Cyber Threat Intelligence : Detect Threats Before Impact

A strategic briefing for CISOs, CTOs, Threat Intelligence Leads, SOC Managers, and Risk Officers. Detect threats earlier, reduce response time, and strengthen cyber resilience.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

CTI

Cyber Threat Intelligence

Seeing Threats Before They Become Incidents

These figures are not meant to alarm. They are the shared context that security leaders are working with right now.

01

11 months

Average time stolen data appears on dark web before the organization discovers the breach.

Attackers are not waiting. They are already using those credentials, planning the next move, or selling access to others.

02

80%

Of breaches involve compromised credentials.

Attackers are not breaking in. They are logging in with real credentials from third-party breach markets. This is the most common initial access vector in use today.

03

$4.88M

Global average cost of a data breach (IBM).

The financial case for early detection is straightforward: finding an exposure on the dark web before it becomes a breach is a fraction of this cost.

04

258 days

Average breach lifecycle to detect and contain.

Cyber intelligence compresses this window by making your organization a proactive observer of its own external exposure, rather than a reactive victim.

Key Insight: The pattern is consistent across sectors: organizations that discover threats early through intelligence programs contain incidents faster, spend less on recovery, and face fewer regulatory consequences. The question most security leads are now asking is not whether CTI is valuable. It is how to build the right program for their organization's threat profile.

The Threat Landscape Your Peers Are Monitoring

Published benchmarks shaping how security teams prioritize intelligence investment

5,414

Ransomware Attacks

Published in a single year, up 11% year-over-year

$75M

Largest Single Ransom

Largest single ransom payment recorded (Fortune 50 company)

89%

AI-Assisted Attacks

Increase in AI-assisted cyberattacks year-over-year (CrowdStrike)

29 min

Attacker Breakout Time

Average attacker breakout time after initial access (CrowdStrike)

Five Conversations We Have With Security Operations Teams Every Week

These are not misconceptions to correct. They are reasonable assumptions that need updated context.

WHAT YOU THINK	THE REALITY
"Dark web monitoring is only relevant after a breach." A common starting point that reflects how many teams first encounter CTI.	Dark web monitoring is a pre-breach detection tool. Credentials, attack planning discussions, and stolen data appear on dark web forums long before an attack executes. Early detection is the point.
"Threat intelligence is only for large enterprises." Understandable, given how CTI platforms are typically marketed.	SMBs are disproportionately targeted because they have weaker defenses. Initial access brokers specifically market compromised SMB credentials. Intelligence is more impactful per dollar for mid-market organizations.
"OSINT only finds public information, so serious threats will not appear." A reasonable assumption about scope that is worth updating.	OSINT encompasses paste sites, breach aggregators, dark web forums, code repositories, and job postings. Professional adversaries use OSINT to plan attacks. Understanding your own exposure is the first defensive step.
"Our threat feed subscriptions cover our CTI needs." Threat feeds are useful and they are one component of broader intelligence capability.	Threat feeds provide IOCs. They do not observe dark web forums, executive credential markets, brand impersonation domains, or Telegram-based threat actor communications. These require dedicated external collection.
"Our SIEM monitors for threats, so we have coverage." SIEMs are foundational and this assumption is logical from an internal security view.	SIEM monitors your internal environment. It does not observe dark web marketplases, Telegram channels, pastebin drops, or brand impersonation infrastructure being prepared against your organization.

Key Insight: Cyber intelligence is not retrospective forensics. It is prospective surveillance of the threat landscape that targets your organization, your executives, and your supply chain. The five conversations above share one common thread: teams that ask these questions are ready to build a proactive program. The six pillars below define what that program covers.

The Six Pillars of Cyber Intelligence

Each pillar addresses a distinct and often unmonitored layer of your external threat surface.

