



SENTRIX PRIVATE LIMITED

DECODE. DETECT. DEFEND.

Digital Evidence • Cyber Security • Investigative Intelligence

Digital Forensics | SOC | DFIR | eDiscovery | Fraud Investigation

Due Diligence | Whistleblower Investigation | Data Recovery

Hardware, OT & Embedded Security Services

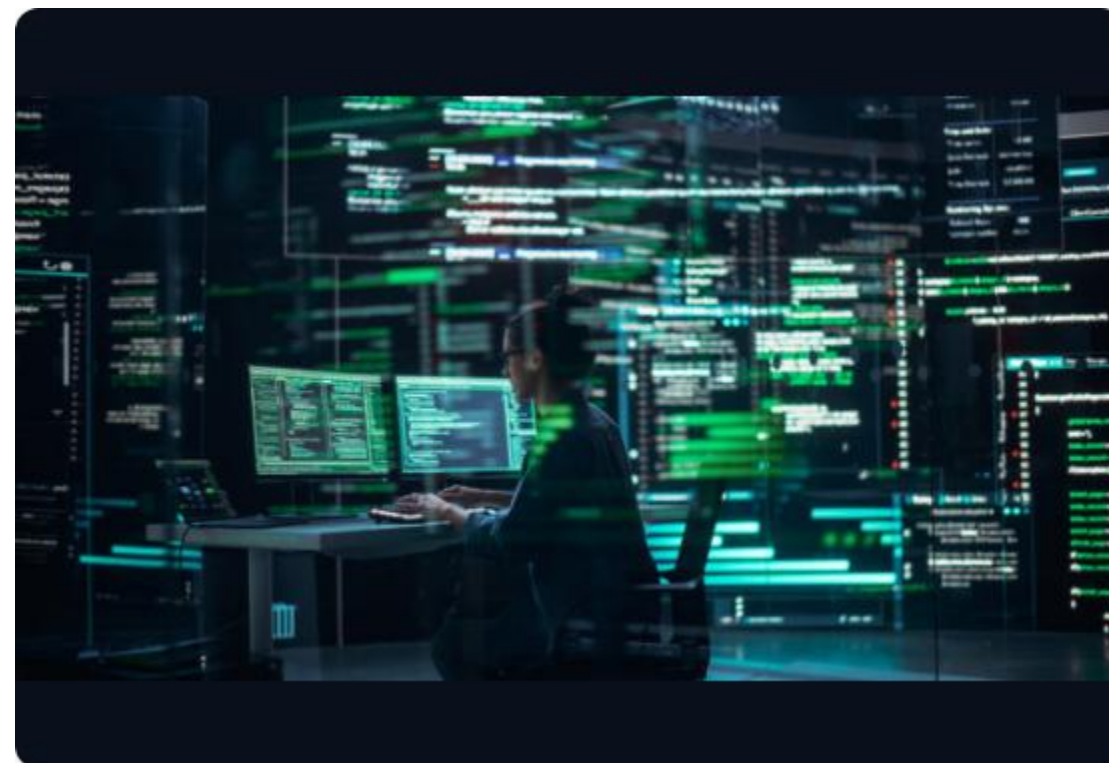
About Sentrix

Sentrix Private Limited is a technology-driven digital investigation and cybersecurity company delivering end-to-end solutions across the digital evidence lifecycle.

We help organizations identify risks, preserve evidence, investigate incidents, uncover hidden information, strengthen security, and make informed decisions.

Our Approach

Technology + Methodology + Intelligence = Actionable Outcomes



The Digital World Problem

Data is everywhere, threats are faster, and evidence is increasingly complex.



Fragmented Evidence

Distributed across computers, mobile, cloud, emails, and SaaS platforms.



Increasing Threats

Rising ransomware, phishing, insider threats, and data theft incidents.



Data Overload

Millions of files and emails make manual investigation slow and inconsistent.



Hidden Data

Critical info is often deleted, encrypted, hidden, or intentionally obfuscated.



Forensic Readiness

Lack of preparation to properly preserve evidence when incidents occur.



Regulatory Pressure

Increasing need for defensible evidence, chain of custody, and reliable audits.

Root Causes Behind Digital Risk

The visible incident is often only the symptom. We look deeper.



01 — PEOPLE

Insider threats, misconduct, credential sharing, and poor security awareness.



