RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CSV-F01

CORPSEC: WHAT HAPPENED TO CORPSES A AND B?

Chris Czub

Senior Information Security Engineer
Duo Security
@chrisczub

What is Corpsec Engineering?

- Corpsec Engineering’s Purpose: prevent and detect threats at Duo as we scale
- We have engineering resources
- You can do this too
- You don’t need a full staff of 7 engineers to do all of this

Corpsec Engineering Responsibilities

- Eat our own dogfood: Duo Beyond
- Manage endpoints
  ~600 MacOS endpoints, ~200 Chromebooks, ~10 Windows
- Manage internal security services and applications
- Cloud service security
- Employee security education and support

Corpsec Motivations

- **Scaling**
- **Enabling business**
- **Securing employees**
- **Building internal trust**

Corpsec Goals

- **Visibility**
- **Consistency**
- **Trust**
- **Preventing compromise**

Corpsec Engineering Programs

- **Detection Engineering**
- Endpoint Detection and Response
- Automation and Orchestration
- Corporate Application Security
- DevOps
- Employee Education
- Data Analytics

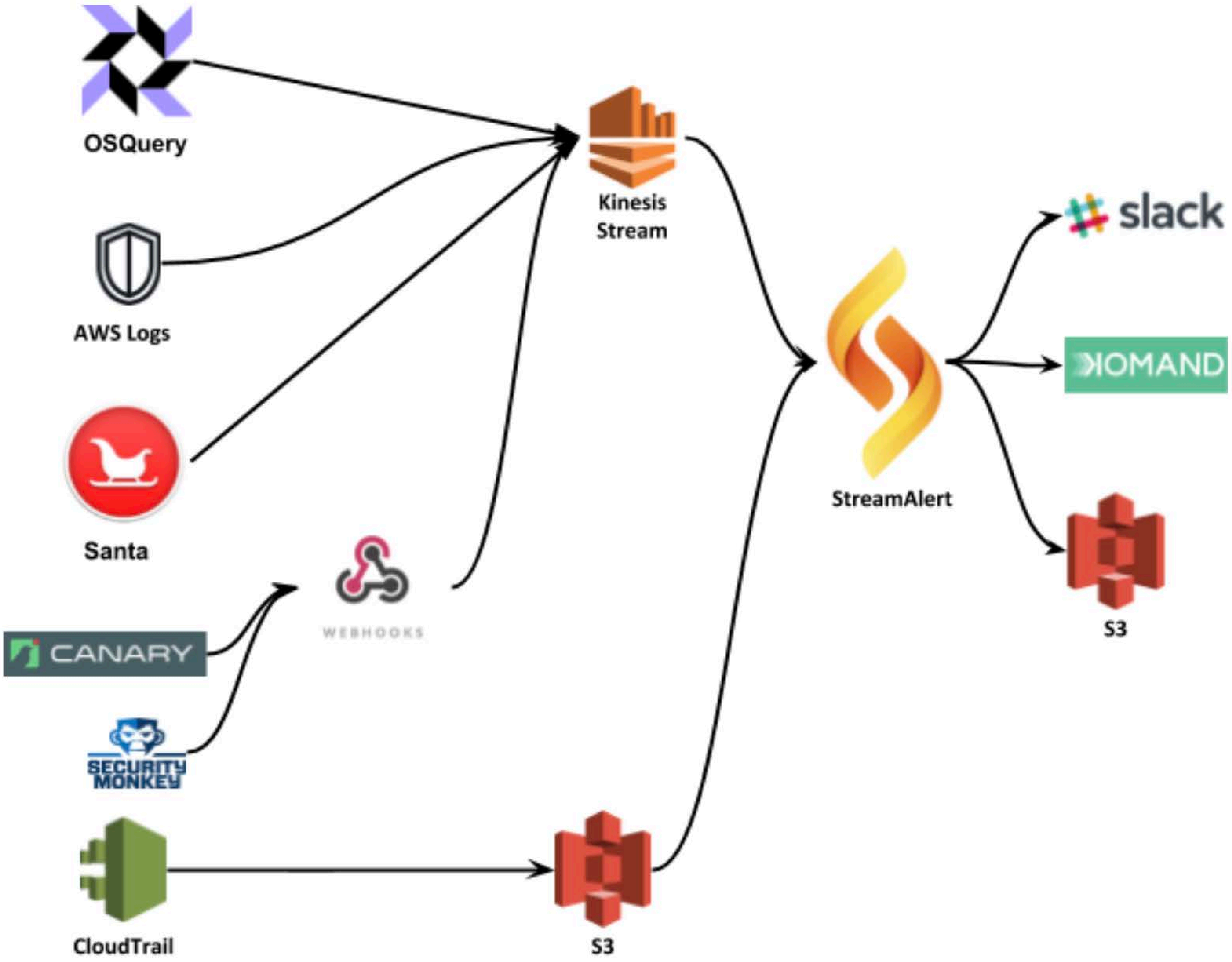
StreamAlert

Why StreamAlert?

- Scalable — just add more shards
- Actively developed
- Rules as code
- Unit Testable
- Supports many data sources/outputs/types

Why NOT StreamAlert

- Rigid
- Difficult to debug
- Hard to test end-to-end locally
- Stateless (for now)
- Need engineering support to deploy and develop on
- No correlation


OSQuery
AWS Logs
Santa
CANARY
SECURITY MONKEY
CloudTrail
WEBHOOKS
Kinesis Stream
S3
StreamAlert
slack
KOMAND
S3

Lessons Learned

- StreamAlert is *not* log aggregation or SIEM
- Will require legwork to customize for your needs
- ChatOps gets noisy fast
- Need feedback loop for alerts
  In our case, we feed them back to our SOA platform

Corpsec Engineering Programs

- Detection Engineering
- **Endpoint Detection and Response**
- Automation and Orchestration
- Corporate Application Security
- DevOps
- Employee Education
- Data Analytics

