




Threatnote

Unified Threat Management Platform



Security teams face constant pressure to keep pace with new and emerging cyber threats, but doing so often requires multiple expensive tools that create silos and inefficiencies. Threatnote is a Unified Threat Management Platform that unifies threat intelligence collection, content management, dark web and brand monitoring, and third-party risk visibility in one system. By replacing fragmented tools and centralizing workflows, Threatnote reduces costs, eliminates tool sprawl, and ensures intelligence not only informs but empowers teams to take action quickly and effectively.

INTRODUCTION

STOP MANAGING TOOLS. START MANAGING THREATS.

Today's security teams are overwhelmed by data from too many disconnected tools. Siloed intelligence, manual correlation, and endless alerts create noise instead of clarity. This wastes valuable analyst time and leaves organizations exposed to threats that slip between the gaps. Traditional Threat Intelligence Platforms (TIPs) focus narrowly on indicators and fail to support the full intelligence lifecycle.

Threatnote was built to change this.

It is the all-in-one command center that unifies intelligence, streamlines workflows, and empowers teams to move from fragmented, reactive defense to intelligence-driven action.



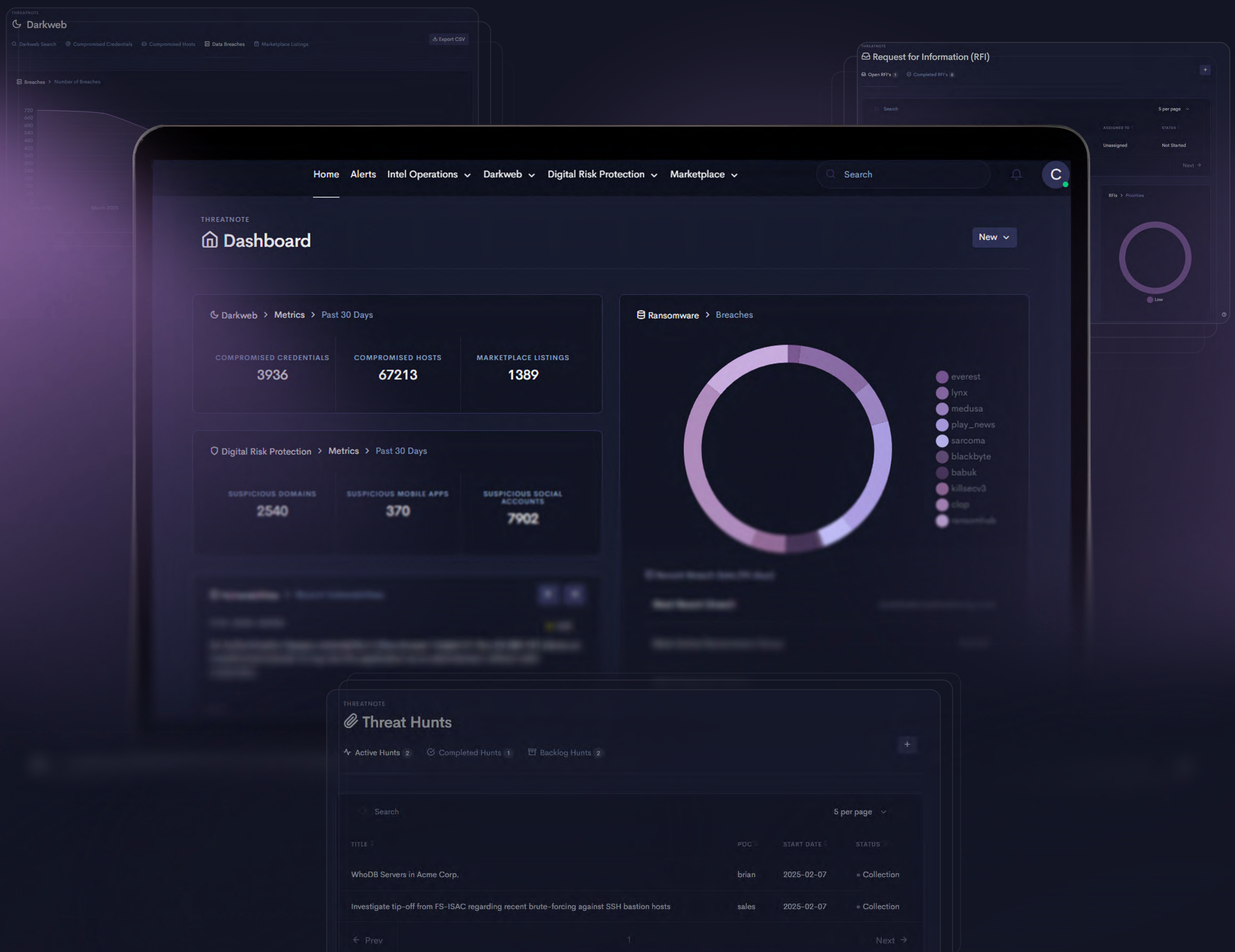
HOW THREATNOTE REDEFINES THREAT INTEL

Most TIP platforms focus narrowly on Indicators of Compromise. Threatnote was built to go much further by unifying all of the data sources required for an effective CTI program into one platform.

