see beyond the surface.

tetharion

Cyber threat intelligence

External attack surface and digital risk visibility



THE SECURITY CHALLENGE

External digital exposure

01

Internet-facing infrastructure

New subdomains, exposed services and configuration changes.

02

Accounts and data

Leak records associated with employee, customer and third-party accounts.

03

Brand and corporate footprint

Lookalike domains, organization-related content and dark web findings.

• Which asset is affected? • What changed? • What needs investigation? •

PLATFORM APPROACH

A shared workspace for external risk

01

External attack surface

Assets, DNS, services, certificates and security findings.

02

Threat intelligence

Global indicators, dark web matches and leaked content.

03

Digital risk monitoring

Account exposure, organization-related content and lookalike domains.

The Dashboard connects the overview to individual modules and record details.

Monitoring scope

DATA CATEGORY	AVAILABLE INFORMATION	DECISION SUPPORT
Assets and infrastructure	Domain, IP, DNS, TLS, WAF/CDN	**Which assets are externally exposed?**
Services and findings	Port, product/version, L4/L7 findings	**Which service needs investigation?**
Accounts and content	Leak records, content matches	**Who or what data may be affected?**
Brand and threats	Lookalike domains, global IOC repository	**Which record needs investigation?**

• Alert records track supported discovery and change events. •

Internet-facing asset discovery

Investigate assets in technical context

Review domains and subdomains alongside IP, DNS, certificate and service records.

- Track new, changed and deleted DNS records.

ILLUSTRATIVE ASSET RECORD

[example.com]

Field	Example value
IP address	192.0.2.10
Service	TCP / 443 / HTTPS
Investigation context	DNS, TLS, host and service

Service changes and security findings

INVESTIGATION AREA	CONTEXT PROVIDED BY TETHARION
Exposed services	Port, protocol, product/version, banner and scan time
Changes	New or closed services and changes in service details
Security findings	Severity, affected host/service and technical details
Certificates	Validity dates, certificate findings and infrastructure context

- CVE/CPE references are provided when available in the record.

Account leak visibility

Assess account records in organizational context

Review employee, customer and third-party records by category, URL and date.

Supports account and session investigations by identity teams.

ILLUSTRATIVE ACCOUNT RECORD

Field	Example value
User	john.doe@example.com
Associated address	[example.com/login]
Category	Employee
Password	●●●●●●●●

• A leak record alone does not prove an active account compromise.

Organization-related content and leak research

Content matches

Filter organization-related records by keyword, URL, discovery date and available metadata.

Dark web findings

Review mentions, files and archive references. Investigate details and raw content where accessible.

Content acquisition status

Track request, approval, queue and processing stages as needed.

Lookalike domain monitoring

ILLUSTRATIVE DOMAINS

example.com

examp1e.test

Similarity type and score

Algorithmic similarity analysis and typosquatting detection.

Reachability and available registration date

Active status, WHOIS registration data and server responses.

Associated corporate asset

Assessment of links to brand assets and corporate infrastructure.

Similarity is a signal for investigating brand impersonation.

Global threat intelligence

Domain

IP:port

URL

File hash

Investigation filters

Threat type, malware family, confidence level, tags and timestamps.

An IOC in the global repository does not imply an incident detected in the customer environment.

Alerts and operational integration

Track new discoveries and changes by alert type, severity and time.

Email

Rules based on user, severity, alert type and subject

Syslog

UDP / TCP / TLS

RFC 5424, RFC 3164, CEF, LEEF, JSON

API

Account and content data

Client scopes, IP allowlists and request limits

Notifications require active delivery services and recipient configuration.

Monitoring scope and access management

01 Scope definitions

Domains, hostnames, IPs, keywords and blocklist entries.

02 Access by responsibility

Module permissions and separate access controls for sensitive account data.

03 VIP monitoring scope

Contact details and digital identity identifiers for key individuals.

04 User experience options

Email verification code sign-in, Turkish/English interface and theme selection.

See external risks in context

01

Asset visibility and change tracking

02

Account, content and brand investigations

03

Data delivery to security operations

Start with your organization's domains and priority investigation scenarios.