Castellum Labs

Powered by
watchOUT

EXTERNAL SURFACE ATTACK MANAGEMENT

Castellum's EASM

Comprehensive Discovery, Analysis & Monitoring
of Your External Attack Surface

- Web Assets
- Network Assets
- DNS Infrastructure
- Cloud Exposure

Know Your Threats Before They Know You • Continuous Visibility • Analyst-Validated Findings

Castellum Labs

Understanding the External Attack Surface

All internet-facing assets visible and targetable by threat actors

The External Attack Surface includes ALL internet-facing digital assets that can be discovered, profiled, and exploited by adversaries without internal access.

Public Websites

Web Applications

Public IPs & Ports

Domains & Subdomains

DNS Infrastructure

Cloud Storage

Third-Party Assets

Shadow IT

Castellum Labs

ESAM Methodology

Hybrid Assessment - Automated Discovery + Expert Analyst Validation

Web Surface

Apps · APIs · Security Headers · Config Review

Network Surface

IPs · Open Ports · Protocols · TLS Validation

DNS Surface

Domains · Subdomains · SPF · DMARC · DNSSEC

Cloud Surface

Cloud Resources · Storage · Config · Exposure

Automated Discovery — Continuous identification · Large-scale enumeration · Asset mapping · Tech fingerprinting

Analyst Validation — Manual verification · False positive removal · Context analysis · Risk prioritization

Castellum Labs

Web Surface Coverage - webWATCH

Comprehensive Web Security Assessment & Exposure Analysis

Asset Discovery

- Public Websites
- Web Applications
- Admin Interfaces
- Public APIs

Identify all public-facing web properties including forgotten, shadow, and third-party hosted assets.

Security Validation

- Misconfigurations
- Auth Weaknesses
- Exposure Validation
- Header Analysis

Validate security controls, detect authentication flaws, and identify dangerous misconfigurations.

Technology Intelligence

- Tech Stack ID
- Framework Detection
- Server Fingerprinting
- Library Audit

Fingerprint technologies, identify outdated components, and map the full software supply chain.

Exposure Assessment

- Attack Vectors
- Security Gaps
- App Security Review
- Risk Prioritization

Map exploitable attack vectors, score risk by severity, and prioritise remediation actions.

DELIVERABLES: Web Exposure Summary • Security Findings Report • Risk Categorization • Remediation Recommendations

Castellum Labs

Network Surface Coverage - netWATCH

External Network Exposure Assessment

Asset Discovery

- Public IP Identification
- Open Service Enumeration
- Service Fingerprinting
- Infrastructure Mapping

Protocol Analysis

- Protocol Assessment
- Service Version Validation
- Exposure Identification
- Security Baseline Review

Vulnerability Correlation

- Known CVE Mapping
- Tech Exposure Analysis
- Risk Classification
- Attack Path Identification

DELIVERABLES: Network Exposure Inventory • Open Service Summary • Risk Overview • Remediation Guidance

Castellum Labs

DNS & Cloud Surface Coverage

dnsWATCH + cloudWATCH

DNS Surface (dnsWATCH)

DNS Visibility

- Domain Discovery
- Subdomain Enumeration
- DNS Infrastructure Mapping
- External DNS Exposure

DNS Security Validation

- Security Config Review
- Reputation Assessment
- DNSSEC Controls Validation
- Exposure Analysis

Cloud Surface (cloudWATCH)

Cloud Asset Discovery

- Public Cloud Resource Enum
- Storage Exposure ID
- Cloud Service Visibility
- Resource Mapping

Cloud Security Validation

- Public Accessibility Review
- Storage Config Assessment
- Sensitive Data Exposure
- Security Control Validation

DELIVERABLES: Cloud Exposure Summary • Misconfiguration Findings • Sensitive Asset Identification • Remediation Recommendations

Castellum Labs

Centralized Dashboard & Reporting

All ESAM Findings Consolidated in One Unified View

Visibility

- Asset Inventory
- Exposure Tracking
- Coverage Status
- Asset Classification

Risk Management

- Severity Classification
- Risk Prioritization
- Trend Monitoring
- Exposure Tracking

Actionable Outputs

- Finding Details
- Technical Evidence
- Validation Results
- Remediation Guidance

Executive Reporting

- Attack Surface Summary
- Risk Overview
- Coverage Metrics
- Security Posture Insights

Dashboard • Severity Distribution Charts • Findings Table • Risk Overview • Coverage Metrics • Exportable Reports

Castellum Labs

Why ESAM?