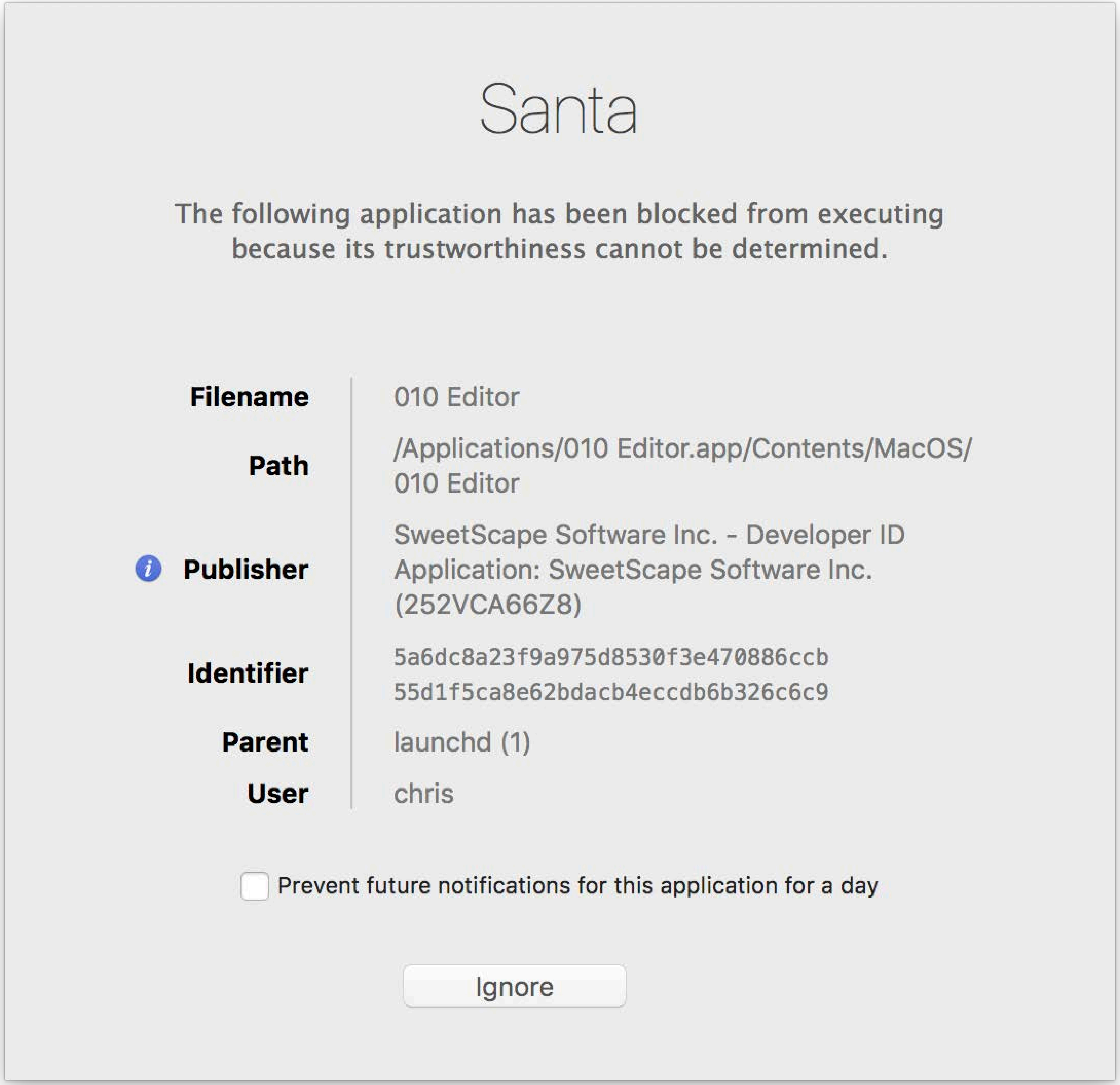
Endpoint Detection and Response

Problem statement

- We need to have an anti-malware strategy for endpoints
- Application whitelisting is one of the most effective ways to prevent malware, but can be a nightmare to deploy without annoying your users
- We wanted to cover the vast majority of malware cases with the least expense
- We wanted to leverage threat intelligence sources to enable detection after the fact

OS X App Whitelisting That Won’t Get You Fired

- Santa from Google
- Open source
- Imperfect
- No built-in server-side component



Santa

The following application has been blocked from executing because its trustworthiness cannot be determined.

Filename	010 Editor
Path	/Applications/010 Editor.app/Contents/MacOS/010 Editor
Publisher	SweetScape Software Inc. - Developer ID Application: SweetScape Software Inc. (252VCA66Z8)
Identifier	5a6dc8a23f9a975d8530f3e470886ccb 55d1f5ca8e62bdacb4eccdb6b326c6c9
Parent	launchd (1)
User	chris

