CFO2TIX-AR

Cyber Forensics and Digital Investigation for Preserving Evidence Proving Truth and Protecting Your Organization

When a breach occurs, forensic investigation determines whether evidence survives, insurance claims succeed, and the root cause is found. This briefing is prepared for CISOs, CTOs, Legal Counsel, and Risk Officers.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

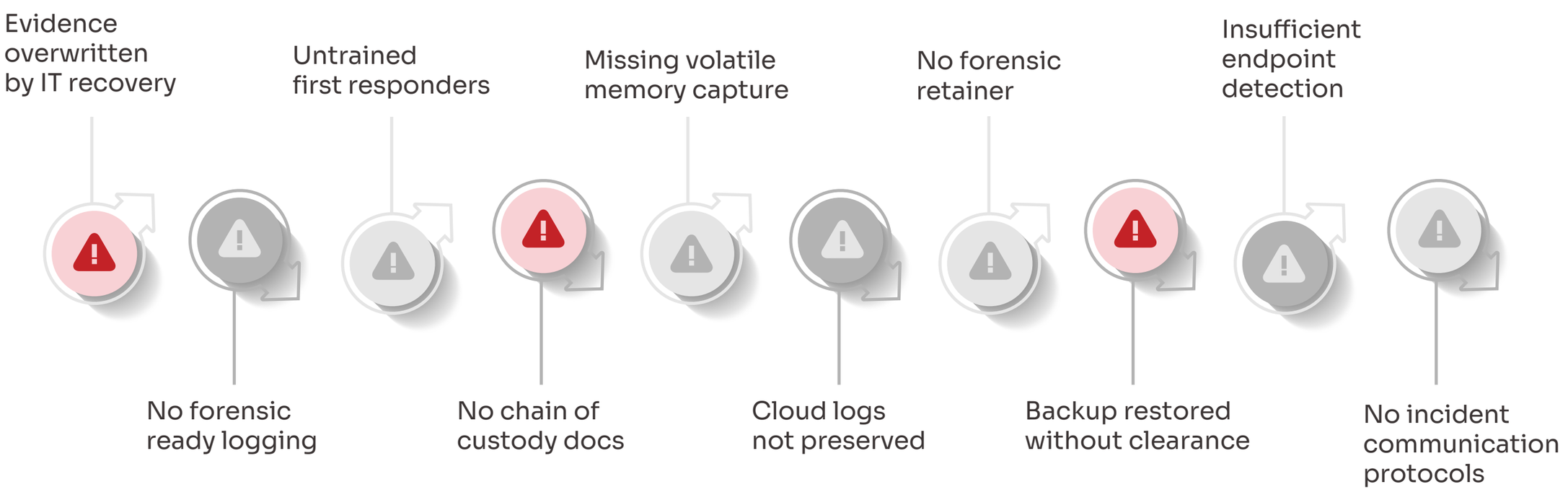
CYBER Forensics

Understanding Cyber Forensics The Gaps Most Organizations Don't See

80% of ransomware victims who restore without forensic investigation are re-attacked within 12 months
Cybereason 2024

What Your Environment May Have Right Now

Security is mandatory for every SOC 2 report. The remaining four are optional selected based on your business model and what your customers care about most.



What You Think vs What We Find

What You Think	Reality
We were breached but contained it quickly	Attacker dwell time averaged 21 days before detection
Our backups are clean and safe to restore	Malware persisted in backup snapshots taken before detection
We know what data was accessed	Log gaps and missing SIEM coverage left blind spots
Our IT team handled the incident correctly	First responder actions overwrote critical volatile evidence
We don't need forensics, we have EDR	EDR telemetry alone is insufficient for legal or insurance purposes

The Real Cost of Inaction And Why Forensic Readiness Is 30-60x Cheaper

$4.88M	€1.2B	$2.73M	$75M
Average Breach Cost	Largest GDPR Fine	Ransomware Recovery	Largest Ransom Paid

Forensic Readiness ~$50K/yr vs Breach Cost $4.88M = 97x ROI, Invest in readiness before the breach, not after.

