

THREAT INTELLIGENCE

Darkweb, Takedown and Brand Monitoring



www.castellumlabs.com



Castellum Labs



reach@castellumlabs.com




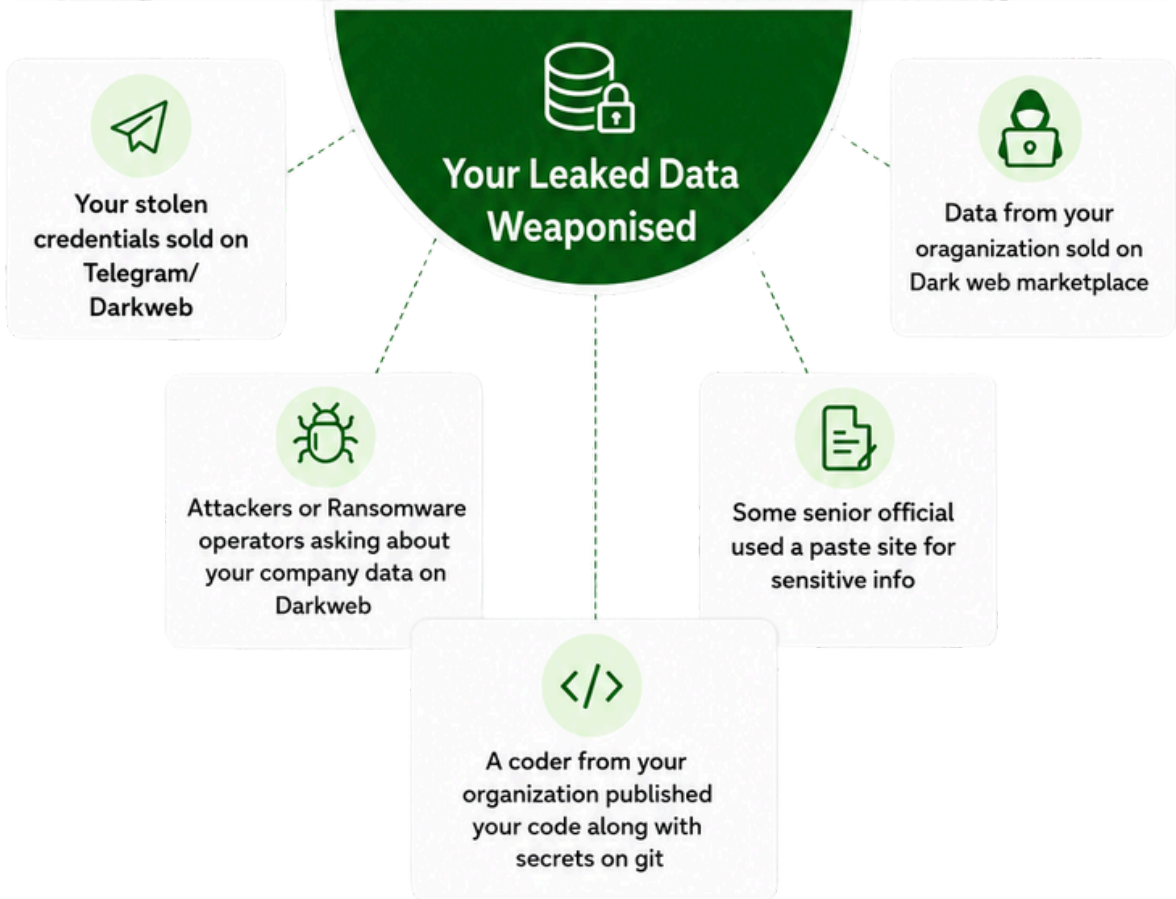
+91 7842046995



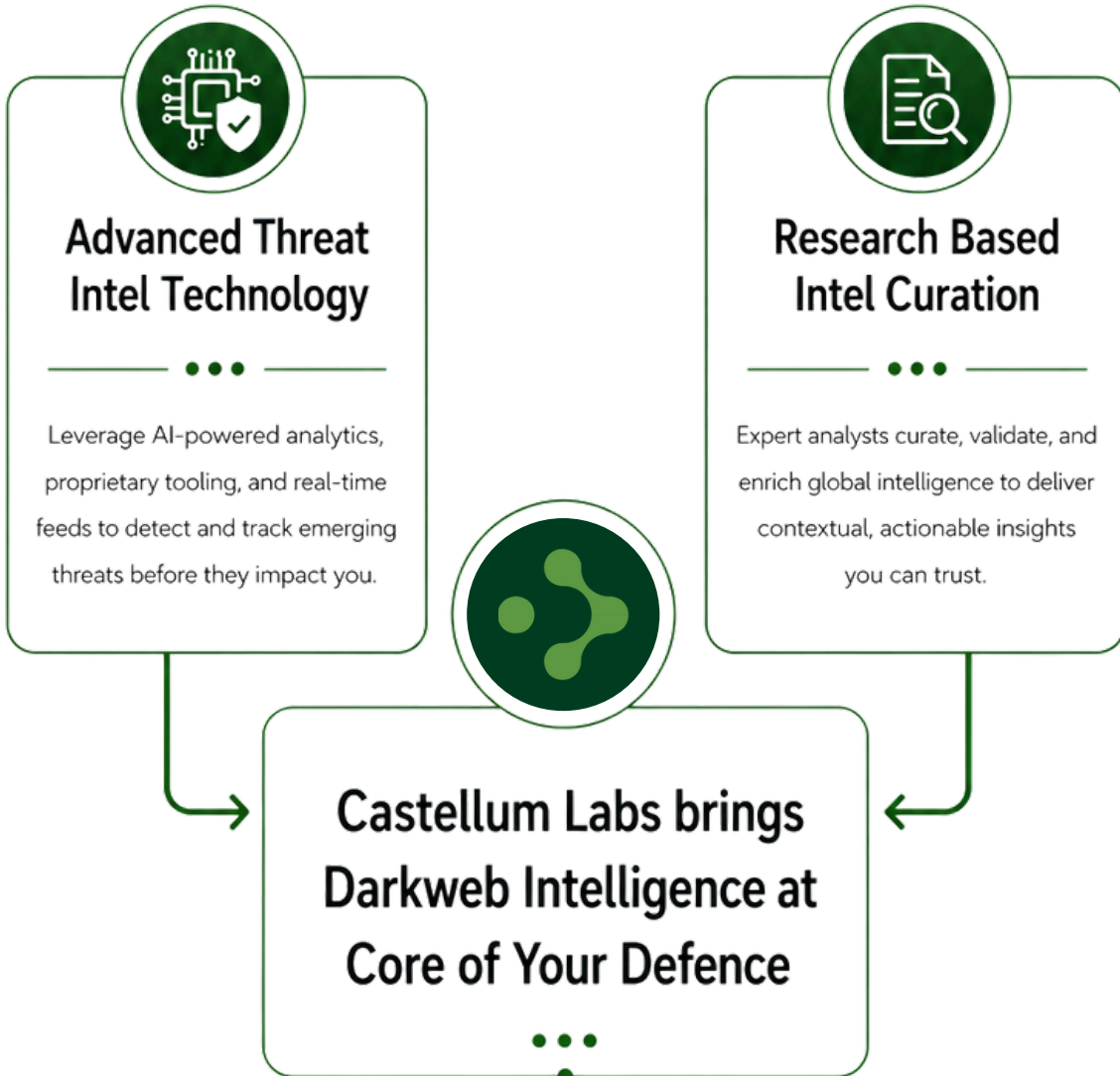
External Threat Exposure



 **A Timely Visibility into this could have stopped 90% of all attack**



Castellum's Darkweb intelligence Service



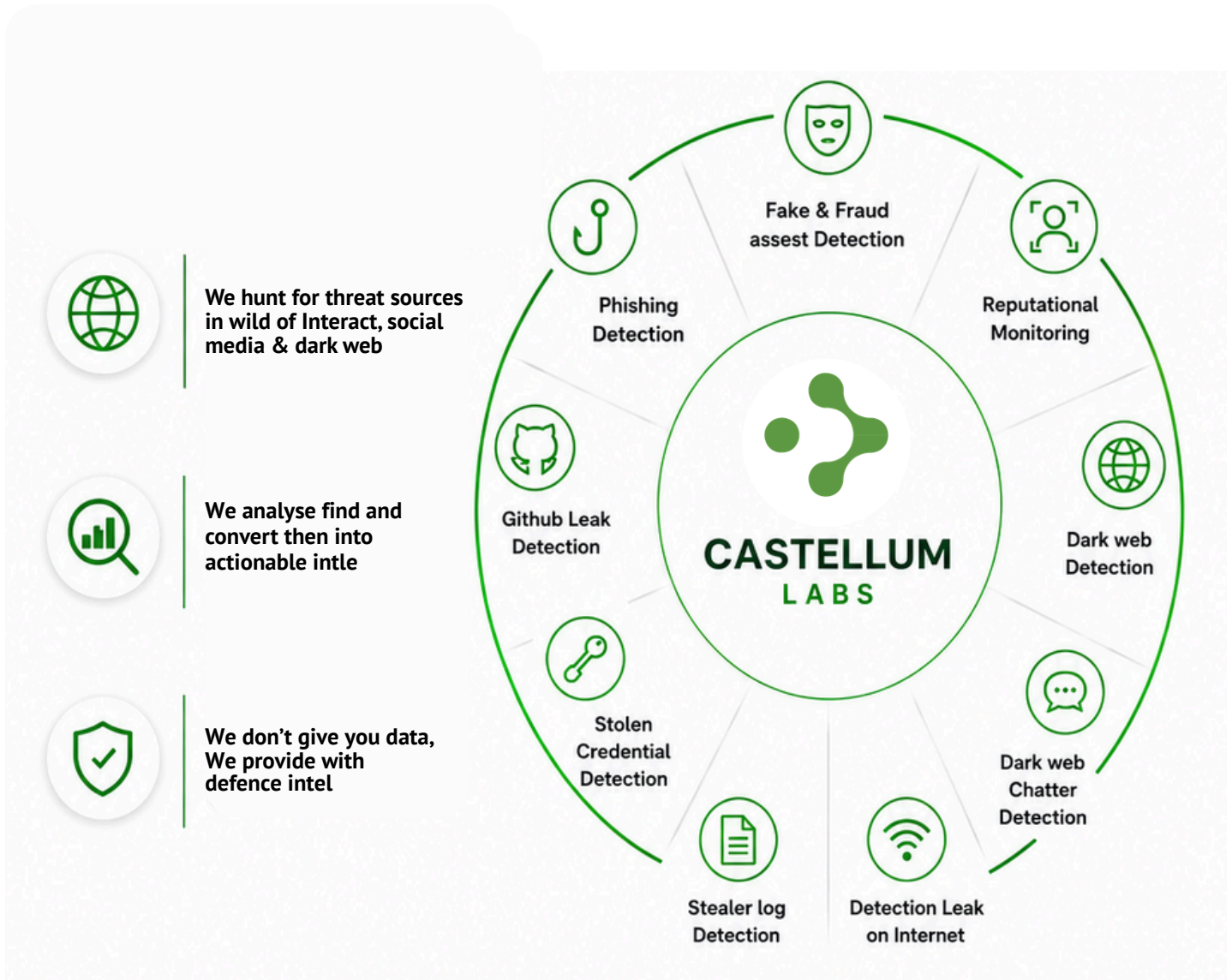
Darkweb Intelligence 24 x 7

Brand Monitoring Service

Attack Surface Management

Take Down Service

Introducing, Darkweb Intelligence 24X7



Use Direct Intel for Real Protection



Block the phishing domain from reaching customer employee



Take action and change password before your app falls to credentials stuffing



Bring down the repositories in leaking secrets & IP

Darkweb Intelligence 24x7, The Coverage


Phish Hunt

Identification of phishing domains, suspicious look a like infrastructure, and malicious hosting environment targeting the organization


Cred Hunt