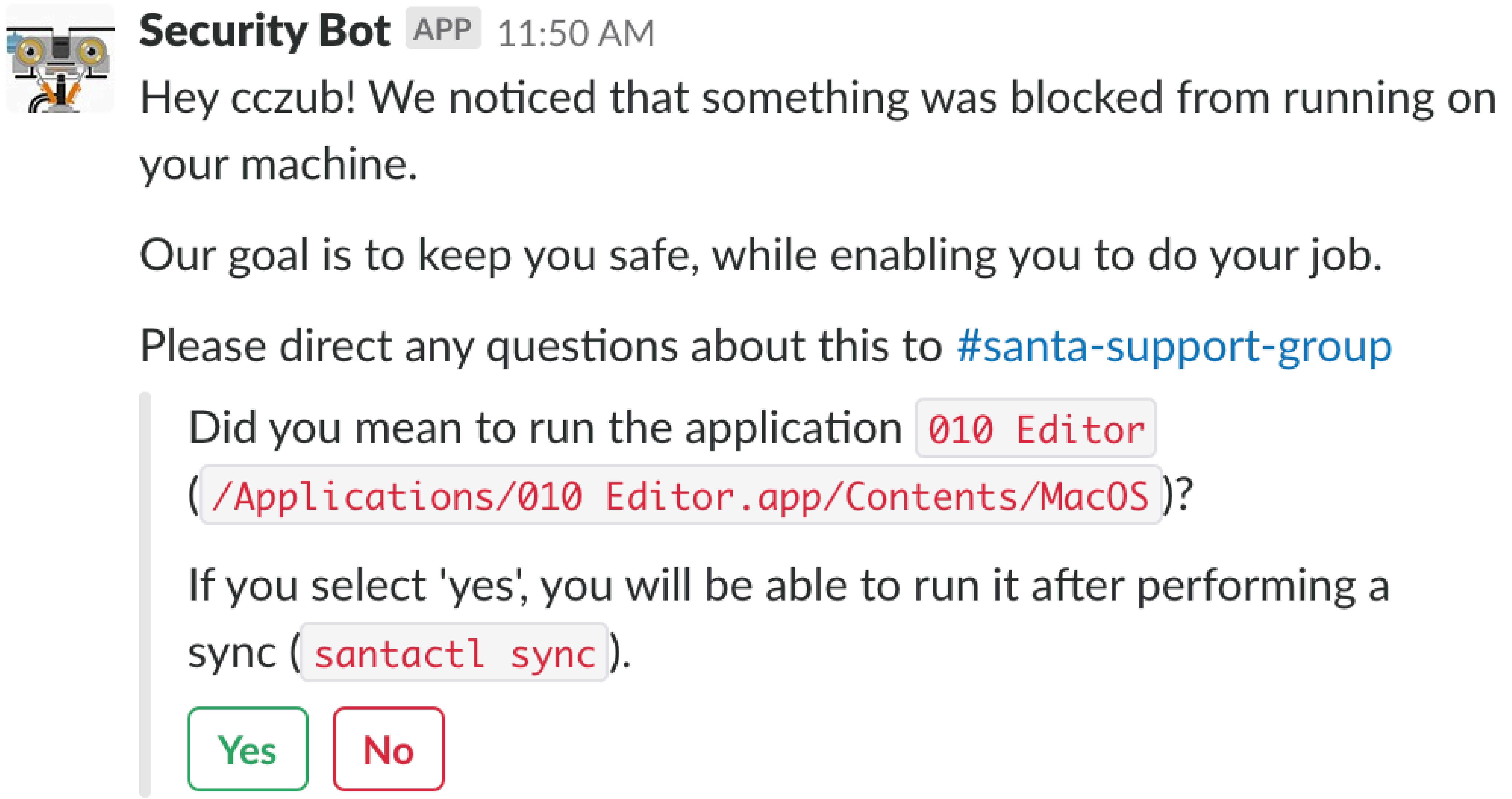
☐ Prevent future notifications for this application for a day

Santa Deployment Strategy

- **Weeks 1-4:** Deploy in monitor mode, collect data
- **Week 5:** Generate initial whitelist
- **Weeks 6-10:** Add pilot groups to enforcing mode, collect feedback
- **Weeks 11-15:** Find better solution than analyst manual whitelisting (self-service in our case) and automate
- **Weeks 16+:** Full deployment

ChatOps Whitelisting

- We used our SOA system (Komand) and some custom code to create a self-service whitelisting flow in Slack



Security Bot APP 11:50 AM

Hey cczub! We noticed that something was blocked from running on your machine.

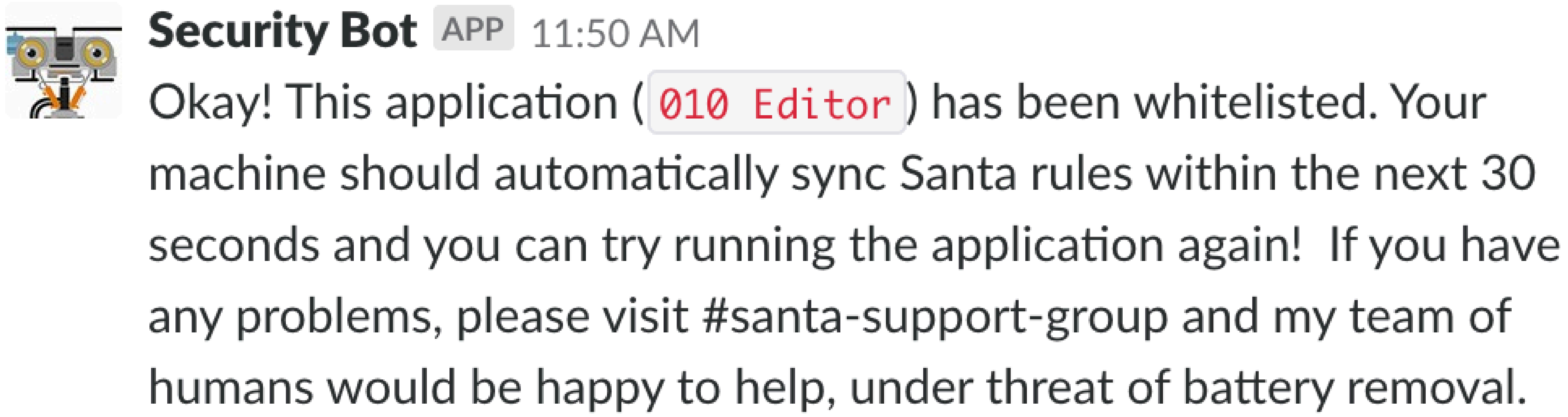
Our goal is to keep you safe, while enabling you to do your job.

Please direct any questions about this to #santa-support-group

> Did you mean to run the application `010 Editor` (`/Applications/010 Editor.app/Contents/MacOS`)?
>
> If you select 'yes', you will be able to run it after performing a sync (`santactl sync`).

