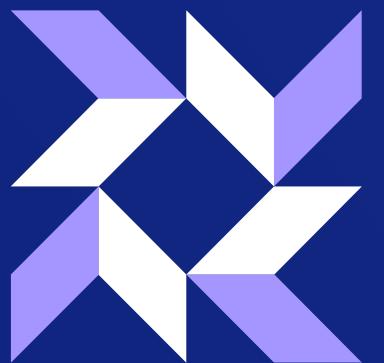




+



User Focused Security w/ Osquery

Querycon 2019



Jason Meller
Cofounder & CEO

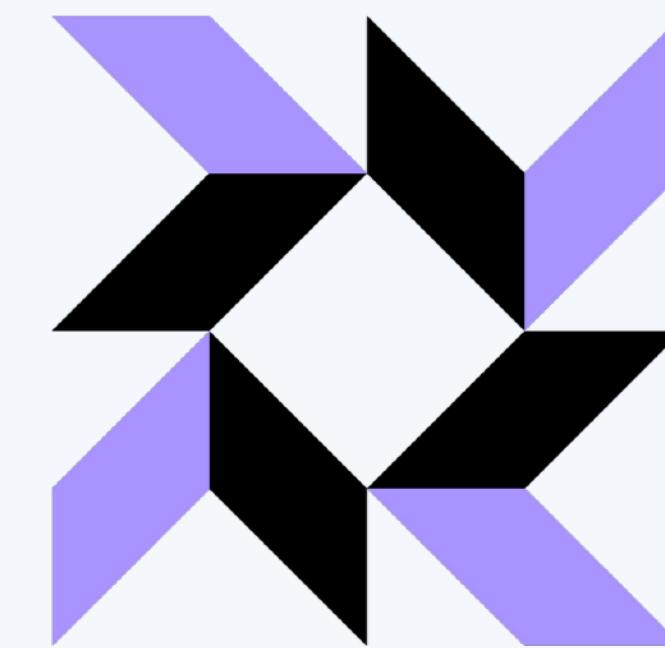
Thank You Trail of Bits

Who Am I?

- Cofounder & CEO of Kolide.
- Cyber Security Intelligence Analyst (GE, Mandiant, FireEye)
- IT Admin/Support (University of Connecticut)
- Software Engineer (Web applications)

About Kolide

Kolide is a security focused infrastructure analytics company. We specialize in collecting and analyzing data from your organization's devices to deliver actionable insights through a thoughtful user experience. We answer all of your infrastructure questions, especially the ones you didn't think to ask.



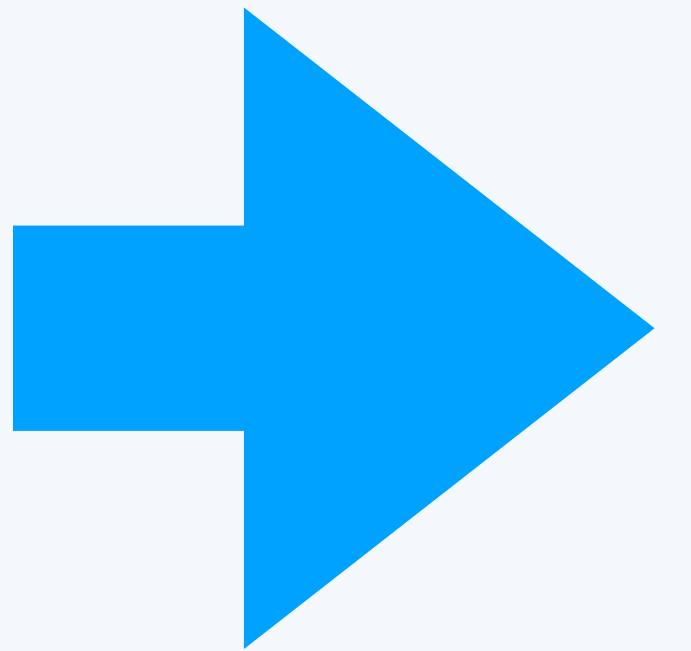
What Are The Questions?

- Incident Response
- Threat Hunting
- Operations
- Business Risk
- Compliance

What Are The Questions?

Typical Compliance Seeker

- 10 - 10,000 employees
- Sells B2B or B2C software
- Lots of Engineers / Macs
- Some Windows and Linux
- International Presence



“Fast Growing High-Tech Companies”

The Culture of Fast Growing High-Tech Companies



Seven Aspects of our Culture

- Values are what we Value
- High Performance
- Freedom & Responsibility
- Context, not Control
- Highly Aligned, Loosely Coupled
- Pay Top of Market
- Promotions & De



Basecamp

Our core values

These are some of the values we live by, as a company. We work by them, too: we're building a platform and products we believe in — knowing there is real value to be gained from helping people, wherever they are, simplify whatever it is that they do and bring more of themselves to their work.

❤️ Empathy

👤 Courtesy

🔨 Craftsmanship

🎭 Playfulness

Solidarity

What We Stand For

Values

Before anything else, values come first. Without clear, shared values, we wander independently and contradict one another. Everything's harder when we all believe different things about what's important to *us*, our company.

