Insider Guidance For Splunk Cloud Vetting Process

Yinqing Hao
Software Engineer | Splunk Inc.

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Agenda

What is Cloud Vetting?

- Why Cloud Vetting?
- What Triggers Cloud Vetting?
- Self-Service Cloud and Managed Cloud

Getting Your Apps Vetted in Cloud

- Verify your App with AppInspect
- Package your App with the Splunk Packaging Toolkit

Common Failures and Best Practices

- Self-Service App Installation failures
- Cloud Vetting failures

What is Cloud Vetting

splunk> .conf19

What is Cloud Vetting?

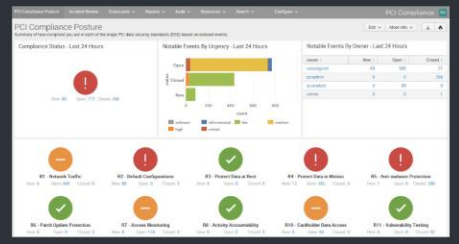
Cloud Vetting is required before an App can be installed on Splunk Cloud

Learn more: https://dev.splunk.com/enterprise/docs/releaseapps/appinspect/cloudvettingguidelines/vetappsandaddons

Splunk App for PCI Compliance - Splunk Enterprise Security

4 ratings

Splunk Built



Overview | Details

The Splunk App for PCI Compliance (for Splunk Enterprise Security) is a Splunk developed and supported App designed to help organizations meet PCI DSS 3.2 requirements. It reviews and measures the effectiveness and status of PCI compliance technical controls in real time. It can also identify and prioritize any control areas that may need to be addressed and let you quickly address any auditor report or data request.

The App provides out-of-the-box searches, dashboards, reports, an incident response framework, and integration with employee and asset information to give you visibility into system, application, and device activity relevant to PCI compliance.

NOTE: There are two installer options for this App. If you are installing the App on Splunk Enterprise Security use the installer on this pag
you are installing the App stand-alone on Splunk Enterprise, use the installer https://splunkbase.splunk.com/app/1143

The Splunk App for PCI Compliance requires a paid license.

Release Notes

Version 3.7.1 Dec. 14, 2018

LOGIN TO DOWNLOAD

VERSION
3.7.1

COMPATIBILITY
Products: Splunk Enterprise Security, Splunk Cloud, Splunk Enterprise

File a case
Flag as inappropriate

COMPATIBILITY
Products: Splunk Enterprise Security, Splunk Cloud, Splunk Enterprise
Splunk Versions: 7.2, 7.1
Platform: Platform Independent
CIM Versions: 4.x

splunk> .conf19

Why Cloud Vetting?

Why Cloud Vetting?

Security Issues

- Crypto Mining

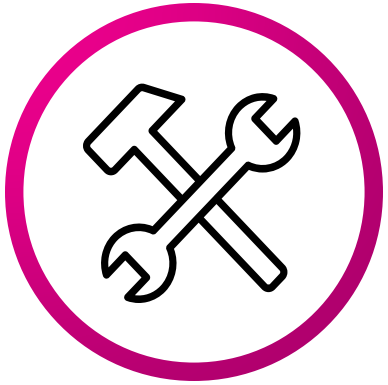
Performance Overhead

- `replicationWhitelist` in distsearch.conf

Why Cloud Vetting?

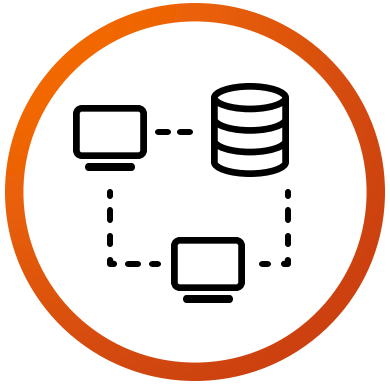
Our focuses

Build Time



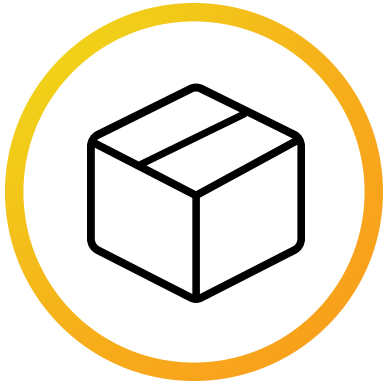
App development best practices

Run Time



- Security vulnerabilities
- Operational issues

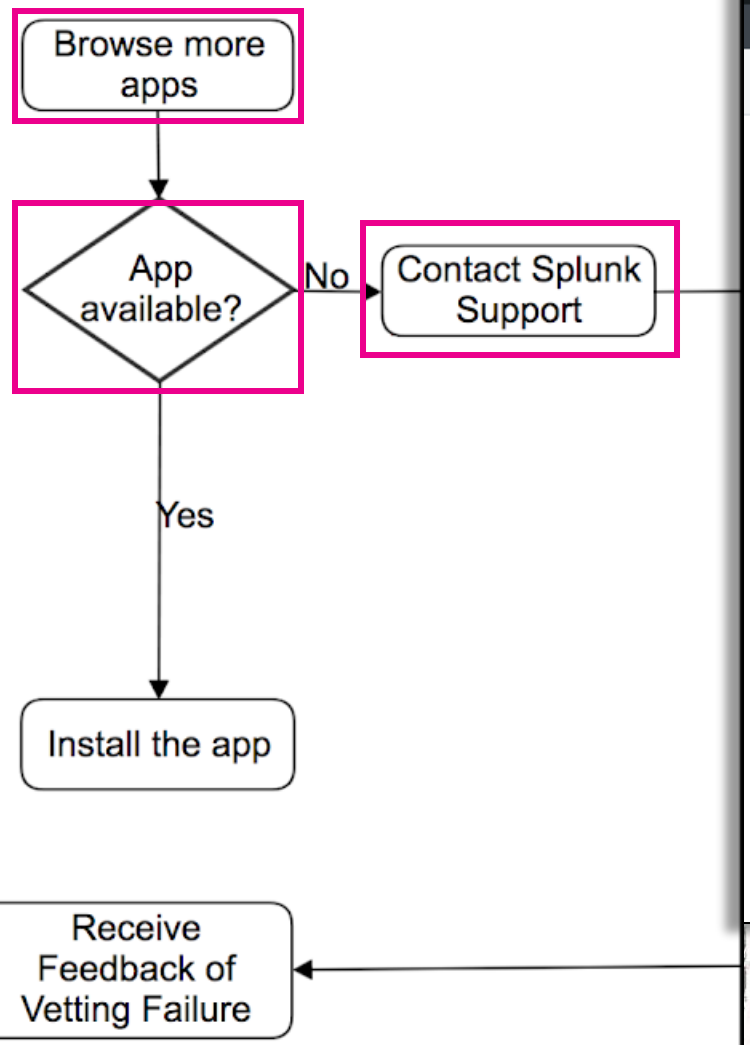
Installation Time



- Installation location
- Self-Service App Installation (SSAI)
- Rolling restart
- Management inputs

What Triggers Cloud Vetting?

Customer



splunk>cloud Apps Messages Settings Activity Find Splunk Administrator Support & Services

Apps Uploaded Apps Install Log App Management

Browse More Apps

machine learning

6 Apps

CATEGORY
- DevOps
- Security, Fraud & Compliance
- IT Operations
- Utilities
- Business Analytics
- IoT & Industrial Data

CIM VERSION
- [x] 4.x
- [ ] 3.x

SUPPORT TYPE
- [x] Developer
- [ ] Splunk
- [ ] Not Supported

APP CONTENT
- Inputs
- Alert Actions
- Visualizations

APP TYPE
- App
- Add-on

Technical Add-on for Malwarebytes — Install

The Add-on for Malwarebytes provides custom Splunk configuration to understand Malwarebytes event data. This app is a requirements for all Malwarebytes apps for Splunk. The app includes Common Information Compliant (CIM) field extractions and pre-defined source types for multiple Malwarebytes products making it compatible with all CIM based Splunk ... More

Category: Security, Fraud & Compliance | Author: Malwarebytes - | Downloads: 152 | Released: a year ago | Last Updated: 5 months ago | View on Splunkbase

Malwarebytes Visibility and Dashboards — Request Install

Please file a support case to install this app.

The Malwarebytes App for Splunk provides custom Splunk searches and dashboards for Malwarebytes endpoint security data. This app extends from the Add-on for Malwarebytes to offer an immediate visual experience for all Malwarebytes users. All dashboards have been highly optimized for fast performance and contain custom drill-downs. Use it to quickly... More

Category: Security, Fraud & Compliance | Author: Malwarebytes - | Downloads: 110 | Released: a year ago | Last Updated: 7 months ago | View on Splunkbase

Malwarebytes Cloud Remediation — Not Yet Available

This app is not yet certified for Splunk Cloud. Please file a support case to request this app.

The Cloud Remediation app integrates Splunk Enterprise and Splunk Cloud to for Malwarebytes Cloud for Incident Response and Endpoint Protection.