ChatOps Whitelisting

- We used our SOA system (Komand) and some custom code to create a self-service whitelisting flow in Slack

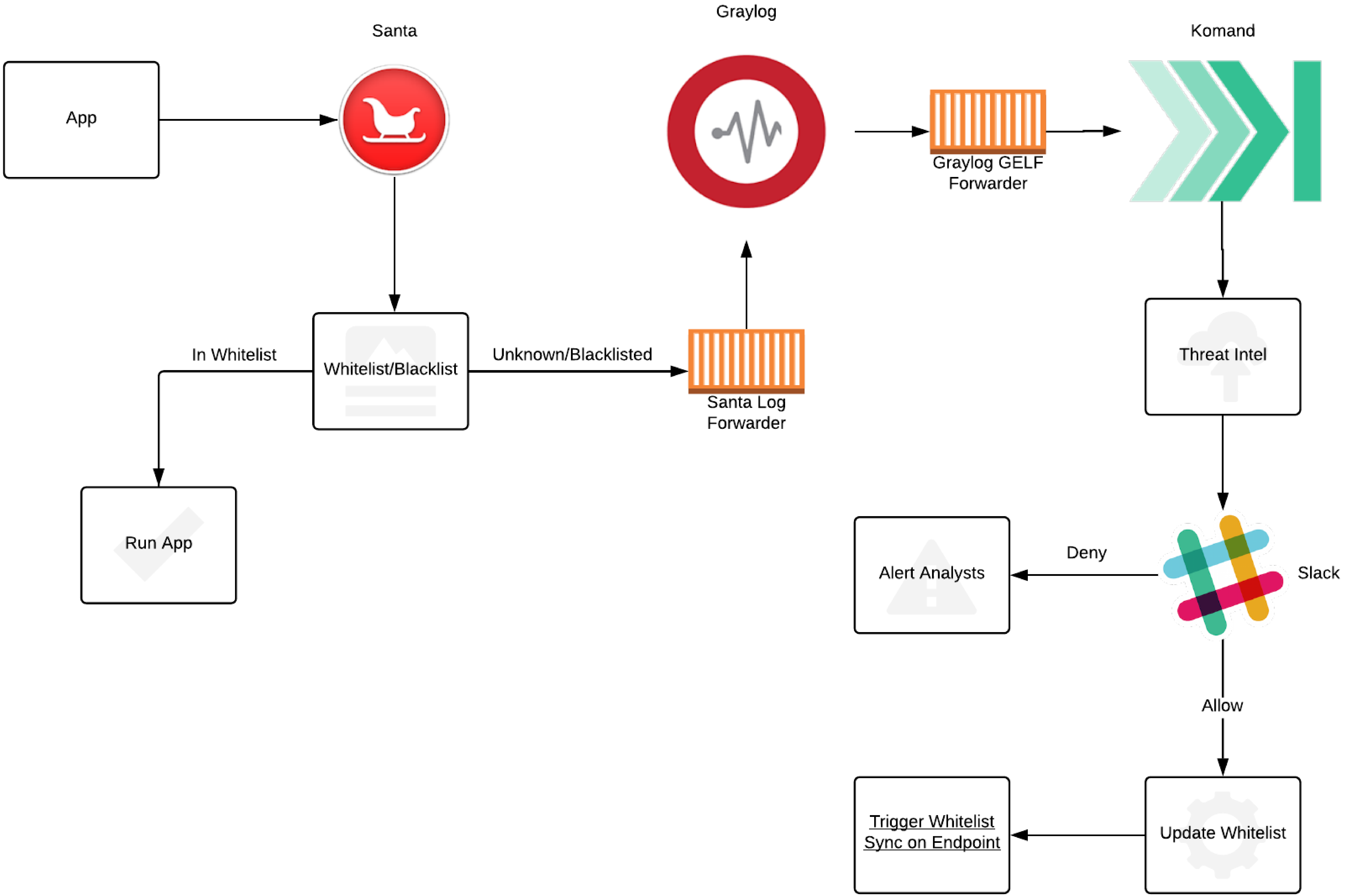


Security Bot APP 11:50 AM

Okay! This application (`010 Editor`) has been whitelisted. Your machine should automatically sync Santa rules within the next 30 seconds and you can try running the application again! If you have any problems, please visit #santa-support-group and my team of humans would be happy to help, under threat of battery removal.

A Look At the Naughty List

- 268 whitelisted developer certificates
- 1238 whitelisted binary hashes
- 20000+ application launches analyzed per week
- Dozens of potentially unwanted applications blocked

