CYTECTRA

Product Overview

Cytectra is a comprehensive Cyber Threat Intelligence (CTI) platform designed to aggregate, correlate, and visualize threat data. It enhances an organization's cybersecurity posture by providing real-time threat landscape insights, supporting automated data ingestion, advanced threat correlation, and security advisory management.

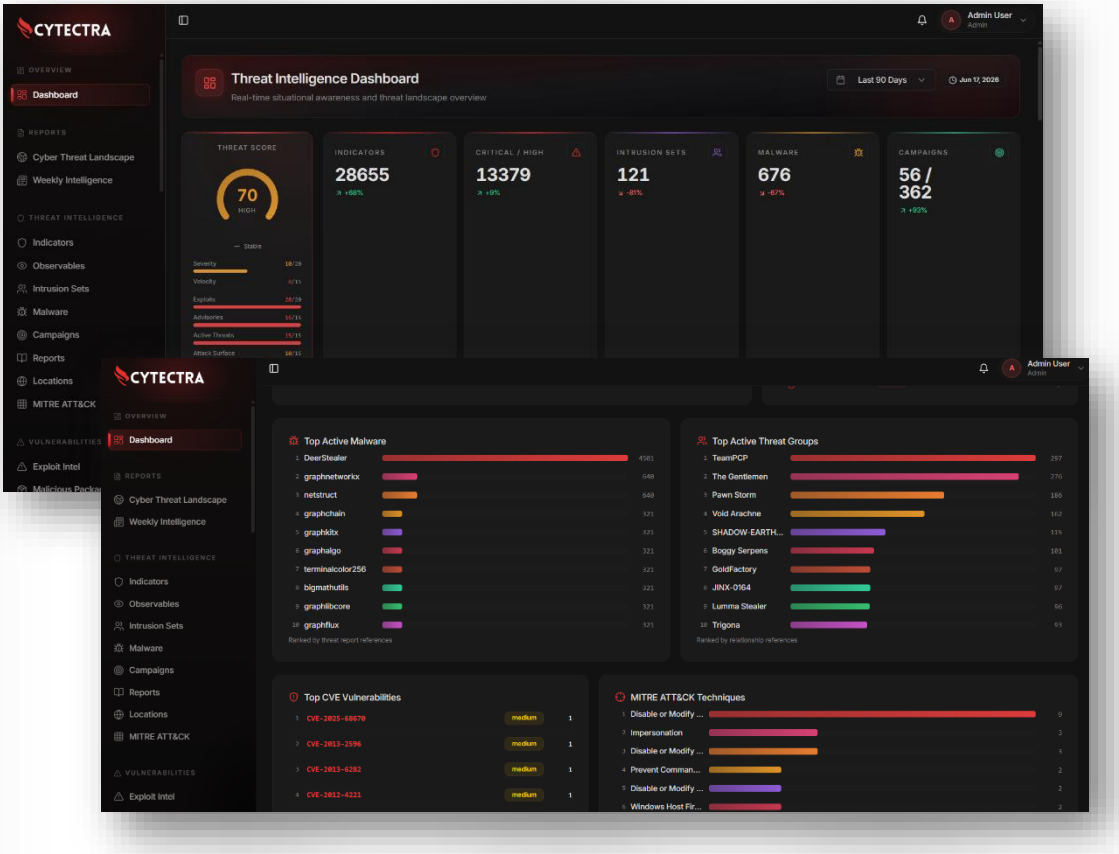
The platform facilitates the exchange of standardized threat information using STIX (Structured Threat Information Expression) 2.1 and TAXII (Trusted Automated eXchange of Intelligence Information) 2.1 protocols, enabling seamless interoperability with other security tools and platforms.

Built for Seamless Integration

Key Benefit

- Unified CTI Workspace Centralize threat intelligence, advisories, campaigns, and ASM findings in one platform
- Share intelligence seamlessly with native STIX/TAXII 2.1 support
- Accelerate investigation and analysis with AI-assisted workflows
- External Risk Visibility Detect exposed assets, typosquatting, and leaked credentials early
- Direct-to-Defense Export Export indicators directly to IDS, SIEM, and firewall platforms
- Lock-In Self-hosted deployment with full control over data and infrastructure