Key values:

- Be Straightforward. Whenever we speak - internally or externally - we should speak plainly and clearly. Watch out for lingo, assumptions, exaggeration, or other things that get in the way of a straightforward explanation. This doesn't mean we strip the poetry and personal expression from our language, but it's got to make sense. With the

The Inspiration - Lockheed Martin Skunk Works

“Kelly” Johnson’s R&D Engineering Corps for Advanced Aircrafts.
Responsible for the U2, SR-71, F-117, F-22, and F-35 aircrafts.

Credited for formalizing what we call “rapid prototyping”

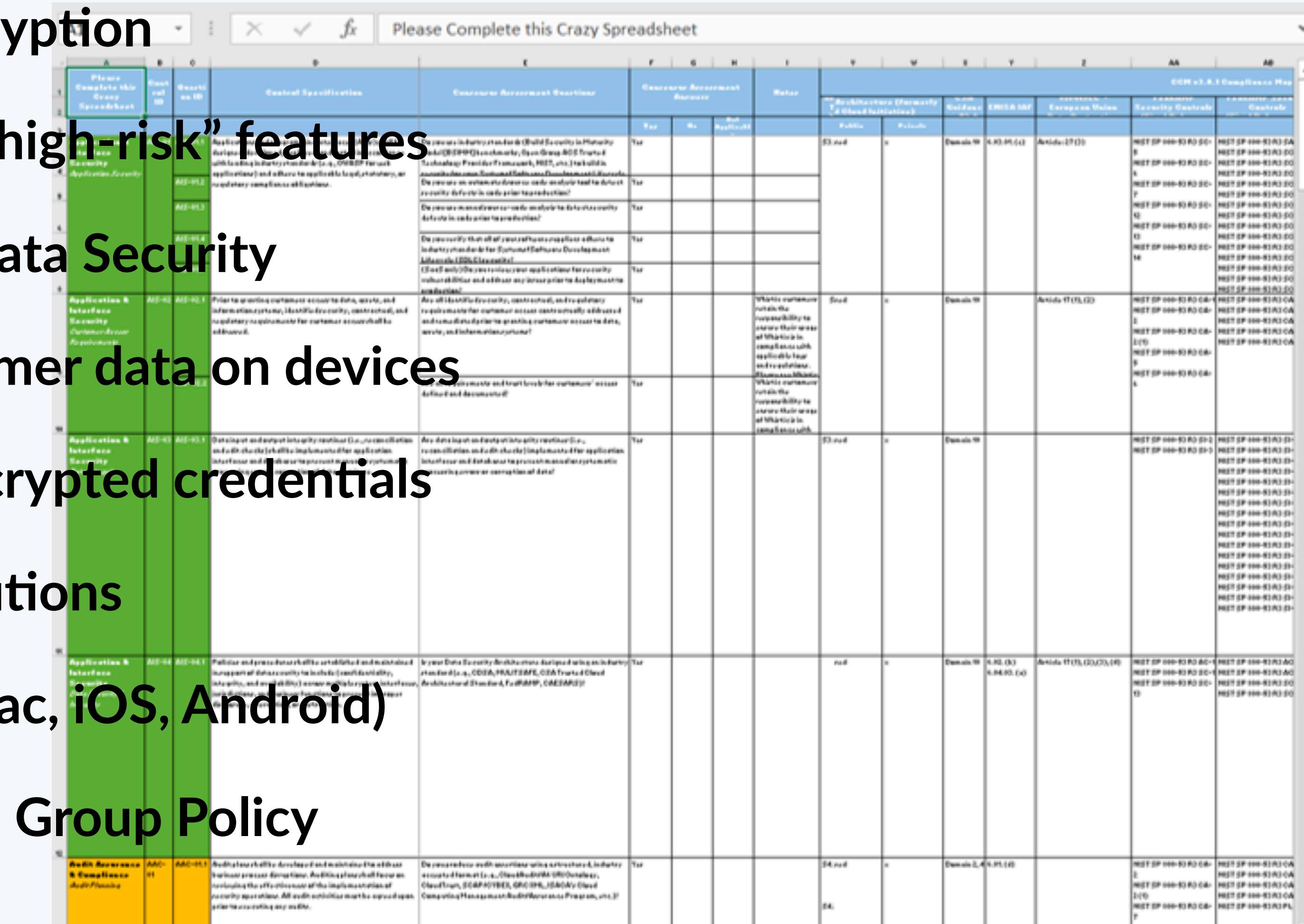
Kelly's 14 Rules The Key Themes

- A timely wrong decision is better than no decision
- Go with the decision of the engineer in-situ over a non-present authority.
- Mutual trust between the people doing the work and the benefactors of that work.



The First Obstacle...

- # • Device Security The Dreaded Vendor Security Assessment







*Preserve our
important culture*



The Solution? Lock It Down!

Achieve complete compliance across known devices with the click of a button.