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


Stealer log Hunt

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


Git Hunt

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


Fake Hunt


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


Leak Hunt

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


Rep Hunt

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


Dark Hunt

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

Darkweb Intelligence 24x7, Intel Data Samples

External Threat Monitoring Report

Comprehensive intelligence across 7 threat domains — Credential Exposure, Phishing Infrastructure, Reputation, Git Leaks, Document Leaks, Fake Profiles, and Stealer Logs. Analysis period: Sep 2024 – Mar 2025.

7	472	551	243
MODULES	PHISH DOMAINS	CREC RECORDS	STEALER LOGS

Overall Threat Risk Score: 72 (HIGH RISK)

Active threats identified across credential, phishing and stealer log modules:

- Phishing: 92
- Credentials: 88
- Stealer Logs: 68
- Reputation: 55
- Git Leaks: 48
- Doc Leaks: 22
- Fake Profiles: 15

Threat Module Overview — All Domains

- 11 CRITICAL
- 40 HIGH
- 138 MEDIUM
- 865 LOW / INFO

Stealer Logs: 243 records, 57 corporate emails, 6 confirmed logins (HIGH)

PhishHunt: 472 suspect domains, 49 blacklisted, 262 MX-enabled (CRITICAL)

CredHunt: 551 records, 152 unique emails, 208 high-privilege (HIGH)

Rephunt: 6 reputation findings, 3 high severity, vuln*****.com (MEDIUM)

GitHunt: 30 findings, 4 critical/high, 14 sensitive data exposures (HIGH)

LeakHunt: 2 leaks, PDF documents, Scribd platform, PII exposure (MEDIUM)

External Threat Monitoring Report

CRITICAL: 29 domains flagged as Critical severity with dual blacklisting (domain + IP). 262 MX-enabled domains indicate active readiness for phishing email campaigns. Two IPs — 13.248.169.48 and 76.223.54.146 — each host 97 domains, suggesting coordinated parking-stack infrastructure. Immediate firewall and DNS blocking recommended across all 472 suspect domains.