		WHAT IT MONITORS	WHAT IT PREVENTS
01	**Strategic Intelligence**	Threat actor profiles, TTPs, industry targeting patterns	Security investment decisions and board-level risk reporting
02	**Tactical Intelligence**	IOCs, malware signatures, phishing infrastructure, exploit kits	SOC alert enrichment, faster triage, reduced false positives
03	**Operational Intelligence**	Active campaign planning in threat actor forums	Pre-attack warning before infrastructure targets your organization
04	**Dark Web Monitoring**	Credential markets, data dumps, IAB listings, ransomware groups	Early detection of credential exposure before breach escalates
05	**Brand Protection**	Typosquatting domains, fake profiles, fraudulent apps, phishing kits	Customer fraud, brand damage, and phishing campaign prevention
06	**OSINT Reconnaissance**	Attack surface via Shodan, GitHub, paste sites, job postings	Credential leaks, shodow IT exposure, supply chain OSINT risk

Regulatory Landscape: What Your Compliance Team Is Tracking

Global regulators now require threat intelligence capabilities as part of cyber risk programs

NIS2

EU: Threat intelligence and incident detection for essential entities (Art. 21)

DORA

EU: ICT threat intelligence sharing for financial entities (Art. 13)

GDPR

EU: 72-hour breach notification — early detection via CTI enables compllance

CERT-In

India: 6-hour incident reporting — intelligence-driven detection reduces reporting leg

Key Insight: Regulators are not just asking if you were breached. They are asking what your organization knew about the threat landscape, when you knew it, and what you did with that knowledge. Cyber intelligence provides the evidence of due diligence.

The Business Case Your Leadership Team Needs to See

Annual CTI program cost (mid-size org): $30–80K.
Average cost of a single breach: $4.88M.
The asymmetry is the argument.

CURRENT STATE (WITHOUT ACTIVE CTI PROGRAM)		FUTURE STATE (WITH BRISKINFOSEC CTI PROGRAM)
Stolen credentials appear on dark web **11 months** before discovery	»	Dark web credential exposure **detected within days**, not 11 months
80% breach vector (credential reuse) not being monitored externally	»	**Continuous monitoring** of the primary breach vector across your domain
Brand impersonation domains active with no detection mechanism	»	**Brand impersonation** domains identified and actioned before customer harm
Executive digital footprint visible to adversaries and unknown to you	»	**Executive exposure minimized** through continuous OSINT monitoring
Threat feeds provide IOCs but not threat actor intent or planning	»	**Threat actor intent and campaign planning** detected through forum monitoring
SIEM monitors internally but not the dark web or external threat forums	»	**Full external threat surface covered:** dark web, OSINT, and brand monitoring
Supply chain third-party exposure not mapped or continuously monitored	»	**Supply chain third-party exposure** mapped and tracked continuously

Key Insight: Cyber intelligence transforms your security posture from reactive to proactive. It gives your organization the visibility to see what attackers see, before they act. Earlier detection. Faster response. Lower cost. Stronger compliance.
That is the business case.

What Proactive CTI Investment Protects Against

Each figure represents a real cost category that early intelligence directly reduces.

$4.88M

Average breach cost.

Early detection through dark web monitoring compresses the 258-day breach lifecycle, reducing containment cost and regulatory exposure significantly.

$2.77B

Total US BEC losses reported to FBI.

Executive email credential monitoring and spear-phishing pre-indicators allow security teams to intervene before transactions occur.

$2.73M

Ransomware recovery cost (excluding ransom).

Dark web credential monitoring detects initial access broker listings before the ransomware operator purchases access.

$137K

Average loss per BEC incident.

Executive exposure monitoring detects the reconnaissance phase of business email compromise before the attack reaches the finance team.

Our Track Record. Your Due Diligence.

Proven outcomes across industries and geographies.

540+

Clients Monitored

Across 20+ countries

83+

Monthly Threatsploit Adversary Report Editions Published

Actionable intelligence. Every month.

0%

Client Breach Rate

Post-engagement across monitored clients

$127M

Estimated Breach Costs Prevented

Across client portfolio

Key Insight: Cyber attacks are no longer a question of if, but when. Organizations with cyber intelligence capabilities detect threats earlier, respond faster, and spend significantly less on recovery. Proactive intelligence is not an expense—it is an insurance policy that pays for itself.