Programmed for one-click compliance

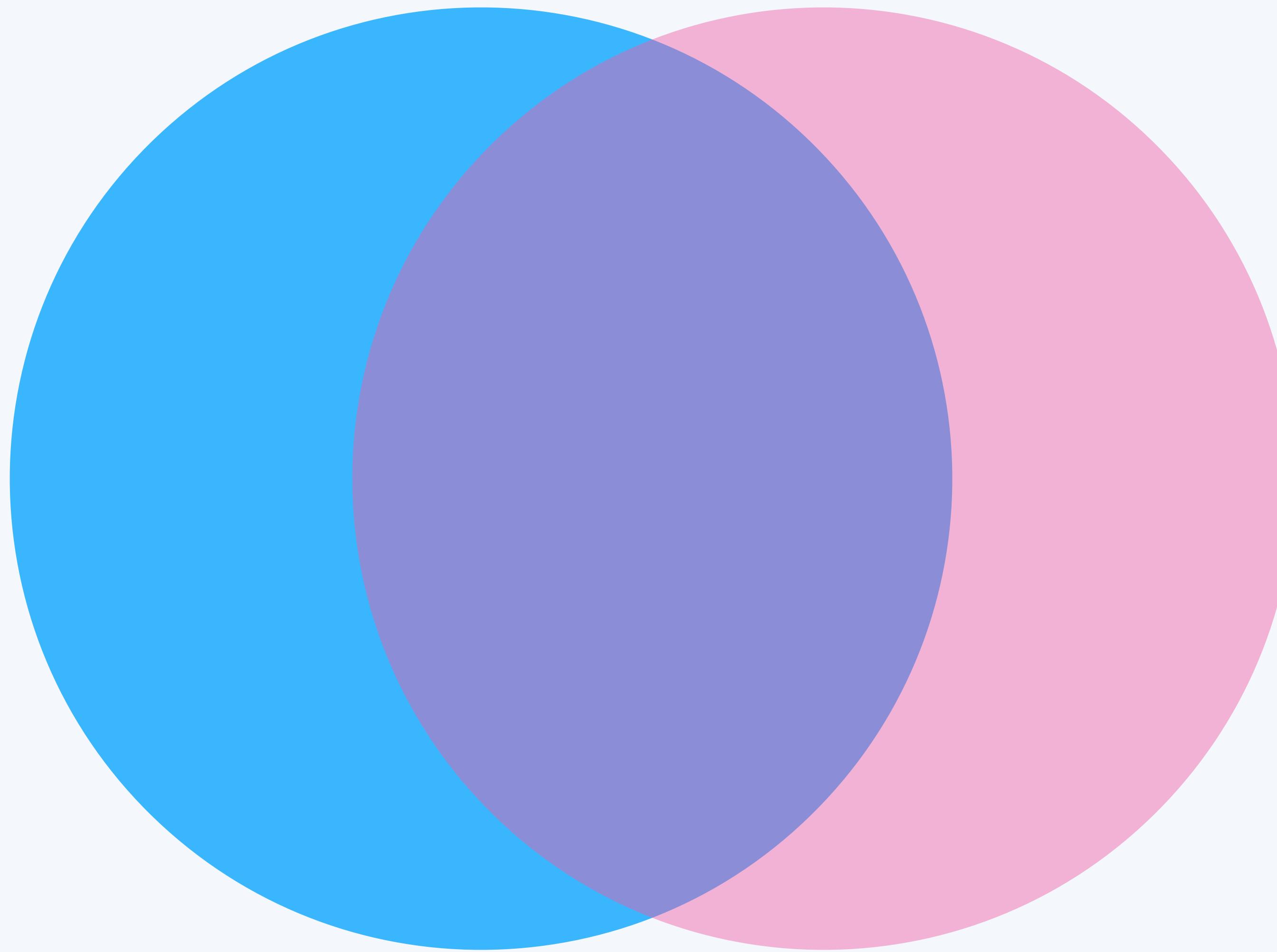
No more questioning or worrying about missing audit trails. Kandji is built to ensure your company or organization adheres to complex governmental and other regulatory standards, including CIS, HIPAA, NIST and FedRAMP.

The screenshot shows a software interface for managing device compliance blueprints. At the top, there's a button labeled '+ NEW BLUEPRINT'. Below it, there are two main sections: 'KANDJI' and 'CIS'. Under 'KANDJI', there are four items: 'Kandji Level I', 'Kandji Level II', 'Kandji Level III', and 'Kandji Level IV'. Under 'CIS', there are two items: 'CIS Level 1 Scored' and 'CIS Level 2 Scored', with 'CIS Level 2 Scored' being highlighted. To the right, a detailed view of the 'CIS Level 2 Scored' blueprint is shown. It features a red circular icon with a padlock symbol. The title 'CIS LEVEL 2 SCORED' is displayed above a section for 'Parameters Enabled' which shows a score of '78'. A progress bar indicates the 'Restriction Rating'. Below this, a 'DESCRIPTION' section provides information about CIS Level 1 and Level 2 Scored parameters. At the bottom right of the blueprint view is a 'CREATE BLUEPRINT' button.