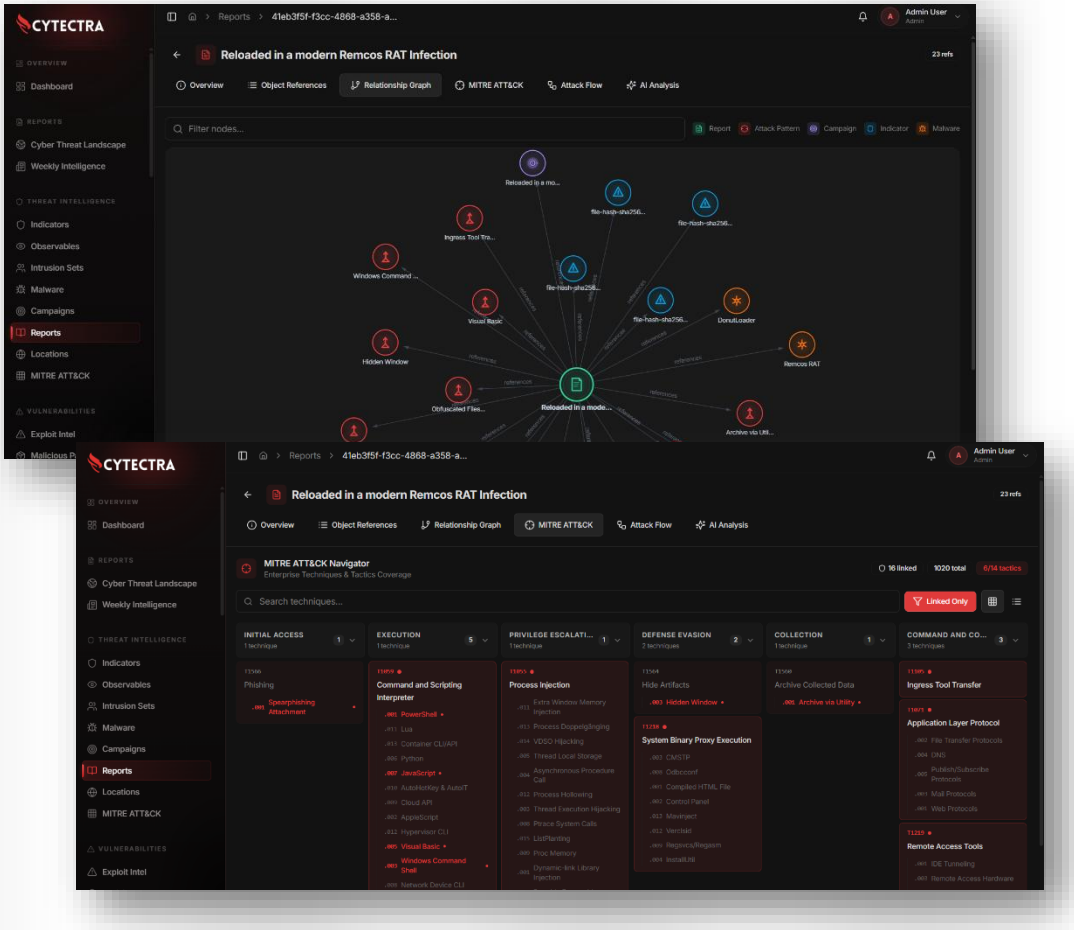
Dashboard



The Dashboard feature delivers a high-level command center for monitoring threat intelligence activity across the security environment. It brings together essential metrics such as threat score, indicators, critical and high-priority findings, intrusion sets, malware, and campaigns, giving users a fast and structured view of the current threat landscape.

Designed for clarity and rapid decision-making, the dashboard presents complex intelligence data through visual summaries and ranked insights, including active malware, threat groups, CVE vulnerabilities, and MITRE ATT&CK techniques. This helps security teams quickly identify priority risks, understand threat patterns, and focus their response efforts with greater confidence.

STIX/TAXII 2.1

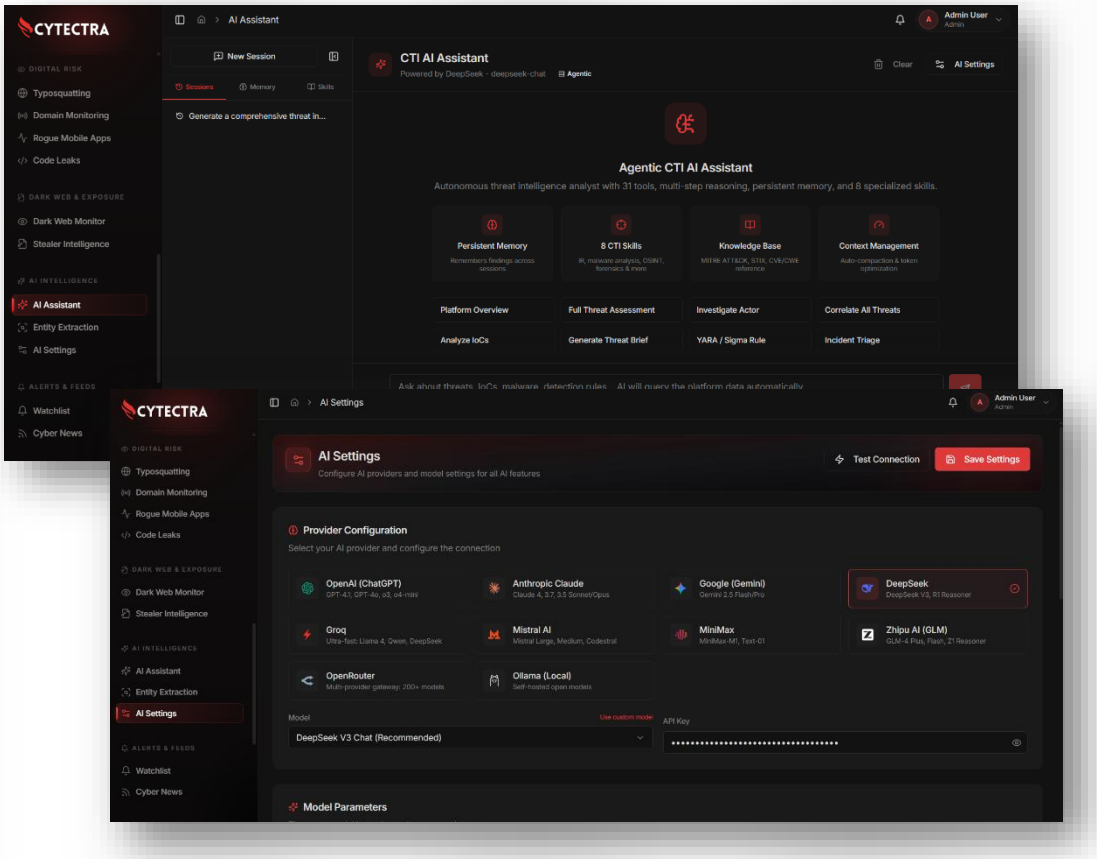


STIX/TAXII 2.1 enables standardized threat intelligence sharing and automated IOC exchange across security platforms. Analysts can visualize relationships between malware, indicators, campaigns, threat actors, and MITRE ATT&CK techniques through an interactive intelligence graph for faster investigation and threat analysis.

Features

- STIX 2.1 & TAXII 2.1 support
- Automated IOC sharing & synchronization
- Interactive relationship graph
- MITRE ATT&CK mapping
- Threat correlation & analysis
- SIEM, SOAR, and EDR integration ready

AI Threat Intelligence Assistant



AI Threat Intelligence Assistant helps analysts accelerate investigation, intelligence correlation, and threat analysis using AI-powered automation. The platform combines CTI data, MITRE ATT&CK knowledge, IOC analysis, and contextual threat insights into a single interactive workspace for faster security operations.

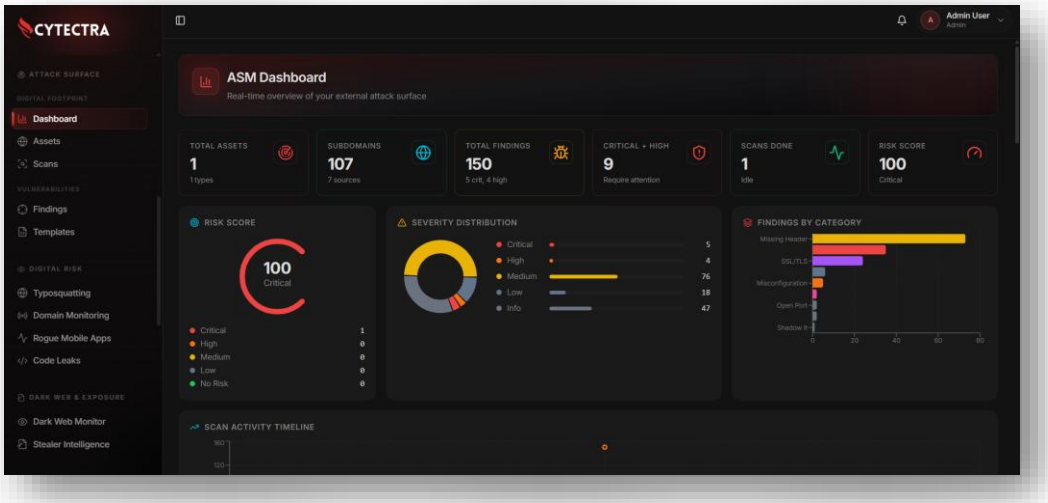
The solution supports multiple AI providers and models, enabling flexible deployment for automated reporting, entity extraction, attack analysis, and threat assessment workflows across SOC and Threat Intelligence teams.