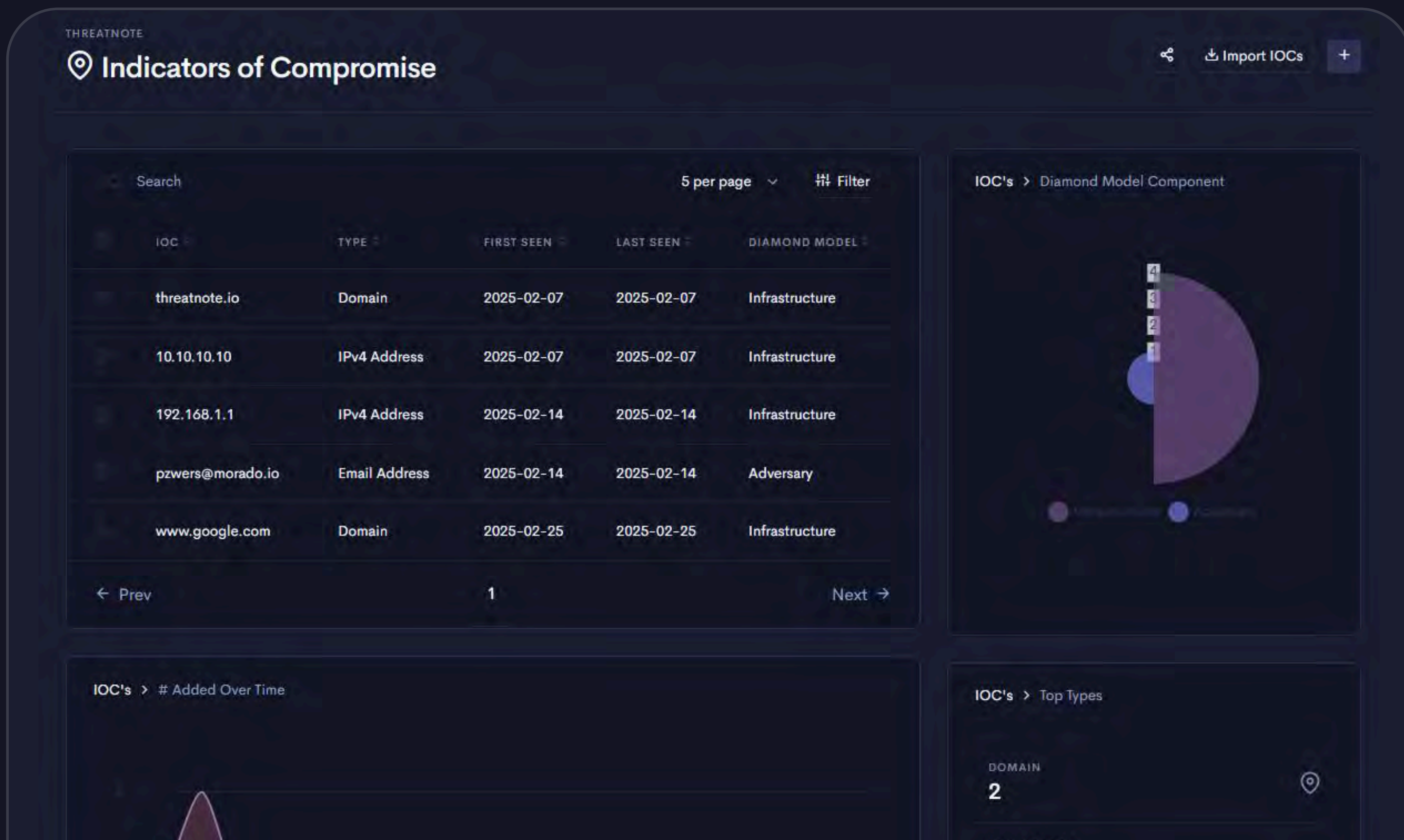
Threatnote pulls in dark web monitoring, brand impersonation, third-party risk intelligence, VIP monitoring, OSINT analysis, and traditional IOC data, all tied back to your intelligence requirements. Instead of tracking requirements in spreadsheets and piecing data together from multiple tools, Threatnote centralizes everything.

Your requirements guide automated collection across every source, and the results flow into a single workspace where they can be turned into action.

By eliminating silos and consolidating intelligence into one platform, Threatnote reduces the time it takes to identify actionable data and accelerates the ability to act on it.