Overcoming Resistance : The Hidden Cost of Delay

What Clients Say	Why It Costs More	The Fact
We'll deal with it when it happens	Reactive forensics cost 3-5x more than retainer-based readiness	Average dwell time is 21 days, and damage compounds daily.
We have cyber insurance, we're covered	Insurers deny claims without forensic proof of breach scope	Forensic reports are required for 78% of cyber insurance payouts
Our IT team can handle the investigation	Untrained responders destroy evidence, invalidating legal claims	Chain of custody failures void court admissibility of digital evidence
Forensics is only needed after a major breach	Small incidents without forensics become large undetected breaches	60% of SMBs that suffer a breach close within 6 months

Compliance Penalty Exposure

Framework	Maximum Penalty
GDPR	€20M or 4% of global annual turnover
certin Empanelled	₹1 Crore
DPDPA	₹250 Crore

Framework	Maximum Penalty
PCI DSS COMPLIANT	$500,000 per month
HIPAA COMPLIANT	$1.5M per violation category per year

Cyber Forensics Report

Active Threat Vectors in Post Breach Environments

RANSOMWARE PERSISTENCE

Multi-stage ransomware leaves backdoors surviving backup restoration (Conti, LockBit, BlackCat variants)

APT LATERAL MOVEMENT

Advanced persistent threats move laterally via compromised credentials, PsExec, WMI, RDP hijacking

DATA EXFILTRATION

Sensitive data staged and exfiltrated via DNS tunneling, cloud storage, encrypted channels before encryption

MEMORY-RESIDENT MALWARE

Fileless malware operating in RAM only, evading disk-based antivirus. (PowerShell Empire, Cobalt Strike)

CREDENTIAL THEFT

Mimikatz, LSASS dumps, Kerberoasting, Pass-the-Hash attacks compromising Active Directory

CLOUD LOG TAMPERING

CloudTrail disabled, Azure Activity Logs deleted, GCP Audit Logs modified to cover tracks

INSIDER THREAT ARTIFACTS

Unauthorized data access patterns, USB device connections, email forwarding rules, shadow IT usage

EMAIL COMPROMISE

Business Email Compromise (BEC), phishing infrastructure, mailbox rule manipulation, OAuth token theft

SUPPLY CHAIN COMPROMISE

Third-party software updates weaponized (SolarWinds-style), dependency poisoning, CI/CD pipeline attacks

ANTI-FORENSIC TECHNIQUES

Timestomping, log wiping, secure deletion tools, steganography, encrypted communications

Did You Know?

The average attacker dwell time is 258 days before detection, making silent compromise the norm rather than the exception.

67% of forensic evidence is lost within 72 hours without proper preservation protocols in place.

Our Investigation Scope :

We investigate EVERY artifact, EVERY system, EVERY timeline. Because partial investigation means partial truth.

MEMORY FORENSICS

- RAM acquisition and analysis
- Process injection detection
- Malware in-memory artifacts
- Credential extraction traces
- Rootkit and hooking detection
- Volatile data preservation

DISK FORENSICS

- File system timeline analysis ($MFT, USN Journal)
- Deleted file recovery
- Registry hive analysis (SAM, SYSTEM, SOFTWARE)
- Prefetch and ShimCache analysis
- Volume shadow copy examination
- Slack space and unallocated cluster analysis

NETWORK FORENSICS

- Packet capture analysis (Wireshark, NetworkMiner)
- DNS query log analysis
- NetFlow and traffic pattern analysis
- Lateral movement detection
- C2 communication identification
- Data exfiltration volume assessment

ENDPOINT FORENSICS

- Windows Event Log analysis (Security, System, PowerShell)
- Linux auditd and syslog analysis
- macOS Unified Log analysis
- Browser artifact examination
- USB device connection history
- Application execution artifacts