02 — PROCESS

Weak evidence preservation, poor incident escalation, and unclear ownership.



03 — TECHNOLOGY

Legacy systems, unpatched infrastructure, and endpoint blind spots.



04 — DATA

Siloed information, excessive data volume, and poor retention policies.



05 — GOVERNANCE

Weak controls, third-party exposure, and severe compliance gaps.



06 — RESPONSE

Late detection, alert fatigue, and incomplete root-cause analysis.

From Digital Risk to Actionable Intelligence

PROTECT

Cyber Security

Identify vulnerabilities and strengthen security posture.

DETECT

SOC

Monitor environments and identify suspicious activity.

RESPOND

DFIR

Contain, investigate, and understand security incidents.

INVESTIGATE

Digital Forensics

Extract, analyze, and mathematically correlate digital evidence.

DISCOVER

eDiscovery

Transform massive digital volumes into reviewable evidence.

ASSESS

Due Diligence

Identify hidden risks before critical business decisions.

RECOVER

Data Recovery

Salvage critical info from damaged or formatted media.

IMPROVE

Intelligence Loop

Convert findings into better controls and decision-making.

Our Core Services



Digital Forensics

Investigate. Extract. Analyze.



Cyber Security

Protect. Assess. Strengthen.



SOC

Monitor. Detect. Respond.

DFIR

Respond. Investigate. Recover.

eDiscovery

Identify. Collect. Process. Review.



Fraud Investigation

Detect. Analyze. Uncover.



Due Diligence

Verify. Assess. Mitigate Risk.



Whistleblower

Receive. Investigate. Validate. Report.



Data Recovery

Recover. Restore. Reconstruct.

Digital Forensics

Investigate. Extract. Analyze.

Challenge: Critical evidence may be deleted, encrypted, hidden, fragmented, or distributed across multiple devices.

Solution: We use industry-standard acquisition and analytical methodologies to securely identify, preserve, and interpret digital evidence.

Outcome: Translating raw, obfuscated digital data into structured, defensible, and evidence-backed findings.



Cyber Security

Protect. Assess. Strengthen.

 **Challenge:** An expanding attack surface across endpoints, cloud, identities, and third parties.

 **Solution:** We conduct rigorous vulnerability assessments, architecture reviews, and threat intelligence mapping.

 **Outcome:** Systematically identify exposure, reduce operational risk, and strengthen core organizational resilience.



Security Operations Center

Monitor. Detect. Respond.

Challenge: Security teams generate massive alert volumes. Without monitoring, organizations miss malware, exfiltration, and unauthorized access.

Solution: Sentries provides 24x7 monitoring, log correlation, threat hunting, and immediate alert triage.

Lifecycle: Monitor → Detect → Triage → Investigate → Escalate → Respond → Report.



Digital Forensics & Incident Response

Respond. Investigate. Recover.

⚡ **Challenge:** Rapid answers are required during breaches: What happened? How did they enter? Are they still present?

🔍 **Solution:** We combine rapid containment with deep forensic investigation, memory analysis, and timeline reconstruction.

⏪ **Outcome:** Contain the threat, understand the root cause, enable safe recovery, and prevent recurrence.



eDiscovery

Identify. Collect. Process. Review.

Challenge: Investigations involve millions of documents, emails, and chats, making manual review slow and highly expensive.

Solution: Sentrrix utilizes advanced deduplication, indexing, and conceptual searching to distill massive data volumes.

Outcome: Less noise. Faster review. Structurally sound and searchable evidence ready for litigation.



Fraud Investigation

Follow the Money. Follow the Data.

- ⚠ **Risks:** Financial, employee, procurement, and vendor fraud. Asset misappropriation and systemic data theft.
- 🔗 **Solution:** We uniquely correlate financial transaction data with digital communications to reconstruct events.
- 🎯 **Outcome:** Identify invisible patterns, establish irrefutable facts, and empower decisive legal action.



Due Diligence & Risk Intelligence

Know the Risk Before You Take It.

Challenge: Hidden risks in individuals, vendors, investments, and acquisition targets threaten business integrity.

Solution: We leverage OSINT, digital footprint analysis, and infrastructure intelligence to uncover red flags.

Outcome: Structured intelligence and comprehensive risk assessment before critical decisions are finalized.



Whistleblower Investigation

Structured, Confidential, Evidence-Led.



