Castellum Labs

SERVICE DESCRIPTION

EMPOWERING LAW ENFORCEMENT

with Advanced Digital Investigation Capabilities

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

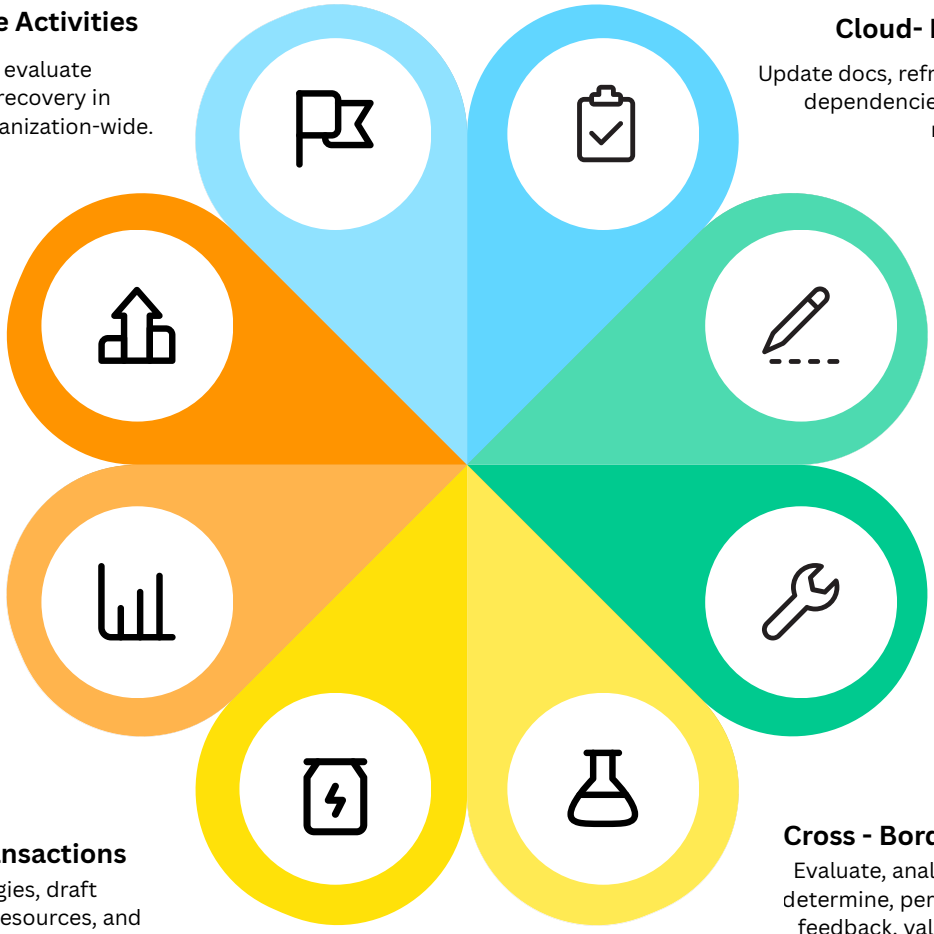
+91 7842046995

The Growing Challenge of Digital Crime

Mobile Device Evidence
Launch, secure commitment, allocate resources, and establish governance for continuity planning.

Dark Web Marketplaces
Execute exercises, simulate scenarios, validate procedures, assess readiness, and identify gaps in preparedness capabilities.

Anonymous Online Activities
Identify vulnerabilities, evaluate impacts, and prioritize recovery in business processes organization-wide.



Cloud- Based Evidence
Update docs, refresh training, review dependencies, adjust strategies, maintain alignment.

Cryptocurrency Transactions
Develop recovery strategies, draft response plans, outline resources, and document continuity framework.

Cross - Border Cybercrime
Evaluate, analyze, assess, gather, determine, performance, metrics, feedback, value, enhancements.

Fake Social Media Profiles
Deploy solutions, train teams, build infrastructure, activate partnerships, and ensure continuity planning.