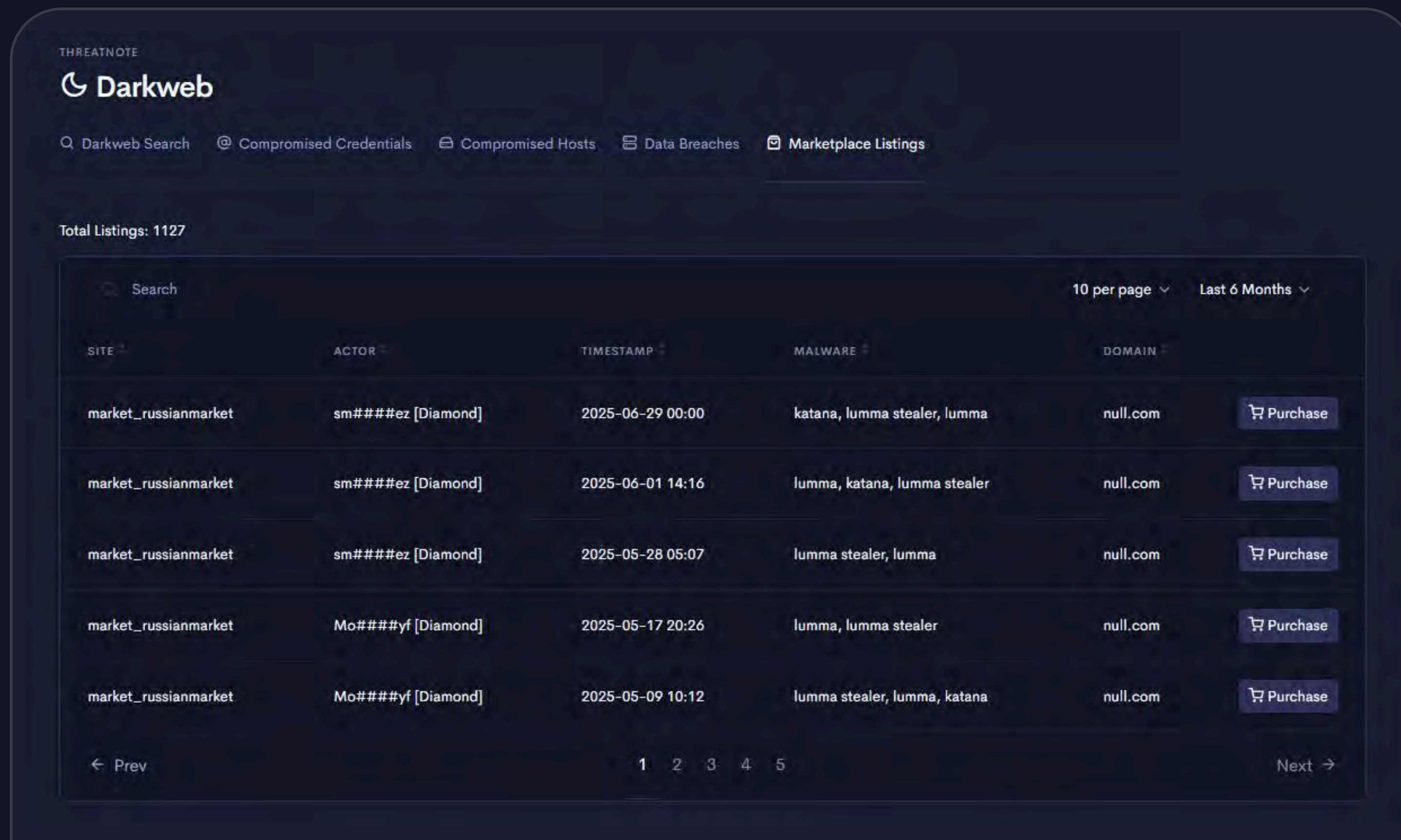
CORE FEATURES



Intel Operations

ALIGN COLLECTION TO GOALS / MEASURE AND IMPROVE EFFORTS

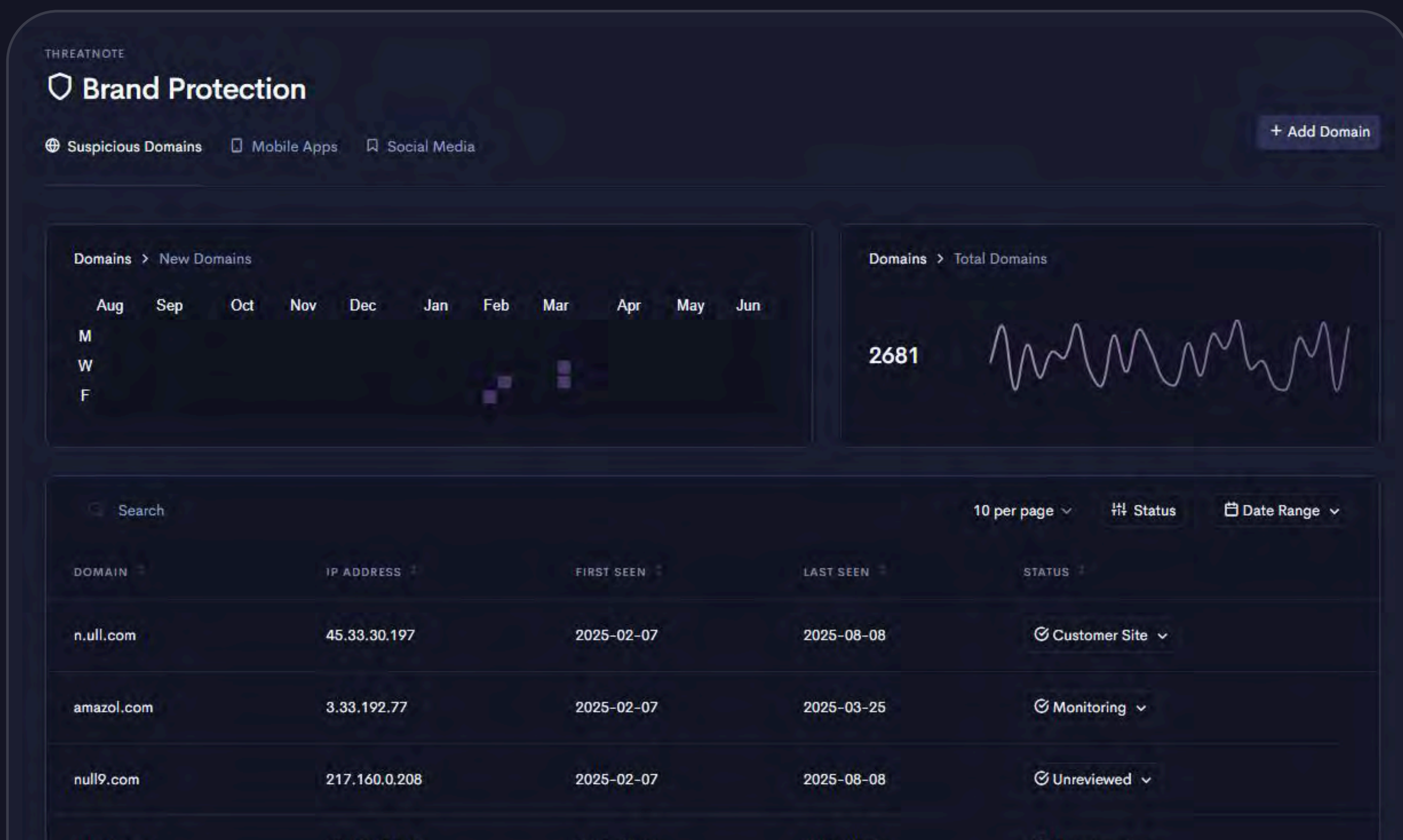
Manage PIRs, RFIs, threat hunts, and reporting in one unified platform. Align collection with stakeholder requirements, centralize workflows, and ensure intelligence drives timely action across the organization.



