

# THREAT INTELLIGENCE

Darkweb, Brand Monitoring & Takedowns



[www.castellumlabs.com](http://www.castellumlabs.com)



Castellum Labs



[reach@castellumlabs.com](mailto:reach@castellumlabs.com)



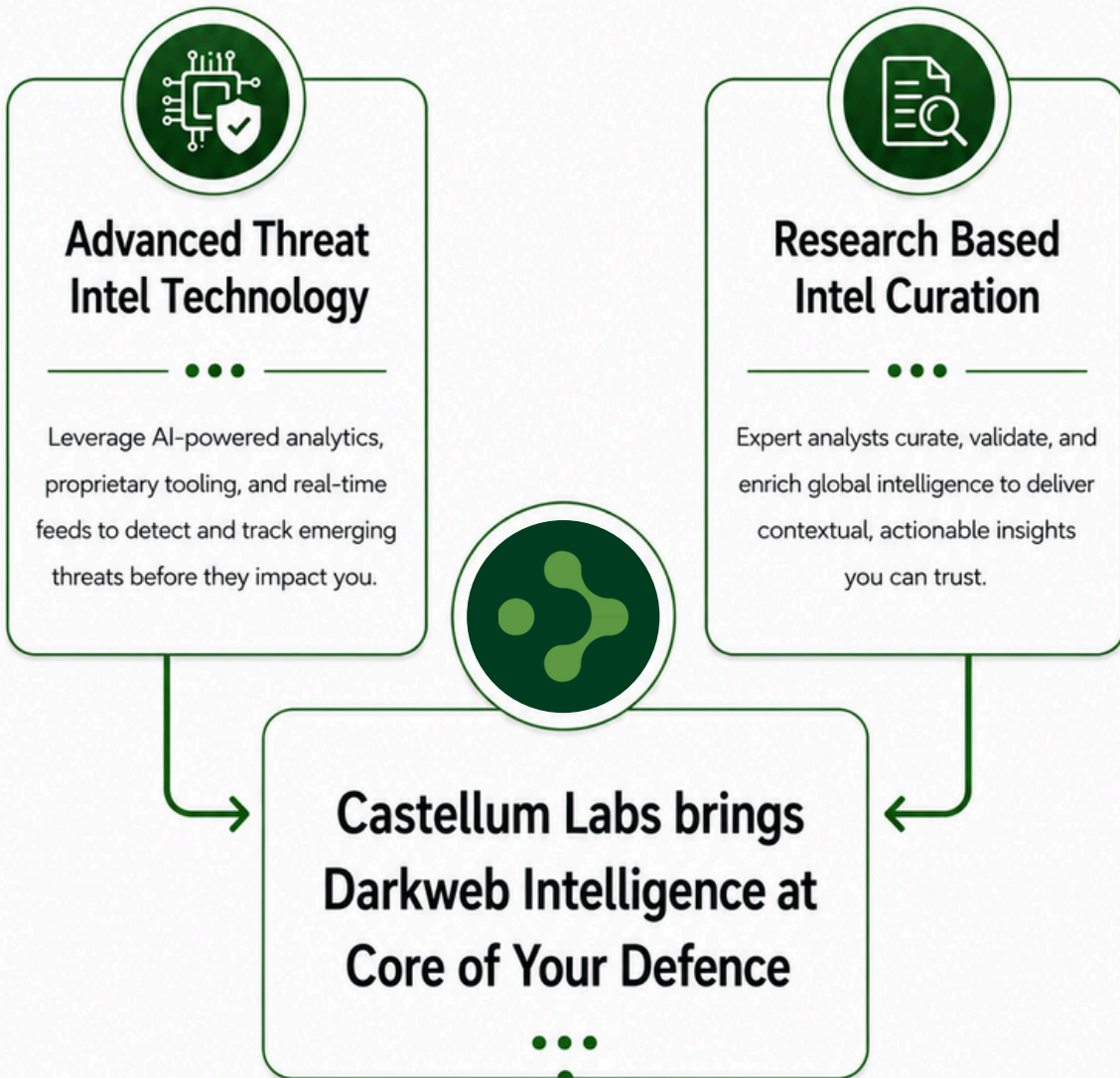
+91 7842046995



# External Threat Exposure



# Castellum's Darkweb intelligence Service



**Darkweb Intelligence 24 x 7**

**Brand Monitoring Service**

**Attack Surface Management**

**Take Down Service**

# Darkweb Intelligence 24x7, The Coverage

Monitoring for leaked employee credentials, compromised email accounts, and credential marketplace activity.



Identification of phishing domains, suspicious lookalike infrastructure, and malicious hosting environment targeting the organization

Detection of stealer malware logs associated, with organizational domains, employee emails, usernames, and related identifiers.

Identification of exposed repositories, hardcoded secrets leaked credentials, configuration files, API keys, and sensitive development artifacts.

Detection of fake social media entities, impersonation accounts, fraudulent applications, and malicious brand impersonation activity.

Monitoring for exposed documents, confidential files, database leaks, internal information, and unauthorized data exposures.

Monitoring external references, underground mentions, malicious discussions, and reputational threats associated with the organization.

Continuous monitoring across underground communities, breach forums, ransomware leak sites, threat actor channels, and cybercrime marketplaces.

# Brand Monitoring Service, The Coverage



## 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



Malicious mobile apps in your company name

Fake contact number driving customers away



# Attack Surface Monitoring, The Coverage



## Web Attack Surface

- Misconfig on external endpoints
- Vulnerable web components
- Penetrable vulnerabilities on surface

- Protocol vulnerabilities
- Cryptographical failures
- Penetration vulnerabilities