Massive Volumes of Digital Evidence
Apply lessons learned, adopt innovations, implement improvements, and strengthen resilience maturity.

Castellum's Darkweb intelleligence Service

01

Digital Forensic

02

Forensic Training

03

Case Simulations

04

Data Correlation & Analysis

05

Take Down Service

06

Social Media Investigation

07

Dark Web Investigation

08

Crypto Tracking

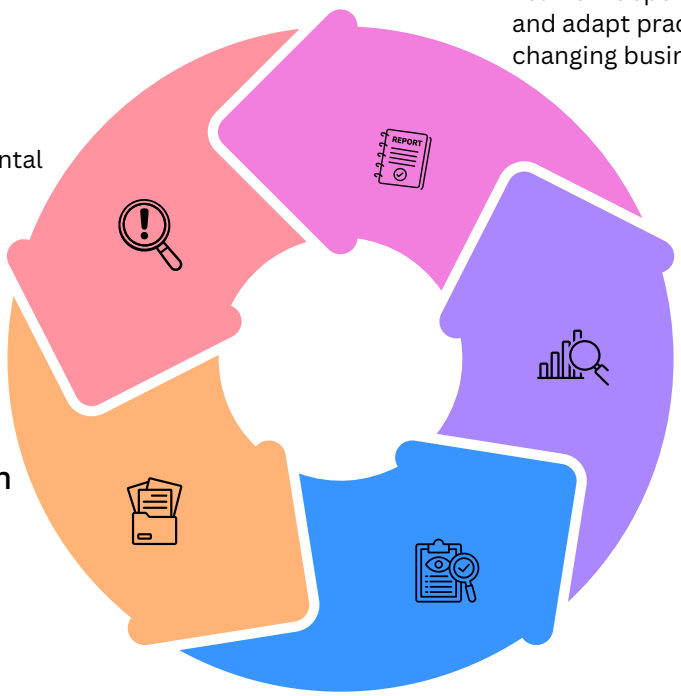
Device Forensic & Data Correlation

Reporting & Presentation

Teams independently innovate and adapt practices to meet changing business needs

Identification

Teams learn basic agile principles and begin implementing fundamental practices



Analysis

Agile mindset becomes deeply embedded in organizational culture and decisions

Collection & Preservation

Optimize workflows and establish consistent patterns for better team coordination

Examination

Incorporate sophisticated tools and techniques for enhanced development efficiency

Mobile Device Forensics

Review the candidate's resume and formulate questions based on their experience

Computer Forensics

Evaluate communication, teamwork, and adaptability throughout the conversation

Memory Analysis

Pay close attention to candidate responses and ask clarifying follow-up questions

Deleted Data Recovery

Avoid personal biases and focus only on the candidate's qualifications for the role

File System Analysis

Encourage detailed answers that reveal problem-solving skills and critical thinking

Timeline Reconstruction

Communicate the next steps and timeline to all interviewed candidates promptly

Forensic Training & Case Simulation

Prepare

Train

Respond

Case Study Simulation

STEP 01
Ransomware Investigation
Gather potential threats from internal and external sources to create an initial record for evaluation