TOTAL SUSPECTS	UNIQUE IP ADDRESSES	BLACKLISTED DOMAINS	BLACKLISTED IPS	MX-ENABLED DOMAINS
472	258	49	76	262
Phishing domains identified	Resolved infrastructure	Confirmed on threat feeds	IP-level threat confirmation	Email-ready for phishing

WHITELISTED DOMAINS	WHITELISTED IPS	ACTIVE WEBSITES	LOGIN PAGES FOUND	CRITICAL ALERTS
423	182	45	10	29
Not yet blacklisted	IP — not confirmed malicious	Domains serving content	Active credential-harvest risk	Highest threat priority

Attack Variant Distribution (18 PATTERN TYPES)

- Replacement: 91
- BitSquatting: 68
- Homoglyph: 60
- Omission: 50
- Subdomain: 50

Geographic Hosting Distribution (15+ COUNTRIES)

- United States: 198
- Germany: 41
- Russia: 25
- Netherlands: 19
- Australia: 13

Phishing Detection Report

OBSERVATION: 2 Facebook accounts referencing *****.com were identified during Fake Hunt monitoring. Both accounts show No posts, are marked Inactive, and are currently assessed as Low severity. Continued monitoring is recommended to detect future impersonation, brand misuse, or activity changes.

TOTAL RECORDS	SOCIAL SURFACE	INACTIVE ACCOUNTS	NO POST ACTIVITY	LOW SEVERITY
2	1	2	2	2
Fake hunt entries	Facebook platform	No active posting	Last post: No posts	No immediate risk

Social Surface Distribution (2 RECORDS)

- Facebook: 2

Account Status

- Inactive: 2

Identified Account Owners (2 ACCOUNTS)

- *****.com, Inc: 1
- Lease 4 Ease supporting to *****.com software co: 1

Severity Distribution

- Low Severity: 2 records (Inactive accounts with no posts)