## Network Attack Surface



## Surface Asset Graph

- Web endpoints map
- Port and protocol map
- Cloud geo location map

- Exposed cloud services
- Buckets exposure
- DBs, servers exposure



## Cloud Attack Surface



## DNS/Mail Attack Surface

- Mail security configurations
- DMARC validations
- Policy state verification

# Take Down Services, The Coverage



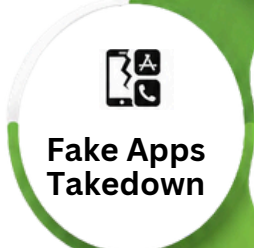
Identification & escalation of phishing domains, impersonations websites, & unauthorized web infrastructure abusing organizational identity.

Detection & takedown coordination for fake social media profiles, fraudulent brand representation, and malicious social presence.



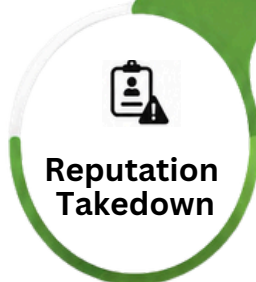
Identification of malicious hosting infrastructure, phishing kits, malicious files, and harmful content abusing organizational asset or branding.

Monitoring & escalation for unauthorized usage of copyrighted material, trademark, and intellectual property abuse across public platforms.



Detection & escalation of counterfeit applications, malicious APKs, and unauthorized customer support impersonation.

Monitoring & escalation for trademark, branding assets, proprietary content, and reality abuse across public platforms



Identification of fake product listing, unauthorized sellers, marketplace abuse tagerting organization product or service

## About Castellum Labs

Based in Hyderabad, India with global customer base across India, US, Europe

Started by people with decades of product, services & deep tech experience

Value + Impact from Day One, No Installation & No Deployment

All Services delivered from Global Security Delivery Center (GSDC)

Strong handpicked team of (best of security talent globally)

Subscription & annual contract modeled services delivered globally



## 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](http://www.castellumlabs.com)



Castellum Labs



[reach@castellumlabs.com](mailto:reach@castellumlabs.com)



+91 7842046995