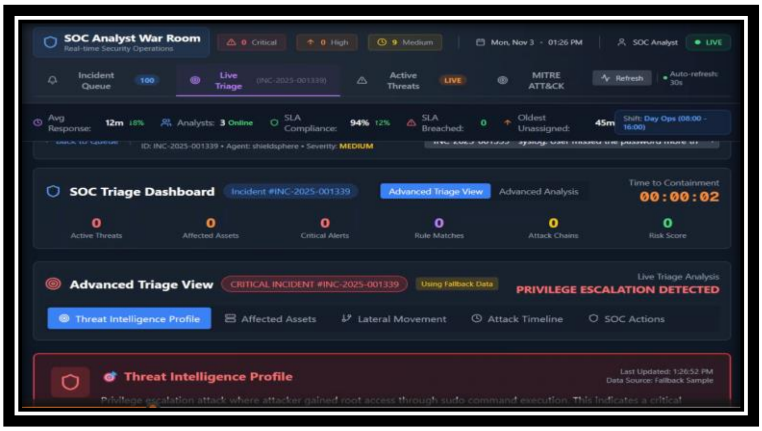
Key Capabilities:

- **Business Risk Scoring**
  - Quantifies risk using non-technical index
  - Tracks score deltas over time
- **Financial Exposure Estimation**
  - Calculates impact from alert volume
  - Highlights conservative exposure values
- **Compliance Coverage Overview**
  - Averages scores across tracked frameworks
  - Flags gaps in regulatory alignment
- **MTTR Performance Tracking**
  - Measures mean time to respond
  - Labels performance (e.g., Excellent)
- **Top Risk Scenarios**
  - Profiles breach, ransomware, insider threats
  - Estimates financial impact per scenario
- **ROI & Cost Metrics**
  - Tracks cost avoidance and investments
  - Calculates year-to-date security ROI
- **Recommended Risk Actions**
  - Suggests MFA, segmentation, EDR, training
  - Quantifies risk reduction per action
- **Mini Trends & Outlook**
  - Summarizes alerts, SLA, and contributors
  - Provides stability forecast and guidance

SOC Analyst War Room

Real-Time Security Operations Center

The SOC Analyst War Room provides real-time operational visibility for security analysts with live incident triage, threat intelligence, attack chain analysis, and collaborative response, workflows designed for 24/7 security operations with auto-refresh shift handoffs and SLA tracking



Avg Response: 12m ↓8% · Analysts: 3 Online · SLA Compliance: 94% ↑2% · SLA Breached: 0 · Oldest Unassigned: 45m · Shift: Day Ops (08:00 - 16:00)

ID: INC-2025-001339 • Agent: shieldsphere • Severity: MEDIUM

Time to Containment 00:00:02

0 Active Threats · 0 Affected Assets · 0 Critical Alerts · 0 Rule Matches · 0 Attack Chains · 0 Risk Score

Live Triage Analysis
PRIVILEGE ESCALATION DETECTED

Threat Intelligence Profile
Last Updated: 1:26:52 PM
Data Source: Fallback Sample

Privilege escalation attack where attacker gained root access through sudo command execution. This indicates a critical

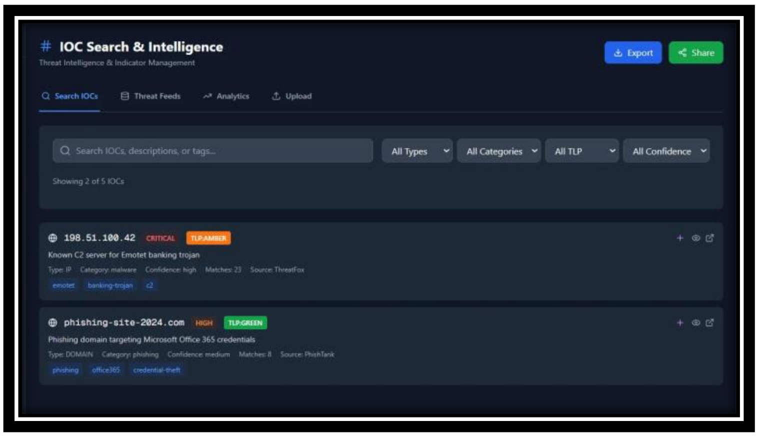
Key Capabilities

- **Incident Queue –** Centralized oversight with clear prioritization, SLA tracking, and streamlined resolution workflows.
- **Live Triage** – Real-time validation and containment with advanced analysis to reduce response times.
- **Active Threats** – Continuous monitoring of compromised assets, critical services, suspicious users, and IOCs for proactive defense.
- **MITRE ATT&CK** – Integrated mapping of detected techniques for standardized classification and regulator-ready reporting.
- **Automated Actions** – Predefined playbooks to isolate hosts, reset credentials, block IOCs, and activate response teams.
- **Framework Alignment** – Guided response workflows based on NIST and SANS methodologies to ensure resilience and compliance.