Key Features

- AI-powered threat investigation assistant
- Multi-model AI provider support

- Automated CTI analysis & summarization
- IOC and entity extraction
- MITRE ATT&CK contextual analysis
- Persistent memory & contextual reasoning
- Threat correlation & enrichment

Attack Surface Management



The Attack Surface Management (ASM) module provides continuous visibility into external-facing assets and exposed services across the organization's internet footprint. It combines automated discovery, vulnerability assessment, SSL/TLS analysis, API security testing, and misconfiguration detection into a unified monitoring platform for proactive exposure management.

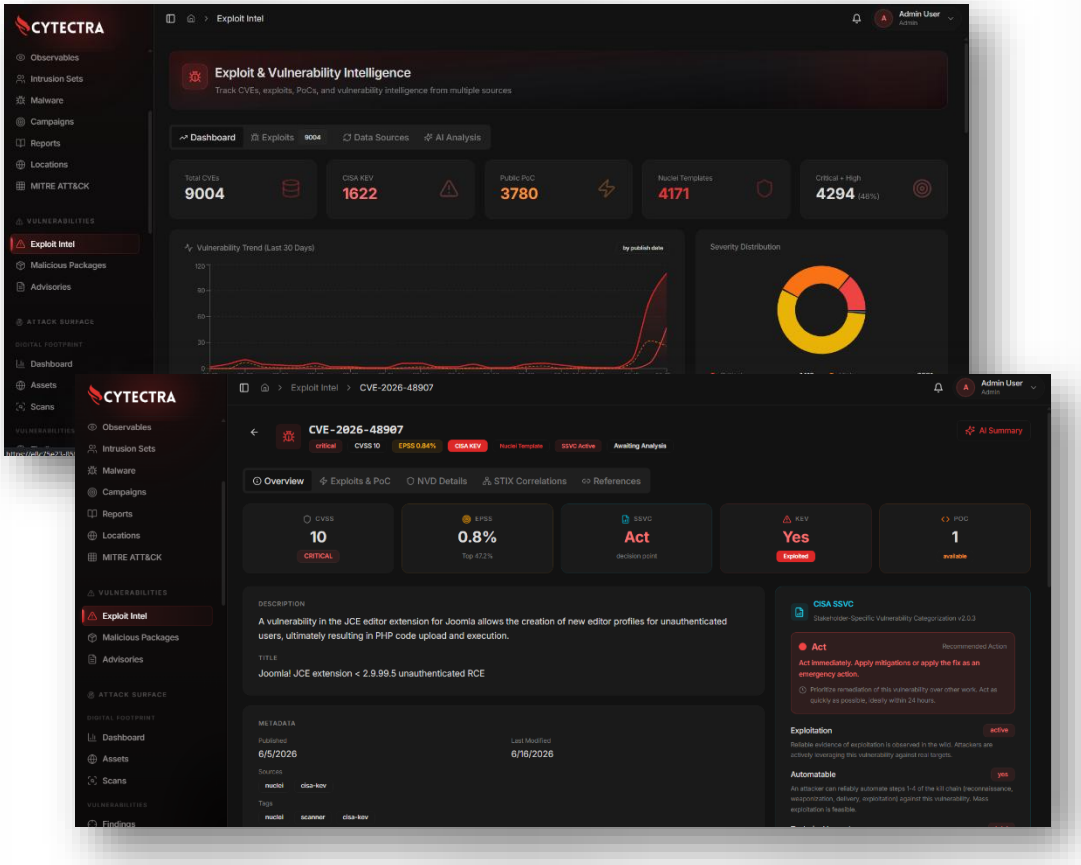
Built with a multi-phase concurrent scanning engine, the platform continuously identifies new assets, detects vulnerabilities, validates exposures, and tracks remediation status over time to help security teams reduce attack surface risk and improve external security posture.

Features

- Continuous external asset discovery and monitoring
- Automated subdomain enumeration and DNS analysis
- Multi-phase vulnerability and exposure scanning
- SSL/TLS, HTTP header, and DNS security assessment
- REST API, GraphQL, and SOAP security testing
- CMS vulnerability and default credential detection

- Service fingerprinting and network exposure analysis
- False-positive reduction with intelligent validation
- Persistent findings lifecycle and remediation tracking
- Flexible scan profiles for quick, full, or targeted assessments