Dark Web Monitoring

SPOT LEAKED DATA EARLY / ACT ON THREATS BEFORE IMPACT

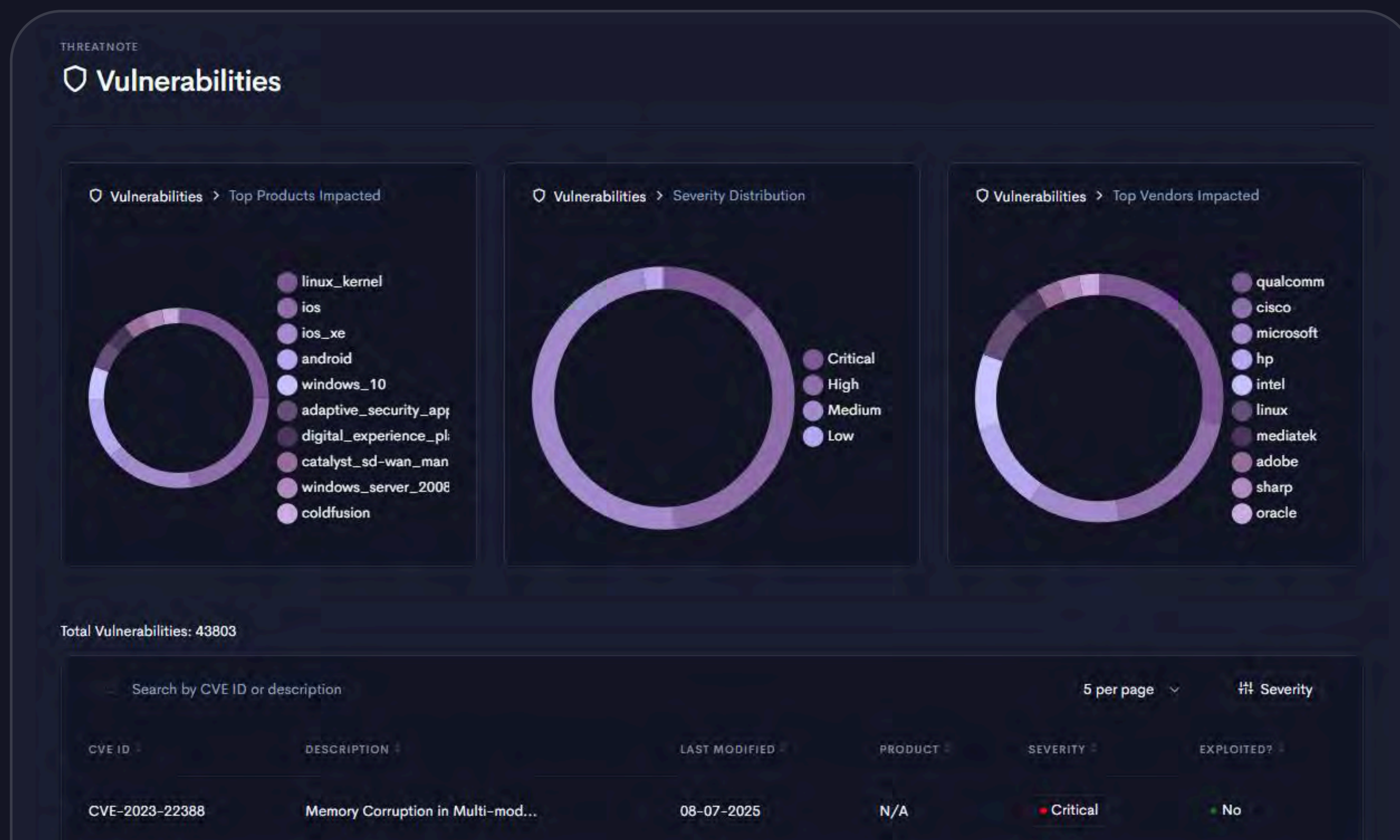
Search across extensive dark web sources to identify leaked credentials, exposed sensitive data, and threat actor activity targeting your organization. Integrate findings directly into your intelligence requirements, reporting, and hunts, with alerts that enable you to take action before attackers can exploit the information.



Brand Protection

DETECT PHISHING AND FRAUD / SAFEGUARD DOMAINS AND APPS

Protect your brand, assets, and customer trust by monitoring domains, app stores, and social media for phishing sites, fraudulent domains, and fake mobile apps. Detect impersonation early and respond quickly to prevent damage before it spreads.



Vulnerability Intelligence

TRACK RELEVANT FLAWS / PRIORITIZE CRITICAL FIXES

Track vulnerabilities as they are disclosed and actively exploited across the threat landscape. Correlate findings with your environment and threat actor activity to prioritize remediation based on real-world risk and reduce exposure.

CORE FEATURES

THREATNOTE





Third Party Intelligence

Total Vendors: 4

Search

10 per page

Show All Vendors

VENDOR	RISK METRICS	RISK SCORE	INDUSTRY
 Acronis	Email Security Credential Leak Increase	Low	Technology & Communications
 Amazon Web Services (AWS)	Data Breach Email Security Credential Leak Increase	Low	Technology & Communications
 Atlassian	Credential Leak Increase	Medium	Technology & Communications
 Cloudflare	Email Security Credential Leak Increase	Medium	Technology & Communications

Third-Party Intelligence

MONITOR VENDOR RISKS / SPOT SUPPLY CHAIN THREATS

Monitor vendors and partners for breaches, leaked data, and other exposures that could put your organization at risk. Gain visibility into third-party threats so you can take action before they impact your business.

THREATNOTE

VIP Risk Protection

Risk Protection > Risk Events

Aug

Sep

Oct

Nov

Dec

Jan

Feb

Mar

Apr

May

Jun

Jul

Aug


M

W

F

Risk Protection > Total Events

0



Risk Protection > Free Search (e.g. email address, full name, company name)

Search for any personal identifiers or keywords (e.g., email address or full name)

2025-02-09

2025-08-08

Submit

Search...

Site

Date Range

USER	SOURCE	TIMESTAMP	CONTENT	STATUS
No Results				
<div>Prev</div>				<div>Next</div>

VIP Monitoring

PROTECT KEY INDIVIDUALS / CATCH LEAKS AND IMPERSONATION

Track executives and high-value individuals for credential leaks, targeted phishing, and impersonation attempts. Protect leadership and reduce the risk of attackers exploiting personal exposures to compromise the organization.