IOC Search & Intelligence

Threat Intelligence & Indicator Management

Comprehensive Indicators of Compromise IOC search and threat intelligence management enables security teams to quickly investigate suspicious IPs domains file hashes and email addresses Integrated with multiple threat feeds for real-time enrichment and attribution



Showing 2 of 5 IOCs

198.51.100.42
Known C2 server for Emotet banking trojan
Type: IP · Category: malware · Confidence: high · Matches: 23 · Source: ThreatFox

phishing-site-2024.com
Phishing domain targeting Microsoft Office 365 credentials
Type: DOMAIN · Category: phishing · Confidence: medium · Matches: 8 · Source: PhishTank

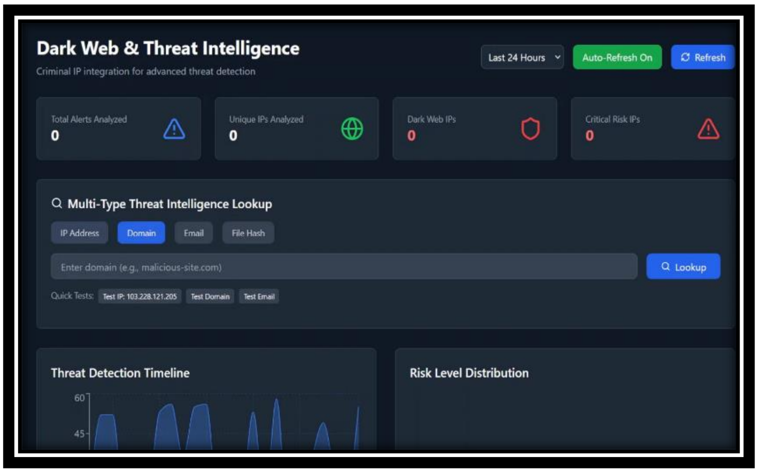
Key Capabilities:

- **Unified Repository** – 6,000+ indicators aggregated from OpenCTI, VirusTotal, OTX, and more.
- **Targeted Search** – Lookup by IP, domain, hash, URL, email, or filename with advanced filters.
- **Confidence & TLP Tags** – Source attribution, scoring, and classification for regulator-ready intelligence.
- **Export & Integration** – CSV/JSON downloads for audit, offline analysis, and SOC workflows.
- **Threat Hunting Support** – Actionable tips and analytics to accelerate detection.
- **Case & Alert Linkage** – Seamless integration across incident lifecycle.

Dark Web & Threat Intelligence

Criminal IP Integration & Advanced Threat Detection

Shield Sphere includes comprehensive dark web monitoring and threat intelligence capabilities providing early warning of credential leaks brand mentions malware distribution and targeted attacks against your organization Criminal IP integration enables advanced threat detection across Tor I2P and paste sites



Dark Web & Threat Intelligence

Criminal IP integration for advanced threat detection

Total Alerts Analyzed 0

Unique IPs Analyzed 0

Dark Web IPs 0

Critical Risk IPs 0

Multi-Type Threat Intelligence Lookup

Enter domain (e.g., malicious-site.com)

Quick Tests: Test IP: 103.228.121.205 Test Domain Test Email

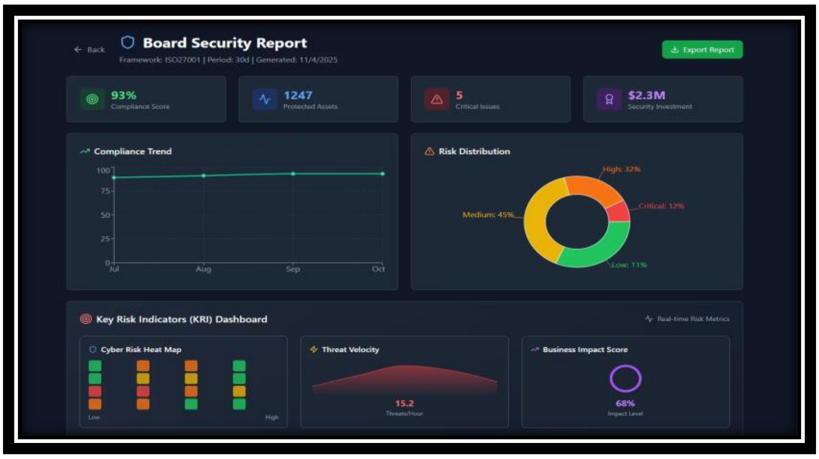
Key Capabilities:

