tetharion

see beyond to surface

Product Datasheet

AI-Powered Cyber Threat and Attack Surface Intelligence Platform

Tetharion unifies brand, asset, vulnerability, account, and threat intelligence into one operational map, helping SOC and CTI teams focus faster on actionable signals.

CTI | ASM | Brand Protection | Leaked Accounts | Vulnerability Exposure | Dark Web Findings

Positioning at a glance

For operational security teams, Tetharion brings external attack surface visibility, structured threat intelligence, alarm triage workflows, deception signals, leaked account monitoring, and vulnerability findings into a single workspace.

Platform Overview

Tetharion combines cyber threat intelligence (CTI) and external attack surface management (ASM) within the same operational context. It helps security teams monitor brand impersonation, external asset discovery, vulnerability exposure, leaked accounts, and dark web findings from one central platform.

One operational map

Brand, asset, vulnerability, account, and threat intelligence are unified in a single view.

Continuous external visibility

Domains, subdomains, IPs, DNS records, certificates, services, and vulnerability findings are monitored.

Analyst-focused triage

IOC feeds, alarm workflows, deception signals, and leaked account findings are correlated.

Designed for

Tetharion is designed for SOC teams, CTI analysts, attack surface management teams, incident response teams, and security leaders who need one operational security view.

Core value proposition

- Operational context: CTI signals, alarm processes, deception findings, and leaked account visibility are handled with business context.
- External exposure visibility: Internet-facing assets and service evidence are tracked in a single inventory.
- Single workspace: Context loss is reduced across detection review, triage, configuration, scanner operations, and integrations.

Modules and Capabilities

The platform brings CTI, ASM, alarm management, and enterprise operations components together in a unified analyst workspace.

Unified CTI Dashboard

Unified CTI view for understanding cyber risk status from one screen.

Global Threat Intelligence Feed

Centralized tracking of IOCs and threat sources with operational context.

Alarm Triage & Workflow

Operational tracking, prioritization, and workflow management for alarms.

Deception Monitor

Monitoring of impersonation domains, lookalike assets, and brand abuse signals.

External Asset Inventory

External attack surface inventory covering domains, subdomains, IPs, and internet-facing services.

Asset Details & Scan Results

Asset details, scan results, and host/service evidence for analysts.

Leaked Account Monitoring

Monitoring leaked accounts and account exposure findings.

Content & Keyword Monitoring

Keyword and content monitoring for relevant exposure signals.

Dark Web Findings

Centralized management of dark web and closed-source signals as findings.

Vulnerability Management

Severity-focused vulnerability visibility to support risk prioritization.

Scanners, Users, Integrations

Operations center for setup, users, scanners, and integrations.

Monitoring Scope

Tetharion categorizes externally visible assets and threat signals into operational areas security teams can act on.

Scope	Monitored signal / data	Operational value
Brand and deception signals	Impersonation domains, lookalike assets, brand abuse, and deception-driven findings.	Brand protection and early-warning visibility.
External attack surface	Domains, subdomains, IPs, DNS records, certificates, services, and internet-facing assets.	Central inventory and exposure map for ASM teams.
Vulnerability findings	Vulnerability visibility for external assets with severity-focused risk tracking.	Shared view for prioritization and remediation tracking.
Leaked accounts	Leaked accounts and account exposure findings.	Supports identity risk and account security processes.
Threat intelligence	IOC feeds, structured threat sources, and closed-source/dark web signals.	Brings CTI data into alarm triage and incident response context.
Content and keyword monitoring	Monitoring keywords, content, and signals related to the target organization.	Strengthens brand, data leakage, and open-source visibility.

Operational Workflow

Tetharion is positioned to accelerate investigation and triage by unifying distributed security signals in one workspace.

1 **Signal collection**
IOC, deception, asset, vulnerability, account, and dark web findings

2 **Correlation**
Findings combined with business context and operational risk visibility

3 **Triage**
Prioritization and review through alarm workflows

4 **Action**
Remediation, tracking, notification, and handoff to incident response processes

5 **Reporting**
Single view and decision support for security leaders

Example use cases

SOC and MDR operations	Alarm triage, IOC correlation, leaked account visibility, and dark web findings in one workflow.
CTI operations	Structured threat intelligence feeds associated with business context and organizational assets.
Attack Surface Management	Continuous visibility of domain, subdomain, IP, DNS, certificate, service, and vulnerability findings.
Brand protection	Monitoring impersonation domains, lookalike assets, and brand abuse signals.
Incident Response readiness	Turning external exposure and identity leakage signals into a centralized evidence set for response teams.

Enterprise Use and Integration

Tetharion provides a workspace that can be adapted to enterprise monitoring and response processes through scanner, user, notification, syslog, and workflow configuration.

Enterprise operations components

Adaptable structure for organizational processes through scanner operations, user management, notification design, syslog integration, and workflow configuration.

Tenant-based access

Access model that redirects each organization to a dedicated workspace at app.tetharion.com using an assigned tenant ID.

Contribution to enterprise security operations

- Centralized visibility: Unifies CTI, ASM, leaked account, vulnerability, and dark web findings in one workspace.
- Operational tracking: Supports prioritization and tracking of findings through alarm triage and workflows.
- Integration-oriented usage: Adapts to existing security processes through scanner, notification, syslog, and user configuration.
- Executive visibility: Helps security leaders understand external exposure, threat signals, and operational status.

Demo and evaluation

A live demo, sample monitoring scenarios based on the organization’s scope, and an evaluation meeting can be planned for Tetharion. The product is positioned to support shared visibility needs across SOC, CTI, ASM, incident response, and security management teams.

Contact: For demo requests and product evaluation meetings, please use tetharion.com.