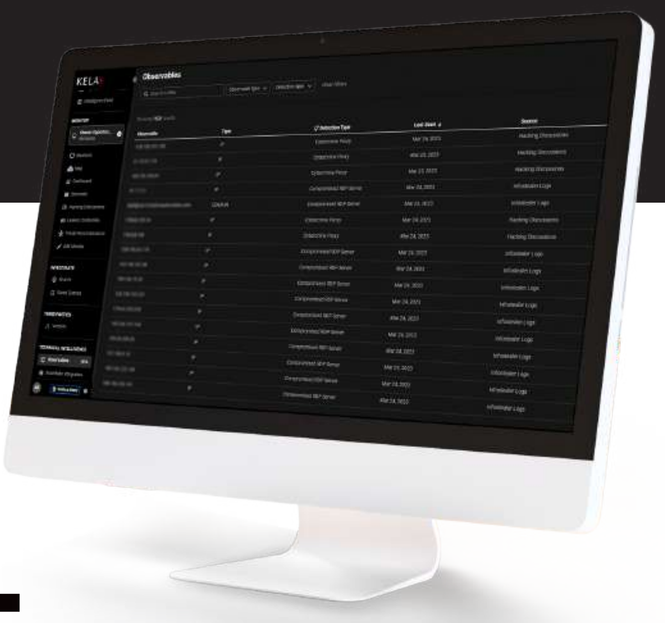
DATASHEET

KELA



TECHNICAL INTELLIGENCE

Detect suspicious IPs and domains involved in cybercrime activities.

OVERVIEW

KELA's Intelligence is collected through automated detection of potentially compromised IPs and domains involved in cybercrime activity. Our sources include closed forums, illicit markets, automated cybercrime shops, instant messaging channels used by criminals, and more. This intelligence is available to consume via KELA's or Snowflake's API as a machine-readable feed and can be easily integrated into your security appliances.

Use KELA's Technical Intelligence module to monitor the latest compromised network assets that can be exploited by threat actors for their next cyber attack. Such assets can be abused to serve as an attack infrastructure (for example, as a C2 server) or as an attack vector such as phishing attacks.

HOW IT WORKS

Collect Data
KELA's automated cyber intelligence technology continuously collects posts, images, and other information in various formats from the cybercrime underground.

Analyze and Extract
The collected data is analyzed to detect potentially compromised assets based on context and source credibility, resulting in an output of indicators, including IP addresses and domains.

Normalize Data
The detected assets, their context, and MRTI properties, such as STIX, are shared with the users via KELA's or Snowflake's API in a structured, machine-readable format.

Build Proactive Defense
Leveraging KELA's Technical Intelligence to monitor or block access to detected compromised assets empowers users to remediate potential risks proactively.

USE CASES

✓

Actionable Threat Intelligence

Use KELA's Technical Intelligence to get actionable cybercrime threat intelligence and protect your organization against compromised network infrastructure that can be exploited by malicious threat actors.

✓

Improved Threat Hunting Capabilities

Leverage KELA's Technical Intelligence to support your investigation and improve your organization's threat-hunting capabilities.

BENEFITS

Seamless Integration
Easily integrate KELA's machine-readable Technical Intelligence into your SIEM, SOAR, or any other security solution, by using the STIX format or any other available fields.

Real-time Updates
Protect your organization by getting real-time updates on compromised IPs and domains mentioned in cybercrime activity. Stay ahead of potential attacks by taking proactive countermeasures.

Comprehensive Coverage
KELA's real-time Technical Intelligence includes information from a wide range of cybercrime underground sources, ensuring that you have access to the most up-to-date and relevant intelligence on cyber threats.

Contextualize Intelligence
Learn more about each threat by gaining a deeper understanding of the intelligence source and how the asset was compromised.

KELA www.ke-la.com / info@ke-la.com / +972-3-970-2720