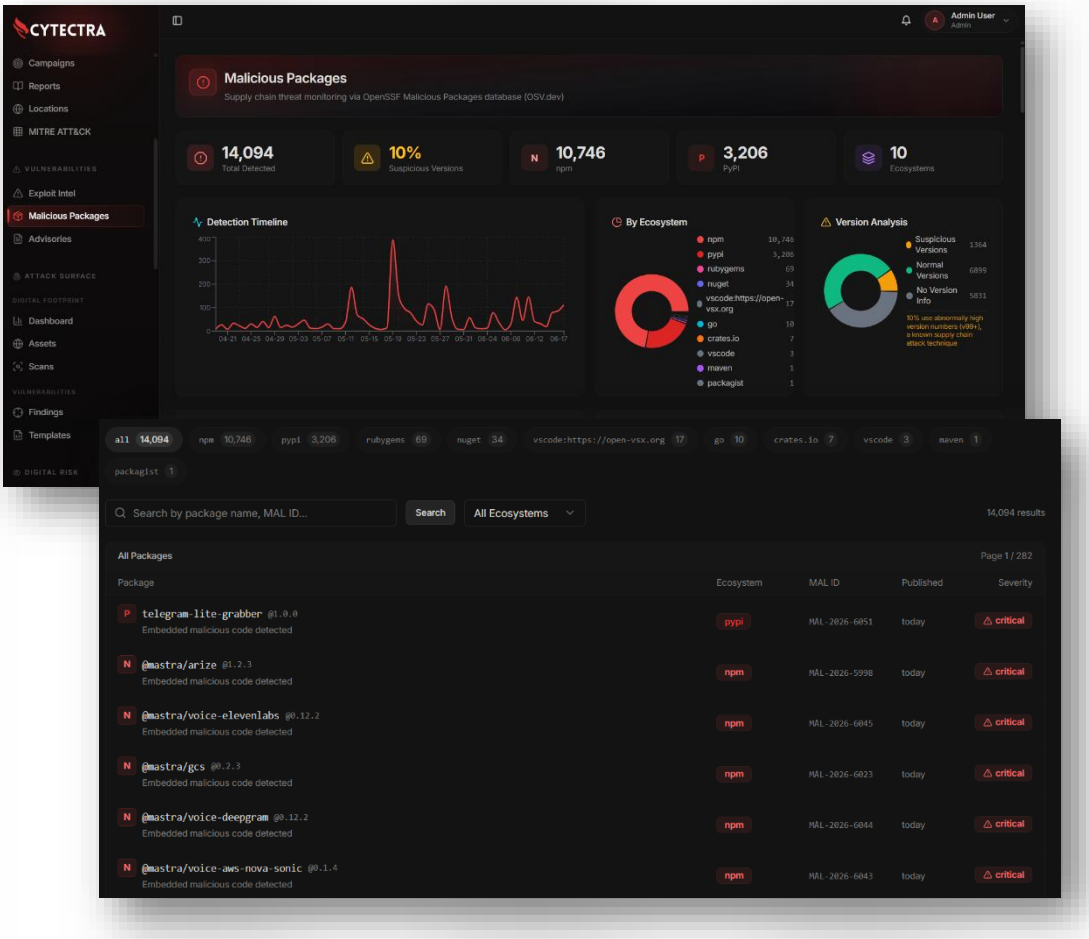
Exploit and Vulnerability Intelligence



The Exploit Intelligence dashboard delivers a clear, consolidated view of the current vulnerability and exploitation landscape, helping security teams quickly identify what matters most and prioritize response efforts effectively.

- Summarizes key metrics, including the total number of CVEs, vulnerabilities known to be exploited in the wild through CISA KEV, available proof-of-concept exploits, and matching Metasploit modules.
- Highlights recently disclosed and actively exploited CVEs so teams can stay ahead of emerging threats.
- Displays Exploit Prediction Scoring System (EPSS) scores to support risk-based prioritization and remediation planning.

Malicious Package Monitoring

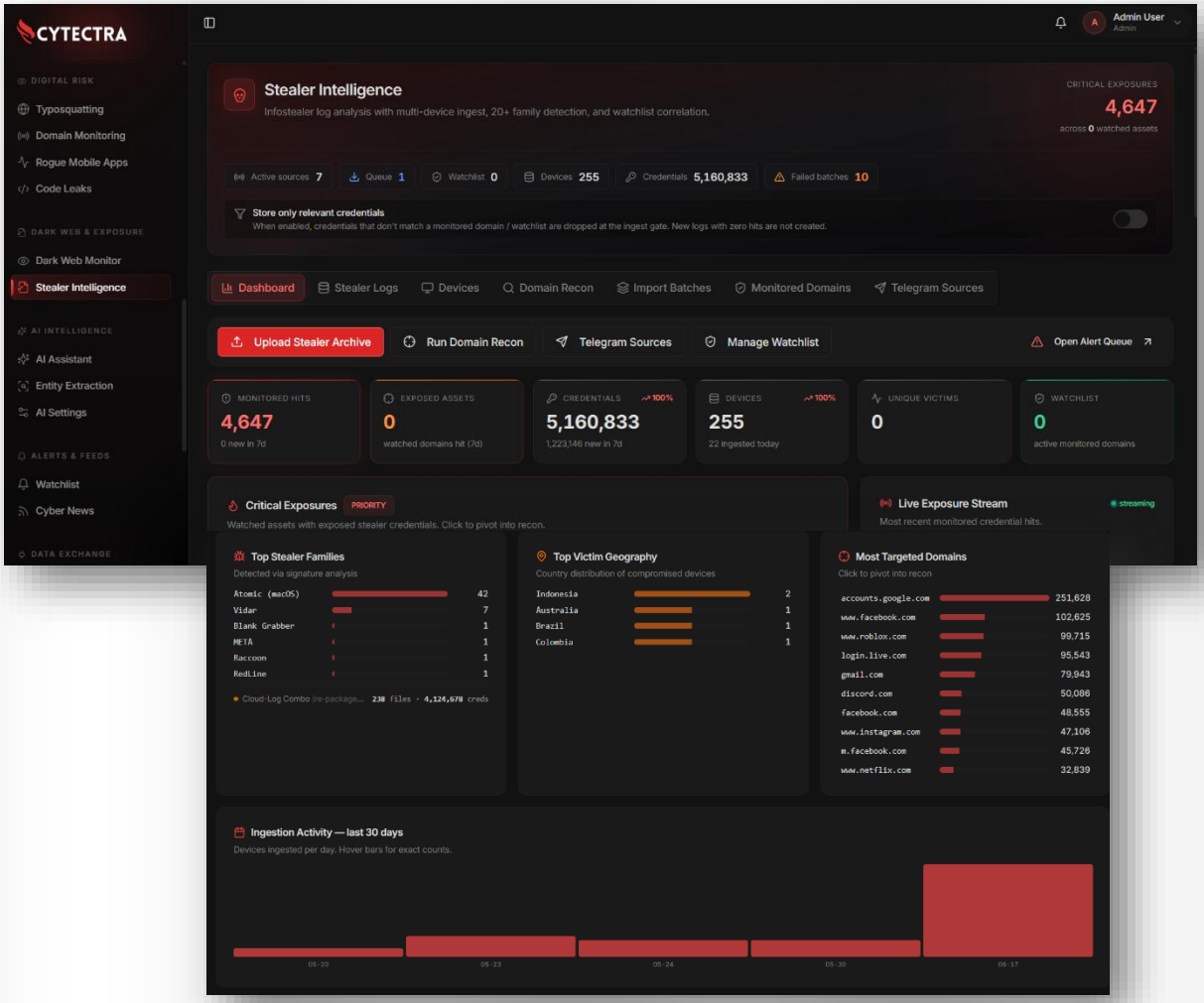


Monitor and analyze software supply chain threats through integrated intelligence from the OpenSSF Malicious Packages database and related enrichment sources. The platform provides deep visibility into malicious open-source packages across major package ecosystems, enabling security teams to detect, investigate, and prioritize supply chain risks more effectively.

