# **IDENTITY**

## **GUARD**



## YOUR ULTIMATE DEFENSE AGAINST **COMPROMISED CREDENTIALS**

The emergence of compromised accounts sourced from the cybercrime underground, and the ever-present threat of unauthorized access to locally stored data or cloud services, poses a constant and escalating threat to businesses of all sizes.

These accounts can serve as gateways for malicious actors to infiltrate your network, steal sensitive data, and cause great damage.

KELA proudly presents Identity Guard, a cutting-edge module designed to safeguard your digital ecosystem and attack surface as well as enhance the security of your company's accounts across external cloud service providers.

proactively monitor your digital assets, detect compromised accounts, and take swift action.

Whether you're a multinational corporation or a small startup, our solution empowers you to

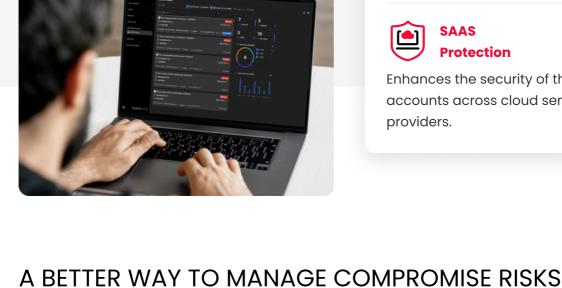
Setting up and using Identity Guard is a breeze, providing immediate, actionable insights, categorized by severity and immediate customizable alerts to protect your company's data and ensure the security of your assets. Additionally, Identity Guard seamlessly integrates with your existing security tooling, streamlining your cybersecurity infrastructure and enhancing its effectiveness.



## **IDENTITY GUARD**

#### Your Real-Time Solution for Proactive **Compromised Account Protection**

KELA's Identity Guard module efficiently identifies compromised accounts related to an organization's digital assets, including domains, subdomains, and third-party SaaS accounts. It seamlessly integrates with existing security tooling, automating the identification of compromised accounts and infected machines. This automation simplifies data analysis and enables prompt actions. Despite a vast dataset of over ten million bots and three hundred million compromised accounts, Identity Guard delivers focused, actionable insights, where stakeholders receive real-time alerts through customizable webhooks, ensuring efficient threat response and communication.



#### **KEY FEATURES & BENEFITS**



## **Simplified Self-Service**

Offers tailored value and capabilities designed to meet the organization's specific needs due to the intuitive and straightforward setup process.



### Classification

**Severity-Based** 

Includes automatic severity classification for compromised accounts, ensuring smart prioritization & resource allocation to allow for timely remediation efforts.



#### **Webhook Automation** Eliminates the need for complex

**Streamlined** 

integrations, enabling effortless communication between the module, internal teams, and applications. Facilitates seamless initiation of a wide range of workflows through intuitive playbook setup.



#### **Protection** Enhances the security of the company's

accounts across cloud service

providers.

#### Tailored to the Needs of **Efficient**



Ω

圁

#### Streamlined Set-Up and Onboarding **Experience:** Simplifies onboarding process with assets suggestions,

**Organizations of All Sizes** 

facilitating prompt remedial actions in response to detected threats and security incidents. **Effortless Monitoring:** Enables even smaller security teams to effectively monitor and mitigate compromised

accounts. Intuitive Filters: The user-friendly interface allows for the configuration of advanced filters based on severity categories, threat types, third-party

providers, service categories, and more.



#### **Feed of Detected Compromised Accounts:** Provides criticality levels and updatable status (Resolved/

Workspace

Unresolved). Clear Visualization: Presents visual

statistics segmented by selected filters

in a concise and digestible manner, facilitating effective action based on insights. **Advanced Context:** Each result provides information on the associated service

the discovery. Flexible Ticket Tracking: allows users to filter tickets by resolution status for reference and future audits. Past

incidents can be easily retrieved and

and the precise threat associated with

reviewed when necessary.

## Timely Notifications: Configure granular

**Seamless Integration for** 

**Effortless Communication** 

and timely alerts setting up intuitive playbook-triggered webhooks for critical events and urgent updates.

**Effortless Integration:** Simplify complex integrations with webhook automation, allowing you to create unlimited playbooks with straightforward rules to initiate workflows across various endpoint applications such as Slack and

## module facilitates the identification and

## prioritization of relevant data based on

**Optimize Data Handling** 

and Respond Instantly

Focus on Relevant Data only: The

severity and chosen filters. By highlighting critical information within the module and sending advanced alerts to relevant recipients, it helps security teams focus their efforts on the most impactful areas for efficient remediation. Actionability: Provides focused and specific insights.

**Real-time Alerting:** Sends immediate

webhook-based alerts ensuring timely response. **Instant Automated Reactions:** 

internal security systems.

Activates remediation workflows on any

www.kelacyber.com • marketing@ke-la.com • +972-3-970-2720

Copyright© 2023 KELA