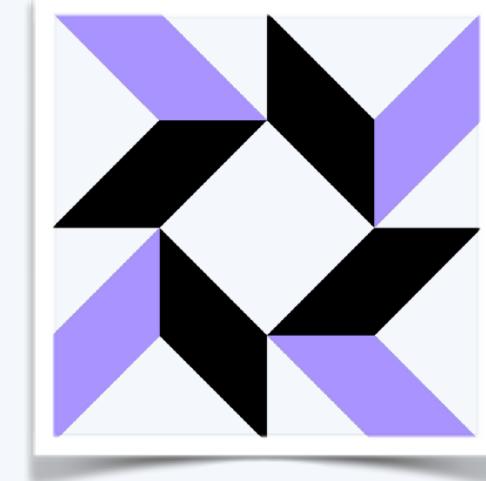
Device Management Capabilities

What is considered “Compliant”



The Solution? **Surveillance** Endpoint “Visibility”

Become “All Knowing” by deploying an endpoint agent and log everything



SELECT * FROM...

account_policy_data
acpi_tables
ad_config
alf
alf_exceptions
alf_explicit_auths
alf_services
app_schemes
apps
apt_sources
arp_cache
asl
augeas
authorization_mechanisms
authorizations
authorized_keys
block_devices

docker_container_mounts
docker_container_networks
docker_container_ports
docker_container_processes
docker_container_stats
docker_containers
docker_image_labels
docker_images
docker_info
docker_network_labels
docker_networks
docker_version
docker_volume_labels
docker_volumes
etc_hosts
etc_protocols
etc_services

keychain_items
known_hosts
last
launchd
launchd_overrides
listening_ports
load_average
logged_in_users
magic
managed_policies
mdfind
memory_devices
mounts
nfs_shares
nvram
opera_extensions
os_version

prometheus_metrics
python_packages
quicklook_cache
routes
safari_extensions
sandboxes
shared_folders
sharing_preferences
shell_history
signature
sip_config
smbios_tables
smc_keys
startup_items
sudoers
suid_bin
system_controls



The Hidden Costs Of Heavy Surveillance + Lock It Down

Sure you are “compliant” but...



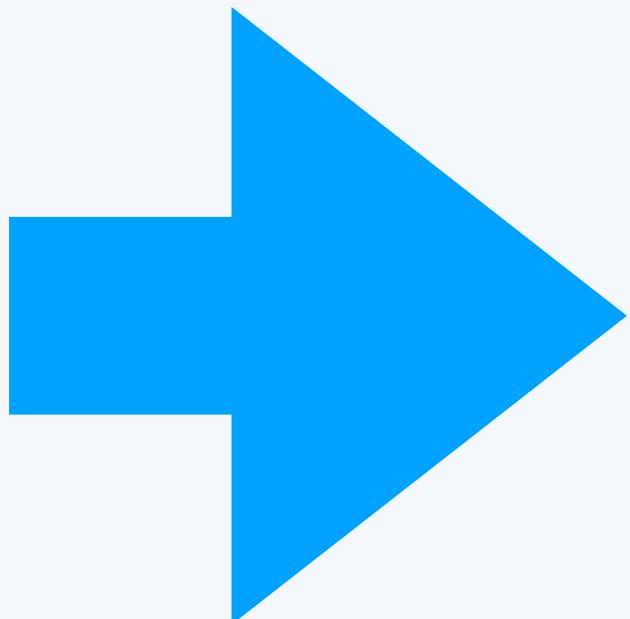
- You are signaling you no longer trust your employees to manage their devices.
- You are blocking your most productive staff from getting work done.
- You are pushing your employees to do work on personal devices.

There Must Be Another Way!

Let's design a system around our values

Our Values

- Transparency / Accountability
- Education / Personal Growth
- Personal Responsibility



Key System Traits

- User Education Over Enforcement.
- Trust Staff To Do What Is Right, But Verify They Did It.
- Respect For Personal Privacy Of Staff & Their Loved Ones.
- Transparent Monitoring That Explains The “What” and the “Why”.

Our Requirements

- Keep our Customer's Data Secure
- Protect Our Intellectual IP
- Pass Required Audits

User Focused Security

User Focused Security

The notion of “User Focused Security” **acknowledges that attacks against corporate users** (e.g., phishing, malware) are **the primary mechanism leading to security incidents and data breaches**, and it’s one of the core principles driving our approach to corporate information security. It’s also **reflective of our philosophy that tools are only effective when they consider the true context of people’s work.**

<https://medium.com/netflix-techblog/introducing-netflix-stethoscope-5f3c392368e3>

Generating Our Technical Requirements

Key System Traits

- User Education Over Enforcement
- Trust Users To Do What Is Right, But Verify It.
- Respect For Personal Privacy Of Users & Their Loved Ones
- Transparent Monitoring that explains the “what” and the “why”

Technical Requirement Checklist

- Accurate** information about devices and people.
- An **actionable** communication medium to reach users.
- Rationale around endpoint** collection that is visible to end-users
- A system to **measure compliance** and **document remediation**

Generating Our Technical Requirements

Technical Requirement Checklist

- Accurate** information about devices and people.
- An **actionable** communication medium to reach users.
- Rationale around endpoint** collection that is visible to end-users
- A system to **measure compliance** and **document remediation**

We should rely on existing solutions to meet these requirements

Requires custom engineering to meet your exact business requirements

Accurate Information About Devices & People

Osquery

Pros: Multi-platform, open source, lots of useful data relevant to our goals, written in C++ so it's "fast".