THREATNOTE

Dashboard

New

Darkweb > Metrics > Past 30 Days

COMPROMISED CREDENTIALS

3800

COMPROMISED HOSTS

67212

MARKETPLACE LISTINGS

1112

Digital Risk Protection > Metrics > Past 30 Days

SUSPICIOUS DOMAINS

2539

SUSPICIOUS MOBILE APPS

368

SUSPICIOUS SOCIAL ACCOUNTS

7901

Vulnerabilities > Recent Vulnerabilities

CVE-2025-43979

7.4

An issue was discovered on FIRSTNUM JC21A-04 devices through 2.01ME/FN that allows authenticated attackers to execute arbitrary OS system commands with root privileges via crafted payloads to the xml_action.cgi?method= endpoint.

N/A

N/A

Ransomware > Breaches

Recent Breach Data (90 days)

Most Recent Breach

promosfera.com

Most Active Ransomware Group

everest

Most Impacted Industry

Manufacturing

Attack Surface Intelligence

FIND EXPOSED ASSETS / FIX HIGH-RISK ISSUES FIRST

Uncover exposed assets, misconfigurations, and vulnerabilities to see your environment as attackers would. Prioritize remediation by risk to shrink your attack surface and strengthen defenses.

Alerts > Recent Alerts

TITLE	PRIORITY	STATUS	DETECTED AT
Custom Keyword test	High	Open	2025-08-08 12:03:14
Custom Keyword test	High	Open	2025-08-08 11:03:17
Custom Keyword test	High	Open	2025-08-08 11:03:16
Custom Keyword test	High	Open	2025-08-08 11:03:15
Custom Keyword test	High	Open	2025-08-08 10:03:18

Hunts > In-Progress Hunts

NAME	POC	START DATE
Investigate tip-off from FS-ISAC regarding recent brute-forcing against SSH bastion hosts	sales	2025-02-07

RFIs > Open RFIs

View all

WhoDB use in our environment

6 months ago

Low

Audit > Recent Activity

View all

sales updated TR-01-2025

1 week ago

sales updated TR-01-2025

3 weeks ago

sales updated TR-01-2025

3 weeks ago

analyst1-acme updated TR-01-2025

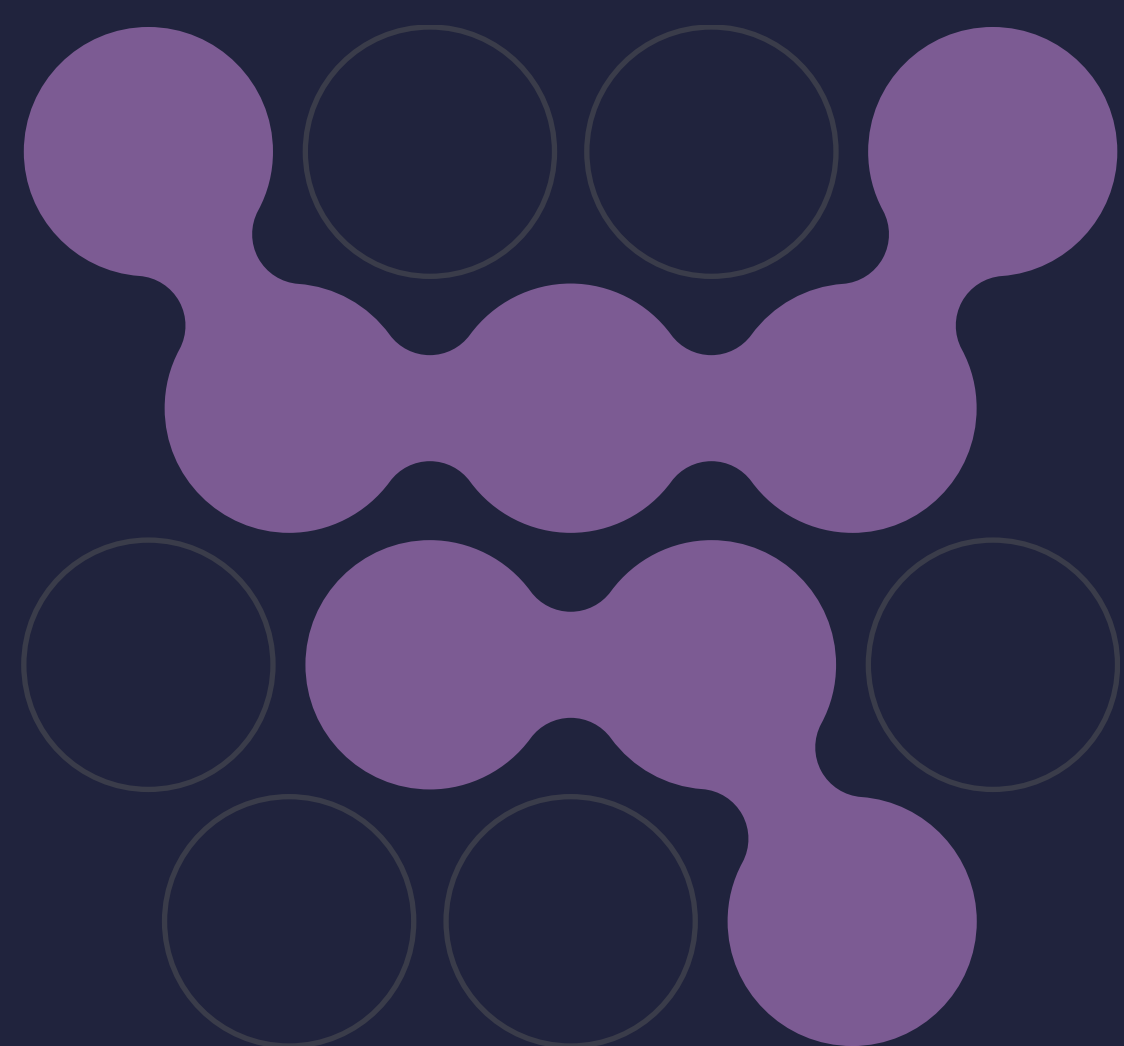
3 weeks ago

Open-Source Intelligence (OSINT)

ADD CONTEXT WITH OSINT / INTEGRATE INTO WORKFLOWS

Continuously gather and analyze open-source intelligence across forums, news, and social platforms. Surface emerging threats and trends that impact your organization and align collection with your intelligence requirements.