- Continuously ingests malicious package intelligence from the OSV.dev API, providing access to trusted open-source vulnerability and malicious package data.
- Supports monitoring across major package repositories including npm, PyPI, RubyGems, Go, Maven, NuGet, crates.io, and additional ecosystems.

- Delivers a centralized dashboard with detailed analytics covering malicious package trends, ecosystem distribution, severity breakdowns, discovery timelines, source attribution, and affected version analysis.
- Performs comprehensive synchronization of all known malicious package records from the OSV database to maintain a complete local intelligence repository.
- Efficiently detects newly published or updated malicious package entries through forward-scanning from the latest known MAL-ID, minimizing bandwidth and synchronization overhead.

Stealer Intelligence



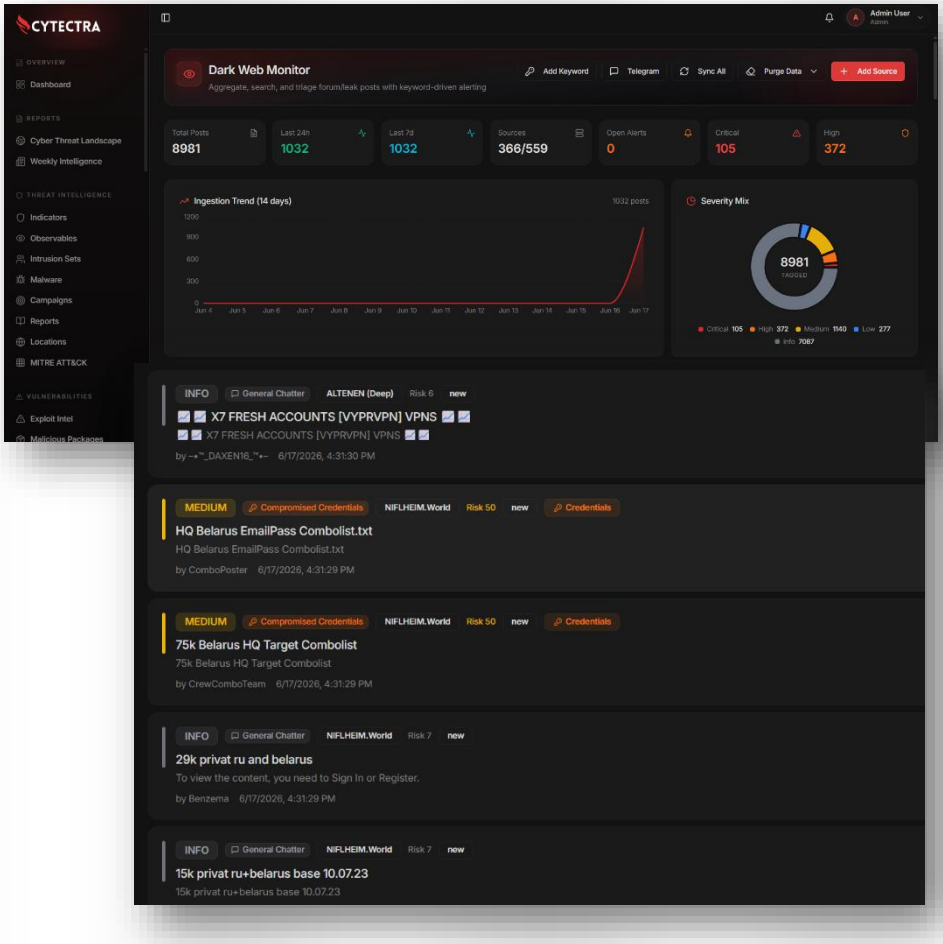
The Stealer Intelligence module enables analysts to identify compromised credentials, devices, and exposed assets from info-stealer logs and cloud-log sources through a centralized reconnaissance dashboard. The platform supports automated ingestion, correlation, and analysis across multiple stealer malware families to accelerate exposure monitoring and threat investigation.

Features

- Support for 20+ stealer malware families.
- Domain-based credential and exposure reconnaissance.
- Manual log and ZIP archive ingestion.

- Telegram cloud-log monitoring and auto-ingest.
- Large-scale archive extraction and parsing.
- Credential, device, and subdomain correlation.
- Import batch tracking and monitoring.
- Detection of leaked combo lists and harvested credentials.

Dark Web Monitoring



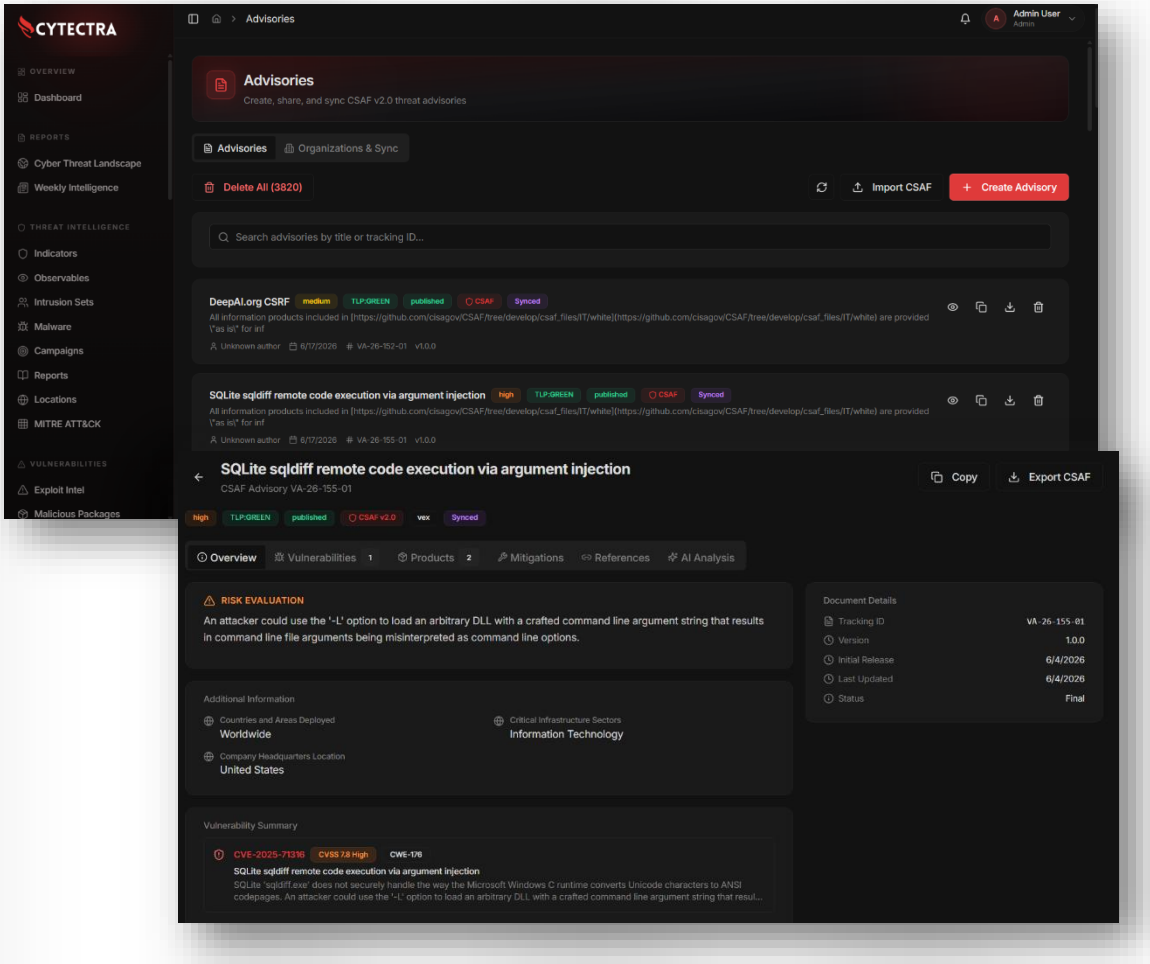
The Dark Web Monitor collects and monitors data from underground forums, marketplaces, leak sites, and Telegram channels to help organizations detect exposed credentials, leaked data, ransomware activity, and brand-related threats from a single platform.