Malwarebytes makes endpoints resilient through adaptive cyber protection, active threat response and orchestrated endpoint control that quickly restores workforce productivity when a compromise occurs. Ou... More

Category: Security, Fraud & Compliance, IT Operations | Author: Malwarebytes - | Downloads: 40 | Released: 4 months ago | Last Updated: 4 months ago | View on Splunkbase

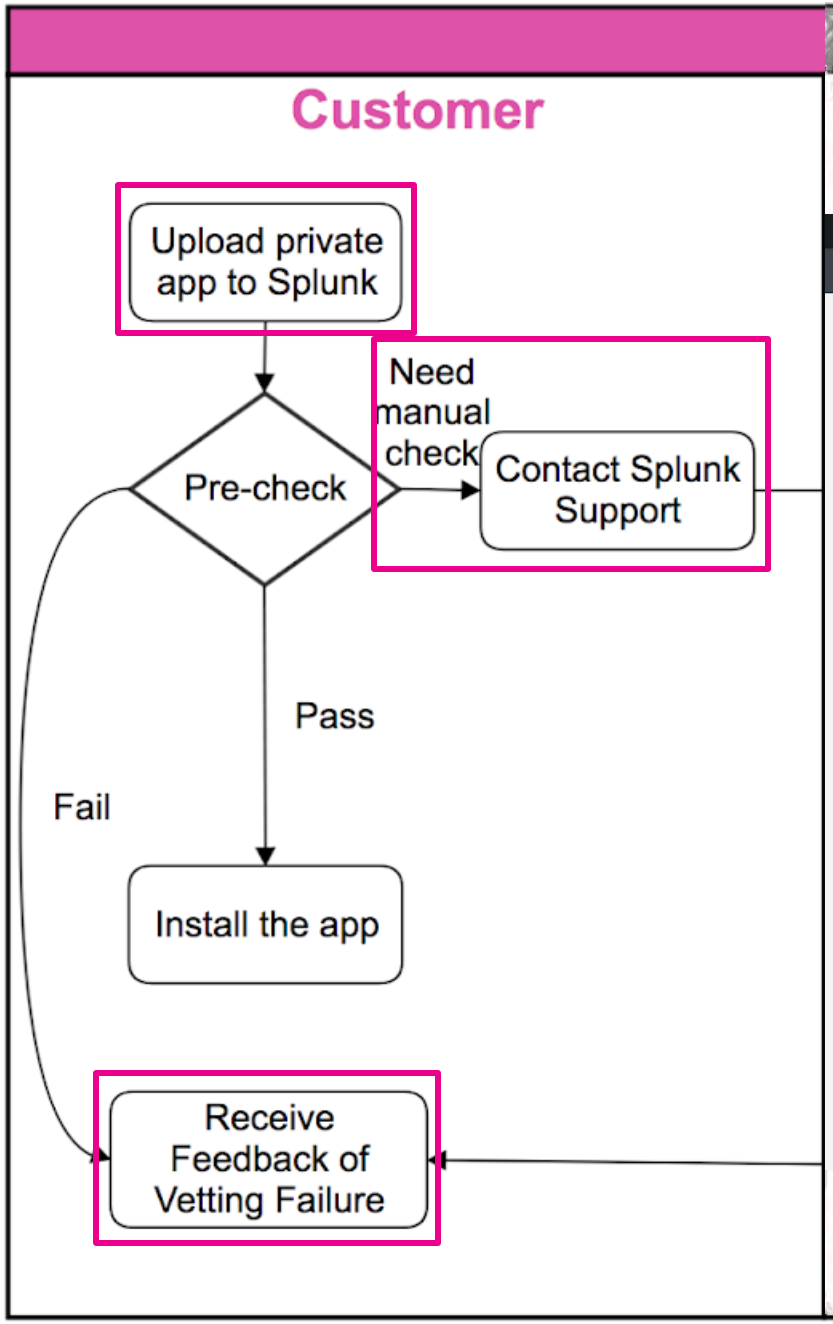
Query.AI Splunk AI Analyst — Not Yet Available

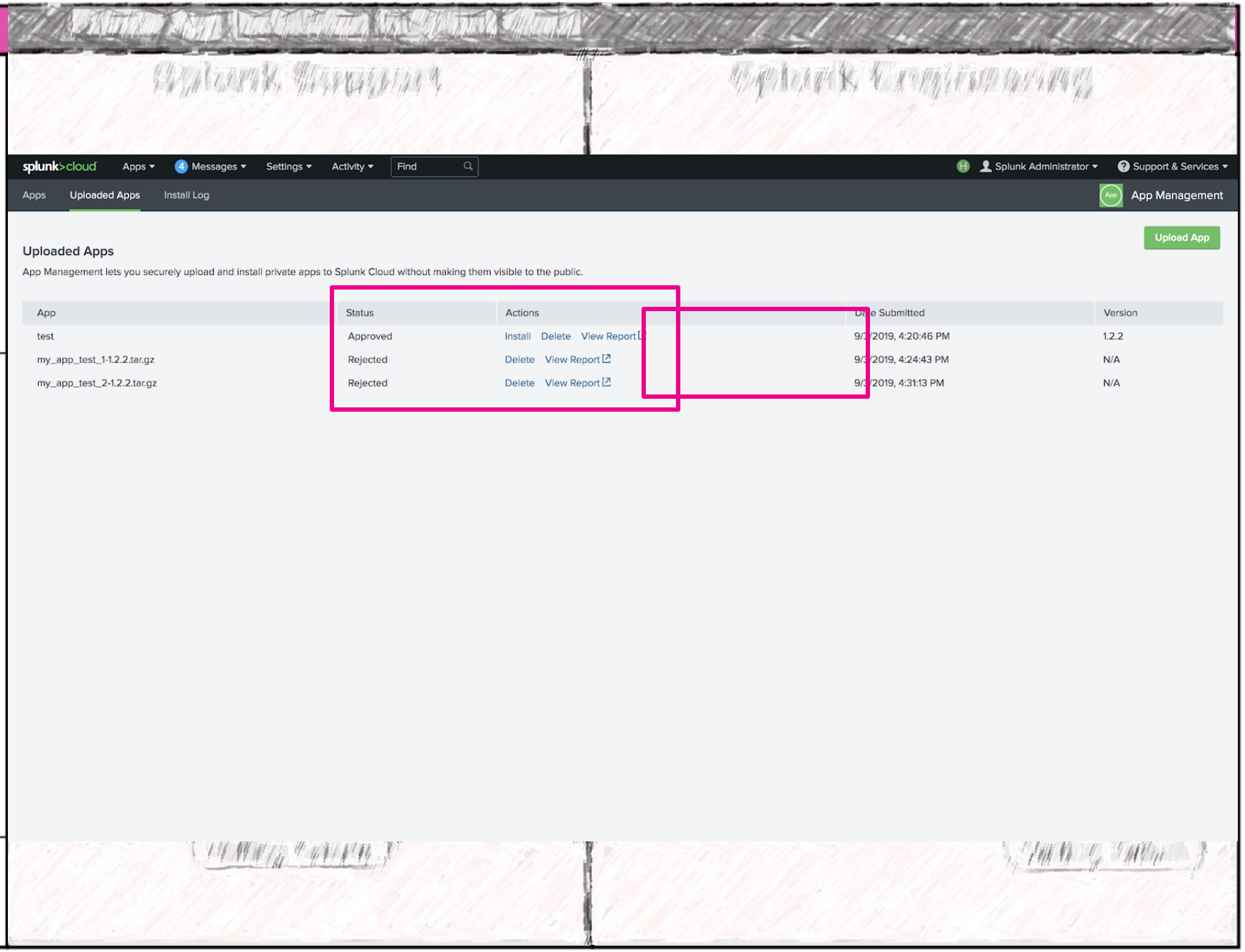
This app is not yet certified for Splunk Cloud. Please file a support case to request this app.

Query.AI democratizes Splunk® data with its Artificial Intelligence virtual Analyst technology. Query.AI IRIS (Investigations Response Intelligence Service) is the AI that talks to you using voice and NLP (Natural Language Processing) to produce answers, insights and automated visualizations from Splunk data. Query.AI also captures and combines inv... More

Category: Security, Fraud & Compliance, Business Analytics | Author: Query AI | Downloads: 9 | Released: 21 days ago | Last Updated: 21 days ago | View on Splunkbase

Customer


Upload private app to Splunk
Pre-check
Need manual check
Contact Splunk Support
Pass
Fail
Install the app
Receive Feedback of Vetting Failure


splunk>cloud
Apps
Messages
Settings
Activity
Find
Splunk Administrator
Support & Services
Apps
Uploaded Apps
Install Log
App Management
Upload App
Uploaded Apps
App Management lets you securely upload and install private apps to Splunk Cloud without making them visible to the public.
App
Status
Actions
Date Submitted
Version
test
Approved
Install Delete View Report
9/3/2019, 4:20:46 PM
1.2.2
my_app_test_1-1.2.2.tar.gz
Rejected
Delete View Report
9/3/2019, 4:24:43 PM
N/A
my_app_test_2-1.2.2.tar.gz
Rejected
Delete View Report
9/3/2019, 4:31:13 PM
N/A

Self-Service Cloud vs. Managed Cloud

Self-Service Cloud vs. Managed Cloud

Self-Service Cloud

- No support for Private Apps
- Paid customers can open a support ticket to request Vetting for Public Apps

Managed Cloud

- Issues with Search Head Clustering (**SHC**):
  - SSAI is supported on SHC in version 7.2 or later
  - Some Public Apps are Cloud-compatible, but not SHC compatible. Splunkbase does not expose this information (yet), but App will not be available in the UI
- Issues with stacks that have multiple Search Heads:
  - SSAI will only be installed on one Search Head or SHC. All other Search Heads require a support case for every app install

