bSOC: Security Operations Center as a Service

A strategic briefing for CISOs, CTOs, CIOs, CFOs, IT Directors, and Board Members on how managed SOC closes the detection gap that tools alone cannot.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

bSOC Security Operations

The Monitoring Gaps Most Organizations Don't See

258

Days to Identify a Breach

Global average (IBM Security 2024). Organizations with 24/7 SOC reduce this window to hours.

45%

Alerts Uninvestigated

In understaffed operations. Average enterprise receives 500 to 1,000+ alerts per day.

29

Minute Breakout Time

Average attacker lateral movement time. Detection windows in days are insufficient.

128+

Unmonitored Hours/Week

With business-hours-only monitoring — nights, weekends, and holidays are left exposed.

What Your Environment May Have Right Now

Unmonitored Windows

128+ hrs/week with no analyst coverage after hours

SIEM Alert Backlog

Alerts accumulating faster than analysts can triage

No Threat Hunting

Reactive detection only; hidden threats not proactively surfaced

Manual Compliance

Audit prep consuming analyst time instead of detection work

Untuned SIEM Rules

False positives causing alert fatigue and missed real threats

No Incident Playbooks

Improvised response when ransomware or BEC strikes

Cloud Log Gaps

AWS CloudTrail, Azure Monitor, and GCP Audit Logs are not centrally correlated

Endpoint Blind Spots

EDR telemetry not integrated into centralized detection workflow

What We Find During Assessment

Every organization believes their monitoring posture is stronger than it is. These are the most common gaps uncovered at onboarding.

SIEM Alert Backlog	SIEM Alert Backlog
We have a SIEM, so we have SOC coverage	A SIEM collects logs. A SOC investigates what the SIEM surfaces. Without analysts, 45% of alerts go unreviewed.
Our team monitors during business hours - that covers most risk	Ransomware deploys nights, weekends, and holidays. 8x5 monitoring leaves 128 hrs/week completely unmonitored.
An in-house SOC will know our environment better	bSOC onboarding covers full asset mapping and SIEM configuration. Managed teams add cross-industry threat pattern recognition no single-org team can develop.
SOC-as-a-Service is for large enterprises only	Mid-market organizations benefit most: enterprise-grade detection without a $2.5M+ capital investment and 12 to 24 months to build.
We have never had a breach, so our monitoring is sufficient	Average dwell time is 258 days. Most breaches are discovered months after initial compromise — not at the point of entry.

Detection is not the same as collection. Every unchecked belief above is a confirmed gap pattern from real bSOC onboarding engagements.

Prevention Is 30 to 60x Cheaper Than Recovery

The Real Cost of Inaction

$4.88M

Average Breach Cost

Global average cost of a data breach (IBM Security 2024)

$2.73M

Ransomware Recovery

Average recovery cost excluding the ransom payment itself

$5.46M

Late Detection Cost

Average breach cost when dwell time exceeds 200 days (IBM)

100

Days Saved

AI-augmented SOC cuts breach lifecycle (IBM)

Framework	Maximum Penalty	Trigger
GDPR	EUR 20M or 4% global revenue	Breach notification failure or inadequate controls
PCI DSS	$5,000 to $100,000/ month	Non-compliance with Req. 10 to 12 log monitoring
RBI / SEBI	Regulatory action + license risk	Cyber resilience framework non-compliance
DORA / NIS2	Up to 2% global turnover	ICT incident management failures
HIPAA	$100 to $50,000 per violation	Failure to detect and report PHI breach

Insurance Benefit

30 to 40% cyber insurance premium reduction with managed SOC and documented SLAs. CREST-certified providers are Tier 1 underwriter evidence accepted by leading insurers.

The ROI Equation

A single breach at $4.88M average cost dwarfs the annual investment in managed SOC by 30 to 60x. Prevention is not a cost center; it is risk capital deployed efficiently.

The Financial Case in Plain Numbers

Objections vs. Facts

These are the four most common forms of resistance encountered before a breach changes the conversation.

What Clients Say	Why It Is Costing Them	The Fact
We have never had a breach	Breaches go unnoticed for 258 days on average	Average cost when detected late: $5.46M
We cannot afford a managed SOC	In-house SOC setup costs $2.5M+ before operations begin	bSOC: device-based pricing, zero capital outlay
Our SIEM handles it	SIEM without analysts means 45% of alerts uninvestigated	Tools without operations leave critical gaps
We will build in-house next year	12 to 24 months to build; attackers do not wait	30 to 40% reduction in cyber insurance premiums with managed SOC now

Every month of deferred decision is a month of 128 unmonitored hours, uninvestigated alerts, and no tested incident playbook. The cost of delay is measurable.