Key Features

- Monitor forums, marketplaces, leak sites, and Telegram channels
- Centralized full-text search across dark web sources
- AI-assisted threat classification and risk scoring
- Keyword watchlists with real-time alerts
- Deep crawling with deduplication and resume support

- False-positive filtering and data validation
- Support for clearnet and Tor-based sources
- Secure access to login-gated forums
- Admin audit logging and bulk management actions

Security Advisory



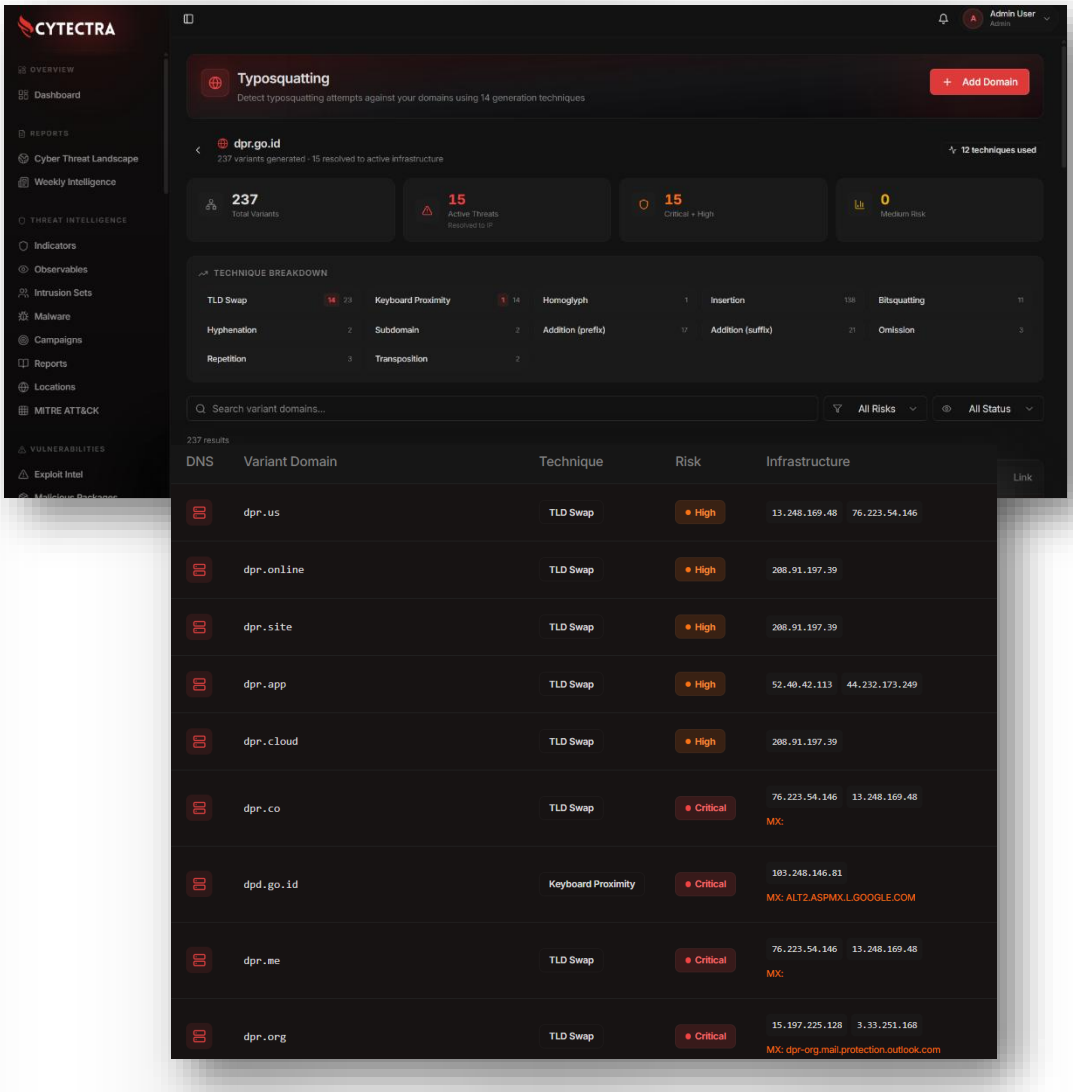
The platform provides centralized Security Advisory Management with full support for industry-standard CSAF v2.0 workflows, enabling organizations to create, publish, import, validate, and synchronize security advisories in a unified environment. Designed for modern CTI and vulnerability management operations, the system streamlines advisory lifecycle management while ensuring compatibility with vendor ecosystems, CERTs, and automated security tooling.

Key capabilities include:

- Centralized security advisory creation and lifecycle management
- Full CSAF v2.0 compliant advisory generation and validation
- Automated CSAF provider feed publishing and distribution

- Import advisories from vendors, CERTs, files, or URLs
- Asset correlation to identify affected systems automatically
- Advisory synchronization with external CSAF providers
- CVE, CVSS, TLP, remediation, and product impact tracking
- Revision history, version control, and de-duplication support

Typosquatting



Typosquatting Detection helps organizations identify malicious domains that imitate legitimate brands using visually or phonetically similar variations. These fake domains are commonly used in phishing campaigns, credential theft, business email compromise (BEC), and malware delivery.