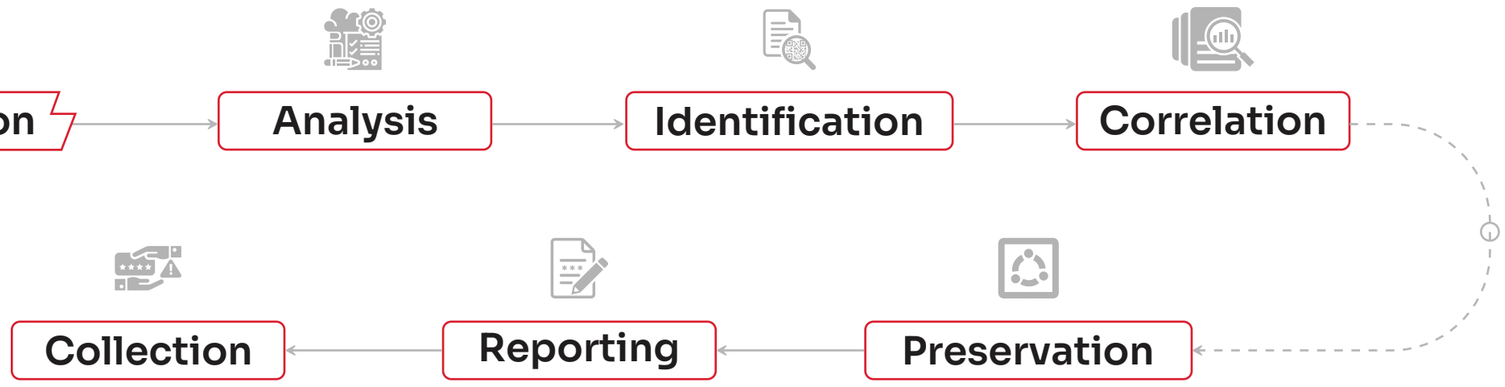
CLOUD FORENSICS

- AWS CloudTrail log analysis
- Azure Activity and Sign-in Logs
- GCP Audit Logs examination
- Container and Kubernetes forensics
- IAM activity timeline reconstruction
- Cloud storage access pattern analysis

LEGAL & COMPLIANCE

- Chain of custody documentation
- Court-admissible evidence packaging
- Expert witness testimony preparation
- Regulatory notification support (GDPR/CERT-In/PCI)
- Insurance claim evidence compilation
- NIST SP 800-86 methodology compliance

Our 7-Phase NIST SP 800-86 Methodology What Happens at Every Step



Your Decision, Who Investigates Your Breach First?