What bSOC Detects and Responds To

74% faster breach detection for organizations with a functioning SOC vs. those without. Every MITRE ATT&CK technique has a corresponding bSOC detection rule - not just signature-based, but behavioral.

Identity & Access

Credential Stuffing and Brute Force : Azure AD, Okta, AWS IAM; login anomaly behavioral rules

Privilege Escalation : MITRE ATT&CK T1078-mapped lateral movement detection

Insider Threat : Anomalous access patterns, off-hours activity, bulk download detection

Network & Perimeter

Lateral Movement : East-west traffic analysis; SMB, RDP, WMI abuse across endpoints

Command and Control (C2) : Beaconing detection, DNS tunneling, unusual outbound to known C2 infrastructure

Endpoint & Computer

Ransomware Deployment : File encryption initiation; average attacker breakout is 29 minutes (CrowdStrike)

Living-off-the-Land (LotL) : PowerShell, WMI, certutil abuse; fileless malware execution chains

Cloud & Data

Cloud Misconfiguration : AWS CloudTrail, Azure Activity Logs, GCP Audit Logs for unauthorized API calls

Data Exfiltration : Large-volume transfers; S3/Blob anomalous access pattern detection

Logging & Compliance

Log Tampering : Alerts on CloudTrail disablement, SIEM log gaps, audit trail manipulation

Business Email Compromise : Inbox rule creation, OAuth app consent abuse in M365/Google Workspace

Every Log Source, Every Layer, Every Threat Vector

"We monitor EVERY log source, EVERY endpoint, EVERY cloud layer. Because partial coverage is the gap attackers exploit."

1. 24/7 Monitoring and Triage

Log ingestion: endpoints, network, cloud, applications

AI-powered alert triage and noise reduction

MITRE ATT&CK rule mapping on every alert

Defined SLAs for detection and escalation

2. Threat Detection and Hunting

Behavioral analytics: user, entity, network baselines

Proactive threat hunting for undetected indicators

Proprietary Threatsploit intelligence (83+ editions)

Third-party and live feed integration

3. Incident Response

Tested playbooks: ransomware, BEC, insider threat, DDoS

Escalation, containment, forensic documentation

Coordination with client IT and legal teams

4. SIEM Management

Continuous rule tuning and false positive reduction

Coverage gap identification and remediation

Integration with existing EDR, NDR, cloud security tools

5. Compliance Reporting

Automated evidence collection via LURA Portal

50+ frameworks: GDPR, PCI DSS, RBI, SEBI, HIPAA, DORA, NIS2

Audit-ready reports generated on demand

6. Cloud Security Monitoring

AWS CloudTrail, Azure Monitor, GCP Audit Logs

Cloud-native misconfiguration and anomaly detection

Multi-cloud correlation across environments

Our 8-Phase Engagement Methodology

What Happens at Every Step

01 SOC Readiness Assessment

Gap analysis of current monitoring posture, tool inventory, and coverage windows

02 Scope and Onboarding

Asset mapping, SIEM configuration, detection rule deployment, integration with existing EDR/NDR/cloud tools

03 LURA Portal Provisioning

AI-powered dashboard setup, compliance framework mapping, alert workflow configuration

04 Go-Live and Baseline

24/7 monitoring activated; behavioral baselines established over first 2 weeks

05 Continuous Detection and Hunting

Ongoing triage, MITRE ATT&CK-mapped alerting, proactive threat hunting cycles

06 Incident Response

Playbook-driven escalation, containment, forensic documentation, client coordination

07 Reporting and Review

Monthly threat reports, compliance evidence packages, executive briefings

08 Continuous Improvement

SIEM tuning, rule updates, threat intelligence refresh, quarterly posture reviews

Deployment Models and Timeline Drivers

Deployment Model	Endpoints	Go-Live Timeline	Includes
Shared SOC	50 to 500 endpoints	2 to 4 weeks	Shared analyst pool, SIEM management, monthly reports
Dedicated SOC	500+ endpoints	3 to 6 weeks	Named analysts, custom detection rules, executive briefings
Hybrid SOC	Existing team + gaps	2 to 4 weeks	After-hours coverage, co-managed playbooks
SOC Readiness Assessment	Any size	48-hour scope	Gap analysis, integration review, cost model