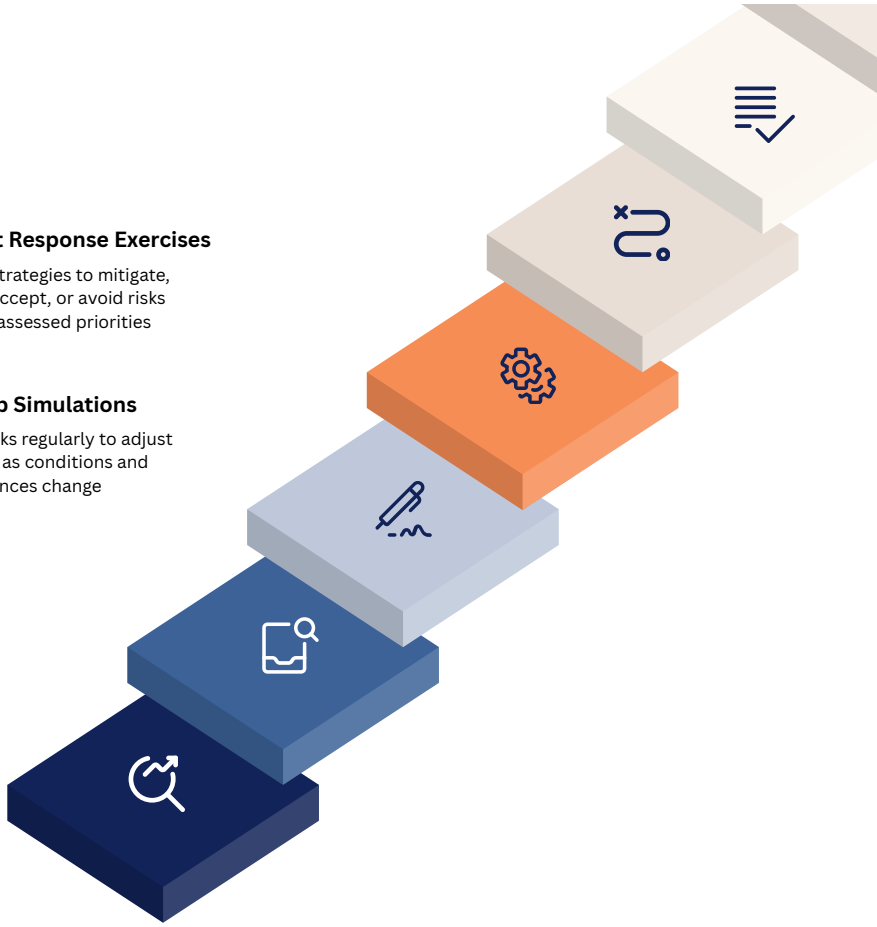
STEP 02
Financial Fraud
Analyze each risk to understand its possible effect on operations, finances, and overall goals

STEP 03
Insider Threat
Estimate the probability of each risk happening to determine its level of urgency

STEP 04
Child Exploitation Cases
Develop strategies to mitigate, transfer, accept, or avoid risks based on assessed priorities

STEP 05
Incident Response Exercises
Develop strategies to mitigate, transfer, accept, or avoid risks based on assessed priorities

STEP 06
Tabletop Simulations
Review risks regularly to adjust strategies as conditions and circumstances change



Who should attend forensic training

Employee
Analyze strengths, weaknesses, opportunities, and threats to understand overall risk position

Senario Based Training for Investigator
Simulate different conditions to explore outcomes and predict how risks may develop