Account Creation Timeline

- 2012: 1
- 2014: 1

Post Activity Findings

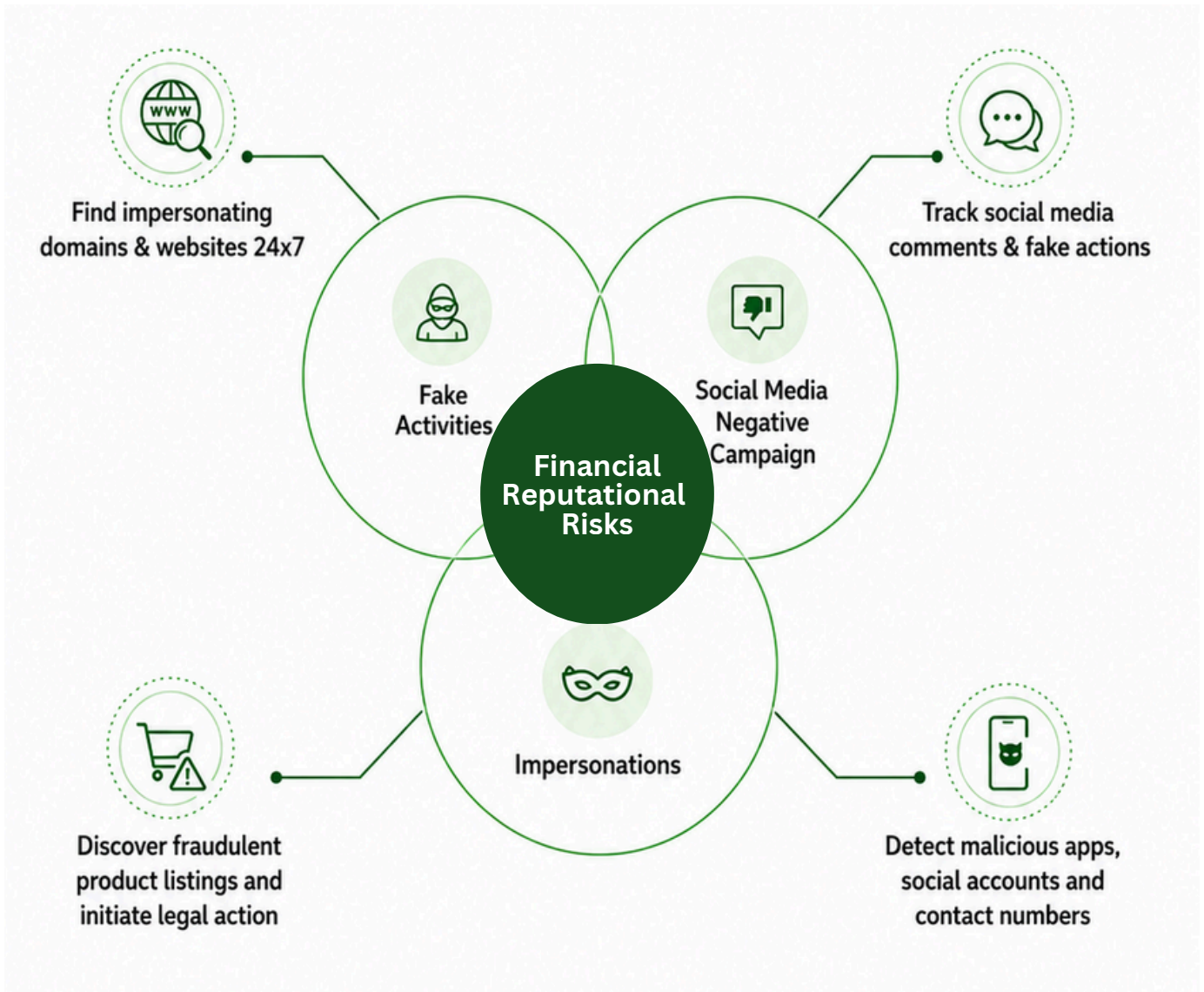
- No posts: 2
- Inactive: 2

Fake Hunt Record Breakdown

- Facebook: 2
- Inactive: 2
- Low severity: 2

Fraudulent assets Monitoring Report

Introducing, Brand Monitoring Service



Protect your Intellectual Property

Defend your Brand

Save Revenue Leakage

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



Brand Monitoring, How it is done



External Attack Surface, Challenges



Exposed EC2 ,
Critical Vul on
public web



VPN public ip
with misconfig



FTP with
anonymous login

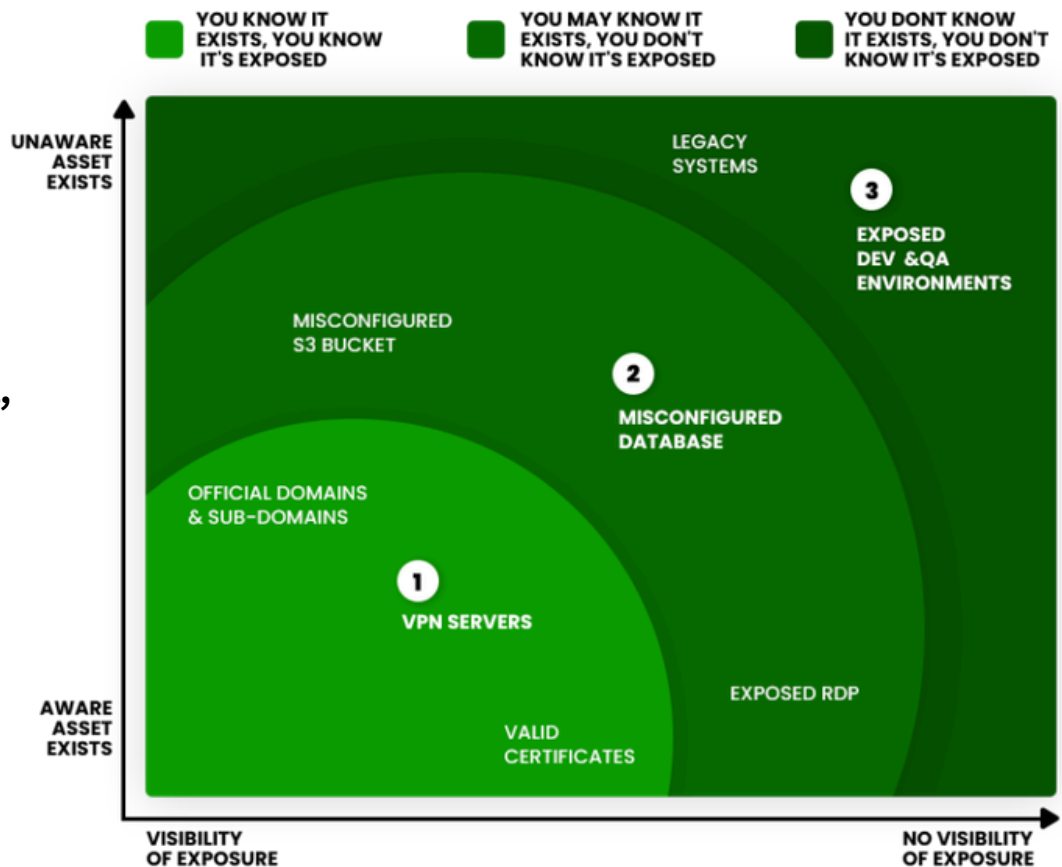


Vulnerability on
External Web Surface

At any time mid to large
org they carry **1000's** of
vulnerabilities & gap
highlight number.