Challenge: Allegations of fraud or misconduct are often incomplete, anonymous, and exceptionally sensitive.



Solution: We provide secure intake, triage, covert preservation, and impartial forensic analysis workflows.



Outcome: Absolute confidentiality paired with evidence integrity and defensible, impartial findings.



Data Recovery

When Data Disappears, Evidence Remains.

Challenge: Accidental deletion, formatted drives, file-system corruption, and physically damaged media.

Solution: Controlled acquisition and forensic-first data carving methodologies to maximize safe recoverability.

Outcome: Safely recover, scientifically validate, and faithfully reconstruct critical business and evidentiary data.



Our Investigation Framework

A Repeatable Evidence-Led Methodology



01 – SCOPE

Define objectives, investigation questions, systems and evidence sources.



02 – PRESERVE

Protect relevant evidence and prevent unnecessary alteration.



03 – ACQUIRE

Perform controlled forensic acquisition or evidence collection.



04 – EXAMINE

Analyze artifacts, files, communications, logs and systems.



05 – CORRELATE

Connect technical, financial, communication and contextual evidence.



06 – VALIDATE

Verify findings through multiple evidence sources wherever possible.



07 – REPORT

Document facts, observations, methodology, findings and conclusions.



08 – PRESENT

Convert technical findings into clear, decision-ready intelligence.

Authenticity | Integrity | Chain of Custody | Repeatability | Documentation | Defensibility

Technology & Tools

Industry-Leading Technologies Powering Accurate Results

Mobile & Computer Forensics



Mobile: Cellebrite, Oxygen Forensics, MOBILedit, Paraben.



Computer/Disk: Magnet AXIOM, FTK, EnCase, X-Ways, Autopsy, OSForensics, FTK Imager.

eDiscovery



Platforms: FTK, Intella, Magnet AXIOM, OSForensics.

DFIR & Security



Response: Wireshark, Volatility, Splunk, Wazuh, KAPE, Enterprise SIEM / EDR ecosystems.

Fraud Investigation



Financial: Sentrix Bank Statement Analysis Tool, Data Analytics logic engines.

Tools are important. Expertise makes the difference.

Evidence Integrity & Defensibility

Technology Alone Is Not Enough. A reliable investigation requires a disciplined methodology.



PRESERVE

Identify relevant evidence and prevent unnecessary alteration.



ACQUIRE

Create controlled forensic copies or exports using documented methods.



VERIFY

Use cryptographic hashes and integrity checks wherever applicable.



DOCUMENT

Strictly record source, custodian, timestamps, and acquisition methods.



ANALYZE

Use proven, repeatable forensic workflows to deeply examine the evidence.



REPORT

Clearly distinguish Facts, Observations, Analysis, Findings, and Conclusions.

Who We Serve



Government & Law Enforcement

Digital Evidence • Investigation Support • Cyber Incident Analysis.



Corporates & Enterprises

Insider Investigations • Cybersecurity
• SOC • DFIR • Fraud.



CA & Accounting Firms

Financial Fraud • Statement Analysis •
Digital Evidence Support.



Law Firms

eDiscovery • Litigation Support •
Digital Forensics • Evidence Analysis.



Insurance Companies

Claims Investigation • Advanced Fraud
Detection • Digital Evidence.



Investors & Leaders

Due Diligence • Risk Intelligence •
Transaction Support.

SECURITY SERVICES PORTFOLIO

Sentrix Security Services

Deep-tech offensive security assessments, hardware vulnerability analysis, and regulatory compliance validation



Hardware, OT & Embedded Security Services



Automotive Cybersecurity

- ECU Penetration Testing & Firmware Security
- CAN, LIN & Automotive Ethernet Bus Audits
- Telematics & TCU Gateway Security Reviews
- ISO 21434 Engineering Standard Alignment



OT & SCADA / ICS Security

- Purdue L0–L5 Architecture & Asset Reviews
- IT-OT Network Segmentation Audits
- Clear-Text Protocol Analysis (Modbus, DNP3, OPC)
- IEC 62443 Industrial Gap Analysis



IoT & Embedded Security

- Firmware Extraction & Reverse Engineering
- Hardware Interface Analysis (UART, JTAG, SPI, I²C)
- BLE & RF Wireless Protocol Security Testing
- Companion Mobile Application Vulnerability Reviews