Cons:

Very easy for a novice to **absolutely wreck** the perf of systems with too many expensive queries.

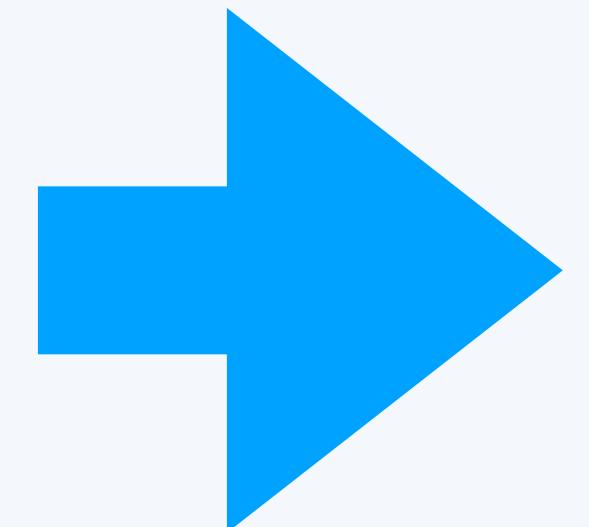
Data accuracy is sometimes a problem

ex: encryption status of SSH keys

Capable of collecting a lot of **personal data** that is out of scope for our needs.

User has limited visibility that it is installed.

Osquery **does not capture all the data we need** for successful User Focused Security.



Conclusion:

Nothing else comes close to our needs, so let's mitigate the problems.

Osquery Problem Mitigations



Kolide Launcher

Open Source Osquery Manager that extends its functionality (fixes data quality issues).



Integrate External Sources

Other systems, like MDM and identity providers can provide valuable context



Auditing & Visibility

Onboarding flow that introduces user focused security, and visibility into what is being collected

An actionable communication medium to reach users

Email

Pros: Everyone has it

Cons:

- Nobody reads it
- Hard to make actionable



Desktop App

Pros: Customized to your exact needs

Cons:

- Requires installation
- Multi-platform is tough



The screenshot shows the Stethoscope application window (version v3.0.1) running on a MacBook Pro. The top bar displays the device information: "MacBook Pro \"Core i7\" 3.1 15\" Touch/Mid-2017 nfm1-Y4H". The main area is titled "Pros:" and lists a single item: "This device is properly configured" with a green checkmark. Below this, under "Stethoscope baseline policy", there is a bulleted list: "People still read it" (with a green checkmark), "System is up-to-date", "Your Firewall is enabled" (with a green checkmark), "Disk Encryption is enabled" (with a green checkmark), "Screen Lock is enabled" (with a green checkmark), "Screen will lock when system is idle for too long" (with a green checkmark), "Automatic Updates are enabled" (with a green checkmark), and "Remote Login is disabled" (with a green checkmark). At the bottom of the window, there is a note: "Last scanned by Stethoscope a few seconds ago" and a thinking emoji icon. A "rescan" button is located at the bottom left.

An actionable communication medium to reach users

Keys To Success With Slack

- Use an App/Bot, not webhooks.
- Do not annoy your staff, at most ping them once a day.
- Allow users to interact with the app by issuing it commands to get their latest status
- Give users the tools to fix problems
- Provide escalation paths
- Use it to distribute dependencies