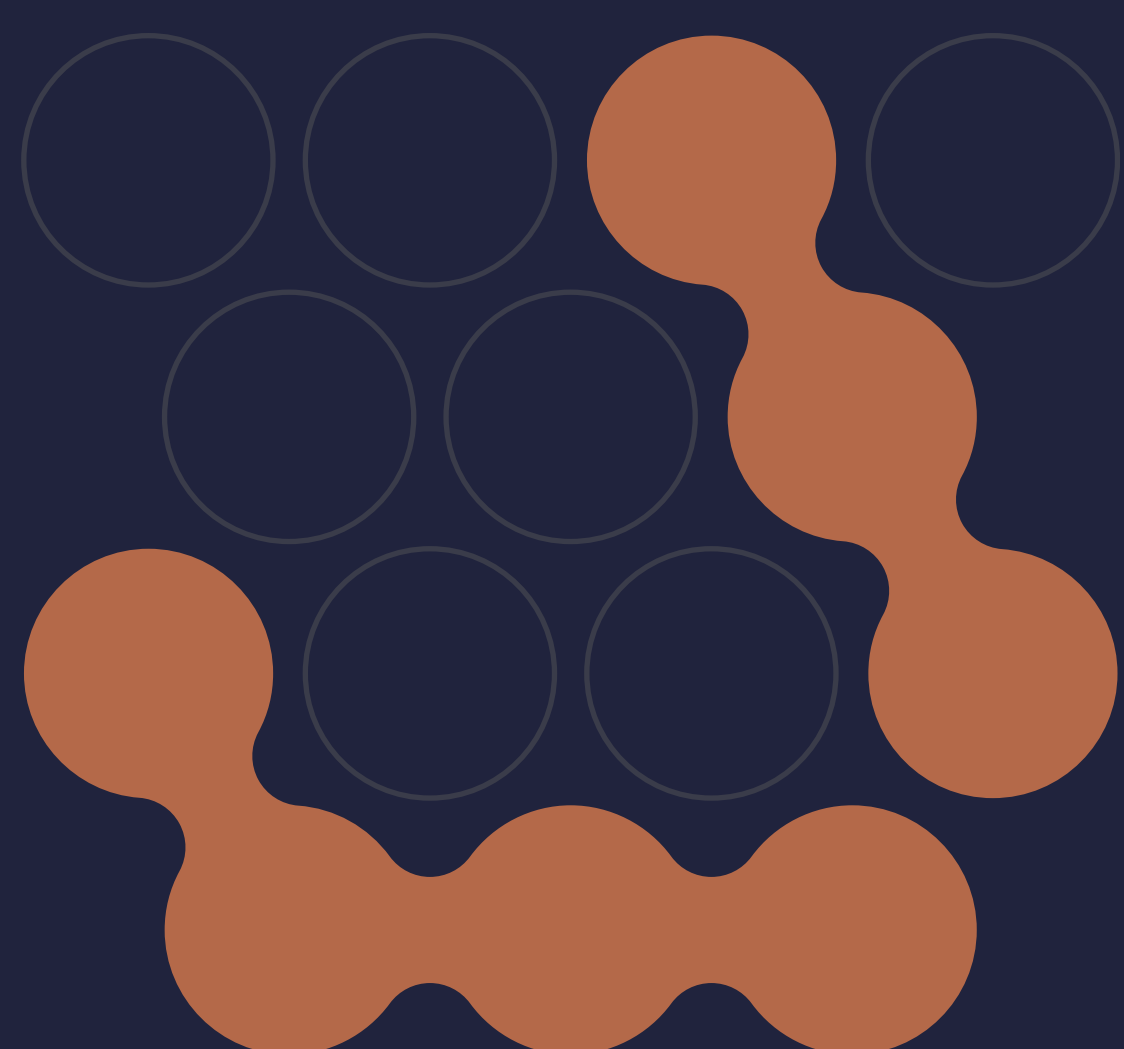
CHALLENGES SOLVED



CHALLENGE 1

Tool Sprawl And Rising Costs

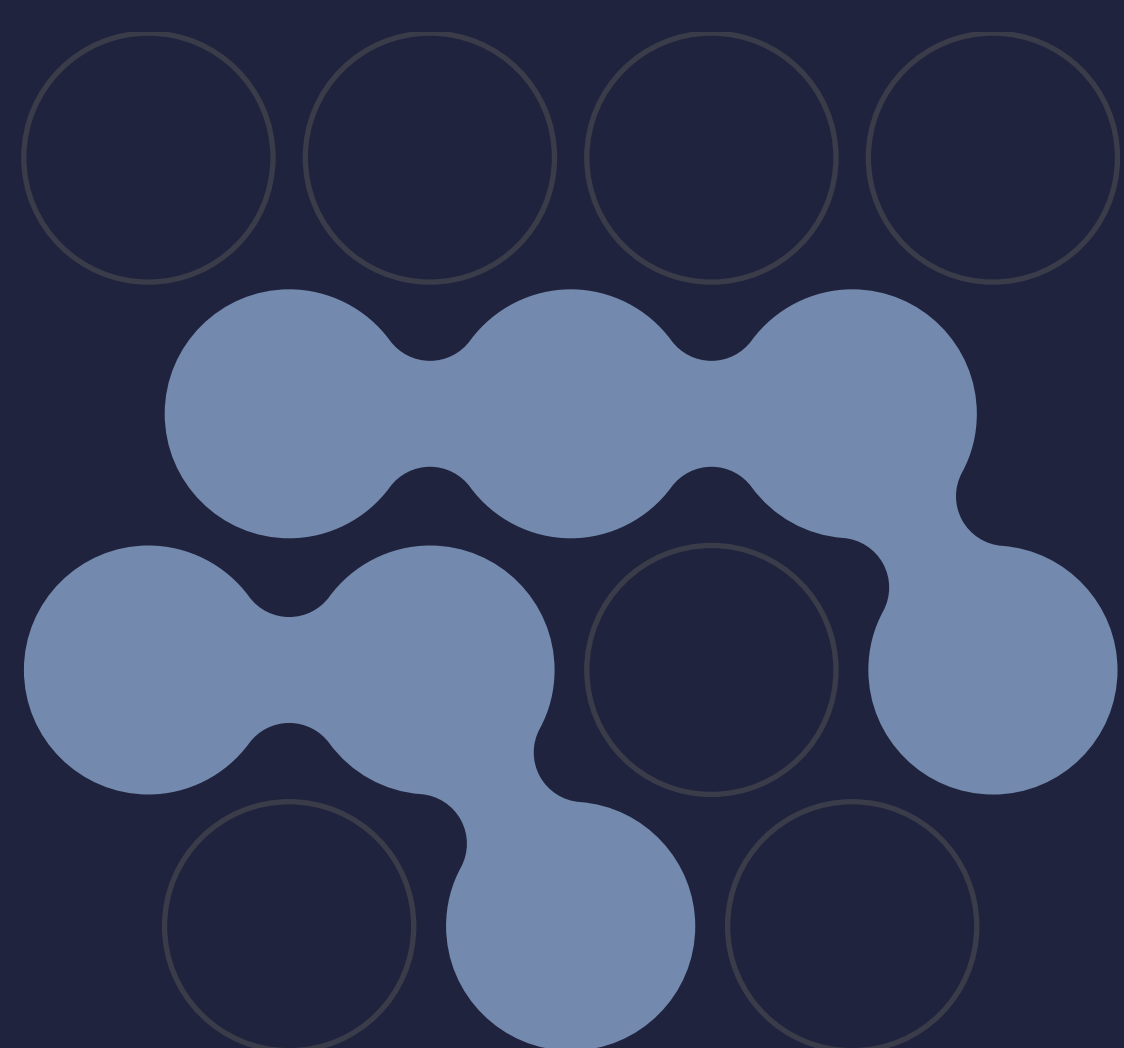
Multiple expensive platforms create silos and inefficiencies. Threatnote unifies intelligence in one platform to cut costs and simplify workflows.



CHALLENGE 2

Actionable Vs. Action

Most tools surface data without a clear path to act. Threatnote connects intelligence to workflows so teams can respond directly.

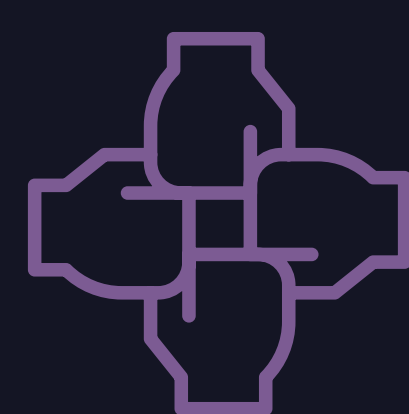


CHALLENGE 3

Disconnected From Requirements

Spreadsheets and siloed tools leave PIRs and RFIs unmanaged. Threatnote ties intelligence directly to requirements, guiding collection and proving value.

REAL-WORLD USE CASES



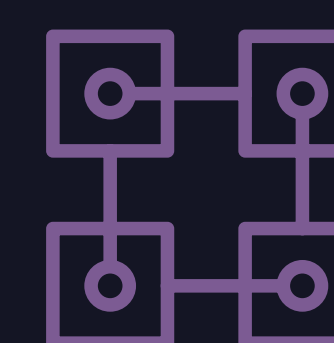
THREAT INTELLIGENCE TEAMS