What Drives Your Timeline

Environment Complexity

Number of log sources, cloud accounts, and endpoint types in scope

Existing Tooling

SIEM, EDR, NDR integration readiness at onboarding

Compliance Requirements

Frameworks requiring specific log retention or evidence formats

Onboarding Responsiveness

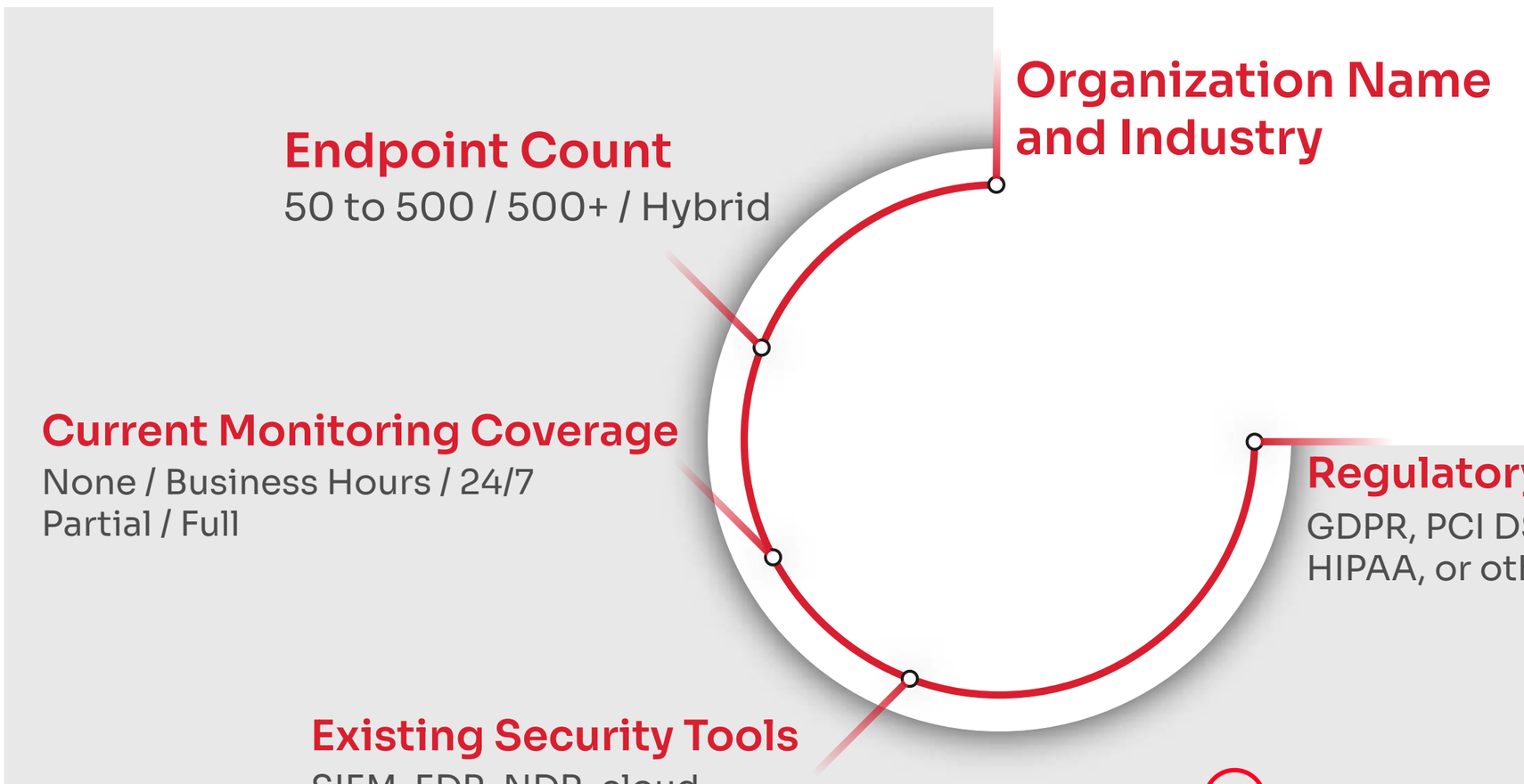
Access provisioning and asset inventory availability from client side

Two Paths for Security Operations

The comparison below is not theoretical. It reflects the operational reality measured across hundreds of bSOC engagements and validated against IBM and CrowdStrike industry benchmarks.