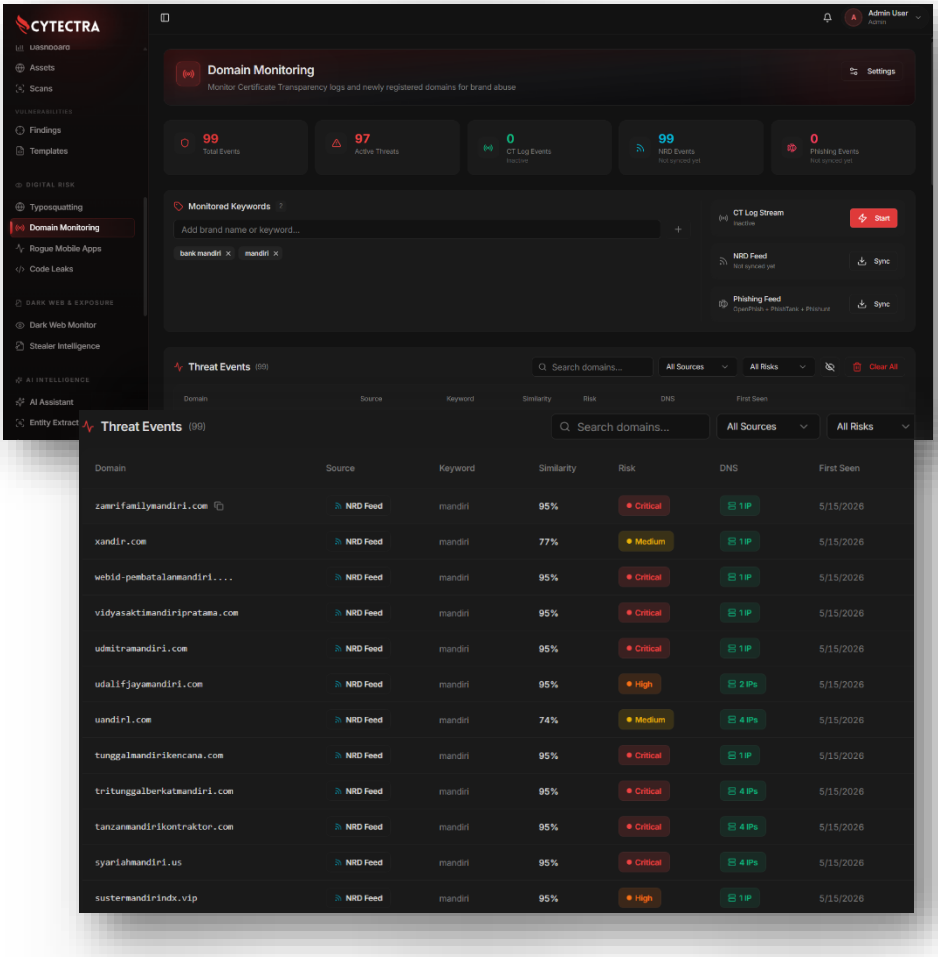
The platform automatically generates and monitors domain variations using multiple typo-generation techniques, performs DNS analysis, and prioritizes risks based on

domain activity and similarity scoring. Security teams can quickly detect suspicious infrastructure targeting their brand before it is used in active attacks.

Features

- Automated typosquatting variant generation using 14 detection techniques
- Detection of phishing-style lookalike and homoglyph domains
- DNS resolution analysis for A, AAAA, MX, and NS records
- Risk scoring based on similarity and active infrastructure
- Identification of potentially malicious mail-enabled domains
- Continuous monitoring for newly active suspicious domains
- Centralized dashboard for investigation and tracking

Domain Monitoring



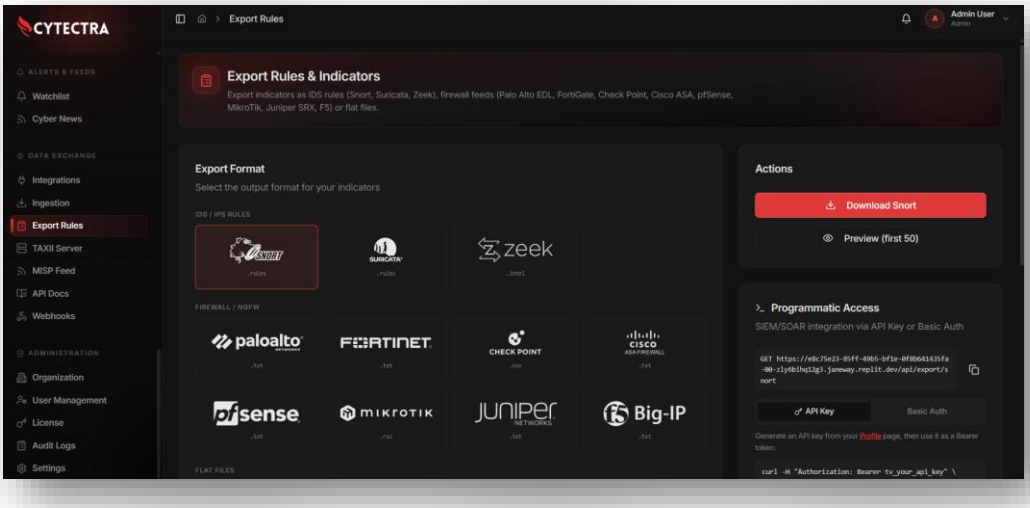
Domain Monitoring continuously tracks newly registered and newly certified domains to detect phishing, typosquatting, and brand impersonation threats targeting your organization. The platform combines Certificate Transparency (CT) logs and Newly Registered Domain (NRD) feeds to provide early visibility into suspicious domains related to your brand.

Key Features

- Real-time CT Log monitoring
- Newly Registered Domain (NRD) detection
- Brand keyword and typosquatting monitoring
- Fuzzy matching with similarity scoring

- Unified threat event dashboard
- DNS activity validation
- Adjustable detection sensitivity
- Event filtering and false-positive management

IDS & Firewall Export



The IDS & Firewall Export module enables security teams to operationalize threat intelligence by exporting indicators directly into IDS, IPS, NGFW, and network security platforms. Indicators can be converted into multiple detection and blocking formats, allowing seamless integration with existing SOC and security infrastructure.