Getting Your Apps Vetted in Cloud

splunk> .conf19

Verify your app with AppInspect

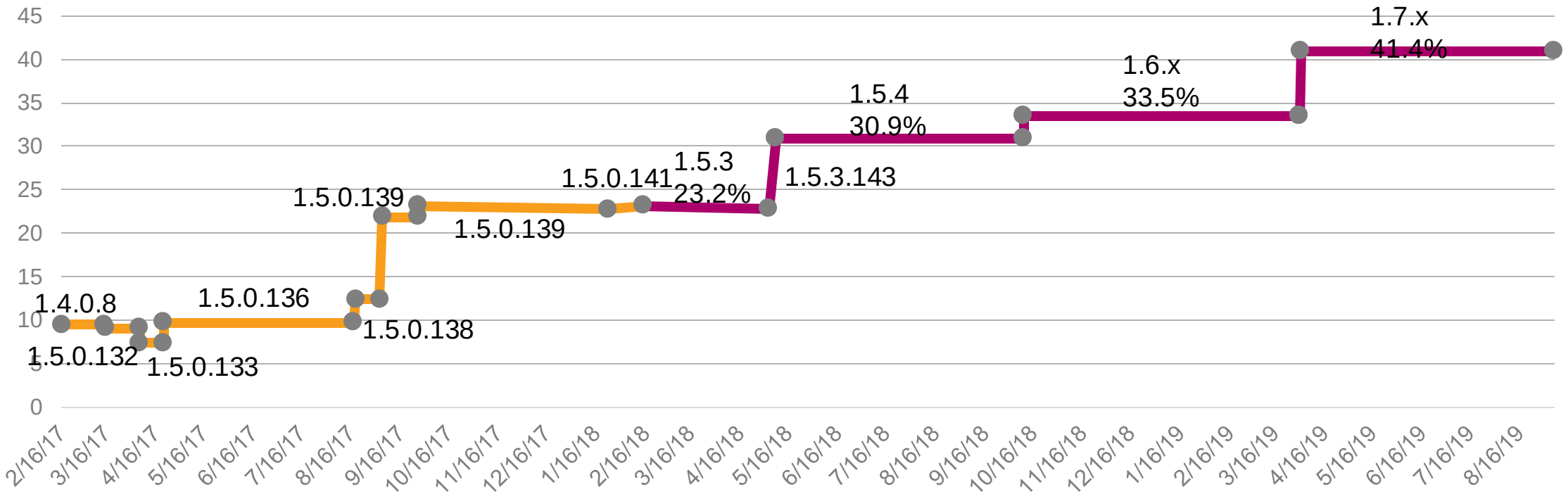
Splunk AppInspect evaluates your Splunk app against a set of Splunk-defined criteria so that you can be assured of the quality and robustness of your app.

Check out the docs:

- https://dev.splunk.com/enterprise/docs/releaseapps/appinspect/
- CLI:
  - Runs Cloud validation with `cloud` tag
  - Has custom check ability
- Web API:
  - Also runs installation checks
  - Also runs antivirus
  - Also runs Packaging Toolkit validation with `self-service` tag

Automation Rate

% of apps that can be auto vetted in AppInspect API service



Verify your app with AppInspect

Results

Result	Description	Resolution
success	Checked functionality adheres to the Cloud Vetting policy.	N/A
warning	Checked functionality is identified as a non-blocking issue in Splunk Cloud	**Suggest to fix the issue based on the AppInspect output**
failure	Checked functionality violate the Cloud Policy	**Fix the issue based on the AppInspect output**
manual_check	Checked functionality must be manually reviewed	**Review the check's message to determine what issues to look for in the app.**
not_applicable	Checked functionality doesn't exist in the app	N/A
error	A failure has occurred within AppInspect	N/A; this code does not indicate a problem in the app package.

Package your app with Splunk Packaging Toolkit

The Packaging Toolkit (also known as “SLIM”) is a tool for authoring, packaging, and validating a Splunk App in a way that eases App management, including installation, configuration, and updating.

SLIM helps:

- Check app packaging issues
- Package the source of the app

SLIM v1.0.0 supports Splunk Cloud 7.2 and later

Learn more: https://dev.splunk.com/enterprise/docs/releaseapps/packagingtoolkit/

Package your app with Splunk Packaging Toolkit

Package command

- Package the source of a Splunk app to a valid format.
- Ignore prohibited file, such as .DS_STORE, by specifying own .slimignore file

```
$ slim package splunk_app_for_nix
slim package: Packaging app at "splunk_app_for_nix"
slim package: [WARNING] Could not find alert_overlay.conf.spec
slim package: [WARNING] Could not find unix_setup.conf.spec
slim package: [WARNING] Skipping validation for dynamic dependency "Splunk_TA_nix"
slim package: [NOTE] Source package exported to "splunk_app_for_nix-5.2.3.tar.gz"
```

Package your app with Splunk Packaging Toolkit

Validate command

- Validates the app and app manifest (if it exists). This includes validating any statically declared dependencies. If a manifest does not exist, one will be generated.
- This command also checks the configuration related issues, such as malformed configuration files

```
$ slim validate splunk_app_for_nix-5.2.3.tar.gz
slim validate: Validating app at "splunk_app_for_nix-5.2.3.tar.gz"...
slim validate: [WARNING] Could not find alert_overlay.conf.spec
slim validate: [WARNING] Could not find unix_setup.conf.spec
slim validate: [WARNING] Skipping validation for dynamic dependency "Splunk_TA_nix"
slim validate: [NOTE] App validation complete
```