Hardware Research & Advanced Attacks

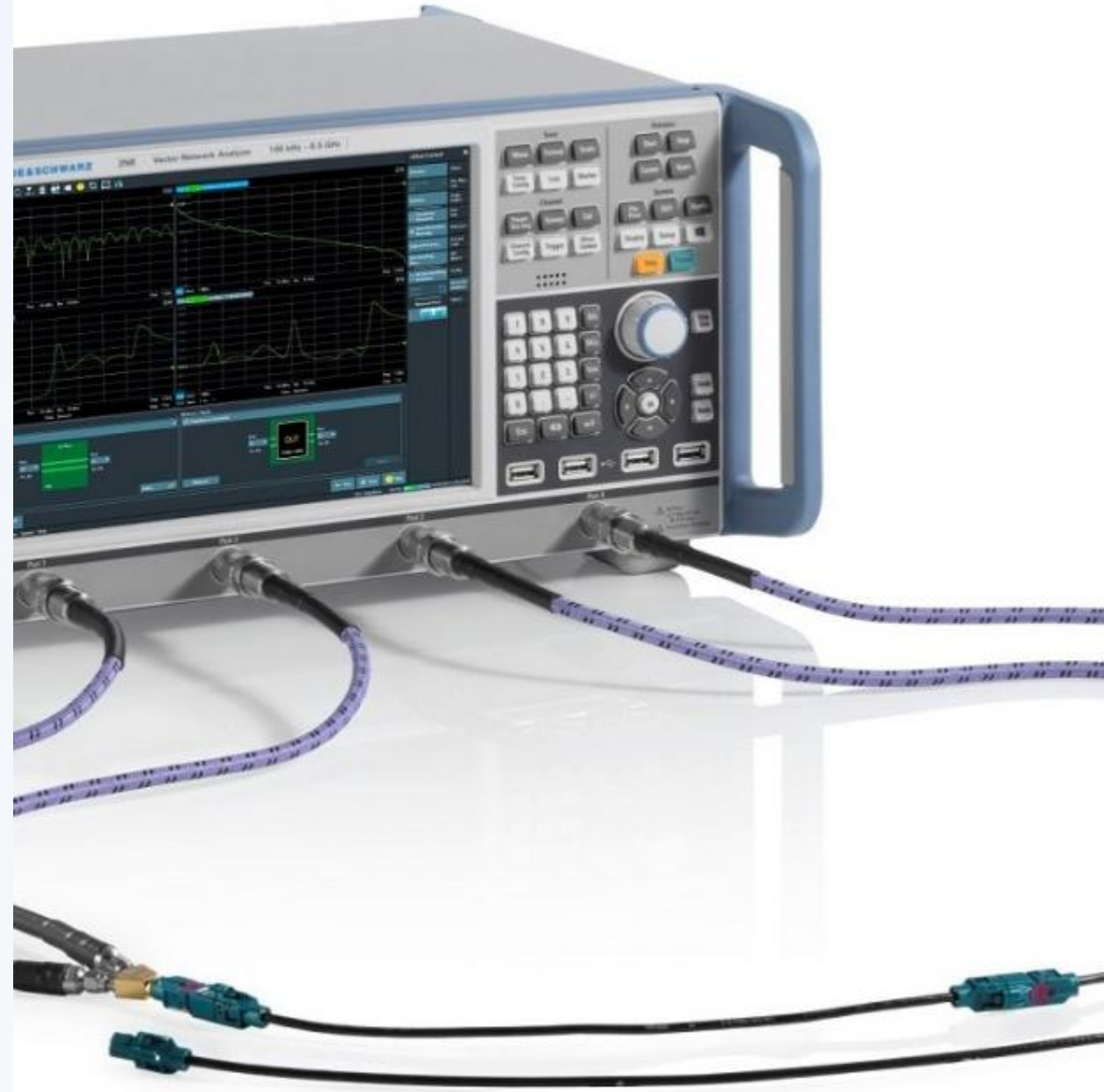
- Clock / Voltage & EM Fault Injection Glitching
- Power & Electromagnetic Side-Channel Analysis
- Secure-Boot Bypass & Cryptographic Audits
- Chip-Level Physical Reverse Engineering

Deep Hardware & ECU Testing

Physical & Fault Injection Capabilities

Sentrix operates state-of-the-art laboratory testing rigs equipped with high-bandwidth oscilloscopes, glitching equipment, and signal analysis tools.

