This document provides accurate information about Kolide's K2 product for the purposes of proving assertions made in a SOC 2 Type II audit.

Using Kolide (K2) for Anti-Virus / Anti-Malware

Detection Capabilities

Kolide utilizes an endpoint agent named "Launcher" to power its detection capabilities. This agent and all of its dependencies are open-source (https://github.com/kolide/launcher).

This agent is capable of collecting detailed information from macOS, Windows, Debian-Based Linux (Ubuntu), and RPM-Based Linux Devices (CentOS, RHEL).

Under the hood, Kolide's agent primarily utilizes osquery which has the following detection capabilities:

- Signature Based Detection
- Broad Device Property Data Collection
- Real-Time File Integrity Monitoring
- Real-Time Process Event Monitoring

Artifacts / Data Collected For Analysis In Kolide's Cloud

Kolide's agent regularly collects and transmits a detailed inventory from devices useful for malware and virus detection. Kolide augments this information with third party data sources to increase the confidence in the alerts it emits.

Using this cloud based analysis, Kolide can perform computationally heavy detection operations on data without impacting device performance, even when the devices are not online. Kolide can also consider the "rarity" of artifacts based on the data collected from other devices across an organization.

The information collected includes:

1. "**Installables**" - Applications, Programs, Packages, Browser Extensions, and other executables.

2. “**Persistence Mechanisms**” - Login Items, Startup Items, LaunchD Entries, Registry Keys, App Compatibility Shims, Crontab entries, and other mechanisms malware use to persistent themselves in a device.

3. “**Network Indicators**” - Listening Ports /etc/hosts entries, APR Cache entries, etc.

4. “**Settings & Logs**” - Artifacts that enable us to determine if a device has been compromised by either malware or human actors regardless of variants (hidden users created, passwordless sudo access granted, etc)

Interaction With Other Anti-Virus Agents

On macOS, Kolide is capable of interacting directly with XProtect, macOS’s default signature based anti-virus solution, and will expose any finding reported locally to an end-user to the administrators of our product.

At a customer’s request, Kolide is also capable of interacting with other A/V vendors to create a single pane of glass for all anti-virus based alerting.

Scanning Frequency

Kolide runs its signature based detection on a custom schedule per signature. While some information may be queried in real-time, other longer queries (such as verifying all applications signatures) can be run once every 2 hours.

These scans occur regardless of whether the device has internet access or not, and results are queued in a local datastore to be transmitted when the device is connected.

Alerting Capabilities and Remediation

Kolide is capable of alerting administrators to problems as it detects them in real-time. In addition, Kolide is also capable of associating the primary users of a device to employer’s identity providers such as Slack and GSuite.

At the administrator’s discretion, Kolide can communicate directly with end-users over a chat solution (eg Slack) and provide step by step instructions to help them resolve security issues discovered on their device.

End-users can verify in real-time that they have completed the instructions correctly and accurately. All remediations including self-service remediations are tracked in the administrative UI.

Updates & Distribution

Kolide agents are directly connected to Kolide's SaaS product and can function in a zero-trust environment (No VPN required). When a device is online, these agents check in approximately every few seconds to report the results of any recent queries, and to download the latest set of signatures and queries.

Kolide releases new signatures and retires older signatures continuously for all customers. As soon as a new signature is created and tested, it is rolled out to Kolide's customers instantly and adjusted and fine-tuned in real time.

Kolide's agent is also capable of automatically updating itself without any end-user interaction. Like the rest of its agent, this code for this process is open-source. Additionally, this capability has been thoroughly vetted by a third party (NCC Group).