terracatta 5:57 PM
devices

Kolide APP 5:57 PM
Name: jasons-laptop

Model: MacBook Pro (15-inch, 2017) Serial: C02VDF5EHTD6

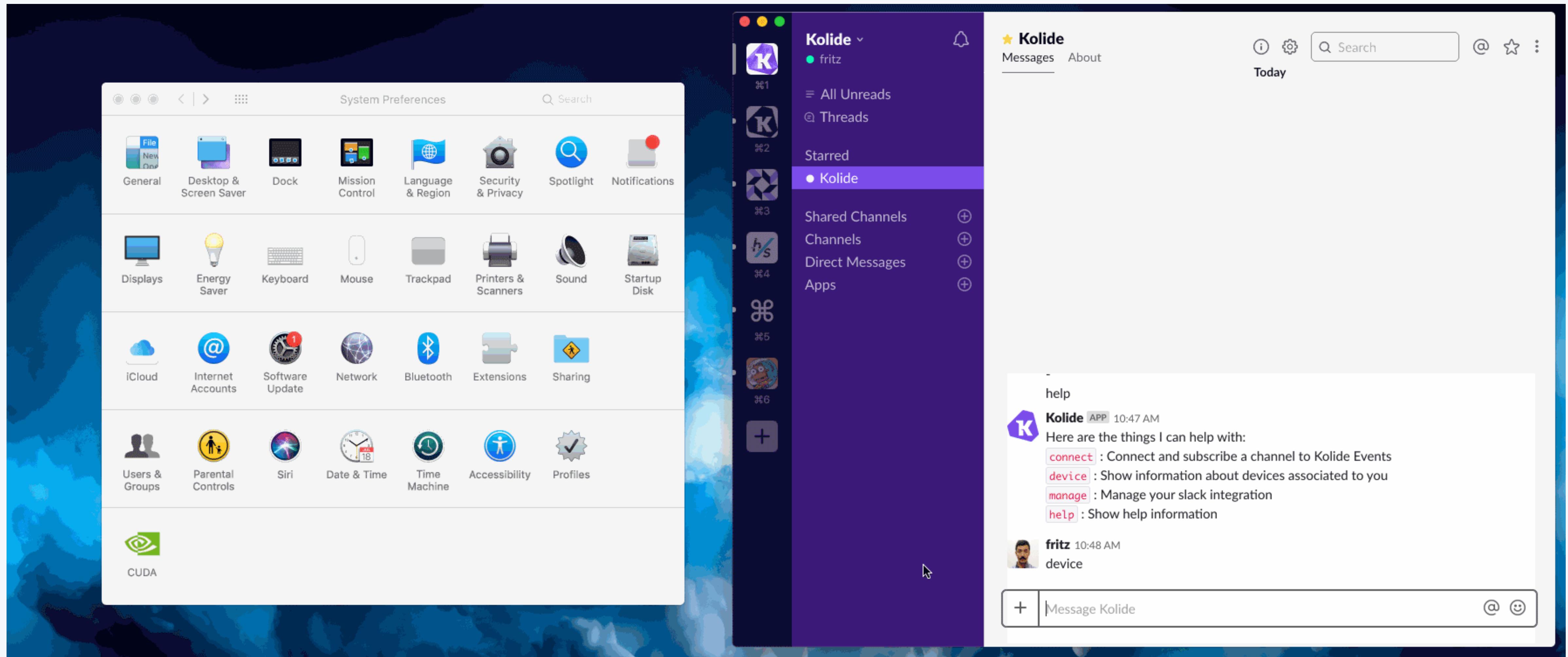
✓ 19 checks passing ✗ 1 Failing

✗ Firewall Enabled

Kolide detected 1 unique failure on this device

More Info / Resolve

An actionable communication medium to reach users



 Kolide APP 3:30 PM

 dover • MacBook Pro (15-inch, 2017) • detected 3 hours ago

Failing Check: SSH Keys Are Encrypted

Reason: Unencrypted SSH Key Detected

Why is this a Problem?

An unencrypted SSH key increases the risk that the key can be used by an unauthorized person to gain access to a privileged system. This is especially true if the key is inadvertently synced to your Dropbox, Google Drive, or a backup.

Since the minor inconvenience of encrypting an SSH key far outweighs the potential impact, we recommend encrypting all SSH keys stored on a system.

Required Action:

Encrypting SSH keys is trivial process that should only take a few minutes. On Mac or Linux simply follow these steps...

1. Open Spotlight search via the following keyboard shortcut: 'Command + Spacebar'
2. Type Terminal.app to locate your Terminal application and hit Enter to launch.
3. Once the terminal is open, at the prompt type the following command

```
ssh-keygen -p -f path_to_ssh_key_goes_here
```

You will be prompted to create a passphrase. We suggest you create a unique passphrase per key and store those passphrases in a secure/approved password manager like 1Password.

You may not see text being entered as you type your password in. Do not worry, this is normal security feature of the terminal and it is receiving your keystrokes.

[I fixed it. Check again](#)

[Contact Admin for Help](#)

The anatomy of a good notification

Receiving notifications is a key part of staying informed about what's happening to your data.

[I fixed it. Check again](#)

[Contact Admin for Help](#)

a Rechecking: jasons-laptop ⏳



macOS Application Firewall Disabled is now fixed.

2. Type Terminal.app to locate your Terminal application and hit Enter to launch.
3. Once the terminal is open, at the prompt type the following command

```
ssh-keygen -p -f path_to_ssh_key_goes_here
```

You will be prompted to create a passphrase. We suggest you create a unique passphrase per key and store those passphrases in a secure/approved password manager like 1Password.