We help tier-1 suppliers, OEMs, and chip designers identify physical vulnerabilities before product mass production and deployment.



Mission-Critical & Enterprise Security



Aerospace, Drone & Satellite

- UAV Flight Controller & Telemetry Audits
- SATCOM Link & Ground Station Security
- Airport Digital Infrastructure Assessments
- RF / GNSS Anti-Spoofing & Anti-Jamming



IoMT & Healthcare Security

- Connected Medical Device Embedded Penetration
- Wireless Telemetry & Patient Monitor Audits
- Clinical Network Isolation & Exposure Analysis
- Regulatory Health Safety & Privacy Compliance



Offensive Red Teaming

- Objective-Based Adversary Emulation
- Multi-Vector Cyber-Physical Attack Chains
- Physical Access & Social Engineering Reviews
- Purple-Team Defense Feedback & Tuning



Application & Cloud Security

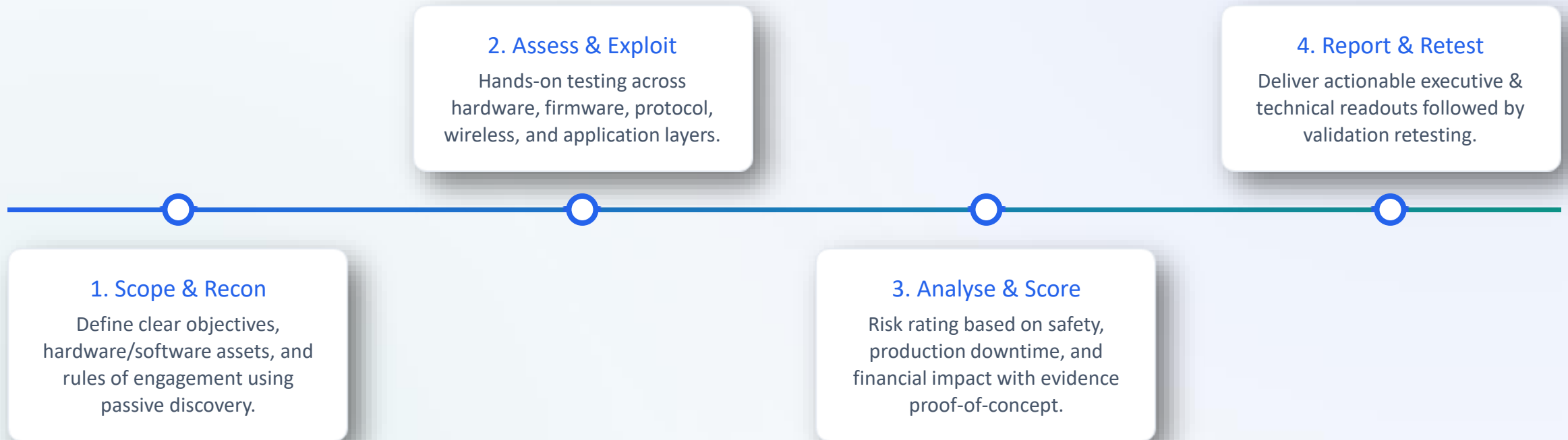
- Web, Mobile & API Security Penetration Testing
- AWS, Azure & GCP Cloud VAPT Audits
- Threat Intelligence & OSINT Reconnaissance
- Secure Code Review & CI/CD Pipeline Checks

Compliance & Governance Frameworks



Standard / Regulation	Industry Target	Compliance Scope & Assurance
ISO 21434	Automotive OEMs & Tier-1s	Road vehicle cybersecurity engineering process audits & threat modeling
UNECE R155 / R156	Global Automotive Market	CSMS (Cyber Security Management System) & SUMS (Software Updates) approval
IEC 62443 (-4-1 / -4-2)	Industrial OT & SCADA	Industrial automation product development lifecycle & technical security checks
EU Cyber Resilience Act (CRA)	Connected Hardware / Software	Mandatory digital product security lifecycle requirements for the European Union
ICSA Certification	Enterprise Hardware / Security Devices	Third-party security testing and product certification preparation

4-Step Delivery Methodology



E-LEARNING & HANDS-ON TRAINING

Sentrix Academy Catalogue

Practical-oriented training with real-world, hands-on experience using industry-standard software tools and hardware.