Centralize intelligence requirements, RFIs, hunts, and reporting in one platform. Threatnote streamlines the full intelligence lifecycle, giving analysts the ability to collect, analyze, and act without juggling multiple tools.



MANAGED SECURITY SERVICE PROVIDERS (MSSPS)

Support multiple customers with a true multi-tenant environment. Threatnote enables MSSPs to deliver managed threat intelligence services, cut tool costs, and even grant clients direct visibility into their own data.

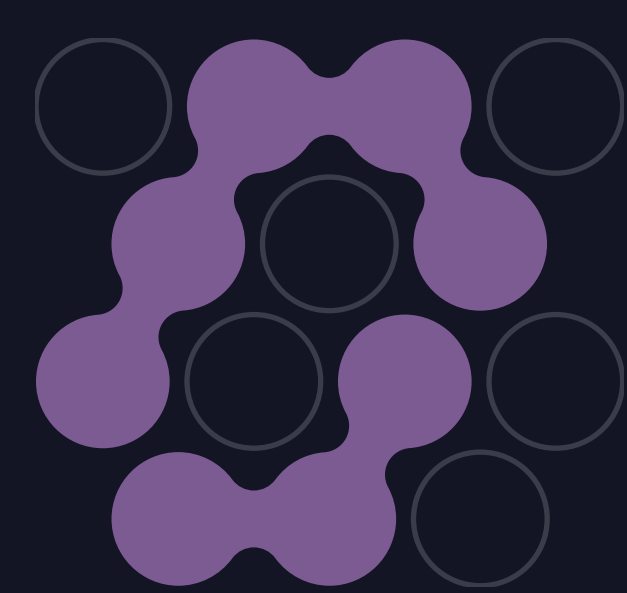


SECURITY OPERATIONS CENTERS (SOCs)

Bring dark web, brand, vulnerability, and third-party intelligence directly into SOC workflows. Threatnote accelerates triage and response by connecting intelligence to action where it matters most.