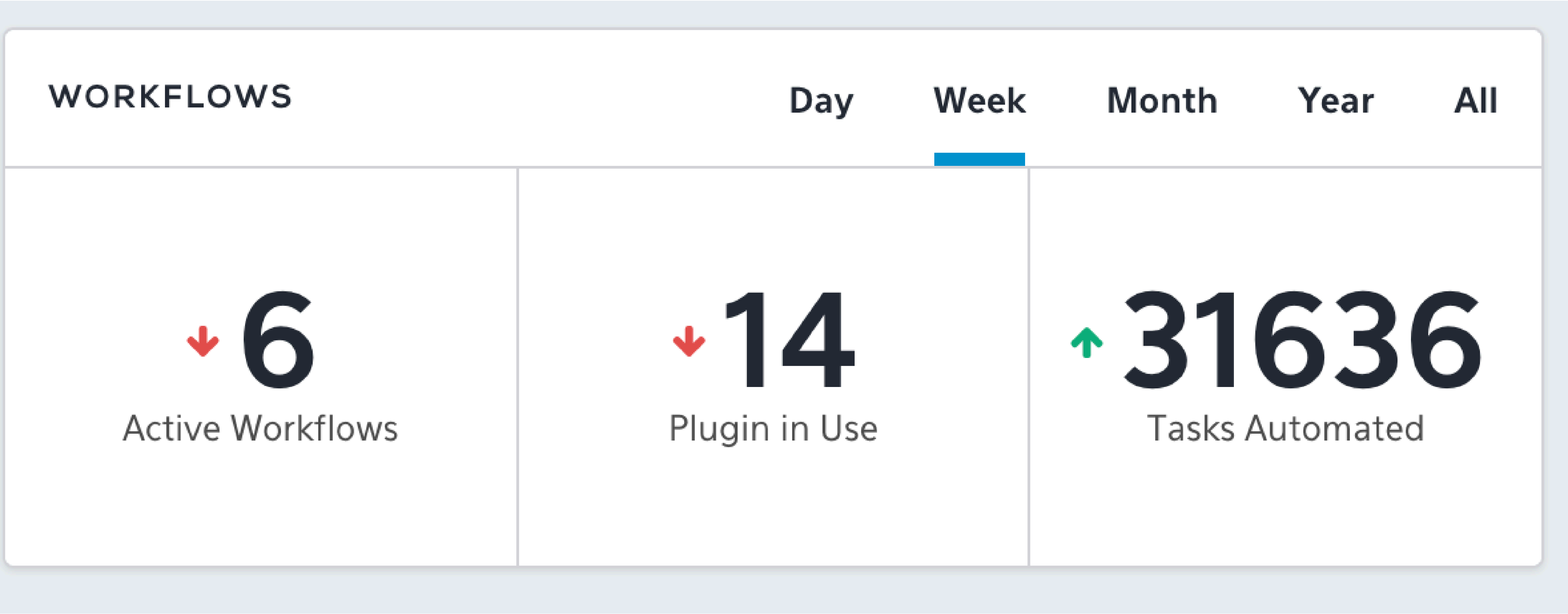

Santa
Graylog
Komand
App
Graylog GELF
Forwarder
In Whitelist
Whitelist/Blacklist
Unknown/Blacklisted
Santa Log
Forwarder
Threat Intel
Run App
Deny
Alert Analysts
Slack
Allow
Trigger Whitelist
Sync on Endpoint
Update Whitelist

Santa Infrastructure

- A server-side component to maintain the whitelist
- A front-end for managing the whitelist (adding, removing, and auditing)
- Configuration management to set the endpoints up
- Orchestration and automation
- Log forwarder from Santa to log management
- Log forwarder from Santa to orchestration platform
- Something to perform periodic checks of whitelist (scheduled Lambda)

Results

- Detected potentially unwanted apps and malware
- Deployed in four months in enforcing mode… without losing our jobs
- Freed up resources to focus on more sophisticated threats
- Quick, automated turnaround from detection to remediation for garden-variety malware and PUAs



WORKFLOWS

↓ 6	↓ 14	↑ 31636
Active Workflows	Plugin in Use	Tasks Automated

OSQuery

Facebook's Open-Source Security Tool

Windows / Mac OS X / Linux

OSQuery and Kolide Fleet

- Open source
- Indicator-based compromise and anomaly detection
- Real-time querying
- Tagging so we can query subgroups
- Slick web UI
- Scheduled Queries

Edit Query

Query Title

All LaunchDaemons

SQL

```sql
SELECT * FROM launchd
```

Description

Select all LaunchDaemons

SAVE
RUN
0 unique hosts

Select Targets

Label Name, Host Name, IP Address, etc.

Choose a Table

users

Local system users.

OS Availability

All Platforms

Columns

uid	big int
gid	big int
uid_signed	big int
gid_signed	big int
username	text
description	text
directory	text
shell	text
uuid	text

Corpsec Engineering Programs

- Detection Engineering
- Endpoint Detection and Response
- **Automation and Orchestration**
- Corporate Application Security
- DevOps
- Employee Education
- Data Analytics

Security Orchestration and Automation

- A few big players here
- We went with Komand
- Hundreds of pre-built integrations
- Reusable components
- Easy to script for in Python/Golang
- Visual flowcharts are easy artifacts to explain and display

RFPIO Processing v1	**Last Edited:** 04/09/18 **By:** April Nance	**Steps:** 6 **Decisions:** 1	**Tags:** no tags
Automated Password Alert Dev Development Workflow for Automated Password Alert. PLUGIN UPDATE AVAILABLE	**Last Edited:** 04/09/18 **By:** Jacob Rickerd	**Steps:** 28 **Decisions:** 2	**Tags:** no tags
Securitybot Slack DM Outgoing Messenger Takes csv-formatted attachments of emails sent to securitybot@d…	**Last Edited:** 04/09/18 **By:** Zack Hardie	**Steps:** 8 **Decisions:** 1	**Tags:** slack gmail email
StreamAlert Connects StreamAlert to Zendesk PLUGIN UPDATE AVAILABLE	**Last Edited:** 03/30/18 **By:** Scott Piper	**Steps:** 6 **Decisions:** 0	**Tags:** no tags
VulnMgmt v2	**Last Edited:** 03/30/18 **By:** April Nance	**Steps:** 15 **Decisions:** 2	**Tags:** no tags
OomnitzaChefWorkflow	**Last Edited:** 03/29/18 **By:** Art Sturdevant	**Steps:** 3 **Decisions:** 0	**Tags:** no tags
BetaBot	**Last Edited:** 03/27/18 **By:** Zack Hardie	**Steps:** 7 **Decisions:** 0	**Tags:** slack gmail email
Santa Whitelist	**Last Edited:** 03/23/18 **By:** Chris Czub	**Steps:** 17 **Decisions:** 2	**Tags:** no tags

Corpsec Engineering Programs

- Detection Engineering
- Endpoint Detection and Response
- Automation and Orchestration
- Corporate Application Security
- DevOps
- **Employee Education**
- Data Analytics

Engineered Employee Education

- Enlighten — gamified security
- SecurityBot — a trusted Slack bot for comms and interactions
- Phishing campaigns
- OAuth phishing

Project Enlighten
Home
Phones
Computers
Browsers
Provide feedback

Welcome,
cczub

Total Security Team Members
45

Average % Up-to-Date
66%
0% From yesterday

Team Security Score
79%

Your Security Score
75%

Your Security Points
6

Your Known Devices

- iOS (11.2.6)
  - Trusted: no
- Mac OS X (10.13.3)
  - Trusted: yes
  - Last Seen: 34 minutes ago.
- Mac OS X (10.13.2)
  - Trusted: no
  - Last Seen: 1 month ago.

