HoundER

ENTERPRISE RECON

ATTACK SURFACE MANAGEMENT

Product Overview

CONTINUOUS ASSET DISCOVERY & MONITORING

Maintaining a up-to-date inventory of all internet-facing assets is a challenge for most businesses. Beyond traditional IT infrastructure web technologies connecting to third-parties are often responsible to introduce new vulnerabilities and the possibility of data leakage for organisations. The continuous discovery and monitoring of internet-facing assets becomes an essential goal for every organisation.

Attack Surface Management: Features

ASSET MANAGEMENT

Manage all your web-facing assets, domains nad CIDRs in a single place

COMPREHENSIVE ASSET DISCOVERY

Scan over 10k ports per IP, discover all your newly created and exposed web service

VULNERABILITY NOTIFICATION

Be the first one to know about vulnerabilities in your environment

WEB APPLICATION SCANNING

Over 1k custom vulnerability and misconfiguration checks that goes beyond traditional CVE findings

API INTEGRATIONS

Easy to use API to integrate with your SIEM, IT Workflow and Collaboration platforms

ZERO DEPLOYMENT

A complete SaaS solution that doesn't require any deployment in your environment

HoundER Attack Surface Management solution provides an adversary's perspective of an organisation's discoverable attack surface, enabling teams to better assess the likelihood and impact of weaknesses.

Attack Surface Management: Features

THREAT INTELLIGENCE INSIGHTS

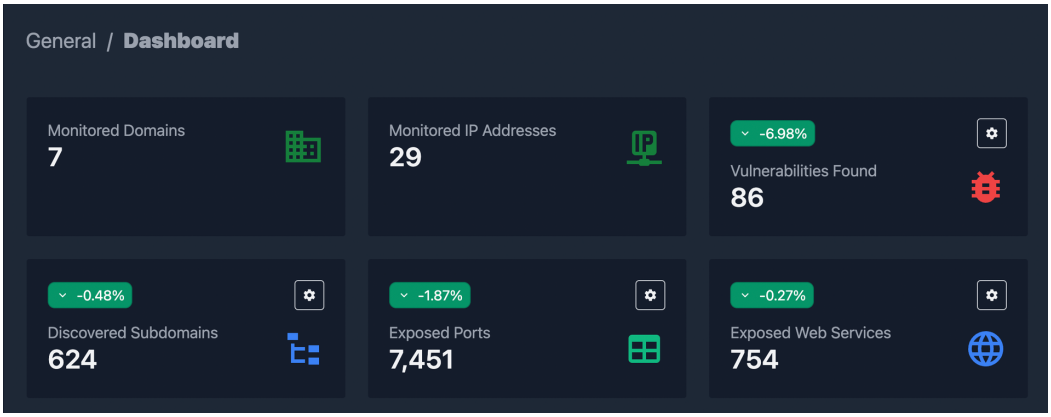
Gain intelligence insights over your attack surface from several data sources including malware analysis, botnets tracking and phishing detection

CUSTOM NOTIFICATIONS AND REPORT

Receive actionable alerts on newly discovered vulnerabilities, track remediation progress over time, and generate reports to demonstrate results

WORKFLOW ORQUESTRATION

Increase your response agility by automating your workflow processes with existing ITSM and collaboration tools



Automatically providing an external assessment of risk beyond those detected by vulnerability scanners. HounderER ASM leverages a variety of methodologies for external risk assessment, including vulnerabilities, asset prevalence, configuration and local indicators of weakness. Automatically reducing the number of false positives and filtering out noise generated by routine changes in dynamic infrastructure.

Product Capabilities

Functionality	Feature	Capability
Automated Discovery	External discovery	HoundER ASM solution requires minimum input to begin the discovery process.
	Comprehensive discovery	Automatically discover and monitor assets across IPv4 and IPv6 as well as data center and cloud infrastructure.
	Detailed service discovery	Enumerate detailed service information for discovered assets, including service name and version running on a system. For select services, configuration information also may be available.
	Detailed artifact discovery	Collect detailed artifacts from monitored assets for each scan.
	Path discovery	Show a user how the solution discovered an asset and the artifacts used to assign it to an organization.
Continuous Monitoring	Ongoing discovery	Discover new assets in an ongoing manner, outside of initial discovery.
	Change monitoring	User can monitor and track changes, such as newfound assets and new or impactful changes in risk, to their attack surface over time.
	Alerting	Automatically alert users to discoveries or changes on their perimeter.
	False positives and noise reduction	Automatically reduce the number of false positives and filter out noise generated by routine changes in dynamic infrastructure.
Risk-based Management	External assessment	Automatically provide an external assessment of risk beyond those provided by vulnerability scanners.
	Impact scoring	User may input information about business value as well as remediation and workflow status into the system to develop a prioritized assessment of risk.

Operational Capabilities

Functionality	Feature	Capability
Alerting	Change Monitoring	Monitors and tracks changes, such as newfound assets and new or impactful changes in risk, to the attack surface over time.
	Email Alerting	Automatically alerts users to discoveries or changes on their perimeter via email.
Enterprise Management	RBAC	Supports role-based access control.
	Rule-based Management	Supports rule-based and policy-based configurations for ongoing management.
	SSO	Supports single sign-on.
Interoperability and Integrations	API and Integrations	Supports third-party integrations and custom development using a provided API.

CORE SERVICES

- Attack Surface Management
- Penetration Testing
- Security Posture Assessment

About Us

HoundER Enterprise Recon helps organisations to manage their cybersecurity risks by offering unique and customised solutions to continuously monitor your attack surface.