Common Failures and Best Practices

splunk> .conf19

Inconsistent/ Invalid Configurations

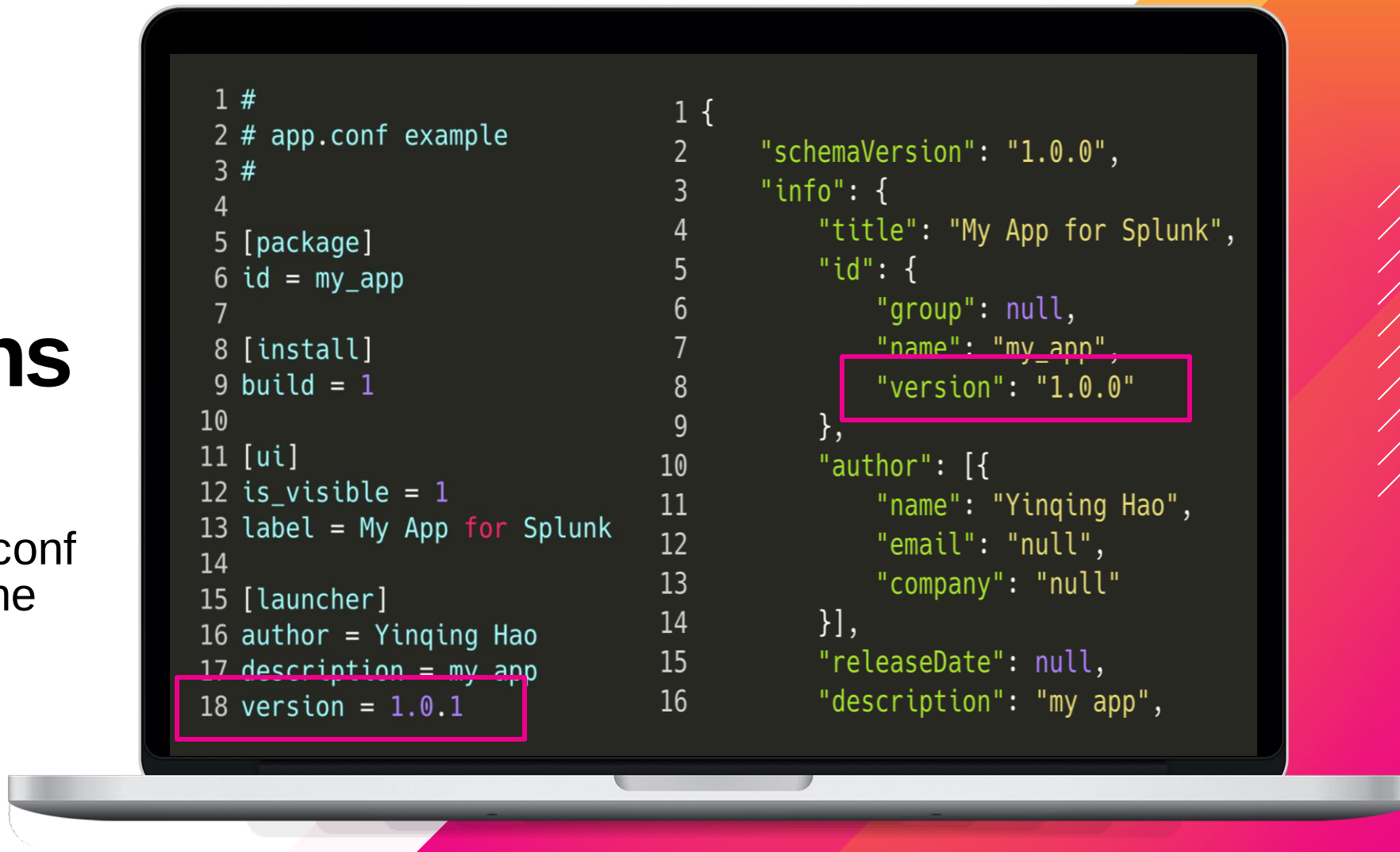
Cloud Incompatible

- Make sure the configurations are valid and consistent in the app

Inconsistent Configurations

Cause of Failure

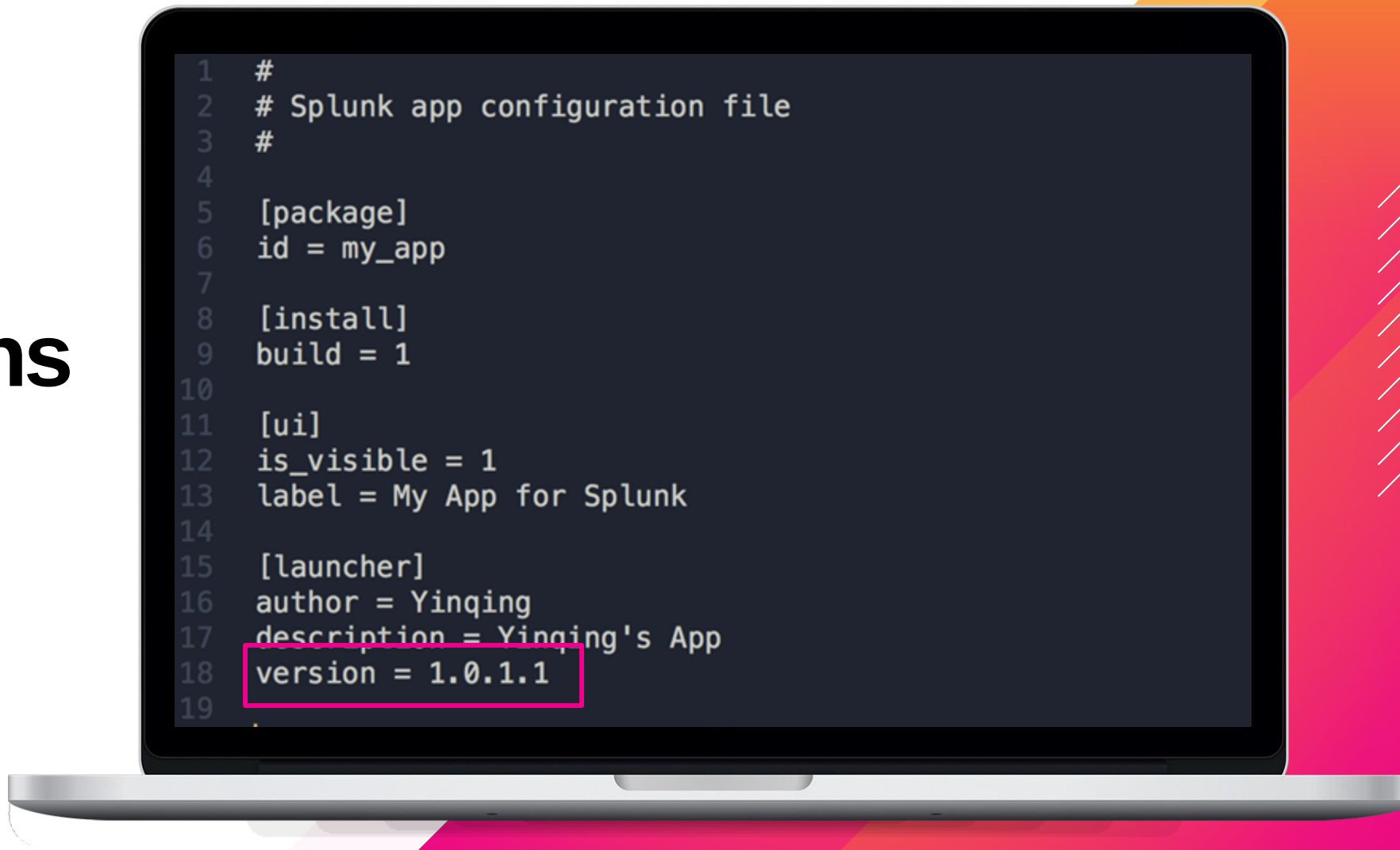
The configurations in the conf file are inconsistent with the app.manifest



Invalid Configurations

Cause of Failure

Not using Semantic Versioning (Major.Minor.Revision)



Inconsistent/Invalid Configuration

Preventive Action

- Run `slim validate` to check the app configurations
- Fix all slim errors if exist