- **Multi-Vector Threat Lookup**
  - Search by IP, domain, email, or hash
  - Detect malicious artifacts across sources
- **Real-Time Threat Metrics**
  - Monitor dark web and TOR activity
  - Track scanner and anonymous VPN threats
- **Risk Level Distribution**
  - Visualize threat severity over time
  - Prioritize critical and high-risk indicators
- **Threat Detection Timeline**
  - View detection trends across 24h intervals
  - Enable auto-refresh for live updates
- **Security Recommendations Engine**
  - Configure API keys for full coverage
  - Adjust policies based on feed analysis
- **SOC-Ready Intelligence Sync**
  - Integrate with Shield Sphere detection workflows
  - Automate response to high-risk threats

Board Security Report

Executive-Ready Compliance & Risk Reporting

Auto-generated board-ready security reports provide comprehensive yet concise visibility into security posture compliance status and key risk indicators Perfect for quarterly board meetings annual reports and investor due diligence.



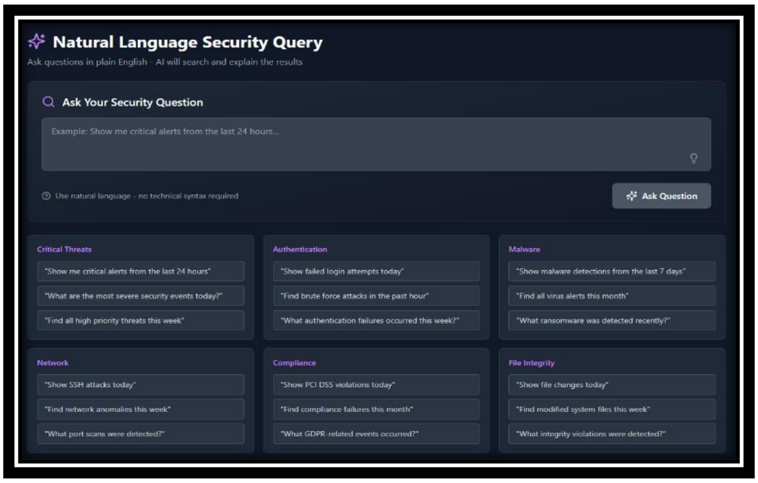
Report Components:

- **Compliance Score** - overall compliance score across frameworks
- **Protected Assets** - assets under active monitoring
- **Critical Issues** - high-priority items requiring board attention
- **Security Investment** - $/million YTD spend on security initiatives
- **Compliance Trend** - historical trend showing continuous improvement
- **Risk Distribution** – [High, Critical, Medium, low]
- **Key Risk Indicators** - cyber risk heat map, threat velocity, business impact score

Natural Language Security Query

AI-Powered Security Questions in Plain English

AI-powered natural language interface enables anyone from executives to analysts to query security data without technical knowledge. Simply ask questions in plain English and receive instant intelligent responses- No need to learn complex query languages or understand database schemas



Ask questions in plain English - AI will search and explain the results

Example: Show me critical alerts from the last 24 hours...

Use natural language - no technical syntax required

Critical Threats

"Show me critical alerts from the last 24 hours"

"What are the most severe security events today?"

"Find all high priority threats this week"

Authentication

"Show failed login attempts today"

"Find brute force attacks in the past hour"

"What authentication failures occurred this week?"

Malware

"Show malware detections from the last 7 days"

"Find all virus alerts this month"

"What ransomware was detected recently?"

Network

"Show SSH attacks today"

"Find network anomalies this week"

"What port scans were detected?"

Compliance

"Show PCI DSS violations today"

"Find compliance failures this month"

"What GDPR-related events occurred?"

File Integrity

"Show file changes today"

"Find modified system files this week"

"What integrity violations were detected?"