[I fixed it. Check again](#)

[Contact Admin for Help](#)

Distributing The Agent

Better to have the users install the agent themselves

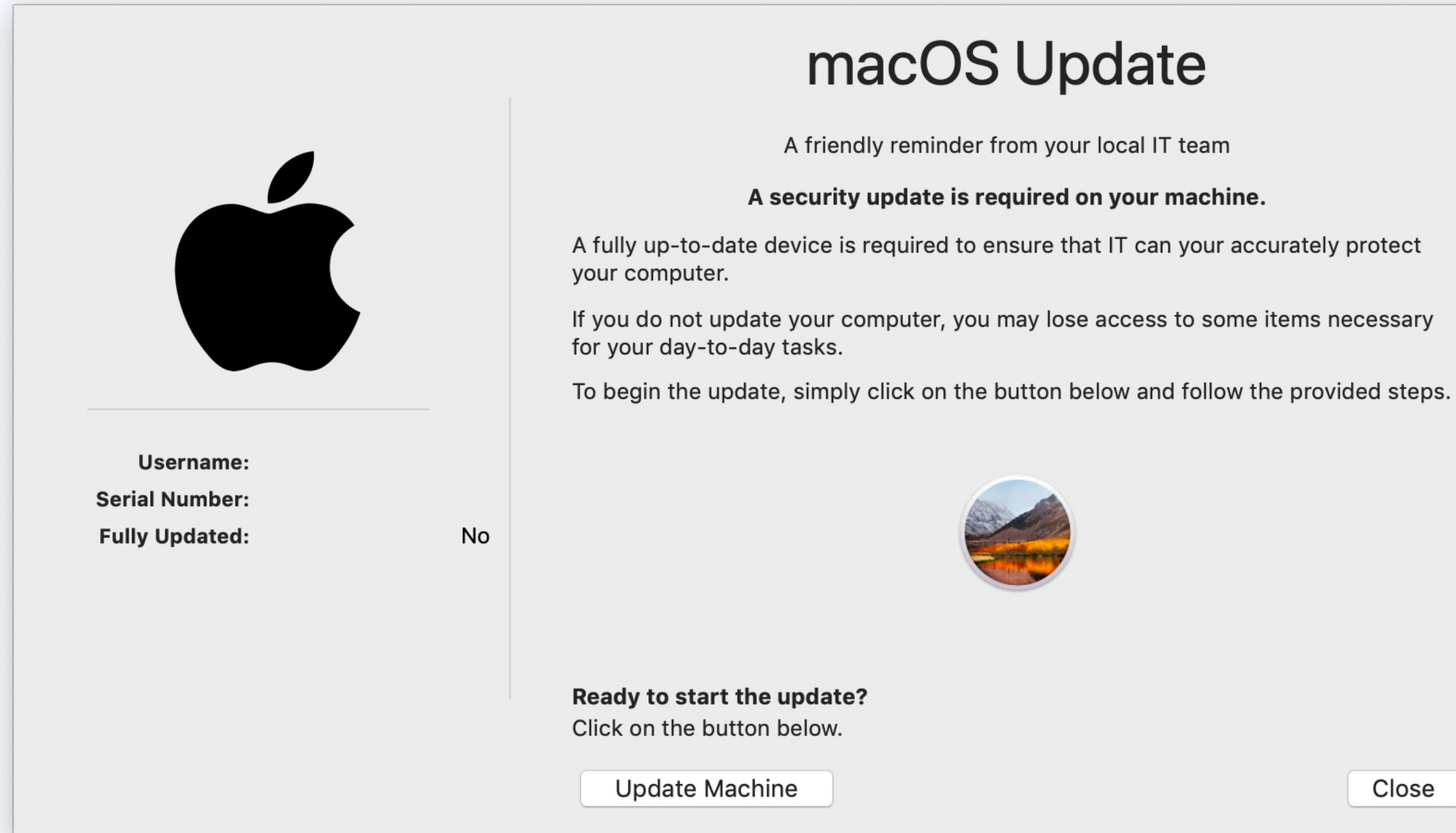
The screenshot shows the Kolide Slack App interface. At the top, there are three sections: 'Test Onboarding on Myself' (green checkmark), 'Onboard everyone!' (green checkmark), and 'Enable Automatic Onboarding' (blue circle). Below these are two circular progress indicators: one green (100% Invited) and one yellow (73% Installed). A 'Send Test to @terracatta' button is present. In the middle section, a 'Setup Guide / Onboarding' header is followed by a message: 'Select the users you want to onboard below and the Slack App will reach out with instructions on how to install Kolide on their device.' It shows a table with 429 users selected out of 429 total. The columns include NAME, SLACK HANDLE, SLACK ACCESS, KOLIDE ACCESS, CONTACTED VIA SLACK, and INSTALLED. The table lists several users with their status and last contact time.

-	NAME	SLACK HANDLE	SLACK ACCESS	KOLIDE ACCESS	CONTACTED VIA SLACK	INSTALLED
✓	Jason Meller	terracatta	Primary Owner	K Admin (Web)	✓ 3 weeks ago	✓ 3 weeks ago
✓	Fritz Ifert-Miller	fritz	Full Member	K Admin (Web)	✓ 2 weeks ago	✓ 2 weeks ago
✓	Antigoni Sinanis	asinanis	Workspace Owner	K Limited (Web)	✓ 2 weeks ago	✓ 2 weeks ago
✓	Jonathan Nogueira	jnog	Full Member	K Limited (Web)	✓ 2 weeks ago	✓ 2 weeks ago
✓	Chris Wood	cwood33	Full Member	K Limited (Web)	✓ 2 weeks ago	✓ 2 weeks ago
✓	JD Beebe	JDBB	Full Member	Slack App Only	✓ yesterday	✓ yesterday