Many of these are on
Public Domain

“Lack of
Visibility”



Introducing, Attack Surface Monitoring



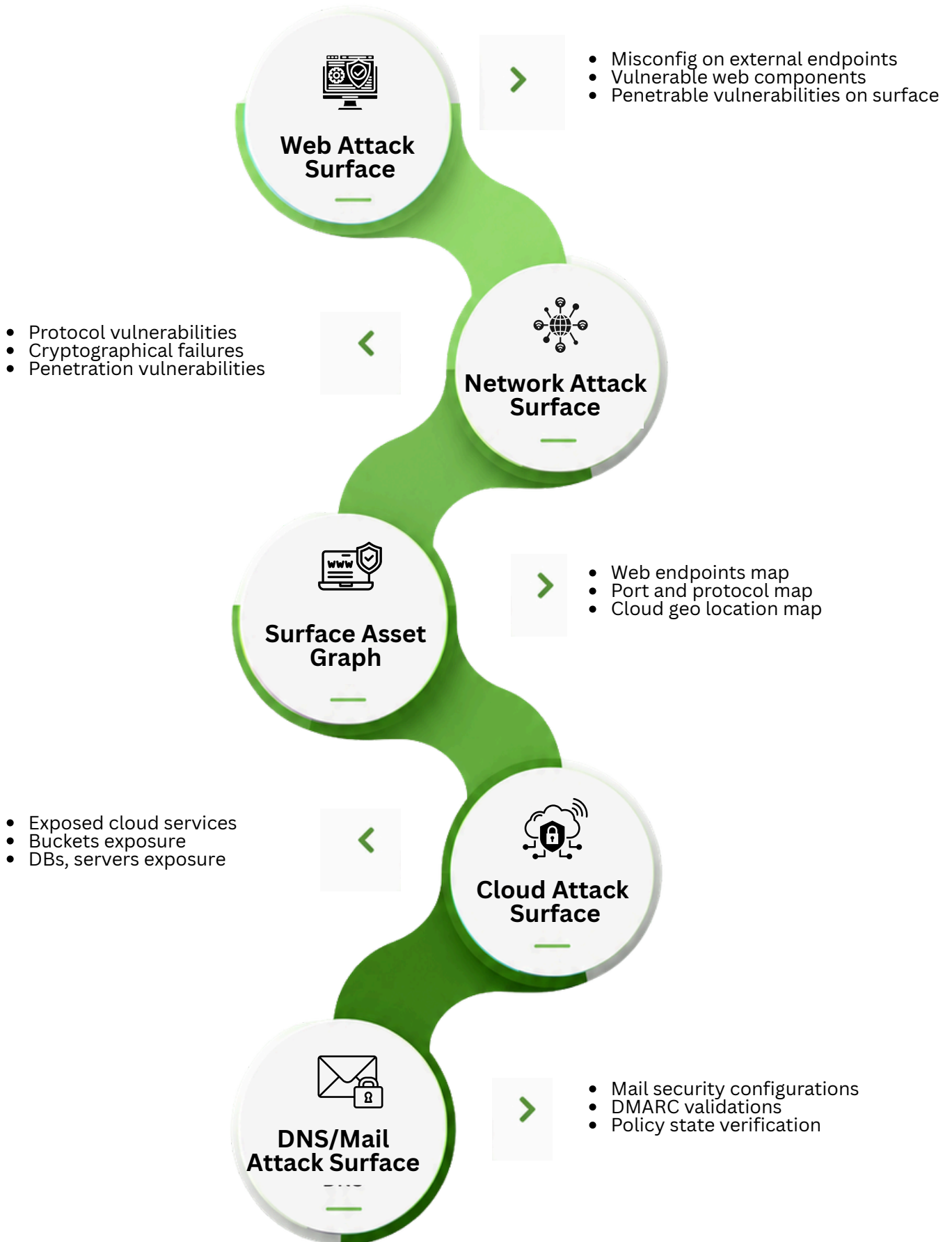
Castellum Attack Surface Mapping and Monitoring

