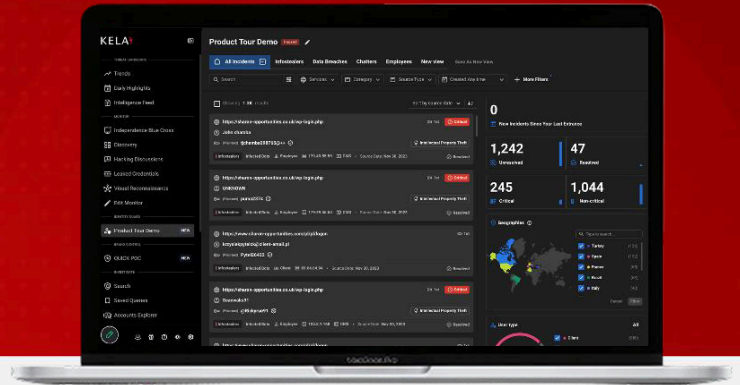


Identity Exposure Monitoring

Billions of credentials compromised globally each year; sold within hours.



Know when a credential tied to your organization's appears in the cybercrime underground, and act **before it is used against you.**

Accurate
Continuous
Anutoomus

Monitor Critical Assets

Domains, IPs & email addresses.

AI Powered Continuous Correlation

Infostealer logs, underground chatter, data breaches, and bot markets.

Direct to Your Stack

Source, infection date, severity & service classification fed directly into your platforms.

✓ Detect exposure before the breach

New compromised accounts matching your assets generate incidents in real time, and retroactive scanning surfaces historical exposure you never knew about.

✓ Incidents worth your time

Choose which source types create incidents, deduplicate repeat appearances, require mandatory credential fields, and auto-suppress irrelevant results.

✓ Context that speeds triage

Incidents arrive pre-classified: service name and category (VPN, SSO, remote desktop, and more), the cyber threat posed, severity, and user type (employee, client, external) by rules you define.

✓ Built into your response stack

Push incidents to Slack, Teams, PagerDuty, or any webhook, and drive remediation workflows through a RESTful API covering incident search, editing, and bot takedown operations.

◆ Anticipate Threats

◆ Act with Precision

◆ Avoid the Attack

How it Works

1 Define your assets

Self-service setup of domains (IDN supported), SaaS domains, single IPs, and email addresses, manually or in bulk via CSV.

The platform suggests related subdomains and IPs from KELA's data lake.

2 Correlation runs continuously

Assets are matched against compromised accounts from five configurable source types: infostealer data, session cookies, underground chatter, data breaches, and market bots.

Matching runs in real time and retroactively across up to 2 years of historical data.

3 Incidents arrive classified

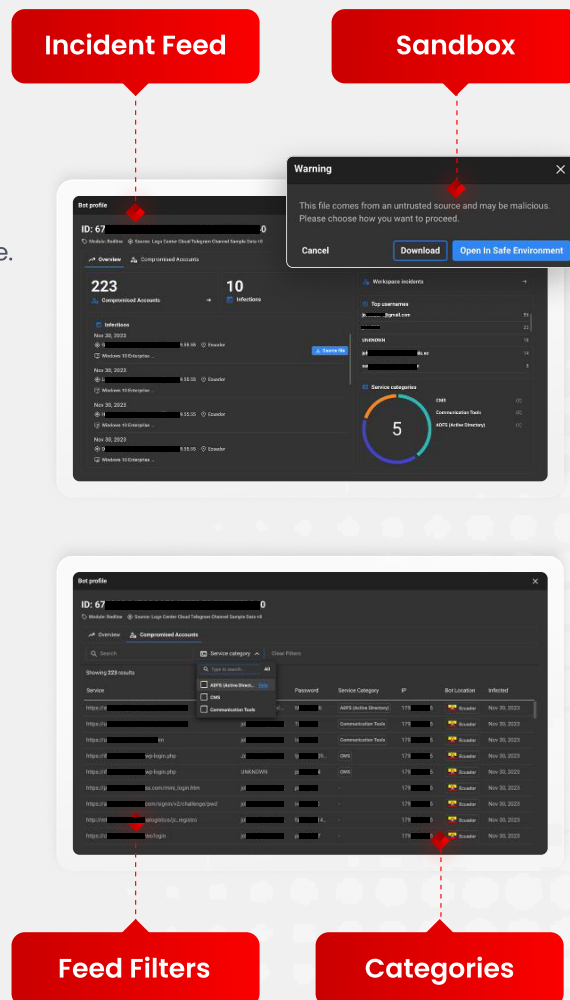
Each incident carries the credential, source, bot context, severity, and first-versus-recurring detection.

Playbooks auto-classify critical services; Cookies Pivot links accounts to related cookie incidents.

4 You act, at scale

Advanced search (including regex) pinpoints incidents by hostname, username, or password pattern.

Automations classify, suppress noise, and notify via playbooks or the API, including bot takedown requests.



Use Cases

Employee account takeover

From learning of compromised employee credentials only after abuse, to resetting them within minutes of the credential appearing in an infostealer log.

Exposed access to critical services

From VPN, SSO, and remote desktop credentials circulating unseen in underground markets, to auto-classified critical incidents naming the exact service at risk.

Customer account fraud

From fraud discovered at chargeback time, to client-type incidents flagged by your own classification rules and routed to the fraud team automatically.

Session hijacking via stolen cookies

From stolen session cookies bypassing MFA invisibly, to cookie incidents flagged with an indicator showing whether the session is still live.

Features

✓ Source Coverage

Five configurable source types: Infostealer logs, session cookies, underground chatter, data breaches, and market bots. Enable or disable each per workspace.

✓ Cookies Pivot

Session cookies linked to accounts: Pivot from a compromised account to its related cookie incidents and see whether they are still active (where licensed). Session cookies bypass MFA and passkeys.

✓ Retroactive Scanning

2 year rolling archive: Real-time monitoring plus retroactive scanning across up to 2 years of historical data, surfacing exposure that predates your monitoring.

✓ Service Classification

Critical services flagged automatically: Okta, Citrix, Fortinet, Palo Alto, Microsoft ADFS, Salesforce and dozens more auto-classified and defaulted to critical severity.

✓ Noise Controls

Refine and optimize: Deduplication, mandatory-field rules, first-versus-recurring configuration, and auto-suppression keep the feed to incidents worth acting on.

✓ Bot View & Safe Environment

Evidence without the risk. Raw bot evidence opens in-platform; files open for forensic inspection in a disposable virtual machine that never touches your endpoint.

✓ API & Administration

Automate at scale: RESTful JSON API for incident search and editing, bot alerts and takedown, and workspace management; multi-workspace with group-based permissions.

✓ Integrations

Into your response stack: Push incidents to Slack, Microsoft Teams, PagerDuty, or any webhook endpoint through playbook automations.

✓ Advanced Search

Regex-grade incident hunting: Multi-condition queries across hostname, path, username, and password, with standard operators and full regex support.

✓ Licensing & Deployment

Module of the KELA platform with self-service setup. Licensed by workspace, monitored-asset quotas with retroactive scanning.