What a Cyber Intelligence Partner Should Bring

The right partner brings operational intelligence capability, not just tool subscriptions or report templates.

CAPABILITY	TYPICAL VENDOR	BRISKINFOSEC APPROACH
Accreditation	✗ Self-certified or limited	✓ CREST Approved (India's ONLY) + CREST STAR + CERT-In + ISO 27001:2022
Dark Web Access	✗ Automated tool feeds only	✓ Automated collection plus analyst access to invitation-only threat actor forums
OSINT Capability	✗ Standard scanning tools	✓ BINT Lab proprietary tooling, OSRFramework, dnstwist, and 250+ open-source tools
Threat Reporting	✗ Generic threat updates	✓ 83+ monthly **Threatsploit** Adversary Report editions, industry-specific
Intelligence Delivery	✗ Periodic report emails	✓ Real-time alerts via **LURA** portal, continuous dashboard, monthly CTIR reports
Compliance Coverage	✗ Regional frameworks only	✓ NIS2, DORA, GDPR, CERT-In, RBI, SEBI, PCI DSS, HIPAA, ISO 27001
After Onboarding	✗ Report and exit	✓ Ongoing monitoring, quarterly executive briefings, **LURA** portal access

Key Insight: Cyber intelligence is a capability, not a product. Tools can collect data. Only skilled analysts working with the right methodology can turn that data into actionable intelligence that prevents real-world impact.
That is the Briskinfosec difference.

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique 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

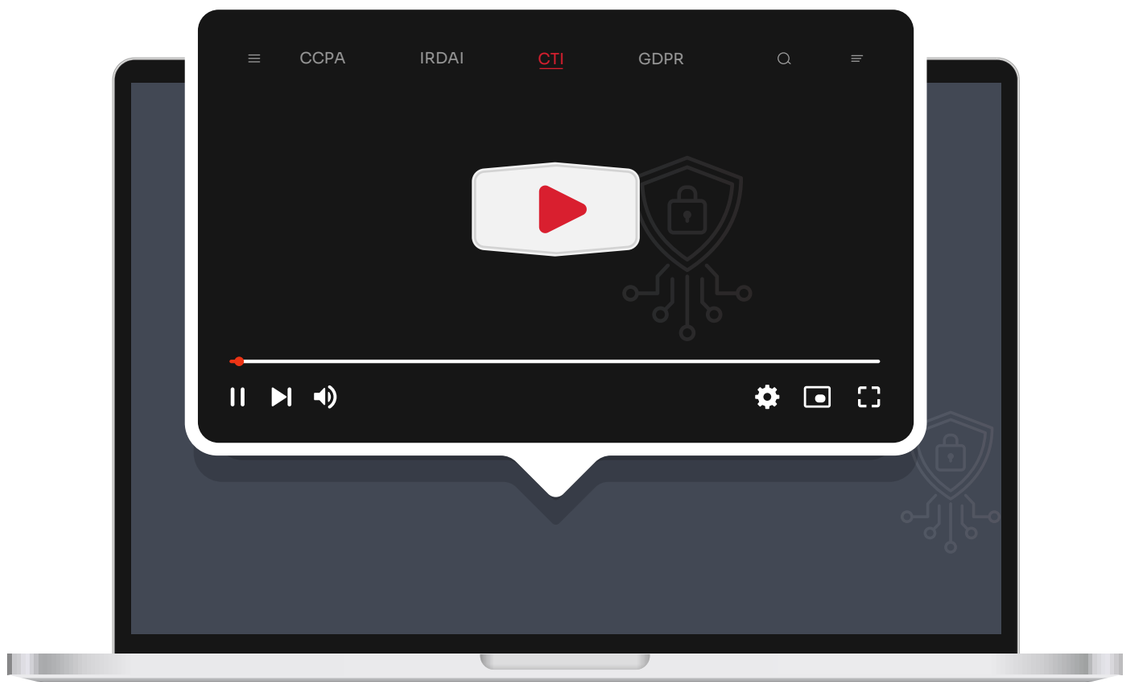
25+
Countries Client Portfolio

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