The screenshot shows the Kolide App interface. It starts with a message from 'Kolide APP 1:33 PM': 'Hi there, I'm the Kolide App! Kolide is a user focused security platform which your team uses to inform users when their device has issues that affect system stability or security. To get started let's enroll your device. Click the Download button below to get the installer package.' Below this are 'Get Download Link for' and 'Contact Admin for Help' buttons. A note says: 'The download link below will expire after 5 minutes: Kolide Mac Installer'. Another message from 'Kolide APP 1:33 PM' says: 'Great! Now double-click the installer so that Kolide can connect to your device. We'll let you know once it enrolls.' It shows a small icon of a laptop. A progress bar indicates 'Waiting for your device to connect...'. A message from 'Kolide APP 1:33 PM' says: 'We found a device that looks like it belongs to you! Name: Evas-Macbook Model: MacBook Pro 15" 2018 Serial: C02V3WTHTX78'. An image of a MacBook Pro is shown. A 'Next' button is at the bottom. The final message from 'Kolide APP 1:33 PM' says: 'Awesome! Kolide will automatically check your device for problems and notify you each day of ongoing issues. If you don't want to wait, you can always check the state of your device by typing: device Try it now to get a report of what issues need to be addressed.'

Strategies for the stubborn

In our experience, there will be a population of users that do not listen to the Slack app. More intrusive alerting is **not the answer** as it has massive diminishing returns and these ceaseless alerts often get rolled out to everyone.



Examples of “intrusive alerting”

https://github.com/google/macops/tree/master/deprecation_notifier

<https://github.com/erikng/nudge> (pictured)

Strategies for the stubborn

Strategies we are currently experimenting with (we do not have data on which ones are the most effective...yet)



Lock them out of sensitive services

Expose device status to IDPs so they can revoke access to sensitive data/apps if the user is not making an effort



Manage their devices

Falling back to managing perpetually non-compliant devices via MDM solutions can provide an incentive to listen to the Slack app.



Give them a Scarlet Letter

Overriding their status in Slack to brand them with a symbol that indicates they have major security failures, can be effective for people capable of feeling shame.

Closing Thoughts

Closing Thoughts

The key to User Focused Security **is to have the right foundational culture** (one that encourages personal responsibility).

Challenge your biases around management and surveillance against the skill of your employees and the likely threats you face.
You will make some surprising discoveries about your assumptions.

Involving your users with important matters like security and compliance **pays dividends down the road.**

Additional Reading

<https://blog.kolide.com/kolide-user-focused-security-for-teams-that-slack-ec9646a0ce0e>

<https://github.com/Netflix-Skunkworks/stethoscope-app>

<https://slackhq.com/how-we-handle-security-at-slack>

<https://slack.engineering/distributed-security-alerting-c89414c992d6>

A screenshot of a Slack conversation. The message from securitybot at 12:47 PM reads: "I see you just ran the command `flurb -export` on `accountingserver01`. This is a sensitive command, so please acknowledge this activity by typing `acknowledge`". The message from ryan at 12:47 PM reads: "acknowledge". The message from securitybot at 12:47 PM reads: "Acknowledging via 2fa."

securitybot BOT 12:47 PM
I see you just ran the command `flurb -export` on `accountingserver01`. This is a sensitive command, so please acknowledge this activity by typing `acknowledge`.

ryan 12:47 PM
acknowledge

securitybot BOT 12:47 PM
Acknowledging via 2fa.

Relevant Talks On Friday

PRODUCTION OSQUERY

Using macOS Spotlight and Osquery to Prevent Data Breaches

For those of us on Macs, Spotlight is a critical operating system feature we rely on daily to find the files we need littered throughout our hard drives. Despite its usefulness in our daily lives, very few security products take advantage of this incredible index of information to find security risks across our device fleet. In this talk, Fritz Ifert-Miller will walk you through Osquery's mdfind virtual table, teach you Spotlight's advanced search syntax, and surprise you with the breadth and depth of information you can uncover. The talk will cover practical use-cases on top of this table to help our users discover and eliminate potential data breach vectors.



Fritz Ifert-Miller

UX @ Kolide

OSQUERY DEVELOPMENT

Building and Distribution: The Kolide Launcher for Osquery

An often overlooked but necessary part of a production Osquery deployment is generating platform native packages and installers. This process can be incredibly challenging, as each operating system has its own idioms and tooling for creating installers, different systems for maintaining persistence through restarts, and distinct processes for code signing. To make this easier for our customers, Kolide created The Kolide Launcher as an open source project aimed at removing the hurdles of installing, updating, and using Osquery at scale. In this talk, Joseph will describe Kolide Launcher's build process, its approach to multi-format packaging, how to build and debug a Windows service, and several lessons learned after one hundred thousand builds.



Joseph Sokol-Margolis

Site Reliability Engineer @ Kolide

Thank you!

-  **Jason** @ kolide.com
-  [github.com / **terracatta**](https://github.com/terracatta)
-  **terracatta** @ osquery Slack
-  [twitter.com / **jmeller**](https://twitter.com/jmeller)