



Threat Intelligence Services Overview

Darkweb, Takedown & Brand Monitoring

AI-powered 24x7 surveillance across dark web, surface web, social media & underground threat actor networks.

CASTELLUM LABS



8000+

Attacks / Year

\$30B+

Annual Losses

24x7

Monitoring

120+

Countries Affected



Castellum Labs
Company Profile - Overview

THE THREAT LANDSCAPE

Ransomware & Dark Web Threats in 2024-25



8,000+

Ransomware
Attacks Occurred



120+

Countries
Affected



16+

Sectors
Impacted



\$30B+

Total Financial
Loss



Almost ALL ransomware attacks have roots in the Dark Web - early detection = prevention

HOW DARK WEB ENABLES RANSOMWARE

1

Malware coded
on TOR

2

Buyer downloads
from dark web

3

Ransomware
spreads

4

Victim machines
infected

5

Ransom paid
via crypto

EXTERNAL THREAT EXPOSURE

🔗 Lookalike phishing domain by attacker

💻 Coder leaked your code & secrets on GitHub

🌐 Website using your logo for fake promo

📱 Fraudulent mobile app in your name

🛒 Your products listed on fake e-commerce

🔑 Stolen credentials on Telegram/Darkweb

Offending Assets Against You

☎️ Fake contact number on Google search

🌐 Data sold on Dark Web marketplace

90% of attacks stopped early

Watch **OUT**

Darkweb Intelligence
At the Core of Your Defence

Advanced Threat Intel Technology

AI-powered analytics, proprietary tooling, and real-time feeds to detect and track emerging threats before they impact you.

Research-Based Intel Curation

Expert analysts curate, validate, and enrich global intelligence to deliver contextual, actionable insights you can trust.

SERVICE MODULES



Darkweb Intelligence 24x7

Real-time dark web surveillance and threat hunting across underground forums, breach sites & Telegram



Brand Monitoring Service

Continuous monitoring for impersonation, fake apps, fraudulent listings & social media abuse



Attack Surface Management

Discover and monitor your exposed digital attack surface across web, cloud, DNS & network



Take Down On-Demand

Rapid identification and takedown of phishing domains, fake profiles, counterfeit listings & IP abuse

watchOUT DARKWEB INTELLIGENCE 24x7



Phish Hunt

Phishing domains, lookalike infra & malicious hosting



Cred Hunt

Leaked employee credentials & compromised accounts



Stealer Log Hunt

Malware stealer logs tied to org domains & emails



Git Hunt

Exposed repos, hardcoded secrets, API keys & dev artifacts



Fake Hunt

Fake social media entities & brand impersonation



Leak Hunt

Exposed docs, database leaks & unauthorized data exposure



Rep Hunt

Underground mentions, malicious discussions & reputational threats

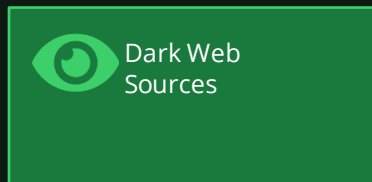


Dark Hunt

Breach forums, ransomware leak sites & cybercrime marketplaces

HOW watchOUT WORKS

SIGNAL COLLECTION



- ✓ Real-time Monitoring
- ✓ Intelligent Filtering
- ✓ Contextual Analysis
- ✓ Unified Dashboard

watchOUT PLATFORM

phishWATCH

credWATCH

leakWATCH

gitWATCH

darkWATCH

fakeWATCH

repWATCH

ANALYSIS & CURATION

Base Curation

Advanced
Correlation

Darkweb
Correlation

Expert
Analyst Team

SUPER-CURATED INTEL OUTPUT

Intel Report

Intel Bundle

STIX/TAXII

Web Dashboard

YARA Rules

BRAND MONITORING SERVICE

PROTECT YOUR IP

Unauthorized use of logos and trademarks

Damaging comments/posts on social media

Fake webpages, social accounts and domains

Campaign against your brand/company

STOP REVENUE LOSS

Unauthorized product listing on e-commerce

Product imitations being sold online

Malicious mobile apps in your company name

Fake contact numbers driving customers away



Protect Your
Intellectual Property

castellumlabs.com



Defend Your
Brand 24x7



Save Revenue
Leakage

Copyright@2026

ATTACK SURFACE MONITORING

THE CHALLENGE

1000s

of vulnerabilities at any time in a mid-to-large org

Many

of these exist on the public internet & dark web

"Lack of Visibility"

is the core problem — you can't fix what you can't see

WHAT WE MONITOR



Web Attack Surface

Misconfigured endpoints, vulnerable components, exploitable vulnerabilities



Network Attack Surface

Protocol vulnerabilities, cryptographic failures, penetration risks



Cloud Attack Surface

Exposed cloud services, bucket exposure, DB & server exposure



DNS/Mail Surface

Mail security configs, DMARC validations, policy state verification



Get Surface Report with Insights → Prioritize Gap & Vulnerability → Take Action & Secure Surface

TAKE DOWN ON-DEMAND SERVICES

Fake Products & Listings

Counterfeit goods & unauthorized brand use in marketplaces

Domain & Web Impersonation

Phishing domains & lookalike websites targeting your customers

Social Media Negative Campaigns

Fraudulent profiles, fake accounts & coordinated brand attacks

 Leaving these threats unaddressed INVITES FRAUD and causes irreversible brand damage

CASTELLUM LABS TAKE DOWN COVERAGE

Web & Domain Abuse

Social Media Abuse

Malicious Content Hosting

Copyright & IP Abuse

Fake Apps & Contact Channels

Counterfeit Products

Reputation Abuse

ABOUT CASTELLUM LABS



Global Delivery

All services delivered from our Global Security Delivery Center (GSDC) in Hyderabad, India



Seasoned Team

Handpicked team of the best security talent globally with decades of product & deep tech experience



Instant Value

Value + Impact from Day One. No installation, no deployment — subscription & annual contracts



Global Reach

Active customer base across India, US, Europe in Retail, Banking, FMCG, IT & Construction sectors

100s of Satisfied Customers Across the Globe

- Retail (Clothing, Sportswear)
- Construction (Cement)

- Retail (Footwear)
- IT Consulting

- Financial Services (Banking)
- Asset Management

- Investment Management
- Consumer Goods



Castellum Labs

Threat Intelligence Platform

- Darkweb Intelligence 24x7
- Brand Monitoring
- Attack Surface Mgmt
- Take Down Services

by **Castellum Labs**

GET STARTED TODAY

INQUIRE NOW

REQUEST DEMO



www.castellumlabs.com



reach@castellumlabs.com



+91 7842046995

#417, 4th Floor, DHLF VC Jayabheri Silicon Towers,
Hitech City Rd, Kondapur, Hyderabad – 500084