Security Vs. Everybody

Cumulative team up-to-date percentage over time

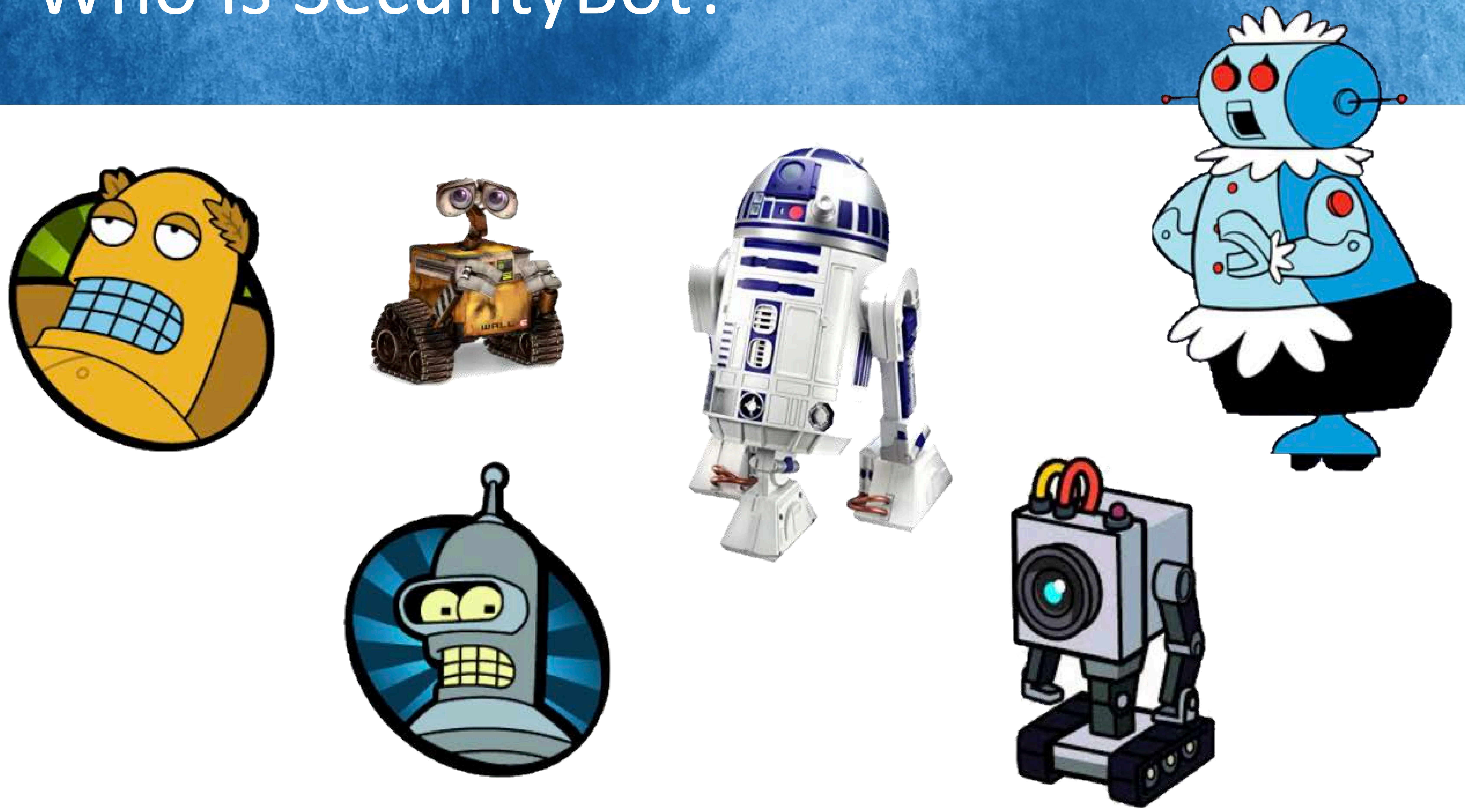
Your Team
All of Duo Security
100
90
80
70
60
50
40
30
20
10
0
Monday
Monday
Monday
Monday
Monday
Monday
Monday