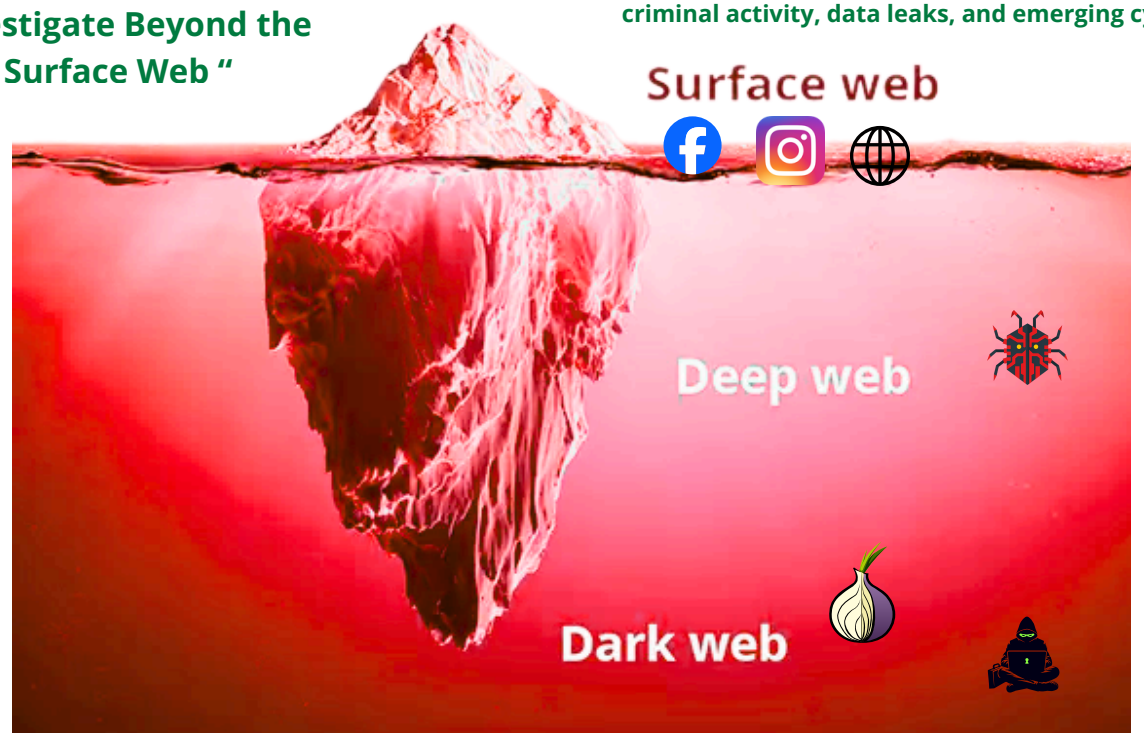
Law Inforcement Officers
Use structured lists to ensure important risks are not missed during evaluation

Forensci Professional
Identify underlying sources of problems to uncover what drives potential threats

Threat Intelligence Service

“Investigate Beyond the Surface Web “

“ Monitor underground forums & marketplace to identify criminal activity, data leaks, and emerging cyber threats



Social Media Intelligence

Open-Source Intelligence
Uses structured methods to analyze problems and reach practical conclusions.

Profile Attribution
Uses structured methods to analyze problems and reach practical conclusions.

Identity Verification
Relies on facts and metrics to confirm assumptions before acting further.

Relationship Mapping
Follows sequences carefully to avoid errors and maintain consistent workflows.

Geolocation Analysis
Reduces uncertainty by controlling steps, decisions, and measurable outputs.

Activity Monitoring
Reduces uncertainty by controlling steps, decisions, and measurable outputs.

Dark web Intellligence

Forum Intelligence
Generates many creative concepts, opening diverse possibilities for experimentation.

Marketplace Monitoring
Generates many creative concepts, opening diverse possibilities for experimentation.

Threat Actor Tracking
Imagines future outcomes and broader opportunities from early-stage ideas.

Stolen Data Monitoring
Adapts quickly to changing circumstances with creativity and fresh perspectives.

Credential Leak Detection
Embraces curiosity, testing different paths to discover innovative solutions

Underground Community Analysis
Embraces curiosity, testing different paths to discover innovative solutions.

Financial & Take Down Service

01 Track
Maintain consistent quality across all customer touchpoints.

02 Disrupt
Introduce perks or rewards to encourage return behavior.

03 Neutralize
Use custom messages that resonate with specific users.

Trace blockchain transactions to identify illicit fund movement, wallet relationships, and exchange interactions.

01
Bitcoin & Ethereum Tracking

02
Wallet Attribution

03
Transaction Tracing

04
Exchange Identification

05
Asset Flow Analysis

Blockchain Intelligence

Take Down Coverage

01 Human Capital
Evaluate team size, experience, and capability across organizational functions.

02 Technology Assets
Compare software, hardware, and digital tools supporting operational efficiency.

03 Financial Budget
Assess funds allocated for growth strategies and business development.

04 Physical Infrastructure
Review facility capacity, equipment resources, and overall operational readiness.

05 Time Management
Analyze scheduling, deadlines, and timelines ensuring efficient project completion.

06 Knowledge Assets
Evaluate proprietary expertise, intellectual property, and unique business methodologies.

About Castellum Labs

- All Services delivered from Global Security Delivery Center (GSDC)
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong handpicked team of (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995