Sentrix Academy Training Tracks



Track 01: Offensive Hardware & Embedded

- IoT Hacking & Firmware Reverse Engineering
- Hardware Hacking & Bus Sniffing (UART/JTAG)
- Fault Injection & Voltage/Clock Glitching
- Side-Channel Power Analysis & Differential Analysis
- Physical AI Hacking & Medical Device Exploitation



Track 02: Cyber-Physical & Aerospace

- OT/SCADA & Industrial Control Systems Hacking
- Automotive & Connected Vehicle Exploitation
- Drone / UAV Telemetry & RF Hacking
- Satellite Communication & Ground Station Security
- Aviation Networks & Avionics Bus Hacking



Tracks 03 & 04: Red Teaming & Global Compliance

- **Industrial Red Teaming:** OT/ICS zone compromise simulation and adversary emulation.
- **Aviation & Airport Red Teaming:** Flight operations and airport terminal security testing.
- **IEC 62443 Standards Training:** Industrial cyber management and device certification.
- **ISO 21434 & EU CRA:** Automotive cybersecurity engineering and Cyber Resilience Act compliance.

Comprehensive Cyber Defense & Investigation Curriculum

DIGITAL FORENSICS

From Evidence to Investigation

- Evidence Identification & Preservation
- Computer, Disk & Storage Forensics
- Forensic Imaging & Data Acquisition
- Deleted Data Recovery & Data Carving
- Mobile Forensic
- Windows & Mobile Artefact Analysis
- Email & Social Media Investigations
- Incident Timeline Reconstruction
- Chain of Custody & Forensic Reporting

CYBERSECURITY

From Defense to Offensive Security

- Cybersecurity & Network Security Fundamentals
- Vulnerability Assessment & Penetration Testing
- Web & Network Security Testing
- OSINT & Information Gathering
- Red Teaming & Adversary Simulation
- Cyber Threat Intelligence
- SOC & Security Monitoring
- Incident Response & Threat Investigation

MALWARE FORENSICS

From Binary Analysis to Evasion Bypass

- Static & Dynamic Malware Analysis
- Behavioral & Network Traffic Analysis
- Memory Forensics & Volatile RAM Analysis
- Rootkit & Persistence Mechanism Detection
- Disassembly & Reverse Engineering
- Anti-Analysis & Evasion Bypass Techniques
- YARA Rule Creation & IoC Extraction
- Malware Threat Intelligence & Reporting

Why Sentrix?

01 Specialized Expertise

Focused capabilities across Digital Forensics, Cybersecurity, and Risk Intelligence.

02 End-to-End Capability

Covering the entire lifecycle: Detect, Preserve, Investigate, Report, and Remediate.

03 Evidence-Led

Built entirely around integrity, chain of custody, repeatability, and legal defensibility.

04 Technology-Driven

Leveraging industry-standard forensic, cybersecurity, and advanced analytical platforms.

05 Business-Ready

Converting highly technical findings into clear insights for leadership and legal teams.

06 Confidential Handling

Controlled access, disciplined documentation, and strictly professional handling.

We don't simply find data. We connect DATA + EVIDENCE + CONTEXT + RISK.

How We Engage

Flexible. Confidential. Evidence-led. Outcome-focused.



Advisory

Assess → Scope → Plan

Expert guidance before initiating complex investigations or establishing security programs.



Project-Based

Acquire → Analyze → Report

Defined requirements for Digital Forensics, Fraud, eDiscovery, and Due Diligence.



Retainer

Ready → Respond → Investigate

For organizations requiring recurring investigative or rapid incident-response support.



Managed Services

Monitor → Detect → Escalate

Ongoing 24/7 support for SOC, Security Monitoring, and Continuous Threat Detection.

WHEN DATA BECOMES EVIDENCE, TRUST THE EXPERTS.



 www.sentryxprivatelimited.com

 info@sentryxgroup.com

 +91 9920208333

Digital Forensics | Cyber Security | SOC | DFIR | eDiscovery | Fraud Investigation | Due Diligence |
Whistleblower | Data Recovery | Hardware, OT & Embedded Security Services

Office Address - 408, 4th floor, Shivam IT Park, Road No. 16, Wagle Estate, Thane West 400604