Security Team Phones

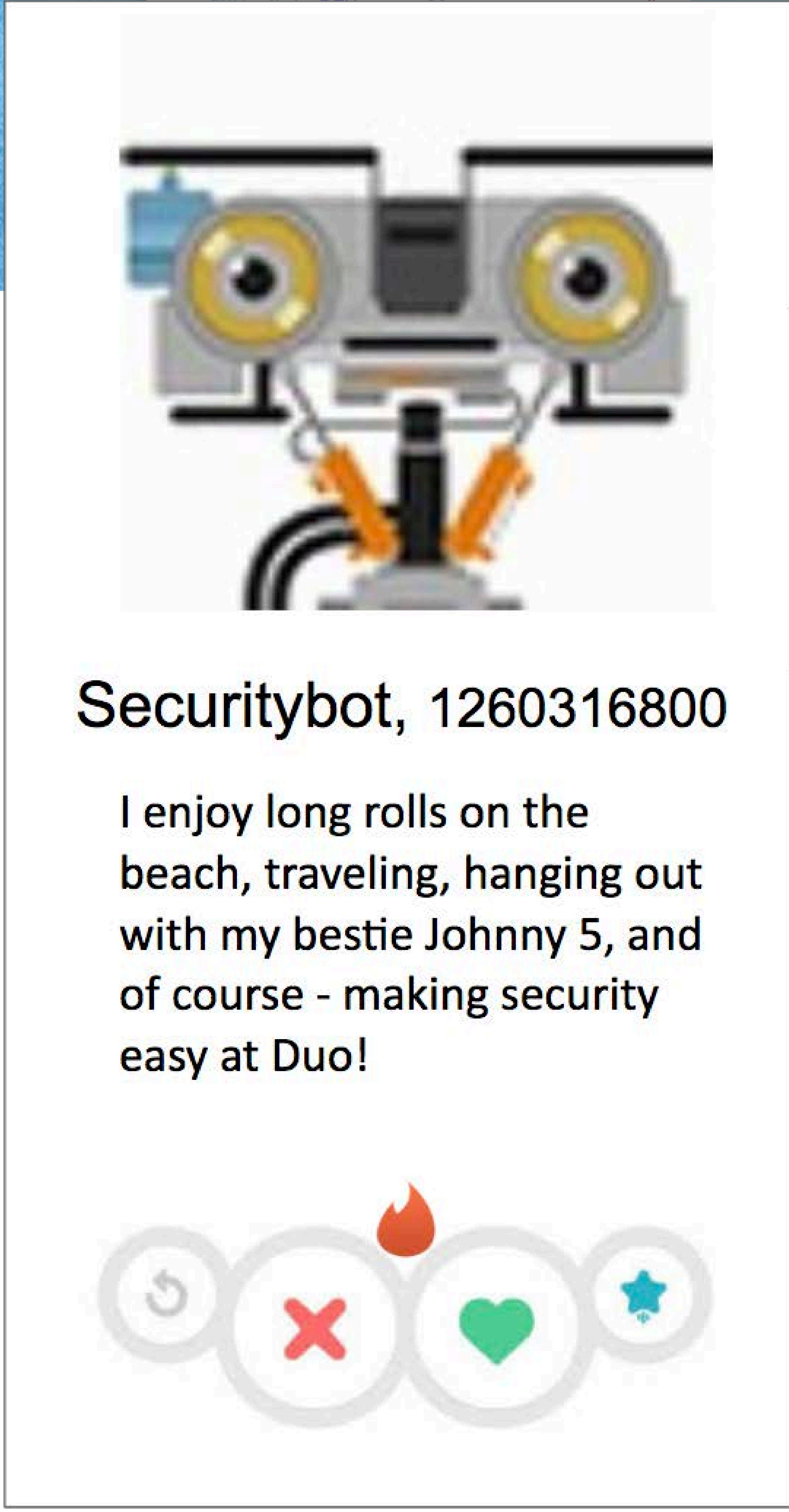
How many of your team members' phones are up to date over time

Security Team Phones

Who Is SecurityBot?



- A little bit of all of the above…

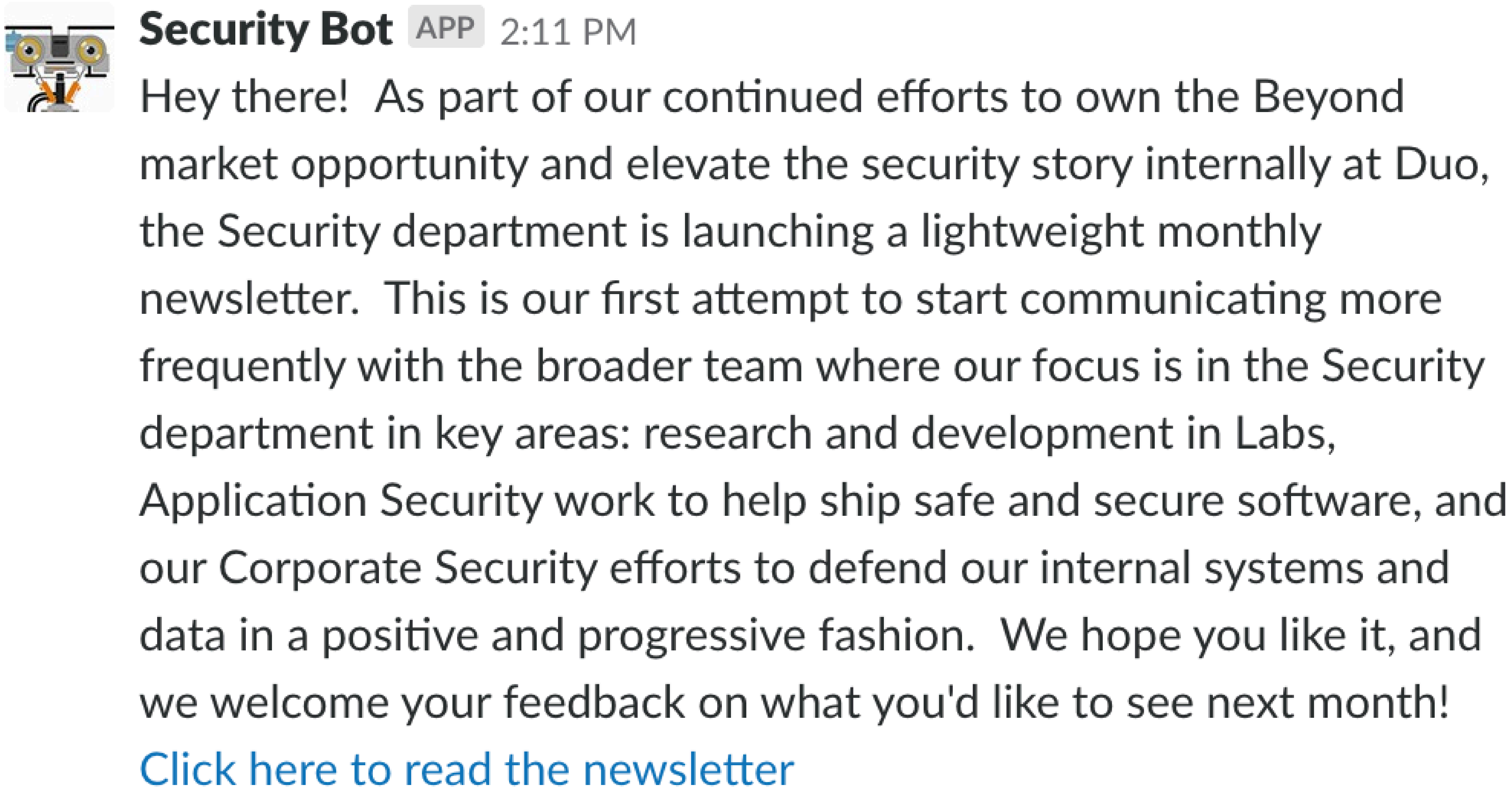


Securitybot, 1260316800

I enjoy long rolls on the beach, traveling, hanging out with my bestie Johnny 5, and of course - making security easy at Duo!