Without Proactive SOC	With bSOC Managed SOC
128+ unmonitored hours/week on nights, weekends, and holidays	24/7/365 coverage with defined SLAs; zero unmonitored windows
45% of alerts uninvestigated; analyst capacity exhausted by volume	AI-powered triage reduces noise; analysts focus on confirmed real threats
258-day average breach dwell time; costs scale with time undetected	AI-augmented detection reduces breach lifecycle by 100 days (IBM)
Improvised incident response without tested playbooks	Tested playbooks for ransomware, BEC, insider threat, and DDoS
Manual compliance evidence; gaps surface only during audit	LURA Portal generates compliance-ready reports automatically on demand
$2.5M+ capital and 12 to 24 months to build in-house SOC	Zero capital outlay; predictable device-based pricing from day one
No 3-year TCO model; hidden costs accumulate over time	Full cost transparency; cyber insurance premium reduction of 30 to 40%

What We Need From You to Begin



Share these 5 details and receive a tailored deployment scope within 48 hours.

Start With Zero Commitment

5,600+
Security Projects Delivered

640+
Customers Across Industries

98%
Client Retention Rate

99.8%
Compliance Achievement Rate Across 50+ Frameworks

25+
Countries: India, UAE, and beyond

0
Client Breaches Post-Engagement

CREST Approved
India's ONLY CREST-approved SOC provider

CERT-IN Empanelled
Government of India recognized security partner

ISO 27001:2022
Information security management system certified

Team Certifications

OSCP | OSWE | CISSP | CISA | CEH | GCFA | GCFE | GPEN | GWAPT | CompTIA Security+

Step 1 :

Book a SOC Readiness Assessment
45-min confidential conversation to map your monitoring posture against threats targeting your sector

Step 2 :

Receive Your Deployment Scope
Tier recommendation, integration review, compliance mapping, and timeline within 48 hours

Step 3 :

Go Live Within Weeks
Environment onboarding, SIEM configuration, and LURA Portal provisioning in 2 to 6 weeks

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique cloud security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

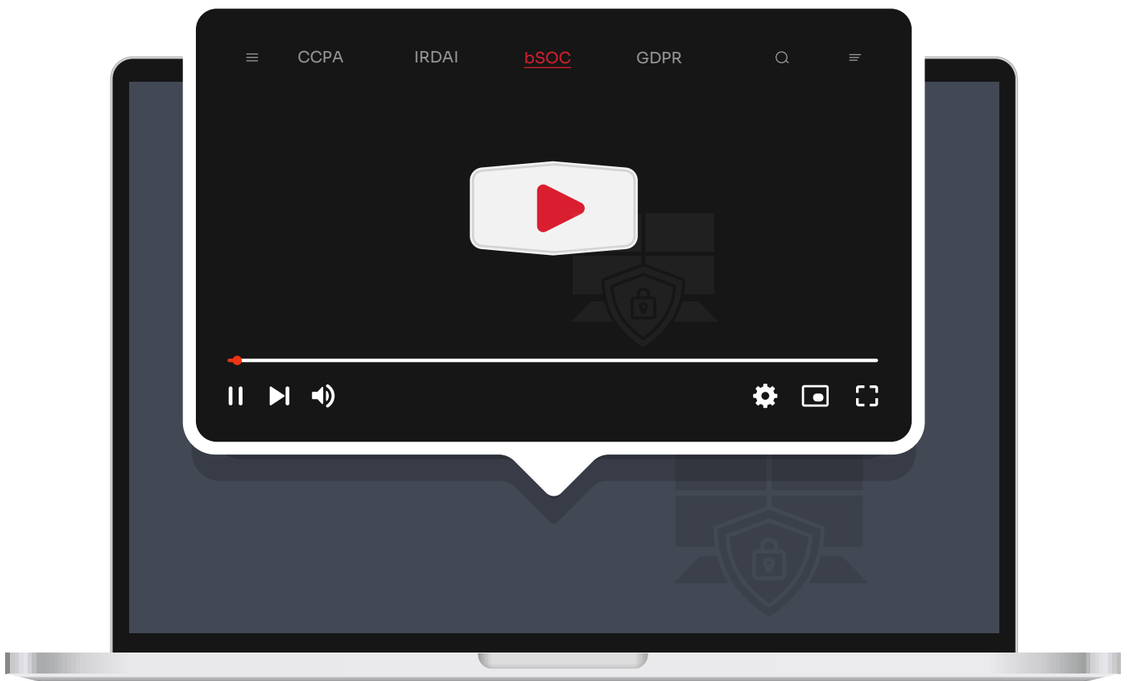
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE
consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence
India
UAE