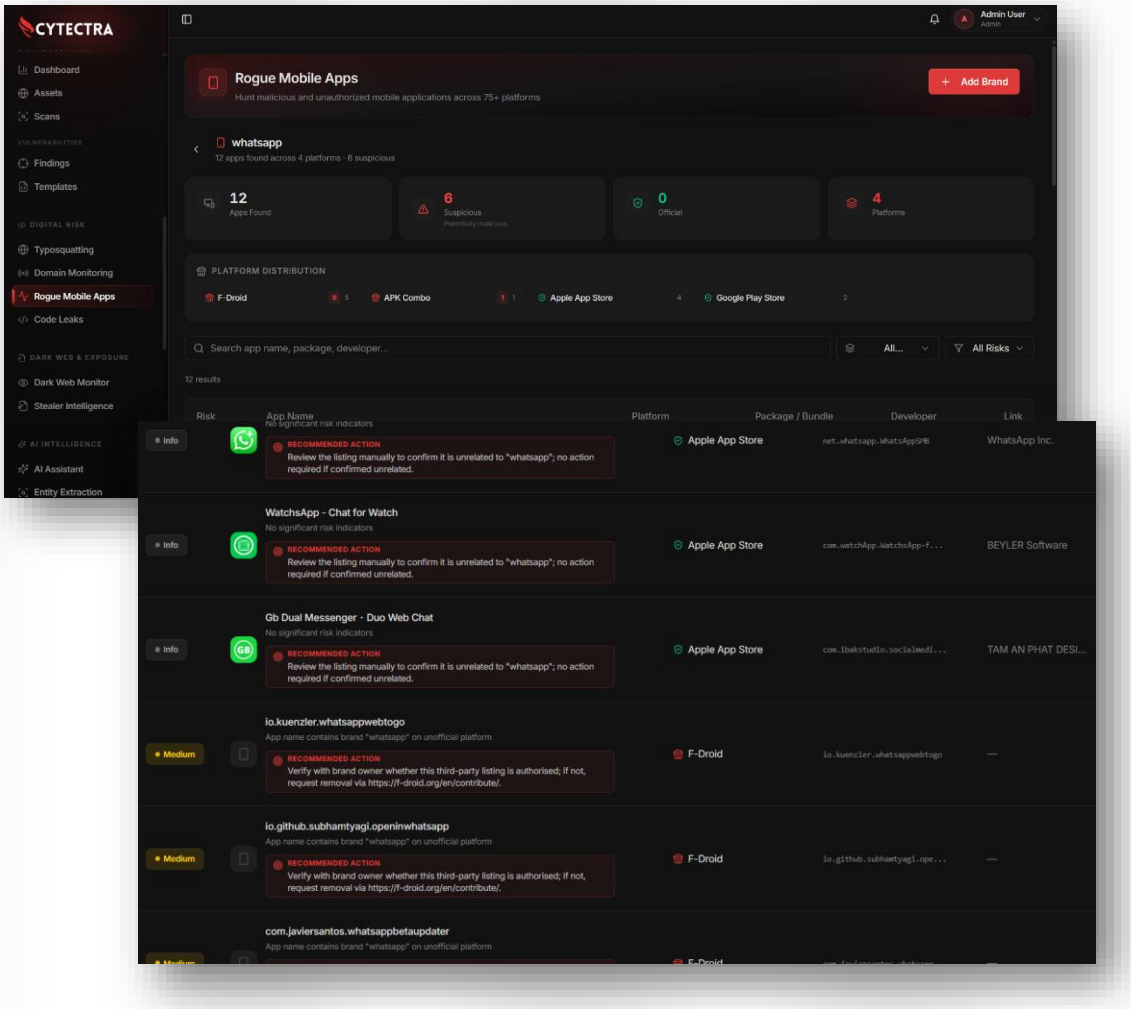
The platform supports automated feed generation, filtering, and stable polling URLs to ensure indicators remain continuously updated across firewalls, detection systems, and security appliances.

Features

- Export indicators to Snort, Suricata, and Zeek/Bro formats
- NGFW and firewall feed support for Palo Alto, FortiGate, Check Point, Cisco, Juniper, MikroTik, F5, pfSense, and OPNsense
- Flat file export in CSV and plain-text formats
- Filter indicators by type, severity, and source
- Custom IDS Signature ID (SID) configuration
- Stable feed URLs for automated firewall synchronization

- Compatible with automated blocklists and threat feed ingestion workflows

Rogue Mobile App



Rogue Mobile App Detection helps organizations identify unauthorized, fake, or malicious mobile applications that impersonate their brand across official app stores, third-party marketplaces, APK hosting sites, forums, and social platforms. The module continuously monitors more than 75+ distribution platforms to detect potential brand abuse, phishing apps, pirated versions, and malware-laced applications.

Detected applications are enriched with package details, developer information, source platform, verification status, and risk scoring to help security teams quickly assess threats and take remediation actions.

Key Features

- Detection of counterfeit and malicious mobile applications
- Monitoring across 75+ official and third-party platforms
- Coverage for Android APK stores and iOS sideload ecosystems
- Risk scoring and official verification analysis
- App metadata visibility (package name, developer, platform)
- Platform and risk-level filtering for investigation
- Manual re-scan for updated threat discovery

System Requirements

This section lists the hardware, operating system, and runtime dependencies needed to run Cytectra. The platform is distributed as a Docker Compose stack so the host only needs Docker every other dependency (Node.js, PostgreSQL, nginx) is bundled inside the official images.

Minimum Requirements

The values below are the floor for a small lab or evaluation deployment serving a single team and a few thousand indicators. Production installs should follow the recommended profile in the next section.

Component	Requirement
Operating System	Linux (Ubuntu 20.04+, Debian 11+, CentOS 8+, or any Docker-compatible OS)
CPU	4 cores
RAM	8 GB
Disk Space	120 GB
Docker	Docker Engine 20.10+ with Docker Compose v2
Network	Internet access for threat feed synchronization

Recommended Requirements (for 100K+ IoCs)

Sized for an active SOC running multiple connectors, dark-web ingestion, weekly Cyber Threat Landscape reports, and the AI Assistant. Increase RAM and storage proportionally as the indicator and stealer-credential corpora grow.

Component	Requirement
CPU	16+ cores

RAM	36+ GB
Disk Space	1+ TB (SSD recommended)
PostgreSQL	14+ (included in Docker deployment)

Software Dependencies

All runtime dependencies ship inside the Docker images so the host only needs Docker Engine and Compose.

- **Node.js**: 20.x (included in Docker image)
- **PostgreSQL**: 16 (included in Docker Compose)
- **Nginx**: Latest Alpine (included in Docker Compose for SSL termination)