Non-Unicode Encoding

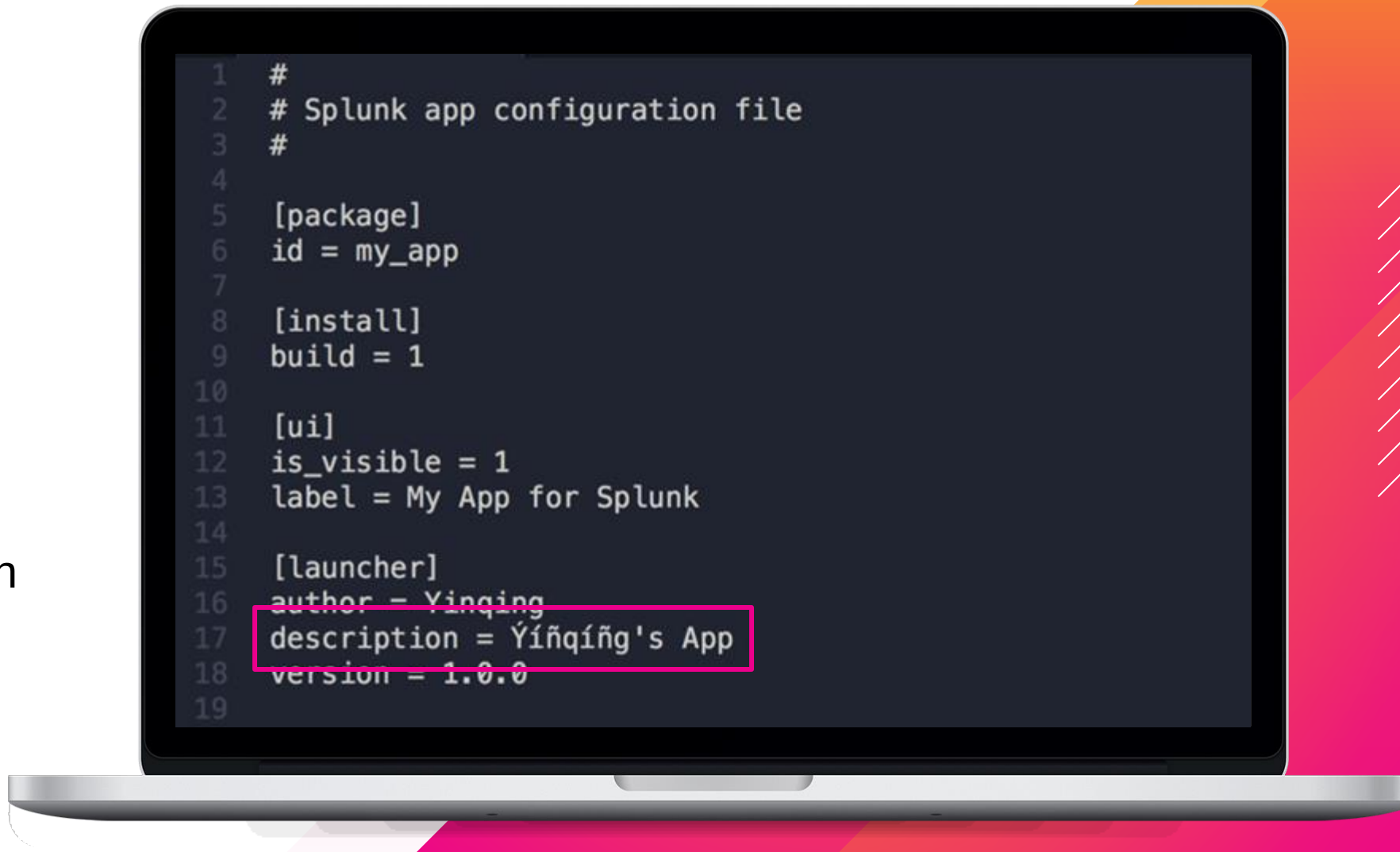
Cloud Incompatible

- Only Unicode encoding is allowed in Splunk app

Non-Unicode Encoding

Cause of Failure

The app contains files with unexpected encoding



Common Failures

Non-Unicode Encoding

Preventive Action

- Enable the encoding of unicode string in all app files

Confliction of Splunkbase and Custom App Id

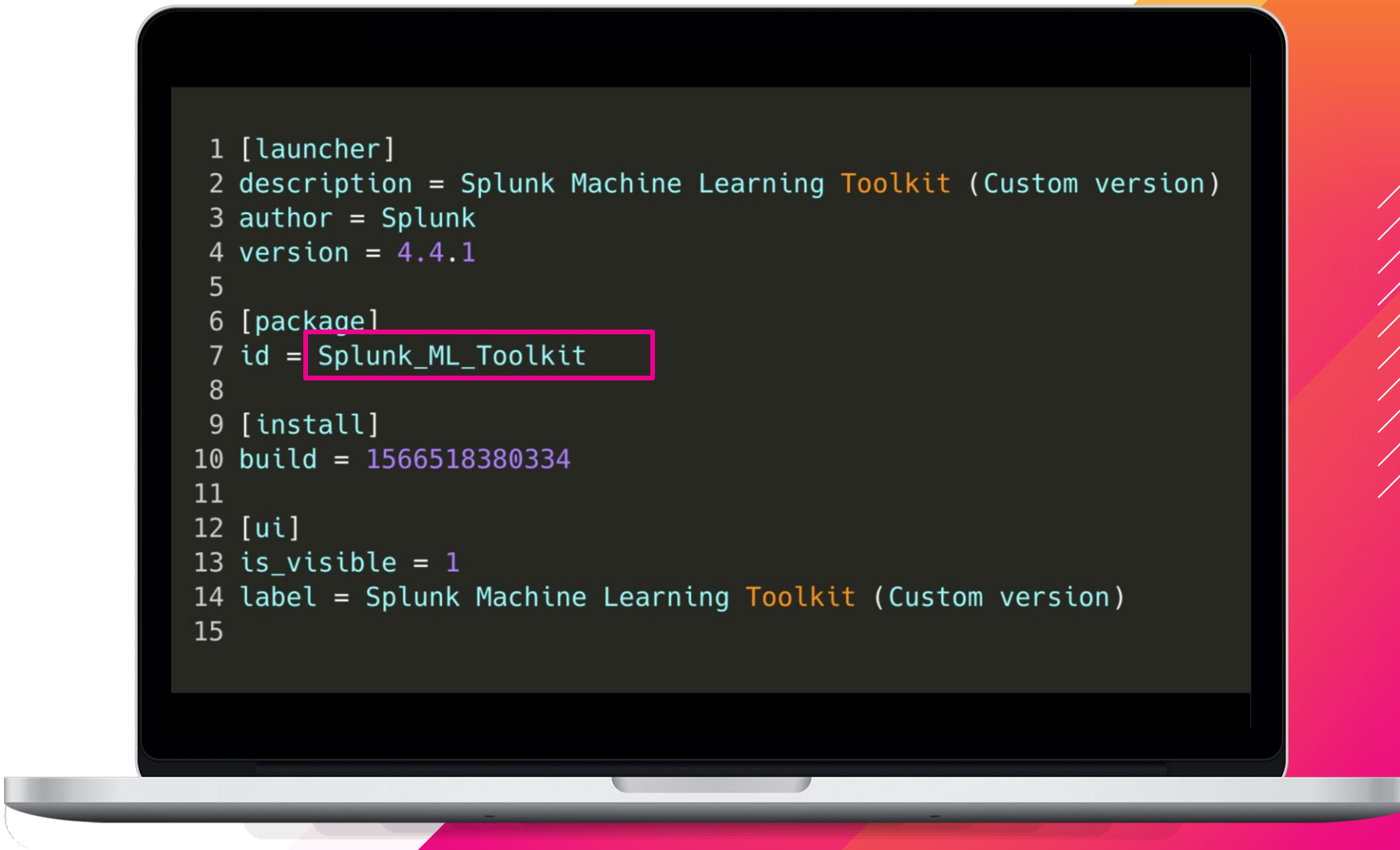
Cloud Incompatible

- Custom app ID should be different with the Splunkbase app ID

Confliction of Splunkbase and Custom App Id

Preventive Actions

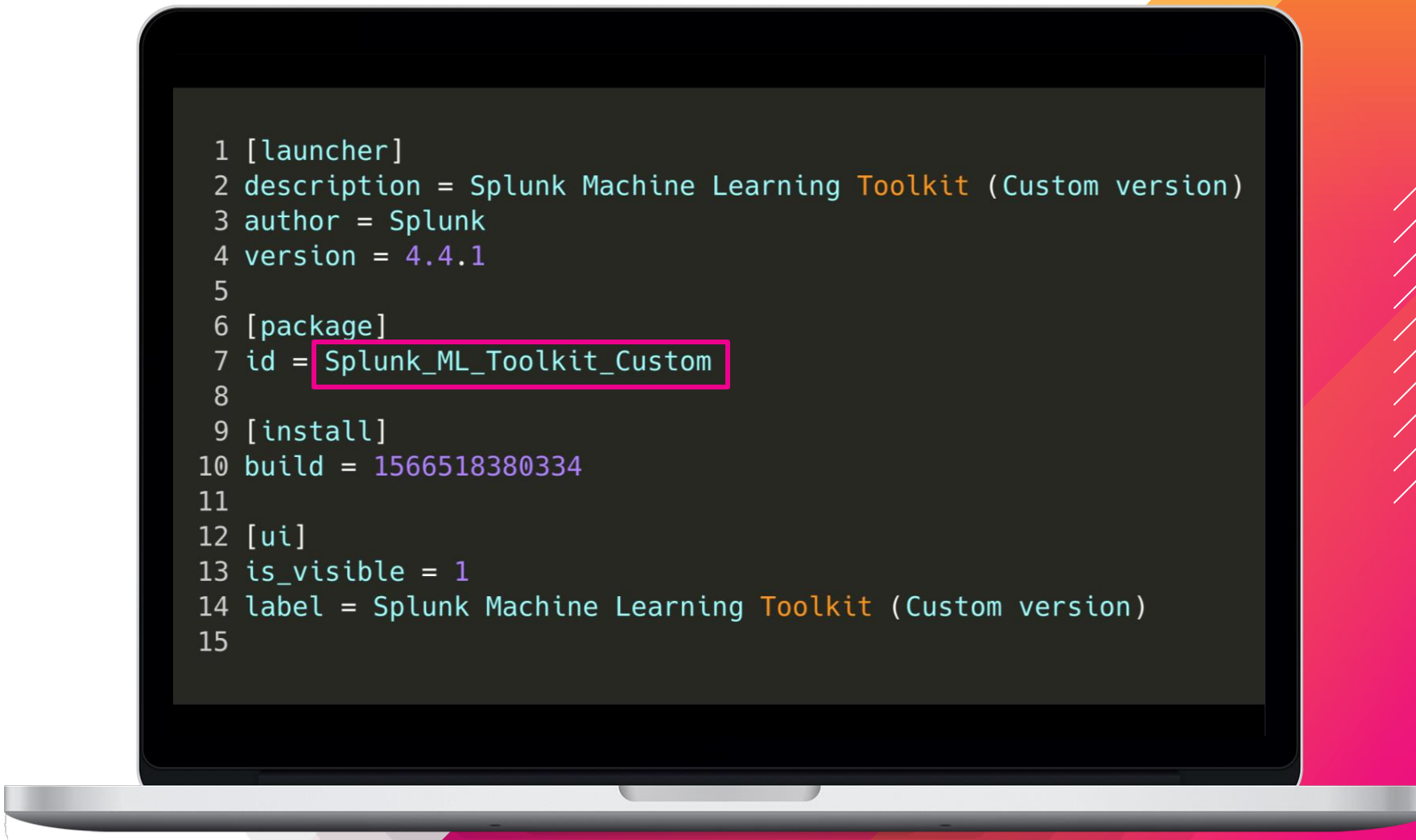
- The custom app id remain the same as the Splunkbase app
- It may cause issues when the custom app gets deployed on Splunk Cloud



Confliction of Splunkbase and Custom App Id

Preventive Actions

- Always modify the app id in the custom app
- App id format should be "customerName_ the_original_app_ID”
- Test the app functionality after modification in case the app id is hard-coded in the script