Type of Vulnerabilities	Endpoints and IP Points																	
	Web endpoint URLs					Public IP address					Domains							
	https://app.example.com	https://api.example.com	https://portal.example.com	https://admin.example.com	https://login.example.com	...	203.0.113.10	203.0.113.20	198.51.100.5	192.0.2.25	203.0.113.30	...	example.com	api.example.com	portal.example.com	cdn.example.com	mail.example.com	...
Header Misconfigurations	Secure	Secure	Exposure / Misconfig	Secure	Secure	...	Exposure / Misconfig	Secure	Secure	Secure	Secure	...	Exposure / Misconfig	Secure	Secure	Secure	Secure	...
Vulnerable Technologies	Exposure / Misconfig	Secure	Exposure / Misconfig	Secure	Secure	...	Secure	Exposure / Misconfig	Secure	Secure	Secure	...	Exposure / Misconfig	Exposure / Misconfig	Secure	Exposure / Misconfig	Secure	Secure
Brute Force Susceptible	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	...	Exposure / Misconfig	Exposure / Misconfig	Secure	Exposure / Misconfig	Secure	...	Exposure / Misconfig	Secure	Exposure / Misconfig	Secure	Exposure / Misconfig	Exposure / Misconfig
Credential Stuffing Risk	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Secure	Secure	...	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Secure	...	Exposure / Misconfig	Secure	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig
Default Password Exposure	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Secure	Secure	...	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Secure	...	Exposure / Misconfig	Secure	Secure	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig
Cryptographic Failure	Secure	Secure	Exposure / Misconfig	Secure	Secure	...	Secure	Exposure / Misconfig	Secure	Secure	Secure	...	Secure	Exposure / Misconfig	Secure	Secure	Secure	Exposure / Misconfig
Vulnerable Protocol	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	...	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	...	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig
Spoofing Exposure	Exposure / Misconfig	Secure	Exposure / Misconfig	Exposure / Misconfig	Secure	...	Exposure / Misconfig	Secure	Exposure / Misconfig	Exposure / Misconfig	Secure	...	Exposure / Misconfig	Secure	Exposure / Misconfig	Exposure / Misconfig	Exposure / Misconfig	Secure

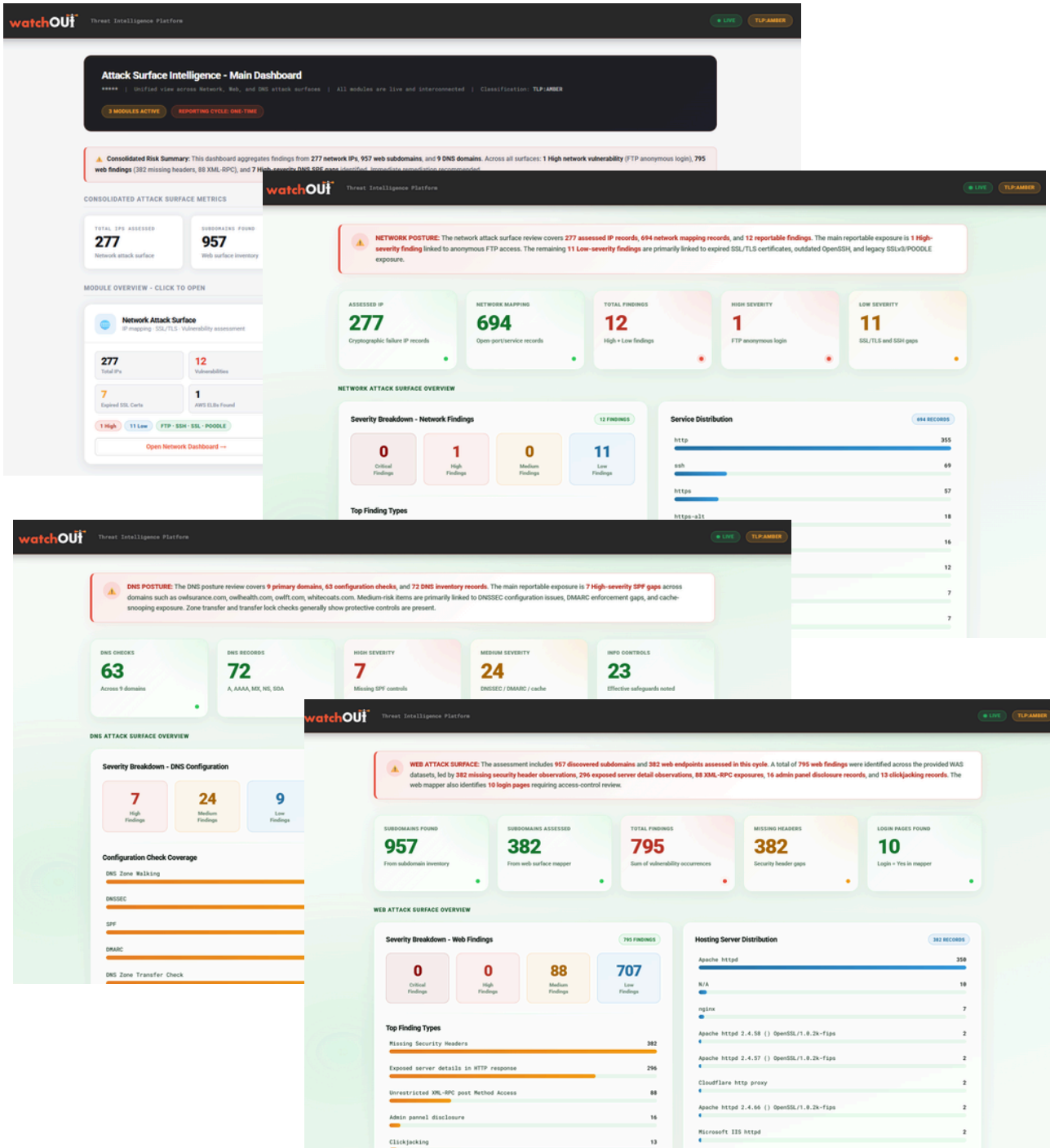
■ Secure
No known risk
 ■ Not Applicable
Not relevant / Not assessed
 ■ Exposure / Vuln / Misconfig
Risk identified