Example Queries:

Critical Threats:

- Show me critical alerts from the last 24 hours
- What are the most severe security events today
- Find all high priority threats this week

Authentication:

- Show failed login attempts today
- Find brute force attacks in the past hour
- What authentication failures occurred this week

Malware:

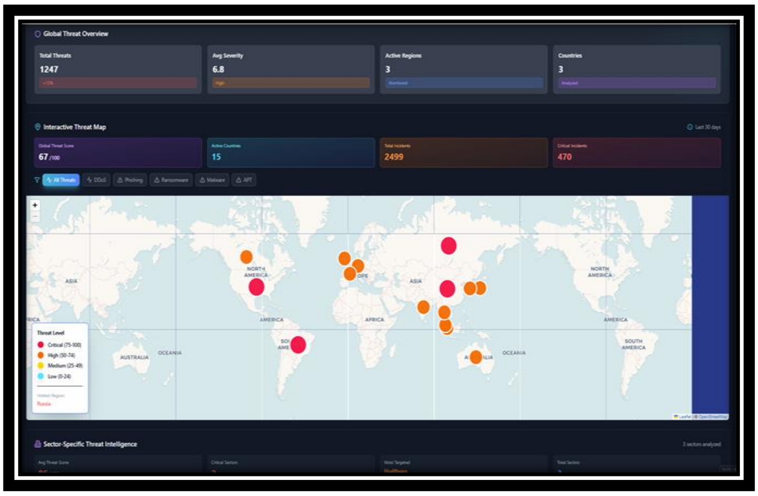
- Show malware detections from the last 7 days
- Find all virus alerts this month
- What ransomware was detected recently

Compliance:

- Show PCI DSS violations today
- Find compliance failures this month
- What GDPR-related events occurred

Global Threat Landscape

AI-Powered Security Questions in Plain English



Global Threat Overview

Total Threats 1247

Avg Severity 6.8

Active Regions 3

Countries 3

Interactive Threat Map

Last 30 days

Global Threat Score 67 /100

Active Countries 15

Total Incidents 2499

Critical Incidents 470

Sector-Specific Threat Intelligence

3 sectors analyzed

Avg Threat Score

Critical Sectors

Most Targeted Healthcare

Total Sectors

Provides localized situational awareness by mapping IOCs, domains, and IPs against regional adversary activity. It contextualizes raw indicators with confidence levels, TLP classifications, and sector relevance, enabling SOCs and executives to act on threats most pertinent to their geography.

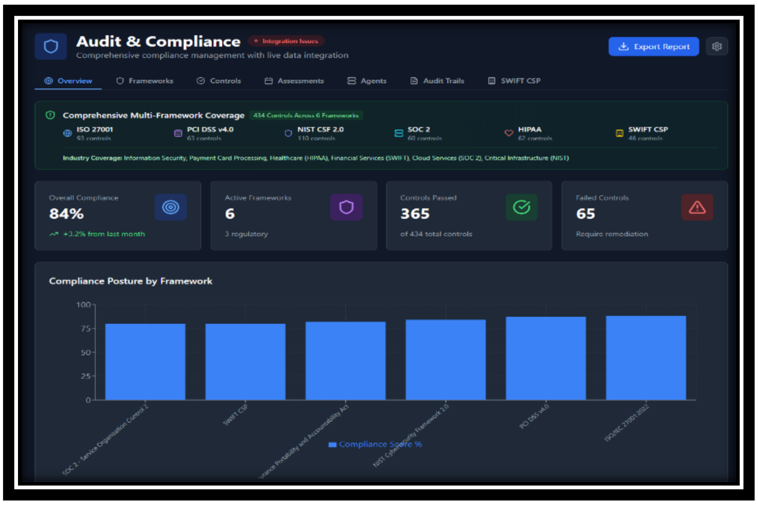
Key Capabilities

- **IOC Aggregation**
  - Consolidates hashes, domains, and IPs
  - Sources: OpenCTI, VirusTotal, OTX
- **Regional Contextualization**
  - Filters by type, category, and confidence
  - Highlights region-specific threat indicators
- **Threat Actor Profiling**
  - Maps indicators to known adversary tactics
  - Links to local and regional campaigns
- **Sector-Specific Insights**
  - Focuses on BFSI and regulated industries
  - Surfaces targeted attack vectors
- **Executive Reporting**
  - Generates regulator-ready CSV/JSON exports
  - Summarizes threats in concise dashboards
- **SOC Integration**
  - Syncs with Shield Sphere detection engine
  - Enables automated response to local threats

Audit & Compliance

Centralized oversight of regulatory frameworks, control health, and audit readiness.