Insecure Network Communication

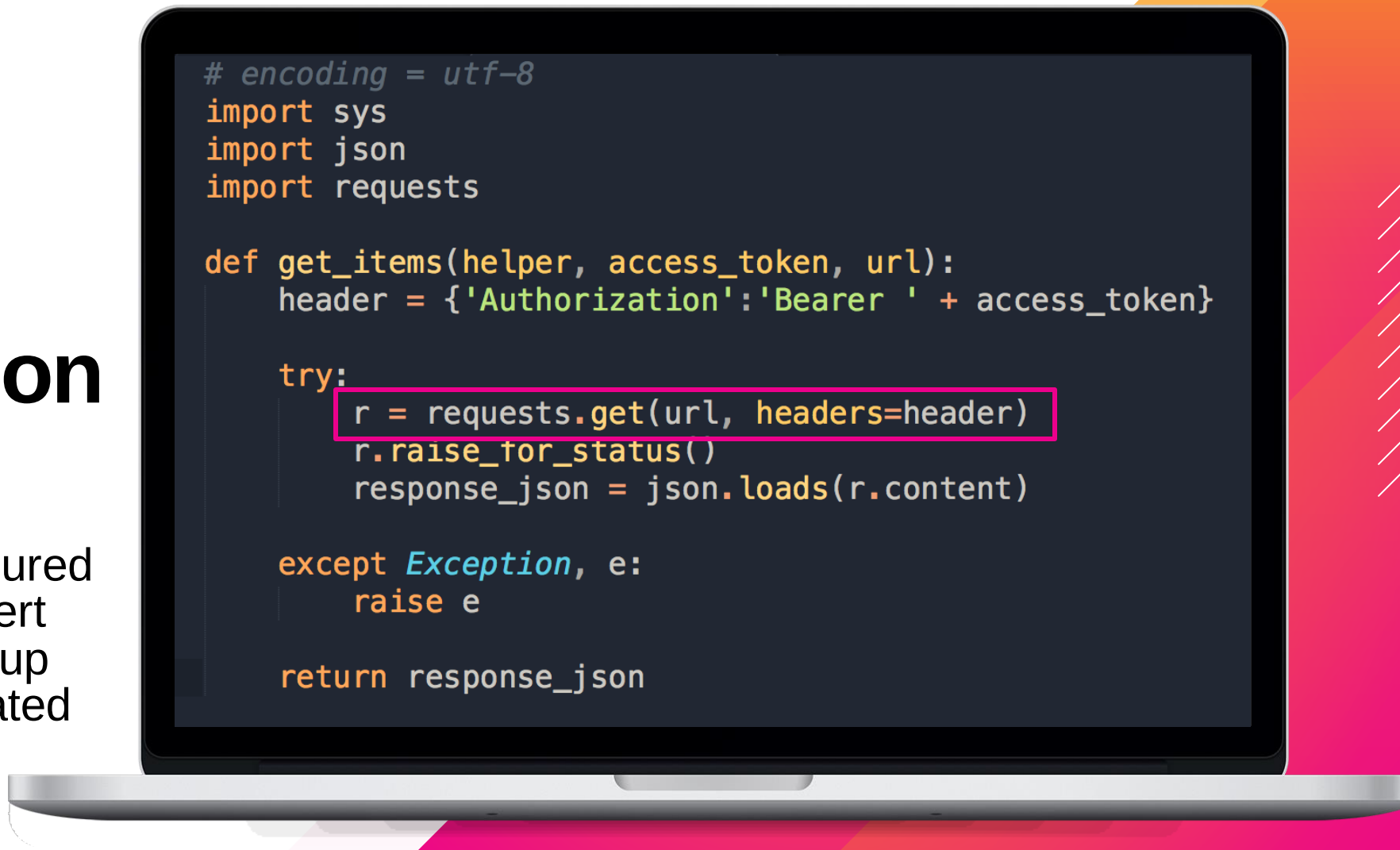
Cloud Incompatible

- All network communications must be encrypted on Splunk Cloud

Insecure Network Communication

Cause of Failure

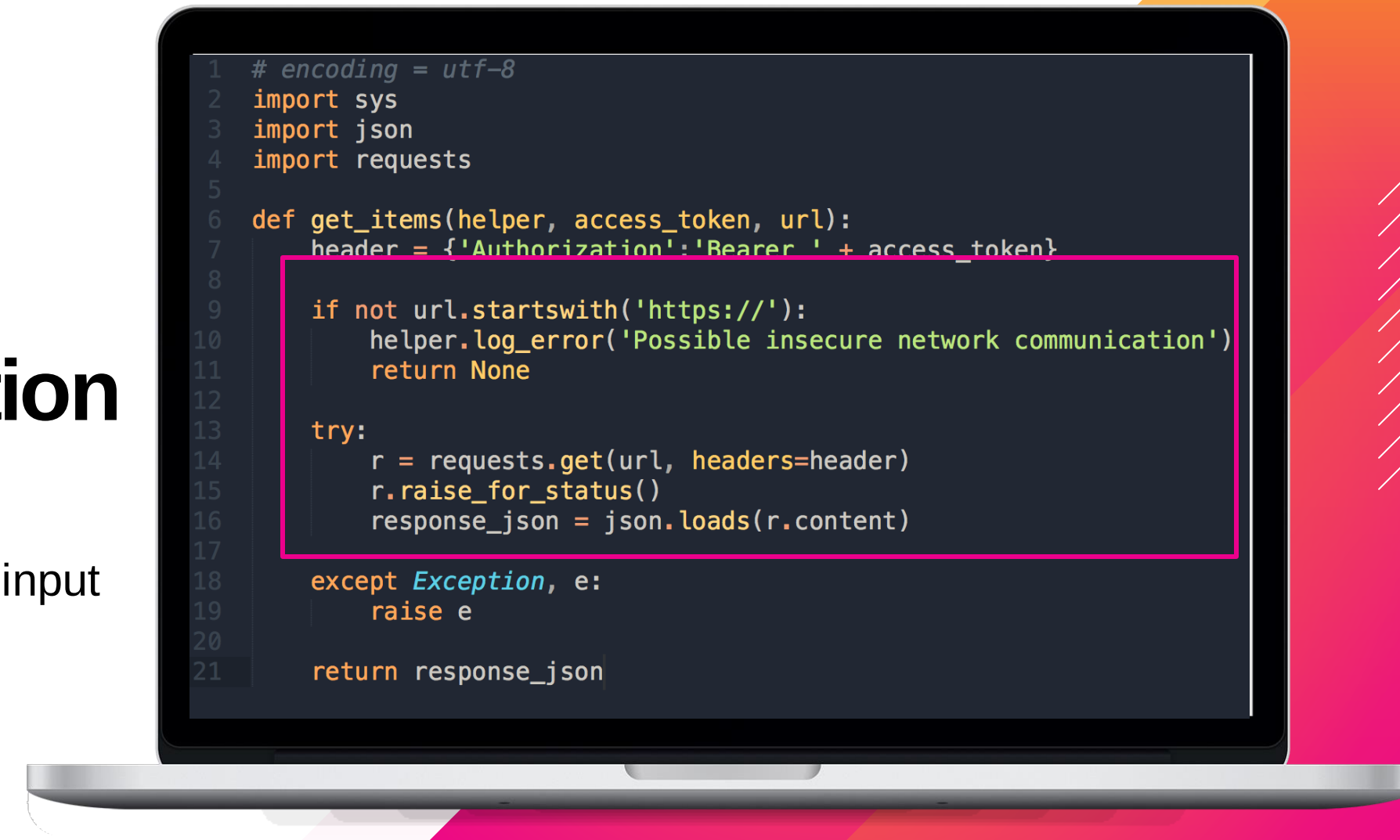
The http scheme is configured or hard-coded from the alert actions, data inputs or setup page, which is NOT validated



Insecure Network Communication

Preventative Actions

Always validate the user input and only accept https communications



Secret Disclosure

Cloud Incompatible

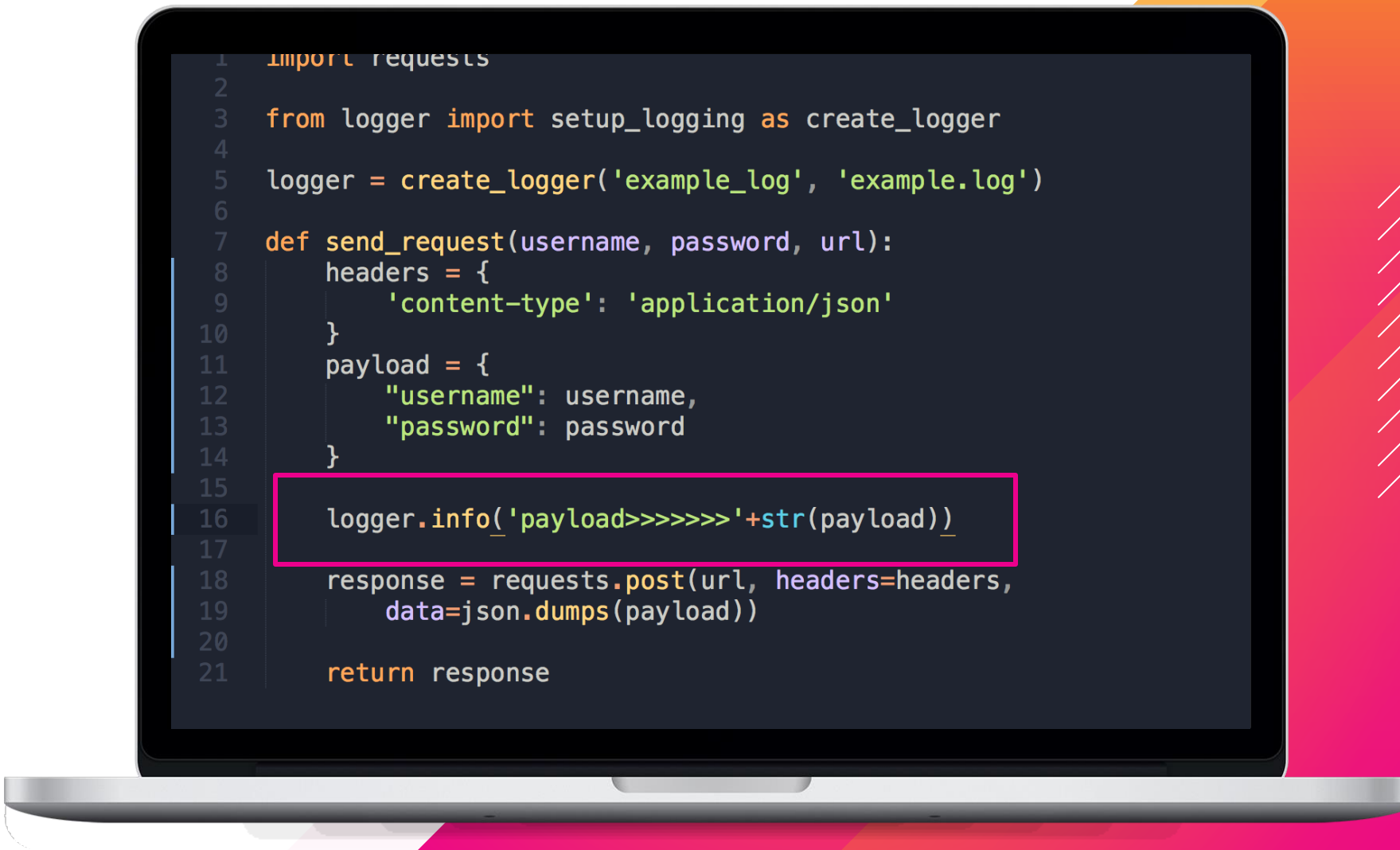
- All secrets must be encrypted all time and not even temporarily exposed

Secret Disclosure

Plain Text Secrets Storage in the Files

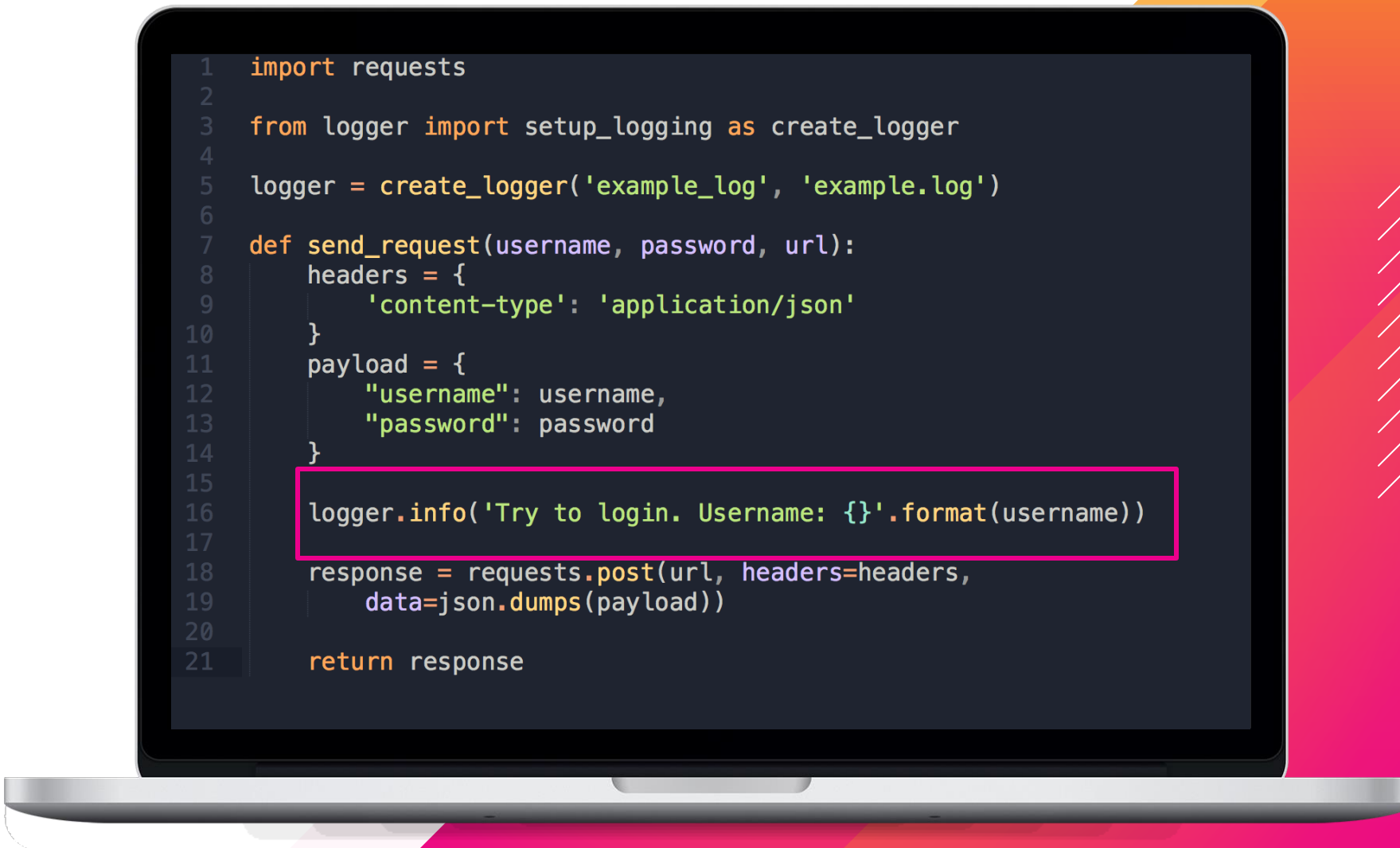
Cause of failure:

- API key, password, private key, token, splunk session key
- Save secrets to log files/conf files in plain text



Secret Disclosure

Plain Text Secrets Storage in the Files



Preventative actions:

- Avoid to save secrets to log files
- Use `storage/passwords` endpoint to save your credentials
- https://dev.splunk.com/enterprise/docs/python/sdk-python/howtousesplunkpython/howtoworkwithusersroles/

Out of Boundary

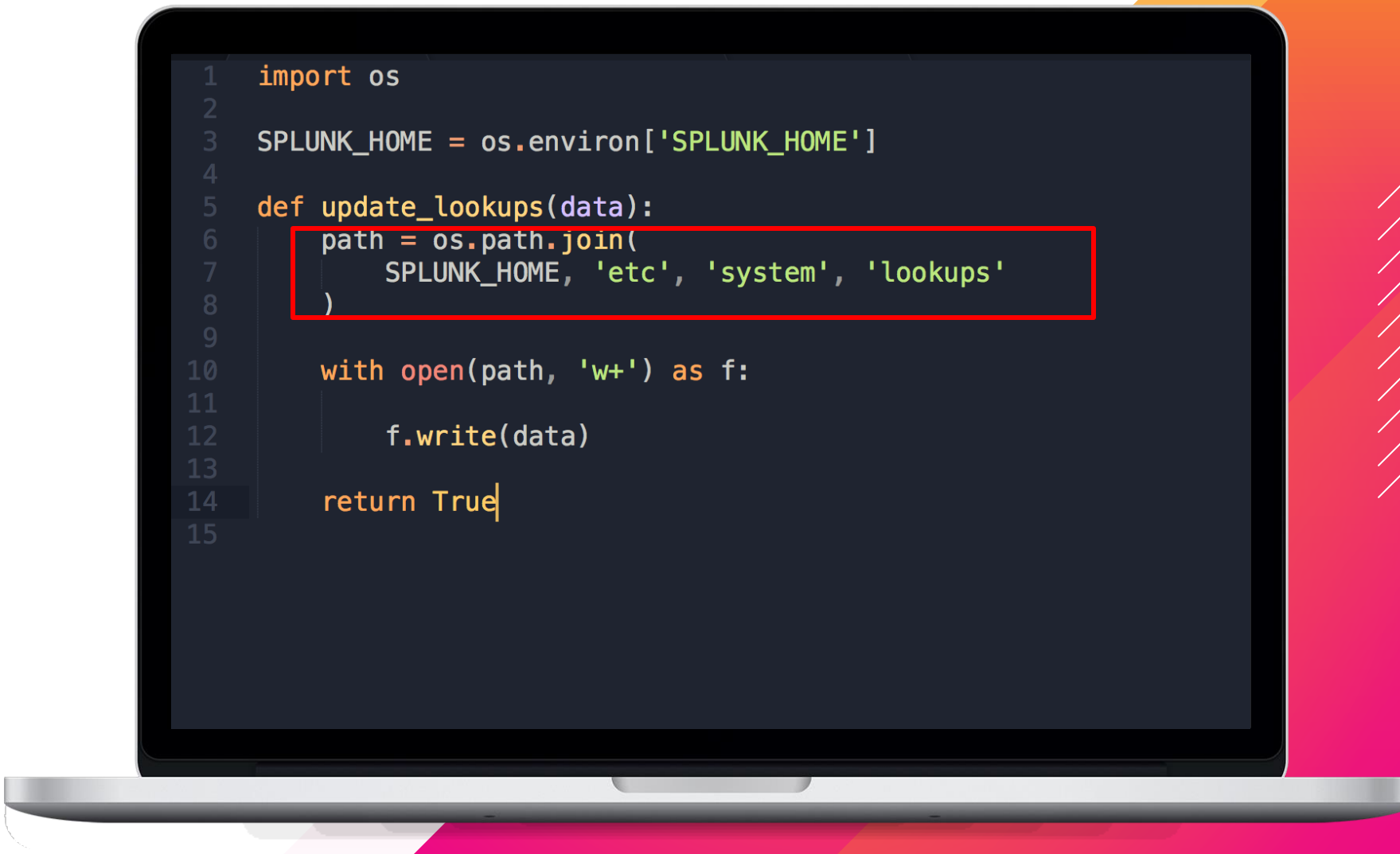
Cloud Incompatible

- Splunk app is only allowed to manipulate the files within the app container

Out of Boundary

Cause of Failure

The app manipulates files outside of the app's boundary



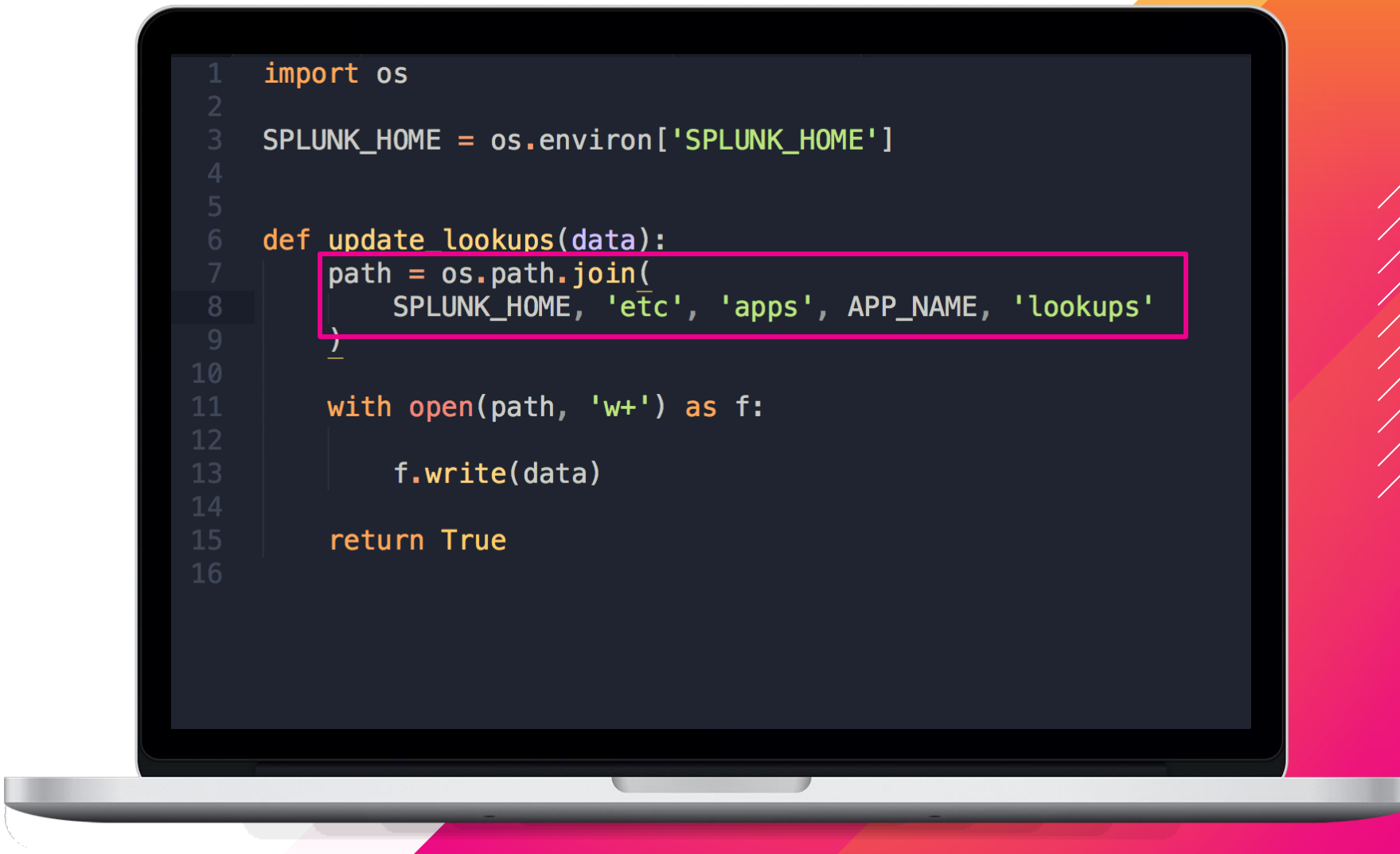
Out of Boundary

Cause of Failure

Make sure all file manipulations are limited inside the app's boundary, which includes the following paths:

$SPLUNK_HOME/etc/apps/<APP_NAME>

$SPLUNK_HOME/var/log/<APP_NAME>



Shell Injection Vulnerabilities

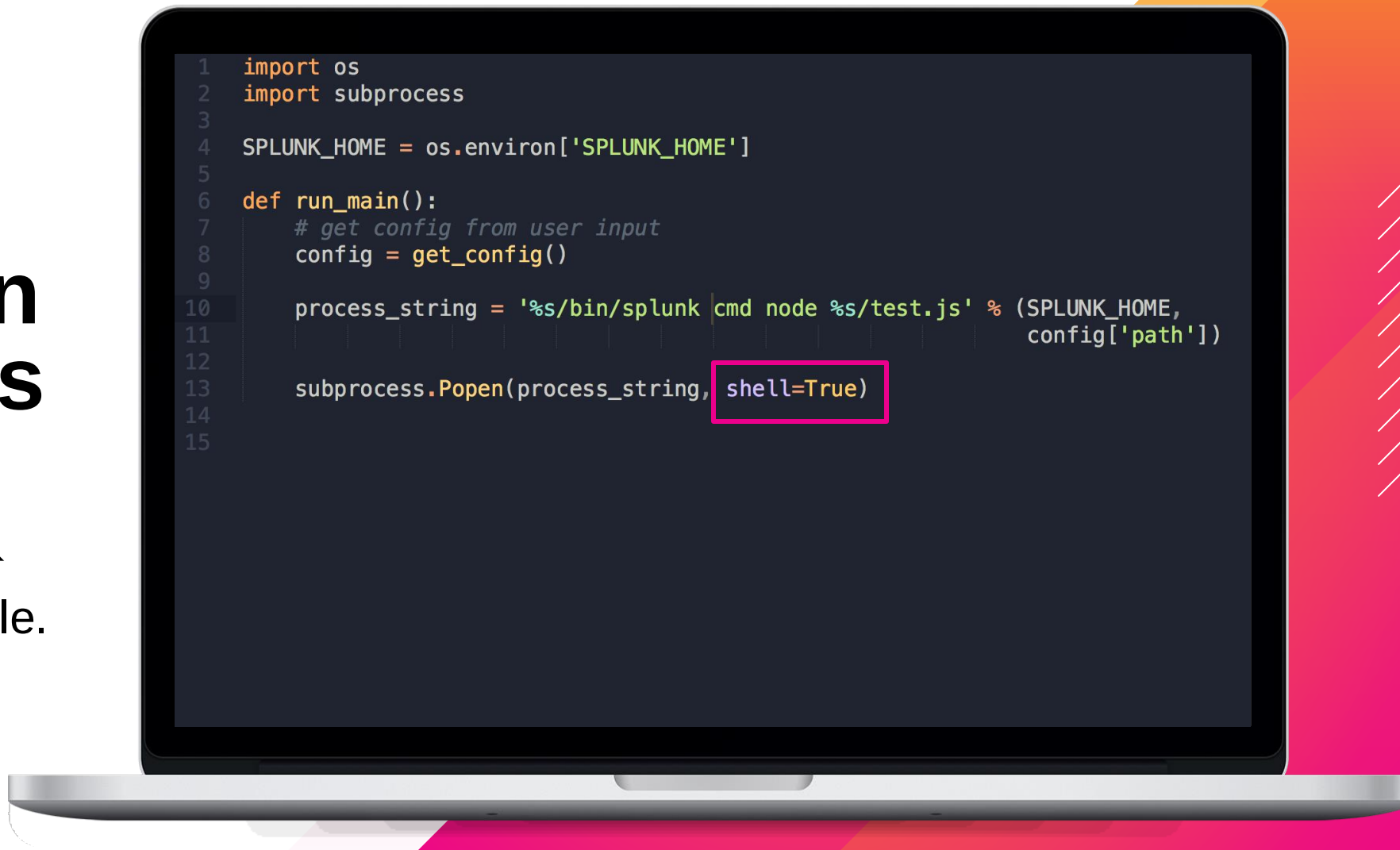
Cloud Incompatible

- Shell injection is a serious security flaw that should be avoided

Shell Injection Vulnerabilities

Cause of Failure

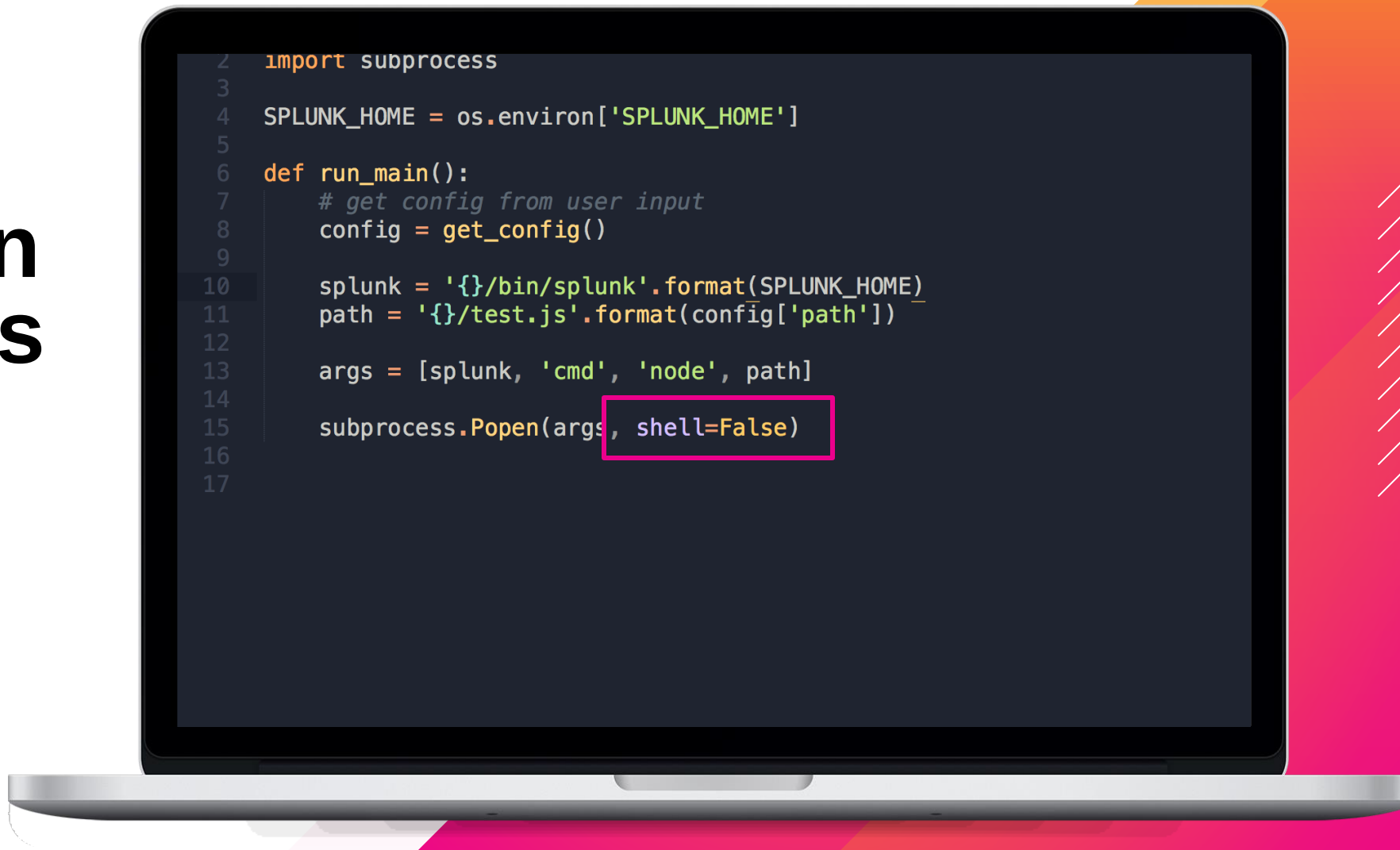
The use of `shell=True` in `subprocess` module.



Shell Injection Vulnerabilities

Preventative actions

Set `shell=False` to disables all shell based features and prevent the shell injections



Key Takeaways

1. Cloud Vetting makes your data safer
2. Use AppInspect and Packaging Toolkit to make your app more compliant with Splunk standards
3. Avoid the common failures and make your app better

Additional Links

Splunk Packaging Toolkit Documentation

- https://dev.splunk.com/enterprise/docs/releaseapps/packagingtoolkit/

Splunk AppInspect Documentation

- https://dev.splunk.com/enterprise/docs/releaseapps/appinspect/

Splunk Cloud app requirements and best practices

- https://dev.splunk.com/enterprise/docs/releaseapps/appinspect/cloudvettingguidelines/vetappsandaddons#Common-failures-and-preventive-actions

Storage/Passwords Tutorial

- https://dev.splunk.com/enterprise/docs/python/sdk-python/howtousesplunkpython/howtoworkwithusersroles/

Types of Splunk Cloud

- https://docs.splunk.com/Documentation/SplunkCloud/latest/User/TypesofSplunkClouddeployment

Contact

Contact Splunk Application Health Team

- appinspect@splunk.com

Contact Splunk Cloud SRE Team

- cloud-apps-SRE@splunk.com

Slack channel

- https://splunk-usergroups.slack.com/messages/CF5QNJAJX

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION

Q&A

Samuel Ni | Principal Software Engineer
Yinqing Hao | Software Engineer

splunk> .conf19