ARCHITECTURE AND TECH SPECS

Threatnote is built on a modern, scalable architecture designed to meet the diverse needs of threat intelligence teams, MSSPs, and SOCS. Leveraging multi-cloud support and microservices, the platform ensures flexibility, reliability, and seamless scalability for organizations of all sizes. Below is an overview of Threatnote's architecture, data management, security, and scalability.

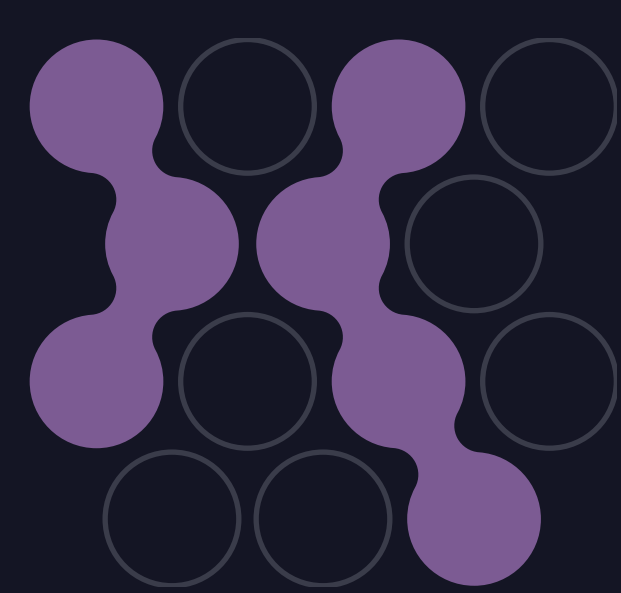


Platform Architecture

Threatnote's microservices architecture is built for modularity, scalability, and fault tolerance. Each service runs independently, allowing smooth updates and maintenance without affecting performance. As a multi-tenant system, Threatnote securely manages intelligence data for multiple customers in siloed environments. This ensures strict data segregation, tailored management, and consistent platform performance for every tenant.

The platform supports both cloud and on-premises deployments:

- **Cloud Deployment (AWS):** Deployed primarily in AWS, Threatnote uses Amazon Elastic Container Service (ECS) to orchestrate microservices and scale resources based on demand.
- **On-Premises Deployment:** For self-hosted environments, Threatnote offers Docker-based deployment, giving teams complete control over infrastructure while keeping all platform capabilities.

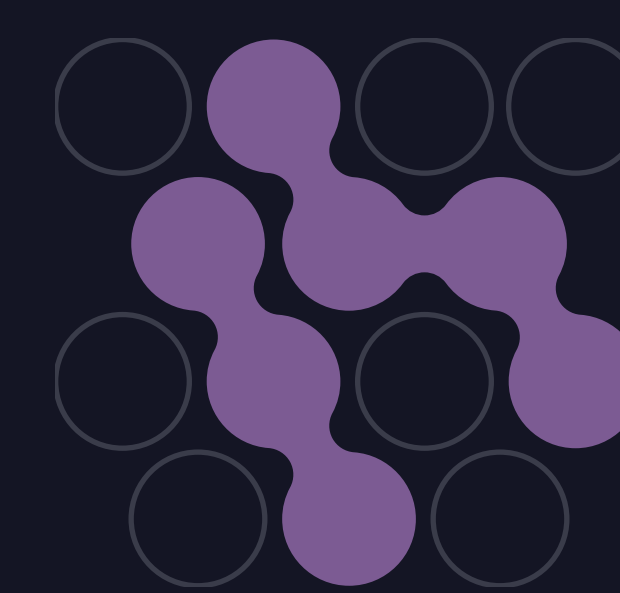


Data Management And Storage

Threatnote efficiently manages large volumes of threat intelligence data, including IOCs, reports, and threat actor profiles. It provides fast and reliable access through integrations, advanced querying, and structured storage. Built for scale, the platform supports complex searches and detailed filtering so analysts can quickly find, correlate, and act on relevant intelligence without losing critical context.

Key Capabilities:

- **Data Storage:** AWS Relational Database Service (RDS) ensures secure and highly available data storage with automated backups and multi-AZ redundancy for stability.
- **Data Querying:** Full-text search across large datasets, with advanced querying and filtering tools to quickly analyze and correlate intelligence.



Security Considerations

Security is a core part of Threatnote's design and daily operation. The platform applies encryption, role-based access, and other best practices to protect sensitive intelligence data. Each layer of security is designed to safeguard stored information, control user permissions, and ensure data availability, giving teams the confidence to operate in a secure and compliant environment at all times.

Security Measures:

- **User Authentication:** Auth0 handles authentication with MFA and SSO, while role-based access control (RBAC) ensures users can only reach approved data.
- **Backup and Redundancy:** AWS RDS backups protect data integrity and availability with daily automated backups and real-time replication across availability zones.
- **Encryption:** Data is encrypted at rest using AWS Key Management Service (KMS) and in transit with TLS for secure storage and communication.

DEPLOYMENT OPTIONS

- Cloud on AWS for scalability and ease of management
- On-premises with Docker for full infrastructure control

ARCHITECTURE

- Microservices for modularity and fault tolerance
- Multi-tenant design with strict data segregation

DATA MANAGEMENT

- AWS RDS for secure, redundant storage with automated backups
- Robust query capability with advanced search and filtering

SECURITY

- Encryption at rest and in transit
- MFA, SSO, and role-based access control
- Redundant backups and multi-AZ replication



Morado is a veteran-owned cyber threat intelligence company helping security teams cut through noise and act on what matters most.

Our platform, Threatnote, unifies intel operations, dark web monitoring, brand protection, third-party risk intelligence, and more into a single solution for enterprises and MSSPs. With AI-driven correlation, connected workflows, and advisory expertise, we reduce the workload for security teams and turn intelligence into outcomes.

**STOP MANAGING TOOLS AND START MANAGING THREATS.
CONNECT WITH US TODAY TO SEE HOW THREATNOTE CAN UNIFY
YOUR INTELLIGENCE AND TURN DATA INTO DECISIVE ACTION.**