Our Audit & Compliance modules deliver over 4,000+ automated controls and seamlessly connect with more than 50+ recognized audit and regulatory compliance organizations or certifying authorities. With these powerful features, organizations can efficiently meet regulatory requirements, keep operations secure and consistent, and clearly demonstrate accountability through streamlined assessments and transparent reporting.



Audit & Compliance

Comprehensive compliance management with live data integration

Comprehensive Multi-Framework Coverage — 434 Controls Across 6 Frameworks

ISO 27001	PCI DSS v4.0	NIST CSF 2.0	SOC 2	HIPAA	SWIFT CSP
93 controls	63 controls	110 controls	60 controls	62 controls	46 controls

Industry Coverage: Information Security, Payment Card Processing, Healthcare (HIPAA), Financial Services (SWIFT), Cloud Services (SOC 2), Critical Infrastructure (NIST)

Overall Compliance	Active Frameworks	Controls Passed	Failed Controls
84%	6	365	65
+3.2% from last month	3 regulatory	of 434 total controls	Require remediation

Compliance Posture by Framework

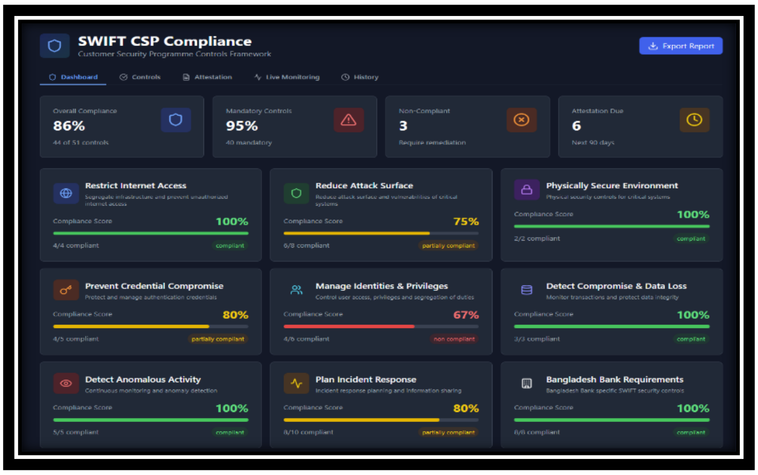
Key Capabilities:

- **Multi-Framework Coverage**
  - Tracks ISO, SOC 2, PCI, NIST, HIPAA, SWIFT
  - Monitors 434 controls across 6 frameworks
- **Live Compliance Scoring**
  - Calculates scores per framework and agent
  - Flags failed controls for remediation
- **Control Center Dashboard**
  - View control status, priority, and owner
  - Filter by category, framework, or risk level
- **Agent-Level Compliance Checks**
  - Assess system benchmarks across OS platforms
  - View passed/failed checks per device
- **Audit Trail Monitoring**
  - Log user actions and system events
  - Filter by category, severity, and compliance
- **Assessment & Certification Tracking**
  - Record external audits and remediation stats
  - Visualize findings by severity level
- **Compliance Posture Visualization**
  - Compare frameworks by compliance percentage
  - Highlight trends and improvement areas
- **SWIFT CSP Compliance Panel**
  - Track mandatory and regional controls
  - Monitor attestation deadlines and gaps

SWIFT Compliance

Targeted monitoring of SWIFT CSP controls and attestation timelines for financial integrity.

Shield Sphere platform automates SWIFT CSP control monitoring, collects and analyzes relevant security logs, and generate audit-ready reports. This ensures financial services organizations meet SWIF requirements, detect threats quickly, and maintain continuous compliance.