The Strategic Case for External Attack Surface Management

Continuous Monitoring

Always-on asset discovery ensures new exposures are found as they emerge — not months later during an incident.

Proactive Risk Reduction

Identify and close attack vectors before adversaries exploit them. Shrink your exposure window dramatically.

Analyst-Validated

Automated tools surface candidates; expert analysts validate and prioritise — eliminating false-positive fatigue.

Holistic Coverage

Web, Network, DNS, and Cloud surfaces under one unified program with centralised, consistent reporting.

Threat-Informed

Findings mapped to real-world adversary techniques and attack playbooks for context-driven, prioritised remediation.

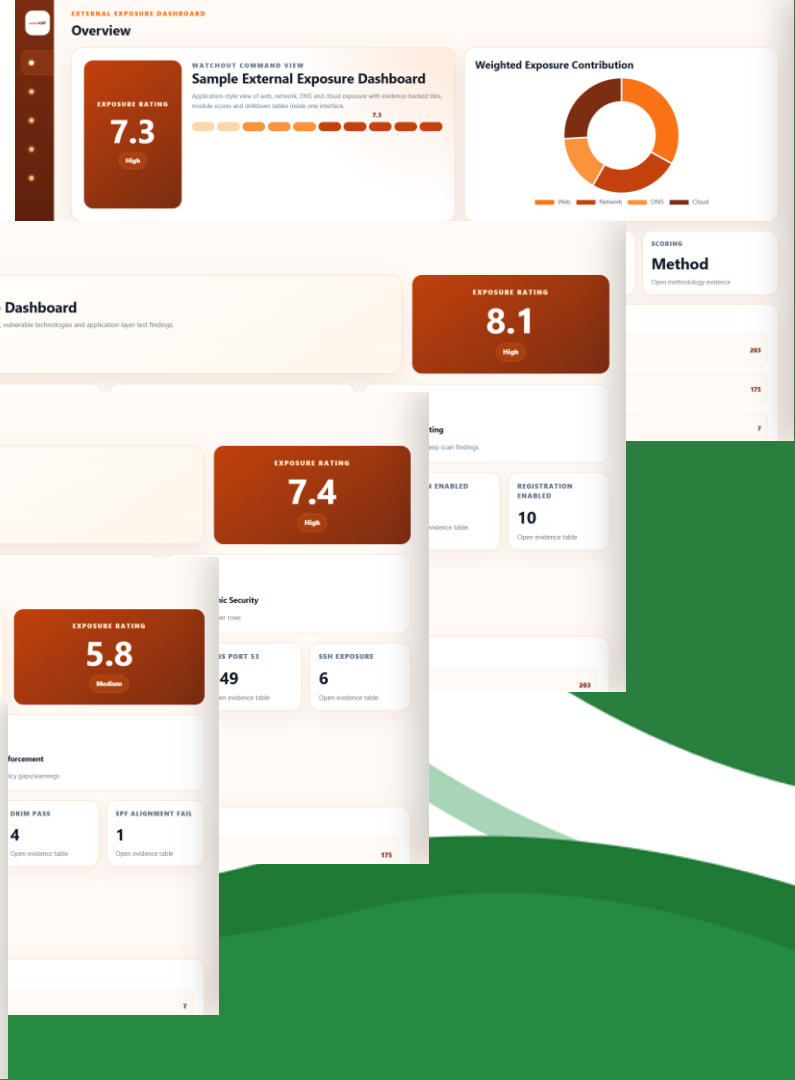
Actionable Outputs

Clear remediation guidance with severity ratings, technical evidence, and step-by-step fix instructions per finding.

Castellum Labs

watchOUT Dashboard - Delivery

“watchOUT, An Advance Intelligence & Dark Web Platform Designed To Discover Deep Intelligence”



Castellum Labs

Thank You

Questions? Reach out to Castellum Labs for further details.

+91 8639953505 | reach@castellumlabs.com| www.castellumlabs.com