✔ Risk Formula:
 $Risk = F(Vulnerabilities \times Exposure \times Active Threats \times Mitigating Controls \times Business Impact)$

Attack Surface Monitoring, The Coverage



Attack Surface Monitoring, Data Samples



Get Surface Report with Insights



Prioritize Gap & Vulnerability

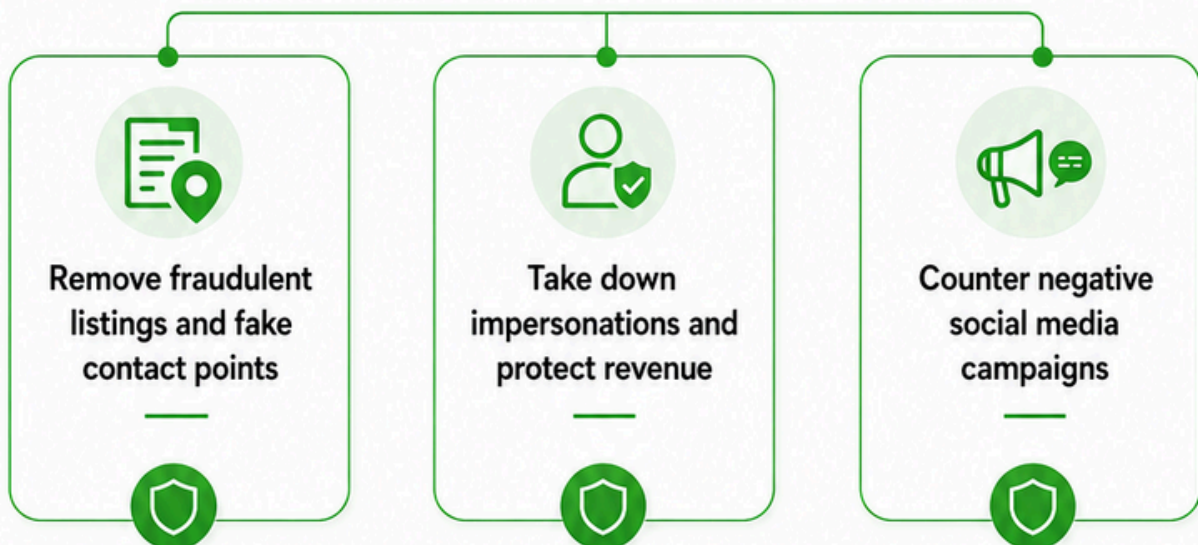


Take Action & Secure Surface

Introducing, Take Down Services



Castellum Labs Take Down Can Help



Take Down Services, The Coverage



Web & Domain Abuse Takedown

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.



Social Media Abuse Takedown



Malicious Content Hosting Takedown

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.



Copyright & IP Abuse Take Down



Fake Apps & Contact Channel Takedown

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.



Counterfeit Product & Abuse Takedown



Reputation Abuse Takedown

Identification of fake product listing, unauthorized sellers, marketplace abuse targeting 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



Castellum Labs



reach@castellumlabs.com



+91 7842046995