SWIFT CSP Compliance
Customer Security Programme Controls Framework

Overall Compliance
86%
44 of 51 controls

Mandatory Controls
95%
40 mandatory

Non-Compliant
3
Require remediation

Attestation Due
6
Next 90 days

Restrict Internet Access
Segregate infrastructure and prevent unauthorized internet access
Compliance Score 100%
4/4 compliant — compliant

Reduce Attack Surface
Reduce attack surface and vulnerabilities of critical systems
Compliance Score 75%
6/8 compliant — partially compliant

Physically Secure Environment
Physical security controls for critical systems
Compliance Score 100%
2/2 compliant — compliant

Prevent Credential Compromise
Protect and manage authentication credentials
Compliance Score 80%
4/5 compliant — partially compliant

Manage Identities & Privileges
Control user access, privileges and segregation of duties
Compliance Score 67%
4/6 compliant — non compliant

Detect Compromise & Data Loss
Monitor transactions and protect data integrity
Compliance Score 100%
3/3 compliant — compliant

Detect Anomalous Activity
Continuous monitoring and anomaly detection
Compliance Score 100%
5/5 compliant — compliant

Plan Incident Response
Incident response planning and information sharing
Compliance Score 80%
8/10 compliant — partially compliant

Bangladesh Bank Requirements
Bangladesh Bank specific SWIFT security controls
Compliance Score 100%
8/8 compliant — compliant

Key Capabilities:

- **Framework Management**
  - Supports multiple regulatory and industry frameworks (e.g., ISO 27001, PCI DSS, GDPR, HIPAA, SWIFT)
  - Tracks compliance posture across frameworks with unified dashboards
- **Control Mapping & Assessment**
  - Maps controls to frameworks and business units
  - Automates control testing and evidence collection
  - Flags failed or in-progress controls for remediation
- **Audit Trails & Forensics**
  - Maintains immutable logs of system and user activities
  - Enables traceability for internal and external audits
- **Compliance Scoring & Reporting**
  - Calculates real-time compliance scores by framework
  - Generates executive-ready reports with audit timelines and remediation status
- **Agent & Asset Monitoring**
  - Links compliance status to monitored agents and assets
  - Identifies gaps in coverage or hygiene
- **Case & Remediation Management**
  - Opens cases for failed controls or audit findings
  - Tracks remediation progress with ownership and deadlines
- **Regulatory Intelligence**
  - Integrates updates from global regulatory bodies
  - Flags changes impacting current compliance posture

Deployment Models

Shield Sphere offers flexible deployment options from complete on-premise control to fully managed security operations. Select the model that best fits your organizational needs, infrastructure requirements and operational capabilities

On-Premise Solutions and Services

Product/Service	Tier	Agent Range	Inclusions
Raptas Shield Sphere	Standard	1001-2000	Complete platform, all dashboards, SOAR, 8x5 support
Raptas Shield Sphere	Enterprise	2001+	Everything + custom integrations, dedicated support
Dark Web Intelligence	Add-on	Small	Proactive dark web monitoring (Agents less than 500)
Dark Web Intelligence	Add-on	Medium	Proactive dark web monitoring (Agents less than 2K)
Dark Web Intelligence	Add-on	Large	Proactive dark web monitoring (Agents more than 2K+)
Advanced Threat Intel	Add-on	Small	Real-time threat intelligence (Agents less than 500)
Advanced Threat Intel	Add-on	Medium	Real-time threat intelligence (Agents less than 2K)
Advanced Threat Intel	Add-on	Large	Real-time threat intelligence (Agents more than 2K+)

Managed Security Services - MSS

Package Name	Agent Limit	Key Features
SOC Starter	Up to ~100	24x7 monitoring, event correlation, 1 month Indexed data retention, 3 months Archive data retention, standard support
SOC Essentials	Up to ~250	24x7 monitoring, event correlation, 3 month Indexed data retention, 12 months Archive data retention, standard support
SOC Professional	Up to ~500	24x7 monitoring, event correlation, 3 month Indexed data retention, 12 months Archive data retention, standard support, active response, monthly reports
SOC Enterprise	Up to ~1000	24x7 monitoring, event correlation, 3 month Indexed data retention, 12 months Archive data retention, standard support, active response, monthly reports, QBRs, board reporting
SOC Enterprise Plus	Up to ~1500	24x7 monitoring, event correlation, 3 month Indexed data retention, 12 months Archive data retention, standard support, active response, monthly reports, QBRs, board reporting, full compliance
Large Enterprise	1500+	24x7 monitoring, event correlation, 3 month Indexed data retention, 12 months Archive data retention, standard support, active response, monthly reports, QBRs, board reporting, full compliance, SOC Analyst's monthly review

Connect with Us or contact our partners:

Get Started with Shield Sphere

Transform your security operations today

📧 Email: connect@raptas.ai

🌐 Website: www.raptas.ai

Schedule personalized demo or consultation

POWERING DIGITAL FUTURES