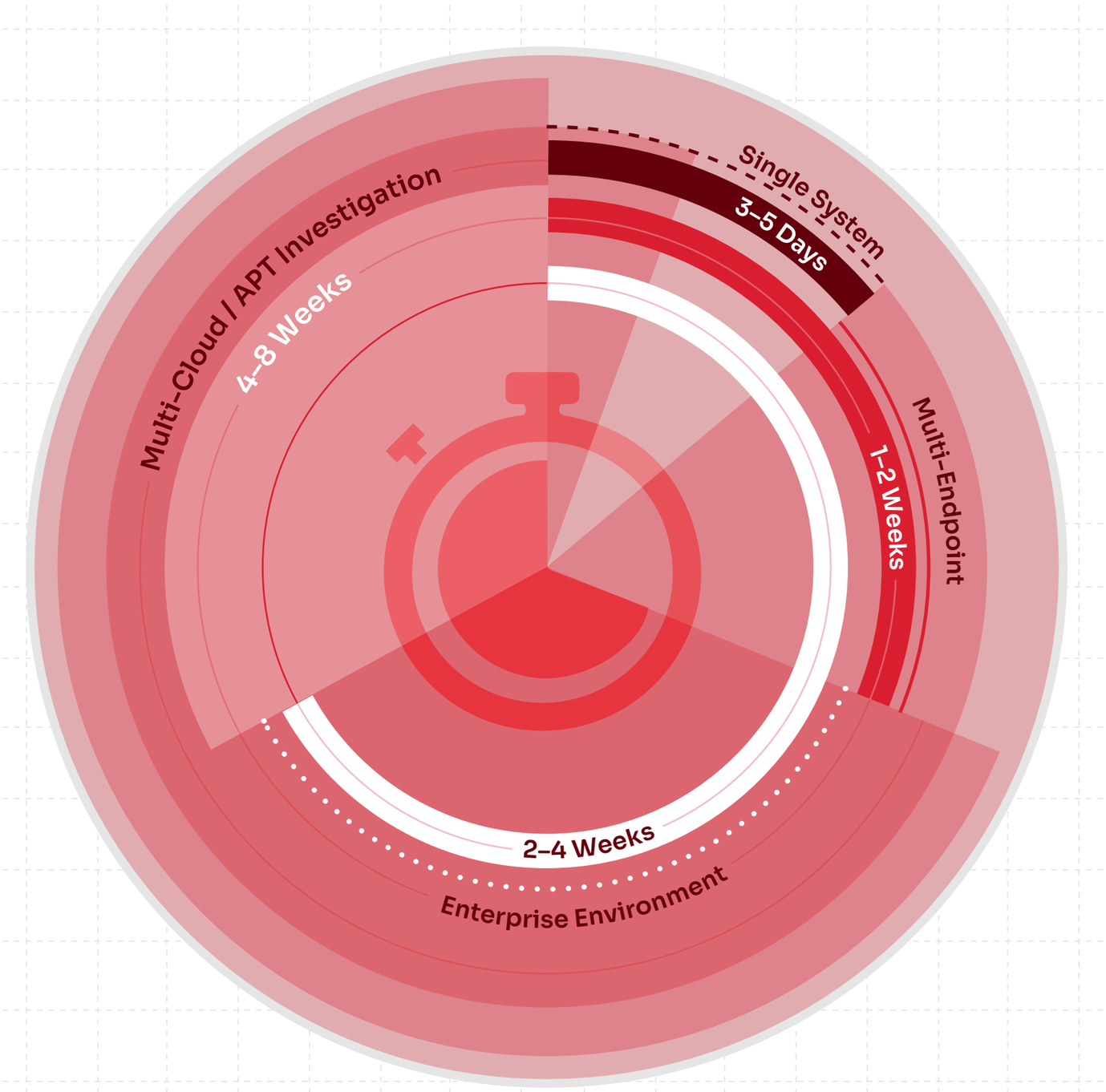
Without Forensic Readiness

- Evidence lost by untrained responders
- 80% ransomware recurrence
- Insurance claims disputed
- Regulatory deadlines missed
- 258-day breach lifecycle
- No admissible evidence for court
- Root cause never identified

With Briskinfosec

- Retainer activates in hours
- Full attack chain mapped before restore
- Chain of custody supports claims
- Notifications filed on time
- Breach contained in days
- Court-ready evidence package
- Complete root cause with remediation

Investigation Timeline by Scope



What We Need From You to Begin

- System Access
- Incident Timeline
- Affected Machine List
- Compliance Requirements
- Insurance Policy Info

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

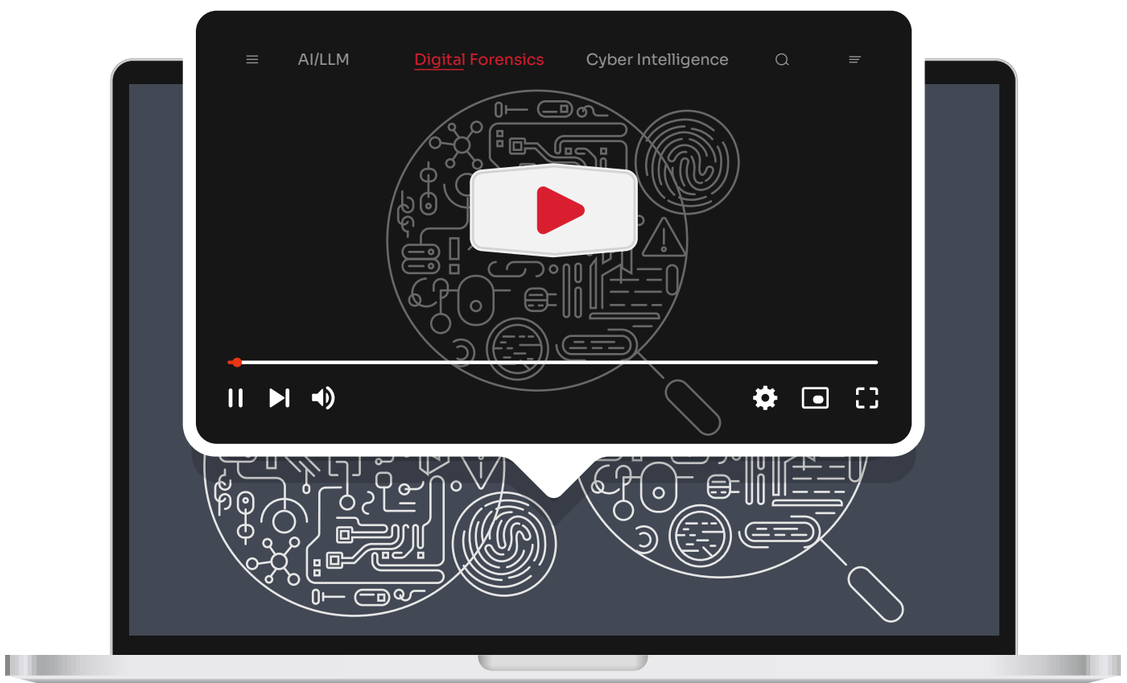
25+
Countries Client Portfolio

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