Whatcha Thinkin' About, SecurityBot?

- Santa Notifications
- Beta Program Invitations
- Password Alert Messaging
- Messages from the Security Team
- A Source of Trusted Information and True Facts #nophish



Security Bot APP 2:11 PM

Hey there! As part of our continued efforts to own the Beyond market opportunity and elevate the security story internally at Duo, the Security department is launching a lightweight monthly newsletter. This is our first attempt to start communicating more frequently with the broader team where our focus is in the Security department in key areas: research and development in Labs, Application Security work to help ship safe and secure software, and our Corporate Security efforts to defend our internal systems and data in a positive and progressive fashion. We hope you like it, and we welcome your feedback on what you'd like to see next month!

Click here to read the newsletter

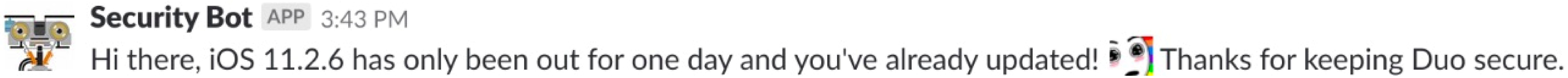
Security Bot 10:21

Hi asturdevant,

The CorpSec team is requesting your help to test a new product/feature. If you decide to help, you can join the channel: #corpsec where you can ask questions and get help, if needed. We understand if you're too busy to help with a beta feature right now, you can also click, `Sorry, not now` or simply ignore me to `opt-out` of this invitation. Below is a quick description of the product/feature that the CorpSec needs help testing.

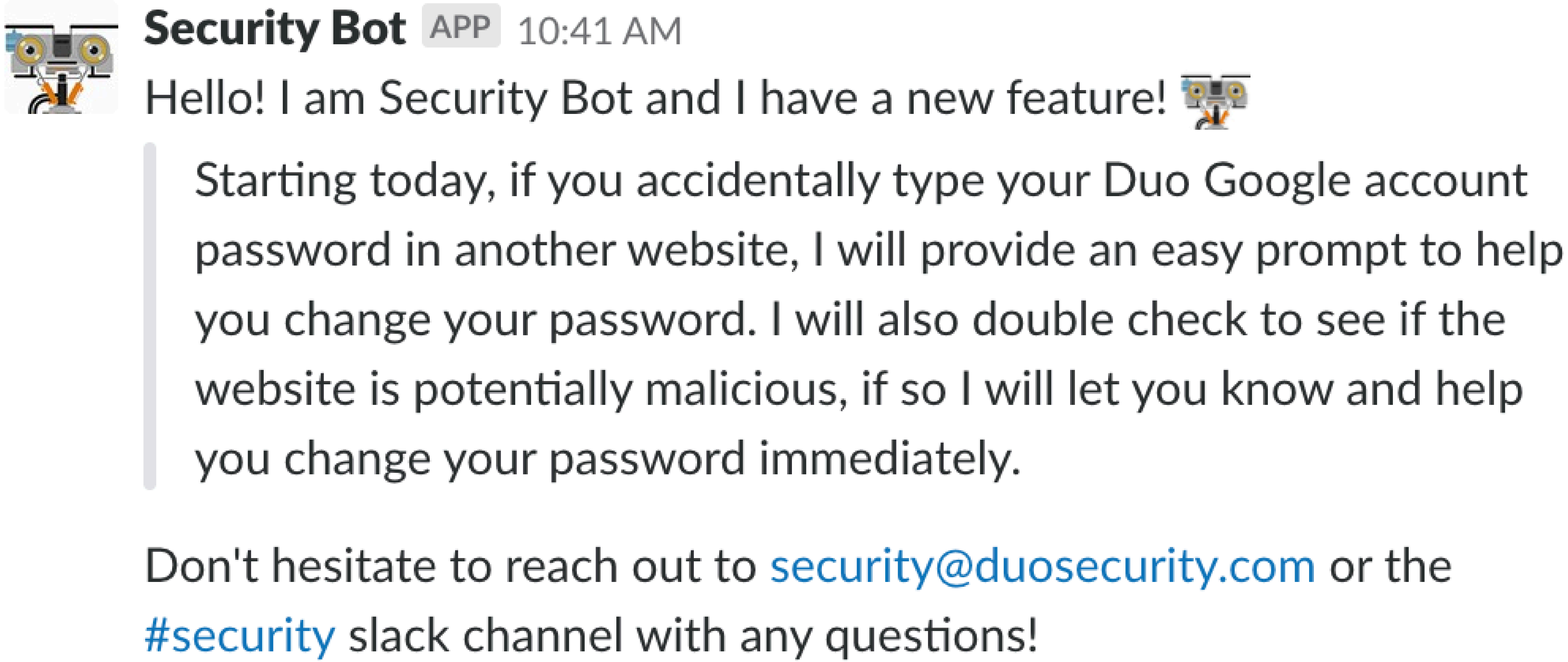
Description:
Hello! This is a sample beta program enrollment from Security Bot!

> Would you like to participate?
>
> Awesome, Yes! Sorry, not now.



Security Bot APP 3:43 PM

Hi there, iOS 11.2.6 has only been out for one day and you've already updated! Thanks for keeping Duo secure.



Security Bot APP 10:41 AM

Hello! I am Security Bot and I have a new feature!

> Starting today, if you accidentally type your Duo Google account password in another website, I will provide an easy prompt to help you change your password. I will also double check to see if the website is potentially malicious, if so I will let you know and help you change your password immediately.

Don't hesitate to reach out to security@duosecurity.com or the #security slack channel with any questions!

- Questions?